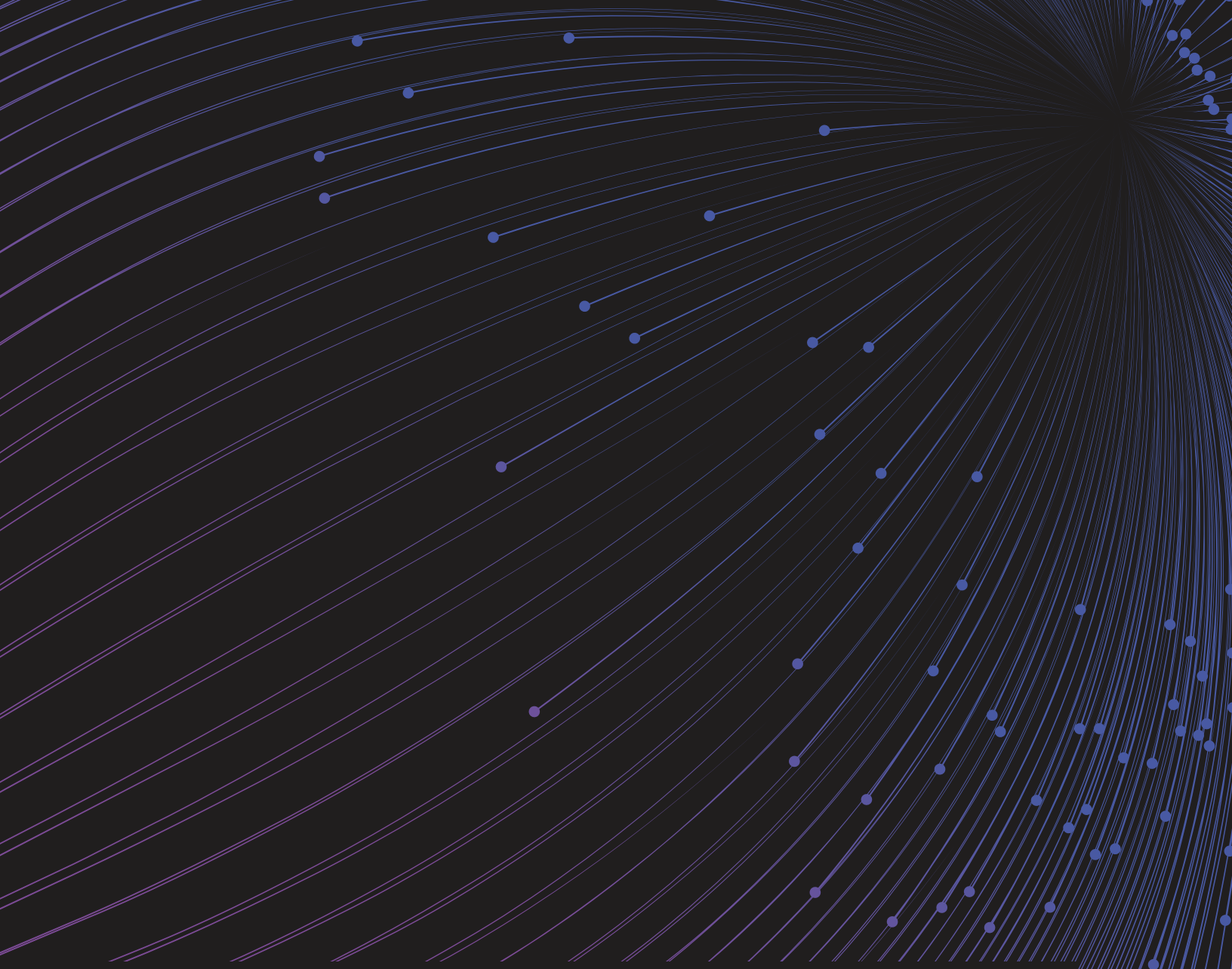

Cylance® and Phantom Partner To Optimize Security Operations

Allowing for Faster Response Times To Alerts and Investigations

CYLANCE

Phantom

Introduction

Cylance and Phantom help customers improve their Security Operations Center (SOC) by automating work flow tasks and improving accuracy and response time to alerts and investigations.

Value Statement

The integration of Cylance and Phantom allows organizations to apply true prevention of modern threats while closing the security gap. This is accomplished by enabling enterprise security operations to be smarter, faster, and stronger through orchestrating key stages of security operations from prevention to triage and resolution, delivering dramatic increases in productivity and effectiveness. Cylance's endpoint intelligence contributes to the creation of automated playbooks that can execute at machine speed for all the phases of a threat response, including investigation, mitigation, hunting, containment, and remediation.

The results are increased overall security, decreased incident response and dwell times, and increased ROI on security operations.

Use Cases

Lower Mean Time To Respond (MTTR) To Alerts

- Challenge: SOC analysts must sort through and prioritize thousands of alerts then perform investigations involving research and correlation which can take a significant amount of time and are prone to error.
- Solution: With Cylance's prevention-first methodology, which lowers noise, along with Phantom's Orchestration and Automation Platform that can automate all data aspects, and operations and response actions of alert-based workflows, customers can respond faster with greater efficiency and accuracy to modern threats.
- Additional Benefit: With the above solution, SOC analysts will get more time back to perform more important tasks for the security organization. Also, the SOC team will experience less endpoint infections and alerts, operationally requiring less remediation and re-imaging.

DATA Enrichment/Incident Response

- Challenge: SOC analysts must collect, correlate, and analyze alert information which is time consuming, and prone to error and inconsistencies.
- Solution: Utilizing a CylancePROTECT® threat event as a trigger, Phantom captures full ecosystem environmental meta-data related to the incident (including Cylance data over APIs) so analysts can respond faster and with more accuracy. This amounts to full ecosystem capture, not just an expanded data set from the security device on which the incident originated.
- Additional Benefits: Phantom can respond automatically to update Cylance devices/policies.

About Cylance

Cylance uses artificial intelligence to deliver prevention-first security solutions and specialized services that change the way organizations approach endpoint security. Cylance security solutions combine AI-driven predictive prevention with dynamic threat detection and response to deliver full spectrum threat prevention and threat visibility across the enterprise. Visit www.cylance.com for more information.

About Phantom

Phantom was the first Security Automation & Orchestration (SAO) product on the market in 2016 and is the winner of the RSA Sandbox Innovation Award. Phantom integrations provide customers with the connective tissue to several siloed security point solutions.

API-Enabled Integrated Workflows	Description
Data Enrichment	Threat information is communicated from CylancePROTECT to the Phantom dashboard with selectable levels of details.
Malware Analysis	CylancePROTECT leverages AI to detect and quarantine a malicious file. Phantom receives the threat details as well as a download of the malicious file to another security device, such as a sandbox, for further analysis. The results are aggregated with existing file details in the Phantom dashboard.
Environment Check/Update	Highlight the areas of high risk by filtering for devices that satisfy Cylance's "is_Safe" condition. Users can use this check for all devices, or just one, and take automated subsequent actions in a Phantom playbook.
Blacklisting	Given a hash, Phantom can update the Cylance blacklist. The hash can come from a Cylance detection or somewhere else (FW, CERT list, etc.).
Malware Hunting	Given a hash, Phantom can search Cylance endpoints to see if the hash has been seen. The hash can come from a Cylance detection or another device, CERT list, etc.
Policy/Zone Orchestration	Following an alert, Phantom can update/alter Cylance policies and device groupings without leaving the Phantom interface.

Phantom Console Dashboard showing Events, Analyst Workloads, and Playbook Status.

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

CYLANCE

20180914-0422