SOLUTION BRIEF

Eliminate Alert Overload and Automate Incident Response

Pair real-time visibility with security automation, orchestration and response

Security orchestration and automation from Siemplify can help security teams get even more benefit from their McAfee Enterprise Security Manager investment by streamlining alerts, automating repetitive security operations processes and speeding up incident response.

McAfee Compatible Solution

- Siemplify Security Orchestration and Automation Platform
- Integrates with McAfee Enterprise Security Manager (ESM)

The Business Problem

As the threat landscape expands, analysts rely on an increasing number of disparate tools and multiple consoles for alert triage, investigation and remediation. Security operations teams are under pressure to investigate and respond to an unprecedented volume of alerts from these tools in the hope of detecting and containing the next cyberattack. And, in most cases, these incident response processes are largely manual, leaving teams more resource constrained than ever.

McAfee & Siemplify Security Orchestration and Automation Platform

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

- **Reduce alert overload –** address cases of related alerts instead of weeding through individual alerts
- **Resolve more cases, faster –** automate workflows and repetitive tasks
- **Gain deeper insight –** context applied to alerts illuminates the who, what and when of a security event
- **Work more efficiently –** manage and orchestrate disparate tools from a single console
- **Create consistent processes –** document processes using a drag-and-drop playbook builder
- **Track, measure and improve –** define and monitor security operations KPIs and create automated reports

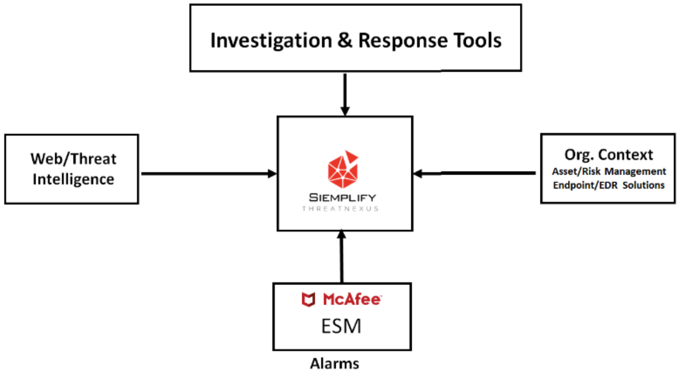
The integration between McAfee Enterprise Security Manager and Siemplify enables security analysts to increase their productivity and reduce the time to respond to threats.

Alert Grouping and Automated Enrichment

As multiple alerts from different security controls are generated, Siemplify automatically consolidates and groups the different alerts from the various tools into one cohesive interface. The platform then automatically enriches these alerts with other important data sources within the ecosystem and provides analysts with the means to quickly and effectively triage, improving analyst productivity.

Automated Rapid Response to an Attack

Remediation actions such as blocking URLs or applications, and tuning policies need to happen quickly once malicious activity has been confirmed. Siemplify acts as a central workbench for the SOC analyst and allows for instant and automated execution of remediation activities throughout an environment.



Challenges

Too many tools, not enough people

- Alert overload from disparate technologies
- Teams lack enough staffing, budget and time to address all alerts
- SOC processes are largely manual and rely on internal knowledge to execute

McAfee Solution

Real-time visibility plus orchestration and automation

- McAfee Enterprise Security Manager delivers real-time visibility into all activity on systems, networks, databases and applications
- Siemplify integrates with McAfee ESM to add context to alerts, enrich cases with additional data and automate triage and response processes

Results

Improved productivity, reduced time to remediate

- 80% case reduction
- 300% increase in caseload capacity
- 70% average reduction in mean time to respond (MTTR)

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. Learn more at www.siemplify.co

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

Learn More

For more information or to start an evaluation of McAfee Enterprise Security Manager, contact your McAfee representative or channel partner, or visit **www.mcafee.com.**

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com