SOLUTION BRIEF

Fortinet And Siemplify Security Orchestration

Broad, integrated and automated security with simplified and automated orchestration, and incident response

Challenges

Resource-constrained security operations teams are constantly 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.

Joint Solution Description

The Fortinet and Siemplify integrated solution addresses the above challenges by leveraging the Fortinet Security Fabric. The Fortinet Security Fabric is designed around a series of open APIs, Open Authentication Technology, and standardized telemetry data to enable organizations to seamlessly integrate existing security technologies via open interfaces and provide uncompromising security. The joint solution combines advanced security automation, orchestration and response capabilities from Siemplify with industryleading security protection from Fortinet to deliver unparalled security and streamlined security operations.

Because Siemplify leverages the open ecosystem of the Fortinet security fabric, organizations gain broad protection and visibility to every network segment, device, and application, whether virtual, in the cloud, or on-premise. By seamlessly managing and orchestrating different security tools, Siemplify enables security teams to gain a full understanding of the various entities involved in a security event and the relationship between them, the activities that occur in each part of the affected system and the timeline of the events, assets and artifacts involved to understand the full threat storyline.

Joint Solution Benefits

- Automate and orchestrate incident response processes for faster triage, investigation and remediation
- Enhanced visibility into available policies with automated playbooks for rapid incident response
- One network security operating system and unified policy management with Fortinet's FortiGate integration
- Automated blocking/unblocking of malicious IP addresses with FortiGate integration
- Protection against advanced threats, including zero-day attacks with Fortinet's FortiGuard Security Subscription Services

The Siemplify platform uniquely combines security orchestration and automation delivered through a holistic security operations workbench. Developed by security operations experts, 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. This enables analysts to resolve issues faster with minimal effort.

- **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.

Siemplify uniquely combines security orchestration and automation with patented contextual investigation and case management to deliver intuitive, consistent and measurable security operations processes.

Siemplify Security Orchestration and Automation Platform

The Siemplify Security Orchestration and Automation Platform is a holistic, purpose-built security operations workbench that provides SOC teams the deep insights they need to take fast, decisive action against cyberthreats. From triage and investigation to collaboration and remediation, Siemplify serves as the foundation for day-today security operations and incident response activities. By using Siemplify, SOC teams can reduce their analyst caseload by 80% and their mean time to respond by up to 70%.

Fortinet FortiGate Enterprise Firewall

The Fortinet FortiGate network security platform provides high performance, layered security services and granular visibility for end to end protection across the entire enterprise network. Innovative security processor (SPU) technology delivers high-performance application layer security services (NGFW, SSL inspection, and threat protection), coupled with the industry's fastest SSL inspection engine to help protect against malware hiding in SSL/TLS encrypted traffic. The platform also leverages global threat intelligence to protect individual customers, by using Fortinet's FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

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 Forces security operations experts,

Siemplify is headquartered in New York with offices in Tel Aviv.
www.siemplify.co

FORTINET

www.fortinet.com

June 8, 2019 5:27 AM

D:\Fortinet\Solution Brief\TEAL SB\Fortinet Siemplify\FA - SB - Fortinet Siemplify

292956-A-0-EN