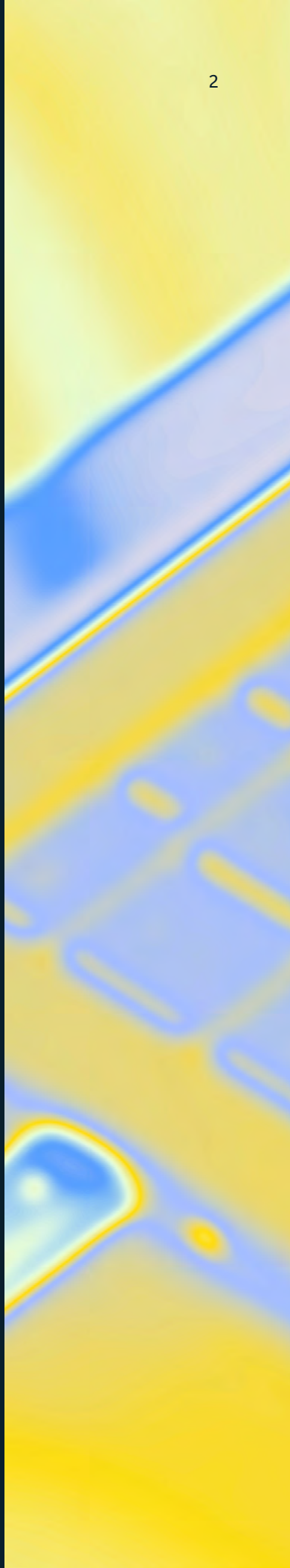
Microsoft Security

AI-Powered and Human-Driven

The Future of SecOps

Table of contents



Introduction

The role of AI in the SOC: Amplifying human capabilities, not replacing them

Cybersecurity defense operates on an uneven playing field: The organization must be protected against every possible attack angle, while attackers need to find just one way in. It's an asymmetrical battle that can't be ignored.

Armed with the latest technology, like generative AI, and spurred on by a $9.5 trillion cybercrime economy in 2024,[1] attackers are innovating faster than ever. Our teams have observed AI being used to craft hyper-personalized social engineering campaigns, create malicious scripts and payload development, and research organizational vulnerabilities. We've even seen AI embedded in malware that helps tailor the malware based on the device configuration after delivery.

Traditional tools and point solutions simply don't provide security teams with the tools and visibility they need to protect against these types of attacks. Security operations centers (SOCs) are buried in alerts while blind spots multiply.

SecOps: Current state

Current tools are either generating too many alerts or too few, allowing attackers to move undetected. Correlation requires hard-earned expertise that is becoming increasingly scarce, as burnout and environment complexity take their toll on the defender. Engineers are busy managing custom integrations or constantly updating complex manual playbooks. Threat hunters and forensic analysts are juggling portals and numerous data tables, painstakingly trying to find the right data.

> It's a familiar story for security teams—more threats to catch, more gaps to fill, and rarely enough resources to do either effectively.

Compounding these challenges is the fact that on average, SOC team members spend one-third of their typical workday investigating or validating incidents that are not a real threat (32%).[2] Simply put, SOC teams spend too much of their time filling in the gaps left by their traditional tools—and attackers are taking advantage.

The future of the SOC

Fortunately, recent innovations in AI, hyperscale cloud infrastructure, and the platformization of security tools will shift the strategic balance, enabling defenders to engage with the threat landscape through new solutions and methodologies.

Engineering will become easier when everything is on a single platform using a unified data lake. Less time will be spent managing integrations, and more time can be put into new detections and optimizing. Analysts and threat hunters will have greater context and streamlined workflows for threat identification and response. Data and many core protection capabilities will be available to non-SecOps teams, who will work more closely with security to better manage endpoints, identities, data, and more.

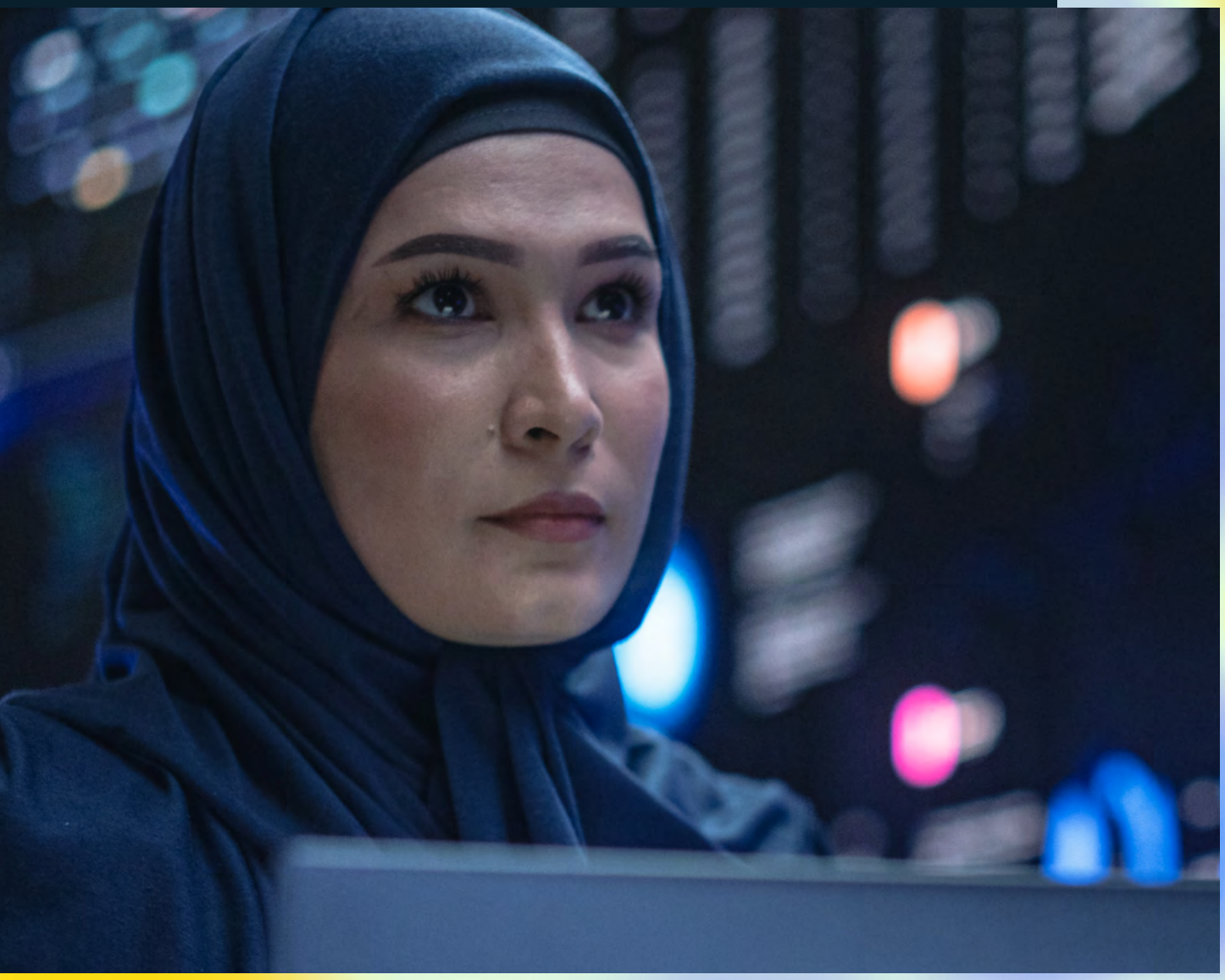
> The SOC of the future will be defined by how security teams shift their reactive posture to a proactive focus on emerging threats.

In the following pages, we'll outline Microsoft's projections for the future of the SOC, based on our own frontline observations and the development of new security technologies. Our forecasting shows that AI-powered security tools aren't aspiring to replace human expertise with automation. Instead, they will play a key role in amplifying human strengths.

The most successful SOC teams won't be the ones that automate the most—they'll be the ones that empower analysts most effectively.

Chapter 1

AI-powered. Human-driven.



The SOC of the future will fundamentally break down the silos that exist today due to the limitations of legacy tools and processes, and the team structures they require. This will be done through a unified cybersecurity platform that enhances the tools and capabilities used across prevention, protection, detection, investigation, and response.

This signals a new era for security operations. It's one where AI and automation play significant roles in day-to-day SOC operations.

Which isn't to say that this next era will be defined by the "autonomous SOC." We don't believe there's a future where security is fully autonomous.

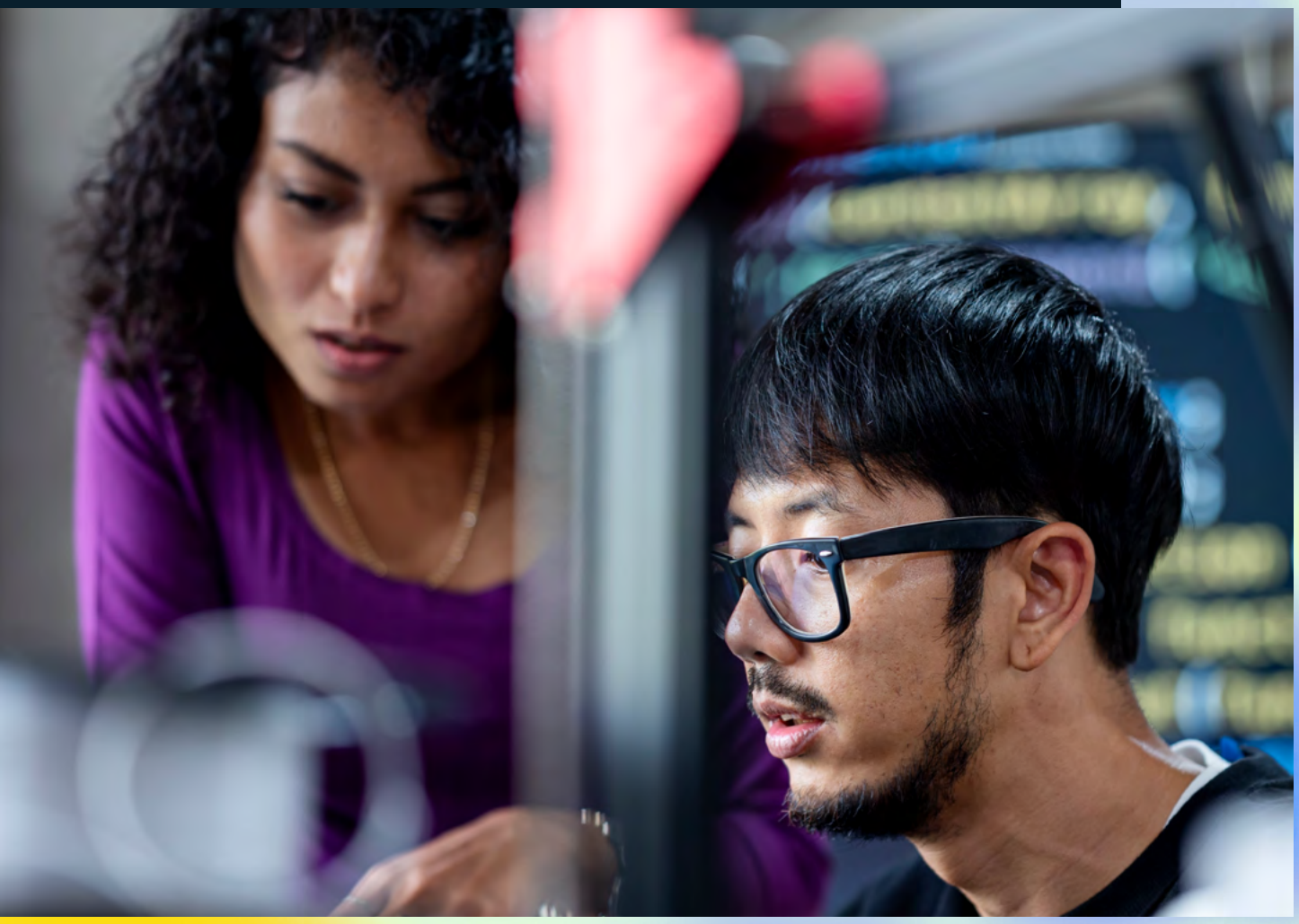
> Attackers will always be able to outsmart AI, as they don't have to play by the same rules that govern AI and other software programming.

Instead, AI will power services that assist analysts, engineers, and hunters, and in some cases, automate tasks. But fundamentally, the strengths of AI tools will be used to augment the SOC team: by reasoning over huge data sets, uncovering patterns and anomalies, and coordinating with services. In these ways, AI enables security teams to do their jobs better—on the people side, the process side, and the technology side.

We've identified five key ways that AI-powered solutions will help address the security gaps currently filled by humans, allowing defenders to shift the focus of their roles from task based to outcome oriented. Let's dive in.

Chapter 2

Five critical AI-powered transformations shaping the future of the SOC



The evolution of security operations will be shaped by fundamental shifts in how teams operate, collaborate, and measure success. These transformations aren't just about adopting new technologies—they will significantly change how security teams work, and where they deliver the most value.

Each transformation builds upon another, creating a new foundation for security operations. One that's more adaptable, more effective, and more attuned to human potential.

Transformation 1

Replacing tool sprawl with a unified platform

The era of disconnected security tools will end by necessity. Organizations will move from managing dozens of point solutions to a cybersecurity platform that unifies all security data, processes, and people. Data onboarding will be cost effective and easy with a unified security data lake, shifting the focus from "What data should I bring in?" to "What can I do with it?"

Advanced analytics will be applied to build a relational model of all your assets, activity, and threat intel, giving your defenders a reliable and comprehensive map of the organization. This new foundation for the SOC team will expose patterns and threats that remain invisible in siloed systems. Connections that were impossible to make across disconnected tools become clear, providing new insight into potential threats.

As platforms evolve, automation becomes truly intelligent. Moving beyond simple rule-based responses, security automation now adapts to changing conditions and emerging threats, learning and improving with each interaction.

Future state:

Security teams shift focus from managing multiple disconnected tools to platform strategy and optimization. This evolution in human oversight leads to more strategic security operations and better security outcomes.

Transformation 2

Reducing threats with autonomous hardening and protection

With a relational graph of the digital environment, AI will be used—along with real-time adaptive threat intel—to build a clear understanding of where vulnerabilities exist, the baseline behavior of entities, and to see where defenses are being tested. This insight will then be used to coordinate preventive actions across different domains and layers based on proven best practices.

This will enable the system to dramatically reduce the exposure of your attack surface, effectively addressing your basic block-and-tackle efforts, 24/7, based on the latest threat intel. As 99% of successful attacks are preventable with basic security hygiene,[3] automated hardening holds the biggest potential impact for your SOC team.

Because we know that breaches are never going to be 100% preventable, and that attackers are using AI and cloud infrastructure to increase the speed of their attacks, it's imperative that your environment has adaptive, real-time protection that adapts to attackers as they work to evade defenses.

The platform will utilize self-defense based on adaptive playbooks, always up to date with the latest threat intel and response actions, to predict an attacker's path and then automatically take action to contain them by isolating affected devices and compromised credentials—dramatically limiting the blast radius of successful breaches.

Future state:

System immunity will substantially reduce the blast radius and impact of successful breaches. Attackers will be less successful since their paths for lateral movement are automatically blocked. The SOC team can then focus on fully remediating the attacker and remove their access.

Transformation 3

Defending from an attacker's perspective

SecOps defenders will shift from their siloed purview of the digital environment—often viewed through huge lists of vulnerabilities, alerts, or assets—to viewing a map of their environment that demonstrates how assets are configured and relate to each other.

Attack path modeling will then leverage AI and threat intel—like tactics, techniques, and procedures (TTPs)—to predict how an attacker could exploit vulnerability and move laterally across the digital environment.

By visualizing their own security environment as an attacker sees it, teams will uncover vulnerable paths and critical chokepoints that traditional alert monitoring might miss. AI-powered tools help construct these relationship maps in real time, connecting seemingly disparate elements to expose potential attack routes before they're exploited.

This further enables the shift from reactive defense to proactive prevention. Teams identify and close security gaps by understanding how different vulnerabilities, misconfigurations, and access patterns could combine to create breach opportunities.

Future state:

Security teams operate with an attacker's mindset, but a defender's knowledge base. By understanding and visualizing potential attack paths, they can prevent breaches before they occur rather than detecting them after the fact.

These paths will then be used to implement autonomous hardening to automatically patch systems, update configurations, and deploy security controls to proactively improve security posture. This will reduce the number of open attack paths automatically.

Transformation 4

From alert triage to emerging threat focus

The daily grind of alert management is being transformed. Agentic assistance can manage and correlate routine alerts, dramatically reducing the current time spent on triage. Alert fatigue, a longstanding critical challenge for security teams, becomes manageable.

This shift enables proactive threat hunting to become a primary function. Security teams move from reactive response and endless triage to proactive threat detection and investigation. Human analysts, freed from burning down lists of alerts to close false positives, can apply their expertise where it matters most: identifying and countering previously unseen attack patterns.

Novel attack detection improves as teams gain the time and space to develop advanced threat-hunting capabilities. Instead of being consumed by routine alerts, analysts can focus on understanding and anticipating new attack methodologies.

Future state:

Prevention replaces reaction as the dominant security paradigm. Teams identify and close security gaps before attackers can exploit them, fundamentally changing the dynamics of enterprise security.

Transformation 5

From analyst tiers to fluid teams

The traditional SOC structure, with its tiers of analysts handling progressively more complex tasks, will dissolve for many organizations. As unified platforms and AI tools transform security operations, a more dynamic model will emerge: Every team member can now contribute to investigating advanced threats. We will also see a significant shift toward proactively tracking, hardening against, and responding to emerging threats.

With most of the security blocking and tackling taken care of automatically, the total alert volumes that need to be assessed by the SOC team will be significantly lower. Rather than working as part of an alert-processing assembly line, analysts become more like engineers, programming and fine-tuning automated systems while ensuring quality control of processes and outcomes.

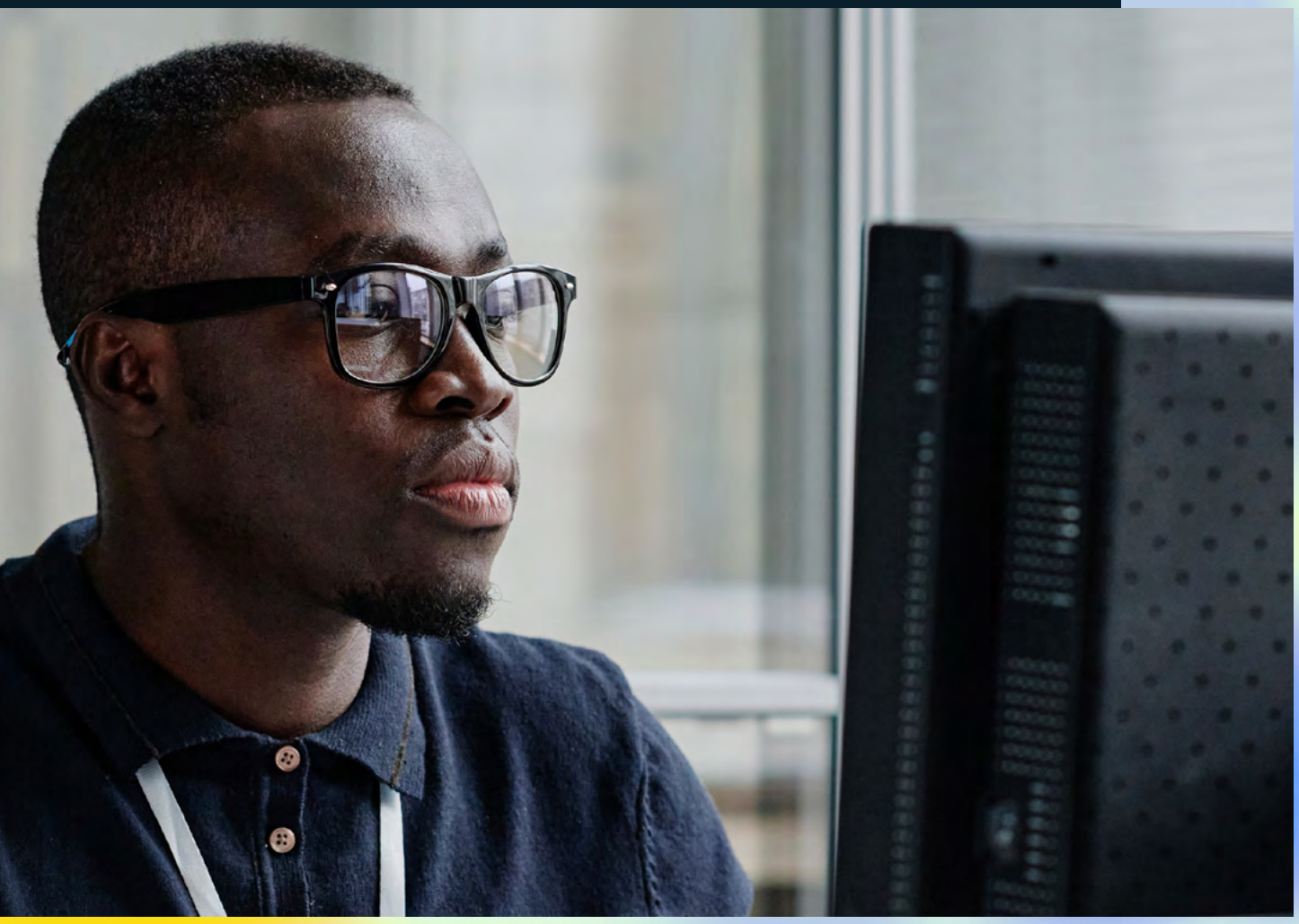
This new reality will also help evolve career progression. Instead of a linear path "up the tiers," security professionals develop expertise across multiple domains, deepening their knowledge over time. With AI-enhanced learning and decision support, security professionals develop broader, more adaptable skillsets, faster.

Future state:

Security teams freed from traditional hierarchical constraints respond faster and more effectively to complex threats. While AI manages routine operations, security professionals focus on higher-value activities that demand human insight and expertise.

Chapter 3

The augmented SOC: Maximizing human and machine intelligence



Semi-autonomous security will be the new standard in security operations. But human-empowered operations continue to drive success in this new paradigm.

Rather than forcing security teams to adapt to rigid technological constraints, AI systems will adapt to human workflows and decision-making processes. Technology serves the security team's needs, enhancing their capabilities without disrupting their essential work patterns.

Trust builds through transparency in this arrangement. AI systems provide clear reasoning for their recommendations, allowing security teams to validate and improve automated decisions. This transparency creates a feedback loop where both human expertise and AI capabilities continuously improve.

> Security professionals grow their expertise through hands-on experience with emerging threats, while AI-enhanced learning tools support their development and decision-making.

This balanced approach ensures that security teams maintain and enhance their skills even as automation increases. By focusing human attention on complex challenges while providing AI support for learning and decision-making, organizations create an environment where humans can thrive, even while AI tools continue to evolve.

Chapter 4

Navigating the transition to tomorrow's SOC

The transformation of security operations is happening—but success isn't guaranteed.

The organizations that thrive will be those that approach this evolution strategically, focusing on three critical areas:

Timing and sequence

Rather than attempting wholesale transformation, successful organizations identify which security functions benefit most from immediate AI integration, and which require more measured transition. This staged approach allows teams to build confidence, demonstrate value, and refine their implementation strategy.

Data readiness

AI's effectiveness depends entirely on the quality and accessibility of security data. Organizations must assess and optimize their data infrastructure, ensuring it can support increasingly sophisticated AI applications while maintaining security and compliance requirements.

Cross-functional alignment

Security transformation impacts every aspect of the organization—from IT operations to business strategy. Success requires early and ongoing collaboration across departments, ensuring security evolution aligns with broader business objectives and capabilities.

The future of security operations is a journey of continuous adaptation. Organizations that embrace this reality, while thoughtfully managing their transformation, will be best positioned to defend against tomorrow's threats.

Conclusion

The next chapter: Human insights, amplified

The imperative for transformation is clear and immediate. Threat actors are already wielding AI to enhance their capabilities, while security teams struggle with increasing alert volumes and complexity. Organizations can't afford to wait and see how AI reshapes security operations. They must actively participate in defining that future.

Microsoft's vision for security operations emphasizes human expertise amplified through AI capabilities. By focusing on augmenting rather than replacing human expertise, organizations can build security operations that are both more efficient and more effective—ready to meet not just today's challenges, but tomorrow's threats.

Explore Microsoft's approach to AI-enhanced security operations:

Discover the AI-powered security operations platform

Explore Microsoft Security Copilot

[1] "Cybercrime To Cost The World $9.5 trillion USD Annually In 2024," *Cybercrime Magazine*, October 2023

[2] "Global Security Operations Center Study Results," Morning Consult and IBM, March 2023

[3] "Microsoft Digital Defense Report," Microsoft, Inc., October 2023