10 Essential Capabilities of a **Modern SOC**

Inside the data-driven security operations center (SOC)

splunk> turn data into doing®

Table of Contents

Turn data into doing in the security operations center

In the last two years, enormous unpredictability has led to radical changes in the way we live and work. For organizations both public and private, digital transformation has gone from priority to urgent imperative, and accelerated cloud technologies and the power of data are driving the most critical innovations. Security teams find themselves not at the perimeter, but at the epicenter, keeping pace with transformation, adapting to pandemic challenges, geopolitical tensions, an acute talent shortage, more sophisticated attacks and a rise in breaches.

To thrive in this unpredictable world, resilient organizations are investing in security solutions that are powerful, flexible and fast — solutions powered by data. With a data-driven security operations center, organizations can protect, adapt and respond quickly to whatever comes their way, securing their organizations from ever-evolving threats.

How can you meet those challenges and tap the power of all that data? It starts with modernizing your security operation center (SOC).

Today's SOC analysts are forced to grapple with data coming from multiple sources, in different formats and at faster speeds, yet most SOCs still don't address security as the data problem it is. Effective security requires visibility into all of your data, from all systems and all the people using them — and the relevant context to better understand and manage what's really at risk. You need solutions that integrate and work across multiple systems and the massive amounts of data they create. You also need solutions that can help you navigate a complex web of tools designed to aggregate, monitor and analyze it all.

A data-driven approach to security

In a hybrid world, the challenge is not only how to keep up with all the data, but how to turn it into insight and action. Optimizing your security stack so that your team can function at peak performance requires a single data platform that frees up teams to take informed action — from investigation and monitoring to orchestration and remediation.

And a single, holistic data platform doesn't just strengthen security. It helps the entire organization tap the power of data with fewer, smarter technology investments, reduced complexity and more opportunities to innovate.

With a data-driven platform as the cornerstone of a modern SOC, you can bring data from across your organization to help solve the most pressing security problems. To secure complex environments, your team needs end-to-end visibility. For that, you need a platform designed to ingest, normalize and provide insights across disparate data streams at enterprise scale, with no sampling required. And schema-on-read and distributed indexing tools can make collecting and analyzing data from any data source fast and easy.

Atop that platform, a modern SOC needs integrated security tools that deliver actionable information when you need it using built-in threat intelligence and advanced, risk-based analysis. These tools can even prioritize incidents by organizational risk so your team won't miss a beat. You can also free up your security analysts to work smarter by automating repetitive tasks and responding to threats at machine speed. Ideally, in addition to all that machine intelligence,

a modern SOC also includes access to real-live human security experts who can keep you up to speed on the fast-moving and high-profile threats you might otherwise miss.

Together, these tools deliver a unified security posture across on-premises, hybrid and multi-cloud environments. A responsive SOC built on a powerful data platform provides better and faster threat detection, investigation and remediation capabilities while also helping your organization build resilience and unlock innovation.

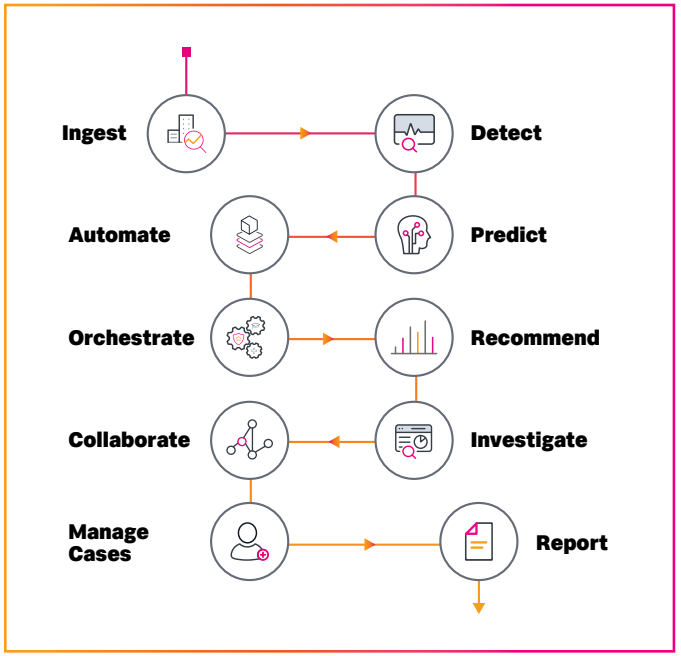
Building a Modern SOC

Security teams are hard at work on the front lines, identifying, analyzing and mitigating threats facing their organization. But despite their best efforts, incident backlogs continue to grow larger every day. The reality is that there simply aren't enough skilled professionals to analyze the volume of incidents that most organizations face.

But a modern SOC powered by and built on a unified data platform has visibility across the entire enterprise, creating a common work surface for every team member. A single security operations solution that seamlessly integrates tools from other vendors means your team doesn't have to pivot between dozens of products anymore. And that, along with one work surface for all team members, frees up your analysts' time to focus on more important things.

A modern SOC requires unified solutions, not tools cobbled together ad hoc. A data-driven security solution with strong analytics capabilities can optimize the abilities of a small to mid-sized staff, giving them insights into potential threats to keep them from wasting time on false alerts. Not only that, but a modern, data-driven SOC can tap into advanced machine learning (ML), automation and orchestration technologies as well as sophisticated threat intelligence, in one unified solution.

To build a modern SOC, organizations need a security operations platform that supports these 10 capabilities:



10 Capabilities

1. Ingest

Because data is a security problem, all data is security-relevant. A modern SOC needs to be able to ingest, normalize and provide insights into all of your data, from any source, and at enterprise scale. You also need to be able to collect and organize that data easily and efficiently.

2. Detect

When a security event happens, you need tools to detect it as quickly and accurately as possible. A modern SOC can help you detect threats using machine learning analytics and provide key insights your team needs to take action.

3. Predict

Imagine you get an alert 30 minutes before you discover a security event. Imagine what that could do for your SOC. The ability to predict a security event allows the SOC to proactively escalate the incident to a human's attention, or to streamline a response with a predefined process. There are new and emerging predictive technologies that can provide analysts with an early warning, precursors or indicators of larger attacks, as well as identifying unknowns before they become bigger risks.

4. Automate

Automation is one of the newer technologies to help SOC analysts. Organizations are at different points on their automation journeys, but when it comes to security operations, the more your SOC can automate mundane, manual tasks, the better. Security automation tools take standard operating procedures and turn them into digital playbooks that accelerate threat investigation, enrichment, hunting, containment and remediation, completing processes that used to take 30 minutes in as little as 40 seconds. With automation at work, your analysts can focus on the priorities that actually require human intelligence.

5. Orchestrate

Over time, you've probably bought dozens of products to power your SOC out of necessity — and not because you had extra budget to spend. The majority of these tools provide ongoing function and add to your defense, but they haven't evolved to keep pace with evolving threats and an API-driven world.

This is where orchestration comes in. Orchestration lets you plug in and connect everything that is inside and outside of your SOC. You no longer have to open new browser tabs or separate point solution logins for every product, and you eliminate copying and pasting from different solutions. The ability to orchestrate all your products removes overhead, reduces frustration and helps analysts focus their energy on meaningful tasks.

6. Recommend

By this point in the data-driven SOC, all security-relevant data (which is all data) has been ingested, filtered through machine intelligence and automated playbooks, and evaluated and managed with closely orchestrated tools. Wouldn't it be great if the platform powering the SOC could also tell your analysts what they should do next? Modern security operations solutions can do just that — by making recommendations. Recommendations can come in the form of individual actions or playbooks and are helpful in two ways: 1) for a new analyst, a recommendation is an educational tool so they can learn what to do when a similar threat arises again, and 2) for experienced analysts, it serves as a trusted second opinion or reminder.

7. Investigate

Chances are, your SOC analysts are drowning in a sea of alerts and wasting hours on low-fidelity alerts that they ultimately abandon. A modern SOC can help them prioritize incident investigation and response with accuracy, confidence and ease. Recent technologies like risk-based alerting reduce the "noise" of all those alerts so they focus on the ones that matter, and detect complex threats they might otherwise miss. Data-driven SOC solutions can also automate the collection of related events into a single incident to help drive to faster action and resolution. All of this helps focus time and resources, prioritize tasks, and provide coordinated tools so that analysts can put their human intelligence to work on the precise, nuanced investigation and analysis that can't be automated.

8. Collaborate

Security is a team sport that requires coordination, communication and collaboration. In a SOC environment, nothing can be dropped, events must be processed comprehensively. Teams need the ability to collaborate in real time across all of the tools, people and processes, with as much visibility and insight as possible. A data-driven security operations solution can do just that, bringing key information, ideas and data to the forefront. These capabilities help security teams to better collaborate, invite people outside the SOC to help with alerts, share critical, time-sensitive details with peers, and ultimately collaborate as an industry.

9. Manage

Even with the best team of analysts and all of these modern, data-driven capabilities, let's face it. Security incidents still happen. What's important is that when they do happen, security teams are armed with everything necessary to manage the response process. Teams need to make sure they have response plans, workflows, evidence collection, communication, documentation and timelines. This is why incident case management has also emerged as a core capability for the modern SOC.

10. Report

You can't manage what you can't measure. We live in a data-driven world and security is no different — that's why you can now measure all aspects of the security process. Having the right reporting tools helps inform on what's performing, so security teams can accurately measure where they are and where they need to go. Today's SOCs often rely on too many different platforms, making it near-impossible to get accurate reporting, let alone quickly. And with the enormous compliance, business and mission challenges today's organizations face, fast, accurate reporting is more important than ever.

Enter Splunk

The Splunk® platform is where you get started. Splunk is the unified platform for security and observability. That means with Splunk, organizations can see across all their data, gain insights quickly, respond with accuracy, confidence and ease — and do it all with one integrated solution.

Splunk can monitor and analyze data in real time, from any source, and at enterprise scale. Spunk works across multicloud and hybrid environments, providing your SOC analysts with robust tools for investigation, analysis and orchestration so they can find and remediate threats quickly, and with accuracy.

Splunk's unified, data-centric security operations solution brings together the leading security information event management (SIEM), user behavior analytics (UBA) and security orchestration, automation and response (SOAR) technologies, with integrated threat intelligence. Splunk also aligns to key industry frameworks like MITRE ATT&CK, The National Institute of Standards and Technology (NIST) and cyber kill chain. And for the public sector, Splunk is compliant with government security requirements such as FedRAMP moderate and IL5.

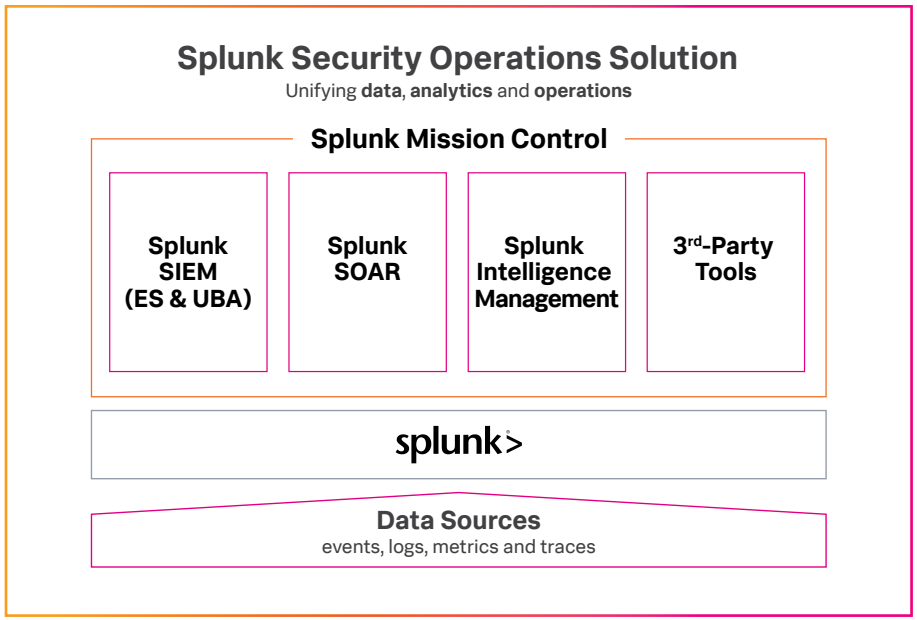
Splunk Enterprise Security (ES) is a data-driven SIEM solution that is fast, powerful and flexible, providing full visibility into your organization's security posture so you can protect against threats and mitigate risk — at scale. With unparalleled search and reporting, advanced analytics, risk-based alerting, integrated intelligence and pre-packaged security content, Splunk ES accelerates threat detection and investigation so your SOC analysts can quickly assess the scope of high-priority threats and take action. Splunk ES combines machine learning, anomaly detection and criteria-based correlation in a single security analytics solution.

With Splunk UBA, Splunk's user behavior analytics tool, organizations can detect unknown threats and anomalous behavior using machine learning. Advanced threat detection discovers abnormalities and unknown threats that traditional security tools miss. Automatically stitching hundreds of anomalies into a single threat will help your security analysts be more productive. And deep investigative capabilities and powerful behavior baselines on any entity, anomaly or threat will accelerate your threat hunting.

Spunk SOAR, Splunk's security operation, automation and response solution, lets security teams work smarter, respond faster and strengthen their organization's security defenses. Splunk SOAR automates repetitive tasks so your team can focus their time and attention on the incidents and actions that matter most. It reduces dwell times with automated investigations and reduces response times with playbooks that execute at machine speed. SOAR also integrates with your existing security infrastructure so that each part actively participates in the defense strategy — and all the parts work together.

Splunk Intelligence Management, Splunk's threat intelligence tool, automates data orchestration to centralize, normalize and prioritize intelligence across all stages of security operations. It breaks down data silos to help align security effectiveness with business objectives, improving cyber resilience and operational efficiency. With Splunk Intelligence Management, your team can easily select intelligence sources, including open source, premium intel providers and collections of historical events and alerts. They can then apply priority scores, safelists and filtering based on indicator types or attributes and submit prepared data into data repositories or a designated application of choice.

Splunk Mission Control is a unified experience that modernizes and optimizes your security operations. The cloud-based software-as-a-service (SaaS) solution allows you to detect, manage, investigate, hunt, contain and remediate threats and other high-priority security issues across the entire security event lifecycle — all from a common work surface. Splunk Mission Control integrates all of your security data and tools, whether on the cloud or on-premises, so that they operate as a unified defense system against cyberthreats of all kinds.



Get Started.

Learn how Splunk's security operations solution can help modernize your SOC.

22-18111-Splunk-10-Essential-Capabilities-of-a-Modern-SOC-109

splunk> turn data into doing®