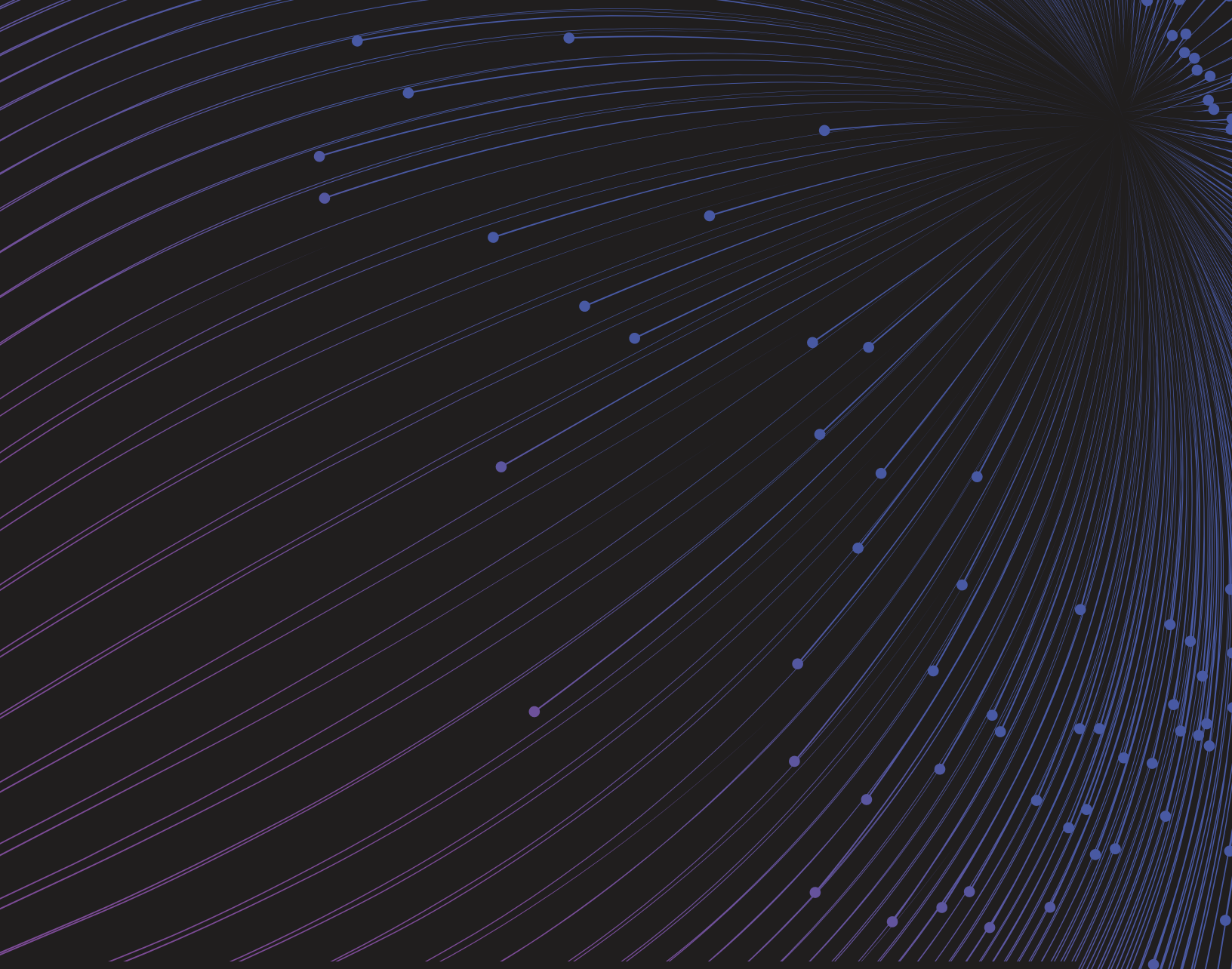

Cylance® and Demisto To Enable the SOC To Automate and Orchestrate Security Operations

Allowing for More Accurate and Faster Response To Alerts

CYLANCE DEMISTO

Introduction

Cylance and Demisto formed a technology alliance to help customers improve their Security Operations Center (SOC) by automating workflow tasks, improving accuracy and response time to alerts and investigations.

Value Statement

The integration between Cylance and Demisto allows organizations to automate significant portions of the alert workflow, allowing security analysts to concentrate on more important decisions, freeing up their time to focus on more critical tasks.

Executives want to know that their organization's assets, people, and property are protected. Whenever there is a new emerging threat, there is always the question of, "Are we protected?" The predictive advantage of protection offered by CylancePROTECT® is leveraged in Demisto Enterprise.

Furthermore, SOC managers can optimize the entire incident life-cycle while auto documenting and journaling all the supporting evidence. Answering the question, "Are we protected?" has never been so easy.

For too long, fearing inadequate collaborating data, SOC analysts have had to switch between several application views to build a story and make decisions around every incident. Through the Cylance-Demisto technology alliance, Cylance technology seamlessly communicates a rich data feed about malicious activity to Demisto. This enriched data is corroborated with other key findings based on automated playbooks, building out an accurate and dependable evidence board and incident timeline. With the Cylance-Demisto technology alliance, customers can expect to see a measured increase in prevention, protection, and ease of threat management.

Use Cases

Lower Mean Time To Respond (MTTR) To Alerts

- Challenge: With the sheer scale of alerts facing modern organizations, sorting and prioritizing alerts can be a challenge for most SOC teams.
- Solution: With Cylance's prevention-first methodology, which lowers noise (therefore less infections, alerts, and remediations), and Demisto's Automation and Orchestration Platform that can automate all aspects of security workflows and response actions, security organizations can respond with much greater speed and accuracy to threats.
- Additional Benefit: SOC analysts will be able to focus on more important tasks for the security organization with the time they save.

DATA Enrichment/Incident Response

- Challenge: SOC analysts are often overwhelmed with the amount of data they must collect and analyze for alerts which can be time consuming and prone to error.
- Solution: Once an alert is received from Cylance technology, Demisto will obtain full ecosystem data related to the incident, including data enrichment over Cylance APIs. This allows SOC analysts to respond to important alerts faster and with more accuracy.
- Additional Benefit: Through Demisto, automated responses can be used over the Cylance API 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 Demisto

Demisto Enterprise Security Orchestration Platform delivers a complete solution that helps **Tier-1 through Tier-3** analysts and **SOC managers** to optimize the entire incident life cycle while auto documenting and journaling all the evidence. More than 150 integrations enable security orchestration workflows for incident management and other critical security operation tasks.

API Driven Features	Description
Data Enrichment	Demisto can call the Cylance APIs to get threat, device, policy, and other information to update its dashboard. Demisto can also perform data enrichment to the rest of the environment for more information based on any alert or other workflow.
Environment Check/Update	Using Demisto, users can check devices via the Cylance API for up to date status on device date, threat details, alerts, etc.
Malware Analysis	CylancePROTECT detects a malicious binary and quarantines the file. Demisto calls the Cylance API frequently to get threat information and update its dashboard. Demisto downloads the quarantined malware via the Cylance User API, sends it to another security device, such as a sand box, for further analysis, then updates the results to its dashboard.
Blacklisting	Given a hash, update the Cylance blacklist. The hash can come from a Cylance detection or somewhere else (FW, CERT list, etc.).
Malware Hunting	Using a file hash, Demisto can search Cylance endpoints to see if the hash has been seen. The hash can come from Cylance or another device, CERT list, etc.
Policy/Zone Orchestration	Following an alert, Demisto can update/alter Cylance policies and device groupings.

Demisto Dashboard for Security Alerts, Active Incident Workflow, and Ecosystem Status.

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

CYLANCE

20180914-0422