Essential Guide

10 Essential Capabilities of the SOC of the Future

How unified threat detection, investigation, and response is the core of a resilient SOC

splunk>
a CISCO company

Contents

What makes the SOC of the future?

Keeping your organization secure has never been more difficult — or more important. Security teams are dealing with a growing volume of threats, across a complex and fragmented technology stack. Attackers are evolving quickly, with criminal groups and nation-states using automation and AI to increase speed and scale. At the same time, organizations are under pressure to meet constantly changing compliance requirements, while trying to make sense of data scattered across environments and systems.

The problem isn't just more data or more alerts — it's siloed operations that make it hard to respond quickly, with confidence.

The SOC of the future is built to solve this. It's not a single tool. Rather, it's a set of core capabilities across people, processes, and technologies that work together to deliver resilience. A resilient SOC provides complete visibility across your environment, gives analysts context to make faster decisions, and builds in collaboration and automation at every step of the workflow.

This is the SOC that positions you to deliver on risk management, governance, security metrics, and compliance goals across your organization.

Security will never be simple. But with the right operating model, it can be manageable — and even proactive. That's the promise of the SOC of the future.

This guide outlines the **10 essential capabilities every modern SOC should master** — from managing distributed data to automating response workflows. Together, these capabilities enable teams to operate at scale, stay ahead of threats, and drive outcomes that matter.

> **There's no magic button for building the SOC of the future. It's an intentional, iterative process that requires collaboration and buy-in across the entire business.**
>
> — Mike Horn, SVP and GM, Splunk Security Products, Cisco

Why unified TDIR is the core of the SOC of the future

To keep up with today's volume and velocity of threats, security teams need more than just detection — they need an end-to-end workflow that connects detection, investigation, and response in a single platform.

A unified TDIR platform is the foundation of the SOC of the future. When these capabilities are siloed across tools and teams, it slows response time, introduces gaps in context, and burdens analysts with unnecessary friction. Bringing these workflows together — from initial alert to resolution — drives real operational impact.

The benefits go beyond faster response. A single platform supports tool consolidation, reducing the sprawl of overlapping solutions and scattered data. It drives simplicity and efficiency, helping teams focus on high-value work rather than chasing down context across systems. And it helps keep budgets in check, with optimized data management and smarter ingestion strategies that scale to meet rising volumes without the spiraling costs.

This shift is essential to building a more resilient SOC — one that not only reacts to threats but operates with speed, confidence, and clarity.

Up next: The 10 essential capabilities that bring this vision to life, and help teams build a SOC that's ready for what's ahead.

> **Security teams have been vying for a single platform for a long time. In the future, we'll finally see that come to fruition.**
>
> — Kamal Hathi, SVP, Products & Technology, Splunk

The 10 capabilities of the SOC of the future

1. Federate and manage all of your data

Search, analyze, and act on data — no matter where it lives. By federating access across diverse data stores, you can reduce duplication, improve time to insight, and drive smarter decisions without moving or rehydrating data. It's the fastest path to visibility, flexibility, and scale — particularly in today's hybrid environments.

2. Continuously discover and monitor your attack surface

SecOps teams struggle to understand their asset landscape. Continuous asset discovery helps uncover shadow infrastructure, out-of-policy deployments, and security blind spots across your environment. Map and monitor your full attack surface — and close compliance and control gaps before adversaries can exploit them.

3. Detect threats with full context

Detect smarter, not noisier. Use a range of methodologies — from behavioral analytics to correlation across events and sources — all mapped to frameworks like MITRE ATT&CK. By enriching alerts with context and aligning to detection-as-code practices, your SOC can focus on what's real, not just what's flagged.

4. Automate routine but error-prone tasks with AI

Security teams are overloaded and analysts need to be trained faster. AI can help. Use AI to write summaries, prioritize incidents, and enrich alerts — giving your team time back to focus on judgment calls, not copy-paste busywork. Simplify the analyst experience and reduce burnout without losing control.

5. Investigate holistically

Investigations shouldn't be scavenger hunts. Pull together timelines, telemetry, context, and historical activity into a single view so analysts can quickly understand the who, what, when, and how of an incident. Streamlined investigation workflows mean faster response, deeper insight, and fewer handoffs.

6. Engineer and evolve your detection strategy

Your threat landscape changes daily. Your detections should, too. Use behavioral analytics, threat modeling, and detection-as-code practices to continuously refine and expand your detection library. With automation and version control, detection engineering becomes repeatable, testable, and scalable.

7. Automate threat response

Accelerate your response with automated playbooks that streamline containment, ticketing, notifications, and remediation. Reduce mean time to response (MTTR) while improving consistency and coordination. Automation doesn't replace analysts — it helps them act faster, with confidence.

8. Unify TDIR with integrated workflows

Break down silos across detection, investigation, and response. A unified TDIR workflow keeps everything — evidence, context, handoffs — in one place, so teams can move faster and stay aligned. Custom playbooks help automate steps while preserving flexibility and human oversight.

9. Collaborate across the SOC and organization

Security is a team sport. Make it easier for analysts, threat intel teams, and IT responders to work together with shared context, case notes, and escalation paths. Collaboration isn't just internal — build the muscle to engage with legal, compliance, and leadership, too.

10. Report on what matters

Translate SOC activity into business-aligned outcomes. Use dashboards and reporting to track risk reduction, threat coverage, compliance, and operational efficiency — not just raw alert volumes. Help stakeholders understand what's working, where the gaps are, and how security drives resilience.

Powering the SOC of the future with the leading TDIR solution

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 high and IL5.

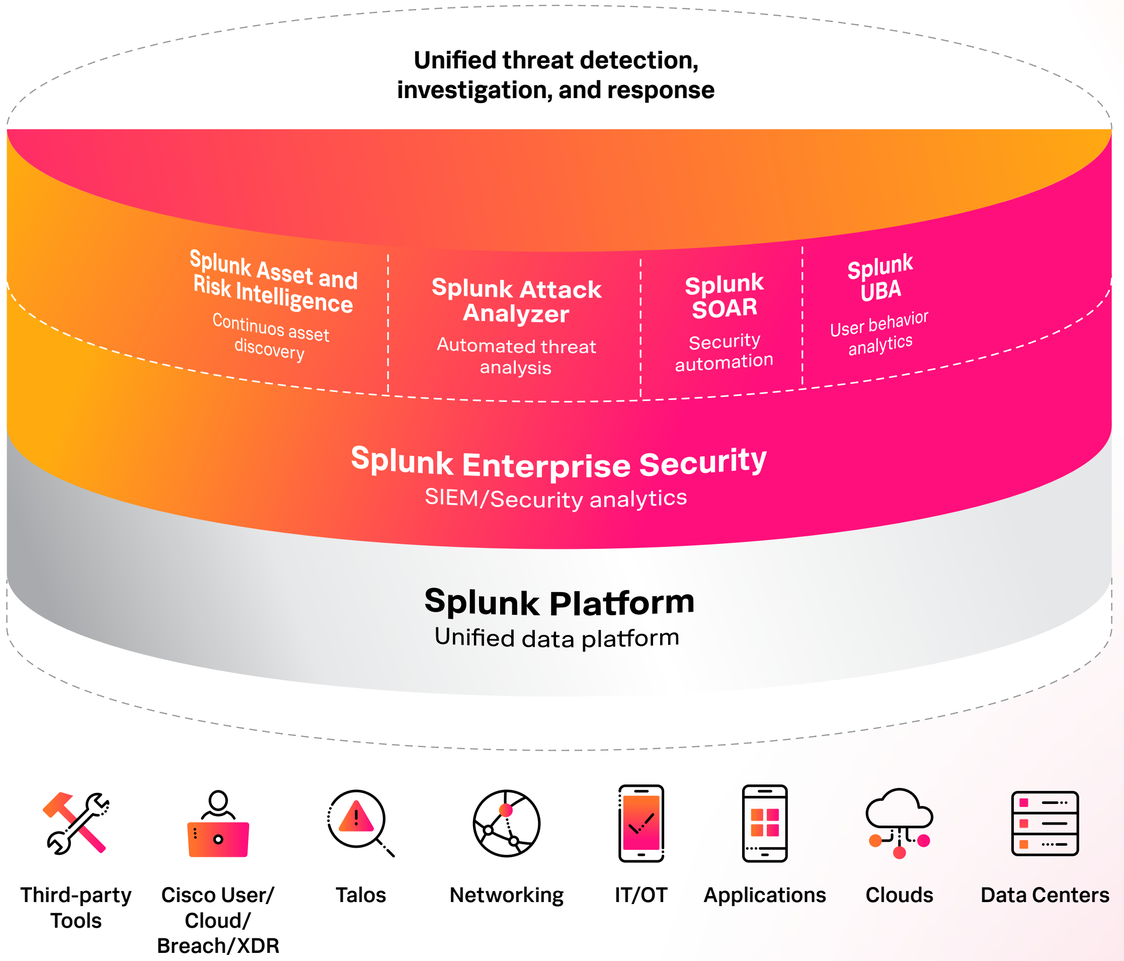
Splunk® Enterprise Security (ES) is the market-leading SIEM and security analytics solution trusted by SOCs around the globe. Its powerful capabilities enable you to realize comprehensive visibility, empower accurate detection with context, and fuel operational efficiency. Splunk has paved the way in advancing SIEM and security analytics by being at the forefront of innovation in security to help thousands of customers outpace adversaries. Its powerful capabilities enable you to realize comprehensive visibility, empower accurate detection with context and fuel operational efficiency. Built on the Splunk platform powered by AI capabilities, ES powers analytics at scale for continuous security monitoring and cost-effective data optimization. With Splunk, you can detect what matters, investigate holistically and respond rapidly.

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.

Splunk 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 Asset and Risk Intelligence provides a unified, continuously updated inventory of assets and identities by correlating data across multiple sources — including network, endpoint, cloud, and scanning tools. Accelerate security investigations with accurate asset and identity context, uncover compliance gaps in security controls, and reduce risk exposure.

Splunk Attack Analyzer gives your team automatic analysis of active threats for contextual insights to accelerate investigations and achieve rapid resolution. Take the manual work out of threat analysis — and gain consistent, comprehensive, high-quality threat analysis. When paired together, Splunk Attack Analysis and Splunk SOAR provide unique, world-class analysis and response capabilities, making the SOC more effective and efficient in responding to current and future threats.



Build digital resilience with Splunk

Improve data accessibility. Access data-driven insights. Remove data silos. Splunk is a single platform designed for the way you work, with the capabilities your business demands.

- Try Splunk Enterprise free for 60 days.
- Join the discussion on the Splunk Community forum.
- Contact sales to assess your requirements.

splunk> a CISCO company

25_CMP_essential_10-essential-capabilities-of-the-SOC-of-the-future_v6