Essential Guide

# Security Orchestration, Automation and Response (SOAR)

Automation for the SOC of the Future

splunk>

Cybersecurity teams are overwhelmed. There's a shortage of cybersecurity professionals with the necessary knowledge and expertise to adequately staff security operations centers (SOCs) around the world. This makes it exceedingly difficult for understaffed security teams to respond swiftly and resolve the thousands of alerts received each day. In fact, security analysts are drowning in security alerts, with far too many to investigate and resolve each day. This can quickly overwhelm a security team, increase security incident backlogs, and lead to alert fatigue. In fact, 41% of potentially beneficial alerts are overlooked due to limited SOC resources. If even one of those alerts represents a viable threat, and the security team doesn't address it, it could result in a breach.

Furthermore, security operations work is rife with monotonous, repetitive, and time-consuming manual processes and tasks. Trying to handle all of these processes manually or without effective procedures can result in analysts spending an average of three hours or more on each individual investigation, often juggling six different tools while doing so. This is time that could otherwise be spent on activities like strategic planning, mission-critical decision-making, and innovation that can strengthen your security posture and drive high-value business outcomes.

To make matters worse, many security teams are hindered by a lack of established security workflows. In the absence of these security standard operating procedures, analysts are unable to work together efficiently and effectively to resolve incidents rapidly. For other teams, their own security tools get in the way. SOCs are juggling a grab bag of security point-products that lack interoperability. These tools all possess static, independent controls, with no orchestration between them. It's difficult to manage and reduces the speed of investigations. If your tools don't work together, it can create gaps in your armor — gaps that attackers can exploit. Combined, all of these factors result in a slow mean time to triage, investigate, and respond to threats. All the while, threat actors can remain hidden in your network for up to nine weeks before being detected.

As a result, organizations have difficulty drawing insights from and taking action on their data. It's too time consuming and resource intensive. But there's a solution: your organization can meet these challenges by employing the right security information and event management (SIEM) solution; one that allows you to access data-driven insights, combat threats and help protect your business by mitigating risk at scale with ML-powered analytics you can act on.

In this essential guide, we'll take a deep dive into what a security orchestration, automation and response (SOAR) solution is, what it does, and how to find the right SOAR solution for your organization.

# What is a SOAR solution?

A SOAR solution is like a conductor for a symphony orchestra. Much like how it takes an ensemble of different types of instruments to make great music, SOCs often need a variety of security products and tools to get the information they need in order to tackle potential threats. However, not all of these tools play well together, and without proper guidance and organization will generate a lot of discordant noise that becomes difficult to make sense of. SOAR helps to harmonize those tools and ensure that from start to finish, all of the data comes together into a fine symphony of information that your security team can understand and act on.

At the heart of SOAR are two major facets: orchestration and automation.

- **Security orchestration** connects all your tools and data, even when spread across distributed systems. The orchestration piece uses multiple automation tasks for a complete workflow, with a beginning and end.
- **Security automation** is all about simplifying and automating individual tasks: if this one thing happens, then this is the thing to respond with to fix it.

While just one of these can be a powerful tool in a SOC team's arsenal, automation and orchestration are best used in concert.

## What does a SOAR do, exactly?

Gartner defines SOAR as "solutions [that] combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform.

A SOAR should help SOC analysts automate routine, mind-numbing and repetitive tasks through automation. This provides analysts with more time to devote towards strategic activities like threat hunting.

At a high level, the modern SOAR should help a SOC solve three major security challenges:

- Harmonize the data from other tools in the larger security stack
- Reduce noise while providing the ability to prioritize alerts
- Respond to threats via automation with speed and accuracy

Without security automation and orchestration, security teams would be left to investigate every alert and threat manually. In today's world, this simply isn't feasible and is a guarantee for disaster in the form of costly cyberattacks and data breaches.

# Five essential capabilities of a SOAR

## 1. Orchestration

When evaluating a SOAR solution, the orchestration function should direct and oversee all activities relating to a given security scenario from beginning to end. It should be able to ingest security data from any data source and in any format. It should be able to receive data that is pushed to the platform, and it must have the ability to poll data sources and ingest data into the platform. 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.

## 2. Automation

Automation via functions like playbooks should allow a security team to execute a collection of basic but essential actions in seconds, versus minutes or hours if performed manually. For instance, phishing investigations that require the use of multiple actions across several security tools and take 40 minutes to perform 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 also be easy to create and modify. Features like playbook editors 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.

## 3. Interoperability

A SOAR solution should be designed for openness and extensibility. It should easily support incorporating new security scenarios, new products, new actions and new playbooks. Without it, a SOAR solution can lose its value over time. With an open integration ecosystem that follows a common standard and programming model, security teams can capitalize on a few benefits. New and existing technologies can be quickly integrated into the platform without requiring any modification to the core platform or negatively impacting automated playbooks. Users should also be able to develop support for additional integrations without permission or development cycles from the SOAR vendor.

## 4. Event and alert management and prioritization

A SOAR solution should queue and prioritize inbound events and alerts. This will enable alerts to be rapidly consumed and efficiently acted upon, without the need for extensive searching or switching between contexts. Events and alerts should include a status indicator (for example new, open or closed), a severity indicator and a color-coded sensitivity indicator to facilitate a snapshot of key 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 — e.g., playbooks) against this data.

## 5. Metrics and reporting

It is critical to understand the quantitative performance gain and resource savings that automation provides, and to have this information readily available via a dashboard within the SOAR solution. Examples of key performance metrics that should be available on the SOAR solution include MTTR, 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 the SOAR solution is driving.

# Enter Splunk

Stop being overwhelmed and take back control. Splunk SOAR provides security orchestration, automation, and response capabilities that empower your SOC. Splunk SOAR allows security analysts to work smarter, not harder, by automating repetitive tasks; triage security incidents faster with automated investigation and response; increase productivity, efficiency and accuracy; and strengthen defenses by connecting and coordinating complex workflows across their team and tools. Our customers reported that with Splunk SOAR, they were able to save 90% of the time that was typically spent on routine tasks.

Splunk SOAR has been named a Market Leader for SOAR by KuppingerCole and has received multiple awards from TrustRadius like Best Software for Enterprise and Mid-Market Businesses. Splunk Enterprise Security users can use Splunk SOAR to automate investigation and response workflows using playbooks. Subsequent to a detection event in Splunk Enterprise Security, Splunk SOAR can take immediate action to automate investigation and response actions to rapidly and efficiently resolve incidents — without the need for human interaction. Splunk Attack Analyzer and Splunk SOAR empower SOC and IR teams to proficiently triage and respond to active threats with end-to-end threat analysis and response. Customers that integrate Splunk products have found a 30% increase in their operational efficiency, achieved through the reduction of operational complexity by creating a unified platform for data aggregation, analysis, and automation.

Enable your security team to do the impossible and keep up with the never-ending security alerts that plague a highly complex IT environment. Freeing your team from dealing with false positives, repetitive alerts and low-risk warnings, SOAR lets you pivot from a reactionary approach to a more proactive one. Rather than fighting fires, security analysts can put their talents and expertise to better use, ultimately improving your organization's overall security posture.

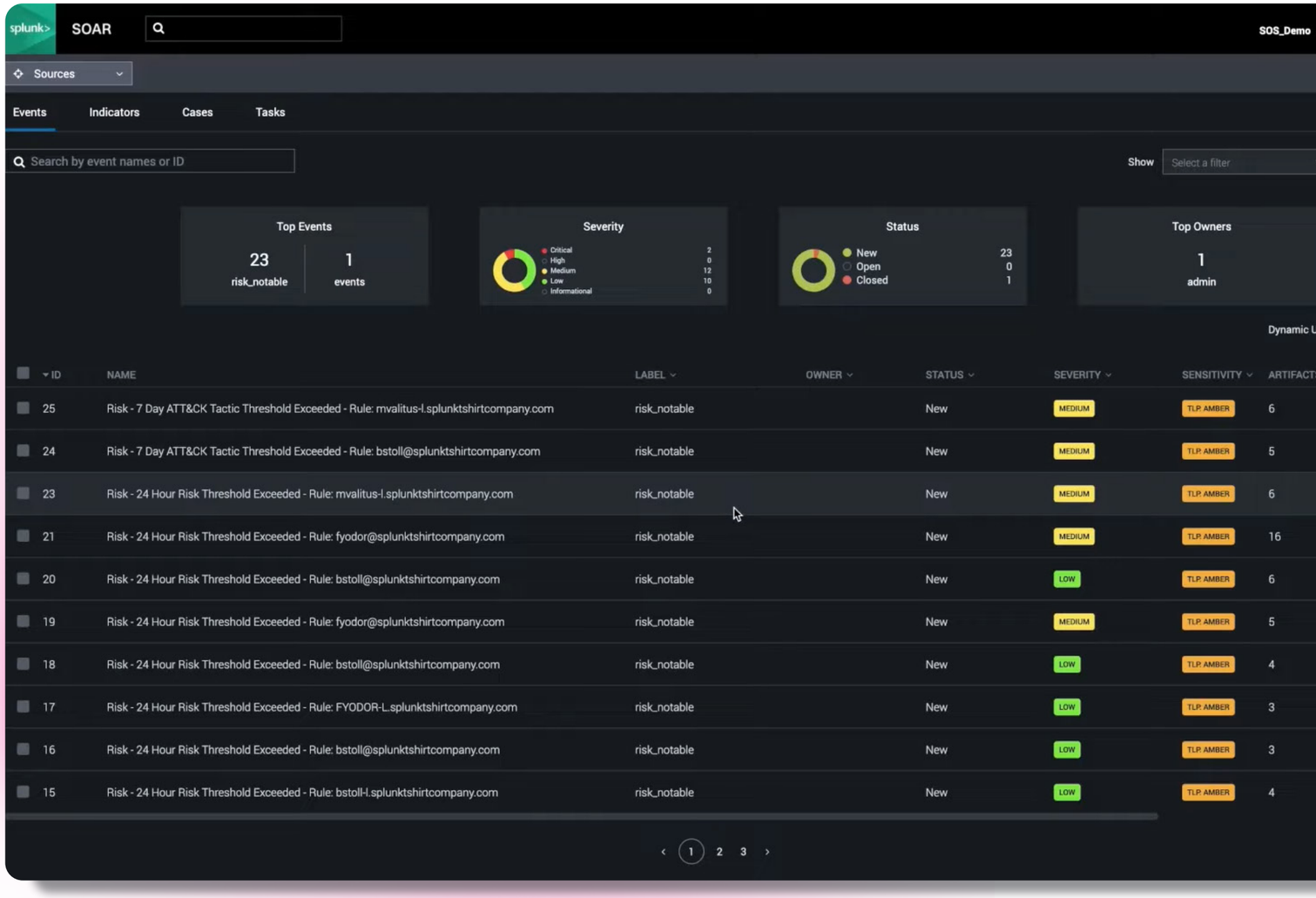
Customers that integrate Splunk products have found a **30% increase** in their operational efficiency.

## Bring order to a chaotic SOC

Splunk SOAR is designed to integrate and enhance your security operations seamlessly. It orchestrates your security stack by connecting with 300+ third-party tools and supporting 2,800+ automated actions. This allows you to streamline complex workflows across various teams and tools without the need to massively overhaul your existing security stack. Splunk SOAR also empowers you to develop custom applications tailored to your specific use cases with an intuitive App Editor. Splunk SOAR's customizable main dashboard offers a comprehensive view of your SOC's efficiency to track crucial metrics and optimize your decision-making process.

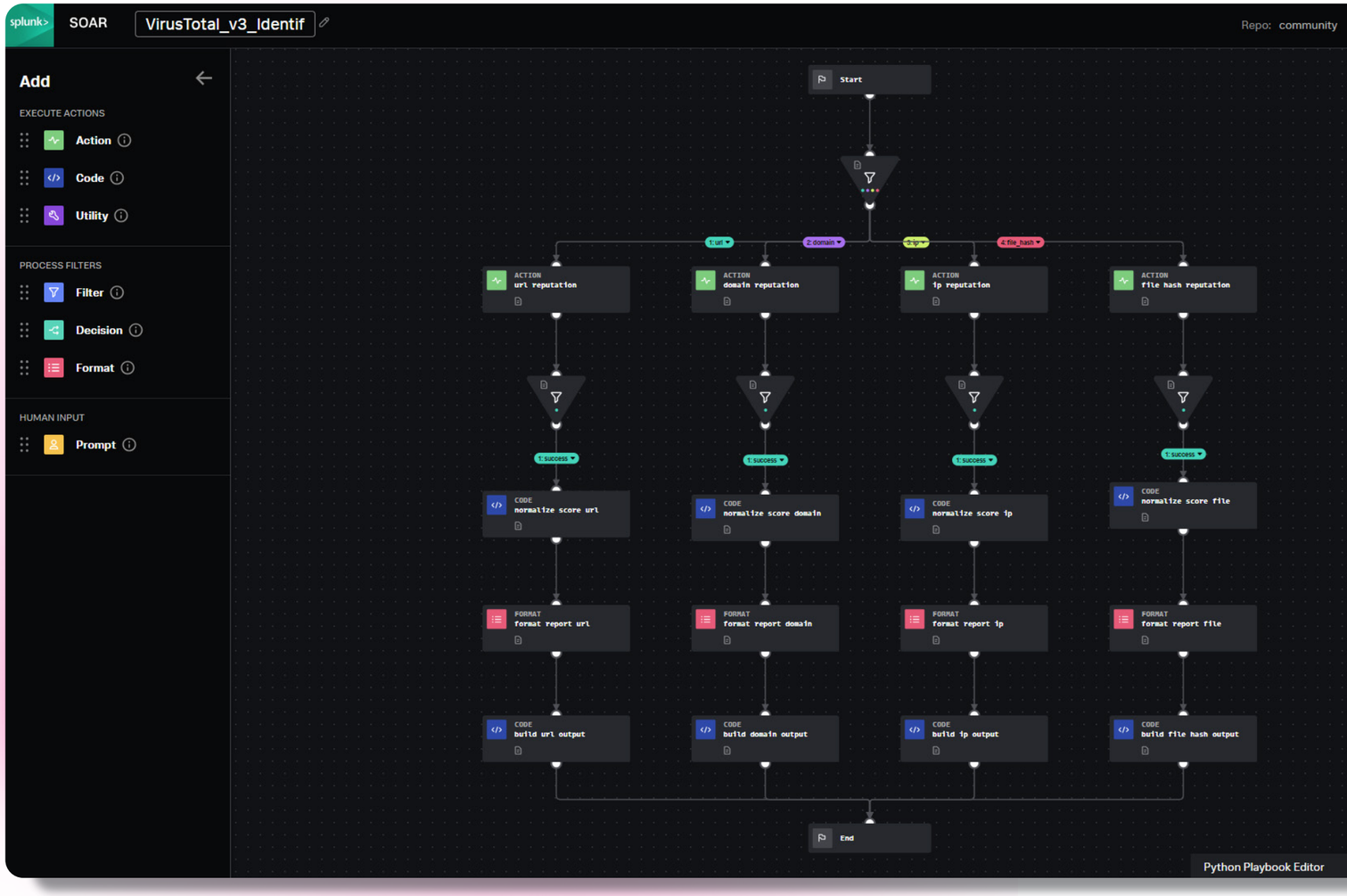
## Go from overwhelmed to in control

Splunk SOAR can reduce alert volumes by consolidating alerts and data across all tools in your environment. Splunk SOAR can then immediately automate all investigation and response actions performed by those tools to resolve incidents faster. Users of Splunk SOAR report drastic reductions in mean time to response (MTTR). For instance, events that used to take 30 minutes to resolve manually now take 30 seconds using automation from Splunk SOAR. Users of Splunk Enterprise Security can harness the power of risk-based alerting to provide enriched indicators of compromise to Splunk SOAR. This allows Spunk SOAR to then use that enriched data to automate actions through playbooks and workflows within Splunk Enterprise Security, offering a collaborative lens into organizational events. Splunk Attack Analyzer also allows for automated analysis of credential phishing and malware threats when paired with Splunk SOAR to have an even greater impact on triage and investigation.



## Respond with speed and accuracy

Splunk SOAR empowers users to easily automate security tasks with playbooks that can be customized to fit your needs. Splunk SOAR features a variety of prebuilt playbooks, which leverage the MITRE ATT&CK and D3FEND frameworks and are all aligned to foundational SOC tasks, ensuring you can automate small steps or end-to-end use cases. Splunk SOAR ensures that your responses are contextually informed through features like Contextual Action Launch. Splunk SOAR champions a collaborative approach with built-in case management functionality and workbooks that transform processes into reusable templates. Whether you're using custom templates or industry standards for incident response, Splunk SOAR facilitates task segmentation, assignment, and documentation, ensuring a cohesive and collaborative investigative process.



# Get Started.

Are you ready to learn more about how Splunk SOAR can future-proof your SOC? Speak with a Splunk expert now.

splunk>



23-494021-Splunk-The Essential Guide to SOAR-EB-107