The Fundamental Guide to Building a **Better SOC**

splunk>
turn data into doing™

Staying ahead of advanced cyberthreats is hard. And detecting unknown or hidden threats is even harder, especially when existing point and legacy security tools can't address the complexity and volume of advanced security threats.

These outdated solutions struggle to detect risks posed by insider threats, laterally moving malware and compromised accounts, partly because they're not built for today's cyberthreats, but also because the software solutions that powered legacy security operation centers (SOCs) flood analysts with a high volume of alerts, many of which are false alarms.

No matter how hard-working or talented your security team is, there will be a considerable backlog of security incidents — and that's not going to get better. The reality is that there simply isn't enough skilled security talent out there — we're 3.5 million short, in fact — and the talent that does exist is expensive.

Their jobs actually get harder because of the tools they use. Dated tools used in today's SOC are not only eating away at budgets, but are also built by different vendors who don't play nicely together. And when vendors don't play nicely together, processes get slowed down and data gets lost.

As a result, analysts often can't see everything that happens across the enterprise. In fact, on average, business and IT decision makers estimate that 55% of their data is dark, unknown or untapped. So how can security professionals be expected to secure what they can't see when most of the data available is out of sight to start with? After all, all data is security relevant.

This is where understanding the origins of a SOC is imperative to making sense of the problems today. SOCs initially emerged as the new center of gravity for security operations, both physical and virtual. They required constant maintenance, expansion and an unprecedented pace to derive value.

A day in the life of a SOC analyst quickly focused on doing triage of and following up on alerts. There were too many to handle, and tier-1 analysts quickly became overwhelmed, drowning in the feeling of constantly falling further behind.

Their jobs were made harder because 80% of SOCs have been built on disparate and disconnected systems.

We all need to embrace this new reality: There simply aren't enough skilled professionals to analyze the volume of incidents that they're facing, and most don't have the right tools to close the gaps.

So what are companies who rely on dinosaur technology to do? Short of cloning all their SOC analysts and finding the pot of gold on the other side of the rainbow to pay them, it comes down to the technology that companies are using to empower their analysts to get ahead of threats.

Security teams need to respond to new threats by adding new analytic capabilities to their SOC, giving them more insight into potential threats before they grow into big scary cyber monsters. They need tools that allow security professionals to automate certain processes so they can focus on the real alerts — that is, the real threats.

It's time to build a better SOC. It's time to build the next-generation SOC.

Building the SOC of the Future Today

In the future, 90% of tier-1 analyst work will be automated. Most of their workload is mundane and repetitive, and automation lets analysts focus on what actually matters.

Second, we anticipate there being a shift from spending time triaging alerts to fine-tuning detection and response logic — creating correlation rules and playbooks to further the automation process. We anticipate that 50% of an analyst's time will spent on higher value activities.

Finally, we expect platforms like Splunk to connect and create a single platform to monitor and investigate events, which would remove the need to pivot between dozens of products.

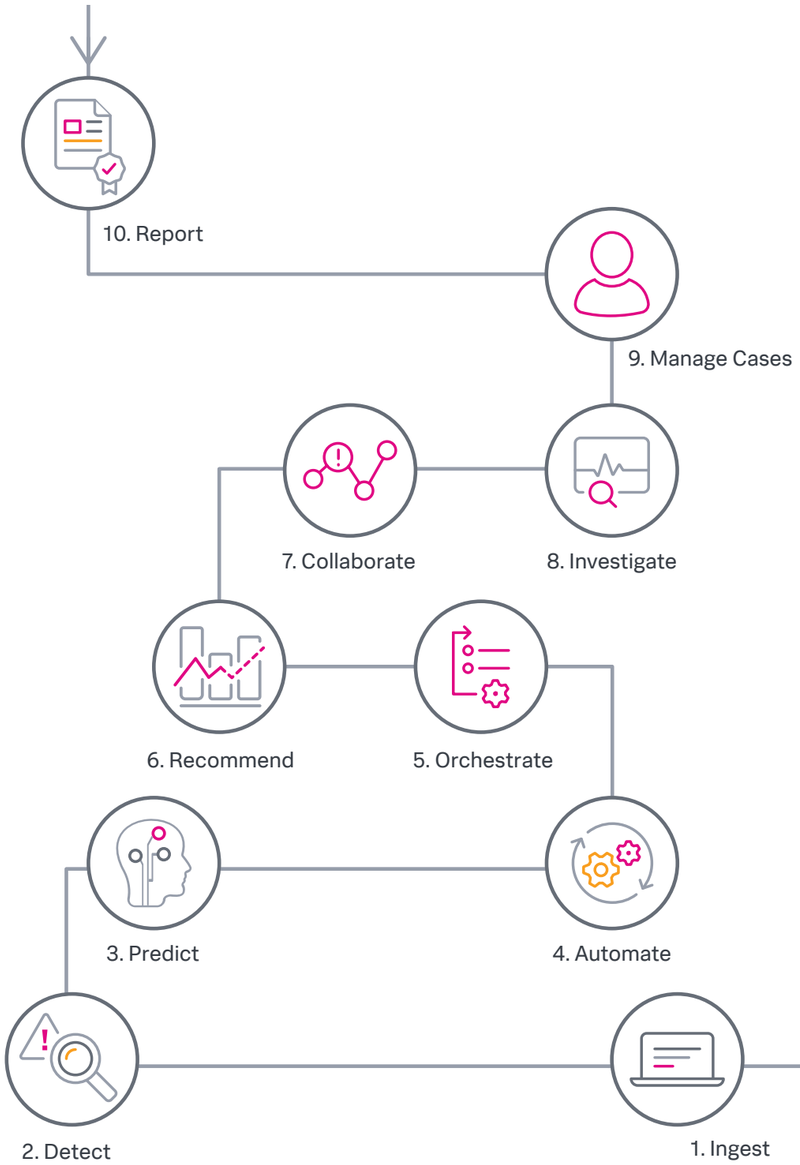
Organization don't have to wait until the future to get the **technology they need today.**

In fact, building a SOC of the future really starts with embracing a mindset that it's okay to power a SOC with a deliberately built platform, and then plug in the automation and machine learning tools necessary. It's about embracing the mindset that it's okay to become the boss of the SOC.

The next-generation SOC is built on a single suite that seamlessly integrates solutions from other vendors to augment existing capabilities. It's not a solution that is pieced together ad hoc.

The security suite should also have strong analytics capabilities that can optimize the abilities of a small 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.

Specifically, to build the SOC of the future today, organizations need a security operations platform that supports 10 capabilities:



1. Ingest

Everything starts with data. 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, just to name a few.

3. Predict

Imagine you get an alert 30 minutes before you actually 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 not likely going 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 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 next-generation 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 aide in what they should already know.

7. Investigate

We mentioned earlier that we expect 90% of tier-1 analyst work to be automated in the near future. 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 him or her prioritize what actually needs to be investigated.

8. Collaborate

Security is a team sport that requires coordination and communication. In another word: collaboration. In a SOC environment, nothing can be dropped, events must be processed comprehensively and teams need to have 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 next-generation 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**

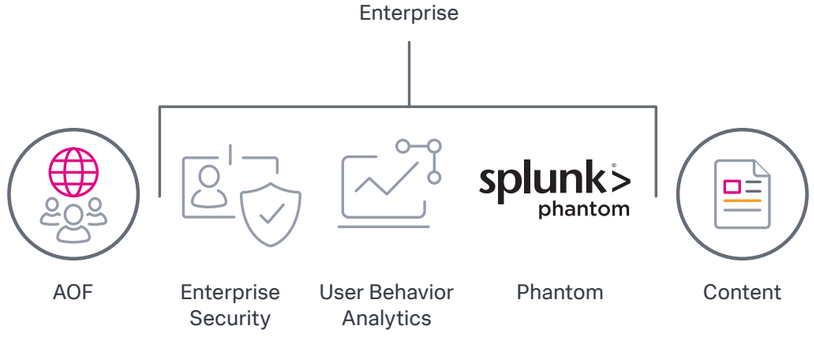
The Splunk Security Operations Suite brings together the leading SIEM, UEBA and SOAR technologies that are built on a single platform to power the next-generation SOC. No Splunk competitor can claim to have all the solutions on one platform.

Splunk not only natively supports these capabilities, but also these following use cases:

Real-Time Monitoring	Splunk Enterprise or Splunk Cloud or Splunk Enterprise Security
Investigation	Splunk Enterprise or Splunk Cloud or Splunk Enterprise Security
Automation and Orchestration	Splunk Phantom
Advanced Threat and Insider Threat Detection	Splunk User Behavior Analytics or Splunk Enterprise Security
Incident Response	Splunk Phantom or Splunk Enterprise Security
Compliance	Splunk Enterprise or Splunk Cloud or Splunk Enterprise Security

The Splunk platform, otherwise known as Splunk Cloud or Splunk Enterprise, is where you get started. This is where you ingest your data. Splunk is a customizable data analytics platform that turns machine data into tangible business outcomes. Unlike SaaS and other open source 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.

Splunk Security Operations Suite



But more specifically, the Splunk Security Operations Suite is made up of:

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-premise sources to discover and determine the scope of user activity, network activity, endpoint activity, access activity 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 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 together so that each part is actively participating in the SOC's defense strategy.

About Splunk.

Splunk Inc. makes data accessible, usable and valuable to everyone.

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

2020-Splunk-SEC-Fundamental-Guide-to-Building-a-Better-Security-Operations-Center-110-EM

splunk>
turn data into doing™