Gartner 2020 Market Guide for SOAR

Gartner.

Market Guide for Security Orchestration, Automation and Response Solutions

Published 21 September 2020 - ID G00727304 - 28 min read

By Claudio Neiva, Craig Lawson, **and 2 more**

SOAR solutions are steadily gaining traction in real-world use to improve security operations. Security and risk management leaders should evaluate how these solutions can support and optimize their broader security operations capabilities.

Overview

Key Findings

- Large security teams with well-established and tested processes to automate are still the main buyers and continue to buy security orchestration, automation and response, primarily for general productivity, efficiency and consistency improvements in their security operations centers.

- Orchestration and automation, basic incident/case management, and operationalizing threat intelligence are "table stakes" for SOAR tools. These capabilities are being embedded in security technologies, such as security information and event management, extended detection and response, and email security to improve the use of those products' services.

- SOAR is also becoming ubiquitous in managed security and managed detection and response services by helping providers improve client interactions, speed and consistency when detecting and responding to threats.

- SOAR tools are still primarily leveraged by organizations with a security operations center. Use cases to support security operations beyond threat monitoring and detection, threat intelligence, and incident response and threat hunting are still nascent.

- Security information and event management vendors continue to add SOAR capabilities via acquisitions, OEM agreements or internal development; however, the solutions are still primarily sold as premium add-ons and not being merged with SIEM tools

Security operations teams can only take full advantage of security orchestration, automation and response (SOAR) tools if their security processes are ready. Read this report from Gartner to understand key aspects of the SOAR landscape, including:

- **SOAR trends**, how the market is changing, and the distinction between broad-based and product-level SOAR

- How service providers are leveraging SOAR to **strengthen the customer experience**
- **Gartner's evaluations** of vendor strengths and why we believe independent, vendor-agnostic SOAR products deliver greater value for users
- How to make **better-informed** security purchasing decisions
- **Best practices** for implementing SOAR

Learn how to take advantage of all the capabilities of a SOAR platform, including threat intelligence and machine learning. You'll also learn how a security orchestration marketplace can help you discover and share new automation use cases.

Read the report to learn more about our recognition and how SOAR aligns to your future plans.