

Micro Focus Security

ArcSight ESM

CIP for HIPAA

Software Version: 3.0

Solutions Guide

Document Release Date: June, 2018

Software Release Date: June, 2018



Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2018 Micro Focus or one of its affiliates.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs

Contents

Chapter 1: CIP for HIPAA Overview & Architecture	6
Compliance Insight Package for HIPAA	7
Overview Dashboards	8
Notify, Investigate, Analyze, and Remediate	12
Solution for CIP for HIPAA Device Coverage	12
Chapter 2: Solution Installation and Configuration	13
Prepare for Installation	13
Prepare Environment	13
Verify Environment	13
Install Solution for HIPAA CIP	15
Assign User Permissions	17
Configure CIP for HIPAA Solution	18
Model Assets (Assign Asset Categories)	20
CIP for HIPAA Categorization	20
Categorizing Assets and Zones	21
Configure Active Lists	22
Configure Active Lists Using Console Active List Editor	25
Configure Active Lists by Importing a CSV File	25
Configure My Filters	26
After Hours Filter	26
Intellectual Property Download Filter	27
Limit Regulation Filter	27
Deploy the CIP for HIPAA Rules	27
Enable Data Monitors	29
Enable and Test Trends	29
Configure Cases	30
Configure Notifications	34
Configure Additional Resources	35
Build FlexConnector(s) for Physical Access Devices	35
Appendix A: CIP for HIPAA Resource Reference	37
Security Management Process 164.308 (a)(1)	38
Workforce Security 164.308 (a)(3)	64

Information Access Management 164.308 (a)(4)	74
Security Awareness and Training 164.308 (a)(5)	87
Security Incident Procedures 164.308 (a)(6)	108
Contingency Plan 164.308 (a)(7)	117
Evaluation 164.308 (a)(8)	122
Business Associate Contracts and Other Arrangements 164.308 (b)(1)	135
Facility Access Controls 164.310 (a)(1)	146
Device and Media Controls 164.310 (d)(1)	150
Workstation Use 164.310 (b)	151
Access Control 164.312 (a)(1)	153
Audit Controls 164.312 (b)	165
Integrity 164.312 (c)(1)	171
Person or Entity Authentication 164.312 (d)	173
Transmission Security 164.312 (e)(1)	177
Active Lists	197
Filters	199
My Filters	199
General Filters	201
Authentication Filters	203
Firewall Filters	204
Overview Filters	204
Ports Filter	205
Vulnerabilities Filters	206
Overview Dashboards	206
Overview Data Monitors	207
Field Sets	208
Overview Rules	209
Appendix B: Asset and Zone Categories	210
Appendix C: Active Lists Requiring Configuration	217
Appendix D: Resources Requiring Enabled Trends	220
Appendix E: CIP for HIPAA Use Cases	223

Appendix F: Compare, Backup and Uninstall Package	245
Generate a List of Resource Changes	245
Back Up the Solution Package	246
Uninstall the CIP for HIPAA	247
Send Documentation Feedback	248

Chapter 1: CIP for HIPAA Overview & Architecture

This chapter contains an overview of the Compliance Insight Package for HIPAA (CIP for HIPAA) and contains the following topics:

• Compliance Insight Package for HIPAA	7
• Overview Dashboards	8
• Notify, Investigate, Analyze, and Remediate	12
• Solution for CIP for HIPAA Device Coverage	12

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was enacted by the United States Congress. Title II of HIPAA has standardized the way electronic health care information is transmitted among providers and insurers to ensure confidentiality and privacy of protected health information (PHI).

All healthcare entities and organizations that use, store, maintain, or transmit patient health information are expected to be in complete compliance with the regulations of HIPAA law. To protect this Protected Healthcare Information (PHI), HIPAA Title II defines the following rules:

- The Privacy Rule—This rule establishes national standards for protecting the privacy of healthcare information of individuals.
- The Security Rule—This rule specifies that covered entities (such as health insurers, hospitals, medical providers) put appropriate safeguards in place to protect the Electronic Protected Healthcare Information (EPHI).

The Security Rule is broken down into 3 major sections:

- Administrative Safeguards § 164.308 are a special subset of the HIPAA Security Rule that focus on internal organization, policies, procedures, and maintenance of security measures that protect patient health information.
- Physical Safeguards § 164.310 : are a special set of HIPAA Security Rule that focus on physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
- Technical Safeguards § 164.312 : are a special set of HIPAA Security Rule that focus on technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Compliance Insight Package for HIPAA

The CIP for HIPAA provides ArcSight ESM resources that can assist with compliance to the three major sections of the Security Rule Safeguards.

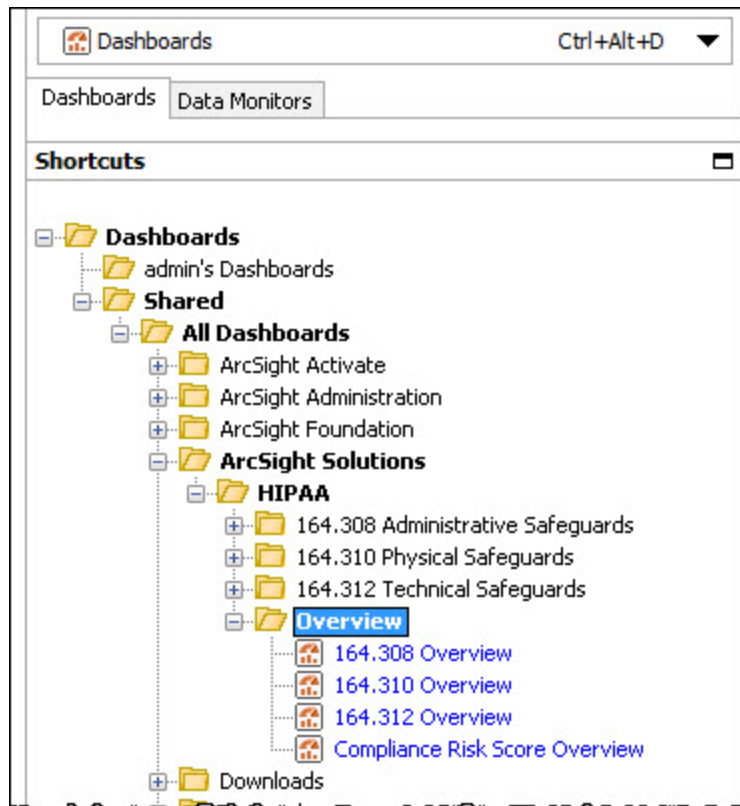
The ESM resources address the following objectives:

- **Compliance reporting**—supports the presentation of requirements to internal and external audit teams, as well as upper management.
- **Real-time detection of compliance breaches**—Pro-actively addresses compliance violations.
- **Security best practices**—Due diligence in complying with HIPAA standards, as well as security policies and best practices.
- **Automation of Monitoring-IT control**—CIP for HIPAA follows and adapts to changes in the IT environment. More than 60 correlation rules can be used to monitor policy compliance violations in real-time.
- **Harmful User and Machine Monitoring**—Tracks potentially harmful users and machines.
- **Visualizing Security Events** — Displaying security events graphically which allows analysts to quickly analyze situations
- **Vulnerabilities and Configuration Changes Monitoring** — Tracking vulnerabilities and configuration changes

In addition to the resources supplied to help address specific HIPAA Safeguard Subsections, there are a common set of filters and active lists that support the entire solution. These common resources are described in ["Solution Installation and Configuration" on page 13](#). These resources require configuration to tailor the content for your environment, such as privileged account names or the working hours in your organization.

Overview Dashboards

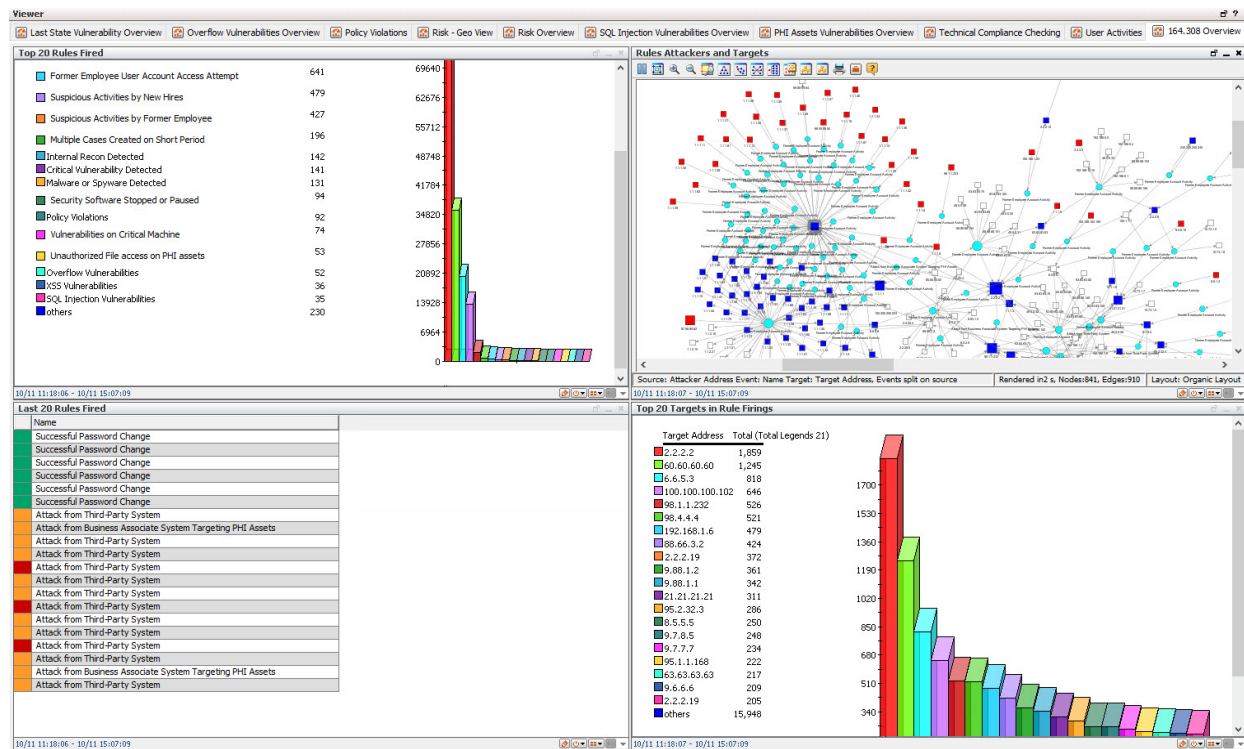
Overview dashboards summarize the compliance state determined by correlation rules for each HIPAA Safeguard. The overview dashboards are available from the HIPAA/Overview group as shown in the following figure.



Each dashboard presents:

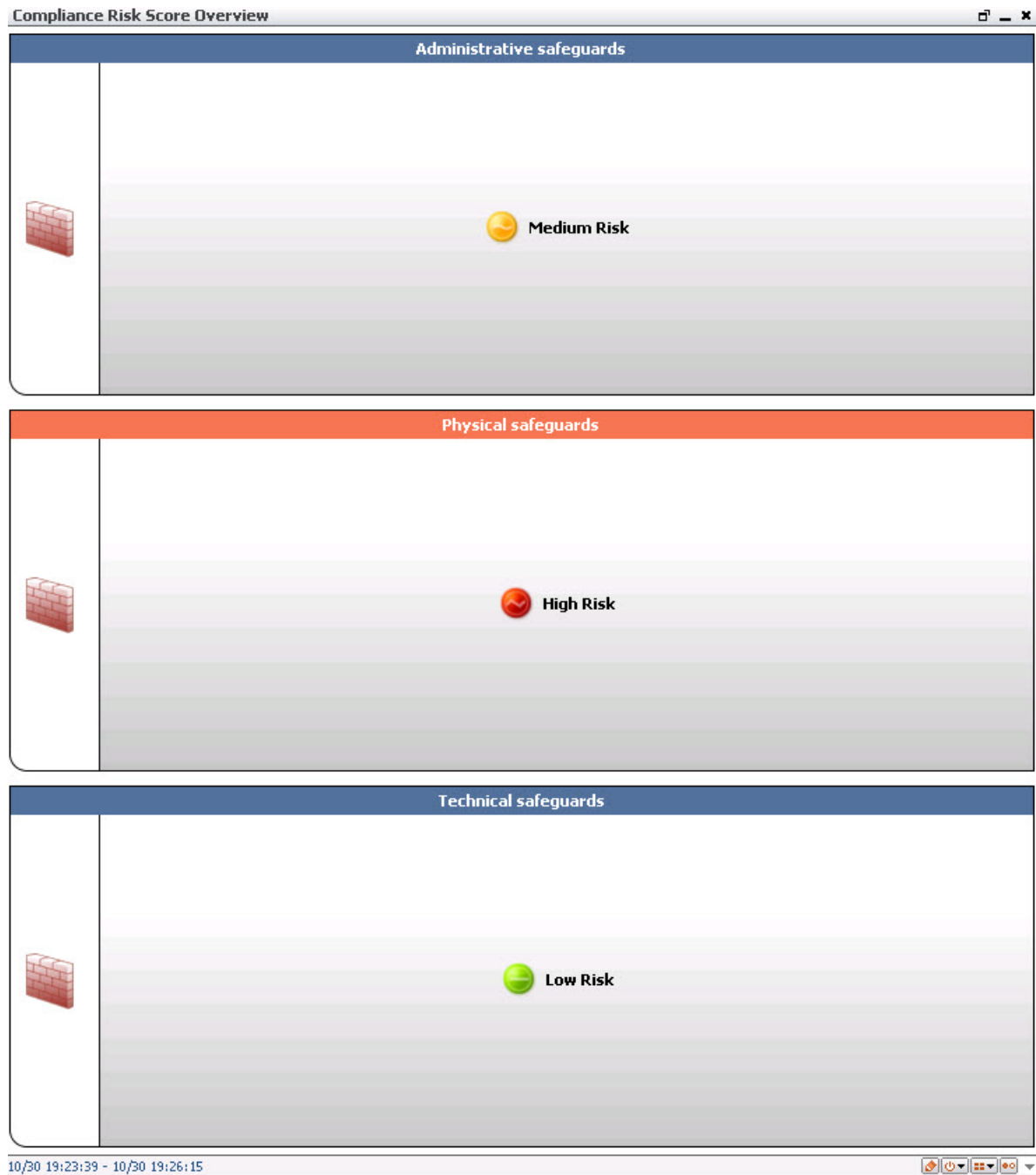
- An event graph to show the relationships of the non-compliant systems with other systems on the network
- A list of the last 20 triggered rules
- A pie chart that breaks down the percentage of each triggered rule
- A bar chart that shows the top 20 targets of the triggered rules

The following figure shows the 164.308 Overview dashboard:






The Compliance Risk Score Overview dashboard (/All Dashboards/ArcSight Solutions/HIPAA/Overview/) is a centralized heads-up display that shows the current state of compliance for each of the HIPAA Section by displaying the results of Compliance Risk Score Overview last-state data monitor (/All Data Monitors/ArcSight Solutions/HIPAA/Overview/). The dashboard summarizes your environment's overall state of compliance with the HIPAA Safeguards Sections as determined by correlation rules triggered for each family.

The following figure shows the Compliance Risk Score Overview dashboard:





The dashboard is populated when a possible violation or an actual violation occurs. A yellow or red data monitor can be turned to green manually when the situation is remedied by right-clicking the data monitor and selecting **Override Status**.

The colors of the traffic lights indicate the current state as described in the following table:

Color	State	Description
Red 	Violation	This situation occurs when one or more rules are triggered by event activity that violates compliance for this HIPAA Security rule section.
Yellow 	Possible Violation	This situation occurs when one or more marginal events occur that could indicate a policy problem, or is a borderline compliance violation.
Green 	Compliant	Systems are considered compliant when any events related to this HIPAA Safeguard remain under the threshold of Yellow.

Notify, Investigate, Analyze, and Remediate

Once a security or compliance-related activity is identified, CIP for HIPAA 3.0 offers the following ways to take action, investigate, and analyze:

- **Notifications** () The first step in any escalation process is to notify the right people of a potential problem. You can configure the rules included in CIP for HIPAA 3.0 to activate your notification hierarchy in case of certain threats. You can configure this hierarchy to notify the right groups in the right situations. For more information, see ["Configure Notifications " on page 34.](#)
- **Cases** () are ArcSight's built-in trouble-ticket system. When certain compliance-related conditions occur, the CIP for HIPAA can be configured to open a case to track an issue so it can be investigated and properly remediated. For more information, see ["Configure Cases" on page 30.](#)

Solution for CIP for HIPAA Device Coverage

CIP for HIPAA leverages event feeds from multiple sources. For a list of devices that are capable of generating events to populate the CIP for HIPAA reports and other resources, see ["CIP for HIPAA Use Cases" on page 223.](#)

To gather events from physical access devices, such as badge readers, you must build a FlexConnector tailored to the type of physical access device you use. For instructions about how to build and configure a FlexConnector for a physical access device, see ["Build FlexConnector\(s\) for Physical Access Devices" on page 35.](#)

Chapter 2: Solution Installation and Configuration

This chapter contains information on installing and configuring the Compliance Insight Package for HIPAA 3.0 (CIP for HIPAA).

Prepare for Installation

Before installing CIP for HIPAA, complete the following preparation tasks:

1. ["Prepare Environment" below](#)
2. ["Verify Environment" below](#)

Prepare Environment

Before installing, prepare your environment for the CIP for HIPAA:

1. Install and configure the appropriate SmartConnectors for the devices found in your environment.

Note: The devices that provide events for the CIP for HIPAA reports are listed in ["CIP for HIPAA Use Cases" on page 223](#).

2. Model your network to include devices that supply events that help satisfy the HIPAA standards. Verify that zones and networks are defined for your environment and that networks are assigned to the connectors reporting HIPAA-relevant events into your ArcSight Manager. Learn more about the ArcSight network modeling process in *ArcSight ESM 101*. Find instructions for how to configure zones and networks in the *ArcSight Console User's Guide* or the *ArcSight Console User's Guide* online help.

Note: RFC 1918 addresses(10.x.x.x, 192.168.x.x, 172.16-31.x.x) are automatically categorized as protected because their zones already are categorized as protected.

Verify Environment

Before installing, verify your ArcSight ESM installation. Compliance Insight Package for HIPAA is supported on ArcSight ESM expect this to be 6.9.1 or later. Refer to the [ESM Support Matrix](#) for operating system requirements. Refer also to the applicable release notes.

Verify that your system has the supported ArcSight Console connected to the Manager.

Note: CIP for HIPAA is a self-contained solution that does not rely on any other ArcSight solution. You can install CIP for HIPAA alongside other solutions on the same ArcSight Manager. Before installing new solutions, Micro Focus recommends that you back up any existing solutions installed on the Manager. For detailed instructions, see ["Compare, Backup and Uninstall Package" on page 245](#).

Updating from CIP for HIPAA 2.0 to CIP for HIPAA 3.0 requires :

1. Back up the old solution installed on the Manager, see ["Compare, Backup and Uninstall Package" on page 245](#).
2. Uninstall CIP for HIPAA 2.0.
3. Install CIP for HIPAA 3.0.

Install Solution for HIPAA CIP

The solution is supplied in a single ArcSight package bundle file called ArcSight-ComplianceInsightPackage-HIPAA.3.0.<nnnn>.arb, where <nnnn> is the 4 character build number.


To install the CIP for HIPAA package:

1. Using the login credentials supplied to you, download the CIP for HIPAA bundle from the software download site to the machine where you plan to launch the ArcSight Console:

ArcSight-ComplianceInsightPackage-HIPAA.3.0<nnnn>.arb

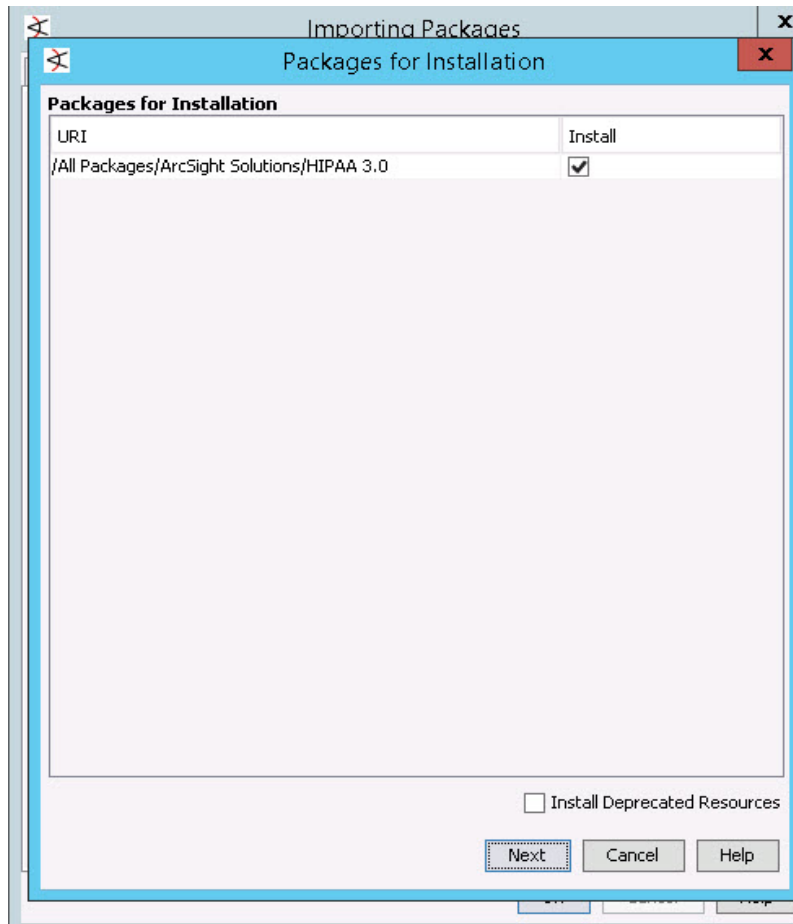
Where <nnnn> is the 4 character build number. (The exact build number is specified in the *ESM CIP for HIPAA Release Notes*.)

Caution: If you use Internet Explorer to download the ARB file, it may convert the ARB file to a ZIP file. If this occurs, rename the ZIP file back to an ARB file before importing.

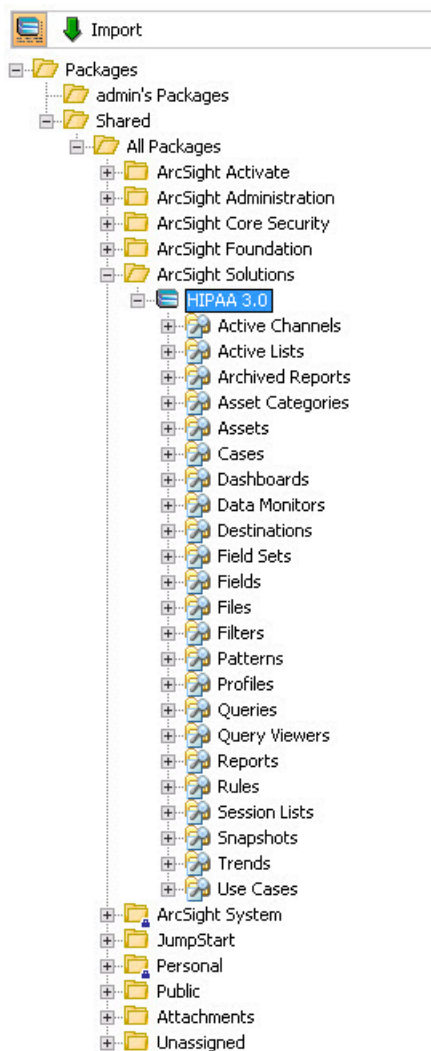
2. Log into the ArcSight Console as an ArcSight Administrator.
3. Click the **Packages** tab in the Navigator panel.
4. Click **Import** .
5. In the Open dialog, browse and select the package bundle file and select **Open**.

The progress of the import of the package bundle is displayed in the Progress tab of the Importing Packages dialog.

When the import is complete, the Results tab of the Importing Packages dialog is displayed as well as the Packages for Installation dialog as shown in the following figure.



6. Leave the HIPAA 3.0 checkbox selected and in the Packages for Installation dialog, click **Next**.
The progress of the install is displayed in the Progress tab of the Installing Packages dialog. When the install is complete, the Results tab of the Installing Packages dialog displays the Summary Report.
7. In the Installing Packages dialog, click **OK**.
8. In the Importing Packages dialog, click **OK**.
9. To verify that the installation was successful and the content is accessible in the Navigator panel, expand the ArcSight Solutions/HIPAA 3.0 group.



Assign User Permissions

By default, users in the Default user group can view CIP for HIPAA content, and users in the ArcSight Administrators and Analyzer Administrators user groups have read and write access to the solution content. Depending on how you have set up user access controls within your organization, you may need to adjust those controls to make sure the new content is accessible to the right users in your organization.

The following process assumes that you have user groups set up and users assigned to them.

In the following procedure, assign user permissions to all the following resource types:

- Active channels
- Active lists
- Cases

- Dashboards
- Data monitors
- Field Sets
- Filters
- Queries
- Reports
- Rules
- Session Lists
- Trends

To assign user permissions:

1. Log into the Console as ArcSight Administrator.
2. For all the resource types listed above, change the user permissions:
 - a. In the Navigator panel, go to the resource type and navigate to ArcSight Solutions/HIPAA.
 - b. Right-click the **HIPAA** group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
 - c. In the ACL editor in the Inspect/Edit panel, select which user groups you want to have permissions to the CIP for HIPAA resources and click **OK**.

Configure CIP for HIPAA Solution

Several of the CIP for HIPAA resources should be configured with values specific to your environment. Some features also require some additional SmartConnector configuration. This section describes these configuration processes.

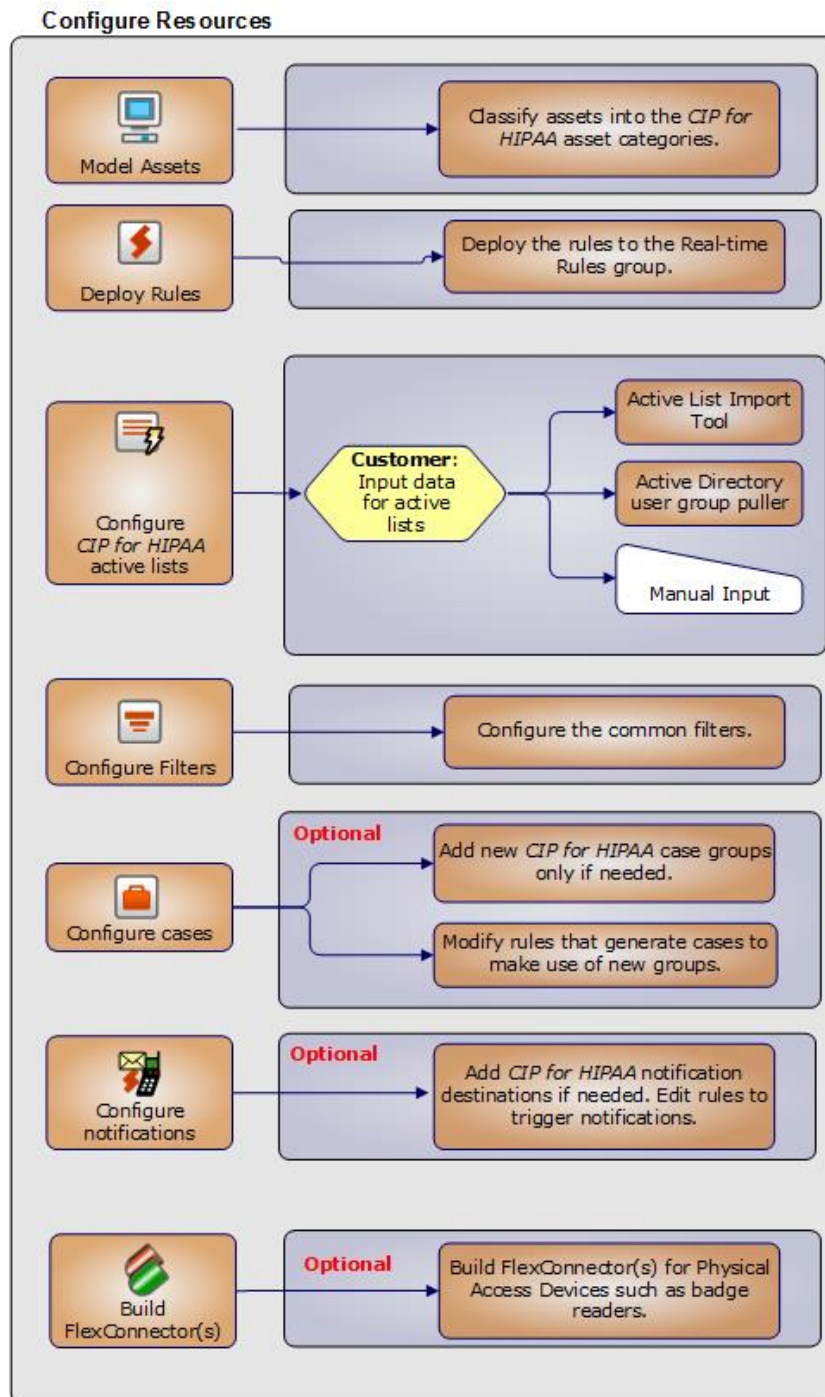
Depending on the features you want to implement and how your network is set up, some configuration is required and some are optional. The list below shows all the configuration tasks involved with the CIP for HIPAA and where to find instructions for performing the configuration.

This section contains the instructions required to enable content for the CIP for HIPAA and contains the following topics:

- ["Model Assets \(Assign Asset Categories\)" on page 20](#)
- ["Configure Active Lists" on page 22](#)
- ["Configure My Filters" on page 26](#)
- ["Deploy the CIP for HIPAA Rules" on page 27](#)
- ["Configure Cases" on page 30](#)

- ["Configure Notifications " on page 34](#)
- ["Configure Additional Resources" on page 35](#)

The configuration processes outlined in this section (shown in the following figure) apply to resources that feed the CIP for HIPAA.



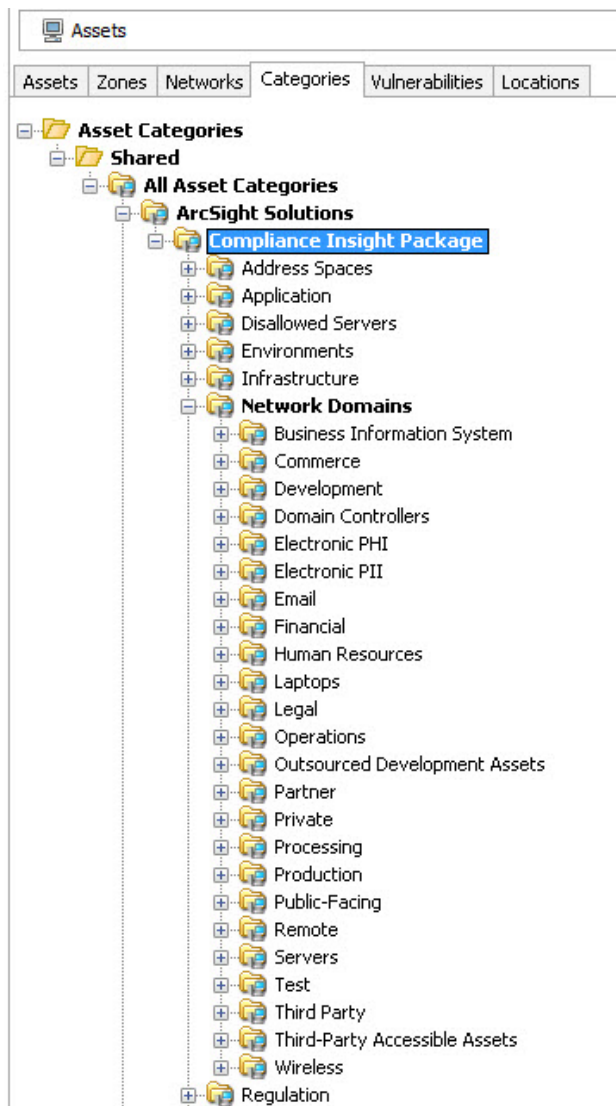
Model Assets (Assign Asset Categories)

Asset modeling is essential to enable *CIP for HIPAA* content. Classifying assets in one or more of the solution asset categories is essential for the following reasons:

- Some of the *CIP for HIPAA* content requires assets to be modeled in order to function correctly.
- In some cases, modeling assets adds valuable business context to the events evaluated by the *CIP for HIPAA*.

CIP for HIPAA Categorization

CIP for HIPAA uses the asset categories under the /ArcSight Solutions/Compliance Insight Package/ group shown below.



Categorizing Assets and Zones

CIP for HIPAA solution relies on ArcSight asset and zone categorization to define your environment. Certain content does not display unless assets or zones are categorized.

- For detailed information about which assets need to be categorized for each resource, refer to ["CIP for HIPAA Resource Reference" on page 37](#).
- For a list of all the asset and zone categorization used and the filters which use those categorizations, see ["Asset and Zone Categories" on page 210](#).

You can assign the solution asset categories with the following methods:

One-by-one using the ArcSight Console

Use this method if you have only a few assets to categorize. One asset can be categorized in more than one asset category. To categorize your assets one-by-one:

1. In the Navigator panel, go to **Assets** and select the **Assets** tab.
2. On the **Asset** tab, expand the groups listed.
3. For each asset you want to classify with an asset category, repeat the following steps:
 - a. Right-click the asset you want to categorize and select **Edit Asset**.
 - b. In the Inspect/Edit panel, click the **Categories** tab. Click the add icon (+) at the top of the screen to select new resources.
 - c. In the Asset Categories Selector pop-up window, navigate to the appropriate network domain category and click **OK**.

After you assign your assets to the CIP asset categories, you can also assign them to other asset categories, either within the solution package or the general ArcSight categories, or those you have created yourself.

Using the Network Model Wizard

A Network Model wizard is provided on the ArcSight Console (menu option **Tools > Network Model**). The Network Model wizard enables you to quickly populate the ESM network model by batch loading asset and zone information from comma-separated value (CSV) files. For more information, see the ArcSight Console User's Guide.

Using the ArcSight Asset Import File Connector

If you have many assets that you want to track, you can configure them in a batch using the ArcSight Asset Import File Connector. This connector can also create new assets as part of the batch function. The ArcSight Asset Import File Connector is available as part of the ArcSight SmartConnector download. For instructions on how to use this connector to configure your assets for CIP HIPAA, see the *ArcSight Asset Import File SmartConnector Configuration Guide*.

Configure Active Lists

CIP for HIPAA contains numerous active lists that retain specific data that is cross-referenced dynamically during run-time by ArcSight resources that use conditions, such as filters, rules, and reports.

You can populate the HIPAA active lists using any of the following processes:

- Add entries to active lists, one-by-one, using the Active List editor in the ArcSight Console. For detailed instructions, see ["Configure Active Lists Using Console Active List Editor" on page 25](#). This method can be used to populate active lists with one, two, or more columns.
- Add entries in batch to active list from a comma separated value (CSV) file. For detailed instructions see ["Configure Active Lists by Importing a CSV File" on page 25](#). This method can be used to populate active lists with one, two, or more columns.

[Active Lists Requiring Configuration](#) defines the active lists that require configuration for the CIP for HIPAA. Some active lists are intended to be populated by rules. For a complete listing (with descriptions) of all active lists provided with CIP for HIPAA, see ["Active Lists" on page 197](#).

Active Lists that Require Configuration

Active List	Description	Expected Input Per Entry
Administrative Accounts List	<p>This active list should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the content pack, but the list can also be added to or referenced in new content built around the provided infrastructure.</p> <p>This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in all lower case. For example, the user Administrator should be added as "administrator".</p>	<p>User name, in lowercase.</p>
Allowed Ports	<p>This active list contains all permissible destination ports (all permissible services). This active list should be populated according to your site policy.</p> <p>By default, all connection types and ports are allowed. To be considered a disallowed port, the connection type and port number must either be specified explicitly in the <code>Disallowed Ports</code> active list, or not specified in the <code>Allowed Ports</code> active list. If all ports are specified in the <code>Allowed Ports</code> active list (using the * character), the policy allows all ports (except those specified explicitly in the <code>Disallowed Ports</code> active list). Explicit (that is, not *) port entries in the <code>Disallowed Ports</code> active list always take precedence over entries in the <code>Allowed Ports</code> active list.</p>	<p>Connection type and port number Where Connection type could be: Inbound, outbound or internal</p>
Badges to Accounts	<p>This list contains the computer account and employee type for every physical device badge.</p>	<p>Badge ID, primary computer account for the badgeholder, and the employee type (in lowercase). Specifically, ensure that contractors are identified with the word "Contractor" (case insensitive) in the employee type field.</p>
Default Vendor Accounts	<p>This active list contains the default user account names for various vendors. This list should be configured at set-up time with existing vendor user account names, and updated as necessary on an ongoing basis.</p>	<p>Default user account and vendor name, in lowercase.</p>

Active Lists that Require Configuration, continued

Active List	Description	Expected Input Per Entry
Disallowed Ports	<p>This active list contains all disallowed destination ports. This active list should be populated according to your site policy.</p> <p>By default, all connection types and ports are allowed. To be considered a disallowed port, the connection type and port number must either be specified explicitly in the Disallowed Ports active list, or not specified in the Allowed Ports active list. If all ports are specified in the Allowed Ports active list (using the * character), the policy allows all ports (except those specified explicitly in the Disallowed Ports active list). Explicit (that is, not *) port entries in the Disallowed Ports active list always take precedence over entries in the Allowed Ports active list.</p>	Connection type and port number Where Connection type could be: inbound, outbound or internal
Former Employees	This active list contains user accounts of former employees. User accounts in this active list are retained indefinitely. All the entries in this list need to be in lowercase.	User Name, in lowercase. This list should be maintained on a regular basis.
Insecure Ports	This active list includes ports related to unencrypted and thus insecure communication services.	Port number
Insecure Processes	This active list includes the names of processes that provide unencrypted and thus insecure communications.	Process name, in lowercase
Instant Messaging Domains	This active list contains all the DNS domains for public instant messaging servers. This list is used to detect when outbound traffic to these domains is detected, signifying a possible information leak. Note: All the domain names must be in lowercase.	Domain name of popular or known instant messaging server in lowercase
Internet Ports	This active list includes ports that are used for monitoring internet (Web traffic) communication. By default, it includes ports 80 and 443.	Port number
Monitored Accounts	This active list is used to maintain user accounts to be monitored.	Usernames in lowercase
New Hire Accounts	This active list contains newly hired users and is automatically populated by the "New Hire Identification" rule. New users are retained for 7 days in the list.	User Name, in lowercase. This list should be maintained on a regular basis.
Peer to Peer Ports	This active list contains the ports involved in peer-to-peer traffic	Should be maintained on a regular basis.
Unsecured Password Signatures	This active list contains unsecured password signatures.	

Configure Active Lists Using Console Active List Editor

You can add entries to active lists, one-by-one, using the Active List editor of the ArcSight Console.

1. In the Navigator panel, go to Lists and navigate to ArcSight Solutions/HIPAA.
2. Right-click the active list you wish to populate and select **Show Entries**. The active list details are displayed in the Viewer panel.
3. For each entry you wish to add to the active list, repeat the following steps:
 - a. To add an entry to the list, click the add icon (+) in the active list header.
 - b. In the Active List Entry editor of the Inspect/Edit panel, enter values for each column in the list except for the dynamic columns listed in the following table and click **Add**.

Name	Value
Creation Time	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field blank.
Last Seen Time	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field blank.
Count	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field unchanged.

Configure Active Lists by Importing a CSV File

Active lists can be populated in a single step, by importing entries from an existing CSV file. The number of columns in the active list must match the number of comma separated values in the CSV file. For example, if the active list has two columns of data, the imported CSV file must have two comma-separated fields.

1. In the Active Lists resource tree of the ArcSight Console, right-click an active list and choose **Import CSV File**.
A file browser opens.
2. Browse to find the CSV file you want to import, select it, and click **Open**. The Import Preview dialog displays the data from the CSV file to be imported into the active list.
3. To add the entries from the selected file into the active list, in the Import Preview dialog, click **OK**. The new entries from the file are appended to the existing entries in the active list.
4. To verify that your entries were imported as expected, right-click the active list you just populated with the CSV file and select **Show Entries**.

This displays the newly-added data from the CSV file in the Viewer panel as active list details.

Tip: By default, the active list displays 2000 entries at a time. To view entries outside the range shown, create an active list filter that specifies a different range (click **Filter** in the active list header).

Configure My Filters

Configure the following common filters stored in the My Filters group to reflect your organization:

- ["After Hours Filter" below](#)
- ["Intellectual Property Download Filter" on the next page](#)
- ["Limit Regulation Filter" on the next page](#)

After Hours Filter

The [My Filters](#) filter defines the time period which is considered to be after business hours. The default after hours time period is set to 8:00 p.m. to 6:00 a.m. on weekdays, and all day Saturday and Sunday.

The filter uses two variables:

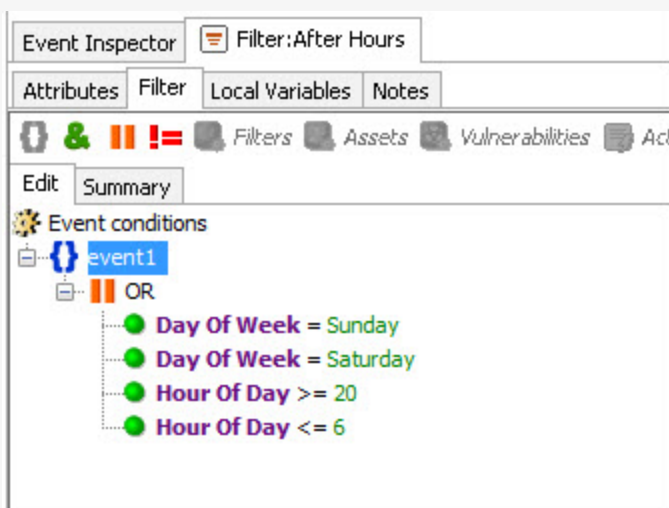
- DayOfWeek
- HourOfDay

You can change this filter to match what is considered to be after hours for your organization.

Tip: The DayOfWeek variable returns an integer value that is displayed on the ArcSight Console as a string value of the current day: Saturday, Sunday, Monday, Tuesday, Wednesday, Thursday, or Friday. Since the DayOfWeek variable is an integer, you can specify a range of days such as (DayOfWeek >= Monday AND DayOfWeek <= Friday).

The HourOfDay variable returns a numerical value for the current hour in 24-hour format ranging from 12 AM = 0 to 11 PM = 23.

For example, to redefine the after business hours from 6:00 PM to 8:00 AM on all weekdays and all of Saturday and Sunday use the filter show in the following figure.



Intellectual Property Download Filter

The [My Filters](#) filter finds events that involve the download of possibly illegal intellectual property. By default, this filter is set to find a Snort signature that indicates video or audio download. Add the signatures for the content monitoring device(s) or NIDS you use that indicate intellectual property downloads, such as video streams, images, audio files, or possibly illegal intellectual property or copyrighted material.

Limit Regulation Filter

The [Limit Regulation](#) filter limits event processing to only those events addressed by the HIPAA regulation. Customize it to reflect your environment.

For example, you could configure it to specify the following conditions:

- The source machine is an asset under the HIPAA
- The source machine's zone is categorized as HIPAA
- The destination machine is an asset categorized as HIPAA
- The destination machine is an asset under the HIPAA group
- The destination machine's zone is categorized as HIPAA
- The device machine is an asset categorized as HIPAA
- The device machine is an asset under the HIPAA group
- The device machine's zone is categorized as HIPAA

By default, the CIP for HIPAA processes all incoming events.

Deploy the CIP for HIPAA Rules

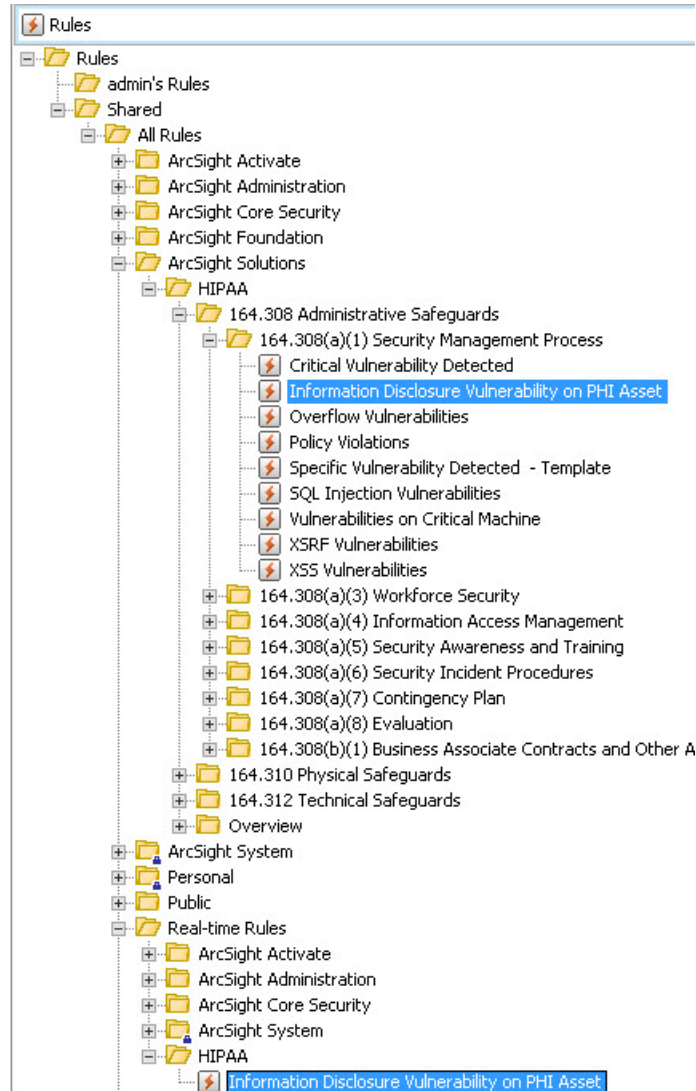
In order for the CIP for HIPAA to process HIPAA-related events, the solution rules have to be deployed to the `Real-time Rules` group. By default, CIP for HIPAA rules are not deployed in the `Real-time Rules` group because deployed rules can have a performance impact. Only deploy a rule into the `Real-time Rules` group if you are interested in the associated use case and have device feeds configured in your environment that can trigger the rule.

To deploy a rule:

1. From the Resources tab in the Navigator panel, go to Rules and navigate to the ArcSight Solutions/Rules group.
2. Expand the HIPAA folder that contains the rule to deploy and select the rule. For example, to select the **Information Disclosure Vulnerability on PHI Asset** rule, expand /Arcsight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process.

3. Drag and drop the selected rule from the appropriate /ArcSight Solutions/HIPAA group into the Real-time Rules/HIPAA group.
4. From the Drag & Drop Options dialog, select the **Link** option.

The rule is listed under the Real-time Rules/HIPAA group as shown in the following figure.



The rule in the Real-time Rules/HIPAA group is a link to the rule in the ArcSight Solutions/HIPAA group.

Note: By default, the CIP for HIPAA rules are disabled. The rules do not trigger until they are deployed and enabled. After you have deployed the CIP for IT HIPAA rules to the Real-time Rules group, you can enable individual rules. Rules can place an additional load on the ArcSight Manager. Enable only the rules for the compliance scenarios you want to implement.

To enable a rule:

1. In the Navigator panel, go to **Rules** and navigate to the Real-time Rules/HIPAA group.
2. Navigate to the rule you want to enable.
3. Right-click the rule and select **Enable Rule**. To select multiple rules, press the **Ctrl** key and click each rule. To select a range of rules, press the **Ctrl** and **Shift** keys and click the first and last rule in the range.

Certain use cases in the CIP for HIPAA require that specific rule actions be enabled to trigger actions in the system, such as the creation of a new case. To enable a rule action, select an action below a trigger in the Actions tab of the Rule Editor and click **Enable Action**.

For more information about working with rules, see the *Rules Authoring* topic in the *ArcSight Console User's Guide*.

Enable Data Monitors

All of the CIP's data monitors for HIPAA must be enabled to display data in the dashboards that use them.

To enable the data monitors:

1. In the Navigator panel, go to **Dashboards** and click the **Data Monitors** tab.
2. Navigate to the /All Data Monitors/ArcSight Solutions/HIPAA group.
3. Right-click the CIP group and select **Enable Data Monitor** to enable all the data monitors in the group.

Enable and Test Trends

By default, trends included in the CIP are not enabled. Some reports, query viewers, and dashboards require enabled trends to show data.

Before enabling a trend, verify that the trend captures data relevant for your environment as described in the procedure below:

1. Generate or identify the required events and verify that they are being processed by ArcSight ESM.
2. Navigate to the appropriate trend, right-click the trend, and then choose **Test**. If you see the events of interest in the test panel, then ArcSight ESM is processing events that can be captured by the trend. The test panel shows relevant events that can be captured by the trend in the last hour, up to 25 rows.

In addition, before enabling a trend, you can also customize its values like Partition Retention Period (in days) and Scheduler Start Time.

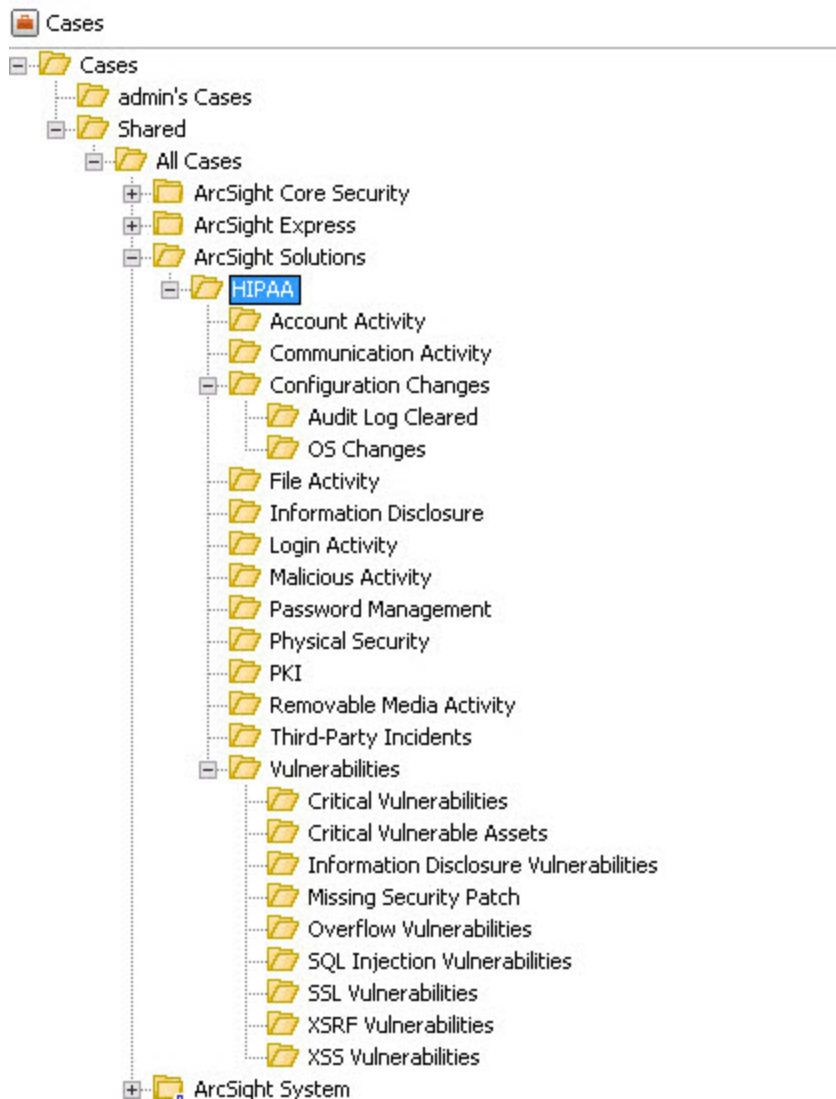
For general information about trends, see:

- *ArcSight Console User's Guide*
- *ESM Best Practices: Trends*

See "[Resources Requiring Enabled Trends](#)" on page 220 for a list of reports, query viewers, and dashboards that use trends to display data.

Configure Cases

Cases are ArcSight's trouble-ticket system that can be used as-is or in conjunction with a third-party trouble-ticket system. CIP for HIPAA includes the ArcSight Solutions/HIPAA group, which holds the cases generated by some CIP for HIPAA rules.



You can add more groups to the ArcSight Solutions/HIPAA group or your own group if you want to add more differentiations. If you do add more groups to the ArcSight Solutions/HIPAA group, modify the ESM rules that generate cases to use of your new case groups.

The following rules can generate cases in the HIPAA directory.

Rules and Auto-Generated Cases

Rule	Generated Case's URI
Critical Vulnerability Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/Critical Vulnerabilities/
Information Disclosure Vulnerability on PHI Asset	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/Information Disclosure Vulnerabilities/
Overflow Vulnerabilities	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/Overflow Vulnerabilities/
Specific Vulnerability Detected- Template	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/
SQL Injection Vulnerabilities	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/SQL Injection Vulnerabilities/
Vulnerabilities on Critical Machine	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/Critical Vulnerable Assets/
XSRF Vulnerabilities	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/XSRF Vulnerabilities/
XSS Vulnerabilities	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/XSS Vulnerabilities/
Former Employee Account Activity	/All Cases/All Cases/ArcSight Solutions/HIPAA/Account Activity/
Former Employee User Account Access Attempt	/All Cases/All Cases/ArcSight Solutions/HIPAA/Account Activity/
Suspicious Activities by Former Employee	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
Suspicious Activities by New Hires	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
Privileged Account Changes	/All Cases/All Cases/ArcSight Solutions/HIPAA/Account Activity/
Consecutive Unsuccessful Logins to Administrative Account	/All Cases/All Cases/ArcSight Solutions/HIPAA/Login Activity/
Malware or Spyware Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
Password not Changed for Longer than Policy Standard	/All Cases/All Cases/ArcSight Solutions/HIPAA/Password Management
Suspicious Internal Trojan Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
Unsuccessful Logins to Multiple Administrative Accounts	/All Cases/All Cases/ArcSight Solutions/HIPAA/Login Activity/
Worm Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/

Rules and Auto-Generated Cases, continued

Rule	Generated Case's URI
Information System Failures of Highly Critical Machine	/All Cases/All Cases/ArcSight Solutions/HIPAA/Configuration Changes/OS Changes/
Resource Exhaustion of Highly Critical Machine	/All Cases/All Cases/ArcSight Solutions/HIPAA/Configuration Changes/OS Change/
Shutdown of Highly Critical Machine	/All Cases/All Cases/ArcSight Solutions/HIPAA/Configuration Changes/OS Changes/
Critical Network Device Configuration Change Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Configuration Changes/
Critical Operating System Change Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Configuration Changes/OS Changes/
Security Patch Missing	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/Missing Security Patch/
Attack from Business Associate System Targeting PHI Assets	/All Cases/All Cases/ArcSight Solutions/HIPAA/Third-Party Incidents/
Attack from Third-Party System	/All Cases/All Cases/ArcSight Solutions/HIPAA/Third-Party Incidents/
After Hours Building Access by Contractors	/All Cases/All Cases/ArcSight Solutions/HIPAA/Physical Security/
Failed Building Access	/All Cases/All Cases/ArcSight Solutions/HIPAA/Physical Security/
Local Logon from Badged Out Employee	/All Cases/All Cases/ArcSight Solutions/HIPAA/Physical Security/
Removable Media Detected on Highly Critical Machine	/All Cases/All Cases/ArcSight Solutions/HIPAA/Removable Media Activity/
Communication between Electronic PHI and Business Associate Domains	/All Cases/All Cases/ArcSight Solutions/HIPAA/Communication Activity/
Communication between Production and Development Domains	/All Cases/All Cases/ArcSight Solutions/HIPAA/Communication Activity/
Communication between Sensitive Asset and Test Domain	/All Cases/All Cases/ArcSight Solutions/HIPAA/Communication Activity/
Communication between Sensitive Asset and Third Party Domain	/All Cases/All Cases/ArcSight Solutions/HIPAA/Communication Activity/
Inactive User Account Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Account Activity/
Login Activity by a Stale Account	/All Cases/All Cases/ArcSight Solutions/HIPAA/Account Activity/
Suspicious Activities by a Stale Account	/All Cases/All Cases/ArcSight Solutions/HIPAA/Account Activity/
User Logged in from different IP Addresses	/All Cases/All Cases/ArcSight Solutions/HIPAA/Account Activity/
User Logged in from Two Countries	/All Cases/All Cases/ArcSight Solutions/HIPAA/Account Activity/

Rules and Auto-Generated Cases, continued

Rule	Generated Case's URI
Audit Log Cleared	/All Cases/All Cases/ArcSight Solutions/HIPAA/Configuration Changes/Audit Log Cleared/
Attempted File Changes in PHI Segment Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/File Activity/
Cryptographic Hash Algorithm Related Vulnerability Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/
Successful Attack - Brute Force Login	/All Cases/All Cases/ArcSight Solutions/HIPAA/Login Activity/
Cryptographic Public Key Related Vulnerability Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/
Cryptographic Symmetric Key Related Vulnerability Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/
Cryptographic Weak Protocol Vulnerability Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/
Disallowed Ports Access	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
DoS Detected	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
Invalid or Expired Certificate	/All Cases/All Cases/ArcSight Solutions/HIPAA/PKI/
One or more rows have been deleted from the certificate database	/All Cases/All Cases/ArcSight Solutions/HIPAA/PKI/
Organizational Data Information Leak	/All Cases/All Cases/ArcSight Solutions/HIPAA/Information Disclosure/
Personal Information Leak	/All Cases/All Cases/ArcSight Solutions/HIPAA/Information Disclosure/
Possible Covert Channel	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
Possible Email Attack	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
Possible Information Interception	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
Possible Redirection Attack	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
Possible Traffic Anomaly	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
Potential Distributed DoS	/All Cases/All Cases/ArcSight Solutions/HIPAA/Malicious Activity/
SSL Vulnerabilities on PHI Machine	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/SSL Vulnerabilities/
SSL Vulnerabilities on Public Facing Assets	/All Cases/All Cases/ArcSight Solutions/HIPAA/Vulnerabilities/SSL Vulnerabilities/

By default, the **Add to Existing Case** action for these rules are disabled. Enable the **Add to Existing Case** actions only for the rules that detect events are important to your organization and therefore should be tracked with cases.

To enable the **Add to Existing Case** action for a rule:

1. From the Resources tab in the Navigator panel, go to Rules and navigate to the ArcSight Solutions/HIPAA group.
2. Right-click a rule and select **Edit Rule**.
The rule displays in the Inspect/Edit panel.
3. Right-click the **Add to Existing Case** action and select **Enable Action**.

After enabling the **Add to Existing Case** action, one of the following occurs when the rule fires:

- If a case with the same name does not exist, a new case is created.
- If a case with the same name does exist, the existing case is updated with additional events.

If you want to generate cases for additional activities, you can edit any rules in the ArcSight Solutions/HIPAA that trigger on that specific behavior and add actions those rules to create cases. For example, if you want to create a case every time an account is locked out, edit the [Account Lockout](#) rule and add an action that creates a case.

Caution: Use caution when adding a **Create New Case** action to a rule. Every time a rule fires, a new case is created. If you expect the rule to fire repeatedly, consider using **Add to Existing Case** action instead.

If you are using the **Add to Existing Case** action and you choose to close the case, consider the following in order to detect new issues when the same circumstances re-occur:

1. Copy the case to another location.
2. Delete the case from the original directory.

Configure Notifications

When enabled, a notification action on a rule sends a notification when the rule fires. The following rules contain notification actions that are disabled by default:

- Successful Default Vendor Account Used
- Account Lockout
- Security Software Stopped or Paused
- Suspicious Internal Trojan Detected
- Multiple Cases Created on Short Period

You can enable the notification actions for these rules. You can add a rule action to other ArcSight Solutions/HIPAA rules. In addition, you can create notification destinations that receive the

notifications when the rules fire. For more information including configuration information, see the *Notifications* topic in the *ArcSight Console User's Guide*. This configuration is optional.

Configure Additional Resources

Additional configuration may be required or desired for the individual resources provided to address a specific HIPAA standard. For more information, see ["CIP for HIPAA Resource Reference" on page 37](#).

Build FlexConnector(s) for Physical Access Devices

The Compliance Insight Package for HIPAA contains resources that make use of feeds from physical access systems, such as badge readers. This process is only required if you want to activate the CIP for HIPAA content that leverages feeds from physical access systems. If you do not complete this process, the content that leverages feeds from physical access systems will remain dormant.

To enable these scenarios, develop a FlexConnector according to the instructions in the *ArcSight FlexConnector Developer's Guide* with the following field mappings to map the key event data into the ArcSight event schema:

Field Mappings

ArcSight Field	Physical Access System Value
deviceEventClassId	Unique value for event type used for categorization
deviceReceiptTime	Access Time
destinationUserId	Users badge Id
deviceCustomString1	Location Accessed / Building

Use the following event categories for the following event types:

Event Categories

Event type	Object	Behavior	Tech nique	Device Group	Outcome	Significance
Successful building access	/Location	/Authentication/Verify		/Physical Access System	/Success	/Normal
Building access rejected	/Location	/Authentication/Verify		/Physical Access System	/Failure	/Information/Warning
Badge-out (someone is leaving a building) [not all badge reader systems support this]	/Location	/Access/Stop		/Physical Access System	/Success	/Normal

Event Categories, continued

Event type	Object	Behavior	Tech nique	Device Group	Outcome	Significance
Account created/deleted/modified - [Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error]	/Actor/User	/Authentication/ [Add Delete Modify]		/Physical Access System	/Success	/Informational
Giving someone access to another room/building - [Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error]	/Actor/User	/Authorization/Modify		/Physical Access System	/Success	/Informational
Granting access to a room/building for an entire group of users	/Actor/Group	/Authorization/Modify		/Physical Access System	/Success	/Informational

You can add more user context to the events generated by your badge reader by creating a connector event mappings file.

Appendix A: CIP for HIPAA Resource Reference

This section includes lists of resources under the following HIPAA 3.0 resource groups:

- Administrative Safeguards:
 - ["Security Management Process 164.308 \(a\)\(1\)" on the next page](#)
 - ["Workforce Security 164.308 \(a\)\(3\)" on page 64](#)
 - ["Information Access Management 164.308 \(a\)\(4\)" on page 74](#)
 - ["Security Awareness and Training 164.308 \(a\)\(5\)" on page 87](#)
 - ["Security Incident Procedures 164.308 \(a\)\(6\)" on page 108](#)
 - ["Evaluation 164.308 \(a\)\(8\)" on page 122](#)
 - ["Business Associate Contracts and Other Arrangements 164.308 \(b\)\(1\)" on page 135](#)
- Physical Safeguards:
 - ["Facility Access Controls 164.310 \(a\)\(1\)" on page 146](#)
 - ["Workstation Use 164.310 \(b\)" on page 151](#)
 - ["Device and Media Controls 164.310 \(d\)\(1\)" on page 150](#)
- Technical Safeguards
 - ["Access Control 164.312 \(a\)\(1\)" on page 153](#)
 - ["Audit Controls 164.312 \(b\)" on page 165](#)
 - ["Integrity 164.312 \(c\)\(1\)" on page 171](#)
 - ["Person or Entity Authentication 164.312 \(d\)" on page 173](#)
 - ["Transmission Security 164.312 \(e\)\(1\)" on page 177](#)
- Other resources not under specific HIPAA sections:
 - ["Active Lists" on page 197](#)
 - ["Filters" on page 199](#) (includes My Filters and General Filters)
 - ["Overview Dashboards" on page 206](#)
 - ["Overview Data Monitors" on page 207](#)
 - ["Field Sets" on page 208](#)
 - ["Overview Rules" on page 209](#)

Security Management Process 164.308 (a)(1)

This section lists all resources under the Security Management Process group.

Resources for Security Management Process 164.308 (a)(1)

Resource	Type	URI	Description
High Priority Events	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This active channel shows high priority events which translate into high risk.
Policy Violations	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Looks for policy violations in the past.
Technical Compliance Check Failures	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This active channel looks for events which indicate that a technical compliance check failed, meaning that an either misconfigured system or system with severe vulnerability was found.
Vulnerability Events	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Looks for events that indicate the existence of vulnerabilities.
Last State Vulnerability Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the last 20 vulnerabilities related to assets and their compliance status.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Overflow Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides overview of overflow vulnerability events.
PHI Assets Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides overview of vulnerability events on PHI assets
Policy Violations	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Displays information about policy violations and violators.
Risk - Geo View	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This dashboard provides a geographical view of potential threatening events.
Risk Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This dashboard displays high-level information around potential malicious events.
SQL Injection Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This Dashboard provides overview of sql injection vulnerability events.
Technical Compliance Checking	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This dashboard displays different views of failed compliance checks.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
User Activities	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Displays information about uses of default vendor and other suspicious accounts.
Vulnerability Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides overview of vulnerability events.
XSRF Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides overview of XSRF vulnerability events.
XSS Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides overview of XSS vulnerability events.
All Attacks - GeoView	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This data monitor shows all the attack events on a map.
Attacks per Asset Category	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This data monitor shows the number of attacks targeting each of the network domains.
Compromised Hosts	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This Last State data monitor shows the last compromised hosts.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Failed User Actions	DataMonitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all failed user actions in the last hour.
Last 10 High Risk Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This data monitor displays in real-time the last 10 Internal Reconnaissance Events.
Last 20 Failed Technical Compliance Checks	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This data monitor shows the last 20 events indicating failed technical compliance checks.
Last 20 Information Disclosure Vulnerabilities on PHI Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides real-time display of the last 20 Information disclosure vulnerabilities.
Last 20 Machines Failing Technical Compliance Checks	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This data monitor reports the last 20 machines that were reported to have failed technical compliance check.
Last 20 Overflow Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides real-time display of the last 20 overflow vulnerabilities.
Last 20 SQL Injection Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides real-time real-time display of the last 20 SQL vulnerabilities.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Last 20 Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the last 20 vulnerabilities.
Last 20 Vulnerabilities on PHI Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the last 20 vulnerabilities on PHI assets.
Last 20 Vulnerabilities with High CVSS	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the last 20 vulnerabilities with CVSS equal or higher than 8.
Last 20 XSRF Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides real-time display of the last 20 XSRF vulnerabilities.
Last 20 XSS Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides real-time display of the last 20 XSS vulnerabilities.
Last 50 User Activities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the last 50 user activities.
Last State Vulnerability Overview	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the last 20 vulnerabilities related to assets and their compliance status.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Priority Distribution	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This data monitor shows the distribution of priorities across all events.
Reconnaissance Only - GeoView	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This data monitor shows all reconnaissance events on a world map.
Successful User Actions	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the moving average number of successful user actions in the last hour.
Top 10 Assets with Critical Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the top 10 assets with critical vulnerability events.
Top 10 Failed Technical Compliance Checks	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This data monitor shows the top 10 events indicating failed technical compliance checks.
Top 10 Information Disclosure Vulnerable PHI Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the top 10 assets with information disclosure vulnerability events.
Top 10 Machines Failing Technical Compliance Checks	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This data monitor shows the top 10 machines with failed compliance checks.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Top 10 Overflow Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the top 10 assets with overflow vulnerability events.
Top 10 Policy Violations	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 10 policy violation events.
Top 10 Policy Violators	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 10 policy violators.
Top 10 SQL Injection Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the top 10 assets with sql injection vulnerability events.
Top 10 Users with Failed Actions	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 10 non-administrative attacker and target user pairs with failed actions in the last hour.
Top 10 Vulnerable PHI Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the top 10 assets with XSS vulnerability events.
Top 10 XSRF Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the top 10 assets with XSRF vulnerability events.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Top 10 XSS Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows real-time display of the top 10 assets with XSS vulnerability events.
Asset Creation	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Select events indicating the creation of a new asset.
Asset Deletion	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Select events indicating the deletion of an asset.
Asset Modification	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Select events indicating the modification of an asset.
Assets with High Severity Vulnerability by Non-Scanners	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This filter selects events that indicate the existence of severe vulnerabilities reported by non-scanners.
Assets with High Severity Vulnerability by Scanners	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This filter selects events that indicate the existence of severe vulnerabilities reported by scanners.
Attacks with Geo Information	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This filter selects attack events with populated Geo fields for both the attacker and target addresses.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Compromises	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This filter identifies generic compromises.
Critical Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Selects events indicating that a critical vulnerability was detected.
Exploit of Vulnerability	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Selects events where an attempt at exploiting a vulnerability is detected.
Failed Technical Compliance Check	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This filter identifies events which indicate a compliance check failure.
Failed User Actions	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Identifies failed non-administrative actions.
High Priority Events	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This filter shows events in which the Priority field is 10.
Information Disclosure Vulnerability Detected on PHI Asset	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Selects events indicating that an information disclosure vulnerability was detected.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Monitored User	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Identifies events with monitored users. These events are defined as such in which either the source or destination users are monitored users. Monitored users are stored in the Active List "Monitored Accounts".
Overflow Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Selects events indicating that an overflow vulnerability detected.
Policy Breaches	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Filter in events with breach of policy.
Policy Violations	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Filter in events with violation of policy.
Reconnaissance - Geo Information	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This filter identifies reconnaissance events in which the Geo information fields are populated for both attacker and target.
SQL Injection Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Selects events indicating that SQL injection vulnerability was detected.
Successful User Actions	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Identifies successful non-administrative actions.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Vulnerability Detected on PHI Asset	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Selects events indicating that a vulnerability was detected on PHI asset.
XSRF Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Selects events indicating that an XSRF vulnerability was detected.
XSS Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Selects events indicating that an XSS vulnerability was detected.
Assets in Partners Network Domain	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of all the assets for the Partners Network Domain.
Assets in Processing Network Domain	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of all the assets for the Processing Network Domain.
Assets in the Public-Facing Network Domain	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of all the assets for the Public-Facing Network Domain.
Assets in the Third Party Domain	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of all the assets for the Third Party Domain.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Clearinghouse Assets	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of all the clearinghouse assets.
Database Assets	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of all of assets which are categorized as databases.
Health Care Provider Assets	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of all the health care provider assets.
Health Plan Assets	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of all the health plan assets.
PHI Assets	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of all the PHI assets.
PII Assets	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of all the assets for the PII Domain.
Policy Violations on Clearinghouse Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of events categorized by ArcSight as policy violations which target clearinghouse assets.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Policy Violations on Health Care Provider Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of events categorized by ArcSight as policy violations which target health care provider assets.
Policy Violations on Health Plan Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of events categorized by ArcSight as policy violations which target health plan assets.
Top 10 Vulnerabilities - Health Care Provider Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This report shows the top 10 vulnerabilities exposed on the health care provider entity.
Top 10 Vulnerabilities - Clearinghouse Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This report shows the top 10 vulnerabilities exposed on the clearinghouse entity systems.
Top 10 Vulnerabilities - Health Plan Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This report shows the top 10 vulnerabilities exposed on the health plan entity systems.
Top 10 Vulnerable Assets - Clearinghouse Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 10 vulnerable assets on clearinghouse assets.
Top 10 Vulnerable Assets - Health Care Provider Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 10 vulnerable assets on health care provider assets.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Top 10 Vulnerable Assets - Health Plan Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 10 vulnerable assets on health plan assets.
Asset Creation by Location	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of newly created assets.
Asset Deletion by Location	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of deleted assets.
Asset Identification Report	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all assets and their respective network domain.
Asset Modification by Location	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of modified assets.
Assets by Network Domain - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a list of all the assets for the various network domains. This query may (and should) be focused based on the network domain of interest. Results are sorted by creation time.
Assets that Failed Technical Compliance Check	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This query finds assets which failed the technical compliance check.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
CVSS Score Greater than or Equal to 8	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows vulnerabilities with CVSS >=8.
Classification of Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the asset classifications.
Critical Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Lists all the critical assets. It can be used to gather the key assets to implement the business continuity process.
Criticality of Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the asset criticality sorted by their criticality and network domain.
Detail Monitored Account Activities in the Last Day - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all activities of a user being monitored within the last day. The user name is stored in the Active List "Monitored Accounts" and has to be specified when using this query.
Exploit of Vulnerability	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all incidents of attempts to exploit vulnerabilities in an application.
High Priority Events	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This query shows events in which the Priority is 10.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Individual Account Activity	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all activity of a particular user. The user name is a required parameter for this report.
Information Disclosure Vulnerabilities on PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows Information Disclosure vulnerabilities on PHI assets identified on the last 24 hours.
Machines Conducting Policy Breaches	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows machines which were involved in policy breaches.
Machines Conducting Policy Violations	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows machines which were involved in policy violations.
Monitored Account Activities in the Last Day by Hour - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all activities of a user being monitored within the last day by hour. The user name is stored in the Active List "Monitored Accounts" and has to be specified when using this query.
Monitored Account Activities in the Past Week - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all activities of one of the users being monitored within the past week. The user name is stored in the Active List "Monitored Accounts" and has to be provided when using this query.
Monitored Account Asset Access in the Last Day by Hour - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the number of assets accessed by one of the users being monitored within the last day. The user name is stored in the Active List "Monitored Accounts" and has to be specified when using this query.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Monitored Account Asset Access in the Past Week - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the number of assets accessed by one of the users being monitored within the past week. The user name is stored in the Active List "Monitored Accounts" and has to be specified when using this query.
Monitored Users	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Identifies monitored users. Monitored accounts are stored in the Active List "Monitored Accounts".
Overflow Vulnerabilities	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows overflow vulnerabilities identified on the last 24 hours.
Policy Violations - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of events categorized by ArcSight as policy violations which target the various Network Domains by Asset. This query may (and should) be focused based on the Network Domain of interest.
Policy Violations from Business Associate Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of events categorized by ArcSight as policy violations coming from assets categorized as Business Associate.
Policy Violations from Third-Party Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of events categorized by ArcSight as policy violations coming from assets categorized as Third-Party.
SQL Injection Vulnerabilities	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows SQL injection vulnerabilities identified on the last 24 hours.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Top 10 Vulnerable Assets on Network Domain - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 10 vulnerable Assets by network domain (default Development)
Top 10 vulnerabilities on network domain - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 10 vulnerabilities on network domain (default Development).
Top 20 Policy Breach Events	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 20 policy breach events.
Top 20 Policy Violation Events	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 20 policy violation events.
Top Critical Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Retrieves the top 10 critical vulnerabilities for the last 14 days.
Top Vulnerable IP Addresses	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Retrieves the top 10 vulnerable IP Addresses for the last 14 days.
Vulnerabilities - Trend Base	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Retrieves all the vulnerabilities for the last hour. Used as trend base query for the vulnerabilities trend.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Retrieves all the vulnerabilities for the last 14 days.
Vulnerabilities Summary	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides overview of the vulnerability summary on IT Governance Assets.
Vulnerabilities by IP Address - on Trend	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Retrieves all the vulnerabilities for the last 14 days for specific IP Address.
Vulnerability Events By Scanner - on Trend	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows vulnerability count per scanner for the last 14 days.
Vulnerability Scans - on Trend	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all the vulnerability scans for the last 14 days
XSRF Vulnerabilities	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows XSRF vulnerabilities identified on the last 24 hours.
XSS Vulnerabilities	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows XSS vulnerabilities identified on the last 24 hours.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Top Critical Vulnerabilities	QueryViewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows summary of top critical vulnerabilities, where the user can drill down to detailed information about those vulnerabilities.
Top Vulnerable IP Addresses	QueryViewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows top vulnerable IP addresses in bar chart format.
Vulnerabilities	QueryViewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all the vulnerabilities.
Vulnerability Events By Scanner	QueryViewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This Query Viewer shows vulnerability events count for each scanner.
Vulnerability Scans	QueryViewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all the vulnerability scans for the last 14 days, where the user can drill down to all the vulnerabilities which pertains to specific scan.
Asset Creation by Location	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of newly created assets by their uri location.
Asset Deletion by Location	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of deleted assets by their uri location.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Asset Identification Report	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all assets and their respective network domain.
Asset Modification by Location	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of modified assets by their uri location.
Assets by Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides the listing of all the assets for the various Network Domains. This report may (and should) be focused based on the network domain of interest. Results are sorted by creation time, if no network domain specified PII domain will be used.
Assets that Failed Technical Compliance Check	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This report shows assets which failed the technical compliance check.
CVSS Score Greater than or Equal to 8 Overview	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides overview of vulnerabilities with CVSS >=8 on the last 24 hours.
Classification of Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the asset classifications sorted by network domain.
Critical Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Lists all the critical assets. It can be used to gather the key assets to implement the business continuity process.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Criticality of Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the asset criticality sorted by their criticality and network domain.
Exploit of Vulnerability	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all incidents of attempts to exploit vulnerabilities in an application. The report is sorted first by the outcome of the attempts and then by the number of events.
High Priority Events	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This report shows events in which the Priority field is 10.
Individual Account Activity in the Last Day	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all activities of a particular user within 1 day. The user name is a required parameter for this report.
Information Disclosure Vulnerabilities on PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows information disclosure vulnerabilities identified on the last 24 hours.
Machines Conducting Policy Breaches	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows machines which were involved in policy breaches.
Machines Conducting Policy Violations	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows machines which were involved in policy violations.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Monitored Account Activity in the Last Day - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all activities of a monitored user in the last day. The user name is stored in the Active List "Monitored Accounts" and has to be specified when running this report.
Monitored Account Activity in the Past Week - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows all activities of a monitored user in the past week. The user name is stored in the Active List "Monitored Accounts" and has to be specified when the report is run.
Overflow Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows overflow vulnerabilities identified on the last 24 hours.
Policy Violations - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of events categorized by ArcSight as policy violations which target the various Network Domains by Asset. This report may (and should) be focused based on the Network Domain of interest.
Policy Violations from Business Associate Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of events categorized by ArcSight as policy violations coming from assets categorized as Business Associate.
Policy Violations from Third-Party Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides a listing of events categorized by ArcSight as policy violations coming from assets categorized as Third-Party.
SQL Injection Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows SQL injection vulnerabilities identified on the last 24 hours.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
Top 10 Vulnerabilities - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This report shows the top 10 vulnerabilities exposed on the systems.
Top 10 Vulnerable Assets on Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 10 vulnerable IT assets on network domain (default Development Network Domain)
Top 20 Policy Breaches Events	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 20 policy breaches events.
Top 20 Policy Violation Events	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows the top 20 policy violation events.
Vulnerabilities by IP Address	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Displays vulnerability overview by IP Address for the last 14 days (default 127.0.0.1).
Vulnerability Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Provides overview of the vulnerability summary in the last 24 hours.
XSRF Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows XSRF vulnerabilities identified on the last 24 hours.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
XSS Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Shows XSS vulnerabilities identified on the last 24 hours.
Critical Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Triggers when a critical vulnerability is detected.
Information Disclosure Vulnerability on PHI Asset	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Triggers when information disclosure vulnerability is detected on PHI Asset.
Overflow Vulnerabilities	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Triggers when an overflow vulnerability is detected.
SQL Injection Vulnerabilities	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Triggers when SQL Injection vulnerability is detected.
Specific Vulnerability Detected-Template	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Triggers when a specific CVE Id vulnerability is detected on PHI asset, CVE ID is defined using deviceCustomString2 = <CVE ID> on the Conditions tab.
Vulnerabilities on Critical Machine	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Triggers when a vulnerability is detected on critical machine.

Resources for Security Management Process 164.308 (a)(1), continued

Resource	Type	URI	Description
XSRF Vulnerabilities	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Triggers when XSRF vulnerability is detected.
XSS Vulnerabilities	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Triggers when XSS vulnerability is detected.
Policy Violations	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	This rule looks for policy violations.
Monitored Users	Trend	/All Trends/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Stores all events that are related to a monitored user either in the target or attacker fields.
Vulnerabilities	Trend	/All Trends/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Collects hourly data using the Vulnerabilities trend Base query.

Workforce Security 164.308 (a)(3)

This section lists all resources under the Workforce Security group.

Resources for Workforce Security 164.308 (a)(3)

Resource	Type	URI	Description
Internal Reconnaissance	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This active channel shows reconnaissance events originating internal to the corporation.
Former Employee Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows information related to activity by former employees.
Internal Reconnaissance	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This dashboard displays information about internal reconnaissance events and sources.
New Hires Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows information related to activity by new hire employees.
Unauthorized File access on PHI Assets	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This dashboard displays information about Unauthorized File access on PHI assets.
Internal Reconnaissance	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This Event Graph data monitor shows all internal reconnaissance activity.

Resources for Workforce Security 164.308 (a)(3), continued

Resource	Type	URI	Description
Internet Activity by New Hires	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows Internet activity per reporting device per new hire over a day's period.
Last 10 Former Employee Activity	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 10 Internal Reconnaissance Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This data monitor displays in real-time the last 10 Internal Reconnaissance Events.
Last 10 Unauthorized File access on PHI assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This data monitor displays in real-time the last 10 unauthorized File access on PHI assets
New Hires Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows the new hire user logins.
Suspicious Activity by New Hires	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows the new hires suspicious activity count. Suspicious activity is counted for 7 days (as long as the user is defined new, see New Hire Accounts active list).
Top 10 Unauthorized File access on PHI Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This data monitor shows the top 10 unauthorized File access PHI targets identified by the filter in this section.

Resources for Workforce Security 164.308 (a)(3), continued

Resource	Type	URI	Description
Top Internal Reconnaissance Sources	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This data monitor shows the top internal reconnaissance sources identified by the filter in this section.
Top Internal Reconnaissance Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This data monitor shows the top internal reconnaissance targets identified by the filter in this section.
File Accesses	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Identifies all file accesses.
File Modifications	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Identifies all file changes.
Former Employee Account Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This filter selects events that identify a former employee account. This filter may need additional configuration.
Former Employee Activity	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This filter identifies base events associated with users who are known to be terminated according to the Former Employees active list.
Internal Recon	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This filter identifies reconnaissance events which were originated internally to the organization. This could indicate that someone is trying to scan the network which is a policy violation.
New Hire Account Added to Group	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This filter identifies when a new hire account added to group.

Resources for Workforce Security 164.308 (a)(3), continued

Resource	Type	URI	Description
New Hire Based Internet Outbound Activity	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This filter identifies the outbound internet activity of new hire users. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
New Hire Suspicious Activities	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This filter identifies suspicious activity by new hires.
New Hires Logins	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This filter identified login attempts by new hire users .
New Hires Successful Logins	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This filter identified successful logins by new hire users .
New Hires Unsuccessful Logins	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This filter identified unsuccessful logins by new hire users .
Unauthorized File access on PHI assets	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This filter looks for Unauthorized file accesses on PHI assets.
Activity by Former Employees	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows any activity performed by users who are known to be terminated.
After Hours File Accesses in PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Retrieves a count of the number of accesses of files on PHI systems(after hours).

Resources for Workforce Security 164.308 (a)(3), continued

Resource	Type	URI	Description
After Hours File Changes in PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Counts the number of creations, deletions and modifications of files on systems in the PHI Assets (after hours).
After Hours Successful New Hire Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows details of all after hours successful new hire logins within the last day.
All Events by New Hires	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows all events by new hires.
All Suspicious Events by New Hires	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows all suspicious events by new hires based on the event table.
File Accesses in PHI Assets by Specific User - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Retrieves a count of the number of accesses of files on PHI systems by user.
File Changes in PHI Assets by Specific User - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Counts the number of creations, deletions and modifications of files on PHI systems.
Former Employee Account Access Attempt	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Lists all log-in activity from a former employee.
Former Employee Accounts in Use	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Identifies all former employee user names and reporting device details associated with recent events.

Resources for Workforce Security 164.308 (a)(3), continued

Resource	Type	URI	Description
Internal Reconnaissance Events	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This query shows the top events executed for internal reconnaissance.
Internal Reconnaissance Events in the Last 2 Hours	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This query shows the internal reconnaissance events.
Internal Reconnaissance Sources	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This query shows the top sources conducting internal reconnaissance.
Internal Reconnaissance Targets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This query shows the top targeted assets by internal reconnaissance activity.
Internal Reconnaissance from Specific Source - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This query shows all internal reconnaissance activities conducted by a particular source.
Internal Reconnaissance to Specific Target - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This query shows all internal reconnaissance activities targeting a particular asset.
New Hire Internet Activity	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays all the identified outbound internet activity of new hire users. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
Summary of Suspicious Activity by New Hires	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays the number of suspicious events per new hire.

Resources for Workforce Security 164.308 (a)(3), continued

Resource	Type	URI	Description
Suspicious Activities by Former Employee	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Lists all suspicious activities by former employee.
Suspicious Activity by New Hires	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays all the identified suspicious activity performed by new users.
Unauthorized Access by Specific User - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Retrieves all the unauthorized Access by Specific User , where the user provided as input, default admin.
Unsuccessful New Hire Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows details of all unsuccessful user logins within the last day.
All Events by New Hires	QueryViewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows all events by new hires.
Former Employee Accounts in Use	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Identifies all former employee user names and reporting device details associated with recent events.
Internal Reconnaissance in the Last 2 Hours	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This query viewer returns all internal reconnaissance activities in the last 2 hours.

Resources for Workforce Security 164.308 (a)(3), continued

Resource	Type	URI	Description
Suspicious Activities by New Hires	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows all suspicious activities by new hires.
Activity by Former Employees	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows any activity performed by users who are known to be terminated.
After Hours File Accesses in PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays a count of the number of accesses of files on PHI system (after hours).
After Hours File Changes in PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays a count of the number of creations, deletions and modifications of files on PHI systems (after hours).
After Hours Successful New Hire Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays all after hours successful new hire logins within the last day.
File Accesses in PHI Assets by Specific User	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays a count of the number of accesses of files on PHIsystems by user.
File Changes in PHI Assets by Specific User	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays a count of the number of accesses of files on PHI systems by user.
Former Employee Account Access Attempt	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Lists all login activity from any former employee.

Resources for Workforce Security 164.308 (a)(3), continued

Resource	Type	URI	Description
Internal Reconnaissance Activities by a Specific Source	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This report shows all internal reconnaissance activities conducted by a particular source.
Internal Reconnaissance Activities to Specific Target	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This report shows all internal reconnaissance activities conducted by a particular source.
Internal Reconnaissance Sources	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This report shows the top sources conducting internal reconnaissance.
Internal Reconnaissance Top Events	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This report shows the top events executed for internal reconnaissance.
Internal Reconnaissance Top Targets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This report shows the top targets accessed by internal reconnaissance activity.
New Hire Internet Activity	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays all the identified internet activity performed by new users.
Summary of Suspicious Activity by New Hires	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Shows a summary of attacks and suspicious events by new hires.
Suspicious Activities by Former Employee	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Lists all suspicious activities by any former employee.

Resources for Workforce Security 164.308 (a)(3), continued

Resource	Type	URI	Description
Suspicious Activity by New Hires	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays all the identified suspicious activity performed by new users.
Unauthorized Access by Specific User	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This report displays all the unauthorized Access by Specific User, where the user provided as input, default admin.
Unsuccessful New Hire Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Displays all unsuccessful new hire logins within the last day.
Former Employee Account Activity	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Looks for any activity of users that have been placed on the Former Employees active list. This rule creates a case for each unique user name that is attempted in the ArcSight Solutions/Compliance Insight Package folder in the case tree.
Former Employee Account Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Detects events that list former employee accounts. When triggered, the rule adds as well as deletes users from the appropriate active lists.
Former Employee User Account Access Attempt	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Detects any authentication event, whether failed or successful, where the username has been placed on the Former Employees active list. This rule creates a case in the ArcSight Solutions folder in the case tree for each unique user name that is attempted.
Internal Recon Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This rule looks for internal reconnaissance activity.
New Hire Identification	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Looks for newly created or renamed user accounts. It writes the new user names to the New Hire Accounts active list.

Resources for Workforce Security 164.308 (a)(3), continued

Resource	Type	URI	Description
Suspicious Activities by Former Employee	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Detects Suspicious Activities events, where the username has been placed on the Former Employees active list. This rule creates a case in the ArcSight Solutions folder in the case tree for each unique user name that is attempted.
Suspicious Activities by New Hires	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Identifies suspicious activity by new hires.
Unauthorized File access on PHI assets	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	This rule looks for unauthorized file accesses on PHI assets.
User Logged in - Added to Active Accounts List	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(3) Workforce Security/	Adds a user account to the Active Users session list upon a successful login.

Information Access Management 164.308 (a)(4)

This section lists all resources under the Information Access Management group.

Resources for Information Access Management 164.308 (a)(4)

Resource	Type	URI	Description
Account Authorization Changes Summary	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows a real-time feed of events reflecting account access rights is attempted to be changed.
Privileged Account Changed	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows a real-time feed of events reflecting alteration of privileges. This is based on the related rule firing. Manager Receipt Time is used as the time-stamp of choice to retain the real-time nature of the channel.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
Removal of Access Rights	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows a live feed of events reflecting the removal of a user's access privileges.
Account Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows information related to user account activity.
Clearinghouse Entity Traffic Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	This dashboard shows information related to clearinghouse entity traffic activity.
Privileged Account Changes	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays information where changes have been made to an administrative account.
User Group Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows information related to user group activity.
Last 10 Privileged Account Changes	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays events where authorization/access changes have been made to an administrative account.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
Last 10 Traffic to Clearinghouse from other Network Domains	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	This data monitor provides the last 10 Traffic to clearinghouse entity from other network Domains
Last 20 Information System Accounts Created	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays the last 20 account creations.
Last 20 Information System Accounts Deleted	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays the last 20 account deletions.
Last 20 Information System Accounts Modified	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays the last 20 account modifications.
Last 20 User Group Created	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays the last 20 user group creations.
Last 20 User Group Deleted	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays the last 20 user group deletions.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
Last 20 User Group Modified	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays the last 20 user group modifications.
Top 10 Asset Network Domains with Account Creation Deletion and Modification	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays the Network Domains asset categories in which the most accounts have been created, modified or deleted.
Top 10 Privileged Account Changes	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays top changed administrative accounts.
Top 10 Traffic to ClearingHouse from other Network Domains	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	This data monitor provides the top10 Traffic to clearinghouse entity from other Network Domains.
Users Changing Accounts	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows the users that added, deleted and modified accounts.
Access Rights Changes	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Selects events where a change was attempted for account access rights.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
Account Creations, Modifications and Deletions	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Identifies all account management events.
Communications between Development and Operations	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	This filter identifies traffic between Development and Operations domains.
Communications between Development and Test	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	This filter identifies traffic between Development and Test domains.
Communications between Test and Operations	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	This filter identifies traffic between Test and Operations domains.
Privileged Account Changes	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Selects events where a change is attempted to a privileged account (as defined by the referenced active list).
Removal of Access Rights	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Identifies events indicating a user access right is removed. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.
Traffic from Others to Clearinghouse	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Selects all traffic destined for the development segment(s) of the network that did not originate from within a development segment.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
User Added to Group	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Identifies when a user is added to a group.
User Group Creation	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Identifies user group creation events.
User Group Deletion	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Identifies user group deletion events.
User Group Modification	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Identifies user group modification events.
User Removed from Group	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Identifies when a user removed from group.
Attempted File Changes in Clearinghouse Originated from Development Asset	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays attempts to change a file on a host in the clearinghouse segment from a source that is in Development.
Attempted File Changes in Clearinghouse Originated from Financial Asset	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays attempts to change a file on a host in the clearinghouse segment from a source that is Financial.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
Attempted File Changes in Clearinghouse Originated from Public-Facing	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays attempts to change a file on a host in the clearinghouse segment from a source that is in Public-Facing.
Attempted File Changes in Clearinghouse Originated from Test	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays attempts to change a file on a host in the clearinghouse segment from a source that is in Test.
Attempted File Changes in Clearinghouse Originated from Third Party	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Displays attempts to change a file on a host in the clearinghouse segment from a source that is in Third Party.
Account Authorization Changes Summary	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Lists details of events regarding changes to account authorization.
Account Creations	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Provides a listing of all Information System accounts that were created.
Account Creations in Network Domain - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Provides a listing of Information System accounts that were deleted in a specific network domain. By default, the Electronic PHI network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Account Deletions	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Provides a listing of all Information System accounts that were deleted.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
Account Deletions in Network Domain - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of Information System accounts that were deleted in a specific network domain. By default, the Electronic PHI network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Account Modifications	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of all Information System accounts that were modified.
Account Modifications in Network Domain - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of Information System accounts that were modified in a specific network domain. By default, the Electronic PHI network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Attacks from Business Associate Targeting Clearinghouse Entity	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of hostile or suspicious traffic from business associate machines targeting clearinghouse entity.
Attempted File Changes in Clearinghouse Assets originated from Other Network Domain - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Displays attempts to change a file on a host in the clearinghouse segment from a source that is in a specific network domain. By default, the Production network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Development and Test Cross-Talk	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides the cross-talk in the last 24 hours between assets in Development category and assets in Test category.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
Failed or Attempted Removal of Access Rights	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows all failed or attempted removal of access rights from a host resource.
Multiple Functions Implemented on a Clearinghouse Asset	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Returns all assets that implement multiple functionality, for example, a database and Web server installed on the same clearinghouse machine.
Operations and Development Cross-Talk	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Provides all cross-talk in the last 24 hours between assets in Operations category and assets in Development category.
Operations and Test Cross-Talk	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Provides all cross-talk in the last 24 hours between assets in Operations category and assets in Test category.
Privileged Account Change Details	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Lists details of events regarding changes to privileged accounts.
Successful Removal of Access Rights	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows all the removal of access rights from a host resource. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.
User Group Creations	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Provides a listing of all Information User Groups that were created.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
User Group Deletions	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of all Information User Groups that were deleted.
Users Added to Groups	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of all Information of Users which added to Groups.
Users Removed from Groups	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of all Information of Users which removed from Groups.
Account Authorization Changes Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Shows a summary of account authorization changes.
Account Creations	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Shows all account creations.
Account Creations in Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of Information System accounts that were created in a specific network domain. The network domain has to be specified at report runtime. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Account Deletions	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Shows all account deletions.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
Account Deletions in Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of Information System accounts that were deleted in a specific network domain. The network domain has to be specified at report runtime. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Account Modifications	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Shows all account modifications.
Account Modifications in Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of Information System accounts that were modified in a specific network domain. The network domain has to be specified at report runtime. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Attacks from Business Associate Targeting Clearinghouse Entity	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Provides a listing of hostile or suspicious traffic from business associate machines targeting clearinghouse entity.
Attempted File Changes in Clearinghouse Originated from Other Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Displays attempts to change a file on a host in the development segment from a source that is not in the development segment.
Development and Test Cross-Talk	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a) (4) Information Access Management/	Shows all cross-talk in the last 24 hours between assets in Development category and assets in Test category.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
Failed or Attempted Removal of Access Rights	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows all the attempts or failed removal of access rights from a host resource. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.
Multiple Functions Implemented on a Clearinghouse Asset	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Returns all assets that implement multiple functionality, for example, a database and Web server installed on the same machine.
Operations and Development Cross-Talk	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows all cross-talk in the last 24 hours between assets in Operations category and assets in Development category.
Privileged Account Change Details	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Lists details of events when an Privileged account was attempted to be changed
Successful Removal of Access Rights	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows the removal of access rights from a host resource. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.
Test and Operations Cross-Talk	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows all cross-talk in the last 24 hours between assets in Test category and assets in Operations category.
User Group Account Creations	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows all user group creations.

Resources for Information Access Management 164.308 (a)(4), continued

Resource	Type	URI	Description
User Group Account Deletions	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows all user group deletions.
Users Added to Groups	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows all user accounts added to groups.
Users Removed from Groups	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Shows all users accounts removed from groups.
Privileged Account Changes	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Fires whenever an access/authorization change is attempted to be made to an administrative account. A case is created for each such incident.
Removal of Access Rights	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(4) Information Access Management/	Triggers when events indicating the following are detected: 1). Either a user is removed from a host, or 2). User's authentication privileges are modified.

Security Awareness and Training 164.308 (a)(5)

This section lists all resources under the Security Awareness and Training group.

Resources for Security Awareness and Training 164.308 (a)(5)

Resource	Type	URI	Description
Failed Virus Removal Attempt	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Looks for events when an attempt to remove or quarantine a virus on a host failed.
Login Attempts	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows a real-time feed of logout events.
Logouts	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows a real-time feed of events where a login attempt was made.
Malicious Code Activity	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	This active channel shows malicious code activity.
Security Software Stopped or Paused	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	This active channel shows events where a security service (as named in the filter tab) is stopped on a system.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Administrative Logins and Logouts	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows an overview of the administrative login and logouts activity on the organization.
Anti-Virus Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows an overview of the anti-virus activity on the organization.
General User Login Attempts	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows an overview of user login attempts on the organization.
Malicious Code Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows an overview of the malicious code activity on the organization.
Unsuccessful Administrative Login	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows an overview of unsuccessful administrative logins activity on the organization.
Unsuccessful User Logins	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows an overview of unsuccessful user activity on the organization.
User Logins and Logouts	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows an overview of the user login and logouts activity on the organization.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Anti-Virus Stopped or Paused	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the last state of systems that have had Anti-Virus services stopped or paused.
Last 10 Anti-Virus Service Stopped or Paused Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the last 10 Anti-Virus service stopped, paused, or disabled events.
Last 10 Failed Anti-Virus Updates	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the last 10 failed Anti-Virus updates.
Last 10 Malware Activity	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the last 10 Malware Activity events.
Last 10 Successful Administrative Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the last 10 successful administrative logins across your assets categorized in Network Domains.
Last 10 Successful Administrative Logouts	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the last 10 administrative logouts across your assets categorized in Network Domains.
Last 10 Successful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the last 10 successful logins by non-administrative users across your assets categorized in Network Domains.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Last 10 Successful User Logouts	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the last 10 successful non-administrative user logouts across your assets categorized in Network Domains.
Last 20 Unsuccessful Administrative Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the last 20 unsuccessful administrative logins across your assets categorized in Network Domains.
Last 20 Unsuccessful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the last 20 unsuccessful non-administrative user logins across your assets categorized in Network Domains.
Last 20 User Login Attempts	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows in real-time the last 20 login attempts for non-administrative users across your assets categorized in Network Domains.
Malicious Code Activity	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the malicious code activity between Attacker-Target pairs.
Top 10 Administrative Users with Successful Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the administrative attacker and target user name pairs with most successful logins.
Top 10 Administrative Users with Unsuccessful Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the administrative attacker and target user name pairs with most failed logins.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Top 10 Hosts with Successful Administrative Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the hosts with most successful administrative logins.
Top 10 Hosts with Unsuccessful Administrative Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the hosts with most unsuccessful administrative logins.
Top 10 Hosts with Unsuccessful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides an ordered list of hosts that most frequently have login failures for non-administrative users.
Top 10 Malwares	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of the top 10 malware activity.
Top 10 Network Domains with Successful Administrative Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides an ordered list of the Network Domains with most successful administrative logins.
Top 10 Network Domains with Unsuccessful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides an ordered list of the Network Domains that most frequently have non-administrative user login failures.
Top 10 Users with Unsuccessful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides an ordered list of non-administrative users who most frequently have failed logins.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Top User Login Activity	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the top 20 non-administrative users attempting to login to a system.
Unsuccessful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Reports on a moving average of the number of unsuccessful user logins.
User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Reports on a moving average of the number of user logins.
Anti-Virus Clean or Quarantine Attempt	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Looks for anti-virus events that indicate a quarantine or cleaning attempt of a detected malware instance.
Anti-Virus Service Stopped or Paused	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Selects events where any of the named security services are stopped on any system. Refer to the Filter tab for the list of such services.
Anti-Virus Service Stopped or Paused in Windows	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Selects Windows events where any of the named security services are stopped on any system. Refer to the Filter tab for the list of such services.
Failed Anti-Virus Updates	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Looks for events when an attempt to update a virus signature on a host failed.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Failed Password Change	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Identifies unsuccessful password change events.
Failed Virus Removal Attempt	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Looks for events when an attempt to remove/quarantine a virus on a host failed.
Malicious Code Activity	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Selects events where malicious code activity is detected.
Malware Activity	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Identifies virus and other malware activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Password Change Attempts	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Identifies password change attempts. By default it only identifies these events on Microsoft Windows systems. Configure this filter to identify password change events from other systems as necessary.
Potential Trojan Inside Network	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Selects events where a trojan is likely to be present inside the company network.
Spyware Activity	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Identifies spyware activity reported by either an Intrusion Detection System (IDS) or an anti-virus application.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Successful Password Change	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Identifies successful password change events.
Trojan Activity	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Selects events where trojan activity is detected.
Virus Activity	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Identifies virus activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Worm Activity	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Identifies worm activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Administrative Logins and Logouts per User	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of administrative logins and logouts per user name.
All Password Change Events	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of all password change events and their outcome.
All User Logins per User	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of user logins per user name.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Anti-Virus Stopped or Paused in the Last Month	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows all events when a anti-virus service is stopped or paused in the last month.
Count of Administrative Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all successful administrative logins.
Daily Anti-Virus Stopped or Paused - Trend Base	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows all events when a anti-virus service is stopped or paused on systems.
Daily Count of Successful User Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Retreives information about the number of successful non-administrative user logins every day over the past week.
Daily Count of Unsuccessful User Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Counts the number of unsuccessful daily user logins.
Daily Successful Administrative Logins per Hour	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the hourly number of successful administrative logins.
Daily Unsuccessful Administrative Logins per Hour	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the hourly number of unsuccessful administrative logins.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Detected Malware Summary by Hosts	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows a summary of malware detected on systems sorted by host.
Failed Anti-Virus Updates	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows all the failed Anti-Virus updates on systems.
Failed Password Changes	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Retrieves failed password change events, ordered by target user name.
Malicious Code Activities from External Sources	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows all malicious code activities from external sources.
Malicious Code Activities from Internal Sources	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows all malicious code activities from internal sources.
Number of Daily User Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Captures the number of logins per user and outcome over the entire day.
Number of Successful Administrative Logins by User and Host Information	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of administrative users with successful logins grouped by user and host information. The administrative users are sorted by the number of attempts in a decreasing order.may (and should) be focused based on the Network Domain of interest.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Number of Unsuccessful Administrative Logins by User and Host Information	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of administrative users with unsuccessful login attempts, grouped by user and host information. The administrative users are sorted by the number of attempts in a decreasing order. This query may be focused based on the Network Domain of interest.
Passwords not Changed for Longer than Policy Standard	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Lists accounts for which the password was not changed for longer than the policy standard permits.
Successful Administrative Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all successful Administrative logins within the last day.
Successful Administrative Logins in the Last 2 Hours	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all unsuccessful administrative logins within the last 2 hours.
Successful Administrative Logins to PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all successful Administrative logins within the last day.
Successful Password Changes	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Lists successful password change events, ordered by target user name.
Successful User Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all successful user logins within the last day.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Successful User Logins by Hour	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Retrieves the number of non-administrative successful user logins per hour.
Successful User Logins to PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all successful user logins within the last day.
Top External Sources with Malicious Code Activities	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the top external sources with most malicious code activities.
Top Hosts with Most Malware Activities	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Finds the top 10 systems with the most malware activities (routine maintenance and remediation events).
Top Hosts with Most Spyware Activities	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Finds the top 10 systems with most spyware activities (routine maintenance and remediation events).
Top Hosts with Most Virus Activities	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the top hosts with most virus activities detected on systems.
Top Internal Sources with Malicious Code Activities	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the top internal sources with most malicious code activities.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Top Malware Instances	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides the names of the top 10 detected malware instances.
Top Spyware Instances	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides the names of the top 10 detected spyware instances.
Top Virus Instances	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows a summary of virus activities detected on systems sorted by virus.
Trend of Unsuccessful Administrative Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the trend of unsuccessful administrative logins over long term.
Unsecured Password Events	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Retrieves unsecured password events
Unsuccessful Administrative Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all unsuccessful administrative logins within the last day.
Unsuccessful Administrative Logins - Long Term Trend	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Counts the number of failed administrative logins per attacker user name, target user name and target address per month.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Unsuccessful Administrative Logins in the Last 2 Hours	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all unsuccessful administrative logins within the last 2 hours.
Unsuccessful Administrative Logins to PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all unsuccessful administrative logins within the last day.
Unsuccessful User Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all unsuccessful user logins within the last day.
Unsuccessful User Logins by Hour	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Retrieves the number of non-administrative successful user logins per hour.
Unsuccessful User Logins to PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all unsuccessful user logins within the last day.
User Local Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of local login events to a MS Windows or UNIX system.
User Logins and Logouts	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of user logins and logouts within the last day.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Worm Activity	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows all worm activity.
Password Changes	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows all password change events.
Successful Administrative Logins in the Last 2 Hours	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all successful administrative logins in the last 2 hours. It Provides drill-downs into various fields.
Unsuccessful Administrative Logins in the Last 2 Hours	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows details of all unsuccessful administrative logins in the last 2 hours. It Provides drill-downs into various fields.
Administrative Logins and Logouts per User	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of administrative logins and logouts per target or attacker user name.
All Password Change Events	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a list of all password change events, ordered by the time in which they occurred.
All User Logins per User	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of all logins for a particular user.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Anti-Virus Stopped or Paused in the Last Month	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows all events when Anti-Virus is stopped or paused in the last month.
Daily Successful Administrative Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of successful administrative login attempts.
Daily Successful Administrative Logins to PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of successful administrative login attempts.
Daily Successful User Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of successful user login attempts.
Daily Successful User Logins to PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of successful user login attempts.
Daily Unsuccessful Administrative Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of unsuccessful administrative login attempts.
Daily Unsuccessful Administrative Logins to PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of unsuccessful administrative login attempts.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Daily Unsuccessful User Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of unsuccessful user login attempts.
Daily Unsuccessful User Logins to PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of unsuccessful user login attempts.
Daily User Logins and Logouts	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Provides a listing of user logins and logouts events.
External Malicious Code Sources	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows information about the external sources of malicious code activities.
Failed Anti-Virus Updates	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows all the failed Anti-Virus updates.
Failed Password Changes	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Displays failed password change events.
Internal Malicious Code Sources	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows information about the internal sources of malicious code activities.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Malware Activities	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows an overview of malware activities.
Malware Activity Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows a summary of virus activities detected on systems, sorted by host.
Monthly Trend of Unsuccessful Administrative Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows different aspects of the trend of unsuccessful administrative logins in the last 16 weeks.
Number of Successful Administrative Logins by User and Host	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the hourly number of successful administrative logins and a list of those logins, grouped by user and host information.
Number of Successful User Logins over the Past Week	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the number of successful user logins every day over the past week.
Number of Successful User Logins per Hour over the Past Day	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the number of non-administrative successful user logins per hour.
Number of Unsuccessful Administrative Logins by User and Host	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the hourly number of unsuccessful administrative logins, and a listing of those attempts, grouped by user and host information.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Number of Unsuccessful User Logins over the Past Week	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the number of unsuccessful user logins every day over the past week.
Number of Unsuccessful User Logins per Hour over the Past Day	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows the number of unsuccessful user logins every hour over the past day.
Passwords not Changed for Longer than Policy Standard	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Lists passwords that were not changed for longer than the policy standard.
Spyware Activities	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows an overview of spyware activities.
Successful Password Changes	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Displays successful password change events.
Unsecured Password Events	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Displays unsecured password events.
User Local Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows local login events to a MS Windows or UNIX system.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Virus Activities	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows a summary of virus activities detected on systems sorted by virus.
Worm Activity Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Shows a summary of worm activities detected on systems, sorted by host.
Consecutive Unsuccessful Logins to Administrative Account	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Fires when it notices a set of 10 consecutive unsuccessful logins by an attacker and target user name pair within 5 minutes.
Malware or Spyware Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Triggers when a spyware or malware activity is reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Password not Changed for Longer than Policy Standard	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Fires when an entry expires out of the referenced active list, signifying that the new (default) password was not changed within the prescribed time. Time limit is defined by the TTL in the active list.
Security Software Stopped or Paused	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Triggers when a security software service has been disabled.
Successful Password Change	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Detects when a user's password is changed.will then take the user name off the list where it was kept to track whether or not the default password was changed.

Resources for Security Awareness and Training 164.308 (a)(5), continued

Resource	Type	URI	Description
Suspicious Internal Trojan Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Triggers when there are trojan events coming from inside the network or successful trojan events from outside the network.
Unsuccessful Logins to Multiple Administrative Accounts	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Fires when it notices a set of 20 continuous unsuccessful logins by different administrative attacker and target user pairs within 5 minutes .
Worm Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Triggers when a worm is reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Count of Administrative Logins	Trend	/All Trends/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Stores a count of successful and unsuccessful administrative logins.
Daily Trend of Anti-Virus Stopped or Paused Events	Trend	/All Trends/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Stores all events when an Anti-Virus service is stopped or paused.
Failed Administrative Logins - Long Term Trend	Trend	/All Trends/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Stores long term information about failed administrative logins.
User Login Count	Trend	/All Trends/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Stores a daily count of user login attempts.

Security Incident Procedures 164.308 (a)(6)

This section lists all resources under the Security Incident Procedures group.

Resources for Security Incident Procedures 164.308 (a)(6)

Resource	Type	URI	Description
All Attacks and Suspicious Activity Events	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This active channel shows all attack and suspicious activity events.
Attacks and Suspicious Activity Targeting PHI Resources	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This active channel shows all attack and suspicious activity events where the target is an asset from Electronic PHI asset category.
Attacks and Suspicious Activity Targeting Public Facing Resources	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This active channel shows all events where the target asset or zone is categorized in the Public-Facing asset category.
Attacks and Suspicious Activity Targeting Third Party Resources	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This active channel shows all attack and suspicious activity events where the target is an asset from Third Party asset category.
Attacks and Suspicious Activity from PHI Resources	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This active channel shows all attack and suspicious activity events where the attacker is an asset from Electronic PHI asset category.

Resources for Security Incident Procedures 164.308 (a)(6), continued

Resource	Type	URI	Description
Attacks and Suspicious Activity from Public Facing Resources	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This active channel shows all attack and suspicious activity events where the source asset or zone is categorized in the Public-Facing asset category.
Attacks and Suspicious Activity from Third Party Resources	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This active channel shows all attack and suspicious activity events where the attacker is an asset from Third Party asset category.
Attacks and Suspicious Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This dashboard displays information about attacks and suspicious activity events.
Attacks and Suspicious Activity Event Names - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This data monitor shows connections between source and destination machines and event names as they appear in attack and suspicious activity events.
Attacks and Suspicious Activity Event Ports - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This data monitor shows connection between source and destination machines and ports as they appear in attack and suspicious activity events.
Last 20 Attacks and Suspicious Activity Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This data monitor displays the last 20 attack and suspicious activity events.

Resources for Security Incident Procedures 164.308 (a)(6), continued

Resource	Type	URI	Description
Ports Used in Attacks and Suspicious Activity Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This data monitor shows the ports used in attack and suspicious activity events. By default the data monitor shows data from the last 5 minutes.
DoS Attacks	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This filter identifies denial of service attacks.
HIPAA Case Created	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This filter identifies events where a new case is created.
Information Security Incidents	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This filter identifies various kinds of information security incidents such as malicious code activities, denial of service attacks and policy violations.
Attacks and Suspicious Activities	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query provides a listing of all hostile or suspicious events sorted by the event's end time.
Attacks and Suspicious Activities Trend	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query summarizes the number of attacks and suspicious activities for long term reporting.
Average Time to Resolution - By Case Severity	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows the Average Time to Resolution by Case Severity. It should be run once a week and reported to management.

Resources for Security Incident Procedures 164.308 (a)(6), continued

Resource	Type	URI	Description
Average Time to Resolution - By Day	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows the average time to resolution of all the closed cases by day. This query should be run once a week and reported to management.
Average Time to Resolution - By User	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows how long it takes individuals to close their cases. This query should be run once a week and reported to management.
Case Audit Events - Trend Base	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query collects Time to Resolution (TTR) information from case audit events and stores them in a trend for case history reporting.
Case Status by Owner	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query provides a breakdown by owner of all cases.
Cases by Stage	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query provides an overview of all cases in their current stages.
Count of Attacks and Suspicious Activities Per Attacker Machine	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query provides a count of attacker addresses appearing in of hostile or suspicious events.
Count of Attacks and Suspicious Activities Per Target Machine	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query provides a count of target addresses appearing in of hostile or suspicious events.

Resources for Security Incident Procedures 164.308 (a)(6), continued

Resource	Type	URI	Description
Count of Attacks and Suspicious Activity Event Names	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report counts the names of attack and suspicious activity events.
Count of Attacks and Suspicious Activity Event Names on Network Domains	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report counts the names of attack and suspicious activity events on a particular Network Domain.
Count of Attacks and Suspicious Activity Per Day	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query counts the total number of weekly attack and suspicious activity events.
HIPAA 164.308 Case Overview	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows the number of open cases per stage for cases that have been created as a result of HIPAA 164.308 section rules actions.
HIPAA 164.310 Case Overview	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows the number of open cases per stage for cases that have been created as a result of HIPAA 164.310 section rules actions.
HIPAA 164.312 Case Overview	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows the number of open cases per stage for cases that have been created as a result of HIPAA 164.312 section rules actions.
Open Cases	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows all currently open cases.

Resources for Security Incident Procedures 164.308 (a)(6), continued

Resource	Type	URI	Description
Open Cases by HIPAA Section	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows all currently open cases by HIPAA sections.
Open Cases by HIPAA Section and Severity	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows a breakdown of open cases by severity for each regulation section.
Open Cases by Severity	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows the number of open cases by severity.
Top DoS Attackers	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows the top attackers responsible for initiating denial of service attacks.
Top DoS Targets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query shows hosts which were targeted the most with denial of service attacks.
Trend of Attacks and Suspicious Activities By Attacker Address	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query provides a weekly count of attacker addresses appearing in hostile or suspicious events.
Trend of Attacks and Suspicious Activities By Target Address	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query provides a weekly count of target addresses appearing in hostile or suspicious events.

Resources for Security Incident Procedures 164.308 (a)(6), continued

Resource	Type	URI	Description
HIPAA 164.308 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query viewer shows the number of open cases per stage for cases that have been created as a result of HIPAA 164.308 rule actions.
HIPAA 164.310 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query viewer shows the number of open cases per stage for cases that have been created as a result of HIPAA 164.310 rule actions.
HIPAA 164.312 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This query viewer shows the number of open cases per stage for cases that have been created as a result of HIPAA 164.312 rule actions.
Attacks and Suspicious Activities	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report displays a count of the event names of attack and suspicious activity events.
Attacks and Suspicious Activity Weekly Trend	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report displays a weekly overview of attack and suspicious activity events.
Average Time to Resolution - By Case Severity	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report will show the Average Time to Resolution by Case Severity. It should be run once a week and reported to management.

Resources for Security Incident Procedures 164.308 (a)(6), continued

Resource	Type	URI	Description
Average Time to Resolution - By Day	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report shows the average time to resolution of all the closed cases by day. This report should be run once a week and reported to management.
Average Time to Resolution - By User	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report shows how long it is taking individuals to close their cases. This report should be run once a week and reported to management.
Cases by Stage	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report provides an overview of all cases and their current stages.
Count of Attacks and Suspicious Activities per Attacker Machine	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This reports shows a count of attack and suspicious activity events per attacker machine.
Count of Attacks and Suspicious Activities per Target Machine	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This reports shows a count of attack and suspicious activity events per target machine.
Count of Attacks and Suspicious Activity Event Names	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report displays a count of the event names of attack and suspicious activity events sorted by the most common events. It also displays the number of unique target machines that were affected by the event.
Count of Attacks and Suspicious Activity Event Names in the Network Domain	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report displays a count of the event names of attack and suspicious activity events in a particular Network Domain sorted by the most common events. It also displays the number of unique target machines that were affected by the event. The Network Domain of interest should be specified at report runtime (default: PHI Network Domain).

Resources for Security Incident Procedures 164.308 (a)(6), continued

Resource	Type	URI	Description
HIPAA Open Cases Overview	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report shows all currently open cases by HIPAA Section.
Open Cases by HIPAA Section and Severity	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report shows all currently open cases by HIPAA Section and Severity.
Open Cases by Owner	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report provides a breakdown by owner of all open cases.
Open Cases by Severity	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report shows all currently open cases by severity.
Top DoS Attackers	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report shows a list of top attackers responsible for initiating denial of service attacks.
Top DoS Targets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This report shows hosts which were targeted the most with a denial of service attack.
Information Security Incident	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This rule fires for various kinds of information security incidents such as malicious code activities, denial of service attacks and policy violations.

Resources for Security Incident Procedures 164.308 (a)(6), continued

Resource	Type	URI	Description
Multiple Cases Created on Short Period	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This rule triggers when multiple cases created on short period of time.
Attacks and Suspicious Activities Trend	Trend	/All Trends/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This trend stores long term aggregated information about attacks and suspicious activity events.
Case History	Trend	/All Trends/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	This trend stores all case audit events.

Contingency Plan 164.308 (a)(7)

This section lists all resources under the Contingency Plan group.

Resources for Contingency Plan 164.308 (a)(7)

Resource	Type	URI	Description
Critical Assets Resource Exhaustion	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This active channel shows critical systems resource exhaustion.
Critical Systems Startup and Shutdown	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This active channel shows critical systems startup and shutdown events .
Information System Failures on Critical Assets	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This active channel looks for information system failures on critical assets.

Resources for Contingency Plan 164.308 (a)(7), continued

Resource	Type	URI	Description
Up Down Status of Highly Critical Assets	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This Last State data monitor shows the state of highly critical assets and whether they are up or down.
Last 10 Shutdowns of Highly Critical Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This data monitor displays the last 10 Shutdowns of Highly Critical Assets .
Top 10 Shutdowns of Highly Critical Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This data monitor shows the 10 highly critical assets with top shutdowns .
Up Down Status of Highly Critical Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This Last State data monitor shows the state of highly critical assets and whether they are up or down.
Information System Failures	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This filter identifies information system failures.
Resource Exhaustion	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shows resources reaching their upper end of utilization (for capacity management and planning purposes).
Startup and Shutdown of Highly Critical Assets	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This filter identifies startups and shutdowns of highly critical machines.
System Shutdown	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This filter identifies system shut downs.

Resources for Contingency Plan 164.308 (a)(7), continued

Resource	Type	URI	Description
System Shutdown of Highly Critical Assets	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This filter identifies system shut downs of highly critical assets.
System Startup	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This filter identifies system startups.
Resource Exhaustion Detected on Business Associate Systems	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on Business Associate domain.
Resource Exhaustion Detected on Clearinghouse Systems	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on Clearinghouse systems.
Resource Exhaustion Detected on Critical Assets	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This report shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on critical assets.
Resource Exhaustion Detected on PHI Systems	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on PHI domain.
Resource Exhaustion Detected on Production Systems	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on production domain.
Resource Exhaustion Detected on Public Facing Systems	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on public facing systems.

Resources for Contingency Plan 164.308 (a)(7), continued

Resource	Type	URI	Description
Fault Logs on Critical Machines	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This query shows events indicating a process has failed to execute in the expected way on critical machine.
Information System Failures per Critical Machines	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This query shows the critical information system which generated error log entries.
Resource Exhaustion Detected	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shows resources reaching their upper end of utilization (for capacity management and planning purposes).
Resource Exhaustion Detected - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shows resources reaching their upper end of utilization (for capacity management and planning purposes) on network domain (default development domain) .
Shutdown of Critical Machines	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This query shows all shutdown events of machines categorized as critical or highly critical.
Weekly Trend - Shutdown of Critical Machines per Day	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This query is based on trend "Shutdown of Critical Machines" and shows all weekly shutdown events of machines which categorized as critical.
Weekly Trend -Top 10 Shutdowns of Highly Critical Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This query is based on trend "Shutdown of Critical Machines" and shows top 10 shutdowns of critical assets on the last week.
Fault Logs on Critical Machines	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This report shows events indicating a process has failed to execute in the expected way on critical machines.

Resources for Contingency Plan 164.308 (a)(7), continued

Resource	Type	URI	Description
Information System Failures per Critical Machines	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This report shows the critical information system which generated error log entries.
Resource Exhaustion Detected	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes).
Resource Exhaustion Detected on Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on network domain (default development domain) .
Shutdown of Critical Machines	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This report shows all shutdown events of machines categorized as critical on the last day.
Weekly Trend - Shutdown of Critical Machines	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This report shows a weekly trend of critical machines shutdown.
Information System Failures of Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This rule looks for information system failure events from highly critical machines.

Resources for Contingency Plan 164.308 (a)(7), continued

Resource	Type	URI	Description
Resource Exhaustion of Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This rule looks for Resource Exhaustion events from highly critical machines.
Shutdown of Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This rule looks for shutdown events from highly critical machines.
Shutdown of Critical Machines	Trend	/All Trends/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	This trend stores long term aggregated information about shutdown of critical machines.

Evaluation 164.308 (a)(8)

This section lists all resources under the Evaluation group.

Resources for Evaluation 164.308 (a)(8)

Resource	Type	URI	Description
Database Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Looks for database configuration change events.
Firewall Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Looks for firewall configuration change events.
Network IDS Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This active channel looks for NIDS configuration changes events.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Network Routing Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Looks for network routing configuration change events.
Software Changes in Operations	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Looks for events that indicate software changes on operations assets.
VPN Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Looks for VPN configuration change events.
Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Displays information about configuration changes.
Firewall Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Displays information about firewall configuration changes.
Missing Security Patches	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Displays missing security patches.
Network Devices Configuration Changes Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Displays information about network devices equipment (such as router, switch, NIDS) configuration changes.
Operating Systems Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Displays information about OS configuration changes.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Last 10 Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks the most recent system configuration modifications.
Last 10 Firewall Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks the most recent firewall configuration modifications.
Last 10 Network Devices Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks the most recent network devices configuration modifications.
Last 10 Network IDSs Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks the most recent NIDSs configuration modifications.
Last 10 Network Routing Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks the most recent network routing configuration modifications.
Last 10 Operating Systems Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks the most recent OS configuration modifications.
Last 10 Security Patch Missing Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Displays in real-time the last 10 security patch missing events.
Top 10 Assets missing Security Patches	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows real-time display of the top 10 assets with security patches missing.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Top 10 Configuration Modifications Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks the top 10 system configuration modifications.
Top 10 Devices with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Provides a list of the assets that have their configurations changed frequently.
Top 10 Firewall Configuration Modifications Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks the top 10 firewall configuration modifications.
Top 10 Firewalls with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Provides a list of the Firewalls that have their configurations changed frequently.
Top 10 Network Devices with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Provides a list of the network devices that have their configurations changed frequently
Top 10 Network IDSs with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Provides a list of the NIDSs that have their configurations changed frequently.
Top 10 Network Routings with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Provides a list of the network routings equipment that have their configurations changed frequently.
Top 10 Operating Systems Configuration Modifications Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks the top 10 OS configuration modifications.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Top 10 Operating Systems with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Provides a list of the operating systems that have their configurations changed frequently.
Configuration Modifications	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Detects non-arcsight configuration modifications events.
Database Configuration Modification	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Detects database configuration modifications.
Driver Loaded	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This filter selects events where driver is loaded.
Driver Unloaded	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This filter selects events where driver is unloaded.
Firewall Configuration Modifications	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks events when the configuration of a firewall is changed.
Module Loaded	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This filter selects events where Module is loaded.
Module Unloaded	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This filter selects events where Module is unloaded.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Network Device Configuration Modifications	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks events when the configuration of an infrastructural equipment (router, switch) is changed.
Network IDS Configuration Modifications	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks events when the configuration of NIDS equipment is changed.
Network Routing Configuration Modifications	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Tracks events when a modification to the routing table of infrastructure equipment (router, switch) is made.
Security Patch Missing	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Selects events indicating that a security patch is missing.
Software Changes	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Detects all changes to any software installed.
Software Installed	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This filter selects events where software is installed.
Software Uninstalled	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This filter selects events where software is un-installed.
Successful Modifications to Operating Systems	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Identifies successful configuration modifications to operating systems.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
VPN Configuration Modifications	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Selects events indicating that a VPN configuration change has occurred.
Windows Domain Policy Changed	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Selects events indicating that a Windows domain policy was changed.
Windows Group Policy Changed	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Selects events indicating that a windows group policy was changed.
Windows Scheduled tasks Created	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Selects Windows scheduled tasks created events.
Windows Services Installed	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Selects Windows service installed events.
Application Configuration Modifications on Operations	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows any configuration modifications of any application on operations. Default time window: Last 24 hours.
Changes to Software Packages on Critical Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This query shows all changes to software packages on critical assets.
Configuration Changes - Trend Base	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Retrieves all configuration changes for the last hour and used as trend base query for the Configuration Changes trend.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Firewall Configuration Modifications	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows any configuration modifications of any firewall. Default time window: Last 24 hours.
Firewall Configuration Modifications by Name	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top configuration modifications of any firewall.
Missing Security Patches Summary	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Provides overview of the missing security patches summary.
Network Device Configuration Modifications	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows any configuration modifications of any network equipment.
Network Device Configuration Modifications by Name	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top configuration modifications of network equipment.
Network Routing Changes	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows all routing configuration modifications.
Network Routing Changes by Name	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top router configuration modifications.
Open Firewall Port Details	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This query gives details of all the ports that are allowed to pass through various firewalls.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Software Changes in Operations	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows all changes to any software installed in the operations network segment.
Successful Changes to Operating Systems	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the number of times changes were made to operating systems.
Successful Database Configuration Modification	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows all events of database configuration modifications.
Top Firewalls with Most Successful Configuration Modifications	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top firewalls with most successful configuration modifications.
Top Network Devices with Most Successful Configuration Modifications	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top network devices with most successful configuration modifications.
Top Network Devices with Most Successful Network Routing Changes	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows top routers/switches with most successful routing configuration modifications.
Top Users with Most Successful Firewall Modifications	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top users who made most successful configuration modifications.
Top Users with Most Successful Network Devices Configuration Modifications	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top users with most successful configuration modifications.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Weekly Trend - Configuration Changes by Address	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top configuration modifications by ip address.
Weekly Trend - Configuration Changes by Name	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top configuration modifications.
Weekly Trend - Configuration Changes by User	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top configuration modifications by user.
Windows Domain Policy Changes	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Lists all the changes to Microsoft Active Directory.
Windows Group Policy Changes	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This query lists all the changes to Microsoft Active Directory.
Windows Scheduled Tasks Created	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows all Windows scheduled tasks created.
Windows Services Installed	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows all Windows services installed.
Application Configuration Modifications on Operations	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows any configuration modifications of any application on a system on operations. Default time window: Last 24 hours.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Changes to Software Packages on Critical Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This report shows all changes to software packages on critical assets on the last day.
Database Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows database configuration changes.
Firewall Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows several top-level views related to firewall configuration modifications.
List of Firewall Configuration Modifications	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows any configuration modifications of any firewall.
List of Network Device Configuration Modifications	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows any configuration modifications of any network equipment. Default time window: Last 24 hours.
List of Network Routing Modifications	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows all routing configuration modifications.
Missing Security Patches Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows missing security patches summary. Default time window: Last 24 hours.
Network Device Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows several top-level views of configuration modifications of any network equipment.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Network Routing Modification Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows the top routers with routing configuration modifications, and top routing modifications.
Open Firewall Port Details	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This report gives details of all the ports that are allowed to pass through various firewalls.
Software Changes in Operations	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows any configuration modifications of any application on a system on operations. Default time window: Last 24 hours.
Successful Changes to Operating Systems	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Displays the number of times changes were made to operating systems.
Weekly Trend - Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows several top-level views related to configuration modifications.
Windows Domain Policy Changes	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Displays changes to Microsoft Domain Policy for the last 24 hours.
Windows Group Policy Changes	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Displays changes to Microsoft Active Directory for the last 24 hours.
Windows Scheduled Tasks Created	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows all Windows scheduled tasks created.

Resources for Evaluation 164.308 (a)(8), continued

Resource	Type	URI	Description
Windows Services Installed	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Shows all installed Windows services and the time of the installation.
Critical Network Device Configuration Change Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Triggers when a network device configuration change is detected and has Very-High agent severity. Devices include: Firewalls VPNs Network Equipment Network Routings Network Intrusion Detection Systems
Critical Operating System Change Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Triggers when operating system change is detected on critical asset and has Very-High agent severity.
Module Loaded or Unloaded on Critical Asset	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	This rule triggers when a module is loaded or unloaded on critical asset.
Security Patch Missing	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Triggers when a security patch missing vulnerability is detected.
Configuration Changes	Trend	/All Trends/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation/	Collects hourly data using the Configuration Changes Trend Base query. Used by other queries to show configuration changes.

Business Associate Contracts and Other Arrangements 164.308 (b)(1)

This section lists all resources under the Business Associate Contracts and Other Arrangements group.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1)

Resource	Type	URI	Description
Attacks and Suspicious Activity Targeting Business Associate Resources	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This active channel shows all attack and suspicious activity events where the target is an asset from Business Associate asset category.
Attacks and Suspicious Activity from Business Associate Resources	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This active channel shows all attack and suspicious activity events where the attacker is an asset from Business Associate asset category.
Attacks and Suspicious Activity to and from Third Party Resources	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This dashboard displays information about third party assets involved in attacks and suspicious behavior.
Information Leaks from Business Associate	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This dashboard displays information around information leakage from Business Associate.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1), continued

Resource	Type	URI	Description
Attacks and Suspicious Activity Events in the Third Party Network Domain - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This data monitor shows connection between source and destination machines and ports as they appear in attack and suspicious activity events in the Third Party Network Domain.
Last 20 Attacks and Suspicious Activity Events Targeting Third Party Resources	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This data monitor displays the last 20 attack and suspicious activity events where the traffic is destined for a Third Party asset or zone.
Last 20 Attacks and Suspicious Activity Events from Third Party Resources	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This data monitor displays the last 20 attack and suspicious activity events where the traffic originated from a Third Party asset or zone.
Organizational Records Leak from Business Associate	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This data monitor displays a graph with events which pertain to information leaks of organizational records from Business Associate.
Personal Information Leak from Business Associate	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This data monitor shows communications pertaining to personal information leaks from Business Associate.
Ports Used in Attacks and Suspicious Activity Events Targeting Third Party Resources	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This data monitor shows the ports used in attack and suspicious activity events that targeted Third Party assets or zones. By default the data monitor shows data from the last 5 minutes.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1), continued

Resource	Type	URI	Description
Ports Used in Attacks and Suspicious Activity Events from Third Party Resources	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This data monitor shows the ports used in attack and suspicious activity events that originated from Third Party assets or zones. By default the data monitor shows data from the last 5 minutes.
Attacks and Suspicious Activity Targeting Business Associate Resources	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This filter identifies attack and suspicious activity events targeting assets or zones categorized in the business associate category.
Attacks and Suspicious Activity Targeting Third Party Resources	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This filter identifies attack and suspicious activity events targeting assets or zones categorized in the Third Party asset category.
Attacks and Suspicious Activity from Business Associate Resources	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This filter identifies attack and suspicious activity events that are generated by assets categorized in the business associate category.
Attacks and Suspicious Activity from Third Party Resources	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This filter identifies attack and suspicious activity events that are generated by assets categorized in the Third Party asset category.
Attacks and Suspicious Activity to and from Third Party Resources	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This filter identifies attack and suspicious activity events targeting or originating from assets or zones categorized in the Third Party asset category.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1), continued

Resource	Type	URI	Description
Organizational Records Information Leak	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This filter identifies information leaks with regard to company information.
Organizational Records Information Leak from Business Associate Resources	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This filter identifies information leaks with regard to company information from Business Associate Resources.
Personal Information Leak	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This filter selects events which indicate a personal information leak.
Personal Information Leak from Business Associate Resources	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This filter selects events which indicate a personal information leak from Business Associate Resources.
Successful Administrative Logins from Third Party Systems	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	The purpose of this filter is to identify successful logins with an administrative account from third party systems. Third party systems have to be modeled as assets in ESM and be categorized as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.
Successful Administrative Logins to Third Party Systems	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	The purpose of this filter is to identify successful logins with an administrative account to third party systems. Third party systems have to be modeled as assets in ESM and be categorized as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1), continued

Resource	Type	URI	Description
Successful User Logins from Third Party Systems	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	The purpose of this filter is to identify successful non-administrative logins from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.
Successful User Logins to Third Party Systems	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	The purpose of this filter is to identify successful non-administrative logins to third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.
Unsuccessful Administrative Logins from Third Party Systems	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	The purpose of this filter is to identify failed logins using an administrative account from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.
Unsuccessful Administrative Logins to Third Party Systems	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	The purpose of this filter is to identify failed administrative logins to Third Party Assets. Third Party systems have to be modeled as assets in ESM and be categorizes as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.
Unsuccessful User Logins from Third Party Systems	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	The purpose of this filter is to identify failed non-administrative logins from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.
Unsuccessful User Logins to Third Party Systems	Filter	/All Filters/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	The purpose of this filter is to identify failed non-administrative logins to third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1), continued

Resource	Type	URI	Description
Top 10 Vulnerabilities - Business Associate Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report shows the top 10 vulnerabilities exposed on the Business Associate Entity.
Top 10 Vulnerable Assets - Business Associate Entity	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	Shows the top 10 vulnerable assets on business Associate assets.
Attacks and Suspicious Activities Targeting Business Associate	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query provides a listing of all hostile or suspicious events targeting Business Associate sorted by the event's end time.
Attacks and Suspicious Activities from Business Associate Targeting PHI Asset	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query provides a listing of all hostile or suspicious events from Business Associate domain targeting PHI assets sorted by the event's end time.
Business Associate Access	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query shows all access attempts to assets by Business Associate.
Organizational Information Leaks Originated from Business Associate	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query shows events which indicate a organizational information leak originated from business associate assets.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1), continued

Resource	Type	URI	Description
Personal Information Leaks Originated from Business Associate	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query shows events which indicate a personal information leak originated from business associate assets.
Reconnaissance from Business Associate Targeting PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query shows reconnaissance activity from assets in the Business Associate domain targeting assets in the PHI domain.
Successful Administrative Logins from Third Party Systems	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query retrieves successful logins with an administrator account from assets categorized as Third Party.
Successful Administrative Logins to Third Party Systems	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query identifies successful logins with an administrative account to third party systems.
Successful User Logins from Third Party Systems	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query retrieves successful logins using a non-administrative account, from assets categorized as Third Party.
Successful User Logins to Third Party Systems	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query retrieves successful logins using a non-administrative account, to assets categorized as Third Party.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1), continued

Resource	Type	URI	Description
Third-Party Incidents - Closed Cases	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query shows all cases involving third-party systems and business associate that have been closed.
Third-Party Incidents - Open Cases	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query shows all cases involving third-party systems and business associate that are still open.
Unsuccessful Administrative Logins from Third Party Systems	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query retrieves failed logins using an administrative account, from assets categorized as Third Party.
Unsuccessful Administrative Logins to Third Party Systems	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query retrieves failed logins using an administrative account, to assets categorized as Third Party.
Unsuccessful User Logins from Third Party Systems	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query retrieves failed logins using a non-administrative account, from assets categorized as Third Party.
Unsuccessful User Logins to Third Party Systems	Query	/All Queries/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This query retrieves failed logins with a non-administrator account to assets categorized as Third Party.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1), continued

Resource	Type	URI	Description
Attacks and Suspicious Activities Targeting Business Associate	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report shows all hostile or suspicious events targeting Business Associate sorted by the event's end time.
Attacks and Suspicious Activities from Business Associate Targeting PHI Asset	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report shows all hostile or suspicious events from Business Associate domain targeting PHI assets sorted by the event's end time.
Business Associate Access	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report shows all access attempts from business associate assets.
Organizational Records Information Leaks Originated from Business Associate	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report shows the communications which were classified as information leaks of organizational records originated from Business Associate domain.
Personal Information Leaks Originated from Business Associate	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report shows events which indicate a personal information leak originated from Business Associate domain.
Reconnaissance from Business Associate Targeting PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report shows reconnaissance activity from assets in the Business Associate domain targeting assets in the PHI domain.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1), continued

Resource	Type	URI	Description
Successful Administrative Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report displays all successful administrative logins from assets categorized as Third Party.
Successful Administrative Logins to Third Party Systems	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report displays all successful logins to assets categorized as Third Party, that were done with an administrator account.
Successful User Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report displays all successful non-administrative logins from assets categorized as Third Party.
Successful User Logins to Third Party Systems	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report displays all successful non-administrative logins to assets categorized as Third Party.
Third-Party Incidents - Closed Cases	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report shows all cases involving third-party systems that have been closed.
Third-Party Incidents - Open Cases	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report shows all cases involving third-party systems that are still open.

Resources for Business Associate Contracts and Other Arrangements 164.308 (b)(1), continued

Resource	Type	URI	Description
Unsuccessful Administrative Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report displays all failed logins with an administrative account from assets categorized as Third Party.
Unsuccessful Administrative Logins to Third Party Systems	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report displays all failed logins with an administrative account to assets categorized as Third Party.
Unsuccessful User Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report displays all failed logins with a non-administrative account from assets categorized as Third Party.
Unsuccessful User Logins to Third Party Systems	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This report displays all failed logins with a non-administrative account to assets categorized as Third Party.
Attack from Business Associate System Targeting PHI Assets	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This rule looks for attacks from business associate systems.
Attack from Third-Party System	Rule	/All Rules/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)(1) Business Associate Contracts and Other Arrangements/	This rule looks for attacks from third-party systems.

Facility Access Controls 164.310 (a)(1)

This section lists all resources under the Facility Access Controls group.

Resources for Facility Access Controls 164.310 (a)(1)

Resource	Type	URI	Description
Physical Security	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a)(1) Facility Access Controls/	Shows all physical access related activities.
Physical Security Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a)(1) Facility Access Controls/	Displays information around physical access.
Building Access - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a)(1) Facility Access Controls/	Used to show the hour of day that users are accessing buildings.
Contractor Access After Hours	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a)(1) Facility Access Controls/	Shows the top contractors accesses after hours.
Last 20 Building Access Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a)(1) Facility Access Controls/	Shows the last 20 physical access events.
Top Users Accessing Buildings	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a)(1) Facility Access Controls/	Shows the top 10 users accessing buildings.
Badge Out	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a)(1) Facility Access Controls/	Identifies badge out event.
Building Access	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a)(1) Facility Access Controls/	Selects all building access events.

Resources for Facility Access Controls 164.310 (a)(1), continued

Resource	Type	URI	Description
Contractor Access After Hours	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Identifies contractors accessing buildings after hours.
Physical Access Events	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Selects all events sent to ArcSight ESM by physical security systems.
Successful After Hours Building Access	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Selects all events indicating successful occurrences of physical access after business hours. The actual time definition is defined in the After Hours filter.
Successful Badge In	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Identifies a successful badge-in event.
Successful Building Access Granting	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Identifies granting user access to a building.
Unsuccessful After Hours Building Access	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Selects all events indicating unsuccessful occurrences of physical access after business hours. The actual time definition is defined in the After Hours filter.
Unsuccessful Badge In	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Identifies an unsuccessful badge-in event.
Building Access and Leave by User	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows successful building access and leave events by user.
Failed After Hours Building Accesses	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows the failed physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.
Failed Building Access Events	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows failed attempts to leave a building at any time.

Resources for Facility Access Controls 164.310 (a)(1), continued

Resource	Type	URI	Description
Successful After Hours Building Accesses	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows the successful physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.
Successful Building Access Events	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows successful building access events at all times.
Successful Building Access Granting	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows all successful building access granting.
Successful Building Leaving Events	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows all successful building leaving events at all times (for badge reader systems support this option).
Building Access and Leave by User	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows successful building access and leave events by user.
Failed After Hours Building Accesses	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows the failed physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.
Failed Building Access Events	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows failed attempts to enter a building at any time.
Successful After Hours Building Accesses	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows the successful physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.
Successful Building Access Events	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows successful building access events.
Successful Building Access Granting	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows successful building access-granting events.

Resources for Facility Access Controls 164.310 (a)(1), continued

Resource	Type	URI	Description
Successful Building Leaving Events	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Shows successful building access events at all times.
After Hours Building Access by Contractors	Rule	/All Rules/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Detects building access events after business hours by contractors.
Badged Out Employee	Rule	/All Rules/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Detects when someone leaves a building and adds the user to the Badged Out active list.
Failed Building Access	Rule	/All Rules/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Detects failed physical building access.
Local Logon from Badged Out Employee	Rule	/All Rules/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Detects a local logon event though the employee is badged out.
Successful Badge In	Rule	/All Rules/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Identifies when an employee badges in and puts the badge id and other information on the Badged In active list.
Successful Badge Out	Rule	/All Rules/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a) (1) Facility Access Controls/	Detects when someone leaves a building and removes the user from the badged in active list.

Device and Media Controls 164.310 (d)(1)

This section lists all resources under the 164.310 Physical Safeguards/Device and Media Controls group.

Resources for Device and Media Controls 164.310 (d)(1)

Resource	Type	URI	Description
Last State External Device Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(d)(1) Device and media controls/	Provides Real-time display of the last 20 external device activities and their status.
Last State External Device Overview	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(d)(1) Device and media controls/	Real-time display of the last 20 external device activity and their status.
Insecure Cryptographic Storage Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(d)(1) Device and media controls/	Selects events indicating that Insecure cryptographic storage has been detected.
Removable Media Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(d)(1) Device and media controls/	This query selects events indicating that a removable device is detected.
Removable Media Detected on Highly Critical Machine	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(d)(1) Device and media controls/	This filter selects events indicating that a removable device is detected on highly critical machine.
Insecure Cryptographic Storage on PHI Asset	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(d)(1) Device and media controls/	Selects events indicating that insecure cryptographic storage has been detected on PHI asset.
Removable Media Activity	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(d)(1) Device and media controls/	Shows all the removable media activity for the last 24 hours.

Resources for Device and Media Controls 164.310 (d)(1), continued

Resource	Type	URI	Description
Insecure Cryptographic Storage on PHI Asset	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(d)(1) Device and media controls/	Shows all insecure cryptographic events identified in PHI assets on the last 24 hours.
Removable Media Activity	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(d)(1) Device and media controls/	Shows all the removable media activity for the last 24 hours using windows events.
Removable Media Detected on Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(d)(1) Device and media controls/	Looks for events indicating that a removable device is detected on highly critical machine.

Workstation Use 164.310 (b)

This section lists all resources under the Workstation Use group.

Resources for Workstation Use 164.310 (b)

Resource	Type	URI	Description
Remote Access to Systems with Insecure Configuration	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	This dashboard displays information about remote access to insecure systems.
Last 10 Remote Accesses to Systems with Insecure Configurations	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	Shows the last 10 remote accesses to systems with Insecure Configurations.
Remote Access to Systems with Insecure Configuration	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	This data monitor displays an Event Graph of access attempts via a VPN gateway to system known for running an insecure service. Such services are listed in the referenced active list.
Privileged Access on a Remote Connection	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	This filter selects events where a connection is reported by a VPN device, and the user name belongs to a privileged account.
Remote Access to Systems with Insecure Configuration	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	This filter selects events showing access attempts via a VPN gateway to system known for running an insecure service. Such services are listed in the referenced active list.

Resources for Workstation Use 164.310 (b), continued

Resource	Type	URI	Description
Unsuccessful VPN Access	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	This filter identifies failed VPN access attempts.
VPN Access Attempt	Filter	/All Filters/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	This filter identifies VPN access attempts.
All VPN Access Attempts	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	Provides an overview of the number of VPN access attempts by non-administrative users.
Privileged VPN Remote Access Attempts	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	Shows all connections reported by a VPN device, where the user name belongs to a privileged account.
Remote Access to Systems with Insecure Configuration	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	This query shows all access attempts via a VPN gateway to system known for running an insecure service.
Unsuccessful VPN Access	Query	/All Queries/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	Lists all failed VPN access attempts.
All VPN Access Attempts	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	Lists all VPN access attempts.
Privileged VPN Remote Access Attempts	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	Shows remote VPN connections attempts by an administrative account. The report is ordered by the connection outcome so you can easily distinguish the successful connections from the unsuccessful ones.
Remote Access to Systems with Insecure Configuration	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	This report shows all access attempts via a VPN gateway to system known for running an insecure service.
Unsuccessful VPN Access	Report	/All Reports/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310 (b) Workstation Use/	Provides a listing of failed VPN access, the number of such failed events and the last failure time.

Access Control 164.312 (a)(1)

This section lists all resources under the Access Control group.

Resources for Access Control 164.312 (a)(1)

Resource	Type	URI	Description
Default Vendor Account Used	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows a real-time feed of events reflecting the use of vendor-provided default credentials. This is based on the related rule firing. Manager Receipt Time is used as the time-stamp of choice to retain the real-time nature of the channel.
Traffic Between Network Domains	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This Active Channel shows all the traffic between network domains.
Blocked Traffic Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This dashboard shows information related to blocked traffic activity.
Default Vendor Account Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This dashboard shows information related to blocked traffic activity.
PHI Assets Traffic Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This dashboard shows information related to PHI assets traffic activity.
Traffic to and from Classified Machines	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Displays information about traffic between assets whose criticality is categorized differently.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Blocked Traffic	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This data monitor presenting blocked traffic in event graph chart .
Classification Level Traffic High to Low	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows a graph of network traffic which went from a higher-classified asset to a lower-classified one.
Classification Level Traffic Low to High	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows a graph of network traffic which went from a lower-classified asset to a higher-classified one.
Last 10 Blocked Traffic Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This data monitor shows the last 10 blocked traffic events.
Last 10 Traffic from PHI Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This data monitor shows the last 10traffic events from PHI assets.
Last 10 Traffic to PHI Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This data monitor shows the last 10traffic events to PHI assets.
Last Default Vendor Account Credentials Observed	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Displays login events where user has attempted to login to a system with vendor-supplied default User ID.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Top 10 PHI Traffic Attackers	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This data monitor displays a bar chart of the top PHI addresses that generating traffic to non-PHI addresses.
Top 10 PHI Traffic Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This data monitor displays a bar chart of the top non PHI addresses that communicating with PHI addresses.
Top Blocked Traffic Attackers	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This data monitor displays a bar chart of the top attacker addresses of blocked traffic.
Top Default Vendor Accounts Observed	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Displays top vendor-supplied default account observed.
Top Targets with Default Vendor Accounts	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Displays login events where user has attempted to login to a system with vendor-supplied default account.
Traffic from PHI Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows a graph of network traffic which went from a PHI asset.
Traffic to PHI Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows a graph of network traffic which went to PHI assets.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Default Vendor Account Access Attempted	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Identifies events where system access with vendor-supplied accounts is attempted.
Default Vendor Account Credential Observed	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Identifies events where system access with vendor-supplied accounts is observed.
Direct Root or Administrator Credential Observed	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Identifies events where system access with root or administrator credential is observed.
External to Internal Traffic	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This filter selects events where the traffic originates from external network segment and the target is in an internal network segment.
Internal to External Traffic	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This filter selects events where the traffic originates from an internal network segment and the target is in an external network segment.
Login Activity by Stale User Accounts	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Identifies login activities by accounts that are on the Stale Accounts active list.
Suspicious Activities by Stale User Accounts	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Identifies suspicious activities by accounts that are on the Stale Accounts active list.
Traffic from Higher to Lower Classification Level	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This filter identifies events going from an asset in a higher classification level to an asset in a lower classification level.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Traffic from Lower to Higher Classification Level	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This filter identifies events going from an asset in a lower classification level to an asset in a higher classification level.
Traffic from PHI Assets	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This filter identifies events going from PHI assets.
Traffic to PHI Assets	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This filter identifies events going to PHI assets.
Blocked Firewall Traffic from Assets in Business Associate	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the blocked outbound firewall traffic originating from assets in the business associate domain.
Blocked Firewall Traffic from Assets in Electronic PHI Domain	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the blocked outbound firewall traffic originating from assets in the Electronic PHI domain.
Blocked Firewall Traffic to Assets in Business Associate	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the blocked inbound firewall traffic directed to assets in the Business Associate domain.
Blocked Firewall Traffic to Assets in Electronic PHI Domain	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the blocked inbound firewall traffic directed to assets in the Electronic PHI domain.
Cross-Talk Between Electronic PHI and Business Associate	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report shows all cross-talk in the last 24 hours between assets in Electronic PHI and Business Associate domains.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Cross-Talk Between Production and Development	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report shows all cross-talk in the last 24 hours between assets in Development and Production domains.
External to PHI Traffic	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report counts all events from external sources to PHI domain per device and source-target pair. The query runs over the last 24 hours.
Firewall Traffic from Assets in Business Associate	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the outbound firewall traffic originating from assets in the business associate domain.
Firewall Traffic from Assets in Electronic PHI Domain	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the outbound firewall traffic originating from assets in the Electronic PHI domain.
Firewall Traffic to Assets in Business Associate	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the inbound firewall traffic directed to assets in the Business Associate domain.
Firewall Traffic to Assets in Electronic PHI Domain	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the inbound firewall traffic directed to assets in the Electronic PHI domain.
PHI to External Traffic	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report counts all events from PHI domain to external sources per device and source-target pair. The query runs over the last 24 hours.
Blocked Firewall Traffic from Assets - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query provides a listing of the blocked outbound firewall traffic originating from assets in the indicated Network Domain of interest.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Blocked Firewall Traffic to Assets - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query provides a listing of the blocked inbound firewall traffic directed at assets in the indicated Network Domain of interest.
Cross Talk between 2 Network Domains	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query provides the cross-talk in the last 24 hours between assets in Development category and assets in Test category.
Detail Default Vendor Account Used	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows if a vendor supplied user account without password is being used to login.
External Traffic to Internal Domain - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query counts all events from external sources to internal domain to per device and source-target pair. The query runs over the last 24 hours.
External to Internal Traffic	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query counts all events from external to internal sources per device and source-target pair. The query runs over the last 24 hours.
Firewall Traffic from Assets - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query provides a listing of the outbound firewall traffic originating from assets in the indicated Network Domain of interest.
Firewall Traffic to Assets - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query provides a listing of the inbound firewall traffic directed at assets in the indicated Network Domain of interest.
Inactive User Accounts	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows all user names that are in the Stale Accounts active list.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Internal Domain to External Traffic - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query counts all events from internal domain to external sources per device and source-target pair. The query runs over the last 24 hours.
Internal to External Traffic	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query counts all events from internal to external sources per device and source-target pair. The query runs over the last 24 hours.
Login Activity by Stale User Accounts	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows stale user accounts from which login activity was attempted.
Open Firewall Port Summary	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query gives a summary of all the ports that are allowed to pass through firewalls.
Suspicious Activity by Stale User Accounts	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows suspicious activities of stale user accounts.
Systems Accessed by Default Vendor Accounts	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows all systems that users have tried to access directly as root or administrator.
Top Attackers Attempted Default Vendor Accounts	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows the top hosts from which attackers most attempted default vendor account.
Top Attackers Using Default Vendor Account	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows the top attackers successfully used a vendor supplied user account.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Top Attackers Using Direct Root or Administrator Account	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows the top attackers attempting direct root or administrator credential.
Top Default Vendor Accounts Attempted	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows the top vendor supplied user account still being used to login.
Top Default Vendor Accounts Used	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows the top vendor supplied user account still being used to login.
Top Target Hosts Where Default Vendor Account Attempted	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows the top hosts where a vendor supplied user account still being used to login.
Top Target Hosts Where Default Vendor Account Used	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows the top hosts where a vendor supplied user account still being used to login.
Top Target Hosts Where Direct Root or Administrator Account Observed	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows the top hosts where direct root or administrator account is attempted.
User Logged in from Two Countries	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Selects user names that have been used to login from two different countries.
User Logged in from different IP Addresses	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Selects single user names that have been used to login from different IP addresses.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Open Firewall Port Summary	QueryViewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This query viewer gives a summary of all the ports that are allowed to pass through various firewalls.
Attempted Default Vendor Accounts - Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows summary views of events and systems when a vendor supplied user account is attempted by a user to login.
Attempted Direct Root or Administrator	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows events and systems when direct root or administrator account is attempted by a user to login.
Blocked Firewall Traffic from Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the blocked outbound firewall traffic originating from assets in the indicated Network Domain of interest.
Blocked Firewall Traffic to Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the blocked inbound firewall traffic directed at assets in the indicated Network Domain of interest.
Cross-Talk Between Network Domains - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report shows all cross-talk in the last 24 hours between assets in 2 network domains . default network domains : development and test.
Detail Specific Default Vendor Account Uses	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows all logins using a specific vendor supplied user account.
External to Internal Domain Traffic -Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report counts all events from external sources to internal Domain (default Development Domain) per device and source-target pair. The query runs over the last 24 hours.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Firewall Traffic from Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the outbound firewall traffic originating from assets in the indicated Network Domain of interest.
Firewall Traffic to Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report provides a listing of the inbound firewall traffic directed at assets in the indicated Network Domain of interest.
Inactive User Account Detected	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows all user names that are in the Stale Accounts active list.
Internal Domain to External Traffic - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This report counts all events from internal domain (default Development Domain) to external sources per device and source-target pair. The query runs over the last 24 hours.
Login Activity by Inactive Users	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows login activity by users that are on the Stale Accounts Active List. The report is ordered by the outcome of the login event.
Successful Default Vendor Account Used - Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows high level summary views of events when a vendor-supplied user account is used to login.
Suspicious Activity by Inactive Users	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows suspicious activity by users that are on the Stale Accounts Active List.
Systems Accessed by Default Vendor Accounts	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows all systems that users have tried to access as a default vendor account.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
User Logged in from Different IP Addresses	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows user names that have been used to login from different IP addresses in very short period. This may indicate user name sharing.
User Logged in from Two Countries	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Shows user names that have been used to login from two different countries. This may indicate user name sharing.
Communication between Electronic PHI and Business Associate Domains	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This rule fires any time communication between a production asset and a machine in the development domain is detected.
Communication between Production and Development Domains	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This rule fires any time communication between a production asset and a machine in the development domain is detected.
Communication between Sensitive Asset and Test Domain	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This rule fires any time communication between a sensitive asset and a machine in the Test domain is detected.
Communication between Sensitive Asset and Third Party Domain	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	This rule fires any time communication between a sensitive asset and a machine in the Third Party domain is detected.
Inactive User Account Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Fires every time an entry ages out of the Stale Accounts active list.
Login Activity by a Stale Account	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Identifies login activities by accounts that are on the Stale Accounts active list.

Resources for Access Control 164.312 (a)(1), continued

Resource	Type	URI	Description
Successful Default Vendor Account Used	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Looks for successful access to system using default user accounts.
Suspicious Activities by a Stale Account	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Identifies suspicious activities by accounts that are on the Stale Accounts active list.
User Logged in from Two Countries	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Fires when someone is using the same user name to login from two different countries. This may indicate user name sharing.
User Logged in from different IP Addresses	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) Access Control/	Fires when someone is using the same user name to login from different ip addresses. This may indicate user name sharing.

Audit Controls 164.312 (b)

This section lists all resources under the Audit Controls group.

Resources for Audit Controls 164.312 (b)

Resource	Type	URI	Description
Audit Log Cleared	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Looks for events that indicate an audit log is cleared.
Information System Audit Tool Logins	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows all the logins to the Information System Audit Tool - ArcSight.

Resources for Audit Controls 164.312 (b), continued

Resource	Type	URI	Description
Audit Log Cleared	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Displays Audit Log Cleared compliant status.
Network Controls	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	This dashboard displays information about logging devices and firewall open ports.
Audit Log Cleared Status	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Reports violation suspected status when an audit log cleared event is present.
Firewall Open Ports	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	This data monitor is used to determine which ports a particular firewall is allowing traffic on.
Last 20 Audit Log Cleared Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Reports the last 10 audit log cleared events.
Logging Devices	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	This data monitor shows all devices that are sending their logs.
Audit Log Cleared	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Selects all events where an audit log was cleared from a host. By default it will recognize events on Microsoft Windows and Symantec Host IDS systems, modify this filter to include events from other devices.

Resources for Audit Controls 164.312 (b), continued

Resource	Type	URI	Description
Audit Log Cleared Rule Fired	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Detects correlated events the rule Audit Log Cleared generates.
Big Difference Between End Time and Manager Receipt Time	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Identifies time discrepancies between endTime and managerReceiptTime. By default it will identify events with a difference of more than 600 seconds (10 minutes).
Clock Synchronization Issues	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Identifies different kinds of clock synchronization issues.
Device Time is Later than Agent Time	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	This filter identifies events in which the device receipt time is after the agent receipt time. By default it will show events for which the device receipt time is more than 300 seconds (5 minutes) than the agent (connector) receipt time.
Information System Audit Tool Login	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Identifies logins to information system audit tools. By default it Shows only logins to ArcSight products.
Audit Log Cleared	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows all events where an audit log was cleared from a host.
Audit Log Cleared per Attacker User Name	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows the number of times an audit log was cleared by an attacker user name.
Audit Log Cleared per Attacker and Target	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows the number of times audit logs were cleared from a host by an attacker and target.

Resources for Audit Controls 164.312 (b), continued

Resource	Type	URI	Description
Audit Log Cleared per Target User Name	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows the number of times an audit log was cleared by a target user name.
Clock Synchronization Issues	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Displays all events in which there are clock synchronization issues between the deviceReceiptTime and agentTime, or the event endTime and managerReceiptTime.
Clock Synchronization Issues - Overview	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Displays a summary of the number of events for each device that had clock synchronization issues.
Device Logging Review	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	This query shows the different products that are logging to ArcSight ESM.
Events per Device	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	This query shows the number of events reported each device over the past day.
Information System Audit Tool Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows logins, both successes and failed, to information system audit tools.
Syslog Restart Events	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows all restarts of syslog on systems.
Windows System audit policy changes	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows all Windows system audit policy changes.

Resources for Audit Controls 164.312 (b), continued

Resource	Type	URI	Description
Events per Device	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	This query viewer shows the number of events that have been reported by a particular device over the last hour.
Logging Devices	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	This query viewer shows the different products that are logging to ArcSight ESM.
Audit Log Cleared	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows all events where an audit log was cleared from a host.
Audit Log Cleared per Attacker User Name	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows all events where an audit log was cleared by an attacker user name.
Audit Log Cleared per Attacker and Target	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows all events where audit logs were cleared from a host by an attacker.
Audit Log Cleared per Target User Name	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows all events where an audit log was cleared by a target user name.
Clock Synchronization Issues	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Displays all events in which there are clock synchronization issues between the deviceReceiptTime and agentTime, or the event endTime and managerReceiptTime. The report is ordered first by the agent information and then by the device information.

Resources for Audit Controls 164.312 (b), continued

Resource	Type	URI	Description
Clock Synchronization Issues - Overview	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Displays a summary of the number of events for each device that had clock synchronization issues. The report is ordered first by the number of problematic agent-device time events and then by the number of problematic end-manager time events.
Device Logging Review	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	This report shows the different products that are logging to ArcSight ESM.
Information System Audit Tool Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows logins, both successful and failed, to information system audit tools.
Syslog Restart Events	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows all restarts of syslog on systems.
Windows System audit policy changes	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Shows all Microsoft system audit policy changes.
Audit Log Cleared	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audit Controls/	Monitors for events on clearing of the audit log on Windows systems.

Integrity 164.312 (c)(1)

This section lists all resources under the Integrity group.

Resources for Integrity 164.312 (c)(1)

Resource	Type	URI	Description
Cryptographic Hash Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Provides an overview of Cryptographic Hash Vulnerabilities.
Last 10 Cryptographic Hash Algorithm Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Provides real-time display of the last 10 cryptographic hash related vulnerabilities.
Top 10 Cryptographic Hash Algorithm Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Provides real-time display of the top 10 assets with cryptographic hash algorithm related vulnerabilities.
Cryptographic Hash Algorithm Related Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Selects events indicating that potential hash algorithm related vulnerability was detected.
Traffic from Others to PHI	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Selects all traffic destined for the PHI segment(s) of the network that did not originate from within a PHI segment.
Attempted File Changes in PHI Segment Originated from HR	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Displays attempts to change a file on a host in the PHI segment from a source that is in HR.

Resources for Integrity 164.312 (c)(1), continued

Resource	Type	URI	Description
Attempted File Changes in PHI Segment Originated from Public-Facing	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Displays attempts to change a file on a host in the PHI segment from a source that is in Public-Facing.
Attempted File Changes in PHI Segment Originated from Remote	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Displays attempts to change a file on a host in the PHI segment from a source that is categorized as Remote.
Attempted File Changes in PHI Segment Originated from Test	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Displays attempts to change a file on a host in the PHI segment from a source that is in test.
Attempted File Changes in PHI Segment Originated from Third-Party	Focused Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Displays attempts to change a file on a host in the PHI segment from a source that is in Third-Party.
Attempted File Changes in PHI Segment originated from Other Network Domain - Template	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Displays attempts to change a file on a host in the PHI segment from a source that is in a specific network domain. By default, the Production network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Cryptographic Hash Algorithm Related Vulnerability Detected	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Selects events indicating that potential hash algorithm related vulnerability was detected.
Attempted File Changes in PHI Segment Originated from Other Network Domain - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Displays attempts to change a file on a host in the PHI segment from a source that is not in the PHI segment.

Resources for Integrity 164.312 (c)(1), continued

Resource	Type	URI	Description
Cryptographic Hash Algorithm Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Shows all cryptographic hash algorithm vulnerabilities that have been detected.
Attempted File Changes in PHI Segment Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Fires when it Detects multiple attempts to change a file on a host in the PHI segment from a source that is not in the PHI segment.
Cryptographic Hash Algorithm Related Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(c)(1) Integrity/	Triggers when potential cryptographic hash algorithm related vulnerability is detected.

Person or Entity Authentication 164.312 (d)

This section lists all resources under the Person or Entity Authentication group.

Resources for Person or Entity Authentication 164.312 (d)

Resource	Type	URI	Description
Account Lockouts	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Shows events where a rule fired to lock out a user ID.
Account Lockouts	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Displays information about account lockouts.
Account Lockouts	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Displays events when an account has been locked out; triggered by a related rule firing.
Account Lockouts	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Identifies account lockouts. By default it will recognize lockouts on Microsoft Windows and Unix systems.

Resources for Person or Entity Authentication 164.312 (d), continued

Resource	Type	URI	Description
All Brute Force Login Attempts	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Identifies all types of Brute Force Login Attempts.
Application Brute Force Login Attempts	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Identifies all application brute force login attempt events.
IDS Detected Brute Force Login Attempts	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Shows events sent by Intrusion Detection Systems that indicate brute force login attempts.
IDS Detected Successful Brute Force Logins	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Selects events from Intrusion Detection Systems that indicate a successful brute force login has occurred.
Successful Brute Force Logins	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Identifies events generated by the Probable Successful Brute Force rule that involve assets categorized in one of your Network Domains.
Account Lockouts	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Retrieves all information about account lockouts.
Account Lockouts per System	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Retrieves a count of all the account lockouts per system during the last 24 hours.
Account Lockouts per User and System	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Counts account lockouts per user and system.
Application Brute Force Login Attempts	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Shows application brute force login attempts.
Frequent Unsuccessful Logins by User Name	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Identifies all user names for which there are a continuous set of unsuccessful login attempts.

Resources for Person or Entity Authentication 164.312 (d), continued

Resource	Type	URI	Description
Frequent Unsuccessful Logins from Attacker Host	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Identifies all attacker hosts from which a continuous set of unsuccessful login attempts have been occurring.
Frequent Unsuccessful Logins to Target Host	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Identifies all target hosts which have received a continuous set of unsuccessful login attempts.
Successful Brute Force Logins	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Provides a listing of events categorized by ArcSight as probable successful brute-force login attempts. May (and should) be focused based on the Network Domain of interest.
Account Lockouts	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Shows all account lockout events in the last hour. You can drill down on either the host address or the user name for more focused results.
Account Lockouts per System	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Shows a count of account lockouts per system. It also shows the number of distinct user names that contributed to the total number of lockouts.
Account Lockouts per User and System	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Shows a counts of account lockouts per user and system, and a chart of the total number of lockouts per user.
Application Brute Force Login Attempts	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Shows application brute force login attempts.
Frequent Unsuccessful Logins by User Name	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Displays all user names for which there are a continuous set of unsuccessful login attempts.
Frequent Unsuccessful Logins from Attacker Host	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Displays all attacker hosts from which a continuous set of unsuccessful login attempts have been occurring.
Frequent Unsuccessful Logins to Target Host	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Lists all target hosts which have received a continuous set of unsuccessful login attempts.

Resources for Person or Entity Authentication 164.312 (d), continued

Resource	Type	URI	Description
Successful Brute Force Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Provides a listing of events categorized by ArcSight as probable successful brute force login attempts.may (and should) be focused based on the Network Domain of interest.
Account Lockout	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Detects account lockouts. This activity is suspicious.
Brute Force Login Attempts	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Identifies brute force login attempts.
Frequent Unsuccessful Logins by User Name	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Fires when it notices the same user is responsible for a continuous set of unsuccessful logins.
Frequent Unsuccessful Logins from Attacker Host	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Fires when it notices a continuous set of unsuccessful logins from the same attacker host.
Frequent Unsuccessful Logins to Target Host	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Fires when it notices a high frequency of unsuccessful logins on the same target host.
Successful Attack - Brute Force Login	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Person or Entity Authentication/	Detects successful brute force login attacks.

Transmission Security 164.312 (e)(1)

This section lists all resources under the Transmission Security group.

Resources for Transmission Security 164.312 (e)(1)

Resource	Type	URI	Description
All Information Leak Events	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This active channel shows real-time feed of events reflecting information leakage.
DoS Attacks	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This active channel shows events that are attributed to denial of service attacks.
Intellectual Property Rights Violations	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This active channel looks for intellectual property rights violations. To do so, it shows all the rule-firings that are indicating intellectual property rights violations.
Invalid or Expired Certificate Presented	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows a real-time feed of events which indicate that an invalid or expired certificate was detected.
Organizational Records Information Leaks	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This active channel shows real-time feed of events reflecting organizational information leakage.
Personal Information Leak	Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This active channel shows real-time feed of events reflecting personal information leakage.
Cryptographic Public Key Related Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides an overview of Cryptographic Public Key Related Vulnerabilities.
Cryptographic Symmetric Key Related Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides an overview of Cryptographic Symmetric Key Related Vulnerabilities.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Cryptographic Weak Protocol Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides an overview of Cryptographic Weak Protocol Vulnerabilities.
Disallowed Ports Communications	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Displays information around events to disallowed ports.
DoS Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This dashboard provides an overview of events associated with denial of service and availability attacks.
Information Interception	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This dashboard displays information about interception events.
Information Leaks	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This dashboard displays information around information leakage.
Intellectual Property Rights Violations	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This dashboard displays information around violations and violators of IPR.
Organizational Information Leak	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This dashboard displays information around organizational information leakage.
Personal Information Leak	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This dashboard displays information around personal information leakage.
SSL Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides an overview of SS Vulnerabilities.
Spam Activity	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This dashboard displays information about spam events.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Traffic Anomaly	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This dashboard displays information about traffic anomaly events.
Disallowed Ports by Policy	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides the distribution of disallowed ports by policies.
DoS Attacks Event Names - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows connections between attacker and target machines and event names as they appear in denial of service attack events
DoS Attacks Event Ports - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows connection between attacker and target machines and ports as they appear in denial of service attack events.
Last 10 Cryptographic Public Key Related Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides real-time display of the last 10 cryptographic public key related vulnerabilities.
Last 10 Cryptographic Symmetric Key Related Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides real-time display of the last 10 cryptographic symmetric key related vulnerabilities.
Last 10 Cryptographic Weak Protocol Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides real-time display of the last 10 cryptographic weak protocol related vulnerabilities.
Last 10 Information Interception Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows the last 10 Information Interception events.
Last 10 Organizational Records Leak	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor provides a list of the last 10 information leaks of organizational records.
Last 10 Personal Records Leak	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor provides a list of the last 10 information leaks of personal records.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Last 10 SSL Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides real-time display of the last 10 SSL vulnerabilities.
Last 10 Spam Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor displays the last 20 spam events.
Last 10 Traffic Anomaly Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows the last 10 Traffic Anomaly events.
Last 20 DoS Attack Events	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor displays the last 20 denial of service attack events.
Last Connections to Disallowed Ports	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows the last 10 connections to disallowed ports to or from the network.
Organizational Records Leak	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor displays a graph with events which pertain to information leaks of organizational records.
Personal Information Leak	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows communications pertaining to personal information leaks.
Top 10 Cryptographic Public Key Related Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides real-time display of the top 10 assets with cryptographic public key related vulnerabilities.
Top 10 Cryptographic Symmetric Key Related Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides real-time display of the top 10 assets with cryptographic symmetric Key related vulnerabilities.
Top 10 Cryptographic Weak Protocol vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides real-time display of the top 10 assets with cryptographic weak protocol-related vulnerabilities.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Top 10 DoS Attackers	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows the top 10 DoS Attackers.
Top 10 DoS Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows the top 10 DoS targets.
Top 10 Intellectual Property Rights Violations	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows the top 10 violations concerning intellectual property by looking for the rule-firing in this use-case.
Top 10 Intellectual Property Rights Violators	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows the top 10 violators downloading intellectual property by looking for the rule-firing in this use-case.
Top 10 Organizational Records Leak Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows the top ten organizational information leak targets.
Top 10 Personal Records Leak Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows the top ten personal information leak targets.
Top 10 SSL Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides real-time display of the top 10 assets with SSL vulnerabilities.
Top 10 Spam Receivers	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows the top 10 spam targets.
Top 10 Spammers	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor shows the top 10 Spammers.
Top Disallowed Ports	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides a list of the top 10 disallowed ports.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Top Information Interception Attackers	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor displays a bar chart of the attacker addresses and priorities for information interception events.
Top Internal Hosts to Disallowed Ports	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides a list of the top 10 internal hosts that accessed disallowed ports.
Top Internal Providers of Disallowed Ports	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Provides a list of the top 10 internal providers of disallowed ports.
Top Traffic Anomaly Attackers	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor provides a list of the top 10 anomaly traffic per Attacker and Target Addresses addresses .
Traffic Anomaly	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor presenting traffic anomaly in event graph chart .
Traffic Anomaly by Protocol	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This data monitor provides the distribution of traffic anomaly by protocol.
All Information Leak Events	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter selects events that reflect information leakage.
Covert Channel	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events indicating a covert channel is being used.
Cryptographic Public Key Related Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that potential public key related vulnerability was detected.
Cryptographic Symmetric Key Related Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that potential symmetric key related vulnerability was detected.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Cryptographic Weak Protocol Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that potential cryptographic weak protocol related vulnerability was detected.
Disallowed Ports Access	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Tracks all connections to disallowed ports.
Disallowed Ports Access from Internal Hosts	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Tracks all connections to disallowed ports from internal hosts.
Disallowed Ports Access to Internal Hosts	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Tracks all connections to disallowed ports hosted by internal hosts.
Email Attacks	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events indicating an email attack occurred.
Email Traffic	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter identifies generic email traffic.
IM Traffic	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter identifies all instant messaging traffic that are not supposed to be allowed.
Information Interception	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events indicating an information interception is being used.
Intellectual Property Rights Violations	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter identifies violations of intellectual property rights by looking at the rule for this use-case.
Invalid or Expired Certificate	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events which indicate that an invalid or expired certificate was detected.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Organizational Records Information Leak	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter identifies information leaks with regard to company information.
Peer to Peer Traffic	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Identifies peer-to-peer traffic.
Personal Information Leak	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter selects events which indicate a personal information leak.
Phishing Attacks	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events indicating an phishing attack occurred.
Redirection Attacks	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events indicating a redirection attack occurred.
SSH Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that an SSH vulnerability was detected.
SSL Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that an SSL vulnerability was detected.
Spamming Attacks	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events indicating an email spam sent.
Successful DoS Attacks	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter identifies successful denial of service attacks.
Traffic Anomaly	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events indicating a traffic anomaly.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Traffic Anomaly on Application Layer	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events indicating a traffic anomaly on application layer
Traffic Anomaly on Network Layer	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events indicating traffic anomaly on network layer.
Traffic Anomaly on Transport Layer	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events indicating traffic anomaly in transport layer .
Traffic from Dark Address Space	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events that are coming from the Dark Address Space.
Traffic to Dark Address Space	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter detects events that are targeting the Dark Address Space.
Unsuccessful and Attempted DoS Attacks	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This filter identifies unsuccessful and attempted denial of service attacks.
VPN Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that a VPN vulnerability was detected.
Count of DoS Attacks per Day	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query counts the total number of weekly denial of service attack events.
Covert Channel Activity	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows all covert channel activity.
Cryptographic Public Key Related Vulnerability Detected	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that potential public key related vulnerability was detected.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Cryptographic Symmetric Key Related Vulnerability Detected	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that potential symmetric key related vulnerability was detected.
Cryptographic Weak Protocol Vulnerability Detected	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that potential cryptographic weak protocol related vulnerability was detected.
Disallowed Ports	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows traffic that should not be seen per the Allowed Ports active list.
Disallowed Ports by Connection Types	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows the top disallowed ports grouped by connection types.
DoS Attacks Trend	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query summarizes the number of DoS attacks for long term reporting.
DoS Attacks by Attacker	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query provides a weekly count of attacker addresses appearing in DoS attack events.
DoS Attacks by Target	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query provides a weekly count of target addresses appearing in DoS attack events.
Email Attacks	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows all email attacks.
External Hosts Receiving Most IM Traffic	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows top external hosts receiving most Instant Messaging traffic.
Inbound Insecure Transmissions	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Lists all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Information Interception Activity	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows all covert channel activity.
Insecure Transmissions	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Lists all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
Intellectual Property Rights Violations	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the various intellectual property rights violations.
Internal IM Sender	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows internal hosts with outgoing (not necessarily outbound) Instant Messaging traffic.
Internal Insecure Service Providers	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Returns the internal providers of insecure services.
Invalid or Expired Certificate	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows incidents which indicate that an invalid or expired certificate was detected.
Most Popular IM Traffic Ports	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the most common Instant Messaging target ports.
Most Popular IM Traffic Services	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the most common Instant Messaging services.
Organizational Records Information Leaks Originated from PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows communications which were classified as information leaks of organizational records originated from PHI assets.
Organizational Records Information Leaks Targeting PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows communications which were classified as information leaks of organizational records on PHI assets.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Peer to Peer Internal Sources	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows the most common sources for peer-to-peer applications.
Peer to Peer Traffic	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows the most common peer-to-peer traffic.
Personal Information Leaks Records Information Leaks Targeting PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows communications which were classified as information leaks of personal records on PHI assets.
Personal Information Leaks Records Originated from PHI Assets	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows communications which were classified as information leaks of personal records originated from PHI assets.
Phishing Attacks	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows all email attacks.
Ports and Events for DoS Attacks	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the various ports and events used in denial of service attacks.
Redirection Attacks	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows all redirection attacks.
SSH Vulnerabilities	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that SSH vulnerability has been detected.
SSL Vulnerabilities	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that SSL vulnerability has been detected.
Spam per Hour	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query gets the number of spam emails sent every hour over the past day.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Successful DoS Attacks	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the details of successful denial of service attacks.
Target Object in Successful DoS Attacks	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the number of times a particular object has been a victim of denial of service attacks.
Target Object in Unsuccessful and Attempted DoS Attacks	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the number of times a particular object has been attempted to be attacked by denial of service attacks.
Top Disallowed Ports	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows the top disallowed ports.
Top Email Receivers by Email Size	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the top email recipients based on the size of emails received.
Top Email Receivers by Number of Emails	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the top email recipients based on the number of emails received.
Top Email Senders by Email Size	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the top email senders based on the size of emails sent.
Top Email Senders by Number of Emails	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the top email senders based on the number of emails sent.
Top Internal Hosts Accessed Disallowed Ports	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows the top internal hosts that accessed most disallowed ports.
Top Internal Hosts Provided Disallowed Ports	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows the top internal hosts that provided most disallowed ports.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Top Phishing Email Receivers	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the top phishing email recipients.
Top Phishing Email Senders	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the topPhishing email senders.
Top Spam Receivers	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the top phishing email recipients.
Top Spam Senders	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the topPhishing email senders.
Traffic Anomaly on Application Layer	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows traffic anomaly on application layer.
Traffic Anomaly on Network Layer	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows traffic anomaly on network layer.
Traffic Anomaly on Transport Layer	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows traffic anomaly on transport layer.
Traffic from Dark Address Space	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows all traffic from a dark address range targeting systems. This should be considered very suspicious.
Traffic to Dark Address Space	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows all traffic directed to a dark address range. This should be considered very suspicious.
Unencrypted Services by Host Name	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Returns all unencrypted services by a particular host name identified in the last 24 hours using vulnerability and port scanning events.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Unsuccessful and Attempted DoS Attacks	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query shows the details of unsuccessful and attempted denial of service attacks.
VPN Vulnerabilities	Query	/All Queries/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Selects events indicating that VPN vulnerability has been detected.
Ports and Events for DoS Attacks	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This query viewer shows the various ports and events used in denial of service attacks.
Covert Channel Activity	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows all covert channel activity.
Cryptographic Public Key Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows all cryptographic public key vulnerabilities that have been detected.
Cryptographic Symmetric Key Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows all cryptographic symmetric key vulnerabilities that have been detected.
Cryptographic Weak Protocol Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows all cryptographic weak protocol vulnerabilities that has been detected.
Detail Disallowed Port Access	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows traffic that should not be seen per the Allowed Ports/Disallowed Ports active list.
Disallowed Port Access Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows several summary aspects of traffic to disallowed ports.
DoS Attacks Weekly Trend	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report displays a weekly overview of DoS attack events.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Email Activity	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows all email activity in the last day.
Email Attacks	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows all email attacks
IM Traffic Summary	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows several high-level views of Instant Messaging traffic.
Inbound Insecure Transmissions	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Lists all inbound traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
Information Interception Activity	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows all information interception activity.
Insecure Transmissions	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Lists all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
Intellectual Property Rights Violations	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows the different intellectual property rights violations.
Internal IM Senders	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows several high-level views of internal Instant Messaging senders.
Internal Insecure Service Providers	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Lists all internal providers of insecure services.
Invalid or Expired Certificate	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows incidents which indicate that an invalid or expired certificate was detected.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Organizational Records Information Leaks Originated from PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows the communications which were classified as information leaks of organizational records originated from PHI assets.
Organizational Records Information Leaks Targeting PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows the communications which were classified as information leaks of organizational records on PHI assets.
Peer to Peer Internal Sources	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows the most common machines within the network involved in peer-to-peer traffic, the number of unique peers communicated with and the total number of peer-to-peer events.
Peer to Peer Traffic	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows the most common peer-to-peer traffic.
Personal Records Information Leaks Originated from PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows the communications which were classified as information leaks of personal records originated from PHI assets.
Personal Records Information Leaks Targeting PHI Assets	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows the communications which were classified as information leaks of personal records on PHI assets.
Phishing Activity	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows all email phishing activity in the last day.
Redirection Attacks	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows all redirection attacks
SSH Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows all SSL vulnerabilities that have been detected.
SSL Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows all SSL vulnerabilities that have been detected.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Spam Activity	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows all email spam activity in the last day.
Successful DoS Attacks	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows details of successful denial of service attacks.
Traffic Anomaly on Application Layer	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows traffic anomaly on application layer.
Traffic Anomaly on Network Layer	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows traffic anomaly on network layer.
Traffic Anomaly on Transport Layer	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows traffic anomaly on transport layer.
Traffic Coming from Dark Address Space	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows all traffic from a dark address range targeting systems. This should be considered very suspicious.
Traffic to Dark Address Space	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows all traffic directed to a dark address range. This should be considered very suspicious.
Unencrypted Services by Host Name	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Returns all unencrypted services by a particular host name (by default localhost) identified in the last 24 hours using vulnerability and port scanning events.
Unsuccessful and Attempted DoS Attacks	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This report shows details of unsuccessful and attempted denial of service attacks.
VPN Vulnerabilities	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Shows all VPN vulnerabilities that have been detected.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Cryptographic Public Key Related Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Triggers when potential cryptographic public key related vulnerability was detected.
Cryptographic Symmetric Key Related Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Triggers when potential cryptographic symmetric key related vulnerability was detected.
Cryptographic Weak Protocol Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Triggers when potential cryptographic weak protocol related vulnerability was detected.
Disallowed Ports Access	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Triggers when traffic to a forbidden target port occurs.
DoS Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This rule looks for DoS .
Intellectual Property Rights Violation	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This rule looks for intellectual property rights violations. The filter references should be configured to contain all the events pertaining to this use-case. The filter is located in the My Filters group.
Internal Insecure Service Provider Detected	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Detects when insecure protocols, such as Telnet or RSH, are used inside the network. When triggered, it adds an entry to the Internal Systems with Insecure Services active list.
Invalid or Expired Certificate	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Detects invalid or expired Certificates.
One or more rows have been deleted from the certificate database	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Detects if one or more rows have been deleted from the certificate database using Windows events.
Organizational Data Information Leak	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This rule looks for any organizational information being sent out of the corporate network.

Resources for Transmission Security 164.312 (e)(1), continued

Resource	Type	URI	Description
Personal Information Leak	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This rule looks for any personal information being sent out of the corporate network.
Possible Covert Channel	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This rule looks for events indicating a covert channel is being used.
Possible Email Attack	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This rule looks for attacks where email activity involved .
Possible Information Interception	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This rule looks for attacks where information could be redirected and collected by an unintended party.
Possible Redirection Attack	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This rule looks for attacks where information could be redirected .
Possible Traffic Anomaly	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This rule looks for attacks where information could be redirected and collected by an unintended party.
Potential Distributed DoS	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This rule looks for Potential Distributed DoS .
SSL Vulnerabilities on PHI Machine	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Triggers when SSL vulnerability is detected on PHI assets.
SSL Vulnerabilities on Public Facing Assets	Rule	/All Rules/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	Triggers when SSL vulnerability is detected on public-facing assets.
DoS Attacks Trend	Trend	/All Trends/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312 (e)(1) Transmission Security/	This trend stores long term aggregated information about DoS attack events.

Active Lists

This section lists all the active lists included with CIP for HIPAA.

Active Lists Resources for HIPAA CIP

Resource	Description	URI
Active Accounts	This active list stores user names who have successfully logged in within the last 30 days.	/All Active Lists/ArcSight Solutions/HIPAA/
Administrative Accounts List	<p>This active list should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the content pack, but the list can also be added to or referenced in new content built around the provided infrastructure.</p> <p>This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in all lower case.</p> <p>For example, the user Administrator should be added as "administrator".</p>	/All Active Lists/ArcSight Solutions/HIPAA/
Allowed Ports	This active list contains all permissible destination ports (all permissible services). This active list should be populated according to your site policy.	/All Active Lists/ArcSight Solutions/HIPAA/
Audit Log Cleared	This active list should be populated only by the rule Audit Log Cleared. It logs every time an audit log is cleared.	/All Active Lists/ArcSight Solutions/HIPAA/
Badged In	This list contains information about employees who are badged in.	/All Active Lists/ArcSight Solutions/HIPAA/
Badged Out	This active list contains the computer accounts of badged out employees.	/All Active Lists/ArcSight Solutions/HIPAA/
Badges to Accounts	This list contains the computer account and employee type for every physical device badge.	/All Active Lists/ArcSight Solutions/HIPAA/
Compliance Score	This active list maintains the compliance risk score for each regulation section. The compliance risk score is calculated based on the triggered rules in the solution package. You can manually change the score as required. This change will be reflected in the Compliance Risk Score dashboard.	/All Active Lists/ArcSight Solutions/HIPAA/
Default Vendor Accounts	<p>This active list contains the default user account names for various vendors.</p> <p>This list should be configured at set-up time with existing vendor user account names, and updated as necessary on an ongoing basis.</p>	/All Active Lists/ArcSight Solutions/HIPAA/

Active Lists Resources for HIPAA CIP, continued

Resource	Description	URI
Disallowed Ports	This active list contains all disallowed destination ports. This active list should be populated according to your site policy.	/All Active Lists/ArcSight Solutions/HIPAA/
Former Employees	This active list contains user accounts of former employees. User accounts in this active list are retained indefinitely. All the entries in this list need to be in lowercase.	/All Active Lists/ArcSight Solutions/HIPAA/
Insecure Ports	This active list includes ports related to unencrypted and thus insecure communication services.	/All Active Lists/ArcSight Solutions/HIPAA/
Insecure Processes	This active list includes the names of processes that provide unencrypted and thus insecure communications.	/All Active Lists/ArcSight Solutions/HIPAA/
Instant Messaging Domains	This active list contains all the DNS domains for public Instant messaging servers. This list is used to detect when outbound traffic to these domains is detected signifying a possible information leak. Note: All the domain names must be in lowercase.	/All Active Lists/ArcSight Solutions/HIPAA/
Internal Systems with Insecure Services	This list stores all internal systems with insecure services detected.	/All Active Lists/ArcSight Solutions/HIPAA/
Internet Ports	This active list includes ports that are used for Internet communication.	/All Active Lists/ArcSight Solutions/HIPAA/
Monitored Accounts	This active list is used to maintain user accounts to be monitored, Entries in this list should be in all lower case.	/All Active Lists/ArcSight Solutions/HIPAA/
New Hire Accounts	This active list contains newly hired users and is automatically populated by the "New Hire Identification" rule. New users are retained for 7 days in the list.	/All Active Lists/ArcSight Solutions/HIPAA/
Password Changes	This active is updated with the user and product information when a successful password change occurs.	/All Active Lists/ArcSight Solutions/HIPAA/
Peer to Peer Ports	This active list contains the ports involved in peer-to-peer traffic.	/All Active Lists/ArcSight Solutions/HIPAA/

Active Lists Resources for HIPAA CIP, continued

Resource	Description	URI
Stale Accounts	This active list is used to maintain user names that have not appeared in login events for the time specified by the Active Accounts active list TTL value.	/All Active Lists/ArcSight Solutions/HIPAA/
Suspicious Activities by New Hires	This active list stores events that were identified as attacks by new hires. The original event name is stored in the deviceCustomString1 field. By default, these events are stored for 60 days.	/All Active Lists/ArcSight Solutions/HIPAA/
Unsecured Password Signatures	This active list contains unsecured password signatures.	/All Active Lists/ArcSight Solutions/HIPAA/

Filters

This section lists all the common filter resources included with CIP for HIPAA:

- ["My Filters" below](#)
- ["General Filters" on page 201](#)

Filters specific to a HIPAA Standard are listed in their appropriate sections.

My Filters

This section lists all the filter resources stored in the My Filters group.

CIP for HIPAA Filters in My Filters Group

Resource	Type	URI	Description
Account Creation	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	Identifies account creation events.
Account Deletion	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	Identifies account deletion events.
Account Modification	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	Identifies account modification events.
After Hours	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter defines the time period of 'after hours'. Change this filter to adjust the default settings.

CIP for HIPAA Filters in My Filters Group, continued

Resource	Type	URI	Description
Attacker Asset is Business Associate	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter looks for events originated from business associate assets.
Attacker Asset is PHI	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter identifies events that are originated from third party assets.
Attacker Asset is Third Party	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter identifies events that are originated from third party assets.
Intellectual Property Download	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter defines events which identify the download of possibly illegal intellectual property. Videos, Images, and Audio files can fall into this category. This filter should be configured to catch all the events in the environment which indicate the download of possibly illegal intellectual property. Do not include content that looks for peer-to-peer protocols. That is handled in a separate filter.
Limit Regulation	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	The purpose of this filter is to limit events processed and reported by this package only to the ones that are relevant to the HIPAA regulation. This is achieved by including this filter in the conditions of every other resource (Rules, Queries, Filters, etc.) in the HIPAA Compliance Insight Package (in addition to the other conditions of the resource). You can control the events processed and reported by this package by editing this filter. For example, to process and report on all events that are sent to ESM, change the condition of this filter to "True". For more information about this filter, see the solution's guide.
New Hire Identification	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter identifies newly created accounts.
Target Asset is Business Associate	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter looks for events that are targeting business associate assets.
Target Asset is Clearinghouse	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter identifies events that are targeting clearinghouse assets.
Target Asset is Critical	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter identifies events that are targeting highly critical assets.
Target Asset is Database	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter selects events targeting database hosts.

CIP for HIPAA Filters in My Filters Group, continued

Resource	Type	URI	Description
Target Asset is PHI	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter identifies events that are targeting PHI assets.
Target Asset is Public Facing	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter identifies events that are targeting Public Facing Assets.
Target Asset is Third Party	Filter	/All Filters/ArcSight Solutions/HIPAA/My Filters/	This filter identifies events that are targeting third party assets.

General Filters

This section lists all the filter resources stored in the following General Filters groups and subgroups.

- General Filters (following table)
- [Authentication Filters](#)
- [Firewall Filters](#)
- [Overview Filters](#) (Dashboard Overview and Section Overview filters)
- [Ports Filter](#)
- [Vulnerabilities Filters](#)

CIP for HIPAA Filters in General Filters Group

Resource	Type	URI	Description
Administrative User	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	The purpose of this filter is identify events with administrative users. These events are defined as such in which either the source or destination users are administrative users. Administrative accounts have to be defined *in all lower case* in the active list Administrative Accounts.
Attacker Asset Categorized in Network Domains	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter checks whether the attacker asset is categorized under the Network Domains category.
Attacker Host or Address Present	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.
Attacker User Present	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter identifies events that have the Attacker User Name event fields populated.

CIP for HIPAA Filters in General Filters Group, continued

Resource	Type	URI	Description
Attacker or Target User Present	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter identifies events that have either the Attacker User Name or Target User Name event fields populated.
Attacks and Suspicious Activity	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter identifies events which indicate compromise, reconnaissance, hostile, or suspicious activity.
Event Limit	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	The purpose of this filter is to limit events processed and reported by the solution pack to only the events that are relevant to the regulation. This is achieved by including this filter in the conditions of all other resources in the package such as rules, queries, and filters etc either directly or indirectly. You can change the events processed and reported by this package by editing this filter. See the solution guide for more information.
Inbound Events	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter looks for events coming from outside the organization network targeting internal networks .
Insecure Services	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	Selects events based on inherently insecure services.
Insignificant Events	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter is used to identify events with no or little value. Preferably, these events should be filtered out by the connector.
Internal Attackers	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter looks for events coming from systems inside the organization network.
Internal Connection	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter is looking for connections within the network.
Internal Targets	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter looks for events targeting systems inside the organization network.
Non Administrative User	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	The purpose of this filter is identify events associated with non-administrative users. These events are defined as such in which neither the source nor destination users are administrative users.
Outbound Events	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter looks for events coming from inside the organization network targeting the public network.
Outbound Internet Activity	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter detects all outbound internet activity related events.

CIP for HIPAA Filters in General Filters Group, continued

Resource	Type	URI	Description
Target Asset Categorized in Network Domains	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter checks whether the target asset is categorized under the Network Domains category.
Target Host or Address Present	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter identifies events that have either the Target Host Name or Target Address event fields populated.
Target MAC Address Present	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter identifies events that have the Target MAC Address event fields populated.
Target User Present	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filter checks whether the Target User Name field is populated.
Windows Events with a Non-Machine User	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.

Authentication Filters**CIP for HIPAA Filters in the General Filters/Authentication Group**

Resource	Type	URI	Description
Administrative Login Attempts	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	The purpose of this filter is to identify login attempts by administrative users. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.
Local Logins	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	This filter identifies local login events to a MS Windows or UNIX system.
Login Attempts	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	This filter selects any attempts at logging into systems, It excludes machine logins into Microsoft Windows systems.
Logouts	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	This filter identifies all logout events, It excludes machine logouts from Microsoft Windows systems.
Successful Administrative Logout	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	This filter identifies events that indicate successful administrative logouts from assets categorized in one of your Network Domains.

CIP for HIPAA Filters in the General Filters/Authentication Group, continued

Resource	Type	URI	Description
Successful Logins	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	This filter identified successful logins by both administrative and non-administrative users.
Successful Logouts	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	This filter identifies successful logouts by both administrative and non-administrative users.
Successful User Login	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	This filter identifies successful logins by non-administrative users.
Successful User Logout	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	This filter identifies events that indicate successful logouts by non-administrative users.
Unsuccessful User Login	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	This filter identifies failed logins by non-administrative users.
User Login Attempts	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Authentication/	This filter selects any attempts at logging into systems by non-administrative users. It excludes machine logins into Microsoft Windows systems.

Firewall Filters

CIP for HIPAA Filters in the General Filters/Firewall Group

Resource	Type	URI	Description
Firewall Accepts	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Firewall/	This filter selects all events where a firewall granted passage to traffic.
Firewall Deny	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Firewall/	This filter selects events where a firewall denied passage to traffic.

Overview Filters

This section lists HIPAA filters in the following groups:

- /General Filters/Overview/Dashboard Overview
- /General Filters/Overview/Section Overview

CIP for HIPAA Filters in General Filters/Dashboard Overview Group

Resource	Type	URI	Description
Compliance Score Rules	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Overview/Dashboard Overview/	This filter identifies the rules associated with the Compliance Score use case.
Compliance Score Updates	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Overview/Dashboard Overview/	This filter identifies events that are generated when values in the Compliance Score active list are changed.
HIPAA Rule Firing	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Overview/Dashboard Overview/	This filter selects all rule firing events, where the rule is a part of the compliance content. This filter is used by the overview last-state data monitors. Also, the filter contains an exclusion list for the rules that should not contribute to the overall state as intended to be shown by the overview data monitor.

CIP for HIPAA Filters in General Filters/Section Overview Group

Resource	Type	URI	Description
164.308 Rules Firing	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Overview/Section Overview/	A generic filter to select events generated by any rule firing in this section.
164.310 Rules Firing	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Overview/Section Overview/	A generic filter to select events generated by any rule firing in this section.
164.312 Rules Firing	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Overview/Section Overview/	A generic filter to select events generated by any rule firing in this section.

Ports Filter**CIP for HIPAA Filters in General Filters/Port Group**

Resource	Type	URI	Description
Port Detected	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Ports/	Selects events indicating that port is detected

Vulnerabilities Filters

CIP for HIPAA Filters in General Filters/Vulnerabilities Group

Resource	Type	URI	Description
Vulnerability Events by Non-Scanners	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Vulnerabilities/	This filter identifies vulnerability events reported by non-scanner devices.
Vulnerability Scanner Events	Filter	/All Filters/ArcSight Solutions/HIPAA/General Filters/Vulnerabilities/	This filter identifies scanner-generated events.

Overview Dashboards

These dashboards provide high level information about their specific HIPAA sections.

Overview Dashboards

Resource	Type	URI	Description
164.308 Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/Overview/	This dashboard shows high-level information around HIPAA 164.308 section.
164.310 Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/Overview/	This dashboard shows high-level information around HIPAA 164.310 section.
164.312 Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/Overview/	This dashboard shows high-level information around HIPAA 164.312 section.
Compliance Risk Score Overview	Dashboard	/All Dashboards/ArcSight Solutions/HIPAA/Overview/	This dashboard displays information about the compliance risk score for each regulation section.

Overview Data Monitors

This table lists data monitors displaying content specific to their HIPAA sections.

Overview Data Monitors

Resource	Type	URI	Description
Last 20 Rules Fired	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.308 Overview/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.308 Overview/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.308 Overview/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.308 Overview/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.310 Overview/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.310 Overview/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.310 Overview/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.310 Overview/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.312 Overview/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.312 Overview/	Event graph to show attacker-target pair relationship for the various rule firings from this section.

Overview Data Monitors, continued

Resource	Type	URI	Description
Top 20 Rules Fired	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.312 Overview/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/164.312 Overview/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Compliance Risk Score Overview	Data Monitor	/All Data Monitors/ArcSight Solutions/HIPAA/Overview/	This data monitor displays an icon indicating the compliance risk score for each regulation section. The compliance score is maintained in the Compliance Score active list, and is calculated based on the severity of the rules that were triggered in the solution package.

Field Sets

This section lists all the field set resources included with CIP for HIPAA.

CIP for HIPAA Field Sets

Resource	Type	URI	Description
Audit Tool Logins	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	This field set shows logins from remote machines to the audit tool.
Default Vendor Account	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	This field set shows the default vendor accounts fields.
Device Configuration Changes	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	Includes device fields.
Event with Attacker Data	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	This field set shows the attacker fields.
Events with Target Assets	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	This field set shows events which are related to target assets.
Information Leakage Events	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	This field set shows the assets involved in information leakage cases.
Physical Security	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	A field set that can be used to show the relevant fields for physical security events.
Service Events	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	This field set shows events which are related to service events.

CIP for HIPAA Field Sets, continued

Resource	Type	URI	Description
Traffic with Target Asset Criticality	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	This field set shows the assets involved in a communication along with the target assets' criticality assignment.
User Authentication	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	This field set is used by an active channel to display all user authentication related events.
Vulnerability Fields	Field Set	/All Field Sets/ArcSight Solutions/HIPAA/	Includes the vulnerability fields.

Overview Rules

This section lists overview rule resources.

Overview Rules

Resource	Type	URI	Description
Compliance Score Update	Rule	/All Rules/ArcSight Solutions/HIPAA/Overview/	This rule is triggered by other HIPAA rules and updates the Compliance Score active list.
Manual Status Change	Rule	/All Rules/ArcSight Solutions/HIPAA/Overview/	This rule is triggered when a section's status on the Compliance Risk Score dashboard is changed manually.

Appendix B: Asset and Zone Categories

Following is a list of all the asset and zone categorization used and the filters which use those categorizations.

Asset and Zone Categorizations and Filters Which Use Those Categorizations

Filters	Asset Categorizing	Zone Categorization
Attacker Asset Categorized in Network Domains	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/	
Target Asset Categorized in Network Domains		
Attacker Asset is Third Party	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party
Target Asset is Third Party		
Attacks and Suspicious Activity from Third Party Resources		
Attacks and Suspicious Activity Targeting Third Party Resources		
Attacks and Suspicious Activity to and from Third Party Resources		
Successful Administrative Logins from Third Party Systems		
Successful Administrative Logins to Third Party Systems		
Successful User Logins from Third Party Systems		
Successful User Logins to Third Party Systems		
Unsuccessful Administrative Logins to Third Party Systems		
Unsuccessful User Logins from Third Party Systems		
Unsuccessful User Logins to Third Party Systems		

Asset and Zone Categorizations and Filters Which Use Those Categorizations, continued

Filters	Asset Categorizing	Zone Categorization
Internal Attacker	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected
Internal Target		
Internal Connection		
Inbound Events		
Outbound Events		
Outbound Internet Activity		
Successful Non Secure Remote Access		
Non Secure Remote Access Attempts		
New Hire Based Internet Outbound Activity		
Disallowed Ports Access from Internal Hosts		
Disallowed Ports Access to Internal Hosts		
Internal Inter-Domain Traffic		
External to Internal Traffic		
Internal to External Traffic		

Asset and Zone Categorizations and Filters Which Use Those Categorizations, continued

Filters	Asset Categorizing	Zone Categorization
Attacker Asset is PHI Information Disclosure Vulnerability Detected on PHI Asset Target Asset is PHI Traffic from Others to PHI Traffic from PHI Assets Traffic to PHI Assets Unauthorized File access on PHI assets Vulnerability Detected on PHI Asset	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PHI	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PHI
Target Asset is Clearinghouse Traffic from Other to Clearinghouse	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/HIPAA/Covered Entity/Clearinghouse	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/HIPAA/Covered Entity/Clearinghouse
Attacker Asset is Business Associate Target Asset is Business Associate Attacks and Suspicious Activity from Business Associate Resources Attacks and Suspicious Activity Targeting Business Associate Resources Organizational Records Information Leak from Business Associate Resources Personal Information Leak from Business Associate Resources	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/HIPAA/Business Associate	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/HIPAA/Business Associate

Asset and Zone Categorizations and Filters Which Use Those Categorizations, continued

Filters	Asset Categorizing	Zone Categorization
Target Asset is Critical Removable Media Detected on Highly Critical Machine Startup and Shutdown of Highly Critical Assets System Shutdown of Highly Critical Assets	/All Asset Categories/System Asset Categories/Criticality/Very High /All Asset Categories/System Asset Categories/Criticality/High	/All Asset Categories/System Asset Categories/Criticality/Very High
Target Asset is Database Database Configuration Modification	All Asset Categories/ArcSight System Administration/Databases /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database	All Asset Categories/ArcSight System Administration/Databases /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database
Target Asset is Public Facing	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Communications between Development and Operations	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/ /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/ /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communications between Development and Test	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/ /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/ /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/

Asset and Zone Categorizations and Filters Which Use Those Categorizations, continued

Filters	Asset Categorizing	Zone Categorization
Traffic from Higher to Lower Classification Level	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified/
Traffic from Lower to Higher Classification Level	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret /All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret /All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret
Traffic from Dark Address Space Traffic to Dark Address Space	All Asset Categories/Site Asset Categories/Address Spaces/Dark/	All Asset Categories/Site Asset Categories/Address Spaces/Dark/

Asset and Zone Categorizations and Filters Which Use Those Categorizations, continued

Filters	Asset Categorizing	Zone Categorization
IM Traffic	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/Yahoo IM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/Yahoo IM
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/Google IM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/Google IM
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/AOL IM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/AOL IM
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/ICQ	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/ICQ
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/IRC	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/IRC
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/MSN IM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/MSN IM
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/KIK	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/KIK
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/SNAPCHAT	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/SNAPCHAT
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/SKYPE	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/SKYPE
	/ArcSight Solutions/Compliance	/ArcSight Solutions/Compliance

Asset and Zone Categorizations and Filters Which Use Those Categorizations, continued

Filters	Asset Categorizing	Zone Categorization
	Insight Package/Disallowed Servers/FACEBOOK IM	Insight Package/Disallowed Servers/FACEBOOK IM
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/WhatsApp	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/WhatsApp
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/VIBER	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/VIBER
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/TELEGRAM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/TELEGRAM

Appendix C: Active Lists Requiring Configuration

Active Lists that Require Configuration

Active List	Description	Expected Input Per Entry
Administrative Accounts List	<p>This active list should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the content pack, but the list can also be added to or referenced in new content built around the provided infrastructure.</p> <p>This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in all lower case. For example, the user Administrator should be added as "administrator".</p>	User name, in lowercase.
Allowed Ports	<p>This active list contains all permissible destination ports (all permissible services). This active list should be populated according to your site policy.</p> <p>By default, all connection types and ports are allowed. To be considered a disallowed port, the connection type and port number must either be specified explicitly in the <code>Disallowed Ports</code> active list, or not specified in the <code>Allowed Ports</code> active list. If all ports are specified in the <code>Allowed Ports</code> active list (using the * character), the policy allows all ports (except those specified explicitly in the <code>Disallowed Ports</code> active list). Explicit (that is, not *) port entries in the <code>Disallowed Ports</code> active list always take precedence over entries in the <code>Allowed Ports</code> active list.</p>	Connection type and port number Where Connection type could be: Inbound, outbound or internal
Badges to Accounts	This list contains the computer account and employee type for every physical device badge.	Badge ID, primary computer account for the badgeholder, and the employee type (in lowercase). Specifically, ensure that contractors are identified with the word "Contractor" (case insensitive) in the employee type field.

Active Lists that Require Configuration, continued

Active List	Description	Expected Input Per Entry
Default Vendor Accounts	This active list contains the default user account names for various vendors. This list should be configured at set-up time with existing vendor user account names, and updated as necessary on an ongoing basis.	Default user account and vendor name, in lowercase.
Disallowed Ports	<p>This active list contains all disallowed destination ports. This active list should be populated according to your site policy.</p> <p>By default, all connection types and ports are allowed. To be considered a disallowed port, the connection type and port number must either be specified explicitly in the Disallowed Ports active list, or not specified in the Allowed Ports active list. If all ports are specified in the Allowed Ports active list (using the * character), the policy allows all ports (except those specified explicitly in the Disallowed Ports active list). Explicit (that is, not *) port entries in the Disallowed Ports active list always take precedence over entries in the Allowed Ports active list.</p>	Connection type and port number Where Connection type could be: inbound, outbound or internal
Former Employees	This active list contains user accounts of former employees. User accounts in this active list are retained indefinitely. All the entries in this list need to be in lowercase.	User Name, in lowercase. This list should be maintained on a regular basis.
Insecure Ports	This active list includes ports related to unencrypted and thus insecure communication services.	Port number
Insecure Processes	This active list includes the names of processes that provide unencrypted and thus insecure communications.	Process name, in lowercase
Instant Messaging Domains	This active list contains all the DNS domains for public instant messaging servers. This list is used to detect when outbound traffic to these domains is detected, signifying a possible information leak. Note: All the domain names must be in lowercase.	Domain name of popular or known instant messaging server in lowercase
Internet Ports	This active list includes ports that are used for monitoring internet (Web traffic) communication. By default, it includes ports 80 and 443.	Port number
Monitored Accounts	This active list is used to maintain user accounts to be monitored.	Usernames in lowercase

Active Lists that Require Configuration, continued

Active List	Description	Expected Input Per Entry
New Hire Accounts	This active list contains newly hired users and is automatically populated by the "New Hire Identification" rule. New users are retained for 7 days in the list.	User Name, in lowercase. This list should be maintained on a regular basis.
Peer to Peer Ports	This active list contains the ports involved in peer-to-peer traffic	Should be maintained on a regular basis.
Unsecured Password Signatures	This active list contains unsecured password signatures.	

Appendix D: Resources Requiring Enabled Trends

Shown below is the list of end user resources which requires enabling trends to show data:

CIP for HIPAA Resources Dependent on Enabled Trends

Resource	Type	URI	Required Trend
Monitored Account Activity in the Last Day - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Monitored Users
Monitored Account Activity in the Past Week - Template	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Monitored Users
Top Critical Vulnerabilities	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Vulnerabilities
Vulnerability Events By Scanner	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Vulnerabilities
Vulnerabilities by IP Address	Report	All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/Vulnerabilities by IP Address	Vulnerabilities
Vulnerability Scans	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Vulnerabilities
Top Vulnerable IP Addresses	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/	Vulnerabilities
Vulnerabilities	Query Viewer	/All Query Viewers/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(1) Security Management Process/Vulnerabilities	Vulnerabilities

CIP for HIPAA Resources Dependent on Enabled Trends, continued

Resource	Type	URI	Required Trend
Monthly Trend of Unsuccessful Administrative Logins	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	Count of Administrative Logins Failed Administrative Logins - Long Term Trend
Anti-Virus Stopped or Paused in the Last Mont	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/Anti-Virus Stopped or Paused in the Last Mont	Daily Trend of Anti-Virus Stopped or Paused Events
Number of Successful User Logins over the Past Week	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	User Login Count
Number of Unsuccessful User Logins over the Past Week	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(5) Security Awareness and Training/	User Login Count
Attacks and Suspicious Activity Weekly Trend	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	Attacks and Suspicious Activities Trend
Average Time to Resolution - By User	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	Case History
Average Time to Resolution - By Case Severity	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	Case History
Average Time to Resolution - By Day	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(6) Security Incident Procedures/	Case History

CIP for HIPAA Resources Dependent on Enabled Trends, continued

Resource	Type	URI	Required Trend
Weekly Trend - Shutdown of Critical Machines	Report	/All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(7) Contingency Plan/	Shutdown of Critical Machines
Weekly Trend - Configuration Modification Summary	Report	All Reports/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)(8) Evaluation	Configuration Changes
DoS Attacks Weekly Trend	Report	/All Reports/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(e)(1) Transmission Security/	DoS Attacks Trend

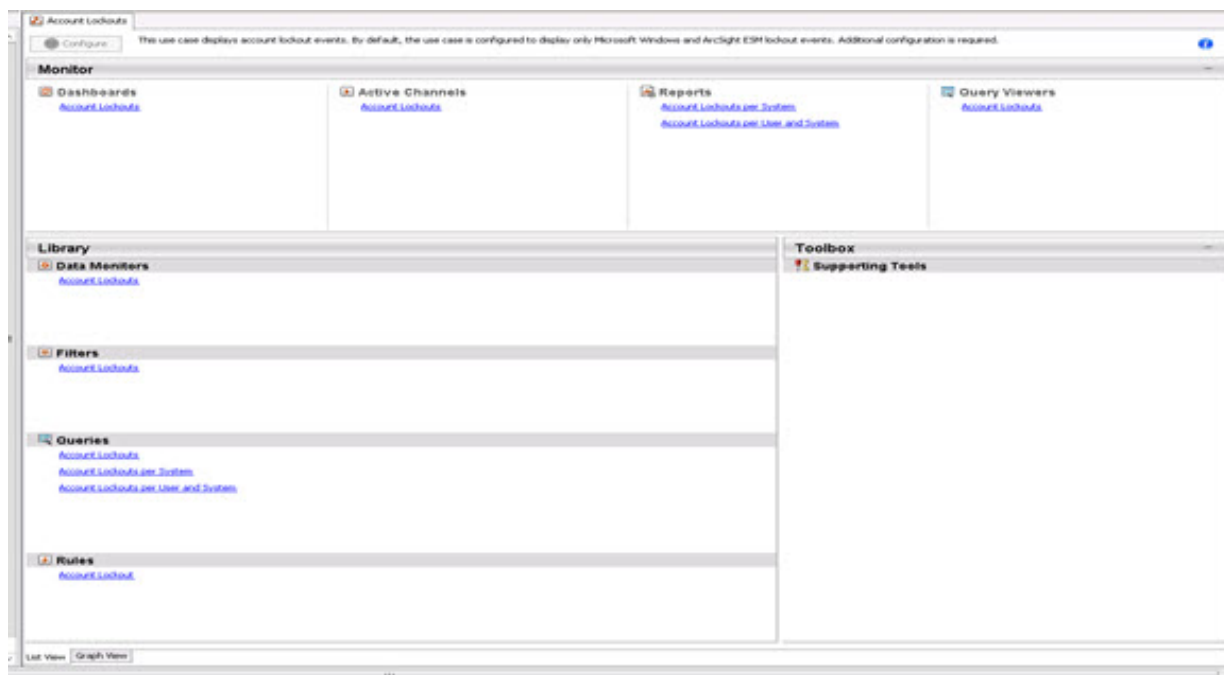
Appendix E: CIP for HIPAA Use Cases

The Compliance Insight Package for HIPAA resources contains different use case resources. A use case resource provides a way to group and view a set of resources that help you to measure and report on compliance with the HIPAA regulation safeguards.

To view the resources associated with a use case resource:

1. In the Console's navigator panel, select the **Use Cases** tab.
2. Browse for the use case resource, such as ArcSight Solutions/HIPAA/Account Lockouts.
3. Right-click the use case resource and select **Open Use Case**.

The resources that make up a use case are displayed as shown below. The use case resource tables listed below contain all the resources that have been explicitly assigned to the use case.



The following table lists the supported devices that may generate events used by CIP for HIPAA reports and other resources.

Key	
APP = Applications	NE = Network Equipment
AV = Antivirus	OS = Operating System
CMS = Content Monitoring System	PM = Policy Management
CS = Content Security	PSS = Physical Security Systems
DB = Database	SIM = Security Information Manager
FW = Firewall	VA = Vulnerability Assessment
IDM = Identity Management	VPN = Virtual Private Network
IDS = Intrusion Detection System	W = Wireless
IPS = Intrusion Prevention System	WF = Web Filtering
NBAD = Network-Based Anomaly Detection	

HIPAA Use Cases

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Account Lockouts	Displays account lockout events. By default, this use case is configured to display only Microsoft Windows and ArcSight ESM lockout events. Additional configuration is required.	164.312 Technical Safeguards - (d) Person or Entity Authentication	APP OS	<ol style="list-style-type: none"> Edit the Account Lockouts filter to add conditions for lockout events from other devices in your environment. By default, the Account Lockouts filter identifies account lockouts on Microsoft Windows and UNIX systems. Verify that the Account Lockouts filter detects events in your environment that match the expected behavior. Deploy the Account Lockout rule to the real-time rules group, and enable case and notification actions if appropriate for your organization.
Administrator Logins and Logouts	Provides information about the administrative logins and logouts.	164.308 Administrative Safeguards - (a)(5) Security Awareness and Training	AV APP CS DB IDM IDS/IPS FW NBAD NE OS PM PSS VA VPN WF W	<ol style="list-style-type: none"> In the Administrative Accounts List active list, define user names that have administrative privileges in your environment. Entries should be lowercase only. The Administrative Login Attempts filter defines the events to be processed by this use case. By default it includes events in which either the source or destination user name is an administrative user defined in the Administrative Accounts List active list.
Anti-Virus Activity	Provides insight into Anti-Virus activity on the organization.	164.308 Administrative Safeguards - (a)(5) Security Awareness and Training	AV OS	No configuration required

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Attacks and Suspicious Activity	Provides information about events that are identified as attacks or suspicious activity.	164.308 Administrative Safeguards - (b)(1) Business Associate Contracts and Other Arrangements 164.308 Administrative Safeguards - (a)(6) Security Incident Procedures	APP AV CS FW IDS IPS NBAD NE W WF	Certain content is not displayed unless assets or zones are categorized. See "Model Assets (Assign Asset Categories)" on page 20.
Audit Log Cleared	Provides information about events that occur when an audit log is cleared or modified manually.	164.312 Technical Safeguards - (b) Audit Controls	FW IPS/IDS OS	By default, the Audit Log Cleared filter returns events indicating that audit logs have been cleared on Microsoft Windows or detected by Symantec HostID systems. Edit this filter to add conditions for additional events known to indicate audit log clearing in your environment
Brute Force Logins	Identifies and provides information about brute force login attempts. Brute force login attempts can either be identified by rules in this use case or by IDSs.	164.312 Technical Safeguards - (d) Person or Entity Authentication	APP DB IDM IDS OS VPN	Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization. <ul style="list-style-type: none"> Frequent Unsuccessful Logins from Attacker Host Brute Force Login Attempts Frequent Unsuccessful Logins to Target Host Successful Attack - Brute Force Login Frequent Unsuccessful Logins by User Name See "Deploy the CIP for HIPAA Rules" on page 27.
Changes to Applications	Provides information about changes to applications.	164.308 Administrative Safeguards - (a)(8) Evaluation	APP	Categorize assets or zones in one of the following groups: <ul style="list-style-type: none"> /System Asset Categories/Criticality/High Or /System Asset Categories/Criticality/Very High See "Categorizing Assets and Zones" on page 21.

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Changes to Database	Provides information about changes to databases.	164.308 Administrative Safeguards - (a)(8) Evaluation	DB	Verify that the Target Asset is Database filter detects events in your environment that match the expected behavior or edit the Target Asset is Database filter to add conditions relevant to your environment.
Changes to Network Equipment	Provides information about changes to firewalls and network equipments.	164.308 Administrative Safeguards - (a)(8) Evaluation	FW IDS/IPS NE	<p>Categorize all firewall, NIDS, or network equipment assets or zones in the following groups, respectively:</p> <p><code>/Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/Firewall</code></p> <p><code>/Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/NIDS</code></p> <p><code>/Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Network</code></p> <p>See "Model Assets (Assign Asset Categories)" on page 20.</p>
Changes to Operating Systems	Provides information about changes to operating systems.	164.308 Administrative Safeguards - (a)(8) Evaluation	OS	<p>Categorize assets or zones in one of the following groups:</p> <ul style="list-style-type: none"> <code>/System Asset Categories/Criticality/High</code> Or <code>/System Asset Categories/Criticality/Very High</code> <p>See "Model Assets (Assign Asset Categories)" on page 20.</p>

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Clock Synchronization Issues	Detects when events' device receipt time is greater than the connector receipt time and when there is a large offset between the end time and manager receipt time.	164.312 Technical Safeguards - (b) Audit Controls	APP AV CS DB FW IDM IDS/IPS NBAD NE OS PM PSS VA VPN W WF	<p>The Clock Synchronization Issues use case requires the following configuration for your environment:</p> <p>In the following filters, set the time offset per your organization's policy:</p> <ul style="list-style-type: none"> • Big Difference Between End Time and Manager Receipt Time • Device Time is Later than Agent Time
Covert Channel Activity	Reports on covert channel activity, such sending TCP traffic over an ICMP channel.	164.312 Technical Safeguards - (e)(1) Transmission Security	IDS/IPS	Verify that the Covert Channel filter detects events in your environment that match the expected behavior.

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Default Vendor Accounts	Provides information about logins using default vendor accounts.	164.312 Technical Safeguards - (a)(1) Access Control	IDS/IPS FW OS NE DB VPN	<p>The Default Vendor Accounts use case requires the following configuration for your environment:</p> <ol style="list-style-type: none"> 1. In the Default Vendor Accounts active list, specify the default vendor accounts for your organization in lowercase in the Vendor Name field. For user names that apply to all vendors, use * (asterisk wildcard). For example: admin,* 2. Note that the Successful Default Vendor Account Used rule is triggered upon successful login to any vendor account. If you do not want to report on all accounts, include only the users and vendors you want to monitor in the Default Vendor Accounts active list. 2. Deploy the Successful Default Vendor Account Used rule to the real-time rules group and enable the notification action if appropriate for your organization. <p>See "Deploy the CIP for HIPAA Rules" on page 27.</p>

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Disallowed Ports	Provides information about connections to non-allowed ports.	164.312 Technical Safeguards - (e)(1) Transmission Security	IDS/IPS FW VPN NE W	<p>The Disallowed Ports use case supports three separate policies for port control depending on the direction of the monitored connection: inbound, outbound, or internal, as indicated in the Connection Type field of the Allowed Ports and Disallowed Ports active lists. These active lists serve as a “whitelist” and “blacklist” of ports to provide more configuration flexibility. By default, all connection types and ports are allowed.</p> <p>To be considered a disallowed port, the connection type and port number must either be specified explicitly in the Disallowed Ports active list, or not specified in the Allowed Ports active list. If all ports are specified in the Allowed Ports active list (using the * character), the policy allows all ports (except those specified explicitly in the Disallowed Ports active list). Explicit (that is, not *) port entries in the Disallowed Ports active list always take precedence over entries in the Allowed Ports active list. Conditions are located in the Disallowed Ports Access filter.</p>
DoS Attacks	Provides an insight into denial of service attacks.	164.312 Technical Safeguards - (e)(1) Transmission Security 164.308 Administrative Safeguards - (a)(6) Security Incident Procedures	IDS OS FW APP SIM NBAD W NE	Verify that the DoS Attacks filter detects events in your environment that match the expected behavior.
Email Activity	Provides information about email activity.	164.312 Technical Safeguards - (e)(1) Transmission Security	Email APP	Verify that the Email Attacks , Email Traffic , Phishing Attacks , and Spamming Attacks filter detects events in your environment that match the expected behavior.

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Firewall Traffic Overview	Reports on various firewall traffic controls namely blocked inbound and outbound traffic and open ports in the enterprise.	164.312 Technical Safeguards - (a)(1) Access Control	FW	<ol style="list-style-type: none"> 1. Verify that the Firewall Deny and Firewall Accepts filters detect events in your environment that match the expected behavior. 2. (Optional) Categorize zones and assets for your environment in the appropriate categories. If you do not perform this configuration step, some reports will not populate. <p>See "Model Assets (Assign Asset Categories)" on page 20.</p>
High Risk Events	Displays an overview of the events that require most attention.	164.308 Administrative Safeguards - (a)(1) Security Management Process	IPS/IDS	Verify that the High Priority Events filter detects events that require immediate attention.
IM Traffic	Provides information about IM messaging usage inside the network.	164.312 Technical Safeguards - (e)(1) Transmission Security	IPS/IDS	<ol style="list-style-type: none"> 1. Identify instant messaging servers using one of the following techniques: Create assets for popular or known instant message servers (Viber, KIK, Facebook, Yahoo, IM, Google Hangout, SKYPE) and categorize them appropriately under /Compliance Insight Package/Disallowed Servers. 2. In the Instant Messaging Domains active list, specify the domain names of popular or known instant messaging servers in lowercase. 3. Verify that the IM Traffic filter detects events in your environment that match the expected behavior.

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Inactive User Account Detected	Identifies user accounts that have not been active for a certain period of time, and then identifies activity from such stale accounts.	164.312 Technical Safeguards - (a)(1) Access Control	OS DB APP FW VPN IDM PM NE PSS	<ol style="list-style-type: none"> In the Active Accounts active list, set the appropriate TTL value for your organization. The TTL value specifies the timeframe by which an account is considered “stale” if no successful logins to the account have occurred. When a successful login to an account occurs, the account is placed on the Active Accounts active List. If, for example, the TTL value is 30 days, then if no successful login event to that account occurs in the next 30 days, the account expires from the Active Accounts active list and is placed on the Stale Accounts active list. When a login attempt (either successful or failed) is identified from an account on the Stale Accounts active list, a case is opened. Verify that the Successful Logins filter detects events in your environment that match the expected behavior. See the topic, "Debugging Filters to Match Events" in the <i>ArcSight Console User's Guide</i>. Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization. User Logged in - Added to Active Accounts List Login Activity by a Stale Account Inactive User Account Detected Suspicious Activities by a Stale Account
Incident Management	Provides information and metrics about opened and close cases in this Compliance Insight Package. Information includes stage, severity, and time to resolution.	164.308 Administrative Safeguards - (a)(6) Security Incident Procedures	AV IDS/IPS OS FW APP SIM VA IDM VPN	No configuration required.

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Information Interception	Identifies and reports on possible kinds of information interception events incidents such as spoofing attempts, man-in-the-middle attacks or instant messaging.	164.312 Technical Safeguards - (e)(1) Transmission Security	FW IDS VPN NBAD	<ol style="list-style-type: none"> 1. Verify that the Information Interception filter detects events in your environment that match the expected behavior. 2. Deploy the Possible Information Interception rule to the real-time rules group, and enable case and notification actions if appropriate for your organization. <p>See "Deploy the CIP for HIPAA Rules" on page 27.</p>
Information Leakage	Identifies and reports on all kinds of information leaks that may have occurred.	164.312 Technical Safeguards - (e)(1) Transmission Security or 164.308 Administrative Safeguard - (b)(1) Business Associate Contracts and Other Arrangements	FW IDS CMS	<ol style="list-style-type: none"> 1. Verify that the following filters detect events in your environment that match the expected behavior for each filter: Personal Information Leak All Information Leak Events Organizational Records Information Leak 2. Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization: Organizational Data Information Leak Personal Information Leak Organizational Data Information Leak Personal Information Leak <p>See "Deploy the CIP for HIPAA Rules" on page 27.</p>
Information System Audit Tool Usage	Shows logins to information security audit tools.	164.312 Technical Safeguards - (b) Audit Controls	CS WF PM APP	Verify that the Information System Audit Tool Login filter detects logins to all information security audit tools.

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Insecure Communications	Provides information about unencrypted and thus insecure communications inside the network.	164.312 Technical Safeguards - (e)(1) Transmission Security	FW IDS/IPS NE	<ol style="list-style-type: none"> 1. In the Insecure Processes active list, add any processes that your organization knows to be insecure. 2. In the Insecure Ports active lists, add the ports that your organization knows to be insecure. 3. Verify that the Insecure Services and Port Detected filters work as expected on your environment . 4. Deploy the Internal Insecure Service Provider Detected rule to the real-time rules group, and enable case and notification actions if appropriate for your organization. <p>See "Deploy the CIP for HIPAA Rules" on page 27.</p>
Intellectual Property Rights Violations	Provides information about Intellectual Property Rights Violations.	164.312 Technical Safeguards - (e)(1) Transmission Security	FW IDS NE	<ol style="list-style-type: none"> 1. Configure the Intellectual Property Download filter to detect all events in your environment that indicate the download of illegal intellectual property. Then verify that the Intellectual Property Download filter detects events in your environment that match the expected behavior. 2. Deploy the Intellectual Property Rights Violation rule to the real-time rules group, and enable case and notification actions if appropriate for your organization.
Internal Reconnaissance Activity	Identifies and reports all reconnaissance activities conducted by internal hosts.	164.308 Administrative Safeguard – (a)(3) Workforce Security	FW IDS/IPS NBAD CS WF	<ol style="list-style-type: none"> 1. Verify that the Internal Attackers filter detects events in your environment that match the expected behavior. 2. Deploy the Internal Recon Detected rule to the real-time rules group, and enable case and notification actions if appropriate for your organization. <p>See "Deploy the CIP for HIPAA Rules" on page 27.</p>

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Malicious Code Activity	Monitors for malicious code (such as viruses, worms, trojans, or backdoor activities) on the network, allowing administrators to remediate infected machines.	164.308 Administrative Safeguard - (a) (5) Security Awareness and Training	AV IDS/IPS NBAD FW CS WF AV	<ol style="list-style-type: none"> Verify that the following filters detect events in your environment that match the expected behavior for each filter: Anti-Virus Clean or Quarantine Attempt Failed Virus Removal Attempt Malicious Code Activity Malware Activity Spyware Activity Anti-Virus Clean or Quarantine Attempt Trojan Activity Virus Activity Worm Activity (Optional) Categorize internal zones and assets as /Site Asset Categories/Address Spaces. Deploy the rules on this use case to the real-time rules group, and enable case and notification actions if appropriate for your organization. <p>For more information about deploying rules, see "Deploy the CIP for HIPAA Rules" on page 27.</p>
PKI Certificate Validity	Provides insight into incidents where an invalid or expired Public Key Infrastructure (PKI) certificate was detected.	164.312 Technical Safeguards - (e)(1) Transmission Security	APP VPN IDS	<p>Review the Invalid or Expired Certificate filter to identify events associated with invalid or expired certificates. Then verify that the filter detects events in your environment that match the expected behavior.</p> <p>The Invalid or Expired Certificate report assumes that the certificate name is included in the Device Custom String1 event field. If it is not, modify as applicable.</p>

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Physical Access	Detects violations and reports on events related to physical security devices such as badge readers. Specifically, it detects after hour building access by contractors and local logins from badged out employees.	164.310 Physical Safeguards - (a)(1) Facility Access Controls	PSS	<ol style="list-style-type: none"> 1. Populate the Badges to Accounts active list with the badge ID, primary computer account for the badge holder, and the employee type for users in your organization (in lowercase). Specifically, ensure that contractors are identified with the word Contractor (case insensitive) in the employee type field. 2. Modify the After Hours filter to specify the appropriate after-business-hours window for your organization. 3. Verify that the: <ul style="list-style-type: none"> Physical Access Events filter correctly identifies events from your physical security systems; Building Access filter correctly identifies building access events; Successful Badge In filter correctly identifies events that are logged when an employee enters the facility. 4. Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization. <ul style="list-style-type: none"> After Hours Building Access by Contractors Failed Building Access Local Logon from Badged Out Employee Badged Out Employee Successful Badge In Successful Badge Out <p>See "Deploy the CIP for HIPAA Rules" on page 27.</p>

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Policy Violations	Provides information about policy violations.	164.308 Administrative Safeguards - (a)(1) Security Management Process	IDS FW OS VA APP SIM IDM VPNs PM	<ol style="list-style-type: none"> 1. Certain content does not display unless assets or zones are categorized: Categorize all assets or zones in one or more categories in the /ArcSight Solutions/Compliance Insight Package/Network Domains group. For more information about categorizing assets or zones, see "Model Assets (Assign Asset Categories)" on page 20 2. Verify that the Policy Breaches and Policy Violations filters detects events in your environment that match the expected behavior.
Redirection Attacks	Provides information about redirection attacks.	164.312 Technical Safeguards - (e)(1) Transmission Security	FW IDS VPN NBAD	<ol style="list-style-type: none"> 1. Verify that the Redirection Attacks filter detects events in your environment that match the expected behavior. 2. Deploy the Possible Redirection Attack rule to the real-time rules group, and enable case and notification actions if appropriate for your organization. <p>See "Deploy the CIP for HIPAA Rules" on page 27.</p>
Security Patches	Provides information about missing security patches.	164.308 Administrative Safeguards - (a)(8) Evaluation	VA	Verify that the Vulnerability Scanner Events filter detects events in your environment that match the expected behavior.
Business Associate and Third Party Monitoring	Provides information about third party and business associate assets.	164.308 Administrative Safeguards - (b)(1) Business Associate Contracts and Other Arrangements	FW IDS OS VA APP SIM IDM VPN PM NE	<p>Model the third-party assets or zones in your environment and categorize them in:</p> <p>/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party</p> <p>See "Model Assets (Assign Asset Categories)" on page 20.</p>

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Traffic Anomaly	Provides information about the traffic anomaly.	164.312 Technical Safeguards - (e)(1) Transmission Security	FW IDS VPN NBAD	<ol style="list-style-type: none"> 1. Verify that the Traffic Anomaly filter detects events in your environment that match the expected behavior. 2. Deploy the Possible Traffic Anomaly rule to the real-time rules group, and enable case and notification actions if appropriate for your organization. <p>See "Deploy the CIP for HIPAA Rules" on page 27.</p>
Traffic Between Entities	Provides information about the traffic flowing between various network entities (like zones, external, internal, operation, development)	164.312 Technical Safeguards - (a)(1) Access Control	NE FW IDS/IPS	<ol style="list-style-type: none"> 1. Certain content does not display unless assets or zones are categorized. Categorize assets or zones in the appropriate network domains in /ArcSight Solutions/Compliance Insight Package/Network Domains See "Model Assets (Assign Asset Categories)" on page 20. 2. Deploy the following rules to the real-time rules group, and enable the case action if appropriate for your organization. Communication between Electronic PHI and Business Associate Domains Communication between Production and Development Domains Communication between Sensitive Asset and Test Domain Communication between Sensitive Asset and Third Party Domain See "Deploy the CIP for HIPAA Rules" on page 27.

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
User Activity	Provides information about the kinds of activities in which users are engaging.	164.308 Administrative Safeguards - (a)(1) Security Management Process	IDS/IPS DB OS FW VPN IDM PM NE AV W APP NBAD	<ol style="list-style-type: none"> 1. In the Administrative Accounts List active list, define usernames that have administrative privileges in your environment. Entries should be in lowercase. By default, the User Activity use case reports on events in which the source and destination users do not have administrative privileges. 2. Populate the Monitored Accounts active list with the usernames to be monitored.
User Logged in from Two Countries	Shows login attempts with the same user name from two different countries.	164.312 Technical Safeguards - (a)(1) Access Control	IDS/IPS DB OS FW VPN IDM PM NE CS WF W APP	<ol style="list-style-type: none"> 1. By default, this use case works only for logins from public IP addresses. To detect login attempts from private IP addresses, associate all appropriate assets or zones with a location resource with a defined Country field. For example, if Asset1 and Asset2 are in two different countries, you should create two location resources, Location1 and Location2. Then, associate those location resources with the corresponding assets, for example Asset1 with Location1. 2. Verify that the Successful Logins filter detects events in your environment that match the expected behavior. 3. Deploy the User Logged in from Two Countries rule to the real-time rules group, and enable case and notification actions if appropriate for your organization. <p>See "Deploy the CIP for HIPAA Rules" on page 27.</p>

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
User Logins and Logouts	Provides insight into login and logout activity for non-administrative users.	164.308 Administrative Safeguards - (a)(5) Security Awareness and Training	IDS/IPS DB OS FW VPN IM PM NE CS WF W APP	<ol style="list-style-type: none"> 1. In the Administrative Accounts List active list, define usernames that have administrative privileges in your environment. Entries should be lowercase only. See "Configure Active Lists" on page 22. 2. By default, this use case processes only those events in which neither the source nor the destination users have administrative privileges. To change this default behavior to include events involving users with administrative privileges, edit the non-administrative user. 3. Verify that the following filters detect the appropriate events: Login Attempts Logouts User Login Attempts Successful User Login Successful User Logout Unsuccessful User Login

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Vulnerability Scanning	Provides information about vulnerabilities that might exist, and how they relate to defined assets.	164.308 Administrative Safeguards - (a)(1) Security Management Process	VA	<ol style="list-style-type: none"> 1. Verify that the Vulnerability Scanner Events filter detects events in your environment that match the expected behavior. 2. Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization. <ul style="list-style-type: none"> Critical Vulnerability Detected Information Disclosure Vulnerability on PHI Asset Overflow Vulnerabilities SQL Injection Vulnerabilities Specific Vulnerability Detected- Template Vulnerabilities on Critical Machine XSRF Vulnerabilities XSS Vulnerabilities See "Deploy the CIP for HIPAA Rules" on page 27 3. Certain content is not displayed unless assets or zones are categorized. Categorize assets or zones in the appropriate network domains in <code>/ArcSight Solutions/Compliance Insight Package/Network Domains</code> See "Model Assets (Assign Asset Categories)" on page 20.
Isolating health care clearinghouse functions	Provides information about possible non isolated clearinghouse functions.	164.308 Administrative Safeguard - (a)(4) Information Access Management	IDS/IPS NE FW	<p>Certain content is not displayed unless assets or zones are categorized. Categorize assets or zones in the appropriate network domains in <code>/ArcSight Solutions/Compliance Insight Package/Network Domains</code>.</p> <p>See "Model Assets (Assign Asset Categories)" on page 20.</p>

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
New Hire Employee Account Activity	Provides information about any activity performed by users who are known to be as new.	164.308 Administrative Safeguard - (a) (3) Workforce Security	OS DB APP FW VPN IDM PM NE PSS	<p>The New Hire Employee Account Activity use case requires configuration for your environment.</p> <p>When a new user account is created, it is placed automatically on the New Hire Accounts active list (list entry is in lowercase). If an account creation event does not accurately identify new hires in your organization, you can</p> <ul style="list-style-type: none"> Change the conditions of the New Hire Identification filter to match an event that better identifies a new hire in your organization, Or Periodically upload new hire accounts (in lowercase) from an external source to the New Hire Accounts active list. If you do so, disable the action in the New Hire Identification rule that writes to the New Hire Accounts active list. <p>By default, the new account expires from the New Hire Accounts active list after 7 days. If your organization prefers to monitor new employees for a different length of time, edit the TTL for the New Hire Accounts active list to reflect the appropriate window for your organization.</p>

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Password Management	Monitors password change events as well as to alert if a password has not been changed for a longer time than allowed by policy.	164.308 Administrative Safeguard - (a) (5) Security Awareness and Training	OS VA	<p>When a successful password change event is detected, the user name for whom the password was changed and the device that reported the event are placed on the Password Changes active list. An entry expiring from this active list indicates that the user has not changed the password on that device for longer than allowed by policy (as indicated by the TTL setting of the active list). In that case, Password not Changed for Longer than Policy Standard rule detects the event and open a case. If the user changes his/her password within the time defined by the policy, a rule detects this event and update the entry on the active list so the entry does not expire.</p> <p>The Password Management use case requires the following configuration for your environment:</p> <ul style="list-style-type: none"> • In the Password Changes active list, edit the TTL to reflect the maximum amount of time allowed between password changes according to your organization's policy. • Edit the Password Change Attempts filter to identify all password change attempts from devices on your system. By default, the filter detects only password change attempts on Microsoft Windows. Verify that the Password Change Attempts filter detects events in your environment that match the expected behavior. • Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization: <ul style="list-style-type: none"> Password not Changed for Longer than Policy Standard Successful Password Change
Removable Media Activity	Provides information about removable media activity.	164.310 Physical Safeguards - (d)(1) Device and media controls	OS	<p>Edit the Removable Media Detected filter to identify all removable media from devices on your system. By default, the filter detects only removable media attempts on Microsoft Windows. Verify that the Removable Media Detected filter detects events in your environment that match the expected behavior.</p>

HIPAA Use Cases, continued

Use Case	Description	HIPAA Section	Supported Devices	Special Configurations
Startup and Shutdown of Machines	Identifies when machines are shut down in your environment.	164.308 Administrative Safeguards - (a)(7) Contingency Plan	OS	Certain content is not displayed unless assets or zones are categorized. Categorize assets or zones in the appropriate network domains in /ArcSight Solutions/Compliance Insight Package/Network Domains See "Model Assets (Assign Asset Categories)" on page 20.
VPN Access Reporting	Provides reports detailing all attempts to gain access to your environment using Virtual Private Network (VPN) facilities.	164.310 Physical Safeguards - (b) Workstation Use	VPN	This use case requires the following configurations for your environment: <ol style="list-style-type: none"> 1. In the Insecure Processes active list, add any processes that your organization knows to be insecure. 2. In the Insecure Ports active lists, add the ports that your organization knows to be insecure.

Appendix F: Compare, Backup and Uninstall Package


This chapter provides instructions for the backup and uninstall of the Compliance Insight Package for HIPAA (CIP for HIPAA). This appendix is not part of the initial configuration and is provided if you want to generate a list of resource changes, back up the solution package or uninstall the CIP for HIPAA at a later date.

Generate a List of Resource Changes

Before backing up a solution package, you may want to generate a list of resource changes since the last time the package was exported to a package bundle. The current resources associated with the selected package are compared against the resources saved in the package bundle and any new, modified or deleted resources are reported.

Note: Every time a package is exported, the change history is reset.

To generate a list of resource changes:

1. Log into the ArcSight Console as ArcSight Administrator.
2. In the **Packages** tab of the Navigator panel, navigate to the solution group.
For CIP for HIPAA, navigate to ArcSight Solutions/HIPAA 3.0.
3. Right-click the solution package () and select **Compare Archive with Current Package Contents**.
In the Viewer panel, a list of resources associated with the package are displayed. In the right column called Change Since Archive, any changes with the resource since the last export are displayed, either Added, Modified, or Removed.

Comparison of Contents for HIPAA 3.0

Comparison for package HIPAA 3.0
Resource Count: 1648

Type	Parent URI	Resource	Change Sinc...
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	High Priority Events	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Policy Violations	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Technical Compliance Check Failures	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Vulnerability Events	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Internal Reconnaissance	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Account Authorization Changes Summary	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Privileged Account Changed	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Removal of Access Rights	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Failed Virus Removal Attempt	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Login Attempts	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Logouts	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Malicious Code Activity	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Security Software Stopped or Paused	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	All Attacks and Suspicious Activity Events	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Attacks and Suspicious Activity Targeting PHI Resources	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Attacks and Suspicious Activity Targeting Public Facing Res...	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Attacks and Suspicious Activity Targeting Third Party Resou...	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Attacks and Suspicious Activity from PHI Resources	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Attacks and Suspicious Activity from Public Facing Resources	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Attacks and Suspicious Activity from Third Party Resources	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Critical Assets Resource Exhaustion	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Critical Systems Startup and Shutdown	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Information System Failures on Critical Assets	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Database Configuration Changes	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Firewall Configuration Changes	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Network IDS Configuration Changes	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Network Routing Configuration Changes	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	Software Changes in Operations	Modified
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(a)...	VPN Configuration Changes	Modified
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)...	Attacks and Suspicious Activity Targeting Business Associat...	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.308 Administrative Safeguards/164.308(b)...	Attacks and Suspicious Activity from Business Associate Res...	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.310 Physical Safeguards/164.310(a)(1) Fa...	Physical Security	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) A...	Default Vendor Account Used	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(a)(1) A...	Traffic Between Network Domains	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audi...	Audit Log Cleared	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(b) Audi...	Information System Audit Tool Logins	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(d) Pers...	Account Lockouts	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(e)(1) T...	All Information Leak Events	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(e)(1) T...	DoS Attacks	
Active Channel	/All Active Channels/ArcSight Solutions/HIPAA/164.312 Technical Safeguards/164.312(e)(1) T...	Intellectual Property Rights Violations	

- Optional—For future reference, you can copy and paste the cells from the list into a spreadsheet.

Back Up the Solution Package

ArcSight recommends that you have a backup of the current state before making content changes or installing/uninstalling solution packages. Before backing up a solution, you may want to get a list of changed resources. You may want to back up only those resources that have been modified or added. For detailed instructions, see ["Generate a List of Resource Changes" on the previous page](#).

You can back up the solution content to a package bundle file that ends in the .arb extension as described in the process below.

To back up a solution package:

- Log into the ArcSight Console as ArcSight Administrator.
- In the Packages tab of the Navigator panel, navigate to the solution group.
For CIP for HIPAA, navigate to ArcSight Solutions/HIPAA 3.0.
- Right-click the solution package (📦) and select **Export Package(s) to Bundle**.
The Package Bundle Export dialog displays.

4. In the Package Bundle Export dialog, browse for a directory location, specify a file name and click **Next**.

The Progress tab of the Export Packages dialog displays the progress of the export.

5. When the export is finished, click **OK**.

The resources are saved into the package bundle file that ends with the .arb extension. You can restore the contents of this package at a later time by importing this package bundle file.

Uninstall the CIP for HIPAA

Before uninstalling the CIP for HIPAA, backup all the packages (📁) for all the solutions currently installed on the ESM Manager.

For example, if the CIP for HIPAA and the PCI solution are both installed on the same ESM Manager, export the package(s) for each solution before uninstalling either solution. Back up the PCI package into a package bundle (ARB) file and then back up the CIP for HIPAA into a different package bundle (ARB) file before uninstall either solution. For detailed instructions, see ["Back Up the Solution Package" on the previous page](#). You may also want to generate a list of changes before the uninstall. For detailed instructions, see ["Generate a List of Resource Changes" on page 245](#).

To uninstall the CIP for HIPAA:

1. Log into the ArcSight Console as ArcSight Administrator.
2. Click the Packages tab in the Navigator panel.
3. In the Packages tab of the Navigator panel, navigate to ArcSight Solutions/HIPAA 3.0.
4. Right-click the HIPAA 3.0 package (📁) and select **Uninstall Package**.
5. In the Uninstall Packages dialog, click **OK**.

The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog.

6. When the uninstall is finished, click **OK**.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Solutions Guide (ESM CIP for HIPAA 3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!