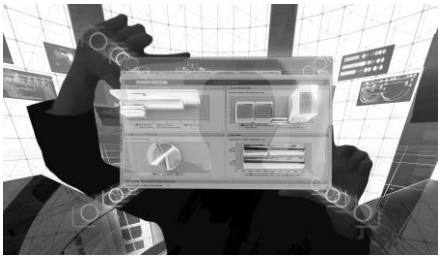
RSA SECURITY OPERATIONS MANAGEMENT

Orchestrate Intelligence, Process, and Resources in the SOC



AT-A-GLANCE

- Centralize incident management for security incidents
- Effective incident response for security incidents
- Optimize SOC investments
- Monitor and measure SOC KPIs
- Manage the overall SOC program including shift management, team capabilities, and security control effectiveness

CHALLENGES

Advanced Persistent Threats (APTs) are the one constant and enterprises are centralizing incident-response teams to detect and respond to them. The Security Operations Center (SOC) is the centralized incident-response team reporting through the CSO/CISO and consisting of people, process, and technology.

As customers design and deploy a SOC, there are challenges. Today, SOCs are event-focused and reactive because there is no centralization of alerts and incident management. Additionally, the incident-response team lacks business context, process, and people collaboration.

As customers implement SOCs, a framework is required to seamlessly orchestrate the multiple roles, processes, and technologies. This framework should transform the overall SOC to be a consistent and predictable business process.

SOLUTION

RSA Security Operations Management (SecOps) enables enterprises to seamlessly orchestrate people, process, and technology to effectively detect and respond to security incidents. Architected and designed by benchmarking world-class Security Operations Centers, the solution is SOC process and persona focused. SecOps enables organizations to manage the overall incident response, breach response, and SOC program that is aligned to business risk.

From incident response to data-breach response, the SecOps solution enables organizations to manage the entire lifecycle with integrated business context and best practices aligned with industry standards. The incident analyst, breach coordinator, and SOC manager have full visibility into the entire process lifecycle with focused workflows, dashboards, and reports.

SOC Managers and the CISO can report on the overall effectiveness of the SOC program because they have full visibility into incidents and data breaches. Additionally, with intuitive dashboards, reports, and workflows, key stakeholders can be engaged throughout the incident-management process.

The overall process from alert to incident investigation is automated, including workflows and integration with security-monitoring systems for alert aggregation. From a remediation perspective, any security incident requiring action from IT operations could be automated by integrating SecOps with ticket-management systems.

Using SecOps, an enterprise can manage the overall SOC program as a consistent and predictable business process.

Key benefits of SecOps are as follows:

- An out-of-the-box solution for incident management and prioritization with workflows to guide the incident-response process.
- Centralized incident management with business context by aggregating alerts from multiple security-monitoring systems.
- Data-breach response to meet regional regulatory requirements by engaging key stakeholders and providing visibility to senior executives.
- Optimization of SOC investments by monitoring KPIs and measuring the effectiveness of security controls.
- Measurement and reporting on the SOC program through monitoring and dashboard KPIs that generate persona-based reports

KEY FUNCTIONALITY

– ***Incident Response***

RSA SecOps collects security alerts from various security controls using standard protocols. SecOps provides a workflow-driven incident-response process with context, which is critical for an effective security-incident-management process. SecOps collects the context from different sources and makes it available to an analyst during the investigation of an incident. Additionally, RSA SecOps uses incident-management best practices aligned with industry standards.

– ***Breach Response***

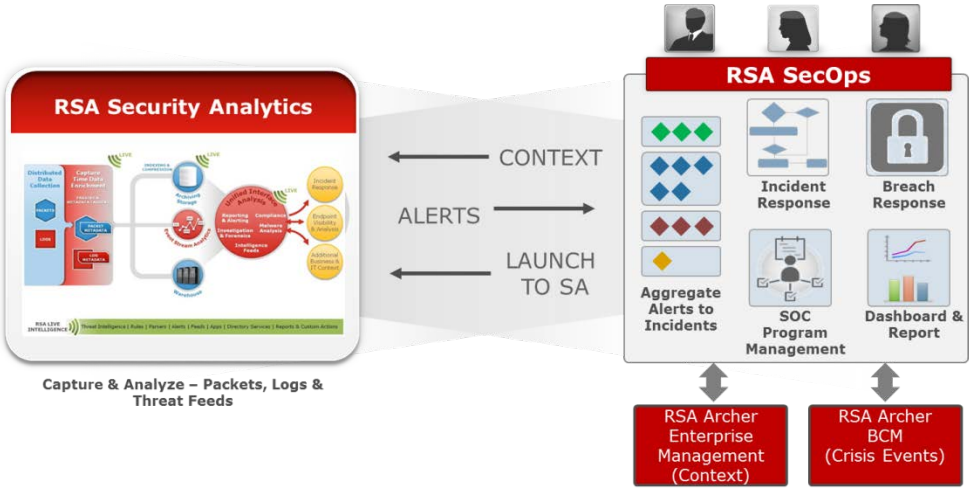
The RSA SecOps solution helps organizations manage breach-remediation tasks and procedures by engaging key stakeholders and providing visibility to senior executives.

– ***SOC Program Management***

RSA SecOps enables the SOC manager to effectively monitor SOC KPIs, measure control efficacy, and manage the overall SOC team.

– ***Business Risk Management***

RSA SecOps integrates OOTB with enterprise-risk-management solutions to assess the risk and business impact of security incidents and data breaches.



EMC², EMC, RSA, RSA Logo, RSA Archer and RSA Archer logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners. ©2013 EMC Corporation. All rights reserved. Published in the USA. 10/13 H12427

www.rs .com