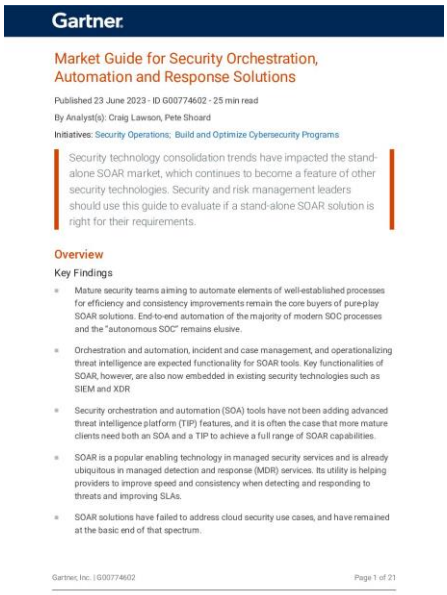
splunk> turn data into doing

2023 Gartner® Market Guide for Security, Orchestration, Automation and Response Solutions



Gartner

Market Guide for Security Orchestration, Automation and Response Solutions

Published 23 June 2023 - ID G00774602 - 25 min read

By Analyst(s): Craig Lawson, Pete Shoard

Initiatives: Security Operations; Build and Optimize Cybersecurity Programs

Security technology consolidation trends have impacted the stand-alone SOAR market, which continues to become a feature of other security technologies. Security and risk management leaders should use this guide to evaluate if a stand-alone SOAR solution is right for their requirements.

Overview

Key Findings

- Mature security teams aiming to automate elements of well-established processes for efficiency and consistency improvements remain the core buyers of pure-play SOAR solutions. End-to-end automation of the majority of modern SOC processes and the "autonomous SOC" remains elusive.
- Orchestration and automation, incident and case management, and operationalizing threat intelligence are expected functionality for SOAR tools. Key functionalities of SOAR, however, are also now embedded in existing security technologies such as SIEM and XDR.
- Security orchestration and automation (SOA) tools have not been adding advanced threat intelligence platform (TIP) features, and it is often the case that more mature clients need both an SOA and a TIP to achieve a full range of SOAR capabilities.
- SOAR is a popular enabling technology in managed security services and is already ubiquitous in managed detection and response (MDR) services. Its utility is helping providers to improve speed and consistency when detecting and responding to threats and improving SLAs.
- SOAR solutions have failed to address cloud security use cases, and have remained at the basic end of that spectrum.

Gartner, Inc. | G00774602 Page 1 of 21

The security technology market is in a state of general overload with pressure on budgets, staff hiring/retention, and having too many point solutions are pervasive issues for organizations today."

Security and risk management leaders should evaluate how security orchestration, automation and response (SOAR) can support and optimize their broader security operations by automating repetitive tasks; triaging security incidents faster with automated investigation and response; increasing productivity, efficiency and accuracy; and strengthening defenses by connecting and coordinating complex workflows across their team and tools.

Download the 2023 Gartner Market Guide for SOAR to understand:

- Why the ability to better orchestrate and automate horizontal "processes" across a number of solutions is a key feature of SOAR.
  - How to investigate the potential crossover with enterprise automation use cases typically delivered by low-code application platforms.
- How key functionalities of SOAR are now also embedded in existing security technologies such as SIEM and XDR.

disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner, Magic Quadrant for Security Information and Event Management, Kelly Kavanagh, Toby Bussa, John Collins, 29 June 2021