Siemplify

PRAGMATIC SOAR SELECTION

GOING BEYOND THE CHECKLIST

WHITE PAPER

Introduction

With the explosion of security technologies in the marketplace, there is no shortage of choices when it comes to securing a business. While on the surface this is good news, it does not take long to realize that identifying the right solution mix to address specific security challenges is extremely difficult. With many security vendors touting similar, if not the same, capabilities and benefits even deciding who to short-list can be challenging.

In a perfect world, there would be enough time and resources to meet with all vendors, perform detailed proof of concepts of each technology, and negotiate for the best price/contract from everyone, but that is not possible. The purpose of this document is to provide security buyers a pragmatic approach to selecting one of the most important, if not most important, security tools for the Security Operations Center (SOC): A Security Orchestration, Automation, and Response (SOAR) technology.

This process goes beyond the "checklist" approach to selection by outlining a simple, yet thorough, way to ensure the SOAR platform meets the needs of the business. This paper begins with a short discussion on the origins of SOAR platforms and the different types of SOAR solutions available. Next, several considerations are discussed that should be included in the criteria for technology selection that go beyond the straight functionality of the product. Finally, the paper describes a simple approach to evaluating a SOAR solution in a business environment. Of course, every business need will vary so the intent here is not to define a single process all security buyers should follow. Rather the intent is to provide a roadmap of activities and considerations that help make the difficult process of selecting a SOAR technology as easy as possible.

SOAR Origins

Years ago, when attacks were infrequent, and antivirus was an effective security control, security professionals did not need a tool designed to orchestrate and automate incident response. Today, however, things are quite different. While security professionals could debate why SOAR solutions exist three reasons would more than likely garner widespread agreement:

- Threats continue to escalate at a breakneck pace
- Complex security stacks are causing analyst fatigue
- Lack of security experts makes consistent investigation and response challenging

Threat Escalation

In the early days of computing, cyber-attacks were few and far between. Antivirus (AV) software was generally all that was required to combat these limited attacks. Today, however, hundreds of thousands of new pieces of malware are discovered daily. This escalation is in addition to new techniques attackers are deploying to compromise organizations. To stay ahead of the attacker's organizations must adopt multiple security tools, increasing the complexity of their security stack.

Complex Security Stacks

It is not uncommon for an organization to have more than a dozen security tools running simultaneously to identify, and ideally prevent, successful cyber-attacks. Unfortunately, this results in a complex security stack with increased overhead, both in terms of cost and analyst time. With numerous dashboards to monitor and a continuous stream of alerts coming into the SOC daily analysts are fatigued from fighting what seems to be a losing battle. However, the overwhelming reason SOAR technology came into existence is not threats or security stack complexity -- it’s people.

Resource Scarcity

The increase in attacks and security tools has driven a significant increase in the demand for trained security professionals outstripping the available resources. Due to this scarcity, many security teams are made up of security professionals and IT generalist with limited in-the-field security experience. Even for organizations that have sizable security teams and an ample budget to add additional headcount, finding a person with the desired security skills is daunting. This lack of resources has been validated by many research organizations, estimating the gap between available security-trained resources and open positions to be upwards of three million people over the next ten years.

Types of SOAR Solutions

In general SOAR solutions take alert data from a security control, such as a SIEM, and using predefined workflows take automated actions, from enrichment to fully automatic response, to make security analyst more effective. For SOAR solutions to be successful, however, they must integrate with a wide swath of security and IT tools and support custom response workflows.

Beyond the basic table stakes (see appendix for the "table stakes) of SOAR solution, many vendors develop their tools to target certain types of organizations or focus areas. According to Gartner1, SOAR solutions fall into three distinct groups: IR Focused, Orchestration and Automation Focused, or TI Management focused. There is a fourth group of tools emerging that combine IR, orchestration, and automation capabilities with capabilities to improve overall SOC performance. We will call this group SOC Focused, or SOC Centric. Finally, in addition to the Gartner classification and the newly emerging group, there is another set of solutions that are SOAR adjacent. These tools developed for another purpose, potentially general IT management and have been modified slightly to deliver scalable case and incident management.

Incident Response

Incident response (IR) focused SOAR solutions deliver capabilities required to recover from a successful breach or compromise. These solutions provide user-centric capabilities around workflow, ticket, and case management with emphasis on collaboration features as well as ensuring proper handling of case information associated with a successful breach.

Since these tools focus on incident response and less for determining if a successful breach did occur, they may not enable fully automated responses or extensive threat intelligence and external tool integration. That said these tools are generally a good choice for IR teams that need to act quickly to recover from a widespread breach.

Orchestration and Automation

If IR-focused solutions have recovering from a successful compromise in mind, orchestration and automation tools have the technology in mind. Their goal is to make the integration of the security stack as easy as possible with a wide variety of pre-built integrations into the most common security controls in the market.

They also will generally provide an integrated development environment (IDE) where security engineers and architects can create custom integrations. From an investigation standpoint, these tools focus on automation above all else. This focus means playbooks, while robust in their ability to reach out to other security and IT tools for data, offer minimal capabilities to support manual investigations or the management of analysts' time. This type of SOAR solution is primarily useful for organizations trying to reduce the number of false positive alerts and automate Tier 1 investigations.

Threat Intelligence Management

The final Gartner defined category of SOAR solutions is very specific in its nature and applicability. Threat Intelligence (TI) Management focused SOAR solutions are ultimately designed to make the ingestions, consolidation, and sharing of TI easier.

These tools capture TI from third-party sources and consolidate the data in a single user interface an analyst can query. So, in this context, the orchestration and automation are focused on TI and not overall IR. To that end, this type of SOAR solution would more than likely be useful as an add-on to an existing SOC management tool and not as the primary SOAR solution.

SOAR Adjacent

SOAR adjacent solutions are designed to provide a minimal set of SOAR-like capabilities to enable users to implement basic orchestration or automation. These tools are not for a pure security use case; however, based on customer demand vendors in this space have delivered add-on modules that positioned as SOAR solutions. Advanced capabilities are generally not available in these SOAR adjacent solutions.

SOC Centric

SOC Centric SOAR solutions take a different approach to solving the security challenges faced by organizations. These solutions are designed to be the hub of the SOC where analysts, security engineers, security architects, and SOC managers have a single view into all alert and case activity.

Also, SOC Centric solutions deliver real-time metrics on analyst performance to assist SOC managers in making data-informed decisions when it comes to staffing and case assignment. These solutions deliver automation and orchestration capabilities intended to cut down on triage and investigation time, driving up analyst efficiency and overall SOC performance. SOC Centric solutions are a good choice for most organizations dealing with a large volume of alerts from their SIEM or other alerting technology and have a strong desire/need to improve analyst efficiency.

Going Beyond the Checklist

Now that we have discussed the reason SOAR solutions are needed to combat some serious challenges facing today's modern security teams, we will now turn to our attention to defining a process for selecting a specific SOAR solution.

Primary Objective

According to Gartner1, three general use cases drive SOAR solution adoption. While it is not uncommon for security teams to have competing priorities, it is important to identify the most compelling use case and make the appropriate selection. While the use cases Gartner defined do encapsulate the primary drivers for a SOAR solution, it is equally important to keep in mind a fourth use case that should cut across all use cases; the need to improve SOC management.

SOC Management

Recently leading SOAR solution providers have incorporated capabilities to manage and optimize day-to-day analyst activities. Capabilities such as shift handover, case assignment, and collaboration that when combined with the core SOAR solutions features can significantly improve the performance of the entire SOC.

Additionally, these solutions provide real-time measurement of analyst performance, as well as trending information on important metrics such as mean time to resolution (MTTR) and which security controls are contributing the most cases. When identifying the primary use case for the adoption of a SOAR solution, make sure not to lose sight of the equally important ability to drive improved SOC management.

SOAR Prerequisites

When a new technology such as SOAR emerges, it is tempting to rush to a selection and implementation with the expectations that the stated benefits will materialize quickly. Unfortunately, this is not always the case. To give a SOAR solution the best possible chance to deliver benefits, it's imperative an organization has, at a minimum, the following prerequisites:

- **Alerting technology deployed**: SOAR solutions are intended to make sense of the sea of alerts generated by a security stack; however, if no alerts exist SOAR solutions cannot deliver their stated value. Generally, the best source of alerts for a SOAR solution to ingest come from a SIEM, however other alerting tools, such as EDR or DLP, can be used as well.
- **Investigation and response workflows**: The ability to normalize investigation and response built into SOAR solutions can drive real improvement across the SOC. If the organization does not have formal processes defined the SOAR solution process will push the SOC team to define these processes. Fortunately, some SOAR solutions do make creating those workflows from scratch in the system simple. However, it's important that the internal SOC team bring their expertise into the process to ensure the workflows defined meet the individual business's need.
- **Resources:** SOAR solutions make existing SOC resources more efficient; however, if there are no resources dedicated to reviewing and acting on the results of the SOAR solution cannot deliver their stated value.

Detection and Triage

Some may think detection as an odd objective of a SOAR solution deployment. However, detection is not necessarily a point-in-time activity. In certain situations, detection represents a continuum of action. An example will help clarify this use case.

Brute force attacks are quite common in that there is a very low barrier of entry for the attacker. All he or she needs to do is to identify a user name or names, a network IP, and a set of potential passwords. Organizations wishing to identify these types of attacks will create rules in their SIEM that will be triggered if X number of failed logins occur in rapid succession. The problem, however, is that many of these failed logins are valid so security analysts get flooded with alerts that are, in fact, false positives. SOAR solutions can assist by providing a secondary detection function by analyzing data associated with the failed login, such as IP address, to automatically close these alerts without any human intervention, saving significant analyst time.

Similarly, organizations can make use of SOAR solutions to perform triage of alerts for analyst review. SOAR solutions can add valuable information to an alert that a SIEM does not have access to such as third-party threat intelligence, additional metadata from the assets in question as well as scour previously handled alerts of the same type to determine their resolution.

Incident Response

Organizations may also seek out SOAR solutions to structure the incident response process to drive consistency across analysts. It is quite common for SOC teams to include analysts of different skill sets. Fortunate organizations may have several seasoned analysts who have developed comprehensive response processes enabling them to complete investigations quickly. However, many times these processes are in shorthand that makes sharing across the SOC team problematic. With a SOAR solution, these critical playbooks (sometimes called runbooks) can be converted into workflows in the system that all analysts can use. This benefit, by itself, can make the investment in a SOAR solution worthwhile.

Much like the triage use case, enrichment of alerts is also part of the incident response use case. Having insightful data added to the alerts automatically can dramatically shorten the investigation time, especially for time-consuming investigations.

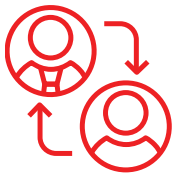
Threat Intelligence

The final use case driving SOAR solution adoption is the need to aggregate threat intelligence from multiple sources into one easily searchable portal. So, for instance, if the organization subscribes to multiple threat feeds, analysts in the SOC may be forced to manually copy and paste threat intel into their investigation platform without a SOAR solution. However, with the SOAR solution in place, analysts can easily interact with the threat intel speeding the rate of case closure.

Whether driven by SOC management, detection, and triage, incident response, or threat intelligence it is important to ensure that a primary driver is identified to ensure that the correct type of solution is selected. Beyond the use case, several other considerations must be part of the evaluation process

Other Considerations

While it is straightforward to compare the technical features of multiple SOAR solutions, it is important that when making this important investment the selection team look beyond the mere technical merits of the solution and apply additional criteria to the evaluation. Below are several key considerations to include in the SOAR selection process.



Staffing

While it would be ideal if every organization were sufficiently resourced, as discussed earlier that is not the case. Some businesses are stretched thin across multiple shift days with limited to no advanced analysts on staff. In this case, it will be important to pick a solution that is easy to use with built-in workflow. Alternatively, for the lucky few that have security teams with years, or decades, of experience under their proverbial belt, bringing in a tool designed for the novice, or beginner security analyst, may fall flat.

When considering a solution ask the vendor this question directly, “who is your product designed for?” If given an “everyone” answer it’s advised to push harder for more clarity. While vendors may strive to deliver a “one-size-fits-all” solution, it is highly unlikely to be the case. Some tools will lean towards a more experienced user offering more of a toolkit requiring manual configuration. On the opposite end of the spectrum, some tools will deliver a very basic user interface with limited customizable options. Regardless it is imperative that the selected tool maps to the SOC team makeup.

Budget

Budget is an obvious consideration when selecting a SOAR solution. However, it’s important to obtain an all-in cost for the solution before making any decision. SOAR solutions may be priced in several different ways: by the user, by automation, or by another variable such as organization size.

Comparing solutions priced differently will require some analysis. It is also worth noting that, out of the two most common pricing models (per user or automation), per automation pricing brings with it the most variability and costs can escalate very quickly.

The Pragmatic SOAR Solution Selection Process

Below is a simple SOAR solution selection roadmap that can help eliminate wasted time and missed expectations. It is worth noting that this is a general process outline; in certain situations, some of these processes may be combined or eliminated. No matter which steps are removed, or added, following a defined, well thought out selection process will make selecting the appropriate solution for the businesses needs easier.

Selection Team

The SOAR solution selection team should be structured as follows:

- **Executive Sponsor:** Projects always go smoother if an executive with the power to push through a contract, and protect the budget from being diverted, is part of the selection team from the onset. The executive sponsor could be anyone from the CISO, CIO, or even a senior executive from the Risk and Compliance team.

- **End Users (SOC Analyst):** One of the most common mistakes made during the selection of a SOAR solution is to exclude the end users from the evaluation team, relying on the technical evaluator alone to make the selection. All too often this results in selecting a solution that may meet the technical requirements outlined but misses the mark when it comes to usability. Make sure to include a representative group of SOC analyst with varying skills and abilities to ensure the chosen solution matches the team's capabilities and expectations.

- **Technical Evaluator (Security Architect/Engineer):** Including a security engineer in the selection team will ensure the security stack is properly integrated with the SOAR solution so a full evaluation can occur. Additionally, a security engineer/architect can push the vendor to provide detailed technical information to avoid a scenario where the vendor is minimizing/obscuring the technical complexity of the solution.

Selection Criteria

The selection criteria should include everything discussed in this paper but need not be overly complicated. Fortunately for the selection team, many features can be assumed to be available from all credible SOAR solution vendors, such as alert ingestion and support for third-party integrations. That said, the selection criteria should include the existing security controls in use so that, at a minimum, to verify the availability of integration support.

Research

With the selection criteria finalized, a member (or multiple members) of the selection team can begin researching potential vendors. Fortunately, a good portion of this information is available via self-guided research. Scour the vendors' websites for datasheets, webinars, videos, specifications, and case studies. Once freely available information is collected and reviewed reach out to the top three vendors to set up initial meetings.

The "Demo and Decide" Trap

With so much upfront work completed there will no doubt be a desire to have the vendor immediately demonstrate their solution to the selection team. Unfortunately taking this approach will decrease the usefulness of the demonstration. The recommended approach is to set up a meeting where the vendor presents its SOAR approach and solution differentiation.

The initial meeting will allow the selection team to immediately determine if the vendor's approach (IR, Orchestration, Automation, or TI focus) maps to the primary use case driving the SOAR solution project. The selection team can also begin to gain a sense of vendor fit before diving into the demonstration. Assuming these initial discussions are favorable, a secondary meeting should be scheduled where the selection team will see a demonstration of the solution. Will all demonstrations completed the selection team should review all the criteria and select the top two vendors for a proof of concept (POC).

The POC

The POC is the organization's opportunity to put the selected vendors' solution through the paces in their environment. While not recommended to POC in a production environment, the testing environment needs to mirror production as closely as possible. It is especially important to simulate integration to the deployed security controls. Further, the testing environment needs to be seeded with a good cross-sampling of the types of alerts typically encountered. Keep in mind the makeup of the SOC team when performing the POC. Several SOC analysts should dedicate time to working with the solution, user interface attempting to complete common tasks with the product.

It is critical that the POC be tied directly back to the primary use cases identified earlier in the process. So, for example, if the primary use case is detection and triage, develop several specific scenarios where detection and triage can be tested, such as examples of phishing and brute force attacks. When testing these specific scenarios ensure to test from beginning to end. For example, ensure proper data ingestion, playbooks actions occur appropriately with the expected enrichment occurring, and the investigation workflow is logical. In short, without a properly developed POC plan, the evaluation team will struggle to gain a complete picture of the product, and further have difficulty comparing products to each other.

Before closing out the POC process, have the vendors present the results of the POC use case scenarios, giving them the opportunity to discuss any unexpected results. Finally, request that the vendor share their short and long-term roadmaps to ensure a plan exists for continued product development.

Making the Decision

With the POC complete now is the time to make the selection.
Review in detail the requirements set at the beginning of the process against each vendor's results. Be prepared to reach back out to the vendor to get clarification on responses to complete the data analysis. If each vendor did not answer the following questions, provide them with the opportunity to do so before the final selection.

1. Does the SOAR solution integrate with all my security controls? If not, how can they be integrated?
2. Can analysts build and modify custom playbooks?
3. How do analysts and playbooks work together?
4. Does the SOAR solution have built-in collaboration/workflow support?
5. Can the SOAR solution track individual analyst performance?
6. What kind of workload improvement will the SOAR solution provide?
7. Does the SOAR solution group alert into cases?
8. Does the SOAR solution provide automated context?
9. Does the SOAR solution support simulation to test playbooks?
10. What could cause unexpected changes in the cost associated with the SOAR solution?

With all the testing complete and questions answered the selection team could make an informed selection.

Conclusion

When securing a business was simple, organizations could get by with a simple security solution, but not today. To deliver consistent results and security across a diverse environment SOC teams need a SOAR solution capable of automating investigation and response actions, enabling analysts to be more efficient, security engineers to be more effective, and SOC managers to be more informed about the activities in the SOC When selecting a SOAR solution, it's important to look beyond the "speeds and feeds" of the tool and evaluate the solution holistically. There is no "one size fits all" when it comes to SOAR solutions, so it's critical that the evaluation team identifies the driving use case for the SOAR solution, considers staffing, and budget, as well as vendor fit when making a selection. With proper planning and execution, the selection of a SOAR can be one of the most impactful projects completed by the SOC team.

References:

1 - Preparing Your Security Operations for Orchestration and Automation Tools, 22 February 2018, ID G00325580, Analysts: Anton Chuvakin and Augusto Barros, Gartner.

Appendix

The Table Stakes

The purpose of this paper was to go beyond the table stakes of a SOAR solution; however, it is quite possible that the reader of this paper does not have a succinct list of the basic SOAR capabilities each solution must provide. To that end here is a short table stakes list of features for easy reference

Feature	Capability Description
Alert Ingestion	The ability to ingest alerts from a security control, generally a SIEM
Alert Visualization	A means to review alerts via a user interface
Alert enrichment	Ability to add additional information to an alert to give analysts more insight
Playbooks (or Runbook)	A way for analysts and security engineers to define a set investigation and response process that can be used by all analysts in the SOC
Reporting	Ability to collect metrics around SOC performance
Integrations	Ability to connect a variety of security, IT, productivity, and web-based applications into the tool for alert enrichment, investigation, and remediation/response actions.

Sample Selection Criteria Sheet

Criteria	Vendor 1	Vendor 2	Vendor 3
Solution Focus (IR, Orchestration/Automation, Threat Intelligence, SOC Centric)			
Integration Support (List out security controls in use)			
Tech Features			
Pricing Model			
Customer Service Model			
Roadmap			
Customer References			
Staff (Who is the solution built for)			
Budget (purchase plus recurring)			

About Siemplify

Siemplify is a security orchestration, automation and response (SOAR) provider that is redefining security operations for enterprises and MSSPs worldwide. Its holistic security operations platform is a simple, centralized workbench that enables security teams to better investigate, analyze, and remediate threats. And, using automated, repeatable processes and enhanced measurement of KPIs, Siemplify empowers SOC teams to create a culture of continuous improvement. Siemplify's patented context-driven approach reduces caseload and complexity for security analysts, resulting in greater efficiency and faster response times. Founded by Israeli Defense Forces security operations experts with extensive experience running and training numerous SOCs worldwide, Siemplify is headquartered in New York with offices in Tel Aviv.

Siemplify

siemplify.co