REDUCING RISK WITH SECURITY AUTOMATION AND ORCHESTRATION

- **Reduce** the amount of uninvestigated and unresolved alerts
- **Automate** time-consuming investigations and remediate well-known threats
- **Act as a force multiplier** for resource-constrained security teams
- **Reduce** your organization's security risk exposure, including the time to containment and remediation

Security teams are usually hard at work on the front lines, identifying, analyzing and mitigating threats when and where possible. Yet despite their best efforts, security incident backlogs continue to grow. The reality is that there simply aren't enough skilled professionals to analyze the volume of incidents that most organizations face. With limited resources, an ever-growing skills gap and an escalating volume of security alerts, new sources of risk are constantly being added to the surface of your environment.

Luckily, leveraging a security orchestration, automation and response (SOAR) solution allows organizations to reduce risk in a number of powerful ways. Some of the key benefits of a SOAR solution is its ability to strengthen an organization's defenses and reduce its security risk exposure.

Orchestration

A key factor that determines an organization's operational maturity is attributed to orchestration — a methodology that connects tools, integrates systems, and ultimately streamlines and automates workflows. While processes should always be reviewed and iterated upon to improve efficacy, organizations gain significant ground in the reduction of risk by codifying process. For example, in a manual mode of operation, newer analysts are not as familiar with standard operating procedures (SOPs) and are prone to making more mistakes. More experienced analysts know the processes well, but may be tempted to cut corners to save time. Both of these scenarios can increase risk and also create problems with auditors. In contrast, a SOAR platform processes alerts and cases consistently, following codified SOPs with precision.

Automation

Adversaries have long since introduced automation into their attack suites. From distributed denial-of-service (DDoS) attacks to automated port scanning and beyond, the bad guys know that they need automation to intensify and quicken their assault. Once inside a victim's network, the more dwell time that a threat actor has can greatly increase the amount of damage caused. Therefore, security teams should measure dwell time and actively work to reduce it. Demonstrating shorter dwell times directly correlates to less risk exposure.

Automation can help with this critical metric. It's not uncommon for threat investigations to execute in seconds when automated, versus hours or more if performed manually. SOAR solutions can also reduce the time to containment and remediation. Whether the platform is operating without an analyst approving security actions (such as on-the-loop or out-of-the loop supervision) or with analysts reviewing security actions before they are performed (e.g. in-the-loop supervision), speed is gained in all cases, resulting in reduced risk.

SOAR platforms can help quantify and report on an organization's dwell time. This allows security teams to demonstrate the reduction in risk as a result of implementing a SOAR platform.

Incident Response

Most security teams would agree that one of the largest security risks comes from their limited capacity to investigate and respond to security alerts. In fact, the **Cisco 2017 Annual Cybersecurity Report** revealed that an average of 44 percent of alerts are ignored due to resource challenges. An unknown amount of risk lies in these uninvestigated alerts. Making matters worse, the Cisco report also indicates that only 54 percent of investigated and confirmed threats are remediated. Combined, these stats support a sobering fact — that resource constraints and unresolved threats create serious risk for an organization. The impact of a successful attack can be significant; customers may be lost, revenue may be impacted and the organization could experience immeasurable brand damage.

SOAR solutions act as a force multiplier for resource-constrained security teams. They allow teams to automate time-consuming investigations and even automatically remediate well-known threats where the team has an established SOPs. This allows the team to dramatically scale their capacity and reduce the amount of uninvestigated and unresolved alerts, thereby reducing the organization's security risk exposure in the process.

To learn more about the Phantom security automation and orchestration platform, download the **FREE Phantom Community Edition** or **ask sales** for more information.

splunk>

Learn more: **www.splunk.com/asksales**

www.splunk.com

SG-Splunk-Reducing-Risk-with-SOAR-Phantom-101