Emerging Technology Analysis: SOAR Solutions

Published: 7 December 2018 **ID:** G00372967

Analyst(s): Eric Ahlm

SOAR technologies promise to bring about automation, consistency and efficiencies in security operations centers beyond what is possible in SIEM today. Technology product managers at SOAR providers must understand the real value they bring to buyers, or face competition from evolving SIEM providers.

Key Findings

- Some basic security orchestration, automation and response (SOAR) capabilities may be consumed by the security information and event management (SIEM) market. However, SOAR is a distinct market unlikely to consolidate completely into a SIEM platform.
- The market opportunity for SOAR providers is limited to buyers that currently have or want to invest in building their own security operations center (SOC). Many enterprise buyers will choose to never build an SOC.
- The value propositions (and the related technical capabilities) for SOAR solutions come in one of three varieties: SIEM workflow automation, building a better investigation platform or building an operations management platform for the SOC.

Recommendations

To successfully exploit evolving security market dynamics, technology product managers at SOAR vendors must:

- Avoid being consumed as a feature by a SIEM provider by creating product visions and roadmaps that go beyond basic SIEM workflow automation.
- Develop offerings that appeal to non-SOC buyers, such as enabling service providers to offer SOC-like services, or greatly enhancing built-in intelligence features.
- Prioritize decision support for security workers and management-level program metrics in the solution roadmap to further differentiate against basic workflow automation as a function of a SIEM solution.

Table of Contents

List of Figures

Strategic Planning Assumptions

By 2021, 70% of enterprise organizations with a dedicated SOC will include SOAR capabilities, either through their SIEM solution or a dedicated platform, up from less than 5% in 2018.

By 2020, SOAR tools will begin to deliver credible decision support capabilities powered by advanced analytics, such as machine learning.

Analysis

SOAR technologies promise to bring about efficiency in SOCs, but will they emerge to solve a greater market need? Or will the capabilities to perform SOAR functions be consumed by the SIEM market? This note discusses the potential evolution of the SOAR market.

It's important to understand the origins of the SOAR market to best grasp the current trends. SOAR formed as a concept of the convergence of three technology solutions — security orchestration and automation, threat intelligence platforms, and incident response (IR) platforms.

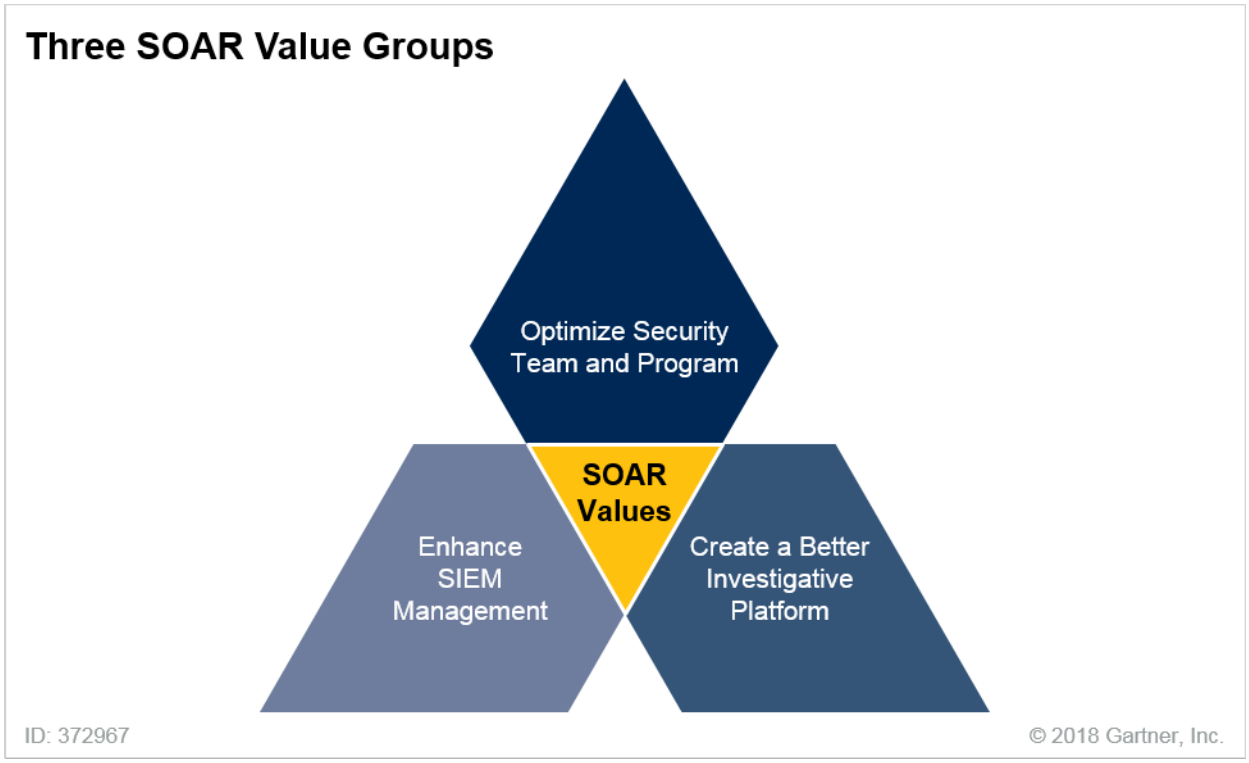
As such, there was no original SOAR vendor, but many vendors from distinct areas that began to create their own vision of a SOAR solution. Each vendor, however, was approaching the problem from different points of view or with different core competences. As such, SOAR vendors, although similar by definition, offer different value propositions to buyers (see Figure 1).

The different values from SOAR providers can be best grouped into three logical groups:

- Enhance SIEM management
- Create a better investigative platform
- Optimize security team and program management

Although these values may overlap or be somewhat inclusive, how a SOAR provider emphasizes one of these values over another will shape their market potential.

Figure 1. The Three SOAR Value Groups



Source: Gartner (December 2018)

No matter what value a SOAR providers puts first, SOAR solutions are distinct in the marketplace. They are not a next-generation SIEM tool, nor are they similar in function to forensics or governance management tools. This distinct and dissimilar value gives the SOAR marketplace, as an emerging technology, a high likelihood of not converging or colliding with other security markets. This is a positive indicator of growth for the market's foreseeable future.

Technology Description

Taken from "Hype Cycle on Threat-Facing Technologies, 2018":

> "SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from SIEM and other security technologies, where incident analysis and triage can be performed, leverage a combination of human and machine power to help define, prioritize and drive standardized incident response activities according to a standard workflow. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format."

The definition of SOAR is fairly broad, and, as such, has attracted a wide field of vendors fighting for market leadership. Many of these vendors have pivoted from their existing solutions to become a SOAR provider. As such, they tend to have very different subvalues, which can make them appeal more or less to a buyer based on the buyer's role and specific problems.

The Three Value Categories of SOAR Solutions

Enhance SIEM Management

The center of this value is tactical and tied directly to program objectives in security operations, specifically, the objective of being able to apply integration, automation and orchestration to functions related to the security analyst role in the SOC. Most often, this will be directly related to workflow around events coming from a SIEM tool. A key metric to compare solutions in this value segment is the ability to provide efficiencies to a team of SOC analysts in the tasks they most often perform in a SIEM solution.

Key Technology Features:

- Simplified (or abstracted) scripting, allowing for customer-side automation of SIEM functions
- Enrichment of SIEM events, making them easier to investigate or close

Create a Better Investigation Platform

This value is centered, again, on a security investigator, but the goal is helping the analyst perform better through the augmentation of their investigative abilities using system-side intelligence. Beyond the execution of static playbooks, these solutions endeavor to create a more complete view of any incident to the SOC analyst.

More visualizations and the ability for the SOAR solution to apply its own intelligence (analytics or machine learning) to augment the investigation are key differences. This might appeal to not only SOC analysts, but also other investigative or response teams within a buyer's organization.

These types of SOAR solutions can provide decision support for the investigator. SOAR platforms of this type might use another application of machine learning to guide the investigator in the tasks they should take. This provides additional value for the buyer, enabling the organization to better scale its team, making junior investigators more effective.

In addition to enhancing data for investigation, local indicators of comprise (IOCs) and other local-side intelligence can be gathered. This additional layer of intelligence is added by using analysis techniques to relate key information for extraction (and use as an IOC), or by watching lessons learned on true and false-positive events. Some SOAR providers may choose to gather this information in a smaller local-side data store to enhance their local and global threat intelligence data. This can be not only more effective than storing the same data in a SIEM solution, but also more cost-effective.

These systems also have the ability to be a data aggregator — for the purpose of investigation — but do not need to be the complete data store like a SIEM solution. This means, for example, that data from a SIEM tool, email server, cloud application and a few specialized databases can all be viewed (and investigated) in one place.

Key Technology Features:

- System intelligence beyond the created playbooks that aid in better incident investigation and management.
- The ability to relate incidents across very wide data sources, including non-SIEM data sources, such as email, cloud applications or any other helpful source, without the cost burden of putting the data in the SIEM tool.
- The ability to provide a decision support system that helps with critical items. For example, the systems can help with: "What did we do the last time something like this was seen?" and "Here is more context on this type of threat." This information allows end users to make better decisions, faster.

Optimize the Security Team and Program Management

Like the other two value categories, these products help aid investigative teams. However, the value in this category is greater than just programmatic automation or augmenting security investigators with greater investigation abilities. This is about giving security leaders a tool to make strategic decisions and operational decisions about their program with more context, faster.

The key is developing and tracking metrics around the operations performed in the SOAR solution by team members. For example, which processes created by the investigative team are most important to the company? Which are the least effective? How much could team operations be

reduced by adding a new preventative security control or measure? Which team members perform best, and which ones need more training?

In essence, a SOAR platform has the potential to be the manager's system of record and tool of choice for management optimization, based on analysis of data around actual operations. This value could extend beyond SOC managers to other layers of the organization's security management including a chief information security officer (CISO).

Key Technology Features:

- Manager dashboard on key team operations and programwide metrics
- Use of machine learning or other automated analysis methods on the operations that can highlight systemic, process or people problems that would lead to program betterment

Technology Adoption

The adoption of SOAR solutions is dependent on which enhancement the buyer is seeking for their organization for threat investigation. Sometimes, they might not be seeking enhancements.

A small, yet important point about SOAR solutions: they don't fully automate the entire process of investigating all security events. They add automation and other enhancements to people that investigate events.

As such, the value of a SOAR solution to a buyer with no dedicated investigative team members will be a hard sell. Buyers with a virtual or moderately sized investigation team might only desire basic automation and scripting around functions they already do in a SIEM solution. Buyers with larger investigative teams will seek not only a SOAR solution that helps their investigators, but also solutions that can add to overall program optimization.

The size of the buyer's team that investigates threats is the most important qualifying point as to whether that buyer will seek a SOAR solution or not.

Factors That Will Drive Adoption

SOAR solutions can solve a range of buyer problems related to security investigation, such as in an SOC. As such, a number of market trends and factors are positioned to drive growth of the SOAR market. If the following trends persist or increase, so will the growth of the SOAR market.

Automation Is the Only Way Forward in Scaling an SOC

Cutting dwell time of hackers is a key metric for security program success. Cutting dwell time requires a commitment to investigating events and resolving security issues within an organization.

The primary issue is there are too many security events and not enough people to work through them all. Additionally, for the events people can get to, they don't have enough context to make a good decision in the time frame they have to make a decision. Today, it's a problem of scaling security operations. The factor that will drive the SOAR market is if traditional methods to scale an

SOC fail, a new shift in approach is required. Gartner believes that shift will be toward an "automate first" mentality in the SOC, and SOAR platforms will be the tool of choice to do just that.

Traditional methods, such as hiring, training, custom-scripting and process optimization, have all been tried. If ground-up, automate-first methods, such as those in SOAR, prove to be measurably superior in reaching high-level program goals (such as reducing dwell time), then the SOAR market is well-positioned for future growth.

Threat Complexity Forces Better Investigative Context

Threats are becoming more complex, multifaceted and easy to miss if you are only looking at one piece of the investigation puzzle. It takes collaboration from various security technologies, and great use of the data coming from external and internal sources to understand the big picture of which threats are truly a problem for an organization. It takes collaboration, context, system intelligence and visualization to really solve modern security problems.

The need to better relate, visualize, and use any and all data to solve threat investigation is a driver for the SOAR market. SOAR solutions don't require all point security solutions to be integrated to each other, nor do they require all data of interest for an investigation to be stored in one place — like a SIEM solution does. SOAR solutions simply bring and relate the right data to be used by investigators, thus simplifying the investigative process. All of this can be done without massive systemic integration, expensive data storage duplication or rearchitecture.

Security Programs Require Modern Management Platforms to Thrive

As organizations continue to explore new ways to do business, a well-run security operations team that can better manage risks by making better decisions, faster becomes increasingly important. As such, a manager of security programs will be faced with making increasingly strategic decisions, not only about their organization, but also how their program relates to companywide goals. Making these management-level decisions is hard, but making them without any data is near impossible.

SOAR is positioned to be the security manager's decision platform of choice. A SOAR platform can capture team management and program data just by watching and tracking how people, processes and technologies do their job. For example, which security technology investment did the most work last year, and which should be turned off? Which process in the SOC reduces the most risk, and which causes the most friction with other business units? Which security analyst should be promoted, and which should receive more training?

As making more strategic security decisions becomes more important to companies betting big on leveraging new and emerging technology to grow, so will the SOAR market, which can deliver program optimization metrics.

Factors That Will Inhibit Adoption

Several factors could inhibit the SOAR market's future growth.

Buyers Decide to Not Build Out an SOC Themselves

An SOC can't run without qualified people trained in security threat analysis. No toolset can fully automate all of the functions done by the humans of a security operations team. Despite the efficiency benefits that a SOAR solution can bring to buyers looking to set up an SOC, the reality is that many buyers may opt to not even build an SOC.

As such, they won't budget for or spend on optimization tools such as SOAR. More likely, these buyers will seek a service provider to do more of these investigative functions for them. SOAR product managers can get ahead of this potential market inhibitor by enabling service providers to deliver new services for buyers with no plans for an SOC based on the buyer's platform.

Buyers Only Value Basic Automation of SIEM Functions

As distinct as the SOAR market might be, there is certainly a degree of overlap with SIEM solutions. This is evident by the acquisition of Phantom Cyber by Splunk, Komand by Rapid7, and Resilient Systems by IBM. Also, other SIEM providers are now including more SOAR-like functionality as enhanced feature sets.

A potential inhibitor to the SOAR market is that many buyers will have their SOC optimization needs fulfilled by their current SIEM provider rather than buy a stand-alone SOAR solution.

As stated in earlier, a SOAR solution can bring different values to a buyer. The risk to the SOAR market is that if buyers only want to automate functions around the workflow of SIEM events, then SIEM solutions that can automate investigative and workflow functions through playbooks are well-suited for the job. Customers that are okay to only work on data in the SIEM solution, or add new data to the SIEM, will likely choose this path over a stand-alone SOAR solution.

Technology Impact

A number of adjacent markets have degrees of overlap with SOAR solutions and may be impacted as SOAR grows, or may themselves be a factor that impacts SOAR's growth.

SIEM

Of all the markets adjacent to SOAR, SIEM is the largest market in terms of revenue. Although there is a degree of technical dependency on SIEM for SOAR solutions to function, the overall market dependencies between the two are low.

What is more likely is that a portion of the SOAR market will be consumed by SIEM providers that have integrated SOAR-like functions into their platforms. SOAR providers that only focus on the value of enhancing SIEM events are likely the first to be consumed by SIEM providers.

IR Tools

IR tools, in this context, refer to vendors that make forensic capture devices that aid SOC analysts in their investigations. These can include full packet capture devices, and network session record and playback.

SOAR is in no way a replacement or alternate for these systems, as SOAR solutions do no capture. As such, it's unlikely the SOAR market will consume IR tools. However, SOAR might slow the growth of the IR tools market for buyers that seek to use them not only for capture, but also for investigation.

IT Operations Management Software

Although the responsibilities of security should be independent of IT, security operations are in fact a subset of IT operations. One can also say the way to resolve things found by security operations is to kick off a request for more IT operations (such as go fix a system, or rebuild or repair that comprised system). As such, some customers will want tighter integration of the management platforms that watch both IT and security operations.

If this trend takes hold, the SOAR market could be threatened by providers that can span their platform between both IT and security operations, and offer increased value to buyers by nature of the integration.

Integrated Risk Management (IRM) Platforms

Earlier definitions of SOAR included some capacity for risk management, in addition to SOC and investigation management. Gartner has since removed risk and governance management capabilities from the SOAR market description. However, some providers still offer both.

As such, there could be some market dependencies between SOAR and IRM in use cases where the SOC manager is seeking to manage both their SOC program and risk more tightly.

Vendors of Interest

- Anomali
- Ayehu
- D3 Security
- Demisto
- DFLabs
- EclecticIQ
- IBM Resilient
- ServiceNow

- Siemplify
- Splunk (Phantom)
- Swimlane
- ThreatConnect
- ThreatQuotient
- TruSTAR

References

"Hype Cycle for Threat-Facing Technologies, 2018"

"Forecast Analysis: Information Security, Worldwide, 2Q18 Update"

Gartner Recommended Reading

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

"Innovation Insight for Security Orchestration, Automation and Response"

"Preparing Your Security Operations for Orchestration and Automation Tools"

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp