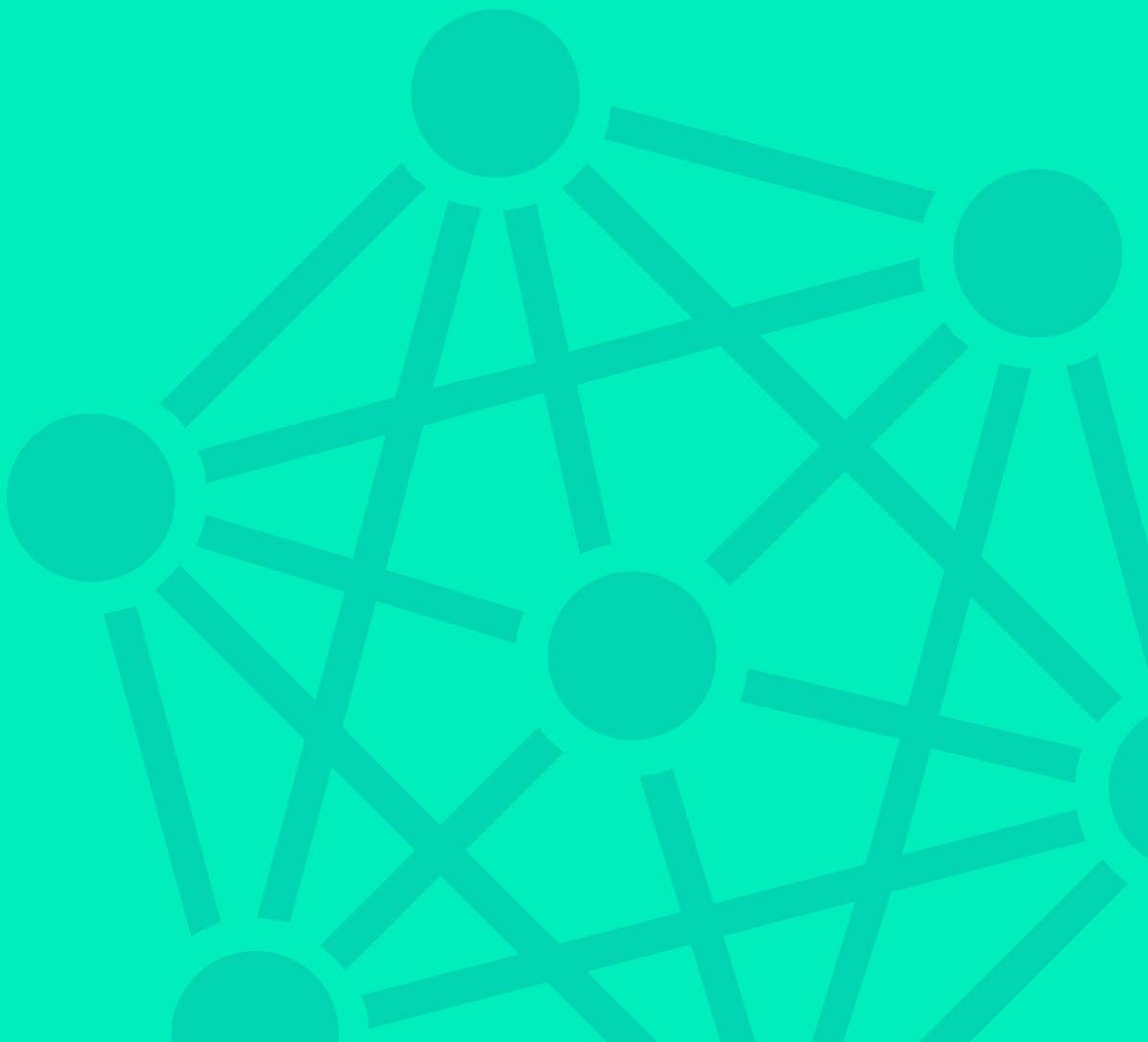
Logsign

Security Orchestration, Automation and Response (SOAR) Buyer's Guide

An Ultimate Guide for SOAR



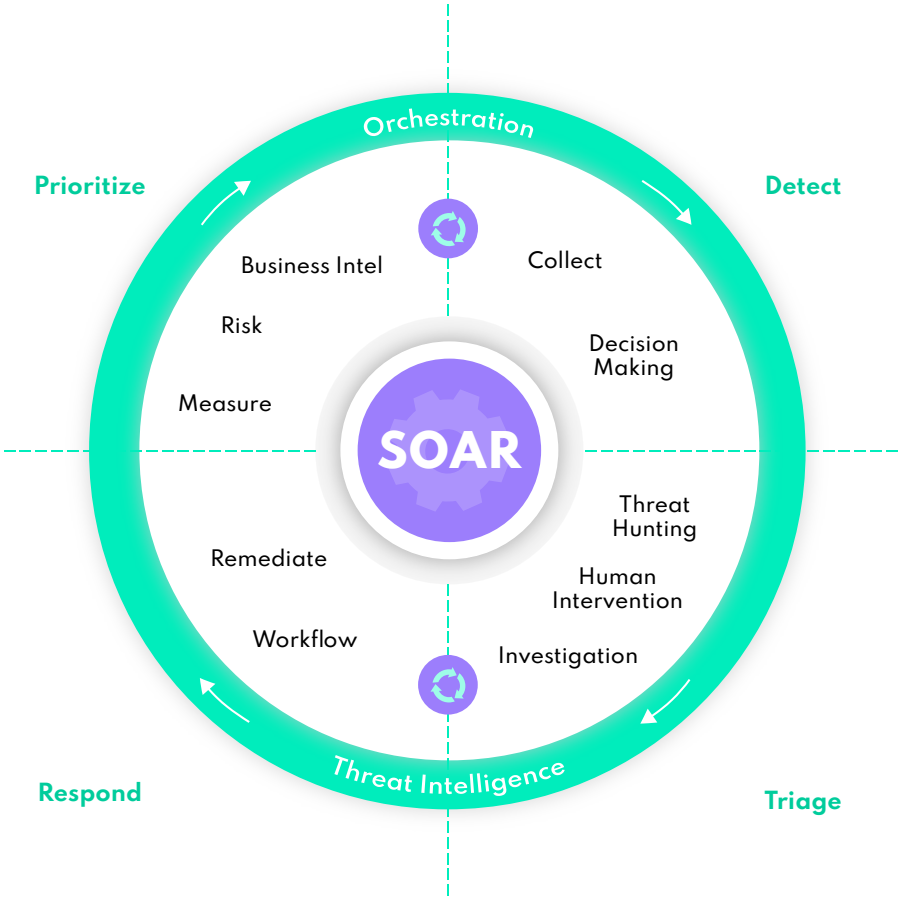
Contents

1. Introduction

Absolute security is a myth. Organizations cannot remain in denial and believe that their systems are absolutely secure. Threats in the modern-day business environment continuously evolve in sophistication and precision. As the attack surface area continues to expand, existing security systems generate a plethora of alerts for security teams to address. Responding to each alert can be a tedious task, and a security team may miss important high-risk alerts. While organizations across the globe are improvising their capabilities to understand security challenges, they invest significantly to detect, respond, and mitigate security incidents effectively. Their primary goals are to minimize the detection time and swiftly mitigate the incident so that business impact is negligible.

Often, organizations are not able to realize a good return on their security investments due to a staggering number of alerts generated by devices, applications, and systems. Other reasons include a lack of specialized tools and formal procedures for incident mitigation. It is vital that an organization's security team prioritizes high-risk alerts and not be bogged down by repetitive low-risk alerts that decrease efficiency and increase frustration.

To minimize security risks, organizations cannot continue to rely on isolated tools and informal processes. They must ensure that their security teams effectively manage incoming threats using specialized tools to help them fulfill their objectives. A security orchestration, automation, and response (SOAR) tool allows security teams to aggregate log data from various sources and turn them into actionable insights.



1.1. What is SOAR?

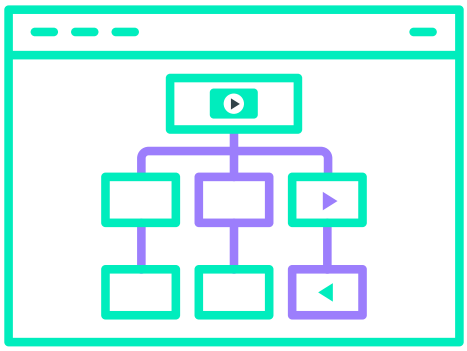
Gartner initially defined SOAR as "technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from the SIEM system and other security technologies – where incident analysis and triage can be performed by leveraging a combination of human and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

With the help of a SOAR tool, security teams can automate a substantial percentage of incident response activities. As a result, mean-time-to-detect (MTTD) and mean-time-to-response (MTTR) decrease. The SOAR tool equips a security team gets with reporting features, interactive dashboard, and detailed insights and metrics. While the team continues to address high-risk alerts, all the actions get documented, and its productivity enhances substantially. To sum up, a SOAR platform brings together threat intelligence, automated workflows, incident management, and flexible integrations.

1.2 Orchestration, Automation & Response

Though the security industry has been late in adopting automation in processes and procedures, the apparent benefits of automating incident management or parts thereof are driving factors behind the increasing popularity of SOAR platforms. The orchestration component of a SOAR platform facilitates the integration of a broad range of tools and technologies for incident management. An organization can make informed decisions, automate response actions based on risk posture, implement defensive measures, and formalize their incident response process. Business intelligence, case management, contextual information, playbook automation, interactive investigation, and collaboration are six critical elements of this component. After aggregating data from various sources, orchestration provides contextual information to enrich individual alerts.

SOAR performs automation using inbuilt or customized playbooks to undertake incident management tasks without manual intervention. Many experts believe that automation is a subset of orchestration in the practical sense. Ideal platforms come with sufficient playbooks for organizations to get started with their security operations. Further, the efficiency of automated actions is expected to grow with time with the help of machine learning algorithms. An excellent example to understand how automation works is the detection of malware. As soon as a SOAR platform detects the presence of malware, it implements sufficient measures to prevent the infection from spreading and sends an alert to the security team.



The third component of a SOAR platform is incident response. This component should allow security teams to collaborate, share information, and manage security incidents. An ideal SOAR platform would document actions as they are performed and minimizes documentation responsibilities on the security team. Further, there should be an interactive dashboard to give insights into an organization's security operations at a single point. This dashboard should also feature reporting capabilities to export customizable reports for different types of audience.

1.3 Why Do You Need SOAR?

A SOAR platform enables security teams to run security operations on their own, without manual intervention. The extent of automation in security operations varies from one operation to another. At times, it can be a single automated step with a manual workflow, or it can be an automated workflow requiring security personnel to approve after review. SOAR platforms allow security teams to implement automation at various levels during an incident response process. As security operations formalize and mature, the extent of automation subsequently increases.

Without automation, a security team deals with alerts individually. This means that certain alerts will wait for a while before the team addresses them. If critical alerts are missed due to this wait time, an organization may not end up in a favorable situation. Using a SOAR platform, this wait time is out of context and security teams can focus on complex activities. As a result, the time taken to respond decreases and potential risks are minimized. SOAR platforms allow organizations to derive the maximum possible return on investment (ROI) by enabling people, process, and technology to work together. For any security program to be successful, there must be a cohesive integration between people, process, and technology. Key benefits of a SOAR solution can be illustrated as:

- Increased efficiency of security operations
- Enhanced productivity of security team personnel
- Lesser mean-time-to-detect and mean-time-to-respond
- Availability of complete alert context for security teams
- Reduced repetitive mundane tasks and frustration Improved ROI and decreased financial burden over time

2. SOAR Use Cases

SOAR solutions that integrate with an existing SIEM solution provide all the information for security teams at one location. They do not need to move from one tool to another as they would have a single workbench. In the case of multiple tools, chances of human error increase due to different platforms and interfaces. A SOAR platform streamlines security operations as it coordinates and automates incident response workflow. To help prospective buyers in understanding how a SOAR solution may benefit their organization, the following sections discuss common SOAR use cases.

2.1 Phishing Attacks

Phishing attacks have been around for close to three decades and they continue to pose a significant risk to businesses. As phishing attacks continue to grow in numbers, an organization shall ensure that it is adequately protected. The motives behind carrying out phishing attacks are gaining access to financial information, stealing login credentials, or getting hands onto sensitive corporate data. A SOAR platform allows security teams to automate detection and mitigation of phishing attempts and saves valuable time of security teams.

It may determine the level of risk for each email by conducting a comprehensive analysis covering subject line, sender email, recipient(s), message contents, links, attachments, etc. A workbook will direct actions such as quarantining a suspicious email, blocking senders, and checking if any user clicked on suspicious emails before they were quarantined.

2.2. Incident Triage

Many security tools in the market generate alerts as soon as they detect malicious or abnormal behavior. However, alerts without contextual information are mostly useless. For effective incident management, mere knowledge of alerts and incidents is not sufficient. Security teams need actionable information to triage and resolve the alerts.

Without contextual information, security teams will spend most of their time in finding such information for each alert. This will increase their workload, apart from their existing responsibilities.

The provision of contextual information helps security analysts make informed decisions as contextual information enriches the quality of alerts. If the security team identifies an abnormal activity, contextual information helps them quickly understand the background for this behavior, take a decision, and respond without wasting any time.

2.3 Threat Hunting

Attackers need to succeed once, and it takes a matter of a few minutes for them to compromise a system. Security teams must work around the clock to defend IT infrastructure against emerging threats. Oftentimes it takes weeks and months for a security team to detect that their systems have been compromised. For minimizing the time taken to detect and respond, security teams require a solution that automates threat hunting activities.

While it can be automated, threat hunting would also involve manual and system-assisted modes for searching threats across a network or from a massive information dataset such as threat intelligence feeds. For maximum utilization of threat hunting capabilities, security teams require automation for accelerating threat hunts. In the case of manual threat hunting, security personnel must be familiar with contextual information about an organization such as internal processes, technology architecture, security measures, and incident management capabilities.

An ideal platform would create a case and generate an alarm as soon as it detects a threat. It may add additional information about the threat and start taking automated actions, if available.

2.4 Insider Threat Detection

Insider threat is one of the costliest types of data breaches. Considering that it involves a trusted user, they are relatively hard to detect. However, by implementing a data loss prevention (DLP) solution and connecting it with a SIEM solution with SOAR capabilities, it becomes possible for organizations to detect unauthorized and unexpected exfiltration of data. Many SOAR platforms come with inbuilt playbooks to support insider threat detection for organizations. As soon as the SOAR platform detects a suspicious behavior for insider threat, it starts gathering information about the user, their communication, and source addresses. These source addresses are matched with threat intelligence feeds to determine the likelihood of them being malicious. Other information sources can also be added to SOAR platforms to provide additional contextual information about alerts.

2.6 Rapid Investigation

When a SOAR platform detects a high-risk alert or event, time is of critical essence. Security teams cannot spend time on manually gathering information from different sources.

A SOAR solution provides a platform for security teams to complete their investigation in the least amount of time possible. In some cases, a part of incident response actions is automated while the rest needs to be done manually. In other cases, the situation is reversed.

The availability of contextual information helps security teams make informed decisions and prepare incident/alert reports without any delay. With the help of available information, security teams can conduct a straight forward investigation and proceed further.

2.7 Vulnerability Management

Unpatched or unmitigated vulnerabilities allow the attackers to get unauthorized access to organizational network and systems. In the last few years, attackers have started adopting stealthy attacks to avoid getting detected by security tools.

A SOAR solution provides a security team with real-time insights into the organization's security posture. As it is capable of swiftly going through large amounts of data, it provides detailed information about vulnerabilities and combines it with information derived from threat intelligence feeds.

This puts security teams in a better position to make informed decisions and address the existing vulnerabilities with all the information they need. This response to vulnerabilities can be either automated, semi-automated, or manual. As a matter of general practice, SOAR platforms send an alert to security teams if they encounter a vulnerability which is potentially harmful and considered severe in nature.

2.5 Endpoint Protection

Endpoints are entry points for end-users to interact with an organizational network. Endpoints include devices such as mobile devices, laptops, desktops, printers, IoT devices, etc. Advanced attacks such as fileless malware, polymorphic attacks, and zero-day attacks are getting more popular than ever.

A SOAR solution accepts log data from various security solutions such as endpoint detection and response (EDR) tools. While security teams have limited functionality with EDR solutions, a SOAR platform allows a security team to understand the context, investigate an alert, check the endpoints, and orchestrate changes across all the points at once.

While the number of endpoints is roughly proportional to the number of alerts an organization generates, SOAR uses contextual information to automate alert resolution with the help of playbooks and workflows.

2.8 Malicious Network Traffic

Organizational networks often encounter malicious traffic in various forms, but the purpose behind such traffic is mostly nefarious. An attacker may try to shut down the website, steal confidential user information, and sell it on the dark web.

SOAR platforms have proven to be particularly useful in the identification and analysis of malicious network traffic. With regular incoming data for scanning network traffic, a SOAR platform is in a better position to identify suspicious behavior. With the help of playbooks and other available resources, a SOAR solution can block malicious network traffic before it impacts network operations.

2.9 Threat Intelligence

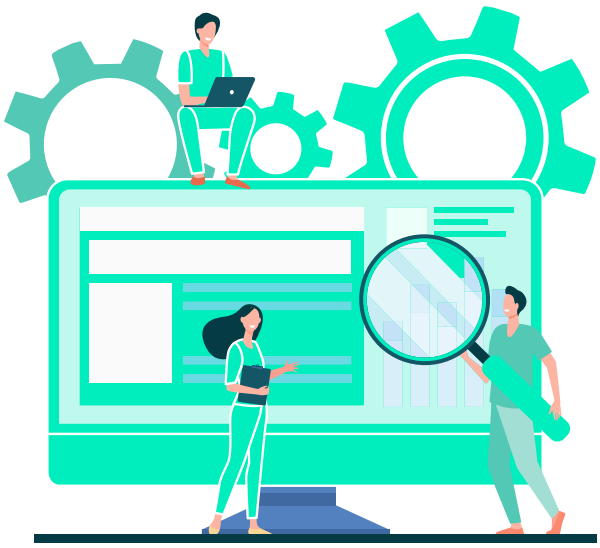
SOAR solutions thrive on the amount of available data as it improves accuracy and decision making. For effective incident management practices, threat intelligence is a crucial component. A SOAR platform must provide valuable insights by analyzing threat intelligence feeds. A security team needs to know tactics, techniques, and procedures (TTPs) for responding to an incident. When a SOAR platform gathers this information from threat intelligence feeds, it also provides contextual information as it is in a unique position to aggregate actionable information. Ideal SOAR platforms would be capable of correlating threat intelligence feeds with incoming logs of an organization for discovering attack patterns, vulnerabilities, and any abnormal behavior. While automated correlation is looked after by the SOAR platform, security teams can also perform visual correlation to look for patterns or behavior that might have been missed by automated methods. For this to happen, a SOAR platform must present this information in an easy-to-consume manner.

3. Evaluation Criterias

3.1 Easy and Free Integration With Your Technology

SOAR platform must be flexible enough for supporting a wide range of security products. However, the chances of a single SOAR platform providing integration support for all vendors by default are very low. A SOAR solution must allow its customers to create integrations which are not supported by default. Even if it directly does not allow them, security teams should be able to request their vendor to add new integrations.

For achieving orchestration and automation in full sense, it is pertinent to implement bidirectional integrations. While in many cases, customers may not need bidirectional integration capabilities. It is comparatively easier for customers to configure unidirectional integrations. For this very reason, the integration of a SOAR solution should not involve a steep learning curve and seamlessly integrate with an organization's existing infrastructure.



3.2 Scalability and Extensibility

Log data and threat intelligence feeds drive the accuracy of a SOAR platform. Over time, an organization observes a consistent increase in the volume of log data generated by network tools, applications, and devices. Organizations that implement a SOAR solution increase their team's productivity by creating new playbooks and automated workflows. The dynamics of modern-day business environment require that SOAR platforms must be scalable and extensible. They must support the needs of a growing business, whether it is the number of users or volume of log data.

It is reasonable to expect that an effective SOAR platform will not encounter the degradation of front-end performance and availability. An organization must select a SOAR platform that allows for seamless integration, data acquisition, normalization, and enrichment, as well as clustering and sharing to support database scalability.

3.3 Ease of Use

The presence of out-of-the-box content for a SOAR deployment plays an important role. However, every organization faces its own set of risks and has a different level of cohesiveness between people, process, and technology.

A complicated user interface on a SOAR platform can result in security team losing interest in their operations, and the platform may become obsolete.

Ideal SOAR vendors continuously incorporate customer feedback to streamline the functioning of their solution. This consistently simplifies the functions of a SOAR platform and in turn, contributes to overall incident management capabilities.

3.4 Case Management

A SOAR platform is a centralized point for security teams to simultaneously track the security posture of their organization in real-time and manage security operations. A security team must be able to derive insights in an actionable and easy-to-understand format. When responding to a single alert, a security team should not be needed to move from one tool to another. SOAR solutions provide a single platform for case management, right from generating alerts to mitigation and documentation. Conversation-driven case management enhances the productivity of security teams and allows them to manage more cases in less time.

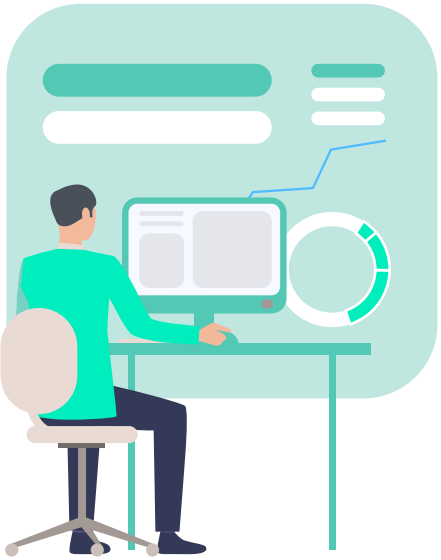
Case management capabilities of a SOAR platform should combine orchestration, automation, and incident management features. Ideal scenarios include the ability to visualize individual case record, standardized incident management processes, and results of third-party systems.

3.5 Codeless Bots & Playbooks

Playbooks and workflows allow security teams to break down well-known attack vectors into simple steps for automated detection and response. An organization may already have documented security processes and operational procedures in place. Instead of changing them without any business-use case, SOAR platforms enable security teams to create playbooks and workflows in line with existing security practices. To create bots, playbooks, and workflows, the interface should involve simple operations such as drag and drop, instead of complex coding. Generally, SOAR solutions come with a certain set of inbuilt playbooks and workflows. These configurations can be modified by security teams based on the threat environment and business requirement.

3.6 Workbench

SOAR platforms should provide a single workbench that becomes the driving force behind security operations. A unified workbench simplifies security operations by integrating different security tools and solutions into a centralized system. This system is capable of being deployed in virtually any environment. SOAR solutions also come with out-of-the-box connectors that provide security teams with a centralized point to control their security operations across the organizational network. This integration eliminates unnecessary fragmentation among security tools, reduces complexity in security operations, and maximizes the life of existing tools.



3.7 Collaboration and Information Sharing

SOAR solutions bolster security operations by integrating people, process, and technology. The orchestration component aggregates data from various security tools such as firewalls, IDS/IPS, vulnerability scanners, endpoint security tools, etc. This eliminates the manual efforts of security teams to check each security tool and address the generated alerts individually. Automation and incident response components bring together human beings and machine power. Advanced case management features provide security teams with various roles and responsibilities through which tracking and assigning of tasks is easy and straightforward. An ideal SOAR platform must contain a controlled environment for information sharing among team members of a security team.

3.8 Automated & 1-Click Manual Response

A SOAR solution provides security teams to perform automated, semi-automated, and manual workflows. For example, resolving low-risk alerts can be an entirely automated process without any human intervention. Resolving medium risk processes can be subject to a final review by a security team.

On similar lines, high-risk alerts may require approval by security teams at each stage. The level of automation in security operations increases with the maturity of playbooks and workflows. An ideal SOAR solution should be capable of recognizing decision-making patterns and recommending the same for automation.

3.9 Incident Triage

There is no upper limit for the pace at which security teams receive alerts for malicious activities or behavior in organizational networks. It becomes increasingly difficult for them to keep up with incoming alerts. To accelerate resolutions of these alerts, a SOAR platform enriches them by adding contextual information. While minimizing false positives is an objective, SOAR provides advanced case management features to escalate investigation.

SOAR platforms assign a level of risk for each alert. This risk level plays a crucial role in automating response to alerts and presenting a prioritized list of alerts for resolution to security teams. Inbuilt sophisticated automation capabilities minimize the chances of alert fatigue so that the efficiency of security teams remains unaffected.

3.10 Licensing Model

Considering the role of SOAR platforms in an organization's security model, organizations should have clarity on potential costs and expenses. Hence, the predictable nature of costs is vital to continue the operation of a SOAR platform. At present, there are multiple pricing models in place. Some SOAR vendors charge for providing their solution based on the number of events per day. In effect, the costs in this pricing model accelerate as security teams increase their reliance on a SOAR platform.

Another pricing model relies on the volume of data, number of playbooks, and processes. Ideally, as security teams start utilizing a SOAR platform for their operations, there must be a decrease in the total cost of ownership with an increased return on investment (ROI). This is precisely why organizations need to understand the vendors' pricing models. A cost-effective pricing model should have predictable costs and align with the organization's requirements in the future.

3.11 Multi-Tenancy

IT environments are getting significantly complicated and involve physical hardware, cloud-based platforms, virtual platforms, IaaS, PaaS, and whatnot. For managed security service providers, non-segregation of client data can turn into a compliance nightmare. Multi-national organizations may operate in different locations with complex infrastructures. Vendors should be able to respond quickly without compromising security.

SOAR vendors should have a multi-tenant architecture so that every client's data is separate from others and remains secure. They should place sufficient technical measures to prevent malicious software from traveling across the boundaries. The parent-child model of deployment is generally preferred for SOAR solutions as it prevents malignant processes from crossing the barrier.

3.12 Dashboards and Reports

If a SOAR platform does not help security teams in minimizing their average response time, it decreases the efficacy of security operations. SOAR solutions should visually present analyzed data in a way that is instantly understandable. Through intuitive and interactive dashboards, security teams can visualize the ongoing alerts in real-time. An ideal SOAR platform would allow security teams to utilize various types of graphical representations and detailed lists.

When security teams start using a SOAR platform, they would not know the most important dashboard right from day one.

Many SOAR vendors provide preconfigured dashboards with unlimited customizations to support security operations. Ideally, dashboards should be able to access data from all the systems and perform rapid visualizations with minimal configuration requirements. Similarly, with flexible

dashboards, automation promises well-documented reports to understand the areas for improvement and make informed decisions. The reporting component of a SOAR solution must be flexible and allow security teams to generate reports for parameters they require, instead of limiting them to a constrained set of report types.

3.13 Team Efficiency and High ROI

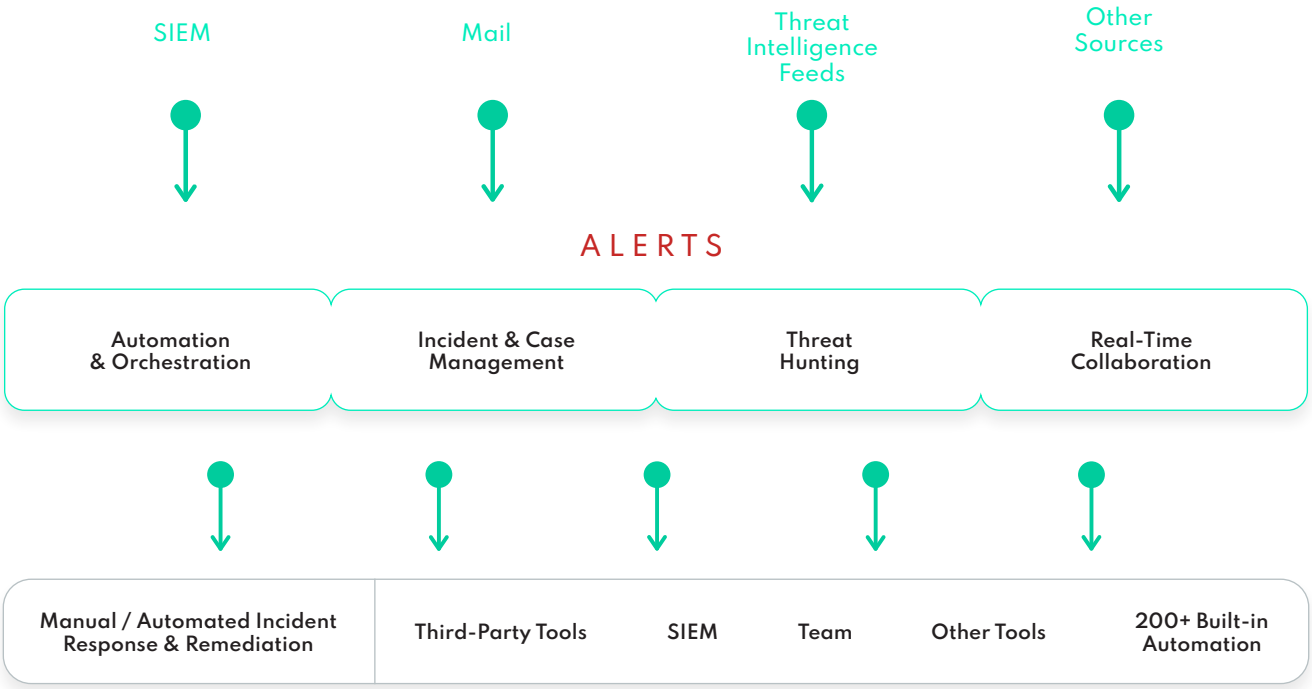
Security teams work tirelessly to protect an organization's IT infrastructure and keep it safe and secure. If implemented and adopted correctly, SOAR solutions reduce security costs over time. For SOAR platforms, one can look at ROI from three perspectives: people, process, and technology. Manual security operations require time, efforts, and financial resources. While there is a well-known skills gap in the cybersecurity industry, a substantial part of security budgets is spent on salaries and other employment benefits. Without automation, security teams spend most of their time addressing alerts. However, a SOAR solution provides them with the leverage they need to focus on strategic security actions.

Defining processes is often a tedious process, but with the help of SOAR solutions, security teams can define repetitive processes for once and let the SOAR platform handle the rest. This indeed adds a significant boost to the daily operations of a security team. People and processes alone cannot help you in winning the battle. For security operations, investments on technology are made for threat hunting, malware analysis, sandboxing environment, and remediation activities, among others. A SOAR platform functions on the top of existing IT infrastructure to maximize utilization of existing resources, instead of building custom integrations and performing manual tasks.

Logsign Security Orchestration, Automation and Response

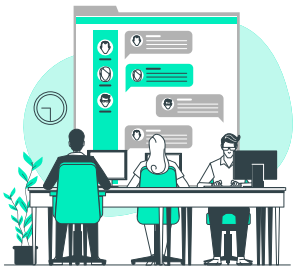
Security Orchestration and Automation	Incident Management	Bots and Playbooks
Built-in Integrations	Modern Security Case Management	Pre-Defined Bots & Playbooks
Bots and Playbooks	Interactive Investigation	Visual Playbook Editor
Workflow Management	Contribution & Collaboration	DSL Editor
Automated Actions	SLA&Metric Tracking	Easy-to-Use
Knowledge Base/Documentation	Dashboards & Reports	Customizable and Drag-and-Drop
	Single Workbench	

How Logsign SOAR Works?



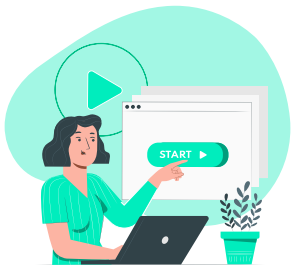
Why Logsign SOAR?

Conversation-Driven Case Management



Performance-Oriented Workbench

Interactive Bots & Playbooks



Logsign SOAR platform brings people, processes, and technology together. It helps security teams respond to alerts and incidents by orchestrating technical and human resources on a single workbench. For coherent security operations, it automates repetitive tasks, standardizes workflows, enables tracking of incidents, supports auto-documentation, communication, and collaboration between team members. Logsign SOAR empowers security operations and has a force multiplier effect on incident response. SOAR platform must be flexible enough for supporting a wide range of security products. However, the chances of a single SOAR platform providing integration support for all vendors by default are very low. A SOAR solution must allow its customers to create integrations which are not supported by default. Even if it directly does not allow them, security teams should be able to request their vendor to add new integrations.

For achieving orchestration and automation in full sense, it is pertinent to implement bidirectional integrations. While in many cases, customers may not need bidirectional integration capabilities. It is comparatively easier for customers to configure unidirectional integrations. For this very reason, the integration of a SOAR solution should not involve a steep learning curve and seamlessly integrate with an organization's existing infrastructure.