RSA

# AUTOMATING PHISHING IDENTIFICATION AND ACTION

## RSA NETWITNESS® ORCHESTRATOR USE CASE

## OVERVIEW

According to the 2020 Data Breach Investigations Report from Verizon, credential theft, social engineering attacks and errors cause the majority of breaches (67% or more). Because these tactics are so effective for attackers, they use them over and over, so it makes sense for many organizations to focus the bulk of security efforts on those three tactics.

Indeed, many security operations teams are finding that the number of reported phishing attempts are growing, which means that employees are becoming more aware of them (a good thing). But security analysts are struggling to validate if all the reported incidents are truly phishing attempts (a bad thing). RSA NetWitness Platform with RSA NetWitness Orchestrator can help by automating the triage, analysis and response to high volumes of reported phishing attempts in seconds.

## FEATURES

- Automatically extracts relevant information from potential phishing emails.
- Automatically analyzes extracted information by leveraging broad threat intelligence sources.
- Determines if the perceived phishing attempt is in fact a real threat.
- Takes action against threats deemed legitimate and notifies recipients when emails they've reported are deemed harmless.

## BENEFITS

- Helps you protect sensitive data and defend against infiltration from phishing attacks.
- Reduces the time and resources needed to sift through and validate user-reported phishing emails.
- Improves the security operations team's response time.

## HOW IT WORKS

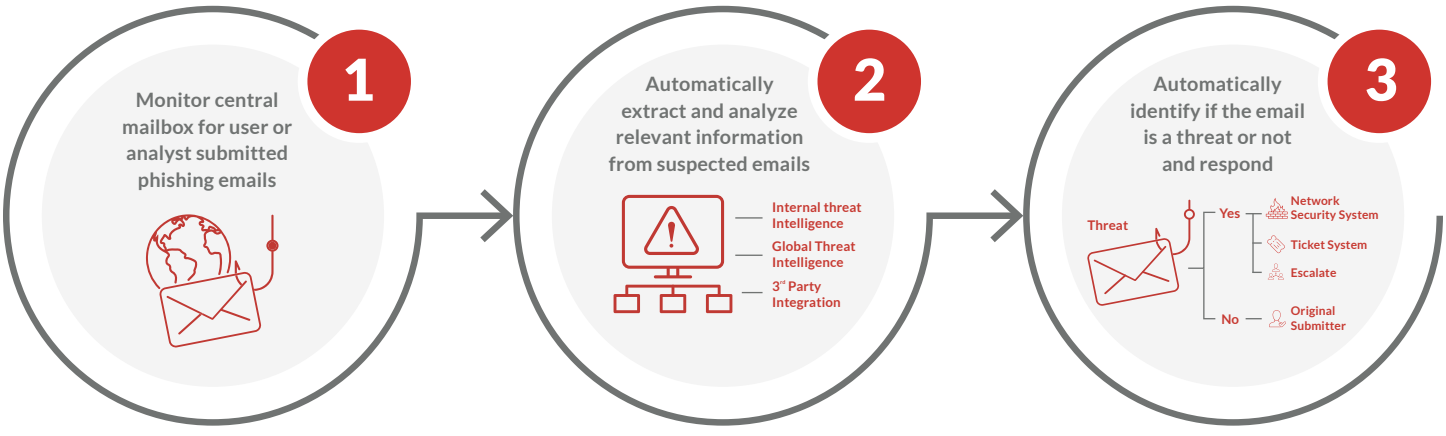


*Figure 1: Automating Phishing Identification and Action*

RSA NetWitness Platform with RSA NetWitness Orchestrator reduces the time it takes security operations teams to sift through and validate user-reported emails. It does this by monitoring an established central mailbox where users or security analysts can submit suspected phishing emails.

When an email hits the mailbox, RSA NetWitness Platform automatically extracts relevant information from the message, including headers, body copy, attachments, URLs and other indicators, and stores them as artifacts. It then analyzes the artifacts using embedded intelligence, the global connected analytics layer and third-party feeds to understand the nature of the potential phishing attempt.

Once it has analyzed the email, RSA NetWitness Platform produces a threat/no threat verdict. The solution then feeds observed indicators back into the RSA NetWitness Orchestrator threat intelligence ecosystem to inform future analysis of suspected phishing.

When a threat verdict has been reached, the solution can automatically generate a remediation ticket through various ticketing systems, escalate the issue to an identified security analyst or even act within other network security systems like firewalls. If the email isn't a threat, the system can automatically notify the original recipient that the email is safe, and the system marks it as a false positive for future investigations.

## 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.