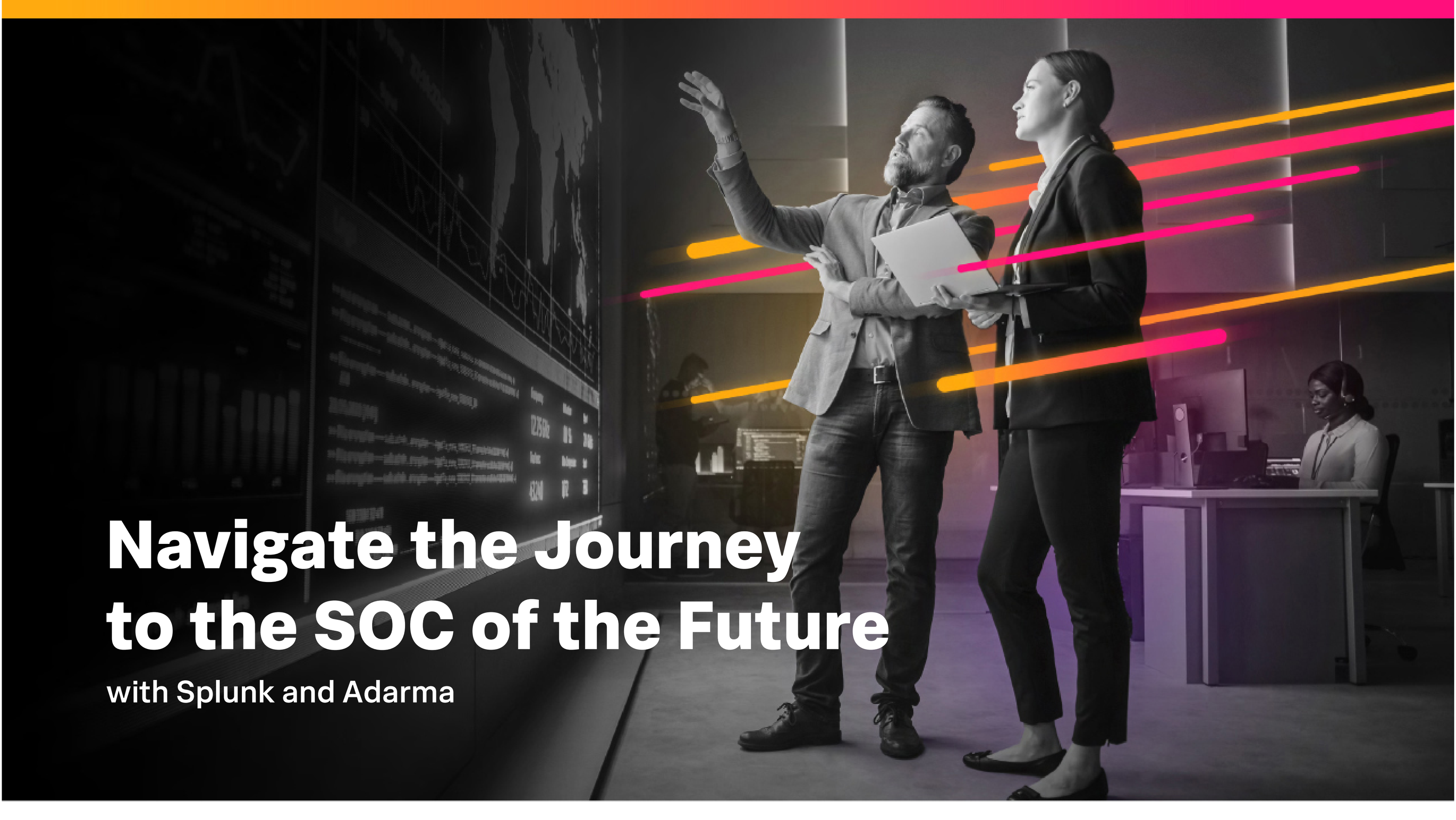
SECURITY



Navigate the Journey to the SOC of the Future

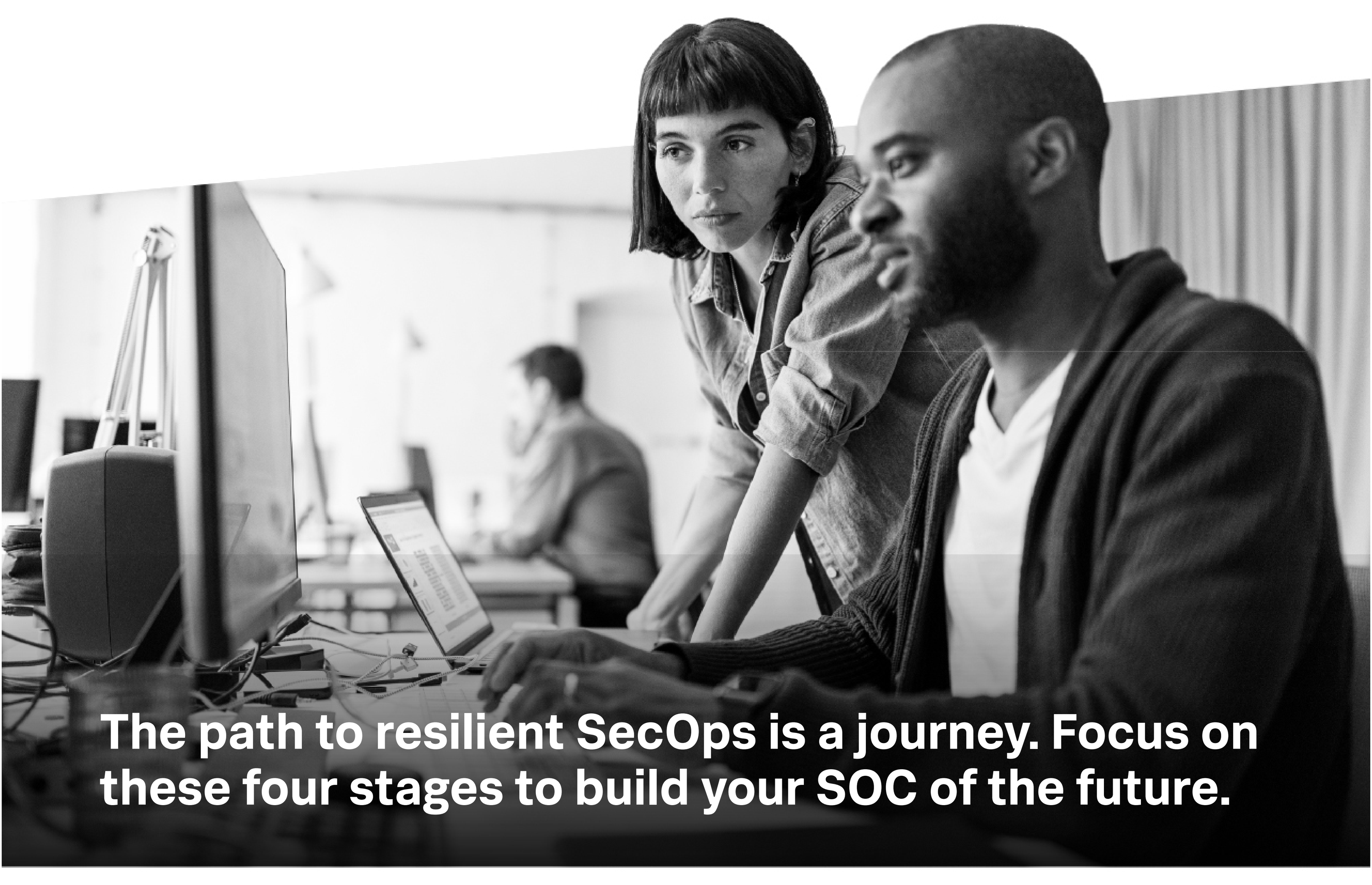
with Splunk and Adarma

90% of security leaders say digital resilience factors into security operations (SecOps) strategies more now than just 12 months ago[1]

That's why global security leaders are racing to modernize their security operations center (SOC) to:

- Detect threats at scale
- Unify security operations
- Empower security innovation

> **Security risk is business risk, and boards are realizing it.**
>
> **Mick Baccio,**
> Global Security Advisor, SURGe



The path to resilient SecOps is a journey. Focus on these four stages to build your SOC of the future.

1 Visibility is the foundation of the SOC of the future

Security teams want visibility across environments to detect and respond to threats at the scale and complexity of the modern enterprise.

Adarma and the Splunk platform can help you build a centralized home for structured and unstructured data that paves the way for more accurate and timely threat detection. With greater visibility, you can:

Eliminate blind spots

Gain end-to-end visibility across your entire environment, whether on-premises, hybrid, or multicloud.

Enable security monitoring

Analyze a continuous stream of near-real-time data for threats and other potential security issues.

79% of businesses report visibility gaps in their cloud infrastructure

75% report visibility gaps in their end-user devices

> **In light of increasingly stringent penalties for violating regulations, security professionals around the globe need to break down silos and boost visibility to respond to threats faster than ever before. Much faster.**
>
> **Splunk Security Predictions**

2 Gain insights to better prioritize and investigate threats at scale

SOCs are overwhelmed with alerts that dilute focus, including false positives. Risk-based alerting (RBA) points your team to what matters — reducing alert fatigue and wasted time.

Reduce alert volume

RBA users see anywhere from a 50% to 90% reduction in alerts.[2]

Improve speed

Splunk customers are 90% faster at identifying the root cause of threats and determining appropriate remediation than with previous solutions.[3]

Gain needed context

A recent survey found that a lack of context was the number one barrier to SOC success.[4]

RBA helps to improve alert fidelity and reduces alert volumes, allowing analysts to prioritize their investigations based on risk.

- **Prioritized by attributing risk to users and systems**
- **Mapped to cybersecurity frameworks**
- **Triggered when risks exceed set thresholds**

The SOC of the future needs to detect and investigate at scale in a way that is both holistic and prioritized. Let Adarma and Splunk get you there with RBA, anomaly detection, threat hunting, and integrated threat intel to stay ahead of the latest attacks.

3 Force multiply the efficiency and productivity of your team with automated response

Under-staffed SOCs manage more than 25 siloed tools.[5] The process leads to slower response times and wasted analyst cycles. At the same time, security teams that are bogged down with manual analysis and large alert volumes don't have the bandwidth to catch up with threat actors that are continuously adapting.

RBA is a great first step toward prioritizing alerts and providing analysts with valuable context for more efficient threat detection, investigation, and response (TDIR), but it's just the start. Adding automation through workflows or playbooks allows organizations to respond to threats more quickly and effectively, and free up your SOC team to better prepare for what's next.

Automated containment and response actions

41% of potentially beneficial alerts are overlooked due to limited SOC resources.

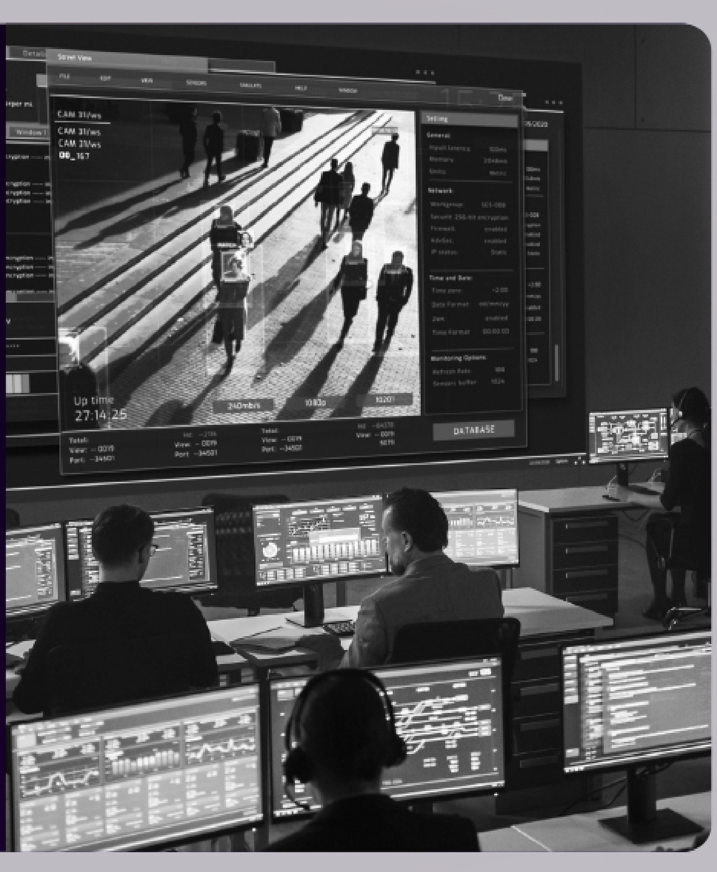
Orchestrated response workflows

Security analysts spend an average of 3 hours on each investigation.

315+ third-party app integrations power Splunk's automation use cases

2,800+ automated actions streamline complex workflows across various teams and tools

> **The idea that humans are going to keep up with the speed of cyber events is ludicrous. We can't keep up; it's impossible. There will be jobs in security that migrate or are heavily supplemented by AI tools. That said, IT and communications systems will continue to drive the need for more analysts and operators to support and defend evolving applications of AI.**
>
> **Paul Kurtz,**
> Chief Cybersecurity Advisor and Field CTO, Splunk



4 Maximize efficiency with seamless collaboration

How well you can coordinate workflows and build well-defined automated processes that can consistently combat persistent security threats will determine how well your company can shift to more proactive security.

To work faster and smarter, automate the complete TDIR life cycle.

With Splunk and Adarma, SOCs can achieve seamless, automated workflows from a single, unified workbench that stitches together and standardizes TDIR processes for better efficiency and accuracy.

80% faster investigation and remediation of security incidents

90% reduction in MTTD and MTTR

84% of organizations claim improving the efficacy and efficiency of their security operations is among their top 5 technology priorities[6]

Wherever you're at in your digital resilience journey, Adarma and Splunk can get you to the SOC of the future.

[1] ESG, *SOC Market Trends Report.*
[2] Splunk, *The Essential Guide to Risk Based Alerting.*
[3] ESG, *Analyzing the Economic Benefits of Splunk.*
[4] SANS, *2023 SOC Survey.*
[5] ESG, *SOC Market Trends Report.*
[6] ESG, *Analyzing the Economic Benefits of Splunk.*

Learn more: www.splunk.com

Learn more: https://adarma.com/