WHITE PAPER

# 10 Essential Capabilities of a Best-of-Breed SOAR

Respond to threats faster with security orchestration, automation and response

splunk>

turn data into doing

## Cybersecurity is evolving

If you ask security professionals about the challenges they face working in cybersecurity, odds are, you'd hear some common themes. These include (but are certainly not limited to):

- A shortage of skilled cybersecurity talent.
- A high volume of security alerts.
- Too many security point-products to manage.
- A lack of integration between those products.
- Inability to scale security operations over time.
- Increasing costs and shrinking budgets.
- Increasing sophistication of malware.
- Slow speed of threat detection and response.

Considering these challenges, it's no surprise that security teams feel perpetually overwhelmed.

Many teams have turned to security orchestration, automation and response (SOAR) tools as a remedy. A SOAR solution can orchestrate security actions (like investigations, triage and response) across various security products in a team's arsenal, and automate otherwise manual repetitive security tasks.

But not all SOAR solutions are created equal. A best-of-breed SOAR solution will provide a set of capabilities that can completely revolutionize your team's approach to security operations. These capabilities will allow you to:

- Work smarter by automating manual and repetitive tasks.
- Respond faster and reduce dwell time with automated detection, investigation and response.
- Help your security team automate security operations and free up time to focus on other strategic activities.

The following are the 10 essential capabilities of a best-of-breed SOAR solution, which will help your security team go from overwhelmed to in-control of their security operations.

| Essential capabilities of a best-of-breed SOAR | |
|---|---|
| Orchestration | This is the machine-based coordination of a series of security actions across a complex IT ecosystem. This helps everything work in concert, while automating tasks across products and workflows. |
| Automation | The machine-based execution of security actions with the power to programmatically detect, investigate and remediate threats without requiring human intervention. Security automation does most of the work for analysts, so they no longer have to weed through and manually address every alert as it comes in. |
| Event and Alert Management | After data is ingested into a SOAR solution, inbound alerts should be queued up and prioritized. Investigations should then be performed using manual or automated actions to yield the highest level of productivity and accuracy. |
| Threat Intelligence | Security teams should be able to tap into the latest threat intelligence without exhausting their resources. Effective threat intelligence should also include scoring options to determine which threat intelligence sources analysts should focus on. |
| Case Management and Collaboration | Case management should take a broader, cross-functional view of an incident's life cycle, all the way from creation to resolution. Multiple alerts and/or events should be able to be confirmed, aggregated and escalated as a single case. This, in turn, enables effective collaboration and communication across the organization's security team, thereby accelerating the resolution of security events. |

| | |
|---|---|
| Metrics and Reporting | Metrics and reporting are necessary for understanding and quantifying pretty much anything, and a SOAR solution is no exception. Metrics are the way to gauge a SOAR solution's effectiveness, and to also identify where improvements can be made to improve ROI. |
| Mobility | It's vital for a SOAR solution to offer access, interactivity and control of the platform from the convenience of an analyst's mobile device. This way, analysts can run playbooks on the go, review security artifacts and triage events without opening a laptop, respond to prompts from the palm of their hand, and always be reachable regardless of where they are. |
| Scalability | A SOAR solution should grow right along your organization. As more use cases are added over time, the platform should be designed in a way that allows for vertical scaling by increasing hardware resources (for example CPU and RAM) and horizontal scaling by increasing the number of server instances supporting the deployment. |
| Open and Extensible | A SOAR solution should be designed for openness and extensibility. It should easily incorporate new security scenarios, new products, new actions and new playbooks. |
| Community Powered | A SOAR solution should support a community model by adopting an open ecosystem for app development. This helps promote long-term success by avoiding vendor lock-in, and technologies can easily transition in and out without negatively impacting automated playbooks. |

Let's take a deeper look at each of these capabilities:

### Orchestration

When a security team responds to a security incident, they use a multitude of different security tools. Each of these tools plays a different role within a defined workflow. For example, you can tell VirusTotal to check a file's reputation, use your firewall to block an IP, and then use your endpoint security tool to block an executable. Without orchestration, the security team would coordinate these workflows manually. But a SOAR solution can integrate across all of these deployed security tools via APIs, and then coordinate workflows across these tools to detect, investigate or respond to specific security incidents. For comparison, if your security tools are instruments that make up a symphony orchestra, your SOAR solution is the conductor, ensuring that every instrument is playing in sync and on time.

When evaluating a SOAR solution, the orchestration function should direct and oversee all activities relating to a given security scenario from beginning to end, as well as be able to ingest security data from any data source and in any format. Furthermore, an orchestrator should ensure that the output data from one action is properly parsed, normalized and structured so that future actions can make use of it.

### Automation

For most security analysts, their day is filled with too many repetitive and mind-numbing security tasks or actions. These actions are manually executed by the team. Automation using playbooks should allow the security team to execute a collection of these actions in seconds, versus minutes or hours — and sometimes even days or weeks. For instance, phishing investigations that may require the use of multiple actions across four to five different security tools, and take approximately 40 minutes to perform if done manually, should now take under a minute using an automated playbook. In this way, SOAR tools can drastically reduce mean time to detect (MTTD) and mean time to respond (MTTR).

Playbooks should be easy to create and modify. The automation editor within a SOAR solution is where an analyst or manager codifies their processes into automation playbooks. The editor should allow for both source code editing and visual editing. This allows all security team members, regardless of preference or coding expertise, to construct comprehensive and sophisticated playbooks. While constructing the playbook in a visual editor, the resulting playbook source code should be generated in real time and be accessible to the author — with seamless toggling and editing between the visual and source code editor.

### Event and alert management

Just after data ingestion, event and alert management should queue up and prioritize inbound events and alerts. This means alerts can be rapidly consumed and efficiently acted upon, without extensive searching or switching between contexts. Events and alerts should include a status indicator (e.g., new, open or closed), a severity indicator, and a color-coded sensitivity indicator to facilitate quick consumption of information. The technical attributes of a security event or alert should be organized to allow for rapid understanding of the security scenario. This includes an organized view of data like IPs, domains, file hashes, user names and email addresses. A security analyst should be able to seamlessly issue investigative, containment or response actions (or a collection of actions, i.e., playbooks) against this data.

Finally, the SOAR solution should provide a comprehensive activity log that displays a record of all actions that have been executed against an event or alert, whether they were initiated manually or via a playbook. Each action should display its results, including an indicator of action success or failure.

### Threat intelligence

Threat intelligence is key to helping analysts understand the threat actor's actions and mitigate any further damage to the organization. There are a few varieties of intelligence — strategic, technical and operational — that are collected and consolidated from both external and internal sources. Once the intelligence is aggregated into one single location, the data is then evaluated in the context of its source and reliability and analyzed to determine which pieces of data are important to help make rapid and effective decisions.

Many security teams today are using threat intelligence to provide relevant context and intel pieces that help analysts understand the threat. However, they are often toggling between a number of product interfaces to understand how different pieces of information are connected. Even with the use of threat intelligence feeds, it can send an overwhelming amount of indicators that would be impossible to track down manually. With the use of orchestration and automation, security teams can quickly view the aggregated pieces of information on one single platform and make quick informed decisions that can be automated without any human interaction.

### Case management and collaboration

Once alerts or events are confirmed and escalated, case management component should take over and drive a broader, cross-functional lifecycle from creation to resolution. SOAR will take multiple events and then confirm, aggregate and escalate them into a single case. The case management interface should support attaching relevant technical data such as the alert's source data and action results to the case. The interface should also support attaching relevant non-technical data such as notes, memos, emails, screenshots, recordings or any other arbitrary file with relevance to the case. Any changes to a case should be logged in an audit trail and be exportable.

Case management should also easily map to an organization's existing processes. Many organizations have developed standard operating procedures (SOPs) for incident response. The case management functionality should provide a user with the ability to define stages according to their process and save them as a template. A user should have the ability to break the SOP into multiple stages where each stage has one or more tasks, and each task can be assigned to an owner. The interface should provide an indicator of progress for the case as well as the case status.

A best-of-breed SOAR solution should include built-in collaboration features. Collaboration features like integrated chat and the ability to attach and share case notes should be available alongside the investigation or response workflow to provide incontext collaboration. With real-time chat and notes alongside event, alert and case information, analysts can achieve a level of situational awareness that allows for efficient and fast resolution of security incidents. This also creates an easy audit trail. It's ideal for the record of this collaboration to be captured and organized alongside the relevant event data and actions that were captured. That's not so easy if your communication is on an external tool, separated from the workflow information within your SOAR solution.

### Metrics and reporting

A security team must be able to easily measure the state of their security operations, and drive toward continuous improvement over time. Therefore, robust metrics and reporting are a must-have. They help the security team understand the impact of automation, and where improvements can be made to increase ROI.

Automation is used to increase efficiency across multiple functions of a SOC (security operations center). It's critical to understand the quantitative performance gain and resource savings that automation provides, and to have this information readily available via a dashboard.

Examples of key performance metrics that should be available within SOAR includes mean time to resolve (MTTR), mean dwell time (MDT), analyst hours saved through automated execution, number of full time equivalents (FTEs) gained through automated execution, average time saved per playbook run, money saved (FTE-cost x FTEs-gained), total number of open alerts, alerts opened and closed per day (hour, week, month) and performance against service level agreements (SLAs). All of this information should be easily organized and aggregated into reports for upper management and CISOs to quickly understand the overall state of their security operations as well as the improvements that SOAR is driving.

### Mobility

SOAR solutions are designed to accelerate response times. To achieve rapid response, security analysts need to be reachable when a case or security prompt requires human intervention. But analysts are not always sitting at their desk with their laptop open, ready to answer prompts at a moment's notice.

That's why it's important to offer access, interactivity and control capabilities from the convenience of the analyst's mobile device. This way, analysts can run playbooks on the go, review security artifacts and triage events without a laptop, respond to prompts from the palm of their hand and always be reachable, regardless of where they are.

### Scalability

A SOAR solution should grow with you and your organization. As you inevitably add more use cases over time, there will be additional processing loads placed on the platform.

The automation engine should be designed in a way that allows for vertical scaling (e.g., increasing CPU and RAM resources) and horizontal scaling (e.g., increasing server instances) to optimize performance and protect the automation return on investment.

### Open and extensible

A SOAR solution should be designed for openness and extensibility, easily incorporating new security scenarios, new products, new actions and new playbooks. Without this, SOAR can lose its value over time.

With an open ecosystem that follows a common standard and programming model, security teams can capitalize on a few benefits. New technologies can be quickly integrated into the solution without requiring any modification to the core platform, or negatively impacting automated playbooks. Users can develop additional integrations without permission or development cycles from the SOAR vendor. For instance, they can write their own integrations, develop homegrown applications or write an early access API from a vendor.

## Community powered

The ever-evolving nature of security also fuels the need for professionals to work together to share playbooks, best practices and strategies for dealing with the latest threats. A SOAR solution must support a strong community model and make sharing of app integrations and playbooks easy.

Measuring the installed base of a SOAR solution is a good indicator of its associated community's collaborative potential. Most users prefer to draw on the experiences of other like-minded users. A large-and-active user community provides the opportunity to share playbooks and apps, or brainstorm ideas for new automation use cases. Moreover, vendor participation in the community is a strong indicator of their commitment to both the community and collaboration.

Can SOAR help you improve your security operations? See how Splunk's best-of-breed SOAR technology can supercharge your security team's efficiency and effectiveness.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com