CylancePROTECT®
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. Stay ahead of external attacks, malicious insiders, and costly fraud 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 the security.

Whether being used to search for threat hash values or metrics, the CylancePROTECT Splunk App provides more visibility into the threat landscape to mitigate advanced threats.

Benefits of the CylancePROTECT Splunk App:

- Search, monitor 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

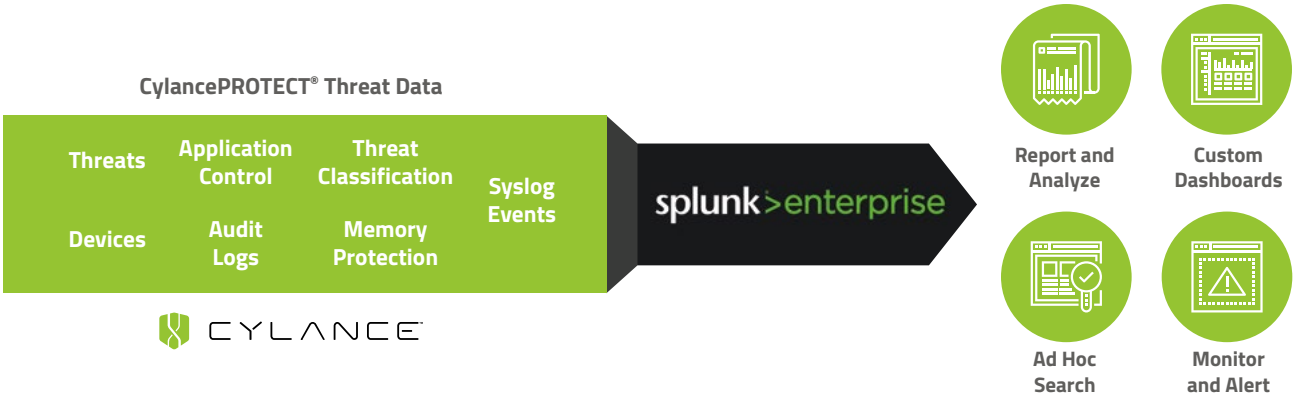

Figure 1 – CylancePROTECT threat details displayed in Splunk Enterprise dashboard

Feature	Description
Cylance Search	▪ Search by hash and/or device name ▪ View file names and status ▪ Classify threats (PUP, etc.)
Threat Center	▪ Configure threat metrics and reports according to time, including all time, last 30 days, last 7 days, last 24 hours, etc. ▪ 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 & Reports	▪ Threat details ▪ Infected hosts ▪ New threats ▪ Online and offline devices ▪ Duplicate devices ▪ Agent versions
Syslog Events Integration	▪ Threats ▪ Devices ▪ Memory protection ▪ Threat classifications ▪ Cylance Script Control ▪ Cylance Application Control ▪ Audit logs

SYSTEM REQUIREMENTS

1. Operating Systems

a. CentOS7 (64-bit)
b. Red Hat Enterprise Linux 7.2 Server (64-bit)
c. Ubuntu 14.04 (64-bit)
d. Windows Server 2012 R2 (64-bit)

2. Splunk Version

a.Splunk Enterprise 6.3.x

About Cylance

Cylance is the only company to offer a preventive cybersecurity solution that stops advanced threats and malware at the most vulnerable point: the endpoint. Applying a revolutionary artificial intelligence approach, the Cylance endpoint security solution, CylancePROTECT, analyzes the DNA of code prior to its execution on the endpoint to find and prevent threats others can't, while using a fraction of the system resources associated with endpoint antivirus and detect and respond solutions that are deployed in enterprises today. For more information, visit www.cylance.com

1.844.CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Ave., Suite 700, Irvine, CA 92612