Demisto And Splunk For Automated Data Enrichment

Benefits

• Extract new insight from existing security architectures

• Improve investigations with more context from key security and IT domains

• Automate incident response and playbook-driven triage of security alerts

• Shorten decision-making cycle by automating key tasks with analyst review

Compatibility

• Products: Splunk Cloud, Splunk Enterprise

• Splunk Versions: 6.5, 6.4, 6.3

• Platform: Platform Independent

New forms of sophisticated cybersecurity threats continually emerge to target enterprises in novel ways, utilizing multiple attack vectors. When investigating a security event or breach, users can now enrich Splunk’s correlated alerts and notables’ data through Demisto Enterprise’s orchestration capabilities.

Demisto Add-on for Splunk allows users to trigger specific playbooks to gather information about Splunk ES events, take actions on point products with the help of the Adaptive Response Framework, and manage the complete incident lifecycle within Demisto Enterprise.

Demisto App for Splunk helps in tracking Splunk-to-Demisto incident metrics. It visually displays all saved searches and relevant incident details, providing users a succinct summary of incidents created from Splunk into Demisto Enterprise.
EXTRACTING CONTEXT FROM INVESTIGATION DATA

Challenge: During investigations, analysts need to check indicators, find out whether they are malicious, and weave a contextual thread through the endless holes of data at their disposal. Faced with many indicators sans context, this can be a repetitive and time-consuming process.

Solution: After ingesting incidents from Splunk ES, Demisto uses hypersearch to give analysts critical context about the indicators associated with an incident. Analysts can view indicator malice, repeating patterns, and cross-correlations at a glance in both the work plan and war room windows.

Benefit: Contextual viewing of data allows for quicker identification of remediation procedures and running the respective playbooks/actions to curtail the incident.

USE CASE #2

CUSTOMIZED ENRICHMENT FOR INCIDENTS

Challenge: No two incidents are equal, with each incident having different metrics and labels considered important for analysis and reporting. Analysts face challenges across the board with incident ingestion, especially with low number of default labels transferred and tough mapping procedures.

Solution: While ingesting incidents from Splunk ES to Demisto, all 111 labels will be captured by default. Analysts can also easily map Splunk labels to Demisto incident fields and request for a specific number of labels to be captured depending on the incident at hand.

Benefit: A large number of labels transferred by default allows for comprehensive enrichment of incidents. Intuitive mapping lets analysts customize incident labels according to relevance and needs, giving them better initial context to deal with incidents.

ABOUT SPLUNK ENTERPRISE

Do you want to get more value from your data? Splunk Enterprise collects data from any source, including logs, clickstreams, sensors, stream network traffic, web servers, custom applications, hypervisors, containers, social media and cloud services. It then enables you to search, monitor and analyze that data to discover powerful insights across multiple use cases like security, IT operations, application delivery, industrial data and IoT, giving you valuable intelligence across your entire organization. To know more, check the product brief here: [https://www.splunk.com/pdfs/product-briefs/splunk-enterprise.pdf](https://www.splunk.com/pdfs/product-briefs/splunk-enterprise.pdf)

ABOUT DEMISTO

Demisto Enterprise is the first and only comprehensive Security Operations Platform to combine security orchestration, incident management, machine learning from analyst activities, and interactive investigation. Demisto's orchestration engine automates security product tasks and weaves in the human analyst tasks and workflows. Demisto enables security teams to reduce mean time to resolution (MTTR), create consistent incident management process, and increase analyst productivity. Demisto is backed by Accel and other prominent investors and has offices in Silicon Valley and Tel Aviv. For more information, visit [www.demisto.com](http://www.demisto.com) or email [info@demisto.com](mailto:info@demisto.com).