Security and Threat Detection

Docs for Sumo apps for Security and Threat Detection.

Sumo provides a variety of apps for security products and platforms, from firewalls and endpoint protection to security automation and orchestration. This guide has documentation for those apps. If you're looking for an app for AWS, Microsoft, or Google, see Amazon and AWS, Microsoft and Azure, or Google.

- Barracuda WAF

The Barracuda WAF App analyzes traffic flowing through the Barracuda WAF and provides pre-configured dashboards that allow you to monitor WAF traffic as well to analyze various types of attacks detected both by Barracuda and the Sumo Logic Threat Intelligence database.

- Collect logs for Barracuda WAF App
- Install the Barracuda WAF App and view the Dashboards
• Carbon Black

The Carbon Black App provides comprehensive visibility into the security posture of your endpoints, enabling you to determine the effects of a breach across your environment. The App provides visibility into key endpoint security data with preconfigured dashboards for alerts, threats intelligence, feeds, sensors, alerts, users, hosts, processes, IOCs, devices and network status.

◦ Collect logs for Carbon Black
◦ Install the Carbon Black App and view the Dashboards

• Cisco ASA

The Cisco ASA App gives you insight into website visitor patterns, monitors infrastructure operations, and provides easy access to threat monitoring. The App uses a predefined parser, searches, and Dashboards which provide visibility into your environment for analysis of overall usage and threats.

◦ Collect Logs for the Cisco ASA App
◦ Install the Cisco ASA App and view the Dashboards
• **Cisco Meraki**

The Sumo Logic App for Cisco Meraki provides a single-pane-of-glass for monitoring and troubleshooting network security, end-to-end performance, switch port management, and device management in your environment.

- Collect logs for the Cisco Meraki App
- Install the Cisco Meraki App and View the Dashboards

• **CloudPassage Halo**

The CloudPassage Halo App enables security operators and administrators to correlate security events across their Halo-managed infrastructure. You can leverage the security visibility provided by CloudPassage’s Halo platform with Sumo Logic’s correlation and visualization capabilities to deliver a security reporting and analysis tool.

- Collect Logs for the CloudPassage Halo App
- Install the CloudPassage Halo App and view the Dashboards
• CrowdStrike Falcon

The CrowdStrike Falcon App gives you visibility into the overall security posture of your environment, as analyzed by CrowdStrike Falcon deployed in your network. This allows you to analyze and group detections by user, tactic, technique, and objective, and find hosts on your network with the highest malware detection. The App dashboards provide detailed analysis of malware detections, from which you can drill down to investigate malicious behaviors.

  ◦ Collect logs for the CrowdStrike Falcon App
  ◦ Install the CrowdStrike Falcon App and view the Dashboards

• Cylance

The Cylance App enables you to analyze Cylance security events by type, status, and detection method. You can use the App to investigate Cylance-specific events and provide operational visibility to team members without logging into Cylance.

  ◦ Collect Logs for the Cylance App
  ◦ Install the Cylance App and view the Dashboard
Duo Security

The Duo Security App helps you monitor your Duo account’s authentication logs, administrator logs, and telephony logs. Duo provides two-factor authentication, endpoint remediation, and secure single sign-on tools.

- Collect Logs for the Duo Security App
- Install the Duo Security App and View the Dashboards

Evident.io Evident Security Platform

Copyright 2020 Sumo Logic, Inc. All rights reserved.
The Evident.io ESP App provides pre-configured searches and Dashboards that allow you to investigate Evident-specific events and provide operational visibility to team members without logging into Evident.io. The Evident.io Evident Security Platform (ESP) streamlines and optimizes vulnerability and risk management.

- Collect Logs for the Evident.io ESP App
- Install the Evident.io ESP App and view the Dashboards

### F5 - BIG-IP LTM

The F5 - BIG-IP Local Traffic Manager (LTM) App helps you optimize and secure network traffic patterns coming into your data center using the F5 BIG-IP platform.

- Collect Logs for the F5 - BIG-IP LTM App
- Install the F5 - BIG-IP LTM App and view the Dashboards

### Imperva - Incapsula Web Application Firewall

The Imperva Incapsula - Web Application Firewall (WAF) App helps you monitor your web application protection service. The preconfigured dashboards provide insights on the threat alerts events on the BOT access control, blocked countries, and user agents.

- Collect Logs for the Imperva - Incapsula Web Application Firewall App
- Install the Imperva - Incapsula Web Application Firewall App and view the Dashboards
• Netskope

![Netskope Logo]

The Netskope App created by Sumo Logic provides visibility into security posture for your applications, as well as allowing you to determine the overall usage of software and SaaS applications in your environment. Netskope is a Cloud Access Security Broker (CASB) hosted in the cloud, primarily used to enforce security policies for cloud-based resources.

- Collect logs for Netskope
- Install the Netskope App and view the Dashboards

• Observable Networks

![Observable Networks Logo]

The Observable Networks App allows you to monitor your Observable Networks deployment from Sumo Logic. The App Overview Dashboard provides insight to high-level data about your network.

- Collect logs for the Observable Network App
- Install the Observable Networks App and view the Dashboard

• Palo Alto Networks 6

![Palo Alto Networks Logo]

The Palo Alto Networks 6 App provides four dashboards, giving you several ways to discover threats, consumption, traffic patterns, and other security-driven issues, providing additional insight for investigations.

- Collect Logs for the Palo Alto Networks 6 App
- Install the Palo Alto Networks 6 App and View the Dashboards
• Palo Alto Networks 8

The Palo Alto Networks 8 App gives you visibility into firewall and traps activity, including information about firewall configuration changes, details about rejected and accepted firewall traffic, traffic events that match the Correlation Objects and Security Profiles you have configured in PAN, and events logged by the Traps Endpoint Security Manager.

- Collect Logs for the Palo Alto Networks 8 App
- Install the Palo Alto Networks 8 App and View the Dashboards

• Palo Alto Networks 9

The Sumo Logic App for Palo Alto Networks 9 utilizes PANOS 9 new features in predefined dashboards to provide extensive security analytics throughout your Palo Alto Networks environment. Palo Alto Networks 9 provides consistent protection across the data center, perimeter, branch, mobile and cloud networks.

- Collect logs for the Palo Alto Networks 9 App
- Install the Palo Alto Networks 9 App and view the Dashboards
• Threat Intel Quick Analysis

The Threat Intel Quick Analysis App correlates CrowdStrike’s threat intelligence data with your own log data, providing security analytics that helps you to detect threats in your environment, while also protecting against sophisticated and persistent cyber-attacks. The Threat Intel Quick Analysis App scans selected logs for threats based on IP, URL, domain, Hash 256, and email.

◦ Install the Threat Intel Quick Analysis App and view the Dashboards
◦ Threat Intel Optimization
◦ Threat Intel FAQ

• Trend Micro Deep Security

The Trend Micro Deep Security App works with system and security events to monitor event history such as anti-malware, IPS, web reputation, firewall, integrity and log inspection events.

◦ Collect on-premises logs for the Trend Micro Deep Security App
◦ Collect cloud-based logs for the Trend Micro Deep Security App
◦ Install the Trend Micro Deep Security App and view the Dashboards

• Twistlock

The Sumo Logic App for Twistlock provides comprehensive monitoring and analysis solution for detecting vulnerabilities and potential threats throughout your environment, including hosts, containers, images, registry.

◦ Collect logs for the Twistlock App
◦ Install the Twistlock App and view the Dashboards
The Zscaler Web Security App collects logs from Zscaler with Nanolog Streaming Service (NSS) to populate pre-configured searches and Dashboards. The dashboards provide easy-to-access visual insights into web traffic behaviors, security, user browsing activities, and risk.

- Collect Logs for the Zscaler Web Security App
- Install the Zscaler Web Security App and view the Dashboards