PALO ALTO NETWORKS AND SIEMPLIFY

Security Orchestration, Automation and Response

Resource-constrained security operations teams are under pressure to investigate and respond to an unprecedented volume of alerts in the hope of detecting and containing the next cyberattack. But incident response processes are mostly manual, and analysts rely on a growing number of disparate tools and multiple consoles for alert triage, investigation and remediation.

HIGHLIGHTS

- Automate and orchestrate response processes for faster triage, investigation and remediation.
- Seamlessly integrate Palo Alto Networks actions, such as URL or application blocking, as part of automated playbooks.
- Automatically enrich alerts with AutoFocus threat intelligence.

Siemplify Security Orchestration and Automation Platform

The Siemplify® platform uniquely combines security orchestration and automation delivered through a holistic security operations workbench. Developed by analysts, for analysts, Siemplify's platform enables security teams to work from a single pane of glass to manage the tools needed to triage alerts as well as investigate and remediate threats.

- **Reduce alert overload:** Address cases made up of related alerts instead of weeding through individual alerts.
- **Resolve more cases, more quickly:** Automate workflows and repetitive tasks to accelerate response and focus analyst time on higher-value activities.
- **Gain deeper insight:** Apply context to alerts for a threat storyline that illuminates the who, what and when of a security event.
- **Work more efficiently:** Orchestrate and manage disparate technologies from a single console.
- **Create consistent processes:** Document processes to retain internal knowledge using a drag-and-drop playbook builder.
- **Track, measure and improve:** Define and monitor security operations KPIs and create automated reports.

Palo Alto Networks

Palo Alto Networks® Security Operating Platform enables enterprises, service providers and governments to protect our digital way of life with a prevention-first approach to cybersecurity. The platform comprises multiple natively integrated and centrally managed technologies. Among them:

- **WildFire® cloud-based threat analysis service** is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware. The service employs a unique multi-technique approach, combining dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats.
- **AutoFocus™ contextual threat intelligence service** accelerates analysis, correlation and prevention workflows. Unique, targeted attacks are automatically prioritized with full context, allowing security teams to respond to critical attacks more quickly without the need for additional IT security resources.
- **Next-Generation Firewall with Threat Prevention** identifies and controls users and applications flowing across both physical and cloud-based networks, enforces granular security policies, and inspects files and URLs for known and unknown threats.
- **Traps™ advanced endpoint protection** replaces traditional antivirus with multi-method prevention, a proprietary combination of purpose-built malware and exploit prevention methods that protects users and endpoints from known and unknown threats, making use of constant updates from the Palo Alto Networks threat intelligence cloud.

Palo Alto Networks and Siemplify

The integration between Palo Alto Networks and Siemplify enables security analysts to seamlessly integrate Palo Alto Networks Next-Generation Firewall and threat intelligence functionality as part of automated security playbooks for richer investigation and faster response.

USE CASE NO. 1

Automated Enrichment of Phishing Alerts

Challenge

When investigating alerts about suspected phishing attacks, analysts typically manually query threat intelligence services, such as AutoFocus, for additional insight. An analyst may check the validity of a sender URL or examine a checksum of an attachment to determine if it has been used in known phishing attacks. These manual parses and queries are mundane and repetitive tasks that waste precious analyst time and increase mean time to respond.

Answer

Siemplify's out-of-the-box playbooks and Palo Alto Networks integration can automatically enrich every phishing alert with relevant information from AutoFocus, saving precious time and allowing analysts to focus on decision-making rather than data collection.

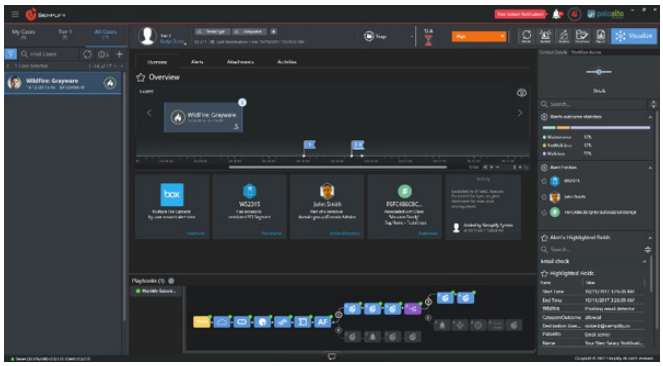

Figure 1: Siemplify – analyst assessment

Additional Benefit

Analysts can free up even more time by creating playbooks that automatically close phishing alerts as false positives if AutoFocus determines all relevant parameters, such as the recipient domain, URLs and attachments, to be non-malicious.

USE CASE NO. 2

Automated Rapid Response to an Attack

Challenge

When analysts determine that malicious activity has occurred on the network, they need to take remedial action as quickly as possible. SOC analysts typically lack the expertise to conduct such activities across a set of disparate technologies, meaning urgent remedial actions are delayed due to cumbersome communication and manual execution.

Answer

The Siemplify security orchestration and automation platform acts as a central workbench for the SOC analyst, allowing for instant and automated execution of remedial activities. Through its Palo Alto Networks API-based integration, analysts can execute remedial activities at the click of a button or via automated playbooks without deep knowledge of the underlying technology.

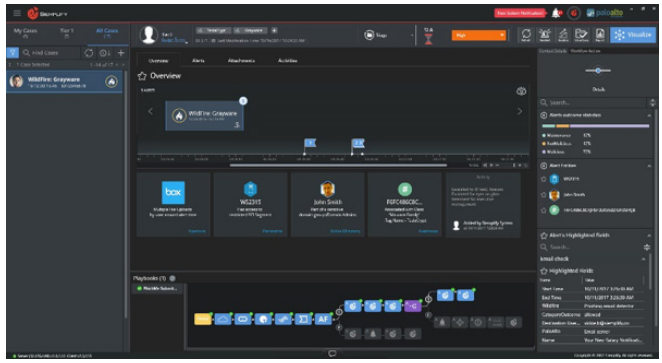

Figure 2: Siemplify – orchestrate response

Additional Benefit

On top of conducting remedial actions, playbooks can automatically update threat intelligence platforms with malicious URLs and applications to improve their accuracy.

About Siemplify

Siemplify provides a holistic security operations platform that empowers security analysts to work smarter and respond faster. Siemplify uniquely combines security orchestration and automation with patented contextual investigation and case management to deliver intuitive, consistent and measurable security operations processes. Leading enterprises and MSSPs leverage Siemplify as their SOC workbench, tripling analyst productivity by automating repetitive tasks and bringing together disparate security technologies. Founded by Israeli Defense Force security operations experts, Siemplify is headquartered in New York with offices in Tel-Aviv. Learn more at www.siemplify.co.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com