# Table of Contents

**Introduction**.......................................................................................................... 1  
Overview of the Splunk App for PCI Compliance................................................. 1  
Access the Splunk App for PCI Compliance....................................................... 1  

**Using the Splunk App for PCI Compliance**....................................................... 3  
Dashboard overview.......................................................................................... 3  
PCI Compliance Posture dashboard.................................................................. 3  
Incident Review................................................................................................... 5  
Scorecards........................................................................................................... 14  
Reports.................................................................................................................. 16  
Audit dashboards.............................................................................................. 27  
Define a primary service................................................................................... 35  
Set up adaptive response actions in Splunk App for PCI Compliance............ 36  
Included adaptive response actions with Splunk App for PCI Compliance..... 38  

**Supporting dashboards**..................................................................................... 44  
Asset Center......................................................................................................... 44  
Identity Center.................................................................................................... 45  
Predictive Analytics dashboard.......................................................................... 47  

**Investigations**.................................................................................................. 50  
Investigations in Splunk App for PCI Compliance.......................................... 50  
Start an investigation in Splunk App for PCI Compliance.............................. 50  
Investigate a potential security incident on the investigation workbench in the Splunk App for PCI Compliance.............................................. 52  
Add details to an investigation in Splunk App for PCI Compliance............... 56  
Make changes to an investigation in Splunk App for PCI Compliance............ 56  
Collaborate on an investigation in Splunk App for PCI Compliance.............. 59  
Review an investigation in Splunk App for PCI Compliance.......................... 61  
Share or print an investigation in Splunk App for PCI Compliance................. 63  
Refer to your action history in Splunk App for PCI Compliance....................... 64  
Review the summary of an investigation in Splunk App for PCI Compliance... 64  
Administer and customize the investigation workbench................................. 65  
Manage and customize investigation statuses in Splunk App for PCI Compliance................................................................. 72  

# Table of Contents

**Asset and Identity Management**
- Asset and Identity Correlation ................................................. 75

**Resources**
- Search View Matrix ............................................................... 79
- Search macros ....................................................................... 81
- FAQ ...................................................................................... 93
- Learn more and get help .................................................... 93
Introduction

Overview of the Splunk App for PCI Compliance

The Splunk App for PCI Compliance provides the compliance practitioner with visibility into compliance-relevant threats found in the cardholder data environment. The Splunk App for PCI Compliance provides a top-down and bottom-up view of an organization's current PCI compliance status, allowing a compliance specialist to effectively monitor, investigate, and report on compliance with current Payment Card Industry Data Security Standards (PCI DSS).

The Splunk App for PCI Compliance uses the native search and correlation capabilities in Splunk platform, allowing PCI compliance practitioners to capture, monitor, and report on data from devices, systems, users, and applications in the cardholder data environment. With this app, analysts can quickly investigate and resolve compliance issues.

This manual is intended for PCI compliance practitioners and analysts who are responsible for monitoring, reporting, and investigating PCI DSS compliance status in cardholder data environments.

• Installation and Configuration Manual: This manual describes how to plan your PCI Compliance deployment, and then install and configure the Splunk App for PCI Compliance.

• Release Notes: What’s new in this release; features and new functionality.

Access the Splunk App for PCI Compliance

After you install the Splunk App for PCI Compliance, access it.

1. Open a web browser and navigate to Splunk Web. Make sure that the address for Splunk Web starts with HTTPS. For example, https://splunkserver:8000.
2. Type your username and password for the Splunk App for PCI Compliance.
3. Click PCI Compliance. The PCI Compliance Posture dashboard displays.
See PCI Compliance Posture dashboard in this manual.
Using the Splunk App for PCI Compliance

Dashboard overview

The dashboards in the Splunk App for PCI Compliance provide both a high-level overview of your cardholder data environment, and the ability to investigate into particular events or compliance issues. Using the navigation bar at the top of the screen, you can access the PCI Compliance Posture, Incident Review, Scorecards, Reports, and other PCI compliance dashboards and resources.

- The **PCI Compliance Posture** dashboard provides a centralized overview of your current compliance status, both overall and by PCI requirement category. This dashboard is a centralized view of your requirement status, notable events, notable events by owner, notable events by requirements, notable events by urgency, and compliance status history. Use this dashboard to monitor your PCI compliance status daily. See PCI Compliance Posture dashboard for more information.
- The **Incident Review** dashboard helps to identify threats and respond to those threats quickly. See Incident Review dashboard for more information.
- **Scorecards** provide a daily log review and the ability to monitor each of the compliance areas. See Scorecards for more information.
- **Reports** provide reporting on each of the requirement areas of PCI compliance. These are provided as templates and can be customized. See Reports for more information.
- **Audit** dashboards validate continuous monitoring of the environment. Using these dashboards you can audit changes in the incident review dashboard, suppressions, forwarders, search, and view. See Audit dashboards for more information.
- **Resources** - Use the Asset Center to identify assets included in your cardholder data environment, and the Identity Center to identify the identities.
- **Search**: A freeform search view is included to use for manual searches of your data.

PCI Compliance Posture dashboard

The **PCI Compliance Posture** scorecard provides a summary of how compliant you are in each of the major PCI data security standards (DSS) requirements.
based on the data you are collecting in your environment. The PCI data security standard requires that you monitor your log data on a daily basis to look for anomalies that can impact cardholder data within the cardholder data environment.

Use this dashboard to see the total number of new issues, open issues, and closed issues found in your PCI environment. Compare the current status with the historical trend. View a summary of each requirement to see the current status of compliance for each control section. Use this dashboard to open individual Requirement Scorecards or to view the incidents within the Incident Review dashboard. Identify the issue owners and respond efficiently.

**Compliance Status - Last 24 Hours**

This panel displays the compliance status in your environment overall.

- If there are any new issues, the status indicator will be red.
- If there are no new issues, but any open issues, the status indicator will be yellow.
- If all issues are closed, the status indicator will be green.

The numbers indicate the number of new, open, and closed compliance issues. These statuses are configurable.

**Notable Events by Owner ? Last 24 Hours**

This view shows a list of notable events over the past 24 hours in real time sorted by owner. The default is "unassigned" and status options are New, Open, and Closed.

**Notable Events by Urgency ? Last 24 Hours**

This view shows a list of notable events over the past 24 hours (in real time) sorted by Urgency and status (options are New, Open, and Closed).

**Requirement Status**

The status indicator in this view show the status of your PCI compliance over the past 24 hours by requirement, indicating the number of issues in each area. The is red if there are any new issues, yellow if there are any open issues, and green if all issues are closed. Click the status indicator to link to the relevant scorecard.
Notable Event History

A history of notable events for the past year, new and open, is displayed. Click a notable event to view details.

Notable Event History by Requirements

A history of notable events for the past year, new and open, displays by requirements. Click a notable event to view details.

Compliance Status History

This graph displays a 30-day overview of your organization’s compliance history (Compliant, Partial, and Non-Compliant) by PCI requirement. If your organization is not in compliance with a PCI requirement, and does not become compliant within five days, the graph shows your organization as non-compliant for that requirement on the sixth day. This allows you time to remediate compliance issues before the issues negatively affect the organization’s compliance status history. You can configure this time period from the default of five days to match your expected or promised compliance remediation timeline.

Incident Review

The Incident Review dashboard displays notable events and their current status. As an analyst, you can use the dashboard to gain insight into the severity of events occurring in your system or network. You can use the dashboard to triage new notable events, assign events to analysts for review, and examine notable event details for investigative leads.

How Splunk App for PCI Compliance identifies notable events

Splunk App for PCI Compliance detects patterns in your data and automatically reviews events for security-relevant incidents using correlation searches. When a correlation search detects a suspicious pattern, the correlation search creates an alert called a notable event.

The Incident Review dashboard surfaces all notable events, and categorizes them by potential severity so you can quickly triage, assign, and track issues.

To view sequenced events in the Incident Review dashboard, make sure that governance="pci" is cleared from the Search field.
Incident review workflow

You can use this example workflow to triage and work notable events on the Incident Review dashboard.

1. An administrative analyst monitors the Incident Review dashboard, sorting and performing high-level triage on newly-created notable events.
2. When a notable event warrants investigation, the administrative analyst assigns the event to a reviewing analyst to start investigating the incident.
3. The reviewing analyst updates the status of the event from New to In Progress, and begins investigating the cause of the notable event.
4. The reviewing analyst researches and collects information on the event using the fields and field actions in the notable event. The analyst records the details of their research in the Comments field of the notable event.
5. After the reviewing analyst addresses the cause of the notable event and any remediation tasks have been escalated or solved, the analyst sets the notable event status to Resolved.
6. The analyst assigns the notable event to a final analyst for verification.
7. The final analyst reviews and validates the changes made to resolve the issue, and sets the status to Closed.

Triage notable events on the Incident Review dashboard

Use this dashboard as part of your incident triage workflow. You can monitor notable events and the actions that analysts take to resolve the issues that triggered a notable event.

You must wait for your search to complete before you can manage notable events or view event details.

Accelerate triage with tags and filters

Speed up your notable event triage with search filters, tagging, and sorting. For example, focus on groups of notable events or an individual notable event with the search filters and time range selector. Notable events contain Urgency, Status, and Owner fields to help you categorize, track, and assign events.

Simplify searching and add identifiers to notable events using tags. Click Edit Tags in the field actions menu for a notable event field such as Title, Status, or Owner to add new tags or modify existing ones. After you create a tag, you can use it to filter the dashboard.
**Assign notable events**

You can assign one event at a time or several at once.

1. Select a notable event.
2. Click **Edit selected**.
3. Select an **Owner** to assign the event or events to. Or, click **Assign to me** to assign the event or events to yourself.
4. Save your changes.

Owners are unassigned by default, and you can assign notable events to any user with an **administrator**, **pci_admin**, or **pci_analyst** role. For more on user roles, see Configure users and roles in the *Installation and Upgrade Manual*.

**Update the status of a notable event**

New notable events have the *New* status. As analysts triage and move a notable event through the incident review workflow, the owner can update the status of the notable event to reflect the actions they take to address the event.

1. Select one or more events, then click **Edit all selected**. To take action on all displayed events, click **Edit all ## matching events**.
2. In the **Edit Events** window, update the fields to reflect your actions.
3. (Optional) Add a **Comment** to describe the actions you took.
4. Save changes.

**Note:** If your changes are not immediately visible, check the dashboard filters. For example, if the filter is set to "New" after you changed an event to "In Progress", your updated event will not display.

You can require analysts to enter comments when updating a notable event. See *Customize Incident Review* for more.

You can choose from the following notable event statuses.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unassigned</td>
<td>The event has not been assigned to an owner.</td>
</tr>
<tr>
<td>New</td>
<td>Default status. The event has not been reviewed.</td>
</tr>
<tr>
<td>In Progress</td>
<td>An owner is investigating the event.</td>
</tr>
<tr>
<td>Pending</td>
<td>An action must occur before the event can be closed.</td>
</tr>
<tr>
<td>Resolved</td>
<td></td>
</tr>
</tbody>
</table>
The owner has addressed the cause of the event and is waiting for verification.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closed</td>
<td>The resolution of the event has been verified.</td>
</tr>
</tbody>
</table>

You can customize the notable event status names and workflow progression to match your process.

**Prioritize notable events by urgency**

Use the urgency level of a notable event to prioritize incident review. Every notable event is assigned an urgency. Urgency levels can be unknown, low, medium, informational, high, or critical.

Urgency levels are calculated using the severity of the correlation search event and the priority of the asset or identity involved in the event.

By default, security analysts can change the urgency of a notable event. See Customize Incident Review to learn how to change that default.

**Notify an analyst of untriaged notable events**

You can use a correlation search to notify an analyst if a notable event has not been triaged.

1. Select **Configure > Content Management**.
2. Locate the **Untriaged Notable Events** correlation search using the filters.
3. Modify the search, changing the notable event owner or status fields as desired.
4. Set the desired alert action.
5. Save the changes.
6. Enable the **Untriaged Notable Events** correlation search.

**Review details of notable events**

After you finish triaging notable events, begin your investigation. Use the available fields on a notable event to assess the urgency, contributing events, and risk scores associated with the notable event.

Open the event details to learn more about a notable event.

- Review the **History** to see the recent investigation activity on the notable event. Click **View all recent activity for this Notable Event** to see
analyst comments, status changes, and other activities for the event.

- See which correlation search generated the notable event. Click the name of the correlation search to make changes to or review the correlation search to understand why the notable event was created.
- View the Contributing Events that caused the notable event to be created.
- Review the risk scores listed for assets and identities involved in a notable event. Click a risk score to open the Risk Analysis dashboard filtered on that asset or identity.
- If one original event created a notable event, you can see the full details.
- Review the Adaptive Responses to see which adaptive response actions have been performed for this notable event, whether the actions were successfully performed, and drill down for more details. Click the name of the response action to see potential results generated by this action’s invocation. Click View Adaptive Response Invocations to see the raw audit events for the response actions associated with this correlation search. It takes up to five minutes for updates to appear on this table.
- Review the Next Steps to see if any next steps for notable event triage are defined.

**Take action on a notable event**

From Incident Review, you can suppress or share a notable event, add an event or multiple events to an investigation, analyze the risk that an asset or identity poses to your environment, or investigate a field in more detail on another dashboard.

**Run an adaptive response action**

Based on the details in a notable event, you may want to run a response action to gather more information, take an action in another system, send information to another system, modify a risk score, or something else.

1. From a notable event, select the arrow to expand the Actions column.
2. Click Run Adaptive Response Actions.
3. Click Add New Response Action and select an adaptive response action from the list. You can use the category filter or search to reduce the number of actions that you can select.
4. Fill out the form fields for the response action. Use the field name to specify a field, rather than the name that shows on Incident Review. For example, type "src" instead of "Source" to specify the source field for an action.
5. Click Run.
You can check the status of the response action in the notable event details. You cannot run adaptive response actions from the Search dashboard. View the original field names of fields displayed on Incident Review on the Incident Review - Event Attributes panel of the Incident Review Settings dashboard.

Adblock extensions in your browser can cause response actions to fail. Add the host name of your Splunk Enterprise Security host to the site whitelist for the adblock extension.

See Included adaptive response actions with Splunk App for PCI Compliance for more about the different adaptive response actions included with Splunk App for PCI Compliance.

**Share or bookmark a notable event**

Share a link to a notable event with another analyst, or bookmark it for later. From the event actions, click **Share Notable Event**. You cannot share a notable event from the Search dashboard.

**Analyze risk of an asset or identity**

You can analyze the risk that an asset or identity poses to your environment in the Incident Review dashboard.

1. Open the event details.
2. Review the risk score next to asset or identity fields such as src or host.
3. Click the risk score to open the Risk Analysis dashboard filtered on the asset or identity.

Not all assets and identities display a risk score. Risk scores that display for an asset or identity in Incident Review may not match the risk score on the Risk Analysis dashboard for that risk object. See How risk scores display in Incident Review for more.

**Add a notable event to an investigation**

Add a single event by selecting **Add Event to Investigation** from the Event Actions.

Add multiple events to an investigation timeline to investigate them further.

1. Select several notable events, then click **Add to Investigation**.
2. A dialog box appears. Select **Create new investigation**.
3. Add a title (required) and a description (optional) for your new investigation.
4. Click Save to add the selected events to the investigation. Clicking Cancel will create a new investigation without adding the selected notable events.

See Investigation Timelines for more.

**Investigate a field in more detail**

Take action on a specific field, such as host, src, src_ip, dest, or dest_ip. Different actions are available to take depending on the field you select.

- Tag fields by selecting **Edit tags**.
- Investigate an asset by selecting **Asset Investigator** to open the Asset Investigator dashboard filtered on the asset.
- Search for access-related events for a specific destination IP address by selecting **Access Search (as destination)**.
- Investigate a domain by selecting **Domain Dossier**.
- Find other notable events with matching malware signatures by selecting **Notable Event Search**.

**Suppress a notable event**

Hide notable events from the Incident Review dashboard by suppressing them. Creating a notable event suppression does not change the counts of notable events on the posture or auditing dashboards.

1. Select a notable event on the Incident Review dashboard.
2. From the **Actions** menu, select **Suppress Notable Events**.
3. Type a **Suppression Name**.
   For example, Excessive_Failed_Logins.
4. (Optional) Provide a reason for the suppression using the Description field.
5. (Optional) Set a date range. After the time limit ends, the suppression filter expires and stops hiding events.
6. Review the Selected Fields to validate the fields that you want to suppress notable events from. For example, the src field.
7. (Optional) Click change to modify the notable event fields used for the suppression.

8. Save changes.

This example notable event suppression hides all notable events created after June 10, 2016 that contain a src=_jdbc_ field from Incident Review.

You cannot suppress notable events from the Search dashboard.

**Audit incident review activity**

You can audit and review incident review activity on the Incident Review Audit dashboard.

**Customize Incident Review**

Customize the display of the Incident Review dashboard, and also modify analyst capabilities and permissions.

**Modify analyst capabilities and permissions**

You can change the default capabilities and permissions assigned to analysts to better fit your workflow.

Configure whether analysts can override the calculated urgency of a notable event and choose whether to require an analyst to add a comment when
updating a notable event on the **Incident Review Settings** page.

1. Select **Configure > Incident Management > Incident Review Settings** to view the Incident Review settings.
2. Allow or prevent analysts from overriding the calculated urgency of a notable event with the **Allow Overriding of Urgency** checkbox. Analysts are allowed to override urgency by default.
3. Require analysts to add a comment when updating a notable event by checking the **Required** checkbox under **Comments**.
4. If you require analysts to add a comment, enter the minimum character length for required comments. The default character length is 20 characters.

Configure the desired capacity of your security analysts on the **General Settings** page.

1. Select **Configure > General > General Settings** to view the General Settings.
2. Enter a preferred number of incidents that should be assigned to an analyst with the **Incident Review Analyst Capacity** setting. The default is 12.

This value is used for tracking purposes, and does not prevent more than the default number of notable events from being assigned to an analyst.

**Change Incident Review columns**

You can change the columns displayed on the **Incident Review** dashboard.

1. Review the existing columns in **Incident Review - Table Attributes**.
2. Use the action column to edit, remove, or change the order of the available columns.
3. Add custom columns by selecting **Insert below** or selecting **More...**, then **Insert above**.

**Change notable event fields**

Make changes to the fields displayed on the Incident Review dashboard for notable events on the Incident Review Settings dashboard.

1. From the Splunk App for PCI Compliance menu bar, select **Configure > Incident Management > Incident Review Settings**.
2. Review the **Incident Review - Event Attributes**.
3. Click **Edit** to change the field or the field label for a specific field.
4. Click **Remove** to remove a field from displaying on the Incident Review dashboard.

**How risk scores display in Incident Review**

Risk scores do not display in Incident Review for every asset or identity. Only assets or identities (risk objects) that have a risk score and a risk object type of "system" or "user" display in Incident Review. Risk scores only show for the following fields: `orig_host`, `dvc`, `src`, `dest`, `src_user`, and `user`.

The risk score for an asset or identity might not match the score on the Risk Analysis dashboard. The risk score is a cumulative score for an asset or identity, rather than a score specific to an exact username.

- For example, if a person has a username of "buttercup" that has a risk score of 40, and an email address of "buttercup@splunk.com" with a risk score of 60, and the identity lookup identifies that "buttercup" and "buttercup@splunk.com" belong to the same person, a risk score of 100 displays on Incident Review for both "buttercup" and "buttercup@splunk.com" accounts.
- As another example, if an IP of 10.11.36.1 has a risk score of 80 and an IP of 10.11.36.19 has a risk score of 30, and the asset lookup identifies that a range of IPs "10.11.36.1 - 10.11.36.19" belong to the same asset, a risk score of 110 displays on Incident Review for both "10.11.36.1" and "10.11.36.19" IP addresses.

Risk scores are calculated for Incident Review using the **Threat - Risk Correlation - Lookup Gen** lookup generation search. The search runs every 30 minutes and updates the `risk_correlation_lookup` lookup file. To see more frequent updates to the risk scores in Incident Review, update the `cron_schedule` of the saved search.

**Scorecards**

Scorecards display a real-time summary view of your compliance with the PCI data security standard in each of the requirement areas.

The Splunk App for PCI Compliance includes these scorecards:
• Requirement 1: **Network Traffic** - Summary of firewall and network traffic-related compliance issues
• Requirement 2: **Default Configurations** - Summary of configuration-related compliance issues
• Requirement 3: **Protect Data At Rest** - Summary of compliance issues related to cardholder data at rest
• Requirement 4: **Protect Data In Motion** - Summary of compliance issues related to cardholder data in motion
• Requirement 5: **Anti-malware Protection** - Summary of anti-malware related compliance issues
• Requirement 6: **Patch Update Protection** - Summary of system and application patch related compliance issues
• Requirement 7: **Access Monitoring** - Summary of access-related compliance issues
• Requirement 8: **Activity Accountability** - Summary of user activity related compliance issues
• Requirement 10: **Cardholder Data Access** - Summary of cardholder data access related compliance issues
• Requirement 11: **Vulnerability Testing** - Summary of vulnerability, IDS, and file integrity related compliance issues

**Using the scorecards**

The consolidated compliance workflow status for each requirement area is indicated in the form of a status indicator. Red indicates a new status, yellow indicates an open status, and green indicates a closed status. Notable events are shown in the form of a bar chart by urgency. Notable events are also shown in the form of a table by owner.

Each scorecard or requirement area has its available reports listed, showing when the report was last viewed, and which user viewed the report. Notable event history displays as a chart. The following example shows a scorecard for requirement 1.
Reports

The Splunk App for PCI Compliance provides a variety of built-in reports for areas of PCI compliance. The reports are organized by PCI DSS requirement. Some reports apply to more than one requirement and appear in more than one place. Use these reports to show compliance in each of the PCI DSS requirement areas.

Requirement 1 - Network Traffic

Firewall Rule Activity

Use this report to track activity related to the firewall rules. Use the filters to modify the search results.

The Activity by Month panel shows activities in the timeline view based on the filters provided. In the timeline view, you can customize the search or save the search to view the same results at a later time.

The Traffic By Source And Destination Domain panel shows all traffic events over time grouped by all source and destination domains.

To configure this report see Firewall Rule Activity in the Splunk App for PCI Compliance Installation and Configuration Manual.
**Network Traffic Activity**

Use this report to capture network traffic activity. Use the filters to modify the search results.

The Traffic Detail panel shows activities in the timeline view based on the filters provided. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Network Traffic Activity in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Prohibited Services**

Use this report to review host ports, processes, and services. Use the filters to modify the search results.

The Service Details panel shows events in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Prohibited Services in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Requirement 2 - Default Configurations**

**Default Account Access**

Use this report to report on default account access in your PCI compliance environment. Use the filters to modify the search results.

The Default Account Access Details panel shows all events in the timeline view. In the timeline view you can work with the search results in the same way you can work with any search. Customize the search or save the search to view the same results at a later time.

To configure this report see Default Account Access in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Insecure Authentication Attempts**

Use this report to track insecure authentication attempts. Use the filters to modify the search results.
The **Insecure Authentication Attempts** panel shows events in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Insecure Authentication Attempts in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**PCI System Inventory**

Use this report to maintain an inventory of software components running in the PCI compliant environment. Use the filters such as Asset and Category to modify the search results.

In the **System Inventory** panel, use the Resource selector to view results by Ports, Processes, or Services. This panel shows events in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see PCI System Inventory in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Primary Functions**

Use this report to identify systems where multiple primary functions may be running or where unexpected services could be in use. Use the filters to modify the search results.

The **Primary Function Details** panel shows events in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Primary Functions in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Prohibited Services**

Use this report to monitor prohibited services that may be running in your environment. Use the filters to modify the search results.

The **Service Details** panel shows events in the timeline view. In the timeline view you can work with the search results in the same way you can work with any search; customize the search or save the search to view the same results at a later time.
To configure this report see Prohibited Services in the Splunk App for PCI Compliance Installation and Configuration Manual.

System Misconfigurations

Use this report to track the configuration of systems in your environment. Use the filters to modify the search results.

The System Misconfiguration Details panel shows events in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

The Systems With Misconfigurations (Last 90 Days) panel shows the count of misconfigured systems over last 90 days on a time chart.

To configure this report see System Misconfigurations in the Splunk App for PCI Compliance Installation and Configuration Manual.

Weak Encrypted Communication

Use this report to track communication between source and destination that use SSL or early TLS encryption protocols in your environment. Use the filters to modify the search results.

The Weak Encrypted Communication (By SSL Version) panel shows a count of events that use encryption grouped by SSL or TLS version. The Weak Encrypted Communication Detail panel shows all events in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Weak Encrypted Communication in the Splunk App for PCI Compliance Installation and Configuration Manual.

Wireless Network Misconfigurations

Use this report to track wireless usage in your environment. Use the filters to modify the search results.

The Wireless Misconfigurations Details panel shows all events in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.
Requirement 3 - Protect Data at Rest

*Credit Card Data Found*

Use this report to monitor any credit card data that might be found on systems in your environment. Use the filters to modify the search results.

The *Credit Card Transmission Events Details* panel shows the results from this panel in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

*Credit Card Transmission Event Summary (By Source)* shows the number of events over time grouped by the source.

To configure this report see *Credit Card Data Found* in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

Requirement 4 - Protect Data In Motion

*Weak Encrypted Communication*

Use this report to track communication between source and destination that use SSL or early TLS encryption protocols in your environment. Use the filters to modify the search results.

The *Weak Encrypted Communication (By SSL Version)* panel shows a count of events that use encryption grouped by SSL or TLS version. The *Weak Encrypted Communication Detail* panel shows all events in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

*Credit Card Data Found*

Use this report to monitor any credit card data that might be found on systems in your environment. Use the filters to modify the search results.

The *Credit Card Transmission Events Details* panel shows the results from this panel in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.
Credit Card Transmission Event Summary (By Source) shows the number of events over time grouped by the source.

To configure this report see Credit Card Data Found in the Splunk App for PCI Compliance Installation and Configuration Manual.

Requirement 5 - Anti-malware Protection

Endpoint Product Deployment

Use this report to track software products deployed in your PCI compliance environment. Use the filters to modify the search results.

The Missing Antivirius and the Disabled Antivirius panels show results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Endpoint Product Deployment in the Splunk App for PCI Compliance Installation and Configuration Manual.

Endpoint Product Versions

Use this report to track product versions of software deployed in your PCI compliance environment. Use the filters to modify the search results.

The Details panel shows the results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Endpoint Product Versions in the Splunk App for PCI Compliance Installation and Configuration Manual.

Malware Activity

Use this report to track malware that might exist in your deployment. Use the filters to modify the search results.

The dashboard consists of a single panel which shows the results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Malware Activity in the Splunk App for PCI Compliance Installation and Configuration Manual.
**Malware Signature Updates**

Use this report to track and identify malware signature updates. Use the filters to modify the search results.

At the bottom of list of events in the **Anti-malware Signature Details** panel, click "View full results" to open the results from this panel in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Malware Signature Updates in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Requirement 6 - Patch Update Protection**

**Anomalous System Uptime**

Use this report to track systems that have gone offline and then come back online. Use the filters to modify the search results.

The **Anomalous System Uptime** panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Anomalous System Update in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Default Account Access**

Use this report to track the access to the default accounts in your PCI compliance environment.

The **Default Account Access Details** panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Default Account Access in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Patch Service Status report**

Use this report to verify the status of your software patch updates. Use the filters to modify the search results.
The **Service Details** panel shows the results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Patch Service Status in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**System Patch Status**

Use this report to track the status of any system patches. Use the filters to modify the search results.

The **System Patch Status** panel shows the results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see System Patch Status in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Requirement 7 - Access Monitoring**

**PCI Command History**

Use this report to track commands run on PCI resources. Use the filters to modify the search results.

The **PCI Command History** panel shows the results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see PCI Command History in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**PCI Resource Access**

Use this report to track any access to PCI resources. Use the filters to modify the search results.

The **PCI Resource Access Details** panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.
To configure this report see PCI Resource Access in the Splunk App for PCI Compliance Installation and Configuration Manual.

**Requirement 8 - Activity Accountability**

*Default Account Access*

Use this report to report on access to default accounts in your PCI compliance environment.

The Default Account Access Details panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Default Account Access in the Splunk App for PCI Compliance Installation and Configuration Manual.

*PCI Resource Access*

Use this report to track any access to PCI resources. Use the filters to modify the search results.

The PCI Resource Access Details panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see PCI Resource Access in the Splunk App for PCI Compliance Installation and Configuration Manual.

**Requirement 10 - Cardholder Data Access**

*Endpoint Changes*

Use this report to monitor any endpoint changes. Use the filters to modify the search results.

The Endpoint Changes panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Endpoint Changes in the Splunk App for PCI Compliance Installation and Configuration Manual.
PCI Asset Logging

Use this report to track activity related to PCI resources. Use the filters to modify the search results.

At the bottom of the PCI Resource Logging panel, click "View full results" to open the results from this panel in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see PCI Asset Logging in the Splunk App for PCI Compliance Installation and Configuration Manual.

PCI Resource Access

Use this report to track any access to PCI resources. Use the filters to modify the search results.

The PCI Resource Access Details panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see PCI Resource Access in the Splunk App for PCI Compliance Installation and Configuration Manual.

Privileged User Activity

Use this report to monitor any data activity that includes a privileged user account in your PCI compliance environment. You can use the filters in the report to modify the search results.

For example, if you look at the past 24 hours for user "buttercup", category "cardholder", and domain "dmz", the search would return any activity by "buttercup" in the "dmz" domain involving "cardholder" category data.

The Privileged User Activity panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Privileged User Activity in the Splunk App for PCI Compliance Installation and Configuration Manual.
**System Time Synchronization**

Use this report to monitor system time synchronizations. Use the filters to modify the search results.

The **System Time Synchronization Details** panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see System Time Synchronization in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Requirement 11 - Vulnerability Testing**

**Endpoint Changes**

Use this report to monitor any endpoint changes.

The **Endpoint Changes** panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Endpoint Changes in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Rogue Wireless Access Point Protection**

Use this report to monitor any unauthorized wireless access in your PCI compliance environment. Use the filters to modify the search results.

The **Rogue Device Details** panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Rogue Wireless Access Point Protection in the Splunk App for PCI Compliance *Installation and Configuration Manual*.

**Vulnerability Scan Details**

Use this report to track vulnerability scans from your environment. Use the filters to modify the search results.
All vulnerabilities include a Common Vulnerabilities and Exposures (CVE) identifier used to define the specific vulnerability. CVEs are unique, common identifiers for publicly known information security vulnerabilities. The Vulnerability Scan report can be filtered on the CVE, and includes a column listing the CVE.

The report also includes a Common Vulnerability Scoring System (CVSS) number that can also be used as a filter. This is a number that indicates the severity of a computer system's security vulnerabilities. The number attempts to establish a measure of how much concern a vulnerability warrants, compared to other vulnerabilities.

The Vulnerability Details panel shows results in the timeline view. In the timeline view, you can customize the search or save the search to view the same results at a later time.

To configure this report see Vulnerability Scan Details in the Splunk App for PCI Compliance Installation and Configuration Manual.

**IDS/IPS Alert Activity**

Use this report to track intrusion detection system or intrusion prevention system activity in your environment.

To configure this report see IDS/IPS Alert Activity in the Splunk App for PCI Compliance Installation and Configuration Manual.

**Audit dashboards**

Audit dashboards in the Splunk App for PCI Compliance provide the ability to audit different areas and activities in your PCI compliance environment. Audit dashboards are shared with the Splunk Enterprise Security framework.

Use the audit dashboards to validate the security and integrity of the data in Splunk App for PCI Compliance. Ensure that forwarders are functioning, that data has not been tampered with and is secured in transmission, and that analysts are reviewing the notable events detected by correlation searches.

**Incident Review Audit**

The Incident Review Audit dashboard provides an overview of incident review activity. The panels display how many incidents are being reviewed and by which
user, along with a list of the most recently reviewed events. The metrics on this dashboard allow security managers to review the activities of analysts.

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Activity by Reviewer</td>
<td>Displays the numbers of events reviewed by each user. This panel is useful for determining which user is performing the incident reviews and if the total number of incidents reviewed is changing over time. The drilldown opens a search with all activity by the selected reviewer.</td>
</tr>
<tr>
<td>Top Reviewers</td>
<td>Displays the top users that have performed incident reviews. The panel includes details for each user, including the date they first performed an incident review, the date they last performed a review, and the total number of incidents reviewed. The drilldown opens a search with all activity by the selected reviewer.</td>
</tr>
<tr>
<td>Notable Events By Status - Last 48 Hours</td>
<td>Displays the status, count, and urgency for all notable events in the last 48 hours. This panel is useful for determining if the incident review users are keeping up with incidents, or whether a backlog of unreviewed incidents is forming. The drilldown opens the Incident Review dashboard and searches on the selected urgency and status over the last 48 hours.</td>
</tr>
<tr>
<td>Notable Events By Owner - Last 48 Hours</td>
<td>Displays the owner, count, and urgency for all notable events in the last 48 hours. This panel is useful for determining how many events are assigned to a user and the urgency of the events. The drilldown opens the Incident Review dashboard and searches on the selected urgency over the last 48 hours.</td>
</tr>
<tr>
<td>Mean Time to Triage - Last 14 days</td>
<td>Displays the average time it took for a notable event to be triaged after it was created over the last 14 days, split by the name of the notable event. This panel is useful for determining how quickly analysts are triaging notable events, or whether certain types of events take longer to triage than others. The drilldown opens the Incident Review dashboard and searches on the matching notable event names over the last 14 days.</td>
</tr>
<tr>
<td>Mean Time to Closure - Last 60 days</td>
<td>Displays the average time it took for a notable event to be closed after it was created over the last 60 days, split by the name of the notable event. This panel is</td>
</tr>
</tbody>
</table>

28
useful for determining how long it takes to close certain types of notable event investigations. The drilldown opens the Incident Review dashboard and searches on the matching notable event names that have a status of closed from the last 60 days.

Recent Review Activity Displays the 10 most recent changes on the incident review dashboard, such as triage actions. The drilldown opens a search with the selected rule ID.

Data sources

The reports in the Incident Review Audit dashboard reference fields in the notable index and the incident review objects in a KV store collection.

Suppression Audit

The Suppression Audit dashboard provides an overview of notable event suppression activity. This dashboard shows how many events are being suppressed, and by whom.

The metrics on this dashboard allow security managers to review the activities of analysts, which is useful for tuning correlation searches. You can identify correlation search rules that are generating more events than your analysts are capable of looking at, and tune them accordingly.

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppressed Events Over Time - Last 24 Hours</td>
<td>Displays notable events suppressed in the last 24 hours.</td>
</tr>
<tr>
<td>Suppression History Over Time - Last 30 Days</td>
<td>Displays the history of suppressed notable events.</td>
</tr>
<tr>
<td>Suppression Management Activity</td>
<td>Displays suppression management activity for the time period.</td>
</tr>
<tr>
<td>Expired Suppressions</td>
<td>Displays expired suppressions.</td>
</tr>
</tbody>
</table>
**Data sources**

The reports in the **Suppression Audit** dashboard reference events in the Notable index.

**Per-Panel Filter Audit**

The **Per-Panel Filter Audit** dashboard provides information about the filters currently in use in your deployment.

The following table describes the panels for this dashboard.

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per-Panel By Reviewer</td>
<td>Displays the count of updates to per-panel filters by user</td>
</tr>
<tr>
<td>Top Users</td>
<td>Shows users, sparkline for trends, number of views, and first and last time viewed.</td>
</tr>
<tr>
<td>Recent Filter Activity</td>
<td>Activity by time, user, action, and filename</td>
</tr>
</tbody>
</table>

**ES Configuration Health**

Use the **ES Configuration Health** dashboard to compare the latest installed version of the application to prior releases and identify configuration anomalies. The dashboard does not report changes to a TA or add-ons. Select the previous version of Enterprise Security installed in your environment using the Previous ES Version filter. You can use this dashboard with PCI by selecting the version of ES that has the same framework components. For example, the 3.4.x version of PCI contains framework components from the 4.7.x version of Enterprise Security.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unshipped</td>
<td>The Unshipped setting compares the latest installed version of Enterprise Security with the content in the ES installation package. Any item that was not provided as part of the Enterprise Security installation, such as files or scripts used for customization, is labeled as an Unshipped item. Review Unshipped items to evaluate their use, determine if they are still needed, and reconcile if necessary. The Unshipped</td>
</tr>
<tr>
<td>Mode</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Removed Stanzas</td>
<td>The Removed Stanzas setting compares the latest installed version of Enterprise Security with the version that you select in the filter. Removed Stanzas are configuration stanzas that changed between versions, such as a deprecated threat list or input. Review Removed Stanzas to evaluate their use, determine if they are still needed, and reconcile if necessary.</td>
</tr>
<tr>
<td>Local Overrides</td>
<td>The Local Overrides setting compares the installed version of Enterprise Security with the version that you select in the filter. A setting that conflicts with or overrides the installed version of Enterprise Security is labeled as a Local Override. Review any Local Override settings to evaluate their use, determine if they are still needed, and reconcile if necessary.</td>
</tr>
</tbody>
</table>

**Data Model Audit**

The **Data Model Audit** dashboard displays information about the state of data model accelerations in your environment.

<table>
<thead>
<tr>
<th>Field Name Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Accelerations By Size</td>
<td>Displays the accelerated data models sorted in descending order by MB on disk</td>
</tr>
<tr>
<td>Top Accelerations By Run Duration</td>
<td>Displays the accelerated data models sorted in descending order by the time spent on running acceleration tasks.</td>
</tr>
<tr>
<td>Accelerations Details</td>
<td>Displays a table of the accelerated data models with additional information.</td>
</tr>
</tbody>
</table>

**Data sources**

The reports in the **Data Model Audit** dashboard reference fields in the Splunk Audit data model. For a list of data model objects and constraints, see Splunk Audit Logs in the *Common Information Model Add-on Manual.*

**Forwarder Audit**

The **Forwarder Audit** dashboard reports on hosts forwarding data to Splunk Enterprise.
Use the search filters and time range selector to focus on groups of forwarders, or an individual forwarder.

<table>
<thead>
<tr>
<th>Filter by</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show only expected hosts</td>
<td>An expected host is a host defined by the field <code>is_expected</code> in the Asset table.</td>
<td>Drop-down, select to filter by</td>
</tr>
<tr>
<td>Host</td>
<td>Filter by the host field in the Asset table.</td>
<td>Text field. Wildcard with an asterisk (*)</td>
</tr>
<tr>
<td>Business Unit</td>
<td>Filter by the business unit <code>bunit</code> field in the Asset table.</td>
<td>Text field. Wildcard with an asterisk (*)</td>
</tr>
<tr>
<td>Category</td>
<td>Filter by the category field in the Asset table.</td>
<td>Drop-down, select to filter by</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Count Over Time By Host</td>
<td>Displays the number of events reported over the time period selected in the filter. The events are split by host.</td>
</tr>
<tr>
<td>Hosts By Last Report Time</td>
<td>Displays a list of hosts, ordered by the last time they reported an event.</td>
</tr>
<tr>
<td>Splunkd Process Utilization</td>
<td>Displays the resource utilization of the forwarder's Splunk daemon <code>splunkd</code>.</td>
</tr>
<tr>
<td>Splunk Service Start Mode</td>
<td>Displays the host names that are forwarding events, but are not configured to have <code>splunkd</code> start on boot.</td>
</tr>
</tbody>
</table>

**Data sources**

Relevant data sources for the Forwarder Audit dashboard include data from all forwarders in your Splunk environment and the Application_State data model. See the Common Information Model Add-on Manual for more information. The Common Information Model fields `bunit` and `category` are derived by automatic identity lookup and do not need to be mapped directly.

**Indexing Audit**

The Indexing Audit dashboard is designed to help administrators estimate the volume of event data being indexed by Splunk Enterprise. The dashboard displays use EPD (Events Per Day) as a metric to track the event volume per index and the rate of change in the total event counts per index over time. The EPD applies only to event counts and is unrelated to the Volume Per Day metric used for licensing.
Panel | Description
--- | ---
Key Indicators | The key indicators on this dashboard are scoped to All Time, not the Last 24 hours.
Events Per Day Over Time | Displays a column chart representing the event counts per day.
Events Per Day | Displays a table representing event counts per day and the average eps.
Events Per Index (Last Day) | Displays a table of event counts per index for the last day.

**Data sources**

The reports in the **Indexing Audit** dashboard reference data generated by the **Audit - Events Per Day - Lookup Gen** saved search and are stored within a KVStore collection.

**Search Audit**

The **Search Audit** dashboard provides information about the searches being executed in Splunk Enterprise. This dashboard is useful for identifying long running searches and tracking search activity by user.

Panel | Description
--- | ---
Searches Over Time by Type | Shows the number of searches executed over time by type, such as ad-hoc, scheduled, or real-time. Helps determine whether Splunk’s performance is being affected by excessive numbers of searches.
Searches Over Time by User | Shows the number of searches executed by each user. Helps determine when a particular user is executing an excessive number of searches. The **splunk-system-user** is the name of the account used to execute scheduled searches in Splunk Enterprise.
Top Searches by Run Time | Lists the most expensive searches in terms of duration. Helps to identify specific searches that may be adversely affecting Splunk performance.

**Data sources**

The reports in the **Search Audit** dashboard reference scheduled search auditing events from the **audit index**.
View Audit

The View Audit dashboard reports on the most active views in Enterprise Security. View Audit enables tracking of views that are being accessed on a daily basis and helps to identify any errors triggered when users review dashboard panels.

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Activity Over Time</td>
<td>Displays the Enterprise Security views that have the greatest access counts over time. The drilldown opens a search view of all page activity for the time selected.</td>
</tr>
<tr>
<td>Expected View Activity</td>
<td>Lists the views set up in the Expected View list. Review these views on a daily basis for your deployment. Select a dashboard to see details in the Expected View Scorecard panel below. Use Configure &gt; Lists and Lookups &gt; Expected Views to set up the Expected View list.</td>
</tr>
<tr>
<td>Web Service Errors</td>
<td>Displays errors that occurred while loading the web interface. Helps identify custom views that contain errors or an underlying issue that need to be escalated to Splunk.</td>
</tr>
</tbody>
</table>

Data sources

The reports in the View Audit dashboard reference fields in the Splunk Audit data model. For a list of data model objects and constraints, see Splunk Audit Logs in the Common Information Model Add-on Manual.

Data Protection

The Data Protection dashboard reports on the status of the data integrity controls.

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Integrity Control By Index</td>
<td>Displays a view of all indexes with data protection enabled, sorted by search peer. For more information on configuring and validating data integrity, see Manage data integrity in the Securing Splunk Enterprise Manual.</td>
</tr>
<tr>
<td>Sensitive Data</td>
<td>Displays the count of events with sensitive data. This panel requires enabling the Personally Identifiable Information Detected correlation search.</td>
</tr>
</tbody>
</table>
Panel Description

Define a primary service

As part of the Splunk App for PCI Compliance, primary functions are defined as one or more of the following items:

- Running Process (process name)
- Installed Service (service name)
- Listening Port (transport/port combination)

Primary functions are defined in a Splunk lookup table (SA-EndpointProtection/lookups/primary_functions.csv). This lookup table contains three separate primary keys (one for service, process, and transport/port respectively). The remainder of the header determines whether or not the function is primary and what that function is. This results in the following CSV header:

```
process,service,transport,port,is_primary,function
```

Function names are arbitrary, but we recommend the following:

```
Application (name, for instance "Tomcat")
Authentication
Database
Domain Name Service (DNS)
Mail
Proxy
Network Time Protocol (NTP)
Web
```

The SA-EndpointProtection/lookups/primary_functions.csv file contains examples that come with the Splunk App for PCI Compliance.

Lookups

Primary functions running on a system are determined by comparing the defined primary functions with the running processes, installed services, and listening ports found on a system.

- Running processes are found in the "localprocesses_tracker"
- Services are found in the "services_tracker"
• Listening ports are found in the "listeningports_tracker"

For example, the following search examines the "localprocesses_tracker for primary functions":

```
| inputlookup append=T localprocesses_tracker |
| `get_primary_function(process)` | rename app as process |
```

Compliance Managers may want to use multiple services and/or processes to determine the **primary function** of a system. This is easily done as long as the function name is consistent among applications in the stack.

To do this, you will need to define a **primary service**. You can have several service names that represent an application stack but a single function. In the SA-EndpointProtection/lookups/primary_functions.csv file identify all of the services and/or processes associated with the primary function with the same function name.

For example:

<table>
<thead>
<tr>
<th>process</th>
<th>service</th>
<th>transport</th>
<th>port</th>
<th>is_primary</th>
<th>function</th>
</tr>
</thead>
<tbody>
<tr>
<td>apple</td>
<td></td>
<td></td>
<td></td>
<td>true</td>
<td>improve health</td>
</tr>
<tr>
<td>banana</td>
<td></td>
<td></td>
<td></td>
<td>true</td>
<td>improve health</td>
</tr>
<tr>
<td>carrot</td>
<td></td>
<td></td>
<td></td>
<td>true</td>
<td>improve health</td>
</tr>
</tbody>
</table>

The following search simulates a system running these services to show how they result in a single function:

```
| head 1 | stats count | eval service="apple|banana|carrot" |
|        |             | `makemv(service)` | rename service as app | mvexpand app | `get_primary_function(service)` |
|        |             | `stats dc(function)` |
```

This search will result in a \( \text{dc(function)} == 1 \)

### Set up adaptive response actions in Splunk App for PCI Compliance

**Adaptive response actions** allow you to gather information or take other action in response to the results of a correlation search or the details of a notable event. Splunk App for PCI Compliance includes several adaptive response actions. See [Included adaptive response actions with Splunk App for PCI Compliance](#).
You can add adaptive response actions and alert actions to correlation searches, or run adaptive response actions from notable events on the Incident Review dashboard. Collect information before you start your investigation to save time at triage by adding adaptive response actions to correlation searches. Take action at triage time by running adaptive response actions from the Incident Review dashboard.

Add new adaptive response actions


Audit adaptive response actions

Audit all adaptive response actions on the Adaptive Response Action Center.

Configure permissions for adaptive response actions

Restrict certain adaptive response actions to certain roles by adjusting the permissions for adaptive response actions in the alert actions manager. You can find information about the alert actions manager in the Splunk platform documentation.

- For Splunk Enterprise, see Using the alert actions manager in the Splunk Enterprise Alerting Manual.
- For Splunk Cloud, see Using the alert actions manager in the Splunk Cloud Alerting Manual.

In order to run adaptive response actions from the Incident Review dashboard that have credentials stored in the credential manager, you must have the appropriate capability.

- For Splunk platform version 6.5.0 and later, list_storage_passwords.
- For earlier Splunk platform versions, admin_all_objects.

Add an adaptive response action to a correlation search

1. On the Splunk App for PCI Compliance menu bar, click Configure > Content Management.
2. Click an existing correlation search, or click **Create New > Correlation Search**.
3. Click **Add New Response Action** and select the response action you want to add.
4. Complete the fields for the action. If you want, add another response action.
5. Click **Save** to save all changes to the correlation search.

### Run an adaptive response action from Incident Review

See Run an adaptive response action on the Incident Review dashboard.

### Troubleshoot why an adaptive response action is not available to select

If an adaptive response action is not available to select on the correlation search editor or Incident Review, several things could be the cause.

- Your role may not have permissions to view and use the adaptive response action. See Using the alert actions manager in the Alerting Manual.
- Check the alert actions manager to determine if the adaptive response actions exist in Splunk platform. See Using the alert actions manager in the Alerting Manual.
- If the adaptive response actions from an add-on do not appear in Splunk App for PCI Compliance, but do appear in the alert actions manager, make sure that the add-on is being imported by Splunk App for PCI Compliance. See Install and deploy add-ons in the Install and Upgrade Manual.
- If you can select the adaptive response action on the correlation search editor, but not on Incident Review, the adaptive response action might be an ordinary alert action, or the response action does not support ad-hoc invocation. See Determine whether your action supports ad hoc invocation on the Splunk developer portal.

### Included adaptive response actions with Splunk App for PCI Compliance

Splunk App for PCI Compliance includes several adaptive response actions that you can run on a notable event from Incident Review or add to a correlation
search.

- Create a notable event.
- Modify a risk score with a risk modifier
- Send an email.
- Start a stream capture with Splunk Stream
- Ping a host
- Run nbtstat
- Run nslookup
- Add threat intelligence

PCI admins can configure these and additional adaptive response actions to be triggered by correlation searches.

Create a notable event

Create a notable event when the conditions of a correlation search are met.

1. On the Splunk App for PCI Compliance menu bar, click Configure > Content Management.
2. Click an existing correlation search, or click Create New > Correlation Search.
3. Click Add New Response Action and select Notable to add a notable event.
4. Type a Title of the notable event on the Incident Review dashboard. Supports variable substitution from the fields in the matching event.
5. Type a Description of the notable event. Supports variable substitution from the fields in the matching event.
6. Select the Security Domain of the notable event from the drop-down list.
7. Select the Severity of the notable event from the drop-down list. The severity is used to calculate the Urgency of a notable event.
8. (Optional) Change the default owner of the notable event from the system default, unassigned.
9. (Optional) Change the default status of the notable event from the system default, New.
10. Type a drill-down name for the Contributing Events link in the notable event.
11. Type a drill-down search for the Contributing Events link in the notable event.
12. In the Drill-down earliest offset field, type the amount of time before the time of the triggering event to look for related events for the Contributing Events link in the notable event.
   For example 2h to look for contributing events 2 hours before the
triggering event.

13. In the **Drill-down latest offset** field, type the amount of time after the time of the triggering event to look for related events for the **Contributing Events** link in the notable event.
   For example, **1h** to look for contributing events 1 hour after the triggering event.

14. Type **Next Steps** for an analyst to take after triaging a notable event. Type text or click **Insert Adaptive Response Action** to reference a response action in the text of the next steps. You can only type plain text and links to response actions in the next steps field. Use next steps if you want to recommend response actions that should be taken in a specific order.
   For example, ping a host to determine if it is active on the network. If the host is active, increase the risk score by 100, otherwise, increase the risk score by 50.

15. Select **Recommended Actions** to complement the next steps. From the list of all adaptive response actions, click the name of an action that you recommend as a triage or investigation step for this notable event to add it to the list of recommended actions that analysts can take for this notable event. You can add as many recommended actions as you like. Use recommended actions to recommend response actions that do not need to be taken in a specific order.
   For example, increase the risk score on a host and perform an nslookup on a domain name.

**Modify a risk score with a risk modifier**

Modify a risk score as a result of a correlation search or in response to notable event details with the **Risk Analysis** adaptive response action. The risk adaptive response action creates a risk modifier event.

1. Click **Add New Response Action** and select **Risk Analysis**.
2. Type the score to assign to the risk object.
3. Select a field from the notable event to apply the risk score to for the **Risk Object Field**.
4. Select the **Risk Object Type** to apply the risk score to.

**Send an email**

Send an email as a result of a correlation search match. You cannot send an email from the Incident Review dashboard.

**Prerequisite**
Make sure that the mail server is configured in the Splunk platform before setting up this response action.

- For Splunk Enterprise, see Configure email notification settings in the Splunk Enterprise Alerting Manual.
- For Splunk Cloud, see Configure email notification settings in the Splunk Cloud Alerting Manual.

Steps

1. Click Add New Response Action and select Send email.
2. In the To field, type a comma-separated list of email addresses to send the email to.
3. (Optional) Change the priority of the email. Defaults to Lowest.
4. Type a subject for the email. The email subject defaults to "Splunk Alert: $name$", where $name$ is the correlation search Search Name.
5. Type a message to include as the body of the email. Defaults to "The scheduled report '$name$' has run."
6. Select the check boxes of the information you want the email message to include.
7. Select whether to send a plain-text or HTML and plain-text email message.

Run a script

Run a script stored in $SPLUNK_HOME/bin/scripts.

1. Click Add New Response Action and select Run a script.
2. Type the filename of the script.

More information about scripted alerts can be found in the Splunk platform documentation.

- For Splunk Enterprise, see Configure scripted alerts in the Splunk Enterprise Alerting Manual.
- For Splunk Cloud, see Configure scripted alerts in the Splunk Cloud Alerting Manual.

Start a stream capture with Splunk Stream

Start a Stream capture to capture packets on the IP addresses of the selected protocols over the time period that you select. You can view the results of the capture session on the Protocol Intelligence dashboards.
A stream capture will not work unless you integrate Splunk Stream with Splunk App for PCI Compliance.

1. Click **Add New Response Action** and select **Stream Capture** to start a packet capture in response to a correlation search match.
2. Type a **Description** to describe the stream created in response to the correlation search match.
3. Type a **Category** to define the type of stream capture. You can view streams by category in Splunk Stream.
4. Type the comma-separated event fields to search for IP addresses for the Stream capture. The first non-null field is used for the capture.
5. Type the comma-separated list of protocols to capture.
6. Select a **Capture duration** to define the length of the packet capture.
7. Type a **Stream capture limit** to limit the number of stream captures started by the correlation search.

**Ping a host**

Determine whether a host is still active on the network by pinging the host.

1. Click **Add New Response Action** and select **Ping**.
2. Select the field that contains the host that you want to ping in the **Host Field**.
3. Type the number of maximum results that the ping returns. Defaults to 1.

**Run nbtstat**

Learn more about a host and the services that the host runs by running nbtstat. You must have nbtstat installed on the search head for this to run successfully.

1. Click **Add New Response Action** and select **Nbtstat**.
2. Select the field that contains the host that you want to run the nbtstat for in the **Host Field**.
3. Type the number of maximum results that the nbtstat returns. Defaults to 1.

**Run nslookup**

Look up the domain name of an IP address, or the IP address of a domain name, by running nslookup. You must have nslookup installed on the search head for this to run.
1. Click **Add New Response Action** and select **Nslookup**.
2. Select the field that contains the host that you want to run the nslookup for in the **Host Field**.
3. Type the number of maximum results that the nslookup returns. Defaults to 1.

**Add threat intelligence**

Create threat artifacts in a threat collection.

1. Click **Add New Response Action** and select **Add Threat Intelligence**.
2. Select the **Threat Group** to attribute this artifact to.
3. Select the **Threat Collection** to add the threat artifact to.
4. Select the **Field from event** that contains the value to add as a threat artifact to the threat intelligence collection.
5. Type a **Description** for the threat artifact.
6. Type a **Weight** associated with the threat list. Defaults to 1.
7. Type a number of **Max Results** to specify the number of results to process as threat artifacts. Each unique search field value counts as a result. Defaults to 100.
Supporting dashboards

Asset Center

Use the Asset Center dashboard to review and search for objects in the asset data added to Splunk platform that stores the information for each of the cardholder assets in scope for monitoring. The asset data represents a list of hosts, IP addresses, and subnets within the organization, along with information about each asset. Use this dashboard to see a list of the assets, the owners for each asset, and other relevant information such as asset categories, business units, and PCI domain that are used in the filtering for each report.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels.

<table>
<thead>
<tr>
<th>Filter by</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>A known or unknown asset</td>
<td>Text field. Empty by default. Wildcard strings with an asterisk (*)</td>
</tr>
<tr>
<td>Priority</td>
<td>Filter by the Priority field in the Asset table</td>
<td>Drop-down by Priority.</td>
</tr>
<tr>
<td>Business Unit</td>
<td>A group or department classification for the asset.</td>
<td>Text field. Empty by default. Wildcard strings with an asterisk (*)</td>
</tr>
<tr>
<td>Category</td>
<td>Filter by the Category field in the Asset table.</td>
<td>Drop-down by Category.</td>
</tr>
<tr>
<td>PCI domain</td>
<td>The PCI domain in which the asset is located</td>
<td>Drop-down by PCI domain.</td>
</tr>
<tr>
<td>Owner</td>
<td>Filter by the Owner field in the Asset table.</td>
<td>Text field. Empty by default. Wildcard strings with an asterisk (*)</td>
</tr>
<tr>
<td>Time Range</td>
<td>Select the time range to represent.</td>
<td>Drop-down: select to filter.</td>
</tr>
</tbody>
</table>
**Dashboard Panels**

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets by Priority</td>
<td>Displays the number of assets by priority level. The drilldown opens a search with the selected priority level.</td>
</tr>
<tr>
<td>Assets by Business Unit</td>
<td>Displays the relative amount of assets by business unit. The drilldown opens a search with the selected business unit.</td>
</tr>
<tr>
<td>Assets by Category</td>
<td>Displays the relative amount of assets by category. The drilldown opens a search with the selected category.</td>
</tr>
<tr>
<td>Asset Information</td>
<td>Shows all assets that match the current dashboard filters. The drilldown opens the Asset Investigator dashboard if the ip, nt_host, mac, or dns fields are selected. Any other field will open a search with the selected field.</td>
</tr>
</tbody>
</table>

**Data sources**

The reports in the Asset Center dashboard reference fields in the Asset and Identities data model. Relevant data sources include lists of assets and identities collected and loaded as lookups, scripted inputs, or search-extracted data.

**Identity Center**

Use the **Identity Center** dashboard to review and search for objects in the identity data added to Splunk. This table drives the correlation between user identity data and event data captured from the PCI resources sending data to Splunk. Identity data represents a list of account names, legal names, nicknames, and alternate names, along with other associated information about each identity.

**Filtering Identities in Identity Center**

The filter for the Identity Center dashboard uses a key=value pair search field. To filter identities, enter a key=value pair instead of a name or text string.

Some sample key=value pairs are email=*acmetech.com or nick=a_nickname.

Use the available dashboard filters to refine the results displayed on the dashboard panels.
<table>
<thead>
<tr>
<th>Username</th>
<th>A known or unknown user</th>
<th>Text field. Empty by default. Wildcard strings with an asterisk (*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Filter by the Priority field in the Identities table</td>
<td>Drop-down by Priority.</td>
</tr>
<tr>
<td>Business Unit</td>
<td>A group or department classification for the identity.</td>
<td>Text field. Empty by default. Wildcard strings with an asterisk (*)</td>
</tr>
<tr>
<td>Category</td>
<td>Filter by the Category field in the Identities table.</td>
<td>Drop-down by Category.</td>
</tr>
<tr>
<td>Watchlisted Identities Only</td>
<td>Filter by the identities tagged as &quot;watchlist&quot; in the Identities table.</td>
<td>Drop-down: select to filter by</td>
</tr>
<tr>
<td>Time Range</td>
<td>Select the time range to represent.</td>
<td>Drop-down: select to filter by</td>
</tr>
</tbody>
</table>

**Dashboard Panels**

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identities by Priority</td>
<td>Displays the count of Identities by priority level. The drilldown opens a search with the selected priority level.</td>
</tr>
<tr>
<td>Identities by Business Unit</td>
<td>Displays the relative number of Identities by business unit. The drilldown opens a search with the selected business unit.</td>
</tr>
<tr>
<td>Identities by Category</td>
<td>Displays the relative number of Identities by category. The drilldown opens a search with the selected category.</td>
</tr>
<tr>
<td>Identity Information</td>
<td>Shows a list of identities active in the PCI compliance environment, with details from the Identity table. Click &quot;View full results&quot; for more information about the event. The drilldown opens the Identity Investigator dashboard if the identity field is selected. Any other field opens a search with the selected field.</td>
</tr>
</tbody>
</table>

**Data sources**

The reports in the **Identity Center** dashboard reference fields in the Asset and Identities data model. Relevant data sources include lists of assets and identities collected and loaded as lookups, scripted inputs, or search extracted data.
**Predictive Analytics dashboard**

Use the Predictive Analytics dashboard to search for different varieties of anomalous events in your data. Predictive Analytics uses the predictive analysis functionality in Splunk to provide statistical information about the results, and identify outliers in your data. The predict command can take some time to generate results.

To analyze data with predictive analytics, choose a data model, then an object, a function, an attribute, and a time range, and click **Search**.

**Dashboard filters**

Use the available dashboard filters to refine the results displayed on the dashboard panels. The Predictive Analytics dashboard filters are implemented in a series from left to right. For example, the **Object** filter is populated based on the **Data Model** selection.

<table>
<thead>
<tr>
<th>Filter by</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Model</td>
<td>Specifies the data model for the search. Available data models are shown in</td>
</tr>
<tr>
<td></td>
<td>the drop-down list.</td>
</tr>
<tr>
<td>Object</td>
<td>Specifies the object within the data model for the search. You must select</td>
</tr>
<tr>
<td></td>
<td>a <strong>Data Model</strong> to apply an <strong>Object</strong>.</td>
</tr>
<tr>
<td>Function</td>
<td>Specifies the function within the object for the search. Functions specify</td>
</tr>
<tr>
<td></td>
<td>the type of analysis to perform on the search results. For example, choose</td>
</tr>
<tr>
<td></td>
<td>&quot;avg&quot; to analyze the average of search results. Choose &quot;dc&quot; to create a</td>
</tr>
<tr>
<td></td>
<td>distinct count of the results.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Specifies the constraint attributes within the object for the search.</td>
</tr>
<tr>
<td></td>
<td>Attributes are constraints on the search results. For example, choose &quot;src&quot;</td>
</tr>
<tr>
<td></td>
<td>to view results from sources. You must select an <strong>Object</strong> to apply an</td>
</tr>
<tr>
<td></td>
<td><strong>Attribute</strong>.</td>
</tr>
<tr>
<td>Time Range</td>
<td>Select the time range to represent.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Access to the options for the predict command.</td>
</tr>
</tbody>
</table>

You can find information about the predict command options in the Splunk platform documentation.

- For Splunk Enterprise, see predict options in the Splunk Enterprise Search Reference.
For Splunk Cloud, see predict options in the Splunk Cloud Search Reference.

**Dashboard Panels**

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prediction Over Time</td>
<td>The Prediction Over Time panel shows a predictive analysis of the results over time, based on the time range you chose. The shaded area shows results that fall within two standard deviations of the mean value of the total search results.</td>
</tr>
<tr>
<td>Outliers</td>
<td>The Outliers panel shows those results that fall outside of two standard deviations of the search results.</td>
</tr>
</tbody>
</table>

**Data sources**

The Predictive Analytics dashboard references data in any user selected data model. If the data model accelerations are unavailable or incomplete for the chosen time range, the dashboard reverts to searching unaccelerated, raw data.

**Create a correlation search**

From this dashboard, create a correlation search based on the search parameters for your current predictive analytics search. This correlation search will create an alert when the correlation search returns an event.

1. Click **Save as Correlation Search...** to open the Create Correlation Search dialog.
2. Select the Security domain and Severity for the notable event created by this search.
3. Add a search name and description.
4. Click **Save**.

![Create Correlation Search dialog](image)
To view and edit correlation searches, go to **Configure > Content Management**. See Configure correlation searches in the *Install and Upgrade Manual.*
Investigations

Investigations in Splunk App for PCI Compliance

Visualize and document the steps you take during an investigation by creating and adding details to an investigation in Splunk App for PCI Compliance.

- Start an investigation in Splunk App for PCI Compliance.
- Investigate a potential security incident on the investigation workbench in Splunk App for PCI Compliance.
- Add details to an investigation in Splunk App for PCI Compliance.
- Make changes to an investigation in Splunk App for PCI Compliance.
- Collaborate on an investigation in Splunk App for PCI Compliance.
- Review an investigation in Splunk App for PCI Compliance.
- Share or print an investigation in Splunk App for PCI Compliance.
- Review the summary of an investigation in Splunk App for PCI Compliance.

You can start, manage, and add details to investigations on the Investigations page. View or filter the investigations assigned to you, or create one. You can view all investigations that you collaborate on using the Investigations page. As an analyst, you can only see investigations assigned to you if you also have been granted the capability to manage all investigations.

Manage your investigations

Manage ongoing investigations from the Investigations page. You can see the titles, descriptions, time created, last modified time, and collaborators on the investigations assigned to you. If you have the capability to manage all investigations, you can see all the same details for all investigations, not just the investigations that you collaborate on.

Find an investigation or refine the list of investigations by filtering. Type in the Filter box to search the title and description fields of investigations.

Example investigation workflow

1. You are notified of a security incident that needs investigation through a notable event, an alert action, or by an email, ticket from the help desk, or
a phone call.
2. Create an investigation in Splunk App for PCI Compliance.
3. If you must work with someone else on the investigation, add them as a collaborator.
4. Investigate the incident. While you investigate, add helpful or insightful steps to the investigation.
   1. Run searches, adding useful searches to the investigation from your action history with the investigation bar or relevant events using event actions. This makes it easy to replicate your work for future, similar investigations, and to make a comprehensive record of your investigation process.
   2. Filter dashboards to focus on specific elements, like narrowing down a swim lane search to focus on a specific asset or identity on the asset or identity investigator dashboards. Add insightful filtering actions from your action history to the investigation using the investigation bar.
   3. Triage and investigate potentially related notable events. Add relevant notable events to the investigation.
   4. Add notes to record other investigation steps, such as notes from a phone call, email or chat conversations, links to press coverage or social media posts. Upload files like screenshots or forensic investigation files.
5. Complete the investigation and add a note to record a summary of your findings.

Start an investigation in Splunk App for PCI Compliance

You can start an investigation in several ways in Splunk App for PCI Compliance.

- Start an investigation from Incident Review while triaging notable events. See Add a notable event to an investigation.
- Start an investigation with an event workflow action. See Add a Splunk event to an investigation.
- Start an investigation from the Investigations dashboard.
- Start an investigation when viewing a dashboard using the investigation bar.

After you start an investigation, you can investigate assets and identities using the investigation workbench, and start adding details to the investigation.
By default, users with the \texttt{pci\_admin} and \texttt{pci\_analyst} roles can start an investigation.

**Start an investigation from the Investigations dashboard**

Start an investigation from the Investigations dashboard.

1. Click \texttt{Create New Investigation}.
2. Type a title.
3. (Optional) Select a status.
4. (Optional) Type a description.
5. Click \texttt{Save}.

**Start an investigation from the investigation bar**

When viewing dashboards in Splunk App for PCI Compliance, you can see an investigation bar at the bottom of the page. You can use the investigation bar to track your investigation progress from any page in Splunk App for PCI Compliance.

1. Click the \texttt{+} icon to create an investigation.
2. Type a title.
3. (Optional) Select a status.
4. (Optional) Type a description.
5. Click \texttt{Save}.

The investigation is loaded in the investigation bar.

**Investigate a potential security incident on the investigation workbench in the Splunk App for PCI Compliance**

Investigate assets and identities, or artifacts, involved in a potential security incident on the investigation workbench. After you create an investigation in the Splunk App for PCI Compliance, you can start using the workbench for that investigation. Each investigation has a separate workbench.

When you investigate artifacts on an investigation workbench, by default you see Context, Endpoint Data, and Network Data tabs. Those tabs contain panels that help you gain context into the assets and identities you investigate,
endpoint-related data such as file system activity, and network data such as network traffic.

Add artifacts to the scope of your investigation

As part of your investigation on the workbench, you can add assets and identities as artifacts to the scope of your investigation so that you can verify whether or not they are affected by, or participants in, the overall security incident.

- Add artifacts automatically from a notable event. See Set up artifact extraction for notable events in this manual.
- Add artifacts manually. See Manually add artifacts to the scope of your investigation in this topic.
- Add artifacts from a workbench panel. See Add artifacts from a workbench panel in this topic.
- Add artifacts from an event on the investigation. See Add artifacts from a raw event on the investigation in this topic.

For example, if you’re investigating a malware outbreak at your organization, you can add hosts to the scope that you suspect are infected with malware without adding the associated events to the timeline and recording them as verifiably compromised. Add them to the scope first and review the relevant panels for additional context. If you discover that an artifact is part of the security incident you are investigating, you can add the event or detail that revealed that insight to the investigation to record that information for later.

You can add any value as an artifact on the workbench. Assets and identities added as artifacts to the scope are not limited to the assets and identities in the asset and identity framework in the Splunk App for PCI Compliance.

Manually add artifacts to the scope of your investigation

You can manually add artifacts such as assets and identities to the scope of your investigation on the workbench.

1. From the PCI menu bar, select Investigations.
2. Open an investigation to view the workbench for that investigation.
3. On the Artifacts panel, click Add Artifact.
   ♦ To add one artifact, use the default Add artifact tab:
     1. For Artifact, type the value of the asset or identity.
     2. For Type, select the type of the artifact: asset or identity.
     3. (Optional) Type a description.
        For example, Personal computer infected by ransomware.
4. (Optional) Type one or more labels to contextualize the entity. Use a comma or press enter to add multiple labels. For example, ransomware, laptop, mac.

5. (Optional) Click **Expand Artifacts** to look up the asset or identity in the asset or identity lookups and add the correlated artifacts to the investigation scope.

To add multiple artifacts:
1. Select **Add multiple artifacts**.
2. Select the type: asset or identity. All artifacts that you add must be the same type.
3. You can use a comma or a line break as a delimiter. Select a **Separator** that delimits the list of assets or identities.
4. Type or paste the values for the assets or identities, using the separator specified in the previous step.
5. (Optional) Type a description to apply to all assets or identities that you are adding.
   For example, Potentially-infected computers in the HR department.
6. (Optional) Type one or more labels to apply to all assets or identities that you are adding.
   For example, infected, maybe, HR.

4. Click **Add to Scope** to add the artifacts to your investigation scope.

The artifacts that you add to your investigation scope manually are automatically selected so that you can click **Explore** and continue your investigation with the new artifacts.

**Add artifacts from a workbench panel**

If a workbench panel has drilldown enabled, you can add field values as artifacts from the panel.

1. Open the investigation and view the workbench.
2. Select artifacts and click **Explore**.
3. In a panel, click a field value.
   The Add Artifact dialog box appears with the value already added.
4. Select a **Type** for the artifact. Some types, such as IP addresses, are automatically detected.
5. (Optional) Add a description for the artifact.
6. (Optional) Add labels for the artifact.
7. (Optional) Click **Expand Artifacts** to look up the asset or identity in the asset or identity lookups and add the correlated artifacts to the investigation scope.
8. Click **Add to Scope** to add the artifact to your investigation scope.

The ability to add artifacts replaces any other drilldown that might exist on the panel. See **Administer and customize the investigation workbench** in this manual.

**Add artifacts from a raw event on the investigation**

After you add an event to the investigation, you can add field values from the event as artifacts to your investigation scope.

1. Open the investigation and view the **Timeline** of the investigation.
2. Locate the event in the **Slide View**.
3. Click **Details** to view a table of fields and values in the event.
4. Click the value that you want to add to the investigation scope.
   The Add Artifact dialog box appears with the value already added.
5. Select a **Type** for the artifact. Some types, such as IP addresses, are automatically detected.
6. **(Optional)** Add a description for the artifact.
7. **(Optional)** Add labels for the artifact.
8. **(Optional)** Click **Expand Artifacts** to look up the asset or identity in the asset or identity lookups and add the correlated artifacts to the investigation scope.
9. Click **Add to Scope**.

**Adjust the time range of your investigation**

If there are notable events on the investigation, the workbench searches over a suggested time range based on the times of the notable events on the investigation. Time analysis suggests a time range based on the `_time` value of the earliest and latest notable events on the investigation.

If there are no notable events on an investigation, the workbench uses your default time range settings. See **Change the default time range in the Search Manual**.

If a time range is defined in the XML or in the search of a prebuilt panel, that time range takes precedence over the time range that you choose on the workbench.

**Add new tabs and profiles to the workbench**

Your administrator can develop additional panels, tabs, and profiles, which you can then add to the workbench to further simplify your investigation process. See **Administer and customize the investigation workbench**.
Add the new profiles and tabs to an investigation workbench.

1. Open an investigation and click **Explore** to explore artifacts on the workbench.
2. Click **Add Content**.
3. To load a profile on the workbench, click **Load profile**.
   1. Select a profile.
   2. Click **Save**.
4. To add a tab to the workbench, click **Add single tab**.
5. Select a profile or a tab.
   1. Click **Save**.

Tabs and profiles that you add to the investigation workbench disappear when you refresh the workbench. Only the default tabs display.

**Add details to an investigation in Splunk App for PCI Compliance**

As an analyst working on an investigation, add details and evidence to your investigation by adding events, actions, and notes. While you conduct your investigation using Splunk App for PCI Compliance, you can add notable events or Splunk events that add insight to the investigation. Add searches, suppression filters, and dashboard views to the investigation from your action history. Record important investigation steps that you take, such as phone, email, or chat conversations as notes on the investigation. You can use notes to add relevant information like links to online press coverage, tweets, or upload screenshots and files.

**Run a quick search from the investigation bar**

Run a search without opening the search dashboard by clicking **Quick Search** on the investigation bar.

- Add the search to the investigation in the investigation bar by clicking **Add to Investigation**.
- Use the **Event Actions** to add specific events in the search results to an investigation.
- To save the search results at investigation time, click **Export** to export the search results as a CSV file. Add the search results as an attachment to a
note on the investigation.

- Click **Open in Search** to view the search results on the Search dashboard.
- Enlarge or shrink your view of the search results by clicking and dragging the corner of the window. Double click to expand the search view to cover most of your screen, or double click again to shrink it.

**Add a notable event to an investigation**

You can add a notable event to an investigation from the Incident Review dashboard. See **Add a notable event to an investigation**.

If the status of a notable event changes, or if an adaptive response action is run from the notable event, the investigation is updated with that information.

**Add a Splunk event to an investigation**

Add an event from the Splunk search page to an investigation. You can only add an event to an investigation from the search page in the Splunk App for PCI Compliance context.

1. Expand the event details to see the **Event Actions** menu and other information.
2. Click **Event Actions** and select **Add to Investigation**.
3. A tab opens. Select from existing investigations, or create one.
4. Click **Save**.

**Add an entry from your action history to an investigation**

The action history stores a history of the actions that you have performed in Splunk App for PCI Compliance, such as searches that you have run, dashboards you have viewed, and per-panel filtering actions that you have performed.

Add an entry to an investigation from your action history with the investigation bar. Search for specific types of action history items over time to find the action history items that you want to add to your investigation.

1. From the investigation bar, click the ⌡ icon.
2. Select an action history type and optionally change the time range.
3. Click **Search** to retrieve a list of action history items.
4. Find the actions that you want to add to the investigation. For example,
view the dashboards that you viewed to add them to your investigation.

![Image of Add Action History](image)

5. The actions that you’ve taken display in the action history dialog box. You can only add actions from your own action history.

6. Locate the action you want to add and select the check box next to the action or actions that you want to add to the investigation timeline.

7. Click **Add to Investigation**.

   The actions are added to the investigation that you are viewing or that is selected in the investigation bar.

See Refer to your action history.

### Add a note to an investigation

Add a note to an investigation to record investigation details or add attachments. You can add a note from dashboards in Splunk App for PCI Compliance.

1. From the investigation bar, click the **Note** icon.

2. Type a title.
   
   For example, "Phone conversation with police."

3. (Optional) Select a time. The default is the current date and time.
   
   For example, select the time of the phone call.

4. (Optional) Type a description.
   
   For example, a note to record a phone conversation might include the description: Called the police. Spoke with Detective Reggie Martin. Discussed an employee stealing identities from other employees.
5. (Optional): Attach a file to the note.
   1. From the note, click the  icon or drag the file onto the note.
   2. Select a file to add from your computer.
      The maximum file size is 4 MB. You can add multiple files to a note.
      The first file you add to the note previews on the investigation timeline.
   6. Click **Add to Investigation** to add the note to the open investigation or click **Save as Draft**.

When you save a note as a draft, it stays associated with the investigation that was selected when you created the note but does not appear on the investigation. Retrieve draft notes by clicking the  icon.

**Make changes to an investigation in Splunk App for PCI Compliance**

Make changes to the entries on an investigation from the timeline list or slide view.

**Change the title and description of an investigation**

Change the title and description of an investigation from the investigation bar. For example, change the name of the investigation as your investigation progresses to more accurately describe the security incident you are investigating.
1. From the investigation bar, click the icon. From the investigation view, click Edit.
2. Change the title or description.
3. Click Save.

**Update the status of an investigation**

Update the status of an investigation from the workbench, summary, or timeline view.

1. While viewing the investigation, click Edit > Edit title, description, and status.
2. Select a new status.
3. Click Save.

You can also update the status of an investigation from the investigation bar.

1. Click the icon and select your investigation.
2. After loading your investigation into the investigation bar, click the icon and select a status.
3. Click Save.

Similar to notable events, administrators can customize the statuses available to select, and restrict the status workflow. Because of this, you might not be able to transition from some statuses to other statuses. See Manage and customize investigation statuses in this manual.

**Delete investigation entries**

You can delete investigation entries when viewing the investigation timeline list or slide views.

1. Find the entry on the investigation.
2. Click Action > Delete Entry.
3. Click Delete to confirm deleting the entry.

To delete multiple entries:

1. Click List to view the investigation as a list of entries.
2. Select the check box next to the investigation entries that you want to delete.
3. Click Action and select Delete.
4. Click Delete to confirm deleting the entry.
Change a note

1. Find the note in the investigation and open the note for editing.
   1. From the timeline view of the investigation click **Action > Edit Note**
   2. From the list view of the investigation click **Edit** in the **Actions** column.
2. Make changes. For example, add a new attachment and add a sentence to the description describing the new attachment.
3. Remove a file attachment by clicking the X next to the file name.
4. Click **Save**.

Change the title of an entry

You can change the title of an entry to make it more clear.

1. Locate the notable event, Splunk event, action history item, or other entry on the investigation.
2. From the **Actions** menu, click **Edit**.
3. Change the title.

Collaborate on an investigation in Splunk App for PCI Compliance

You can collaborate with other analysts on an investigation.

Add a collaborator to an investigation

1. Open the investigation that you want to add a collaborator to.
2. Click the icon.
3. Type the name of the person you want to add and select their name from the list to add them to the investigation.
4. Their initials appear in a circle to confirm that they were added.

You can add any Splunk user in your deployment as a collaborator. By default, a collaborator has write permissions on the investigation.

**View the collaborators assigned to an investigation**

You can view the collaborators assigned to an investigation from an individual investigation or from the Investigations dashboard.

- Hover over the collaborator icons to see the names of the collaborators on your investigation.
- If a collaborator does not have write permissions for an investigation, the icon is gray and *(read-only)* is appended to their name.
- Click the icon of a collaborator to see information about them. See their name and the permissions that the user has for the investigation.

![Collaborator](image)

**Make changes to the collaborators on an investigation**

If you are a collaborator on an investigation with write permissions, you can change the permissions of other collaborators on the investigation.

1. Click the icon of a collaborator.
2. Change the **Write permissions**. By default, all collaborators have **Yes** for **Write permissions**. All investigations must have at least one collaborator with write permissions.

You can remove a collaborator if they are not the only collaborator on the investigation with write permissions.

1. Click the icon of a collaborator.
2. Click **Remove**.
Review an investigation in Splunk App for PCI Compliance

Revisit past investigations, or view a current investigation by clicking the title from the investigation bar or from the Investigations dashboard. Users with the capability to manage all investigations can view all investigations. Only collaborators on an investigation with write permissions can edit an investigation.

You can also review the summary of an investigation. See Review the summary of an investigation in Splunk App for PCI Compliance.

Review the entries investigation for training or research purposes. Click an entry on an investigation to see all details associated with it.

- For notes with file attachments, click the file name to download the file attachment.
- For notable events, click View on Incident Review to open the Incident Review dashboard filtered on that specific notable event.
- For action history entries, you can repeat the previously-performed action. For a search action history entry, click the search string to open it in search. For a dashboard action history entry, click the dashboard name to view the dashboard.
Gain insight into an attack or investigation by viewing the entire timeline of the investigation or view only part of it by expanding or contracting the timeline.

Click the timeline to move it and scan the entries. View a chronological list of all timeline entries by clicking the list icon, or refine your view of the timeline using filters. You can filter by type or use the Filter box to filter by title.

**Review the status history of an investigation**

You can review the status history of an investigation visually on the investigation timeline. The timeline changes color to reflect changes in status assignments. The color does not relate directly to the status of the investigation, and is automatically assigned. The colors cannot be changed, customized, or removed.

**Share or print an investigation in Splunk App for PCI Compliance**

To share an investigation with someone that does not use Splunk App for PCI Compliance, such as for auditing purposes, you can print any investigation or save any investigation as a PDF.

1. From the investigation, click the icon. Splunk App for PCI Compliance generates a formatted version of the investigation timeline with entries in chronological order.
2. Print the investigation or save it as a PDF using the print dialog box options.

**Refer to your action history in Splunk App for PCI Compliance**

While you investigate an attack or other security incident, actions that you take in Splunk App for PCI Compliance are recorded in your action history. You can only view your own entries in your action history. After you add an item to an investigation, all collaborators on the investigation can view that entry.

Your action history tracks the following types of actions using searches:

- Dashboards you visit
- Searches you run
• Per-panel filtering actions you take
• Changes you make to a notable event
• Changes you make to the suppression filters of a notable event

When you select a type of action history to add an investigation, the corresponding search runs to retrieve results. Splunk App for PCI Compliance tracks these actions to help you add context to an investigation, audit an investigation, and give a complete history of actions taken during an investigation that resulted in relevant findings.

For example, if you run a search that gives helpful information for an investigation, you can add that search to the investigation. You can then find that search string in the investigation, run the search again, or revisit a search to save it as a report when the investigation is over. See Add an entry from your action history to an investigation for more about using your action history when investigating in Splunk App for PCI Compliance.

Review the summary of an investigation in Splunk App for PCI Compliance

Every investigation in Splunk App for PCI Compliance includes a summary. From an investigation, click Summary to view the summary. The summary provides an overview of the notable events and the artifacts, or investigated assets and identities, that are associated with your investigation.

You can use the summary to provide an overview of an investigation to a manager or to get an overview of the current state of an investigation before you continue working on it.

The summary reflects a point in time of the investigation, rather than the overall progress of an investigation. Therefore, the artifacts listed on the summary page reflect the artifacts present at the end of the investigation, rather than all artifacts that you investigated on the workbench.

Administer and customize the investigation workbench

The workbench extends existing investigation functionality in Splunk App for PCI Compliance by allowing analysts to perform investigative actions in one location.
Analysts investigate artifacts, or assets and identities, using panels, tabs, and profiles on the workbench. You can customize the workbench by creating panels, tabs, and profiles to help analysts. You can also set up artifact extraction from notable events to accelerate investigations that start from notable events.

The workbench introduces a configuration file, `es_investigations.conf`, that is used to manage the metadata for panels, tabs, and profiles. You can make changes in the file system by adding stanzas to the `es_investigations.conf` file. Refer to `es_investigations.conf.spec` and `es_investigations.conf.example` for details.

**Create panels and tabs for the investigation workbench**

The investigation workbench can display any prebuilt panel that has a workbench panel reference and has been added to a workbench tab.

1. Create or modify a prebuilt panel. See Create or modify a prebuilt panel for the investigation workbench in this topic.
2. Create a workbench panel that references the prebuilt panel. See Create a tab for the investigation workbench in this topic.
3. Create a workbench tab that includes the workbench panel. See Create a tab for the investigation workbench in this topic.

For an example of this entire process, see Example panel conversion and workbench panel creation in this topic.

**Create or modify a prebuilt panel for the investigation workbench**

You can use any prebuilt panel on the investigation workbench. You can create one specifically for the workbench, or you can modify an existing panel. You can create or modify a prebuilt panel with Splunk App for PCI Compliance in several ways:

- Create a panel from Content Management.
  1. From the PCI menu bar, select Configure > Content Management.
  2. Select Create New Content > Panel.
  3. Type a Prebuilt panel ID.
  4. Select a Destination App.
  5. Type Prebuilt panel XML.
  6. Click Save.
- Convert a dashboard panel to a prebuilt panel. See Convert an existing panel to a prebuilt panel in Dashboards and Visualizations.
Modify a panel in Splunk Settings.

1. From the Splunk menu bar, select Settings > User Interface.
2. Click Prebuilt Panels and click Edit > Edit Panel for the panel that you want to modify.

If you modify an existing prebuilt panel, consider cloning it before you modify it. If you clone the panel, change the panel ID so that you remember which one is specific to the workbench.

• Create a panel in Splunk Settings. See Add panels to dashboards in Dashboards and Visualizations.

When creating or modifying a prebuilt panel for the workbench, follow these guidelines for the best user experience:

• Add one or more tokens to the panel search to limit your search results to the artifacts investigated on the workbench. Use multiple tokens to substitute more than one type of artifact. Define your token using the syntax $token$. You set up the format of the token when you create the workbench panel.
• Remove the panel name from the panel XML. If you do not do this, two panel titles appear on the workbench. Workbench panels get the title from the Label field when you create a workbench panel.
• Add a drilldown to the panel so that analysts can add artifacts from the panel. Add a drilldown using the syntax <option name="drilldown">cell</option> in the panel XML. The workbench replaces existing panel drilldowns, such as custom searches, with this ability to add artifacts to the workbench scope from the panel.
• Update the permissions on the panel to be shared with Splunk App for PCI Compliance. Confirm that the panel is Shared in App or set to Display For: All Apps.
• (Optional) To make your panel use a different time range than the one set by the workbench, set a time range in the panel search or panel XML.

Then, follow the steps to create a panel for the investigation workbench. See Create a panel for the investigation workbench in this topic.

Create a panel for the investigation workbench

Create a workbench panel.

1. Select Configure > Content Management.
2. Select Create New Content > Workbench Panel.
3. Select the prebuilt panel that you want to use on workbench from the drop-down list.
4. (Optional) Type a Label to replace the default panel title on the workbench.
5. (Optional) Type a Description to provide information about the panel.
6. Add a token to replace the token in the panel search. See Example panel conversion and workbench panel creation in this topic or see Define tokens for multiselect inputs in the Splunk Enterprise Dashboards and Visualizations Manual.
7. Click Save.

Then add the panel to a tab so that it is visible on the workbench.

*Create a tab for the investigation workbench*

Create a tab to display information specific to a particular data type, use case, or something else.

1. Select Configure > Content Management.
2. Select Create New Content > Workbench Tab.
3. Type a Tab Name. This name becomes part of the stanza name in `es_investigations.conf` and is used as the label if you do not specify a label.
4. (Optional) Type a Label to provide a user-facing name for the workbench tab.
5. In Workbench Panels, select the panels that you want to appear on this tab. The order in which you select the panels is the order in which they appear on this tab on the workbench.
6. (Optional) Select a workbench profile to associate with this tab. You can only associate a tab with one profile. Profiles allow analysts to load multiple tabs that relate to a use case on the workbench.
7. (Optional) Change the Load by default selection. Select True if you want this tab to load for all workbench investigations.
8. (Optional) Type a Description for the tab. This helps analysts determine what types of information and context they can gather using the panels on the tab.
9. Click Save.

*Example panel conversion and workbench panel creation*

Prerequisite
You must have the Splunk Add-on for Blue Coat ProxySG installed, and data from the add-on in your Splunk App for PCI Compliance deployment. You can download the Splunk Add-on for Blue Coat ProxySG from Splunkbase.

1. Clone a panel and modify the search to use an input token with the workbench.
   1. Select Settings > User Interface.
   2. Click Prebuilt panels.
   3. Click Edit > Clone for the actions_by_destination_ip for the Splunk_TA_bluecoat-proxysg.
   4. Type a Prebuilt panel ID. workbench_actions_by_dest_ip.
   5. Remove the title from the XML, unless you want two titles to appear on the workbench.
   6. Modify the query in the XML to include a token that limits the results to the investigated asset artifacts.
      sourcetype="bluecoat:proxysg:access*" $dest_token$ | iplocation dest | geostats count by action
   7. Decide whether to remove the <earliest> and <latest> time range for the panel. This time range takes precedence over the time range set on the workbench, so you likely want to remove it so that analysts can perform context-sensitive searches.
   8. Click Save.

2. Modify the permissions of the panel.
   1. Locate the panel that you just created, workbench_actions_by_dest_ip.
   2. Select Edit > Edit Permissions.
   3. For Display for, select All apps.
   4. Click Save.

3. Return to Splunk App for PCI Compliance and set up the panel to be used on the workbench.
   1. Select Configure > Content Management.
   2. Select Create New Content > Workbench Panel.
   3. Select a Panel Name of workbench_actions_by_dest_ip.
   4. (Optional) Type a user-facing Label that appears on the workbench: Proxy Actions by Destination.
   5. (Optional) Type a user-facing description that appears on the workbench: Displays a map that graphs the actions by destination IP, when possible, specific to the investigated assets.
   6. Click Add a Token to add a token for the $dest_token$ from the search.
   7. Type a Token Name that corresponds to the token name. dest_token
8. Type a **Prefix** of (.
9. Type a **Suffix** of ).
10. Type a **Value Prefix** of dest=".
11. Type a **Value Suffix** of ".
12. Unselect the check box for **Is Null** for the **Delimiter** and type **or** in the text box. Include the spaces on either side of the OR.
13. Leave the check box for **Is Null** for the **Default field** selected. If this check box is selected, the search runs only when an artifact of the relevant type is selected on the workbench. In this case, the search runs only if you are exploring assets on the workbench.
14. Select a **Type** of **Artifact**.
15. Select a **Field Type** of **Asset**, because the destination is an asset, not an identity.
16. Click **Save**.

This panel now contains a search that would be constructed as follows for two assets investigated on the workbench:

```plaintext
sourcetype="bluecoat:proxysg:access*"
(dest="<investigated_asset_1>" OR dest="<investigated_asset_2>") | iplocation dest | geostats count by action
```

4. Add the new panel to a new tab.
   1. On Content Management, select **Create New Content > Workbench Tab**.
   2. Type a **Tab Name** of **proxy_data**. This name becomes the stanza name in es_investigations.conf and is used as the label if the label is not specified.
   3. (Optional) Type a **Label** of **Proxy Data**.
   4. In **Workbench Panels**, type and select the **Proxy Actions by Destination IP** panel.
   5. For **Load by default**, leave it as **False**. Select True if you want this tab to load for all workbench investigations.
   6. (Optional) Type a **Description** for the tab. **Proxy data related to investigated assets and identities**.
   7. Click **Save**.

Analysts can then open a workbench and add the new tab to start investigating proxy data in the workbench.

**Create a workbench profile**

You can use profiles on the workbench to associate several tabs together that all fit a specific use case. For example, a DDoS Investigation profile might include a
Firewall data tab and a general Network data tab. An analyst can then add the DDoS Investigation profile to an investigation to add both of those tabs to the workbench, rather than having to individually add tabs that fit the investigation.

1. Select **Configure > Content Management**.
2. Select **Create New Content > Workbench Profile**.
3. Type a **Profile Name**. This name becomes the stanza name in `es_investigations.conf` and is used as the label if the label is not specified.
4. (Optional) Type a **Label** to provide a user-facing name for the workbench profile.
5. (Optional) Type a **Description** for the profile. This helps analysts determine what types of information and context they can gather by adding the profile to their investigation.
6. Click **Save**.

After creating a profile, update the tabs with the profile that you created. For the DDoS investigation example, edit the Firewall data and Network data tabs and select the new DDoS Investigation profile.

**Set up artifact extraction for notable events**

For each correlation search with a notable event associated with it, you can define the fields that are automatically extracted as identities or assets on the workbench when the notable event is added to an investigation. By default, the same fields that are used for asset and identity correlation are the fields extracted from the notable events created by included correlation searches. You must add fields to be extracted for any custom correlation searches.

<table>
<thead>
<tr>
<th>Type of investigation artifact</th>
<th>Fields extracted for investigation scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td><code>dest, src, dvc, orig_host</code></td>
</tr>
<tr>
<td>Identity</td>
<td><code>user, src_user</code></td>
</tr>
</tbody>
</table>

If your correlation search does not use data models, or the search results contain different fields that you want to extract, you can specify the fields to extract into the investigation scope.

1. Select **Configure > Content Management**.
2. Click the correlation search that you want to customize to open it for editing.
3. Select the notable event adaptive response action.
4. For **Asset Extraction**, type a field name from the correlation search results that identifies an asset. Press Enter to add the field name.
5. For **Identity Extraction**, type a field name from the correlation search results that identifies an identity. Press Enter to add the field name.

6. Click **Save**.

**Manage and customize investigation statuses in Splunk App for PCI Compliance**

Starting in version 3.5.0, you can add statuses to investigations. After upgrading to this version, investigations that did not have a status are assigned the **New** status.

To change the status of an investigation, an analyst must have the `transition_reviewstatus-<x>_to_<y>` capability for the statuses that they want to transition between. The `ess_analyst` role and the `ess_admin` role have those capabilities for all statuses by default. Modifying status transitions for investigations modifies these capabilities.

To make changes to statuses as an analyst, you must have the `edit_reviewstatuses` capability. The `ess_admin` role has this capability by default. See Configure users and roles in the *Installation and Configuration Manual*.

**Create an investigation status**

Create a status for analysts to select when performing an investigation.

If you restrict status transitions, update status transitions after creating a status, otherwise analysts will be unable to select the new status. See **Restrict status transitions for investigations** in this topic.

1. From the PCI toolbar, select **Configure > Incident Management > Status Configuration**.
2. (Optional) Select the **Investigation** tab to review existing investigation statuses.
3. Select **Create New Status > Investigation**.
4. Type a **Label** that appears as the name of the status on the investigation. For example, Waiting on Desktop IT.
5. (Optional) Type a **Description** that appears on the **Status Configuration** page to describe the status. For example, Investigation is waiting for desktop IT to perform additional remediation or forensics steps.
6. (Optional) Select the check box for Default Status to set this status as the default for newly-created investigations.
7. (Optional) Select the check box for End Status to set this status as a possible last status for an investigation.
8. (Optional) Deselect the check box for Enabled to create the status without allowing anyone to use it yet.
9. Update the user roles that are able to transition an investigation from this new status, for example Waiting on Desktop IT, to another status, such as Closed. If you do not select any roles that can transition from this status to another one, no one will be able to move the investigation to a different status after transitioning the investigation to this status.
10. Click Save.

Restrict status transitions for investigations

The status transitions that can be made on an investigation define the path of an investigation. By default, an investigation in any status can be changed to any other status. For example, someone can change the status of an investigation in the New status to any other status, such as Closed.

You can restrict the statuses that analysts can choose when investigating. Determine which statuses to require, and whether analysts must follow a specific sequence of statuses before completing an investigation. Determine whether any roles can bypass the full sequence of statuses.

This example walks you through setting up restricting status transitions for analysts. Restrict status transitions so that analysts must follow a path from New, to In Progress or Pending, to Resolved, then to Closed.

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>In Progress</td>
<td>Pending</td>
<td>Resolved</td>
</tr>
</tbody>
</table>

Prerequisites

- You must have the pci_admin role or your role must be assigned the Edit Statuses capability. For more information about user roles and capabilities, see Configure users and roles in the Installation and Configuration Manual.
1. On the PCI toolbar, select Configure > Incident Management > Status Configuration.
2. Click the Investigation tab.
3. Restrict the transitions from the New status. Select the New status to open the Edit Investigation Status page.
4. In Status Transitions, select the roles for the Resolved status and deselect the check box for the ess_analyst role.
5. Select the roles for the Closed status and deselect the check box for the ess_analyst role.
6. Click Save to save the changes to the New status.
7. Restrict the transitions on the In Progress and Pending statuses to prevent the ess_analyst role from transitioning to New or to Closed.
8. Click the Investigation tab and select the In Progress status.
9. In Status Transition, select the roles for the New status and deselect the check box for the ess_analyst role. Repeat for the Closed status.
10. Click Save to save the changes to the In Progress status. Repeat those steps for the Pending status.
11. Restrict the Resolved status. Click the Investigation tab and select the Resolved status.
12. In Status Transition, select the roles for the New status and deselect the check box for the ess_analyst role. Repeat for the In Progress and Pending statuses.
13. Click Save to save the changes to the Resolved status.
14. Restrict the transitions for the Closed status. Click the Investigations tab and select the Closed status.
15. In Status Transition, select the roles for the New status and deselect the check box for the ess_analyst role. Repeat for the In Progress, Pending, and Resolved statuses.
16. Click Save to save the changes for the Closed status.
Asset and Identity Management

Asset and Identity Correlation

The Splunk App for PCI Compliance compares indexed events with asset and identity data in the asset and identity lists to provide data enrichment and context. See Configure assets and Configure identities in the Installation and Configuration Manual.

The comparison process uses automatic lookups. See Make your lookup automatic in the Knowledge Manager Manual.

Asset and identity correlation enriches events with asset and identity data at search time.

- Asset correlation compares events that contain data in any of the src, dest, or dvc fields against the merged asset lists for matching IP address, MAC address, DNS name, or Windows NetBIOS names.
- Identity correlation compares events that contain data in any of the user or src_user fields against the merged identity lists for a matching user or session.
- The Splunk App for PCI Compliance adds the matching output fields to the event. For example, correlation on the asset src field results in additional fields such as src_is_expected and src_should_timesync.

Asset and identity correlation allows you to determine whether multiple events can relate to the same asset or identity. You can also perform actions on the identity and asset fields added to events to open additional searches or dashboards scoped to the specific asset or identity. For example, open the Asset Investigator dashboard on a src field.

Asset and identity correlation uses several potential match points to establish asset and identity correlations:

- A dashboard view: A flashtimeline looking at indexed raw events or the Asset Center dashboard.
- A point in time reference: A summary or lookup generation that pulls in identity or asset information for later use.
- An alert generation: An email or a script or a report. Notable events do not match in the alert generation category.
- Correlation searches: These searches also match on point-in-time data.
Note: Write searches that look for "individuals matching criteria", and not "emails and account names like this" so that these matches will work correctly.

How asset and identity correlation functions over time

Asset and identity correlation is valuable over time provided that you write searches that refer to asset and identity fields, rather than field values and you keep asset and identity lists updated. This example shows you why this is important.

Month one: In the first month, SERVER42 is at address 192.168.1.1 and is owned by Tom Pynchon, whose email is tpynchon@yoyodyne.com and phone number is 510-555-1212.

Views, dashboards, and searches in the Splunk App for PCI Compliance use this data. Summaries run, some notable events are generated, and some alerts are sent, all using this information.

<table>
<thead>
<tr>
<th>Month</th>
<th>Owner</th>
<th>IP address</th>
<th>hostname</th>
<th>email</th>
<th>phone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tom Pynchon</td>
<td>192.168.1.1</td>
<td>SERVER42</td>
<td><a href="mailto:tpynchon@yoyodyne.com">tpynchon@yoyodyne.com</a></td>
<td>510-555-1212</td>
</tr>
</tbody>
</table>

In month one, two correlation searches are run by the Yoyodyne security admin:

- A custom correlation search looking for "tpynchon@yoyodyne.com". This works fine in month one.
- A custom correlation search looking for "(user_is_privileged="true" OR user_priority="critical" OR user_priority="high")". This also works fine in month one.

Month two: In the second month, Yoyodyne is assimilated by Wintermute. Because Wintermute is very efficient, the lookup tables (asset lists and identity lists, and so on) are updated immediately. Now SERVER42 is at address 172.16.42.42, Tom is the owner, but his email is now tpurhaus@wintermute.net, his phone is 888-123-4567.

Dashboards, views, and searches update to use the new information everywhere. Alerts also use the new information, unless they are using old summary or lookup data.

<table>
<thead>
<tr>
<th>Month</th>
<th>Owner</th>
<th>IP address</th>
<th>hostname</th>
<th>email</th>
<th>phone number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Tom Pynchon</td>
<td>172.16.42.42</td>
<td>SERVER42</td>
<td><a href="mailto:tpurhaus@wintermute.net">tpurhaus@wintermute.net</a></td>
<td>888-123-4567</td>
</tr>
</tbody>
</table>
In month two the two correlation searches are run again by the Yoyodyne security admin:

- The custom correlation search looking for "tpynchon@yoyodyne.com" fails to generate a notable event when Tom emails his friend Bill with some secret files.
- The custom correlation search looking for "(user_is_privileged="true" OR user_priority="critical" OR user_priority="high")" generates a notable event when Tom emails his friend Bill with some secret files.

Month three: In month three, Tom leaves Wintermute to go work with Bill. His role administering SERVER42 is taken over by Jane Doe, whose email address is jdoe6@wintermute.net and phone number is 888-123-9876.

In month three, the two correlation searches are run again by the Yoyodyne security admin:

- The custom correlation search looking for "tpynchon@yoyodyne.com" still does not work.
- The custom correlation search looking for "(user_is_privileged="true" OR user_priority="critical" OR user_priority="high")" still works.

In this example, correlation searches continue to work correctly if the ownership relationship for SERVER42 is updated in the asset list.

<table>
<thead>
<tr>
<th>Month</th>
<th>Owner</th>
<th>IP address</th>
<th>hostname</th>
<th>email</th>
<th>phone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tom Pynchon</td>
<td>192.168.1.1</td>
<td>SERVER42</td>
<td><a href="mailto:tpynchon@yoyodyne.com">tpynchon@yoyodyne.com</a></td>
<td>510-555-1212</td>
</tr>
<tr>
<td>2</td>
<td>Tom Pynchon</td>
<td>172.16.42.42</td>
<td>SERVER42</td>
<td><a href="mailto:tpurhaus@wintermute.net">tpurhaus@wintermute.net</a></td>
<td>888-123-4567</td>
</tr>
<tr>
<td>3</td>
<td>Jane Doe</td>
<td>172.16.42.42</td>
<td>SERVER42</td>
<td><a href="mailto:jdoe6@wintermute.net">jdoe6@wintermute.net</a></td>
<td>888-123-9876</td>
</tr>
</tbody>
</table>

Looking at the same incident for SERVER42 over the three month period would show three different phone numbers, always displaying the current number. Keeping asset and identity lists accurate and up-to-date is necessary for asset
and identity correlation to function properly.
Resources

Search View Matrix

Correlation search thresholds


Dashboard searches

These searches support dashboard panels in the user interface. Most dashboard panels are populated with data from accelerated data models, however some searches use the underlying raw data as well.

Requirement 1 Reports

<table>
<thead>
<tr>
<th>Search or Dashboard</th>
<th>Firewall Rule Activity</th>
<th>Network Traffic Activity</th>
<th>Prohibited Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network - Communication Rule Tracker - Lookup Gen</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint - Listening Ports Tracker - Lookup Gen</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Endpoint - Local Processes Tracker - Lookup Gen</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Endpoint - Services Tracker - Lookup Gen</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Requirement 2 Reports

<table>
<thead>
<tr>
<th>Search or Dashboard</th>
<th>Default Account Access</th>
<th>Insecure Authentication Attempts</th>
<th>Primary Functions</th>
<th>Prohibited Services</th>
<th>System Misconfigurations</th>
<th>Wireless Misconfigurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint - Listening</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search or Dashboard</td>
<td>Default Account Access</td>
<td>Insecure Authentication Attempts</td>
<td>Primary Functions</td>
<td>Prohibited Services</td>
<td>System Misconfigurations</td>
<td>Wireless Misconfigurations</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------</td>
<td>----------------------------------</td>
<td>-------------------</td>
<td>--------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Ports Tracker - Lookup Gen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint - Local Processes Tracker - Lookup Gen</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint - Services Tracker - Lookup Gen</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Requirement 3 Reports**

The **Intrusion Detection** data model populates these dashboards.

**Requirement 4 Reports**

The **Certificate** data model populates these dashboards.

**Requirement 5 Reports**

The **Malware** data model populates these dashboards.

**Requirement 6 Reports**

The **Performance** and **Authentication** data models populate these dashboards.

**Requirement 7 Reports**

The **Authentication** data model populates these dashboards.
Requirement 8 Reports

The Authentication data model populates these dashboards.

Requirement 10 Reports

The Change Analysis, Authentication, and Performance data models populate these dashboards.

Requirement 11 Reports

The Change Analysis, Intrusion Detection, and Vulnerabilities data models populate these dashboards.

Searches that create notable events

Many of the searches in the Splunk App for PCI Compliance create notable events and are not used by dashboards.

Search macros

The Splunk App for PCI Compliance includes a variety of search macros that can be used to create custom searches and notable events. Search macros can be found in the /default directory of the Domain Add-ons (DA) and Supporting Add-ons (SA) listed here.

Some of these search macros provide data. For example:

`authentication`
`malware`
`ids_attack`
`communicate`
`get_summary`
`get_category`

Some search macros bring in lookup table data. For example:

`assets`
`identities`
`categories`

Other search macros perform lookups. For example:
There are also utility search macros. For example:

`ctime(<timestamp>)`
`get_vendor_product`
`uitime`
`uptime2string`

The back ticks ` denote the start and the end of a search macro definition when used in the Splunk search language. The values (<timestamp>) following the search macro name denote the type and number of arguments used with the macro. Overloaded macros are macros with the same name, but a different number of required arguments.

To learn more about the syntax used in macros see Define search macros in Settings and macros.conf in the Splunk Enterprise documentation.

**Access Protection**

These search macros are part of `SA-AccessProtection`.

<table>
<thead>
<tr>
<th>Search macro</th>
<th>Intended purpose</th>
<th>Expected data types</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authentication</code></td>
<td>used to report on access events</td>
<td>system access logs, such as ssh, Windows, or database audit</td>
</tr>
<tr>
<td><code>authentication(&lt;action&gt;)</code></td>
<td>used to validate success or failure of authentication access</td>
<td>system access logs, such as ssh, Windows, or database audit</td>
</tr>
<tr>
<td><code>account_management</code></td>
<td>used to report on account management events, such as Create, Update, or Delete actions</td>
<td>system audit logs, such as Active Directory or OpenLDAP</td>
</tr>
<tr>
<td><code>default_local_accounts</code></td>
<td>used to report usage of default local accounts</td>
<td>Special user accounts table and system access logs</td>
</tr>
</tbody>
</table>
## Audit and Data Protection

These search macros are part of **SA-AuditAndDataProtection**.

<table>
<thead>
<tr>
<th>Search macro</th>
<th>intended purpose</th>
<th>expected data types</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>splunkd_utilization</code></td>
<td>reports resource utilization of the Splunk data engine process</td>
<td>Splunk internal logs</td>
</tr>
<tr>
<td><code>splunkd_startmode</code></td>
<td>reports start mode of the Splunk data engine process</td>
<td>Splunk internal logs</td>
</tr>
<tr>
<td><code>index_thruput(&lt;data_source&gt;)</code></td>
<td>reports throughput of data by index, source, sourcetype, or host</td>
<td>Splunk internal logs (metrics.log)</td>
</tr>
<tr>
<td><code>license_info</code></td>
<td>reports license utilization level</td>
<td>Splunk internal logs (license_audit.log)</td>
</tr>
<tr>
<td><code>view_activity</code></td>
<td>reports usage of Splunk apps</td>
<td>Splunk internal logs (_internal index, sourcetype splunk_web_access)</td>
</tr>
</tbody>
</table>

### Endpoint Protection

These search macros are part of **SA-EndpointProtection**.

<table>
<thead>
<tr>
<th>Search macro</th>
<th>intended purpose</th>
<th>expected data types</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cputime</code></td>
<td>report all processor usage level records</td>
<td>performance monitoring data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td><code>cputime(&lt;machine_name&gt;)</code></td>
<td>report all processor usage level records for a single machine  (<code>cputime(ACME-001)</code>)</td>
<td>performance monitoring data, such as</td>
</tr>
<tr>
<td>Search macro</td>
<td>intended purpose</td>
<td>expected data types</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td><code>cputime(&lt;machine_name&gt;, &lt;top_N_processor_usage_records&gt;)</code></td>
<td>report the top N processor usage level records for a single machine (&lt;cputime(ACME-001,10)&gt;</td>
<td>performance monitoring data, such as data from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>disk</code></td>
<td>report all disk space usage level records</td>
<td>performance monitoring data, such as data from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>disk(&lt;machine_name&gt;)</code></td>
<td>report all disk space usage level records for a single machine (&lt;disk(ACME-001)&gt;</td>
<td>performance monitoring data, such as data from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>disk(&lt;machine_name&gt;, &lt;disk_space_usage_level&gt;)</code></td>
<td>report the top N disk space usage level records for a single machine (&lt;disk(ACME-001,10)&gt;</td>
<td>performance monitoring data, such as data from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>endpoint_change</code></td>
<td>report system change events</td>
<td>endpoint audit logs, such as data from Windows or UNIX</td>
</tr>
<tr>
<td>Search macro</td>
<td>intended purpose</td>
<td>expected data types</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td><code>listeningports</code></td>
<td>report all records of listening network ports on endpoints</td>
<td>endpoints</td>
</tr>
<tr>
<td><code>listeningports(&lt;machine_name&gt;)</code></td>
<td>report all records of listening network ports on a single machine <code>&lt;machine_name&gt;</code></td>
<td>performance monitoring data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td><code>listeningports(&lt;machine_name&gt;, &lt;top_N_listening_network_ports&gt;)</code></td>
<td>report the top N records of listening network ports on a single machine <code>&lt;machine_name&gt;</code>, <code>&lt;top_N_listening_network_ports&gt;</code></td>
<td>performance monitoring data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td><code>malware</code></td>
<td>report malware discovery and cleanup events</td>
<td>endpoint protection data, such as from McAfee or Symantec</td>
</tr>
<tr>
<td><code>memory</code></td>
<td>report all RAM usage level records</td>
<td>performance monitoring data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td><code>memory(&lt;machine_name&gt;)</code></td>
<td>report all RAM usage level records for a single machine <code>&lt;machine_name&gt;</code></td>
<td>performance monitoring data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td>Search macro</td>
<td>intended purpose</td>
<td>expected data types</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td><code>memory(&lt;machine_name&gt;, &lt;ram_usage_level&gt;)</code></td>
<td>report the top N RAM usage level records for a single machine</td>
<td>performance monitoring data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td><code>localprocesses</code></td>
<td>report all records of running processes on endpoints</td>
<td>performance monitoring data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td><code>localprocesses(&lt;machine_name&gt;)</code></td>
<td>report all records of running processes on a single machine</td>
<td>performance monitoring data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td><code>localprocesses(&lt;machine_name&gt;, &lt;top_N_running_processes&gt;)</code></td>
<td>report the top N records of running processes on a single machine</td>
<td>performance monitoring data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td><code>selinuxconfig</code></td>
<td>report all SE Linux configuration status records for all machines</td>
<td>system audit data from Linux endpoints</td>
</tr>
<tr>
<td><code>selinuxconfig(&lt;machine_name&gt;)</code></td>
<td>report all SE Linux configuration status records for a single machine</td>
<td>system audit data from Linux endpoints</td>
</tr>
<tr>
<td>Search macro</td>
<td>intended purpose</td>
<td>expected data types</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>`selinuxconfig(&lt;machine_name&gt;,</td>
<td>report the top N SE Linux configuration status records for a single machine</td>
<td>system audit data from Linux</td>
</tr>
<tr>
<td><code>top_N_conf_status_records&gt;)</code></td>
<td>(selinuxconfig(ACME-001,10))</td>
<td>endpoints</td>
</tr>
<tr>
<td><code>service</code></td>
<td>report all records of running services on endpoints (note that &quot;service&quot; is used</td>
<td>performance monitoring data,</td>
</tr>
<tr>
<td></td>
<td>generically to refer to Windows or UNIX system services)</td>
<td>such as data from Windows or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unix endpoints</td>
</tr>
<tr>
<td><code>service(&lt;machine_name&gt;)</code></td>
<td>report all records of running services on a single machine (service(ACME-001))</td>
<td>performance monitoring data,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>such as data from Windows or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unix endpoints</td>
</tr>
<tr>
<td>`service(&lt;machine_name&gt;,</td>
<td>report the top N records of running services on a single machine</td>
<td>performance monitoring data,</td>
</tr>
<tr>
<td><code>top_N_running_services&gt;)</code></td>
<td>(service(ACME-001,10))</td>
<td>such as data from Windows or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unix endpoints</td>
</tr>
<tr>
<td><code>sshdconfig</code></td>
<td>report all SSHD configuration status records for all machines</td>
<td>system audit data from UNIX or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Linux endpoints</td>
</tr>
<tr>
<td><code>sshdconfig(&lt;machine_name&gt;)</code></td>
<td>report all SSHD configuration status records for a single machine</td>
<td>system audit data from UNIX or</td>
</tr>
<tr>
<td></td>
<td>(sshdconfig(ACME-001))</td>
<td>Linux endpoints</td>
</tr>
<tr>
<td>Search macro</td>
<td>intended purpose</td>
<td>expected data types</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><code>sshdconfig(&lt;machine_name&gt;, &lt;top_N_SSHD_config_status_records&gt;)</code></td>
<td>report the top N SSHD configuration status records for a single machine</td>
<td>system audit data from UNIX or Linux endpoints</td>
</tr>
<tr>
<td><code>time_sync</code></td>
<td>report all time synchronization status records from all endpoints</td>
<td>system audit data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td><code>time_sync(&lt;action&gt;)</code></td>
<td>report successful or failed time synchronization status record from all endpoints</td>
<td>system audit data, such as data from Windows or Unix endpoints</td>
</tr>
<tr>
<td><code>index_time_delta</code></td>
<td>report time synchronization problems on endpoints by evaluating difference between reported time and actual time at indexing events</td>
<td>Splunk internal logs</td>
</tr>
<tr>
<td><code>ntp_startmode</code></td>
<td>report all time synchronization service start mode records from all endpoints (note that any service tagged &quot;time&quot; will be reported, not just ntpd)</td>
<td>system audit data, such as from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>ntp_startmode(&lt;endpoint_name&gt;)</code></td>
<td>report all time synchronization service start mode records from a single endpoint. Note that any service tagged &quot;time&quot; will be reported, not just UNIX ntpd.</td>
<td>system audit data, such as from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>system_update</code></td>
<td>report patching status on endpoints</td>
<td>system audit data, such as from Windows or UNIX endpoints</td>
</tr>
<tr>
<td>Search macro</td>
<td>intended purpose</td>
<td>expected data types</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><code>update_startmode</code></td>
<td>report patching service status records from all endpoints (note that any service tagged &quot;update&quot; will be reported)</td>
<td>UNIX endpoints</td>
</tr>
<tr>
<td><code>update_startmode(&lt;endpoint_name&gt;)</code></td>
<td>report all patching service status records from a single endpoint. Note that any service tagged &quot;update&quot; will be reported. (update_startmode(ACME-001))</td>
<td>system audit data, such as from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>uptime</code></td>
<td>report all OS uptime records from all endpoints</td>
<td>system audit data, such as from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>uptime(&lt;endpoint_name&gt;)</code></td>
<td>report all OS uptime records from a single endpoint. (uptime(ACME-001))</td>
<td>system audit data, such as from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>uptime(&lt;endpoint_name&gt;, &lt;top_N_OS_uptime_records&gt;)</code></td>
<td>report the top N OS uptime records from a single endpoints. (uptime(ACME-001,10))</td>
<td>system audit data, such as from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>useraccounts</code></td>
<td>reports all user account status records, management events, and password information records gathered from all endpoints</td>
<td>system audit data, such as from Windows or UNIX endpoints</td>
</tr>
<tr>
<td>Search macro</td>
<td>intended purpose</td>
<td>expected data types</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><code>useraccounts(&lt;endpoint_name&gt;)</code></td>
<td>reports all user account status records, management events, and password information records gathered from a single endpoint. (\text{useraccounts}(\text{ACME-001}))</td>
<td>system audit data, such as from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>useraccounts(&lt;endpoint_name&gt;, &lt;top_N_user_account_status_records&gt;)</code></td>
<td>reports the top N user account status records, management events, and password information records gathered from a single endpoint. (\text{useraccounts}(\text{ACME-001},10))</td>
<td>system audit data, such as from Windows or UNIX endpoints</td>
</tr>
<tr>
<td><code>system_version</code></td>
<td>report all raw events that operating system names and versions have been discovered from</td>
<td>vulnerability scanners such as Nessus or OSSEC, and/or system audit data, such as from Windows or UNIX endpoints</td>
</tr>
</tbody>
</table>

**Identity Management**

These search macros are part of **SA-IdentityManagement**.

<table>
<thead>
<tr>
<th>Macro</th>
<th>Intended purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>get_bunit(&lt;business_unit_name&gt;)</code></td>
<td>search <code>get_bunit(EMEA)</code></td>
</tr>
<tr>
<td><code>get_category(&lt;category_name&gt;)</code></td>
<td>search <code>get_category(email_servers)</code></td>
</tr>
<tr>
<td>Macro</td>
<td>Intended purpose</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------</td>
</tr>
<tr>
<td><code>asset_search(&lt;asset_name&gt;)</code></td>
<td>Find all records associated with a single asset by searching the asset-related fields and leveraging unspecified asset correlation information. For instance, <code>asset_search(ACME-001)</code> can find records via the machine's IP or MAC address, using source or destination fields.</td>
</tr>
<tr>
<td><code>get_events4identity(&lt;name_compound&gt;, &lt;string_to_match&gt;)</code></td>
<td>Return the events associated with a given identity using any field from the Identities table. For instance, <code>get_events4identity(email, jdoe@acmetech.com)</code> can find records associated with the identity that the email address is associated with. Stack the command for more precise usage, such as <code>get_events4identity(first, John)</code> <code>get_events4identity(last, Doe)</code></td>
</tr>
<tr>
<td><code>identity_search(&lt;identity_field_name&gt;)</code></td>
<td>Find all records associated with a single identity specified with any field by searching the identity-related fields and leveraging unspecified identity correlation information. For instance, <code>identity_search(jdoe@acmetech.com)</code> can find records via the person's email address, Active Directory login, SAP account name, or phone number, using applicable fields.</td>
</tr>
<tr>
<td><code>identity_search(&lt;first_name&gt;, &lt;last_name&gt;)</code></td>
<td>Find all records associated with a single identity specified with first and last name by searching the identity-related fields and leveraging unspecified identity correlation information. For instance, <code>identity_search(John, Doe)</code> can find records via the person's email address, Active Directory login, SAP account name, or phone number, using applicable fields.</td>
</tr>
<tr>
<td><code>sessions</code></td>
<td>Reports all discovered network sessions. Sessions are tracked for VPN and DHCP logs.</td>
</tr>
</tbody>
</table>
## Network Protection

These search macros are part of **SA-NetworkProtection**.

<table>
<thead>
<tr>
<th>Macro</th>
<th>Intended purpose</th>
<th>Expected data types</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>communicate</code></td>
<td>Display networking data.</td>
<td>Firewall logs</td>
</tr>
<tr>
<td><code>communicate(&lt;action&gt;)</code></td>
<td>Display networking data by action (allowed or blocked).</td>
<td>Firewall logs</td>
</tr>
<tr>
<td><code>network_change</code></td>
<td>Display records of network change events</td>
<td>Operational logs from network infrastructure devices</td>
</tr>
<tr>
<td><code>ids_attack</code></td>
<td>Display all detected intrusion event records</td>
<td>Intrusion Detection System and Intrusion Prevention System logs, (including network-based, host-based, and other types).</td>
</tr>
<tr>
<td><code>proxy</code></td>
<td>Display web proxy events</td>
<td>Web proxy server logs</td>
</tr>
<tr>
<td><code>vulnerability</code></td>
<td>Display discovered vulnerability data.</td>
<td>Vulnerability scanners, such as Nessus.</td>
</tr>
</tbody>
</table>

## Threat Intelligence

These search macros are part of **SA-ThreatIntelligence**.

<table>
<thead>
<tr>
<th>Macro</th>
<th>Intended purpose</th>
<th>Expected data types</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>notable</code></td>
<td>Displays Notable Events with proper rendering</td>
<td>the app's _notable index</td>
</tr>
<tr>
<td><code>suppression_audit</code></td>
<td>Reports suppression events from audit logs</td>
<td>The Notable Event Suppression feature needs to be used for this to have effect.</td>
</tr>
<tr>
<td><code>suppression_audit-expired</code></td>
<td>Reports suppression</td>
<td>The Notable Event Suppression feature needs</td>
</tr>
<tr>
<td>Macro</td>
<td>Intended purpose</td>
<td>Expected data types</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td>expirations</td>
<td>to be used for this to have effect.</td>
</tr>
<tr>
<td><code>suppressed_notables</code></td>
<td>Reports suppressed Notable Events</td>
<td>The Notable Event Suppression feature needs to be used for this to have effect.</td>
</tr>
</tbody>
</table>

**FAQ**

**Why are some searches using a lot of memory?**

Adding a notable index to the default indexes to be searched causes correlation searches to detect another finding again based on the content of a previous correlation search firing.

The solution is to remove the notable index from the list of indexes to be searched by default.


**Learn more and get help**

**Support**

For general Splunk support, see Splunk Support.

If you have specific questions about the Splunk App for PCI Compliance, you can log a case using the Splunk Support Portal.

**More information**

- Splunk App for PCI Compliance (for Splunk Enterprise) on Splunkbase.
- Splunk App for PCI Compliance (for Splunk Enterprise Security) on Splunkbase.
- PCI-specific questions and answers on Splunk Answers [http://answers.splunk.com/search/?q=pci](http://answers.splunk.com/search/?q=pci)
- The #splunk IRC channel on EFNET.