RSA NetWitness® SecOps Manager

Automation and Orchestration for the Security Operations Center

OVERVIEW

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.

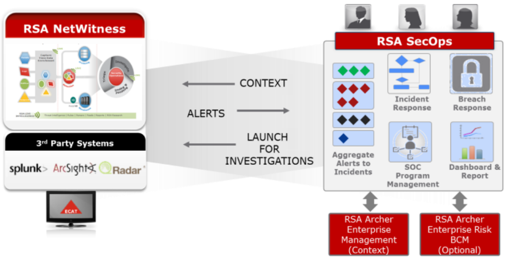
As customers design and deploy a SOC, there are challenges. Today, SOCs are event- focused and reactive because there is no centralization of alerts and incident management. Additionally, the incident-response team lacks business context, process, and people collaboration.

As customers implement SOCs, a solution is required to help better prioritize, investigate and respond to security incidents by automating and orchestrating people, process and technology in a repeatable way.

SECURITY OPERATIONS MANAGEMENT

A Security Operations Center (SOC) is comprised of people, process and technology. The orchestration of people, process and technology increases the effectiveness of the overall SOC program. Investing in technology and considering how the three aspects of the SOC work together is an effective strategy. Orchestration and framework can increase the return on investment and maximize the value of resources in a SOC implementation.

RSA NetWitness SecOps Manager provides the orchestration and framework for the SOC. It integrates with RSA NetWitness Logs and Packets, RSA NetWitness Endpoint and other 3-rd party security monitoring systems, aggregating events/alerts/incidents and managing the overall incident response workflow.



The workflow and capturing incident information is aligned with industry best standards such as NIST, US-CERT, SANS and VERIS. RSA NetWitness SecOps Manager caters to the multiple personas within the SOC from the analysts, incident coordinators, SOC manager and CISO providing a view on the overall effectiveness of the SOC program. By leveraging the Incident Response, Breach Response and SOC Program Management capabilities of RSA NetWitness SecOps Manager, an organization can guarantee that the overall security incident response functionality is being managed as an effective, predictable and consistent process.

KEY FUNCTIONALITY OF RSA NETWITNESS SECOPS MANAGER

RSA NetWitness SecOps Manager has three key functions:

- **Incident Response** – RSA NetWitness SecOps Manager aggregates events/alerts/incidents from various security monitoring systems using standard protocols. RSA NetWitness SecOps Manager provides the required workflow to triage, investigate, escalate, and effectively remediate the security incident. The response procedure library can be customized based on the threat category of the incident. Additionally, the incidents are prioritized with business context so the analysts investigate the incidents that pose the biggest risk to the organization.
- **Breach Response –** When an incident is escalated and categorized as a data breach, RSA NetWitness SecOps Manager enables organizations to manage the overall breach response process. Incident and breach information is protected and shared with stakeholders that have a need to know. Additionally, RSA NetWitness SecOps Manager helps organizations assess the Confidentiality, Impact and Availability (CIA) of the breach in order to develop an effective breach response plan. Breach response procedures can be pre-populated in the response procedure library, so organizations are prepared when an incident

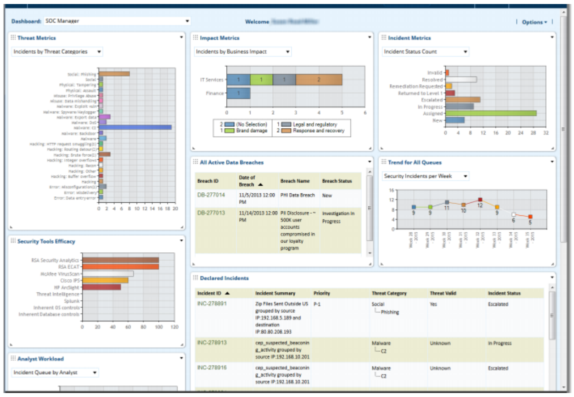
leads to a breach.

- **SOC Program Management –** RSA NetWitness SecOps Manager enables organizations to manage the overall effectiveness of SOC team from resources, scheduling, contacts, security controls efficacy and shift-handoff.

Customers leveraging the SOC Program Management functionality can assure that the overall SOC program is being managed as an effective, consistent and predictable process.

PERSONA DRIVEN SOLUTION

RSA NetWitness SecOps Manager is designed and architected by benchmarking world-class Security Operations Centers. The solution is SOC process and persona focused. As such, Out-of-the-Box, SecOps Manager workflow, reports, dashboards and KPIs cater to the SOC personas including the analysts, Incident Coordinators, SOC Manager, Breach Coordinator and CISO.



All Active Data Breaches

Breach ID	Date of Breach ▲	Breach Name	Breach Status
DB-277014	11/5/2013 12:00 PM	PHI Data Breach	New
DB-277013	11/14/2013 12:00 PM	PII Disclosure - ~ 500K user accounts compromised in our loyalty program	Investigation in Progress

Declared Incidents

Incident ID ▲	Incident Summary	Priority	Threat Category	Threat Valid	Incident Status
INC-278891	Zip Files Sent Outside US grouped by source IP:192.168.5.189 and destination IP:80.80.208.193	P-1	Social └ Phishing	Yes	Escalated
INC-278913	cep_suspected_beaconing_activity grouped by source IP:192.168.10.201		Malware └ C2	Unknown	In Progress
INC-278916	cep_suspected_beaconing_activity grouped by source IP:192.168.10.201		Malware └ C2	Unknown	Escalated

RSA NETWITNESS SECOPS MANAGER TIME TO VALUE

RSA NetWitness SecOps Manager's capabilities enable organizations to effectively operate a SOC by orchestrating people, process and technology. As such, capabilities such as Incident Response, Breach Response and SOC Program Management are core to the RSA NetWitness SecOps Manager solution.

RSA NetWitness SecOps Manager can be customized and deployed in customer environments based on the immediate needs and priorities. For example, an early stage customer that is starting to build out their incident response capabilities might want to leverage the Incident Response functionality 1st. The Incident Response functionality will initially help organizations get really effective at responding to security incidents and managing the different analysts in the organization. As customers further mature their SOC deployment, they can leverage the additionally functionality of RSA NetWitness SecOps Manager. RSA NetWitness SecOps Manager is flexible so customers can prioritize and leverage the functionality that will bring immediate value to their SOC deployment.

ADVANCE CYBER DEFENSE (ACD) PRACTICE

The RSA ACD Practice is a set of professional services that helps organizations improve their security maturity and posture, and prepare for and respond to security incidents and to evolve with the threat environment. These services also help organizations develop strategies and tactics for building and improving their security operations programs, with a specific focus on the design and optimization of security operation centers (SOCs) or incident response teams as well as the effective use of threat intelligence.

The ACD practice can be leveraged by RSA NetWitness SecOps Manager customers to assess and prioritize their immediate Security Operations Center (SOC) requirements.

EMC2 , EMC, the EMC logo, RSA, the RSA logo, and Archer are registered trademarks or trademarks of EMC Corporation in the United States and other countries. VMware is a registered trademark or trademark of VMware, Inc., in the United States and other jurisdictions. © Copyright 2016 EMC Corporation. All rights reserved. Published in the USA. 2/16 Data Sheet H14905. RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.