Google Cloud

splunk>

Enhancing Data Security with Splunk and Google Cloud

Google Cloud splunk>

Security is a growing business challenge.

One look at the headlines is enough to realize that security threats are increasing in size, number, frequency, and sophistication. As companies move along the path toward digital transformation, they must keep security top of mind. Doing this, however, can be a costly, time-consuming venture.

How can companies maintain the level of data security they need to protect themselves and customers while driving digital transformation, keeping costs under control and freeing up IT teams for more value-add work?

$10.5 trillion

The global cost of cybercrime already exceeds $6 trillion and is expected to reach $10.5 trillion by 2025.[1]

3.5 million

There's a serious cybersecurity talent crunch, with 3.5 million unfilled cybersecurity jobs globally, up from one million in 2014.[2]

[1] Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com)

[2] Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021 (cybersecurityventures.com)

Google Cloud splunk>

Google Cloud security fundamentals

Splunk works to enhance Google Cloud's extensive security measures by providing additional analysis and automated response so that IT security teams can work more efficiently. It starts with Google Cloud's advanced threat defense as well as security monitoring and alerts, including:

A robust security foundation to protect against threats

A wide and growing array of controls customers can utilize

Continuous improvement and compliance

Capabilities to make security and compliance easier for customers

Transparency and visibility as well as automation, blueprints, and infrastructure as code

Google's security-relevant cloud data

In addition to defending against threats, Google Cloud provides the visibility that customers need, including logs and alerts that help them respond to security issues quickly and efficiently. It's this information that Splunk processes to generate automated responses to threats. Google Cloud Dataflow transfers the necessary information from logs, security alerts, and asset changes to Splunk, which uses this information to prioritize alerts and automate responses.

The purpose-built Pub/Sub to Splunk Dataflow template with associated Terraform module supports real-time data streaming of Google Cloud security data to Splunk Enterprise or Splunk Cloud via Splunk HTTP Event Collector (HEC).

ESSENTIAL GOOGLE TOOLS AT THIS STAGE INCLUDE:

01

Cloud Logging, which includes Google Workspace audit logs, VPC flow logs, DNS logs, firewall logs, application logs, and more

02

Security Command Center, which leverages multiple purpose-built tools to alert users to such issues as security misconfigurations, anomalies that could indicate threats such as brute force SSH attacks or cryptomining, app vulnerabilities, and improperly stored sensitive data such as personally identifiable information (PII)

03

Cloud Asset Inventory, which lets users know when there are asset and metadata changes around cloud resources and associated permission policies

Map Google Cloud security data to the Splunk data model

Splunk Enterprise Security (ES) is a next-generation security information and event manager (SIEM) built to detect multiple security issues based on the MITRE ATT&CK framework, a widely accepted knowledge base of adversary tactics and techniques based on real-world observations.

Splunk ES uses 49 Google Cloud-tailored correlation searches (detection rules) that cover cloud infrastructure and user activities. After Splunk ingests events data from Google Cloud, it parses and normalizes it to conform to the Splunk Common Information Model (CIM).

The Splunk Add-on for Google Cloud Platform includes automatic field extractions, sourcetype mappings for Google Cloud log data, and corresponding data models when applicable.

By normalizing Google Cloud-specific data formats, CIM data models greatly accelerate time to value as they:

Provide you with out-of-the-box threat detections and security dashboards

Enable you to create and share your own threat detections with custom correlation searches across all providers in your hybrid or multi-cloud environments

Accelerate correlation searches

Leverage data in Splunk to detect multiple types of threats

Splunk ES performs analysis on the incoming Google Cloud data to detect threats at both the user and infrastructure levels:

User activities being monitored include such actions as suspicious behavior, Google Cloud cross-account activity, suspicious authentications, access to sensitive Kubernetes objects, and other outlying access activities.

Network-level activity monitored by Splunk includes actions occurring on customer infrastructure, such as suspicious provisioning activities, open storage buckets, anomalous Kubernetes sensitive roles or scanning activity, unexpected container implementation, crypto mining, and suspicious DNS traffic.

The Splunk Security Essentials App includes 25-plus sample Splunk searches for the detection of threats in your Google Cloud (and multi-cloud) environment to get your SIEM deployment off to a running start.

Google Cloud splunk>

Automate response with Splunk SOAR

Splunk SOAR is Splunk's security orchestration and automation platform. After reducing the time it takes to detect a threat, the next step is to reduce the threat-response time. This is accomplished with the use of the Splunk SOAR. Automated response in Splunk SOAR is accomplished by authoring playbooks using actions in Splunk SOAR apps for third-party technologies.

Chronicle App for Splunk SOAR (published by Google) enables end-users to search, analyze, and ingest the enterprise security data stored in Chronicle.

Google Cloud IAM (published by Splunk) integrates with Google Cloud IAM API to support various investigation and mitigation actions like disabling service accounts, and delete associated keys.

Google Cloud Compute Engine app (published by Splunk) integrates with Google Cloud Compute Engine API to support investigation and remediation actions.

Google Cloud Storage app (published by Splunk) integrates with Google Cloud Storage API to support various investigation and mitigation actions.

G Suite for Drive app (published by Splunk) allows various file manipulation actions to be performed on Google Drive.

G Suite for GMail app (published by Splunk) integrates with G Suite for various investigative and containment actions.

To learn more about how Google Cloud and Splunk can enhance your threat prevention, detection, and response practices, tune in to our webinar, "Enhance Your Threat Prevention, Detection, and Response with Splunk and Google Cloud."

Google Cloud splunk>