Splunk® Enterprise Security
Use Splunk Enterprise Security 8.0.0

Generated: 11/19/2024 10:38 am

Table of Contents

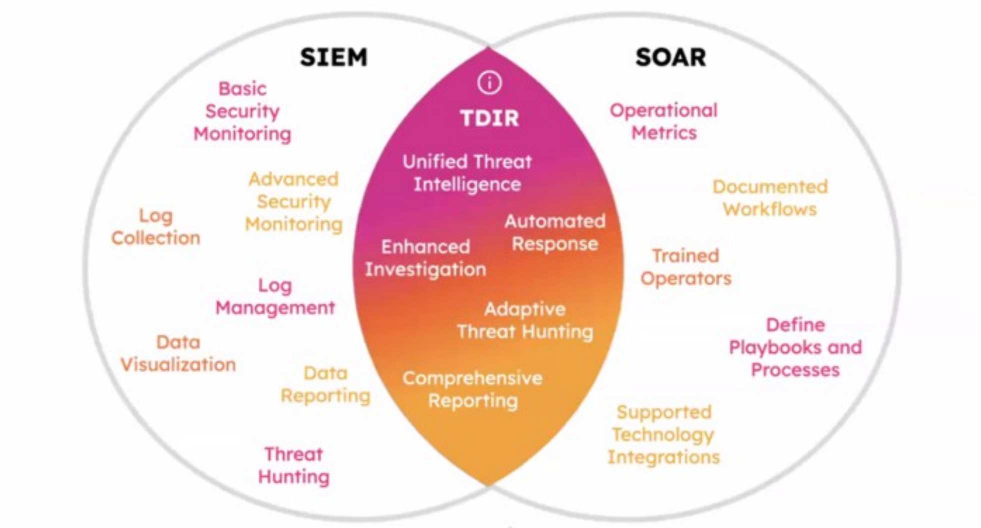
Table of Contents

Introduction

About Splunk Enterprise Security

Splunk Enterprise Security version 8.0 and higher provides a comprehensive threat detection, investigation, and response solution, which is key to the security monitoring strategy of today's enterprise infrastructure. Splunk Enterprise Security combines the best features and functionalities of Splunk's Security Infrastructure and Event Monitoring (SIEM), Security Orchestration Automation and Response (SOAR), and threat intelligence management capabilities to identify security threats and effectively respond to them.

The following figure shows the evolution of Splunk's threat detection, investigation, and response solution in Splunk Enterprise Security:



Using Splunk Enterprise Security version 8.0 and higher offers the following benefits:

- Unified user experience and a seamless integrated workflow for case management, alert triage, investigation, and response
- Aligned taxonomy with Open Cybersecurity Schema framework (OCSF) and industry standards
- Enhanced detection and turnkey capabilities to implement risk-based alerting that creates high confidence alerts for investigations
- Alert aggregation capabilities using finding groups that map to pre-determined rules based on common security frameworks and techniques
- Automation with Splunk SOAR and full access to actions and playbooks.

Splunk Enterprise Security is built on the Splunk operational intelligence platform and uses the search and correlation capabilities, allowing users to capture, monitor, and report on data from security devices, systems, and applications. As issues are identified, security analysts can quickly investigate and resolve the security threats across the access, endpoint, and network protection domains.

Access Splunk Enterprise Security

1. Open a web browser and go to Splunk Web.
2. Log in with your username and password.
3. From the **Apps** list, select **Enterprise Security**.

Get started with Splunk Enterprise Security

Get started with common analyst workflows in Splunk Enterprise Security.

- Get an overview of your detections, findings and investigations on the **Mission Control** page of Splunk Enterprise Security. The analyst queue on the **Mission Control** page integrates the **Incident review** page of prior releases of Splunk Enterprise Security and Splunk Mission Control.
- Get an overview of the dashboards available on the **Analytics** page of Splunk Enterprise Security and learn how to use them for your use cases.
- Manage your security content and response plans on the **Security content** page of Splunk Enterprise Security.
- Manage your settings for findings and investigations, threat intelligence data, and Splunk SOAR data integrated with Splunk Enterprise Security on the **Configure** page of Splunk Enterprise Security.
- Use the Splunk platform search function for Splunk Enterprise Security data on the **Search** page of Splunk Enterprise Security.

Licensing for Splunk Enterprise Security

Splunk Enterprise Security is a premium app, which is used in conjunction with Splunk Enterprise or Splunk Cloud Platform. This means that you must have Splunk Enterprise or Splunk Cloud Platform along with a Daily Indexing Volume or vCPU usage license to download the app from the Splunk Support portal.

For example, if you purchase a 1 GB Daily Indexing Volume license for Splunk Enterprise and purchase Splunk Enterprise Security app, you can only ingest 1 GB of data to use in Splunk Enterprise and Enterprise Security. You do not receive any additional ingestion capacity. However, you are entitled to use Splunk Enterprise Security on your ingested data.

Contact your Sales representative to get pricing details based on your specific workload. Splunk Enterprise Security monitors Splunk indexes for Daily Indexing Volume and vCPU consumption, irrespective of whether you are using the on-prem or the cloud version.

Splunk monitors daily indexing volume into Splunk and the use of that data for security use cases. Splunk also monitors the vCPU usage based on the data summarized in Splunk Enterprise Security specific summary and metrics indexes. For more information, see Use Summary indexing for increased search efficiency.

License usage is measured on Daily Indexing Volume for data sources, vCPUs, and SVC. For more information, see Splunk Offerings Purchase Capacity and Limitations.

To calculate capacity consumption for ingest-based licenses for premium apps such as Splunk Enterprise Security, use the Splunk App for Chargeback.

SOAR license information

See Obtain and configure a Splunk SOAR (On-premises) license

Get started with Splunk Enterprise Security

Use Splunk Enterprise Security to triage, investigate, and respond to security incidents. You can identify and remediate findings and investigations while collaborating with others on your team.

Use Splunk Enterprise Security to complete the following tasks:

- Triage findings. See Triage findings and finding groups in Splunk Enterprise Security.
- Start investigations. See Start investigations in Splunk Enterprise Security.
- Respond to investigations with response plans. See Respond to investigations with response plans in Splunk Enterprise Security.
- Automate your investigation response. See Automate your investigation response with actions and playbooks in Splunk Enterprise Security.
- Analyze risk with risk-based alerting. See Analyze risk with risk-based alerting in Splunk Enterprise Security.
- Investigate observables with threat intelligence management. See Investigate observables related to an investigation in Splunk Enterprise Security.

To get started, select the **Mission Control** tab in Splunk Enterprise Security, and then select a finding and start investigating.

Splunk Enterprise Security terminology

The main components of Splunk Enterprise Security each play a role in delivering security triage, investigation, and response. Some of these components are present in other Splunk security software.

Term	Definition
Analyst queue	A list of findings and investigations that analysts can triage. Intermediate findings are not displayed in the analyst queue.
Detection	A scheduled correlation search that runs analytics on Splunk events, third-party alerts, or findings and generates findings, intermediate findings, or finding groups.
Detection editor	An editor to configure event-based and finding-based detections. Using the detection editor, you can also configure time range to run the detection searches, configure adaptive response actions, and so on.
Entity	Asset, identity, user, or device in your network that generates machine data. Entities are the subject of suspicious, anomalous, or malicious activity and help to identify potential security threats. Entities are normalized in lookups against known assets and identities using the Assets and Identities framework in Splunk Enterprise Security. Entities also carry weighted risk scores that are updated automatically in real time.
Event	A contributing event or raw data associated with an investigation or finding. It can represent the finding itself or a series of activities that resulted in the creation of the finding.
Event-based detection	A type of detection that reviews raw events ingested into the Splunk platform and creates findings, which might or might not indicate a potential security threat. Event-based detections generate findings or intermediate findings depending on how the user configures the detection.
Finding	One or more anomalous incidents or alerts generated by event-based detections. A finding contains all the relevant information about what was observed and which entity was impacted.
Finding-based detection	A type of detection that reviews the findings in the risk index and the notable index for anomalous events and threat activities and uses an aggregation of findings impacting a single entity, or other group type and criteria, to generate finding groups that indicate a security risk.
Finding group	A group of findings and intermediate findings created by finding-based detections. Finding groups can be manually included in an investigation and triaged by the SOC. Finding groups are stored in KV Store collections.
Intermediate finding	A record or observation created by event-based detections that indicate an anomaly but might not be a standalone security incident. Intermediate findings in conjunction with other findings might be used as input by advanced finding-based detections to discover potential security incidents with high fidelity and confidence. Intermediate findings might look identical to findings based on the data stored in the index. However, intermediate findings are not displayed in the analyst queue and are not triaged by analysts. The style and format of an intermediate finding is identical to that of a traditional finding and contains fields such as timestamp, key/value pairs, an entity, risk score, threat objects, and other metadata.
Investigation	

Term	Definition
	A case that has been manually or automatically flagged and is displayed in the analyst queue of the **Mission Control** page in Splunk Enterprise Security. Investigations are a collaborative process for security personnel such as analysts, SOC managers, automation engineers, security architects and so on to identify, collect, and examine findings or finding groups.
Investigation type	A category of investigations that share common characteristics, such as source or severity. After creating an investigation type, you can associate the investigation type with a response plan to automate and personalize your response workflow.
Note	Additional information such as PDFs, slide decks, reference materials, screenshots, extracts of log files, notes, Splunk events, email messages, and so on that can be attached to an investigation or finding.
Threat list	A list of threat-indicators published by your threat intelligence management (cloud) data sources for use in Splunk Enterprise Security threat-matching searches and investigation enrichment. You can set up multiple threat lists to pinpoint responses or target data to specific tools in your cybersecurity setup.
Response plan	A template of guidelines for analysts to follow so that they can provide a standardized response for investigations of the same type. You can use response plans provided by Splunk Enterprise Security, such as NIST 800-61 or Vulnerability Disclosure, or you can create your own custom response plan.

Use behavioral analytics service with Splunk Enterprise Security 7.1.0 or higher

This topic applies only to customers on the Splunk Cloud platform.

If you have enabled Splunk Enterprise Security version 7.1 or higher, you can also provision behavioral analytics service on a tenant in Splunk Cloud Solutions.

Behavioral analytics service is a cloud-native analytics solution that streams data from your platform to a shared service for processing and helps investigative analysts uncover hidden threats. This service uses a near real-time analytics engine that integrates with Splunk Enterprise Security's risk-based alerting framework (RBA) to improve insider threat detection without adding to alert fatigue in your security operations center (SOC). It brings streaming analytics capabilities to the Splunk Cloud Platform environment and provides security visibility to uncover hidden and unknown threats that cannot be easily detected through searches.

For more information on prerequisites to enable behavioral analytics service with Splunk Enterprise Security, see How do I get behavioral analytics service?

What do I need to run behavioral analytics service?

Verify that you have the following in order to run behavioral analytics service:

- Splunk Cloud stack on 9.0.2209 or later in the US East (Virginia) region
- Splunk Enterprise Security version 7.1 or later
- You are a Splunk Enterprise Security customer from the US East (Virginia) AWS region
- You are a non-FedRamp customer
- Your data ingestion volume is less than 4 TB

Behavioral analytics service is not available in the following compliant environments:

- FedRAMP Moderate
- IL5
- IRAP

The behavioral analytics service for Splunk Enterprise Security is not available to on-prem users.

How do I get behavioral analytics service?

To get access to behavioral analytics service, you need Splunk Enterprise Security. Behavioral analytics service ingests asset and identity data from Splunk Enterprise Security in Splunk Cloud Platform for optimal identity resolution.

Turn on behavioral analytics service on Splunk Enterprise Security

This topic applies only to customers on the Splunk Cloud platform.

Enable behavioral analytics service on Splunk Enterprise Security to leverage threat detections so that you can monitor cyber threats and enhance your security operations. Enabling behavioral analytics service on Splunk Enterprise Security allows you to ingest raw data from various supported source types and provision tenants automatically. Additionally, you can also forward notables, risk events, assets, and identity data from Splunk Enterprise Security to the behavioral analytics service.

Prerequisites to enable behavioral analytics service

Following is a list of prerequisites to enable behavioral analytics service with Splunk Enterprise Security:

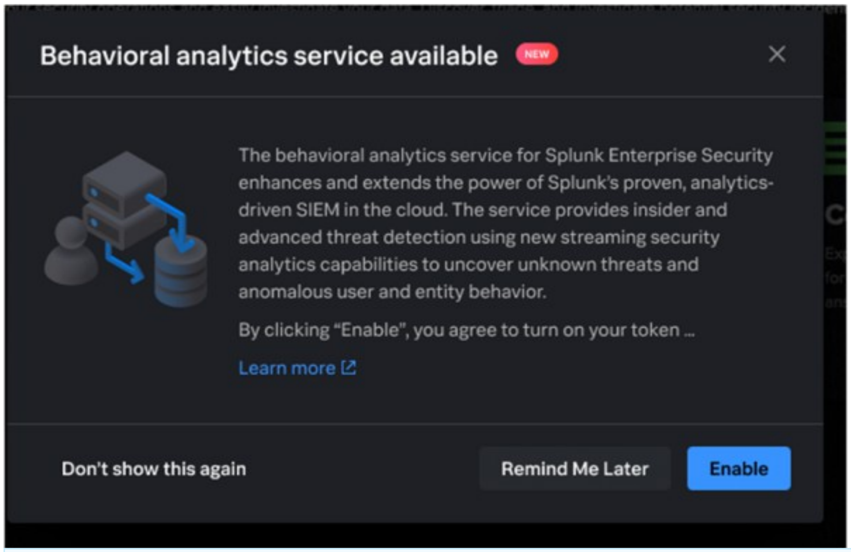
- Splunk Cloud stack on 9.0.2209 or later in the US East (Virginia) region
- Splunk Enterprise Security version 7.2 or later
- You are a Splunk Enterprise Security customer from the US East (Virginia) AWS region
- You are a non-FedRamp customer
- Your data ingestion volume is less than 4 TB

The behavioral analytics service for Splunk Enterprise Security is not available to on-prem users.

Turn on behavioral analytics service from Splunk Enterprise Security

Follow these steps to turn on behavioral analytics service on Splunk Enterprise Security:

1. Log in to the Splunk Enterprise Security app to display the option to turn on the service.
2. Select the checkbox to allow Splunk to turn on token authentication, generate a token, and send data from Splunk Enterprise Security to behavioral analytics service.



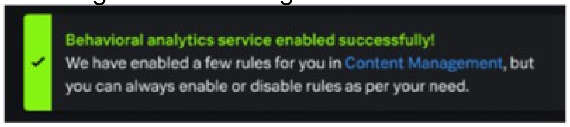
Behavioral analytics service available

The behavioral analytics service for Splunk Enterprise Security enhances and extends the power of Splunk's proven, analytics-driven SIEM in the cloud. The service provides insider and advanced threat detection using new streaming security analytics capabilities to uncover unknown threats and anomalous user and entity behavior.

By clicking "Enable", you agree to turn on your token ...

> You must select the checkbox and allow Splunk to turn on token authentication to proceed with enabling the service. If you choose to disable token authentication later, the behavioral analytics service is not disabled, and you can continue to use the service.

3. Select **Enable** to turn on the service.
   Enabling the service might take 1-2 hours. The following notification is sent when the service is turned on.



Behavioral analytics service enabled successfully!
We have enabled a few rules for you in Content Management, but you can always enable or disable rules as per your need.

For more information on token authentication, see Enable or disable token authentication.

Alternatively, you can also turn on the behavioral analytics service by following these steps:

1. In Splunk Enterprise Security, go to **Configure**.
2. Select **General settings**.
3. Scroll to the panel for **Behavioral analytics service**.
4. Select the checkbox to allow Splunk to turn on token authentication, generate a token, and send date from Splunk Enterprise Security to behavioral analytics service.

> You must select the checkbox and allow Splunk to turn on token authentication to proceed with enabling the service. Enabling tokens allow users with sc_admin role to make API calls to the Administrator Configuration Service (ACS) and use behavioral analytics with Splunk Enterprise Security. If you choose to disable token authentication later, the behavioral analytics service is not disabled, and you can continue to use the service.

5. Select **Enable** to turn on the service.
   Enabling the service might take 1-2 hours. The following notification is sent when the service is turned on.

```
Behavioral analytics service enabled successfully.
```

Contact *Splunk Support Portal or your account team if you want to disable the behavioral analytics service. If you see errors while enabling the behavioral analytics service, retry enabling the service again. If you see errors while enabling behavioral analytics detection, retry enabling the detections. Contact Splunk Support if the errors persist.

Turn on or turn off behavioral analytics detections in Splunk Enterprise Security

If you are an eligible user, you can view all behavioral analytics detections on the **Content Management** page in Splunk Enterprise Security. You can also turn on or turn off individual detections, if required. You also have the option to manage behavioral analytics detections by forwarding findings to a test index without impacting the risk environment. For more information on using test index for detections, see Manage Behavioral Analytics Service detections in Splunk Enterprise Security.

Follow these steps to turn on or turn off detections:

1. In Splunk Enterprise Security, go to **Security content** and then select **Content management** to view all content.
2. Filter the security content by type **Detection**.
3. Turn on or turn off the detections by selecting **On** or **Off** from the **Status** column.

Use federated searches in transparent mode with Splunk Enterprise Security

Run federated searches in transparent mode to search datasets beyond your local Splunk platform deployment. Using federated search with Splunk Enterprise Security provides a holistic view of datasets to identify threats across multiple Splunk Platform deployments, for both Splunk Cloud and Splunk Enterprise. Transparent mode is especially useful if your datasets are partly on Cloud and partly on-prem and you plan to migrate from on-prem to Cloud. Federated search in transparent mode is subject to the constraints of the Splunk Platform. For more information, see About the standard and transparent modes in the *Splunk Cloud Platform Federated Search* manual.

For more information, see About federated search in the *Splunk Cloud Platform Federated Search* manual.

> Federated search in standard mode is not supported on Splunk Enterprise Security. The ES administrator must ensure that Enterprise Security is installed on the federated search head and not the remote search head. Federated search might not work as expected if Splunk Enterprise Security is installed on a remote search head. Using federated search to access deployments in different geographical locations might also impact regulatory requirements.

Limitations of using federated search with Splunk Enterprise Security in transparent mode

Following are some limitations of using federated search with Splunk Enterprise Security irrespective of whether your Enterprise Security instance is installed on a remote search head or not:

> These limitations apply to versions prior to Splunk Platform version 9.1.5, 9.2.2, and 9.3.0. These limitations do not apply if you upgrade to Splunk Platform versions 9.1.5, 9.2.2, and 9.3.0.

- The makeresults command fails to write events to custom indexes. Some correlation searches depend on the command to generate only a single event. Therefore, using the command for federated search might cause issues since it returns results for all federated providers that are added to the deployment. However, this issue impacts only custom searches and does not have a major impact on Splunk Enterprise Security.

- Threat match searches in the threat intelligence framework might not properly match against the search results that come from the remote search head. However, threat matching searches work locally on the federated search head.

See also

Migrate from hybrid search to Federated Search for Splunk in the *Splunk Cloud Platform Federated Search* manual

Overview of the federated search options for the Splunk platform in the *Splunk Cloud Platform Federated Search* manual

Search over a transparent mode federated provider in the *Splunk Cloud Platform Federated Search* manual

Service accounts and security for Federated Search for Splunk in the *Splunk Cloud Platform Federated Search* manual

Use Federated Analytics with Splunk Enterprise Security for threat detection in Amazon Security Lake (ASL) datasets

Use the search capabilities of Federated Analytics with the risk-based alerting capabilities of Splunk Enterprise Security to run correlation searches or detections and identify threats within the data located in Amazon Security Lake (ASL) datasets.

Using Federated Analytics with Splunk Enterprise Security provides the following benefits:

- Extended visibility into your security operations center (SOC): Access remote and distributed data stored in data lakes for historical data analysis that helps in threat hunting and compliance.

- Unified and consistent user experience: Run detections and ad-hoc searches on data lakes and integrate findings with existing investigations.

- Transform security data: Refine, filter, and compress information from multiple teams to create valuable findings.

Configure Federated Analytics with Splunk Enterprise Security 8.0 and higher

You can use Federated Analytics with Splunk Enterprise Security version 8.0.0 and higher.

Prerequisites

Ensure the following prerequisites are met:

- Configure Federated Analytics on Splunk Cloud Platform and ensure that data lake indexes are configured. Federated Analytics is available on Splunk Cloud Platform 9.3.2408 and higher. See About Federated Analytics in the Splunk Cloud Platform *Federated Search* manual.
- Install the Splunk Enterprise Security app version 8.0.
- Install the Enterprise Security Content update (ESCU) app version 4.32.0 or higher

Follow these steps to configure Federated Analytics in Splunk Enterprise Security version 8.0 and higher:

1. In Splunk Enterprise Security, go to the **Analyst queue** on the **Mission Control** page, which displays the **Update ASL search macro** dialog box.
2. Follow the instructions in the **Update ASL search macro** dialog box to automatically update the federated provider for ASL. Splunk Enterprise Security version 8.0 and higher automatically detects if data lake indexes are configured on the Splunk Platform and updates relevant AWS security detections that are mapped to the Open Cybersecurity Framework (OCSF) schema using the ESCU app.

3. Accept the terms and conditions and select **Accept and continue** to update the ESCU app automatically.
4. Select **Next**. The ESCU app automatically updates the detections.
5. Select **Confirm and continue** to update the macro and turn on the detections.
6. Review the detections that are turned on.

See also

For information on troubleshooting Federated Analytics in Splunk Enterprise Security, see the product documentation:

Troubleshoot common issues when using Federated Analytics with Splunk Enterprise Security

Mission Control

Overview of Mission Control in Splunk Enterprise Security

Triage, investigate, and respond to security incidents using the **Mission Control** page in Splunk Enterprise Security. You can also collaborate with others on your team to identify and remediate security incidents.

The **Mission Control** page includes the following:

- An analyst queue for viewing findings and investigations
- Charts and a timeline for visualizing finding and investigation details

The analyst queue

In Splunk Enterprise Security, detections generate the findings and finding groups that appear in the analyst queue based on raw events and third-party alerts. An investigation is a structured approach for gathering evidence and responding to a security incident. Each investigation is based on one or more findings related to the security incident, and they appear alongside findings in the analyst queue.

As an analyst, you can use the analyst queue to review findings, finding groups, and investigations to gain insight into the severity of events occurring in your system or network.

Charts and timeline

Gain insight into findings and investigations using the pie charts and timeline visualization. To see the charts on the **Mission Control** page, select **Charts**.

The four pie charts show findings and investigations by the following criteria:

Chart	Criteria
Urgency	Classifies all findings and investigations based on importance, such as **Critical**, **High**, **Low**, **Medium**, **Informational**, or **Unknown**.
Status	Classifies all findings and investigations based on status, such as **New**, **In progress**, **Pending**, **Resolved**, or **Closed**.
Owner	Classifies all findings and investigations based on owners, such as **Unassigned**, **Administrator**, or by a specific username.
Domain	Classifies all findings and finding groups based on the security domain from which they're generated, such as **Access**, **Audit**, **Endpoint**, **Identity**, **Network**, or **Threat**.

Identify when findings were generated using the timeline visualization. To display the timeline on the **Mission Control** page, select **Timeline**. You can zoom in, zoom out, select, or deselect to focus on specific periods of time and view related events that might be of interest for more targeted threat investigations.

Example: Analyst workflow on the Mission Control page

The following high-level example workflow covers how to triage and investigate a finding by assigning it to yourself, reviewing its details, and responding to it by starting an investigation and using automation and a response plan.

1. In Splunk Enterprise Security, select **Mission Control** from the main menu navigation bar to view a list of findings

and investigations in the analyst queue.
2. Review the findings and investigations from the last 24 hours from newest to oldest, and filter to focus on the ones that are most important to you.
3. Select the name of a finding in the analyst queue to open the side panel.
4. Triage the finding by selecting **Assign to me**, updating the status to reflect that you're working on it, and then selecting **Save**.
5. Select **Start investigation**, and then view details such as events, additional fields, notes, and files.
6. Add a response plan to the investigation to follow standardized tasks and phases for remediating the security incident.
7. Automate your security workflow by running actions and playbooks on the investigation to gather more information and then remediate the security incident.
8. Use threat intelligence sources to update the investigation and assess the risk posed by observables.
9. Continue to update the investigation to keep other analysts informed of your progress. For example, update the status of the investigation to **Pending** to reflect that you're waiting for other information, action, or help from other teams, such as a crucial playbook or action approval.
10. After you come to a conclusion about the investigation, update the disposition value. Available outcome values include **True positive**, **Benign positive**, **False positive**, and **Undetermined**.
11. Close the investigation to indicate that you took all of the appropriate actions to resolve the security incident.

Using the Mission Control page in Splunk Enterprise Security

Use the following links to learn more about what you can do on the **Mission Control** page in Splunk Enterprise Security:

- Triage findings and finding groups
- Start investigations
- Respond to investigations with response plans
- Add events to an investigation
- Automate your investigation response with actions and playbooks
- Analyze risk with risk-based alerting
- Investigate observables related to an investigation

See also

For more details on how to customize your experience in Splunk Enterprise Security, see the following links in the *Administer Splunk Enterprise Security* manual:

- Manage analyst workflows using the analyst queue in Splunk Enterprise Security
- Configure the settings for the analyst queue in Splunk Enterprise Security
- Sort and filter findings and investigations for triage in Splunk Enterprise Security
- Manage saved views to display findings and investigations in Splunk Enterprise Security
- Customize table settings for the analyst queue in Splunk Enterprise Security
- Collaborate on investigations in Splunk Enterprise Security

Triage findings and finding groups in Splunk Enterprise Security

Triage findings and finding groups on the **Mission Control** page in Splunk Enterprise Security by assigning them an owner and modifying the status. Review the list of findings and finding groups in the analyst queue for potential security incidents that require further investigation.

To triage a finding or finding group, follow these steps:

1. In Splunk Enterprise Security, select **Mission Control** to find the list of findings and investigations in the analyst queue.
2. Select a finding or finding group that you want to triage from the table.
3. Triage the finding or finding group by configuring your desired fields such as **Owner**, **Status**, **Urgency**, or **Disposition**.
4. (Optional) Review the associated risk scores to help you determine if the finding is a potential threat.
5. (Optional) Open the **Detection** that generated the finding.
6. (Optional) Select the **Drill-down search** to open a predefined search and gather additional context.

   > Finding groups show a maximum of only 100 findings and intermediate findings. To see a complete list of all the findings contributing to a finding group, select the DEFAULT_FBD_DRILLDOWN link. Selecting the drill-down search link opens the search page in a new tab.
7. (Optional) Review **Included findings** or **Related investigations**.
8. (Optional) View **Adaptive responses**.
9. (Optional) Add a note.
10. (Optional) Edit the finding fields by selecting the more icon (⋮) , then **Edit**.

See also

For more details on triaging findings and investigations in Splunk Enterprise Security, see the product documentation:

- Use findings for security monitoring in Splunk Enterprise Security
- Configure findings manually to track specific fields in Splunk Enterprise Security
- Merge findings and finding groups into investigations in Splunk Enterprise Security
- Run adaptive response actions in Splunk Enterprise Security
- Create and share notes on an investigation
- Risk scoring in Splunk Enterprise Security

Start investigations in Splunk Enterprise Security

In Splunk Enterprise Security, an investigation is a structured approach for gathering evidence and responding to a security incident. Each investigation is based on one or more findings related to the security incident.

Investigations appear alongside findings in the analyst queue. You can manually start a new investigation based on a single finding or a group of findings in Splunk Enterprise Security.

> You can also automatically create investigations using a playbook in Splunk SOAR. Investigations created from Splunk SOAR playbooks also appear in the analyst queue of Splunk Enterprise Security.

Start an investigation

To start a new investigation, follow these steps:

1. In Splunk Enterprise Security, select **Mission Control**.
2. From the analyst queue, select the name of the finding or finding group that you want to investigate.
3. From the side panel preview, select **Start investigation**.

After you start an investigation, you can respond with response plans and automate your response with Splunk SOAR playbooks.

Data associated with an investigation

To view the data associated with an investigation, select the name of the investigation in the analyst queue and then select **View details**. The following table describes the data found in the **Overview** tab of the investigation details page:

Investigation data	Description
Events	Raw data ingested by event-based detections.
Original event	The raw event that triggered the alert contributing to the investigation.
Included findings and intermediate findings	Findings and intermediate findings that have been added to the investigation.
Drill-down search	A predefined search that you can run to gather additional context about the investigation.
Drill-down dashboard	A predefined dashboard with more than one drill-down search that you can view to gather additional context about the investigation.
Adaptive response	A type of custom alert action that conforms to the common action model. You can trigger adaptive response actions from detections or on an ad hoc basis when examining findings and investigations.
Detection	The detection, or the scheduled correlation search or risk rule, that generated the findings added to the investigation.
Custom fields	Fields that you can populate on the investigation to store relevant additional information about the investigation or the response.
Additional fields	Field-value pairs related to the investigation, such as destination, risk score, severity, and time.
History	The progress other analysts have made on the investigation, such as status changes, notes, and automation.
MITRE ATT&CK	The MITRE ATT&CK tactics and techniques associated with the investigation.

Edit tags for field-value pairs in an investigation

When you're working on an investigation in Splunk Enterprise Security, you can edit and automatically save changes to the following field values using the drop-down lists in the **Info** section of the side panel:

- Owner
- Status
- Urgency
- Sensitivity
- Disposition

In the **Overview** tab, you can edit tags for field-value pairs, including custom fields you created. To edit tags for field-value pairs, follow these steps:

1. In Splunk Enterprise Security, select **Mission Control** and then select the investigation you want to edit in the analyst queue.
2. Select **View details** in the side panel preview of the investigation.
3. In the **Overview** tab of the investigation, use the expansion arrows to see field-value pairs in sections such as **Additional fields**, **Events**, or **MITRE Attack**.
4. Select the down arrow icon (▾) for the field you want to edit.
5. Select **Edit tags**.
6. Make your changes to the tags of the field-value pair.
7. Select **Save**.

See also

For more details on starting an investigation in Splunk Enterprise Security, see the product documentation:

- Merge findings and finding groups into investigations in Splunk Enterprise Security
- View the details of an investigation in Splunk Enterprise Security
- Collaborate on investigations in Splunk Enterprise Security
- Create investigation types in Splunk Enterprise Security
- Configure investigation macros to assign investigation types in Splunk Enterprise Security
- Associate an investigation type with a response plan in Splunk Enterprise Security

Respond to investigations with response plans in Splunk Enterprise Security

A response plan is a template of standardized guidelines for responding to an investigation in Splunk Enterprise Security. A response plan includes tasks and phases for security analysts to complete while investigating and responding to security incidents. You can use response plans provided by Splunk Enterprise Security, such as **NIST 800-61** or **Vulnerability Disclosure**, or you can create your own custom response plan.

You can apply a response plan to a particular investigation as you're working on it, or you can assign a response plan to an investigation type. After you create an investigation type and assign it to a response plan, the response plan you selected applies to any new investigation ingested or started in Splunk Enterprise Security.

Example: Response workflow

After you add a response plan to an investigation, use the phases and tasks to guide your investigation in Splunk Enterprise Security.

1. In Splunk Enterprise Security, select **Mission Control**.
2. Select the name of the investigation you want to respond to from the analyst queue.
3. Select **View details**.
4. From the **Response** tab of the investigation, review the current phase.
5. Review the phase details, such as the number of tasks.
6. Select a task to assign it to someone.
7. Select **Start** to start the work, or use the **Owner** drop-down list to assign the task to someone else. When you start a task, the task is automatically assigned to you.
8. Expand the **Respond** section to browse response options.
    1. If there's a search embedded in the response plan task, open the search in the **Search** tab by selecting the search icon (🔍). You can edit the search, or you can run the search as is. By default, the search runs over the last 24 hours, but you can specify a custom time using the drop-down list.
    2. To run an action or playbook set up with the task, select the run icon (▶). Then select **View results** to see the action or playbook results associated with the investigation.
9. If the response plan requires a note, add a note to the task by expanding the **Notes** section. By default, the title of the note is the task name and number. If you have multiple notes, the number corresponds to the order you created the note in.

    > You can't use more than 250 characters in the note title. Additionally, you can't use more than 10,000 characters in the note description.
10. Expand the **Files** section to add a file to the task.
11. When you complete the task, select **End**.
12. Review and complete all the tasks in a phase to end a phase.

13. Review and complete all the phases to finish your response to the investigation.
14. To review additional response plans for the investigation, select the down arrow next to the current response plan name. From the drop-down list, select the name of another applied response plan.

If you want to share a phase or a task with someone without assigning it to them, you can copy the URL of the investigation while viewing the phase or task and send it to the other person. If you want to reopen a task, select the checkmark icon.

Included response plans in Splunk Enterprise Security

You can use the response plans included in Splunk Enterprise Security, or you can create your own. Splunk Enterprise Security includes the following response plans:

Response plan name	Details	When to use
Account Compromise	Outlines phases and tasks relevant to potential compromise of system or application accounts.	When investigating a likely account compromise.
Data Breach	Outlines response to a data breach by contacting affected system owners and containing data exfiltration.	When investigating a likely data breach.
Network Indicator Enrichment	Gathers and analyzes contextual information about URLs, host names, top level domain names, IP addresses, TLS certificates, and MAC addresses.	To gather information about artifacts involved in the investigation.
NIST 800-61	Outlines response phases and tasks based on the NIST Computer Security Incident Handling Guide, SP 800-61.	To standardize responses for all investigations.
Generic Incident Response	Outlines response phases and tasks for basic investigation response: detect, analyze, contain, eradicate, recover, and review.	To standardize responses for all investigations, especially malware infection.
Self-Replicating Malware	Outlines response phases and tasks relevant to containing and remediating a self-replicating malware infection.	When investigating self-replicating malware infections, especially those infecting network services or shared resources.
Suspicious Email	Outlines response phases and tasks for a suspicious email campaign, including external investigations, internal hunting activities, enforcement, and increased monitoring.	When investigating suspicious emails.
Vulnerability Disclosure	Outlines response phases and tasks for a vulnerability disclosure, such as a critical CVE.	To determine the impact of a vulnerability disclosure on your environment.

See also

For more details on response plans in Splunk Enterprise Security, see the product documentation:

- Create response plans in Splunk Enterprise Security
- Add a response plan to an investigation in Splunk Enterprise Security
- Associate an investigation type with a response plan in Splunk Enterprise Security

Add events to an investigation in Splunk Enterprise Security

An event is a single piece of data in Splunk software similar to a record in a log file or other data input. When data is indexed, it is divided into individual events. Each event is given a timestamp, host, source, and source type. In Splunk

Enterprise Security, an event can be raw data associated with a finding or investigation, or it can represent activity that contributes to the creation of a finding or investigation. You can add events to an investigation through a search macro or automation and then track the related raw data.

All of the events added to an investigation are in the **Events** tab. You can expand each event to see all of the fields related to that event. For some fields, you can choose field actions by selecting the expand icon (⌄) in the **Action** column of the events table.

You can add an event to an investigation using a search macro. Adding an event to an investigation saves the event with the investigation itself and helps other users, such as auditors or managers, extract critical data related to the investigation. Adding events to an investigation can also provide justification for the remediation of that investigation.

> If you create, update, or delete events from playbooks in Splunk SOAR (Cloud), your changes automatically reflect in the Events tab of your investigation in Splunk Enterprise Security.

Add events using the add_events search macro

Use the `add_events` macro to add multiple events to an investigation in Splunk Enterprise Security. Add the macro to the end of a search.

You can run a search to add particular events to an investigation. For example, to add events with a source IP of `192.168.1.8` from your chosen index, use the following search:

```
index=<index_name> | search src="192.168.1.8" | `add_events(investigation_id)`
```

To add events to an investigation using the add_events macro, you must run a search that produces `Events` results. To ensure that your search produces Events results, do the following:

- Include an event-generating command, such as `search`, in your search. You can add transforming commands, such as `stats`, in addition to an event-generating command, but the SPL that follows the transforming command isn't included in the SPL added to the investigation.

  > Some commands, such as makeresults, synthesize results without actually producing Events results. You can't use these commands to add events to an investigation.

  For more information on search command types and to see which ones generate events, see Generating commands in the Splunk Enterprise *Search Reference* manual.
- Run the search in **Verbose** mode. Searches run in Smart mode or Fast mode don't produce Events results and don't add any events to an incident.

If you choose to use the full syntax for `add_events` instead of the macro, ensure to use the following syntax.

```
| sendalert add_events param.investigation_id=<investigation_id>
```

Following the previous example of using the add_events macro, to add events with a source IP of 192.168.1.8 from your chosen index, use the following search.

```
index=<index_name> | search src="192.168.1.8" | sendalert add_events
param.investigation_id=<investigation_id>
```

After you add events to an investigation using the add_events macro, you can find them on the **Events** tab of your investigation. Adding events to an investigation in Splunk Enterprise Security also adds the events in Splunk SOAR (Cloud). In Splunk SOAR (Cloud), you can find the newly added events on the **Investigation** page and continue to investigate them there. See Manage the status, severity, and resolution of events in Splunk SOAR (Cloud) in the *Use Splunk SOAR (Cloud)* manual.

> If you run a search that produces events with missing indexer location values, you can still add the events to an investigation. For example, events produced using a transaction command don't have _cd or _bkt values. If you add these events to an investigation, Splunk Enterprise Security automatically adds them to the index associated with the investigation.

Open a search to find an event

Sometimes, when an investigation has a long list of events, it's difficult to search for a particular event. To find a particular event for your investigation, you can open the search used to generate the investigation's events in the **Events** tab of Splunk Enterprise Security. Then, you can edit the search to filter for particular events.

To open a search to find an event, complete the following steps:

1. Select **Mission Control** in Splunk Enterprise Security.
2. Select an investigation from the **Analyst queue** and then select **View details**.
3. Select the **Events** tab.
4. Select **Open events in search**.
5. Edit the Splunk Search Processing Language (SPL) to reduce the list of events and find the event you're looking for. For example, if you want to find an event with a particular time stamp, such as `time="2022-11-02T19:48:24Z"`, you can edit the SPL to include that time by adding it to the search.

After you open a search from the **Events** tab, you can also use the **Search** tab to start a new search or add events to other investigations.

Automate your investigation response with actions and playbooks in Splunk Enterprise Security

Splunk Enterprise Security uses security orchestration and automation functionality provided by Splunk SOAR (Cloud). You can automate your security workflows in Splunk Enterprise Security by running **actions** and **playbooks** that you created in Splunk SOAR (Cloud). To customize playbook action workflows, you can also respond to prompts.

When you're working on an investigation in Splunk Enterprise Security, you can use the **Automation** tab to review the results of actions and playbooks set to run automatically on the investigation. You can also run playbooks and actions manually and review the results.

> To use automation functionality in Splunk Enterprise Security, an admin must pair your Splunk Enterprise Security instance with your Splunk SOAR instance.

Use automation in Splunk Enterprise Security to complete the following tasks:

- Run a playbook
- Run an action
- Review playbook and action results

- Delegate or respond to a prompt

> When you start an investigation with summary data in Splunk Enterprise Security, all active playbooks that operate on the investigation type for that investigation are triggered to run automatically.

Run a playbook

When you're working on an investigation in Splunk Enterprise Security you can use the **Automation** tab to run a playbook that you created in Splunk SOAR (Cloud) or a playbook included with Splunk Enterprise Security.

Prerequisite

Before you can run a playbook on an investigation, you must first create a playbook in Splunk SOAR (Cloud).

> If you're creating a playbook that uses Splunk Enterprise Security data from investigations, use the Enterprise Security block. If your data doesn't come from Splunk Enterprise Security, use the Utility block. For more information on the Utility block, see Add functionality to your playbook in Splunk SOAR (Cloud) using the Utility block in the Splunk SOAR (Cloud) Build Playbooks with the Playbook Editor manual.

Steps

1. Select an investigation from the **Analyst queue** on the **Mission Control** page in Splunk Enterprise Security.
2. Select the **Automation** tab.
3. Select **Run playbook**.
4. Locate and select the playbook that you want to run from the list.
5. Select **Run playbook**.

After you run a playbook, you can view the playbook details by selecting the entry in the list of automation history on the **Automation** tab.

Run an action

When you're working on an investigation in Splunk Enterprise Security, you can use the **Automation** tab to run an action. With the SOAR Community Edition license, you can run up to 100 actions per day in Splunk Enterprise Security. To upgrade to unlimited actions, contact your account manager.

Prerequisite

Before you can run actions on an investigation, you must configure apps in Splunk SOAR (Cloud).

Steps

1. Select an investigation from the **Analyst queue** on the **Mission Control** page in Splunk Enterprise Security.
2. Select the **Automation** tab.
3. Select **Run Action**.
4. Run an action by following these steps in any order:
    1. Select the **App** that you want to use to run the action.
    2. Select the **Action** that you want to run from the list.
5. Add the required information for your app and action to configure the action.

6. Select **Run Action**.

After you run an action, you can view the action details by selecting the entry in the list of automation history on the **Automation** tab.

Review playbook and action results

After a playbook or action runs, you can view the results from the list of automation history on the **Automation** tab of an investigation. Each entry represents an app with actions run on the investigation. You can select an entry to view more details about the action or playbook run.

Follow these steps to review the results of an action or playbook:

1. Select an investigation from the analyst queue on the **Mission Control** page in Splunk Enterprise Security.
2. Select the **Automation** tab.
3. From the list of automation history, select an action or playbook run that you want to learn more about. You can search for a particular playbook or action run by name, filter runs with the **Show** drop-down list, and sort runs with the **Sort** drop-down list.
    1. (Optional) Some entries default to a table view while others default to a map view. You can view the action or playbook run details by the default visual format, or you can switch to a JSON format. To switch from either a map or a table view to a JSON format view, select the JSON source code icon (</>).

        > You can only review failed action and playbook runs with the JSON format view.
    2. (Optional) Select the download icon (⬇) to download the JSON output for the action or playbook run.
    3. (Optional) For playbook runs, select **Open Playbook** to view the associated playbook in Splunk SOAR (Cloud).

Stop a playbook run in progress

You can stop a playbook run while it's in progress for an investigation in Splunk Enterprise Security. If you stop a playbook, you lose any progress made on the playbook run. You must rerun the playbook to complete any actions in the playbook.

Follow these steps to stop a playbook run for an investigation:

1. Select the investigation from the analyst queue on the **Mission Control** page in Splunk Enterprise Security.
2. Select the **Automation** tab.
3. From the list of automation history, locate the playbook run that you want to stop and select the cancel (x) icon.
4. Select **Stop playbook run** to confirm that you want to stop it.

Set up actions and playbooks to run with response plan tasks

You can automate your response by setting up actions and playbooks to run with a specific response plan task in Splunk Enterprise Security. Setting up an action or playbook to run on a task might be helpful for analysts who prefer to add tasks or response plans as they undergo their investigation. For example, if you want a response plan to automatically add a new phase at the completion of a task, you can set up a playbook to run with that response plan task.

To set up an action or playbook to run with a response plan task, complete the following steps:

1. In Splunk Enterprise Security, select **Security content** and then **Response plans**.
2. Open an existing response plan, or create a new one.

3. Expand the phase you want to edit, or select **+ Phase**.
4. Expand the task you want to edit, or select **+ Task**.
5. To set up an action to run with a response plan task, complete the following steps:
    1. Expand the **Actions** section.
    2. Select **+ Action**.
    3. Select the **App** that you want to use to run the action.
    4. Select the **Action** that you want to run from the list.
    5. Add the required information for your app and action to configure the action.
    6. Select **Submit**.
6. To set up a playbook to run with a response plan task, complete the following steps:
    1. Expand the **Playbooks** section.
    2. Select **+ Playbook**.
    3. Locate and select the playbook that you want to run from the list.
    4. Select **Submit**.
7. (Optional) To remove an action or playbook run from a response plan task, select the remove icon (☒) next to the respective action or playbook.
8. Toggle the **Status** switch to **Published**, and select **Save changes** to publish the response template. You can only add published response plans to investigations.

After you set up an action or playbook to run with a response plan task, you can find the status of the action or playbook, such as `Failed` or `Completed`, by selecting the task in the **Response** tab of an investigation.

Delegate or respond to a prompt

A prompt is a checkpoint that determines a playbook action workflow based on a user's response in Splunk Enterprise Security. Respond to a prompt to change or confirm the next playbook action, or delegate the prompt to another user.

For example, if a playbook locks an account for suspicious login attempts, a prompt block can pose the question "Do you want to lock this user's account?" to an analyst before running the action. To delegate or respond to a prompt, complete the following steps:

1. Select an investigation from the **Analyst queue** in Splunk Enterprise Security.
2. Select the **Automation** tab.
3. Select **Prompts**. The badge represents the number of prompts assigned to you that you haven't responded to yet.
4. Find the prompt you want to delegate or respond to and select **View**.

    > You can only view a prompt if you are the owner of that prompt.
5. Review the prompt details such as the deadline, the associated playbook, and the message.
6. If you want to respond to the prompt, answer the question. Some prompts are informational only and do not include questions. If the prompt does not include a question, continue to the next step.
7. If you want to assign the prompt to another user, select the **Delegate** check box.
    1. Select a user or role from the drop-down list to delegate the prompt to.
    2. Enter a reason for delegating the prompt so that the receiving user understands why you're assigning it to them.
8. Select **Submit**.

After you delegate or respond to a prompt, the status and response for that prompt updates. If the status is `Approved`, for example, the playbook runs the succeeding action. If the status is `Delegated`, the reason for delegation appears as the response.

See also

For more details on automating your investigation response in Splunk Enterprise Security, see the product documentation:

- Use playbooks to automate analyst workflows in Splunk SOAR (Cloud) in the Splunk SOAR (Cloud) *Build Playbooks with the Playbook Editor* manual
- Create a new playbook in Splunk SOAR (Cloud) in the Splunk SOAR (Cloud) *Build Playbooks with the Playbook Editor* manual
- Automate responses with Splunk Enterprise Security playbooks in the Splunk SOAR (Cloud) *Build Playbooks with the Playbook Editor* manual
- Add and configure apps and assets to provide actions in Splunk SOAR (Cloud) in the *Administer Splunk SOAR (Cloud)* manual
- Create response plans in Splunk Enterprise Security in the *Administer Splunk Enterprise Security* manual
- Pair Splunk Enterprise Security with Splunk SOAR in the *Administer Splunk Enterprise Security* manual

Analyze risk with risk-based alerting in Splunk Enterprise Security

Splunk Enterprise Security uses risk-based alerting (RBA) to accelerate and simplify the process of detecting risk in your security environment. The Risk Analysis framework integrates with content management in Splunk Enterprise Security to provide context and enrich raw data.

As a security analyst or threat detection engineer responsible for identifying threats and prioritizing detections in your security environment, you can use detections to generate findings instead of using the Splunk Search Processing Language (SPL) to drill down on high volumes of alerts or raw data. With RBA, you can create high fidelity findings based on risk and increase true positive rates. You can also frame how findings relate to specific assets or identities and develop security stories based on user behaviors to proactively identify threats. This can help you focus on higher impact tasks such as threat hunting and adversary simulation instead of manually triaging findings. Use RBA to identify the most difficult-to-detect security use cases such as the following:

- Insider threats
- Compromised user accounts
- Compromised systems
- Recurring infections
- Suspicious use of credentials
- Lateral movement
- Living off-the-land cyber-attacks

How risk-based alerting works in Splunk Enterprise Security

With risk-based alerting (RBA), analysts receive findings from detections, which surface from multiple intermediate findings. Risk-based alerting uses the existing Splunk Enterprise Security detection framework to collect all intermediate findings into a single risk index. Events collected in the risk index create a single finding when they meet a specific criteria, which warrants an investigation.

For example, suppose a single system creates five intermediate findings from several detections. Each of these intermediate findings have a low risk score. However, when taken together these intermediate findings surpass the risk score threshold, pertain to specific MITRE ATT&CK techniques, and are associated with unique data sources over multiple time frames. Risk-based alerting can pick up on this threat even when the system generates only a single finding because it performs correlated alerting that tells a high-fidelity security story, which analysts can investigate.

Similarly, RBA helps detect complex behavior over a period of time instead of a point in time. For example, an impatient hacker might try various techniques to attack a single server over a period of time. Risk-based alerting uses a variety of alerting criteria over a varying duration of time to provide insight into your environment, which helps to tune detections to your environment in addition to threat hunting.

Therefore, you can review the following alerts, which use different factors and time duration to detect threat:

Alert	Description
Score threshold 100 exceeded over 24 hours	This alert uses combined scores of events to trigger an alert.
Events from multiple sourcetypes over 3 days	This alert uses three unique data sources that generate events from a single machine.
Multiple MITRE ATT&CK tactics observed over 7 days	This alert uses observations tagged with MITRE ATT&CK tactics and techniques.

The following steps illustrate how RBA works in Splunk Enterprise Security.

Step 1: Detections identify anomalies and assign risk scores to events

A detection runs against raw events and indicates potentially malicious activity. A detection contains the following three components:

- Search logic using the Search Processing Language (SPL)
- Risk annotations
- Risk analysis adaptive response action for generating intermediate findings

All intermediate findings are written to the risk index. The following list includes examples of detections:

- Traffic to Non-standard Port
- Threat Intel Match
- Suspicious Logon Type

The detections identify anomalies and log search results or intermediate findings to the risk index. Splunk Enterprise Security uses the Risk Framework to dynamically calculate a risk score for each event using risk modifiers. Splunk Enterprise Security also associates the event with specific assets and identities such as users or systems.

Step 2: Detections review the events in the risk index and use an aggregation of events impacting a single entity to generate findings

Detections review the risk index for anomalous events and threat activities. When the detections find an entity associated with several intermediate findings, the detections create findings in Splunk Enterprise Security. When the risk scores associated with the findings surpass a specified threshold over a period of time, analysts focus their efforts on connected behaviors associated with the finding. The aggregated risk score of an asset or identity is the sum of all the risk scores for intermediate findings in the risk index that apply to the specific asset or identity over a period of time.

For example, a finding might be created when the detection identifies a single machine that generated 5 intermediate findings. These events can be combined to cross a threshold of the following factors:

- Risk score
- MITRE ATT&CK techniques
- Unique data sources over various time frames

Step 3: Risk factors trigger intermediate findings in the risk index

Analysts can also define risk factors that add or multiply risk scores associated with assets and identities such as users or systems when suspicious behavior occurs. For example, an analyst might want to multiply risk scores by 1.5 for a privileged user, who is also an administrator. Instead of triggering a finding that populates the Mission Control page, risk factors trigger an intermediate finding in the risk index.

Step 4: Context rich findings help to triage and neutralize threat

Analysts can also add relevant context to risk attributions by mapping them against a relevant cybersecurity framework or applying a risk score to the finding. You can associate findings with conditions such as MITRE ATT&CK tactics or techniques. MITRE ATT&CK tactics are categories of activities such as privilege escalation or command and control, while MITRE ATT&CK techniques are specific activities such as kerberoasting or protocol tunneling. Using Splunk Security Essentials or Splunk Enterprise Security content updates, you can identify the techniques covered by your data sources and build a breadth of detections across every tactic. Splunk Enterprise Security also supports NIST, CIS, Critical Security Controls, and the Lockheed Martin Cyber Kill Chain frameworks. When a risk score or behavioral pattern of an asset or identity meets a predetermined threshold, it triggers a finding or alert, which provides analysts with valuable context at the onset of their investigation process and expedites the neutralization of threats.

Advantages of using risk-based alerting in Splunk Enterprise Security

Using RBA to analyze risk in your security environment offers the following advantages:

Advantage	Description
Address threats and identify security gaps with leading cybersecurity frameworks	Apply insights from cybersecurity frameworks such as MITRE ATT&CK, CIS 20, and NIST Controls to create visualizations that highlight the tactics and techniques observed in intermediate findings. You can use these visualizations to quickly build situational awareness around a given user or system in the context of the ATT&CK matrix and view the associated documentation on a given technique. With this additional context, you can proactively detect threats such as adversary simulation. With your preferred framework, you can also quantify security gaps and identify the MITRE tactics covered to plan your response without using SPL.
Identify relationships between threat actors using visualizations	Visualizations such as Threat Topology and Risk Event Timeline allow analysts to quickly visualize relationships between malicious threat actors and their users and systems when working with findings. Analysts can discover the scope of a security incident immediately and quickly pivot between affected assets and identities in the investigation.
Detect complex threats by expanding security coverage	Surface attacks by building a comprehensive collection of attributes. You can build investigations that span over longer periods of time and prevent malicious tactics that infiltrate the SOC through low-level attacks. For example, you can configure alerts when an entity's behavior spans three or more MITRE ATT&CK tactics over a two-week period, expanding your security coverage.
Streamline investigations and remediation	Reduce the triage time for security incidents by providing context to the investigative process and reducing alert volume, which helps analysts focus on other high-value activities within the SOC.

Detect fraud using RBA in the Splunk App for Fraud Analytics

You can also use the Splunk App for Fraud Analytics to detect fraud. This app uses the RBA framework to provide high fidelity and actionable fraud alerts for account takeovers and new account fraud. You can also use this app to get started with RBA using some default searches and dashboards even if you do not have prior knowledge of SPL.

Download and install the Splunk App for Fraud Analytics in your Splunk Platform environment from Splunkbase. For more information on the app, see Splunk App for Fraud Analytics User Guide.

Additionally, you can contact your Splunk Sales representative to deploy this app along with your existing Splunk Enterprise Security deployment. With this app, you can display fraud related alerts and drill down on fraud analysis dashboards in Splunk Enterprise Security.

You do not need to download the app to use RBA in Splunk Enterprise Security.

See also

For more details on risk-based alerting in Splunk Enterprise Security, see the product documentation:

- Risk scoring in Splunk Enterprise Security
- Modifying risk using risk modifiers in Splunk Enterprise Security
- Assign risk using risk modifiers in Splunk Enterprise Security
- Review risk-based findings in Splunk Enterprise Security
- Create risk factors to adjust risk scores in Splunk Enterprise Security

Investigate observables related to an investigation in Splunk Enterprise Security

In Splunk Enterprise Security, you can add threat intelligence data to enhance your security monitoring capabilities and enrich investigations with added context from observables. An observable is a piece of data indicating that an event has occurred or been observed on a computer system, network, or other digital entity. Splunk Enterprise Security record observables, which can be malicious or benign, as part of an investigation. With threat intelligence data, you can correlate known threats and indicators of suspicious activity with your events.

After you have access to threat intelligence data, you can start managing observables and reviewing their priority scores on the **Intelligence** tab of your investigation.

Filter and sort observables

Filter, sort, and search for observables on the **Intelligence** tab of your investigation in Splunk Enterprise Security. To manage observables, complete the following steps:

1. In Splunk Enterprise Security, select **Mission Control**.
2. Select an investigation from the analyst queue.
3. Select **View details**.
4. Select the **Intelligence** tab.
5. To filter observables, select the column header of the field you want to filter by. You can sort and filter a field by selecting the down arrow icon (▾) in the column header or by entering a search in the observable search bar. Fields that aren't filterable don't have a filter menu with check boxes.
6. In the filter menu, select a value. For some fields, such as **Score**, you can select multiple values, such as **Medium** and **High**.
7. To remove a filter so that it no longer applies to observables, select the remove icon (✕) next to the respective filter, or select **Clear all** to remove them all.
8. To sort observables, select the column header of the field you want to sort by. Then, select the up arrow icon (↑) or the down arrow icon ( ) to determine which observables appear first.

Review priority scores for observables

After you set up threat intelligence in Splunk Enterprise Security, select an observable in the **Intelligence** tab of your investigation to begin exploring potential pain points.

The list of observables includes those found in the following investigation fields:

- risk_object
- threat_object
- threat_match_value
- host
- orig_host
- dvc
- dest
- src
- src_user
- user

Different intelligence sources often use different scoring systems, which makes it difficult to compare threats across sources. For example, one source might use the scale of 1 through 10 for severity, and another source might use text labels such as `Benign` or `Malicious`.

The threat intelligence system normalizes the different scores using a conversion table so that you can compare all scores across different intelligence sources. You can use these scores to evaluate the risk associated with an observable or risk event.

After you select an observable, you can find its **passthru score** and **normalized score** by expanding the **Most recent reporting from each source** section. The priority score is the badge that appears in the **Summary of "`<observable>`"** section.

The following table defines the scores associated with each observable.

Score	Description
Passthru score	The original score assigned to the observable by an external intelligence source.
Normalized score	The score created by the threat intelligence system and assigned to the observable to show the relative severity of the observable. Normalized scoring automatically converts the passthru score from an intelligence source into a value that reflects the observable's severity on a standardized scale.
Priority score	The score that aggregates the normalized scores from all the IOCs to create one score for that observable.

Some observables don't have any intelligence information. If you select an observable with no intelligence information, select Search to open the Search page and find related threat intelligence indicators.

Intelligence sources provide the tags and attributes for the observable in the **Summary of "`<observable>`"** section. However, you can't distinguish which specific intelligence source provided each tag or attribute.

See also

For more details on threat intelligence in Splunk Enterprise Security, see the product documentation:

- Overview of threat intelligence in Splunk Enterprise Security
- Configure intelligence source integrations in Splunk Enterprise Security
- Turn on threat-matching searches in Splunk Enterprise Security
- Configure threat lists in Splunk Enterprise Security
- Create and manage safelist libraries in Splunk Enterprise Security

Analytics

Available dashboards in Splunk Enterprise Security

Splunk Enterprise Security includes more than 100 dashboards that provide integrated views and communicate key data that you can customize and share with intended end users. Use Splunk Enterprise Security dashboards to identify and analyze findings and investigations, reveal insights in your events, accelerate investigations, monitor the status of various security domains, and audit your investigations and your Splunk Enterprise Security deployment.

Finding and investigation overview dashboards

You can identify and investigate findings with a suite of dashboards and workflows. Splunk Enterprise Security uses event-based detections to identify and investigate findings in your environment. See the following dashboards:

- Security posture dashboard
- Executive summary dashboard
- SOC operations dashboard

Security intelligence dashboards

You can accelerate your investigations with specific types of intelligence using security intelligence dashboards.

- The **Risk analysis** dashboard allows you to assess the risk scores of systems and users across your network and identify particularly risky devices and users posing a threat to your environment. See Risk analysis dashboard.
- The **Protocol intelligence** dashboards use packet capture data from stream capture apps to provide network insights that are relevant to your security investigations. Identify suspicious traffic, DNS activity, and email activity, and review the connections and protocols in use in your network traffic. See Protocol intelligence dashboards.
- The **Threat intelligence** dashboards use the threat intelligence sources included in Splunk Enterprise Security and custom sources that you configure to provide context to your investigations and identify known malicious actors in your environment. See Threat intelligence dashboards.
- The **User intelligence** dashboards allow you to investigate and monitor the activity of users and assets in your environment. See Asset and identity investigator dashboards and User activity dashboard.
- The **Web intelligence** dashboards help you analyze web traffic in your network and identify notable HTTP categories, user agents, new domains, and long URLs. See Web intelligence dashboards.

Security domain dashboards

Security domain dashboards provided with Splunk Enterprise Security allow you to monitor the events and status of important security domains. You can review the data summarized on the main dashboards, and use the search dashboards for specific domains to investigate the raw events.

- The **Access** domain dashboards display authentication and access-related data, such as login attempts, access control events, and default account activity. See Access dashboards.
- The **Endpoint** domain dashboards display endpoint data relating to malware infections, patch history, system configurations, and time synchronization information. See Endpoint dashboards.
- The **Network** domain dashboards display network traffic data provided by devices such as firewalls, routers, network intrusion detection systems, network vulnerability scanners, proxy servers, and hosts. See Network dashboards and Web center and network changes dashboards and Port and protocol tracker dashboard.

- The **Identity** domain dashboards display data from your asset and identity lists as well as the types of sessions in use. See Asset and identity dashboards.

Audit dashboards

The audit dashboards provide insight into background processes and tasks performed by Splunk Enterprise Security. Some audit dashboards allow you to review actions taken by users in Splunk Enterprise Security, while others provide insight into your deployment and the status of your data models and content use. See Audit dashboards.

Cloud security dashboards

You can explore your cloud security environment by displaying visualizations from your Amazon Web Services (AWS) and Microsoft 365 environments using the **Cloud security** dashboards. You can access the dashboards through the cloud security menu and use them for insights into potential security issues such as errors, unusual events, unintended access, and suspicious activity.

- Security groups for your VPC in Splunk Enterprise Security
- User and authentication activity in Splunk Enterprise Security
- Network ACL analytics in Splunk Enterprise Security
- AWS access analyzer in Splunk Enterprise Security
- Microsoft 365 security in Splunk Enterprise Security

Prerequisites to use cloud security dashboards

Using cloud security dashboards, you can onboard cloud data sources and explore your cloud security environment by displaying visualizations of your Amazon Web Services (AWS) and Microsoft 365 environments. To use cloud security dashboards, you must meet the following prerequisites:

> If you are currently using the Amazon Web Services (AWS) and Microsoft 365 TAs, you can configure your existing indexes following these steps, instead of creating a new index.

1. Create indexes to populate the cloud security dashboards. For more information on creating custom indexes, see Create custom indexes.
2. Provide the index name in the Splunk Enterprise Security app settings following these steps:
    1. From the Splunk Enterprise Security menu, select **Configure** then **General** and then **General settings**. This displays the configuration settings of Splunk Enterprise Security by applications.
    2. Navigate to **AWS Index** or **Microsoft 365**. The default index value for the **AWS Index** is: `aws_security` and the default index value for the **Microsoft 365** is `o365_security`.

        > No indexes exist with the default names. You must create your own indexes to populate the cloud security dashboards and provide the name of the index field for both the AWS Index and the MS 365 Index.
    3. Populate the index name in the app settings for **AWS Index** and **Microsoft 365** Index.
3. Install the Splunk Add-on for Amazon Kinesis Firehose and Splunk Add-on for Microsoft Office 365 from Splunkbase.
    - For more information on installing the add-on, see Splunk Add-on for Amazon Kinesis Firehose
    - For more information on installing the add-on, see Splunk Add-on for Microsoft Office 365

Installing these add-ons helps to populate the cloud security dashboards and use them for insights into potential security issues such as errors, unusual events, unintended access, and suspicious activity.

4. Configure the add-ons to send data to the Splunk platform and prepare the Splunk platform to receive the data.
   - For more information on configuring Splunk Add-on for Amazon Kinesis Firehose, see Configure Firehose.
   - For more information on configuring Splunk Add-on for Microsoft 365, see Configure Microsoft 365

Now you can use the visualizations on the following cloud security dashboards to explore your Amazon Web Services (AWS) and Microsoft 365 environments.

Risk factors turned on by default

The following risk factors are turned on by default:

- The Critical Severity Alert risk factor increases the risk when the alert is critical severity.
- The High Severity Alert risk factor increases the risk when the alert is high severity.
- The Medium Severity Alert risk factor does not increase or decrease the risk when the alert is medium severity.
- The Informational Severity Alert risk factor decreases the risk when the alert is informational severity.
- The Low Severity Alert risk factor decreases the risk when the alert is low severity.

> You can modify the calculated score for AWS GuardDuty and Security Hub alert risk events.

See also

- Security groups for your VPC in Splunk Enterprise Security
- User and authentication activity in Splunk Enterprise Security
- Network ACL analytics in Splunk Enterprise Security
- AWS access analyzer in Splunk Enterprise Security
- Microsoft 365 security in Splunk Enterprise Security

Security posture dashboard

The **Security posture** dashboard is designed to provide high-level insight into the findings across all domains of your deployment, suitable for display in a security operations center (SOC). This dashboard shows all events from the past 24 hours, along with the trends over the past 24 hours, and provides real-time event information and updates.

Dashboard panels

Panel	Description
Key indicators	Displays the count of findings by security domain over the past 24 hours.
Findings by urgency	Displays the findings by urgency in the last 24 hours. Findings by urgency uses an urgency calculation based on the priority assigned to the asset and the severity assigned to the detection. The drilldown opens the analyst queue on the **Mission Control** page, showing all findings with the selected urgency in the last 24 hours.
Findings over time	Displays a timeline of findings by security domain. The drilldown opens the analyst queue on the **Mission Control** page, showing all findings in the selected security domain and time frame.

Panel	Description
Top findings	Displays the top findings by rule name, including a total count and a sparkline to represent activity spikes over time. The drilldown opens the analyst queue on the **Mission Control** page scoped to the selected finding rule.
Top findings sources	Displays the top 10 findings by `src`, including a total count, a count per correlation and domain, and a sparkline to represent activity spikes over time. The drilldown opens the analyst queue on the **Mission Control** page scoped to the selected finding source.

Executive summary dashboard

The **Executive summary** dashboard is designed to provide a high level insight into security operations so that executives can evaluate security trends over time based on key metrics, findings, risk, and other additional metrics. Use the **Executive Summary** dashboard to prioritize security operations, monitor the overall health and evaluate the risk to your organization.

Dashboard panels

Key metrics

Panel	Description and default search
Mean time to triage	Displays the average time in minutes to triage or prioritize an investigation over the duration of a specified time period. Also, displays a trendline in absolute value that indicates how the mean time taken to triage the finding compares to the previous mean time taken to triage the finding over the same time period. For example, the trendline may display that the mean time to triage a finding over the last 7 days is 0.5% up or down over the mean time taken to triage the finding during the previous 7 day time period. For more information, see Triage notable events in Splunk Enterprise Security. `| tstats summariesonly=true earliest(_time) as _time FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | rename "Notable_Events_Meta.*" as "*" | lookup update=true incident_updates_lookup rule_id OUTPUTNEW time | search time=* | stats earliest(_time) as create_time, earliest(time) as triage_time by rule_id | eval diff=triage_time-create_time, stat_type=if(create_time < relative_time(now(), "-7d@d"), "past", "current"), past=if(stat_type="past", 1, 0), current=if(stat_type="current", 1, 0), past_diff=if(stat_type="past", diff, 0), current_diff=if(stat_type="current", diff, 0) | stats sum(past) AS past, sum(current) AS current, sum(past_diff) AS past_diff, sum(current_diff) as current_diff | eval past = round(past_diff/past/60), current = round(current_diff/current/60) | table past, current | transpose | rename "column" as stat_type,"row 1" as mean_triage_time | fillnull value=0 mean_triage_time`
Mean time to resolution	Displays the average time in minutes taken by the finding to reach its configured end status over the duration of a specified time period. Also, displays a trendline in absolute value that indicates how the mean time taken by the finding to reach its configured end status compares to the previous mean time taken by the finding to reach its configured end status over the same time period. For more information, see Take action on notable events in Splunk Enterprise Security. `| tstats summariesonly=true earliest(_time) as _time FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | rename "Notable_Events_Meta.*" as "*" | eval temp_time=time()+86400 | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUTNEW time, status | `get_reviewstatuses` | search time=* AND status_end=true | stats first(_time) as create_time, last(time) as resolve_time by rule_id | eval`

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td></td><td>diff=resolve_time-create_time, stat_type=if(create_time < relative_time(now(), "-7d@d"), "past", "current"), past=if(stat_type="past", 1, 0), current=if(stat_type="current", 1, 0), past_diff=if(stat_type="past", diff, 0), current_diff=if(stat_type="current", diff, 0) | stats sum(past) AS past, sum(current) AS current, sum(past_diff) AS past_diff, sum(current_diff) as current_diff | eval past = round(past_diff/past/60), current = round(current_diff/current/60) | table past, current | transpose | rename "column" as stat_type,"row 1" as mean_resolution_time | fillnull value=0 mean_resolution_time</td></tr>
<tr><td>Investigations created</td><td>Displays the number of investigations created in the SOC over the duration of a specified time period. Also, displays a trendline in absolute value that indicates how the mean number of investigations created compares to the previous mean number of investigations created over the same time period. For more information, see Start an investigation in Splunk Enterprise Security.

| inputlookup investigation_lookup | where create_time > relative_time(now(), "-14d@d") | stats count(eval(create_time < relative_time(now(), "-7d@d"))) AS past, count(eval(create_time >= relative_time(now(), "-7d@d"))) AS current | transpose | rename "column" as count_type, "row 1" as count</td></tr>
</table>

You can access the key performance indicator (KPI) panel for **Investigations created** on the **Executive summary** dashboard. Only the `admin` and the `ess_admin` roles have the `manage_all_investigations` capability by default. For all other roles such as `ess_analyst`or `ess_user`, you see an error message on the **Investigations created** KPI panel. An administrator can add the `manage_all_investigations` capability for users that allows other users to access the **Investigations created** KPI panel on the executive summary dashboard. For more information on adding capabilities to a specific role, see Specify role capabilities.

Findings

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td>Distribution by urgency</td><td>Displays the distribution of the urgency level that is calculated based on the severity and priority level of a finding over the duration of a specified time period. The distribution is based on the following categories: <b>Critical</b>, <b>High</b>, <b>Medium</b>, <b>Low</b>, <b>Information</b>, and <b>Unknown</b>. For more information, see How urgency is assigned to a notable event in Splunk Enterprise Security.

`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW severity | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT urgency as new_urgency | eval urgency=if(isnotnull(new_urgency),new_urgency,urgency) | `get_urgency` | eval urgency = upper(substr(urgency,1,1)).lower(substr(urgency,2)) | timechart span=1d count by urgency</td></tr>
<tr><td>Findings by domain</td><td>Displays the classification of the findings by security domains, such as <b>Access</b>, <b>Endpoint</b>, <b>Network</b>, <b>Threat</b>, <b>Identity</b>, and <b>Audit</b> over the duration of a specified time period.

| tstats summariesonly=true earliest(_time) as _time, first(source) as source FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW security_domain | fillnull value="threat" security_domain | lookup update=true security_domain_lookup security_domain OUTPUTNEW label as security_domain_label | timechart span=1d count by security_domain_label</td></tr>
<tr><td>Untriaged findings by domain</td><td>Displays the classification the untriaged findings by security domain, such as <b>Access</b>, <b>Endpoint</b>, <b>Network</b>, <b>Threat</b>, <b>Identity</b>, and <b>Audit</b> over the duration of a specified time period.</td></tr>
</table>

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td></td><td>| tstats summariesonly=true earliest(_time) as _time, first(source) as source FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | rename "Notable_Events_Meta.*" as "*" | eval temp_time=time()+86400 | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT time as triage_time | where isnull(triage_time) | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW security_domain | fillnull value="threat" security_domain | lookup update=true security_domain_lookup security_domain OUTPUTNEW label as security_domain_label | timechart span=1d count by security_domain_label</td></tr>
<tr><td>Top 10 untriaged findings by source</td><td>Displays the top 10 untriaged findings by their sources over the duration of a specified time period.

`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT time as triage_time | where isnull(triage_time) | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW rule_name | eval rule_name=if(isnull(rule_name),source,rule_name) | stats count by rule_name | sort - count | head 10</td></tr>
<tr><td>Untriaged findings by type</td><td>Displays the classification of findings based on whether or not they indicate risk over the duration of a specified time period.

`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT time as triage_time | where isnull(triage_time) | eval type=if(isnotnull(risk_object), "Risk Notable", "Notable") | timechart span=1d count by type</td></tr>
<tr><td>Frequent finding sources</td><td>Displays the sources that generate the most number of findings over the duration of a specified time period.

`get_notable_index` | eval source=case(isNotNull(orig_source), orig_source, isNotNull(source_correlation_search), source_correlation_search, 1=1, source) | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW rule_name | eval rule_name=if(isnull(rule_name),source,rule_name) | stats count by rule_name | sort - count | head 10</td></tr>
<tr><td></td><td>Displays the sources that generate the least number of findings over the duration of a specified time period.

`get_notable_index` | eval source=case(isNotNull(orig_source), orig_source, isNotNull(source_correlation_search), source_correlation_search, 1=1, source) | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW rule_name | eval rule_name=if(isnull(rule_name),source,rule_name) | stats count by rule_name | sort + count | head 10|}</td></tr>
</table>

Risk

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td>Risk Notables vs Notable Events</td><td>Displays a comparison graph of regular notables versus risk notables in the SOC over the duration of a specified time period.

`get_notable_index` | eval notable_type=if(isnotnull(risk_object) AND isnotnull(risk_object_type), "Risk Notable", "Notable") | fields notable_type, count | timechart span=1d count by notable_type</td></tr>
<tr><td>Risk Events Contributing to Risk Notables</td><td>Displays a comparison graph of risk events that generated risk notables versus the risk events that did not generate risk notables over the duration of a specified time period.

(index=risk) OR (`get_notable_index` risk_object=*) | eval source=case(index="risk",source,isnull(orig_source),source_correlation_search,1=1,orig_source),search</td></tr>
</table>

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td></td><td><code>_time=if(index="notable",mvzip(info_min_time,mvsort(info_max_time)),null()),risk_id=if(index="risk",replace(_bkt,".*~(.+)","\1")."@@".index."@@".md5(_time._raw),null()), risk_id_time=if(index="risk",mvzip(risk_id,_time),null()) | stats values(index) AS index, values(risk_id_time) AS risk_id_time, values(search_time) AS search_time by source, risk_object, risk_object_type | mvexpand risk_id_time | mvexpand search_time | eval risk_id=if(isnull(risk_id_time),null(),mvindex(split(risk_id_time,","),0)),risk_time=if(isnull(risk_id_time),null(),mvindex(split(risk_id_time,","),1)),search_earliest=if(isnull(search_time),null(),mvindex(split(search_time,","),0)), search_latest=if(isnull(search_time),null(),mvindex(split(search_time,","),1)),contributing=if(isnull(search_earliest) OR isnull(search_latest) OR risk_time <= search_earliest OR risk_time >= search_latest,"false","true") | stats values(contributing) as contributing, values(risk_time) as _time by risk_id | eval contributed=if(contributing="true", "Contributed", "Not Contributed") | timechart span=1d count by contributed</code></td></tr>
<tr><td>Risk Event Types Not Contributing to Risk Notables</td><td>Displays a list in descending order of frequency of the type of risk events that did not generate risk notables over the duration of a specified time period.
<code>(index=risk) OR (`get_notable_index` risk_object=*) | eval source=if(index="notable",if(isnull(orig_source),source_correlation_search, orig_source), source) | stats count, values(index) as index by source | where index != "notable" | `get_correlations` | table rule_name, count | sort - count</code></td></tr>
</table>

Additional Metrics

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td>Adaptive Response Actions Triggered</td><td>Displays a graph indicating the type and frequency of the adaptive response actions that were triggered over the duration of a specified time period.
<code>| tstats summariesonly=true count from datamodel=Splunk_Audit.Modular_Actions where Modular_Actions.is_Modular_Action_Invocations=1 by _time, Modular_Actions.action_mode, Modular_Actions.action_name | `drop_dm_object_name("Modular_Actions")` | eval action_mode=if(action_mode="saved","automated", action_mode), action_name=action_mode+"-"+action_name | fields - action_mode | timechart span=1d sum(count) as count by action_name</code></td></tr>
<tr><td>Sources with Notable Action vs Risk Action Enabled</td><td>Displays a graph indicating how many enabled sources have risk actions versus notables actions over the duration of a specified time period.
<code>| inputlookup correlationsearch_changes_lookup | where _time > relative_time(now(),"-7d@d") | sort - _time | bin _time span=1d | dedup label, _time | where (disabled == 0) | mvexpand actions | where actions="notable" OR actions="risk" | eval actions=if(actions="notable", "Notable Action", "Risk Action") | timechart span=1d count by actions</code></td></tr>
<tr><td>Correlation Searches Enabled vs Disabled</td><td>Displays a bar chart that provides a distribution of the correlation searches enabled versus correlation searches disabled in the SOC over the duration of a specified time period.
<code>| inputlookup correlationsearch_changes_lookup | where _time > relative_time(now(),"-7d@d") | sort - _time | bin _time span=1d | dedup label, _time |</code></td></tr>
</table>

Panel	Description and default search
	`timechart span=1d count by disabled | rename 0 as Enabled, 1 as Disabled`

For key indicator panels and time chart visualizations on the Executive Summary dashboard, some arguments in the underlying SPL searches may be dynamically updated based on the time range selected on the dashboard UI.

SOC operations dashboard

The SOC Operations dashboard is designed to provide insight into the security operations center (SOC) based on key metrics, workflows, and dispositions so that you can monitor the efficiency of the SOC and ensure that all security operations (detections, analysis, and responses) are on track.

Dashboard panels

Key metrics

Panel	Description and default search
Mean Time to Triage	Displays the average time (in minutes) to triage or prioritize the investigation of a notable over the duration of a specified time period. Also, displays a trendline (in absolute value) that indicates how the mean time taken to triage the notable compares to the previous mean time taken to triage the notable over the same time period. For example, the trendline may display that the mean time to triage a notable over the last 7 days is 0.5% up or down over the mean time taken to triage the notable during the previous 7 day time period. For more information, see Triage notable events in Splunk Enterprise Security. `| tstats summariesonly=true earliest(_time) as _time FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | rename "Notable_Events_Meta.*" as "*" | lookup update=true incident_updates_lookup rule_id OUTPUTNEW time | search time=* | stats earliest(_time) as create_time, earliest(time) as triage_time by rule_id | eval diff=triage_time-create_time, stat_type=if(create_time < relative_time(now(), "-7d@d"), "past", "current"), past=if(stat_type="past", 1, 0), current=if(stat_type="current", 1, 0), past_diff=if(stat_type="past", diff, 0), current_diff=if(stat_type="current", diff, 0) | stats sum(past) AS past, sum(current) AS current, sum(past_diff) AS past_diff, sum(current_diff) as current_diff | eval past = round(past_diff/past/60), current = round(current_diff/current/60) | table past, current | transpose | rename "column" as stat_type,"row 1" as mean_triage_time | fillnull value=0 mean_triage_time`
Mean Time to Resolution	Displays the average time (in minutes) taken by the notable to reach its configured end status over the duration of a specified time period. Also, displays a trendline (in absolute value) that indicates how the mean time taken by the notable to reach its configured end status compares to the

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td></td><td>previous mean time taken by the notable to reach its configured end status over the same time period. For more information, see Take action on notable events in Splunk Enterprise Security.

| tstats summariesonly=true earliest(_time) as _time FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id" | rename "Notable_Events_Meta.*" as "*" | eval temp_time=time()+86400 | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUTNEW time, status | `get_reviewstatuses` | search time=* AND status_end=true | stats first(_time) as create_time, last(time) as resolve_time by rule_id | eval diff=resolve_time-create_time, stat_type=if(create_time < relative_time(now(), "-7d@d"), "past", "current"), past=if(stat_type="past", 1, 0), current=if(stat_type="current", 1, 0), past_diff=if(stat_type="past", diff, 0), current_diff=if(stat_type="current", diff, 0) | stats sum(past) AS past, sum(current) AS current, sum(past_diff) AS past_diff, sum(current_diff) as current_diff | eval past = round(past_diff/past/60), current = round(current_diff/current/60) | table past, current | transpose | rename "column" as stat_type,"row 1" as mean_resolution_time | fillnull value=0 mean_resolution_time</td></tr>
<tr><td>Investigations Created</td><td>Displays the number of investigations created in the SOC over the duration of a specified time period. Also, displays a trendline (in absolute value) that indicates how the mean number of investigations created compares to the previous mean number of investigations created over the same time period. For more information, see Start an investigation in Splunk Enterprise Security.

| `investigations` all=true strict=true | where create_time > relative_time(now(), "-14d@d") | stats count(eval(create_time < relative_time(now(), "-7d@d"))) AS past, count(eval(create_time >= relative_time(now(), "-7d@d"))) AS current | transpose | rename "column" as count_type, "row 1" as count</td></tr>
</table>

Workflow

<table>
<tr><th>Panel</th><th>Description and default search</th></tr>
<tr><td>Assigned Notables Over Time</td><td>Displays a comparison graph of assigned versus unassigned notables over the duration of a specified time period.

`get_notable_index` | eval `get_event_id_meval`, rule_id=event_id | `get_current_status` | `get_owner` | timechart span=1d count(eval(owner!="unassigned")) AS "Assigned Notables", count(eval(owner="unassigned")) AS "Unassigned Notables"</td></tr>
<tr><td></td><td></td></tr>
</table>

Panel	Description and default search
Notables in End State by Time	Displays a comparison graph for notables that are assigned versus the notables that have been resolved i.e. reached the configured end state over the duration of a specified time period. `get_notable_index` | eval `get_event_id_meval`, rule_id=event_id | `get_current_status` | `get_owner` | where owner != "unassigned" | timechart span=1d count(eval(status_end="true")) AS "In End State", count AS "Total Assigned"
Analyst Close Rate Over Time	Displays a comparison graph for assigned open versus assigned closed notables by an analyst over the duration of a specified time period. `get_notable_index` | eval `get_event_id_meval`, rule_id=event_id | `get_current_status` | `get_owner` | where owner != "unassigned" | stats count(eval(status_end = "true")) AS "Notables Closed", count(eval(status_end = "false")) AS "Notables Open" by owner_realname | rename owner_realname AS "Analyst"

Dispositions

Panel	Description and default search
Dispositions Over Time	Displays a distribution of the various dispositions that are assigned to notables over the duration of a specified time period. This visualization provides insight into the number of notables that are false positives versus notables that are true positives. For more information on assigning dispositions to notables, see Add dispositions to notables. `get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW default_disposition | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT disposition as new_disposition | eval disposition=if(isnotnull(new_disposition),new_disposition,default_disposition) | `get_notable_disposition` | timechart span=1d count by disposition_label
Sources Contributing to False Positive - Incorrect Analytic Logic	Displays a list of sources, which generated notables that have the disposition **False Positive - Incorrect Analytic Logic** over the duration of a specified time period. `get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW default_disposition | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT disposition as new_disposition | eval disposition=if(isnotnull(new_disposition),new_disposition,default_disposition) | `get_notable_disposition` | where disposition="disposition:3" | stats count by source | sort - count
Sources Contributing to False Positive - Inaccurate Data	Displays a list of sources, which generated notables that have the disposition **False Positive - Inaccurate Data** over the duration of a specified time period. `get_notable_index` | eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400 | lookup update=true correlationsearches_lookup _key as source OUTPUTNEW default_disposition | lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT disposition as new_disposition | eval disposition=if(isnotnull(new_disposition),new_disposition,default_disposition)

Panel	Description and default search
	``	`get_notable_disposition`	where disposition="disposition:4"	stats count by source	sort - count``
Sources Contributing to True Positive - Suspicious Activity	Displays a list of sources, which generated notables that have the disposition **True Positive - Suspicious** over the duration of a specified time period. ``` `get_notable_index`	eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400	lookup update=true correlationsearches_lookup _key as source OUTPUTNEW default_disposition	lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT disposition as new_disposition	eval disposition=if(isnotnull(new_disposition),new_disposition,default_disposition)	`get_notable_disposition`	where disposition="disposition:1"	stats count by source	sort - count ```
Sources Contributing to True Positive - Suspicious but Expected	Displays a list of sources, which generated notables that have the disposition **True Positives - Suspicious, but Expected** over the duration of a specified time period. ``` `get_notable_index`	eval `get_event_id_meval`, rule_id=event_id, temp_time=time()+86400	lookup update=true correlationsearches_lookup _key as source OUTPUTNEW default_disposition	lookup update=true event_time_field=temp_time incident_review_lookup rule_id OUTPUT disposition as new_disposition	eval disposition=if(isnotnull(new_disposition),new_disposition,default_disposition)	`get_notable_disposition`	where disposition="disposition:2"	stats count by source	sort - count ```

For key indicator panels and time chart visualizations on the SOC Operations dashboard, some arguments in the underlying SPL searches may be dynamically updated based on the time range selected on the dashboard UI.

Audit dashboards

Use the audit dashboards to validate the security and integrity of the data in Splunk Enterprise Security. Ensure that forwarders are functioning, that data has not been tampered with and is secured in transmission, and that analysts are reviewing the findings generated by detections.

Analyst queue audit

The **Analyst queue audit** dashboard provides an overview of activity on findings. The panels display how many findings 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.

Panel	Description
Review activity by reviewer	Displays the numbers of findings and investigations reviewed by each user. This panel is useful for determining which user is performing the security incident reviews and if the total number of reviews is changing over time. The drilldown opens a search with all activity by the selected reviewer.
Top reviewers	Displays the top users that review security incidents in the analyst queue. The panel includes details for each user, including the date they first reviewed a finding or investigation, the date they last performed a review, and the total number of findings and investigations reviewed. The drilldown opens a search with all activity by the selected reviewer.
Findings by status: Last 48	Displays the status, count, and urgency for all findings in the last 48 hours. This panel is useful for determining if the analyst queue users are keeping up with security incidents, or whether a backlog of unreviewed incidents is forming. The drilldown

Panel	Description
hours	opens the analyst queue on the **Mission Control** page and searches on the selected urgency and status over the lat 48 hours.
Findings by owner: Last 48 hours	Displays the owner, count, and urgency for all findings 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 analyst queue on the **Mission Control** page and searches on the selected urgency over the lat 48 hours.
Mean time to triage: Last 14 days	Displays the average time it took for a finding to be triaged after it was created over the last 14 days, split by the name of the finding. This panel is useful for determining how quickly analysts are triaging findings, or whether certain types of events take longer to triage than others. The drilldown opens the analyst queue on the **Mission Control** page and searches on the matching finding names over the last 14 days.
Mean time to closure: Last 60 days	Displays the average time it took for a finding to be closed after it was created over the last 60 days, split by the name of the finding. This panel is useful for determining how long it takes to close certain types of findings and investigations. The drilldown opens the analyst queue on the **Mission Control** page and searches on the matching finding names that have a status of closed from the last 60 days.
Recent review activity	Displays the 10 most recent changes on the analyst queue, such as triage actions. The drilldown opens a search with the selected rule ID.

To audit data from the analyst queue in Splunk Enterprise Security prior to version 3.2, you must perform an ad hoc search like the following example:

```
index=_audit sourcetype=incident_review | rex field=_raw "^(?<end_time>[^,]*),(?<rule
_id>[^,]*),(?<owner>[^,]*),(?<urgency>[^,]*),(?<status>[^,]*),(?<comment>[^,]*),(?<user>[^,]*),(?<rule_name>[^,]*)"
```

Data sources

The reports in the **Analyst queue audit** dashboard reference fields in the notable index and the incident review objects in a KVStore collection. See Notable index on the Splunk dev portal for more on the notable index.

Investigation overview

The **Investigation overview** dashboard gives insight into investigations, including monitoring open investigations, time to completion, and number of collaborators. You can filter by investigations where you're a collaborator or by investigations that exist on the system. you can use the **All** filter only if you have the "manage_all_investigations" capability.

In the descriptions that follow, there are references to "progress state" and "end state." Depending on your configuration, progress states can include statuses such as new, pending, and resolved. These states are considered unclosed because there is more work to do on the investigations. Also depending on your configuration, end states can include statuses such as closed, withdrawn, and fixed. These states are considered closed because there is no more work to do on the investigations.

Panel	Description
Unclosed investigations	Displays the number of investigations in a progress state during the time set in the time range picker. This includes investigations that were closed yesterday but are reopened today, as the only states that are included in this panel are progress states.
Investigations created	Displays the number of investigations created in the time set in the time range picker.
Investigations closed	Displays the number of investigations that have reached an end state during the time set in the time range picker. This does not include investigations that were closed yesterday but are reopened today, as the only states that are included in this panel are current end states.
Oldest unclosed investigations	Displays the age of the investigations in a progress state during the time set in the time range picker. The investigations are sorted by create time. This is the list of investigations that corresponds to the number shown in

Panel	Description
	the Unclosed Investigations panel.
Total time spent on investigations	Displays the investigations, which were created in the time set in the time range picker, that spent the most cumulative time in a progress state.
Time unclosed (in days)	Displays the average and median number of days that investigations spent in a progress state during the time set in the time range picker.
Time to complete (in days)	Displays the average and median number of days for investigations to reach an end state during the time set in the time range picker. This includes the total lifetime from when the investigation started, went through states of progress, and even if it reached an end state, then was opened and completed again.
Investigations unclosed per collaborator	Displays the number of investigations in a progress state for each collaborator during the time set in the time range picker, and the status of the investigations.
Investigations unclosed per creator	Displays the number of investigations in a progress state for each person who created an investigation during the time set in the time range picker.
Investigations unclosed per status	Displays the number of investigations in a progress state for each status during the time set in the time range picker.
Number of collaborators per unclosed investigation	Displays the number of people working on investigations in a progress state during the time set in the time range picker.
Longest inactive investigation (unclosed)	Displays the investigations in a progress state that haven't been modified during the time set in the time range picker. These are investigations that are underway, but are not being actively worked on.
Most often reopened	Displays the investigations that have been completed and reopened the most amount of times during the time set in the time range picker.
Investigations created per day	Displays the investigations created each day during the time set in the time range picker.

Suppression audit

The **Suppression audit** dashboard provides an overview of finding suppression activity. This dashboard shows how many events are being suppressed, and by whom, so that finding suppression can be audited and reported on.

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

Panel	Description
Suppressed events over time: Last 24 hours	Displays findings suppressed in the last 24 hours.
Suppression history over time: Last 30 days	Displays the history of suppressed findings.
Suppression management activity	Displays suppression management activity for the time period.
Expired suppressions	Displays expired suppressions.

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.

Panel	Description
Per-panel by reviewer	Displays the count of updates to per-panel filters by user.
Top users	Shows users, sparkline for trends, number of views, and first and last time viewed.
Recent filter activity	Activity by time, user, action, and filename.

Adaptive response action center

The **Adaptive response action center** dashboard provides an overview of the response actions initiated by adaptive response actions, including finding creation and risk scoring.

Panel	Description
Action invocations over time by name	Displays a time chart of the adaptive response actions triggered by name.
Top actions by name	Displays the top adaptive response actions by name.
Top actions by search	Displays the top adaptive response actions by search.
Recent response actions	Displays the most recent adaptive response actions.

Data sources

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

Threat intelligence audit

The **Threat intelligence audit** dashboard tracks and displays the current status of all threat and generic intelligence sources. As an analyst, you can review this dashboard to determine if threat and generic intelligence sources are current, and troubleshoot issues connecting to threat and generic intelligence sources.

Panel	Description
Intelligence downloads	Displays the status of all intelligence sources defined on the **Intelligence downloads** configuration page. Use the filters to sort by status or download location.
Intelligence audit events	Displays log events related to intelligence downloads configured on the **Intelligence downloads** configuration page and modular inputs configured on the **Threat intelligence manager** configuration page. Use the filters to sort and filter the events displayed.

If an intelligence download fails, a search automatically creates a system message. See Troubleshoot intelligence downloads in Splunk Enterprise Security.

Data sources

The reports in the **Threat intelligence audit** dashboard reference events in the `_internal` index and state information from the `/services/data/inputs/threatlist` REST endpoint.

Machine learning audit

The **Machine learning audit** dashboard displays information related to usage of the Machine Learning Toolkit (MLTK).

Panel	Description
Machine learning toolkit errors and failed fit and apply searches: Last 7 days	The `mlspl.log` log file itself doesn't contain a lot of details about specific models and when they ran as part of a search or a rule. As an analyst, you can review this chart to help determine where MLTK errors are happening. It shows all the MLTK errors over the last 7 days. If you click on the chart to drill-down into the details, you can see the audits of failed searches that contain the `fit` or `apply` commands, which can help you correlate errors with the actual searches that produced the issues.
Machine learning models	The list shows the names of the MLTK models. If you click on a model name to drill-down into the details, it opens a custom search that helps audit your model generating searches and the corresponding rules that apply them. See Audit searches using an MLTK Model.
List of model generating searches	The button shows all the MLTK model generating searches and their statuses.

ES configuration health

Use the **ES configuration health** dashboard to compare the latest installed version of Splunk Enterprise Security to prior releases and identify configuration anomalies. The dashboard does not report changes to add-ons (TA.) Select the previous version of Splunk Enterprise Security installed in your environment using the Previous ES Version filter.

Mode	Description
Unshipped	The unshipped setting compares the latest installed version of Splunk Enterprise Security with the content in the ES installation package. Any item that was not provided as part of the Splunk 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 setting ignores the **Previous ES version** filter.
Removed stanzas	The removed stanzas setting compares the latest installed version of Splunk 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.
Local overrides	The local overrides setting compares the installed version of Splunk Enterprise Security with the version that you select in the filter. A setting that conflicts with or overrides the installed version of Splunk 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.

Data model audit

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

Field Name Panel	Description
Top accelerations by size	Displays the accelerated data models sorted in descending order by MB on disk.
Top accelerations by run duration	Displays the accelerated data models sorted in descending order by the time spent on running acceleration tasks.
accelerations details	Displays a table of the accelerated data models with additional information.

Data model acceleration can be in progress and 100% complete at the same time. The process running and the status completing are not directly tied together.

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.

Filter by	Description	Action
Show only expected hosts	An expected host is a host defined in ES by the expected host field `is_expected` in the Asset table.	Drop-down, select to filter by
Host	Filter by the host field in the Asset table.	Text field. Wildcard with an asterisk (*)
Business Unit	Filter by the business unit `bunit` field in the Asset table.	Text field. Wildcard with an asterisk (*)
Category	Filter by the category field in the Asset table.	Drop-down, select to filter by

Panel	Description
Event count over time by host	Displays the number of events reported over the time period selected in the filter. The events are split by host.
Hosts by last report time	Displays a list of hosts, ordered by the last time they reported an event.
Splunkd process utilization	Displays the resource utilization of the forwarder's Splunk daemon `splunkd`.
Splunk service start mode	Displays the host names that are forwarding events, but are not configured to have `splunkd` start on boot.

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 run 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 run 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 might 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 Splunk Enterprise Security. The **View audit** dashboard allows tracking of views that are being accessed on a daily basis and helps to identify any errors triggered when users review dashboard panels.

Panel	Description
View activity over time	Displays the Splunk 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.
Expected view activity	Lists the views set up in the **Expected view** lookup. You want to review these views on a daily basis for your deployment. Select a dashboard to see details in the **Expected view scorecard** panel below. See Manage internal lookups in Splunk Enterprise Security.
Web service errors	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.

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*.

Managed lookups audit

The **Managed lookups audit** dashboard reports on managed lookups and collections such as services, data, transforms, KV Store lookups, and CSV lookups in Splunk Enterprise Security. The **Managed lookups audit** dashboard shows the growth of lookups over time and the markers for anomalous growth. You can use this to help determine if any managed lookups are growing too large for your particular environment's performance and need to be pruned.

Field	Description
Name	Displays the name of the Splunk Enterprise Security lookup. The drill-down takes you to all the contributing events for this particular lookup name from the audit_summary index.
Growth	

Field	Description
	Lists the lookup size over time as measured by a saved search that writes to the audit_summary index, running every 24 hours, displayed as a sparkline.
Count	Displays the estimated number of rows in the lookup file.
Size	Displays the size of the file in megabytes, sorted by the largest first.

Data protection

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

Panel	Description
Data integrity control by index	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 *Securing Splunk Enterprise*. If you use Splunk Cloud Platform, file a support case to request enablement of data integrity control.
Sensitive data	Displays the count of events with sensitive data. This panel requires turning on the **Personally Identifiable Information Detected** detection. For more information on how the IIN and the LUHN lookups are leveraged by detections and displayed on the **Data protection** dashboard, see Internal lookups that you can modify.

Predictive analytics dashboard

With Common Information Model Add-on 4.15.0 and later, the Predictive Analytics dashboard is removed. Machine Learning Toolkit functionality can be leveraged instead. MLTK is more robust for finding different varieties of anomalous events in your data than the | predict command used by the Predictive Analytics dashboard. See Machine Learning Toolkit Overview in Splunk Enterprise Security and see Release Notes in the Common Information Model Add-on Manual.

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.

Filter by	Description
Data Model	Specifies the data model for the search. Available data models are shown in the drop-down list.
Object	Specifies the object within the data model for the search. You must select a **Data Model** to apply an **Object**.
Function	Specifies the function within the object for the search. Functions specify the type of analysis to perform on the search results. For example, choose "`avg`" to analyze the average of search results. Choose "`dc`" to create a distinct count of the results.
Attribute	Specifies the constraint attributes within the object for the search. Attributes are constraints on the search results. For example, choose "`src`" to view results from sources. You must select an **Object** to apply an **Attribute**.

Filter by	Description
Time Range	Select the time range to represent.
Advanced	Access to the options for the predict command.

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 Platform, see predict options in the Splunk Cloud Platform *Search Reference*.

Dashboard Panels

Panel	Description
Prediction Over Time	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.
Outliers	The Outliers panel shows those results that fall outside of two standard deviations of the search results.

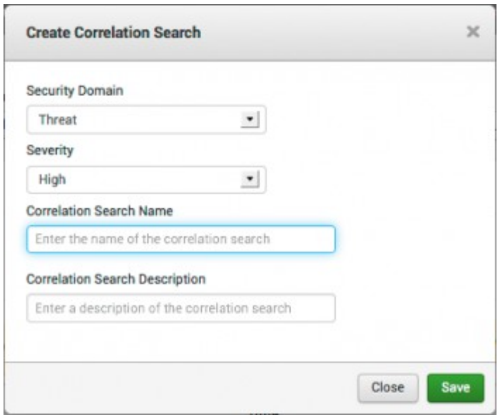
Data sources

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

Security Domain: Threat

Severity: High

Correlation Search Name: Enter the name of the correlation search

Correlation Search Description: Enter a description of the correlation search

To view and edit correlation searches, go to **Configure > Content > Content Management**. See Configure correlation searches in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Troubleshooting

This dashboard references data from various data models. Without the applicable data, the panels will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Access dashboards

The access protection domain monitors authentication attempts to network devices, endpoints, and applications within the organization. Access protection is useful for detecting malicious authentication attempts, as well as identifying systems users have accessed in either an authorized or unauthorized manner.

Access center dashboard

Access center provides a summary of all authentication events. This summary is useful for identifying security incidents involving authentication attempts such as brute-force attacks or use of clear text passwords, or for identifying authentications to certain systems outside of work hours.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description	Action
Action	Filter based on authentication success or failure.	Drop-down: select to filter by
App	Filter based on authentication application.	Drop-down: select to filter by
Business unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host or user belongs. See Format an asset or identity list as a lookup in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by
Special access	Restricts the view to events related to privileged access. See Administrative Identities in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by
Time range	Select the time range to view.	Drop-down: select to filter by

Dashboard panels

Panel	Description
Access over time by action	Displays the count of authentication events over time by action.
Access over time by app	Displays the count of authentication events over time by app. For example, "win:local" refers to the local authentication performed on a Windows system and "win:remote" refers to remote API access.
Top access by source	Displays a table of highest access counts by source. This table is useful for detecting brute force attacks, since aggressive authentication attempts display a disproportionate number of auth requests.

Panel	Description
Top access by unique users	Displays a table of the sources generating the highest number of unique user authentication events.

Access tracker dashboard

The **Access tracker** dashboard gives an overview of account statuses. Use it to track newly active or inactive accounts, as well as those that have been inactive for a period of time but recently became active. Discover accounts that are not properly de-provisioned or inactivated when a person leaves the organization.

As inactive accounts or improperly active accounts are vulnerable to attackers, it is a good idea to check this dashboard on a regular basis. You can also use this dashboard during an investigation to identify suspicious accounts and closely examine user access activity.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description	Action
Business unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host or user belongs. See Format an asset or identity list as a lookup in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by

Dashboard panels

Panel	Description
First time access: Last 7 days	Displays new account access by user and destination.
Inactive account usage: Last 90 days	Displays accounts that were inactive for a period of time, but that have shown recent activity.
Completely inactive accounts: Last 90 days	Displays accounts that have shown no activity. Use this panel to identify accounts that should be suspended or removed. If the organization has a policy that requires a password change after a specified interval, then accounts that have shown no activity for more than that interval are known to be inactive. This panel also indicates the effectiveness of the enterprise's policy for closing or de-provisioning accounts. If a large number of accounts display here, the process might need to be reviewed.
Account usage for expired identities: Last 7 days	Displays activity for accounts that are suspended within the specified time frame. Use this panel to verify that accounts that should be inactive are not in use.

Access search dashboard

Use the **Access search** dashboard to find specific authentication events. The dashboard is used in ad-hoc searching of authentication data, but is also the primary destination for drilldown searches used in the Access Anomalies dashboard panels.

The **Access search** page displays no results unless it is opened in response to a drilldown action, or you set a filter or time range and select **Submit**.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description	Action
Action	Filter based on authentication success or failure.	Drop-down: select to filter by
App	Filter based on authentication application.	Drop-down: select to filter by
Source	A string that the source field `src` must match.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	A string that the destination field `dest` must match.	Text field. Empty by default. Wildcard strings with an asterisk (*)
User	A string that the user field `user` must match.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time range	Select the time range to view.	Drop-down: select to filter by

Account management dashboard

The **Account management** dashboard shows changes to user accounts, such as account lockouts, newly created accounts, disabled accounts, and password resets. Use this dashboard to verify that accounts are being correctly administered and account administration privileges are being properly restricted. A sudden increase in the number of accounts created, modified, or deleted can indicate malicious behavior or a rogue system. A high number of account lockouts could indicate an attack.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description	Action
Business unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host or user belongs. See Format an asset or identity list as a lookup in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by
Special accounts	Restricts the view to events related to privileged access. See Administrative identities in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by
Time range	Select the time range to view.	Drop-down: select to filter by

Dashboard panels

Panel	Description
Account management over time	Displays all account management events over time.
Account lockouts	Displays all account lockouts, including the number of authentication attempts per account.

Panel	Description
Account management by source user	Tracks the total account management activity by source user, and shows the source users with the most account management events. The source user is the user that performed the account management event, rather than the user that was affected by the event. For example, if user "Friday.Adams" creates an account "Martha.Washington", then "Friday.Adams" is the source user. This panel helps identify accounts that should not be managing other accounts and shows spikes in account management events, such as the deletion of a large number of accounts.
Top account management events	Shows the most frequent management events in the specified time period.

Default account activity dashboard

The **Default account activity** dashboard shows activity on "default accounts", or accounts activated by default on various systems such as network infrastructure devices, databases, and applications. Default accounts have well-known passwords and are often not deactivated properly when a system is deployed.

Many security policies require that default accounts be deactivated. In some cases, you may need to monitor or investigate authorized use of a default account. It is important to confirm that the passwords on default accounts are changed before use. Abnormal or deviant user behavior from a default account can indicate a security threat or policy violation. Use this dashboard to ensure that security policies regarding default accounts are properly followed.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description	Action
Business unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host or user belongs. See Format an asset or identity list as a lookup in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.	Drop-down: select to filter by
Time range	Select the time range to view.	Drop-down: select to filter by

Dashboard panels

Panel	Description
Default account usage over time by app	Shows default account activity on all systems and applications during the selected time frame, split by application. For example, sshd or ftpd. Application accounts are shown by the number of successful login attempts and when the last attempt was made. Use this chart to identify spikes in default account login activity by application, which may indicate a security incident, as well as to determine whether default account use is common (for example, a daily event) or rare for a certain application.
Default accounts in use	Shows all default user accounts with a high number of login attempts on different hosts, including the last attempt made. Abnormal default user account activity that could indicate a security threat. Also helps ensure that default account behavior matches the security policy.
Default local accounts	Lists all default accounts that are active on enterprise systems, including accounts "at rest". Any available default accounts are listed, regardless of whether the account is actually in use. Only accounts detected on a local system, for example by examining the users list on a host, are included in this list.

Troubleshooting access dashboards

This dashboard references data from various data models. Without the applicable data, the dashboards will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Endpoint dashboards

The Endpoint Protection domain provides insight into malware events including viruses, worms, spyware, attack tools, adware, and PUPs (Potentially Unwanted Programs), as well as your endpoint protection deployment.

Malware Center dashboard

Malware Center is useful to identify possible malware outbreaks in your environment. It displays the status of malware events in your environment, and how that status changes over time based on data gathered by Splunk.

Search malware events directly using Malware Search, or click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. Configure new data inputs through the Settings menu.

You can use the filters to refine which events are shown.

Filter by	Description	Action
Action	All, allowed, blocked, or deferred.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Malware Activity Over Time By Action	Shows all malware detected over the specified time period, split by action (allowed, blocked, deferred). Use this chart to detect whether too many malware infections are allowed.
Malware Activity Over Time By Signature	Shows all malware detected over the specified time period, split by signature. Example signatures are Mal/Packer, LeakTest, EICAR-AV-Test, TROJ_JAVA.BY. Use this chart to detect which infections are dominant in your environment.
Top Infections	Shows a bar chart of the top infections in your environment, split by signature. This panel helps identify outbreaks related to a specific type of malware.
New Malware - Last 30 Days	Shows new malware detected on the network over the last 30 days. For each malware signature identified, the date and time it was first detected and the total number of infections are shown. First-time infections are the most likely to cause outbreaks.

Malware Search dashboard

The Malware Search dashboard assists in searching malware-related events based on the criteria defined by the search filters. The dashboard is used in ad-hoc searching of malware data, but is also the primary destination for drilldown searches used in the Malware Center dashboard panels.

The Malware Search dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
Action	Filter by the action taken on the malware (allowed, blocked, or deferred).	Drop-down: select to filter by
Signature	Filter on malware with matching signatures.	Text field. Empty by default. Wildcard strings with an asterisk (*)
File	Filter on file name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter on endpoint systems.	Text field. Empty by default. Wildcard strings with an asterisk (*)
User	Filter based on username.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Malware Operations dashboard

The Malware Operations dashboard tracks the status of endpoint protection products deployed in your environment. Use this dashboard to see the overall health of systems and identify systems that need updates or modifications made to their endpoint protection software. This dashboard can also be used to see how the endpoint protection infrastructure is being administered.

You can click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. Configure new data inputs through the Settings menu.

Use the filters to refine which events are shown.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Clients by Product Version	Shows a bar chart of the number of clients with a certain version of the endpoint protection product installed.

Panel	Description
Clients by Signature Version	Shows a bar chart of the number of clients with a certain signature version.
Repeat Infections	Shows repeated malware infections. Sort by signature, destination, action, or number of days.
Oldest Infections	Shows the oldest malware infections in your environment. Sort by date that the infection was detected (first or last time), the signature, destination host (affected system), or days the infection has been active.

System Center dashboard

The System Center dashboard shows information related to endpoints beyond the information reported by deployed anti-virus or host-based IDS systems. It reports endpoint statistics and information gathered by the Splunk platform. System configuration and performance metrics for hosts, such as memory usage, CPU usage, or disk usage, can be displayed on this dashboard.

Click chart elements or table rows to display raw events. See Drill down to raw events for more information on this feature. Configure new data inputs through the Settings menu.

Use the filters to refine which events are shown.

Filter by	Description	Action
Destination	Host name of the affected endpoint system.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Operating Systems	Shows the operating systems deployed on the network. Use this chart to detect operating systems that should not be present in your environment.
Top-Average CPU Load by System	Shows the systems on the network with the top average CPU load.
Services by System Count	Shows services ordered by the number of systems on which they are present.
Ports By System Count	Shows the transport method (e.g., tcp) and destination ports, ordered by the number of systems.

Note: If incorrect or missing data is showing up in the System Center dashboard, be sure that the technology add-ons that supply the data for this dashboard are installed on the full forwarders in the deployment. Technology add-ons containing knowledge needed for parsing of data need to be installed on the full forwarders.

Time Center dashboard

The Time Center dashboard helps ensure data integrity by identifying hosts that are not correctly synchronizing their clocks.

Splunk will create an alert when it discovers a system with time out of sync. When you receive an alert, you can drill down to the raw data and investigate further by clicking any of the chart elements or table rows on the dashboard. See Drill down to raw events for more information on this feature.

Use the filters to refine which events are shown.

Filter by	Description	Action
Show only systems that should timesync	Select true to filter by systems categorized as `should_timesync=true` in the Asset table or false to filter by systems categorized as `should_timesync=false` in the Asset table. See Configure the new asset or identity list in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for more about asset configuration.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Time Synchronization Failures	A list of systems where time synchronization has failed.
Systems Not Time Synching	Shows a list of systems that have not synchronized their clocks in the specified time frame.
Indexing Time Delay	Shows hosts with significant discrepancies between the timestamp the host places on the event and the time that the event appears in the Splunk platform. For example, if the timestamp on an event is later than the time that Splunk indexes the event, the host is timestamping events as future events. A large difference (on the order of hours) indicates improper time zone recognition.
Time Service Start Mode Anomalies	Shows hosts that have a time service start mode, such as `Manual` that others do not.

Endpoint Changes dashboard

The Endpoint Changes dashboard uses the Splunk change monitoring system, which detects file-system and registry changes, to illustrate changes and highlight trends in the endpoints in your environment. For example, Endpoint Changes can help discover and identify a sudden increase in changes that may be indicative of a security incident.

You can click chart elements or table rows on this dashboard to display raw events. See Drill down to raw events for more information on this feature.

Use the filters to refine which events are shown.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

Filter by	Description	Action

The following table describes the panels for this dashboard.

Panel	Description
Endpoint Changes by Action	Summarizes changes over time. A substantial increase in changes may indicate the presence of an incident that is causing changes on the endpoints such as a virus or worm.
Endpoint Changes by Type	Summarizes the type of changes observed on the endpoints, such as file or registry changes.
Changes by System	Summarizes changes by system
Recent Endpoint Changes	Shows the most recent endpoint changes observed.

Update Center dashboard

The Update Center dashboard provides additional insight into systems by showing systems that are not updated. It is a good idea to look at this dashboard on a monthly basis to ensure systems are updating properly.

You can click any of the chart elements or table rows on the dashboard to see raw events. See Drill down to raw events for more information on this feature.

Use the filters to refine which events are shown.

Filter by	Description	Action
Show only systems that should update	Select true to filter by systems categorized as `should_update=true` in the Asset table or false to filter by systems categorized as `should_update=false` in the Asset table. See Configure the new asset or identity list in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for more about asset configuration.	Drop-down: select to filter by
Destination	Host name of the system.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the malware belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

The following table describes the panels for this dashboard.

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Top Systems Needing Updates	A bar chart of the top systems that need updates installed.
Top Updates Needed	A bar chart of the top updates needed across the environment, sorted by signature, such as the KB number.
Systems Not Updating - Greater Than 30 Days	Systems that have not been updated, sorted by the number of days for which they have not been updated.
Update Service Start Mode Anomalies	Shows all systems where the update startup task or service is disabled. Administrators sometimes disable automatic updates to expedite a restart and can forget to re-enable the process.

Panel	Description

Update Search dashboard

The Update Search dashboard shows patches and updates by package and/or device. This dashboard helps identify which devices have a specific patch installed. This is useful when, for example, there is a problem caused by a patch and you need to determine exactly which systems have that patch installed.

The Update Search dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
Show only systems that should update	Select true to filter by systems categorized as `should_update=true` in the Asset table or false to filter by systems categorized as `should_update=false` in the Asset table. See Configure the new asset or identity list in Splunk Enterprise Security in *Administer Splunk Enterprise Security* for more about asset configuration.	Drop-down: select to filter by
Update Status	Filter by the status of the update on a machine.	Drop-down: select to filter by
Signature	Filter by the signature, for example the KB number, of a particular update.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter on affected endpoint systems.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Asset and identity dashboards

The Identity domain dashboards provide information about the assets and identities defined in Splunk Enterprise Security. See Add asset and identity data to Splunk Enterprise Security in *Administer Splunk Enterprise Security* for instructions on defining assets and identities.

Asset center dashboard

Use the **Asset Center** dashboard to review and search for objects in the asset data added to Enterprise Security. The asset data represents a list of hosts, IP addresses, and subnets within the organization, along with information about each asset. The asset list correlates asset properties to indexed events, providing context such as asset location and the priority level of an asset.

Dashboard filters

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

Filter by	Description
Asset	A known or unknown asset
Priority	Filter by the Priority field in the Asset table.
Business Unit	A group or department classification for the asset.

Filter by	Description
Category	Filter by the Category field in the Asset table.
Owner	Filter by the Owner field in the Asset table.
Time Range	Select the time range to represent.

Dashboard Panels

Panel	Description
Assets by Priority	Displays the number of assets by priority level. The drilldown opens a search with the selected priority level.
Assets by Business Unit	Displays the relative amount of assets by business unit. The drilldown opens a search with the selected business unit.
Assets by Category	Displays the relative amount of assets by category. The drilldown opens a search with the selected category.
Asset Information	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.

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 dashboard

Use the **Identity Center** dashboard to review and search for objects in the identity data added to Enterprise Security. Identity data represents a list of account names, legal names, nicknames, and alternate names, along with other associated information about each identity. The identity data is used to correlate user information to indexed events, providing additional context.

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.

Filter by	Description
Username	A known or unknown user
Priority	Filter by the Priority field in the Identities table
Business Unit	A group or department classification for the identity.
Category	Filter by the Category field in the Identities table.
Watchlisted Identities Only	Filter by the identities tagged as "watchlist" in the Identities table.
Time Range	Select the time range to represent.

Dashboard Panels

Panel	Description
Identities by Priority	Displays the count of Identities by priority level. The drilldown opens a search with the selected priority level.
Identities by Business Unit	Displays the relative number of Identities by business unit. The drilldown opens a search with the selected business unit.
Identities by Category	Displays the relative number of Identities by category. The drilldown opens a search with the selected category.
Identity Information	Shows all assets that match the current dashboard filters. The drilldown opens the Identity Investigator dashboard if you select the `identity` field. Any other field opens a search with the selected field.

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.

Session Center dashboard

The **Session Center** dashboard provides an overview of network sessions. Network sessions are used to correlate network activity to a user using session data provided by DHCP or VPN servers. Use the Session Center to review the session logs and identify the user or machine associated with an IP address used during a session. You can review network session information from the Network Sessions data model, or user and device association data from Splunk UBA.

Dashboard Panels

Network Sessions tab:

Panel	Description
Sessions Over Time	Displays the total count of network sessions over time. The drilldown opens a search with the selected session and time range.
Session Details	Displays the top 1000 network sessions that have been most recently opened, based on the session start time. The drilldown opens a search with the selected session details.

User Behavior Analytics tab:

Panel	Description
Sessions of Associated Entities	Based on the search filter, displays the sessions of users and devices associated with a device that you search, or devices associated with a user that you search. Hover over a session to learn more about the session activity.
Session Details	Shows the entity ID from Splunk UBA, the name of the entity, the type of entity, the start and end times of the session, and event data from Splunk UBA. Expand a row to view more details.

For more about viewing data from Splunk UBA, see Viewing data from Splunk UBA in Enterprise Security.

Troubleshooting Identity dashboards

The dashboards reference data from various data models. Without the applicable data, the panels will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Asset and identity investigator dashboards

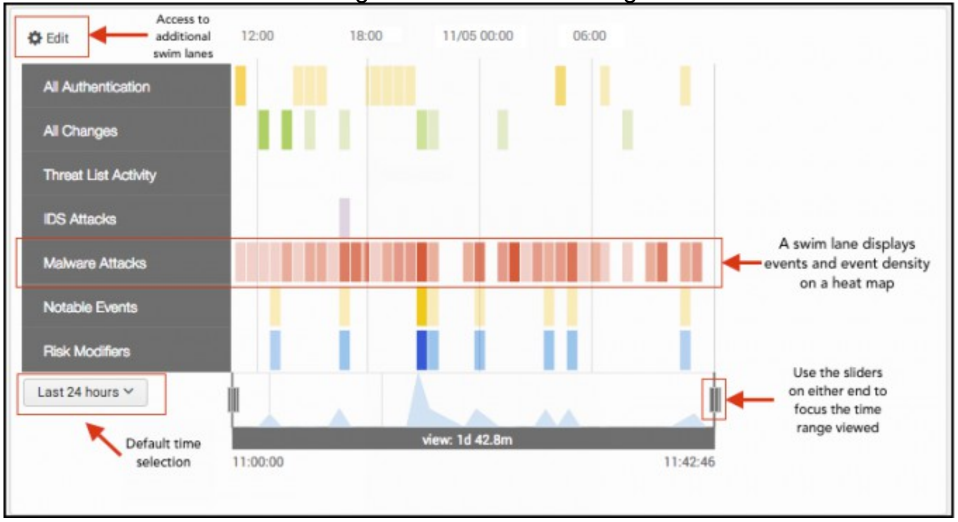
The Asset and Identity Investigator dashboards visually aggregate security-related events over time using category-defined swim lanes. Each swim lane represents an event category, such as authentication, malware, or notable events. The swim lane uses a heat map to display periods of high and low activity. The color saturation on the swim lane corresponds to the event density for a given time. For example, high activity periods display a darker color. An analyst can visually link activity across the event categories and form a complete view of a host or user's interactions in the environment.

Asset Investigator

The Asset Investigator dashboard displays information about known or unknown assets across a pre-defined set of event categories, such as malware and notable events.

Use the Asset Investigator dashboard

You can use the Asset Investigator dashboard to triage an asset's interactions with the environment.



The dashboard contains multiple event categories, with each one represented by its own swim lane. Each event category contains relevant events that correspond to a data model. For example, the Malware Attacks swim lane displays events from an anti-virus management or other malware data source, limited to the asset searched. Multiple swim lanes are displayed at once to make it easier for you to track the actions of an asset across event categories.

Additionally, you can use this dashboard for ad hoc searching.

1. Browse to **Security Intelligence > User Intelligence > Asset Investigator**.
2. Type the host name or IP address in the search bar with an optional wildcard.
3. Set a time range and click **Search**.

A workflow for asset investigation

To initiate the asset investigation workflow, perform a workflow action from any dashboard that displays events with network source or destination addresses.

1. Look at the asset description at the top of the dashboard to confirm that you are viewing the asset you would like to investigate. All events displayed in the swim lanes are limited to the selected asset.
2. Use the time range picker to narrow down the general time range you are interested in. Use the time sliders to isolate periods of interesting events or peak event counts.
3. Add or change the swim lanes using the edit menu. For example, to display data collected on an asset from packet analysis tools, change the selected collection from Default to Protocol Intelligence, which represents packet capture data. See Edit the swim lanes.
4. Review individual and grouped events. After selecting an event, you can use the Event Panel to examine common fields represented in the individual or grouped events.
5. If there is an event or pattern that you want to share or investigate further, you can do this using the Event Panel.
    1. Click **Go to Search** to view a drilldown of the selected events.
    2. Click **Share** for a shortened link to the current view.
    3. Click **Create Notable Event** to open a dialog box to create an ad-hoc notable event. See Manually create a notable event in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Data sources

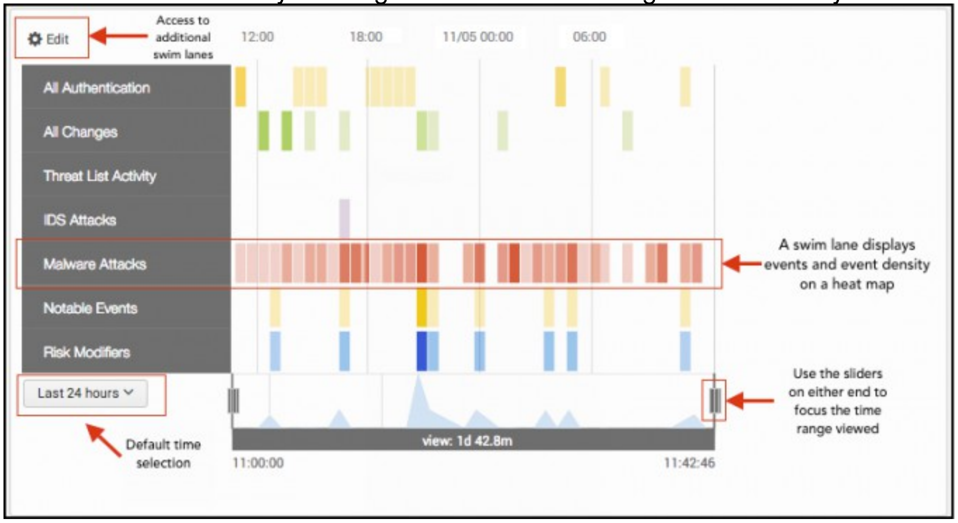
The event categories in the Asset Investigator dashboard display events from a number of data models containing an asset or host field. In any given time selection, a selected asset may not have data to display in one or more event categories. When a data model search returns no matching events, the swim lane displays "Search returned no results." See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Identity Investigator

The Identity Investigator dashboard displays information about known or unknown user identities across a predefined set of event categories, such as change analysis or malware.

Use the Identity Investigator dashboard

You can use the Identity Investigator dashboard to triage a user identity's interactions with the environment.



The dashboard contains multiple event categories, with each one represented by its own swim lane. Each event category contains relevant events that correspond to a data model. For example, the Malware Attacks swim lane displays events from an anti-virus management or other malware data source, limited to the user identity or credential searched. Multiple swim lanes are displayed at once to make it easier for you to track the actions of a user across event categories.

Additionally, you can use this dashboard for ad-hoc searching.

1. Browse to **Security Intelligence > User Intelligence > Identity Investigator**.
2. Type a user credential in the search bar. Optionally, include a wildcard.
3. Set a time range and click Search.

A workflow for identity investigation

The identity investigation workflow is initiated through a workflow action from any dashboard that displays events with network source or destination address.

1. Look at the identity description at the top of the dashboard to confirm that you are viewing the identity you would like to investigate. All events displayed in the swim lanes are limited to the selected identity.
2. Use the time range picker to narrow down the general time range you are interested in. Use the time sliders to isolate periods of interesting events or peak event counts.
3. Add or change swim lanes by using the edit menu. For example, to display identity information collected for user activity monitoring, change the selected collection from Default to User Activity. See Edit the swim lanes.
4. Review individual and grouped events. After selecting an event, you can use the Event Panel to examine common fields represented in the individual or grouped events.
5. If there is an event or pattern that you would like to share or investigate further, you can do this using the Event Panel.
    1. Click **Go to Search** to view a drilldown of the selected events.
    2. Click **Share** for a shortened link to the current view.
    3. Click **Create Notable Event** to open a dialog box to create an ad-hoc notable event. See Manually create a notable event in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Data sources

The event categories in the Identity Investigator dashboard display events from a number of data models containing an identity or a user field. In any given time selection, an identity may not display data in one or more event categories. When a data model search returns no matching events, the swim lane displays "Search returned no results." See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Edit the swim lanes

You can add or remove swim lanes from the Entity Investigator dashboards by opening the Edit Lanes customization menu. The Entity Investigator dashboards support the addition of custom swim lanes bundled with add-ons or created using ES Content Management. For more information, see Managing content in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

1. Choose **Edit** at the top of the dashboard.
2. Select the radio button for a Custom collection.
3. Select a checkbox to add a swim lane to the dashboard.
4. Deselect a checkbox to remove a swim lane from the dashboard.
5. Click the color next to a swim lane to change it.
6. Click the **X** to close the edit menu.

The order of swim lanes can be changed on the dashboard and does not require the Edit Lanes menu.

1. Select a swim lane category.
2. Drag and drop the swim lane where you would like it.

The Asset Investigator has additional, optional swim lanes in the collection Protocol intelligence to display data collected about an asset using packet analysis tools. The Identity Investigator has additional, optional swim lanes in the collection User Activity to display data collected about an identity for user activity monitoring.

Swimlane Name	Asset or Identity dashboard	Description
All Authentication	Both	Matches events in the Authentication data model.
All Changes	Both	Matches events in the Change Analysis data model.
Threat List Activity	Both	Matches events in the Threat Lists data model.
IDS Attacks	Both	Matches events in the Intrusion Detection data model.
Malware Attacks	Both	Matches events in the Malware data model.
Notable Events	Both	Matches events in the Notable index.
Risk Modifiers	Both	Matches events in the Risk Analysis data model.
DNS Errors	Asset only	Matches events in the Network Resolution DNS data model.
Cloud Emails	Asset only	Matches events in the Email data model.
SSL Expired Certs	Asset only	Matches events in the Certificates data model.
HTTP Errors	Asset only	Matches events in the Web data model.
Non-corporate Emails	Identity only	Matches events in the Email data model.
Non-corporate Web Uploads	Identity only	Matches events in the Web data model.
Remote Access	Identity only	Matches events in the Authentication data model.
Ticket Activity	Identity only	Matches events in the Ticket Management data model.
Watchlisted Sites	Identity only	Matches events in the Web data model.

Troubleshooting Asset and Identity Investigator dashboards

The Asset and Identity Investigator dashboards display events from the data model named in each swim lane. When a data model search returns no matching events, the swim lane displays "Search returned no results." See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

User activity monitoring

User Activity

The **User Activity** dashboard displays panels representing common risk-generating user activities such as suspicious website activity. For more information about risk scoring, see How Splunk Enterprise Security assigns risk scores.

Dashboard filters

You can use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description
User	A known or unknown identity
Business Unit	A group or department classification for the identity.
Watchlisted Users	Designates a monitored identity.
Time Range	Select the time range to represent.

Dashboard Panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Users By Risk Scores	Displays the top 100 highest risk users. As an insider threat can represent subtle and indirect changes in behavior, this panels assists an analyst in focusing on the riskiest users in the organization. The drilldown opens the Identity Investigator dashboard and searches on the selected user.
Non-corporate Web Uploads	Displays high volume upload and download activity by user. An irregular pattern of upload or download activity can be an indicator of data exfiltration. The drilldown opens the Identity Investigator dashboard and searches on the selected user.
Non-corporate Email Activity	Displays the top 100 users performing high volume email activity to non-corporate domains. A pattern of large or high volume email activity can be an indicator of data exfiltration. The drilldown opens the Identity Investigator dashboard and searches on the selected user.
Watchlisted Site Activity	Displays web access by user. Accessing specific categories of web sites while using workplace resources and assets can be an indicator of insider threat activity. The drilldown opens the Identity Investigator dashboard and searches on the selected user.
Remote Access	Displays remote access authentication by user. A user performing risky web or email activity while using remote access services can be an indicator of data exfiltration, or exploited credentials. The drilldown opens the Identity Investigator dashboard and searches on the selected user.
Ticket Activity	Displays ticketing activity by user. A user performing risky web or email activity while filing tickets to provide additional services or internal access can be an indicator of data exfiltration, or exploited credentials. The drilldown opens the Identity Investigator dashboard and searches on the selected user.

Data sources

The reports in the **User Activity** dashboard reference data fields in multiple sources. Relevant data sources include proxy servers, gateways and firewalls, or other sources that reference a distinct user. In order for the dashboards to populate, new lookup content and fields in the identities list must be added. For a list of additional data sources, see Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Access Anomalies

The **Access Anomalies** dashboard displays concurrent authentication attempts from different IP addresses and improbable travel anomalies using internal user credentials and location-relevant data.

Dashboard filters

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

Filter by	Description
Action	A successful or failed authentication attempt.
App	The application field in the authentication data model.
User	A known or unknown identity.
Business Unit	A group or department classification for the identity.
Time Range	Select the time range to represent.

Dashboard Panels

Panel	Description
Geographically Improbable Accesses	Displays users that initiated multiple authentication attempts separated by an improbable time and distance. Authenticating from two geographically distant locations in a time frame lower than typical transportation methods provide can be an indicator of exploited credentials. The drilldown opens the Access Search dashboard and searches on the selected user.
Concurrent Application Accesses	Displays users that initiated multiple authentication attempts from unique IP addresses within a short time span. This pattern of authentication can be an indicator of shared or stolen credentials. The drilldown redirects the page to the Access Search dashboard and searches on the selected user.

Data sources

The reports in the **Access Anomalies** dashboard reference data fields in the Authentication data model. Relevant data sources include proxy servers, gateways and firewalls, or other sources that reference a distinct user. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Troubleshooting

This dashboard references data from various data models. Without the applicable data, the dashboards will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Risk analysis

The **Risk analysis** dashboard displays recent changes to risk scores and entities that have the highest risk scores. As an analyst, you can use this dashboard to assess relative changes in risk scores and examine the events that contribute to an entity's risk score.

You can use the **Risk analysis** dashboard to review changes to an entity's risk score, determine the source of a risk increase, and decide if additional action is needed.

Risk analysis dashboard filters

Use any of the available filters on the **Risk analysis** dashboard to search and filter the results. A filter is applied to all panels in the dashboard, but not the key security indicators.

Filter by	Description

Index	Filter by the risk index or test index.
Source	Filter by the detection that has risk modifiers.
Entity type	Filter by the type of entity such as **system**, **user**, **hash_values**, **network_artifacts**, **host_artifacts**, **tools**, **other**.
Entity	Select an entity type and enter a string to filter by entity. Entity type defaults to **All**.
Time	Filter by time window such as **Relative time**, **Real time**, **Date Range**, **Date & Time Range**, and so on.

The **Entity** filter works by performing a reverse lookup against the asset and identity tables to find all fields that have been associated with the specified **Entity**. All associated entities found by the reverse lookup then display on the dashboard. For example, if you select an entity type of **system** and enter an **Entity** of 10.10.1.100, the reverse lookup against the assets table could return a MAC address. The **Risk analysis** dashboard updates to display any risk score applied to the 10.10.1.100 address and a MAC address. If no match to another entity was found in the asset table, only the IP address matches from the risk analysis data model will be displayed.

Risk analysis dashboard panels

The risk analysis dashboard offers additional views to help analyze risk scoring changes and what caused the changes. Use the filters to refine the view to a specific entity or group of entities. Use the drilldown to explore the data as events.

Panel	Description
Key indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard.
Risk score by entity	Displays the entities with the highest risk score. The drilldown opens a search with the selected entity and scoped to the selected time frame.
Most active sources	Displays the detections that contribute the highest amount of risk to any entity. The drilldown opens a search with the selected source.
Risk modifiers over time	Displays the changes made to risk modifiers over time. Use the dashboard filters to scope the view to a specific entity or group of entities. The drilldown opens a search on all events in the risk data model scoped to the selected time frame.
Risk score by annotations	Pie chart displays the risk score distribution and classifies them by annotations.
Risk modifiers by annotations	Displays the changes to risk modifiers by annotations.
Risk modifiers by threat object	Displays the risk modifiers by threat objects.

Use behavioral analytics detections on test index

Using the risk analysis dashboard, you can specify whether the panels use test or risk index, not the detections.

Specifying the test index gives you the option of vetting the data that is best suited for surfacing threats effectively instead of experimenting on the production data in the risk index.

Follow these steps to use the test index for your detections:

1. In Splunk Enterprise Security, select **Analytics** and then **Security intelligence**.
2. Select **Risk analysis**.
3. In the **Index** field, select **Risk** or **Test**.

Review active detections

Using the risk analysis dashboard, you can identify the total number of detections that are turned on and point to the risk index. You can also review the total number of detections that are available in Splunk Enterprise Security as opposed to the number of detections that are pointed at the risk index. You can also turn on or turn off detections or point them to the test index as required.

Follow these steps to review the detections on the risk analysis dashboard:

1. In Splunk Enterprise Security, select **Analytics** and then **Security intelligence**.
2. Select **Risk analysis**.
3. Go to the key indicator panel **BA DETECTIONS IN THE RISK INDEX** that displays the number of detections being used versus the number of available detections. For example: 24/74 that indicates 24 detections are being used out of 74 available detections.
4. Select the key indicator, such as 24/74, which opens a new tab that displays the entire list of available detections and the detections that are already turned on for the risk index.
5. Select **Enable to the risk index** to turn on a detection on the risk index.
6. Select **Disable** to turn off the detection.
7. Select **Enable on the test index** to turn on a detection on the test index.

For more information on activating behavioral analytics service on Splunk Enterprise Security, see Enable behavioral analytics service on Splunk Enterprise Security.

Review detailed information on risk annotations in context

On the risk analysis dashboard, you can review detailed information on risk annotations to get additional context that makes it easier to identify the root problem and detect security threats during the phases of a cybersecurity investigation.

Follow these steps to review detailed information on risk annotations in the context of an investigation:

1. In Splunk Enterprise Security, select **Analytics** and then **Security intelligence**.
2. Select **Risk analysis**.
3. Go to the table on **Risk modifiers by annotations**.
4. Select an annotation such as T1059 to display all the information on that MITRE tactic or technique.

For more information on how risk annotations provide additional context during an investigation, see How risk annotations provide additional context in Splunk Enterprise Security.

View the Risk Event Timeline visualization

On the risk analysis dashboard, you can access the Risk Event Timeline visualization for entities to review historical events easily during an investigation.

Follow these steps to access the Risk Event Timeline visualization from the risk analysis dashboard:

1. In Splunk Enterprise Security, select **Analytics** and then **Security intelligence**.
2. Select **Risk analysis**.
3. Go to the panel **Risk score by entity**.
4. Select the entity, which opens a new dialog box that displays the Risk Event Timeline visualization.

For more information on how the Risk Event Timeline visualization works in Splunk Enterprise Security, see How the Risk event Timeline visualization works in Splunk Enterprise Security.

Access threat object activity

From the risk analysis dashboard, you can navigate to activities related to specific threat objects and select a time range to isolate threats during an investigation.

Follow these steps to navigate to the **Threat findings** dashboard from the risk analysis dashboard:

1. In Splunk Enterprise Security, select **Analytics** and then **Security intelligence**.
2. Select **Risk analysis**.
3. Go to the panel **Risk modifiers by threat object** .
4. Select any threat object. This displays the **Threat findings** dashboard, which is populated with information on that specific threat object.
5. Specify a time range on the threat findings dashboard if required. By default, the time range is set to when the investigation was initially opened and matches the time range used for the risk analysis dashboard.

Network dashboards

The Network Protection domain provides insight into the network and network-based devices, including routers, switches, firewalls, and IDS devices. This domain aggregates all the traffic on the network, including overall volume, specific patterns of traffic, what devices or users are generating traffic, and per-port traffic. It also shows results from the vulnerability scanners on the network.

Traffic Center dashboard

The **Traffic Center** dashboard profiles overall network traffic, helps detect trends in type and changes in volume of traffic, and helps to isolate the cause (for example, a particular device or source) of those changes. This helps determine when a traffic increase is a security issue and when it is due to an unrelated problem with a server or other device on the network.

You can use the filters to limit which items are shown. Configure new data inputs through the **Settings** menu, or search for particular network intrusion events directly through **Incident Review**.

Filter by	Description	Action
Action	Filter based on firewall rule actions.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.

Panel	Description
Traffic Over Time by Action	Displays network traffic by action. The drilldown redirects the page to the Traffic Search dashboard and searches on the selected action and time range.
Traffic Over Time By Protocol	Displays the number of events per day for a specified protocol. The drilldown redirects the page to the Traffic Search dashboard and searches on the selected protocol and time range.
Top Sources	Displays the top sources of total traffic volume over the given time frame with a sparkline representing peak event matches. The drilldown opens the Traffic Search dashboard and searches on the selected source IP and time range.
Scanning Activity (Many Systems)	Displays network activity from port scanners or vulnerability scanners and helps identify unauthorized instances of these scanners. The drilldown redirects the page to the Traffic Search dashboard and searches on the selected source IP and time range.

Traffic Search dashboard

The **Traffic Search** dashboard assists in searching network protocol data, refined by the search filters. The dashboard is used in ad-hoc searching of network data, but is also the primary destination for drilldown searches used in the Traffic Center dashboard panels.

The **Traffic Search** dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
Action	Filter based on firewall rule actions.	Drop-down: select to filter by
Source	Filter based on source IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter based on destination IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Transport Protocol	Filter based on transport protocol.	Drop-down: select to filter by
Destination port	Filter based on destination host port.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Intrusion Center dashboard

The **Intrusion Center** provides an overview of all network intrusion events from Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) device data. This dashboard assists in reporting on IDS activity to display trends in severity and in volume of IDS events.

Filter by	Description	Action
IDS Type	Filter based on events matching a specified type of IDS.	Drop-down: select to filter by
IDS Category	Filter based on events matching vendor-defined categories.	Drop-down: select to filter by
Severity	Filter based on event severity.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by

Filter by	Description	Action
Time Range	Select the time range to view.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Attacks Over Time By Severity	Displays the top attacks over time by severity. The drilldown opens the Intrusion Search dashboard and searches on the selected severity and time range.
Top Attacks	Displays the top attacks by count and signature. The drilldown opens the Intrusion Search dashboard and searches on the selected signature.
Scanning Activity (Many Attacks)	Displays source IP's showing a pattern of attacks. The drilldown opens the Intrusion Search dashboard and searches on the selected source IP and time range.
New Attacks - Last 30 Days	Displays attacks that have been identified for the first time. New attack vectors indicate that a change has occurred on the network, potentially due to the presence of a new threat, such as a new malware infection. The drilldown opens the Intrusion Search dashboard and searches on the selected signature and time range.

Intrusion Search dashboard

The **Intrusion Search** dashboard assists in searching IDS-related events such as attacks or reconnaissance-related activity, based on the criteria defined by the search filters. The dashboard is used in ad-hoc searching of network data, but is also the primary destination for drilldown searches used in the Intrusion Center dashboard panels.

The **Intrusion Search** dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
IDS Category	Filter based on events matching vendor-defined categories.	Drop-down: select to filter by
Severity	Filter based on event severity.	Drop-down: select to filter by
Signature	Filter based on IDS signature name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Source	Filter based on source IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter based on destination IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Vulnerability Center dashboard

The **Vulnerability Center** provides an overview of vulnerability events from device data.

Filter by	Description	Action
Severity	Filter based on event severity.	Drop-down: select to filter by
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by

Filter by	Description	Action
Time Range	Select the time range to represent.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 60 days. Key indicators represent summary information and appear at the top of the dashboard. See Key indicators in Splunk Enterprise Security.
Top Vulnerabilities	Displays the most common issues reported by the vulnerability scanners. The reported issues are aggregated by host so that the chart represents the number of unique occurrences of the issue as opposed to the number of times the issue was detected (since scanning a single host multiple times will likely reveal the same vulnerabilities each time). The drilldown opens the Vulnerability Search dashboard and searches on the selected signature and time range.
Most Vulnerable Hosts	Displays the hosts with the highest number of reported issues. The drilldown opens the Vulnerability Search dashboard and searches on the selected severity, host, and time range.
Vulnerabilities by Severity	Displays issues by the severity assigned by the vulnerability scanner. Helps identify trends that are not visible when looking at vulnerabilities individually. The drilldown opens the Vulnerability Search dashboard and searches on the selected severity and time range.
New Vulnerabilities	Displays the most recent new vulnerabilities detected as well as the date each one was first observed. Helps identify new issues appearing on the network that need to be investigated as potential new attack vectors. The drilldown opens the Vulnerability Search dashboard and searches on the selected signature and time range.

Vulnerability Operations dashboard

The Vulnerability Operations dashboard tracks the status and activity of the vulnerability detection products deployed in your environment. Use this dashboard to see the overall health of your scanning systems, identify long-term issues, and see systems that are no longer being scanned for vulnerabilities.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Scan Activity Over Time	Displays vulnerability scan activity by systems over time. Hover over item for details. The drilldown opens the Vulnerability Search dashboard and searches on the selected time range.
Vulnerabilities by Age	Displays detected vulnerabilities by age, with signature, destination, and event time. Click an item to view in the Vulnerability Profiler for more detail. The drilldown opens the Vulnerability Search dashboard and searches on the selected signature or destination host, and time range.
Delinquent Scanning	Displays vulnerability scans with a severity of "high". Includes signature. The drilldown opens the Vulnerability Search dashboard and searches on the selected destination host and time range.

Vulnerability Search dashboard

The **Vulnerability Search** dashboard displays a list of all vulnerability-related events based on the criteria defined by the search filters. The dashboard is used in ad-hoc searching of vulnerability data, but is also the primary destination for drilldown searches used in the Vulnerability Center dashboard panels.

The **Vulnerability Search** dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
Vuln. category	Filter based on events matching vendor-defined categories.	Drop-down: select to filter by
Severity	Filter based on event severity.	Drop-down: select to filter by
Signature	Filter based on vendor signature name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Reference (bugtraq, cert, cve, etc.)	Filter based on common reference standards.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter based on destination IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to represent.	Drop-down: select to filter by

Troubleshooting Network Dashboards

This dashboard references data from various data models. Without the applicable data, the dashboards will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Web center and network changes dashboards

Use the **Web center** and **Network changes** dashboards to profile web traffic events and track configuration changes to firewalls in your environment.

Web Center

You can use the Web Center dashboard to profile web traffic events in your deployment. This dashboard reports on web traffic gathered by Splunk from proxy servers. It is useful for troubleshooting potential issues such as excessive bandwidth usage, or proxies that are no longer serving content for proxy clients. You can also use the Web Center to profile the type of content that clients are requesting, and how much bandwidth is being used by each client.

You can configure new data inputs through Splunk Settings, or search for particular traffic events directly through Incident Review. Use the filters at the top of the screen to limit which items are shown. Filters do not apply to Key Indicators.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Key Indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard.

Panel	Description
Events Over Time by Method	Shows the total number of proxy events over time, aggregated by Method, or the HTTP method requested by the client (POST, GET, CONNECT, etc.).
Events Over Time by Status	Shows the total number of proxy events, aggregated by Status, or the HTTP status of the response.
Top Sources	Sources associated with the highest volume of network traffic. This is useful for identifying sources that are using an excessive amount of network traffic (for example, file-sharing hosts), or frequently-requested destinations generating large amounts of network traffic (for example, YouTube or Pandora).
Top Destinations	Destinations associated with the highest volume of network traffic. This is useful for identifying sources that are using an excessive amount of network traffic (for example, file-sharing hosts), or frequently-requested destinations generating large amounts of network traffic (for example, YouTube or Pandora).

Web Search

The **Web Search** dashboard assists in searching for web events that are of interest based on the criteria defined by the search filters. The dashboard is used in ad-hoc searching of web data, but is also the primary destination for drilldown searches used in the dashboard panels.

The Web Search dashboard displays no results unless it is opened in response to a drilldown action, or you update a filter, select a time range, and click Submit.

Filter by	Description	Action
HTTP Method	Filter based on HTTP Method.	Text field. Empty by default. Wildcard strings with an asterisk (*)
HTTP Status	Filter based on HTTP Status code.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Source	Filter based on source IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Destination	Filter based on destination IP or name.	Text field. Empty by default. Wildcard strings with an asterisk (*)
URL	Filter based on URL details.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Time Range	Select the time range to view.	Drop-down: select to filter by

Network Changes

Use the Network Changes dashboard to track configuration changes to firewalls and other network devices in your environment. This dashboard helps to troubleshoot device problems; frequently, when firewalls or other devices go down, this is due to a recent configuration change.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by
Time Range	Select the time range to represent.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Network Changes by Action	Shows all changes to the devices by the type of change, or whether a device was added, deleted, modified, or changed. The drilldown opens the "New Search" dashboard and searches on the selected action and time range.
Network Changes by Device	Shows all devices that have been changed as well as the number of the changes, sorted by the devices with the highest number of changes. The drilldown opens the "New Search" dashboard and searches on the selected device and time range.
Recent Network Changes	Shows a table of the most recent changes to network devices in the last day.

Port and protocol tracker dashboard

The Port and Protocol Tracker tracks port and protocol activity, based on the rules set up in **Configure > Content > Content Management** in Enterprise Security. To edit, search for interesting_ports_lookup or use the Type dropdown menu to filter on **Managed Lookup** and scroll to **Interesting Ports**.

The lookup table specifies the network ports that the enterprise allows. From this dashboard, you can view new activity by port to identify devices that are not in compliance with corporate policy, as well as detect prohibited traffic.

Filter by	Description	Action
Business Unit	A group or department classification for the identity.	Text field. Empty by default. Wildcard strings with an asterisk (*)
Category	Filter based on the categories to which the host belongs.	Drop-down: select to filter by

Dashboard Panels

Panel	Description
Port/Protocol Profiler	Displays the volume network transport and port activity over time, to evaluate if port activity is trending upwards or downwards. Sudden increases in unapproved port activity may indicate a change on the networked devices, such as an infection. The drilldown opens the "New Search" dashboard and searches on the selected transport destination port and time range.
New Port Activity - Last 7 Days	Displays a table of transport and port traffic communication over time. The drilldown opens the Traffic Search dashboard and searches on the selected transport and time range.
Prohibited Or Insecure Traffic Over Time - Last 24 Hours	Displays the volume of prohibited network port activity over time, and helps determine if unapproved port activity is trending upwards or downwards. The drilldown opens the "New Search" dashboard and searches on the selected transport destination port and time range.
Prohibited Traffic Details - Last 24 Hours	Displays a table of the number of prohibited network traffic events. The drilldown opens the "New Search" dashboard and searches on the selected source IP, destination IP, transport, port, and time range.

Troubleshooting

This dashboard references data from various data models. Without the applicable data, the dashboards will remain empty. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Protocol intelligence dashboards

Protocol intelligence is a collection of dashboards and searches that report on the information collected from common network protocols. As an analyst, you can use these dashboards to gain insight into HTTP, DNS, TCP/UDP, TLS/SSL, and common email protocols across your system or network.

The **Protocol intelligence** dashboards use packet capture data. Packet capture data contains security-relevant information not typically collected in log files. Integrating network protocol data provides a rich source of additional context when detecting, monitoring, and responding to security related threats.

Obtain packet capture data from apps such as Splunk Stream and the Splunk Ad-on TA for Zeek. The dashboards will be empty without applicable data.

Protocol center dashboard

The **Protocol center** dashboard provides an overview of security-relevant network protocol data. The dashboard searches display results based on the time period selected using the dashboard time picker.

Dashboard panels

Panel	Description
Key indicators	Displays metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard. Key indicators displayed include **Protocol activity**, **Long lived connections**, **Stream connections**, **Encrypted connections**, and **Total bytes**.
Connections by protocol	Displays the sum of all protocol connections, sorted by protocol over time. The connection distribution by protocol shows the most common protocols used in an environment, such as email protocols and HTTP/SSL. An exploited protocol may display a disproportionate number of connections for its service type.
Usage by protocol	Displays the sum of all protocol traffic in bytes, sorted by protocol over time. The bandwidth used per protocol will show consistency relative to the total network traffic. An exploited protocol may display a traffic increase disproportionate to its use.
Top connection sources	Displays the top 10 hosts by total protocol traffic sent and received over time. A host displaying a large amount of connection activity may be heavily loaded, experiencing issues, or represent suspicious activity. The drilldown redirects the page to the traffic search dashboard and searches on the selected source IP.
Usage for well known ports	Displays the sum of protocol traffic, sorted by ports under 1024 over time. The bandwidth used per port will show consistency relative to the total network traffic. An exploited port may display an increase in bandwidth disproportionate to its use. The drilldown redirects the page to the traffic search dashboard and searches on the selected port.
Long lived connections	Displays TCP connections sustained longer than 3 minutes. A long duration connection between hosts may represent unusual or suspicious activity. The drilldown opens the traffic search dashboard and searches on the selected event.

Data sources

The reports in the **Protocol center** dashboard use fields in the network traffic data model. Relevant data sources include all devices or users generating TCP and UDP protocol traffic on the network captured from vulnerability scanners and packet analysis tools such as Splunk Stream and the Bro network security monitor.

Traffic size analysis dashboard

Use the **Traffic size analysis** dashboard to compare traffic data with statistical data to find outliers, traffic that differs from what is normal in your environment. Any traffic data, such as firewall, router, switch, or network flows, can be summarized and viewed on this dashboard.

- Investigate traffic data byte lengths to find connections with large byte counts per request, or that are making a high number of connection attempts with small byte count sizes.
- Use the graph to spot suspicious patterns of data being sent.
- Drill down into the summarized data to look for anomalous source/destination traffic.

Dashboard filters

Use the filters to refine the traffic size events list on the dashboard.

Filter by	Description
Standard deviation index	The percentage (%) shows the amount of data that will be filtered out if that number of standard deviations is selected. Choose a higher number of deviations to see fewer traffic size anomalies and details, or choose a lower number of deviations to see a greater number of traffic size anomalies and details.
Time range	Select the time range to represent.
Advanced filter	Select this option to see the list of category events that can be filtered for this dashboard.

Dashboard panels

Select chart elements or table rows to display raw events. The following table describes the panels for this dashboard.

Panel	Description
Key indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard.
Traffic size anomalies over time	The chart displays a count of anomalous traffic size in your environment over time. It displays traffic volume greater than the number of standard deviations selected in the filter (2 by default) displayed in a line graph with time as the x-axis and count as the y-axis.
Traffic size details	Table that displays each of the traffic events and related details such as the size of the traffic event in bytes. If there is more that one event from a source IP address, the `count` column shows how many events are seen. In the `bytes` column, the minimum, maximum, and average number of bytes for the traffic event are shown. Z indicates the standard deviations for the traffic event.

DNS activity dashboard

The DNS activity dashboard displays an overview of data relevant to the DNS infrastructure being monitored. The dashboard searches display results based on the time period selected using the dashboard time picker.

Dashboard panels

Panel	Description
Key indicators	Displays metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard.
Top reply codes by unique sources	Displays the top DNS Reply codes observed across hosts. A host initiating a large number of DNS queries to unknown or unavailable domains will report a large number of DNS lookup failures with some successes. That pattern of DNS queries may represent an exfiltration attempt or suspicious activity. The drilldown opens the DNS search dashboard and searches on the selected reply code.
Top DNS query sources	Displays the top DNS query sources on the network. A host sending a large amount of DNS queries may be improperly configured, experiencing technical issues, or represent suspicious activity. The drilldown opens the DNS search dashboard and searches on the selected source IP address.
Top DNS queries	Displays the top 10 DNS QUERY requests over time. The drilldown opens the DNS search dashboard and searches on the queried host address.
Queries per domain	Displays the most common queries grouped by domain. An unfamiliar domain receiving a large number of queries from hosts on the network may represent an exfiltration attempt or suspicious activity. The drilldown opens the DNS search dashboard and searches on the queried domain address.

Panel	Description
Recent DNS queries	Displays the 50 most recent DNS response queries with added detail. The drilldown opens the DNS search dashboard and searches on the selected queried address.

Data sources

The reports in the DNS dashboard use fields in the network resolution data model. Relevant data sources include all devices or users generating DNS protocol traffic on the network captured from vulnerability scanners and packet analysis tools such as Splunk Stream and the Bro network security monitor.

DNS search dashboard

The **DNS search** dashboard assists in searching DNS protocol data, refined by the search filters. The dashboard is used in ad-hoc searching of DNS data, but is also the primary destination for drilldown searches in the DNS dashboard panels.

The **DNS search** page displays no results unless it is opened in response to a drilldown action, or you set a filter or time range and select **Submit**.

Filter by	Description
Source	Source IP address
Destination	Destination IP address
Query	DNS query
Message type	DNS message type: Query, Response, or All.
Reply Code	DNS reply type: All, All Errors, and a list of common reply codes

SSL activity dashboard

The **SSL activity** dashboard displays an overview of the traffic and connections that use SSL. As an analyst, you can use these dashboards to view and review SSL encrypted traffic by usage without decrypting the payload. The dashboard searches display results based on the time period selected using the dashboard time picker.

Dashboard panels

Panel	Description
Key indicators	Displays metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard.
SSL activity by common name	Displays outbound SSL connections by common name (CN) of the SSL certificate used. An unfamiliar domain receiving a large number of SSL connections from hosts on the network may represent unusual or suspicious activity. The drilldown redirects the page to the SSL search dashboard, and searches on the selected common name.
SSL cloud sessions	Displays the count of active sessions by CN that represents a known cloud service. The CN is compared to a list of cloud service domains pre-configured in the cloud domains lookup file. The drilldown opens the SSL search dashboard and searches on the selected source IP and common name.
Recent SSL sessions	Displays the 50 most recent SSL sessions in a table with additional information about SSL key. The fields `ssl_end_time`, `ssl_validity_window`, and `ssl_is_valid` use color-coded text for fast identification of expired, short lived, or invalid certificates. The drilldown redirects the page to the SSL search dashboard and displays the full details of the selected event.

Data sources

The reports in the SSL activity dashboard use fields in the certificates data model. Relevant data sources include all devices or users generating SSL protocol traffic on the network captured from vulnerability scanners and packet analysis tools such as Splunk Stream and the Bro network security monitor.

SSL search dashboard

The SSL search dashboard assists in searching SSL protocol data, refined by the search filters. The dashboard is used in ad-hoc searching of SSL protocol data, but is also the primary destination for drilldown searches in the SSL activity dashboard panels.

The **SSL search** page displays no results unless it is opened in response to a drilldown action, or you set a filter or time range and select **Submit**.

Filter by	Description
Source	Source IP address.
Destination	Destination IP address.
Subject/Issuer	Subject or issuer fields.
Subject/Issuer common name	Common name retrieved from the x.509 certificate subject or issuer fields.
Certificate serial number	The x.509 certificate serial number field.
Certificate hash	The x.509 certificate signature field.

Email activity dashboard

The **Email activity** dashboard displays an overview of data relevant to the email infrastructure being monitored. The dashboard searches displays result based on the time period selected using the dashboard time picker.

Dashboard panels

Panel	Description
Key indicators	Displays metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard.
Top email sources	Displays the hosts generating the most email protocol traffic. A host sending excessive amounts of email on the network may represent unusual or suspicious activity. Periodicity displayed across hosts viewed on the sparklines may be an indicator of a scripted action. The drilldown opens the email search dashboard and searches on the selected source IP.
Large emails	Displays the hosts sending emails larger than 2MB. A host that repeatedly sends large emails may represent suspicious activity or data exfiltration. The drilldown opens the email search dashboard and searches on the selected source IP.
Rarely seen senders	Displays sender email addresses that infrequently send email. An address that represents a service account or non-user sending email may indicate suspicious activity or a phishing attempt. The drilldown opens the email search dashboard and searches on the selected sender.
Rarely seen receivers	Displays receiver email addresses that infrequently receive email. An address that represents a service account or non-user receiving email may indicate suspicious activity or a phishing attempt. The drilldown opens the email search dashboard and searches on the selected recipient.

Data sources

The reports in the **Email activity** dashboard use fields in the email data model. Relevant data sources include all the devices or users generating email protocol traffic on the network captured from vulnerability scanners and packet analysis tools such as Splunk Stream and the Bro network security monitor.

Email search dashboard

The **Email search** dashboard assists in searching email protocol data, refined by the search filters. The dashboard is used in ad-hoc searching of email protocol data, but is also the primary destination for drilldown searches used in the email activity dashboard panels.

The **Email search** page displays no results unless it is opened in response to a drilldown action, or you set a filter or time range and select **Submit**.

Filter by	Description
Email protocol	The email communication protocol.
Source	Source IP address.
Sender	The sender's email address.
Destination	Destination IP address.
Recipient	The recipient's email address.

Troubleshooting protocol intelligence dashboards

The **Protocol intelligence** dashboards use packet capture data from apps such as Splunk Stream and the Splunk Add-on for Bro IDS. Without applicable data, the dashboards remain empty. For an overview of Splunk Stream Integration with Splunk Enterprise Security, see Splunk Stream integration in the Enterprise Security *Installation and Upgrade Manual*. See Troubleshoot dashboards in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Threat intelligence dashboards

Splunk Enterprise Security includes two dashboards for reviewing threat intelligence data: the **Threat findings** dashboard and the **Indicators** dashboard.

Threat findings

The **Threat findings** dashboard provides information on threat findings by matching threat intelligence source content to events in Splunk Enterprise Security.

Dashboard filters

Use the available dashboard filters to refine the results displayed on the dashboard panels. The filters do not apply to key security indicators.

Filter by	Description

Threat group	A named group or entity representing a known threat, such as a malware domain.
Threat category	A category of threat, such as advanced persistent threat, financial threat, or backdoor.
Search	Used for searching on a value related to fields: Destination, Sourcetype, Source, Threat Collection, Threat Collection Key, Threat Key, Threat Match Field, and Threat Match Value.
Time range	The time range of threat intelligence data.

Dashboard panels

Panel	Description
Key indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard.
Threat findings over time	Displays the count of events by all threat collections over the selected time. The drilldown opens a search with the selected threat collection and scoped to the selected time frame.
Most active threat collections	Displays the top threat collections by event matches over the selected time with a sparkline representing peak event matches. The drilldown opens a search with the selected threat collection.
Most active threat sources	Displays the top threat sources over the selected time by event count matches. The drilldown opens a search with the selected threat source.
Threat findings details	Displays a breakout of the most recent threat findings. Use the event selection box **Threat findings details** with the **Per-panel filter** option to: • Allowlist by `threat_match_value` to remove matches. • Highlight specific `threat_match_value` matches and place them at the top of the table.

Data sources

The reports in the **Threat findings** dashboard use fields in the `Threat_Intelligence` data model. Relevant data sources include threat source event matches in the `threat_activity` index along with the associated indicators.

Indicators

The **Indicators** dashboard provides a single location to explore and review threat content sourced from all configured threat download sources. It provides additional context by showing all indicators related to a user-specified threat source or indicator.

The dashboard offers multiple selection filters and tabs to isolate the threat content.

Begin by changing the **Indicator** filter to select from available indicator types. Other available filters will change depending on your selection.

Indicator selection	Filter by text: (*) wildcard defaulted	Filter by drop-down
Threat ID	Malware Alias, Intel Source ID, and Intel Source Path	Threat Category, Threat Group
Network	IP, Domain	HTTP. Select from: Referrer: User Agent, Cookie, Header, Data, or URL and add a string to search.
File	File Name, File Extension, File Path, and File Hash	n/a
Registry		n/a

Indicator selection	Filter by text: (*) wildcard defaulted	Filter by drop-down
	Hive, Path, Key Name, Value Name, Value Type, and Value Text	
Service	Name, Descriptive Name:, Description:, and Type	n/a
User	User, Full Name, Group Name, and Description	n/a
Process	Process, Process Arguments, Handle Names, and Handle Type	n/a
Certificate	Serial Number, Subject, Issuer, Validity Not After, and Validity Not Before	n/a
Email	Address, Subject, and Body	n/a

Use the tabs to review threat source context:

Tab	Panels
Threat overview	Endpoint artifacts, Network artifacts, Email artifacts, Certificate artifacts
Network	HTTP intelligence, IP intelligence, Domain intelligence
Endpoint	File intelligence, Registry intelligence, Process intelligence, Service intelligence, User intelligence
Certificate	Certificate intelligence
Email	Email intelligence

Data sources

The **Indicator** dashboard references fields in the threat collection KV Store. Relevant data sources include threat sources such as STIX and OpenIOC documents. -->

Web intelligence dashboards

Use the **Web intelligence** dashboards to identify potential and persistent threats in your environment.

HTTP category analysis dashboard

The **HTTP category analysis** dashboard looks at categories of traffic data. Any traffic data, such as firewall, router, switch, or network flows, can be summarized and viewed in this dashboard.

- Compare statistical data to identify traffic outliers, or traffic different from what is typically found in your environment.
- Look for category counts that fall outside of the norm (small or large) that might indicate a possible threat.
- Find low volume traffic activity and drill down from the summarized data to investigate events.
- Use sparklines to identify suspicious patterns of activity by category.

Filter unknown traffic categories

Use the "Show only unknown categories" filter on the **HTTP category analysis** dashboard to filter and view unknown categories of web traffic.

Before you can filter unknown traffic, define which categories are unknown.

1. In the Splunk Web menu, select **Settings** and then **Tags**.
2. Select **List by tag name**.
3. Select an **App context** of DA-ESS-NetworkProtection or a related network add-on, such as TA-websense.
4. Select **New**.
5. Enter a **Tag name** of `unknown`.
6. Enter a **Field-value pair** to define as unknown traffic.
   For example, `category=undetected`.
7. Select **Save**.

Dashboard filters

Filters can help refine the HTTP category list.

Filter by	Description
Time range	Select the time range to represent.
Advanced filter	Select this option to see the list of category events that can be filtered for this dashboard.

Dashboard panels

Select chart elements or table rows to display raw events. The following table describes the panels for this dashboard.

Panel	Description
Key indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard.
Category distribution	Displays category counts as a scatter plot, with `count` as the x-axis and `src_count` as the y-axis. The chart updates when you change filters or the time range. Hover over an item to see details.
Category details	Displays details of the HTTP categories, including a sparkline that represents the activity for that HTTP category over the last 24 hours.

HTTP user agent analysis dashboard

Use the **HTTP user agent analysis** dashboard to investigate user agent strings in your proxy data and determine if there is a possible threat to your environment.

- A bad user agent string, where the browser name is misspelled (like Mozzila) or the version number is wrong (v666), can indicate an attacker or threat.
- Long user agent strings are often an indicator of malicious access.
- User agent strings that fall outside of the normal size (small or large) might indicate a possible threat that should be looked at and evaluated.

The advanced filter can be used to include or exclude specific user agents. Use the statistical information to visually identify outliers. In the summarized data, you can evaluate user agents for command and control (C&C) activity, and find unexpected HTTP communication activity.

Dashboard filters

The dashboard includes a number of filters that can help refine the user agent list.

Filter by	Description
Standard deviation index	The percentage (%) shows the amount of data that will be filtered out if that number of standard deviations is selected. Choose a higher number of deviations to see fewer user agent strings, or choose a lower number of deviations to see a greater number of user agent strings.
Time range	Select the time range to represent.
Advanced filter	Select this option to see the list of category events that can be filtered for this dashboard.

Dashboard panels

Select chart elements or table rows to display raw events. The following table describes the panels for this dashboard.

Panel	Description
Key indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard.
User agent distribution	Displays user agent strings as a scatter plot, with `length` as the x-axis and `count` as the y-axis. The chart updates when you change the filters or the time range. Hover over an item to see details about the raw data.
User agent details	Displays details of the user agents in your environment, including the string value of the user agent and a sparkline that represents the activity for that user agent string over the last 24 hours.

New domain analysis dashboard

The **New domain analysis** dashboard shows any new domains that appear in your environment. These domains can be newly registered, or simply newly seen by Splunk Enterprise Security. Panels display **New domain activity events**, **New domain activity by age**, **New domain activity by top level domain (TLD)**, and **Registration details** for these domains.

- View hosts talking to recently registered domains.
- Discover outlier activity directed to newly registered domains in the **New domain activity by age** panel.
- Identify unexpected top level domain activity in the **New domain activity by TLD** panel.
- Investigate high counts of new domains to find out if your network has an active Trojan, botnet, or other malicious entity.

Dashboard filters

The dashboard includes a number of filters to refine the list of domains displayed.

Filter by	Description
Domain	Enter the domain (access, endpoint, network).
Domain type	Select **Newly Registered** or **Newly Seen** to filter the types of domains to be viewed.
Maximum age (days)	The time range for the newly seen or newly registered domains. The default is 30 days.
Time range	Select the time range to represent.
Advanced filter	Select this option to see the list of category events that can be filtered for this dashboard.

Dashboard panels

Select chart elements or table rows to display raw events. The following table describes the panels for this dashboard.

Panel	Description

Panel	Description
New domain activity	Table view of information about new domain activity
New domain activity by age	Scatter plot that displays `Age` as the x-axis and `Count` as the y-axis. Hover over a square for the exact age and number of new domains.
New domain activity by TLD (top level domain)	A bar chart with `Count` as the x-axis and `TLD` as the y-axis. Hover over a bar for the current number of events for a top level domain.
Registration details	A table view of information about new domain registrations. Select a domain in the table to open a search on that domain and view the raw events.

Configure the external API for WHOIS data

To see data in the **New domain analysis** dashboard, you must configure a connection to an external domain lookup data source. You can use the example domain lookup data source provided in Splunk Enterprise Security or you can use one of your choice. The dashboard will only report whether or not a domain is newly seen until this modular input is configured and enabled.

The example uses the external domain source domaintools.com, which provides a paid API for WHOIS data.

1. Sign up for a domaintools.com account.
2. Collect the API host name and your API access credentials from the site. Note that the API access credentials are different from your account email address.

Use the API information to set up a modular input in Splunk Enterprise Security

1. From the Splunk Enterprise Security menu bar, Select **Configure** then **All configurations** and then **Whois**.
2. Select **Enable** next to **whois_domaintools**.
3. Select the name of the modular input to add the API hostname and username used to access the domaintools API.
4. Save the API credentials on the **Credential and certificate management** page.

Use a different domain source to set up a modular input in Splunk Enterprise Security

Follow these steps if you use a different domain source to set up a modular input in Splunk Enterprise Security:

1. From the Splunk Enterprise Security menu bar, Select **Configure** then **All configurations** and then **Whois**.
2. Select **New**.
3. Enter the name of the modular input to add the API hostname and username used to access the API.
4. Save the API credentials on the **Credential and certificate management** page.
5. Select **Enable** next to the name of the modular input you just created.

> Until you enable the modular input, domains processed by the input will not be queued. This prevents the checkpoint directory from filling up with files.

After enabling the modular input, enable the `outputcheckpoint_whois` macro to create checkpoint data.

1. Select **Configure** and then **General Settings**.
2. Select **Enable** for the **Domain analysis** setting to enable WHOIS tracking.

The modular input stores information in the `whois_tracker.csv` lookup file. After a file exists in the `$SPLUNK_HOME/var/lib/splunk/modinputs/whois` directory, the `whois` index will begin to populate with data. After they are processed, checkpoint files will be deleted.

Add Infoblox as a new `whois` provider

Splunk Enterprise Security version 8.0.0 supports Infoblox as an external `whois` provider.

Follow these steps to add Infoblox as a new `whois` provider:

1. Create an Infoblox account.
2. Add your bearer token authentication details from Infoblox in the **Password** field of the **Credential and certificate management** page.
3. Add a new `whois` provider in the **WHOIS Management** settings page. To access the page, go to the Splunk Enterprise Security menu bar, select **Configure** then **All configurations** and then **Whois**.
4. Add the API user that you set up to this new **WHOIS Provider** page.
5. Add **WhoisInfoblox** as the provider to the **WHOIS Provider** page.
6. Add the remaining details such as proxy server if applicable.

Errors versus normal behavior

- If you see `404` errors in the logs, this is normal behavior when querying domains that don't exist.
- If you see `400` errors in the logs returned from the domaintools API, this is normal behavior when querying domains with invalid top level domains.
- If you don't see new events in the whois index, this might be normal behavior if using `HTTP://` the api_url when it should be `HTTPS://`. You can use either `HTTP://` or `HTTPS://` in the url. However, if you don't pick `HTTP://` or `HTTPS://`, then `HTTP://` is prepended to the api_url by default .

URL length analysis dashboard

The **URL length analysis** dashboard looks at any proxy or HTTP data that includes URL string information. Any traffic data containing URL string or path information, such as firewall, router, switch, or network flows, can be summarized and viewed in this dashboard.

- Compare each URL statistically to identify outliers.
- Investigate long URLs that have no referrer.
- Look for abnormal length URLs that contain embedded SQL commands for SQL injections, cross-site scripting (XSS), embedded command and control (C&C) instructions, or other malicious content.
- Use the details table to see how many assets are communicating with the URL.

Use the key indicators to compare each new URL and to identify outlier URL strings, ones that are different from what is typically found in your environment. URLs that fall outside of the normal size (small or large) may indicate a possible threat. Unusually long URL paths from unfamiliar sources and/or to unfamiliar destinations are often indicators of malicious access and should be examined.

Dashboard filters

Use the filters to refine the URL length events represented on the dashboard.

Filter by	Description

Filter by	Description
Standard deviation index	The percentage (%) shows the amount of data that will be filtered out if that number of standard deviations is selected. Choose a higher number of deviations to see fewer user agent strings, or choose a lower number of deviations to see a greater number of user agent strings.
Time range	Select the time range to represent.
Advanced filter	Select this option to see the list of category events that can be filtered for this dashboard.

Dashboard panels

Select chart elements or table rows to display raw events. The following table describes the panels for this dashboard.

Panel	Description
Key indicators	Displays the metrics relevant to the dashboard sources over the past 48 hours. Key indicators represent summary information and appear at the top of the dashboard.
URL length anomalies over time	The chart displays a count of URL length anomalies across time. It displays URL lengths greater than the number of standard deviations selected in the filter (2 by default) displayed in a line graph with time as the x-axis and count as the y-axis.
URL length details	Table that displays the URL strings and details such as the full URI string. If there is more that one event from a source IP address, the `count` column shows how many events are seen. Z indicates the standard deviations for the URL length.

Security group dashboard

Monitor security groups in your Amazon Web Services (AWS) environment so that you have visibility into your virtual firewalls and can manually detect any suspicious activity.

Use the **Security group** dashboard to monitor security group activity in the AWS environment, including error events, number of security groups and rules, any unused security groups, activity over time, and the detailed list of error activities.

> The security groups and security group rules panels are snapshots based on the AWS lambda ingestion interval of three hours. If no events occur during that interval, your dashboards continue to show data based on the last snapshot from three hours ago. Also, if no events occur during the time you've chosen in the time range picker, such as one hour, your dashboards still show data based on the last snapshot from three hours ago. See Data Ingestion Mechanisms and Intervals in Data Manager in the Data Manager User Manual.

1. From the Splunk Enterprise Security menu bar, select **Analytics** and then **Cloud security**.
2. Select **Security groups**.

The **Security group** dashboard includes the following panels:

Panel	Source Type	Datamodel

Error events	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Security group actions	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Security group activity over time	`aws:cloudtrail`	`datamodel=Change.All_Changes`

Panel	Source Type	Datamodel
		`nodename=All_Changes.Network_Changes`
Most recent security group activity	`aws:cloudtrail`	`datamodel:"Change"."Network_Changes"`
Most recent authorize and revoke activity	`aws:cloudtrail`	`datamodel:"Change"."Network_Changes"`
Security group error activity	`aws:cloudtrail`	`datamodel:"Change"."Network_Changes"`

IAM activity dashboard

Monitor your Amazon Web Services (AWS) user activity to uncover suspicious behaviors that might be associated with malicious activity, such as activity spikes or unusual events.

Use the **IAM activity** dashboard to monitor user activity in your environment, including the error events, which users have the most activity, activity over time, and the detailed list of error activities.

1. From the Splunk Enterprise Security menu bar, select **Analytics** and then **Cloud security**.
2. Select **IAM activity**.

The **IAM activity** dashboard includes the following panels:

Panel	Source type	Datamodel

Error events	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Account_Management`

Activity by user	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Account_Management`

IAM actions	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Account_Management`

IAM actions over time	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Account_Management`

Success vs failure activity	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Account_Management`

Most recent IAM activity	`aws:cloudtrail`	`datamodel:"Change.Account_Management"`
IAM error activity	`aws:cloudtrail`	`datamodel:"Change.Account_Management"`

Filter your panel results

You can filter the results that you see in the dashboard panels.

Filter	Description
Account ID	Specify one or more of the data account IDs that you chose during onboarding.

Filter	Description
Regions	Specify one or more of the data source regions that you chose during onboarding.
Status	Choose from the following statuses: • All - All event statuses, including both successes and errors. • Error - Only error event statuses. Some panels are based on error trends, so there is no difference in the results if you select All or if you select Error.
Action	Choose from the following actions: • All - All event actions. • Each action - You can filter on each action individually or a combination of actions.
Time range	Define the time range of a search with the **time range picker**.

Network ACLs dashboard

Monitor your Amazon Web Services (AWS) network infrastructure for bad configurations and malicious activity. Investigative searches help you probe deeper when the facts warrant it.

Use the **Network ACLs** dashboard to monitor the network ACL activity in your AWS environment, including error events, the number of network ACLs, activity over time, and the detailed list of error activities.

1. From the Splunk Enterprise Security menu bar, select **Analytics** and then **Cloud Security**.
2. Select **Network ACLs**.

The **Network ACLs** dashboard includes the following panels:

Panel	Source Type	Datamodel

Error events	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Network ACL actions	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Network ACL activity over time	`aws:cloudtrail`	`datamodel=Change.All_Changes`
		`nodename=All_Changes.Network_Changes`

Most recent network ACLs activity	`aws:cloudtrail`	`datamodel:"Change"."Network_Changes"`
Network ACL error activity	`aws:cloudtrail`	`datamodel:"Change"."Network_Changes"`

Access analyzer dashboard

Monitor your Amazon Web Services (AWS) shared resources to identify potential unintended access. Use the **Access analyzer** dashboard to monitor your AWS public facing queues, lambdas, and S3 buckets.

1. From the Splunk Enterprise Security menu bar, select **Analytics** and then **Cloud security**.
2. Select **Access analyzer**.

The **Access analyzer** dashboard includes the following panels:

Panel	Source Type	Datamodel
Number of public facing queues	`aws:accessanalyzer:finding`	`n/a`
Number of public facing AWS lambda	`aws:accessanalyzer:finding`	`n/a`
Number of public facing S3 buckets	`aws:accessanalyzer:finding`	`n/a`
Access analyzer trend	`aws:accessanalyzer:finding`	`n/a`

Microsoft 365 security dashboard

Get a summary of relevant Microsoft 365 security data to monitor your Microsoft 365 applications such as Active Directory, Exchange, Security and Compliance, Teams, and so on. Investigative searches help you probe deeper, when the facts warrant it.

Active Directory

To access the Active Directory dashboard, do the following:

1. From the Splunk Enterprise Security menu bar, select **Analytics** and then **Cloud security**.
2. Select **Microsoft 365**.
3. Select **Active Directory**.

The Active Directory dashboard includes the following panels:

Panel	Source Type	Datamodel
Password account lockouts	`o365:management:activity`	`n/a`
Users with enable vs. disable MFA	`o365:management:activity`	`n/a`
Failed user logins	`o365:management:activity`	`n/a`
Impossible travel	`o365:management:activity`	`n/a`
Added or removed bembers from group	`o365:management:activity`	`n/a`

Exchange

To access the Exchange dashboard, do the following:

1. From the Splunk Enterprise Security menu bar, select **Analytics** and then **Cloud security**.
2. Select **Microsoft 365**.
3. Select **Exchange**.

The Exchange dashboard includes the following panels:

Panel	Source Type	Datamodel
Exchange operations	`o365:management:activity`	`n/a`
External domain with forwarding policy	`o365:management:activity`	`n/a`
Mailbox exports	`o365:management:activity`	`n/a`
Mailbox forwarding rules	`o365:management:activity`	`n/a`
Full access permission changes	`o365:management:activity`	`n/a`

Panel	Source Type	Datamodel

OneDrive and SharePoint

To access the OneDrive and SharePoint dashboard, do the following:

1. From the Splunk Enterprise Security menu bar, select **Analytics** and then **Cloud security**.
2. Select **Microsoft 365**.
3. Select **OneDrive and SharePoint**.

The OneDrive and SharePoint Dashboard includes the following panels:

Panel	Source Type	Datamodel
Activity by location	`o365:management:activity`	`n/a`
Operations over time	`o365:management:activity`	`n/a`
Activity by user	`o365:management:activity`	`n/a`
Items shared with external users	`o365:management:activity`	`n/a`
Risky downloads over time	`o365:management:activity`	`n/a`
Permission changes	`o365:management:activity`	`n/a`
Top SharePoint sites accessed	`o365:management:activity`	`n/a`

Security and Compliance

To access the Security and Compliance dashboard, do the following:

1. From the Splunk Enterprise Security menu bar, select **Analytics** and then **Cloud security**.
2. Select **Microsoft 365**.
3. Select **Security and Compliance**.

The Security and Compliance dashboard includes the following panels:

Panel	Source Type	Datamodel
Alerts over time	`o365:management:activity`	`n/a`
Alerts by user	`o365:management:activity`	`n/a`
Alerts by name	`o365:management:activity`	`n/a`
Alert details	`o365:management:activity`	`n/a`

Filter your panel results

You can filter the results that you see in the dashboard panels.

Filter	Description
Time range	Define the time range of a search with the **time range picker**.

Filter	Description
	Even though you can change the time range for all the panels, the behavior is different for the **Password account lockouts** panel. Changing the time range only changes the trend line in the panel. It doesn't change the number that displays in the panel. The time range for the number is hardcoded to 24 hours.

Sharing your Threat Data

Share Threat Data in Splunk Enterprise Security

We can respond much faster and more precisely to the evolving threat landscape when our Splunk Enterprise Security customers share their threat and event data with us for enhanced insights and analytics. Shared data from our Splunk Enterprise Security community helps us to provide improved detection capabilities, update threat intelligence, analyze threat trends, and perform more informed testing, improvement and operations of our security offerings. With our updated Splunk General Terms and Splunk Specific Offering Terms for Enterprise Security, you give us instructions to collect and analyze threat and event data in your Splunk Enterprise Security Hosted Service. Our mission with this data sharing program is to develop new analytics and machine learning (ML) models as well as make our security offerings more responsive and predictive to the needs of you and our other customers.

What is the benefit to me?

Following is a list of benefits for participating in Threat Data usage in Splunk Enterprise Security enhancement program:

- **Reduced noise and higher fidelity outcomes**: Customers who share their data under this program have the benefit of new analytics and ML models in our security offerings tested and tuned against their data. When your data is part of this processing, we expect less false positives and noise, and more reliable outcomes, when those new analytics and models are processing your data in your production environment.

- **Early access to new detections**: Customers who allow Splunk to process their data might be given early access to new detections based on the insights gained from the shared information and knowledge of how it performs using your data. This can help you to stay ahead of the curve by utilizing the latest security content as quickly as possible.

- **Customized security insights**: Customer data contributes to tailored analytics and insights into the latest security trends, that can be shared for more relevant and actionable outcomes.

- **Transparency and control**: Splunk is committed to the transparent handling of data with clear options to manage the data you instruct Splunk to use for these purposes. You can have confidence of knowing how your data is used and retain the ability to withdraw your permission at any time.

How to opt-out of sharing Threat Data

To opt-out of the sharing of your Threat Data that is ingested into Splunk Enterprise Security and use as described above, please submit an email to optoutdatause@splunk.com. For timely processing of your request, be sure the email contains the following information:

- The full name of your company
- Splunk Enterprise Security Cloud customers should include the name of your company's Splunk Enterprise Security stack (the URL of your Cloud deployment)
- The name of your Splunk Sales Representative (if known)