Hewlett Packard
Enterprise

HPE ArcSight Security Solution Guide

Compliance Insight Package for PCI 3.0

ArcSight Logger

May 10, 2012

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from HPE 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

Contact Information

Phone	A list of phone numbers for HPE ArcSight Technical Support is available on the HPE Enterprise Security contacts page: www.hpe.com/software/support/contact_list
Support Web Site	www.hpe.com/software/support
Protect 724 Community	https://www.protect724.hpe.com

Contents

Chapter 1: Logger CIP for PCI Architecture 7

About ArcSight Logger™ 7
Logger CIP for PCI Architecture 8
Identifying PCI-Related Events to Process 8
PCI Resources 9

Chapter 2: Installation and Configuration 11

Before Upgrade or Install 11
Verify the Logger Version 11
Supported Devices 11
Connectors Needed for Non-CEF Devices 11
Upgrade from Logger CIP for PCI v2.1 12
Install Logger CIP for PCI v3.0 12
Install Logger CIP for PCI on the Logger Appliance 12
Install Logger CIP for PCI on the Software Logger 13
Verify Logger CIP for PCI Content 13
Configure Logger CIP for PCI 14
Process All Events or Limit the Events 14
Process All Events 14
Limit the Events Processed 16
Configure Alerts with Site-Specific Data 21
Configure Reports with Site-Specific Data 21
Configure and Enable PCI Alerts 22
Running Logger CIP for PCI Reports 23

Chapter 3: Overview of PCI Resources 25

PCI Alerts 25
Match Count and Threshold (Sec) Fields 26
Customizing PCI Alerts with Regular Expressions 26
PCI Reports 26
PCI Executive Report 27
Top 10 Vulnerabilities Query 28
Top 10 Users Accessing DB Query 28
10 Most Attacked Hosts Query 28

10 Hosts with Most Virus Events Query 29
PCI Standard Reports 29
Anatomy of a Standard Report 30
Drill-Down Reports 30
PCI Queries 31

Chapter 4: PCI Resources 33

Requirement 1: Firewall Configuration 40
Requirement 1 Alerts 41
Requirement 1 Reports 43
Requirement 2: Default Security Parameters 45
Requirement 2 Alert 46
Requirement 2 Report 47
Requirement 3: Protect Stored Data 47
Requirement 3 Alerts 48
Requirement 3 Report 50
Requirement 4: Encrypt Transmissions 50
Requirement 4 Alerts 51
Requirement 4 Reports 52
Requirement 5: Anti-Virus 53
Requirement 5 Alerts 54
Requirement 5 Reports 55
Requirement 5 Drill-Down Report 57
Requirement 6: System Applications 58
Requirement 6 Alerts 58
Requirement 6 Reports 59
Requirement 7: Business Need-To-Know 62
Requirement 7 Reports 63
Requirement 8: Unique User ID 63
Requirement 9: Physical Access 65
Requirement 9 Alerts 65
Requirement 9 Reports 66
Requirement 10: Track and Monitor Data Access 68
Requirement 10 Alerts 70
Requirement 10 Reports 84
Sending Virtualization Component Events to ArcSight ESM 98
Requirement 11: Test Systems and Networks 99
Requirement 11 Alerts 100
Requirement 11 Reports 100
Requirement 11 Drill-Down Reports 103
Requirement 12: Maintain an Information Security Policy 106
Requirement 12 Reports 106
Requirement 12 Drill-Down Reports 106

PA-DSS Requirement 4: Log Payment Application Activity 109
Sending Payment Application Events to ArcSight ESM 109
PA-DSS Requirement 4 Alerts 111
PA-DSS Requirement 4 Reports 114

Appendix A: Supported PCI Devices 119

Supported Devices for PCI Reports 119
Supported Devices for PCI Alerts 125

Appendix B: Upgrade from CIP for Logger PCI v2.1 131

Upgrade Considerations 131
Upgrade Logger CIP for PCI on the Logger Appliance 132
Upgrade Logger CIP for PCI on the Software Logger 133
Uninstall Logger CIP for PCI 133

Appendix C: Drill-Down Report Reference 135

Requirement 5: Anti-Virus Report Drill-Downs 136
Requirement 10: Track and Monitor Data Access Report Drill-Downs 138
Requirement 11: Test Systems and Networks Report Drill-Downs 138
Requirement 12: Maintain an Information Security Policy Report Drill-Downs 145
PA-DSS Requirement 4: Log Payment Application Activity Report Drill-Downs 146

Index 147

Chapter 1

Logger CIP for PCI Architecture

The Payment Card Industry (PCI) Data Security Standard 2.0 is a comprehensive standard defined by the Payment Card Industry Security Standards Council to help organizations protect customer account data and to advance the broad adoption of consistent data security measures across the globe. The standard includes twelve requirements for security management, policies, procedures, network architecture, software design, and other key protective measures.

ArcSight Logger™ Compliance Insight Package for Payment Card Industry (Logger CIP for PCI) is a package of reports and alerts that can assist you in complying with the PCI requirements specified in Payment Card Industry Data Security Standard 2.0 and the Payment Application Data Security Standard (PA-DSS) 2.0.

Logger CIP for PCI leverages ArcSight Logger's litigation-quality, long-term repository of log and event data to facilitate better PCI compliance audits, security forensics, and system maintenance using ArcSight Logger's reporting and alerting capability.

Logger CIP for PCI addresses the PCI standard by providing:

- Detailed reports on the 12 requirements defined in the PCI Standard
- Detailed reports on Requirement 4 of the Payment Application Standard (PA-DSS)
- Alerts that monitor incoming events in real time and notify PCI analysts when events of interest are detected

Providing these reports and alerts helps demonstrate the following to stakeholders and auditors:

- Controls are implemented on your company's systems that contain credit card data
- Due diligence to comply with the PCI standard

This chapter contains the following topics:

"About ArcSight Logger™" on page 7
"Logger CIP for PCI Architecture" on page 8
"PCI Resources" on page 9

About ArcSight Logger™

ArcSight Logger is a scaleable, high performance log management platform for collection, cost effective storage, and analysis of all log data across the enterprise for use cases ranging from security and compliance to IT operations and networking.

ArcSight Logger is optimized for extremely high event throughput. An event is a time-stamped text message, either a syslog message sent by a host or a line appended to a log file. Logger receives and stores events, supports search and retrieval, and can optionally forward selected events to any syslog-ready device.

For more about ArcSight Logger, see the *ArcSight Logger™ Administrator's Guide*. The *ArcSight Logger™ Online Help* is the *ArcSight Logger™ Administrator's Guide* in a context-sensitive, online format and is available from the ArcSight Logger™Web console.

Logger CIP for PCI Architecture

Logger CIP for PCI reports work on events in Common Event Format (CEF) format, an industry standard for the interoperability of event or log-generating devices.

CEF events can come from a device that is already configured to post events in CEF format, or they can come from any network device whose events are first run through an ArcSight SmartConnector.

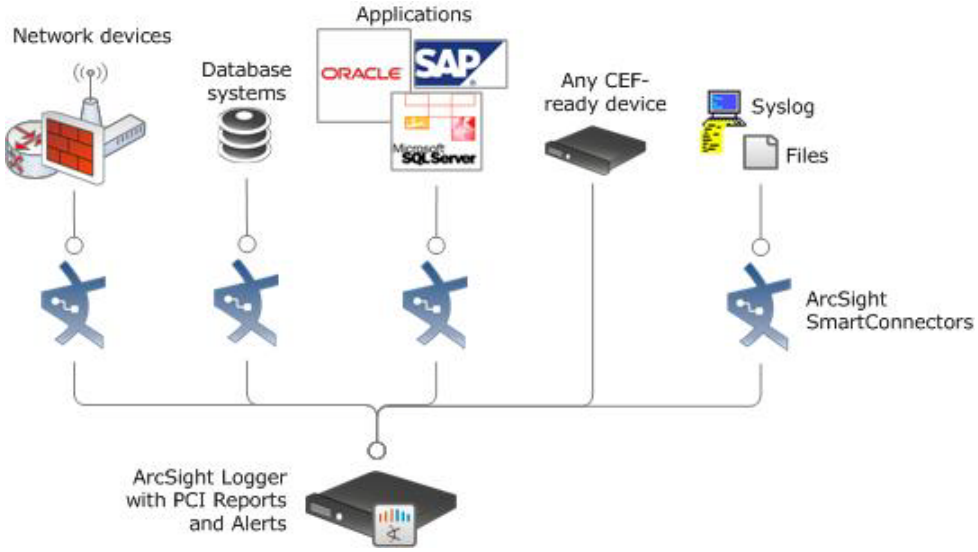


Figure 1-1 Logger CIP for PCI operates on events received from devices on the network in CEF format. PCI-relevant devices that are not already CEF-ready should be run through an ArcSight SmartConnector.

For more about CEF events and how they are used by Logger, see *Appendix A: Common Event Format* in the *ArcSight Logger™ Administrator's Guide*.

Identifying PCI-Related Events to Process

The ArcSight Logger can be configured to process PCI-related events, using one of the following methods:

- **Process all events received**—If all the devices in your environment are subject to PCI compliance, you can configure the ArcSight Logger so all received events are processed by the Logger CIP for PCI reports and alerts.
- **Limit the events processed**— If only some of your devices are subject to PCI compliance, configure the ArcSight Logger to only process the PCI-related events. Configuring the ArcSight Logger in this way, means only the PCI-related events are processed by the Logger CIP for PCI reports and alerts, so system performance should improve.

For more information and instructions, see “Process All Events or Limit the Events” on page 14.

PCI Resources

Logger CIP for PCI provides the following Payment Card Industry (PCI) resources:

- **PCI Alerts**—PCI alerts monitor incoming events in real time and notify PCI analysts when events of interest are detected.
- **PCI Reports**—Each PCI report displays the following information:
  - the results of the associated query displayed as a table and/or graph
  - a summary of the PCI requirement the report addresses
  - how the report supports the PCI requirement
  - the testing criteria an auditor can use to determine your organization’s compliance with the PCI requirement
- **PCI Executive Report**—This shows an executive overview of the vulnerabilities, database access, attacked hosts and virus events in the PCI environment.

For more information, see Chapter 3, Overview of PCI Resources, on page 25.

Chapter 2

Installation and Configuration

This section describes how to install and configure Logger CIP for PCI v3.0 to work in your environment.

"Before Upgrade or Install" on page 11

"Upgrade from Logger CIP for PCI v2.1" on page 12

"Install Logger CIP for PCI v3.0" on page 12

"Verify Logger CIP for PCI Content" on page 13

"Configure Logger CIP for PCI" on page 14

"Configure and Enable PCI Alerts" on page 22

"Running Logger CIP for PCI Reports" on page 23

Before Upgrade or Install

Before installing or upgrading to Logger CIP for PCI v3.0, review the following information.

Verify the Logger Version

Before installing Logger CIP for PCI v3.0, verify that you are running the correct version of ArcSight Logger, as indicated in the *ArcSight™ Compliance Insight Package PCI v3.0 Release Notes.*

1. Log into the Logger user interface. The Logger user interface is a web browser application. For detailed instructions and browser requirements, see the *Using the User Interface* topic of the ArcSight Logger™ Administrator's Guide.
2. In the upper-right corner, click the **About** option to display a window that indicates the Logger version.

Supported Devices

The device categories listed in Table A-1 on page 120 and Table A-2 on page 125 are capable of generating events to populate the listed reports and to trigger the listed alerts. For more information, see Appendix A, Supported PCI Devices, on page 119.

Connectors Needed for Non-CEF Devices

Logger CIP for PCI reports and alerts operate on events from the devices listed in Table A-1 on page 120 and Table A-2 on page 125. If these devices in your environment are not already CEF-enabled, it is strongly recommended that you apply an ArcSight

SmartConnector for these devices so that the Logger CIP for PCI reports will yield the most accurate results.

Use the supported devices Table A-1 on page 120 and Table A-2 on page 125 to determine which non-CEF enabled devices in your environment would benefit from the installation of an ArcSight SmartConnector to optimize results from Logger CIP for PCI. For more information, see the *Installing SmartConnectors to Send Events to Logger* topic in the *ArcSight Logger™ online Help* or the *ArcSight Logger™ Administrator's Guide*.

Upgrade from Logger CIP for PCI v2.1

If you are upgrading from Logger CIP for PCI v2.1, skip the installation section below and see the instructions in Appendix B, Upgrade from CIP for Logger PCI v2.1, on page 131.

After you complete the upgrade, see "Verify Logger CIP for PCI Content" on page 13.

Install Logger CIP for PCI v3.0

To install Logger CIP for PCI v3.0 on an ArcSight Logger, follow the appropriate procedure for your Logger type:

- "Install Logger CIP for PCI on the Logger Appliance" on page 12—Logger Appliance is the preconfigured hardware version of Logger.
- "Install Logger CIP for PCI on the Software Logger" on page 13—Software Logger is the downloadable version of Logger installed on your hardware.

Install Logger CIP for PCI on the Logger Appliance

This section describes how to install Logger CIP for PCI v3.0 on a Logger appliance.

If you are upgrading from Logger CIP for PCI v2.1, follow the steps provided in Appendix B, Upgrade from CIP for Logger PCI v2.1, on page 131.

To install Logger CIP for PCI v3.0 on a Logger Appliance:

1. Download the following Logger CIP for PCI ENC to the machine where you plan to log into the Logger user interface:

   `ArcSight-ComplianceInsightPackage-Logger-PCI.3.0.nnnn.0.enc`

   where `nnnn` is the four-digit build number specified in the *Release Notes ArcSight Compliance Insight Package PCI v3.0*.

2. Log into the Logger user interface. The Logger user interface is a web browser application. For detailed instructions and browser requirements, see the *Using the User Interface* topic of the *ArcSight Logger™ online Help* or *ArcSight Logger™ Administrator's Guide*.

3. From the Logger navigation bar, click **System Admin**.

4. From the left panel menu, select **License & Update**.

5. Click **Browse** to locate and open the ENC file you downloaded in Step 1.

6. Click **Upload Update**.

   A dialog warning that the update process may take some time is displayed.

7. Click **OK**.

A message indicating that the upgrade is progressing displays. Once the content of the ENC is installed, another message indicating that the upgrade succeeded displays. The ENC file installs PCI reports, parameters, queries and alerts.

8 Verify that the Logger CIP for PCI content is installed. See "Verify Logger CIP for PCI Content" on page 13.

If you decide to uninstall Logger CIP for PCI at a later date, see "Uninstall Logger CIP for PCI" on page 133.

Install Logger CIP for PCI on the Software Logger

This section describes how to install Logger CIP for PCI v3.0 on the software version of Logger.

If you are upgrading from Logger CIP for PCI v2.1, follow the steps provided in Appendix B, Upgrade from CIP for Logger PCI v2.1, on page 131.

To install Logger CIP for PCI v3.0 on the Software Logger:

1 On the system running the software Logger, log into the system using the same user that you used to install the software version of Logger.

2 Download the following Logger CIP for PCI BIN:

```
ArcSight-ComplianceInsightPackage-Logger-PCI.3.0.nnnn.0.bin
```

where `nnnn` is the four-digit build number specified in the *Release Notes ArcSight Compliance Insight Package PCI v3.0*.

3 Go to the directory that contains the BIN file.

4 Change the permissions of BIN file to be executable:

```
chmod +x
ArcSight-ComplianceInsightPackage-Logger-PCI.3.0.nnnn.0.bin
```

5 Run the installer:

```
./ArcSight-ComplianceInsightPackage-Logger-PCI.3.0.nnnn.0.bin
```

6 Follow the instructions provided by the installer. When prompted to choose an installation folder, enter the same directory you specified when you installed the software Logger. For example, if when installing the software Logger you specified the `/opt/logger` directory, specify `/opt/logger` as the installation folder.

The BIN file installs the PCI reports, parameters, queries and alerts.

7 Verify that the Logger CIP for PCI content is installed. See "Verify Logger CIP for PCI Content" on page 13.

If you decide to uninstall Logger CIP for PCI at a later date, see "Uninstall Logger CIP for PCI" on page 133.

Verify Logger CIP for PCI Content

This section provides steps to verify that the Logger CIP for PCI content is installed and applies to both the Logger appliance and software Logger.

To verify that the Logger CIP for PCI reports, parameters, queries and alerts have been installed:

1. To view the installed alerts, select **Configuration**. In the left panel menu, select **Alerts**. The set of PCI alerts are displayed.
2. To view the installed reports, select **Reports**. In the left panel menu:
   - for Logger v5.1, select **Solution Reports/PCI**
   - for Logger v5.2, select **Report Navigation/Report Explorer/PCI**

   The Logger CIP for PCI reports are displayed. For a list of the alerts and reports, see Table 4-1 on page 34.

Configure Logger CIP for PCI

Configure the Logger CIP for PCI reports and alerts:

- "Process All Events or Limit the Events" on page 14—Determine the best event processing model for your environment and configure the Logger CIP for PCI alerts and reports to support that model.
- "Configure Alerts with Site-Specific Data" on page 21—Several Logger CIP for PCI alerts refer to site-specific details, such as admin user account names and default ports and protocols, which should be configured with details specific to your environment for more accurate results.
- "Configure Reports with Site-Specific Data" on page 21—Several Logger CIP for PCI reports refer to site-specific details, such as admin user account names and default ports and protocols, which should be configured with details specific to your environment for more accurate results.

For basic instructions about enabling the Logger CIP for PCI alerts, see "Configure and Enable PCI Alerts" on page 22.

For instructions about running the Logger CIP for PCI reports, see "Running Logger CIP for PCI Reports" on page 23 on page 25.

Process All Events or Limit the Events

For your environment, choose the appropriate method for processing events received by the ArcSight Logger:

- "Process All Events" on page 14—If all the devices in your environment are subject to PCI compliance, configure the ArcSight Logger so all events it receives are processed by the Logger CIP for PCI reports and alerts.
- "Limit the Events Processed" on page 16— If only some of your devices are subject to PCI compliance, configure Logger CIP for PCI reports and alerts on the ArcSight Logger to only process the PCI-related events. This should improve system performance.

Select one method and follow the instructions provided in the appropriate section.

Process All Events

Follow the instructions provided in this section to configure the Logger CIP for PCI resources so the ArcSight Logger processes all the events it receives:

- **PCI Reports**—By default, the Logger CIP for PCI reports are ready to process all events received by the ArcSight Logger and no configuration is required.

- **PCI Alerts**— Some configuration of the Logger CIP for PCI alerts is required in order for the alerts to process all the events received by the ArcSight Logger. Follow the instructions in the following procedure to configure the Logger CIP for PCI alerts.

Configure Alerts to Process All Events

By default, all PCI alerts contain the following placeholder condition (Query Term):

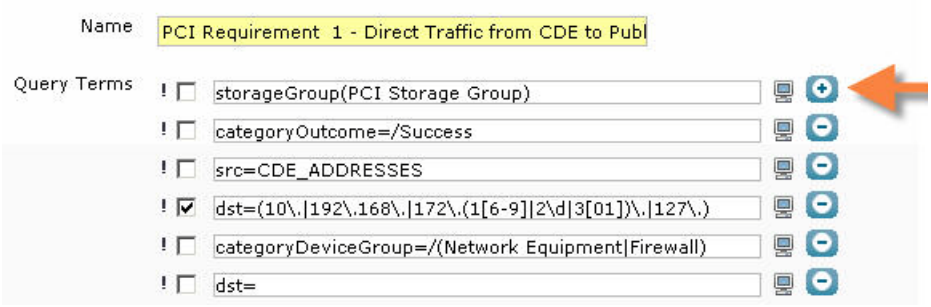
```
storageGroup(PCI Storage Group)
```

If you want all the enabled PCI alerts to process all the events received by the ArcSight Logger, edit each enabled PCI alert and remove this Query Term (condition) as described in the following procedure.

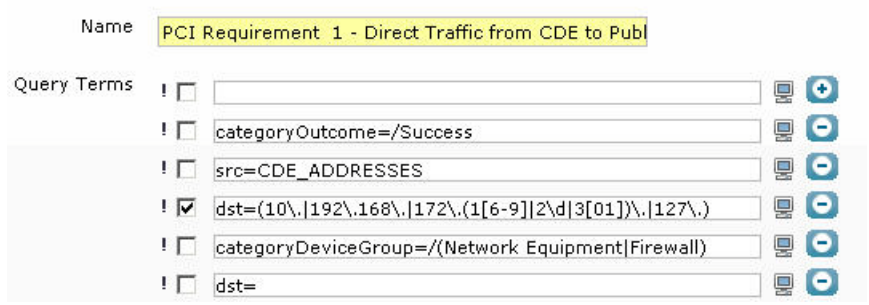
A maximum of five alerts can be enabled on Logger at one time. You do not need to configure all the PCI alerts. You can configure only those alerts that you plan on enabling. In order to enable an additional alert, you may need to disable another alert. For more information including a list of the five alerts that are enabled by default, see "Configure and Enable PCI Alerts" on page 22.

To edit and remove the placeholder storageGroup (PCI Storage Group) Query Term from an alert:

1. Select **Configuration**.
2. From the left panel menu, select **Alerts**.
3. To edit the alert, click the PCI alert in the Name column.
4. Find the placeholder Query Term with the text: `storageGroup(PCI Storage Group)`, as shown in the following figure.



5. Remove all the text in the Query Term field, as shown in the following figure.



6. Click **Save**.
7. For each alert you plan on enabling, repeat Step 3 through Step 6.
8. Skip to "Configure Alerts with Site-Specific Data" on page 21.

Limit the Events Processed

If only some of your devices are subject to PCI compliance, you may want to limit the events processed by the Logger CIP for PCI reports and alerts for the following benefits:

- System performance on the ArcSight Logger should improve
- More accurate and PCI-relevant information reported by the Logger CIP for PCI reports and alerts

You can limit the events processed by PCI reports and alerts, using one or more of the following strategies:

- Use a PCI-related *Device Group* to limit the events processed by the PCI reports and alerts. With this strategy, you create a PCI-specific Device Group and only process events from devices in the Device Group.
- Use a PCI-related *Storage Group* to limit the events processed by the PCI reports and alerts. Using a designated Storage Group to limit events is only appropriate if an additional Storage Group (besides the Default Storage and Internal Event Storage Groups) was created during the ArcSight Logger initialization process. Once the ArcSight Logger has been initialized, no additional Storage Groups can be allocated. For details, see the *Storage Groups* topic in the ArcSight Logger *online Help* or the ArcSight Logger *Administrator's Guide.* Using this method to constrain the alerts and reports yields the best performance results.
- Only process events from specified devices

Which strategy you choose depends on how your environment is set up, and how you want to organize your PCI compliance program.These limiting strategies can be combined.

Reducing the amount of data a resource has to process translates to better performance.

If only a small subset of the overall data feeding into ArcSight Logger is subject to PCI compliance, using a different Storage Group to store events from PCI-related devices yields the best performance results.

To limit the events processed by the Logger CIP for PCI reports and alerts, implement one or more of these limiting strategies by following the configuration steps provided in the following sections:

- "Step 1: Classify PCI-Related Devices in PCI Device Group" on page 17—This step is only required if you plan on using a Device Group to limit the events processed reports and alerts. Skip this step if you do not plan on using a Device Group to limit the events processed by PCI reports and alerts.
- "Step 2: Create a PCI Filter to Limit the Events Processed" on page 17—In this step, you create a filter that constrains the events processed by the alerts and reports.
- "Step 3: Limit Events Processed by Alerts" on page 18—In this step, you limit the events that an alert processes by either:
  - Applying the filter created in "Step 2: Create a PCI Filter to Limit the Events Processed" on page 17 to the alert
  - Adding a condition to directly to the alert
- "Step 4: Limit Events Processed by Reports" on page 20—In this step, you apply the filter to the entire PCI report category or specify at report run time how to limit the events processed by a report.

Step 1: Classify PCI-Related Devices in PCI Device Group

If you plan on using a Device Group to limit the events processed by reports and alerts, create the PCI Device Group and classify the PCI-related devices into it as described in following procedure. After the PCI-Related Devices are categorized, you can use the Device Group to focus alerts and reports. For example, you could create a filter that only returns events from devices listed in the PCI Device Group filter and then configure alerts and reports to use that filter to limit the events processed.

To classify PCI-related devices in PCI Device Group:

1. Select **Configuration**.
2. From the left panel menu, click **Devices**.
3. Click the **Device Groups** tab.
4. Click **Add**.
5. In the *Name* field, enter a name for the new device group, such as `PCI`.
6. In the *Devices* field, click to select devices from the list. To add additional devices to the selection, press and hold the **Ctrl** key when selecting more devices.
7. Click **Save** to create the new Device Group.

For more about device groups, see the *Device Groups* topic in the *ArcSight Logger™ online Help* or *ArcSight Logger™ Administrator's Guide*.

Step 2: Create a PCI Filter to Limit the Events Processed

Create a filter that identifies the PCI-related events for your environment. The filter can be used to limit the events processed by PCI alerts and reports. A filter can limit events using one or more of the following strategies:

- **Limit using a PCI-related Device Group**—Only those events from devices listed in the Device Group are processed.
- **Limit using a PCI-related Storage Group**—Only those events stored in the specified Storage Group are processed.
- **Limit by specific devices**—Only events from specific devices are processed.

For example, you could create any of the following filters:

- A filter called `PCI Device Group Filter` which returns events from devices categorized as PCI devices.
- A filter called `PCI Storage Group Filter` which returns events that are stored in a designated Storage Group.
- A filter called `PCI Devices Filter` which returns events from specified devices.
- A filter called `PCI Storage Group and Devices Filter` which returns events that are stored in a designated Storage Group (such as a PCI Storage Group) or from a set of specific devices.

To create a filter:

1. Select **Configuration**.
2. From the left panel menu, select **Filters** and click **Add**.

3 In the *Add Filter* page, enter the following information:

Field	Description
Name	Enter a name for the filter that identifies it with Logger CIP for PCI and identifies the purpose of the filter, such as `PCI Device Group Filter` or `PCI Storage Group Filter` or `PCI Devices Filter`.
Type	From the drop-down menu, select **Search Group**. A filter of type Search Group can be used by both alerts and reports to constrain events.

4 In the Query field, construct a query, using one of the following options:

- In the Query field, directly enter a regular expression, for example: `storageGroup(Default Storage Group)|deviceGroup(PCIDeviceGroup)`
- Use the *Constrain search by* dialog—Select the  icon. In the *Constrain search by* dialog, select from one of the following options:
  - Focus alerts to only process events from devices listed in the Device Group—Click **Device Groups**. Select a Device Group from the list and click **Submit.**
  - Focus alerts to only process events saved in a designated Storage Group—Click **Storage Groups**. Select a Storage Group from the list and click **Submit**.
  - Focus the alerts to only process events from individual devices subject to PCI compliance—Select devices from the lists and click **Submit**. To select more than one device, press and hold the **Ctrl** key while selecting more devices.

5 Click **Save**.

The filter created in this step can be used to limit the events processed by both reports and alerts as described in "Step 3: Limit Events Processed by Alerts" on page 18 and "Step 4: Limit Events Processed by Reports" on page 20.

Step 3: Limit Events Processed by Alerts

To constrain the events that an alert processes, configure the alert using one of the following methods:

- "To add a filter to the alert:" on page 18
- "To add a Query Term to the alert:" on page 19

A maximum of five alerts can be enabled on Logger at one time. You do not need to configure all the PCI alerts. You can configure only those alerts that you plan on enabling. In order to enable an additional alert, you may need to disable another alert. For more information including a list of the five alerts that are enabled by default, see "Configure and Enable PCI Alerts" on page 22.

To add a filter to the alert:

1 Select **Configuration**.

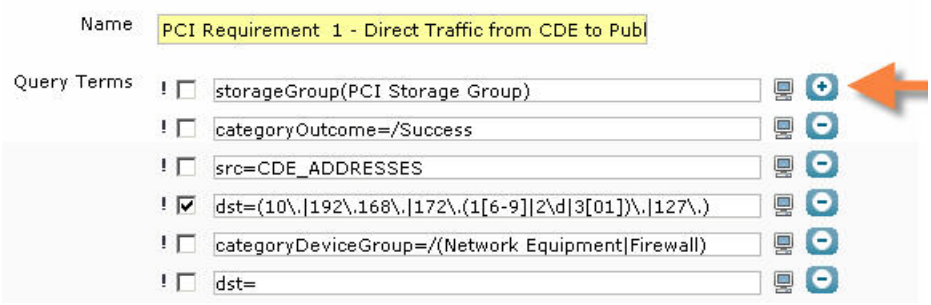
2 From the left panel menu, select **Alerts**.

3 To edit the alert, click the PCI alert in the Name column.

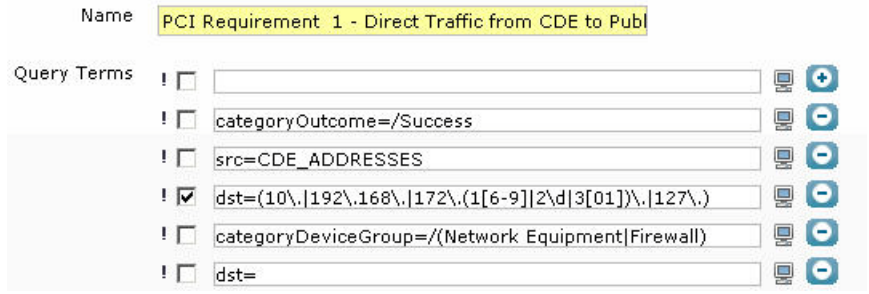
4 In the Filters field, select the filter you created in "Step 2: Create a PCI Filter to Limit the Events Processed" on page 17 that limits the events processed by the alert.

5 Locate and remove the placeholder `storageGroup(PCI Storage Group)` condition:

a Find the Query Terms field with the text: `storageGroup(PCI Storage Group)`, as shown in the following figure.



b Remove all the text in the Query Term field, as shown in the following figure.



6 Click **Save**.

7 For each alert you plan on enabling, repeat Step 3 through Step 6.

To add a Query Term to the alert:

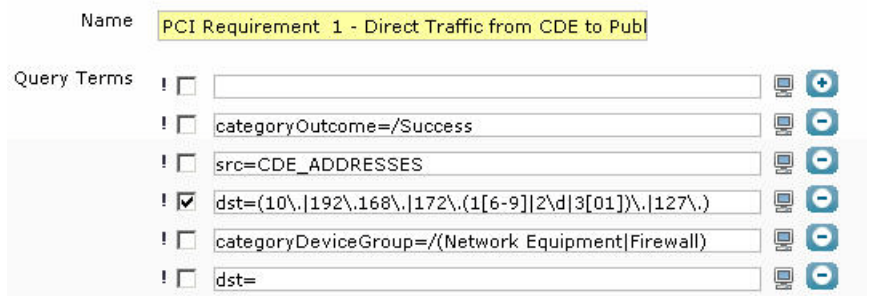
1 Select **Configuration**.

2 From the left panel menu, select **Alerts**.

3 To edit the alert, click the PCI alert in the Name column.

4 Locate the placeholder `storageGroup(PCI Storage Group)` condition. Find the Query Terms field with the text: `storageGroup(PCI Storage Group)` as shown in the preceding figure.

5 Remove all the text in the Query Term field, as shown in the following figure.



6 In the same Query Terms field, add a condition to the alert, using one of the following methods:

- In the Query Terms field, directly enter a regular expression, for example:
  `storageGroup(Default Storage Group)|deviceGroup(PCIDeviceGroup)`
- Use the *Constrain search by* dialog—Select the  icon. In the *Constrain search by* dialog, select from one of the following options:
  - Focus alerts to only process events from devices listed in the Device Group—Click **Device Groups**. Select a Device Group from the list and click **Submit**.
  - Focus alerts to only process events saved in a designated Storage Group—Click **Storage Groups**. Select a Storage Group from the list and click **Submit**.
  - Focus the alerts to only process events from individual devices subject to PCI compliance—Select devices from the list and click **Submit**. To select more than one device, press and hold the **Ctrl** key while selecting more devices.

7 Click **Save**.

8 For each alert you plan on enabling, repeat Step 3 on page 19 through Step 7.

Step 4: Limit Events Processed by Reports

You can limit events processed by the PCI reports, using the following methods:

- "Limit the Events Processed by all the Reports in the PCI Report Category Using a Filter" on page 20
- "Specify at Report Run Time How to Limit Events Processed by a Report" on page 20

Limit the Events Processed by all the Reports in the PCI Report Category Using a Filter

A Report Category (Search Group) filter can be applied to a whole report category, in this case, the PCI report group.

Assign the filter you created in "Step 2: Create a PCI Filter to Limit the Events Processed" on page 17 to the PCI report group:

1 Select the **Reports** tab.

2 In the left menu pane, click **Administration > Report Category Filters**.

3 In the drop-down menu associated with the PCI reports group, select the filter you created in "Step 2: Create a PCI Filter to Limit the Events Processed" on page 17 and click **Save**.

For more information about report category filters and scheduling reports, the *ArcSight Logger™ online Help* or the *ArcSight Logger™ Administrator's Guide.*

Specify at Report Run Time How to Limit Events Processed by a Report

To limit events at report run time, run the report using the Quick Run () option. In the Select tab, select one or more Devices, Device Groups, or Storage groups. To select more than one device or group, press and hold the **Ctrl** key while selecting more devices or groups.

If you apply a Report Category (Search Group) filter to the PCI Report Category, you do not limit the events at report run time.

Configure Alerts with Site-Specific Data

Many of the Logger CIP for PCI alerts contain site-specific data, such as administrator account names and default ports and protocols, which should be configured with details specific to your environment.

To configure an alert with site specific data:

1. Select the **Configuration** tab.
2. From the left panel menu, select **Alerts**.
3. Click on a PCI alert.
4. Find the Query Term with the site specific data and change it to reflect your site.
5. Click **Save**.

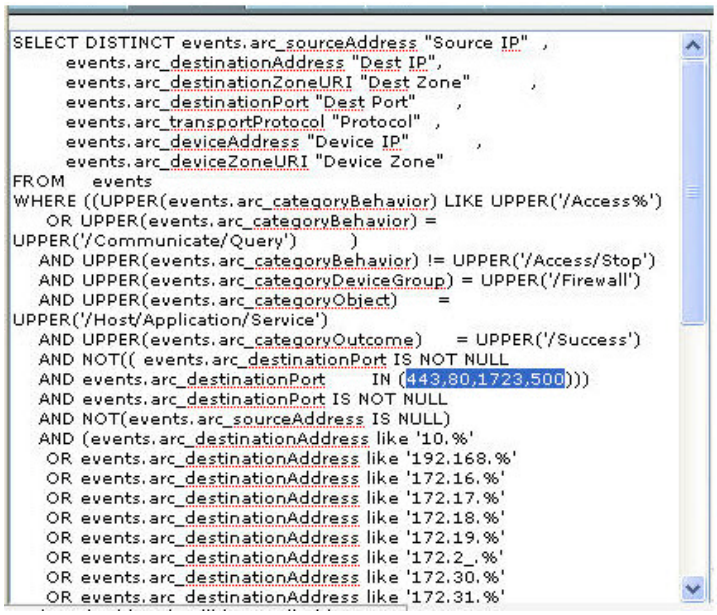
Configure Reports with Site-Specific Data

Many of the Logger CIP for PCI reports contain site-specific data, such as administrator account names and default ports and protocols, which should be configured with details specific to your environment. Typically, you would configure the report query or parameters. For configuration information about a particular report, see Chapter 4, PCI Resources, on page 33.

To configure a query with site specific data:

The following example shows how to edit the query for the report *Requirement 1-External to PCI Systems on Disallowed Ports*:

1. Select the **Reports** tab, navigate to the report query, and open the query.
2. In the SQL area, click Edit. This opens the SQL editor in a separate window.
3. Find the line that specifies the default disallowed ports (`AND events.arc_destinationPort IN (443,80,1723,500)))`) and add or remove ports from the list to match the disallowed ports for your site. The disallowed reports included by default in the query are highlighted by the dark band in the example below.



```
SELECT DISTINCT events.arc_sourceAddress "Source IP" ,
      events.arc_destinationAddress "Dest IP",
      events.arc_destinationZoneURI "Dest Zone"      ,
      events.arc_destinationPort "Dest Port"     ,
      events.arc_transportProtocol "Protocol" ,
      events.arc_deviceAddress "Device IP"       ,
      events.arc_deviceZoneURI "Device Zone"
FROM    events
WHERE ((UPPER(events.arc_categoryBehavior) LIKE UPPER('/Access%')
    OR UPPER(events.arc_categoryBehavior) =
UPPER('/Communicate/Query')       )
   AND UPPER(events.arc_categoryBehavior) != UPPER('/Access/Stop')
   AND UPPER(events.arc_categoryDeviceGroup) = UPPER('/Firewall')
   AND UPPER(events.arc_categoryObject)     =
UPPER('/Host/Application/Service')
   AND UPPER(events.arc_categoryOutcome)    = UPPER('/Success')
   AND NOT(( events.arc_destinationPort IS NOT NULL
   AND events.arc_destinationPort      IN (443,80,1723,500)))
   AND events.arc_destinationPort IS NOT NULL
   AND NOT(events.arc_sourceAddress IS NULL)
   AND (events.arc_destinationAddress like '10.%'
    OR events.arc_destinationAddress like '192.168.%'
    OR events.arc_destinationAddress like '172.16.%'
    OR events.arc_destinationAddress like '172.17.%'
    OR events.arc_destinationAddress like '172.18.%'
    OR events.arc_destinationAddress like '172.19.%'
    OR events.arc_destinationAddress like '172.2_.%'
    OR events.arc_destinationAddress like '172.30.%'
    OR events.arc_destinationAddress like '172.31.%'
```

4 Click **OK** to exit the SQL editor. Click **Save** in the Query Object List page.

Configure and Enable PCI Alerts

The following procedure provides an overview for configuring and enabling PCI alerts. For more information, see the *Alerts* topic in the *ArcSight Logger™ online Help* or the *ArcSight Logger™ Administrator's Guide.*

To configure and enable an alert:

1 If required, create the alert destinations:

   a Determine what action(s) the alert will take when triggered:

   - Send an e-mail notification to one or more e-mail addresses
   - Log a notification message to a Syslog destination
   - Send an SNMP TRAP to an SNMP destination

   b If the alert is sending information to a syslog or SNMP destination, create the destination before configuring the alert. For more information, see the *Alerts* topic in the *ArcSight Logger™ online Help* or the *ArcSight Logger™ Administrator's Guide.*

2 Select **Configuration**.

3 From the left panel menu, select **Alerts**.

4 To edit an alert, in the Name field click a PCI alert.

5 Configure the conditions in an alert, using one of the following methods:

   - Limit the events that are processed by alerts. For more information, see "Limit the Events Processed" on page 16.
   - Enable the alert to process all events received by the ArcSight Logger. For instructions, see "Process All Events" on page 14.

6 If required, configure the alert with site specific data. For more information, see "Configure Alerts with Site-Specific Data" on page 21.

7 Customize the Match Count and Thresholds fields. For more information, see "Match Count and Threshold (Sec) Fields" on page 26.

8 If you want the alert to send an e-mail notification when triggered, in the Email Address(es) field specify a set of e-mail addresses separated by semi-colons(;).

9 If you want the alert to send a notification to an SNMP destination, select the SNMP Destination (created in b on page 22) from the pull-down menu.

10 If you want the alert to send a notification to an Syslog destination, select the SNMP Destination (created in b on page 22) from the pull-down menu.

11 Click **Save**.

12 Enable the alert:

Click the **Disabled** ( ) icon.

Tip

A maximum of five alerts can be enabled at one time. In order to enable an additional alert, you may need to disable another alert. By default, the following set of PCI alerts are enabled:

- "PCI Requirement 10 - Device Clock Synchronization Problems Alert" on page 70
- "PCI Requirement 10 - Excessive Failed Administrative Actions Alert" on page 71
- "PCI Requirement 10 - Excessive Failed Administrative Logins Alert" on page 72
- "PCI Requirement 10 - Excessive Successful Administrative Actions Alert" on page 76
- "PCI Requirement 10 - Excessive Successful Administrative Logins Alert" on page 76

Running Logger CIP for PCI Reports

For information about running, formatting, publishing, and scheduling reports in Logger, see the *ArcSight Logger™ online Help* or the *ArcSight Logger™ Administrator's Guide.*

Chapter 3

Overview of PCI Resources

Logger CIP for PCI contains the following Payment Card Industry (PCI) resources:

"PCI Alerts" on page 25

"PCI Reports" on page 26

"PCI Queries" on page 31

This chapter contains an overview of the different Logger PCI resources. For a detailed listing of all the Logger PCI resources including descriptions and configuration information, see Chapter 4, PCI Resources, on page 33.

PCI Alerts

PCI alerts monitor incoming events and notify PCI analysts when events of interest are detected. Once a PCI alert has been customized and enabled, the alert is ready to be triggered. When PCI base events trigger an alert, the following notification actions can occur:

- Send an e-mail notification to one or more e-mail addresses
- Log a notification message to a Syslog host
- Send an SNMP TRAP to an SNMP destination

When the alert is triggered, an internal alert event is generated. You can search and view these internal alert events in real-time from the **Analyze** tab of the Console. These internal alert events stored in the Internal Storage Group. For more information, see the *Alerts* topic in the *ArcSight Logger™ online Help* or the *ArcSight Logger™ Administrator's Guide* and "Configure and Enable PCI Alerts" on page 22.

Some PCI alerts are enabled by default and the rest are disabled. You can view the list of PCI alerts by selecting the **Configuration** tab and then **Alerts** in the left menu panel. To enable an alert: Click the **Disabled** ( ) icon.

By default, the following set of PCI Alerts are enabled:

- "PCI Requirement 10 - Device Clock Synchronization Problems Alert" on page 70
- "PCI Requirement 10 - Excessive Failed Administrative Actions Alert" on page 71
- "PCI Requirement 10 - Excessive Failed Administrative Logins Alert" on page 72

- “PCI Requirement 10 - Excessive Successful Administrative Actions Alert” on page 76
- “PCI Requirement 10 - Excessive Successful Administrative Logins Alert” on page 76

For detailed instructions on configuring an alert, see the *Alerts* topic in the *ArcSight Logger™ online Help* or the *ArcSight Logger™ Administrator's Guide*.In addition, the following topics are provided to assist you in configuring alerts:

- “Match Count and Threshold (Sec) Fields” on page 26
- “Customizing PCI Alerts with Regular Expressions” on page 26

Match Count and Threshold (Sec) Fields

The **Match Count** and **Threshold (sec)** fields determine when an enabled alert is triggered. An alert is triggered when the specified number of matches is seen within the specified time threshold. You can customize these settings. For more information, see the *Alerts* topic in the *ArcSight Logger™ online Help* or the *ArcSight Logger™ Administrator's Guide.*

Customizing PCI Alerts with Regular Expressions

For some PCI alerts, you may need to edit and customize the conditions specified in the Query Terms fields before enabling the alert to run. For some PCI alerts, you may need to specify a regular expression in a Query Terms field. For example, the PCI Requirement 1 - Direct Traffic from CDE to Public Addresses Alert requires a change to the following **Query Terms** field:

```
dst=CDE_ADDRESSES
```

Replace the `CDE_ADDRESSES` string with a regular expression that specifies a range of IP addresses for machines in the Cardholder Data Environment (CDE). For example, the following regular expression could be specified in the **Query Terms** field:

```
dst=(172\.168\.(1[6-9]|2[0-9]|3[0-1])\.)
```

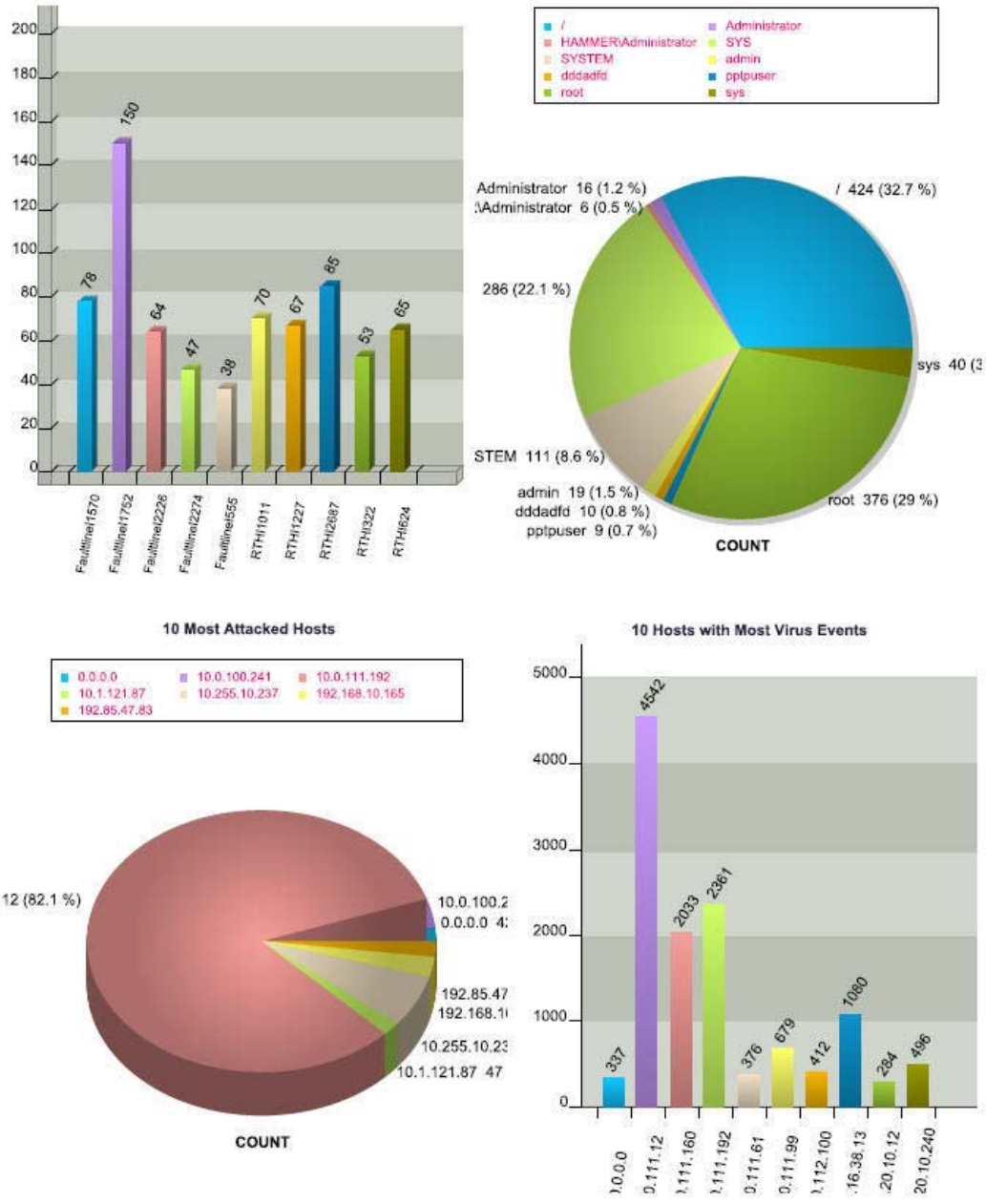
This regular expression matches addresses in the range of 172.168.16-31.

PCI Reports

Logger CIP for PCI contains one PCI Executive report and a set of PCI Standard reports.

PCI Executive Report

The *General - Executive Report* shows an executive overview of the vulnerabilities, database access, attacked hosts and virus events in the PCI environment.



The *General - Executive Report* invokes the following queries:

- Top 10 Vulnerabilities Query
- Top 10 Users Accessing DB Query
- 10 Most Attacked Hosts Query

- 10 Hosts with Most Virus Events Query

You cannot customize these queries or view these queries from ArcSight Logger. The following SQL code listings of these queries are provided for your reference.

In order for the *General - Executive Report* to be populated with data during report run time, the following types of events must be received by the ArcSight Logger:

- anti-virus events
- intrusion detection system (IDS) events
- vulnerability scanner events
- database events

Top 10 Vulnerabilities Query

```
SELECT events.arc_deviceEventClassId "Vulnerability ID",
COUNT(events.arc_deviceEventClassId) "Count"
FROM events
WHERE ((UPPER(events.arc_categoryTechnique) LIKE
UPPER('/Scan/Vulnerability%')
       OR UPPER(events.arc_categoryTechnique) LIKE
UPPER('/scanner/device/vulnerability%'))
       AND UPPER(events.arc_categoryBehavior) LIKE
UPPER('/Found/Vulnerable%')
       AND UPPER(events.arc_categoryDeviceGroup) LIKE UPPER('/Assessment
Tools%')
       AND UPPER(events.arc_categoryOutcome) = UPPER('/Success')
       AND events.arc_deviceEventClassId IS NOT NULL)
GROUP BY events.arc_deviceEventClassId
ORDER BY COUNT(events.arc_deviceEventClassId) DESC
LIMIT 10
```

Top 10 Users Accessing DB Query

```
SELECT events.arc_destinationUserName "Dest User",
COUNT(*) "Count"
FROM    events
WHERE ((UPPER(events.arc_categoryBehavior) = UPPER('/Authentication/Verify')
       OR UPPER(events.arc_categoryBehavior) = UPPER('/Access/Start'))
       AND UPPER(events.arc_categoryDeviceGroup) = UPPER('/Application')
       AND UPPER(events.arc_categoryObject) =
UPPER('/Host/Application/Database')
       AND UPPER(events.arc_categoryOutcome) = UPPER('/Success')
       AND events.arc_destinationUserName IS NOT NULL)
GROUP BY events.arc_destinationUserName
ORDER BY COUNT(*) DESC
LIMIT 10
```

10 Most Attacked Hosts Query

```
SELECT events.arc_destinationAddress "Dest IP",
        Count(*) "Count"
FROM events
WHERE ((UPPER(events.arc_categorySignificance) = UPPER('/Hostile')
       OR UPPER(events.arc_categorySignificance) LIKE UPPER('/Compromise%')
       OR UPPER(events.arc_categorySignificance) LIKE UPPER('/Suspicious%'))
       AND events.arc_destinationaddress IS NOT NULL)
GROUP BY events.arc_destinationAddress,
       events.arc_destinationHostName,
```

```
       events.arc_destinationZoneURI
ORDER BY Count(*) DESC
LIMIT 10
```

10 Hosts with Most Virus Events Query

```
SELECT events.arc_destinationAddress "Dest IP",
        COUNT(*) "Count"
FROM events
WHERE ((UPPER(events.arc_categoryObject)=UPPER('/Host/Infection/Virus')
       AND UPPER(events.arc_categoryBehavior) LIKE UPPER('/Found%')
       AND UPPER(events.arc_categoryDeviceGroup)=UPPER('/IDS/Host/Antivirus')
       AND UPPER(events.arc_categoryOutcome) =UPPER('/Success')
       AND UPPER(events.arc_categorySignificance)= UPPER('/Compromise'))
       OR (UPPER(events.arc_categoryObject) = UPPER('/Host/Resource/File')
       AND (UPPER(events.arc_categoryBehavior) = UPPER('/Modify/Attribute')
       OR UPPER(events.arc_categoryBehavior) = UPPER('/Modify/Content')
       OR UPPER(events.arc_categoryBehavior) = UPPER('/Delete'))
       AND UPPER(events.arc_categoryDeviceGroup) =
UPPER('/IDS/Host/Antivirus')
       AND UPPER(events.arc_categorySignificance) =
UPPER('/Informational/Warning'))
       OR (UPPER(events.arc_categoryObject)= UPPER('/Vector/Virus')
       AND UPPER(events.arc_categoryBehavior) = UPPER('/Communicate/Query')
       AND UPPER(events.arc_categoryDeviceGroup) = UPPER('/IDS/Network')
       AND UPPER(events.arc_categorySignificance) = UPPER('/Compromise')))
GROUP BY events.arc_destinationAddress,
       events.arc_destinationHostName,
       events.arc_destinationZoneURI
ORDER BY COUNT(*) DESC LIMIT 10
```

PCI Standard Reports

Each standard Logger PCI report has an associated SQL query that queries the database for the specified conditions. Some of the queries contain default values, which you are encouraged to configure to match conditions relevant to your environment. Any recommended query configuration is listed as part of the report description provided in Chapter 4, PCI Resources, on page 33. In addition, the reports that recommend site-specific configuration are noted in “Configure Reports with Site-Specific Data” on page 21. For more information on configuring a query see the *Modifying a Query Object* topic in the *ArcSight Logger™ online Help* or the *ArcSight Logger™ Administrator’s Guide.*

Anatomy of a Standard Report

The Logger PCI standard reports are optimized to help companies and PCI auditors determine the status of your systems for each PCI requirement addressed by the solution report.

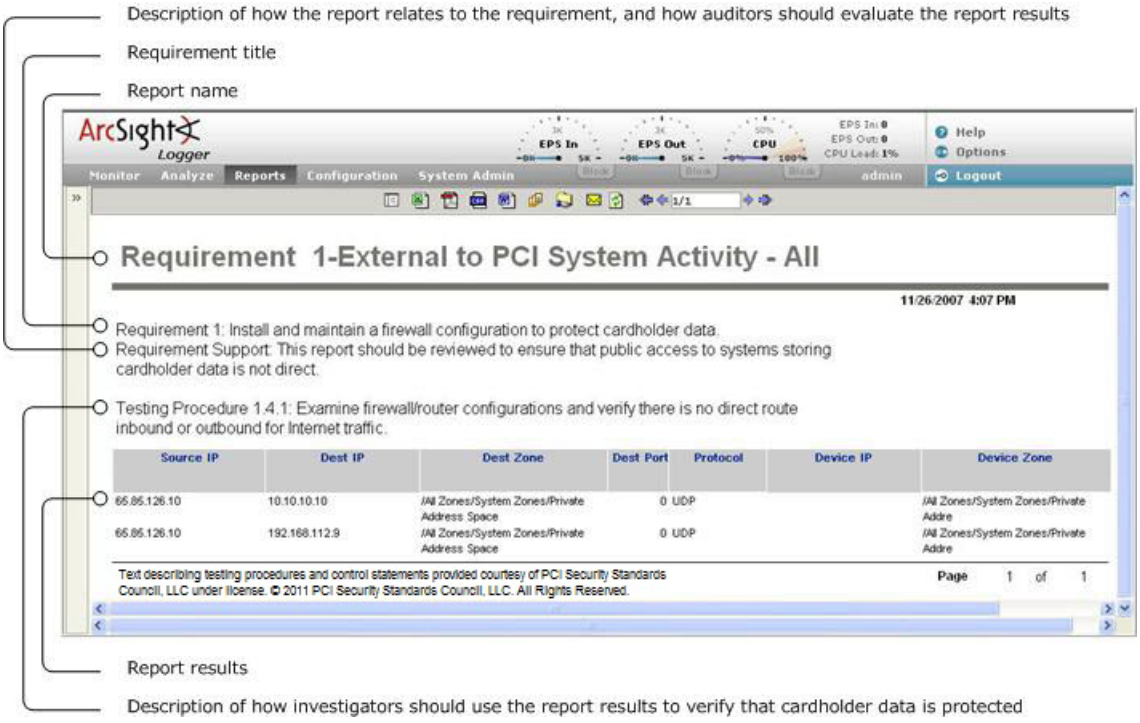


Figure 3-1 Standard Report Anatomy

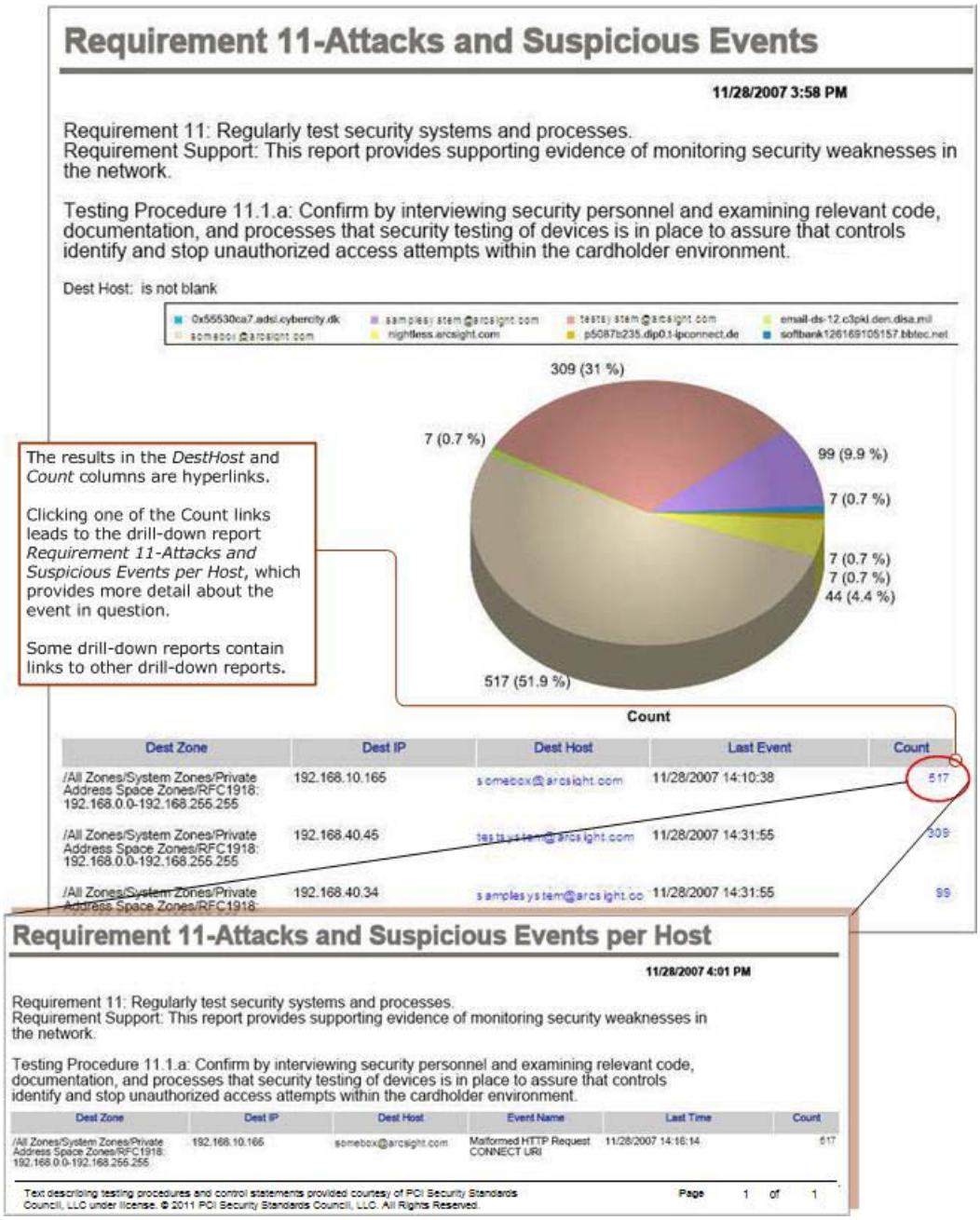
In addition to detailed report results, each Logger PCI report contains a summary of the PCI requirement it addresses, how the report supports the requirement, and testing criteria an auditor can use to determine your organization's compliance with the requirement.

Drill-Down Reports

Logger CIP for PCI has several reports that contain hyperlinks to *drill-down reports* (the report output format must be HTML). Drill-down reports provide additional information to help you pinpoint events that can jeopardize the security of cardholder data. Some drill-down reports link to other drill-down reports, as shown in the sample report below, to provide more than one perspective of an event.

During an investigation, it can be useful to run a drill-down report directly, rather than from a hyperlink in another report. To run a drill-down report directly, you pass the drill-down field name from the calling report as a parameter. For example, to run the *Requirement 5 - Detailed Anti-Virus Report per Host* report, you would specify the Destination Host Name as a parameter.

For a complete list of the reports that contain active hyperlinks, and the drill-down reports they invoke, see Appendix C, Drill-Down Report Reference, on page 135.



PCI Queries

The SQL queries that support the PCI reports have similar names as the reports themselves. For example, the *Requirement 1-External to PCI System Activity - All* report invokes the *PCI 1-External To PCI Systems* query. The queries can be viewed from the *Reports* tab by selecting **Queries** from the left panel menu.

For detailed instructions on viewing and editing queries, see the *Setting up Queries* topic in the *ArcSight Logger™ online Help* or the *ArcSight Logger™ Administrator's Guide.*

For details about which queries are recommended for configuration with site-specific data, see the report descriptions provided in Chapter 4, PCI Resources, on page 33. In addition, see “Configure Reports with Site-Specific Data” on page 21.

Chapter 4

PCI Resources

This section lists all the Logger PCI resources (alerts and reports) by PCI Requirement:

"Requirement 1: Firewall Configuration" on page 40
"Requirement 2: Default Security Parameters" on page 45
"Requirement 3: Protect Stored Data" on page 47
"Requirement 4: Encrypt Transmissions" on page 50
"Requirement 5: Anti-Virus" on page 53
"Requirement 6: System Applications" on page 58
"Requirement 7: Business Need-To-Know" on page 62
"Requirement 8: Unique User ID" on page 63
"Requirement 9: Physical Access" on page 65
"Requirement 10: Track and Monitor Data Access" on page 68
"Requirement 11: Test Systems and Networks" on page 99
"Requirement 12: Maintain an Information Security Policy" on page 106
"PA-DSS Requirement 4: Log Payment Application Activity" on page 109

For an overview of PCI reports, queries, and alerts, see "Overview of PCI Resources" on page 25.

In each Requirement section, the alerts and reports provided to support the PCI Requirement are listed.

- **Alerts**—For each alert the following information is provided:
  - The action that causes the alert to trigger
  - If the alert is enabled by default
  - The default **Match Count** setting—For more information, see "Match Count and Threshold (Sec) Fields" on page 26.
  - The default **Threshold (Sec)** setting—For more information, see "Match Count and Threshold (Sec) Fields" on page 26.
- **Reports**—For each standard report the following information is provided:
  - The top-level PCI requirement the report addresses.

- A brief description of how the report supports the requirement.
- A brief description of how an auditor can read the report to understand how the data returned demonstrates the status of your PCI compliance.
- Any recommended configuration is described.

In addition to the standard reports provided for the PCI requirements, one overview PCI Executive report is available. For more information, see "PCI Executive Report" on page 27.

Table 4-1 summarizes all the supplied PCI alerts and reports.

Table 4-1 PCI Alerts and Reports

PCI Requirement	Associated PCI Alerts and Reports
Requirement 1: Firewall Configuration	**PCI Alerts** • "PCI Requirement 1 - Direct Traffic from CDE to Public Addresses Alert" on page 41 • "PCI Requirement 1 - Direct Traffic from Public Addresses to CDE Alert" on page 41 • "PCI Requirement 1 - Firewall Configuration Changes Alert" on page 42 • "PCI Requirement 1 - Network Equipment Configuration Changes Alert" on page 42 • "PCI Requirement 1 - VPN Configuration Changes Alert" on page 42 **PCI Reports** • "Requirement 1-External to PCI System Activity - All Report" on page 43 • "Requirement 1-External to PCI Systems on Disallowed Ports Report" on page 43 • "Requirement 1-Firewall Configuration Changes Report" on page 43 • "Requirement 1-Network Equipment Configuration Changes Report" on page 44 • "Requirement 1-Open Ports by Device Report" on page 44 • "Requirement 1-PCI Systems to External - All Report" on page 44 • "Requirement 1-VPN Configuration Changes Report" on page 45
Requirement 2: Default Security Parameters	**PCI Alert** • "PCI Requirement 2 - Default Account Usage Alert" on page 46 **PCI Report** • "Requirement 2-Default Account Usage Report" on page 47

PCI Requirement	Associated PCI Alerts and Reports
Requirement 3: Protecting Stored Data	**PCI Alerts** • "PCI Requirement 3 - Credit Card Number in Clear Text Alert" on page 48 • "PCI Requirement 3 - Credit Card Number in Clear Text (TippingPoint) - Updated Alert" on page 48 • "PCI Requirement 3 - Credit Card Number in Clear Text (Juniper) Alert" on page 48 • "PCI Requirement 3 - Credit Card Number in Clear Text (Reconnex) Alert" on page 49 • "PCI Requirement 3 - Credit Card Number in Clear Text (Vericept) Alert" on page 49 • "PCI Requirement 3 - Credit Card Number in Clear Text (Vontu) Alert" on page 49 **PCI Report** • "Requirement 3-Credit Card Numbers in Clear Text Report" on page 50
Requirement 4: Encrypted Transmissions	**PCI Alerts** • "PCI Requirement 4 - Internal Systems Running Insecure Services Alert" on page 51 • "PCI Requirement 4 - Internal Systems Using Insecure Public Services Alert" on page 52 **PCI Reports** • "Requirement 4-Outbound Unencrypted Services Report" on page 52 • "Requirement 4-PCI Systems Providing Unencrypted Services Report" on page 53
Requirement 5: Anti-Virus	**PCI Alerts** • "PCI Requirement 5 - Failed Virus Quarantine or Clean or Deletion Alert" on page 54 • "PCI Requirement 5 - Network Traffic matching a Virus Signature is Detected Alert" on page 54 • "PCI Requirement 5 - Successful Virus Quarantine or Clean or Deletion Alert" on page 55 • "PCI Requirement 5 - Virus Discovered Alert" on page 55 **PCI Reports** • "Requirement 5-Anti-Virus Disabled Report" on page 55 • "Requirement 5-Detailed Anti-Virus Report" on page 56 • "Requirement 5-Failed Anti-Virus Updates Report" on page 56 • "Requirement 5-Successful Anti-Virus Updates-Summary Report" on page 56 • "Requirement 5-Virus Summary By Host Report" on page 57 • "Requirement 5-Virus Summary By Virus Report" on page 57 • "Requirement 5-Detailed Anti-Virus Report per Host Report" on page 57

PCI Requirement	Associated PCI Alerts and Reports
Requirement 6: System Applications	**PCI Alerts** • "PCI Requirement 6 - Excessive Failed Application Level Changes Alert" on page 58 • "PCI Requirement 6 - Excessive Failed Operating System Changes Alert" on page 59 **PCI Reports** • "Requirement 6-All Configuration Changes to Virtualization Management Systems Report" on page 59 • "Requirement 6-All Configuration Modifications to Virtual Machines Report" on page 60 • "Requirement 6-Application Modifications Report" on page 61 • "Requirement 6-Device Configuration Modifications Report" on page 61 • "Requirement 6-Operating System Changes Report" on page 62
Requirement 7: Business Need-To-Know	**PCI Report** • "Requirement 7-Users Accessing CDE - All Report" on page 63
Requirement 8: Unique User ID	**PCI Reports** • "Requirement 8-Successful Password Changes Report" on page 63 • "Requirement 8-Windows Account Lockouts by System Report" on page 64 • "Requirement 8-Windows Account Lockouts by User Report" on page 64
Requirement 9: Physical Access	**PCI Alerts** • "PCI Requirement 9 - Excessive Failed Physical System Access Attempts Alert" on page 65 • "PCI Requirement 9 - Excessive Failed Physical System Account Creation or Modification Alert" on page 65 **PCI Reports** • "Requirement 9-Physical Access System Account Creation Report" on page 66 • "Requirement 9-Physical Access System Account Deletion Report" on page 66 • "Requirement 9-Physical Access System Account Modification Report" on page 67 • "Requirement 9-Physical Facility Access Attempts Report" on page 67

PCI Requirement	Associated PCI Alerts and Reports
Requirement 10: Tracking and Monitoring Data Access	**PCI Alerts** • "PCI Requirement 10 - Device Clock Synchronization Problems Alert" on page 70 • "PCI Requirement 10 - Excessive Failed Account Creations Alert" on page 70 • "PCI Requirement 10 - Excessive Failed Account Deletions Alert" on page 70 • "PCI Requirement 10 - Excessive Failed Account Modifications Alert" on page 71 • "PCI Requirement 10 - Excessive Failed Administrative Actions Alert" on page 71 • "PCI Requirement 10 - Excessive Failed Administrative Logins Alert" on page 72 • "PCI Requirement 10 - Excessive Failed Authorization Changes (including Windows 2008) Alert" on page 72 • "PCI Requirement 10 - Excessive Failed Database Access Alert" on page 73 • "PCI Requirement 10 - Excessive Failed File Creations Alert" on page 73 • "PCI Requirement 10 - Excessive Failed File Deletions Alert" on page 73 • "PCI Requirement 10 - Excessive Failed File Modifications Alert" on page 74 • "PCI Requirement 10 - Excessive Failed Resource Access Alert" on page 74 • "PCI Requirement 10 - Excessive Failed User Actions Alert" on page 74 • "PCI Requirement 10 - Excessive Failed User Logins Alert" on page 75 • "PCI Requirement 10 - Excessive Successful Administrative Actions Alert" on page 76 • "PCI Requirement 10 - Excessive Successful Administrative Logins Alert" on page 76 • "PCI Requirement 10 - Excessive Successful Authorization Changes (including Windows 2008) Alert" on page 77 • "PCI Requirement 10 - Excessive Successful Account Creations Alert" on page 77 • "PCI Requirement 10 - Excessive Successful Account Deletions Alert" on page 77 • "PCI Requirement 10 - Excessive Successful Account Modifications Alert" on page 78 • "PCI Requirement 10 - Excessive Successful Database Access Alert" on page 78 • "PCI Requirement 10 - Excessive Successful File Creations Alert" on page 78 • "PCI Requirement 10 - Excessive Successful File Deletions Alert" on page 79 • "PCI Requirement 10 - Excessive Successful File Modifications Alert" on page 79 • "PCI Requirement 10 - Excessive Successful Resource Access Alert" on page 79 • "PCI Requirement 10 - Excessive Successful User Actions Alert" on page 80 • "PCI Requirement 10 - Excessive Successful User Logins Alert" on page 80 • "PCI Requirement 10 - Microsoft Audit Log Cleared (including Windows 2008) Alert" on page 81 • "PCI Requirement 10 - Virtual Machine Down Alert" on page 81 • "PCI Requirement 10 - Virtual Machine Modifications Alert" on page 82 • "PCI Requirement 10 - Virtual Machine Data Manipulations Alert" on page 82 • "PCI Requirement 10 - Virtual Management System Alerts Alert" on page 83

PCI Requirement	Associated PCI Alerts and Reports
Requirement 10: Tracking and Monitoring Data Access	**PCI Reports** • "Requirement 10-Account Creation Report" on page 84 • "Requirement 10-Account Deletion Report" on page 85 • "Requirement 10-Administrative Actions Report" on page 85 • "Requirement 10-Administrative Logins - All Report" on page 85 • "Requirement 10-Administrative Logins - Failed Report" on page 86 • "Requirement 10-Administrative Logins - Successful Report" on page 86 • "Requirement 10-All Detected Virtual Machine IP Addresses Report" on page 87 • "Requirement 10-All Detected Virtual Machine MAC Addresses Report" on page 87 • "Requirement 10-All Hypervisors per Reporting Device Report" on page 88 • "Requirement 10-All Virtualization Infrastructure Events Report" on page 90 • "Requirement 10-All Virtual Machine Creation and Deletion Events Report" on page 88 • "Requirement 10-All Virtual Machine Data Manipulations Report" on page 89 • "Requirement 10-Authorization Changes Report" on page 90 • "Requirement 10-Clock Synchronization Problems Report" on page 90 • "Requirement 10-Database Access - All Report" on page 91 • "Requirement 10-Database Access - Failed Report" on page 91 • "Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices Report" on page 91 • "Requirement 10-File Creation Attempts Report" on page 92 • "Requirement 10-File Deletion Attempts Report" on page 92 • "Requirement 10-File Manipulations - All Report" on page 93 • "Requirement 10-File Modification Attempts Report" on page 93 • "Requirement 10-Microsoft Audit Log Cleared Report" on page 93 • "Requirement 10-Number of Hypervisors Detected per Reporting Device Report" on page 94 • "Requirement 10-Number of Virtual Machines by Reporting Device and Hypervisor Report" on page 94 • "Requirement 10-Resource Access - Failed Report" on page 95 • "Requirement 10-Top Hypervisors with the Most VM Activities Report" on page 95 • "Requirement 10-Top Hypervisors with the Most VM Creations Report" on page 96 • "Requirement 10-Top Users with the Most VM Activities Report" on page 96 • "Requirement 10-User Logins - All Report" on page 97 • "Requirement 10-User Logins - Failed Report" on page 97 • "Requirement 10-User Logins - Successful Report" on page 98

PCI Requirement	Associated PCI Alerts and Reports
Requirement 11: Testing Systems and Networks	**PCI Alerts** • "PCI Requirement 11 - Suspicious Events Alert" on page 100 • "PCI Requirement 11 - Vulnerabilities Alert" on page 100 **PCI Reports** • "Requirement 11-All Vulnerabilities by Assets Report" on page 101 • "Requirement 11-Attacks and Suspicious Events Overview Report" on page 101 • "Requirement 11-HIDS Event Review by Device Report" on page 101 • "Requirement 11-NIDS Event Review by Device Report" on page 102 • "Requirement 11-Top 20 Vulnerabilities Report" on page 102 • "Requirement 11-Top 20 Vulnerable Assets Report" on page 102 • "Requirement 11-Attack in Network Report" on page 103 • "Requirement 11-Attack on Host - Detail Report" on page 103 • "Requirement 11-Attacks and Suspicious Events per Host Report" on page 104 • "Requirement 11-Attacks on Host - All Report" on page 104 • "Requirement 11-Vulnerability Count per Scanner Report" on page 104 • "Requirement 11-Vulnerability in Network Report" on page 105 • "Requirement 11-Vulnerabilities on Host per Scanner Report" on page 105 • "Requirement 11-Vulnerabilities per Host - All Report" on page 105
Requirement 12: Maintaining an Information Security Policy	**PCI Reports** • "Requirement 12-All Reporting Devices Report" on page 106 • "Requirement 12-Device to Host Event Count Report" on page 106 • "Requirement 12-Device to Host Event Detail Report" on page 107 • "Requirement 12-Event in Network Report" on page 107 • "Requirement 12-Host Event Count Report" on page 108 • "Requirement 12-Host Event Count Report" on page 108

The following table summarizes all the supplied payment application reports and alerts.

PA-DSS Requirement	Associated Alerts and Reports
Requirement 4: Log Payment Application Activity	**PA-DSS Alerts** • "PA-DSS 4 - Anonymous Payment Application Access to Cardholder Data Alert" on page 111 • "PA-DSS 4 - Consecutive Invalid Payment Application Access Attempts Alert" on page 112 • "PA-DSS 4 - Payment Application Access to Cardholder Data with no User Name Alert" on page 112 • "PA-DSS 4 - Payment Application Access with Anonymous User Name Alert" on page 112 • "PA-DSS 4 - Payment Application Access with No User Name Alert" on page 113 • "PA-DSS 4 - Payment Application Audit Log Initialized Alert" on page 113 **PA-DSS Reports** • "PA-DSS Requirement 4 - All Administrative Actions in Payment Applications Report" on page 114 • "PA-DSS Requirement 4 - Anonymous Access to Payment Application Report" on page 114 • "PA-DSS Requirement 4 - Anonymous Payment Application Access to Cardholder Data Report" on page 115 • "PA-DSS Requirement 4 - Creations and Deletions of Payment Application Objects Report" on page 115 • "PA-DSS Requirement 4 - Details of Invalid Payment Application Access Attempts" on page 115 • "PA-DSS Requirement 4 - Individual Access to Payment Applications Report" on page 116 • "PA-DSS Requirement 4 - Insufficient Audit Trail in Payment Application Events Report" on page 116 • "PA-DSS Requirement 4 - Summary of Administrative Actions in Payment Applications Report" on page 117 • "PA-DSS Requirement 4 - Summary of Invalid Payment Application Access Attempts Report" on page 117 • "PA-DSS Requirement 4 - Summary of Payment Applications with Insufficient Audit Trail Report" on page 118

Requirement 1: Firewall Configuration

Requirement 1 states that companies should install and maintain a firewall configuration that protects cardholder data. The following PCI alerts and reports are provided to address PCI Requirement 1:

- **Requirement 1: Firewall Configuration Alerts**
  - "PCI Requirement 1 - Direct Traffic from CDE to Public Addresses Alert" on page 41
  - "PCI Requirement 1 - Direct Traffic from Public Addresses to CDE Alert" on page 41
  - "PCI Requirement 1 - Firewall Configuration Changes Alert" on page 42

- "PCI Requirement 1 - Network Equipment Configuration Changes Alert" on page 42
- "PCI Requirement 1 - VPN Configuration Changes Alert" on page 42

- **Requirement 1: Firewall Configuration Reports**
  - "Requirement 1-External to PCI System Activity - All Report" on page 43
  - "Requirement 1-External to PCI Systems on Disallowed Ports Report" on page 43
  - "Requirement 1-Firewall Configuration Changes Report" on page 43
  - "Requirement 1-Network Equipment Configuration Changes Report" on page 44
  - "Requirement 1-Open Ports by Device Report" on page 44
  - "Requirement 1-PCI Systems to External - All Report" on page 44
  - "Requirement 1-VPN Configuration Changes Report" on page 45

Requirement 1 Alerts

Logger PCI Requirement 1 alerts notify PCI analysts when events occur that indicate the direct flow of traffic between public IPs and the Cardholder Data Environment (CDE).

PCI Requirement 1 - Direct Traffic from CDE to Public Addresses Alert	
Alert is triggered when ...	... a router or firewall reports direct communication from the Cardholder Data Environment (CDE) to public IP addresses. This type of activity is a violation of the PCI Data Security Standard (DSS).
Configuration	Edit the alert and in the Query Terms field that contains the string: `CDE_ADDRESSES`, replace `CDE_ADDRESSES` with a regular expression that specifies the range of IP addresses for machines in the Cardholder Data Environment (CDE). For more information, see "Customizing PCI Alerts with Regular Expressions" on page 26.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26

PCI Requirement 1 - Direct Traffic from Public Addresses to CDE Alert	
Alert is triggered when ...	... a router or firewall reports communications from public IP addresses to the Cardholder Data Environment (CDE). This type of activity is a violation of the PCI Data Security Standard (DDS).
Configuration	Edit the alert and in the Query Terms field that contains the string: `CDE_ADDRESSES`, replace `CDE_ADDRESSES` with a regular expression that specifies the range of IP addresses for machines in the Cardholder Data Environment (CDE). For more information, see "Customizing PCI Alerts with Regular Expressions" on page 26.

PCI Requirement 1 - Direct Traffic from Public Addresses to CDE Alert	
Enabled by Default	No
Default **Match Count**	1 - See “Match Count and Threshold (Sec) Fields” on page 26.
Default **Threshold (Sec)**	1 - See “Match Count and Threshold (Sec) Fields” on page 26.

.

PCI Requirement 1 - Firewall Configuration Changes Alert	
Alert is triggered when ...	... changes to a Firewall’s configuration file are reported.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See “Match Count and Threshold (Sec) Fields” on page 26.
Default **Threshold (Sec)**	1 - See “Match Count and Threshold (Sec) Fields” on page 26.

PCI Requirement 1 - Network Equipment Configuration Changes Alert	
Alert is triggered when ...	... changes to a network device's configuration file are reported.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See “Match Count and Threshold (Sec) Fields” on page 26.
Default **Threshold (Sec)**	1 - See “Match Count and Threshold (Sec) Fields” on page 26.

PCI Requirement 1 - VPN Configuration Changes Alert	
Alert is triggered when ...	... changes to a VPN device's configuration file are reported.
Configuration	None required

PCI Requirement 1 - VPN Configuration Changes Alert	
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26

Requirement 1 Reports

Logger PCI Requirement 1 reports provide the following views of events from firewalls, routers, and intrusion prevention systems that involve traffic with systems that are subject to PCI compliance.

Requirement 1-External to PCI System Activity - All Report	
PCI Section	1.4.1
Description	This report shows all external systems that are communicating directly with PCI systems. This traffic should be justified.
Requirement Support	This report should be reviewed to ensure that public access to systems storing cardholder data is not direct.
Testing Procedure	Examine firewall/router configurations and verify there is no direct route inbound or outbound for Internet traffic.
Configuration	None required.

Requirement 1-External to PCI Systems on Disallowed Ports Report	
PCI Section	1.4.1
Description	This report shows all traffic from external sources to PCI systems that is not explicitly allowed based on commonly used ports. The list of ports should be configured within the query.
Requirement Support	This report provides evidence for monitoring used protocols.
Testing Procedure	Verify that firewall configuration standards include justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN.
Configuration	Configure the *PCI 1-External To PCI Systems On Disallowed Ports* query with disallowed ports for your site. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Requirement 1-Firewall Configuration Changes Report	
PCI Section	1.1.8a and 1.1.8b

Requirement 1-Firewall Configuration Changes Report	
Description	This report shows all firewall configuration changes.
Requirement Support	This report can provide evidence for reviewing firewall configuration changes.
Testing Procedure	1.1.8 a: Verify that firewall configuration standards require quarterly review of firewall and router rule sets. 1.1.8 b: Verify that the rule sets are reviewed each quarter.
Configuration	None required.

Requirement 1-Network Equipment Configuration Changes Report	
PCI Section	1.1.8a and 1.1.8b
Description	This report shows all PCI network equipment configuration changes, including changes to routers and switches.
Requirement Support	This report can provide evidence for reviewing router configuration changes.
Testing Procedure	1.1.8 a: Verify that firewall configuration standards require quarterly review of firewall and router rule sets. 1.1.8 b: Verify that the rule sets are reviewed each quarter.
Configuration	None required.

Requirement 1-Open Ports by Device Report	
PCI Section	1.1.6
Description	This query finds all ports that were passed by a firewall, as well as the firewall rule number that it triggered.
Requirement Support	This report provides evidence for monitoring used protocols.
Testing Procedure	Verify that firewall configuration standards include justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN.
Configuration	None required.

Requirement 1-PCI Systems to External - All Report	
PCI Section	1.3.6, 1.3.8, 1.4.2
Description	This report shows PCI systems that are communicating with external systems. This traffic should be justified.
Requirement Support	This report should be reviewed to ensure that public access to systems storing cardholder data is not direct.

Requirement 1-PCI Systems to External - All Report	
Testing Procedure	Examine firewall/router configurations and verify that internal outbound traffic from cardholder applications can only access IP addresses within the DMZ.
Configuration	None required.

Requirement 1-VPN Configuration Changes Report	
PCI Section	1.1.8/6.4
Description	This report shows all configuration changes made to PCI related VPN devices.
Requirement Support	This report can provide evidence for reviewing router configuration changes.
Testing Procedure	1.1.8 a: Verify that firewall configuration standards require quarterly review of firewall and router rule sets. 1.1.8 b: Verify that the rule sets are reviewed each quarter.
Configuration	None required.

Requirement 2: Default Security Parameters

Newly deployed systems are often left with default configuration parameters enabled, such as default accounts and passwords. These can leave open known, easily exploitable vulnerabilities. Requirement 2 states that companies should not use vendor-supplied defaults for system passwords and other security parameters.

The following PCI alert and report are provided to address PCI Requirement 2:

- **Requirement 2: Default Security Parameters Alert**
  - “PCI Requirement 1 - Direct Traffic from Public Addresses to CDE Alert” on page 41
- **Requirement 2: Default Security Parameters Report**
  - “Requirement 2-Default Account Usage Report” on page 47

Requirement 2 Alert

The Logger PCI Requirement 2 alert notifies PCI analysts when default configuration parameters (such as default vendor accounts) are used.

PCI Requirement 2 - Default Account Usage Alert	
Alert is triggered when ...	... the source or destination account name matches one of the following default account names: • admin • root<space> • sa<space> • nobody<space> • guest<space> • manager<space> • sys<space> • system<space> • oracle<space> • orcladmin<space> • cisco<space> • pixadmin<space> Where <space> represents the space character. All account names are case insensitive. In the Query Terms field that specifies the account names, the admin account name is specified without a trailing space. Specifying an account name without a trailing space means any account name that starts with the same set of characters is matched, for example, the account name admin matches any string beginning with admin including Administrator or admins. This pattern matching does not occur with the account names that end with the <space> character, for example the account name sa<space> does not match the string sarah.
Configuration	Edit the alert and in the Query Terms field that lists the default user names, change the set of default account names to reflect the set of account names used by software applications at your site. For example, add the CTXSYS user name to the user list: user=(admin|root |sa |nobody |guest |manager |sys |system |oracle |orcladmin |cisco |pixadmin |CTXSYS) Separate the user names using the pipe character (|). The pipe character represents an OR operator.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

Requirement 2 Report

The following Logger PCI Requirement 2 report tracks systems that use default accounts.

Requirement 2-Default Account Usage Report	
PCI Section	2.1
Description	This report shows default account usage. To view or modify the default account names and vendors, see the "Default Account Usage" query.
Requirement Support	Default account usage is a requirement violation.
Testing Procedure	Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)
Configuration	Configure *PCI 2-Default Account Usage* query with the default accounts in use on your site.

Requirement 3: Protect Stored Data

Even if someone breaks through the outer defenses of your network, encrypted data is still unreadable, which makes encryption the ultimate protection mechanism. PCI requirement 3 provides guidelines for safeguarding encrypted data and its keys.

ArcSight specifically addresses section 3.3 of this requirement by recommending how certain security devices, such as network intrusion detection and prevention systems, can be set up to detect cardholder data that makes it to the wire, where it should not be.

The following PCI alerts and reports are provided to address PCI Requirement 3:

- **Requirement 3: Protecting Stored Data Alerts**
  - “PCI Requirement 3 - Credit Card Number in Clear Text Alert” on page 48
  - “PCI Requirement 3 - Credit Card Number in Clear Text (TippingPoint) - Updated Alert” on page 48
  - “PCI Requirement 3 - Credit Card Number in Clear Text (Juniper) Alert” on page 48
  - “PCI Requirement 3 - Credit Card Number in Clear Text (Reconnex) Alert” on page 49
  - “PCI Requirement 3 - Credit Card Number in Clear Text (Vericept) Alert” on page 49
  - “PCI Requirement 3 - Credit Card Number in Clear Text (Vontu) Alert” on page 49
- **Requirement 3: Protecting Stored Data Reports**
  - “Requirement 3-Credit Card Numbers in Clear Text Report” on page 50

Requirement 3 Alerts

Logger PCI Requirement 3 alerts notify PCI analysts when events occur that indicate credit card information is not encrypted.

PCI Requirement 3 - Credit Card Number in Clear Text Alert	
Alert is triggered when ...	... a credit card number appears in the logs as clear text, using one of the following formats: <n><n><n><n>-<n><n><n><n>-<n><n><n><n>-<n><n><n><n> <n><n><n><n>-<n><n><n><n><n><n>-<n><n><n><n> <n><n><n><n>-<n><n><n><n><n><n>-<n><n><n><n><n> Where <n> is single numeric digit.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 3 - Credit Card Number in Clear Text (TippingPoint) - Updated Alert	
Alert is triggered when ...	... a TippingPoint UnityOne IPS reports that credit card information was sent in clear text.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

.

PCI Requirement 3 - Credit Card Number in Clear Text (Juniper) Alert	
Alert is triggered when ...	... a Juniper Netscreen IDS reports that credit card information was sent in clear text using HTTP.
Configuration	None required
Enabled by Default	No

PCI Requirement 3 - Credit Card Number in Clear Text (Juniper) Alert	
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 3 - Credit Card Number in Clear Text (Reconnex) Alert	
Alert is triggered when ...	... a Reconnex information monitoring system reports that credit card information was sent in clear text.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 3 - Credit Card Number in Clear Text (Vericept) Alert	
Alert is triggered when ...	... a Vericept information monitoring system reports that credit card information was sent in clear text.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 3 - Credit Card Number in Clear Text (Vontu) Alert	
Alert is triggered when ...	... a Vontu information monitoring system reports that credit card information was sent in clear text.
Configuration	None required
Enabled by Default	No

PCI Requirement 3 - Credit Card Number in Clear Text (Vontu) Alert	
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

Requirement 3 Report

The following Logger PCI Requirement 3 report detects credit card numbers that appear in clear text.

Requirement 3-Credit Card Numbers in Clear Text Report	
PCI Section	3.3
Description	This report presents occasions of credit card transmission in clear text. It is based on IDS reports and information leakage prevention systems. The query should be customized with the appropriate event and/or identification information for your IDS and IPS systems.
Requirement Support	Any instance of credit card numbers in clear-text is a potential violation of the requirement.
Testing Procedure	Obtain and Examine written policies and examine online displays of credit card data to verify that credit card numbers are masked when displaying cardholder data, except for those with a specific need to see full credit card numbers.
Configuration	Configure the *PCI 3-Credit Card Numbers in Clear Text* query with the event and/or identification information for your IDS and IPS systems. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Requirement 4: Encrypt Transmissions

Requirement 4 states that transmissions from cardholder systems to public networks should be encrypted across open, public networks.

The following PCI alerts and reports are provided to address PCI Requirement 4:

- **Requirement 4: Encrypted Transmissions Alerts**
  - "PCI Requirement 4 - Internal Systems Running Insecure Services Alert" on page 51
  - "PCI Requirement 4 - Internal Systems Using Insecure Public Services Alert" on page 52
- **Requirement 4: Encrypted Transmissions Reports**
  - "Requirement 4-Outbound Unencrypted Services Report" on page 52
  - "Requirement 4-PCI Systems Providing Unencrypted Services Report" on page 53

Requirement 4 Alerts

Logger PCI Requirement 4 alerts notify PCI analysts when events occur that indicate use of non-secure protocols or ports.

PCI Requirement 4 - Internal Systems Running Insecure Services Alert	
Alert is triggered when ...	... insecure services are running on an internal system or a connection is made to insecure port on an internal system. The following services are defined as insecure: • telnetd • ftpd • rexec • pop3 • rsh • imapd An insecure port is a port number that is commonly used by an insecure service. The following ports are defined as insecure: • 20 • 21 • 25 • 110 • 143 • 23 According to PCI Data Security Standard (DSS), use of such services has to be justified and cannot be used to transmit cardholder or sensitive information.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 4 - Internal Systems Using Insecure Public Services Alert	
Alert is triggered when ...	... internal systems are using public insecure services or ports available on the Internet. The following services are defined as insecure: • telnetd • ftpd • rexec • pop3 • rsh • imapd An insecure port is a port number that is commonly used by insecure service. The following ports are defined as insecure: • 20 • 21 • 25 • 110 • 143 • 23 According to PCI Data Security Standard (DSS), use of such services has to be justified and cannot be used to transmit cardholder or sensitive information.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

Requirement 4 Reports

The following PCI Requirement 4 reports monitor PCI system-related traffic that uses non-secure protocols or ports.

Requirement 4-Outbound Unencrypted Services Report	
PCI Section	4.1
Description	This report shows systems (clients) that communicate with servers with an external address over unencrypted protocols and the number of such events recorded. An unencrypted protocol is defined as one of the following: telnetd, ftpd, in.rexecd, rexec, pop3, rsh, imapd; or is performed on the following ports: 20, 21, 25, 110, 143, 23. These values are defined in the query and can be adjusted according to the customer's definitions.

Requirement 4-Outbound Unencrypted Services Report	
Requirement Support	PCI Systems that are communicating with external systems over unencrypted channels are a potential violation of the requirement. Such communications should be justified.
Testing Procedure	Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks.
Configuration	Configure the *PCI 4-Outbound Unencrypted Communication* query with any additional unencrypted ports or protocols relevant to your site. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Requirement 4-PCI Systems Providing Unencrypted Services Report	
PCI Section	4.1
Description	This report shows PCI systems that provide unencrypted communications and the number of such events recorded. Unencrypted communication is defined as using one of the following services: telnetd, ftpd, in.rexecd, rexec, pop3, rsh, imapd; or is performed on the following ports: 20, 21, 25, 110, 143, 23. These values are defined in the query and can be adjusted according to the customer's definitions. A PCI system is defined as one with an internal IP address.
Requirement Support	PCI Systems that are providing unencrypted services are a potential violation of the requirement. Such communications should be justified.
Testing Procedure	Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks.
Configuration	Configure the *PCI 4-PCI Systems Providing Unencrypted Services* query with any additional unencrypted ports or protocols relevant to your site. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Requirement 5: Anti-Virus

PCI requires that anti-virus software be used on PCI-governed systems and regularly maintained.

The following PCI alerts and reports are provided to address PCI Requirement 5:

- **Requirement 5: Anti-Virus Alerts**
  - "PCI Requirement 5 - Failed Virus Quarantine or Clean or Deletion Alert" on page 54
  - "PCI Requirement 5 - Network Traffic matching a Virus Signature is Detected Alert" on page 54
  - "PCI Requirement 5 - Successful Virus Quarantine or Clean or Deletion Alert" on page 55
  - "PCI Requirement 5 - Virus Discovered Alert" on page 55
- **Requirement 5: Anti-Virus Reports**

- "Requirement 5-Anti-Virus Disabled Report" on page 55
- "Requirement 5-Detailed Anti-Virus Report" on page 56
- "Requirement 5-Failed Anti-Virus Updates Report" on page 56
- "Requirement 5-Successful Anti-Virus Updates-Summary Report" on page 56
- "Requirement 5-Virus Summary By Host Report" on page 57
- "Requirement 5-Virus Summary By Virus Report" on page 57
- "Requirement 5-Detailed Anti-Virus Report per Host Report" on page 57

Requirement 5 Alerts

Logger PCI Requirement 5 alerts notify PCI analysts when events occur that indicate systems are infected with viruses.

PCI Requirement 5 - Failed Virus Quarantine or Clean or Deletion Alert	
Alert is triggered when ...	... anti-virus software is not able to quarantine, clean or delete virus files. When notified, PCI analysts should quickly investigate this issue.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 5 - Network Traffic matching a Virus Signature is Detected Alert	
Alert is triggered when ...	... an IDS detected network traffic that matches a virus signature.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 5 - Successful Virus Quarantine or Clean or Deletion Alert	
Alert is triggered when ...	... anti-virus software quarantined, cleaned or deleted virus files.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 5 - Virus Discovered Alert	
Alert is triggered when ...	... anti-virus software discovered a virus on a machine.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

Requirement 5 Reports

The following Logger PCI Requirement 5 reports identifies systems on which the anti-virus service has been disabled, and provides detailed accountings of anti-virus activities, from updates and remediation activity to failed updates. It also shows any viruses detected by host and by virus name.

The *Requirement 5 - Anti-Virus Disabled* report provides access to drill-down reports as described in Figure C-1 on page 136.

Requirement 5-Anti-Virus Disabled Report	
PCI Section	5.2
Description	This report shows all anti-virus disabled events as reported by Microsoft systems.
Requirement Support	Disabling anti-virus software is a requirement violation. However, having a record of such incidents demonstrates the capability to generate logs and is a mitigating factor.

Requirement 5-Anti-Virus Disabled Report	
Testing Procedure	Verify that anti-virus software is current, actively running, and capable of generating logs.
Configuration	None required.

The *Requirement 5 - Detailed Anti-Virus Report* report provides access to drill-down reports as described in Figure C-2 on page 136.

Requirement 5-Detailed Anti-Virus Report	
PCI Section	5.1.1
Description	This report shows a detailed listing of anti-virus events (routine maintenance and remediation events) ordered according to zone, IP address and virus name.
Requirement Support	This report demonstrates compliance with requirement 5.1.1.
Testing Procedure	For a sample of system components, critical servers, and wireless access points, verify that anti-virus programs detect, remove, and protect against other malicious software, including spyware and adware.
Configuration	None required.

The *Requirement 5 - Failed Anti-Virus Updates* report provides access to drill-down reports as described in Figure C-4 on page 137.

Requirement 5-Failed Anti-Virus Updates Report	
PCI Section	5.2
Description	This report shows when anti-virus software fails to retrieve its updates. Is shows the system on which it happened, the minute it happened, and how many failed updates occurred in that minute.
Requirement Support	Failed anti-virus updates violates the requirement to have current anti-virus software. However, having a record of such incidents demonstrates the capability to generate logs and is a mitigating factor.
Testing Procedure	Verify that anti-virus software is current, actively running, and capable of generating logs.
Configuration	None required.

The *Requirement 5 - Successful Anti-Virus Updates-Summary* report provides access to drill-down reports as described in Figure C-5 on page 137.

Requirement 5-Successful Anti-Virus Updates-Summary Report	
PCI Section	5.2
Description	This report shows the number of successful times anti-virus updates were performed, for each host in the selected time frame.

Requirement 5-Successful Anti-Virus Updates-Summary Report	
Requirement Support	This report provides supporting evidence to maintaining an up-to-date anti-virus deployment.
Testing Procedure	Verify that anti-virus software is current, actively running, and capable of generating logs.
Configuration	None required.

The *Requirement 5 - Virus Summary by Host* report provides access to drill-down reports as described in Figure C-6 on page 137.

Requirement 5-Virus Summary By Host Report	
PCI Section	5.1.1
Description	This report shows systems infected with viruses and the number of infections for each system.
Requirement Support	This report provides information on detected viruses, demonstrating compliance with requirement 5.1.1.
Testing Procedure	For a sample of system components, critical servers, and wireless access points, verify that anti-virus programs detect, remove, and protect against other malicious software, including spyware and adware.
Configuration	None required.

Requirement 5-Virus Summary By Virus Report	
PCI Section	5.1.1
Description	This report shows systems infected with viruses and the number of infections for each system.
Requirement Support	This report provides information on detected viruses, demonstrating compliance with requirement 5.1.1.
Testing Procedure	For a sample of system components, critical servers, and wireless access points, verify that anti-virus programs detect, remove, and protect against other malicious software, including spyware and adware.
Configuration	None required.

Requirement 5 Drill-Down Report

The *Requirement 5-Detailed Anti-Virus Report per Host* report is a drill-down report that can be accessed by using Destination Host Name as a parameter.

Requirement 5-Detailed Anti-Virus Report per Host Report	
PCI Section	5.1.1
Description	This report shows a detailed listing of anti-virus events (routine maintenance and remediation events) ordered according to zone, IP address and virus name.

Requirement 5-Detailed Anti-Virus Report per Host Report	
Requirement Support	This report demonstrates compliance with requirement 5.1.1 by showing anti-virus activity on a specific host.
Testing Procedure	For a sample of system components, critical servers, and wireless access points, verify that anti-virus programs detect, remove, and protect against other malicious software, including spyware and adware.
Configuration	None required.

Requirement 6: System Applications

Requirement 6 states that companies should develop and maintain secure systems and applications. This requirement is concerned with ensuring that you have adequate processes in place to maintain the security of your systems and applications. This includes maintaining the latest patch levels, vulnerability reports, in-house software security, change control procedures, and web application security.

The following PCI alerts and reports are provided to address PCI Requirement 6:

- **Requirement 6: System Applications Alerts**
  - "PCI Requirement 6 - Excessive Failed Application Level Changes Alert" on page 58
  - "PCI Requirement 6 - Excessive Failed Operating System Changes Alert" on page 59
- **Requirement 6: System Applications Reports**
  - "Requirement 6-All Configuration Changes to Virtualization Management Systems Report" on page 59
  - "Requirement 6-All Configuration Modifications to Virtual Machines Report" on page 60
  - "Requirement 6-Application Modifications Report" on page 61
  - "Requirement 6-Device Configuration Modifications Report" on page 61
  - "Requirement 6-Operating System Changes Report" on page 62

Requirement 6 Alerts

Logger PCI Requirement 6 alerts notify PCI analysts when events occur that indicate excessive numbers of unsuccessful changes to applications and operating systems have been attempted.

PCI Requirement 6 - Excessive Failed Application Level Changes Alert	
Alert is triggered when ...	... an excessive number of unsuccessful changes to applications are attempted.
Configuration	None required
Enabled by Default	No
Default **Match Count**	30 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 6 - Excessive Failed Application Level Changes Alert	
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 6 - Excessive Failed Operating System Changes Alert	
Alert is triggered when ...	... an excessive number of unsuccessful changes to operating systems are attempted.
Configuration	None required
Enabled by Default	No
Default **Match Count**	30 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

Requirement 6 Reports

The following PCI Requirement 6 reports detect modifications made to applications, device configurations, and operating systems.

Requirement 6-All Configuration Changes to Virtualization Management Systems Report	
PCI Section	6.4.5.3
Description	This report shows all configuration changes to virtualization management systems.
Requirement Support	This report provides evidence that change control processes and procedures are in place for all changes to virtualization management system components.
Testing Procedure	6.4.5.3.a: For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system. 6.4.5.3.b: For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.

Requirement 6-All Configuration Changes to Virtualization Management Systems Report	
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 6-All Configuration Modifications to Virtual Machines Report	
PCI Section	6.4.5.3
Description	This report shows all configuration modifications to virtual machines (VMs) in your environment, reported by their hypervisors.
Requirement Support	This report should be reviewed to determine all configuration modifications to virtual machines (VMs), that were reported by hypervisors.
Testing Procedure	6.4.5.3.a: For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system. 6.4.5.3.b: For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 6-Application Modifications Report	
PCI Section	6.4
Description	This report shows modifications made to application configuration files.
Requirement Support	This report is aimed for security managers and PCI assessors for correlation and support of actual changes with documentation of approved change. Manual assessment of change control documents is still required, however.
Testing Procedure	For a sample of system components, critical servers, and wireless access points, examine the three most recent changes/security patches for each system component, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures: • 6.4.1: Verify that documentation of customer impact is included in the change control documentation for each sampled change. • 6.4.2: Verify that management sign-off by appropriate parties is present for each sampled change. • 6.4.3: Verify that operational functionality testing was performed for each sampled change. • 6.4.4: Verify that back-out procedures are prepared for each sampled change.
Configuration	None required.

Requirement 6-Device Configuration Modifications Report	
PCI Section	6.4
Description	This report shows device configuration changes on network equipment, such as switches and routers.
Requirement Support	This report is aimed for security managers and PCI assessors for correlation and support of actual changes with documentation of approved change. Manual assessment of change control documents is still required however.

Requirement 6-Device Configuration Modifications Report	
Testing Procedure	For a sample of system components, critical servers, and wireless access points, examine the three most recent changes/security patches for each system component, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures: • 6.4.1: Verify that documentation of customer impact is included in the change control documentation for each sampled change. • 6.4.2: Verify that management sign-off by appropriate parties is present for each sampled change. • 6.4.3: Verify that operational functionality testing was performed for each sampled change. • 6.4.4: Verify that back-out procedures are prepared for each sampled change.
Configuration	None required.

Requirement 6-Operating System Changes Report	
PCI Section	6.4
Description	This report shows changes made to operating system configurations.
Requirement Support	This report is aimed for security managers and PCI assessors for correlation and support of actual changes with documentation of approved change. Manual assessment of change control documents is still required, however.
Testing Procedure	For a sample of system components, critical servers, and wireless access points, examine the three most recent changes/security patches for each system component, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures: • 6.4.1: Verify that documentation of customer impact is included in the change control documentation for each sampled change. • 6.4.2: Verify that management sign-off by appropriate parties is present for each sampled change. • 6.4.3: Verify that operational functionality testing was performed for each sampled change. • 6.4.4: Verify that back-out procedures are prepared for each sampled change.
Configuration	None required.

Requirement 7: Business Need-To-Know

Requirement 7 states that access to critical cardholder data should be restricted only to users who have express authorization.

The following PCI Report is provided to address PCI Requirement 7:

- **Requirement 7: Business Need-To-Know Report**

- "Requirement 7-Users Accessing CDE - All Report" on page 63

Requirement 7 Reports

The following PCI Requirement 7 report displays users who have accessed the Cardholder Data Environment (CDE).

Requirement 7-Users Accessing CDE - All Report	
PCI Section	7.1
Description	This Report displays all users who accessed the Cardholder Data Environment (CDE) and the last time they accessed it.
Requirement Support	Knowing which users accessed the cardholder data environment (CDE) can help assess accuracy of access controls.
Testing Procedure	Testing Procedure 7.1: Obtain and examine written policy for data control, and verify that the policy incorporates the following: • Access rights to privileged User IDs are restricted to the least privileges necessary to perform job responsibilities • Assignment of privileges is based on individual personnel's job classification and function • Requirement for an authorization form signed by management that specifies required privileges • Implementation of an automated access control system
Configuration	None required.

Requirement 8: Unique User ID

Requirement 8 states that each user with access to cardholder data systems has a unique user ID so that any actions taken on systems that affect cardholder data can be traced to known and authorized users.

The following PCI Reports are provided to address PCI Requirement 8:

- **Requirement 8: Unique User ID Reports**
  - "Requirement 8-Successful Password Changes Report" on page 63
  - "Requirement 8-Windows Account Lockouts by System Report" on page 64
  - "Requirement 8-Windows Account Lockouts by User Report" on page 64

The following PCI Requirement 8 reports keep track of user password changes and account lockouts on Windows systems.

Requirement 8-Successful Password Changes Report	
PCI Section	8.5.9
Description	This report shows which users have changed their passwords and when.
Requirement Support	This report lists password changes per user. The interval between changes should not exceed 90 days.

Requirement 8-Successful Password Changes Report	
Testing Procedure	For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days. For Service Providers only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change.
Configuration	None required.

Requirement 8-Windows Account Lockouts by System Report	
PCI Section	8.5.13
Description	This report shows all account lockouts on Windows systems.
Requirement Support	This report can be used as evidence that access attempts are limited to no more than 6 attempts.
Testing Procedure	For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that a user's account is locked out after not more than six invalid logon attempts. For Service Providers only, review internal processes and customer/user documentation to verify that customer accounts are temporarily locked-out after not more than six invalid access attempts.
Configuration	None required.

Requirement 8-Windows Account Lockouts by User Report	
PCI Section	8.5.13
Description	This report shows all account lockouts on Windows systems.
Requirement Support	Requirement Support: This report lists password changes per user. The interval between changes should not exceed 90 days.
Testing Procedure	For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days. For Service Providers only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change.
Configuration	None required.

Requirement 9: Physical Access

Requirement 9 states that companies should restrict physical access to cardholder data. This requirement ensures restricted physical access to data or systems that house cardholder data.

Most of the items in PCI Requirement 9 are geared toward safeguarding physical access to buildings and equipment, and maintaining control over access to paper and electronic media.

The following PCI alerts and reports are provided to address PCI Requirement 9:

- **Requirement 9: Physical Access Alerts**
  - "PCI Requirement 9 - Excessive Failed Physical System Access Attempts Alert" on page 65
  - "PCI Requirement 9 - Excessive Failed Physical System Account Creation or Modification Alert" on page 65
- **Requirement 9: Physical Access Reports**
  - "Requirement 9-Physical Access System Account Creation Report" on page 66
  - "Requirement 9-Physical Access System Account Deletion Report" on page 66
  - "Requirement 9-Physical Access System Account Modification Report" on page 67
  - "Requirement 9-Physical Facility Access Attempts Report" on page 67

Requirement 9 Alerts

Logger PCI Requirement 9 alerts notify PCI analysts when events occur that indicate too many failed access, creation or modification attempts have occurred to a physical access system such as a badge reader.

PCI Requirement 9 - Excessive Failed Physical System Access Attempts Alert	
Alert is triggered when ...	... too many failed access attempts to a physical access system occur.
Configuration	None required
Enabled by Default	No
Default **Match Count**	20 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

.

PCI Requirement 9 - Excessive Failed Physical System Account Creation or Modification Alert	
Alert is triggered when ...	... too many failed attempts to create or modify an account on a physical access system occur.
Configuration	None required

PCI Requirement 9 - Excessive Failed Physical System Account Creation or Modification Alert	
Enabled by Default	No
Default **Match Count**	5 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

Requirement 9 Reports

Because ArcSight Logger deals with feeds from devices connected to the network, the Logger PCI Requirement 9 Reports focuses on monitoring building access events from badge card readers and monitoring account creations, modifications, and deletions from these systems.

Requirement 9-Physical Access System Account Creation Report	
PCI Section	9.1
Description	This report shows all authentication verification events (badge-ins) involving physical access systems.
Requirement Support	This report can demonstrate that physical access procedures are in place and are being followed.
Testing Procedure	Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems that contain cardholder data. • Verify that access is controlled with badge readers and other devices including authorized badges and lock and key • Observe a system administrator's attempt to log into consoles for three randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.
Configuration	None required.

Requirement 9-Physical Access System Account Deletion Report	
PCI Section	9.1
Description	Shows all new accounts added to physical access systems sorted by user name for the time period you specify when you run the report.
Requirement Support	This report can demonstrate that physical access procedures are in place and are being followed.

Requirement 9-Physical Access System Account Deletion Report	
Testing Procedure	Testing Procedure 9.1: Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems that contain cardholder data • Verify that access is controlled with badge readers and other devices including authorized badges and lock and key • Observe a system administrator's attempt to log into consoles for three randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.
Configuration	None required.

Requirement 9-Physical Access System Account Modification Report	
PCI Section	9.1
Description	Shows all deletions of accounts from physical access systems.
Requirement Support	This report can demonstrate that physical access procedures are in place and are being followed.
Testing Procedure	Testing Procedure 9.1: Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems that contain cardholder data • Verify that access is controlled with badge readers and other devices including authorized badges and lock and key • Observe a system administrator's attempt to log into consoles for three randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.
Configuration	None required.

Requirement 9-Physical Facility Access Attempts Report	
PCI Section	9.1
Description	Shows all deletions of accounts from physical access systems.
Requirement Support	This report supports the existence of physical access controls to cardholder data.
Testing Procedure	Testing Procedure 9.1: Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems that contain cardholder data • Verify that access is controlled with badge readers and other devices including authorized badges and lock and key • Observe a system administrator's attempt to log into consoles for three randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.
Configuration	None required.

Requirement 10: Track and Monitor Data Access

Requirement 10 states that companies should track and monitor all access to network resources and cardholder data. This requirement ensures that system activity logs adequately track, monitor, and test all access to network resources and cardholder data.

The following PCI alerts and reports are provided to address PCI Requirement 10:

- **Requirement 10: Tracking and Monitoring Data Access Alerts**
  - “PCI Requirement 10 - Device Clock Synchronization Problems Alert” on page 70
  - “PCI Requirement 10 - Excessive Failed Account Creations Alert” on page 70
  - “PCI Requirement 10 - Excessive Failed Account Deletions Alert” on page 70
  - “PCI Requirement 10 - Excessive Failed Account Modifications Alert” on page 71
  - “PCI Requirement 10 - Excessive Failed Administrative Actions Alert” on page 71
  - “PCI Requirement 10 - Excessive Failed Administrative Logins Alert” on page 72
  - “PCI Requirement 10 - Excessive Failed Authorization Changes (including Windows 2008) Alert” on page 72
  - “PCI Requirement 10 - Excessive Failed Database Access Alert” on page 73
  - “PCI Requirement 10 - Excessive Failed File Creations Alert” on page 73
  - “PCI Requirement 10 - Excessive Failed File Deletions Alert” on page 73
  - “PCI Requirement 10 - Excessive Failed File Modifications Alert” on page 74
  - “PCI Requirement 10 - Excessive Failed Resource Access Alert” on page 74
  - “PCI Requirement 10 - Excessive Failed User Actions Alert” on page 74
  - “PCI Requirement 10 - Excessive Failed User Logins Alert” on page 75
  - “PCI Requirement 10 - Excessive Successful Administrative Actions Alert” on page 76
  - “PCI Requirement 10 - Excessive Successful Administrative Logins Alert” on page 76
  - “PCI Requirement 10 - Excessive Successful Authorization Changes (including Windows 2008) Alert” on page 77
  - “PCI Requirement 10 - Excessive Successful Account Creations Alert” on page 77
  - “PCI Requirement 10 - Excessive Successful Account Deletions Alert” on page 77
  - “PCI Requirement 10 - Excessive Successful Account Modifications Alert” on page 78
  - “PCI Requirement 10 - Excessive Successful Database Access Alert” on page 78
  - “PCI Requirement 10 - Excessive Successful File Creations Alert” on page 78
  - “PCI Requirement 10 - Excessive Successful File Deletions Alert” on page 79
  - “PCI Requirement 10 - Excessive Successful File Modifications Alert” on page 79
  - “PCI Requirement 10 - Excessive Successful Resource Access Alert” on page 79
  - “PCI Requirement 10 - Excessive Successful User Actions Alert” on page 80
  - “PCI Requirement 10 - Excessive Successful User Logins Alert” on page 80
  - “PCI Requirement 10 - Microsoft Audit Log Cleared (including Windows 2008) Alert” on page 81
  - “PCI Requirement 10 - Virtual Machine Down Alert” on page 81
  - “PCI Requirement 10 - Virtual Machine Modifications Alert” on page 82

- "PCI Requirement 10 - Virtual Machine Data Manipulations Alert" on page 82
- "PCI Requirement 10 - Virtual Management System Alerts Alert" on page 83

Requirement 10: Tracking and Monitoring Data Access Reports

- "Requirement 10-Account Creation Report" on page 84
- "Requirement 10-Account Deletion Report" on page 85
- "Requirement 10-Administrative Actions Report" on page 85
- "Requirement 10-Administrative Logins - All Report" on page 85
- "Requirement 10-Administrative Logins - Failed Report" on page 86
- "Requirement 10-Administrative Logins - Successful Report" on page 86
- "Requirement 10-All Detected Virtual Machine IP Addresses Report" on page 87
- "Requirement 10-All Detected Virtual Machine MAC Addresses Report" on page 87
- "Requirement 10-All Hypervisors per Reporting Device Report" on page 88
- "Requirement 10-All Virtual Machine Creation and Deletion Events Report" on page 88
- "Requirement 10-All Virtual Machine Data Manipulations Report" on page 89
- "Requirement 10-All Virtualization Infrastructure Events Report" on page 90
- "Requirement 10-Authorization Changes Report" on page 90
- "Requirement 10-Clock Synchronization Problems Report" on page 90
- "Requirement 10-Database Access - All Report" on page 91
- "Requirement 10-Database Access - Failed Report" on page 91
- "Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices Report" on page 91
- "Requirement 10-File Creation Attempts Report" on page 92
- "Requirement 10-File Deletion Attempts Report" on page 92
- "Requirement 10-File Manipulations - All Report" on page 93
- "Requirement 10-File Modification Attempts Report" on page 93
- "Requirement 10-Microsoft Audit Log Cleared Report" on page 93
- "Requirement 10-Number of Hypervisors Detected per Reporting Device Report" on page 94
- "Requirement 10-Number of Virtual Machines by Reporting Device and Hypervisor Report" on page 94
- "Requirement 10-Resource Access - Failed Report" on page 95
- "Requirement 10-Top Hypervisors with the Most VM Activities Report" on page 95
- "Requirement 10-Top Hypervisors with the Most VM Creations Report" on page 96
- "Requirement 10-Top Users with the Most VM Activities Report" on page 96
- "Requirement 10-User Logins - All Report" on page 97
- "Requirement 10-User Logins - Failed Report" on page 97
- "Requirement 10-User Logins - Successful Report" on page 98

Requirement 10 Alerts

Logger PCI Requirement 10 alerts notify PCI analysts when events occur that indicate failed log-ins or access to resources, user authentications and authorizations, audit log management and audit trails, and clock synchronization.

PCI Requirement 10 - Device Clock Synchronization Problems Alert	
Alert is triggered when ...	... ArcSight SmartConnectors are reporting source events with an incorrect time stamp.
Configuration	None required
Enabled by Default	Yes
Default **Match Count**	20 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed Account Creations Alert	
Alert is triggered when ...	... an excessive number of unsuccessful attempts to create computer accounts occur.
Configuration	None required
Enabled by Default	No
Default **Match Count**	3 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed Account Deletions Alert	
Alert is triggered when ...	... an excessive number of unsuccessful attempts to delete computer accounts occur.
Configuration	None required
Enabled by Default	No
Default **Match Count**	3 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed Account Deletions Alert	
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed Account Modifications Alert	
Alert is triggered when ...	... an excessive number of unsuccessful attempts to modify computer accounts occur.
Configuration	None required
Enabled by Default	No
Default **Match Count**	3 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed Administrative Actions Alert	
Alert is triggered when ...	... an excessive number of failed actions occur by administrative user accounts.
Configuration	Change the set of default administrative accounts defined in this alert, to reflect the administrative accounts used at your site: • admin • root • super • sa<space> • sys<space> • system • manager For more information, see "Configure the Administrative Accounts for the Alert" on page 83.
Enabled by Default	Yes
Default **Match Count**	20 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed Administrative Logins Alert	
Alert is triggered when ...	... an excessive number of failed login attempts occur by administrative user accounts.
Configuration	Change the set of default administrative accounts defined in this alert, to reflect the administrative accounts used at your site: • admin • root • super • sa<space> • sys<space> • system • manager For more information, see "Configure the Administrative Accounts for the Alert" on page 83.
Enabled by Default	Yes
Default **Match Count**	3 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed Authorization Changes (including Windows 2008) Alert	
Alert is triggered when ...	... an excessive number of failed attempts to change authorizations occur—such as changes to access lists. This alert is triggerd for both Windows 2003 and Windows 2008 events.
Configuration	None required
Enabled by Default	No
Default **Match Count**	10 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed Database Access Alert	
Alert is triggered when ...	... an excessive number of unsuccessful database access attempts occur. Database access attempts can be logins or queries.
Configuration	None required
Enabled by Default	No
Default **Match Count**	10 - See "Match Count and Threshold (Sec) Fields" on page 26
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed File Creations Alert	
Alert is triggered when ...	... an excessive number of unsuccessful attempts to create files occur.
Configuration	None required
Enabled by Default	No
Default **Match Count**	20 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed File Deletions Alert	
Alert is triggered when ...	... an excessive number of unsuccessful attempts to delete files occur.
Configuration	None required
Enabled by Default	No
Default **Match Count**	20 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed File Modifications Alert	
Alert is triggered when ...	... an excessive number of unsuccessful attempts to modify files occur.
Configuration	None required
Enabled by Default	No
Default **Match Count**	10 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed Resource Access Alert	
Alert is triggered when ...	... an excessive number of failed attempts to access resources occur. For example, an excessive number of failed attempts to create ssh tunnels occur.
Configuration	None required
Enabled by Default	No
Default **Match Count**	10 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed User Actions Alert	
Alert is triggered when ...	... an excessive number of failed actions occur by non-administrative user accounts. This alert is triggered for any accounts that are *not* listed as an administrative account in the alert.

PCI Requirement 10 - Excessive Failed User Actions Alert	
Configuration	Change the set of default administrative accounts defined in this alert, to reflect the administrative accounts used at your site: • admin • root • super • sa<space> • sys<space> • system • manager For more information, see "Configure the Administrative Accounts for the Alert" on page 83.
Enabled by Default	No
Default **Match Count**	20 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Failed User Logins Alert	
Alert is triggered when ...	... an excessive number of failed login attempts occur by non-administrative user accounts. This alert is triggered for any accounts that are *not* listed as an administrative account in the alert.
Configuration	Change the set of default administrative accounts defined in this alert, to reflect the administrative accounts used at your site: • admin • root • super • sa<space> • sys<space> • system • manager For more information, see "Configure the Administrative Accounts for the Alert" on page 83.
Enabled by Default	No
Default **Match Count**	10 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful Administrative Actions Alert	
Alert is triggered when ...	... an excessive number of successful actions by administrative user accounts occur.
Configuration	Change the set of default administrative accounts defined in this alert, to reflect the administrative accounts used at your site: • admin • root • super • sa<space> • sys<space> • system • manager For more information, see "Configure the Administrative Accounts for the Alert" on page 83.
Enabled by Default	Yes
Default **Match Count**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful Administrative Logins Alert	
Alert is triggered when ...	... a large number of successful logins by administrative user accounts occur.
Configuration	Change the set of default administrative accounts defined in this alert, to reflect the administrative accounts used at your site: • admin • root • super • sa<space> • sys<space> • system • manager For more information, see "Configure the Administrative Accounts for the Alert" on page 83.
Enabled by Default	Yes
Default **Match Count**	10 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful Administrative Logins Alert	
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful Authorization Changes (including Windows 2008) Alert	
Alert is triggered when ...	... a large number of authorization changes occur—such as changes to access lists. This alert is triggerd for both Windows 2003 and Windows 2008 events.
Configuration	None required
Enabled by Default	No
Default **Match Count**	100- See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful Account Creations Alert	
Alert is triggered when ...	... a large number of computer accounts are successfully created.
Configuration	None required
Enabled by Default	No
Default **Match Count**	5 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful Account Deletions Alert	
Alert is triggered when ...	... a large number of computer accounts are successfully deleted.
Configuration	None required
Enabled by Default	No

PCI Requirement 10 - Excessive Successful Account Deletions Alert	
Default **Match Count**	5 - See “Match Count and Threshold (Sec) Fields” on page 26.
Default **Threshold (Sec)**	300 - See “Match Count and Threshold (Sec) Fields” on page 26.

PCI Requirement 10 - Excessive Successful Account Modifications Alert	
Alert is triggered when ...	... a large number of computer accounts are successfully modified.
Configuration	None required
Enabled by Default	No
Default **Match Count**	5 - See “Match Count and Threshold (Sec) Fields” on page 26.
Default **Threshold (Sec)**	300 - See “Match Count and Threshold (Sec) Fields” on page 26.

PCI Requirement 10 - Excessive Successful Database Access Alert	
Alert is triggered when ...	... a large number of successful database accesses are reported. Database access attempts can be logins or queries.
Configuration	None required
Enabled by Default	No
Default **Match Count**	100 - See “Match Count and Threshold (Sec) Fields” on page 26.
Default **Threshold (Sec)**	300 - See “Match Count and Threshold (Sec) Fields” on page 26.

PCI Requirement 10 - Excessive Successful File Creations Alert	
Alert is triggered when ...	... a large number of files are successfully deleted.
Configuration	None required
Enabled by Default	No

PCI Requirement 10 - Excessive Successful File Creations Alert	
Default **Match Count**	500 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful File Deletions Alert	
Alert is triggered when ...	... a large number of files are successfully deleted.
Configuration	None required
Enabled by Default	No
Default **Match Count**	500 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful File Modifications Alert	
Alert is triggered when ...	... a large number of files are successfully modified.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1000 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful Resource Access Alert	
Alert is triggered when ...	... a large number of successful resource access attempts occur. For example, the successful creation of an excessive number of ssh tunnels.
Configuration	None required
Enabled by Default	No

PCI Requirement 10 - Excessive Successful Resource Access Alert	
Default **Match Count**	50 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful User Actions Alert	
Alert is triggered when ...	... a large number of successful actions occur by non-administrative user accounts. This alert is triggered for any accounts that are *not* listed as an administrative account in the alert.
Configuration	Change the set of default administrative accounts defined in this alert, to reflect the administrative accounts used at your site: • admin • root • super • sa<space> • sys<space> • system • manager For more information, see "Configure the Administrative Accounts for the Alert" on page 83.
Enabled by Default	No
Default **Match Count**	2000 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Excessive Successful User Logins Alert	
Alert is triggered when ...	... a large number of successful logins by non-administrative user accounts occur. This alert is triggered for any accounts that are *not* listed as an administrative account in the alert.

PCI Requirement 10 - Excessive Successful User Logins Alert	
Configuration	Change the set of default administrative accounts defined in this alert, to reflect the administrative accounts used at your site: • admin • root • super • sa<space> • sys<space> • system • manager For more information, see "Configure the Administrative Accounts for the Alert" on page 83.
Enabled by Default	No
Default **Match Count**	30 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Microsoft Audit Log Cleared (including Windows 2008) Alert	
Alert is triggered when ...	... the Microsoft Audit Log is cleared. This alert is triggerd for both Windows 2003 and Windows 2008 events.
Configuration	None required
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	120 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Virtual Machine Down Alert	
Alert is triggered when ...	...a virtual machine is powered off or suspended.

PCI Requirement 10 - Virtual Machine Down Alert	
Configuration	1 Edit the alert and change the following query `^CEF:0|.*|(VirtualCenter 4.1|ESX|VProduct)|` by replacing `VirtualCenter 4.1|ESX|VProduct` with a list of the virtual device products in your environment. The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, change the alert query conditions to match events from these products, or configure the connector to change the categorization of the specific events to match the alert query conditions.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	120 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Virtual Machine Modifications Alert	
Alert is triggered when ...	...virtual machine modifications occur (including deletions and relocations).
Configuration	1 Edit the alert and change the following query `^CEF:0|.*|(VirtualCenter 4.1|ESX|VProduct)|` by replacing `VirtualCenter 4.1|ESX|VProduct` with a list of the virtual device products in your environment. The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, change the alert query conditions to match events from these products, or configure the connector to change the categorization of the specific events to match the alert query conditions.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	120 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Virtual Machine Data Manipulations Alert	
Alert is triggered when ...	...manipulation of virtual machine data (images, snapshots, and so on) occurs.

PCI Requirement 10 - Virtual Machine Data Manipulations Alert	
Configuration	1 Edit the alert and change the following query `^CEF:0|.*|(VirtualCenter 4.1|ESX|VProduct)|` by replacing `VirtualCenter 4.1|ESX|VProduct` with a list of the virtual device products in your environment. The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, change the alert query conditions to match events from these products, or configure the connector to change the categorization of the specific events to match the alert query conditions.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	120 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 10 - Virtual Management System Alerts Alert	
Alert is triggered when ...	...alerts from virtualization management systems occur.
Configuration	1 Edit the alert and change the following query `^CEF:0|.*|(VirtualCenter 4.1|ESX|VProduct)|` by replacing `VirtualCenter 4.1|ESX|VProduct` with a list of the virtual device products in your environment. The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, change the alert query conditions to match events from these products, or configure the connector to change the categorization of the specific events to match the alert query conditions.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	120 - See "Match Count and Threshold (Sec) Fields" on page 26.

Configure the Administrative Accounts for the Alert

Some PCI Requirement 10 alerts contain conditions that define a set of default administrative accounts. For each of these alerts, the following administrative accounts are defined by default:

- `admin`
- `root`
- `super`

- sa<space>
- sys<space>
- system
- manager

Where <space> represents the space character.

For each alert you plan on enabling, customize the set of administrative accounts in each alert, to reflect the set of administrative accounts used at your site.

Edit the alert and in the Query Terms field that lists the default administrative account names, change the set of default administrative accounts to reflect the set of administrative accounts used at your site. For example, add the CTXSYS account name to the user list:

```
(duser|suser)=(admin|root|super|sa |sys |system|manager|CTXSYS)
```

Separate the user names using the pipe character (|). The pipe character represents an OR operator.

All account names are case insensitive. An alert triggers if the account name in the incoming PCI event matches one of the defined administrative accounts and the other conditions in the alert are satisfied.

A account name matches if the name starts with the same set of characters as one of the defined administrative accounts—additional characters at the end of the account name are allowed. For example, the account name Administrator matches the account name admin. This type of pattern matching does not occur with the sys<space> and sa<space> account names because these account names are specified with a space at the end of the name. For example, the account name sarah does not match the sa<space> account name.

Requirement 10 Reports

The Logger PCI Requirement 9 Reports leverage many system logs to report on different types of log activity, including failed log-ins or access to resources, user authentications and authorizations, audit log management and audit trails, and clock synchronization.

Requirement 10-Account Creation Report	
PCI Section	10.2.7
Description	This report shows user account creations on any type of system sorted by zone and time.
Requirement Support	This report provides evidence of logging access to system level objects.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that creation and deletion of system level objects are logged into system activity logs.
Configuration	None required.

Requirement 10-Account Deletion Report	
PCI Section	10.2.7
Description	This report shows user account deletions from any type of system sorted by zone and time.
Requirement Support	This report provides evidence of logging access to system level objects.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that creation and deletion of system level objects are logged into system activity logs.
Configuration	None required.

Requirement 10-Administrative Actions Report	
PCI Section	10.2.2
Description	This report shows all event names of actions involving the administrator user (except logins), sorted by device. It also shows the last time the event happened. Administrative users are defined as admin, administrator, root, superuser, super. The default administrator names should be modified according to the actual administrator user names in the site, in which case this report will show all administrative actions (except logins).
Requirement Support	This report provides evidence of logging actions taken by administrative users.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that actions taken by any individual with root or administrative privileges are logged into system activity logs.
Configuration	Configure the *PCI 10-Administrative Actions* query as needed with the names of the admin accounts used at your site. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Requirement 10-Administrative Logins - All Report	
PCI Section	10.2.5
Description	This report shows all administrative logins to systems. It shows the system to which the login was attempted, the outcome of the attempt, the number of times the attempt happened, and the last time it happened. Administrative users are defined as admin, administrator, root, superuser, super. These administrative user names should be changed to the actual administrator names on site.
Requirement Support	This report provides evidence of logging the use of identification and authentication mechanisms.

Requirement 10-Administrative Logins - All Report	
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that use of identification and authentication mechanisms are logged into system activity logs.
Configuration	Configure the *PCI 10-Administrative Logins - All* query as needed with the names of the admin accounts used at your site. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Requirement 10-Administrative Logins - Failed Report	
PCI Section	10.2.5
Description	This report shows all failed logins to systems performed by default administrative users. It shows the system to which the login was attempted, the number of times the attempt happened, and the last time it happened. Administrative users are defined as admin, administrator, root, superuser, super. The default administrative user names should be changed to the actual administrator names on site.
Requirement Support	This report provides evidence of logging the use of identification and authentication mechanisms.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that use of identification and authentication mechanisms are logged into system activity logs.
Configuration	Configure the *PCI 10-Administrative Logins - All* query as needed with the names of the admin accounts used at your site. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Requirement 10-Administrative Logins - Successful Report	
PCI Section	10.2.5
Description	This report shows all successful logins to systems performed by default administrative users. It shows the system to which the login was attempted, the number of times the attempt happened, and the last time it happened. Administrative users are defined as admin, administrator, root, superuser, super. The default administrative user names should be changed to the actual administrator names on site.
Requirement Support	This report provides evidence of logging the use of identification and authentication mechanisms.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that use of identification and authentication mechanisms are logged into system activity logs.
Configuration	Configure the *PCI 10-Administrative Logins - All* query as needed with the names of the admin accounts used at your site. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Requirement 10-All Detected Virtual Machine IP Addresses Report	
PCI Section	10.1
Description	This report shows the association between virtual machines and their IP addresses.
Requirement Support	This report should be reviewed to show the association between virtual machines and their IP addresses.
Testing Procedure	Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 Edit the underlying query for this report so that the DHCPAssign section captures IP address assignment events. 3 If you have virtual device products other than VMware, edit the underlying query so that the MACAssign section captures MAC Address to virtual machine assignment events. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98. 4 If you change either the MACAssign or DHCPAssign sections of the query as described in Step 2 and Step 3, modify the conditions at the bottom of the query accordingly.

Requirement 10-All Detected Virtual Machine MAC Addresses Report	
PCI Section	10.1
Description	This report shows the association between virtual machines and their MAC addresses.
Requirement Support	This report should be reviewed to show the association between virtual machines and their MAC addresses.
Testing Procedure	Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.

Requirement 10-All Detected Virtual Machine MAC Addresses Report	
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 10-All Hypervisors per Reporting Device Report	
PCI Section	10.1
Description	This report shows all hypervisors detected per reporting device.
Requirement Support	This report should be reviewed to show all virtual machine hypervisors by their respective reporting devices.
Testing Procedure	Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 10-All Virtual Machine Creation and Deletion Events Report	
PCI Section	10.2.7
Description	This report shows all virtual machine creations and deletions.

Requirement 10-All Virtual Machine Creation and Deletion Events Report	
Requirement Support	This report should be reviewed to see events that describe the creation and deletion of virtual machines.
Testing Procedure	Verify that the creation and deletion of system level objects are logged.
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 10-All Virtual Machine Data Manipulations Report	
PCI Section	10.2.7
Description	This report shows all manipulations of virtual machine data (images, snapshots, datastore, and so on).
Requirement Support	This report should be reviewed to see all manipulations of virtual machine data (for example, images, snapshots, and datastores). These manipulations also include creation and deletion events.
Testing Procedure	Verify that creation and deletion of system level objects are logged.
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 10-All Virtualization Infrastructure Events Report	
PCI Section	10.1
Description	This report shows all events from virtualization infrastructure systems.
Requirement Support	This report should be reviewed to make sure that events from virtualization infrastructure systems are being logged.
Testing Procedure	Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 10-Authorization Changes Report	
PCI Section	10.2.5
Description	This report shows authorization privilege changes made on systems and the number of times these events happened per host name.
Requirement Support	This report provides evidence of logging changes to the identification and authentication mechanisms.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that use of identification and authentication mechanisms are logged into system activity logs.
Configuration	None required.

Requirement 10-Clock Synchronization Problems Report	
PCI Section	10.4

Requirement 10-Clock Synchronization Problems Report	
Description	This report shows all ArcSight SmartConnectors that report inaccurate times. This might be an indication of clocks that are not synchronized with each other in the logging infrastructure and thus affect the credibility of data access reports.
Requirement Support	Entries in this report may indicate clock synchronization issues and possible failure to distribute the correct time within the organization.
Testing Procedure	Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points.
Configuration	None required.

Requirement 10-Database Access - All Report	
PCI Section	10.4
Description	This report shows all login attempts to all database systems.
Requirement Support	This report provides evidence of database access logins.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that all individual access to cardholder data is logged into system activity logs.
Configuration	None required.

Requirement 10-Database Access - Failed Report	
PCI Section	10.2.1
Description	This report shows all failed login attempts made to database systems.
Requirement Support	This report provides evidence of and audit trail of individual access to cardholder data.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that all individual access to cardholder data is logged into system activity logs.
Configuration	None required.

The *Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices* report provides access to drill-down reports as described in Figure C-7 on page 138.

Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices Report	
PCI Section	10.1

Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices Report	
Description	This report shows all virtual machines that have been detected along with information about their respective hypervisors.
Requirement Support	This report shows all virtual machines that have been detected so far along with information about their hypervisors.
Testing Procedure	Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 10-File Creation Attempts Report	
PCI Section	10.5.5
Description	This report shows attempts to create files. It displays the machine on which the file creation attempt occurred, the outcome of the attempt, the user involved, the name of the file, and how many times the attempt happened.
Requirement Support	Supporting Evidence that logging and file integrity monitoring are enabled and monitored.
Testing Procedure	Verify the use of file integrity monitoring or change detection software for logs by examining system settings and monitored files and results from monitoring activities.
Configuration	None required.

Requirement 10-File Deletion Attempts Report	
PCI Section	10.5.5
Description	This report shows attempts to delete files. It displays the machine on which the deletion attempt occurred, the outcome of the attempt, the user involved, the name of the file, and how many times the attempt happened.

Requirement 10-File Deletion Attempts Report	
Requirement Support	Supporting Evidence that logging and file integrity monitoring are enabled and monitored.
Testing Procedure	Testing Procedure 10.5.5: Verify the use of file integrity monitoring or change detection software for logs by examining system settings and monitored files and results from monitoring activities
Configuration	None required.

Requirement 10-File Manipulations - All Report	
PCI Section	10.5.5
Description	This report displays all attempts to access, modify or delete files. It is sorted according to zone/host, reporting device and time.
Requirement Support	Supporting Evidence that logging and file integrity monitoring are enabled and monitored.
Testing Procedure	Testing Procedure 10.5.5: Verify the use of file integrity monitoring or change detection software for logs by examining system settings and monitored files and results from monitoring activities
Configuration	None required.

Requirement 10-File Modification Attempts Report	
PCI Section	10.5.5
Description	This report shows attempts to modify files. It displays the machine on which the file modification attempt occurred, the outcome of the attempt, the user involved, the name of the file, and how many times the attempt happened.
Requirement Support	Supporting Evidence that logging and file integrity monitoring are enabled and monitored.
Testing Procedure	Verify the use of file integrity monitoring or change detection software for logs by examining system settings and monitored files and results from monitoring activities
Configuration	None required.

Requirement 10-Microsoft Audit Log Cleared Report	
PCI Section	10.5.2 / 10.5.5 / 10.2.6
Description	This report shows the clearing of windows audit logs, which should usually not be done and could indicate a security problem.
Requirement Support	Clearing the audit log can indicate unauthorized modification to audit trail files.

Requirement 10-Microsoft Audit Log Cleared Report	
Testing Procedure	Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.
Configuration	None required.

The *Requirement 10-Number of Hypervisors Detected per Reporting Device* report provides access to drill-down reports as described in Figure C-8 on page 138.

Requirement 10-Number of Hypervisors Detected per Reporting Device Report	
PCI Section	10.1
Description	This report shows the number of detected hypervisors per reporting device.
Requirement Support	This report should be reviewed to show the number of virtual machine hypervisors by their respective reporting devices.
Testing Procedure	Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

The *Requirement 10-Number of Virtual Machines by Reporting Device and Hypervisor* report provides access to drill-down reports as described in Figure C-9 on page 138.

Requirement 10-Number of Virtual Machines by Reporting Device and Hypervisor Report	
PCI Section	10.1
Description	This report shows the detected number of virtual machines by their respective hypervisors and reporting devices.
Requirement Support	This report should be reviewed to show all virtual machine hypervisors by their respective reporting devices.
Testing Procedure	Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.

Requirement 10-Number of Virtual Machines by Reporting Device and Hypervisor Report	
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 10-Resource Access - Failed Report	
PCI Section	10.2.4
Description	This report shows failed attempts to access resources systems (except for failed logins which are shown in a separate report) that happened in the report time frame, the number of times these failures occurred, and the last time they occurred. The report is sorted by zone, host and time.
Requirement Support	This report provides evidence of failed access to resources (except for logins).
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that invalid logical access attempts are logged into system activity logs.
Configuration	None required.

Requirement 10-Top Hypervisors with the Most VM Activities Report	
PCI Section	10.1
Description	This report shows the top 10 hypervisors with the most virtual machine activities (powered on, off, suspension, and so on).
Requirement Support	This report should be reviewed to determine the top 10 virtualization hypervisors with the most virtual machine activities (power on, power off, suspension, and so on).
Testing Procedure	Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.

Requirement 10-Top Hypervisors with the Most VM Activities Report	
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 10-Top Hypervisors with the Most VM Creations Report	
PCI Section	10.2.7
Description	This report shows the top 10 virtualization hypervisors with the most virtual machine creations.
Requirement Support	This report should be reviewed to determine the top 10 hypervisors with the most virtual machine creations.
Testing Procedure	Verify that the creation and deletion of system level objects are logged.
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 10-Top Users with the Most VM Activities Report	
PCI Section	10.1

Requirement 10-Top Users with the Most VM Activities Report	
Description	This report shows the top 10 users with the most virtual machine activities (power on, power off, suspension, and so on).
Requirement Support	This report should be reviewed to determine the top 10 users with the most virtual machine activities (power on, power off, suspension and so on).
Testing Procedure	Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.
Configuration	1 Specify the virtual device products used in your environment. Edit the Default Value field of the pciVirtualizationProducts parameter and specify a quoted, comma separated list of device products, for example: `'VirtualCenter 4.1','ESX'` The product names will be present in the Device Product event field. 2 If you have virtual device products other than VMware, either change the query conditions for this report's query to match the events from those products, or configure the connector to change the categorization of the specific events to match the conditions in this query. For information about sending events from those products to ArcSight ESM, see "Sending Virtualization Component Events to ArcSight ESM" on page 98.

Requirement 10-User Logins - All Report	
PCI Section	10.2.1
Description	This report shows all non-administrative users who attempted to log into a system. The report is sorted first by zone and then by time. A non-administrative user is one whose user name is not Admin, Administrator, root, superuser, or super. This list should be changed according to the actual administrative names on site.
Requirement Support	This report provides evidence of an audit trail of individual access to cardholder systems.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that all individual access to cardholder data is logged into system activity logs.
Configuration	Configure the *PCI 10-User Logins - All* query as needed with the names of the user accounts used at your site. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Requirement 10-User Logins - Failed Report	
PCI Section	10.2.1

Requirement 10-User Logins - Failed Report	
Description	This report shows all failed non-administrative user logins. The report is sorted first by zone and then by time. A non-administrative user is one whose user name is not Admin, Administrator, root, superuser, or super. These names should be changed according to the actual administrative user names on site.
Requirement Support	This report provides evidence of an audit trail of individual access attempts to cardholder systems.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that all individual access to cardholder data is logged into system activity logs.
Configuration	Configure the *PCI 10-User Logins - All* query as needed with the names of the user accounts used at your site. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Requirement 10-User Logins - Successful Report	
PCI Section	10.2.1
Description	This report shows all successful non-administrative user logins. The report is sorted first by zone and then by time. A non-administrative user is one whose user name is not Admin, Administrator, root, superuser, or super. This list should be changed according to the actual user names on site.
Requirement Support	This report provides evidence of an audit trail of individual access to cardholder systems.
Testing Procedure	Verify though interviews, examination of audit logs, and examination of audit log settings, that all individual access to cardholder data is logged into system activity logs.
Configuration	Configure the *PCI 10-User Logins - All* query as needed with the names of the user accounts used at your site. For instructions on modifying the query, see "Configure Reports with Site-Specific Data" on page 21.

Sending Virtualization Component Events to ArcSight ESM

The Logger CIP for PCI queries for virtualization components accommodate events from VMware, by default. If you have virtualization products other than VMware in your environment, as an optional step, you can develop a FlexConnector to parse specific events related to the virtualization components on your network. When you develop the FlexConnector, make sure that you use the following field mappings to map the key event data into the ArcSight event schema. Refer also to the instructions in the *FlexConnector Developer's Guide*.

ArcSight Field	Mapping
deviceCustomString5	The name of the virtual machine.
sourceUserName	The name of the user performing the event. Note: If only one user name appears in the event, map the name to the `destinationUserName` field, described below.

ArcSight Field	Mapping
destinationUserName	The name of the user on which the event is performed. Note: If only one user name appears in the event, map the name to this field.
sourceAddress sourceHostName	The network address (sourceAddress) or hostname (sourceHostName) from which the operation is taking place. Note: If only one address or hostname appears in the event, map the address or hostname to the destinationAddress or destinationHostName field, described below.
destinationAddress destinationHostName	The network address (destinationAddress) or hostname (destinationHostName) on which the operation is taking place. Note: If only one address or hostname appears in the event, map the address to this field. Note: For events that apply to hypervisors, map the hypervisor address to the destinationAddress field or the hypervisor hostname to the destinationHostName field.

Requirement 11: Test Systems and Networks

Requirement 11 states that companies should regularly test security systems and processes.

New vulnerabilities are discovered every day. Requirement 11 focuses on regular monitoring and testing practices to keep up with these changes over time.

- **Requirement 11: Testing Systems and Networks Alerts**
  - “PCI Requirement 11 - Suspicious Events Alert” on page 100
  - “PCI Requirement 11 - Vulnerabilities Alert” on page 100
- **Requirement 11: Testing Systems and Networks Reports**
  - “Requirement 11-All Vulnerabilities by Assets Report” on page 101
  - “Requirement 11-Attacks and Suspicious Events Overview Report” on page 101
  - “Requirement 11-HIDS Event Review by Device Report” on page 101
  - “Requirement 11-NIDS Event Review by Device Report” on page 102
  - “Requirement 11-Top 20 Vulnerabilities Report” on page 102
  - “Requirement 11-Top 20 Vulnerable Assets Report” on page 102
  - “Requirement 11-Attack in Network Report” on page 103
  - “Requirement 11-Attack on Host - Detail Report” on page 103
  - “Requirement 11-Attacks and Suspicious Events per Host Report” on page 104
  - “Requirement 11-Attacks on Host - All Report” on page 104
  - “Requirement 11-Vulnerability Count per Scanner Report” on page 104
  - “Requirement 11-Vulnerability in Network Report” on page 105

- "Requirement 11-Vulnerabilities on Host per Scanner Report" on page 105
- "Requirement 11-Vulnerabilities per Host - All Report" on page 105

Requirement 11 Alerts

Logger PCI Requirement 11 alerts notify PCI analysts when events occur that indicate suspicious behavior, hostile behavior, a compromise or vulnerabilities.

PCI Requirement 11 - Suspicious Events Alert	
Alert is triggered when ...	... occurrence of events that are categorized as suspicious behavior, hostile behavior, or a compromise.
Configuration	None required
Enabled by Default	No
Default **Match Count**	3 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

PCI Requirement 11 - Vulnerabilities Alert	
Alert is triggered when ...	... more that 10 vulnerabilities are reported in less that 5 minutes.
Configuration	None required
Enabled by Default	No
Default **Match Count**	10 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	300 - See "Match Count and Threshold (Sec) Fields" on page 26.

Requirement 11 Reports

The Logger PCI Requirement 11 Reports track vulnerabilities, attacks and suspected attacks that target PCI systems, and event reviews from network and host-based intrusion detection systems.

Conditions that cause requirement status to be non-compliant include:

- A successful attack against a PCI-related system
- Multiple failed anti-virus updates
- Non-private address used internally (NAT addresses should be used)

Requirement 11 - All Vulnerabilities by Assets report provides access to drill-down reports as described in Figure C-10 on page 138.

Requirement 11-All Vulnerabilities by Assets Report	
PCI Section	11.2
Description	This report shows all vulnerabilities on systems as reported by vulnerability scanners. The report is ordered by zone, host name, scanning device and criticality. By default, the report will show up to 10,000 assets.
Requirement Support	This report provides supporting evidence of running network vulnerability scans.
Testing Procedure	Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs.Verify that the scan process includes rescans until “clean” results are obtained.
Configuration	None required.

Requirement 11 - Attacks and Suspicious Events Overview report provides access to drill-down reports as described in Figure C-13 on page 141.

Requirement 11-Attacks and Suspicious Events Overview Report	
PCI Section	11.1a
Description	This report shows attacks and suspicious events that target PCI systems in the network. Attacks and suspicious events are defined by the `categorySignificance` field.
Requirement Support	This report provides supporting evidence of monitoring security weaknesses in the network.
Testing Procedure	Confirm by interviewing security personnel and examining relevant code, documentation, and processes that security testing of devices is in place to assure that controls identify and stop unauthorized access attempts within the cardholder environment.
Configuration	None required.

Requirement 11-HIDS Event Review by Device Report	
PCI Section	11.4
Description	This report shows all events that were triggered on HIDS systems and the number of times each event occurred.
Requirement Support	This report provides supporting evidence of running network vulnerability scans.
Testing Procedure	Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs.Verify that the scan process includes rescans until “clean” results are obtained.

Requirement 11-HIDS Event Review by Device Report	
Configuration	None required.

Requirement 11-NIDS Event Review by Device Report	
PCI Section	11.4
Description	This report shows the number of different events that were triggered on NIDS systems. The report is sorted by device.
Requirement Support	This report provides supporting evidence of running network vulnerability scans.
Testing Procedure	Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs.Verify that the scan process includes rescans until “clean” results are obtained.
Configuration	None required.

Requirement 11 - Top 20 Vulnerabilities contains access fields to the *Requirement 11-Vulnerabilities per Host* and *Requirement 11 - Vulnerability Count per Scanner* drill-down reports.

Requirement 11-Top 20 Vulnerabilities Report	
PCI Section	11.2
Description	This report shows the 20 most common vulnerabilities on systems, the number of systems on which they are found, and additional information regarding the vulnerability.
Requirement Support	This report provides supporting evidence of running network vulnerability scans.
Testing Procedure	Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs.Verify that the scan process includes rescans until “clean” results are obtained.
Configuration	None required.

Requirement 11-Top 20 Vulnerable Assets Report	
PCI Section	11.2
Description	This report shows the 20 systems with the most vulnerabilities as reported by vulnerability scanners.
Requirement Support	This report provides supporting evidence of running network vulnerability scans.

Requirement 11-Top 20 Vulnerable Assets Report	
Testing Procedure	Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs.Verify that the scan process includes rescans until “clean” results are obtained.
Configuration	None required.

Requirement 11 Drill-Down Reports

The requirement 11 drill-down reports support investigation drill-down for vulnerabilities and attacks.

Requirement 11-Attack in Network Report	
PCI Section	11.1a
Description	This report was designed as a drill-down report. This report shows all the hosts on the network that were targeted by a specific attack or suspicious event, and the number of times the event targeted the host. Attacks and suspicious events are defined by the `categorySignificance` field.
Requirement Support	This report provides supporting evidence of monitoring security weaknesses in the network.
Testing Procedure	Confirm by interviewing security personnel and examining relevant code, documentation, and processes that security testing of devices is in place to assure that controls identify and stop unauthorized access attempts within the cardholder environment.
Configuration	None required.

Requirement 11-Attack on Host - Detail Report	
PCI Section	11.1a
Description	This report was designed as a drill-down report. This report details in what time a specific attack or suspicious event targeted a specific host. Attacks and suspicious events are defined by the `categorySignificance` field.
Requirement Support	This report provides supporting evidence of monitoring security weaknesses in the network.
Testing Procedure	Confirm by interviewing security personnel and examining relevant code, documentation, and processes that security testing of devices is in place to assure that controls identify and stop unauthorized access attempts within the cardholder environment.
Configuration	None required.

Requirement 11-Attacks and Suspicious Events per Host Report	
PCI Section	11.1
Description	This report shows attacks and suspicious events that target a specific PCI Host. Attacks and suspicious events are defined by the categorySignificance field.
Requirement Support	This report provides supporting evidence of monitoring security weaknesses in the network.
Testing Procedure	Confirm by interviewing security personnel and examining relevant code, documentation, and processes that security testing of devices is in place to assure that controls identify and stop unauthorized access attempts within the cardholder environment.
Configuration	None required.

Requirement 11-Attacks on Host - All Report	
PCI Section	11.1
Description	This report was designed as a drill-down report. This report details all attacks and suspicious activities that targeted a specific host. Attacks and suspicious events are defined by the categorySignificance field.
Requirement Support	This report provides supporting evidence of monitoring security weaknesses in the network.
Testing Procedure	Confirm by interviewing security personnel and examining relevant code, documentation, and processes that security testing of devices is in place to assure that controls identify and stop unauthorized access attempts within the cardholder environment.
Configuration	None required.

Requirement 11-Vulnerability Count per Scanner Report	
PCI Section	11.2a
Description	This report was designed as a drill-down report. This report shows the number of vulnerabilities found by each scanner that scanned the host.
Requirement Support	This report provides supporting evidence of running network vulnerability scans.
Testing Procedure	Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs.Verify that the scan process includes rescans until "clean" results are obtained.
Configuration	None required.

Requirement 11-Vulnerability in Network Report	
PCI Section	11.2
Description	This report was designed as a drill-down report. This report shows all the hosts with the selected vulnerability.
Requirement Support	This report provides supporting evidence of running network vulnerability scans.
Testing Procedure	Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs.Verify that the scan process includes rescans until “clean” results are obtained.
Configuration	None required.

Requirement 11-Vulnerabilities on Host per Scanner Report	
PCI Section	11.2
Description	This report was designed as a drill-down report. This report shows all the vulnerabilities on a host for a specific scanner.
Requirement Support	This report provides supporting evidence of running network vulnerability scans.
Testing Procedure	Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs.Verify that the scan process includes rescans until “clean” results are obtained.
Configuration	None required.

Requirement 11-Vulnerabilities per Host - All Report	
PCI Section	11.2a
Description	This report was designed as a drill-down report. This report shows all the vulnerabilities for a certain host name.
Requirement Support	This report provides supporting evidence of running network vulnerability scans.
Testing Procedure	Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs. Verify that the scan process includes rescans until "clean" results are obtained.
Configuration	None required.

Requirement 12: Maintain an Information Security Policy

Requirement 12 states that companies should maintain a policy that addresses information security for employees and contractors. This requirement ensures an information security policy and procedures that enable employees and contractors to uphold their responsibility in protecting sensitive cardholder data.

The following PCI Reports are provided to address PCI Requirement 12:

- **Requirement 12: Maintaining an Information Security Policy Reports**
  - "Requirement 12-All Reporting Devices Report" on page 106
  - "Requirement 12-Device to Host Event Count Report" on page 106
  - "Requirement 12-Device to Host Event Detail Report" on page 107
  - "Requirement 12-Event in Network Report" on page 107
  - "Requirement 12-Host Event Count Report" on page 108
  - "Requirement 12-Host Event Count Report" on page 108

Requirement 12 Reports

Logger PCI Requirement 12 Reports generates a list of devices that report to ArcSight Logger, and tracks the last time an event from each device was received. This supports requirement 12's purpose of maintaining up-to-date security policies by providing a current inventory of all reporting systems and their status.

Requirement 12 - All Reporting Devices contains access fields to the *Requirement 12-Device to Host Event Count* drill-down report.

Requirement 12-All Reporting Devices Report	
PCI Section	12.9.3
Description	This report shows all devices that report into Logger sorted by Device Vendor, Product, zone, and IP. It also shows the last time an event from the device was received. This can be used for inventory purposes.
Requirement Support	This report helps understand the scope of monitoring and alerting implementations.
Testing Procedure	Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.
Configuration	None required.

Requirement 12 Drill-Down Reports

The requirement 12 drill-down reports support investigation drill-down for event activity and counts by host.

Requirement 12-Device to Host Event Count Report	
PCI Section	12.9.3

Requirement 12-Device to Host Event Count Report	
Description	This report was designed as a drill-down report. This report shows the number of events per Host that a specific device reported.
Requirement Support	This report helps understand the scope of monitoring and alerting implementations.
Testing Procedure	Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.
Configuration	None required.

Requirement 12-Device to Host Event Detail Report	
PCI Section	12.9.3
Description	This report was designed as a drill-down report. This report shows all the events from a specific device that targeted a specific host.
Requirement Support	This report helps understand the scope of monitoring and alerting implementations.
Testing Procedure	Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.
Configuration	None required.

Requirement 12-Event in Network Report	
PCI Section	12.9.3
Description	This report was designed as a drill-down report. This report shows the hosts that were targeted by a specific event and the number of times they were targeted.
Requirement Support	This report helps understand the scope of monitoring and alerting implementations.
Testing Procedure	Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.
Configuration	None required.

Requirement 12-Host Event Count Report	
PCI Section	12.9.3
Description	This report was designed as a drill-down report. This report shows the number of events different events that targeted a specific host.
Requirement Support	This report helps understand the scope of monitoring and alerting implementations.
Testing Procedure	Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.
Configuration	None required.

PA-DSS Requirement 4: Log Payment Application Activity

PA-DSS Requirement 4 states that companies should log all payment application activity. The following PCI alerts and reports are provided to address PA-DSS Requirement 4:

- **Requirement 4 Log Payment Application Activity Alerts**
  - "PA-DSS 4 - Anonymous Payment Application Access to Cardholder Data Alert" on page 111
  - "PA-DSS 4 - Consecutive Invalid Payment Application Access Attempts Alert" on page 112
  - "PA-DSS 4 - Payment Application Access to Cardholder Data with no User Name Alert" on page 112
  - "PA-DSS 4 - Payment Application Access with Anonymous User Name Alert" on page 112
  - "PA-DSS 4 - Payment Application Access with No User Name Alert" on page 113
  - "PA-DSS 4 - Payment Application Audit Log Initialized Alert" on page 113
- **Requirement 4 Log Payment Application Activity Reports**
  - "PA-DSS Requirement 4 - All Administrative Actions in Payment Applications Report" on page 114
  - "PA-DSS Requirement 4 - Anonymous Access to Payment Application Report" on page 114
  - "PA-DSS Requirement 4 - Anonymous Payment Application Access to Cardholder Data Report" on page 115
  - "PA-DSS Requirement 4 - Creations and Deletions of Payment Application Objects Report" on page 115
  - "PA-DSS Requirement 4 - Details of Invalid Payment Application Access Attempts" on page 115
  - "PA-DSS Requirement 4 - Individual Access to Payment Applications Report" on page 116
  - "PA-DSS Requirement 4 - Insufficient Audit Trail in Payment Application Events Report" on page 116
  - "PA-DSS Requirement 4 - Summary of Administrative Actions in Payment Applications Report" on page 117
  - "PA-DSS Requirement 4 - Summary of Invalid Payment Application Access Attempts Report" on page 117
  - "PA-DSS Requirement 4 - Summary of Payment Applications with Insufficient Audit Trail Report" on page 118

Sending Payment Application Events to ArcSight ESM

To send payment application audit events to ArcSight ESM, you might need to create payment application FlexConnectors. When you develop the FlexConnectors, make sure that you use the following field mappings to map the key event data into the ArcSight event schema. Refer also to the instructions in the *FlexConnector Developer's Guide*.

ArcSight Field	Mapping
deviceProduct	The name of the application.
deviceVendor	The application vendor.

ArcSight Field	Mapping
sourceUserName	The name of the user performing the event. For example, if user A is changing the access permissions for user B within the payment application, map user A to the `sourceUserName` field. Note: If only one user name appears in the event, map the name to the `destinationUserName` field, described below.
destinationUserName	The name of the user on which the event is performed. For example, if user A is changing the access permissions for user B within the payment application, map user B to the `destinationUserName` field. Note: If only one user name appears in the event, map the name to this field.
sourceAddress	The network address from which the operation is taking place. For example, if a user with address 1.1.1.1 logs into address 2.2.2.2, map 1.1.1.1 to the `sourceAddress` field. Note: If only one address appears in the event, map the address to the `destinationAddress` field, described below.
destinationAddress	The network address on which the operation is taking place. For example, if a user with address 1.1.1.1 logs into address 2.2.2.2, map 2.2.2.2 to the `destinationAddress` field. Note: If only one address appears in the event, map the address to this field.

Use the following event categories for the event types listed:

It is a PA-DSS requirement to indicate the outcome in every event.

Event type	Behavior	Device Group	Outcome	Significance
Successful login to the application	/Authentication/ Verify	/Payment Application	/Success	/Informational
Failed login to the application	/Authentication/ Verify	/Payment Application	/Failure	/Informational

Event type	Behavior	Device Group	Outcome	Significance
An object was created in the payment application (Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error)	/Create	/Payment Application	/Success	/Informational
An object was deleted in the payment application (Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error)	/Delete	/Payment Application	/Success	/Informational

PA-DSS Requirement 4 Alerts

The Logger PA-DSS Requirement 4 alerts notify PCI analysts of events that indicate problems with payment application activity.You can configure the alert queries as described in the following tables.

PA-DSS 4 - Anonymous Payment Application Access to Cardholder Data Alert	
Alert is triggered when ...	...an anonymous user attempts to access cardholder data via a payment application.
Configuration	1 Edit the alert and change the query `^CEF:0|.*|(PAYMENT_APP_1|PAYMENT_APP_2)|` to specify the payment applications to be monitored. 2 Change the query `dst=CDE_ADDRESSES` to indicate the destination addresses of the cardholder systems. For more information, see "Customizing PCI Alerts with Regular Expressions" on page 26.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	120 - See "Match Count and Threshold (Sec) Fields" on page 26.

PA-DSS 4 - Consecutive Invalid Payment Application Access Attempts Alert	
Alert is triggered when ...	... consecutive, invalid attempts to access a payment application occur.
Configuration	Edit the alert and change the query `^CEF:0|.*|(PAYMENT_APP_1|PAYMENT_APP_2)|` to specify the payment applications to be monitored. For more information, see "Customizing PCI Alerts with Regular Expressions" on page 26.
Enabled by Default	No
Default **Match Count**	7 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	60 - See "Match Count and Threshold (Sec) Fields" on page 26.

PA-DSS 4 - Payment Application Access to Cardholder Data with no User Name Alert	
Alert is triggered when ...	...an event indicates access to cardholder data via a payment application but the event has no username in it.
Configuration	Edit the alert and change the query `^CEF:0|.*|(PAYMENT_APP_1|PAYMENT_APP_2)|` to specify the payment applications to be monitored. For more information, see "Customizing PCI Alerts with Regular Expressions" on page 26.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	120 - See "Match Count and Threshold (Sec) Fields" on page 26.

PA-DSS 4 - Payment Application Access with Anonymous User Name Alert	
Alert is triggered when ...	...an anonymous user attempts to access a payment application.

PA-DSS 4 - Payment Application Access with Anonymous User Name Alert	
Configuration	Edit the alert and change the query `^CEF:0|.*|(PAYMENT_APP_1|PAYMENT_APP_2)|` to specify the payment applications to be monitored. For more information, see "Customizing PCI Alerts with Regular Expressions" on page 26.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	120 - See "Match Count and Threshold (Sec) Fields" on page 26.

PA-DSS 4 - Payment Application Access with No User Name Alert	
Alert is triggered when ...	...an event that indicates access to a payment application but the event has no username in it.
Configuration	Edit the alert and change the query `^CEF:0|.*|(PAYMENT_APP_1|PAYMENT_APP_2)|` to specify the payment applications to be monitored. For more information, see "Customizing PCI Alerts with Regular Expressions" on page 26.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.
Default **Threshold (Sec)**	120 - See "Match Count and Threshold (Sec) Fields" on page 26.

PA-DSS 4 - Payment Application Audit Log Initialized Alert	
Alert is triggered when ...	...a payment application log has been initialized.
Configuration	1 Edit the alert and change the query `^CEF:0|.*|(PAYMENT_APP_1|PAYMENT_APP_2)|` to specify the payment applications to be monitored. 2 Change the query `|AUDIT_LOG_INITIALIZED|` to indicate the name of the event that identifies audit log initialization.
Enabled by Default	No
Default **Match Count**	1 - See "Match Count and Threshold (Sec) Fields" on page 26.

PA-DSS 4 - Payment Application Audit Log Initialized Alert	
Default **Threshold (Sec)**	60 - See "Match Count and Threshold (Sec) Fields" on page 26.

PA-DSS Requirement 4 Reports

The following tables describe the reports that address PA-DSS Requirement 4.

PA-DSS Requirement 4 - All Administrative Actions in Payment Applications Report	
PA-DSS Section	4.2.2
Description	This report displays details of all actions taken by administrative users in payment applications.
Requirement Support	This report should be reviewed to analyze the details of actions taken by administrative users in payment applications.
Testing Procedure	Verify actions taken by any individual with administrative privileges to the payment application are logged.

Configuration	1 Edit the pciPaymentApplications parameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example:
	`'Internet Information Server','RealSecure'`
	2 Edit the pciAdminUsers parameter Default Value field to indicate a quoted, comma separated list of all the administrative users of the payment applications, in lowercase letters, for example:
	`'root','administrator','admin','sys'`

PA-DSS Requirement 4 - Anonymous Access to Payment Application Report	
PA-DSS Section	4.1.a
Description	This report identifies access events to payment applications in which no user name appears.
Requirement Support	This report should be reviewed to identify access events to payment applications in which no user name appears.
Testing Procedure	Examine payment application settings to verify that payment application audit trails are automatically enabled or are available to be enabled by customers.
Configuration	Edit the pciPaymentApplications parameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: `'Internet Information Server','RealSecure'`

PA-DSS Requirement 4 - Anonymous Payment Application Access to Cardholder Data Report	
PA-DSS Section	4.2.1
Description	This report shows events indicating access of payment applications to cardholder systems without proper identification of the user who is accessing the data. This is a violation of the PA-DSS.
Requirement Support	This report should be reviewed to identify access events by payment applications to cardholder systems without proper identification of the user who is accessing the data.
Testing Procedure	Verify all individual access to cardholder data through the payment application is logged.
Configuration	1 Change the conditions in the query to reflect the destination addresses or zones of systems that hold cardholder data. 2 Edit the pciPaymentApplications parameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: `'Internet Information Server','RealSecure'`

PA-DSS Requirement 4 - Creations and Deletions of Payment Application Objects Report	
PA-DSS Section	4.2.7
Description	This report shows events indicating creations and deletions of payment application objects.
Requirement Support	This report should be reviewed to identify events that indicate the creation or deletion of payment application objects.
Testing Procedure	Verify the creation and deletion of system-level objects within or by the application is logged.
Configuration	Edit the pciPaymentApplications parameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: `'Internet Information Server','RealSecure'`

PA-DSS Requirement 4 - Details of Invalid Payment Application Access Attempts	
PA-DSS Section	4.2.4
Description	This report shows details of invalid access events to payment applications.

PA-DSS Requirement 4 - Details of Invalid Payment Application Access Attempts	
Requirement Support	This report should be reviewed to get details of invalid access events to payment applications.
Testing Procedure	Verify that invalid logical access attempts are logged.
Configuration	Edit the pciPaymentApplications parameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: `'Internet Information Server','RealSecure'`

PA-DSS Requirement 4 - Individual Access to Payment Applications Report	
PA-DSS Section	4.1.a
Description	This report shows events indicating successful individual access to payment applications.
Requirement Support	This report should be reviewed to identify individual access events to payment applications.
Testing Procedure	Examine payment application settings to verify that payment application audit trails are automatically enabled or are available to be enabled by customers.
Configuration	Edit the pciPaymentApplications parameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: `'Internet Information Server','RealSecure'`

PA-DSS Requirement 4 - Insufficient Audit Trail in Payment Application Events Report	
PA-DSS Section	4.3
Description	This report displays payment application events with insufficient information, as defined in the PA-DSS. It is intended to help resolve these issues.
Requirement Support	This report should be reviewed to analyze payment application events with insufficient information, as defined in the PA-DSS.

PA-DSS Requirement 4 - Insufficient Audit Trail in Payment Application Events Report	
Testing Procedure	Test the payment application and examine the payment application's audit logs and audit log settings, and, for each auditable event (from 4.2), perform the following: 4.3.1: Verify user identification is included in log entries. 4.3.2: Verify type of event is included in log entries. 4.3.3: Verify date and time stamp is included in log entries. 4.3.4: Verify success or failure indication is included in log entries. 4.3.5: Verify origination of event is included in log entries. 4.3.6: Verify identity or name of affected data, system component, or resources is included in log
Configuration	Edit the pciPaymentApplications parameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: `'Internet Information Server','RealSecure'`

PA-DSS Requirement 4 - Summary of Administrative Actions in Payment Applications Report	
PA-DSS Section	4.2.2
Description	This report displays a summary of all actions taken by administrative users in payment applications.
Requirement Support	This report should be reviewed to analyze a summary of actions taken by administrative users in payment applications.
Testing Procedure	Verify actions taken by any individual with administrative privileges to the payment application are logged.

Configuration	1 Edit the pciPaymentApplications parameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example:
	`'Internet Information Server','RealSecure'`
	2 Edit the pciAdminUsers parameter Default Value field to indicate a quoted, comma separated list of all the administrative users of the payment applications, in lowercase letters, for example:
	`'root','administrator','admin','sys'`

PA-DSS Requirement 4 - Summary of Invalid Payment Application Access Attempts Report	
PA-DSS Section	4.2.4
Description	This report shows a count of events indicating invalid access attempts to payment applications.

PA-DSS Requirement 4 - Summary of Invalid Payment Application Access Attempts Report	
Requirement Support	This report should be reviewed to get a summary of invalid access events to payment applications.
Testing Procedure	Verify invalid logical access attempts are logged.
Configuration	Edit the pciPaymentApplications parameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: `'Internet Information Server','RealSecure'`

PA-DSS Requirement 4 - Summary of Payment Applications with Insufficient Audit Trail Report	
PA-DSS Section	4.3
Description	This report displays the number of events with insufficient audit trail entries per payment application.
Requirement Support	This report should be reviewed to determine the number of events per payment application with insufficient information, as defined in the PA-DSS.
Testing Procedure	Test the payment application and examine the payment application's audit logs and audit log settings, and, for each auditable event (from 4.2), perform the following: 4.3.1: Verify user identification is included in log entries. 4.3.2: Verify type of event is included in log entries. 4.3.3: Verify date and time stamp is included in log entries. 4.3.4: Verify success or failure indication is included in log entries. 4.3.5: Verify origination of event is included in log entries. 4.3.6: Verify identity or name of affected data, system component, or resources is included in log
Configuration	Edit the pciPaymentApplications parameter Default Value field to indicate a quoted, comma separated list of all the payment applications, for example: `'Internet Information Server','RealSecure'`

Appendix A

Supported PCI Devices

This appendix provides the supported devices for PCI reports and alerts.

"Supported Devices for PCI Reports" on page 119

"Supported Devices for PCI Alerts" on page 125

The supported devices for the Logger PCI reports are listed in Table A-1 on page 120. The supported devices for Logger PCI alerts are listed in Table A-2 on page 125.

The device categories listed in the columns of Table A-1 on page 120 and Table A-2 on page 125 are capable of generating events to populate the listed reports and trigger alerts. However, it is possible that not all products in the device category will generate the required events. For example, CheckPoint NG firewalls may generate events that will populate certain reports, whereas Cisco Pix will not, even though they are both under the firewall category.

It is possible that even though a device is capable of generating certain event types, it will not do so frequently, and it may take a long time for the event to appear.

Content in the Logger PCI reports and alerts usually depends on more than just the generating device. Other factors such as zones, user names, IP addresses and so on, are part of the variety of factors that the content depends on.

For each Logger PCI report or alert, the device categories in the matrixes are not the only ones that are capable of generating events that will populate it, but are the major and most likely sources for such events.

Use the supported devices listed in Table A-1 on page 120 and Table A-2 on page 125 to determine which non-CEF enabled devices in your environment would benefit from the installation of an ArcSight SmartConnector to optimize results from Logger CIP for PCI. For more information, see the *Installing SmartConnectors to Send Events to Logger* topic in the in the *ArcSight Logger™ Online Help* or the *ArcSight Logger™ Administrator's Guide*.

Supported Devices for PCI Reports

Table A-1 on page 120 lists the supported devices for the PCI reports.

Table A-1 Supported Devices for Reports

Report Name	APP	AV	CS, WF	DB	FW	IDM	IDS / IPS	NE	OS	PM	PSS	VA	VMS	VPN	W
Requirement 1-External to PCI System Activity - All					X			X							
Requirement 1-External to PCI Systems on Disallowed Ports					X			X							
Requirement 1-Firewall Configuration Changes					X										
Requirement 1-Network Equipment Configuration Changes								X							
Requirement 1-Open Ports by Device					X			X							
Requirement 1-PCI Systems to External - All					X			X							
Requirement 1-VPN Configuration Changes														X	
Requirement 2-Default Account Usage					X			X	X						
Requirement 3-Credit Card Numbers in Clear Text	X		X				X								
Requirement 4-Outbound Unencrypted Services					X			X							
Requirement 4-PCI Systems Providing Unencrypted Services					X			X							
Requirement 5-Anti-Virus Disabled		X							X						
Requirement 5-Detailed Anti-Virus Report		X													
Requirement 5-Detailed Anti-Virus Report per Host		X													
Requirement 5-Failed Anti-Virus Updates		X													
Requirement 5-Successful Anti-Virus Updates-Summary		X													
Requirement 5-Virus Summary By Host		X													
Requirement 5-Virus Summary By Virus		X													
Requirement 6- All Configuration Modifications to Virtual Machines Report													X		

Report Name	APP	AV	CS, WF	DB	FW	IDM	IDS/IPS	NE	OS	PM	PSS	VA	VMS	VPN	W
Requirement 6-All Configuration Changes to Virtualization Management Systems													X		
Requirement 6-Application Modifications	X			X	X	X	X		X	X				X	
Requirement 6-Device Configuration Modifications			X					X						X	
Requirement 6-Operating System Changes					X	X	X		X	X				X	
Requirement 7-Users Accessing CDE - All	X			X		X		X	X		X			X	
Requirement 8-Successful Password Changes	X			X	X		X		X					X	
Requirement 8-Windows Account Lockouts by System									X						
Requirement 8-Windows Account Lockouts by User									X						
Requirement 9-Physical Access System Account Creation											X				
Requirement 9-Physical Access System Account Deletion											X				
Requirement 9-Physical Access System Account Modification											X				
Requirement 9-Physical Facility Access Attempts											X				
Requirement 10-Account Creation	X			X	X	X	X		X	X				X	
Requirement 10-Account Deletion	X			X	X	X	X		X	X				X	
Requirement 10-Administrative Actions				X	X			X	X						
Requirement 10-Administrative Logins - All				X	X			X	X						
Requirement 10-Administrative Logins - Failed				X	X			X	X						
Requirement 10-Administrative Logins - Successful				X	X			X	X						
Requirement 10-All Detected Virtual Machine IP Addresses								X					X		
Requirement 10-All Detected Virtual Machine MAC Addresses													X		

Report Name	APP	AV	CS, WF	DB	FW	IDM	IDS/IPS	NE	OS	PM	PSS	VA	VMS	VPN	W
Requirement 10-All Hypervisors per Reporting Device													X		
Requirement 10-All Virtual Machine Creation and Deletion Events													X		
Requirement 10-All Virtual Machine Data Manipulations													X		
Requirement 10-All Virtualization Infrastructure Events													X		
Requirement 10-Authorization Changes					X	X	X	X	X	X				X	
Requirement 10-Clock Synchronization Problems	X	X	X	X	X	X	X	X	X	X	X	X		X	X
Requirement 10-Database Access - All				X		X			X						
Requirement 10-Database Access - Failed				X		X			X						
Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices													X		
Requirement 10-File Creation Attempts	X	X		X	X	X	X		X	X					
Requirement 10-File Deletion Attempts	X	X		X	X	X	X		X	X					
Requirement 10-File Manipulations - All	X	X		X	X	X	X		X	X					
Requirement 10-File Modification Attempts	X	X		X	X	X	X		X	X					
Requirement 10-Microsoft Audit Log Cleared									X						
Requirement 10-Number of Hypervisors Detected per Reporting Device													X		
Requirement 10-Number of Virtual Machines by Reporting Device and Hypervisor													X		
Requirement 10-Resource Access - Failed					X	X	X	X	X	X				X	
Requirement 10-Top Hypervisors with the Most VM Activities													X		

Report Name	APP	AV	CS, WF	DB	FW	IDM	IDS/IPS	NE	OS	PM	PSS	VA	VMS	VPN	W
Requirement 10-Top Hypervisors with the Most VM Creations													X		
Requirement 10-Top Users with the Most VM Activities													X		
Requirement 10-User Logins - All	X			X	X	X	X	X	X	X	X			X	X
Requirement 10-User Logins - Failed	X			X	X	X	X	X	X	X	X			X	X
Requirement 10-User Logins - Successful	X			X	X	X	X	X	X	X	X			X	X
Requirement 11-All Vulnerabilities by Assets												X			
Requirement 11-Attack in Network			X		X		X	X		X					X
Requirement 11-Attack on Host - Detail			X		X		X	X		X					X
Requirement 11-Attacks and Suspicious Events Overview			X		X		X	X		X					X
Requirement 11-Attacks and Suspicious Events per Host			X		X		X	X		X					X
Requirement 11-Attacks on Host - All			X		X		X	X		X					X
Requirement 11-HIDS Event Review by Device		X			X		X								
Requirement 11-NIDS Event Review by Device		X	X		X		X	X							
Requirement 11-Top 20 Vulnerabilities												X			
Requirement 11-Top 20 Vulnerable Assets												X			
Requirement 11-Vulnerabilities on Host per Scanner												X			
Requirement 11-Vulnerabilities per Host - All												X			
Requirement 11-Vulnerability Count per Scanner												X			
Requirement 11-Vulnerability in Network												X			
Requirement 12-All Reporting Devices	X	X	X	X	X	X	X	X	X	X	X	X		X	X

Report Name	APP	AV	CS, WF	DB	FW	IDM	IDS / IPS	NE	OS	PM	PSS	VA	VMS	VPN	W
Requirement 12-Device to Host Event Count	X	X	X	X	X	X	X	X	X	X	X	X		X	X
Requirement 12-Device to Host Event Detail	X	X	X	X	X	X	X	X	X	X	X	X		X	X
Requirement 12-Event in Network	X	X	X	X	X	X	X	X	X	X	X	X		X	X
Requirement 12-Host Event Count	X	X	X	X	X	X	X	X	X	X	X	X		X	X
PA-DSS 4-All Administrative Actions in Payment Applications	X														
PA-DSS 4-Anonymous Access to Payment Application	X														
PA-DSS 4-Anonymous Payment Application Access to Cardholder Data	X														
PA-DSS 4-Creations and Deletions of Payment Application Objects	X														
PA-DSS 4-Details of Invalid Payment Application Access Attempts	X														
PA-DSS 4-Individual Access to Payment Applications	X														
PA-DSS 4-Insufficient Audit Trail in Payment Application Events	X														
PA-DSS 4-Summary of Administrative Actions in Payment Applications	X														
PA-DSS 4-Summary of Invalid Payment Application Access Attempts	X														
PA-DSS 4-Summary of Payment Applications with Insufficient Audit Trail	X														

Key	
IDS = Intrusion Detection System	PM = Policy Management
IPS = Intrusion Prevention System	NE = Network Equipment
DB = Database	CS, WF = Content Security, Web Filtering
OS = Operating System	AV = Antivirus
FW = Firewall	W = Wireless
VPN = Virtual Private Network	PSS = Physical Security Systems
VA = Vulnerability Assessment	APP = Applications
IDM = Identity Management	VMS =Virtual Management Systems

Supported Devices for PCI Alerts

Table A-2 on page 125 lists the supported devices for the PCI alerts.

Table A-2 Supported Devices for Alerts

Alert Name	APP	AV	CS, WF	DB	FW	IDM	IDS/IPS	NE	OS	PM	PSS	VA	VMS	VPN	W
PCI Requirement 1 - Direct Traffic from CDE to Public Addresses Alert					X			X							
PCI Requirement 1 - Direct Traffic from Public Addresses to CDE Alert					X			X							
PCI Requirement 1 - Firewall Configuration Changes Alert					X										
PCI Requirement 1 - Network Equipment Configuration Changes Alert								X							
PCI Requirement 1 - VPN Configuration Changes Alert														X	
PCI Requirement 2 - Default Account Usage Alert					X			X	X						
PCI Requirement 3 - Credit Card Number in Clear Text Alert	X	X	X	X	X	X	X	X	X	X	X	X		X	X
PCI Requirement 3 - Credit Card Number in Clear Text (TippingPoint) Alert			X												
PCI Requirement 3 - Credit Card Number in Clear Text (Juniper) Alert			X												

Alert Name	APP	AV	CS, WF	DB	FW	IDM	IDS/IPS	NE	OS	PM	PSS	VA	VMS	VPN	W
PCI Requirement 3 - Credit Card Number in Clear Text (Reconnex) Alert			X												
PCI Requirement 3 - Credit Card Number in Clear Text (Vericept) Alert			X												
PCI Requirement 3 - Credit Card Number in Clear Text (Vontu) Alert			X												
PCI Requirement 4 - Internal Systems Running Insecure Services Alert					X			X							
PCI Requirement 4 - Internal Systems Using Insecure Public Services Alert					X			X							
PCI Requirement 5 - Failed Virus Quarantine or Clean or Deletion Alert		X													
PCI Requirement 5 - Network Traffic matching a Virus Signature is Detected Alert		X													
PCI Requirement 5 - Successful Virus Quarantine or Clean or Deletion Alert		X													
PCI Requirement 5 - Virus Discovered Alert		X													
PCI Requirement 6 - Excessive Failed Application Level Changes Alert	X			X	X	X	X		X	X				X	
PCI Requirement 6 - Excessive Failed Operating System Changes Alert					X	X	X		X	X				X	
PCI Requirement 9 - Excessive Failed Physical System Access Attempts Alert											X				
PCI Requirement 9 - Excessive Failed Physical System Account Creation or Modification Alert											X				
PCI Requirement 10 - Device Clock Synchronization Problems Alert	X	X	X	X	X	X	X	X	X	X	X	X		X	X
PCI Requirement 10 - Excessive Failed Account Creations Alert	X			X	X	X	X		X	X				X	
PCI Requirement 10 - Excessive Failed Account Deletions Alert	X			X	X	X	X		X	X				X	

Alert Name	APP	AV	CS, WF	DB	FW	IDM	IDS/IPS	NE	OS	PM	PSS	VA	VMS	VPN	W
PCI Requirement 10 - Excessive Failed Account Modifications Alert	X			X	X	X	X		X	X				X	
PCI Requirement 10 - Excessive Failed Administrative Actions Alert				X	X			X	X						
PCI Requirement 10 - Excessive Failed Administrative Logins Alert				X	X			X	X						
PCI Requirement 10 - Excessive Failed Authorization Changes Alert					X	X	X	X	X	X				X	
PCI Requirement 10 - Excessive Failed Database Access Alert				X		X			X						
PCI Requirement 10 - Excessive Failed File Creations Alert	X	X		X	X	X	X		X	X					
PCI Requirement 10 - Excessive Failed File Deletions Alert	X	X		X	X	X	X		X	X					
PCI Requirement 10 - Excessive Failed File Modifications Alert	X	X		X	X	X	X		X	X					
PCI Requirement 10 - Excessive Failed Resource Access Alert					X	X	X	X	X	X				X	
PCI Requirement 10 - Excessive Failed User Actions Alert				X	X			X	X						
PCI Requirement 10 - Excessive Failed User Logins Alert	X			X	X	X	X	X	X	X	X			X	X
PCI Requirement 10 - Excessive Successful Administrative Actions Alert				X	X			X	X						
PCI Requirement 10 - Excessive Successful Administrative Logins Alert				X	X			X	X						
PCI Requirement 10 - Excessive Successful Authorization Changes Alert					X	X	X	X	X	X				X	
PCI Requirement 10 - Excessive Successful Account Creations Alert	X			X	X	X	X		X	X				X	
PCI Requirement 10 - Excessive Successful Account Deletions Alert	X			X	X	X	X		X	X				X	
PCI Requirement 10 - Excessive Successful Account Modifications Alert	X			X	X	X	X		X	X				X	

Alert Name	APP	AV	CS, WF	DB	FW	IDM	IDS/IPS	NE	OS	PM	PSS	VA	VMS	VPN	W
PCI Requirement 10 - Excessive Successful Database Access Alert				X		X			X						
PCI Requirement 10 - Excessive Successful File Creations Alert	X	X		X	X	X	X		X	X					
PCI Requirement 10 - Excessive Successful File Deletions Alert	X	X		X	X	X	X		X	X					
PCI Requirement 10 - Excessive Successful File Modifications Alert	X	X		X	X	X	X		X	X					
PCI Requirement 10 - Excessive Successful Resource Access Alert					X	X	X	X	X	X				X	
PCI Requirement 10 - Excessive Successful User Actions Alert				X	X			X	X						
PCI Requirement 10 - Excessive Successful User Logins Alert	X			X	X	X	X	X	X	X	X			X	X
PCI Requirement 10 - Microsoft Audit Log Cleared Alert									X						
PCI Requirement 11 - Suspicious Events Alert			X		X		X	X		X					
PCI Requirement 10 - Virtual Machine Down													X		
PCI Requirement 10 - Virtual Machine Modifications													X		
PCI Requirement 10 - Virtual Machine Data Manipulations													X		
PCI Requirement 10 - Virtual Management System Alerts													X		
PCI Requirement 11 - Vulnerabilities Alert												X			
PA-DSS 4-Anonymous Payment Application Access to Cardholder Data	X														
PA-DSS 4-Consecutive Invalid Payment Application Access Attempts	X														
PA-DSS 4-Payment Application Access to Cardholder Data with no User Name	X														
PA-DSS 4-Payment Application Access with Anonymous User Name	X														

Alert Name	APP	AV	CS, WF	DB	FW	IDM	IDS/IPS	NE	OS	PM	PSS	VA	VMS	VPN	W
PA-DSS 4-Payment Application Access with No User Name	X														
PA-DSS 4-Payment Application Audit Log Initialized	X														

Key	
APP = Applications	NE = Network Equipment
AV = Antivirus	OS = Operating System
CS, WF = Content Security, Web Filtering	PM = Policy Management
DB = Database	PSS = Physical Security Systems
FW = Firewall	VA = Vulnerability Assessment
IDM = Identity Management	VMS =Virtual Management Systems
IDS = Intrusion Detection System	VPN = Virtual Private Network
IPS = Intrusion Prevention System	W = Wireless

Appendix B

Upgrade from CIP for Logger PCI v2.1

This section explains how to upgrade from Logger CIP for PCI v2.1.

"Upgrade Considerations" on page 131

"Upgrade Logger CIP for PCI on the Logger Appliance" on page 132

"Upgrade Logger CIP for PCI on the Software Logger" on page 133

"Uninstall Logger CIP for PCI" on page 133

Upgrade Considerations

Consider the following information before you upgrade:

- Upgrading to Logger CIP for PCI v3.0 requires Logger CIP for PCI v2.1 installed on ArcSight Logger v5.1 or later (either the appliance or the software).

  If you are running a version of Logger CIP for PCI prior to v2.1, you will need to upgrade to v2.1 before installing v3.0.

  For instructions on upgrading to Logger CIP for PCI v2.1, see the *Release Notes - ArcSight Compliance Insight Package PCI v2.1*.

  For instructions on upgrading ArcSight Logger, see the *Release Notes - ArcSight Logger*.

- The following queries and reports have been updated to include Windows 2008 events in addition to Windows 2003 events. During an upgrade, these queries and reports will be overwritten. If you customized the queries and reports previously, you will need to apply those customizations again.

  Queries:

  - PCI 8-Windows Account Lockouts by System
  - PCI 8-Windows Account Lockouts by User
  - PCI 10-Authorization Changes
  - PCI 10-Microsoft Audit Log Cleared

  Reports:

  - Requirement 8-Windows Account Lockouts by System
  - Requirement 8-Windows Account Lockouts by User
  - Requirement 10-Authorization Changes
  - Requirement 10-Microsoft Audit Log Cleared

  The following new alerts also reference Windows 2008 events:

- PCI Requirement 10 - Excessive Failed Authorization Changes (including Windows 2008)
- PCI Requirement 10 - Excessive Successful Authorization Changes (including Windows 2008)
- PCI Requirement 10 - Microsoft Audit Log Cleared (including Windows 2008)

- The following query and report will be overwritten because they have been updated to refer to TippingPoint, rather than Tipping Point (with an extra space). If you customized the query and report previously, you will need to apply those customizations again.
  - **Query:** PCI 3-Credit Card Numbers in Clear Text
  - **Report:** Requirement 3-Credit Card Numbers in Clear Text

  The following new alert also references TippingPoint:

  - **Alert:** PCI Requirement 3 - Credit Card Number in Clear Text (TippingPoint) - Updated
- The PCI report template, pci, will be overwritten because it has been updated to include PCI copyright information, and fields that contain the requirement description, support statement, and testing procedure for the new v3.0 reports.
- The default View Option for reports is now Multipage, as recommended in the *Logger Administrator's Guide*. However, if you upgrade from Logger for PCI v2.1, only the reports that are new or replaced in v3.0 will use the Multipage option by default. For a list of those reports, see the *Release Notes - ArcSight Compliance Insight Package PCI v3.0*.

For information about what's new in this release, see the *Release Notes - ArcSight™ Compliance Insight Package PCI v3.0*.

Upgrade Logger CIP for PCI on the Logger Appliance

1. Download the following Logger CIP for PCI ENC to the machine where you plan to log into the Logger user interface:

   `ArcSight-ComplianceInsightPackage-Logger-PCI.3.0.nnnn.0.enc`

   where `nnnn` is the four-digit build number specified in the *Release Notes ArcSight Compliance Insight Package PCI v3.0*.

2. Log into the Logger user interface. The Logger user interface is a web browser application. For detailed instructions and browser requirements, see the *Using the User Interface* topic of the *ArcSight Logger™ online Help* or *ArcSight Logger™ Administrator's Guide*.

3. From the Logger navigation bar, click **System Admin**.

4. From the left panel menu, select **License & Update**.

5. Click **Browse** to locate the file you downloaded in Step 1.

6. Click **Upload Update**.

   A dialog warning that the update process may take some time is displayed.

7. Click **OK**.

   A message indicating that the upgrade is progressing displays. Once the content of the ENC is installed, another message indicating that the upgrade succeeded displays.

After you complete the upgrade, see "Verify Logger CIP for PCI Content" on page 13.

Upgrade Logger CIP for PCI on the Software Logger

1. On the system running the software Logger, log into the system using the same user that you used to install the software version of Logger.
2. Download the following Logger CIP for PCI BIN:

   `ArcSight-ComplianceInsightPackage-Logger-PCI.3.0.nnnn.0.bin`

   where `nnnn` is the four-digit build number specified in the *Release Notes ArcSight Compliance Insight Package PCI v3.0*.
3. Go to the directory that contains the BIN file.
4. Change the permissions of BIN file to be executable:

   ```
   chmod +x ArcSight-ComplianceInsightPackage-Logger-
   PCI.3.0.nnnn.0.bin
   ```
5. Run the installer:

   `./ArcSight-ComplianceInsightPackage-Logger-PCI.3.0.nnnn.0.bin`
6. Follow the instructions provided by the installer. When prompted to choose an installation folder, enter the same directory you specified when you installed the software Logger. For example, if when installing the software Logger you specified the `/opt/logger` directory, specify `/opt/logger` as the installation folder.

   The BIN file installs the PCI reports, parameters, queries and alerts.
7. Verify that the Logger CIP for PCI content is installed. See "Verify Logger CIP for PCI Content" on page 13.

After you complete the upgrade, see "Verify Logger CIP for PCI Content" on page 13.

Uninstall Logger CIP for PCI

This section provides instructions for uninstalling Logger CIP for PCI. This section is not part of the initial configuration and is provided if you want to uninstall Logger CIP for PCI at a later date.

If you need to undeploy Logger CIP for PCI, follow the steps in this section.

The following procedure pertains to Logger v5.1.

With Logger v5.2 and later, you can delete an entire PCI category and its content. Click the **Report Explorer**, **Query Explorer**, or **Parameter Explorer**; highlight **PCI**; and then click the delete button ( ).

1. Delete each report in the PCI category:
   a. From the Reports tab, click the PCI report category to display the Logger CIP for PCI reports.
   b. For the first Requirement 1 report, click the delete button ( ). The system launches a confirmation screen verifying that you want to delete the report. Click **OK** to complete the deletion.
   c. Repeat step 1-b for every report in Logger CIP for PCI.

When the process is completed, the PCI report category should be empty, and the PCI report category will remain in the left panel menu.

2 Delete each Logger CIP for PCI query individually:

a From the main reports page, click **Queries** in the left panel menu.

b In the Queries column, scroll down to the PCI queries. Select the first PCI query: *PCI 1-External To PCI Systems* and click the delete button ().

c Repeat step 2-b for every PCI query.

d When all PCI queries have been deleted, click **Save**. Logger will display a Query Objects List with the name of every report object deleted.

3 Optionally, you can delete the parameters included in Logger CIP for PCI. Parameters do not affect system performance, but removing them ensures a clean state in case other cab files with similarly named parameters are imported at a later time.

a From the main reports page, click **Parameters** in the left panel menu.

b In the Parameters column, select each of the following Logger CIP for PCI parameters and click the delete button ().

- destinationHostName
- destinationZone
- deviceProduct
- eventName
- parameters prefixed with pci, such as pciAdminUsers

When all PCI parameters have been deleted, click **Save**. Logger will display a Parameter Objects List with the name of every report object deleted.

4 Delete each Logger CIP for PCI alert individually:

a Select **Configuration**.

b From the left panel menu, select **Alerts**.

c For each alert that is prefixed with PCI or PA-DSS, click the **Remove** () icon.

Appendix C

Drill-Down Report Reference

Some reports contain active hyperlinks to drill-down reports for additional information. This appendix provides a graphical representation of each report, its active hyperlink columns, and the drill-down reports they invoke. (For an overview of drill-down reports, see "Drill-Down Reports" on page 30.)

The figures in the following sections display a report as the root node in a tree of column names and drill-down reports. Some drill-down reports contain links to other drill-down reports and this nested relationship is shown in the figures.

Some sets of drill-down reports invoke the same report from different places in the drill-down tree. For brevity, those figures contain the text `See expanded children under [n]`, rather than repeating the information.

This appendix contains the following topics:

"Requirement 5: Anti-Virus Report Drill-Downs" on page 136

"Requirement 10: Track and Monitor Data Access Report Drill-Downs" on page 138

"Requirement 11: Test Systems and Networks Report Drill-Downs" on page 138

"Requirement 12: Maintain an Information Security Policy Report Drill-Downs" on page 145

"PA-DSS Requirement 4: Log Payment Application Activity Report Drill-Downs" on page 146

Requirement 5: Anti-Virus Report Drill-Downs

Figure C-1 Requirement 5 - Anti-Virus Disabled

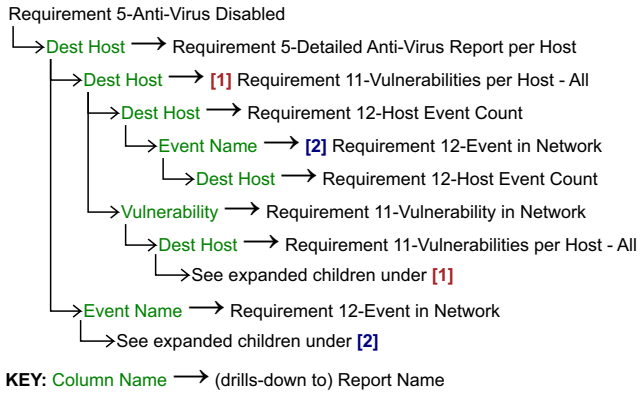


Figure C-2 Requirement 5 - Detailed Anti-Virus Report

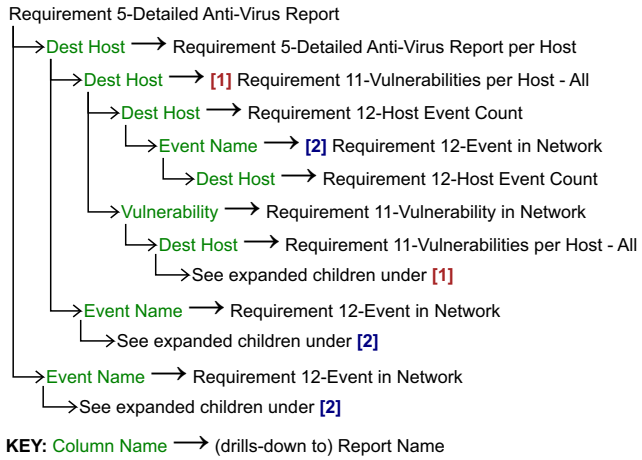


Figure C-3 Requirement 5 - Detailed Anti-Virus Report per Host

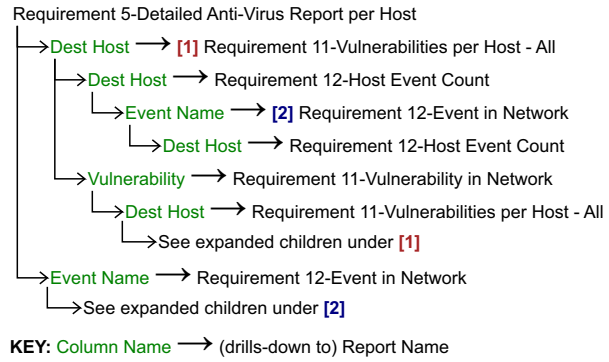


Figure C-4 Requirement 5 - Failed Anti-Virus Updates

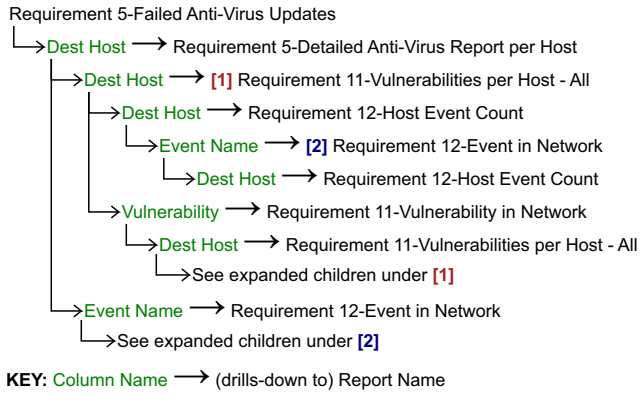


Figure C-5 Requirement 5 - Successful Anti-Virus Updates Summary

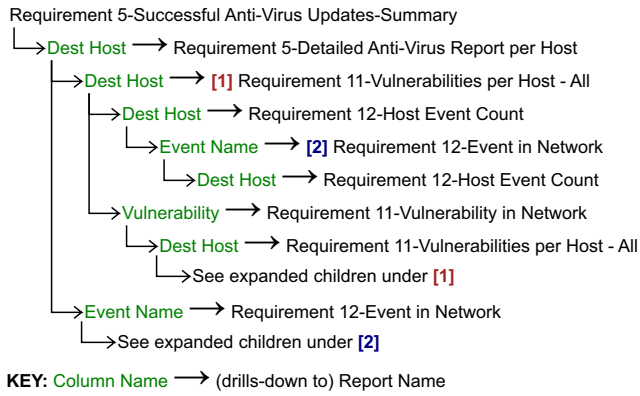
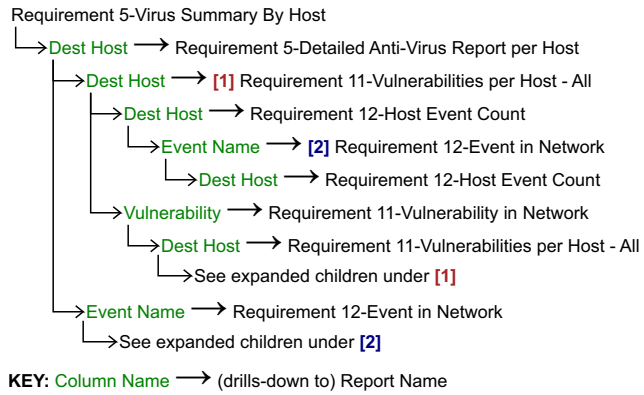


Figure C-6 Requirement 5 - Virus Summary By Host



Requirement 10: Track and Monitor Data Access Report Drill-Downs

Figure C-7 Requirement 10 - Detected Virtual Machines with their Hypervisors and Reporting Devices

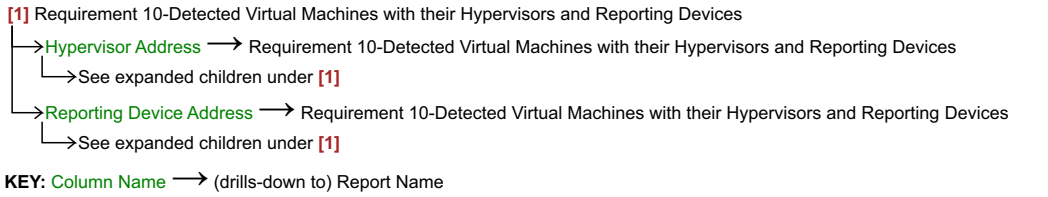


Figure C-8 Requirement 10 - Number of Hypervisors Detected per Reporting Device

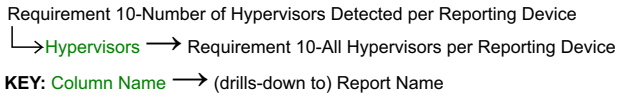
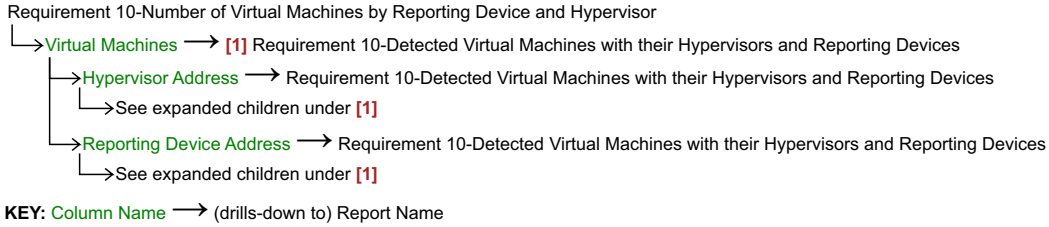


Figure C-9 Requirement 10 - Number of Virtual Machines by Reporting Device and Hypervisor



Requirement 11: Test Systems and Networks Report Drill-Downs

Figure C-10 Requirement 11 - All Vulnerabilities by Assets

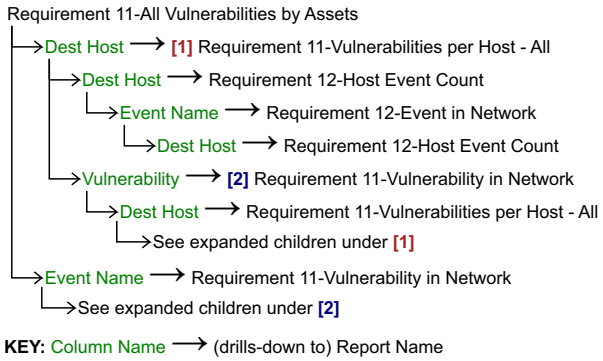


Figure C-11 Requirement 11 - Attack in Network

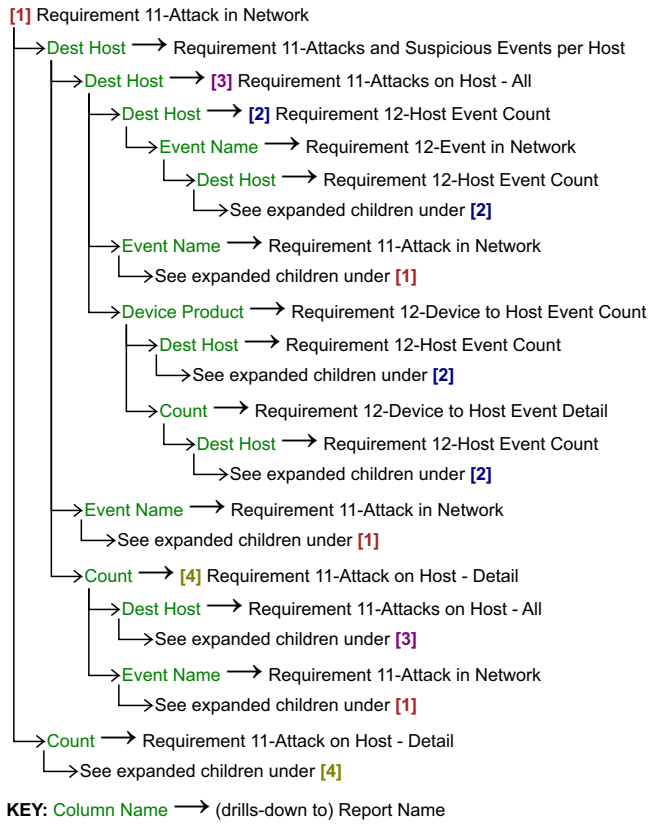


Figure C-12 Requirement 11 - Attack on Host - Detail

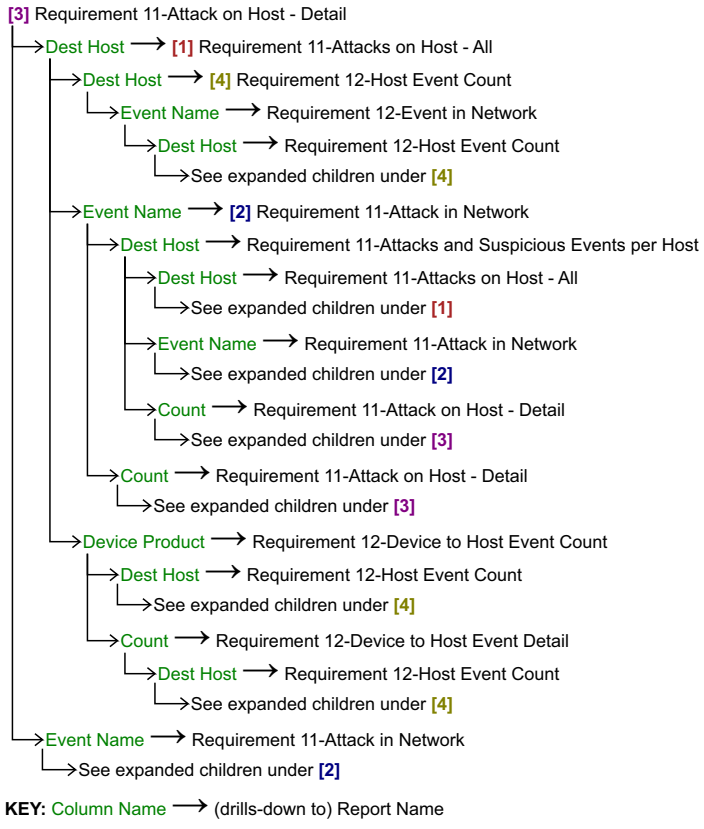


Figure C-13 Requirement 11 - Attacks and Suspicious Events Overview

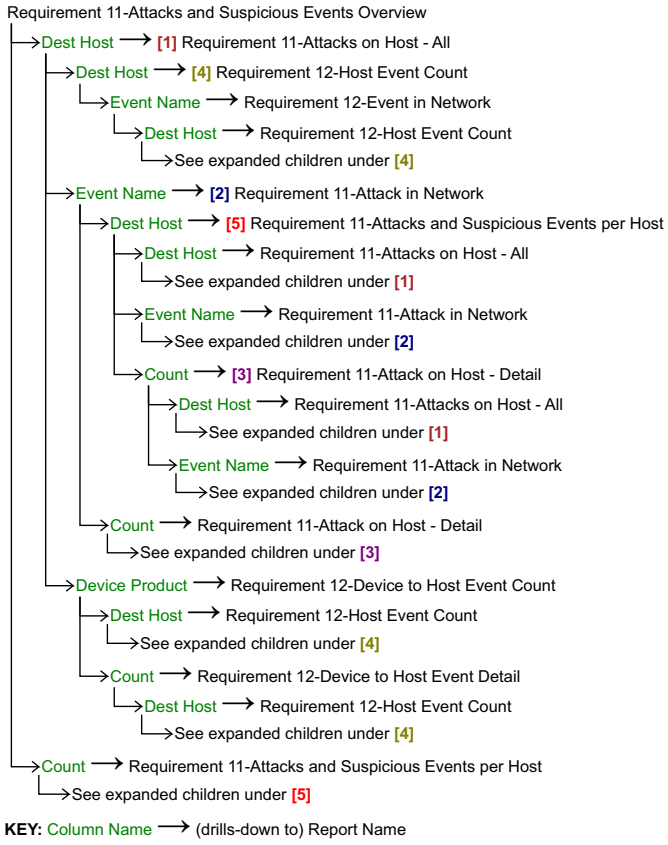


Figure C-14 Requirement 11 - Attacks and Suspicious Events per Host

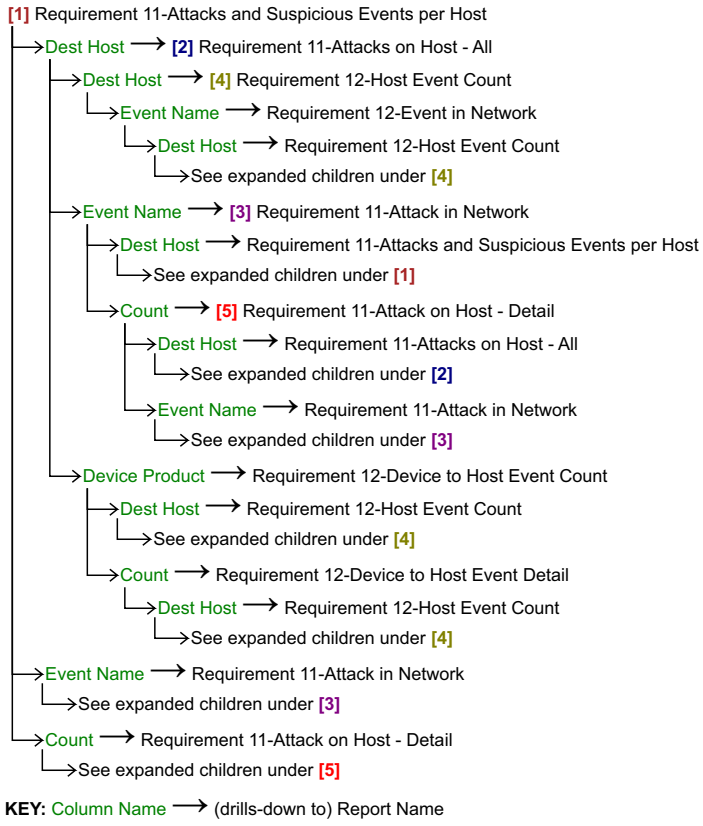


Figure C-15 Requirement 11 - Attacks on Host - All

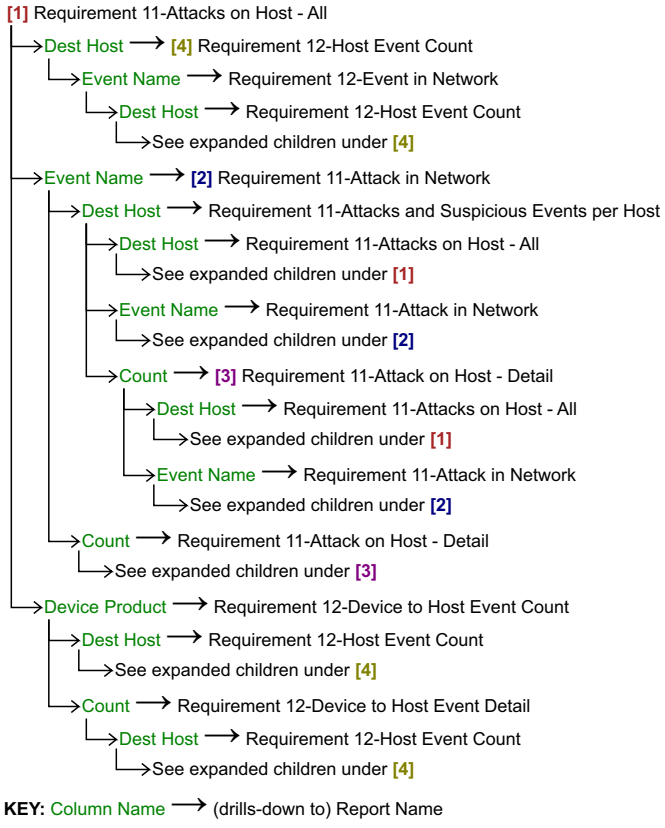


Figure C-16 Requirement 11 - Top 20 Vulnerable Assets

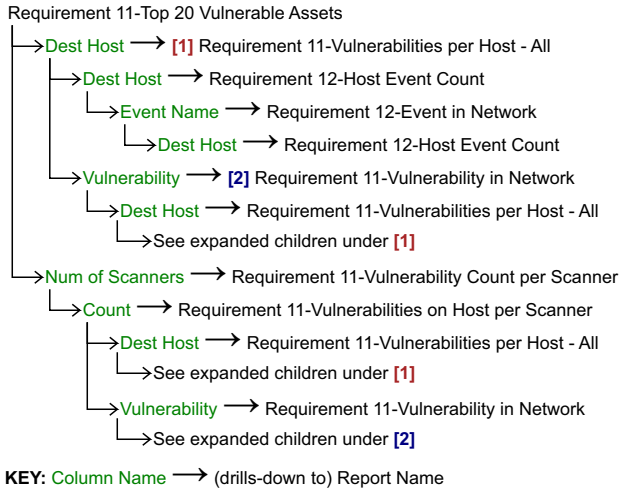


Figure C-17 Requirement 11 - Vulnerabilities on Host per Scanner

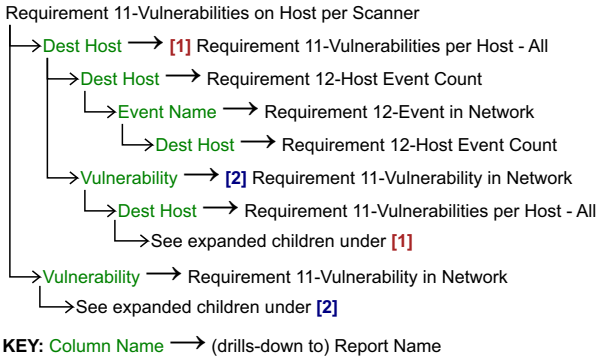


Figure C-18 Requirement 11 - Vulnerabilities per Host- All

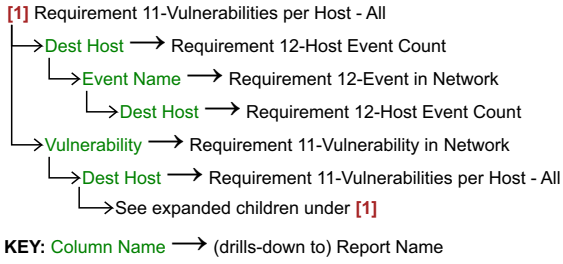


Figure C-19 Requirement 11 - Vulnerability Count per Scanner

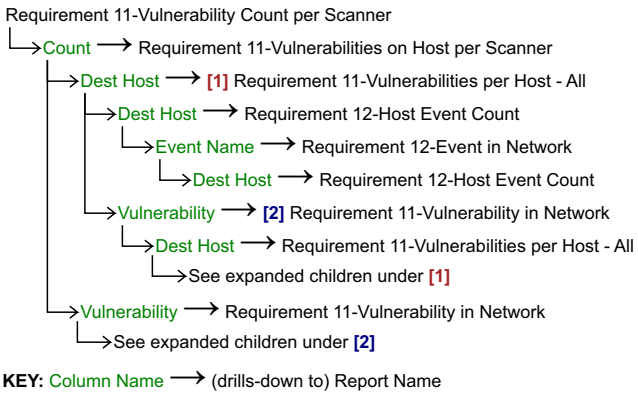
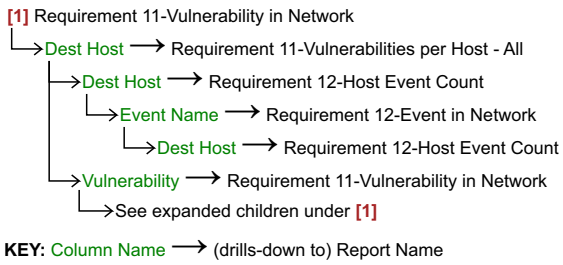


Figure C-20 Requirement 11 - Vulnerability in Network



Requirement 12: Maintain an Information Security Policy Report Drill-Downs

Figure C-21 Requirement 12 - All Reporting Devices

Figure C-22 Requirement 12 - Device to Host Event Count

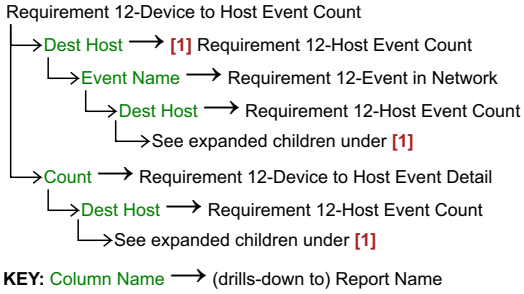


Figure C-23 Requirement 12 - Device to Host Event Detail

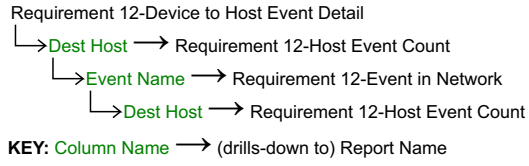


Figure C-24 Requirement 12 - Event in Network

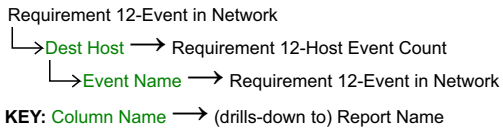
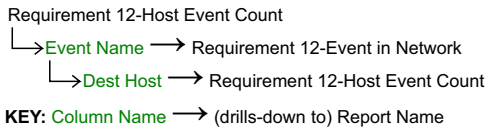


Figure C-25 Requirement 12 - Host Event Count



PA-DSS Requirement 4: Log Payment Application Activity Report Drill-Downs

Figure C-26 PA-DSS 4 - Insufficient Audit Trail in Payment Application Events

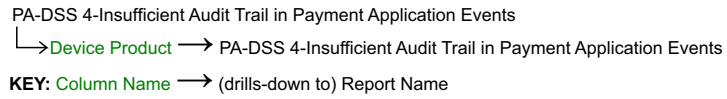


Figure C-27 PA-DSS 4 - Summary of Administrative Actions in Payment Applications

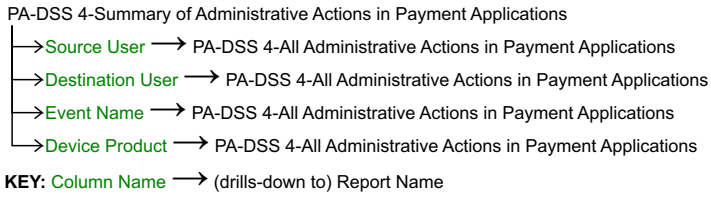


Figure C-28 PA-DSS 4 - Summary of Invalid Payment Application Access Attempts

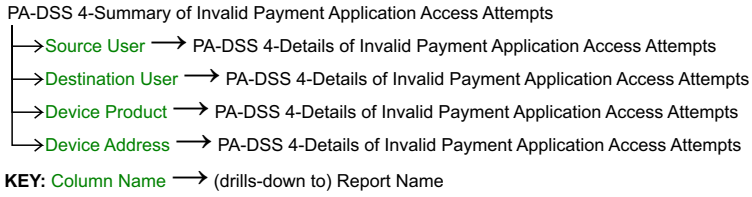
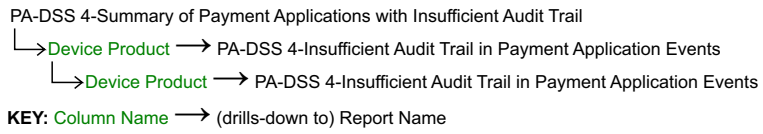


Figure C-29 PA-DSS 4 - Summary of Payment Applications with Insufficient Audit Trail



Index

Numerics

10 Hosts with Most Virus Events query 29
10 Most Attacked Hosts query 28

A

account
  creations 84
  deletions 67, 85
  lockouts 64
administrative
  actions 71, 72, 76, 85, 114, 117
  logins 76, 85, 86
adware 56
Alerts
  about PCI alerts 25
  overview of 25
  PA-DSS 4 - Anonymous Payment Application Access to Cardholder Data 111
  PA-DSS 4 - Consecutive Invalid Payment Application Access Attempts 112
  PA-DSS 4 - Payment Application Access to Cardholder Data with no User Name 112
  PA-DSS 4 - Payment Application Access with Anonymous User Name alert 112
  PA-DSS 4 - Payment Application Access with No User Name alert 113
  PA-DSS 4 - Payment Application Audit Log Initialized alert 113
  PCI Requirement 1 - Direct Traffic from CDE to Public Addresses 41, 125
  PCI Requirement 1 - Direct Traffic from Public Addresses to CDE 41, 125
  PCI Requirement 1 - Firewall Configuration Changes 42, 125
  PCI Requirement 1 - Network Equipment Configuration Changes 42, 125
  PCI Requirement 1 - VPN Configuration Changes 42, 125
  PCI Requirement 10 - Device Clock Synchronization Problems 70, 126
  PCI Requirement 10 - Excessive Failed Account Creations 70, 126
  PCI Requirement 10 - Excessive Failed Account Deletions 70, 126
  PCI Requirement 10 - Excessive Failed Account Modifications 71, 127
  PCI Requirement 10 - Excessive Failed Administrative Actions 71, 127
  PCI Requirement 10 - Excessive Failed Administrative Logins 72, 127
  PCI Requirement 10 - Excessive Failed Authorization Changes 127
  PCI Requirement 10 - Excessive Failed Authorization Changes (including Windows 2008) 72
  PCI Requirement 10 - Excessive Failed Database Access 73, 127
  PCI Requirement 10 - Excessive Failed File Creations 73, 127
  PCI Requirement 10 - Excessive Failed File Deletions 73, 127
  PCI Requirement 10 - Excessive Failed File Modifications 74, 127
  PCI Requirement 10 - Excessive Failed Resource Access 74, 127
  PCI Requirement 10 - Excessive Failed User Actions 74, 127
  PCI Requirement 10 - Excessive Failed User Logins 75, 127
  PCI Requirement 10 - Excessive Successful Account Creations 77, 127
  PCI Requirement 10 - Excessive Successful Account Deletions 77, 127
  PCI Requirement 10 - Excessive Successful Account Modifications 78, 127
  PCI Requirement 10 - Excessive Successful Administrative Actions 76, 127
  PCI Requirement 10 - Excessive Successful Administrative Logins 76, 127
  PCI Requirement 10 - Excessive Successful Authorization Changes 127
  PCI Requirement 10 - Excessive Successful Authorization Changes (including Windows 2008) 77
  PCI Requirement 10 - Excessive Successful Database Access 78, 128
  PCI Requirement 10 - Excessive Successful File Creations 78, 128
  PCI Requirement 10 - Excessive Successful File Deletions 79, 128
  PCI Requirement 10 - Excessive Successful File Modifications 79, 128
  PCI Requirement 10 - Excessive Successful Resource Access 79, 128
  PCI Requirement 10 - Excessive Successful User Actions 80, 128
  PCI Requirement 10 - Excessive Successful User Logins 80, 128
  PCI Requirement 10 - Microsoft Audit Log Cleared 81, 82, 128
  PCI Requirement 10 - Microsoft Audit Log Cleared

(including Windows 2008) 81
PCI Requirement 11 - Suspicious Events 100, 128
PCI Requirement 11 - Vulnerabilities 100, 128
PCI Requirement 2 - Default Account Usage 46, 125
PCI Requirement 3 - Credit Card Number in Clear Text 48, 125
PCI Requirement 3 - Credit Card Number in Clear Text (Juniper) 48, 125
PCI Requirement 3 - Credit Card Number in Clear Text (Reconnex) 49, 126
PCI Requirement 3 - Credit Card Number in Clear Text (TippingPoint) 48, 125
PCI Requirement 3 - Credit Card Number in Clear Text (Vericept) Alert 49, 126
PCI Requirement 3 - Credit Card Number in Clear Text (Vontu) 49, 126
PCI Requirement 4 - Internal Systems Running Insecure Services 51, 126
PCI Requirement 4 - Internal Systems Using Insecure Public Services 52, 126
PCI Requirement 5 - Failed Virus Quarantine or Clean or Deletion 54, 55, 126
PCI Requirement 6 - Excessive Failed Application Level Changes 58, 126
PCI Requirement 6 - Excessive Failed Operating System Changes 59, 126
PCI Requirement 9 - Excessive Failed Physical System Access Attempts 65, 126
PCI Requirement 9 - Excessive Failed Physical System Account Creation or Modification 65, 126
anonymous access to payment application
alerts 111, 112
reports 114, 115
anti-virus 56, 57
devices 125
events 56
listed per host 57
failed updates 56, 100
PCI requirement 53
requirement 5 53
software
disabling 55
summary of updates 56
updates 57
application configuration file
modifications 61
applications 125
ArcSight Logger 7
ArcSight SmartConnector 8
audit log settings 84, 85, 86, 90, 91, 95, 97, 98
audit logs 84, 85, 86, 90, 91, 93, 95, 97, 98
authentication verification events 66

B

badge readers 66, 67
business need-to-know
requirement 7 62

C

cardholder data 47, 67
monitor 68
cardholder data environment 41, 63
CDE 41, 63
CEF (Common Event Format) 8
CheckPoint NG firewall 119
Cisco Pix firewall 119
clear text 48, 50, 125
Common Event Format (CEF) 8
configure
logger PCI solution 14
content security, web filtering 125
credit card data systems 7
credit card information 48
credit card numbers 50
Custom Report 27

D

Data Security Standard 41, 51, 52
database 125
DDS 41
default security parameters
requirement 2 45
deploy
logger PCI solution 12, 133
Device 106
anti-virus 125
applications 125
configuration changes 61
content security, web filtering 125
database 125
firewall 125
identity management 125
intrusion detection system 125
intrusion prevention system 125
network equipment 125
operating system 125
physical security systems 125
policy management 125
supported 120, 125
virtual private network 125
vulnerability assessment 125
wireless 125
device categories 11, 119
Device Group 16, 17
Device Matrix 119
devices
CEF-ready 8
non-CEF 11
DMZ 45
drill-down reports 30
Requirement 11-Attack in Network 103
requirement 11-Attack on Host - Detail 103
Requirement 11-Attacks and Suspicious Events per Host 104
Requirement 11-Attacks on Host - All 104
Requirement 11-Vulnerabilities on Host per Scanner 105
Requirement 11-Vulnerabilities per Host - All 105
Requirement 11-Vulnerability Count per Scanner 104
Requirement 11-Vulnerability in Network 105
Requirement 12-Device to Host Event Count 106
Requirement 12-Device to Host Event Detail 107
Requirement 12-Event in Network 107
Requirement 5-Detailed Anti-Virus Report per Host

57
DSS 41, 51, 52

E

ENC file
Upload 12, 132
encrypted transmissions
requirement 4 50
enrcryption 53
Executive Report 27

F

Filters
Search Group 20
filters
PCI report category 17
firewall
125
firewalls
CheckPoint NG 119
Cisco Pix 119
configuration: requirement 1 40
FlexConnector for payment application audit events 109

G

General - Executive Report report 27

H

HIDS systems 101
hypervisor reports 88, 91, 94, 95, 96, 122, 123

I

identity management 125
IDM 125
IDS 47, 48, 125
IDS reports 50
information leakage prevention systems 50
Information Monitoring System 49
intrusion detection system 48
intrusion detection systems 47, 125
intrusion prevention systems 43, 47, 48, 125
IP address report 87, 121
IPS 43, 47, 48, 125

J

Juniper 48, 125

L

log management platform 7
Logger CIP for PCI
install 12
Logger PCI
alerts 25
reports 29
logger PCI solution
configure 14
deploy 133

M

MAC address report 87, 121
maintaining an information security policy
requirement 12 106
Match Count field 26

N

network equipment 125
network resources
monitor 68
NIDS 102
non-CEF devices 11
non-encrpted credit card information 48

O

operating system 125

P

PA-DSS 4 - Consecutive Invalid Payment Application Access alert 112
PA-DSS 4 - Payment Application Access to Cardholder Data with no User Name alert 112
PA-DSS 4 - Payment Application Access with Anonymous User Name alert 112
PA-DSS 4 - Payment Application Access with No User Name alert 113
PA-DSS 4 - Payment Application Audit Log Initialized alert 113
PA-DSS Anonymous Payment Application Access to Cardholder Data alert 111
PA-DSS Requirement 4 - All Administrative Actions in Payment Applications report 114
PA-DSS Requirement 4 - Anonymous Access to Payment Application report 114
PA-DSS Requirement 4 - Anonymous Payment Application Access to Cardholder Data report 115
PA-DSS Requirement 4 - Creations and Deletions of Payment Application Objects report 115
PA-DSS Requirement 4 - Individual Access to Payment Applications report 115, 116
PA-DSS Requirement 4 - Insufficient Audit Trail in Payment Application Events report 116
PA-DSS Requirement 4 - Summary of Administrative Actions in Payment Applications report 114, 117
PA-DSS Requirement 4 - Summary of Invalid Payment Application Access Attempts report 117
PA-DSS Requirement 4 - Summary of Payment Applications with Insufficient Audit Trail report 118
parameters 134
password
changes 63
Payment Card Industry Data Security Standard 7
PCI
Storage Group 16, 17
PCI 10-Administrative Actions query 85
PCI 10-Administrative Logins - All query 86
PCI 10-User Logins - All query 97, 98
PCI 2-Default Account Usage query 47
PCI 3-Credit Card Numbers in Clear Text query 50
PCI 4-Outbound Unencrypted Communication query 53
PCI 4-PCI Systems Providing Unencrypted Services query 53

PCI alert 25
PCI alerts 25
    supported devices 125
PCI device groups
    PCI device group 17
PCI DSS 7
PCI Executive report 27
PCI report category filters 17
PCI reports
    supported devices 119
PCI Requirement 1 - Direct Traffic from CDE to Public Addresses alert 41, 125
PCI Requirement 1 - Direct Traffic from Public Addresses to CDE alert 41, 125
PCI Requirement 1 - Firewall Configuration Changes alert 42, 125
PCI Requirement 1 - Network Equipment Configuration Changes alert 42, 125
PCI Requirement 1 - VPN Configuration Changes alert 42, 125
PCI Requirement 10 - Device Clock Synchronization Problems alert 70, 126
PCI Requirement 10 - Excessive Failed Account Creations alert 70, 126
PCI Requirement 10 - Excessive Failed Account Deletions alert 70, 126
PCI Requirement 10 - Excessive Failed Account Modifications alert 71, 127
PCI Requirement 10 - Excessive Failed Administrative Actions alert 71, 127
PCI Requirement 10 - Excessive Failed Administrative Logins alert 72, 127
PCI Requirement 10 - Excessive Failed Authorization Changes (including Windows 2008) alert 72
PCI Requirement 10 - Excessive Failed Authorization Changes alert 127
PCI Requirement 10 - Excessive Failed Database Access alert 73, 127
PCI Requirement 10 - Excessive Failed File Creations alert 73, 127
PCI Requirement 10 - Excessive Failed File Deletions alert 73, 127
PCI Requirement 10 - Excessive Failed File Modifications alert 74, 127
PCI Requirement 10 - Excessive Failed Resource Access alert 74, 127
PCI Requirement 10 - Excessive Failed User Actions alert 74, 127
PCI Requirement 10 - Excessive Failed User Logins alert 75, 127
PCI Requirement 10 - Excessive Successful Account Creations alert 77, 127
PCI Requirement 10 - Excessive Successful Account Deletions alert 77, 127
PCI Requirement 10 - Excessive Successful Account Modifications alert 78, 127
PCI Requirement 10 - Excessive Successful Administrative Actions alert 76, 127
PCI Requirement 10 - Excessive Successful Administrative Logins alert 76, 127
PCI Requirement 10 - Excessive Successful Authorization Changes (including Windows 2008) alert 77
PCI Requirement 10 - Excessive Successful Authorization Changes alert 127
PCI Requirement 10 - Excessive Successful Database Access alert 78, 128
PCI Requirement 10 - Excessive Successful File Creations alert 78, 128
PCI Requirement 10 - Excessive Successful File Deletions alert 79, 128
PCI Requirement 10 - Excessive Successful File Modifications alert 79, 128
PCI Requirement 10 - Excessive Successful Resource Access alert 79, 128
PCI Requirement 10 - Excessive Successful User Actions alert 80, 128
PCI Requirement 10 - Excessive Successful User Logins alert 80, 128
PCI Requirement 10 - Microsoft Audit Log Cleared (including Windows 2008) alert 81
PCI Requirement 10 - Microsoft Audit Log Cleared alert 81, 82, 128
PCI Requirement 11 - Suspicious Events alert 100, 128
PCI Requirement 11 - Vulnerabilities alert 100, 128
PCI Requirement 2 - Default Account Usage Alert 46, 125
PCI Requirement 2 - Default Account Usage alert 46, 125
PCI Requirement 3 - Credit Card Number in Clear Text (Juniper) alert 48, 125
PCI Requirement 3 - Credit Card Number in Clear Text (Reconnex) alert 49, 126
PCI Requirement 3 - Credit Card Number in Clear Text (TippingPoint) alert 48, 125
PCI Requirement 3 - Credit Card Number in Clear Text (Vericept) alert 49, 126
PCI Requirement 3 - Credit Card Number in Clear Text (Vontu) alert 49, 126
PCI Requirement 3 - Credit Card Number in Clear Text alert 48, 125
PCI Requirement 4 - Internal Systems Running Insecure Services Alert 51, 126
PCI Requirement 4 - Internal Systems Using Insecure Public Services alert 52, 126
PCI Requirement 5 - Failed Virus Quarantine or Clean or Deletion alert 54, 126
PCI Requirement 5 - Network Traffic matching a Virus Signature is Detected alert 54, 126
PCI Requirement 5 - Successful Virus Quarantine or Clean or Deletion alert 55, 126
PCI Requirement 5 - Virus Discovered alert 55, 126
PCI Requirement 6 - Excessive Failed Application Level Changes alert 58, 126
PCI Requirement 6 - Excessive Failed Operating System Changes alert 59, 126
PCI Requirement 9 - Excessive Failed Physical System Access Attempts alert 65, 126
PCI Requirement 9 - Excessive Failed Physical System Account Creation or Modification alert 65, 126
PCI resources 33
PCI solution reports 29
performance
    improving 16
physical access
    deletion of accounts 67
    procedures 66
    requirement 9 65
physical security systems 125
policy management 125
protecting stored data
    requirement 3 47

Q

queries 21, 31, 134
10 Hosts with Most Virus Events 29
10 Most Attacked Hosts 28
configure 21
PCI 10-Administrative Actions 85
PCI 10-Administrative Logins - All 86
PCI 10-User Logins - All 97, 98
PCI 2-Default Account Usage 47
PCI 3-Credit Card Numbers in Clear Text 50
PCI 4-Outbound Unencrypted Communication 53
PCI 4-PCI Systems Providing Unencrypted Services 53
Top 10 Users Accessing DB 28
Top 10 Vulnerabilities 28

R

Reconnex 49, 126
regular expressions
PCI alerts 26
report 114
reports
access
Requirement 11-All Vulnerabilities by Assets 101
Requirement 11-Attacks and Suspicious Events Overview 101
Requirement 11-Top 20 Vulnerabilities 102
Requirement 12-All Reporting Devices 106
Requirement 5-Anti-Virus Disabled 55
Requirement 5-Detailed Anti-Virus Report 56
Requirement 5-Failed Anti-Virus Updates 56
Requirement 5-Successful Anti-Virus Updates-Summary 56
Requirement 5-Virus Summary By Host 57
anatomy 30
Custom 27
drill-down 30
Requirement 11-Attack in Network 103
requirement 11-Attack on Host - Detail 103
Requirement 11-Attacks and Suspicious Events per Host 104
Requirement 11-Attacks on Host - All 104
Requirement 11-Vulnerabilities on Host per Scanner 105
Requirement 11-Vulnerabilities per Host - All 105
Requirement 11-Vulnerability Count per Scanner 104
Requirement 11-Vulnerability in Network 105
Requirement 12-Device to Host Event Count 106
Requirement 12-Device to Host Event Detail 107
Requirement 12-Event in Network 107
Requirement 5-Detailed Anti-Virus Report per Host 57
Executive 27
General - Executive Report 27
logger PCI 29
PA-DSS Requirement 4 - Anonymous Access to Payment Application 114
PA-DSS Requirement 4 - Anonymous Payment Application Access to Cardholder Data report 115
PA-DSS Requirement 4 - Creations and Deletions of Payment Application Objects report 115
PA-DSS Requirement 4 - Individual Access to Payment Applications 115, 116
PA-DSS Requirement 4 - Insufficient Audit Trail in Payment Application Events report 116
PA-DSS Requirement 4 - Summary of Administrative Actions in Payment Applications report 117
PA-DSS Requirement 4 - Summary of Invalid Payment Application Access Attempts report 117
PA-DSS Requirement 4 - Summary of Payment Applications with Insufficient Audit Trail report 118
Requirement 10-Account Creation 84, 121
Requirement 10-Account Deletion 85, 121
Requirement 10-Administrative Actions 85, 121
Requirement 10-Administrative Logins - All 85, 121
Requirement 10-Administrative Logins - Failed 86, 121
Requirement 10-Administrative Logins - Successful 86, 121
Requirement 10-All Detected Virtual Machine IP Addresses 87, 121
Requirement 10-All Detected Virtual Machine MAC Addresses 87, 121
Requirement 10-All Hypervisors per Reporting Device Report 88, 122
Requirement 10-All Virtual Machine Creation and Deletion Events 88, 122
Requirement 10-All Virtual Machine Data Manipulations 89, 122
Requirement 10-All Virtualization Infrastructure Events 90, 122
Requirement 10-Authorization Changes 90, 122
Requirement 10-Clock Synchronization Problems 90, 122
Requirement 10-Database Access - All 91, 122
Requirement 10-Database Access - Failed 91, 122
Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices 91, 122
Requirement 10-File Creation Attempts 92, 122
Requirement 10-File Deletion Attempts 92, 122
Requirement 10-File Manipulations - All 93, 122
Requirement 10-File Modification Attempts 93, 122
Requirement 10-Microsoft Audit Log Cleared 93, 122
Requirement 10-Number of Hypervisors Detected per Reporting Device 94, 122
Requirement 10-Number of Virtual Machines by Reporting Device and Hypervisor Report 94, 122
Requirement 10-Resource Access - Failed 95, 122
Requirement 10-Top Hypervisors with Most VM Activities 95, 122
Requirement 10-Top Hypervisors with Most VM Creations 96, 123
Requirement 10-Top Users with the Most VM Activities 96, 123
Requirement 10-User Logins - All 97, 123
Requirement 10-User Logins - Failed 97, 123

Requirement 10-User Logins - Successful 98, 123
Requirement 11-All Vulnerabilities by Assets 101, 123
Requirement 11-Attack in Network 103, 123
Requirement 11-Attack on Host - Detail 123
requirement 11-Attack on Host - Detail 103
Requirement 11-Attacks and Suspicious Events Overview 101, 123
Requirement 11-Attacks and Suspicious Events per Host 104, 123
Requirement 11-Attacks on Host - All 104, 123
Requirement 11-HIDS Event Review by Device 101, 123
Requirement 11-NIDS Event Review by Device 102, 123
Requirement 11-Top 20 Vulnerabilities 102, 123
Requirement 11-Top 20 Vulnerable Assets 102, 123
Requirement 11-Vulnerabilities on Host per Scanner 105, 123
Requirement 11-Vulnerabilities per Host - All 123
Requirement 11-Vulnerability Count per Scanner 123
Requirement 11-Vulnerability in Network 105, 123
Requirement 12-All Reporting Devices 106, 123
Requirement 12-Device to Host Event Count 106, 124
Requirement 12-Device to Host Event Detail 107, 124
Requirement 12-Event in Network 107, 124
Requirement 12-Host Event Count 108, 124
Requirement 1-External to PCI System Activity - All 43, 120
Requirement 1-External to PCI Systems on Disallowed Ports 43, 120
Requirement 1-Firewall Configuration Changes 43, 120
Requirement 1-Network Equipment Configuration Changes 44, 120
requirement 1-Network Equipment Configuration Changes 44
Requirement 1-Open Ports by Device 44, 120
Requirement 1-PCI Systems to External - All 44, 120
Requirement 1-VPN Configuration Changes 45, 120
Requirement 2-Default Account Usage 47, 120
Requirement 3-Credit Card Numbers in Clear Text 50, 120
Requirement 4-Outbound Unencrypted Services 52, 120
Requirement 4-PCI Systems Providing Unencrypted Services 53, 120
Requirement 5-Anti-Virus Disabled 55, 120
Requirement 5-Detailed Anti-Virus Report 56, 120
Requirement 5-Detailed Anti-Virus Report per Host 57, 120
Requirement 5-Failed Anti-Virus Updates 56, 120
Requirement 5-Successful Anti-Virus Updates-Summary 56, 120
Requirement 5-Virus Summary By Host 57, 120
Requirement 5-Virus Summary By Virus 57, 120
Requirement 6-All Configuration Changes to Virtualization Management Systems 59, 121
Requirement 6-All Configuration Modifications to Virtual Machines 60
Requirement 6-Application Modifications 61, 121
Requirement 6-Device Configuration Modifications 61, 121
Requirement 6-Operating System Changes 62, 121
Requirement 7-Users Accessing CDE - All 63, 121
Requirement 8-Successful Password Changes 63, 121
Requirement 8-Windows Account Lockouts by System 64, 121
Requirement 8-Windows Account Lockouts by User 64, 121
Requirement 9-Physical Access System Account Creation 66, 121
Requirement 9-Physical Access System Account Deletion 66, 121
Requirement 9-Physical Access System Account Modification 67, 121
Requirement 9-Physical Facility Access Attempts 67, 121
Requirement 10: tracking and monitoring data access 68
Requirement 10-Account Creation report 84
Requirement 10-Account Deletion report 85
Requirement 10-Administrative Actions report 85
Requirement 10-Administrative Logins - All report 85
Requirement 10-Administrative Logins - Failed report 86
Requirement 10-Administrative Logins - Successful report 86
Requirement 10-All Detected Virtual Machine MAC Addresses report 87, 121
Requirement 10-All Detected Virtual MachineIP Addresses report 87, 121
Requirement 10-All Hypervisors per Reporting Device Report 88, 122
Requirement 10-All Virtual Machine Creation and Deletion Events Report 88, 122
Requirement 10-All Virtual Machine Data Manipulations Report 89, 122
Requirement 10-All Virtualization Infrastructure Events report 90, 122
Requirement 10-Authorization Changes report 90
Requirement 10-Clock Synchronization Problems report 90
Requirement 10-Database Access - All report 91
Requirement 10-Database Access - Failed report 91
Requirement 10-Detected Virtual Machines with their Hypervisors and Reporting Devices Report 91, 122
Requirement 10-File Creation Attempts report 92
Requirement 10-File Deletion Attempts report 92
Requirement 10-File Manipulations - All report 93
Requirement 10-File Modification Attempts report 93
Requirement 10-Microsoft Audit Log Cleared report 93
Requirement 10-Number of Hypervisors Detected per Reporting Device Report 94, 122
Requirement 10-Number of Virtual Machines by Reporting Device and Hypervisor Report 94, 122
Requirement 10-Resource Access - Failed report 95
Requirement 10-Top Hypervisors with Most VM Activities Report 95, 122
Requirement 10-Top Hypervisors with Most VM Creations Report 96, 123
Requirement 10-Top Users with the Most VM Activities Report 96, 123
Requirement 10-User Logins - All report 97
Requirement 10-User Logins - Failed report 97
Requirement 10-User Logins - Successful report 98
Requirement 11: testing systems and networks 99

Requirement 11-All Vulnerabilities by Assets report 101
Requirement 11-Attack in Network report 103
Requirement 11-Attack on Host - Detail report 103
Requirement 11-Attacks and Suspicious Events Overview report 101
Requirement 11-Attacks and Suspicious Events per Host report 104
Requirement 11-Attacks on Host - All report 104
Requirement 11-HIDS Event Review by Device report 101
Requirement 11-NIDS Event Review by Device report 102
Requirement 11-Top 20 Vulnerabilities report 102
Requirement 11-Top 20 Vulnerable Assets report 102
Requirement 11-Vulnerabilities on Host per Scanner report 105
Requirement 11-Vulnerabilities per Host - All reports 105
Requirement 11-Vulnerability Count per Scanner report 104
Requirement 11-Vulnerability in Network report 105
Requirement 12: maintaining an information security policy 106
Requirement 12-All Reporting Devices report 106
Requirement 12-Device to Host Event Count report 106
Requirement 12-Device to Host Event Detail report 107
Requirement 12-Event in Network report 107
Requirement 12-Host Event Count report 108
Requirement 1-External to PCI System Activity - All report 43
Requirement 1-External to PCI Systems on Disallowed Ports report 43
Requirement 1-Firewall Configuration Changes report 43
Requirement 1-Open Ports by Device report 44
Requirement 1-PCI Systems to External - All report 44
Requirement 1-VPN Configuration Changes report 45
Requirement 2: default security parameters 45
Requirement 2-Default Account Usage report 47
Requirement 3: protecting stored data 47
Requirement 3-Credit Card Numbers in Clear Text report 50
Requirement 4: encrypted transmissions 50
Requirement 4-Outbound Unencrypted Services report 52
Requirement 4-PCI Systems Providing Unencrypted Services report 53
Requirement 5: anti-virus 53
Requirement 5-Anti-Virus Disabled report 55
Requirement 5-Detailed Anti-Virus Report per Host report 57
Requirement 5-Detailed Anti-Virus Report report 56
Requirement 5-Failed Anti-Virus Updates report 56
Requirement 5-Successful Anti-Virus Updates-Summary report 56
Requirement 5-Virus Summary By Host report 57
Requirement 5-Virus Summary By Virus report 57
Requirement 6: system applications 58
Requirement 6-All Configuration Changes to Virtualization Management Systems report 59, 121
Requirement 6-All Configuration Modifications to Virtual Machines Report 60
Requirement 6-Application Modifications report 61
Requirement 6-Device Configuration Modifications report 61
Requirement 6-Operating System Changes report 62
Requirement 7: business need-to-know 62
Requirement 7-Users Accessing CDE - All report 63
Requirement 8: Unique User ID 63
Requirement 8: unique user id 63
Requirement 8-Successful Password Changes report 63
Requirement 8-Windows Account Lockouts by System report 64
Requirement 8-Windows Account Lockouts by User report 64
Requirement 9: physical access 65
Requirement 9-Physical Access System Account Creation report 66
Requirement 9-Physical Access System Account Deletion report 66
Requirement 9-Physical Access System Account Modification report 67
Requirement 9-Physical Facility Access Attempts report 67
Requirements
  1.1.6 44
  1.1.8 44, 45
  1.1.8a 43
  1.1.8b 43, 44
  1.3.6 44
  1.3.8 44
  1.4.1 43
  1.4.2 44
  10.2.1 91, 97, 98
  10.2.2 85
  10.2.4 95
  10.2.5 85, 86, 90
  10.2.6 93
  10.2.7 84, 85
  10.4 90, 91
  10.5.2 93
  10.5.5 92, 93
  11.1 104
  11.1a 103
  11.2 101, 102, 104, 105
  11.4 101, 102
  12.9.3 106, 107, 108
  2.1 47
  3.3 50
  4.1 52, 53
  5.1.1 56, 57
  5.2 55, 56
  6.4 45, 61, 62, 63
  8.5.13 64
  8.5.9 63
  9.1 66, 67
resources
  PCI 33

S

Search Group filters 20
security weaknesses
  monitoring 101
SmartConnector 119
SNMP TRAP 22, 25
spyware 56
SQL queries 21, 29
Storage Group 16, 17
supported devices 120, 125
  PCI alerts 125
  PCI reports 119

Syslog 22, 25
syslog message 8
system activity logs 86
system applications, requirement 6 58

T

testing systems and networks
    requirement 11 99
Threshold field 26
TippingPoint 48, 125
Top 10 Users Accessing DB query 28
Top 10 Vulnerabilities query 28
tracking and monitoring data access
    requirement 10 68

U

unencrypted communications 53
unique user id
    requirement 8 63
UnityOne 48
Upload ENC file 12, 132

V

Vericept 49, 126
virtual infrastructure
    alerts 83, 128
    reports 59, 90, 122
virtual machine
    alerts 81, 82, 128
    reports 60, 87, 88, 89, 91, 94, 95, 96, 121, 122, 123
virtual private network 125
virus
    detection 57
    systems infected by 57
Vontu 49, 126
VPN 125
vulnerability
    assessment 125
    scans 101

W

wireless 125
    access points 47, 56, 57, 58, 61, 62, 64, 91