Splunk® InfoSec App User Guide 1.7.0

Generated: 5/12/2022 12:55 am

Table of Contents

Introduction to the InfoSec app for Splunk

Overview of the InfoSec app for Splunk

Use the InfoSec App for Splunk as an entry level security solution powered by the Splunk platform to address the most common security use cases, including continuous monitoring and security investigations. You can also use the InfoSec app for a number of advanced threat detection use cases and expand them using other security apps and add-ons that you can download from Splunkbase.

Following is a list of the applications supported by the Infosec App (version 1.7.0):

- Force Directed app For Splunk (version 3.1.0)
- Lookup File Editor (version 3.5.0)
- Punchcard - Custom Visualization (version 1.5.0)
- Splunk Sankey Diagram - Custom Visualization (version 1.6.0)
- Splunk Common Information Model (CIM) (version 4.20.0)

How the InfoSec app for Splunk works

The InfoSec app is a free app for the Splunk platform that can be downloaded and installed into your Splunk environment. Download the InfoSec app for Splunk from Splunkbase.

The InfoSec app is a collection of comprehensive, extensible dashboards and alerts that focus on the most common security-oriented technology components within your typical corporate environment. Use this app to investigate incidents, automate compliance tasks, and help protect your network, users, and intellectual property from external adversaries and malicious insider threats. You can also use the app to provide executive-level reporting metrics, trends, and summaries. You can use this app to assist in completing audits by mapping customizable reports to common compliance frameworks such as NIST, HIPPA, PCI, and ISO.

The InfoSec app provides a standard Splunk search page from within the app. For more information on how to search using the Splunk Platform, see this introductory Search, filter, and correlate video.

Use the Dashboards page to list all the saved dashboards within the Splunk platform. The Dashboards page allows you to perform the following actions:

- Open and view a dashboard
- Adjust who can access a dashboard by modifying it's permissions
- Edit a dashboard
- Clone a dashboard

Use the following table to learn about the dashboards available on the InfoSec app and how you can use them to monitor your Splunk environment:

Dashboard	Function
Security Posture	Provides a high level view to monitor the security in your Splunk environment. For more information to monitor your security posture, see Monitor your security posture using the InfoSec app for Splunk.
Continuous Monitoring	Comprises of the following dashboards that continuously monitor your Splunk environment:

Dashboard	Function
	• Windows Access and Changes dashboard to view events in MS Windows • All Authentications dashboard to view all authentication actions • Malware dashboard to view antivirus solutions • Intrusion Detection (IDS/IPS) dashboard to view intrusion detection and prevention systems • Firewalls dashboard to view firewall events • Network Traffic dashboard to view firewall data in your network • VPN Access dashboard to view VPN session data For more information to continuously monitor your Splunk environment, see Monitor your environment continuously using the InfoSec app for Splunk
Advanced Threat	Comprises of the following dashboards that leverage the power of the Splunk Platform's search capabilities to highlight security events of interest: • Access Anomalies dashboard to identify security risks • Network Anomalies dashboard to identify network anomalies • Custom Use Cases dashboard to incorporate custom searches and dashboards For more information to highlight interesting security events, see Identify advanced threats using the InfoSec app for Splunk
User and Host Investigation	Helps to investigate user and host-based behaviors and actions For more information to investigate user or host behaviors, see Investigate behaviors using the InfoSec app for Splunk
Compliance	Provides visibility into controls that are required under different compliance frameworks. For more information to set up up visibility into compliance requirements, see Set up controls using the InfoSec app for Splunk.
Executive View	Provides a high-level view of certain security metrics and the environment status. For more information to report on high level security metrics, see Display high level security metrics using the InfoSec app for Splunk
Alerts	Helps to investigate and manage alerts For more information to investigate and manage alerts, see Manage alerts using the InfoSec app for Splunk
Health	Performs a health-check of your Splunk environment For more information to perform a health check, see Perform a health check using the InfoSec app for Splunk

For more information on the InfoSec app, review the InfoSec app for Splunk - Introduction video.

What you can do with the InfoSec app for Splunk

Use the InfoSec app dashboards to provide coverage in the following areas:

- Authentication, including Active Directory, LDAP
- Malware, including antivirus, next generation antivirus
- Network traffic, including firewalls, next generation firewalls

You can use the InfoSec app to accomplish the following tasks:

- Direct the powerful features of the Splunk platform towards security.
- Access a single pane view of security events and posture.
- Investigate security alerts and incidents.
- Customize and expand a base security platform to integrate with additional apps and add-ons from Splunkbase.

Extending the features of the InfoSec App for Splunk

You may configure and integrate the InfoSec app with the SSE app, the Common Information Model (CIM), Splunk Enterprise Security, Splunk Phantom, and other Splunk apps and add-ons. You may also use the InfoSec app with the Splunk Machine Learning Toolkit (MLTK) and enable advanced ML based correlation searches within the InfoSec app to detect threats and provide alerts.

Download any of the following apps to extend the capabilities of the Infosec app:

- Splunk Security Essentials (SSE) app.
- Splunk Phantom
- Splunk Machine Learning Toolkit (MLTK) app
- Splunk Enterprise Security

Additionally, you can directly download and install many other apps and add-ons from the Splunkbase library and configure them within your Splunk environment. Using these Splunk apps with the InfoSec app provide solutions for many common use case and provide specialized insight into your data and systems with preconfigured dashboards, reports, data inputs, and saved searches.

Dashboards in the InfoSec app for Splunk

Monitor your security posture using the InfoSec app for Splunk

Use the Security Posture dashboard for a high-level view of your security posture.

Security posture indicators that report on events hosts and accounts

For an immediate view of the state of your environment compared to the previous 24 hours, use the first two panels of indicators. These provide information on the statistical counts of events and the number of detected hosts and devices.

Use the indicators that display the statistical counts of events on the Security posture dashboard to track the number of events from intrusion detection systems (IDS), antivirus, and malware systems. Each indicator shows the current state, with an arrow identifying the rate of change (positive, neutral, or negative) and the previously recorded statistic from the previous 24 hours.

Use the indicators that display the hosts, devices, and accounts to monitor the number of detected hosts, devices, and accounts being monitored on the Security Posture dashboard. Each indicator also includes the 24-hour trend and previous results for comparative purposes. Clicking on any of these indicators opens a new dashboard with more detailed information.

Security posture dashboards that report on intrusion alerts

Use the following three dashboards within the Security Posture dashboard to break down the reporting of the intrusion alerts into a statistical count:

- Intrusion Alerts by Severity classifies the intrusion alerts by severity
- Intrusion Alerts over Time provides a 24-hour view of the intrusion alerts over time
- Top 10 High Severity Intrusion Alerts indicates the top 10 critical intrusion alerts charted over the same 24-hour window

Click any of these dashboards to get more detail on your IDS.

Security posture dashboards that report on accounts and assets

Use the punch-card-style dashboards within the Security Posture dashboard to provide a swim-lane view of the type and count of events that are detected against the assets and identities within your organization over the past 24 hours. You can use these dashboards to quickly identify bursts of activity that might need an investigation.

You must install and enable the punch card visualization within your Splunk platform instance for these dashboards to populate. If you see the message "No matching visualization found for type: punchcard, in app: punchcard_app", the punch card visualization might not be installed or enabled.

To install the Splunk InfoSec app, review Install the InfoSec app for Splunk in the *Installation Guide*.

Monitor your environment continuously using the InfoSec app for Splunk

Use the following dashboards in the InfoSec app for Splunk to monitor your environment continuously for security threats:

- Windows Access and Changes dashboard to View events in Windows
- All Authentications dashboard to View all authentication actions
- Malware dashboard to View antivirus solutions
- Intrusion Detection (IDS/IPS) dashboard to View intrusion detection and prevention systems
- Firewalls dashboard to View firewall events
- Network Traffic dashboard to View firewall data in your network
- VPN Access dashboard to View VPN session data

View events in Windows

Use the Windows Access and Changes dashboard to review events within your Windows environment, including the following information:

- Locked out accounts
- Privilege escalations
- Change metrics
- Authentication metrics

The Windows Access and Changes dashboard and other dashboards within the InfoSec app displays the search time period for the last 24 hours by default. You can access and modify the search filters associated with these dashboards by selecting **Show Filters** near the title of each dashboard.

View authentication actions

Use the All Authentications dashboard for a consolidated view of authentication actions across all data sources. You can use this dashboard to identify authentication anomalies within your environment or problem accounts that repeatedly fail to log in.

The All Authentications dashboard also provides an interactive filter that allows you to filter by User, Host, Action, and a frequency criteria. For example: You can use the All Authentications dashboard to authenticate against five or more hosts.

View antivirus solutions

Use the Malware dashboard for a consolidated view of your antivirus solutions over the last 24 hours.

The first row of the dashboard displays the count of Unresolved, Deferred and Blocked infections. These metrics are derived from the action field of the Malware data model. Clicking an action constrains the results of the remaining dashboards to the selected action.

Selecting a destination takes you to the Host Investigation dashboard. Selecting anything else within the presented dashboards displays the results of the underlying search.

View intrusion detection and prevention systems

Use the Intrusion Detection (IDS/IPS) dashboard for a consolidated view across all IDS/IPS systems within your environment. This data typically comes from your NG Firewall solutions and dedicated IPS solutions like Snort, Suricata,

Darktrace, and so on.

The first row provides a breakdown of the total events by action over the last 24 hours. Clicking an action constrains the results in the other dashboards to the selected action.

The second row provides a breakdown of the total events by severity. Clicking a severity also constrains the results presented in the other dashboards to the selected severity.

Click any of the displayed data to display the results of the underlying search.

View firewall events

Use the Firewalls dashboard for a high-level consolidated view of all firewall events within your organization.

The first row displays whether the event was blocked or allowed as well as the total counts for source and destination IP addresses. You can only select the action values, which constrain the other dashboards to the selected action.

The displayed results are geo-tagged by country.

Click any of the presented results to display the results in the underlying search.

View firewall data

Use the Network Traffic dashboard to display your firewall data in more detail. Click any source or destination pivots to the Host Investigation dashboard.

The second part of the dashboard allows you to filter and investigate the firewall detailed results through a series of filters. A communications map displays the relationship of the filtered results.

View VPN session data

Use the VPN dashboard to present VPN session data from all monitored data sources. You can view a list of geographically improbable VPN connections on the dashboard.

You can filter the VPN data by user. Select any of the presented results to display the results in a search.

Identify advanced threats using the InfoSec app for Splunk

Use the Advanced Threat dashboards combined with searches to highlight security events of interest. Searches aim to identify out-of-character behaviors within the event data. The search indicators can be considered anomalies but does not necessarily indicate a threat.

To highlight security risks, use the following Advanced Threat dashboards in the InfoSec app for Splunk:

- Access Anomalies dashboard to Identify security risks
- Network Anomalies dashboard to Identify network anomalies
- Custom Use Cases dashboard to Incorporate custom searches and dashboards

Identify security risks

Use the Access Anomalies dashboard to identify events that can potentially pose a security risk as follows:

- Spikes or out-of-character increases in access to hosts
- Brute force attacks by source or user
- Accounts that have a high percentage of login failures versus success
- Users performing new privileged actions
- Geographically improbable access

Identify network abnormalities

Use the Network Anomalies dashboard to identify the following abnormalities in your network:

- Spikes in access to destinations
- Suspected network scanning
- BOT/C2 network indicators
- SMB and DNS anomalies

Include custom searches and dashboards

Use the Custom Use Cases dashboard to incorporate your own searches and dashboards. You may also incorporate searches from the Splunk Security Essentials app into this dashboard.

Investigate behaviors using the InfoSec app for Splunk

Access the User Investigation and Host Investigation dashboards by drilling down from one of the other dashboards within the InfoSec app for Splunk. Alternatively, navigate to the dashboards directly and search using the provided filters. Select any represented data within these two dashboards to drill down to that user or host, or display the results of the underlying Splunk search.

Use the following dashboards in the InfoSec app to investigate user- and host-based behaviors and actions:

Investigate user behavior

Use the User Investigation dashboard to investigate user activity using the following information:

- User information
- User access by source
- Access over time by action
- Access by source
- Authentication map that shows up to 250 authentication destinations
- The 100 most recent events

Investigate host behavior

Use the Host Investigation dashboard to investigate host activity using the following information:

- Network communications

- Network communications map
- Authentications and changes
- Malware and intrusion

Set up controls using the InfoSec app for Splunk

Use the Compliance dashboard for visibility into controls that are often required under different compliance frameworks. The Compliance dashboard provides reports that are mapped to common compliance and security frameworks like NIST, PCI, ISO, NERC, and HIPAA. These reports utilize authentication, network, and malware data that are already used within the InfoSec App for Splunk.

You can edit and customize this dashboard based on your requirements. If you perform regular audits, you might want to add the searches that you use to respond to the audits to this dashboard.

> The Compliance dashboard does not cover all aspects of information security compliance. Use this dashboard as an introduction into how you can use the Splunk platform to address compliance requirements.

Use the Compliance dashboard for the following processes:

- Actively manage the life cycle of system and application accounts, including their creation, use, dormancy, and deletion, to minimize opportunities for attackers
- Detect, prevent, and correct the flow of security information in networks of different trust levels
- Control the installation, spread, and implementation of malicious code at multiple points in the Splunk Platform
- Optimize automating the rapid update of defense, data gathering, and corrective actions

Display high level security metrics using the InfoSec app for Splunk

Use the Executive View dashboard for a high-level view of certain security metrics.

In this dashboard, you can access the following information to report on the status of the environment:

- Attacks stopped
- Malware blocked
- Users protected
- Devices protected
- User trends
- Attack origins

Manage alerts using the InfoSec app for Splunk

Use the Alerts dashboard to investigate and manage alerts raised by the InfoSec app for Splunk.

Alerts are scheduled searches that run frequently to look for matching events within your data. You can drill-down to the current alerts defined within the InfoSec app and modify or add to them through this dashboard. Consider using the Alert Manager app with the InfoSec app to improve your alert management framework.

You can save any search that you create within the Splunk platform as an alert. All alerts need to include a search schedule. When creating an alert, select the time during which a search can be run. Selecting the cron schedule allows you to set the scheduled frequency as often as every minute.

Do not set up alerts by scheduling a real-time search.

See also

Refer to this video to create a new alert.

Download the Splunk Alert Manager app from Splunkbase.

For more information to define scheduled alerts, see Define scheduled alerts.

Perform a health check using the InfoSec app for Splunk

Use the Health dashboard to perform a health-check of your Splunk environment using the InfoSec app for Splunk.

You can check the Health dashboard to view the issues that might impact the InfoSec app. The dashboard identifies the source and type of data that is indexed by your Splunk environment. It also displays the data models and the status for each data model.

Configure lookups in the InfoSec app for Splunk

Use the lookups that are bundled in the Infosec app for Splunk to enrich the event data within your environment. You can modify the following lookups to provide additional context when viewing certain data within the InfoSec app:

- Host
- User

Requirements

To configure lookups through the InfoSec app, download the Splunk Lookup File Editor app on Splunkbase.

Configure the Host lookup for information on hosts

Use the Host lookup to manually enter the context associated with your organization's assets. You can record fields, such as location, description, owner, priority, make, and model. The information in this lookup table is mapped to events within the Splunk platform through the IP address of the host.

You can configure this lookup manually through the InfoSec app or write a search that regularly populates this lookup from Active Directory and other sources.

Configure the User lookup for information on user events

Use the User lookup to enrich the user event data within your environment with additional information. You can enrich user event data to assist with triaging and creating actionable events during investigation. You can configure the User lookup to record fields such as the full-name, phone number, email address, priority, and so on.

You can configure this lookup manually through the InfoSec app or write a search that regularly populates this lookup from Active Directory and other sources.