10 Essential Capabilities of a **Modern SOC**

Data-to-Everything in the Security Operations Center (SOC)

splunk> turn data into doing™

Table of Contents

Data-to-Everything in the Security Operations Center (SOC)

We're living in a time of unprecedented innovation. Technology is refactoring entire industries, globalizing our businesses and multiplying the efficiency of our workforce. But we've only scratched the surface. As innovation continues to surge, there's no telling what we'll be able to achieve, and the consequences we could subsequently face.

As the number of connected devices swiftly approaches 80 billion, and as automation is ingrained in our everyday routines, changes in our world will only accelerate — and the attack surface will inevitably grow. Security departments are forced to grapple with data coming from multiple sources, in different formats and at faster speeds, making it clear that many organizations aren't prepared for the data challenges of today and tomorrow.

Your organization needs visibility to know what's there, and context to better understand what's really at risk. Having more data around the systems and people using them can ultimately give us a better understanding of how to manage risk.

That's why organizations are spending billions of dollars and countless hours to try and tap into the value of their data, plugging security vulnerabilities exposed by a holistic view across their infrastructure. They're creating data lakes — integrating and working across countless systems that create massive data volumes, while also navigating the complex web of tools designed to aggregate, monitor and analyze this data to address their greatest security challenges.

Our Approach: Data-to-Everything

It's vital to bring data to every question our organizations ask, every decision we make and every action we take. But in an evolving and increasingly connected world that produces ever more data, the challenge is not only how to keep up with it all, but how to turn it into insight and action. Data comes in different forms, from varying sources, which many organizations have yet to tap to better secure themselves.

Optimizing your security stack so that your team can function at peak performance requires a single platform that frees up teams to take action — from investigation and monitoring to orchestration and remediation. It must be a robust platform that enables the entire organization to leverage the power of data through a singular, holistic lense. This approach means fewer, smarter technology investments, less complexity and fewer barriers between data and action.

We call this the **Data-to-Everything Platform**. It's the very foundation of any modern security operations center (SOC), bringing data from across your organization to your most pressing security use cases.

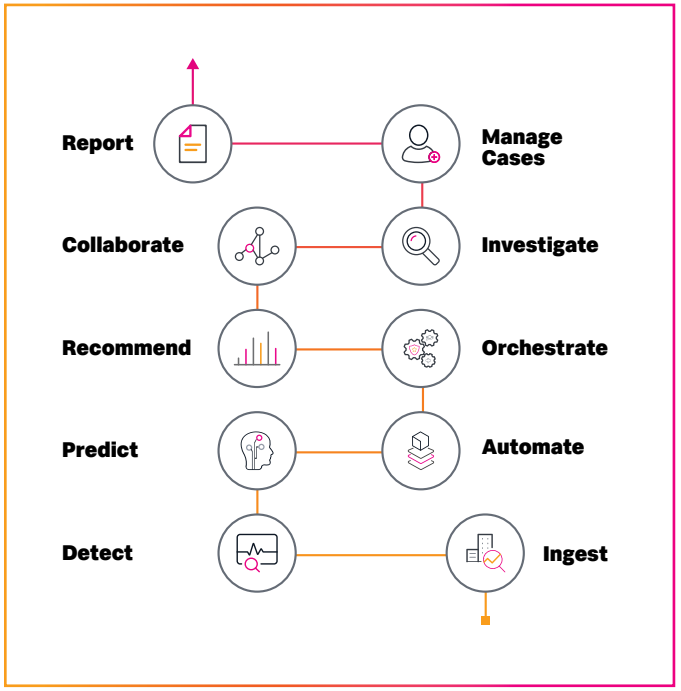
Building a Modern SOC

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 data-to-everything platform, has visibility across the entire enterprise, creating a common work surface for every team member. A single suite that seamlessly integrates solutions from other vendors to augment existing capabilities means an analyst's time will be spent on higher value activities, removing the need to pivot between dozens of products and creating a common work surface for every team member.

And this shouldn't be a solution that's pieced together ad hoc. The security suite should have strong analytics capabilities that 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. And then the last mile is the suite being able to tap into advanced machine learning (ML), automation and orchestration technologies.

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



10 Capabilities

1. Ingest

All data is security relevant. Data is the oxygen that gives life to a SOC. Analytics and algorithms breathe it. Just as important is the ability to ingest data from any source, structured or unstructured, at scale. You also need the ability to organize that data to make it actionable by machine or human.

2. Detect

Once an event has entered the system, it's imperative that the security operations suite has the ability to detect the event. In this case, detection is focused on events, which is different than traditional solutions that used to focus on files or network traffic. A security operations suite may leverage a combination of correlation rules, machine learning and analytics stories, to name a few.

3. Detect

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 or to streamline a response with a predefined process. There are emerging predictive technologies that hold a lot of promise to 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. Splunk's recent acquisition of Phantom is a prime example. Automation tools take standard operating procedures and turns them into digital playbooks to accelerate investigation, enrichment, hunting, containment and remediation.

A SOC with automation capabilities can handle more events because processes that used to take 30 minutes, for example, can now been done in as little as 40 seconds. In the evolution of a SOC, automation is no longer a choice and has become a mandatory tool.

5. Orchestrate

So you bought dozens of products to power your SOC out of necessity — not just because you had the extra budget. The majority of these tools serve a purpose and add to your defense, but they're unlikely to change. This is a problem because threats evolve, and the products that hunt threats need to keep pace in 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

At this point, events have passed through a machine. Wouldn't it be great if the platform powering the SOC could tell the analysts what to do next? The modern SOC can do just this by making a recommendation. This can come in the form of individual actions or playbooks. This is helpful in two ways: 1) For a new analyst it's educational to teach them what to do when a similar threat arises again, and 2) For experienced analysts it serves as a sanity check, or a reminder of an accelerant to aid in what they should already know.

7. Investigate

We expect 90% of tier-1 analyst work to be automated in the near future. But what happens to all that other work? Inevitably, it requires detailed, precise human analysis to finish the last mile. Intuitive security tools aid an analyst's human ability and helps them prioritize what needs to be investigated.

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 and teams need ChatOps capabilities, or the ability to collaborate and connect the tools, people, process and automation into a transparent workplace.

This brings information, ideas and data to the forefront. It enables 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 Cases

Incidents happen even when we do our best to prevent them. 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 case management has 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, the challenge SOCs face is their reliance on too many platforms, which makes it impossible to get accurate reporting.

Enter Splunk

The Splunk® platform, otherwise known as Splunk Cloud or Splunk Enterprise, is where you get started. Splunk is a customizable data analytics platform that turns machine data into tangible business outcomes. Unlike other alternatives, Splunk Cloud and Splunk Enterprise enable you to leverage your existing technology investments, as well as the expansive and expanding data generated by your IT, security and business systems, apps and devices to investigate, monitor, analyze and act in near real-time.

But more specifically, the Splunk Security Operations Suite brings together the leading SIEM, UEBA and SOAR technologies that are built on a common work surface to power the modern SOC.

Splunk Enterprise Security (ES) is an analytics-driven SIEM solution that provides real-time security monitoring, advanced threat detection, incident investigation and forensics, and incident response for efficient threat management.

With **Splunk ES**, security teams gain faster threat detection, investigation and response capabilities. They can use purpose-built frameworks and workflows to speed up detection, investigation and incident response. They can also use pre-built dashboards, reports, investigation capabilities, use case categories, analytics, correlation searches and security indicators to simplify threat management and incident management. They can then use those capabilities to correlate across software as a service (SaaS) and on-prem sources to discover and determine the scope of user, network, endpoint, access and abnormal activity.

Splunk User Behavior Analytics (UBA) is a machine learning-powered solution that finds unknown threats and anomalous behavior across users, endpoint devices and applications. It augments your existing security team and makes them more productive by finding threats that would otherwise be missed due to lack of people, resources and time.

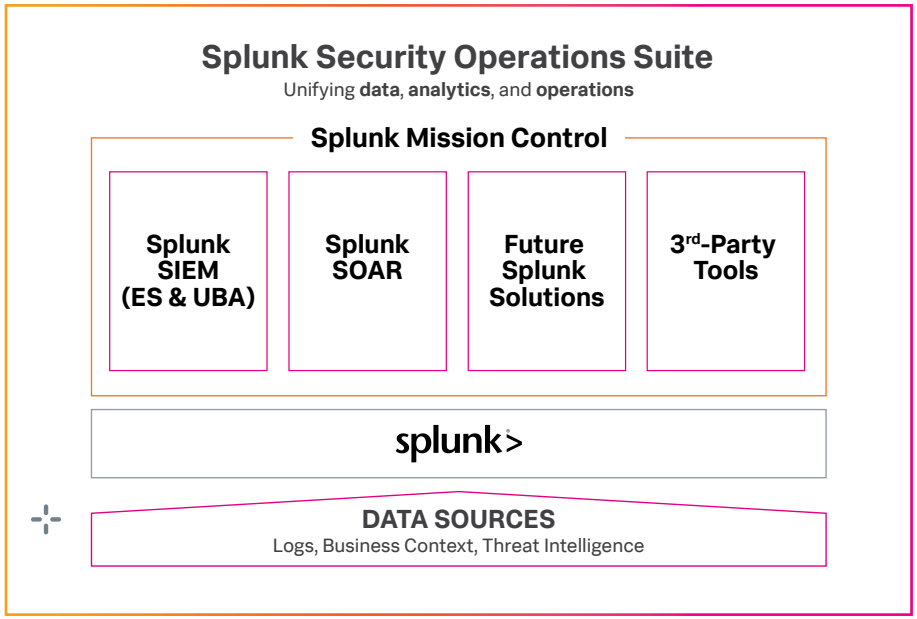
Security teams can use **Splunk UBA** to enhance visibility and threat detection. Specifically, they can detect insider and unknown threats using unsupervised ML algorithms, which traditional security products miss. They can automate the correlation of anomalous behavior into high fidelity threats using sophisticated kill-chain visualizations. This capability frees up teams to spend more time hunting with higher fidelity behavior-based alerts. They can also identify the latest threats without operational downtime with dynamic content subscription updates that empowers security teams to proactively stay current with the latest threat detection techniques.

Splunk Phantom is a SOAR (Security Orchestration, Automation and Response) platform that integrates a team's processes and tools together, enabling them to work smarter, respond faster and improve their defenses.

Phantom helps maximize the security operations efforts of a SOC. Security teams can automate repetitive tasks to optimize efforts and better focus their attention on the decisions that really need human input. They can reduce dwell times with automated detection and investigation, and reduce response times with playbooks that execute at machine speed. Phantom can also help security teams integrate their existing security infrastructure so that each part is actively participating in the SOC's defense strategy.

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 together — no matter if they live in the cloud or on-premises, so that they operate as a unified defense system against those that would do your organization harm.

Simply plug-in your Splunk SIEM, SOAR, and other existing security products into Splunk Mission Control to achieve seamless, unified security operations in the cloud. Protect your existing security investments and achieve faster time-to-value with Splunk Mission Control.



Get Started.

Learn more about how Splunk's Security Operations Suite can help modernize your SOC today.

20-15510-10-Essential-Capabilities-of-a-Modern-SOC-107

splunk> turn data into doing™