Path to Resilience

Building a Modern Security Program

How security teams can use Splunk to power the SOC of the future

splunk>

“Go to Red Alert.”

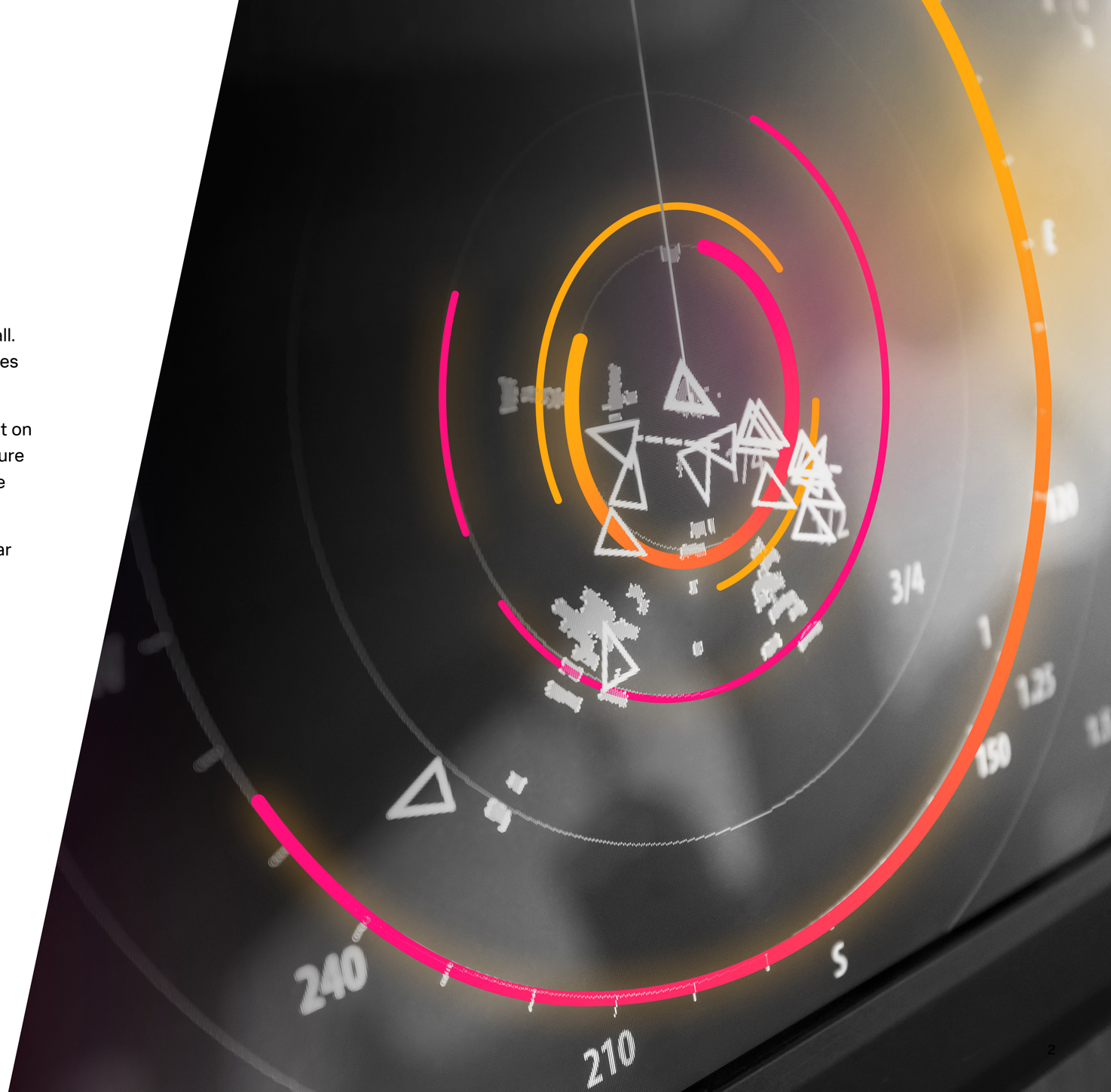
Across galaxies, TV seasons and a smattering of films, William T. Riker makes the familiar call. The deck of the Starship Enterprise bursts into a flurry of activity as each crew member does everything in their power to thwart the attack, stop the breach and secure the ship.

No, you’re not in the wrong e-book. Think of the Enterprise as an enterprise: an entity reliant on a complex and distributed set of digital systems and tech stacks working in concert to ensure mission success. The people, systems, processes — and of course Data — in the bridge are tasked with working together to protect it all.

Although each threat to the Enterprise is seldom the same, each episode follows the familiar arc, capped off by a witty anecdote, some tea or a dram of something stronger in Ten Forward. After the threat fades and the alerts cease to blare, the crew of the Enterprise always have a moment to breathe, laugh and reset before the next threat emerges.

Not so in real life.

Down here on Earth, security teams can struggle to break out of a constant state of “Red Alert.” Their battle is constant: making the impossible choice to respond to the next alert or to be more strategic and improve their security posture over time. It’s getting in the way of digital resilience.



A digitally resilient future written in the ~~stars~~ data

Advancing your security maturity is no longer a “nice to have.” In the increasingly complex threat landscape and technological environment, every team needs to keep their organization safe *today* while also preparing to do better tomorrow.

Maturing your security practice is vital to this journey. Teams need the ability to proactively spot threats and see root causes of problems with full control over their data.

With a modern security program, organizations have more visibility into their vast, interwoven environments and are able to achieve greater digital resilience. This means fewer breaches, shorter dwell time, faster issue resolution and safe, protected digital experiences.

“We now have visibility into all of our tools and resources, whether they’re homegrown or third-party applications. That information raises security consciousness and informs the actions we take across the business.”

— Ojasvi Chauhan Threat Detection Engineer, Tide

Today’s SOC teams face a constellation of challenges:

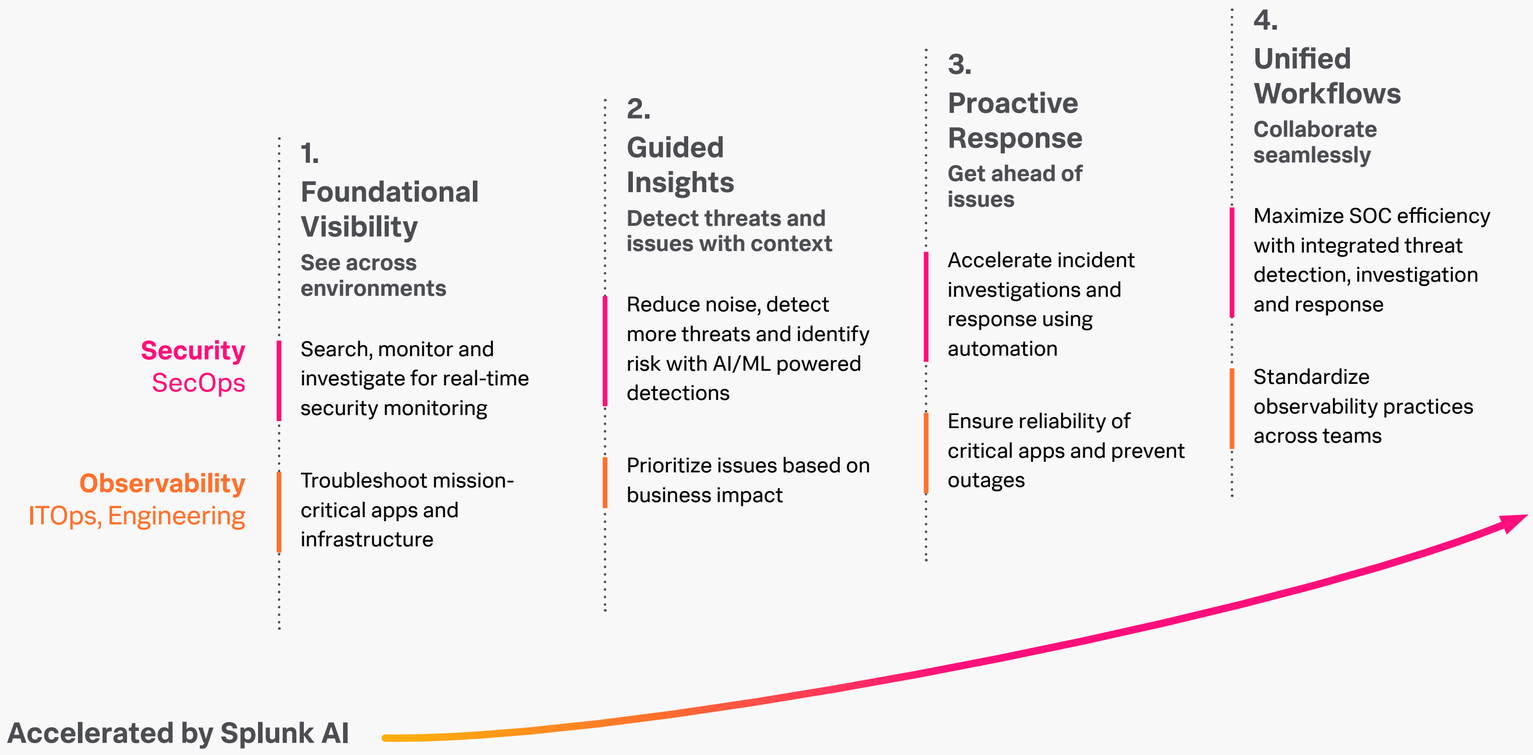
- **Digital complexity:** Organizations often lack a unified view across their infrastructure and security stack, creating data silos and blind spots.
- **Alert fatigue:** Analysts spend too much time triaging events and managing a high volume of isolated, low-fidelity alerts.
- **Disparate tools:** Security operation centers (SOCs) juggle a grab bag of security point products that lack interoperability.

Digital resilience at enterprise scale

All hands on deck. It takes SecOps, ITOps and engineering teams working together to ensure digital systems are reliable, trustworthy and secure. That's why we've created a model to guide teams as they expand into new and complementary use cases across security and observability.

For security teams, this model will help solve pressing point-in-time problems, improve their security posture and optimize operations — helping them stay light years ahead of threats. Or at least detect and stop them even faster.

The Path to Greater Digital Resilience



Make it so: Propelling the SOC of the future

The world's largest organizations rely on Splunk to help keep their digital systems secure and reliable. With Splunk's Unified Security and Observability Platform, organizations can overcome the complexities, threats and disruptions that come between them and their mission — helping them move from foundational visibility, through understanding risk and performance and getting ahead of major issues, to achieving unified workflows that allow teams to collaborate seamlessly.

IDC

Ranked #1

in SIEM Market Share

in ITOps and Analytics Market Share

Gartner

A Leader

Magic Quadrant™ for Security Information and Event Management

Magic Quadrant™ for Application Performance Monitoring and Observability

GIGAOM

A Leader

in Cloud Observability, APM, AIOps and Incident Response Platforms

in Observability and AIOps Markets

FORRESTER®

A Leader

in Forrester Wave™ Security Analytics Platforms

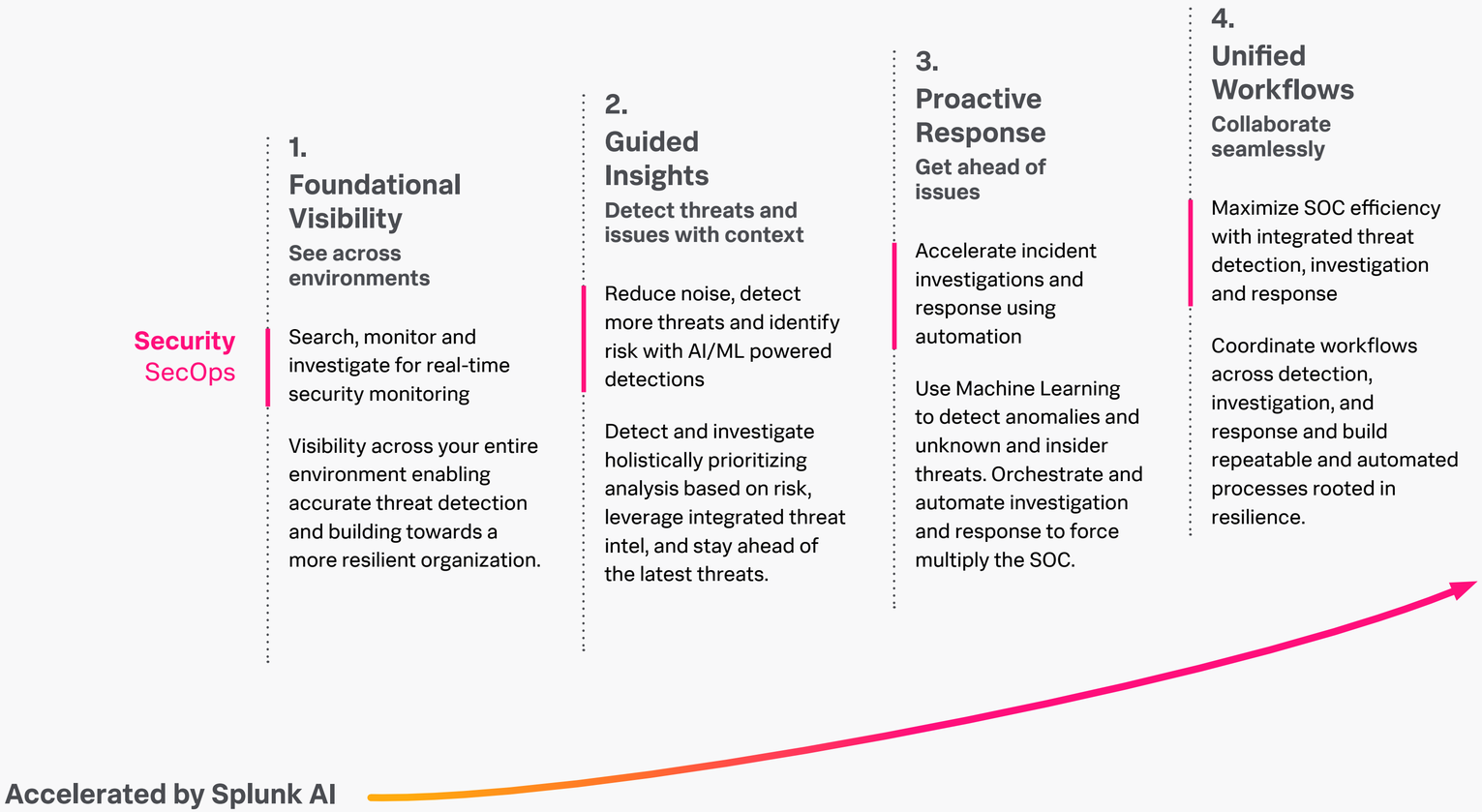
In the following pages, we'll share steps you can take to expand into new or more advanced security use cases across your team and organization. Each section includes check-in questions to help you self-score and determine how to most effectively allocate resources and staff.

As you embark on the journey, remember the wise words Lieutenant Commander Data shared: "The effort yields its own rewards." The most important thing is to start. The time is now, and we'll show you the way.

"I know the number of threats against the university is higher and the complexity greater than ever before. But I also know that we're protecting the university at a level we've never had before. "

— Bill Britton, Chief Information Officer, Cal Poly

Modernizing the SOC: Journey Stages



1. Foundational visibility

See across environments

Organizations need to be able to see across their entire environment and security stack to turn vast volumes of raw data into actionable insights and zero in on impending or existing threats.

The problem

Modern environments are complex. Organizations need to wrangle an increasing level of complexity, forcing data into silos. These silos create blind spots — hindering visibility and impacting teams' ability to keep systems secure and reliable. Even if an organization is able to correlate data between different sources, they're often missing greater context. In combination with the use of disparate tools to detect and resolve incidents, this contributes to teams' inability to identify root causes and implement preventative measures. On top of it all, ever-evolving compliance requirements put a strain on already under-resourced security teams.

The Splunk solution

Visibility is fundamental for a reason. When teams can see across their entire digital footprint, they can search, monitor and investigate in real time. Here's how Splunk helps your team start building (or strengthening) this key step in building greater digital resilience.

1. **Create a data optimization strategy:** Splunk Enterprise and Splunk Enterprise Security can ingest, normalize and analyze log data — no matter its source — from across the enterprise without having to manually stitch together data from disparate tools. With optimized data, teams can filter and route it more efficiently, based on its value to the enterprise. With 1,000+ integrations, Splunk Enterprise Security can ingest, normalize and analyze data from all enterprise sources, helping teams move on more quickly from analyzing and investigating.
2. **Analyze and confirm high-priority incidents:** With optimized data, security teams can then build the foundational security monitoring and incident management capabilities required to detect and investigate threats across their attack surface. Splunk Enterprise Security helps teams quickly detect and investigate threats while remaining flexible and extensible. With powerful security analytics capabilities, teams can easily analyze and confirm high-priority incidents.
3. **Quickly understand risk exposure and easily access deep dive views into security functional areas:** With pre-built, customizable dashboards, content and visualizations, security teams (and anyone in the organization) can gain real-time insight and granular visibility into data, team performance and security metrics on a single pane of glass to simplify security monitoring and incident management. It's also easy for key stakeholders to ensure adherence to the evolving compliance and regulatory landscape.

Check-in

- ☐ **Can you easily identify the most relevant data source types to ingest?**
  Fundamental visibility depends on your ability to optimize your data sources and search data where it lives to leverage key tasks like normalization, enrichment and data availability and retention.
- ☐ **Can you identify all your assets and identities and prioritize alerts based on their relative importance?**
  Do you need better tools for greater visibility across systems so you can improve how you respond to, and recover from, a cyber incident?
- ☐ **How are you tracking and managing compliance for organizational risk?**
  Without real-time posture and insights across all your IT/OT resources, it can be difficult (or impossible) to clear compliance and pass audits in today's ever-evolving regulatory environment.
- ☐ **Are you able to report on real-time security indicators to everyone who needs to know?**
  With one dashboard to highlight relevant key security indicators in real time, you can share that data with stakeholders — or better yet, give them their own dashboard to check themselves.

Resilience in action

Soriana

Soriana, one of Mexico's largest supermarket chains, needed real-time visibility across over 40,000 devices, including 15,000 points of sale. With Splunk, Soriana is able to monitor all its systems across its hybrid infrastructure, reducing MTTR, providing deeper insights to the security team and reducing fraud and security risks.

99% faster mean time to repair for POS monitoring process to thirty minutes, down from two days.

I'm very happy with Splunk. It's a powerful and reliable tool with powerful support — the product, the teams and the partners that come with it.

— Sergio Gonzalez, CISO, Soriana

2. Guided insights

Detect threats and issues with context

By reducing noise and enabling teams to focus on the incidents that pose the greatest risk and impact to the organization, teams are better able to stay ahead of the latest threats — all while saving a lot of time by only chasing real leads.

The problem

Every alert, everywhere, all at once. Today's security teams are often under-resourced — in terms of headcount, processes and tools. With inefficient toolsets that struggle to search through high volumes of data, the latest threats can fly under the radar. And, in a SOC environment overwhelmed with a storm of low fidelity, high-volume alerts, analysts have a hard time accurately detecting, contextualizing and prioritizing threats by organizational risk.

The Splunk solution

When teams are able to detect low-and-slow attacks that can be missed with a traditional search and prioritize threats according to organizational risk, they can optimize investigations and remove the persistent noise that keeps them in fire-fighting mode.

1. **Reduce noise in the SOC with a risk-based approach:** Splunk Enterprise Security delivers continually updated detections and integrates threat intelligence and ML models to help security teams reduce false positives and accurately detect, contextualize and prioritize real threats by organizational risk.

   Risk-Based Alerting (RBA) transforms a multitude of alerts into high-fidelity notables and places them in the context of related risky behaviors that may indicate a threat — saving analysts' time by prioritizing alerts for further investigation.

2. **Use AI and ML to stay on top of advanced and insider threats:** Splunk Enterprise Security includes over 1,700 out-of-the-box detections and integrates threat intelligence and ML models to automatically detect and conceptualize threats accurately.

3. **Use multiple threat intel sources and operationalize industry frameworks:** With Splunk Enterprise Security, detections are built by industry-recognized experts that align to frameworks like MITRE ATT&CK,® NIST, CIS 20 and Cyber Kill Chain. It delivers a continuous stream of updated detection content and threat intelligence enrichment along with ML-based models.

Check-in

- ☐ **Do your SOC analysts have an objective view of critical events *and* a comprehensive view of the potential risk to the enterprise?**
  If not, are alerts and manual repetitive tasks negatively impacting their ability to conduct and prioritize investigations of critical events because they're having to sift through multiple data feeds?
- ☐ **Does your team have the resources to get out of fire-fighting mode and prioritize cultural and technological transformation?**
  Being more resilient takes time, resources and expertise. If that expertise is being spent addressing alert after alert, your team won't be able to optimize your security operations.
- ☐ **Are you able to use industry standards like MITRE ATT&CK®?**
  For your security monitoring practice, are you easily able to find the right content to protect against relevant threats?
- ☐ **Are you relying on human-made correlation rules in your anomaly detection?**
  They've probably caught some threats, but they can't be relied upon to identify all the threats to your environment. While your security team is overwhelmed by the sheer volume and sophistication of threats, stealthy, hidden and unknown threats can be missed.
- ☐ **Are your SOC analysts able to conduct investigations and threat hunting across the entire attack surface with a single tool?**
  Their accuracy (and peace of mind) could be greatly improved if their threat hunting tool is able to surface insights that are generally not found through day-to-day correlation activity.

Nasdaq

Nasdaq needed a data platform for end-to-end visibility across its hybrid infrastructure. With Splunk Enterprise Security, Nasdaq teams are able to quickly investigate unknown and advanced threats. Splunk also provides deep understanding of data and reusable correlation rules across all support engineer levels.

Over 50% increase in analyst efficiency to gather data and speed security investigations

Splunk allows us to have a single skill set that is common across the entire organization. Information security is writing queries but using the same language as our operations team.

— AVP, Nasdaq

3. Proactive response

Get ahead of issues

When SOC teams are overwhelmed, security can suffer. By using automation to accelerate incident investigations and response, analysts can get ahead of issues. Being able to perform initial triage at scale, without human intervention — and orchestrating response workflows across your organization — organizations can get closer to achieving the operational efficiency needed to outpace adversaries. They'll also help reduce burnout to protect any organization's most valuable resource: the team.

The problem

The sheer number of potential threats SOC analysts have to triage and address isn't even half the battle. Having to manually synthesize data, files and URLs to formulate insights and draw conclusions slows MTTR. Complex security stacks that comprise many security tools don't interoperate effectively. This contributes to the problem, leading to alert fatigue, burnout and loss of SOC staff. This isn't a personnel issue: It's a resilience issue. With fewer people and a lack of visibility and context, incidents are inconsistently handled, leading to missed threats and increased dwell time.

The Splunk solution

1. **Automate threat analysis:** Get ahead of issues and accelerate incident investigations with automation. Splunk Attack Analyzer gives security teams automatic analysis of active threats for contextual insights to accelerate investigations and achieve rapid resolution. With interactive visualizations, Splunk Attack Analyzer helps teams determine how threat actors are operating and its proprietary technology ensures analysts can safely interact with malicious content through live detonation capabilities.
2. **Reduce mean time to respond:** SOC teams need to be able to efficiently contain and minimize the impact of attacks to protect the organization. Splunk SOAR helps teams automate initial triage at scale, without human intervention. When paired together, Splunk Attack Analyzer 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.
3. **Mitigate staff burnout:** Automate simple and routine processes to free up time for the SOC team to focus on other tasks — and get out of fire-fighting mode. Splunk SOAR enables SOC teams to quickly automate alert triage and incident response and quickly implement out-of-the-box playbooks that work with the installed apps and tools in their security stack. They can easily determine severity of alerts by looking up indicators of compromise and enrich the data and keep up with evolving threats.

> **Instead of spending hours looking into an incident, it can often be handled in just minutes.**
>
> — Ojasvi Chauhan, Threat Detection Engineer, Tide

Check-in

- ☐ **Is your team feeling overwhelmed from dealing with the number one threat vector: phishing?**
  If you're not automating the analysis of suspected phishing emails, it's easy for your security analysts to feel the strain — and inadvertently miss things.
- ☐ **Have members of your team expressed they feel burned out from alert fatigue?**
  It's hard enough finding and keeping talent. Poor alert triage processes can lead to missed threats, a rise in security breaches — and burnout and loss of SOC staff.
- ☐ **Do your security analysts express they have the time to handle the most sensitive and unique incidents?**
  Workflow actions or playbooks that process repetitive and ordinary alerts protect your organization's security posture, and can protect your analysts from burnout.
- ☐ **Is it relatively easy for you to automate simple and routine processes?**
  By automating repetitive tasks that your analysts do day in and day out, you're ensuring a level of quality for both your outputs and team's wellbeing.
- ☐ **How many tools from different vendors do you have in your security stack?**
  A proliferation of tools doesn't make things better — it can make them worse. Swiveling from product to product to get the right information can delay MTTR.

Resilience in action

Carrefour

Although Carrefour spent significant resources maintaining legacy infrastructure and detecting security events, it's sometimes complicated to provide the multi-channel experience customers expect. With Splunk Cloud Platform, Carrefour better protects its business and improves customer experience with actionable insights into system performance and faster security response times.

3x faster threat response times

We get so much value from Splunk. It maximizes the insights we gain from analyzing detection use cases, rather than wasting time creating rules or struggling with a tool that's too complicated.

— Romaric Ducloux, SOC Analyst, Carrefour

4. Unified workflows

Collaborate seamlessly

Maximize SOC efficiency with integrated threat detection, investigation and response. Coordinate workflows across detection, investigation and response and build repeatable and automated processes rooted in resilience.

The problem

Detection, investigation and response are often spread across siloed tools while security insights are diffused across interfaces, making it difficult to achieve intelligent situational awareness. Security teams are also hindered by a lack of established security workflows. In the absence of these security standard operating procedures, analysts are unable to work together effectively to resolve incidents. A shortage of cybersecurity professionals makes it exceedingly difficult for understaffed security teams to respond to a backlog of thousands of alerts. The most advanced teams look to share data with and collaborate across their ITOps and engineering counterparts to empower that visibility.

The Splunk solution

With an enterprise-grade platform, SOC teams have data and tools unified within a common work surface, helping them align within and across teams and have an easier time prioritizing incident response based on urgency.

1. **Use automation to respond faster:** By automating manual, repetitive security processes across your integrated security stack, you can make a team of three feel like a team of 10. Splunk SOAR provides security orchestration, automation, and response capabilities that empower your SOC, allowing security analysts to work smarter, not harder, by automating repetitive tasks and triaging security incidents faster.
2. **Get out of fire-fighting mode:** Splunk security solutions are powered by an AI-enhanced platform, extended with industry-defining products (such as Splunk Enterprise Security, Splunk SOAR, Splunk User Behavior Analytics, and Splunk Attack Analyzer), transforming your SOC from reactive chaos to a modern, unified threat detection, investigation and response (TDIR) experience.
3. **Empower teams with one unified work surface:** Simplify security workflows by codifying processes into response templates to build repeatable processes. Empower security operations with the speed of automation right from single, modern work surfaces, and any stakeholder can have a real-time view of what they care about on Glass Tables.

> **Splunk enables us to stay ahead of the trends shaping digital transformation — not just keep up with them.**
>
> — Stephen Leung, Head of Information Technology and Fintech Development Department, The Bank of East Asia, Limited

Check-in

- ☐ **Does it feel like your team does a lot of toggling between user interfaces, tools and query languages?**
  Sometimes a shortcut really isn't. Without a unified platform for threat detection, investigation and response, it can be hard for teams to feel aligned.
- ☐ **Is your SOC team able to understand the last attack before the next one happens?**
  Adversaries have access to sophisticated tools and resources. To keep up, organizations need well-defined processes that can consistently combat persistent security risks and attacks.
- ☐ **Does every security analyst know what to do if there's an attack?**
  When an attack happens, you know it's all hands on deck. With a standard response process, even junior analysts can respond to an attack just as well as a senior analyst with lots of experience.
- ☐ **Do you have automations in place for analysis and remediation without human intervention?**
  A critical component of digital resilience is the ability to recover from an attack. SOAR playbooks should be in place to get you back to a good, known operational state — as quickly as possible.
- ☐ **Are you able to manage data storage costs without sacrificing usability?**
  The future is federated. While many organizations are choosing to reduce costs through cheap storage solutions, that can cause an issue accessing data on demand for compliance audits or threat hunting.

Fannie Mae®

Fannie Mae's complex hybrid architecture meant the company had to use separate platforms to monitor and secure its digital systems, so teams spent a lot of time analyzing and sharing data across functions. Now with Splunk, Fannie Mae has a single platform to monitor and analyze data across its ecosystem, so teams can be more efficient as they keep the company — and the housing finance system — secure and resilient.

More efficiencies due to unified monitoring capabilities, increased MTTR and ability to comply with regulatory mandates.

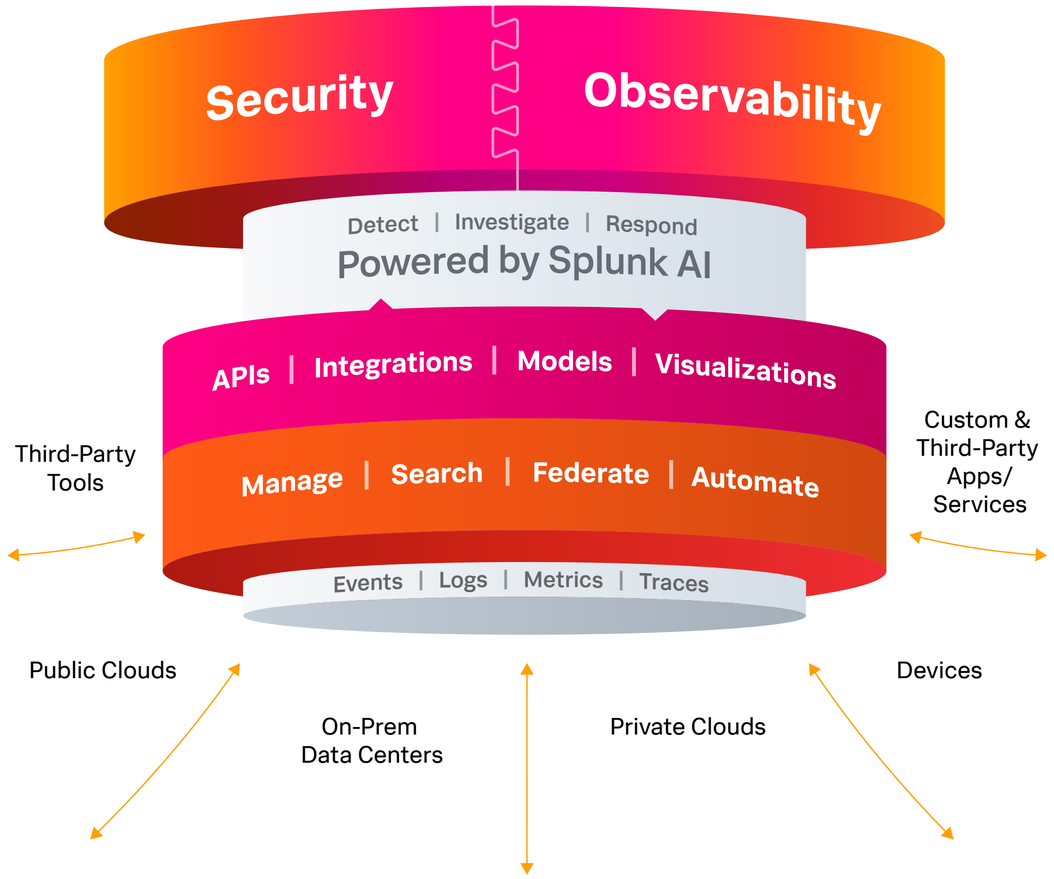
Using Splunk, we now have a greater view of our ecosystem to help ensure that each transaction that goes through Fannie Mae can be traced and monitored from start to finish.

— Nimesh Bernard, Senior Director, Enterprise Observability Applications, Fannie Mae

A unified approach to digital resilience

With Splunk's Unified Security and Observability Platform, security, ITOps and engineering teams have comprehensive visibility across the hybrid and edge technology landscape, as well as powerful tools for investigation and response, at scale, with the added benefit of one journey reinforcing and even accelerating the other.

You've seen how Splunk strengthens security across use cases. By using Splunk for both security and observability, teams gain a shared view of data with a common search language and tooling, simplifying cross-team collaboration to drive greater digital resilience across your organization.



Search, analysis and visualization for actionable insights from all of your data, from edge to cloud.

Start Your Free Trial.

Keep the conversation going with Splunk.

splunk>

24.CMP.ebook.path-to-resilience-building-a-modern-security-program_v6