# 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.

### Recommendations

Security and risk management leaders responsible for security operations must:

- Identify the specific opportunities for both automation and orchestration of existing processes before making any investment in new solutions, and not simply focus on the initial deployment, but on the value of the implementation through the lifetime of the security operations program.
- Invest in skills required to find the best processes to automate and to create the detailed documentation of how processes are being enhanced by SOAR.
- Demand that your security vendors deliver comprehensive APIs when you renew or procure solutions because poor APIs in your security ecosystem directly impinges your security operations effectiveness overall as well as SOAR's ability to deliver value.
- Evaluate security platforms that incorporate SOAR capabilities, like SIEM and XDR, which could meet your requirements without having to have a dedicated SOAR solution. Additionally, you should investigate the potential crossover with enterprise automation use cases typically delivered by low-code application platforms.

## Market Definition

Security orchestration, automation and response (SOAR) solutions combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform. SOAR tools are also used to document and implement processes (aka playbooks, workflows and processes); support security incident management; and apply machine-based assistance to human security analysts and operators.

SOAR solutions must provide:

- Highly customizable workflow process management that enables repeatable automated tasks to be turned into playbooks that run in isolation or joined together into more sophisticated workflows.
- The ability to store (locally or in a third-party system) incident management data to support SecOps investigations.
- Manually instigated and automated triggers that augment human security analyst operators to carry out operational tasks consistently.

- A mechanism to collate and better operationalize the use of threat intelligence.
- Support for a broad range of existing security technologies that supports improved analyst efficiency and acts as an abstraction layer between the desired outcomes and the custom-made set of solutions in place in your environment.

See Note 3 for a more-detailed explanation of SOAR minimum requirements

## Market Description

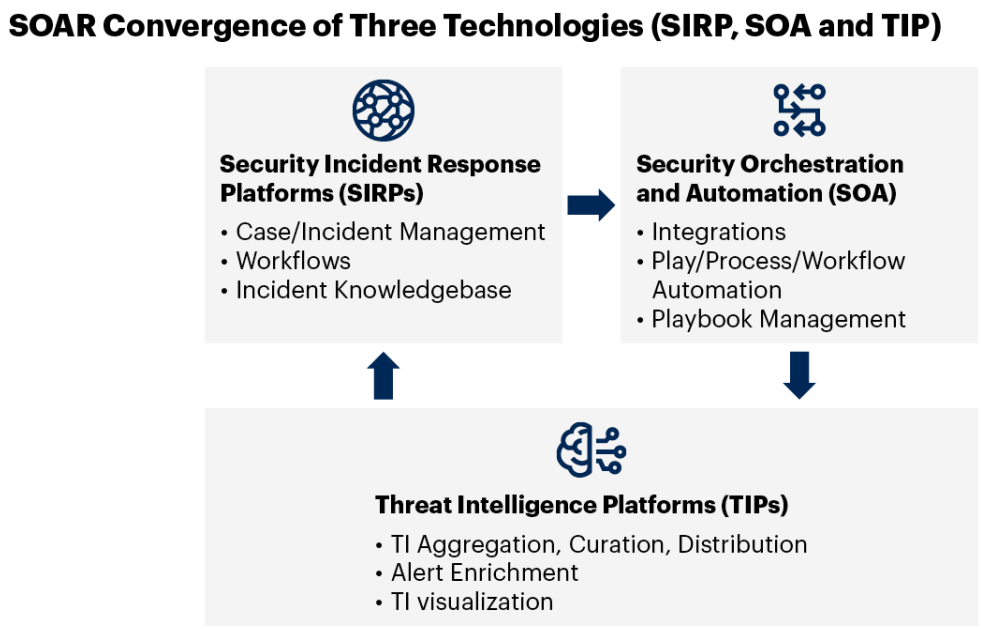
SOAR solutions are an amalgamation of three historically distinct technologies that have some common attributes and some common users consuming them. These technologies were historically distinct and offer utility to security operations teams in the form of a product that can relieve significant amounts of manual labor for a number of security operations functions.

Products that have been developing as this market continues to mature into SOAR are:

- Security incident response platforms (SIRPs)
- Security orchestration and automation (SOA)
- Threat intelligence platforms (TIPs)

These technologies are depicted in Figure 1.

Figure 1: The Convergence of Three Technologies (SOA, SIRP and TIP)




Source: Gartner
727304_C

Gartner

It is possible to achieve the outcomes desired of an SOAR platform by using component parts of existing investments. The flexibility of SOAR allows for workflows to be orchestrated via integrations with other technologies. Examples include:

- Incident triage via SOAR, case management via ITSM.
- Response approval and creation via SOAR, execution via configuration management.
- Threat intelligence (TI) acquisition curation and management via service/subscription.

Below are recommended requirements to consider when selecting a SOAR solution. SOAR solutions should:

- Support a wide range of security products across multiple existing point solution markets (for example, endpoint protection platforms, firewalls, intrusion detection and prevention systems [IDPSs], security information and event management (SIEM), secure email gateways, SSE and vulnerability assessment technologies).

- Support the ability to do event correlation and aggregation for the purpose of improving security operations processes and alerting with better event enrichment. A key way to do this is through the implementation of low-code "playbooks," which allow for the codification of processes where automation can be applied to improve consistency and time savings.
- Have the ability to be deployed either on-premises or as a cloud solution (like SaaS).
- Support the ingestion of a wide variety of sources and formats of TI from third-party sources, supporting open-source, industry and government (information sharing and analysis centers [ISACs] and computer emergency response teams [CERTs]) and commercial providers.
- Bidirectional integrations with IT operations solutions like ticketing systems for case management and collaboration tools, like messaging applications for better real-time communications.

**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.**

Gartner clients continue to see operational struggles in their security environments where they have alert fatigue is exacerbated further by complexity and duplication of tools. In principle, automation continues to show promise to assist with many of these persistent issues.

SOAR solutions are primarily being adopted to:

- Improve security operations efficiency
- Create more consistency in security processes
- Improve threat prevention, detection and response
- Improve prioritization
- Operationalize threat intelligence

In most cases, this is a key deliverable of end-user organizations and service providers that operate security operations centers (see SOC Model Guide).

Automation is most commonly used for improving threat detection and incident response, and the automation of workflows (or for a combination of the two). SOAR tools that have added threat intelligence management to a broader set of playbook/workflow use cases are often seen as more basic when compared to fully featured TIP platforms. TIPs remain the more sophisticated option if users are looking for advanced threat intelligence use cases. Gartner still sees mature clients running both a TIP and an orchestration/automation tool where best-of-breed functionality is required.

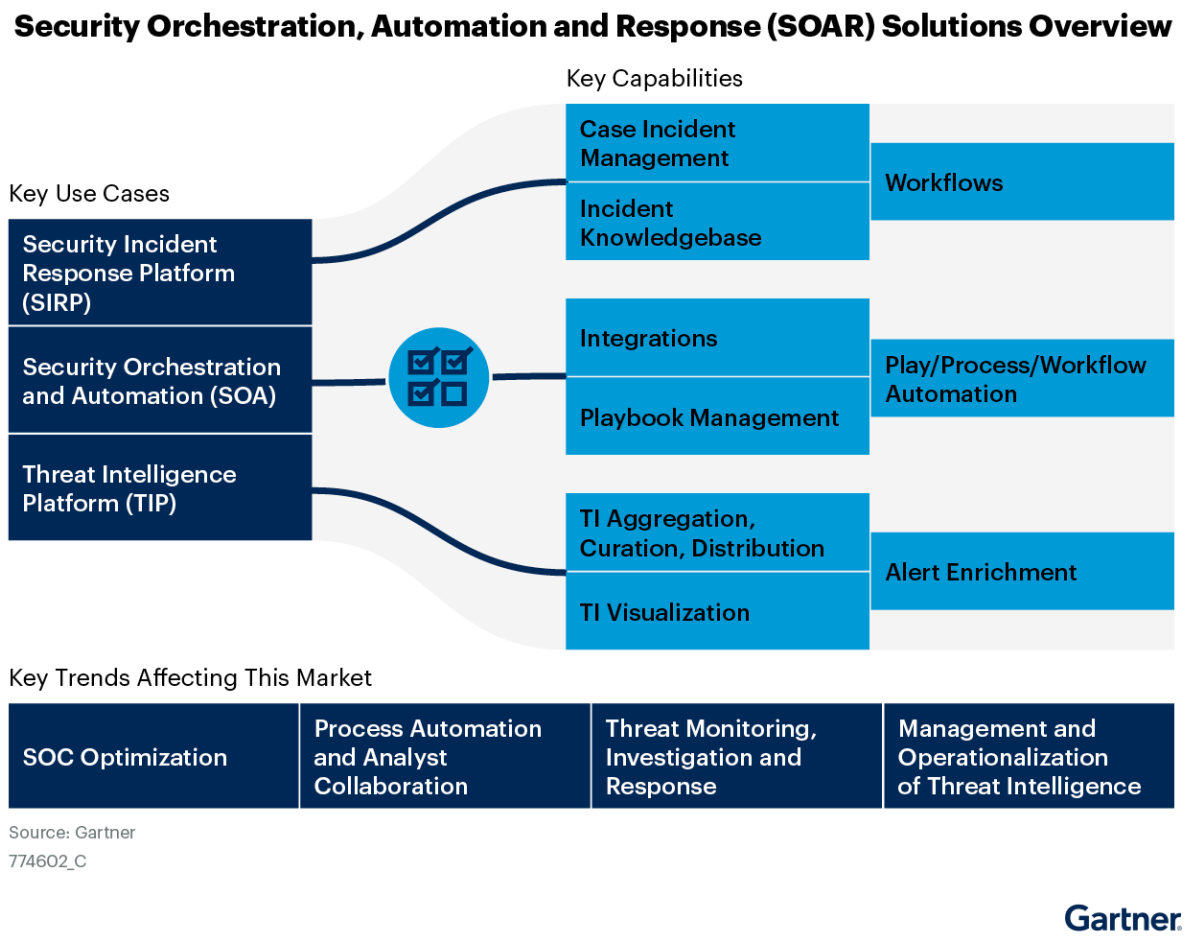
Playbook creation, case management, event enrichment, automation and response capabilities are also commonly found in some other security tools that already address threats. For smaller organizations, and some larger ones, this can make a dedicated SOAR platform less relevant for some features and instead shift focus for the SOAR to centrally manage automations.

## Market Direction

A small number of dedicated SOAR solutions remain, but this market remains niche overall in the context of the overall broader security marketplace. SOAR is primarily consumed by organizations that have larger and more mature security operations programs as well as by security services providers.

Organizations that are less mature — or that tend to outsource their security operations — have shown little interest in distinct SOAR tools, opting for functions and capabilities that are already built in to existing toolsets (such as SIEM, XDR and ITSM platforms, which commonly offer automation and orchestration add-on capabilities — see Figure 2). Additionally, MDR continues its rapid growth trajectory, and SOAR is a key “back end” element of a majority of MDR services today.

Figure 2: SOAR Solution Overview




SIEM vendors continue to both acquire and build out SOAR capabilities in their solutions. This functionality is usually delivered as a premium add-on (see Critical Capabilities for Security Information and Event Management).

The need to apply automation in security operations is well-understood and automation capabilities that focus on response appear in a number of other security technologies such as:

- Secure email gateway (SEG)
- Endpoint protection platform (EPP)
- Network detection and response (NDR)

Broader integrations that support more operational SOC functions commonly appear in more consolidated threat detection, investigation and response (TDIR) solutions such as:

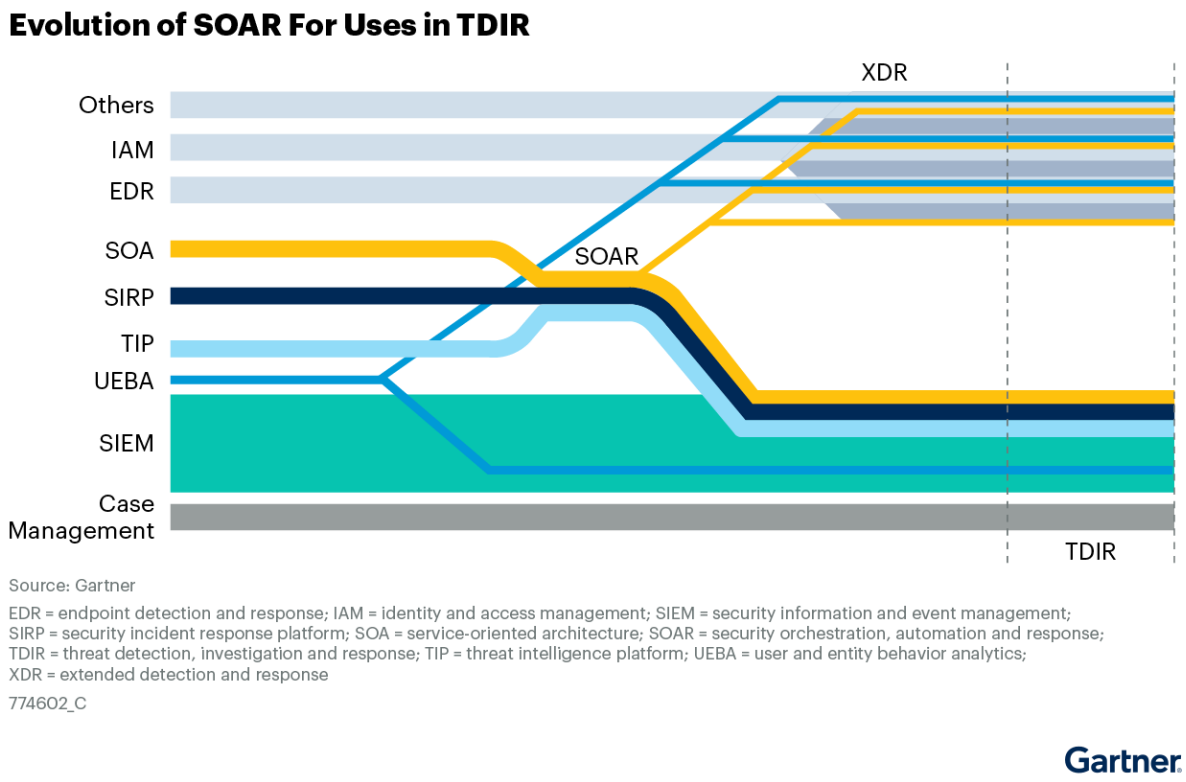
- SIEM (see Magic Quadrant for Security Information and Event Management).
- XDR (see Market Guide for Extended Detection and Response).

Furthermore, a number of robotic process automation (RPA) solutions recognize security use cases as part of a broader set of requirements to enable organizations to leverage automation (see Magic Quadrant for Robotic Process Automation).

## Security Automation Doesn't Always Need Its Own Dedicated Solution

SOAR continues to connect disparate solutions and create a control plane for security operations environments in more productive ways. Very common use cases are in the execution of a variety of repeatable processes for prevalent security issues, like phishing, and manual processes, like indicator-of-compromise-based blocking in prevention devices. These features and capabilities are somewhat universal and based on standard automation principles. They are seen as being helpful in other (often larger) technology markets as well (see Figure 3).

### Figure 3: Evolution of SOAR For Uses in TDIR



It is commonplace for SOAR technologies to offer low-code-like functionality (see Magic Quadrant for Enterprise Low-Code Application Platforms). This makes programming and workflow improvements more accessible to all members of the security operations team even if they do not have a lot of programming experience. While SOAR continues to offer a lot of features for "power users," these individuals can have broader responsibilities for automation across the organization. Power users can develop their own integrations and often reuse existing code/scripts. SOAR is then used to help build out more repeatable playbooks, allowing organizations to utilize this code based on the building blocks that already exist in the technology.

Demand for SIEM technology remains popular for larger organizations (see Magic Quadrant for Security Information and Event Management), with threat management now the main driver — although compliance use cases are still expected features. Almost all SIEM vendors are organically enhancing their threat detection, investigation and response capabilities. They are also introducing integrations for response actions via either natively built (or acquired) capabilities, or third-party integrations with SOAR solutions.

Similarly, with extended detection and response (XDR) solutions (see Market Guide for Extended Detection and Response), it is essential to offer functions similar to SOAR tools. This could include localized incident and case management, and orchestration, automation and handling of threat intelligence. These SOAR capabilities are often preprogrammed by the vendor — which means they tend to be primarily focused inward at their own products — and may lack the ability to support the level of customization available in a dedicated SOAR solution.

The reduction in interest in dedicated SOAR can, in part, be attributed to the increased acquisition of SOAR solutions by broader security platform providers. However, it should also be noted that broader use of automation, including the burst in popularity of generative AI (such as OpenAI's ChatGPT and Google's Bard), embedded and dedicated RPA capabilities are more broadly used by organizations and they can use them for some security use cases.

Although XDR and SIEM now have features replicated from a dedicated SOAR solution, buyers who prefer the best-of-breed approach will find that SOAR still offers more flexibility, genuine vendor-neutrality and opportunities for nonsecurity use cases.

## Market Analysis

While certainly valuable, the aggregate number of use cases implemented by SOAR buyers has remained relatively small. The focus remains on time-consuming and repetitive manual processes that are usually performed by SOC analysts who can benefit from automation. These are worthy of pursuit and are a key value proposition.

A number of the use cases that initially suited SOAR are now more commonly embedded directly into security solutions, for example, automating the triage of suspected phishing emails reported by end users. This is a process that follows a repeatable set of steps, dozens to hundreds of times per day, with the simple goal of determining whether the email (or its content) is malicious, and whether it requires a response. Many of these kinds of repetitive actions that were very popular use cases for SOAR, and were common proof-of-concept or out-of-the-box capabilities, are now surplus to requirements due to advancements in other security technologies.

**A lack of mature processes and procedures in the security operations team, combined with budget and staff constraints, presents obstacles to the adoption of SOAR solutions by a wider audience. This, combined with the varying degrees of maturity in vendors' APIs as integration options, remains a key reason for SOAR not achieving higher rates of adoption.**

Determining operational security maturity means that security leaders can evaluate their readiness to adopt new products, including SOAR solutions. This readiness should be evaluated through at least five areas:

1. Availability of current, operational metrics
2. Defined operational processes
3. Development and security competency among analysts
4. Documentation of workflows/processes
5. Variety of technologies that require integration.

Commercial SOAR vendors can be grouped into two categories — ecosystem-first, and open-compatibility solutions.

## Solutions Where SOAR Is a Feature

Vendors today provide product-level SOAR functions that support activities revolving primarily around that vendor's specific portfolio of products. Of course, integrating with products outside of their own ecosystems is also valuable, but more focus on improved workflow and orchestration improves these offerings in ways that aren't directly related to their native threat-detection engines. For example, a product that uses automation and orchestration to protect email will often include the SOAR functions required to detect phishing emails or malicious attachments and initiate a workflow. Usually, these types of product do not have full SOAR features but are in turn able to support workflows into their own tool from a stand-alone SOAR tool.

## Open-Compatibility Solutions

Providers that supply broad-based, vendor-neutral SOAR can be pure-play vendors or part of a vendor that delivers a broader security portfolio — these are often the result of a previous acquisition of a pure-play SOAR. What sets these products apart is their ability to receive inputs from a broad ecosystem of security products, and organize the workflow of the security operations team. The vast majority of this type of product is also sold separately, maintaining a maximum interoperability level with other vendors, even if they are competing products.

## Identify the Specific Opportunities for Both Automation and Orchestration of Existing Processes Before Making Any Investment

Buyers' use cases can define the most productive way forward when choosing the best type of product to meet your organization's specific needs. Below are the most common use cases mentioned by Gartner customers:

- SOC optimization
- Process automation and analyst collaboration
- Threat monitoring, investigation and response
- Management and operationalisation of threat intelligence

Organizations that are looking to evaluate SOAR products on their technical merits should start with their specific use cases and the supporting capabilities at a high level — those aspects include:

- **Alert triage and prioritization:** This is the ability to take alert inputs from different sources and apply a process of data enrichment and correlation. This reduces, rationalizes and prioritizes the number of incidents that will have a more-significant impact and high probability of causing damage to your organization. The goal is to "leave no alerts behind" and concurrently produce accurate incidents that deserve genuine attention from security analysts.
- **Orchestration and automation:** Security teams are often dealing with a number of point-solution tools with a singular focus. The ability to better orchestrate and automate horizontal "processes" across a number of solutions is a key feature of SOAR. The complexity of combining resources involves the coordination of workflows with manual and automated steps (which, in turn, involve many components affecting information systems and, often, humans).
- **Case management and collaboration:** Manual or automated response provides canned resolution to programmatically defined activities. The response includes activities from a basic level (such as ticket creation in an IT service desk application) to more-advanced actions (for example, responding via another security control, such as blocking a domain name or IP address by changing a firewall rule). This functionality is the most impactful operationally as it applies to the most complex of use cases and can significantly improve analyst effectiveness.
- **Dashboard and reporting:** Dashboard and reporting provides the ability to aggregate security telemetry that allows an understanding of the SOC's situation, the evolution of incident response processes, and performance results. SOC data should be presented to different audiences, such as the SOC manager, SOC analyst and chief information security officer (CISO).
- **Operationalisation of threat intelligence and investigation:** This takes the form of evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject's response to that threat. An incident investigation will be conducted in the form of a workflow to validate the alert into an incident and determine the best workflow to initiate a response (in a manual or automated fashion).

- **Architecture:** This includes items like location (cloud or on-premises), redundancy of the solution to support high-availability, and performance — to include how prioritization can be applied to playbook execution. It also includes role-based access control (RBAC) for functions that support a wider range of users who use the tool during incidents. Architecture also covers licensing models that encourage better adoption and usage rather than punishing for expanding usage, and integration with your existing vendor ecosystem.

## Potential Crossover With Enterprise Automation

Identifying where opportunities exist with the existing investments already made by your organization is often the most efficient and effective method of introducing automation. Many businesses have development teams and custom-made applications. Others have dedicated technologies like RPA and low-code solutions. It would be remiss not to look to these as opportunities to save money and centralize automation requirements. While there *are* repeatable, security-driven functions for automation, this is also true of wider areas within many organizations.

Traditionally, it has been common for security to segregate itself and use dedicated solutions for them and them alone. With today's infrastructure, a large number of capabilities offered by IT solutions benefit the business in a number of ways — from business intelligence data, system maintenance and health monitoring, to cost control and many other functions. This means that security shares many goals and objectives with other business units and therefore has the potential to operate automation use cases on shared platforms. For this reason, among others, security is sometimes associated with a larger function, which is also a factor in platform consolidation. There are many examples in the market of acquisitions and product realignments that demonstrate the reduced need for a dedicated security automation solution.

Acquisitions are still happening, and will shape the state of the SOAR market in the coming years (see Table 1).

## Table 1: SOAR Acquisitions in the Last Two Years

(Enlarged table in Appendix)

| Date | Event |
|---|---|
| January 2020 | FireEye acquires Cloudvisory |
| March 2020 | Fortinet acquires CyberSponse |
| April 2020 | Swimlane acquires Syncurity |
| July 2020 | Micro Focus acquires ATAR Labs |
| March 2021 | Sumo Logic acquires DFLabs |
| September 2021 | Logpoint acquires SecBI |
| January 2022 | Google Cloud acquires Siemplify |
| December 2021 | SentinelOne invests in Torq |
| September 2022 | Devo acquires LogicHub |
| August 2022 | OpenText acquires Micro Focus |
| May 2023 | ReliaQuest acquires EclecticIQ |

Source: Gartner (May 2023)

Vendors have been steadily acquiring SOAR solutions to fill gaps in existing products like SIEM and XDR or to enter the SOAR market, as well as building out their own native capabilities. These acquisition scenarios however require end users to create a contingency plan for vendor acquisition of their current SOAR solutions. Generally speaking, vendor-agnostic SOAR products are the best value when features are a primary decision point. This is due to the need for integration into a wide array of products, and this will be the reality for some time as this is one of their core value propositions in being product-agnostic. Independent solutions will continue to do a better job with their singular focus on roadmap execution for just this single product, and will be better at supporting “vendor neutrality” with available integrations.

### Security Services Providers Are Using SOAR to Improve Service Delivery and Response Capabilities

Demand for better threat detection and response capabilities from managed security services providers (MSSP) is increasing and is already the norm in MDR services. MDRs in particular are universally either using a SOAR tool, or building their own SOAR-like features to help deliver better client outcomes at scale that also help deliver consistent SLAs. We recommend that you consider how MDRs are using automation and orchestration as part of your evaluation of these types of services, even though you might not be planning to run SOAR natively as a stand-alone product.

Security services providers can work through different use cases with you to offer a personalized workflow for your specific environment. Providers also benefit from having a wider view of threats from across their client base and can take lessons from one client and apply remedies to their entire client base. This view can then feed back into service improvement for all of their clients, often via their orchestration and automation technology.

Another evaluation criterion to consider is the need for bidirectional integration with your own technologies to collect data for analysis and to power more effective incident investigations and response activities.

## Representative Vendors

*The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.*

### Market Introduction

Table 2 provides a list of vendors. It is not — nor is it intended to be — a list of every vendor or offering on the market. Neither is it a competitive analysis of the vendors' features, functions or services. For more information, see Note 2.

### Table 2: Representative Vendors in Security Orchestration, Automation and Response

(Enlarged table in Appendix)

| Vendor | Product, Service or Solution Name |
|---|---|
| Anomali | ThreatStream |
| Cyware | Virtual Cyber Fusion Center |
| D3 Security | D3 Smart SOAR |
| Devo | Devo Security Orchestration Automation and Response (SOAR) Platform |
| Fortinet | FortiSOAR |
| Google Cloud | Chronicle SOAR |
| IBM | IBM Security QRadar SOAR |
| Logsign | Logsign SOAR |
| Microsoft | Microsoft Sentinel |
| NSFOCUS | Intelligent Security Operation Platform (ISOP) |
| OpenText ( CyberRes) | ArcSight SOAR |
| Palo Alto Networks | Cortex XSOAR |
| QAX | QAX SOAR |
| Rapid7 | InsightConnect |
| Revelstoke | Revelstoke SOAR |
| ReliaQuest ( EclecticIQ) | EclecticIQ Platform |
| ServiceNow | Security Operations |
| SIRP Labs | SIRP SOAR Platform |
| Splunk | Splunk SOAR |
| Sumo Logic | Cloud SOAR |
| Swimlane | Swimlane Turbine |
| ThreatConnect | Intelligence-Powered Security Operations (IPSO) |
| ThreatQuotient | ThreatQ TDR Orchestrator |
| Tines | Tines |
| Torq | Torq Hyperautomation |

Note: There are providers in this list that — while they offer a SOAR solution — in practice prefer to offer, and have more clients consuming, their SOAR solution as part of a larger offering. SIEM and XDR solutions are relevant examples of this situation today.

Source: Gartner (May 2023)

## Market Recommendations

Security and risk management leaders who have dedicated and mature security operations processes might consider using SOAR tools to improve efficiency and efficacy. SOAR solutions are made up of the following major capabilities:

- Workflow and collaboration
- Ticket and case management
- Orchestration and automation of security processes
- Threat intelligence operationalisation and management

If the need for a dedicated security automation solution is identified, security and risk management leaders should favor SOAR solutions that:

- Are compatible with the collection of existing products installed in the organization environment. Also, plan to update the skill sets of your security team and, where required, the internal development team, to help in the customization of the solution to your specific security operations program. Operational security metrics related to "time to detect threats" and "time to response" styles of metrics should be demonstrably better with, rather than without, a SOAR tool.
- Can deliver the use cases needed to complement the primary set of people, processes and technologies that are critical to your security operations functions. For instance, some clients prefer to use the company ticket system instead of a dedicated case management solution. Others see technology like SOAR as key to improving the efficacy of existing tools like SIEM and EDR. End users also see SOAR as a key tool for improving the efficiency of security staff in the face of rising numbers of threats, while hiring and retaining staff remains an acute pain point for many organizations.
- Have bidirectional integrations with IT operations solutions (like ticketing systems for case management) and collaboration tools (like messaging applications for better real-time communications).

Buying a SOAR solution should primarily be driven by your existing processes (for example, security operations optimization, threat monitoring and response, threat investigation and hunting, and operationalizing threat intelligence).

Other SOAR-specific considerations might include:

- The ability to easily code an organization's existing processes into functional playbooks via an intuitive UI (using a low-code or no-code model), so that the tool can then automate these playbooks. The ability to create playbooks and then execute them regularly is a key capability for a SOAR solution and should be a key design principle for you in your implementation of SOAR.
- Optimized collaboration of analysts, for example, with a chat or instant messaging framework that makes analyst communication more efficient, or with the ability to work together on complex cases across multiple security and nonsecurity teams.

- Have a pricing model that is aligned with the needs of the organization, is predictable, and encourages the creation and usage of the tool. Avoid pricing structures that are based on the volume of data managed by the tool, or the number of playbook executions. These metrics carry a penalty for more frequent use.
- Flexibility in the deployment and hosting of the solution — either in the cloud, on-premises or as a hybrid. Deployment should accommodate the organization's security policies and privacy considerations, or its cloud-first initiatives.

Security teams should, as a general rule, always consider and evaluate incumbent providers solutions that could be used to support a broader programme of automation/orchestration across their organizations. This then helps ensure that, if you choose a dedicated solution, you have a clear picture of the gaps addressed by the new solution and have the staffing and requirements to support a successful implementation for its entire life cycle.

## Evidence

The overall list of representative providers has been validated by responses to client inquiries and in collaboration with the cohort of Gartner analysts that cover the security operations markets that include SOAR.

## Note 1: Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

## Note 2: Representative Vendor Selection

The sample vendors included in this publication are listed in alphabetical order and are representative only. It is not intended to be an exhaustive list. The vendors and solutions provided are those that most closely illustrate the marketplace trends described and provide the individual capabilities described in each section that Gartner sees in day-to-day coverage of the SOAR market.

## Note 3: Minimum Requirements for SOAR

## Resources Needed for Creation of Automation

Automation capabilities need to be based on threats and processes that you specifically have based on real-world scenarios and the capabilities of your security operations program. This means that organizations must have invested in (or be prepared to invest in) delivering these outcomes, regardless of the technology selected and how this technology must be aligned to more efficient security processes.

Development of any application takes trial and error, and automating security is no different. There are a number of key continuous functions that security teams must budget for if they are going to be successful at automation:

- **Requirements gathering and continuous improvement:** A good understanding of the outcomes required, the pressure points that the SOC suffer, and the continued breaches that the organization is subject to create good requirements for automation (see 3 Ways to Apply a Risk-Based Approach to Threat Detection, Investigation and Response). This requires the dedication of a significant amount of time to identify new requirements, maintain and adjust existing requirements, and ensure that automations continue to function as intended.
- **Sprint deployment and rollback processes:** Automation has the potential to break lots of things, very quickly. Deploying automations like applications in sprint cycles is an effective way to ensure that there are testing and rollback capabilities. This requires development planning and can be quite labor intensive to do correctly.
- **Metrics planning:** Automations, like people, need to be measured to ensure the business is receiving value. This means that regular reviews of the value of individual automations and their value back to the organization is imperative. Because most automation solutions are priced based on the number of workflows or playbooks, cost efficiency planning and wastage identification are required.

For most organizations, planning for automation capabilities is something that can be done hand-in-hand with the development of correlation rules, analytics and reporting. However, many organizations view SOAR and automation more generally as an opportunity not to hire, or to reduce staffing levels. This is incorrect. Effective automation augments human involvement, makes people more efficient, and requires good governance and planning.

### Demand That Vendors in Your Security Ecosystem Deliver Comprehensive APIs

Selection of automation and orchestration solutions is not just about picking one product. Introducing these functionalities into your environment, whether just security or more broadly, requires additional steps in other planning processes. APIs — or the lack of credible ones — is one of the key issues that SOAR has faced in meeting ROI requirements. APIs being available for SOAR to then leverage is mandatory. It is important to analyze the other investments your organization has made and is planning to make, to ensure compatibility with automation platforms and capable API functionality, which will allow you to achieve your objectives.

As markets evolve, a number of product consolidation characteristics are emerging, there are two main ways in which this mirrors SOAR solution types:

- Ecosystem compatibility and partnership alignment guarantee a wide range of interconnectivity and interoperability between products.
- Open compatibility and adhering to a common set of standards, such as the Open Cybersecurity Schema Framework (OCSF), MITRE or others.

It is hard to say how long the process of consolidation and market maturation will take, however, the process has already begun and among some of the expected commercial gains for strong ecosystem-driven solutions will likely come a set of standards that all solutions will eventually adhere to for interoperability.

## Document Revision History

Market Guide for Security Orchestration, Automation and Response Solutions - 13 June 2022

Market Guide for Security Orchestration, Automation and Response Solutions - 21 September 2020

Market Guide for Security Orchestration, Automation and Response Solutions - 27 June 2019

## Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Market Guide for Security Threat Intelligence Products and Services

SOC Model Guide

Market Guide for Extended Detection and Response

Magic Quadrant for Security Information and Event Management

Critical Capabilities for Security Information and Event Management

SOAR Will Not Make You Better at Running SIEM

Magic Quadrant for Enterprise Low-Code Application Platforms

Critical Capabilities for Enterprise Low-Code Application Platforms

Magic Quadrant for Robotic Process Automation

---

## Table 1: SOAR Acquisitions in the Last Two Years

| Date | Event |
|---|---|
| January 2020 | FireEye acquires Cloudvisory |
| March 2020 | Fortinet acquires CyberSponse |
| April 2020 | Swimlane acquires Syncurity |
| July 2020 | Micro Focus acquires ATAR Labs |
| March 2021 | Sumo Logic acquires DFLabs |
| September 2021 | Logpoint acquires SecBI |
| January 2022 | Google Cloud acquires Siemplify |
| December 2021 | SentinelOne invests in Torq |
| September 2022 | Devo acquires LogicHub |
| August 2022 | OpenText acquires Micro Focus |
| May 2023 | ReliaQuest acquires EclecticIQ |

Source: Gartner (May 2023)

## Table 2: Representative Vendors in Security Orchestration, Automation and Response

| Vendor | Product, Service or Solution Name |
|---|---|
| Anomali | ThreatStream |
| Cyware | Virtual Cyber Fusion Center |
| D3 Security | D3 Smart SOAR |
| Devo | Devo Security Orchestration Automation and Response (SOAR) Platform |
| Fortinet | FortiSOAR |
| Google Cloud | Chronicle SOAR |
| IBM | IBM Security QRadar SOAR |
| Logsign | Logsign SOAR |
| Microsoft | Microsoft Sentinel |
| NSFOCUS | Intelligent Security Operation Platform (ISOP) |
| OpenText ( CyberRes) | ArcSight SOAR |
| Palo Alto Networks | Cortex XSOAR |
| QAX | QAX SOAR |
| Rapid7 | InsightConnect |
| Revelstoke | Revelstoke SOAR |

| | |
|---|---|
| ReliaQuest ( EclecticIQ) | EclecticIQ Platform |
| ServiceNow | Security Operations |
| SIRP Labs | SIRP SOAR Platform |
| Splunk | Splunk SOAR |
| Sumo Logic | Cloud SOAR |
| Swimlane | Swimlane Turbine |
| ThreatConnect | Intelligence-Powered Security Operations (IPSO) |
| ThreatQuotient | ThreatQ TDR Orchestrator |
| Tines | Tines |
| Torq | Torq Hyperautomation |
| Note: There are providers in this list that — while they offer a SOAR solution — in practice prefer to offer, and have more clients consuming, their SOAR solution as part of a larger offering. SIEM and XDR solutions are relevant examples of this situation today. | |

Source: Gartner (May 2023)