Microsoft Security

The Path to AI

Pave the way for powerful cybersecurity AI with integrated XDR and SIEM

E-book

Contents

Chapter_01

This is a pivotal moment in cybersecurity

This is a pivotal moment in cybersecurity

Security operations are about to undergo a seismic shift. And it's a timely one.

Cybersecurity professionals face tough challenges that show no signs of abating. Attacks such as ransomware and business email compromise are becoming more frequent, highly targeted, and difficult to detect, and malicious actors are continually evolving their tactics. Meanwhile, remote and hybrid work continues in full force, causing organizations to move more critical resources to the cloud. People, devices, and apps need to be able to access networks from virtually anywhere, and the many endpoints and identities that result are tempting avenues of attack for cybercriminals. It's an uphill battle that's nearly impossible to win without the right tools.

What makes it even more difficult to defend against such sophisticated adversaries and protect sprawling attack surfaces—typically spanning multiple clouds and platforms—is that security teams are often short-staffed and lack some of the expertise and resources they need detect modern attacks. The dual problems of an unfavorable economic climate and a worldwide cybersecurity talent shortage, with a projected shortfall of 3.5 million positions by 2025,[1] have left many security teams overwhelmed and overworked.

Security leaders need to empower their teams to combat these issues. Thankfully, new tools, innovative applications, and an integrated approach to detection, investigation, response, and protection can help tip the balance in favor of defenders. A critical part of this next generation of tools is powerful generative AI, such as Microsoft Copilot for Security, that is trained to analyze threat signals and make recommendations to security teams in natural language, giving defenders crucial context help with prioritization. It speeds up detection and response, lessening the need for complex workflows and playbooks and empowering even junior analysts to do work that previously required years of expertise.

Generative AI is poised to revolutionize security operations, shrinking the time to respond to threats from hours and days down to minutes.

Many organizations are refining their security stacks to lay the foundation they'll need to use generative AI cybersecurity tools. Integrating extended detection and response (XDR) with a security information and event management (SIEM) system gives organizations the end-to-end visibility and depth of security signal and response that are the cornerstones of that foundation.

This guide will show you how to begin on your path to using generative security AI, including:

- How simplifying your security tools can help security teams combat some of their biggest challenges.
- What efficiencies integrated XDR and SIEM can add to your security operations.
- How taking the step of integrating XDR and SIEM can prepare you for the next step—using generative security AI.

> ***With SIEM and XDR's technologies rolled into one platform, we get a level of visibility that we have never had before.***

Manager of cybersecurity and IT infrastructure, professional services[2]

[1] Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025, Cybersecurity Ventures, 2023.
[2] The Total Economic Impact™ Of Microsoft SIEM And XDR, a commissioned study conducted by Forrester Consulting, August 2022.

Chapter_02

Stack the odds in your favor

> ***"Having multiple security tools from the same vendor has helped us to save detection and response time. We no longer have to go into a bunch of different screens and tools to conduct investigations and respond to threats. The integration is seamless."***
>
> Head of cyber and technology procurement, logistics[6]

Stack the odds in your favor

For organizations to strengthen their security in today's threat landscape, they need to have tools that simplify the complexity of their security team's work in protection, detection, and response across the entire kill chain. It's common for security teams to work with a patchwork of point solutions that have been added to their security stacks to address specific needs at the time without much forward planning—and accumulated over years. It's too complex for security teams to work this way because it forces them to use a plethora of siloed tools with visibility gaps and manually correlate disparate alerts across them, slowing down their investigation and response and causing alert fatigue. This opens the door for attackers.

Without a holistic and consistent view of threats and their digital estates, organizations lack visibility into the entire kill chain and the full scope of an attack, leading to valuable time lost during investigation. Even mature security teams with strong security solutions can struggle to detect sophisticated attacks such as ransomware if their email, endpoint, identity, cloud apps, workload, and data protection solutions aren't efficiently sharing signal, delaying alerts by hours—or even days. And without tools to prioritize alerts, security professionals can become overwhelmed with the challenges they face every day. For example:

- There are an average of 4,000 password attacks per second[3]
- The median time for an attacker to access private data after a successful phishing email attack is only 72 minutes.[4]
- Attackers are increasingly well resourced, and social engineering, ransomware, and AI-enabled fraud are becoming more sophisticated by the day.

Gartner predicts that by 2025, a lack of security staff or human failure will be responsible for over half of cybersecurity incidents.[5] The latest innovations in security aim to reverse that trend by keeping attacks from slipping through the cracks with more comprehensive, guided, and automated solutions.

Integrated XDR and SIEM can give your security operations the visibility, agility, and resilience it needs to combat these common challenges and keep your organization more secure, whatever the future may bring. And in an economic climate that engenders competing budget priorities, streamlining your tools and preparing your systems to support generative cybersecurity AI makes short-term and long-term financial sense.

> Gartner predicts that by 2025, **a lack of security staff or human failure will be responsible for over half of cybersecurity incidents.**[5]

[3] Microsoft Entra expands into Security Service Edge and Azure AD becomes Microsoft Entra ID | Microsoft Security Blog, Joy Chik, July 11, 2023.
[4] Anatomy of a Modern Attack Surface, Microsoft Security, 2023.
[5] Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025, Gartner, February 22, 2023.
[6] The Total Economic Impact™ Of Microsoft SIEM And XDR, a commissioned study conducted by Forrester Consulting, August 2022.

Chapter_03

Create a strong, secure foundation with integrated XDR and SIEM

Create a strong, secure foundation with integrated XDR and SIEM

Unified XDR and SIEM as the foundation of your organization's security strategy can modernize your security operations and keep your organization protected as threats continue to evolve. Having an integrated tool stack gives security operations centers (SOCs) end-to-end visibility into the entire kill chain of an attack, even across multiple clouds and platforms.

While your SIEM enables you to collect, analyze, and hunt for alerts in huge volumes of data from activity across your enterprise, XDR enhances threat data to make it more granular, not just with data from endpoints but from email, identities, apps, cloud workloads, and more. Together, XDR and SIEM give you comprehensive detection, investigation, remediation, and response to attacks across all your identities, endpoints, applications, email, Internet of Things (IoT) devices, and infrastructure, and even multiple clouds.

When security teams have comprehensive visibility plus the efficiency and accuracy of integrated XDR and SIEM, it gives them a critical edge: speed. The richness of available data gives SOCs the accuracy and insights they need to surface attacks and strike back quickly.

The advantages of integrated XDR and SIEM play out across the entire cyberattack chain.

Use automation to perform routine processes.
Triage is streamlined because the system's machine-learning-based detection surfaces the most pressing security alerts, prioritizes incidents, and automatically remediates most threats. Your valuable team members have greater freedom to focus on what's important.

Move from reactive response to automatic attack disruption.
High-confidence signals collected by XDR help identify in-progress attacks early so built-in automation can stop the progress of the attack in real time, isolate affected devices, and suspend compromised users.

Reduce alert fatigue with prioritized incidents.
An integrated XDR and SIEM solution uses machine learning and depth of signal to correlate alerts into incidents, giving analysts a prioritized, more complete, end-to-end view of active threats across the digital landscape that eliminates time-consuming alert correlation and triage.

Maximize available threat intelligence.
An XDR powered by robust, global threat intelligence can help protect you from ever-evolving threats such as ransomware. The more intelligence your security team has access to, the more resilient your organization will be.

Reduce overhead costs.
Consolidating vendors and tools allows you to create a positive ROI quickly, saving money that's better spent on human ingenuity and innovation.

Together, XDR and SIEM provide distinct advantages for organizations. One study revealed that for a composite organization using an integrated solution, the operational and business benefits included:

- Reducing time to investigate threats by 65% and reducing time to respond to threats by 88%.
- Reducing the time to create a new workbook by 90% and the time to on board new security professionals by 91%.
- Reducing the risk of a material breach by 60%.
- Saving almost $1.6 million annually from vendor consolidation.[7]

For organizations seeking to harden their defenses with best-in-class security, make their security operations more efficient, and keep up with the latest security innovations, integrated XDR and SIEM provides a considerable ROI on all fronts. Plus, approaching security tools with a long-term mindset provides the solid foundation organizations need to take the next technological leap: generative AI–powered security tools.

> ***"We've seen about a 90% improvement in our risk of security breach after deploying SIEM and XDR. It's been a game changer for us."***

CTO, government[8]

[7] The Total Economic Impact™ Of Microsoft SIEM And XDR, a commissioned study conducted by Forrester Consulting, August 2022.
[8] The Total Economic Impact™ Of Microsoft SIEM And XDR, a commissioned study conducted by Forrester Consulting, August 2022.

Chapter_04

Amplify your security operations with generative AI

Amplify your security operations with generative AI

OpenAI's ChatGPT4 signified a considerable leap forward in the science of large language modeling, and it has people in many industries considering how big of a role AI can play in streamlining the way they work. Cybersecurity professionals have a more urgent need for simplified workflows than most, and you might be wondering what natural language prompts and deep learning would look like in your own security operations.

Generative AI–powered security tools will shift the paradigm for threat detection and remediation in favor of defenders. Not only will it enable threat detection to evolve from proactive to predictive, but it will also support analysts throughout the entire cyberattack chain with reports and guidance using time-saving natural language prompts.

A foundation of integrated XDR and SIEM is integral to this new technology. It gives security-trained AI the high-quality signals it needs to learn from trillions of pieces of telemetry data and turn them into customized insights and recommendations. It also provides the platform and framework needed to coordinate response actions across security layers.

Microsoft became a pioneer in generative AI cybersecurity when it launched Copilot. Copilot helps security teams outmaneuver attackers and respond to threats in minutes rather than hours or days using intuitive workflows and the ability to submit natural language prompts. When used in combination with XDR and SIEM, Copilot adds exponential gains for security teams.

Supporting and upskilling security talent. Top security strategies and best practices delivered through simple, natural language make advanced remediation techniques available to every member of the security team, from junior to senior.

Detecting patterns and behaviors that are not obvious to the human eye. Copilot uses the end-to-end visibility in your XDR and SIEM solution and applies security-specific skills to huge amounts of data—helping teams surface threats in real time so they can take proactive measures.

Turning huge amounts of data into clear, actionable insights. The security-trained generative AI transforms threat data into insights delivered in natural language, saving teams precious time when every minute counts.

Giving security analysts immediate, critical guidance and context. Security teams can accelerate their investigations with step-by-step guidance and deep context relating to any security event.

Providing streamlined, natural-language workflows. Empowered with technology that can quickly summarize events and automatically recommend corrective actions, teams can focus their efforts to act together quickly and easily prepare reports in a ready-to-share format.

Predicting an attacker's next move. AI constantly applies its learning to the data in your integrated XDR and SIEM and predicts what a malicious actor might do next—so your team can outmaneuver them.

> *Detection is way better with SIEM and XDR. Prevention is never 100%, so I would rather have the best detection in the world than have the best protection without the visibility.*

Manager of cybersecurity and IT infrastructure, professional services[9]

[9] The Total Economic Impact™ Of Microsoft SIEM And XDR, a commissioned study conducted by Forrester Consulting, August 2022.

Chapter_05

Get ready to use Microsoft Copilot for Security

Get ready to use Copilot

Both Microsoft Defender XDR and Microsoft Defender for Cloud are powerful XDR solutions. They work seamlessly with the Microsoft Sentinel cloud-based SIEM solution to provide the unity, efficiency, and broad visibility that your security team needs to keep your organization protected as criminals' tactics continue to evolve. Consolidating tools with Defender and Sentinel is the first step to take on your path to adopting generative AI as a cybersecurity tool.

Copilot is the first generative AI security analysis tool. It magnifies your SOC's ability to keep your data, people, and operations safe in today's digital landscape. The generative AI that Copilot uses is responsibly developed and ready to continuously reason over 65 trillion global threat intelligence signals daily to provide superior threat protection for your organization. It learns from built-in feedback tools to adapt to your organization's preferences and to continuously improve how it works alongside your team.

Attackers now have AI in their hands, and your defenders can too. It's safe to assume that the enormous numbers of threat signals security teams must triage daily will not decrease in the coming years, and that your team will need to combat that challenge with simpler, comprehensive security solutions that work together. End-to-end threat visibility and the ability to ask questions about your security posture and environment in natural language can prepare your operations for long-term resilience against cybercrime.

Explore your deployment options

[SIEM and XDR Solutions | Microsoft Security]

[Copilot | Microsoft Security]