RSA

# ENHANCED HUNTING WITH THREAT INTELLIGENCE

## RSA NETWITNESS® ORCHESTRATOR USE CASE

## OVERVIEW

Threat hunting has traditionally required security analysts to manually sift through different data sets as part of their process of creating hypotheses about potential threats. In recent years, however, it has become apparent that threat hunting can be partially automated or machine assisted. Indeed, RSA NetWitness Platform with RSA NetWitness Orchestrator enables automated and proactive hunting by leveraging a vast ecosystem of threat intelligence.

## FEATURES

- Comprehensive dashboard that categorizes and prioritizes intelligence attributes
- Collective Analytics Layer that provides context, criticality and confidence
- Playbooks that automatically hunt in RSA NetWitness Platform for notable indicators
- Capabilities for automatically extracting indicators and tagging them with details, and for automating actions to streamline indicator analysis

## BENEFITS

- Applies global threat intelligence to your threat hunting environment Leverages
- Finds indicators quickly and automatically pulls together information that security analysts need to respond to indicators
- Provides context about indicators so analysts can focus on priority issues

## HOW IT WORKS


*Figure 1: Enhanced Hunting with Threat Intelligence*

RSA NetWitness Platform with RSA NetWitness Orchestrator allows security analysts to better focus their threat hunting on the most important indicators for their business by leveraging threat intelligence to automatically and proactively provide necessary context.

The solution does this by using a centralized dashboard that categorizes and prioritizes hunting based on MITRE ATT&CK methodologies, indicators of compromise, incidents or any other intelligence attribute. In addition, it uses the Collective Analytics Layer to crowdsource threat intelligence from across the globe to provide context, criticality and confidence, thereby providing assurance to security analysts that they're focusing on high-priority incidents.

Playbooks within RSA NetWitness Orchestrator automatically hunt in RSA NetWitness Platform or third-party tools for any observance of notable indicators. Once an indicator is discovered, RSA NetWitness Orchestrator tags it, identifies it as observed and abstracts details about the indicator to provide context.

From there, RSA NetWitness Orchestrator can take several actions to aid security analysts in investigating the incident: For example, it can automatically open a case and collect evidence related to it, report on observed indicators to share details across the team, or pivot in-context into RSA NetWitness Platform for deeper investigation.

## 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.