RSA SECURITY OPERATIONS MANAGEMENT
Automation and Orchestration for the Security Operations Center

OVERVIEW

Advanced Persistent Threats (APTs) are the one constant in cyber security, 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 up 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 MANAGMENT

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 Security Operations Management (SecOps) provides the orchestration and framework for the SOC. It integrates with RSA Security Analytics, RSA ECAT for Endpoint Security and other third party security monitoring systems, aggregating events/alerts/ incidents and managing the overall incident response workflow.
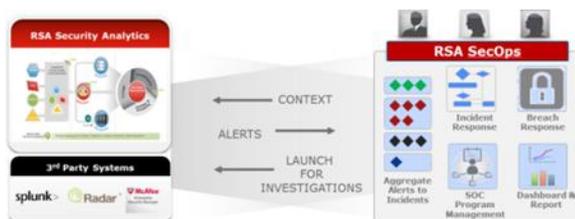
The workflow and capturing of incident information is aligned with industry best standards such as NIST, US-CERT, SANS and VERIS. RSA SecOps caters to the multiple personas within the SOC from the analysts, incident coordinators, SOC manager and CISO providing a view on the overall effectiveness of the SOC program. By leveraging the Incident Response, Breach Response and SOC Program Management capabilities of RSA SecOps, 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 SECOPS

RSA SecOps has three key functions:

- **Incident Response** – RSA SecOps aggregates events/alerts/incidents from various security monitoring systems using standard protocols. RSA SecOps 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 SecOps enables organizations to manage the overall breach response process. Incident and breach information is protected and shared with stakeholders. Additionally, RSA SecOps 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 SecOps enables organizations to manage the overall

RSA

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 SecOps 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, workflow, reports, dashboards and KPIs cater to the SOC personas including the analysts, incident coordinators, SOC manager, breach coordinator and CISO.
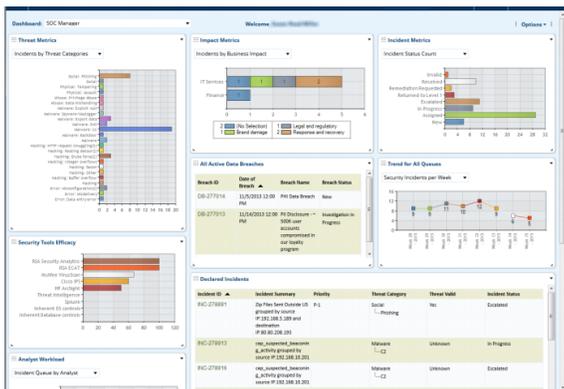
RSA SECOPS TIME TO VALUE

RSA SecOps 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 SecOps solution.

RSA SecOps can be customized and deployed in customer environments based on 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 first. 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 SecOps. It is flexible so customers can prioritize and leverage

the functionality that will bring immediate value to their SOC deployment.

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

RSA