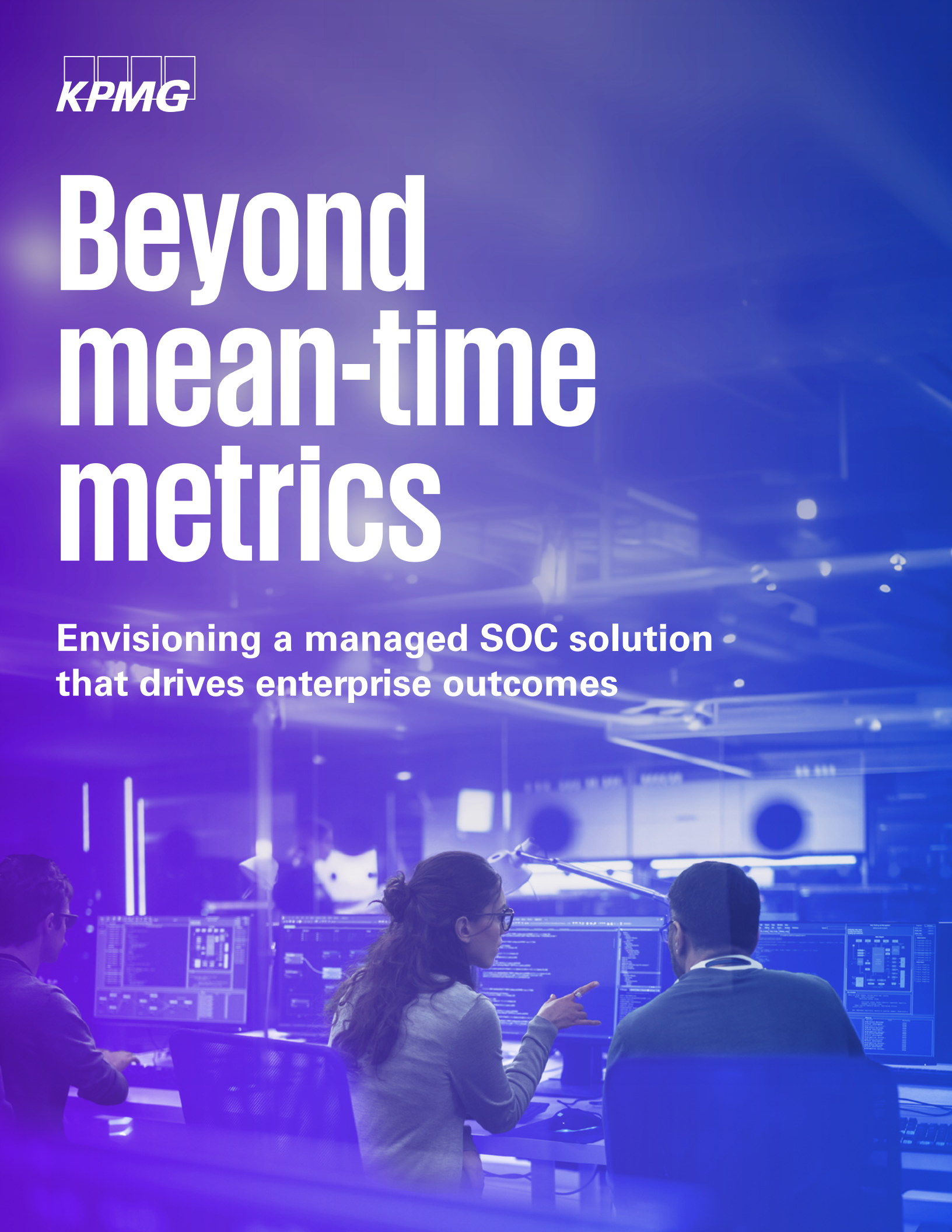
KPMG

Beyond mean-time metrics

Envisioning a managed SOC solution that drives enterprise outcomes



SOCs as strategic enablers

New technology means new attack surfaces—across mobile devices, remote work environments, the public cloud, generative AI models, and more. As a result, many security operations centers (SOCs) are aggressively buying instruments for threat monitoring and combining them in a single pane of glass.

But this patchwork of point solutions can be noisy, expensive and hard to integrate, especially when there's a shortage of skilled practitioners to manage the tools and follow the data path of an adversary.

Without cohesive monitoring, a modern-day threat actor could traverse numerous technologies on your network, exploiting credentials along the way and even threatening the crown jewels.

Most SOCs are so busy fighting fires with point solutions that they struggle to create a proactive, strategic security approach that advances enterprise priorities—such as operational resilience, stakeholder trust, speed to market, or cost reduction. Instead, they're often too focused on metrics like mean time to detection (MTTD) and mean time to response (MTTR).

Looking beyond these short-term measures, forward-thinking CISOs are widening their aperture to improve their return on investment. What is the SOC's role in the growth strategy? How can security teams reduce the company's risk while also giving it confidence to move faster, open up new customer channels, and boldly seize opportunities?

Top 7 security concerns related to cloud technologies

01 Malware moving laterally to cloud workloads

02 Attacks resulting in data loss due to insecure use of APIs

03 Unauthorized access by a third party

04 'Zero Day' exploits of unknown vulnerabilities

05 Misuse of privileged accounts, secrets, or access keys via stolen credentials

06 Targeted penetration attacks

07 Compromise of a cloud service, workload, security group and/or privileged account

Source: 2023 KPMG Cloud Transformation Survey

Future security: from manual firefighting to machine scale

Given the increasing velocity and sophistication of threats—plus companies' need to pivot quickly amid constant change—cyber teams must work at machine speed. This is how SOCs will take their security posture from purely reactive to proactive, adaptive, and aligned to growth objectives.

To create that posture—while continuing to evolve it as needs change—leading SOCs of the future will collaborate with managed services providers in a shared responsibility model. Some have already started down this path.

Focusing on outcomes

In a shared responsibility model for ongoing detection and response, providers will deploy advanced automation at scale, unifying disparate point solutions in a central operational pane while bringing skilled cyber practitioners to "copilot" the technology. In this way, even though the number of data points continues to increase, the SOC will use fewer tools to correlate them and identify threats.

Unlike many managed detection and response (MDR) deals of today, the shared responsibility model of tomorrow will have an outcomes focus as a defining characteristic. That means tracking the right metrics, and one that's growing in importance is dwell time—or how long an adversary is in an environment before they are eradicated. After all, the less time a bad actor is present, the less damage they can do.

Tracking this single measure is a way to show a long-term return on security investments, demonstrating that the SOC can find adversaries and remove them, while protecting critical assets. To do that successfully, SOCs must move at machine speed with automated techniques—whether it's forcing a restart, updating an antivirus signature, adding URLs to the firewall, or dropping a user to a VLAN—until an issue is resolved.

By using a service provider's technology and expertise, SOCs can potentially remove a threat in seconds instead of days or weeks.

Reduced dwell time—as part of an overall improved security posture—can drive meaningful enterprise outcomes.

Engagement models

Shared responsibility comes in different flavors, with services ranging from 8x5 support—through 24x7 monitoring—to L1-L3 tiers of SOC analysts.

Models can include:

Endpoint detection and response (EDR).
Providers monitor and respond to suspicious behavior and threats such as malware and ransomware—but only for end-user devices.

Managed security service providers (MSSPs).
These firms monitor endpoints, other devices and systems, but they typically do not provide response. Instead, they report concerns to clients, who determine what actions to take.

Managed detection and response (MDR).
In this subscription-based model, providers combine proactive threat hunters, security analysts, incident responders and advanced automation to quickly identify, contain and respond to cyber threats—not just for endpoints but for the entire IT environment. Services can range from limited SOC support to a full outsource of detection and response activities—as well as hybrid options in between.

Extended detection and response (XDR).
Some players are beginning to use this phrase to emphasize benefits like actionable threat intelligence, board-level reporting, and reduced alert noise. But this is more of a marketing STRATEGY than differentiated delivery, because these capabilities are already offered by leading MDR providers.

Identity threat detection and response (ITDR).
In another marketing play, some providers are promoting this capability—essentially monitoring the active directory for potential breaches—as a specific use case within MDR.

For example, one healthcare provider, after learning about a data breach, minimized dwell time through advanced threat detection and response.

As a result, the company **protected sensitive patient data, preserved its reputation**, and **earned the trust of regulators and consumers**.

In another example, an e-commerce retailer is reducing dwell time through continuous monitoring, vulnerability scanning, and real-time incident response. In addition to preventing serious data breaches, the company is seeing **increased sales and loyalty** by demonstrating its commitment to customer data protection.

Leading managed services providers also align their day-to-day activities to enterprise priorities, and one way is by using cyber data as a strategic asset. For example, when one U.S.-based company received a large number of firewall alerts in a short amount of time, their MDR provider discovered that the abnormal web traffic was coming from the location of a festival in Canada. The company is now using this insight in its marketing activities—by developing targeted campaigns to capitalize on this festival traffic.

In addition, the leading MDR providers of the future will help ensure that ongoing security monitoring and analytics are built into development processes.

That translates to an ability for organizations to **deploy applications quickly and confidently**—whether it's a new customer-facing mobile app or an online tool for real-time collaboration—so they can run bravely to new opportunities.

Evaluating needs and choosing a provider

A focus on enterprise outcomes—along with a quality assurance function for tracking them—is one of the most important capabilities to seek from a service provider in a shared responsibility model. Also consider these other critical factors:

Building a new operating model

The future of detection and response is about creating an enterprise capability, not a collection of point solutions. That means providers must go beyond gathering information and developing baselines.

To deploy cohesive automation at scale, look for providers who not only have the advanced technology, but also the maturity and expertise to thoroughly assess your environment, determine the rules to be applied, and investigate anomalies.

In addition, keep in mind that while providers are marketing a lot of new security tools using artificial intelligence (AI) and machine learning (ML), there's often a difference between what's promoted and what's delivered. It takes tremendous effort and very large data sets to train AI and ML to work effectively, lest your alert systems become riddled with false positives. Make sure your provider isn't hiding behind the hype.

Importantly, setting up a shared responsibility model is not a one-time engagement. To operate at machine speed and create a proactive security posture, your provider must apply continual attention—with ongoing adjustments based on changes in the threat intelligence.

Transparency and collaboration

In shared responsibility, your provider cannot operate in a black box. Instead, parties must work together. For example, if the service provider's L2 analyst flags a suspicious file, they should notify you to review it so you can identify it as, say, a new driver for laptop webcams.

But keep in mind that you, as the client, shouldn't operate in a black box either. For instance, if your company has an upcoming marketing initiative that could increase cyber risk—such as a potentially controversial social media event—your service provider needs to know about that so teams can take preventive action, such as setting a high-risk alert for the social media accounts of key executives.

Similarly, if there's an upcoming merger, acquisition or divestiture, your legal department will have a shared responsibility to notify the security team, so they can help prevent leaks that could kill the deal—or the stock price. These actions could include close monitoring of emails about intellectual property or setting alerts for data loss prevention.

Cyber domain expertise—plus advisory capabilities

As you visualize a SOC that can keep up with rapid change, consider whether you have enough in-house resources with sufficient cyber IQ. For example, in addition to having the right credentials, the best practitioners should be curious about threats, exploring those with the highest potential impact versus analyzing low-level events that cause alert fatigue.

Moreover, in a constantly shifting market, cyber IQ alone will not be enough. Leading providers will also bring business expertise and advisory capabilities—in specific industries, processes, and data and analytics. It's these kinds of activities that further align your SOC to strategic outcomes, beyond operational outputs.

Take data privacy, for example. In addition to considering a provider's threat monitoring, consider their expertise in data privacy governance and reporting. This kind of work can measurably improve stakeholder trust—for customers, employees, regulators and others—which is a growing imperative in environmental, social and governance (ESG) strategy.

Scope of services

Based on the expertise and overall maturity of your SOC, consider the kind of support you need from a provider (see engagement models on page 3)—and how that support will be delivered. For example, which technologies and capabilities are in the provider's portfolio? Is the provider focused on plans that are mainly conceptual, such as "zero trust," without concrete tactics? Or are the plans actionable, based on industry-accepted frameworks such as MITRE?

As you evaluate providers, also evaluate their solvency and stability, including the risk of potential merger or acquisition. An illustration of this point: In 2019, buyers of Symantec's cybersecurity services learned unexpectedly that Broadcom had acquired the company and, a few months later, would sell off most of the cybersecurity business—including the customer relationships—to another provider. That created significant risks in continuity and reliability for these buyers.

Another consideration in the scope of services is insights. Look for providers who deliver not only detection and response but also intel on emerging threats and actors, such as supply chain compromises in certain parts of the world that could affect your business. As strategic collaborators, leading providers give you foresight for enterprise risk management.

Data sovereignty

What are your data requirements for regulatory compliance? In managed detection and response, where will your data go and what will the provider do with it? These are critical questions to consider in shared responsibility, as many providers must take possession of your data to perform their monitoring service.

The most advanced providers, on the other hand, deliver services while keeping your data where it is. That means if you have data in a particular jurisdiction, such as London or Frankfurt, it will stay there—with no need for the provider to move it to their offices in another country for monitoring.

Named team members

How will you communicate with your service provider? In standard managed services relationships, if your staff has a concern and contacts the service provider, they generally will talk to "the next analyst available"—whoever happens to be looking at the monitoring screen at the time.

But for an effective shared responsibility model, it's important to choose a provider who assigns named analysts to your account. That means, no matter what time of day your staff contacts the provider, they will work with the same knowledgeable, responsive team members who understand your business. This is the kind of collaboration that delivers sustained results.

Eyes on the future

Is your SOC aligned to evolving technology? Evolving threats? Evolving business priorities?

In the new world, CISOs must move beyond a nearsighted focus on security and compliance to also address the bigger picture of business risks and opportunities. That means visualizing a SOC that works at machine scale to drive not only security outcomes but also enterprise outcomes—such as the operational resilience and stakeholder trust that enable the business to boldly advance its growth agenda.

To pave the way, progressive CISOs are leveraging the detection and response capabilities of leading managed services providers.

In a shared responsibility model, these providers bring advanced technology and collaborative professionals, working in harmony to help you define the vision for your SOC, implement it, and continue pivoting as needs change.

That's how tomorrow's frontrunners will gain and sustain advantage in security operations.

About KPMG Managed Services

Business transformation is the path to sustained advantage. But transformation is not a fixed destination; it's an ongoing journey. How can you continually evolve your business functions to keep up with ever-changing targets? KPMG Managed Services can help.

We combine advanced technology with business and technical expertise to handle knowledge-intensive processes across your enterprise—on a subscription, as-a-service basis. We aim to cut your total cost of operations by 15 to 45 percent, in addition to driving outcomes like resilience, customer and employee retention, stakeholder trust, and competitive advantage.

Drawing from our renowned knowledge across functions, processes and industries—plus smart analytics, data governance and change management—KPMG Managed Services is tech-enabled but strategy-led. We help you operationalize your growth ambition, so you can accelerate your transformation journey while minimizing disruption and risk.

Learn more about KPMG Managed Services for cybersecurity.

Learn about other parts of the KPMG Managed Services portfolio.

Contact us

Rajesh Ahuja, CISSP
Managing Director, KPMG LLP
Cyber Managed Services
rajeshahuja@kpmg.com

Evan Rowell
Director, KPMG LLP
Cyber Managed Services
erowell@kpmg.com

Antonio Manelli
Lead Specialist, KPMG LLP
Cyber Managed Services
amanelli@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia