Best practices SIEM and XDR Microsoft Sentinel
5 min read

Unified security operations with Microsoft Sentinel and Microsoft Defender XDR

By Rob Lefferts, Corporate Vice President, Microsoft Threat Protection

January 16, 2024

Security operations

Microsoft Defender

Microsoft Defender XDR

Numerous cybersecurity tools exist to help organizations protect their data, people, and systems. There are different tools that check emails for phishing attempts, secure infrastructure and cloud, and provide generative AI to detect threats and uplevel response beyond human ability. While each of these tools is valuable on its own, each just tells one part of a more comprehensive security story. The most effective approach to safeguarding your organization is to implement a unified security operations center (SOC) platform that combines all these cybersecurity features in one. Microsoft has prioritized efforts to unify these tools and we're now taking the next step in consolidation.

At Microsoft Ignite 2023, we announced that we're bringing Microsoft Sentinel, which delivers intelligent security analytics and threat intelligence, and Microsoft Defender XDR, our extended detection and response (XDR) solution, into a unified security operations platform—providing more comprehensive features, automation, guided experiences, and curated threat intelligence.

- During the session "Microsoft Sentinel: A modern approach to security operations," we explored the SOC capabilities of Microsoft Sentinel, our scalable, cloud-native solution that provides both security information and event management (SIEM) and security orchestration, automation, and response (SOAR).
- And during the session "Unifying XDR + SIEM: A new era in SecOps," we discussed the latest technology around Microsoft's integrated SIEM and XDR solution and how it can protect your environment and protect you from adversaries.
- In both sessions, we shared that Microsoft Security Copilot is an embedded experience in the platform, benefiting organizations with its generative AI capabilities.

But what does it mean to combine multiple cybersecurity tools in one unified security operations platform, and how can it benefit your modern SOC? Throw our generative AI solution Microsoft Security Copilot into the mix and the platform is truly transformative. In this blog post, you'll learn three ways that a unified security platform—like how we combine Microsoft Sentinel, Security Copilot, and Defender XDR—can strengthen your cybersecurity and support your security team in their important work.

Microsoft Sentinel

See and stop cyberthreats across your entire enterprise with intelligent security analytics.

Learn more >

What is a unified SOC platform?

A unified SOC platform is a fully integrated toolset for security teams to prevent, detect, investigate, and respond to threats across their entire environment. For Microsoft, this means delivering the best of SIEM, XDR, posture management, and threat intelligence with advanced generative AI as a single platform. Our objective is to empower security teams to protect more, easily, because we recognize the numerous challenges you face as security teams.

This empowers you to better protect your organization and all its components—including hybrid identities, endpoints, cloud apps, business apps, email and docs, Internet of Things (IoT), network, business applications, operational technology (OT), infrastructure, and cloud workloads—with the capabilities of a unified security platform. And this enables you to protect all that more efficiently. Ours is the only unified security operations platform that delivers full SIEM and XDR capabilities.

1. Unify your insights

A major challenge of a non-unified approach to cybersecurity is that your data is scattered across multiple security tools and logs. This presents a stumbling block when trying to extract insights from data in a timely enough manner to better anticipate cyberthreats and defend against them. Another hurdle of not having a unified solution is that it’s almost impossible to view how a cyberattacker moves across vectors. Since cyberattackers can move laterally, it’s imperative to detect them quickly.[1]

By unifying hunting, incidents, data models, and other threat protection capabilities across SIEM and XDR, you can search everything in one place—no need to remember where data is stored, run two different search queries, or normalize data across tools. Unified incidents give you a holistic view of all threats since all your information is in one place, meaning more threat intelligence. The result of gaining this insight into what is happening in your organization is saved analyst time and higher confidence in your protection.

Keep your organization safe while your analysts benefit by maintaining their focus on risk signs, spending less time correlating alerts, and speeding the mean time to repair. Time is of the essence when you are keeping your organization safe, and a unified solution equips analysts to stay in front of cyberattacks.

2. Gain more out-of-the-box protection

With a unified approach, you get the best of both worlds. Gain all the flexibility of a SIEM with the depth of protection and out-of-the-box value of an XDR. This flexibility aspect begins with your choice of how you implement a unified platform, doing so in a way that works for your needs, priorities, and budget. When your available security capabilities expand across multiple solutions in a platform, your organization stays safer as you gain storage flexibility and automatic attack disruption.

Plus, SOC optimization is a new feature that provides recommendations to ensure you are maximizing the security value; for instance, storing data at the most affordable log tier, getting detections on all your data, and maintaining strong posture.

Once you implement a unified platform, look for one that offers flexibility in data storage and security features. With Microsoft Sentinel data storage, you have flexibility in data retention, with a default of 90 days when data is ingested here. Expanding Microsoft Defender XDR’s unique attack disruption to data being introduced through Microsoft Sentinel, starting with SAP®, increases your immunity to cyberattacks, “freezing” cyberattacks before they can move across your organization.

3. Empower and uplevel threat investigation with generative AI

With the number and complexity of cyberattacks increasing, security teams can feel overwhelmed. That’s where AI assistance can come into play, detecting the threats that might be missed by security teams. A unified platform that includes generative AI can help your security team achieve better security outcomes. For example, generative AI can assist with guided investigations, hunting with natural language, and easy summaries.

Microsoft Security Copilot, our generative AI-powered security solution, **is available for additional purchase to further strengthen the unified SOC platform**. Security Copilot harnesses AI to support analysts with complex and time-consuming daily workflows, including:

- End-to-end incident investigation and response with clearly described cyberattack stories.
- Step-by-step actionable remediation guidance.

- Incident activity summarized reports, natural language Kusto Query Language (KQL) hunting, and expert code analysis—optimizing on SOC efficiency across Microsoft Sentinel and Defender XDR data.

Security Copilot makes it easier than ever for seasoned professionals to take every necessary security step, speed up tasks like writing KQL and decoding scripts, and helps uplevel new employees with intuitive, step-by-step guidance.

Try Microsoft's unified SOC platform for yourself

Protect yourself without significant setup or additional work required. You can gain the out-of-the-box integration of SIEM and XDR, expanded attack disruption onto your SAP data, and the breadth of Microsoft Sentinel's out-of-the-box, customizable content (more than 300 pieces of content!).

The pricing of Microsoft Defender XDR and Microsoft Sentinel and business model will remain the same; if you use both, you'll continue to enjoy your benefits. A recently announced SIEM migration tool will simplify and accelerate migrations to Microsoft Sentinel.

If a unified platform approach to modern SecOps sounds intriguing, make sure you have Microsoft Sentinel, Defender XDR, and Security Copilot and can benefit from a comprehensive security approach. Contact us for more information.

Learn more

Learn more about Microsoft Sentinel and Microsoft Defender XDR.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (@MSFTSecurity) for the latest news and updates on cybersecurity.

---

[1] The SOC's Future Is a Security Platform, Darkreading. December 4, 2023.

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads