RSA

AUTOMATING THREAT DETECTION AND ANALYSIS

RSA NETWITNESS® ORCHESTRATOR USE CASE

OVERVIEW

Information security has been a major challenge for organizations since the dawn of the digital era. Attackers are employing tools, techniques and procedures (TTPs) that are more sophisticated and powerful than ever, including exploits that originated in nation-state intelligence organizations designed to infiltrate and quickly propagate within commercial and government environments. Consequently, security operations teams must move fast to identify, understand and respond to these threats. RSA NetWitness Platform with RSA NetWitness Orchestrator can help by automating the lookups and enrichment of incoming incidents, allowing security teams to get ahead of them before they have an impact.

FEATURES

- Automatically extracts evidence from RSA NetWitness Platform alerts
- Automatically analyzes evidence using broad threat intelligence
- Adds business-level context regarding the incident
- Drives consistent workflows across the security organization
- Automates response actions across the environment

BENEFITS

- Saves time by automatically performing data enrichment and incident analysis
- Reduces workloads and allows security analysts to make better security decisions
- Brings consistency and efficiency to security operations via advanced workflows with automation and allows incident response teams to work from the same game plan

HOW IT WORKS

Figure 1: Automated Threat Detection and Analysis

RSA NetWitness Platform with RSA NetWitness Orchestrator allows security operations teams to maximize the automation of lookups and enrichment of incoming incidents. This reduces the time needed to rationalize and validate an incident detected by RSA NetWitness Platform by leveraging the workflows and automated playbooks within RSA NetWitness Orchestrator.

Once an incident is generated within RSA NetWitness Platform, it is automatically synced with the case management functionality for advanced workflows and automation in RSA NetWitness Orchestrator. These workflows and playbooks automatically extract indicators and artifacts from alerts as evidence for investigations.

The case management functionality then uses broad embedded intelligence to analyze the extracted evidence. From there, the case is enriched with broader context (e.g., user information, business information and third-party information such as Whois, sandboxes and business systems) to give analysts a fuller picture of the incident.

The case management functionality then drives efficient, consistent workflows across the security team by defining and assigning tasks and identifying dependencies to ensure tasks are completed and not duplicated.

Once the incident has been analyzed, RSA NetWitness Orchestrator automates response actions across the environment, such as synchronizing and closing the incident within RSA NetWitness Platform, opening a ticket in a ticketing system, escalating the incident if necessary, and taking automated remediation and response actions.

ABOUT RSA NETWITNESS PLATFORM

RSA NetWitness® Platform enables organizations to quickly detect threats and determine which pose the greatest risk, and mount a coordinated response. The platform is part of the RSA portfolio of business-driven security solutions, which provides a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.