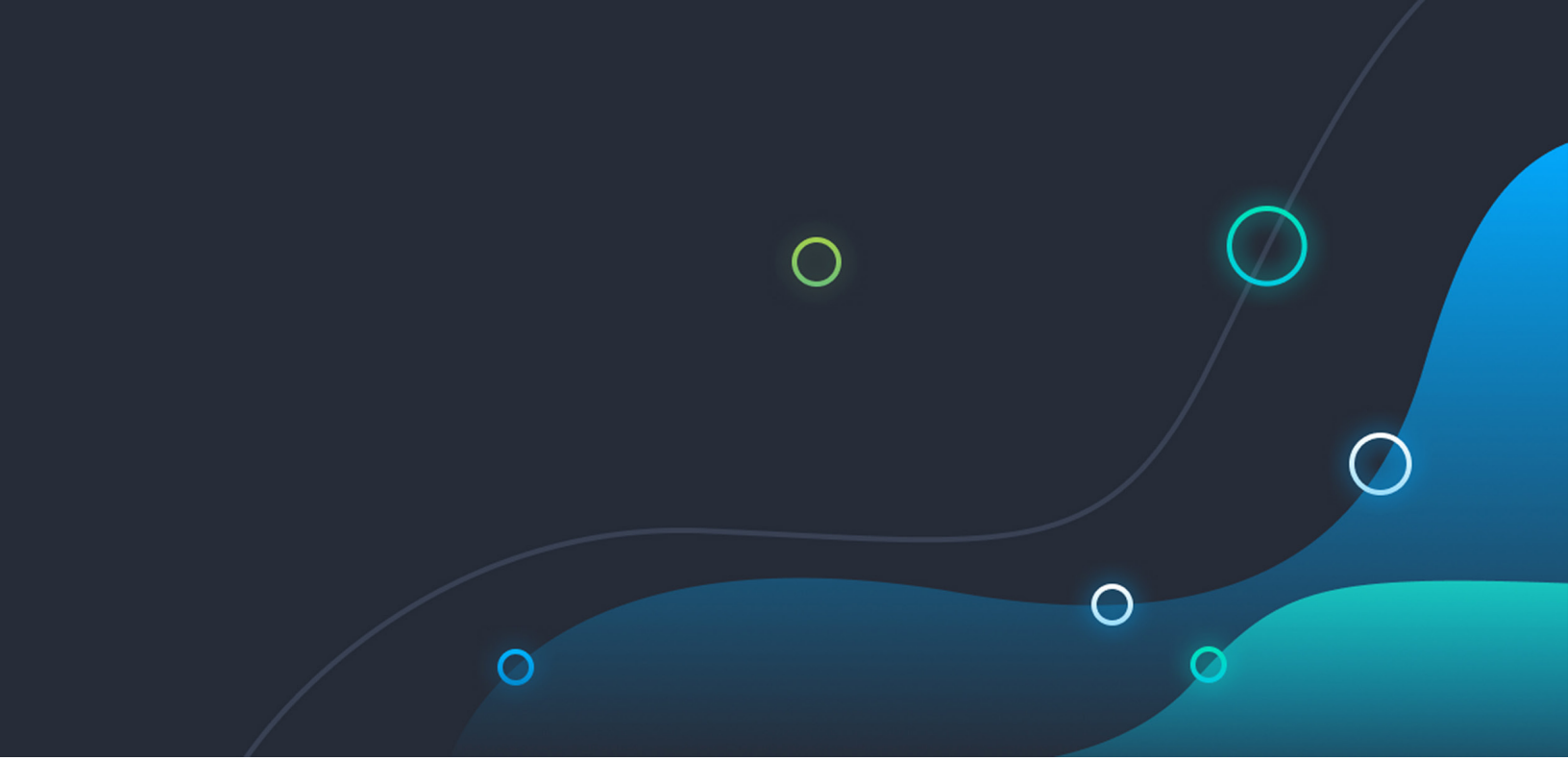




# Security Orchestration, Automation and Response (SOAR) Buyer's Guide

# Contents

Introduction.....	3
How to evaluate a SOAR solution .....	5
Dynamic case management .....	6
API-first architecture .....	7
Simple integration framework.....	8
High availability/disaster recovery (HA/DR) .....	9
Vertical and horizontal scalability.....	10
Customizable dashboards .....	11
Easily created and shareable content .....	12
Multitenancy .....	13
Granular role-based access control.....	14
Multithreaded playbooks and workflow builder .....	15
Implementation time and effort.....	16
Licensing model .....	17
Benefits of SOAR .....	18
SOAR Evaluation Checklist.....	19
About Swimlane.....	20

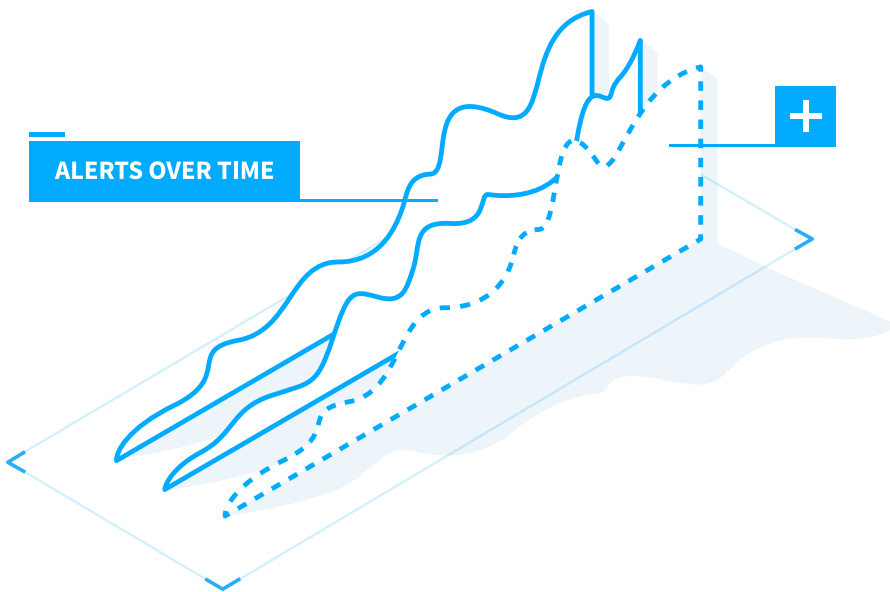


Research published in the 2018 Verizon Data Breach Investigation Report shows that while the execution time for a security breach is measured in seconds, it typically takes weeks or months for the breach to be detected. What's more, according to a global benchmarking report from [ESI Lab](#), organizations with cybersecurity practices that don't keep up with their digital transformation projects are more likely to fall victim to cyberattacks with losses that exceed \$1 million.

Many security threats focus on denial of service (DoS), data lockout or outright data destruction. Verizon reports more than 21,000 DoS attacks in 2018 alone. According to the report, malware, including phishing attacks, ransomware or malicious destructions, accounts for almost 9,000 additional identified events—not including those that used botnets, making the need for high availability and disaster recovery (HA/DR) capabilities critical for every organization.

In today's complex computing environments, it can be hard to determine what actual security coverage is in place. Many organizations have a security posture that resembles an old patchwork quilt—some areas are thick and lumpy because of overlapping coverage, while others are thin and vulnerable, providing minimal, if any, protection. It's impossible to differentiate each of these areas without in-depth analysis. This is something a busy security operations team responding to an endless influx of alerts may not have time to do.

Most organizations understand the magnitude of today's security challenges and have made significant investments to detect, respond to and remediate attacks more effectively. But the combination of an overwhelming number of alerts, the necessary disparate tools used to combat them, and a lack of comprehensive formal procedures for threat resolution has made it difficult to address the continuously evolving threat landscape. Analysts want to use their skills to investigate and resolve more advanced threats, leveraging their training for higher-value work. When they



spend their time bogged down by time-consuming, manual processes, efficacy decreases and frustration grows.

While CISOs may recognize increasing threats, they are often limited by monetary constraints and a lack of available talent. Ongoing maintenance contracts, new projects and training eat up the bulk of their budgets, leaving little to spend on enhancing security operations. Even with available funding, finding skilled security analysts is an increasingly difficult task. Each year as threats grow, CISOs must do more with less. A SOAR solution can help.

Instead of relying on siloed tools and inconsistent manual processes, a security orchestration, automation and response (SOAR) solution lets security teams aggregate proliferating data, turn it into actionable insights, and automate a significant percentage of the incident response process. Analysts are enabled to respond to every alert while reducing mean time to resolution (MTTR) with a comprehensive dashboard presenting a full view of alerts and tools along with insights and metrics to help monitor performance—simplifying, automating and documenting the entire incident response process.

## Key Takeaways

- ▶ Security risk is constantly growing and evolving.
- ▶ The proliferation of security tools results in duplicate alerts that reduce productivity.
- ▶ Analysts should leverage their skills for higher-value tasks.

# How to evaluate a SOAR solution

How does someone decide which SOAR solution makes the most sense for their organization's unique environment?

Selecting new software can be tricky, and organizations want to make sure they are getting the best value for their time and money. However, focusing exclusively on a list of available feature sets is not the best way to make a software choice. Products are constantly evolving. Frequently, evaluators are left looking at a checklist of seemingly identical features without a real understanding of how to assess the differences from one platform to the next.

But if a side-by-side checklist of required features isn't the answer, what methods can organizations use to choose the right SOAR solution?

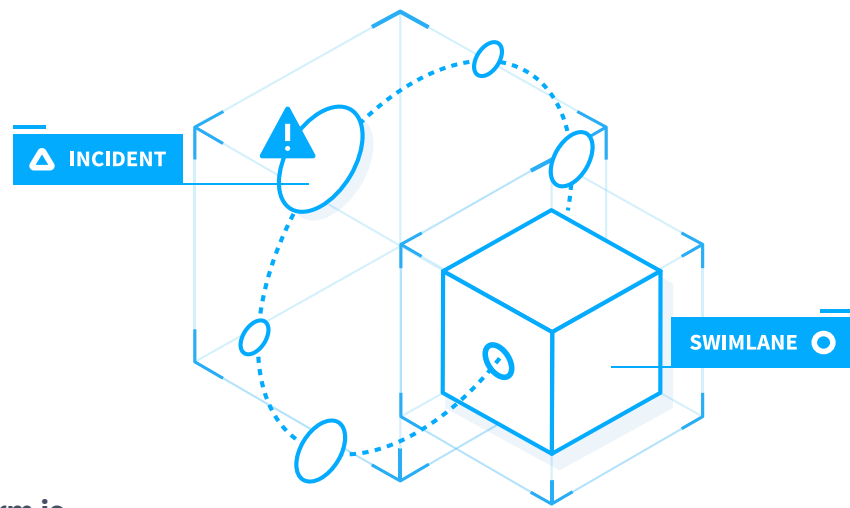
When it comes to likely indicators of successful platform deployment, it's essential to look beyond advertisements and dig into the differentiators.

These solutions should adapt easily to support an organization's processes and people—not the other way around. Organizations shouldn't waste valuable time and resources training staff to follow new processes or rescripting playbooks to integrate with and leverage existing tools.

The right SOAR solution should have built-in capabilities that help measure and bolster efficiency while streamlining and improving processes. The CISO shouldn't need to modify his or her security team or existing tools to take advantage of what the platform offers. Nor should long-term planning be restricted by the ability of the SOAR platform to incorporate future strategies and tools. **A SOAR solution should optimize the work already being done by the organization—better, faster and smarter.**

## Key Takeaways

- ▶ When evaluating possible SOAR solutions, you must understand each platform's differentiators.
- ▶ A SOAR solution must support the organization's existing processes and provide flexibility to adapt as the organization changes.
- ▶ The solution should work the way people do, making it easy to consolidate alerts across tools.



**What's the best way to tell which SOAR platform is right for the organization? Here are 10 important features and functionalities to look for:**

## Dynamic case management

A SOAR solution should deliver rapid insights gleaned by centralizing data from multiple sources, and the insights should be presented in an actionable and easy-to-understand visual format. Overlapping security tools may be unavoidable, but the security team shouldn't have to toggle between different platforms to respond to and remediate an alert—even when there are many alerts for a single threat. The SOAR solution should be able to recognize alerts from multiple sources and analyze them for commonalities. When multiple alerts arise from a single event, the SOAR solution should automatically add them to a single case, keeping the team from duplicating efforts and hunting for details in various places. This improves productivity and allows analysts to manage more cases in less time.

Rather than acting only as an evidence locker, a SOAR solution should provide dynamic case management that combines automation, orchestration and analyst activities. Additionally, analysts should be able to resolve the issue from within the SOAR platform case record without having to initiate a separate login for an underlying reporting system. The best scenario includes the ability to incorporate visualization directly within the individual case record, including views pulled in from third-party systems to facilitate resolutions and enable analysts to work within standardized processes.

### Key Takeaways

- ▶ A SOAR solution should consolidate all relevant event data in a single case record for an analyst to review and remediate the entire incident from a single screen.
- ▶ Case management should be easily customizable and workflow driven to ensure each record is automatically tailored to fit the specific use case.

# API-first architecture

Organizations considering SOAR need to know that whatever solution they implement has the ability to integrate with all the technologies they currently have and any they could potentially implement in the future. Evaluators also need to validate the platform's extensibility to ensure it can accommodate growth by adding the new features and capabilities necessary to adapt to new threats and incident response processes. This is why an API-first architecture is critical.

A solution with an API-first architecture has a standardized way of accessing data that is independent of the UI or the application's own functionality. As requirements evolve, every component in a SOAR solution should be accessible through an API to enable the vendor to quickly add new capabilities as discrete plug-ins. This API-first capability allows security and DevOps engineers to create integrations with homegrown or third-party apps without forcing people to use the SOAR platform's UI. Some SOAR solutions don't have a full API architecture, making functionality difficult to enhance or modify. To keep pace with the rapid changes in the field, the selected SOAR solution should have API coverage for every component to ensure that all functionality and data are available.

## Key Takeaways

- ▶ **Every component and functionality of the SOAR solution should be accessible through an API.**
- ▶ **The platform needs to be extensible so it can accommodate growth by adding the new features and capabilities necessary to adapt to new threats and incident response processes.**

# Simple integration framework

As a corollary to the API-first architecture, look for open access to build integrations into the product. Most mainstream SOAR solutions provide out-of-the-box integrations to common platforms and applications. However, simply providing common integrations fulfills only half the requirement. Even if the SOAR solution offers an out-of-the-box integration for every tool currently in use, there is no guarantee that would remain the case if the organization changes its existing tools or adds new tools in the future.

A SOAR vendor should have the ability to add new integrations quickly and easily, ensuring the SOAR platform continues to match each organization's unique environment. New integrations should be accessible and usable to support an organization's custom applications, and the organization should be able to fork and modify existing integrations to meet specific internal requirements.

When evaluating a SOAR solution, confirm that it offers a fully exposed integration engine for viewing, authoring and modifying scripts. The organization should be able to test the integration directly from within the builder as an important aid for productivity and rapid deployment. A full-featured integration engine should also include the ability to use forkable Python to help with the rapid creation of new integrations.

## Key Takeaways

- ▶ A SOAR platform should have extensive out-of-the-box integrations and easily support new and custom integrations to stay relevant as the organization evolves.



# High availability/disaster recovery (HA/DR)

An organization's security environment should be able to match the availability of the rest of its IT infrastructure.

High availability (HA) and disaster recovery (DR) capabilities should be nonnegotiable requirements of any SOAR solution. Don't be fooled by vendors who offer only "warm spare" capabilities and call it high availability. HA is too critical for "kind of" features or dependencies on third-party solutions that add an additional point of failure and another layer of overhead. Investigate the HA/DR offerings to ensure they use sharding and clustering to enable scalability and automated failover. Also, confirm the SOAR solution uses replica sets that fully support HA/DR.

## Key Takeaways

- ▶ Warm spares are not an adequate substitute for true HA/DR.
- ▶ Reliance on third-party tools for automatic failover adds operating overhead and decreases reliability.



## Vertical and horizontal scalability

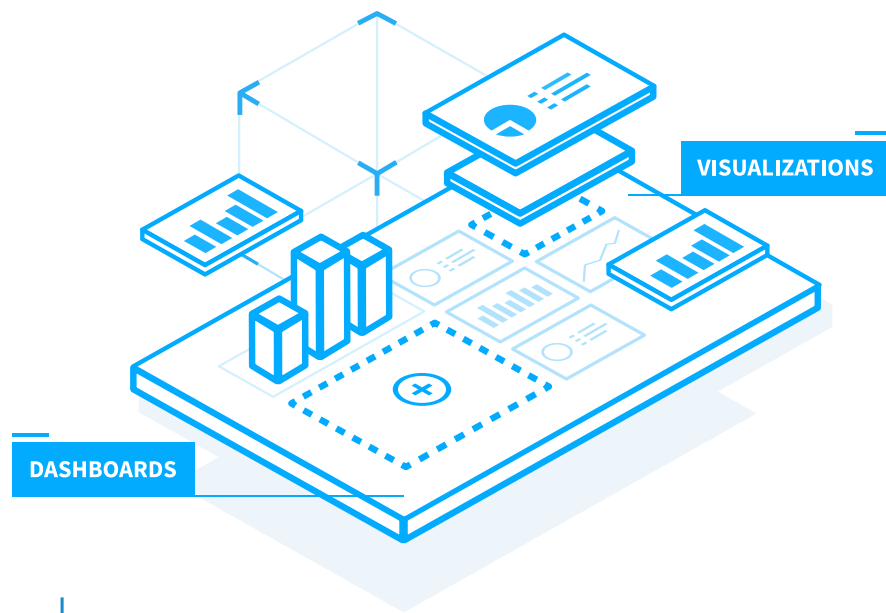
Continued proliferation of required security tools has resulted in a steady increase in the volume of data generated by those tools. Organizations using SOAR solutions to increase productivity do so by implementing an increasing number of playbooks and workflows to address critical use cases. In addition, some organizations must support a large and growing number of analysts, making the ability for the SOAR solution to scale—both horizontally and vertically—a critical factor in the selection.

This complex environment requires that the platform has the ability to balance the web tier across the content delivery network to maximize front-end performance and availability. Look for rapidly deployable task engines to manage integrations, data acquisition and enrichment, as well as sharding and clustering to help support database scalability.



### Key Takeaways

- ▶ **Vertical and horizontal scalability is critical with volume of data and the proliferation of playbooks and workflows.**



## Customizable dashboards

When remediating security threats, time is critical. It's important that applications present supporting data in a way that is understandable instantly and intuitively. This requires reports and visualizations that present data points in a clear and comprehensive format, whether that's through detailed lists, graphical representations of KPIs, or embedded windows that provide insight to integrated products.

Users don't generally know at the onset what they need to see or how they need to see it. A SOAR solution's dashboards should include multiple, preconfigured views, as well as an infinite number of impromptu views to support any use case or operational need quickly and easily.

The ideal dashboard should have the ability to access all integrated systems and present rapid data visualizations of cases and KPIs without requiring users to spend time configuring output when they could be taking steps to remediate the issue.

### Key Takeaways

- ▶ Data should be presented so that it is understandable instantly and intuitively.
- ▶ A SOAR solution should include dashboards with multiple, preconfigured views and an easy way to create an infinite number of views to support any need.



# Easily created and shareable content

Out-of-the-box content is an important component of any SOAR deployment. However, every organization has a different and continually evolving combination of people, processes and technologies, which can quickly render fixed content obsolete. Over time, organizations will need to modify or add to existing capabilities. An accessible library of reusable building blocks and components can provide an invaluable jump-start to these efforts, helping to accomplish goals with a minimal expenditure of time and resources.

This is the reason to work with a SOAR vendor who understands the value of modularity and helps bring a supply of readily accessible content to its users. Vendors who truly buy into this model will encourage a highly engaged customer community and provide a forum for creating content—sharing both knowledge and curated content.

Applets significantly accelerate the development process by leveraging the intelligence of the community, automating activities such as extracting fields, setting relationships or organizing data. Using a simple drag-and-drop UI enables organizations to make use of a rich treasure trove of apps and applets to solve any number of use cases at great time savings. To accommodate changes in technologies, modifying playbooks to replace integrations at any step in the workflow should be as simple as selecting a new app or applet from a drop-down menu.

The library may not always have a component that exactly fits the organization's requirements, but there may be one that provides some of the required key capabilities. Starting with a finished app saves time and improves efficiency over starting from scratch, thus helping to achieve objectives faster and more cost-effectively. Coupled with an API-first architecture, a library created by a vendor-supported user community can make necessary extensions, modifications and integrations much easier.

## Key Takeaways

- ▶ **The SOAR vendor should provide a library of common components.**
- ▶ **Readily available apps and applets can dramatically reduce the time it takes to create integrations and extensions.**
- ▶ **Content should be both sharable and easily modified to adapt to any organization's requirements.**

# Multitenancy

Today's IT environments are complex, consisting of physical hardware, virtual platforms, IaaS, and cloud-based platforms and solutions. Without the ability to segregate and silo data and applications—particularly for managed service providers and multinational organizations—this complexity can be a policy and compliance nightmare. Organizations may manage an intricate combination of subsidiaries or geographies across this complicated environment, and they must be able to respond quickly to changes in workloads without compromising security.

The organization needs the ability to keep each entity's data separate and secure, even in a multitenant environment. There must be barriers that prevent malware and hacking to cross those horizontal boundaries. A SOAR solution should enable parent-child deployment architecture that ensures each distinct entity's data remains protected by preventing malignant processes from crossing the barrier.

## Key Takeaways

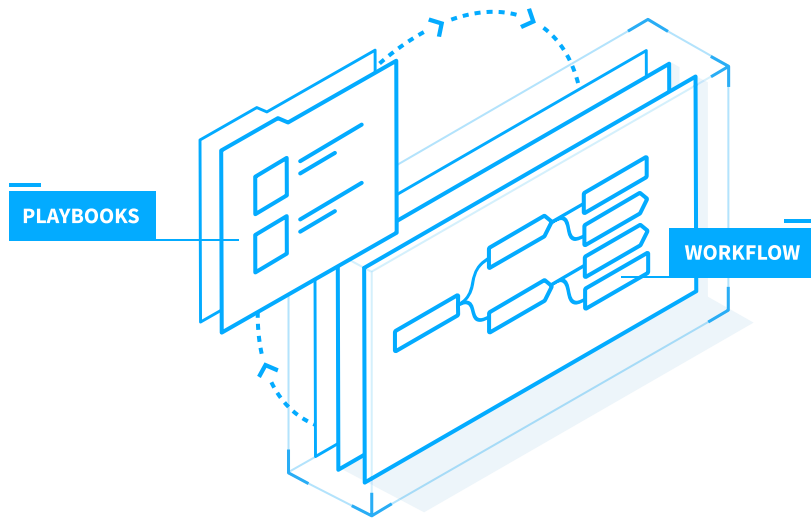
- ▶ A SOAR platform should support parent-child deployments and offer native capabilities to keep data segregated and siloed.

# Granular role-based access control

Complex organizations and IT structures require the ability to grant or restrict access down to the individual field level by user, group or role. Many organizations require the ability to restrict access to the data at the field level anywhere within the product so that analysts can access exactly what they need without exposing data that might be a violation of company policy or legal regulations.

## Key Takeaways

- ▶ Security organizations need granular role-based access (RBAC) that is configurable at the field level to ensure secure data is only accessed by authorized staff.



## Multithreaded playbooks and workflow builder

Processes can be made up of multiple steps or plays that align business and technology systems with workflows or playbooks for enabling rapid response to specific situations. The best workflows can be readily customized to match existing processes, rather than forcing an organization to modify or conform to prebuilt workflows that may not match its organizational structure, skills or environment.

The SOAR solution should enable playbook and workflow creation and modification using simple techniques—such as drag-and-drop interfaces—rather than more complex coding. All workflows, alerts and playbooks should be completely customizable to the organization’s priorities. Ideally, playbooks or workflows could be triggered at any stage by automated third-party products, manual analyst input or a single click inside an existing case record. These multithreaded visual workflows and playbooks enable rapid identification and response to any threat.

Robust workflow builder tools work with custom code as well as out-of-the-box content to allow for complete adaptation to an organization’s unique environment. However, they should not require complex coding, such as Python scripting.

Workflows and playbooks should be nimble and light enough to adapt to the organization’s processes and threat changes quickly. Yet, they must be robust enough to enable analysts to understand threats rapidly and take actions as needed. In the case of recognized threats, workflows should even be able to take actions on their own to improve MTTR.

### Key Takeaways

- ▶ **Multithreaded playbooks that align the business and technology are key to rapid response.**
- ▶ **A SOAR solution should have playbook creation and/or customization that doesn’t require custom coding at any stage.**

## If all that is included, then think about this:

**When the due diligence is done and the solutions on the short list offer all of the necessities, the work is still not finished. All systems require implementation and deployment, and they must fit within the organization's budget. Here are a few tips for analyzing those aspects of the potential choices:**

### Implementation time and effort

Any system can be implemented quickly and inexpensively by following a cookie-cutter approach. In fact, almost any solution can be up and running immediately if the organization only uses the vendor's standard deployment model and happens to have an environment that maps exactly to a limited amount of canned content. But how many organizations fit neatly into that ready-made bucket? What is the cost to their overall effectiveness and efficacy when the organization chooses this approach, and it doesn't work?

Every organization is different and so are the specifics of their individual security needs. From the organizational structure to the security team's staff, skills and experience to specific processes and procedures, organizations require a specific and unique blend of applications and infrastructure—making the out-of-the-box option above less effective.

Because each organization is unique—including people, processes and technologies that change over time—a SOAR solution needs to be both easy to implement and quick to configure and customize. It needs to support a combination of industry-standard processes with the ability to match the existing organizational processes for each environment.

In short, if the implementation time promised by the vendor seems too good to be true, it likely is. They might be able to get the platform up and running, but the built-in approach may not provide the best value to the organization's security operations center.

Ultimately, the time it takes to implement a system—and how much it costs—is almost completely in the hands of the implementing organization. The vendor should be willing to help find the best balance of speed, budget and customization for the organization's needs. It may be worth spending a bit more time during up-front implementation to optimize long-term benefits.

#### Key Takeaways

- ▶ Each organization must find its own balance of implementation speed and customization capabilities.
- ▶ Customer-focused vendors will help an organization find this balance point.





## Licensing model

With a SOAR solution playing such a central role in a security team's operation, the predictability of the operating costs is critical. Some SOAR vendors charge for their solution based on the number of triggering events per day—in effect, charging at an accelerating rate the more an organization uses the platform. Other vendors charge based on data volumes, the number of playbooks deployed or the number of processes. As a solution is used more, the impact of the total cost of ownership (TCO) should decrease while the return on investment (ROI) increases. That's why it is important for organizations to make sure that they won't be charged more for increasing the value they get out of the solution.

While there are many licensing models in use, the most important factor is to ensure that the chosen vendor's model is cost-effective and predictable while continuing to align with the organization's future requirements.

### Key Takeaways

- ▶ Be sure the vendor's pricing model works over the long term.
- ▶ Make sure that the organization isn't penalized for deriving value from the solution through incremental licensing increases based on product usage.

# Benefits of SOAR

The right SOAR solution improves the team's efficiency and the efficacy of SOC operations. Productivity improvements help increase the organization's security by reducing and mitigating risk. The longer a threat remains open, the greater the risk to the organization, so rapid remediation is key to security. Additionally, faster MTTR enables the team to address more threats in less time, helping them keep pace with security alerts and keep FTE costs down.

Organizations can optimize the ROI of their SOC as the SOAR solution automates and orchestrates its capabilities, allowing for existing people, processes and technologies to work together in harmony. What's more, by improving data completeness and providing more and better context for alerts, SOAR solutions reduce the amount of manual work necessary to remediate threats.

The [ESI ThoughtLab research](#) cited earlier shows that as cybersecurity systems mature, the organization's probability of expensive cyberattacks decreases. The survey classified respondents using comparisons to the [NIST Cybersecurity Framework](#). Organizations at the beginning of the cybersecurity journey face up to a 21.1 percent risk of a cyberattack and a risk of more than \$1 million in losses, while others currently in the adoption phase decrease their risk by 15.6 percent.

As the threat landscape continues to get more sophisticated, a SOAR solution can help organizations stay on top of, and even prevent, threats and alerts.

## Key Takeaways

### The benefits of a SOAR solution:

- ▶ Increased SecOps efficiency
- ▶ Enhanced SOC productivity
- ▶ Faster mean time to resolution
- ▶ Complete alert context
- ▶ Lower FTE costs
- ▶ Reduced analyst frustration/turnover

# SOAR EVALUATION CHECKLIST

## Features and Functionality

### □ Dynamic case management

Consolidates all relevant event data into a single view where analysts can review, act on and remediate an incident easily within the case record.

### □ API-first architecture

Enables the integration of all existing and future tools and leverages each component and functionality within each integration via API.

### □ Simple integration framework

Includes extensive out-of-the-box integrations with a fully exposed integration engine for viewing, authoring and modifying scripts. Integrations can be tested directly from within the builder, and there is an ability to use forkable Python to create new integrations.

### □ HA/DR

Matches the availability of the rest of the IT infrastructure, uses sharding and clustering to enable scalability and automated failover, and includes replica sets that fully support HA/DR.

### □ Vertical and horizontal scaling

Balances the web tier across the content delivery network with rapidly deployable task engines to manage integrations, data acquisition and enrichment.

### □ Customizable dashboards

Include multiple, preconfigured views but with the ability to create an infinite number of views quickly and easily. Plus, they have the ability to access all integrated systems to visualize any dataset.

### □ Easily created and shareable content

Should consist of a robust library of common applications and applets available to create integrations and extensions quickly with the ability to share and modify content easily.

### □ Multitenancy

Supports parent-child deployments and offers native capabilities to keep data segregated and siloed as necessary.

### □ Granular role-based access control

Restricts or grants access to data at the field level.

### □ Multithreaded playbooks and workflow builder

Offer drag-and-drop playbook creation and customization with the ability to build workflows without complex coding.

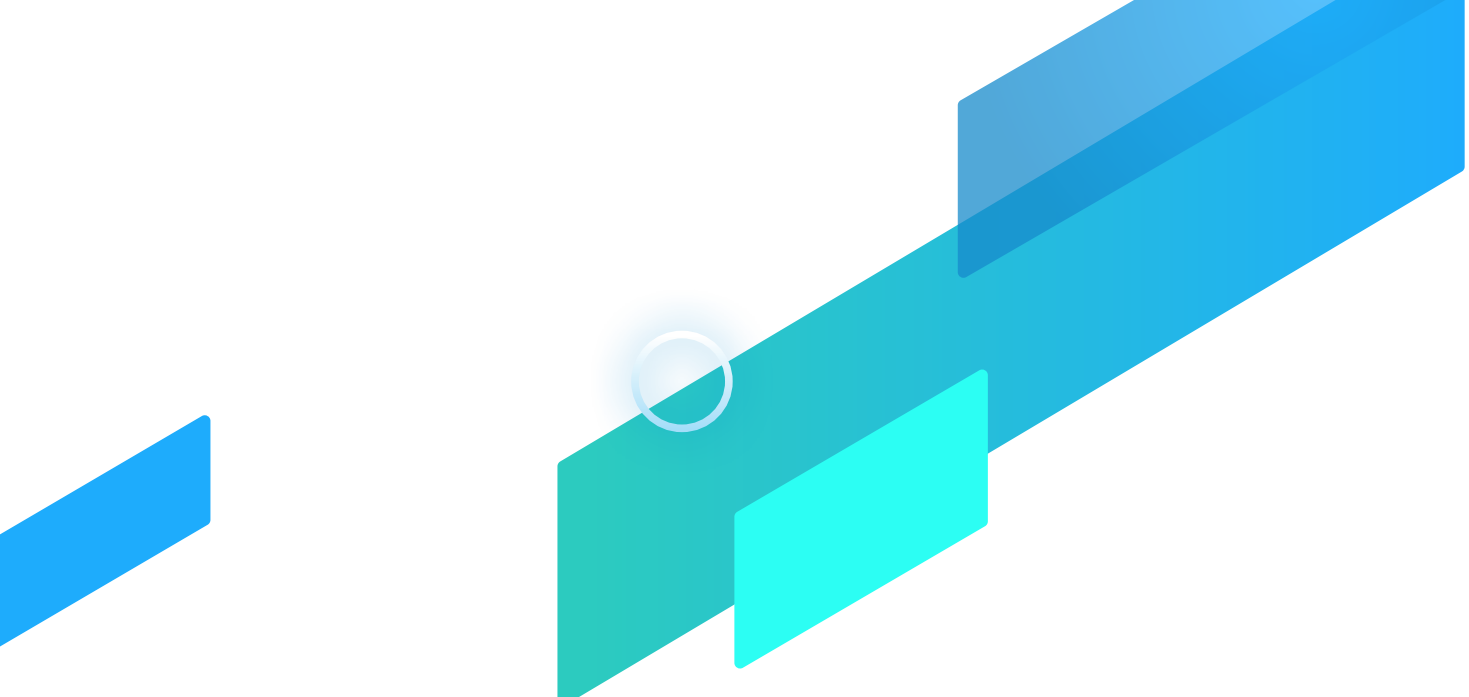
## Key Considerations

### □ Implementation time and effort

Includes the ability to deploy, configure and customize a SOAR solution quickly and in a way that fits the organization's unique environment while providing rapid time to value.

### □ Licensing model

Increases return on investment while the total cost of ownership decreases.



## About Swimlane

Swimlane is a scalable and innovative leader in security orchestration, automation and response (SOAR). The flexible solution delivers powerful, consolidated analytics, real-time dashboards and reporting from across the security infrastructure, maximizing the incident response capabilities of overburdened and understaffed security operations.

The scalable, innovative and flexible security solution offers a broad array of features aimed at helping organizations to address both simple and complex security activities, from prioritizing alerts to remediating threats and improving performance across the entire organization.

To arrange for a demo of Swimlane or to speak with one of our security architects to see if SOAR would be helpful to your organization, please contact us at 1.844.SWIMLANE or [email us](#).