SOAR Insights Report

Explore the role of SOAR in your SOC automation journey.

White Paper

An Origin Story: The Role Security Orchestration, Automation, and Response Tools Play in Initiating and Maintaining an Elevated Security Posture

Sponsored by: Palo Alto Networks

Michelle Abraham   Christopher Kissel
November 2021

EXECUTIVE SUMMARY

Right now, the expectations for vendors of security orchestration, automation, and response (SOAR) platforms are unusually high. As businesses undertake their digital transformation journey, a journey that was in many ways accelerated by the onset of COVID-19, mounting IT and security problems visible from afar become far more pressing. Businesses have had to – and continue to – deal with the following issues:

- **New architectures facilitating remote workers.** As the pandemic caused a diaspora of remote workers, new connectivity options to VPN, logical business segmentations, and multitenant workflows had to be created on the fly.
- **New surfaces to defend and observe.** Straight-to-user SaaS applications and IoT/OT convergence occurred more rapidly.
- **Limited personnel both an ephemeral and a long-term problem.** If an IT or security operations center (SOC) specialist leaves a company, other team members temporarily fill the void until a replacement is found and trained. Often tier 1 security analysts assume more of a tier 2/3 threat hunting role. IT and cybersecurity workers are in short supply anyway, with estimates of a global shortage of roughly 3 million workers.
- **More sophisticated attacks.** Last, and truly the scariest, is that attackers are more automated now than ever, and the only way to defend from machine attacks is to build your own machine speed detection and response capabilities.

All these problems bring us back to SOAR solutions. SOAR has a profound effect on cybersecurity on the troika of "people, processes, and technology." On a high level, SOAR products create the connective fabric between point products and platforms and aggregate alerts in such a way that redundant alerts are weeded out, and in the investigation process, the analyst works with enriched and contextualized data. Ultimately, playbooks help guide the security analyst through the first steps of suggested remediation to the termination of the ticket.

If SOAR sounds heady and disruptive, it is. Orchestrating workflows between multiple systems and solutions is an engineering feat. Highly sophisticated playbooks can be developed, accounting for minute and specific instances as well as for multiple contingencies. In addition, SOAR provides a centralized investigation platform for incidents and alerts for security analysts rather than requiring them to swivel between multiple systems. Last, with the proper automation, the response process

November 2021, IDC #US48325921

Get Insights into Different SOAR Maturity Stages

Over the years, SecOps teams have evolved as the issues they face evolve. The move to implement security orchestration, automation and response (SOAR) tools is certainly one of the steps many have taken. While teams may be at different levels of SOAR adoption, there are insights that can help at every stage.

To understand the most critical issues teams come up against, IDC talked to security operations center (SOC) teams about their SOAR strategy. They summarized their observations in this white paper, where you'll learn:

- How organizations beginning with SOAR derive value
- Best practices to move SOAR capabilities from beginner to intermediate to advanced levels
- Expert use cases
- Efficiencies that can be gained in more mature SOCs

Download now to learn more.