Cylance PROTECT®

Powered By ADAPTIVE RESPONSE SPLUNK APP

Real-Time Threat Monitoring and Analysis Made Easy

Today's business enterprise requires big data security solutions that can adapt to advanced threats and changing demands. Simple static monitoring of traditional security events is no longer enough. Security practitioners need broader, real-time insights from data sources generated at massive scale across IT, the business, and in the cloud. These enterprises need to stay ahead of external attacks, malicious insiders, and costly ransomware demands using continuous security and compliance monitoring.

CylancePROTECT, the world's leading threat prevention solution, integrates with Splunk Enterprise analytics to quickly investigate and respond to known, unknown, and advanced threats.

The integration of CylancePROTECT data into Splunk Enterprise enables organizations to tap into the value of machine learning. Security operations teams can better understand the threats in their environment by taking advantage of context and visual insights based on predictive modeling. Team members at all levels of the organization can understand trends, patterns, and behavior to make more informed decisions about their security.

Whether being used to search for threat details or metrics, the CylancePROTECT Splunk App provides more visibility into the organization's environment to detect and mitigate advanced threats.

Benefits of the CylancePROTECT Splunk App

- Perform sophisticated analytics to investigate and respond to threats by taking actions directly from the Splunk Console using Splunk's Adaptive Response Framework
- Search, monitor, correlate, and analyze high-risk threat details for fast incident response
- Monitor systems and infrastructure in real time to preempt issues before they happen
- Understand trends, patterns of activity, and behavior to make more informed decisions through custom searches, reports, and alerts
- Drive operational security excellence across the entire organization through deep threat analytics
- Integrate detailed threat data into your security operations environment
- Search across all Cylance data from threat data reports and syslog events

About Cylance

Cylance® uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.

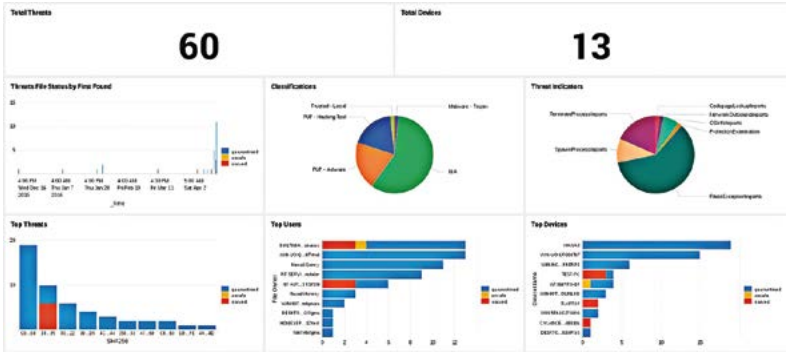

Figure 1 — CylancePROTECT threat details displayed in Splunk Enterprise dashboard

Feature	Description
Threat Overview	▪ Heads-up display for SOC awareness ▪ Overview of all detection categories ▪ Ability to drill down into areas of concern
Cylance Search	▪ Search by hash and/or device name ▪ View file names and status ▪ Classify threats (PUPs, etc.)
Threat Center	▪ Configure threat metrics and reports according to time, including all time, last 30 days, last 7 days, last 24 hours, or a custom user-defined period ▪ Filter and search by threat classifications, threat indicators, files status, etc.
Operations Center	▪ View all registered devices ▪ Monitor device status (online/offline), agent versions, policy and zone assignments, etc.
Searches and Reports	▪ Threat details ▪ Infected hosts ▪ New threats ▪ Online and offline devices ▪ Duplicate devices ▪ Agent versions
Syslog Events Integration	▪ Threats ▪ Devices ▪ Audit logs ▪ Memory protection ▪ Threat classifications ▪ Cylance Script Control ▪ Cylance Application Control ▪ Cylance Device Control

Requirements

Operating Systems

- CentOS7 (64-bit)
- Red Hat Enterprise Linux 7.2 Server (64-bit)
- Ubuntu 14.04 (64-bit)
- Windows Server 2012 R2 (64-bit)

Splunk Requirements

- Products: Splunk Cloud, Splunk Enterprise
  - Versions: 7.1, 7.0, 6.6, 6.5, 6.4, 6.3, 6.2, 6.1, 6.0
- Platform: Platform Independent CIM
  - Versions: 4.9, 4.8, 4.7, 4.6, 4.5, 4.4, 4.3, 4.2, 4.1, 4.0

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE

20180911-1124