Briefing - Envisioning the SOC of the future with Microsoft Security, AI, and Industry Solutions

ISD Security CSA: Todd Ray, with Ralf Winterer, Jorg Finkeisen, Aanya Hagiwara

Reviewers: Colin Brown, Stephen Kaufman, Terence Jackson, Harrison Briggs

22 January 2025

Figure 1 - The Cognitive SOC of the Future

Disclaimer

Executive summary

In an era where cybersecurity threats are escalating in both volume and sophistication, traditional **Security Operations Centers (SOCs)** face significant challenges. Cyber adversaries, including nation-state actors and cybercriminals, are increasingly adopting advanced techniques and converging tactics to exploit vulnerabilities.

This briefing explores the necessity for SOCs to evolve strategically, including the incorporation of AI into tooling and processes, as well as the role that Microsoft Industry Solutions[1] can play in helping customers reach their goals on this journey.

Vision

The SOC of the future must be highly intelligent, automated, and adaptive and is integral to an organization's cyber defense strategy. By embracing innovation, investing in human capital, following best practices, leveraging AI, and proactively planning for technological and regulatory changes, organizations can align themselves with industry leaders and meet their cyber resilience goals following the multi-phase approach shown below and explored further in this briefing.

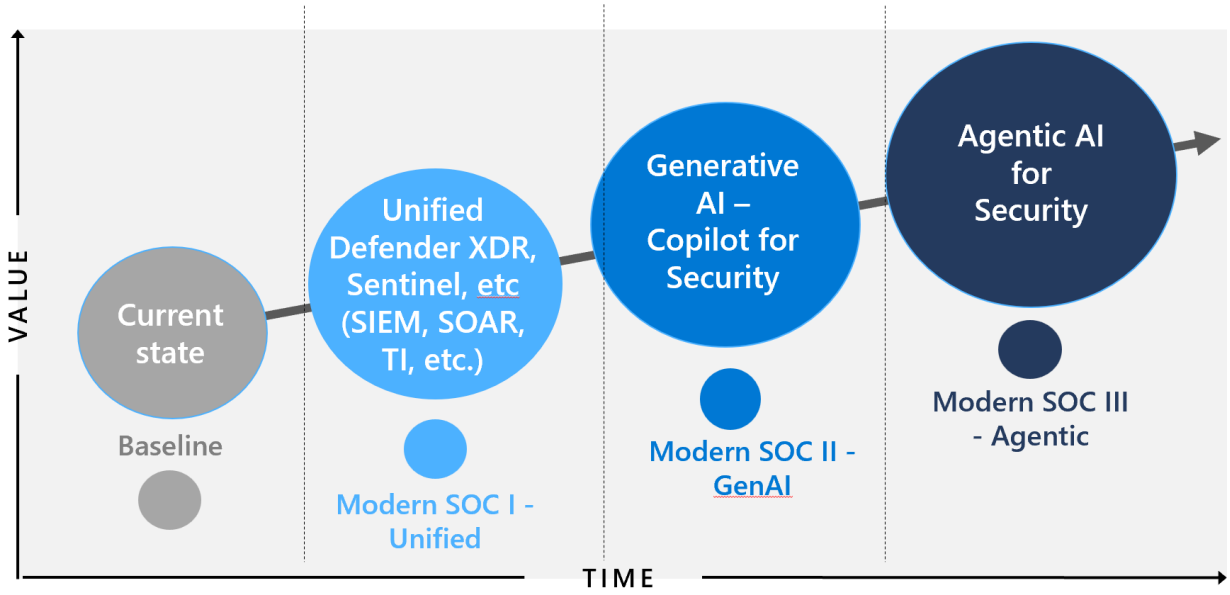


Figure 2 - SOC of the Future - Progression

[1] Microsoft's primary professional services organization, formerly "Microsoft Consulting Services"

How Microsoft Industry Solutions can help

Microsoft Industry Solutions is committed to support organizations in this transformative journey, providing strategic expertise along with implementation assistance to pave the path forward while improving key metrics for CISOs and SOC operations.

To assist organizations in transitioning to a more secure and cyber-resilient future, Microsoft Industry Solutions will take a multi-phase approach, starting with a thorough assessment of the current SOC infrastructure, processes, and workforce to identify gaps and areas for improvement.

Based on a strategic roadmap aligned with business objectives, we will next guide you through the implementation and integration of Microsoft Defender XDR, Microsoft Sentinel (SIEM and SOAR), Copilot for Security, and Threat Intelligence, as well as migration from 3rd party security solutions, as needed.

Figure 3 - Microsoft Industry Solutions Capabilities and Services

Industry Solutions Security offerings

Microsoft Industry Solutions has a number of Security Services offerings and component capabilities that address the SOC security space and SOC modernization vision covered in this briefing.

These include but are not limited to the following (see Section 10 for a complete listing):

- Cyber security strategy, architecture, and roadmap
- Microsoft Defender solution implementation (Identity, Endpoints, Office 365, Cloud, Cloud Apps, etc.)
- Microsoft Sentinel implementation
- Microsoft Sentinel migration (from 3rd party SIEM solutions)
- Security Copilot implementation
- Security operations planning and optimization

By leveraging Microsoft Industry Solutions security expertise and advanced tooling and techniques, organizations can build a highly adaptive, intelligent SOC that is integral to their defense strategy against current and future cybersecurity challenges.

Contents

1. Introduction

In today's rapidly evolving digital landscape, **cybersecurity threats** are not only increasing in volume but also becoming more sophisticated. Cyber adversaries are leveraging advanced techniques to exploit vulnerabilities, making it imperative for organizations to enhance their defense mechanisms.

Simultaneously, the rise of **Artificial Intelligence (AI)** presents both new challenges (such as adversaries using AI techniques) and unprecedented opportunities for security operations that can address cyber threats in innovative ways. As AI technologies continue to mature, they offer powerful tools to detect, protect, and respond to threats more effectively.

Figure 4 -Microsoft Security Operations Center

This briefing explores how **Security Operations Centers (SOCs)** must transform to meet these emerging challenges.

We will first delve into the current state of cybersecurity, drawing insights from the latest Microsoft 2024 Digital Defense Report. The discussion will then highlight the challenges traditional SOCs face and the necessity for strategic evolution, including the adoption of modern SOC practices followed by the integration of AI, providing a comprehensive view of how innovation and automation can be harnessed in a SOC environment.

Our audience includes security executives and practitioners seeking to transform their security operations and plan for the SOC of the future.

Throughout this briefing, we aim to equip you with actionable strategies to improve operational efficiencies, responsiveness, and overall effectiveness, as well as ensure a secure future for your organization, in partnership with and support from Microsoft Industry Solutions.

2. Cyber Trends Summary

Top cyber trends impacting leading organizations

1. **Increased investment in AI-based monitoring, detection and prevention of fraud, misinformation, and deep fakes**
2. **Continued investment in Zero trust and advanced identity and endpoint protection**
3. **Continual review and remediation of application inventories, permissions, and development practices**
4. **Peer and government collaboration and information sharing**
5. **Research and advancement in AI-based defenses and preparation for future threats (e.g., quantum resistance)**
6. **Strategic programs like Microsoft's SFI initiative and adoption of related principles and mechanisms to combat future cyber threats**
7. **Increasing use of AI by both adversaries and SecOps teams changing both the threat and defense landscapes**

Overview

Similar to recent years prior, the cybersecurity landscape continued to change at a rapid pace towards the end of 2023 and into the Fall of 2024, as highlighted in the annual Microsoft Digital Defense Report (MDDR, 2024).

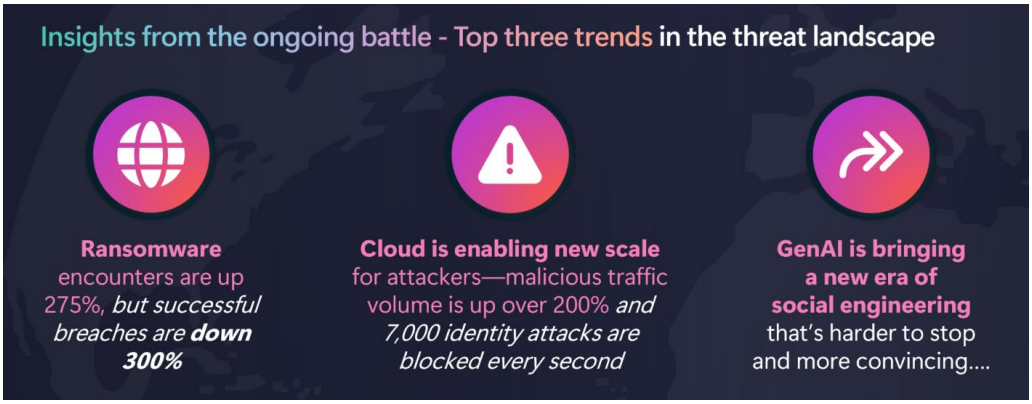


Figure 5 - Top 3 trends in the threat landscape

Complementing data from the MDDR 2024 report, additional trends/data were published in December 2024 in the Foundry study highlights the benefits of a unified security platform in new e-book | Microsoft Security Blog and accompanying E-book The unified security platform era is here.

This section summarizes a few highlights of possible interest to security executives and practitioners/operators from these reports, which includes coverage of Microsoft's "Secure Future Initiative" (SFI).

1. Evolving Cyber threat landscape. The cybersecurity landscape has seen rapid evolution, with increased convergence between nation-state actors and financially motivated cybercriminals, all enabled by the emerging "Industrialized cybercrime economy" and "services sector" (represented in the figure below).

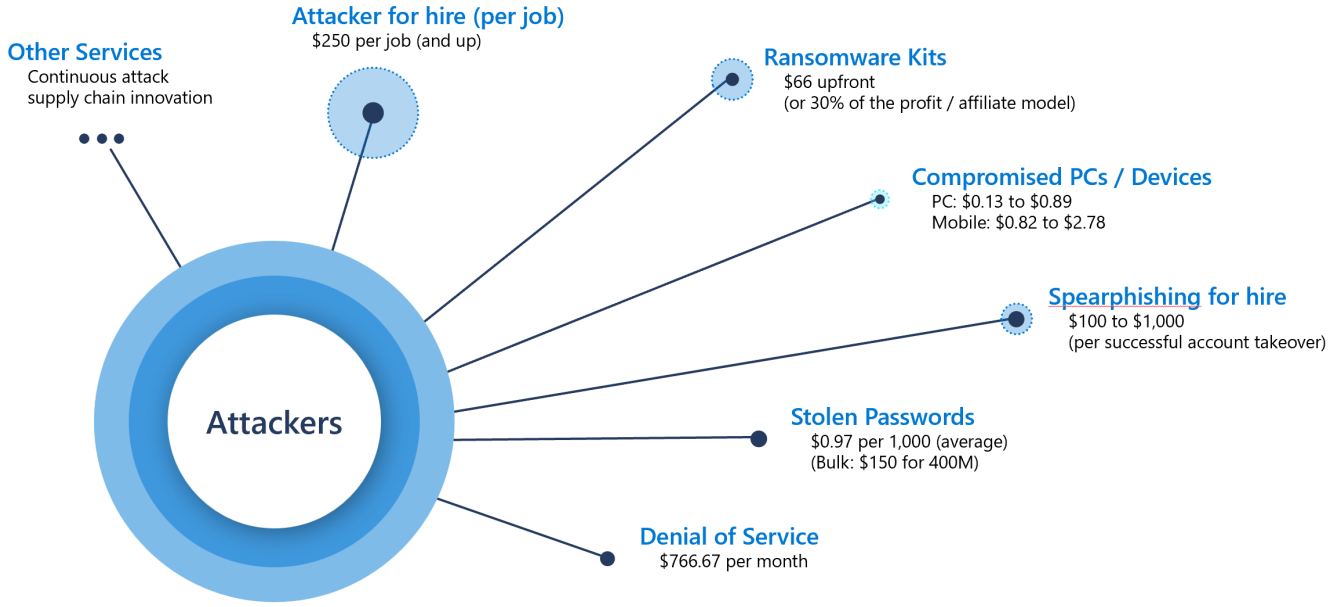


Figure 6 - Emerging cybercrime services sector | 2024 update

As highlighted in the figure above, the industrialized hacker economy has emerged as a significant challenge, characterized by highly specialized roles and the commoditization of illicit services and tools.

This economy enables attackers with varying skill levels to access advanced capabilities at minimal cost, creating a scalable and efficient ecosystem for cybercrime.

In this modern hacker economy, key attack vectors include:

- **Identity and Password/Phishing attacks**: These remain prevalent due to their low cost and high effectiveness. With stolen passwords costing as little as $0.97 per 1,000 credentials (or bulk rates like $150 for 400 million), attackers often bypass traditional security measures entirely by logging in instead of breaking in, where services like "Spear phishing for Hire" can yield $100 to $1,000 per successful account takeover.
- **Denial of Service attacks**. With DDOS services available for less than $800 per month, DDoS attacks have become an accessible weapon, particularly for targeting unprotected sites.
- **Ransomware**. "Ransomware Kits" priced at just $66 upfront (or leverage a profit-sharing affiliate model) empower even low-skill attackers to execute sophisticated ransomware campaigns, democratizing access to advanced attack techniques.

And for those looking for other services, you even have markets for "supply chain" attacks, attackers for hire, and groups of compromised PCs/Devices for later exploitation.

The rise of AI use by adversaries

Notably, advanced technologies such as artificial intelligence (AI) and machine learning (ML) are increasingly helping bad actors create more effective and elusive malware to launch ransomware, phishing attacks, and zero-day exploits. Nation-state threats are growing as well, with rogue groups deploying large language models to gather intelligence or create automated scripts for carrying out attacks at unprecedented scale.

Prevalence

As cited in the December 2024 Foundry Study referenced above, organizations averaged 13 security incidents or breaches over the past year, with nearly one-quarter of respondents (24%) reporting 20 or more.

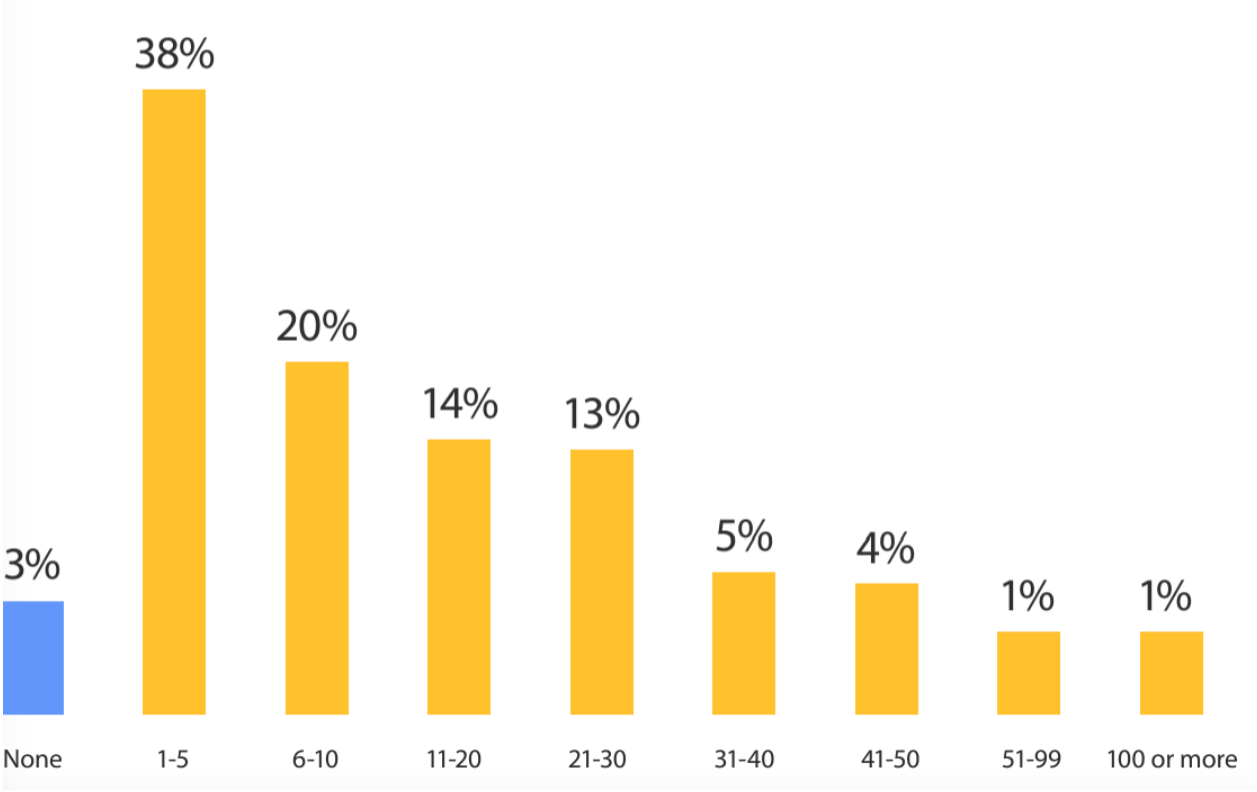


Figure 7 - Incident or breach frequency | Foundry study

Implications

The emerging industrialized approach to cybercrime has reduced barriers to entry, creating an ecosystem where attackers can specialize in individual tasks, collaborate globally, and scale their operations.

Organizations must adapt by prioritizing advanced defenses like multi-factor authentication (MFA), zero trust architectures, real-time threat intelligence, as well as SOC optimization to mitigate these growing threats.

2. Nation-state and cybercriminal convergence Nation-state actors are intensifying efforts to disrupt democratic elections and influence public opinion, leveraging tactics such as covert online campaigns.

Russia, Iran, and China have conducted influence operations, with strategies spanning from social media manipulation to AI-enabled misinformation.

3. Persistent ransomware threats Ransomware continues as a severe cybersecurity risk, with a 2.75-fold increase in human-operated ransomware attacks on Microsoft customers, albeit with a notable downward trend (300%) of successful breaches, likely due to organizations working to improve their cyber resilience based on recommended practices such as those shared by Microsoft and others.

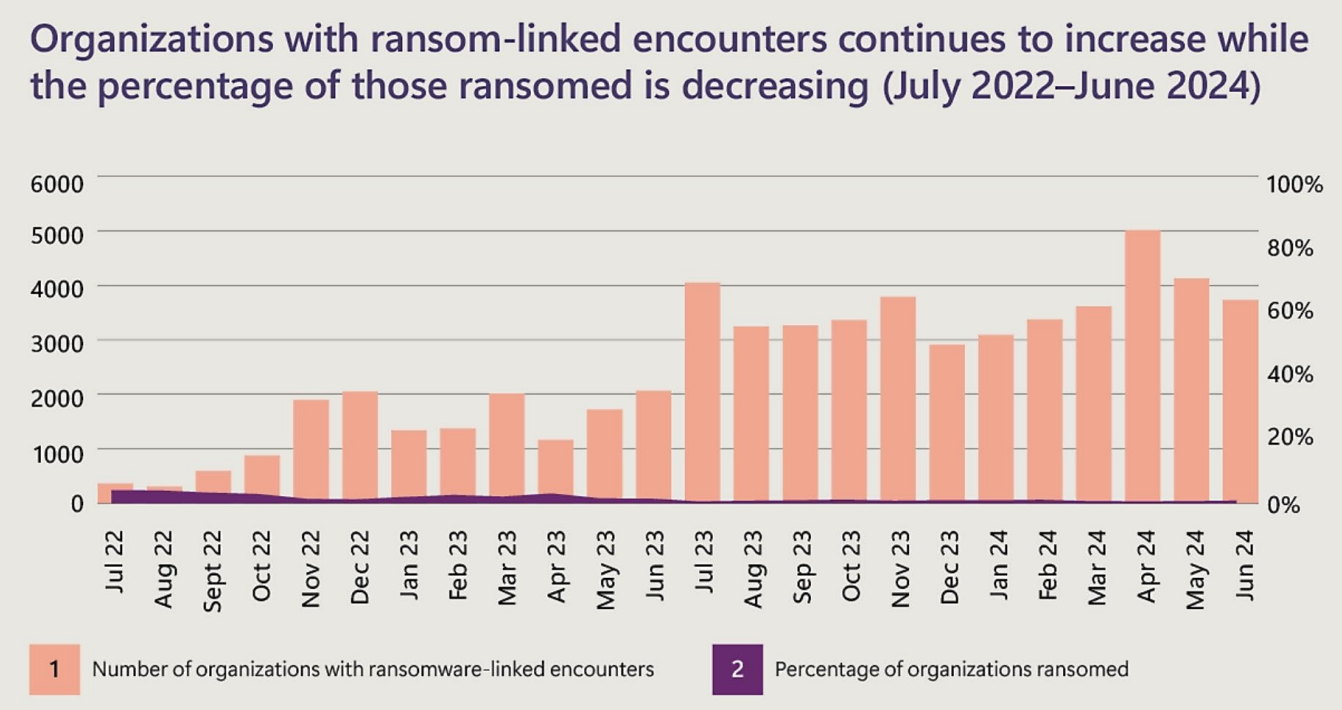


Figure 8 - Ransomware trends

Despite detection improvements, attackers often gain access through unmanaged devices and tamper with security products, prolonging their presence and impact.

4. Escalation of sophisticated fraud tactics Fraud has escalated globally, with an estimated $1 trillion in losses in 2023 alone. Cybercriminals leverage cloud services and advanced AI to launch attacks, impersonate entities, and conduct scams like payment fraud and business email compromise (BEC).

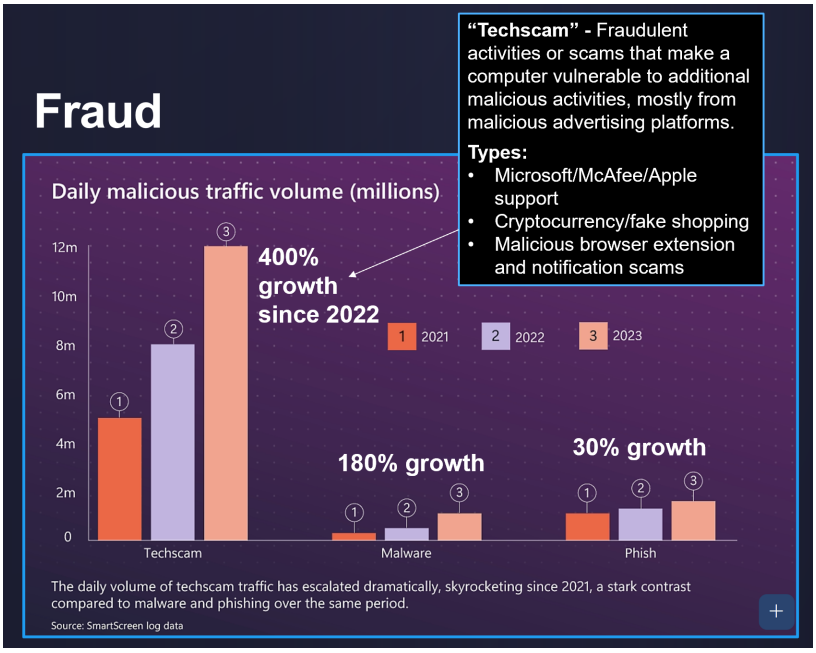


Figure 9 - Fraud trends

Also note that "Techscams" are becoming more common, which are fraudulent activities that make a machine vulnerable for additional malicious activities, often originating from compromised ad network technology.

- Since 2022, malicious traffic volume related to tech scams has increased by a staggering 400%.
- This overshadows the growth in malware (180%) and phishing (30%).
- Common tech scams involve fake support services (e.g., Microsoft, Apple), cryptocurrency schemes, and malicious browser extensions. These scams exploit advertising platforms to compromise systems and lure victims into further malicious activities.

In summary, fraud and tech scams are escalating at an alarming rate, necessitating stronger measures to combat this rapidly growing vector.

5. Rising Phishing threats and other techniques

- **QR code phishing**. Phishing attacks rose by 58% in 2023, with new techniques such as QR code phishing and exploitation of legitimate web services to evade detection.
- **Deep fakes**. Attackers increasingly use voice and video deep-fakes, complicating detection efforts.
- **Phishing, whaling, and malware**. AI is evolving spear phishing and whaling by coupling AI with malware, creating a tool that lies dormant until it identifies its intended target and deploys. Without users knowing, the AI uses device cameras, speakers, and GPS for target verification.
- **Resume swarming and steganography**. AI used by attackers to scrape job postings and create highly qualified – but fake – candidates that get hired and infiltrate from the inside. Resumes further manipulated to use "steganography" to embed invisible information to bypass screening tools.

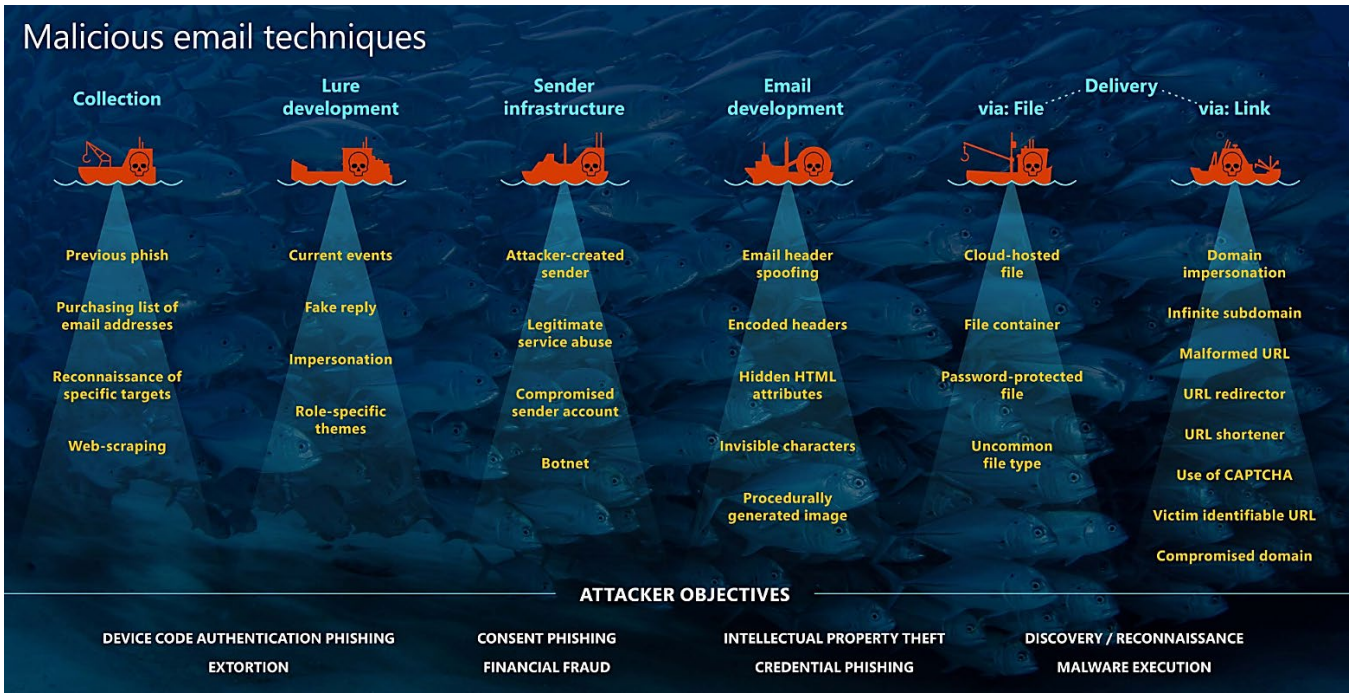


Figure 10 - Malicious email techniques

6. Continued focus on Identity-based attacks. As organizations move to the cloud, identity has become a primary target for attackers. Microsoft blocks millions of password-based attacks daily (comprising 99% of identity-based incidents), as attackers continue to exploit identities through phishing, brute-force (e.g., password spray), breach replay, and token theft techniques.

Figure 11 - Identity-based attack trends

While less than 1% of attacks target multi-factor authentication (MFA) systems (indicating its general effectiveness in mitigating these threats), adversaries can bypass MFA via adversary-in-the-middle (AiTM) attacks and token theft, highlighting the importance of advanced, phishing-resistant authentication methods.

In the meantime, advanced techniques like SIM swapping, MFA fatigue, and post-authentication attacks (e.g., token theft and consent phishing) represent emerging challenges that require vigilance and updated defenses.

7. Increased exploitation of vulnerable and under-secured applications. Cybercriminals exploit under-secured applications, cloud misconfigurations, and excessive permissions. Threat actors use stolen credentials to access high-value resources and modify identity infrastructures to maintain undetected access.

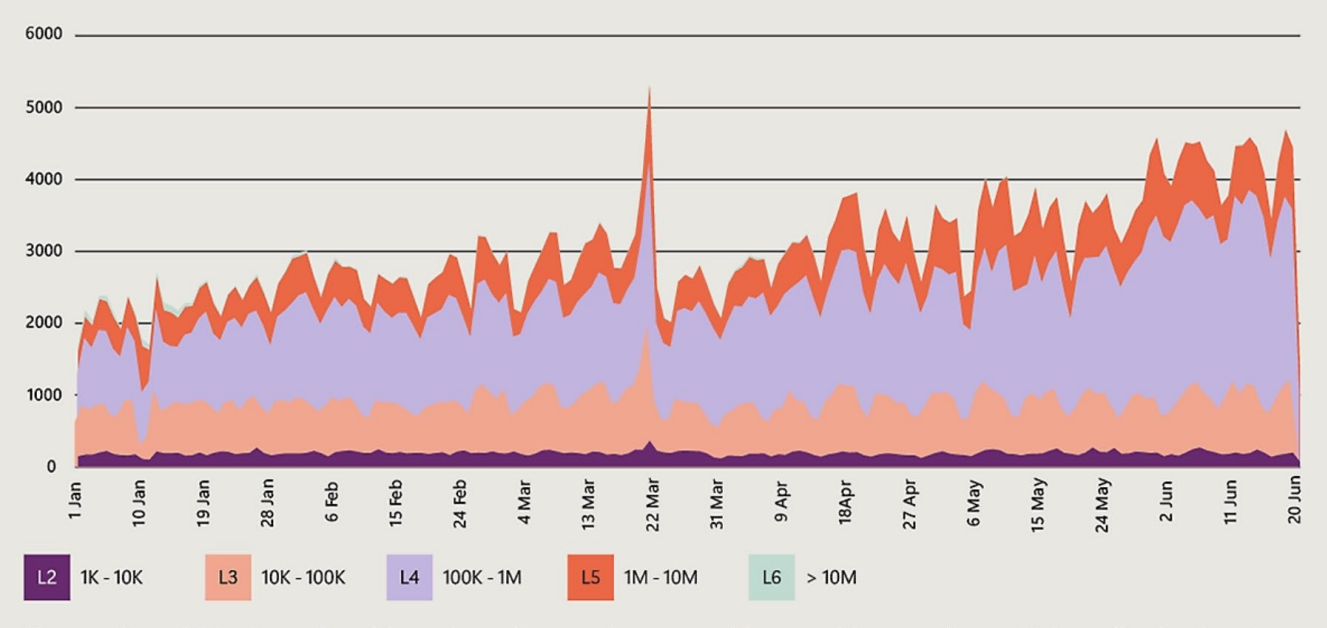


Figure 12 - Application layer attack trends

The frequency and sophistication of application-layer DDoS (distributed denial-of-service) attacks surged in early 2024. These attacks, represented on the graph above, target Layer 4 (transport layer) and Layer 7 (application layer) protocols, with many exceeding 10 million packets per second (L6).

Application-layer attacks are particularly stealthy and difficult to mitigate, requiring advanced, adaptive defenses.

This data underscores the growing prevalence and intensity of these attacks, necessitating proactive strategies to safeguard networks.

8. Legacy operational technology (OT) vulnerabilities threaten critical infrastructure. Since late 2023, Microsoft has observed an increase in reports of attacks on internet-exposed, poorly secured OT devices that control real-world critical infrastructure and processes.

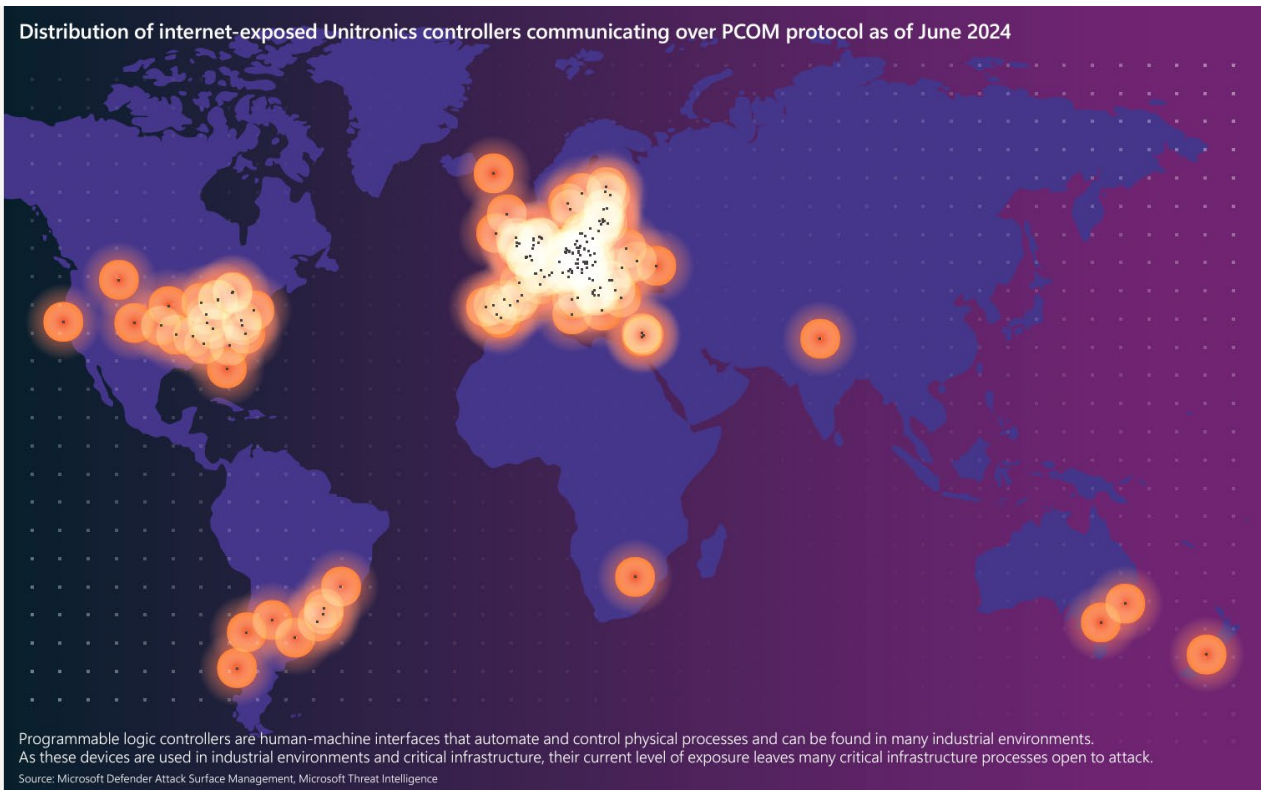


Figure 13 - Distribution of internet exposed, legacy OT controllers

This is particularly concerning given these systems often have inadequate security practices, including being left unpatched, subpar authentication methods, and more.

9. Strategic technology and policy initiatives Emerging technologies like IoT, 5G, and quantum computing introduce new vulnerabilities but also opportunities for innovation in cybersecurity.

As laid out in its Secure Future Initiative | SFI, Microsoft advocates foundational security principles—***secure by design, secure by default, and secure operations***—to combat the rising tide of cyberattacks.

Launched as a multi-year endeavor, SFI evolves how Microsoft designs, builds, tests, and operates products and services to achieve the highest possible standards for security; and along the way, serve as a model for our customers and partners.

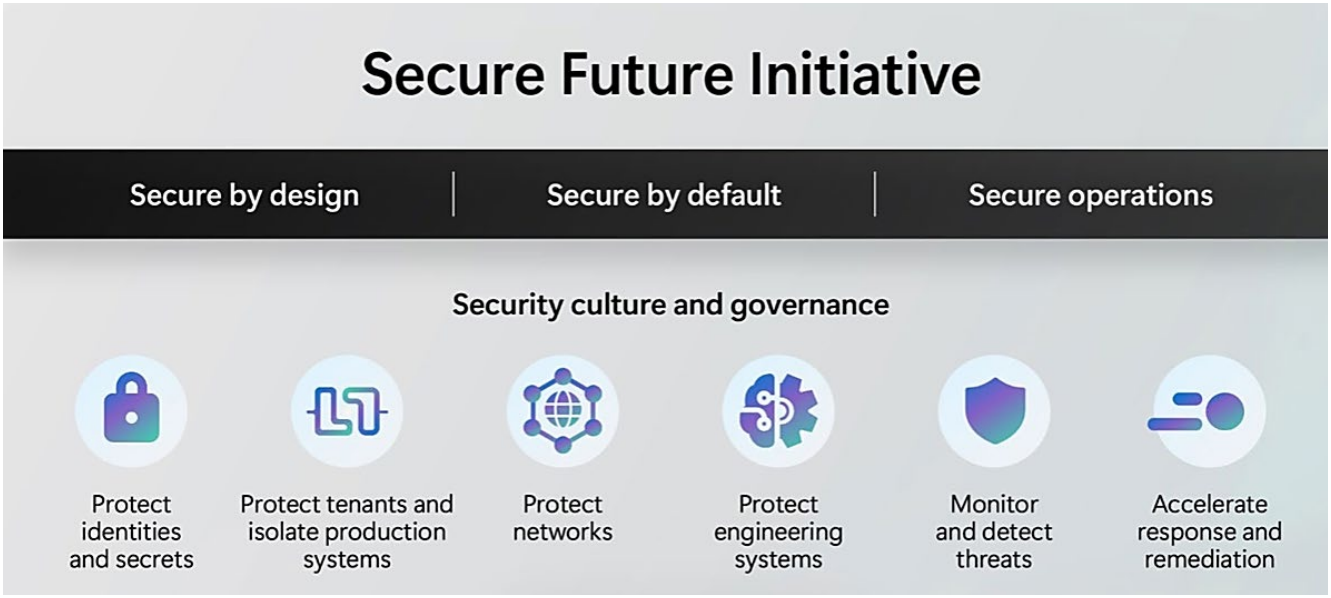


Figure 14 - Secure Future Initiative

As shown in the above diagram – from the SFI report - our security principles are supported by cultural and governance practices and policies to ensure that every employee prioritizes security above all else.

On the technical side, the six (6) engineering pillars shown have underlying standards established to help achieve 100% compliance given risk tolerances and ongoing assessment.

Strategically and practically speaking, our SOC operations play a key role in fulfilling the vision of the SFI initiative, as this briefing will highlight.

10. AI's growing presence for SecOps teams

As cited in the Foundry Study reference above, AI is already proving itself as a game-changer for many SecOps teams. Deployed strategically, it can reduce complexity and improve defenses by removing barriers that inhibit rapid detection and response, though at this early-stage customers vary widely in their adoption at this point, as shown in the Foundry Study results shared below:

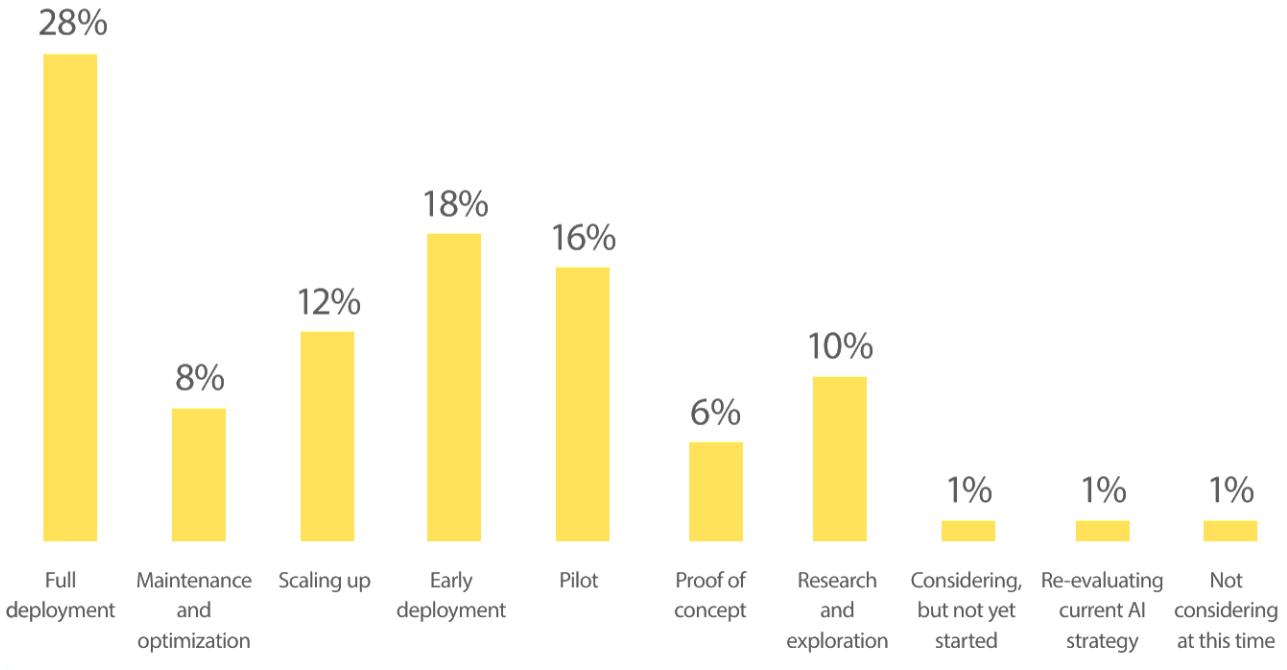


Figure 15 - Deployment of AI for SecOps - Foundry Study

Per Rob Lefferts of Microsoft: "*AI enables SecOps teams not just to be more responsive to an incident but also allows them to proactively address their security posture to reduce vulnerabilities.*"

In summary, SecOps teams are increasingly employing AI in two primary ways, as follows:

1) First, AI solutions such as Security Copilot help analysts improve efficiency by automatically correlating alerts into incidents, prioritizing based on severity, and enriching investigations.
    - With promptbooks and embedded experiences, automated, step-by-step guidance turns complex, multistage incidents into manageable investigations for analysts of every level.
2) Second, when embedded into automated security tool defenses—AI helps with things like the automatic disruption of in-progress attacks, deployment of decoys to mislead attackers, and automating routine remediation such as password resets.

For a more complete listing across SOC functions, see the chart below from the Foundry study cited previously:

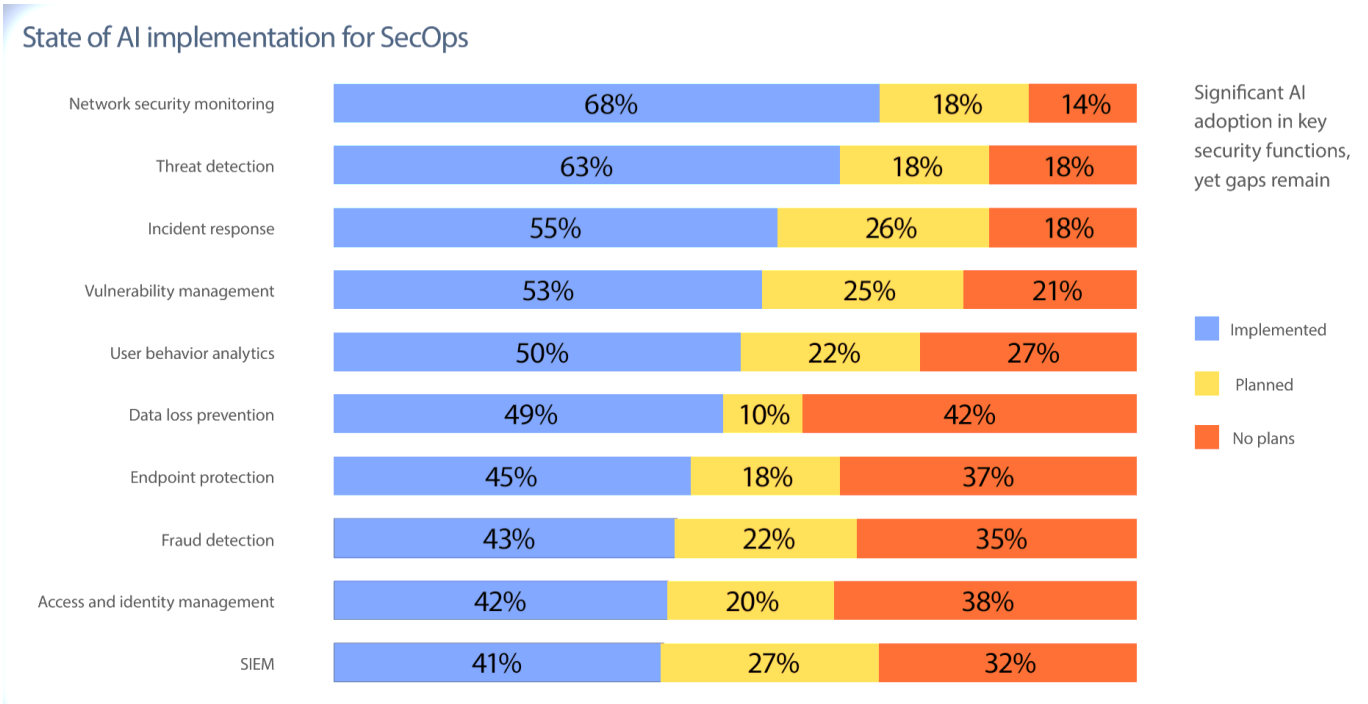


Figure 16 - State of AI Implementation for SecOps | Foundry Study

See also: Pain points of the Modern SOC

3. Regulations, frameworks, and standards

Top actions of leading organizations – Regulations, Frameworks, & Standards

1. **Strict employment of preventative control and response frameworks**
2. **Transition (if not already there) to stricter incident reporting timelines**
3. **Robust documentation of incident handling processes and procedures**
4. **Improved risk management, monitoring and reporting for 1st and 3rd party service providers**
5. **Standards-based data residency, processing, and transfer practices**
6. **Research and advancement in AI-based defenses and preparation for future threats (e.g., Quantum)**

Overview

Organizations worldwide – including ones employing SOCs - are subject to a wide (and growing) range of security (and privacy)-related regulations and therefore are required to make significant investments in alignment with security standards and frameworks to help demonstrate (and/or attest to) compliance with applicable laws.

Figure 17 - Example regulations, frameworks, and standards

Why is this important in a SOC context?

Significant investments may be required to align with security standards and frameworks to help demonstrate (and/or attest to) compliance with applicable laws.

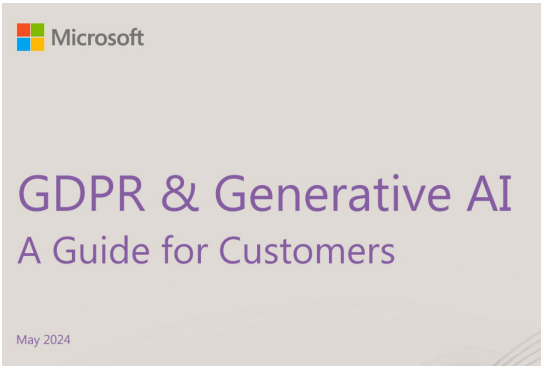
This part of the cybersecurity landscape provides "drivers" for investments in related security capabilities, but since this is such a large topic we will only provide a few examples.

Example EU Regulations specifically impacting SOCs

- **NIS2 Directive (Directive on Security of Network and Information Systems)** – scope includes digital infrastructure, public administration, and the healthcare sector; mandates a higher level of cybersecurity risk management and reporting; SOCs must report significant incidents within tight timelines, often within 24 to 72 hours; non-compliance can result in hefty fines up to 2% of global turnover, making it a significant concern for CISOs.
- **General Data Protection Regulation (GDPR)** - requires organizations to report personal data breaches to supervisory authorities within 72 hours; penalties can reach up to 4% of annual global turnover or €20 million, whichever is higher; affects any organization processing EU residents' data, making compliance a widespread concern.

  Reference:

  Microsoft whitepaper: GDPR & Generative AI – A Guide for Customers



- **Digital Operational Resilience Act (DORA)** - targets banks, insurers, and other financial entities, sectors that heavily rely on SOCs; mandates robust cybersecurity practices and resilience in digital operations; requires immediate reporting of significant ICT-related incidents; emphasizes the need to manage risks stemming from third-party ICT service providers (Microsoft included).
- **Data privacy regulations expansion -** Beyond GDPR, many countries are enacting strict data privacy laws (e.g., CCPA in California, LGPD in Brazil); regulations affecting how data can be transferred internationally (e.g., Schrems II decision impacting EU-US data transfers); SOCs must ensure compliance with a myriad of global data privacy laws, affecting data collection, storage, and processing practices.

Example frameworks and standards specific to SOCs

- **ISO/IEC 27035** – standard for incident management processes, including incident handling.
- **NIST CSF** – core specs for Identify, Protect, Detect, Respond, Recover.
- **CIS Controls** – actionable recommendations to prevent most pervasive cyber-attacks; quick wins in security improvements; prioritized best practices surfaced in Defender.
- **PCI DSS -** Regular testing of security systems and processes; emphasizes real-time monitoring and vulnerability management.

Certification examples specific to SOCs

Recent highlight

- **HIPAA HITRUST** - **Security Copilot** has achieved HITRUST Certification, a significant milestone in our commitment to data security and privacy that validates our adherence to the highest standards of security and compliance.

Other:

- **ISO/IEC 27001** certification enhances credibility with clients and stakeholders.
- **SOC Type 2** certification demonstrates commitment to security best practices.
- **CMMC** Ensures compliance with U.S. Department of Defense (DoD) cybersecurity requirements.

Regulations and standards specific to AI (sampling)

- **EU Artificial Intelligence Act (AI Act) -** The EU AI Act is the first comprehensive regulatory framework for AI, aiming to ensure that AI systems placed on the EU market are safe, transparent, ethical, and respect fundamental rights.
- **NIST AI Risk Management Framework -** comprehensive guide developed by the National Institute of Standards and Technology (NIST) in the United States to help organizations manage risks associated with the design, development, deployment, and use of Artificial Intelligence (AI) systems. While it originates from the U.S., its principles and guidelines are globally relevant and increasingly influential, including within the European Union (EU).
- **ISO 42001 -** standard that specifies requirements for designing/ implementing/managing an Artificial Intelligence Management System (AIMS), ensuring responsible use.
- **ISO 23894** - risk management guidance for organizations that develop, deploy, or use AI systems.

Note: most of the above have Microsoft Purview Compliance Manager and/or Defender for Cloud assessment templates associated with them.

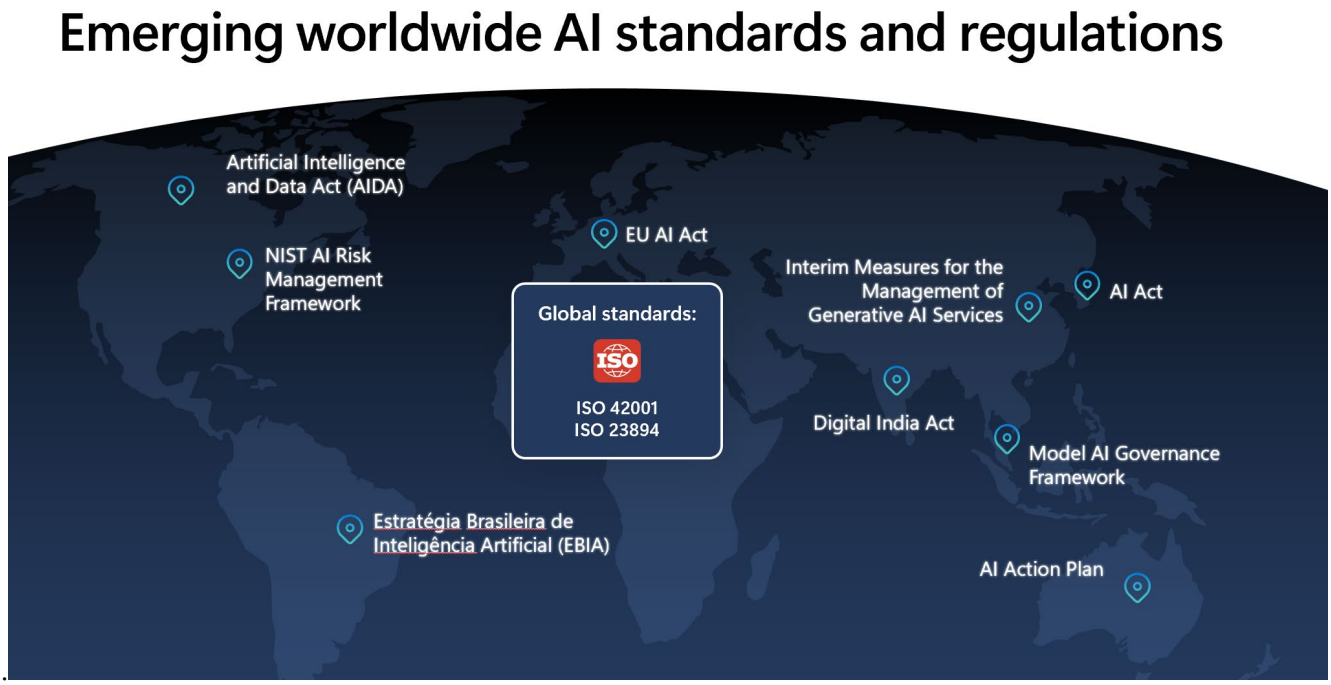


Figure 18 - Emerging worldwide AI standards and regulations

4. The "Modern" SOC

Top architectural practices of leading SOCs

1. **Secure by design and default for both internal (1st party) and external (e.g., customer-facing) systems**
2. **Follow industry best practices like the Microsoft Security Adoption Framework and the Microsoft Cybersecurity Reference Architecture (MCRA), as well as SOC guidance from organizations like MITRE**
3. **Benchmark against standards for cyber organizational functions, technical operations, and strategic as well as operational roles**
4. **Invest in process improvement and skills development in alignment with cyber and technological trends**
5. **Continue to balance the in-house vs. outsourced resource mix to address current and future security trends, including technical as well as market dynamics**
6. **Adopt modern XDR-SIEM-SOAR-TI architecture and unified toolsets**

Introduction

Microsoft operates one of the largest and most advanced private sector security engineering and operations (SecOps) organizations in the world[2], dedicated to safeguarding both its internal assets and those of its global customer base. This dual-focused approach enables Microsoft to not only protect its own infrastructure but also to develop innovative security solutions that empower organizations to secure their information assets and, by extension, those of their clients and partners.

That said, like other organizational functions, security operations are not a one-size-fits-all endeavor - they often adopt diverse forms to meet different challenges and objectives. Different organizations may employ various tools and operational processes tailored to their specific industry requirements, regulatory environments, risk tolerance, budget, internal capabilities, and past experiences (e.g., with cyber-attacks).

Nevertheless, there are common operational functions, patterns, and practices specific to security that are good to be aware of when envisioning/modernizing a SOC function for an organization.

This section lays these out in summary and then reviews some of the more common pain points. Then, in the next section, we highlight how Microsoft's Defender XDR + Sentinel + Threat Intelligence (TI) solution provides an industry leading, unified approach to this space.

What is a SOC?

Reference: What is a SOC? (Microsoft.com ***Security 101*** definition)

- A SOC is a centralized or distributed function or team (or set of interacting teams) responsible for improving an organization's cybersecurity posture and preventing, detecting, and responding to threats.
- The SOC team, which may be sourced with in-house, outsourced, or mixed resources, monitors identities, endpoints, servers, databases, network applications, websites, and other systems to uncover potential cyberattacks in real time.
- It also does proactive security work by using the latest threat intelligence to stay current on threat groups and how they attack infrastructure, as well as identify and address system or process vulnerabilities before attackers exploit them.

Given the variety of conditions in which large organizations (and their cyber adversaries) operate, SOC "staffing" and hours of operation will vary widely, with some SOCs operating 24 x 7 and others on reduced schedules, all employing strategies for staffing optimization relative to anticipated demand, inclusive of outsourcing as appropriate, which may vary across tiers and at certain times of day (see separate section on "Tiering").

[2] Cyber Defense Operations Center (CDOC) - https://www.microsoft.com/en-us/msrc/cdoc

Another consideration is the geographic reach of an organization's electronic assets - large organizations that span multiple countries may require a global security operations center (GSOC) to stay on top of worldwide security threats and coordinate detection and response among several local (affiliate) SOCs as well as government(s) and other institutions.

SOCs will also vary along the lines of public/sector, industry, geo/region/country, digital maturity, and other factors.

For more information on SOC fundamentals, an important set of high-level focus areas are shared in the sections below.

Further exploration is provided in a number of external publications, including the comprehensive and publicly available MITRE SOC guidance: 11 Strategies of a World-Class Cybersecurity Operations Center.

Figure 19 - 24 x 7 operations of a global SOC

Basic functions

As highlighted in the Microsoft.com ***Security 101*** specification Functions of a SOC, a number of functions are specific to the SOC as part of the overall security operation:

- Asset and tool inventory
- Reducing the attack surface
- Continuous monitoring
- Threat intelligence
- Threat detection
- Log management
- Incident response
- Recovery and remediation
- Root cause investigation
- Security refinement
- Compliance management

Refer to MITRE's 11 Strategies of a World-Class Cybersecurity Operations Center for additional details.

SOC Types

Reference: Types of SOCs (Microsoft.com Security 101 specification)

There are a number of ways organizations may set up their SOCs, sometimes characterized as the "**SOC Operating Model**"[3]:

- **Dedicated, in-house SOC.** Some organization maintain a dedicated SOC with an internally resourced staff. This type of SOC can be a physical on-premises location with co-located, in person resources, or it can be virtual with staff coordinating remotely using digital tools, or a mix of both.
    - Many SOCs use a combination of contract (staff augmentation) and full-time staff.
- **Outsourced SOC**. SOC outsourcing is performed by organizations generally referred to in the industry as "Managed Security Service Providers" (**MSSPs**), now complemented with modern variants such as "Managed Detection and Response" (**MDR**)[4] and Managed Extended Detection and Response (**MXDR**) providers, which provide more advanced, specialized services.

  These "provider classes" vary in the types of services they provide but generally take some or all the responsibility for preventing, detecting, investigating, and responding to threats for organizations of all sizes.
    - **Note**: The outsourcing of SOC functions to security service providers is commonplace and is driven by factors such as the complexity of modern cybersecurity needs, tooling sophistication, skill shortages, and cost pressures.

      In the same way as cloud computing has become ubiquitous, many organizations are realizing that they cannot run (all or part of) a datacenter, or a SOC, cheaper or better than specialists.
- **Hybrid**. It is also common for organizations to use a combination of internal staff and one or more MSSP/MXDR/MDR provider(s) for specific functions within a customer's overall security operation. This model is called a co-managed or hybrid SOC.

Note: the above oversimplifies what is often a complex operating model with different SOCs in different regions providing specific services or serving distinct functions (to other SOCs in the system), sometimes within hierarchical structures with affiliate relationships (with outside entities) as well.

[3] Refer to MITRE's 11 Strategies of a World-Class Cybersecurity Operations Center for additional details – this reference provides extensive exploration of this topic.

[4] MDR services were originally focused primarily on endpoint threats and response actions, while MXDR builds upon MDR concepts by integrating a broader range of telemetry sources—such as network, cloud, identity, and applications—into one unified framework. Many vendors use these terms somewhat interchangeably or position MXDR simply as a more holistic evolution of MDR.

Anecdotally, based on a sampling of data from Microsoft customers enrolled in the Security Copilot preview, over 85% of those sampled used some sort of outsourcing on at least one tier (see separate section on Tiering).

A strategic approach that aligns outsourcing decisions with organizational security objectives, operational needs, current and future technical capabilities[5], and compliance requirements will be key to building a resilient and future-ready SOC.

Service types

MSSP vs. MXDR

The distinction between MSSP and MXDR-type outsourced services is worth noting given the nuanced distinctions between the two and the fact that most MSSP providers have extended into the MXDR space, now providing both traditional MSSP-type services and more specialized (and advanced) MXDR.

In addition, the types of services provided by outsourcing providers may have in-house service analogs, which like their external counterparts are constantly addressing new challenges and industry trends, with advanced MXDR-type services (whether outsourced or in-house) increasingly becoming part of Modern SOC operating models.

For this reason, we compare them in the table below, followed by additional insights on these service models in the discussion that follows.

Service type	Scope and focus	Technology and tools	Operating model	Analytics and investigations
MSSP – Broad security services - Model dates to the early 2000s - Remains popular due to its broad coverage and cost-effective approach. - Many organizations start with MSSPs	• Broad security monitoring and device management services. • Firewalls, intrusion detection/prevention systems (IDS/IPS), Virtual Private Networks (VPNs), and Security Information and Event Management (SIEM) solutions. • Gather and forward security alerts but may not engage deeply in root-cause analysis, threat hunting, or complex incident response.	• SIEM platforms and other log aggregation tools. • Often correlate events from various security devices and alerts. • Geared more toward alerting rather than highly automated detection and response (the realm of MXDR)..	• Tiered escalation of threats to customer investigation and response teams • MSSPs sometimes offer incident response retainers. • Role limited to monitoring and advisory support rather than full-scale active	• Alerts lack comprehensive context • Emphasis on filtering noise and escalating probable threats.

[5] **Note**: For outsource partners, Microsoft provides delegated access via Partner Center -> Service Management, and we support Azure Lighthouse for delegated access to Microsoft Sentinel so a partner tenant can prompt the Sentinel data of another tenant (not available for multi-tenancy) using the partner tenant "Sentinel Commit Units" (SCUs). Neither a unified delegated access model nor multi-tenancy is available as of Fall 2024.

Service type	Scope and focus	Technology and tools	Operating model	Analytics and investigations
			containment or remediation.	
MXDR – Advanced services - Evolution of managed services - Adv tech, analytics, and remediation - Bridge gap between detection and resolution.	• Continuous threat detection, forensic investigation, and active response measures • Wider array of data streams. • Telemetry from endpoints, networks, cloud environments, email systems, identity sources, and more. • Integrated and actionable workflow that identifies adversary tactics, techniques, and procedures, provides context, and proactively mitigates threats.	• Use next-generation detection and response platforms • Fusion of multiple data sources, behavioral analytics, machine learning, and automated remediation workflows. • Improved threat visibility	• More proactive stance. • Detection AND response • Help guide clients through a well-defined remediation process.	• Contextual insights and root-cause analyses a • Threat hunts, threat intelligence feeds, and integrated endpoint forensics.

Additional insights

In general, MXDR-type services (either in-house or outsourced) provide more advanced analytics, threat intelligence, and proactive threat hunting to detect subtle attack patterns and reduce response times. Automated workflows and guided remediation further streamline operations, empowering the SOC to contain threats more effectively.

As a result, MXDR-type services complement traditional MSSP approaches in modern environments by enhancing threat detection, response, and overall defense maturity. Organizations increasingly adopt MXDR for its proactive, integrated capabilities, shifting the SOC's posture from reactive alert handling to proactive, intelligence-driven security.

This may also impact traditional Tiering structures, explored in a separate section.

MXDR "Expert" services

Reference:

- What is Microsoft Defender Experts for XDR offering - Microsoft Defender XDR | Microsoft Learn
- DEX eBook

A variant of MXDR services, a number of organizations provide "experts on demand"-type services, including both Microsoft and a number of its partners[6].

Microsoft Defender Experts for XDR

Sold separately from Microsoft Defender XDR products, **Microsoft Defender Experts for XDR** is a service that augments the customer's MSSP/MXDR team(s) through integration of expert access channels into Microsoft Defender XDR and Sentinel incident response feature sets, as well as providing ***Experts on demand, Threat Intelligence, and Threat hunting*** services.

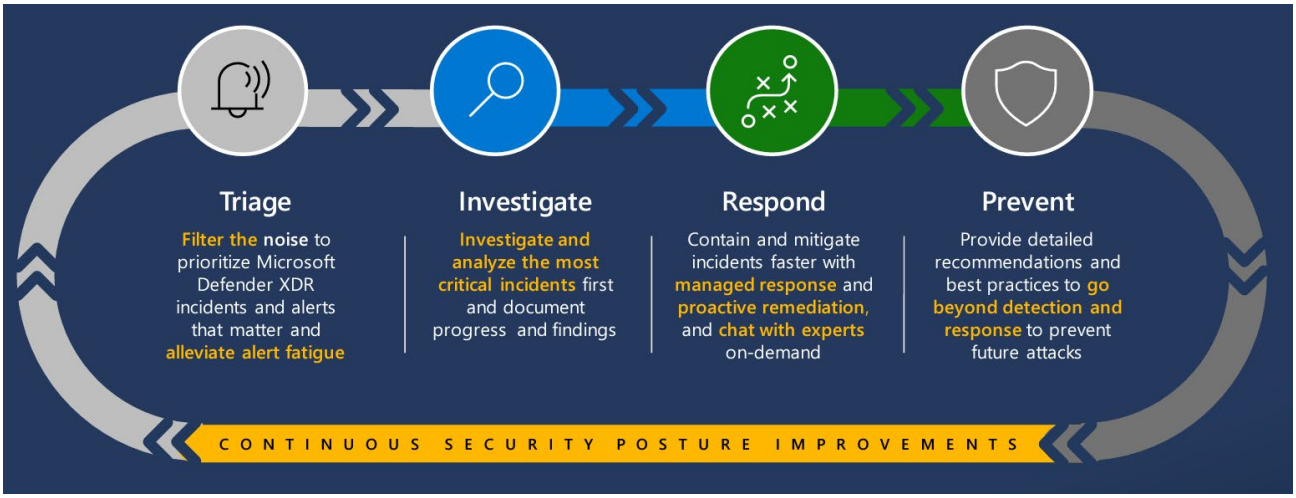


Figure 20 - Microsoft Defender Experts for XDR

Note: as we explore further later in the section addressing Tiering, most MXDR-type services provide what's essentially Tier 2 and 3-type functions, which often require more advanced and experienced (and thus harder to find, and expensive) security analysts.

Incident Response

Another type of service used by organizations - even those with mature MXDR functions - is that of "**Incident response**" (IR). IR is employed for reactive emergencies when organizations have been compromised and lack the internal resources/specialization to respond and recover from a cyberattack.

Upon detecting and validating a security incident (such as a ransomware attack or data breach) that meets pre-defined escalation criteria, the appropriate individual (typically a Sr. SOC manager, Director of Incident Response, or CISO) initiates a formal request for ***IR Services*** in accordance with established operating procedures, documented request processes, and requisite managerial approval.

Due to increased customer demand in this area as cybersecurity attacks have increased in number and severity, Microsoft has offered Microsoft Incident Response (MIR) services for a number of years.

[6] Microsoft verified MXDR partners

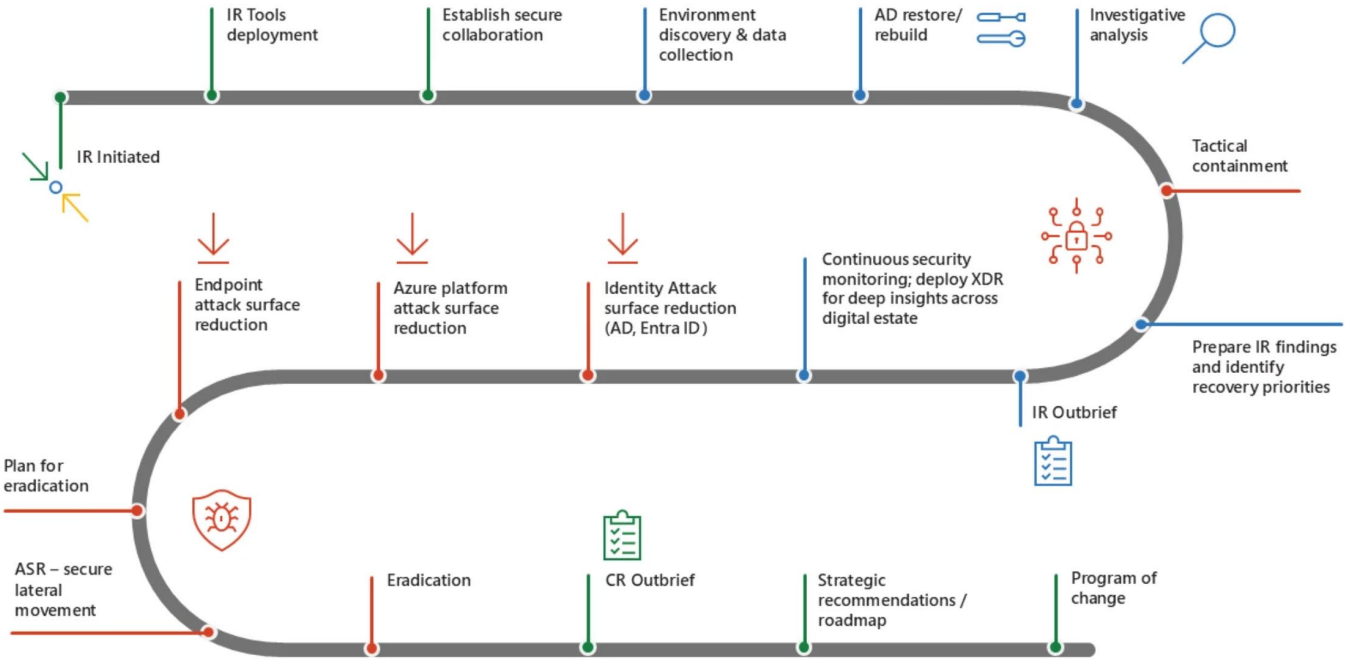


Figure 21 - Microsoft IR Services | Source: Microsoft Security Blog

As shown in the figure above, MIR begins with initiating the response and deploying necessary tools, establishing secure collaboration for efficient coordination, and then the team conducts environment discovery and data collection to understand the scope of the compromise. Tactical containment is achieved through steps like Active Directory restoration and investigative analysis to halt the attack's progression.

The process emphasizes reducing vulnerabilities with targeted attack surface reduction across endpoints, Azure platforms, and identity systems (e.g., Active Directory/Entra ID). Continuous security monitoring and XDR deployment provide enhanced visibility across the digital estate. Recovery efforts focus on planning eradication, securing lateral movement, and eliminating threats.

The engagement concludes with an IR outbrief, strategic recommendations, and a roadmap to guide long-term cybersecurity improvements.

Operational roles

A number of security roles are involved in SOC operations as part of the overall security function, which we cover in this section.

Several of the more common roles related to SOC operations are listed in the table below. Many of these may be directly or indirectly impacted by improvements in SOC functions based on a programmatic transition to a "Modern SOC I" (with the unified solution) or a "Modern SOC II" (with Generative AI/Security Copilot), so it's important to list them here.

Team or Function	Role	Responsibilities/Activities
SOC Leadership and Management	SOC Manager	Oversight of SOC operations, team management, and strategy implementation.
	CISO (Chief Information Security Officer)	Defines and drives overall security policy and governance.
	Security Program Manager	Manages SOC projects, timelines, and performance metrics.
Compliance & Reporting	Governance, Risk, and Compliance (GRC) Management	Manages policies, controls, and risk assessments related to SOC operations.
	Compliance Management	Ensures SOC compliance with regulations (e.g., GDPR, HIPAA); prepares compliance reports.
Security Engineering	SOC Engineer (SIEM Engineer)	Manages and tunes SIEM platforms; maintains detection rules and alerts.
	Security Automation Engineer	Develops automation playbooks, scripts, and automated response mechanisms.
	Security Architect	Designs and enhances SOC infrastructure and integrations with cloud/on-prem environments.
Incident Response & Forensic leadership	Incident Response Lead	Leads incident management during major security events and coordinates responses.
	Digital Forensics Analyst	Conducts forensic investigations into compromised systems and analyzes digital evidence.
Security Analysts	Tier 1 Analyst (Alert Analyst)	Monitors security dashboards and alerts; performs initial triage and alert validation.
	Tier 2 Analyst (Incident Responder)	Investigates escalated alerts; conducts in-depth analysis and containment of incidents.
	Tier 3 Analyst (Threat Hunter/Advanced Incident Responder)	Conducts proactive threat hunting, complex investigations, and major incident responses.
Threat Intelligence and specialist roles	Threat Intelligence Analyst	Tracks emerging threats and adversaries; provides actionable threat intelligence.
	Threat Researcher	Develops deep-dive research into threat actor tactics, techniques, and procedures (TTPs).
	Vulnerability Management Specialist	Scans and remediates vulnerabilities; manages patching and system hardening efforts.
	Penetration Tester/Red Team Member	Conducts simulated attacks to identify weaknesses and provides assessment reports.

Refer to the Microsoft.com ***Security 101*** specification Key roles in a SOC and MITRE's 11 Strategies of a World-Class Cybersecurity Operations Center for further exploration.

Security organization functional architecture

Overview

Extending its ***Security 101*** specifications, Microsoft also provides a set of Security adoption resources on Learn.microsoft.com, which include the ***Security Adoption Framework (SAF)***, the ***Chief Information Security Officer (CISO) workshop*** materials, and more.

Together, these resources provide a ***Modern security blueprint*** for other organizations to follow, including the "**Security Organization Functional architecture**" infographic, adapted for this briefing as shown below.

This depicts how various organizational components come together to manage cybersecurity risks in a large organization, with all pathways ultimately leading to the **Security Operations Center (SOC)** function (on the right side) as the hub (virtual, physical, or combination of both) for operational security.

Key elements of the main functions are summarized below the figure.

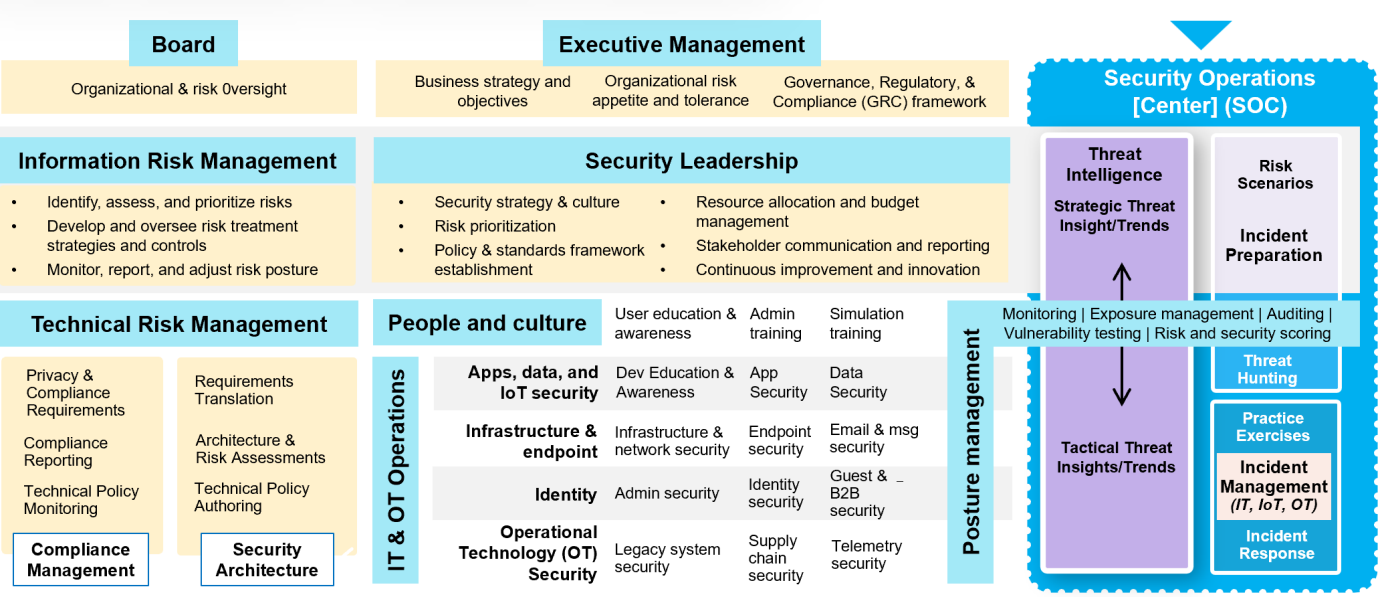


Figure 22 – Security Organization Functional Architecture | Source: Microsoft Security adoption resources

Organizational Leadership

The architecture begins with organizational leadership (**Board** and **Executive management**), which sets the foundation by defining the mission, risk appetite, and alignment of security goals with the broader business model. This layer should drive security strategy at lower levels and provide oversight for risk management and GRC functions, as well as funding approvals (or mandates) for cyber insurance.

Information Risk Management and Leadership

The **Security Leadership** team develops strategy, risk management protocols, and standards to manage Information Risk, including supply chain risks across people, process, and technology. This layer ensures

security aligns with productivity needs and adapts to regulatory and environmental changes, as well as manages budgets and stakeholder communications.

Technical Risk Management

The **Technical Risk Management** function operationalizes security through:

- **Compliance Management**: Ensuring adherence to privacy laws, technical policies, and regulatory requirements.
- **Security Architecture:** Conducting architectural assessments and enforcing technical policies.

People, IT & OT Operations

These functions span multiple domains, including:

- **People Security**: User training and awareness, IT security and admin training, and participation in end-user simulation training, as needed.
- **Apps, Data, and IoT Security**: Secure development and app/data protection.
- **Infrastructure and Endpoints**: Endpoint management, deployment, and mitigation.
- **Identity:** Administrator security and identity governance.
- **Operational Technology (OT):** Securing OT environments critical to operations.

Posture Management: An emerging function driven by cloud-based tools that enable real-time risk discovery, exposure and vulnerability management, auditing, and risk and security scoring. It breaks traditional silos by connecting security operations, compliance, and engineering teams in real time.

Security Operations

At the operational endpoint, the SOC integrates threat intelligence, incident preparation, and incident response/management:

- **Threat Intelligence**: Serves as a "nervous system," providing both tactical and strategic insights. This feedback loop informs leadership and helps SOC teams stay ahead of evolving threats.
- **Incident Preparation:** Builds organizational resilience through practice exercises and real-world scenario planning.
- **Incident response**: Integrates with multiple components of the Security Operations Center (SOC) and IT/OT systems to ensure a comprehensive (and increasingly automated) response to cyber threats with minimal operational disruption.

Impact of AI. Increasingly, these functions are being transformed by further advancements in Generative AI solutions like Security Copilot and other embedded AI enhancements, which we will cover in a later section.

Tiering

Overview

In SOC terminology, "Tiering" is where responsibilities are divided up into a structure that streamlines SOC processes (e.g., alert triage, incident detection and response, etc.) using a cascading set of human and machine filtering "Tiers," representing various levels of granularity and specialization. This is designed to allow the SOC to handle large volumes of alerts and meet defined goals, KPIs and metrics by highly efficient filtering and escalation, as appropriate[7].

When employed, tiering typically starts with a front-end, "intake" layer (commonly referred to as "Tier 1")[8], with the intent to filter out false positives and other "noise" in the system; as well as characterize/classify and qualify incoming threats and alerts and push to the next tier.

This can be depicted as a top-down "funnel" (or left -> right workflow) as shown below from MITRE's 11 Strategies of a World-Class Cybersecurity Operations Center, noting that as information is reduced down at scale in this manner, it relies on automation across the board.

In general, this is typically more "machine-reliant" on the left and "people-reliant" on the right, where major decision making and actions involving other constituencies take place.

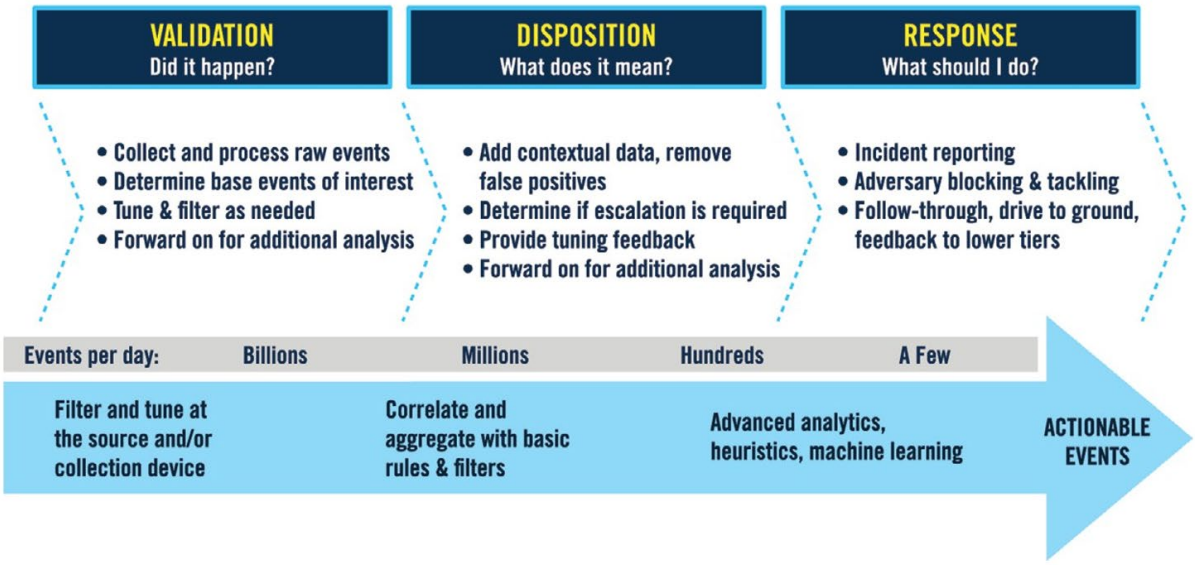


Figure 23 - Basic SOC workflow | MITRE: 11 Strategies of a world class cybersecurity operations center

If Tiering is employed, here is a typical structure:

- **Tier 1:** Security monitoring, alert handling, and triage

[7] In some cases, a SOC tiering structure can also provide a career progression path for analysts to develop and specialize in. Skills combining security and AI expertise are expected to be in high demand moving forward.
[8] In addition, Tier "0" is sometimes used to represent computer automation and systems for additional data collection, monitoring, and alert generation (e.g., a SIEM or XDR solution).

- **Tier 2:** Incident escalation, depth investigation/analysis, correlation, and incident response/remediation.
- **Tier 3**: Threat hunting, advanced analytics/forensics and root-cause analysis.
- **Tier 4:** SOC management

Additional insights

- Some organizations are "Tierless" - not all SOCs are organized into formal "Tiers" of service (or have 4 tiers), with many organized more by function or some combination of tiers and functions, especially when providing MXDR (vs. MSSP)-type services, as discussed further below.
    - *Anecdotally, based on a sampling of data from Microsoft customers enrolled in the Security Copilot preview:*
        - *About 12% were tierless*
        - *Over 85% had no Tier 4*
        - *About 25% were combined across Tiers 1-3 (with no Tier 4), using a so-called "collapsed" tier structure*
        - *About 12% combined Tiers 2 and 3*
        - *About 12% had no Tier 1*
- Many organizations outsource one or more tiers.
    - *Anecdotally, based on a sampling of data from Microsoft customers enrolled in the Security Copilot preview:*
        - *About 12% outsourced Tier 1 and Tier 2 only*
        - *About 25% outsourced Tiers 1 and 2*
        - *None were completely outsourced across all tiers and/or functions*
- Some organizations may supplement the traditional tiering structure with a "Tier 0". This tier might provide proactive, strategic services such as vulnerability assessments, security engineering, threat hunting, continuous improvement efforts, etc.

Tiering with MSSP vs. MXDR service types

As explored further previously in the sections on Service types and Tiering, historically MSSPs and many in-house SOCs have followed a tiered model, performing the types of functions shared above. This hierarchical structure evolved when toolsets were relatively siloed, alerts were less refined, and human analysts had to manually sift through large volumes of data. Escalations through tiers were a way of managing complexity and ensuring that complex investigations reached more skilled staff.

Collapsed tiering

As more and more organizations adopt MXDR-type service models, whether in-house or outsourced, the necessity of rigid, hierarchical tiered structures is reduced. Instead, teams can streamline workflows and collapse multiple tiers into a more unified operational model, resulting in fewer escalation handoffs and a more efficient, integrated threat detection and response cycle.

- *Though anecdotal, the variance from traditional tiering structures is supported in the data from the Security Copilot preview, as shared above.*

Where some form of tiering is maintained and MXDR toolsets are employed, Tier 1 analysts should be able to handle a higher volume of more complex issues with less "scrubbing", and cross-tier teams should likewise be able to handle both triage and deeper investigation tasks, even handling the entire incident lifecycle in some cases. This agility could be crucial to adapting modern SOCs to today's fast-paced threat landscape.

Evolving beyond traditional models

As the industry adopts more MXDR-like platforms and strategies, we see SOC operations transforming.

Instead of relying on escalations through multiple layers, organizations increasingly utilize collaborative pods, advanced tooling, and continuous training to ensure everyone on the team is capable of handling a wide range of scenarios.

This shift reflects the maturity and sophistication of modern detection and response capabilities, which we see enabled by the Modern SOC and Microsoft's unified security approach, as explored in Section 5. Modern SOC I with Microsoft Defender XDR + Sentinel + TI – A unified solution.

Technical reference architecture

Background

The Security Information and Event Management (SIEM) market was formally defined in the mid-2000s and has grown considerably in terms of features and market pervasiveness (most large organizations have some form of a SOC, and most SOCs have some form of a SIEM and/or XDR solution).

In the mid-to-late 2010s, the concept of XDR (Extended Detection and Response) emerged, leading to solutions like Microsoft's Defender XDR.

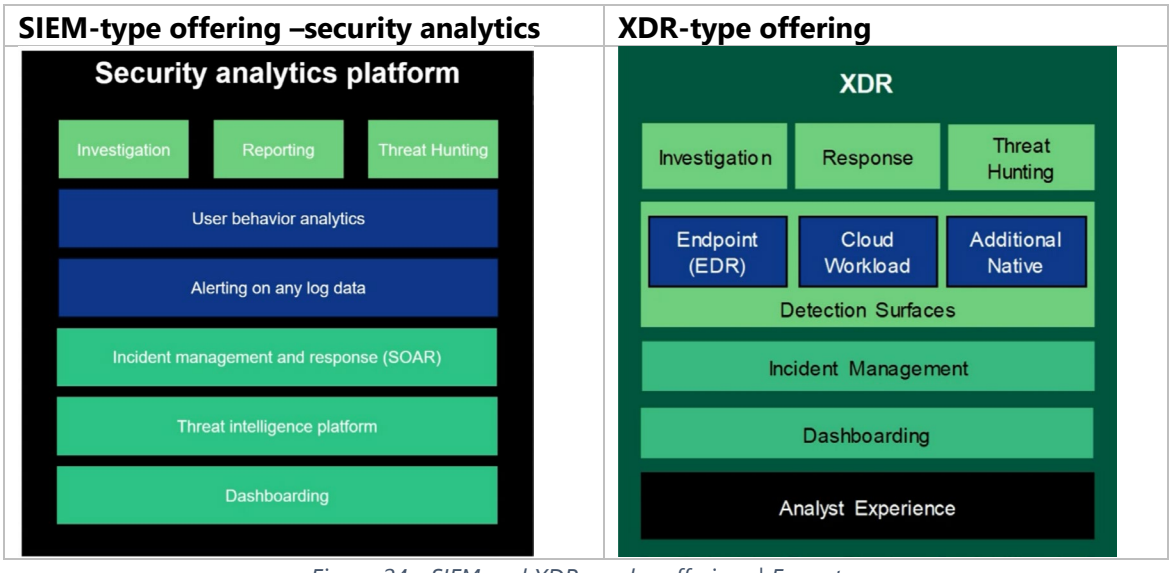


Figure 24 - SIEM and XDR vendor offerings | Forrester

As shown in the above diagram, SIEM and XDR-type solutions have functional similarities and are often integrated into a single solution, which we address below and further in the next section when we cover the Microsoft unified approach that integrates both capability sets.

Modern XDR-SIEM-SOAR-TI architecture

In the early 2020s, customer feedback highlighted the need for a unified platform that integrates SIEM, XDR, SOAR, and TI capabilities, complemented by expert services for everything from strategic planning to ongoing operations and incident response.

While each provider/vendor (like Microsoft) has its own implementation of this architecture, the generalized view shown below provides a sampling of elements typically employed, noting again that the lines can get blurry between the layers in this highly integrated solution space, which is summarized below.

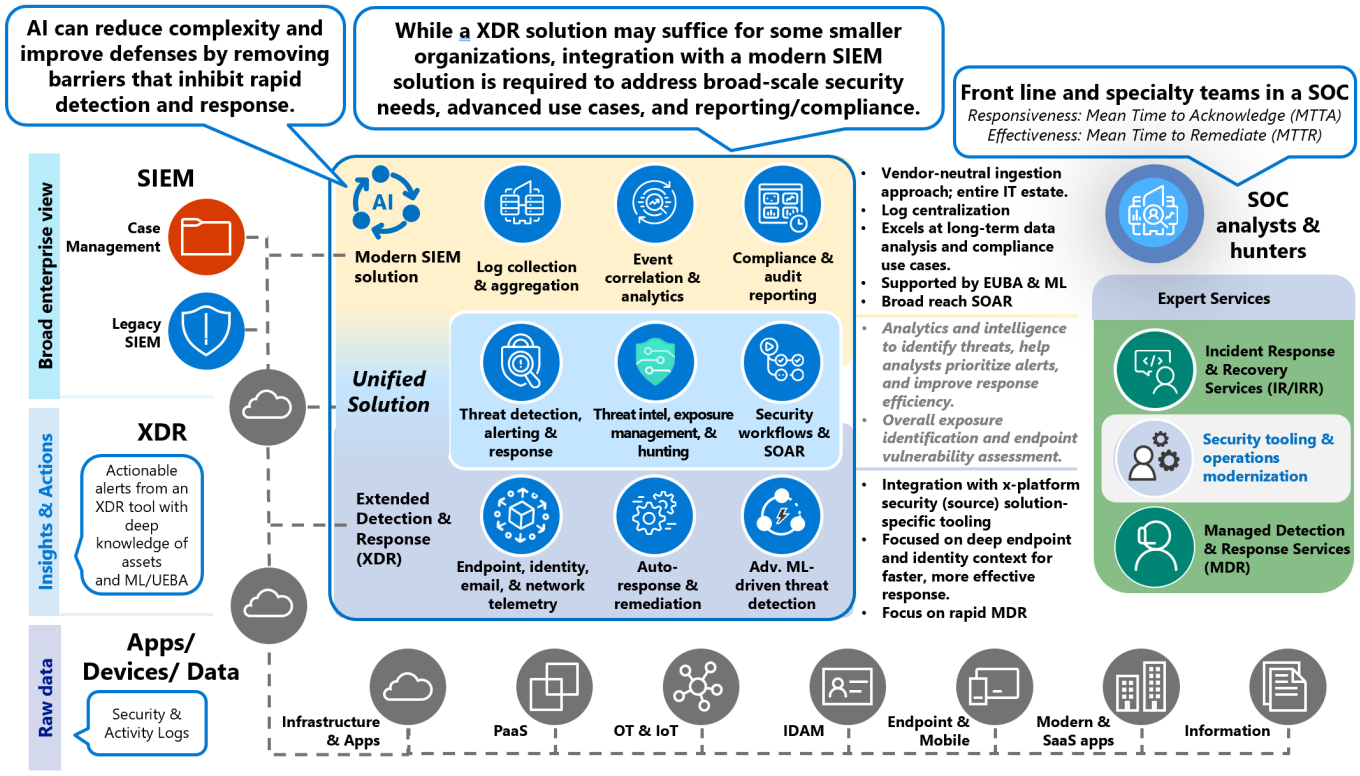


Figure 25 – Modern SOC Technical Reference Architecture

Data sourcing. As shown in the above diagram, access to data/signals is foundational to a modern Security Operations Center (SOC). These data sources typically span an organization's entire digital ecosystem, including networks, infrastructure, platforms, operating systems, mobile devices, modern SaaS applications, and identity and access management systems. This data serves as the cornerstone, providing the input needed to detect and respond effectively to threats.

XDR. Moving up into the XDR level, this is where data is transformed into deep insights through advanced analytics and knowledge of the data types and sources. These insights are actionable, enabling SOC teams

to derive meaningful alerts and prioritize their efforts. XDR of this type also enables SOC teams to correlate activity across silos, ensuring visibility and control over a highly distributed enterprise infrastructure.

SIEM. Next, at the core of the SOC lies the "SIEM" (Security Information and Event Management), which acts as the centralized hub for hunting, investigating, and orchestrating responses. SIEM platforms typically integrate advanced tools like Machine Learning (ML) and User and Entity Behavior Analytics (UEBA).

Commonly integrated capabilities

- **Threat Intelligence (TI)** capabilities typically enable a correlated, enriched view of incidents based on threat intelligence from both internal and third-party sources.
- **Exposure and vulnerability management.** Available at both the SIEM-level as well as for Endpoints (as "Vulnerability management"), provides dashboards of data and associated visualizations/recommendations exposing where exposure and vulnerabilities lie within the customer's network, data, device, identity, application, and cloud estate.
- **SOAR**. SOAR (Security Orchestration, Automation, and Response) functionality is increasingly found in modern SIEM and XDR solutions in various forms. This is sometimes provided through a separate product/platform or built into a core solution (such as Microsoft's unified solution covered in the next section), providing operational efficiency through automation, which reduces analyst effort and increases SOC capacity to handle incidents at scale.

Expert assistance. Leveraging the tools listed as part of the Modern SOC Reference architecture pictured and referenced above, several specialized functions are often employed by organizations to address the problem space.

These include "**Managed Detection and Response**" (**MDR**) and "**Incident Response and Recovery**" (**IR/IRR**) services, defined briefly below, noting that these functions can be executed entirely in-house, outsourced to third-party providers, or implemented as a hybrid model combining internal and external resources to fulfill the needs of the organization.

- **Managed Detection and Response (MDR)** refers to the continuous function of detecting, analyzing, and responding to cybersecurity threats using a combination of advanced tools, processes, and expertise.
- **Incident Response and Recovery (IRR)** involves the structured, reactive management of specific security incidents, focusing on containment, investigation, remediation, and recovery to minimize impact and prevent recurrence.

In addition, another key component is that of modernizing and maintaining the security architecture/infrastructure, where in-house engineering supplemented with 3rd party resources is typically employed.

In summary, by combining raw data, actionable insights, advanced tools, and expert collaboration, this architecture - staffed with the right resources (and supplemented with outside expert assistance), can help organizations stay ahead of evolving cybersecurity threats.

Pain points

Top pain points (sampling)

1. **Legacy infrastructure and technical debt**
2. **Proliferation of endpoints, data, and shadow IT (including AI)**
3. **# and cost of disparate security solutions (as well as visibility and correlation across solutions)**
4. **Increased threats (# and types)**
5. **Talent/skill shortages**
6. **Regulations and fines**
7. **Vendor churn due to M&A**
8. **Roles, responsibilities, and communication paths (not well-defined)**
9. **Lack of simulation training (e.g., "Tabletop exercises")**
10. **Lack of automation for repetitive tasks**

References:

- Microsoft Digital Defense Report (MDDR, 2024)
- MDDR 2024 companion Executive Summary for CISOs
- Foundry study highlights the benefits of a unified security platform in new e-book | Microsoft Security Blog
    - E-book The unified security platform era is here.

Based on the findings highlighted in the Microsoft 2024 MDDR report and the December 2024 "Foundry study" cited above, we continued to see cybersecurity teams operating at their limits over the last period,

with organizations continuing to face staffing constraints, escalating regulatory compliance demands, and an ever-growing number of increasingly sophisticated adversaries.

On top of the major cyber trends noted earlier in this briefing (Cyber threat summary), other notable pain points are summarized below for reference:

- **Cost pressures**. Organizations are being asked to "do more with less" - cutting costs across the board, putting pressure in CISOs and other executives to minimize costs, regardless of the growing threats and cost of talent they are facing.
- **Too many security platforms and applications**. With mergers, acquisitions, and global expansion over time, the number of security platforms, applications and tooling for the average organization has become unmanageable and costly, especially when "Best of breed" (vs. "Best of suite") is pursued. As cited in the Foundry Study referenced above, survey respondents reported:
    - Use of more than 14 security tools on average, with 21% using more than 20.
    - 35% increase in the number of tools over the past year.

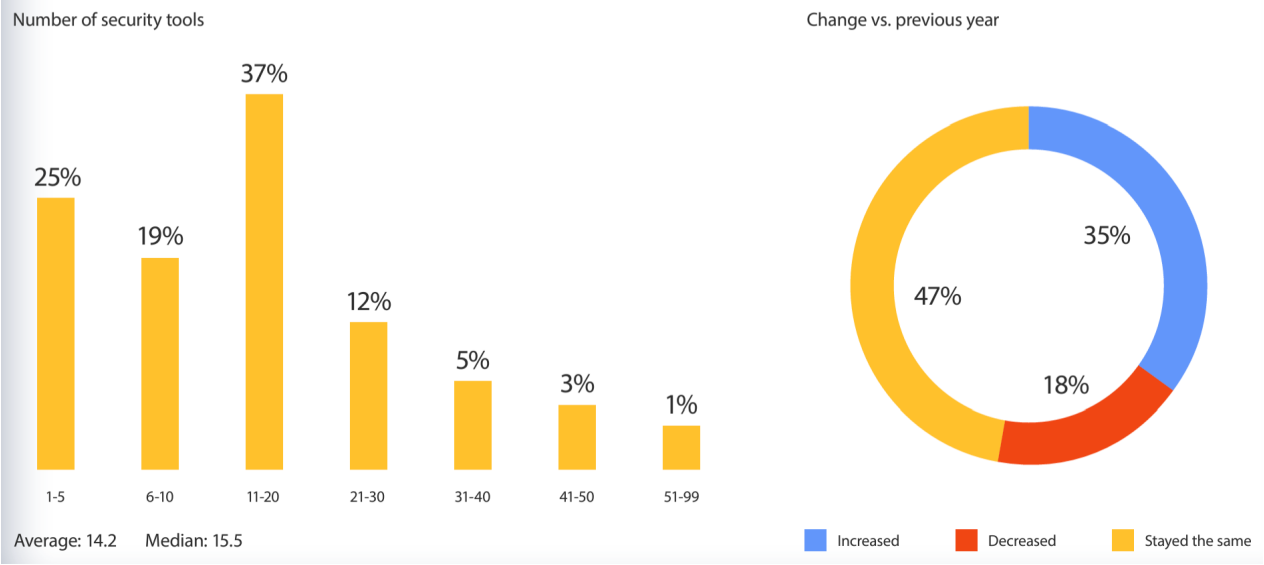


Figure 26 - Increased in number of security tools in use | Foundry Study

With this expanding ecosystem of tools, survey respondents cited the following challenges:

- Complexity of the current environment
- Poor visibility across the landscape
- Higher average number of security incidents (15.3 incidents, vs. 10.5 incidents for organizations with fewer tools)

These challenges speak directly to rapidly expanding IT environments and the growing set of security tools used to protect them.

- **Expensive and inflexible legacy solutions.** Especially with on-premises solutions, many organizations face prohibitive costs to scale their SOC operations, especially for global, complex firms and public sector entities.
- **Technical debt.** Another pain point for many organizations, as highlighted in the MDDR 2024 companion Executive Summary for CISOs, is that of unaddressed technical debt, outdated security controls, and shadow IT.
    - As part of Microsoft's own ***Secure Futures Initiative*** (SFI)[9], Microsoft embarked on rigorous "spring cleaning" to strengthen our environment and cloud services against threats. We removed millions of unused and non-compliant applications and tenants from our environment, refreshed hundreds of thousands of credentials (including security certificates), and segmented and isolated our network.
    - We are also taking proactive steps to keep security deficits from re-accumulating (see MDDR 2024 Executive Summary for CISOs article for details), and in all cases, we're creating "paved paths" for engineers that make the right way to secure something the easiest way.
- **Endpoints and data to manage.** More endpoints to secure and extensive amounts of data to manage.
- **Increased threats**. As highlighted previously from the Microsoft Digital Defense Report 2024 (MDDR 2024), SOCs are facing increased threats from known and emerging actors around the world, putting organizations, users, and devices at risk, with over 345 million cybercriminal and nation state attacks per day.

  As cited in the Foundry Study referenced above, the increasingly complex digital business environment is fueling the threat landscape and putting more pressure on SecOps teams, with 139 out of 156 survey respondents citing Ransomware as one of their top 3 concerns moving forward:

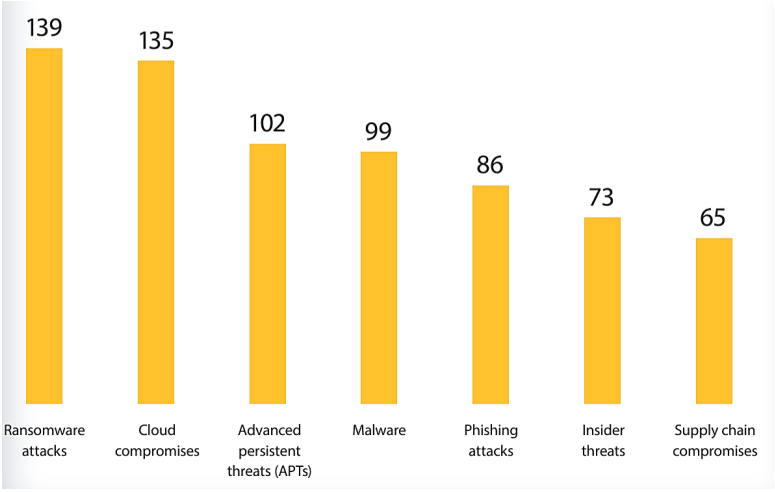


Figure 27 - Inclusion of attack vector in Top 3 list of concerns | Foundry Study

[9] SFI is a multiyear initiative to evolve the way we design, build, test, and operate our products and services so we can achieve the highest possible standards for security.

- **Usage of AI by attackers.** In addition, we are just beginning to see the impact of AI on the cybercrime ecosystem, where nefarious actors are likely to leverage generative AI for malicious activities increasingly in the future.

  Bad actors are not only utilizing cloud scale public AI but also creating their own AI platforms - it's an arms race.

- **Lack of automation for repetitive tasks**. Despite the availability of modern solutions with automated tooling, many organizations continue to struggle with manual processing and repetitive tasks, indicating a need for further business process refinement and alignment with newly emerging advanced SOC technical capabilities.

- **Talent shortage**. The cybersecurity skills shortage has been consistently cited as a persistent challenge for CISOs and their teams for years. As is commonly stated, the cybersecurity industry is facing a critical shortage of professionals with the skills necessary to work in SOCs, with the gap growing as the frequency and complexity of cyber incidents increase.

  On the somewhat positive side, the Foundry Study cited above shows some contrary evidence to this perennial condition.

How organizations are addressing staffing challenges (Source: Foundry Study)

- Many respondents (62%) say they have no open positions, with staff resources allocated evenly across detection, response, and prevention roles.
- Those that are looking to hire cite high competition for the best talent as the biggest challenge in filling security roles (I.e., if CISOs have the budget to fill open positions, they may have trouble finding suitable candidates).

Impact of AI

AI and automation are the top way organizations address staffing challenges, cited by 56% of respondents.

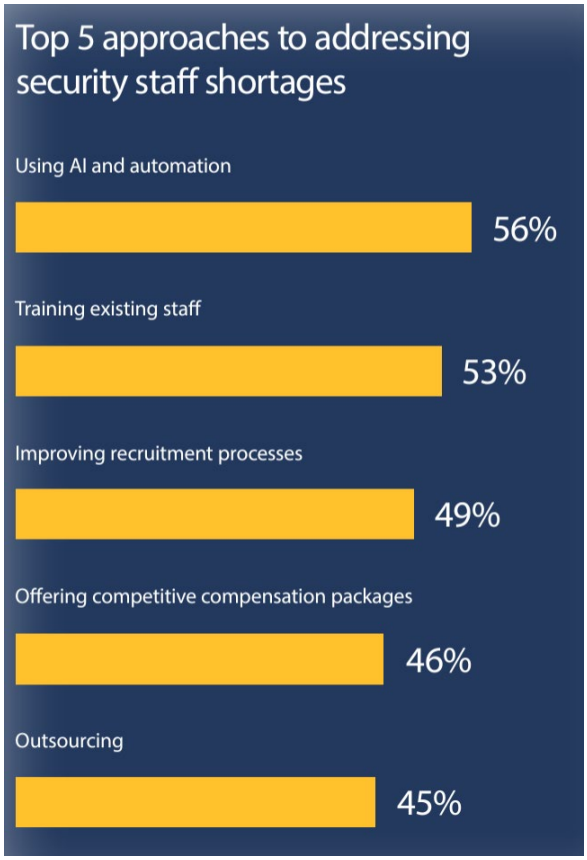


Figure 28 - Approaches to address staffing needs - Foundry Study

Also on the positive side, universities and other institutions are increasingly providing cyber security curricula and hands-on SOC experience, which points to this gap being at least partially addressed over time.

  - A great example of positive movement here can be found with this story about Microsoft and Oregon State University: Microsoft Customer Story-Oregon State University protects vital research and sensitive data with Microsoft Sentinel and Microsoft Defender.

- **Roles, responsibilities, and communication paths**. Microsoft incident response (IR) teams have found that many organizations have unclear (and/or not well-communicated) roles, responsibilities, and reporting lines, which impacts the collective ability to investigate and respond to threats. This includes alignment and communications with in-house legal teams and outside legal or regulatory stakeholders.
- **Lack of advanced simulation training**. Some SOCs report a need to do deeper level simulation training and "tabletop" exercises to equip individuals with the skills and knowledge to handle new and emerging incident types, identifying areas of needed improvement along the way.
- **Increasing regulations and compliance requirements related to AI**. An increasing array of emerging laws will build on existing compliance requirements and further restrict the governance of AI administration and usage in SOCs.

See also: Cyber Trends Summary in the 2nd section of this briefing.

5. Modern SOC I with Microsoft Defender XDR + Sentinel + TI – A unified solution

Reference:

AI-Powered Security Operations Platform | Microsoft Security

Overview

Unified within a single Defender portal experience, **Microsoft Defender XDR and Sentinel** offer an industry-leading set of integrated security features that address the end-to-end set of capabilities laid out

in the previous section. They handle signals, events, and incidents from both first-party sources (e.g., Defender and Purview) and on-premises or third-party security and cloud infrastructures.

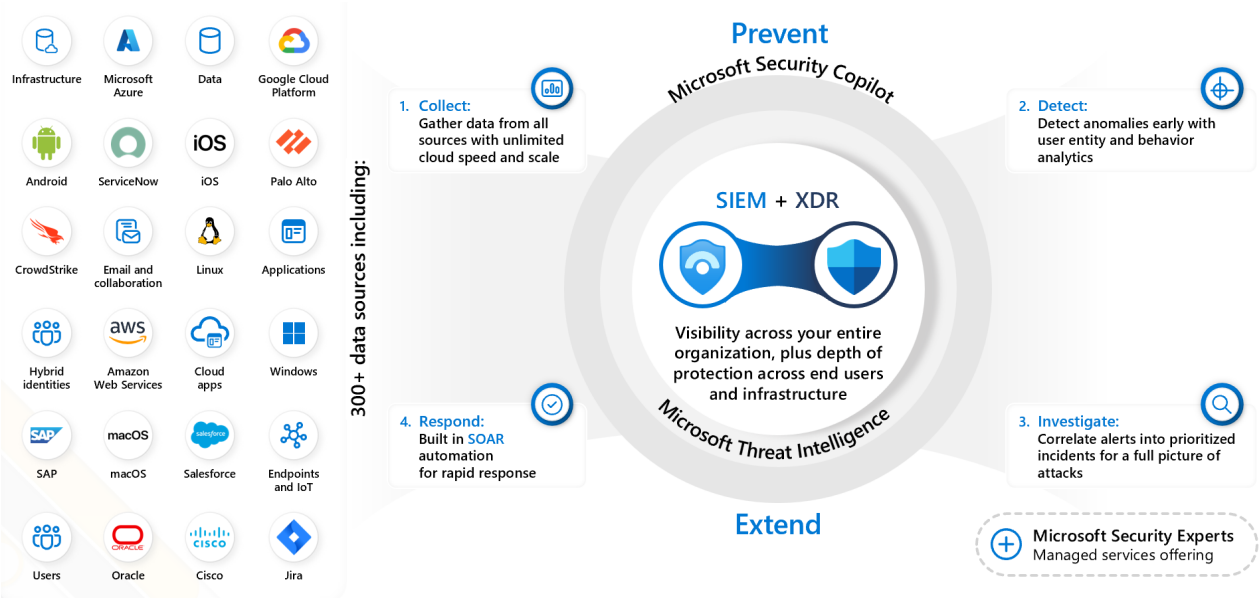


Figure 29 - Modern Defender portal with Microsoft Defender XDR and Sentinel

This unified toolset combines the principal feature sets of XDR, SIEM, SOAR, TI, and AI, allowing Security Operations Center (SOC) personnel to:

- **Aggregate and normalize data** from various IT and operational technology (OT) environments
- **Proactively assess exposure and vulnerabilities** from across the estate (at the SIEM level via "*Exposure Management*" and at the Endpoint level under "*Vulnerability Management*")
- **Perform proactive advanced "hunting"** to seek out (and take action on) undetected threats and malicious behaviors
- **Identify and investigate** security events of interest
- **Support manual and automated response actions**
- **Document and report** on current and historical security events

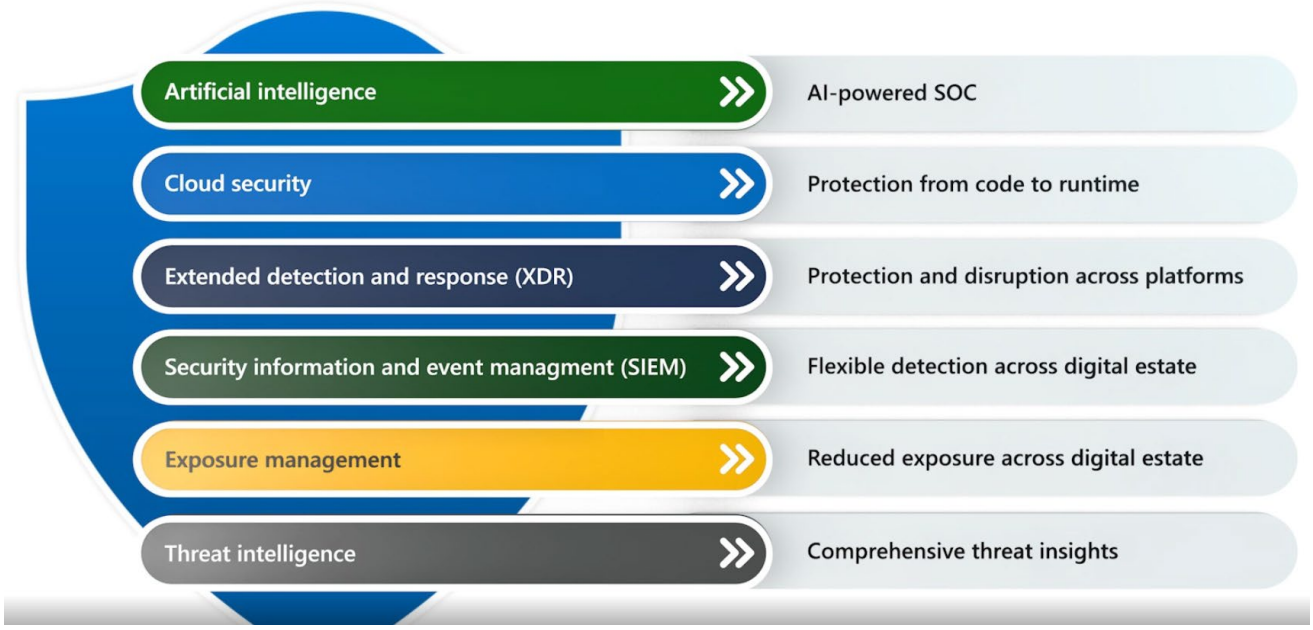


Figure 30 - Primary functions of the Microsoft Unified security solution

For further exploration of how the unified solution set applies across various SOC tiers and functions, refer to the next section below - Unified solution usage across SOC functions.

Features available in the unified Microsoft Defender portal

In the combined Sentinel-Defender XDR solution, the Microsoft Defender portal provides the following navigational elements for various members of the SOC team to manage their day-to-day workflows:

- **Home** (dashboards, guidance, and navigational aids)

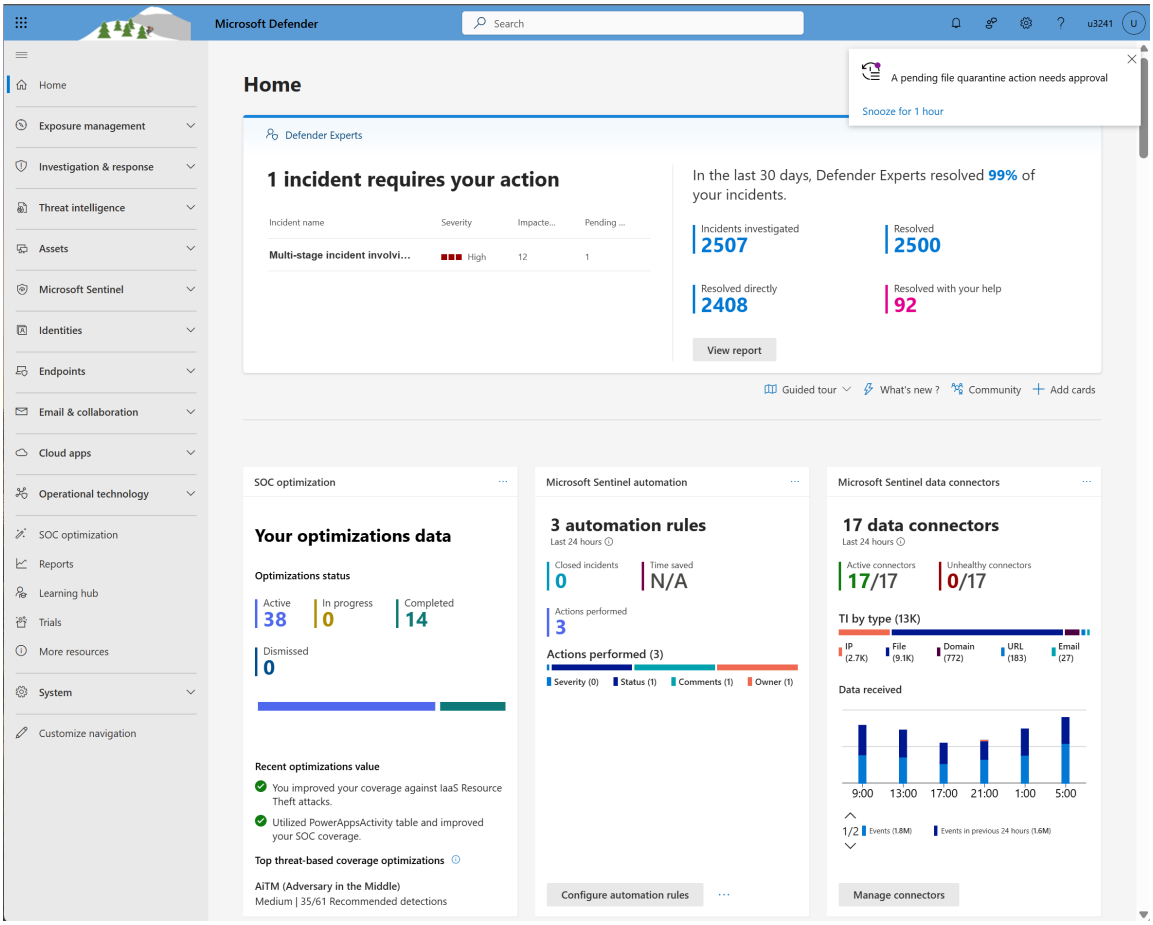


Figure 31 - Microsoft Defender Portal - Unified experience

- **Exposure management** (Attack surface*, Exposure insights**, Secure score, Data connectors)
  **Map, Attack paths*
  ***Initiatives, Metrics, Recommendations, Events*
- **Investigation and response** (Incidents and alerts*, Hunting**, Actions & submissions***, Partner catalog****)
  **Incidents and alerts*
  ***Advanced hunting, Customer detection rules*
  ****Action center, submissions*
  *****Technology partners, Professional services*
- **Threat intelligence** (Threat analytics, Intel profiles, Intel explorer, Intel projects)
- **Assets** (Devices, Identities)
- **Microsoft Sentinel** (Search, Threat management*, Content management**, Configuration***)
  **Workbooks, Hunting, Notebooks (Jupyter), Threat Intelligence, MITRE ATT&CK*
  ***Content Hub, Repositories, Community*
  ****Data Connectors, Analytics, Summary Roles, Watchlist, Automation*
- **Identities** (Dashboard, Health issues, Tools)

- **Endpoints** (Vulnerability management*, Partners and APIs, Configuration management)
  **Dashboard, Recommendations, Remediation, Inventories, Weaknesses,, Event timelines, and Baselines assessment*
- **Email and collaboration** (Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules)
- **Cloud apps** (Cloud discovery, Cloud app catalog, OAuth apps, App governance, Files, Activity log, Governance log, Policies)
- **Operational technology** (Site security)
- **SOC optimization**
- **Reports**
- **Learning hub**

Clarifying Defender XDR and Sentinel roles in the unified solution

At a high level, the **Microsoft Defender XDR** part of the unified solution provides integrated threat detection and response across ***Microsoft*** products (across multiple platforms in some cases)[10], consolidating alerts and incidents from Microsoft Defender components—such as Defender for Endpoint, Defender for Office 365, Defender for Identity, Defender for Cloud, and Defender for Cloud Apps.

The **Microsoft Sentinel** part of the unified solution, on the other hand, provides SIEM and advanced SOAR capabilities capable of ingesting and analyzing large amounts of data from a wide range of sources, including third-party and on-premises systems. From there it provides advanced analytics, threat intelligence, and the ability to create custom detection rules, giving organizations broader visibility and control over their entire security landscape.

In summary, the primary differentiator between the two lies in the scope of data they handle:

- **Defender XDR** focuses on integrating and responding to threats (mostly) within Microsoft's suite of security products.
- **Microsoft Sentinel** extends this capability by ingesting logs and alerts from non-Microsoft solutions, offering a more expansive view of an organization's security posture.

Reference architecture

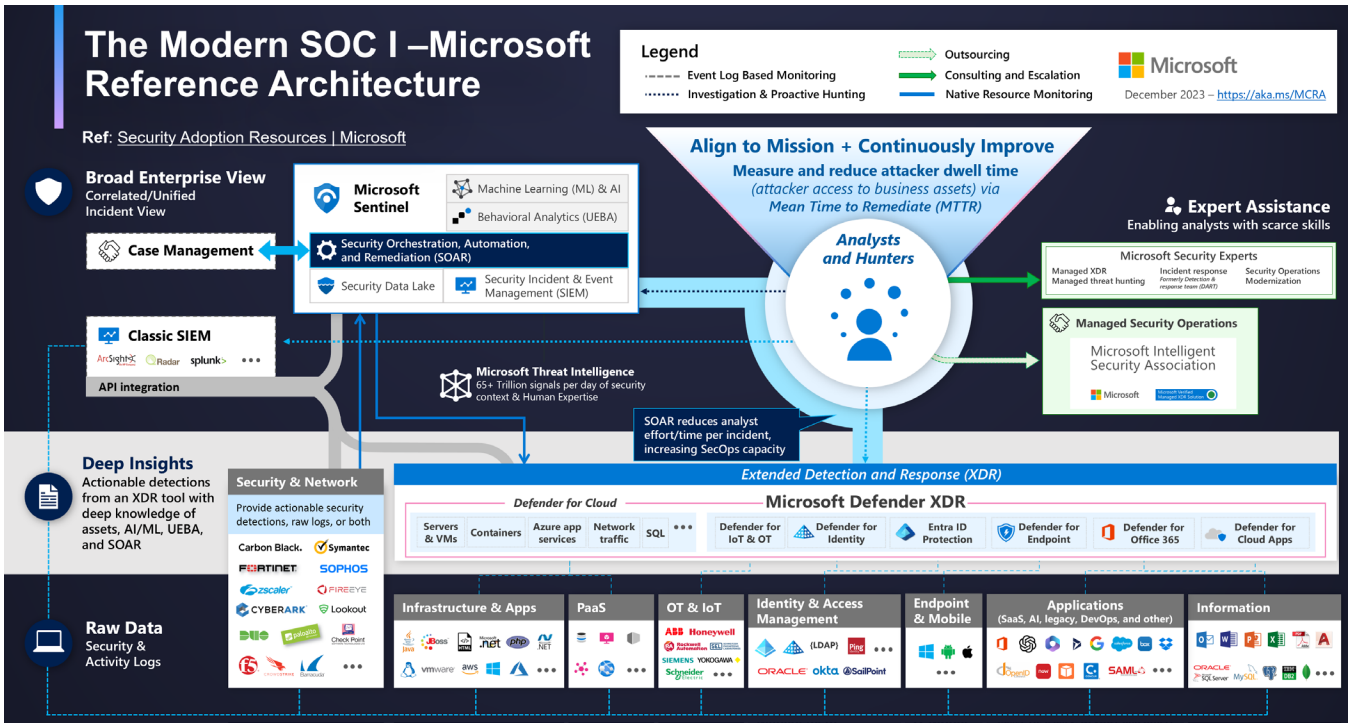
For a deeper level exploration of the unified solution architecture (and many other aspects of security operations), refer to the latest reference architecture documentation published on Security Adoption Resources | Microsoft and other Microsoft resources.

Excerpted from those materials, the infographic shown below shows how data flows through the various elements of the Unified solution, starting with data sourced from numerous apps and services,, consumed and processed by Defender XDR, and then integrated with other sources in Microsoft Sentinel,

[10] Notably, products like Microsoft Defender for Endpoint run on a number of non-Microsoft device types and operating systems.

complemented by other value-add features and services.

This aligns with the Modern SOC Technical Reference Architecture showcased in the previous section.



- *Figure 32 – Modern XDR-SIEM-SOAR-TI architecture with the Microsoft Unified solution*[11]

By integrating Defender XDR with Sentinel in the Defender Portal, organizations benefit from a unified experience that combines the depth of XDR with the breadth of SIEM.

This allows security teams to detect, investigate, and respond to threats more efficiently across their entire environment.

Unified solution usage across SOC functions

In the previous section, we explored SOC types/operating models and associated "Service types" and "Tiering models" employed in SOC operations, either provided in-house, outsourced (as MSSP and/or MXDR services), or a mix of the two.

In the section on Tiering we distinguished between the relevance of rigid, hierarchical tiering with traditional MSSP-type approaches and more modern MXDR service provider models, respectively, noting that in a modern SOC – including that enabled by Microsoft unified solution tooling, new teaming models enabled by "collapsed tiering" are being promoted where a multi-skilled team can handle what used to be multiple tiers of triage and investigation.

[11] Source: Microsoft Security adoption resources

Here, in the table shared below, we show how several SOC functions may cross tiers and leverage different feature sets from unified Defender XDR + Sentinel solution, as well as distinguish between basic and advanced service types for each.

This is expected to be further impacted by the introduction of Generative AI (i.e., Security Copilot) in the SOC, which we cover in the next section, so we provide this here for reference.

Focus Area	Tier mapping	Baseline services	Advanced Functions	Unified solution coverage
1. Security tooling & operations maturity & workflow integration	**Tier 0**: • Process design, workflow automation, and continuous improvement efforts • Part of the proactive strategic foundation	• Ongoing security posture management • Assistance with SIEM tuning and tool configuration	Streamlined integrated workflows across multiple security capability domains (see MITRE capability model coverage)	• Microsoft Defender XDR and Sentinel's unified toolset provides a central control plane for policy management, automated workflows, and continuous improvement. • Investments in Sentinel data source integration and optimization reduce complexity and improve Tier 1 and 2 efficiencies.
Comments: • Often involves security engineering, integration, and platform maintenance.				
2. Infrastructure & monitoring coverage	**Tier 1** - Basic alert monitoring, device health checks, and frontline triage	• 24/7 security Monitoring • Includes traditional security infrastructure monitoring (e.g., firewalls, IDS/IPS, VPNs)	Integrated endpoint, network, and cloud telemetry analysis	• Microsoft Defender XDR and Microsoft Sentinel natively integrate endpoint, network, and cloud data streams, providing unified visibility. • Threat intelligence feeds in Sentinel enrich alerts, enabling quick correlation and more comprehensive coverage.
Comments: • This category can also touch on Tier 0 if we consider proactive configuration hardening and vulnerability scanning. • In general, it primarily aligns with lower-level tiers (Tier 1) for day-to-day monitoring, but some underlying activities (like baseline configurations and preventive measures) might be considered Tier 0.				
3. Threat detection & alerting	**Tier 1**: Initial alert reviews and triage **Tier 2:** Contextual alert correlation	• Basic alerting and log aggregation • Initial alert triage and correlation	Proactive detection of advanced threats	• Microsoft Defender XDR's advanced behavioral analytics and Microsoft Sentinel's automated incident correlation enable rapid detection and prioritization of complex threats.

Focus Area	Tier mapping	Baseline services	Advanced Functions	Unified solution coverage
				• Built-in threat intelligence and ML-driven rules in Sentinel reduce noise and enhance overall detection accuracy.
Comments: • Overall, this area starts at Tier 1 (basic alert handling) and can escalate to Tier 2 for more complex analysis or fine-tuning detections.				
4. Analytics & intelligence integration	**Tier 2**: In-depth analysis incorporating threat intelligence to refine detection logic and identify patterns **Tier 3**: Complex analytics involving advanced skills (e.g., KQL) for intelligence-based threat hunting	Review of threat intelligence feeds	• Behavioral analytics and machine learning for advanced threat detection • Identification of subtle attack patterns	• Combined use of Microsoft Defender XDR with Sentinel's built-in threat intelligence and ML-driven analytics • Pre-built detection rules and continuous analytics improve the quality and speed of detection across the entire SOC ecosystem.
Comments: • For threat hunts and intelligence gathering, the build-out of predictive analytics models or proactive threat intel ingestion and/or enrichment could also be considered Tier 0.				
5. Incident response & remediation	**Tier 2:** In-depth incident analysis and remediation. **Tier 3:** Complex incident remediation and management	• Vulnerability assessments • Incident notifications and escalation	Guided or automated remediation actions (e.g., isolating endpoints, blocking malicious domains)	• Microsoft Defender XDR and Sentinel together support automated response playbooks and direct endpoint isolation. • SOAR capabilities in Sentinel orchestrate rapid containment and remediation, reducing mean-time-to-respond and minimizing attacker dwell time.
Comments: • Incident response can span from Tier 2 (initial containment) to Tier 3 (complex, high-impact incidents), • Tier 0 involved where incident response runbooks and playbooks are developed proactively.				
6. Investigation & forensic depth	**Tier 3**: Forensic investigations, root-cause analysis, and deep threat hunting	• Implementation and maintenance of policy enforcement and	In-depth forensic analysis and root-cause investigations	• Microsoft Defender's rich endpoint telemetry, combined with Sentinel's powerful search and investigation queries (KQL), facilitate deep forensic

Focus Area	Tier mapping	Baseline services	Advanced Functions	Unified solution coverage
		configuration best practices • Response to known threat signatures and patterns		analysis and retrospective threat hunting. • This integrated approach rapidly pinpoints root causes and supports thorough incident post-mortems.
Comments: • Often handled by the highest-skilled analysts with specialized training. • Any proactive forensic readiness or tool preparation might be considered Tier 0 (e.g., ensuring forensic tools and processes are in place before an incident).				

For a summary of the impacts of the Microsoft unified security solution, refer to the section on Impacts.

Zero Trust dependencies and alignment

References:

- New Microsoft guidance for the CISA Zero Trust Maturity Model | Microsoft Security Blog
- Configure Microsoft cloud services for the CISA Zero Trust Maturity Model | Microsoft Learn

Overview

Following the April 2024 release of its Microsoft guidance for the Department of Defense Zero Trust Strategy. Microsoft released its Microsoft Guidance for CISA Zero Trust Maturity Model in December 2024.

This guidance for achieving CISA ZT standards (using Microsoft security technologies) is designed to help government agencies and other large organizations evaluate and progress their Microsoft cloud services security maturity, including that related to SOC modernization initiatives.

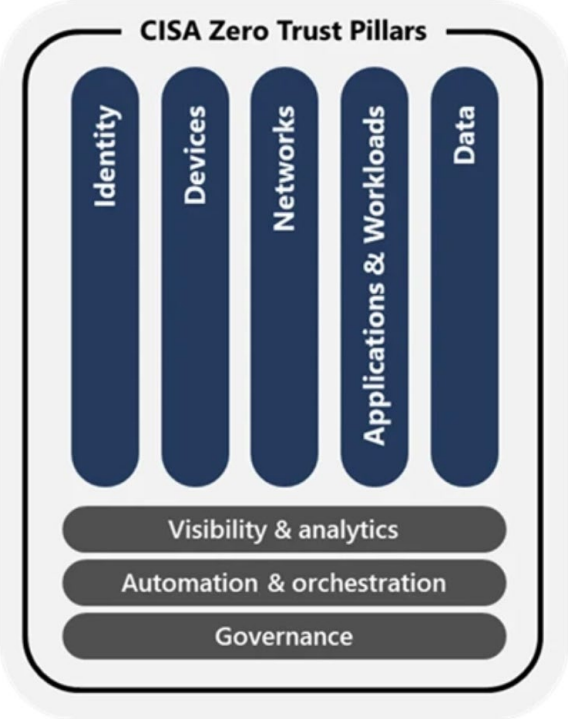


Figure 33 - CISA Zero Trust Maturity Model

The CISA Zero Trust Maturity Model includes **five pillars** that represent protection areas for Zero Trust, along with 3 cross-pillar capabilities and a maturity progression scale of "Traditional, Initial, Advanced, and Optimal", as shown below:

Pillars:

- **Identity**: Unique attributes defining users or entities (including non-person) within an agency.
- **Devices:** Any hardware, software, or firmware-based asset that connects to a network (e.g., servers, desktops, laptops, printers, mobile and IoT devices).
- **Networks**: All communication channels, from internal and wireless networks to the internet, cellular, and application-level pathways.
- **Applications & Workloads**: Systems, programs, and services running on-premises, mobile, or cloud environments.
- **Data**: All structured and unstructured information, wherever it resides, including backups and associated metadata.

Cross-Pillar Capabilities:

- **Visibility & Analytics**: Unified insights and monitoring across all pillars.
- **Automation & Orchestration**: Streamlined, automatic control and enforcement of policies and processes.
- **Governance:** Centralized oversight ensuring alignment with organizational goals and compliance requirements.

Maturity

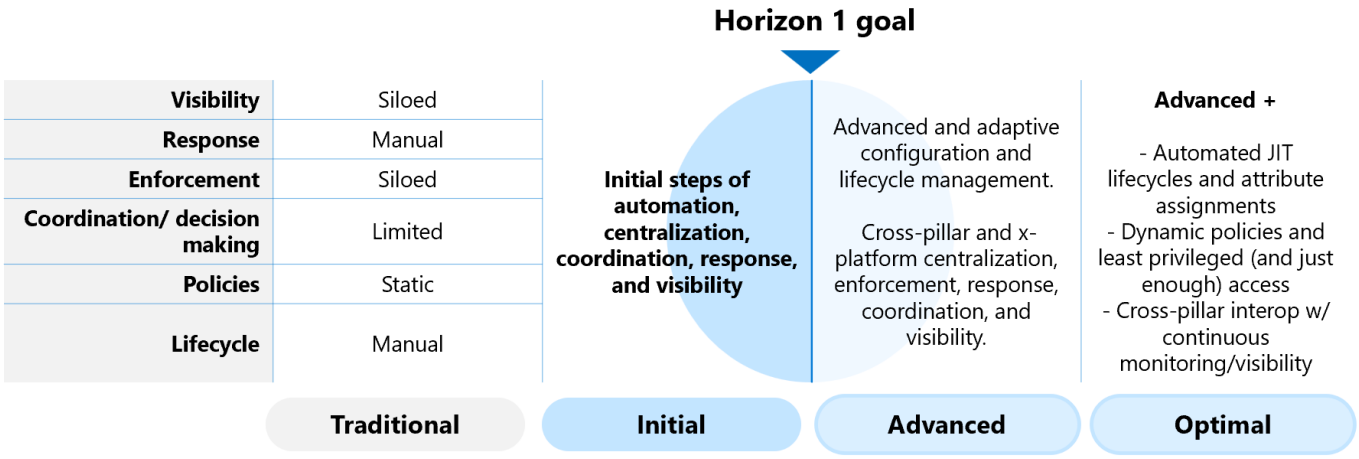


Figure 34 - CISA Zero Trust Maturity Model

While it's possible to implement Microsoft's Unified Defender XDR and Sentinel solutions at early stages of Zero Trust maturity, having at least a foundational ("Initial") level of competence in Identity, Devices, Networks, Applications/Workloads, and Data is generally a prerequisite for meaningful results.

As organizations progress toward more mature ("Advanced" and "Optimal") Zero Trust postures—bolstered by strong Visibility and Analytics, Automation and Orchestration, and Governance capabilities—they create a more robust foundation for integrating and fully leveraging Defender XDR and Sentinel.

The CISA Zero Trust Maturity Model, as referenced by Microsoft, thus provides a useful standard and roadmap for understanding the dependencies and readiness levels that support successful unified XDR and SIEM deployments.

What's new and coming – Unified platform

Reference: Ignite '24 – "Simplify your SOC" – Rob Lefferts

Category	What's new or coming
Prevent	Critical assets and attack paths from exposure management
	Privileged identities and privileged access management integration
Detect	LLM-based BEC detections
	Threat classifications
	Insider risk management in the SOC
	Third-party network signal in unified device timeline
Respond	Cloud detection and response capabilities
	TI-based disruption features across XDR (including TITAN)
Platform level	One platform, one agent

	Unified platform available to Sentinel and Government Cloud customers

Impacts

Measuring impacts of Unified tooling and improved operations for the Modern SOC

Top potential impacts from the Unified Microsoft Defender and Sentinel solution

1. **Percent of incidents avoided due to proactive threat hunting and vulnerability management**
2. **Shorter detection and response times**
3. **Lower number, lower cost and impact per incident and breach**
4. **Lower regulatory fines, personnel, and SOC costs**
5. **Higher team and management efficiency**
6. **Impacts on target SOC capabilities over time**

Overview

To set the stage for the next section on the promise of AI-enabled SOC operations, we first establish the key KPIs, goals, and metrics that are most relevant to accountable roles such as the CISO and other SOC members. We also introduce a standard "SOC capability model" as a framework for assessing the current state, defining a desired future state, and prioritizing strategic actions to address identified gaps. This model will later be revisited to evaluate the potential impacts of AI on specific elements within the capability model..

Impact on KPIs, Goals and Metrics

The ability to impact at least some of the goals and metrics listed below will be a key part of any business case for moving to the unified Microsoft Defender and Sentinel solution, as well as any additional investment in AI (specific to SOC operations).

- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)
- Number of vulnerabilities identified and eradicated per month (incident avoidance)
- Number of security incidents per month
- Cost per incident

- Percentage of incidents discarded, escalated, and remediated.
- Cost of security breach
- Compliance audit scores
- Compliance-related regulatory fines (per year)
- SOC team efficiency (technical and management)
- Yearly capital and operating costs
- Per-tier staffing (headcount, costs)
- Per-tier time-to-competency (for those new to role)
- Business value
- ***Capability impacts*** (see next section)

The Forrester TEI study The Total Economic Impact™ Of Microsoft Sentinel provides a good reference documenting the impact that the unified platform has on many of these metrics (as well as others) based on research carried out with a number of Microsoft customers.

Impact on capabilities

Capability models are commonly used as a mechanism to assess current state/desired future state and define a strategic course of action over time to address a prioritized set of identified gaps.

For the purposes of this briefing, the MITRE SOC capability model highlighted in the 11 Strategies of a World-Class Cybersecurity Operations Center article provides a referenceable example[12] of a structured framework for evaluating and advancing SOC performance, refactored in the figure below..

Here, the MITRE list of Level 1 and 2 SOC capabilities are re-oriented with the areas of highest potential benefit from SOC modernization (using Microsoft Unified security solutions) highlighted with the **dark green** border.

[12] SOC-CMM provides another referenceable framework that includes maturity assessment and report out tooling that may also be useful in strategic planning work of this type. This also provides an option to use NIST CSF scoring that may be useful.

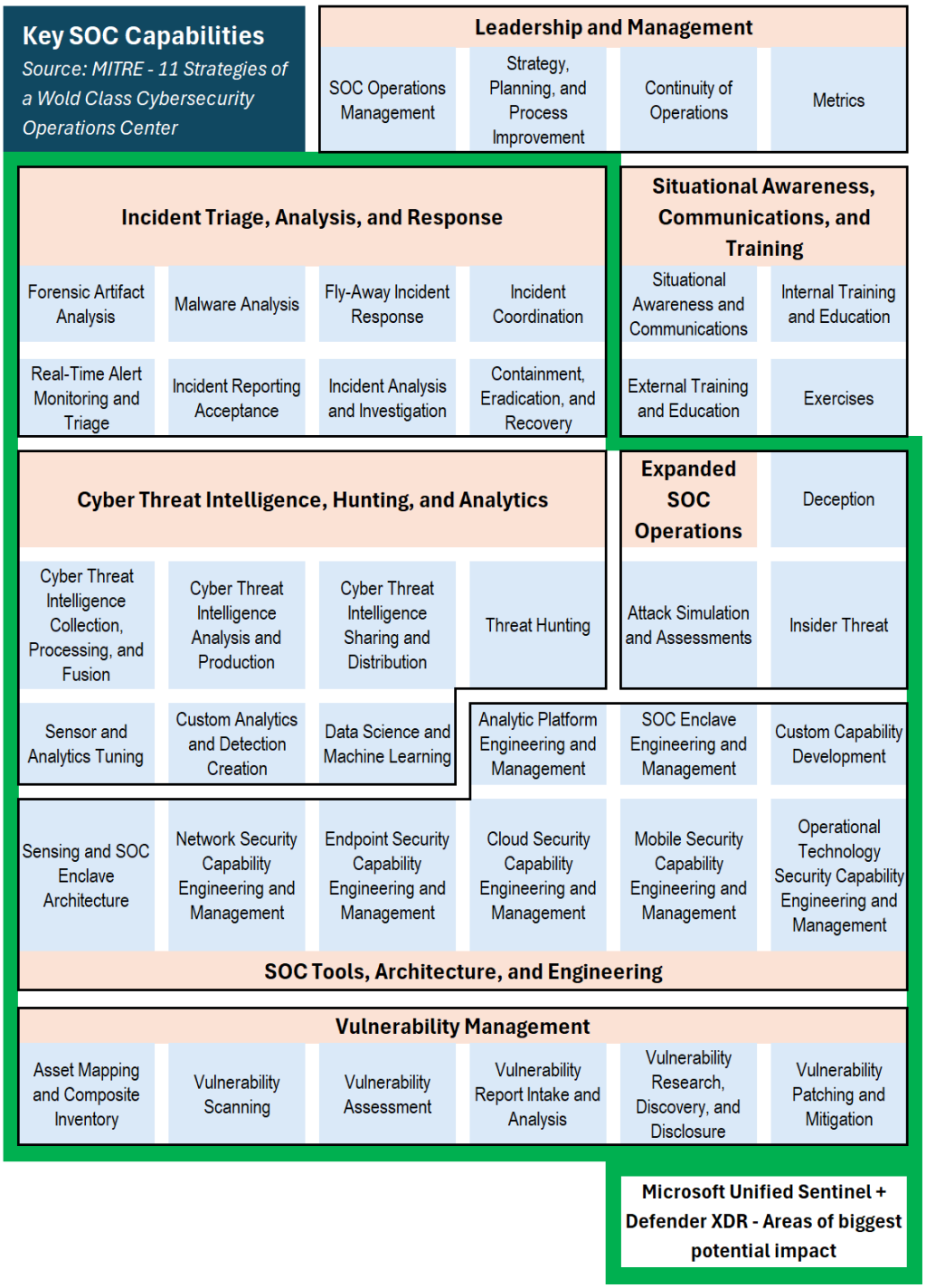


Figure 35 - Key SOC Capabilities – MITRE

While somewhat of a coarse grouping, this set of capabilities – or a subset of them - can be used as a baseline for looking at both shorter-term investments in Microsoft's Unified platform – i.e., Defender XDR and Sentinel, as well as longer-term potential capability benefits of layering in more advanced capabilities like Security Copilot, covered in the next section.

KPIs, goals and metrics vs. capabilities

When approaching SOC modernization, KPIs and metrics offer tactical insights into current performance, while capability modeling provides a long-term strategic framework for aligning SOC operations with maturity goals. Organizations often benefit from employing both, and Microsoft Industry Solutions supports integrating these approaches into strategic SOC planning.

Key distinctions include:

- **Broader context**: Metrics track current performance, while capability models (e.g., MITRE, SOC-CMM) offer a roadmap for incremental maturity aligned with strategic objectives.
- **Gap identification**: Capability modeling highlights underdeveloped areas (e.g., threat hunting, deception) that metrics alone may overlook.
- **Business alignment:** Linking Sentinel and Defender XDR investments to SOC capabilities ensures alignment with enterprise security goals and operational excellence.
- **Metrics as measures**: Capability models can incorporate KPIs (e.g., reduced MTTD/MTTR) to track progress toward strategic improvements, demonstrating how AI and automation enhance SOC objectives.
- **Cost justification**: Capability-driven roadmaps maximize ROI by targeting investments where they deliver the greatest impact, such as reducing false positives, improving detection rates, and alleviating analyst fatigue.

Big picture impacts on SOC I operations

Historically, SOC teams operated with fragmented toolsets, forcing analysts to piece together insights from disparate SIEM platforms, endpoint solutions, and threat intelligence feeds. This disjointed approach led to time-consuming data correlation and multiple escalation tiers to fully assess threats.

The unified Microsoft security solution streamlines these processes. Defender XDR provides detection and response across endpoints, networks, email, and cloud, while Sentinel ingests and correlates telemetry at scale, integrating seamlessly with third-party data. Built-in threat intelligence and advanced analytics surface high-fidelity alerts with recommended remediations, enabling analysts to quickly triage, investigate, and respond without lengthy escalations.

By reducing reliance on tiered handoffs and automating low-level tasks, the modern SOC I-powered by Microsoft's unified security stack—enables an agile, flattened operational structure. As a result, analysts can focus on higher-order challenges, improving responsiveness and transforming the SOC from a reactive alert center into a proactive, intelligence-driven command hub.

Getting there – Deployment of the Unified Microsoft Defender XDR and Sentinel solution

References:

- Turn on Microsoft Defender XDR - Microsoft Defender XDR | Microsoft Learn
- Deploy supported services, Setup guides
- Deployment guide for Microsoft Sentinel | Microsoft Learn
- Defender XDR and Sentinel integration, Data connection
- Post-deployment checklist
- Sentinel migration

Overview

Deployment of the unified Microsoft Defender XDR and Sentinel solution set requires developing an understanding of the architecture and integrated feature set of the platform (see references above) and establishing goals and objectives for your SOC modernization.

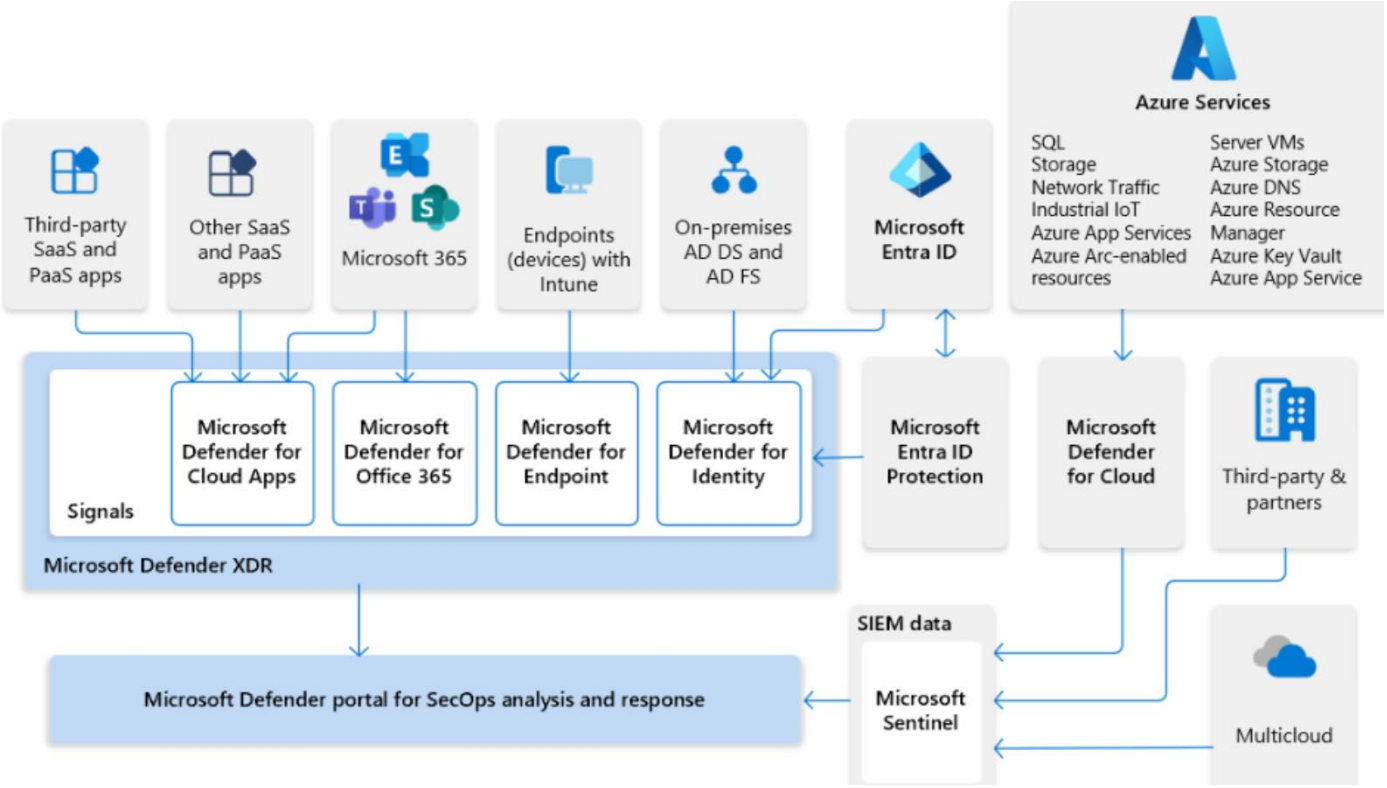


Figure 36 - Integrated Microsoft Defender XDR and Sentinel Architecture – Defender portal | Source[13]

[13] https://learn.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration

Key decisions and planning

General

There are multiple decisions to be made during planning for the journey to the unified solution set. This includes (but is not limited to) the following:

- Whether to integrate Defender XDR into the Azure Sentinel portal or alternatively, Sentinel in the Unified security operations platform in the Defender portal
- Sentinel workplace architecture
- Sentinel data connector needs (data sources and sizing)
- Roles & permissions
- Cost considerations and optimization
- Playbooks
- Analytics and automation rules
- Security operations and workflow optimization
- Etc.

Migration

Another set of major considerations may be whether to integrate or migrate an existing SIEM environment to Sentinel, which requires mapping of playbooks and data - requiring additional planning (and integration or migration execution).

Defender solution integration

Depending on which Defender solutions (e.g., Defender for Identity, Endpoints, Office 365, Cloud Apps, etc.) are in use (or are planned for use) by the organization, each requires its own configuration, maintenance, monitoring, and tuning.

Beyond that, it is important to develop an understanding of the tactical feature sets and workflow options to employ in the modernized SOC operational playbook (e.g., for alert triage and incident management), which the organization should document (in the form of "Standard Operating Procedures") and members of the SOC team should be trained on.

Specialized security services

- Detection rule creation, customization, and tuning
- Automated response playbook design, implementation, and operations
- Process creation and oversight
- Proactive threat hunting program development
- Incident management program development
- Etc.

Deployment options with Microsoft Industry Solutions Security Services – Modern SOC I

Organizations requiring strategic planning and/or deployment guidance to achieve a Modern SOC I have multiple service options, including the use of Microsoft Industry Solutions, which has multiple Security Services offerings that can be tailored to address customer needs in this area.

Strategy and planning

Cybersecurity envisioning

Cybersecurity strategy

Cybersecurity architecture and roadmap

Dependencies and Zero Trust posture maturity[14]

Intune device management
Entra ID identity protection
Privileged Access Workstation (PAW) for Cloud Service Management

Microsoft Defender XDR component implementation

Defender for Office 365
Defender for Identity
Defender for Endpoint
Defender for Cloud Apps
Defender for Cloud
Defender for IoT

Microsoft Sentinel

Implementation and operationalization
Migration (from 3rd party SIEM solutions)

Other

Security Operations Model Planning and Implementation

Refer to the next section on Microsoft Industry Solutions coverage for **Microsoft Security Copilot** and the all-up view in Section 10. Realizing the vision with Microsoft Industry Solutions for more information.

6. Modern SOC II with Generative AI (Microsoft Security Copilot)

SOC metrics and capabilities potentially impacted by Microsoft Security Copilot

1. **Key benefit areas: accuracy, speed, and practitioner augmentation**
2. **Multiple use cases and benefits by role**
3. **Junior analysts: MTTD, MTTR, % incidents mitigated**
4. **Senior analysts: # incidents handled/month, MTTR, cost per incident**

[14] Refer to Section on Zero Trust dependencies and alignment

⑤ TI analysts: # vulnerabilities detected, MTTD, % reduction in incidents, compliance audit scores.

⑥ CISOs: compliance audit scores, % incidents escalated, cost/breach

⑦ High capability improvement opportunity for the MITRE L1 capability area: "Incident triage, analysis and response" + others

Overview - Microsoft Security Copilot

Microsoft Security Copilot – from narrow to Generative AI

As depicted below, both Defender as well as Sentinel have significant amounts of task-specific, non-Generative AI built into them, now supplemented with transformative generative AI capabilities like **Microsoft *Security Copilot***.

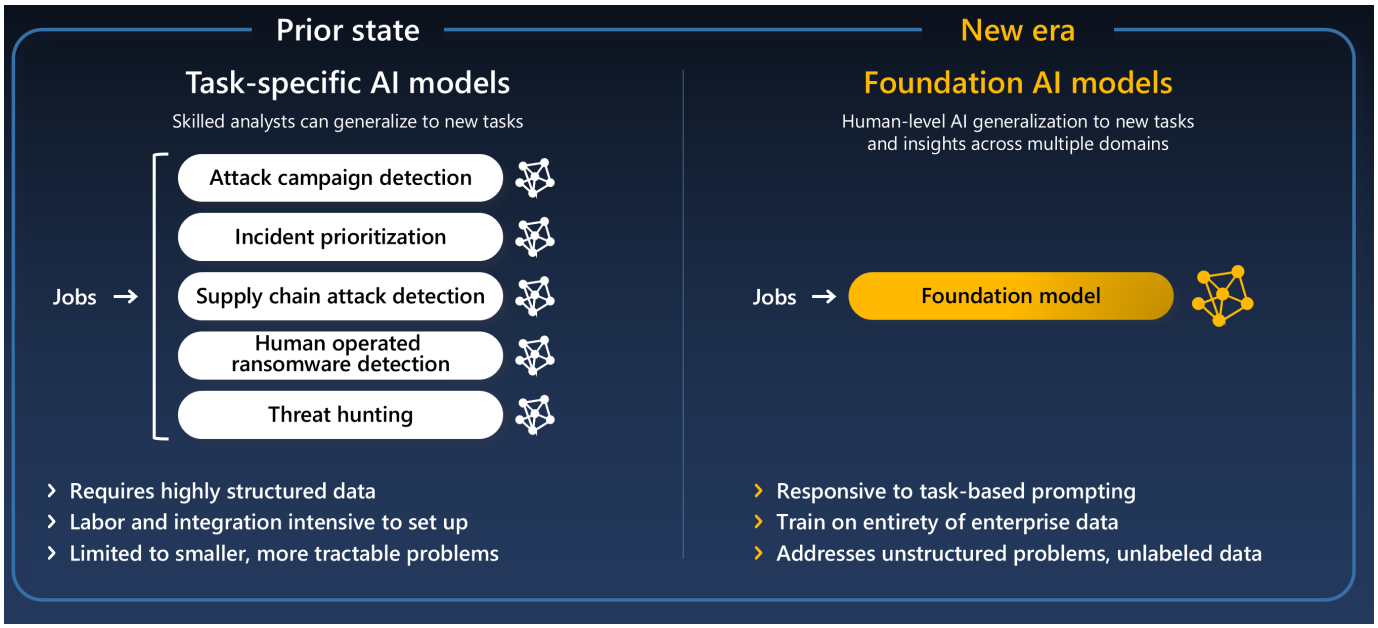


Figure 37 -Moving from narrow to general AI

So, what is "Security Copilot"?

Security Copilot is a generative AI-powered assistant for daily operations in security and IT that empowers teams to protect at the speed and scale of AI, supplementing other types of AI and analytics built into the unified solution covered in the previous section.

Figure 38 - Security Copilot for the Security team

Security Copilot enables security teams to take on even more data, process more incidents, predict more threats, and solve bigger problems than today, allowing personnel to focus on more strategic security initiatives.

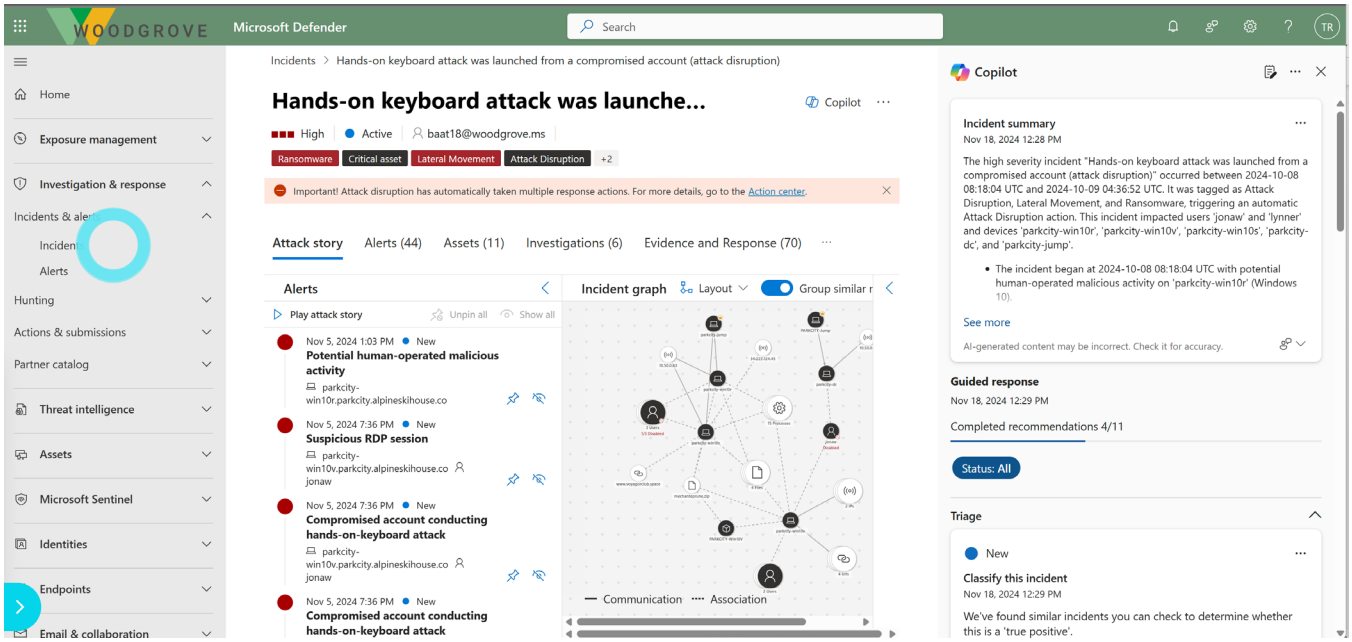


Figure 39 - Security Copilot in the Defender Portal Incident management solution

How it works – Data flows, Plug-ins, Prompts, Experiences, and Extensibility

Overview

Reference: Security Copilot Coverage and Capabilities

At its core, Microsoft Security Copilot (Security Copilot) acts as an orchestrator between entities requesting information[15], information retrieved from Microsoft security (and integrated 3rd party) solutions, and a

[15] End-users through "Standalone," "Embedded" (i.e., in-app), or custom experiences

Large Language Model (LLM) (specific to Security Copilot), all of which combine to enrich the response returned to the requesting party.

This system will be further expanded upon in this section.

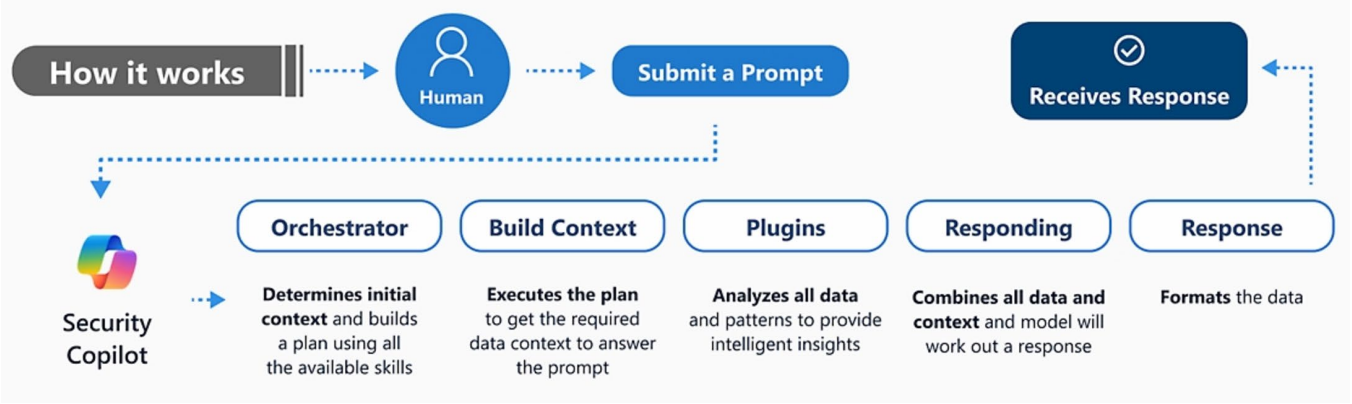


Figure 40 - Security Copilot Logical Architecture

Data flows

Understanding data flow aspects of Security Copilot may be useful in the identification of use cases of potential interest to various SOC roles in an organization, including those involving OOTB feature sets as well as those involving extensibility.

The diagram below highlights the principal elements of the system architecture of Security Copilot, including the logical sequence of steps involved in responding to a system prompt by an end-user.

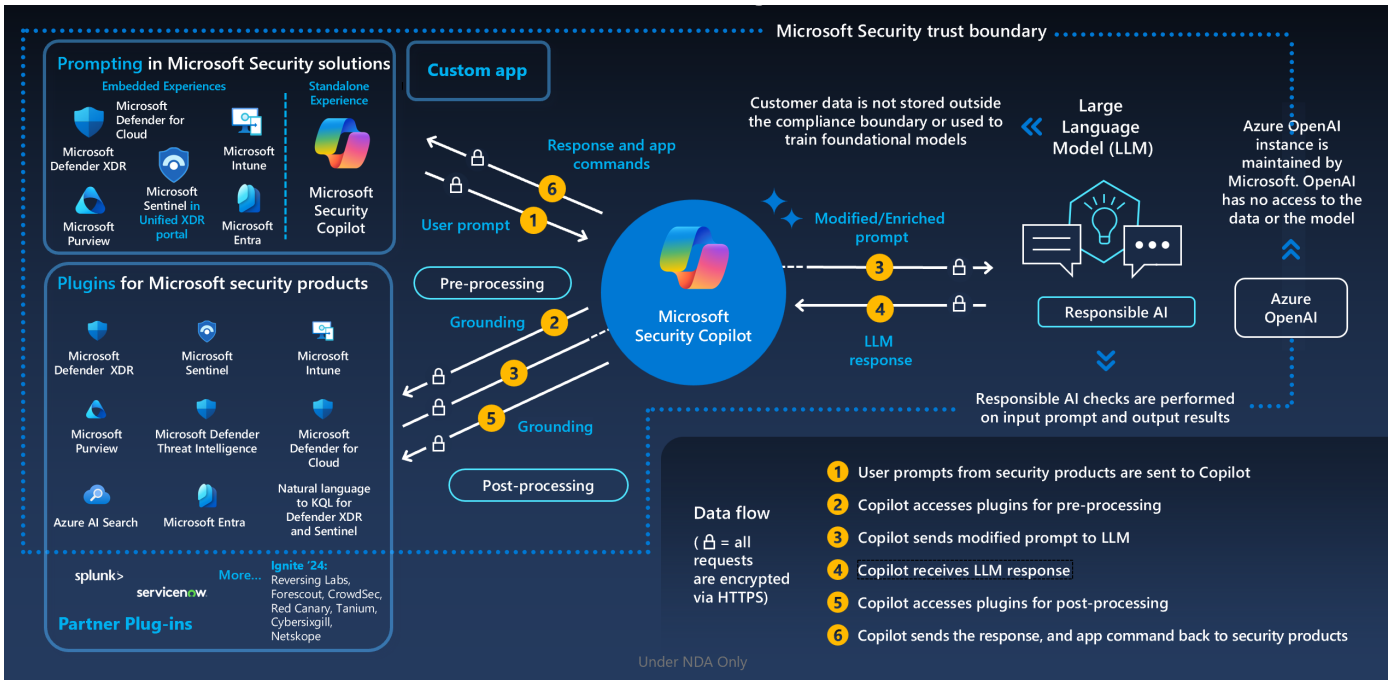


Figure 41 - Data Flow for Microsoft Security Copilot

In addition to understanding the key steps highlighted in the diagram, a few key concepts specific to Security Copilot mechanics are summarized here and expanded on in the next section.

In summary:

- Copilot end-user functionality can be accessed from either **Embedded**, **Standalone,** or **Custom app experieces,** as shown in the to top left of the above diagram.
- Based on the "**Plug-ins**" a customer instance of Security Copilot has access to (and what "skills" a given prompt is invoking), a prompt received by Copilot is "Pre-processed" using data provided by the requested solution and sent to the LLM to "reason over" the enriched data set (i.e., Prompt + Plug-in information) and return intelligent insights to the requesting user, further refined and "grounded" through Security Copiloto Post-processing.

Plug-ins, Prompting and Experiences

Overview

Security Copilot "reasons" through data it has access to (either through OOTB or custom "***Plug-ins***") based on "***Prompting***" from either:

(a) The **"Standalone"** user interface, either through basic prompting (i.e., manual, just-in-time) or the use of built-in "Promptbooks;" or

(b) **"Embedded"** experiences, utilizing built-in security app automation plus integrated prompting built into the various integrated security solution UIs.

Data sourcing through "Plug-ins"

References:

- Plugins overview Microsoft Security Copilot (Preview) | Microsoft Learn
- How to Become a Microsoft Copilot for Security Ninja: The Complete Level 400 Training

Security Copilot plugins are specialized data sourcing components that enable the Security Copilot platform capabilities by providing security data to process/"reason over."

Security Copilot comes with many (OOTB) pre-installed plugins available for activation/connection to Microsoft security services (e.g., for Defender and Sentinel) and other commonly used 1st and 3rd party services and websites that can be used.

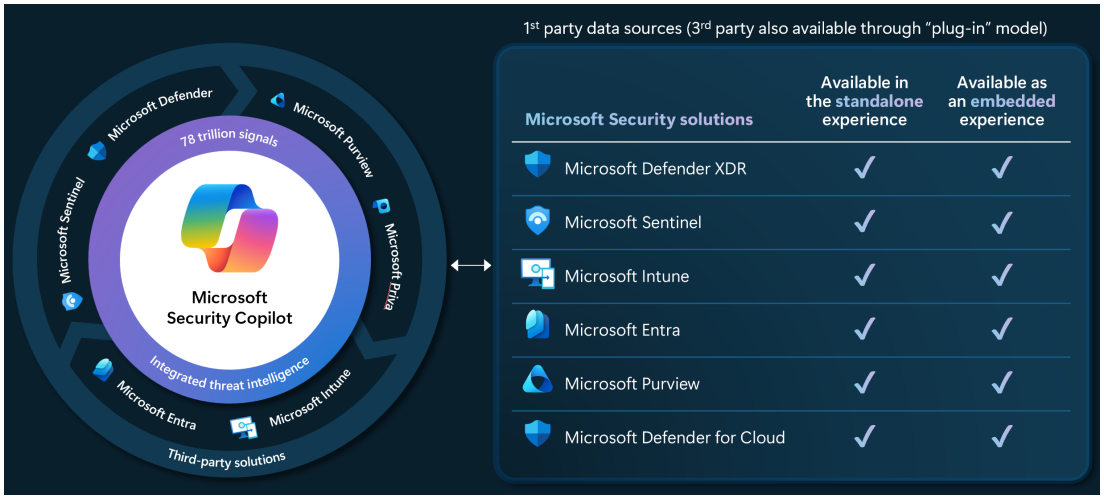


Figure 42 - Security Copilot 1st party security solution integration

Available, customized plug-ins can also be activated using the Plug-in management console in the standalone experience (configured by Copilot "owners").

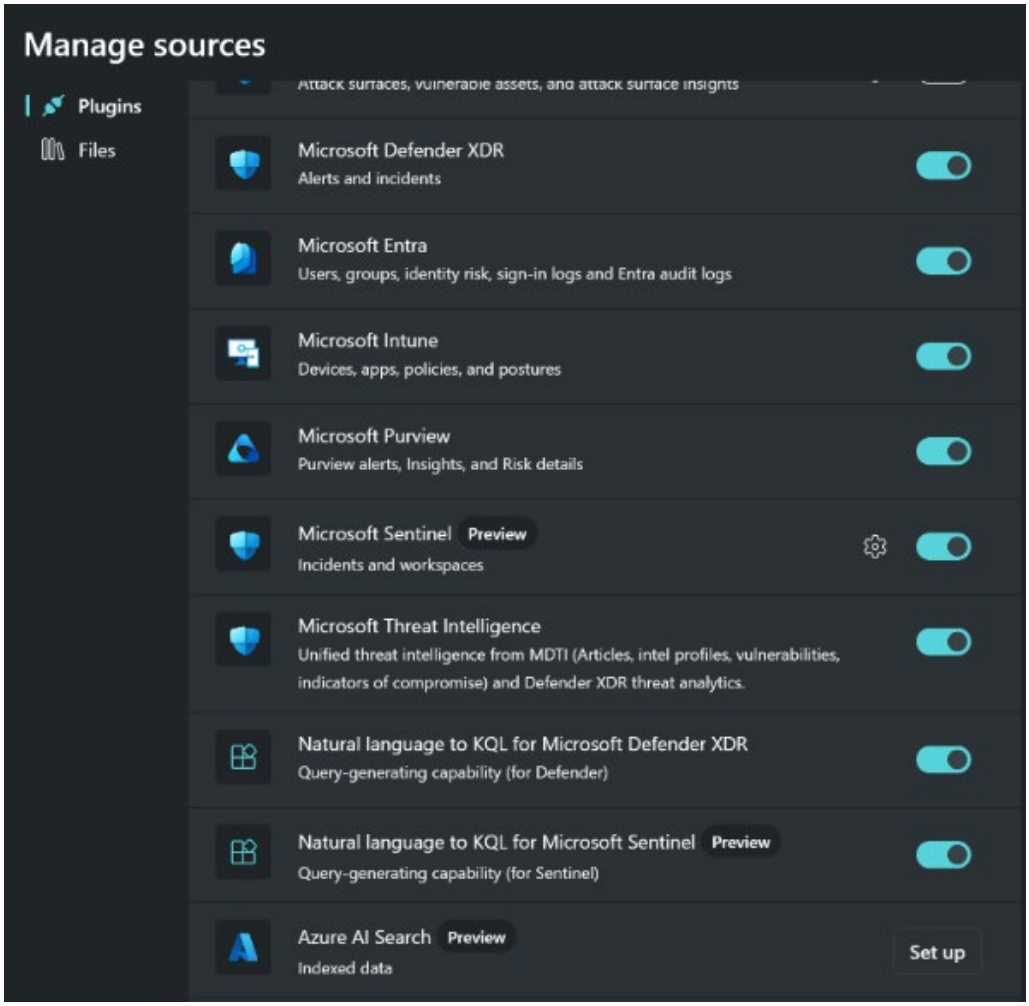


Figure 43 - Security Copilot Plug-in selection/activation experience

Data access through "Prompts"

Reference: How to Become a Microsoft Copilot for Security Ninja: The Complete Level 400 Training

After Security Copilot is set up (including purposeful activation of plug-ins), users can start utilizing "**Prompts"** and "**Promptbooks**," the latter of which are simply purpose-built collections of prompts that work together in a sequence. These prompts serve as the principal input mechanism necessary for Security Copilot to generate responses conducive to aiding users in their security-related endeavors.

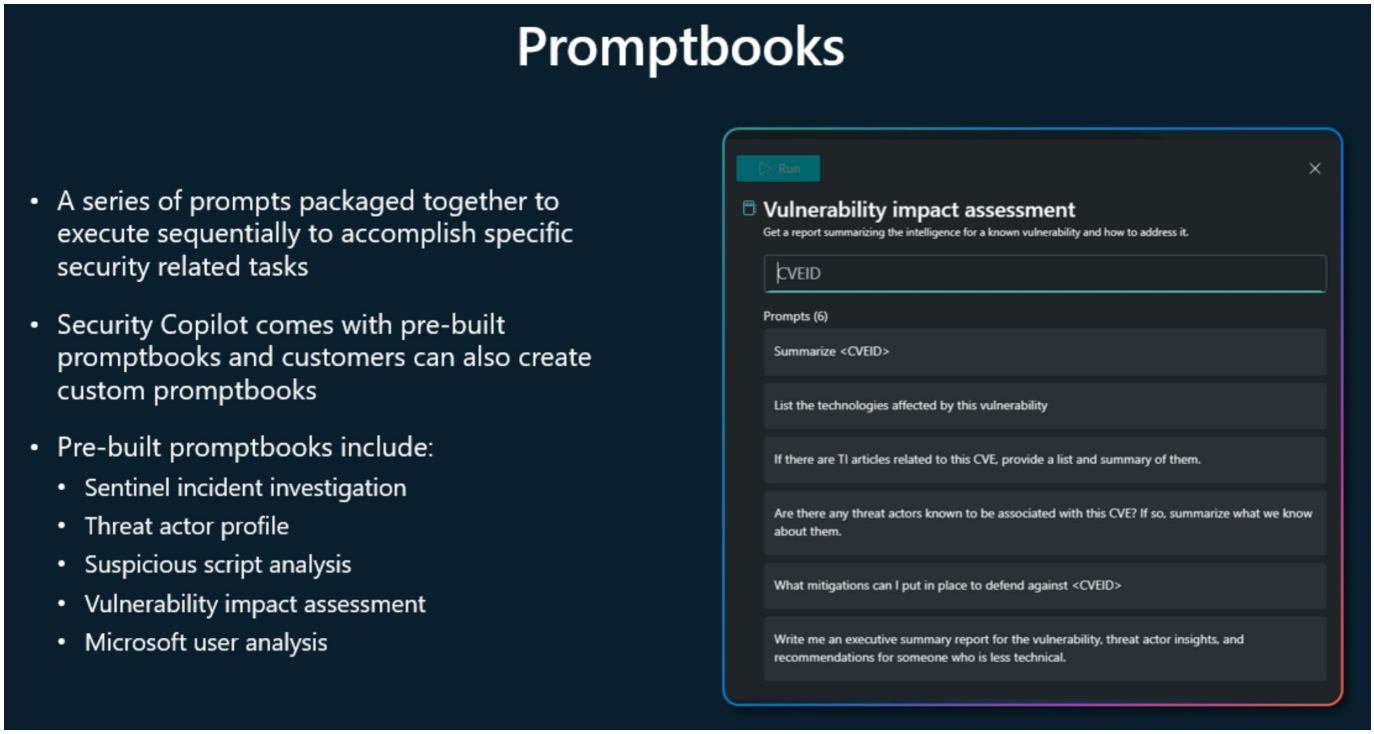


Figure 44 - Promptbooks | Source: Ignite '24 BRK 308

Note that Prompts are relevant to both the Embedded and Standalone experiences, though non-prompt-based Security Copilot functionality is leveraged (behind the scenes) in some parts of the Embedded experience for some Microsoft security solutions (e.g., Incident Management in the Unified solution).

More information

- Create effective prompts
- How to use prompts in Microsoft Security Copilot | Microsoft Security Blog
- Using promptbooks
- Sample prompts on the Security Copilot GitHub.

Custom promptbooks are addressed further below in the section on Extensibility and automation.

Embedded and Standalone experiences

Embedded experiences. The Copilot "Embedded experiences" (see example below for Incident management) provide a great way to get oriented to Security Copilot because they provide more of a

guided workflow, especially valuable for users who might be less experienced with the target Microsoft security products and available data that the Copilot Plug-ins have access to.

For more information, refer to the example use case videos linked to following the figure below.

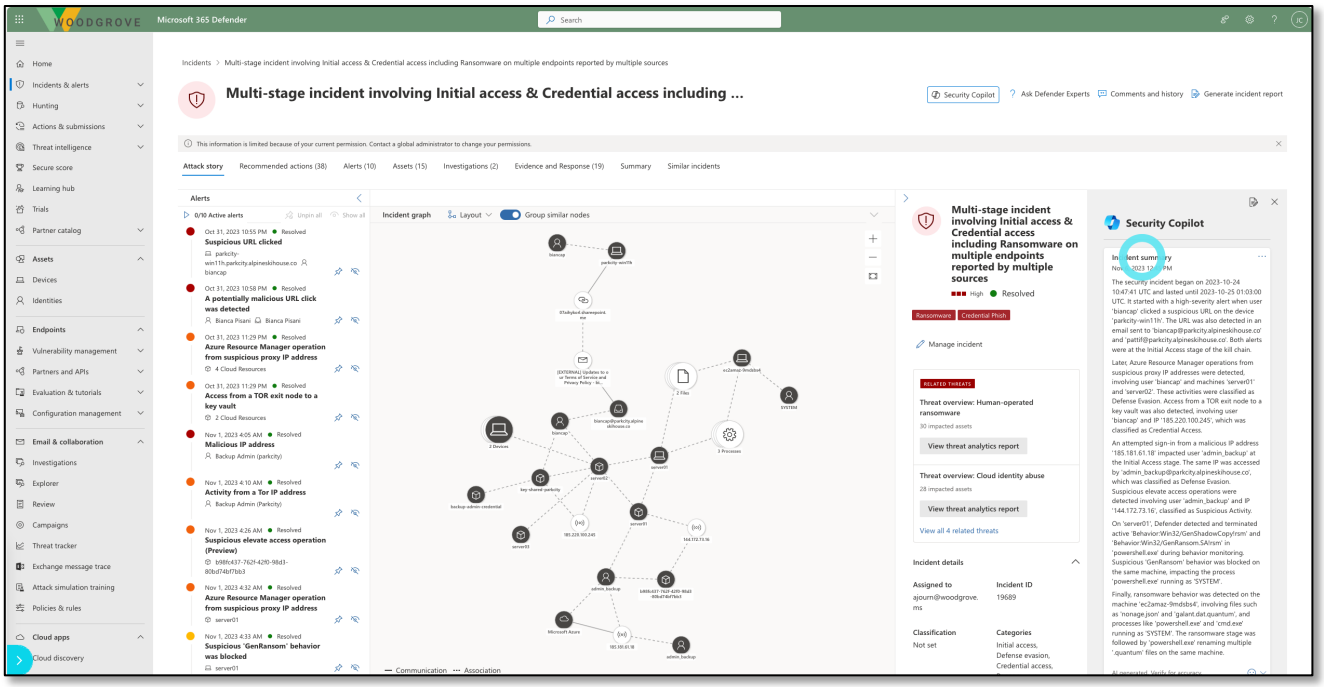


Figure 45 - Example Security Copilot embedded experience

Example use case videos - Embedded

- Human Operated Ransomware
- Incident summarization
- Investigating Business email compromise
- Script Analysis

Standalone experiences. Once Security Copilot is setup and users are granted access, proper permissions, and (presumably) basic training[16], the "Standalone" experience can be leveraged to enter prompts directly into the chat UI or through available promptbooks, noting that the user does need to have some idea of what they're looking for in either case (e.g., a Defender XDR or Sentinel Incident ID) .

As an example, the following screenshot highlights the promptbook experience for "Microsoft 365 Defender Incident Investigation", where the seven (7) individual prompts included would be executed in sequence based on the Defender Incident ID entered by the user in the prompt.

For more information, refer to the example use case videos linked to following the figure below.

[16] At a minimum, end user/analyst training should be provided on target security applications/data sources that the customer instance of Copilot has access to (through activated Plug-ins), prompting techniques/options, available promptbooks, use cases specific to their role, troubleshooting, etc.

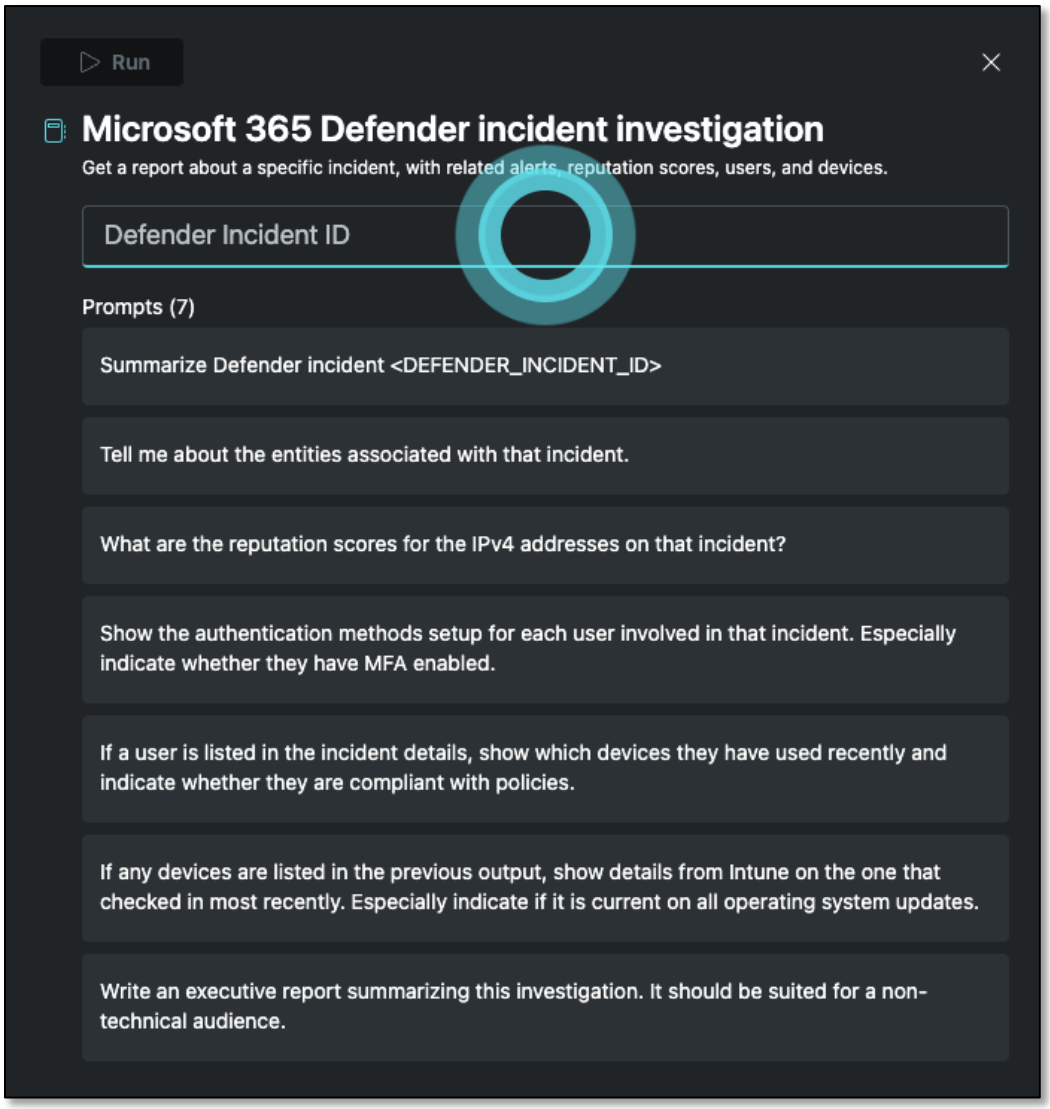


Figure 46 - Example standalone "immersive" experience - Defender investigation promptbook

Example use case videos - Standalone

- Incident triage
- Extended user account investigation with Copilot (accelerated)
- Vulnerability Assessments
- Sample prompts on the Security Copilot GitHub.

Example prompt outputs

Incident summarization

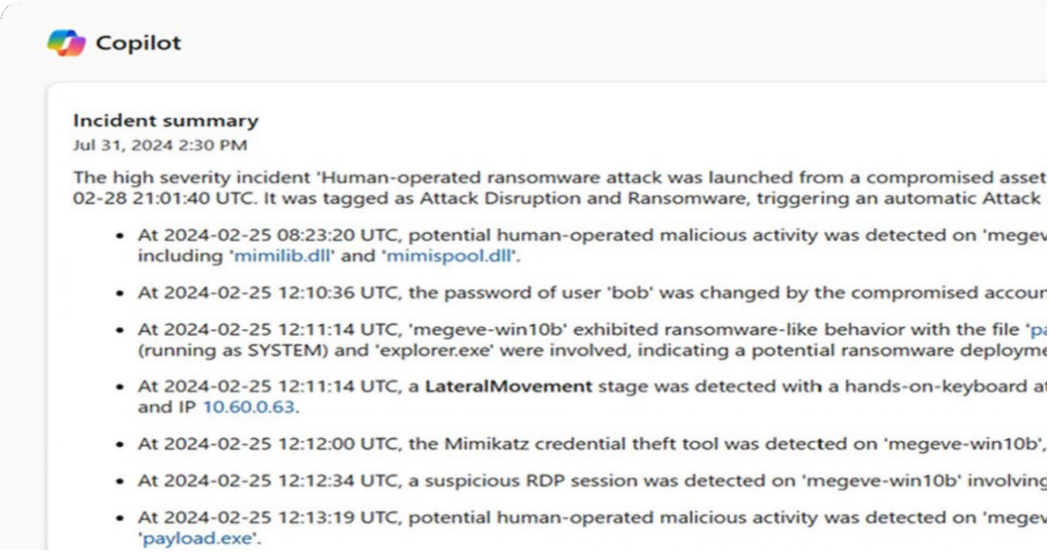


Figure 47 - Copilot Incident summarization

Script analysis

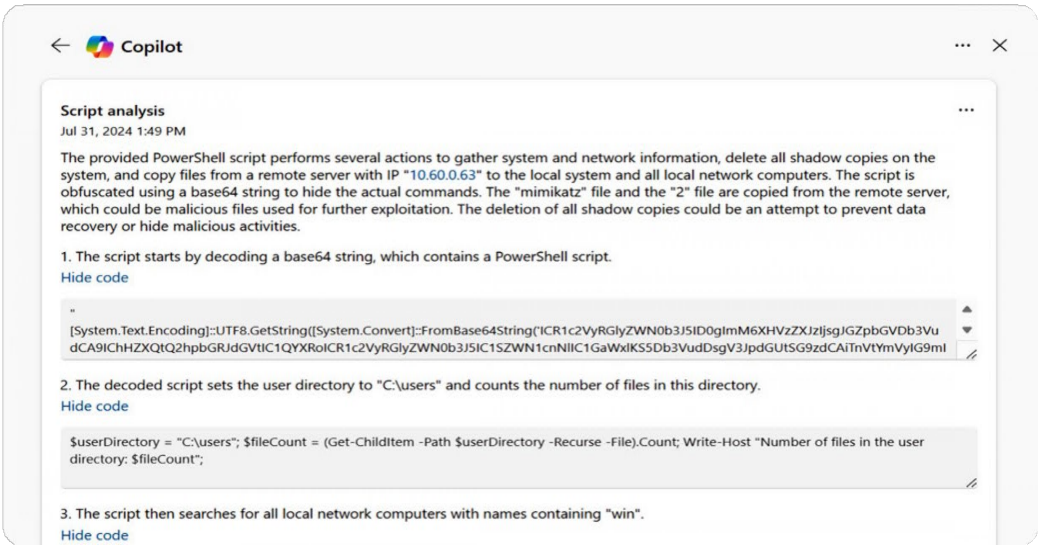


Figure 48 - Copilot script analysis

Extensibility and automation

Many organizations working with Security Copilot have found the variety of "extensibility" features to be useful for both common use cases as well as ones specific to an organization's unique SOC workflow needs.

These include but are not limited to:

(a) 1st and 3rd party custom plug-in integration (for ingesting additional data of use to an investigation team)

Example (1st party): Integration with customer knowledge base via Azure AI Search.

(b) Custom promptbooks

(c) Custom Logic Apps to pull Copilot output into other applications/use cases (which may employ (a) and (b) above.

Custom Plug-ins

Security Copilot comes with many pre-installed plugins available for other commonly used 1st and 3rd party services and websites that customers can leverage OOTB. Customers also have the option of extending default capabilities by adding their own custom plugins.

Refer to the documentation for more information on custom plug-ins[17].

- **References**
  - **Manage plugins in Microsoft Security Copilot | Microsoft Learn**
  - **Create your own custom plugins in Microsoft Security Copilot | Microsoft Learn**

Custom Promptbooks

Custom promptbooks can be created that allow customers to create and save their own collections of natural language prompts for common security workstreams, tasks, and scenarios.

Custom promptbooks can be created from:

- An existing standalone prompting session
- An existing promptbook library entry duplicate
- Through Logic App automation (see "Automation" section below).

References

- Build your own promptbooks | Microsoft Learn
- Microsoft Security Copilot: General Availability details - Microsoft Community Hub
- Leverage Custom Promptbooks to Optimize your Security Workflows | Microsoft Security Copilot Tech Community

Automation – Azure Logic App connector

Based on strong customer demand for automation, including the programmatic access of the organization's Security Copilot system (including Plug-ins, Promptbooks, Microsoft Security application data, etc.), Microsoft introduced the **Security Copilot Azure Logic App** connector.

[17] Additional information will be added once deployment learnings are better known.

This connector enables the creation of workflow automation that accesses Security Copilot from another application, allowing for dynamic input and output processing, enhancing both efficiency and the ability to tailor workflows to specific organizational needs.

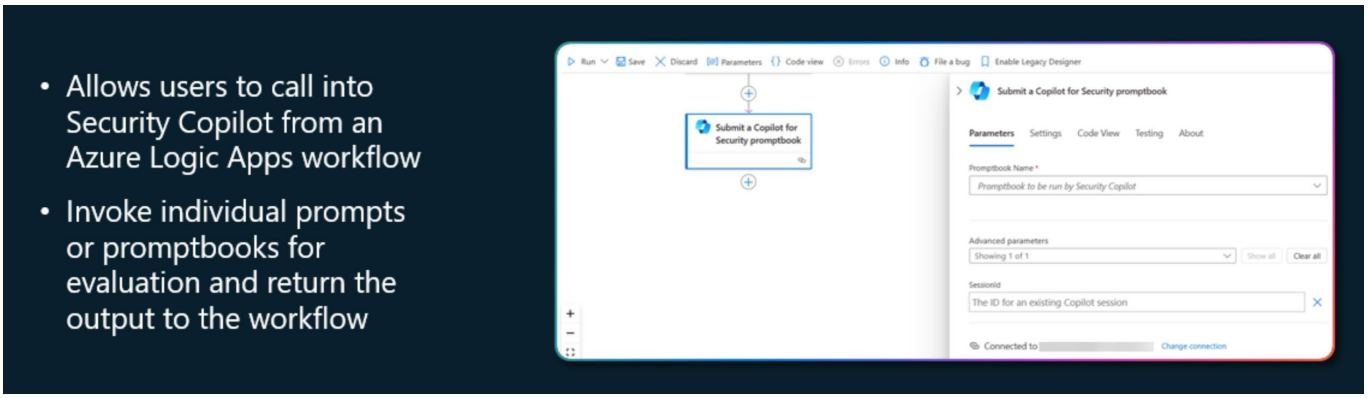


Figure 49 - Logic Apps Connector | Source: BRK 308

For example, when handling a reported phishing email, the **Logic App connector** empowers Security Copilot to automate key steps of the analysis, such as stripping out email header information, evaluating domain reputation, enriching the prompt flow with Threat Intelligence information (e.g., threat actor attribution), etc.

The results can then be automatically routed to the appropriate team for review, reducing response times and minimizing manual effort (e.g., sifting through false positives).

Beyond streamlining incident triage, the connector opens the door to a broader array of Azure Logic App workflows, enabling security teams to integrate existing tools and create bespoke solutions that align with their operational objectives.

References

- **Announcing Copilot for Security Azure Logic App connectors**
- **Security-Copilot/Technical Workshops/Automation Workshop at main · Azure/Security-Copilot · GitHub**

What's new and coming – Microsoft Security Copilot

Reference: Copilot for Security Roadmap – 2024[18]

- Plugin ecosystem – 7 partner releases: Reversing Labs, Forescout, CrowdSec, Red Canary, Tanium, Cybersixgill and Netskope
- Security Copilot integrated into the new Microsoft Purview Data Security Posture Management solution.
- RBAC improvements
- Geo options for data storage

[18] Sampling, partial listing (available to customers under NDA)

- Capacity and workflow customization by team
- Multiple workspaces and/or tenants to address global operation needs
- Plug-in accessibility control by user
- Multi-skillset/data sources per response availability
- Unified CVE[19] (Common Vulnerabilities and Exposures) across sources
- External TI vs. MSFT TI differentiation
- **Current standalone availability**: Threat Intelligence, Defender XDR, Intune, Entra, Purview Data Security, Defender for Cloud, Defender EASM
    - **Upcoming standalone availability**: Sentinel, Defender for Cloud, Azure WAF, Azure Firewall, Windows Autopatch, Windows 365
- **Current embedded availability**: Threat Intelligence, Defender XDR,, Sentinel, Purview Data Security.
    - **Upcoming embedded availability**: Intune, Entra, Purview Daa Governance, Defender for Cloud, Defender for EASM, Azure WAF, Azure Firewall, Windows Autopatch, Windows 365.

Impacts

Key use cases, personas, and benefits

Improvement of SOC capabilities with the Microsoft Unified solution enhanced with the integrated Security Copilot toolset has been found – based on early studies[20] - to have a number of benefits specific to various SOC roles and use cases, as highlighted in this section.

Benefit area 1 – Accuracy

Fundamentally, Security Copilot makes security teams more accurate by distilling the signal from the noise from data sources across the customer's security portfolio, including Microsoft Security and third-party solutions, enriched by the 78T signals Microsoft synthesizes each day, with Microsoft threat intelligence (included with Copilot) for a holistic and comprehensive view of the threat landscape.

From a high-level benefits perspective, in a randomized controlled trial for Security Copilot, security novices saw a 35% increase in accuracy, with a 7% increase in accuracy by security professionals.

[19] CVE Website

[20] Generative AI and Security Operations Center Productivity, November 2024

Figure 50 – Copilot impacts on accuracy

Benefit area 2 – Speed

With Copilot, you can automate many of the more tedious tasks with contextualized data collection and summaries, remediation guidance, and stakeholder reporting. In fact, recent studies[21] have shown a 30% reduction in MTTR within 3 months of Copilot use (see study for details).

Even seasoned security professionals found a 22% increase in speed across SOC use cases.

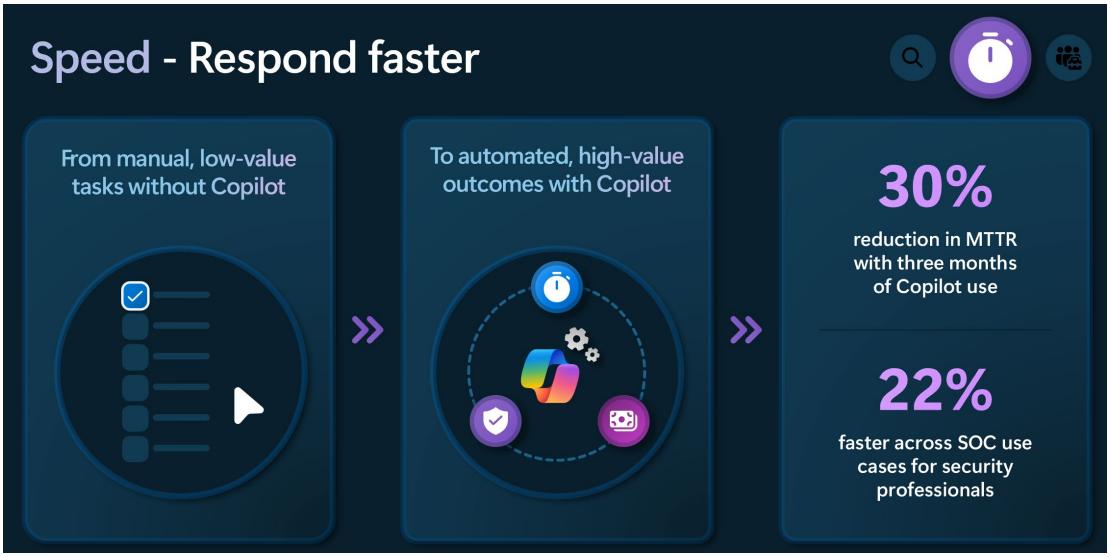


Figure 51 - Copilot benefits for speed/response time

[21] Generative AI and Security Operations Center Productivity, November 2024

Benefit area 3 – Augmentation

And finally, you can strengthen team expertise with Copilot by supplementing analysts with AI-driven assistance and guided remediation in natural language for intuitive next steps.

Figure 52 - Augmenting human expertise

Use cases by function and role

Security Copilot has the potential to enable SOC efficiencies across multiple tiers (or functions) of the SOC, as shown in the following figure and expanded on in the tables below for each major SOC role.

Key insights:

- Metrics like MTTD and MTTR are critical across roles that deal directly with incident detection and response, as they directly measure operational efficiency.
- Compliance Audit Scores and Percentage Reduction in Security Incidents Over Time are pivotal for higher-level roles like CISOs and data security admins that focus on strategic and organizational impact.
- Cost-related metrics such as Cost per Incident are highly relevant for roles aiming to improve efficiency and reduce operational overhead, particularly in IT and identity management

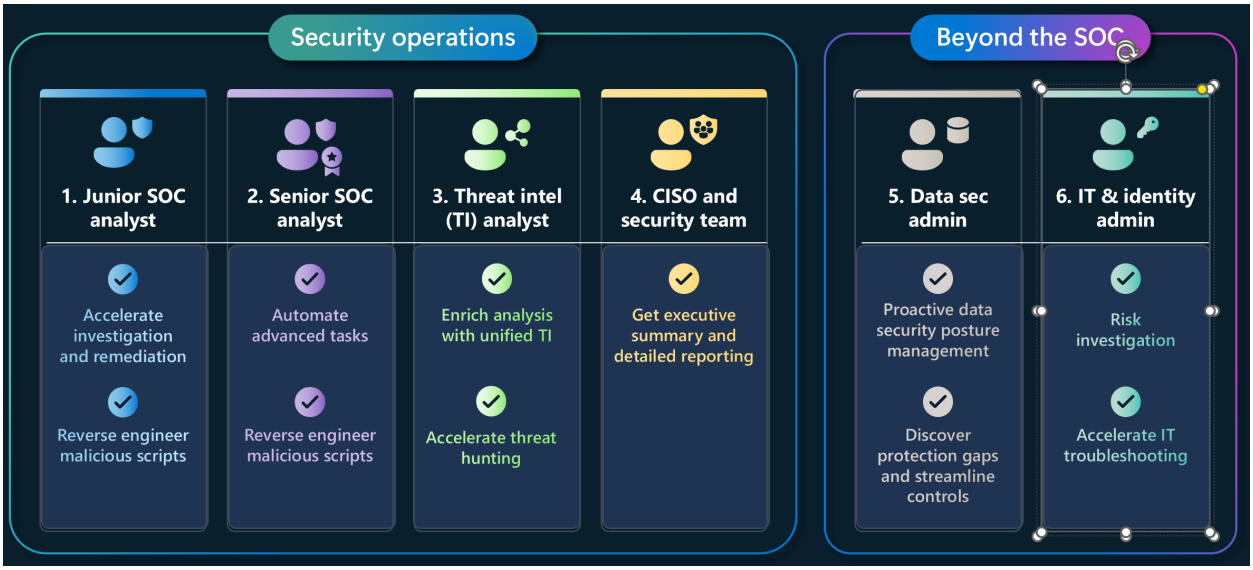


Figure 53 - Key use cases and personas for Security Copilot

1. Junior SOC analysts benefit from features like incident summarizations, which help to accelerate investigations, and they can also take advantage of the remediation guidance that Copilot offers.

Use Case	SOC metric impacted	Benefit rationale
Accelerate investigations and remediation	MTTD, Percentage of Incidents Successfully Mitigated	Accelerated investigations and remediation directly impact detection and mitigation times, improving detection efficiency and response effectiveness.
Reverse engineer malicious scripts	MTTD, Mean Time to Respond (MTTR)	By reducing the time spent on reverse engineering scripts, Copilot can improve both detection and response timelines.

2. Senior SOC analysts can automate advanced tasks like user-reported phishing analysis[22] and incident enrichment.

Use Case	SOC metric impacted	Benefit rationale
Automate advanced tasks like phishing analysis and incident enrichment	Number of Security Incidents per Month, MTTR	Automation reduces the workload on senior analysts, allowing faster response to incidents and increased capacity to handle more incidents per month.
Reverse engineer malicious scripts	MTTR, Cost per Incident	Automating script analysis decreases the time and cost per incident, improving efficiency for senior analysts.

[22] Explored deeper later in this briefing

Both (Junior and Senior SOC analysts). Copilot can reverse engineer malicious scripts and provide actionable insights for next steps, which is a time-consuming process that both senior and junior analysts can benefit from.

Use Case	SOC metric impacted	Benefit rationale
Reverse engineer malicious scripts	MTTD, Mean Time to Respond (MTTR)	By reducing the time spent on reverse engineering scripts, Copilot can improve both detection and response timelines.

In fact, in a productivity study conducted in January, Microsoft researchers found that Copilot professionals were 12% more accurate at Script analysis, and Copilot novices were 34% more accurate at Script analysis.

3. TI analysts can benefit from enriched analysis that pulls in data across the entire threat landscape with unified TI and accelerate threat hunting with AI powered insights and guidance.

Use Case	SOC metric impacted	Benefit rationale
Enrich analysis with unified TI and accelerate threat hunting	Number of Vulnerabilities Identified and Remediated, MTTD	Unified threat intelligence and faster threat hunting enable analysts to identify and address vulnerabilities more quickly, improving detection timelines.
Accelerate threat hunting	Percentage Reduction in Security Incidents Over Time, Compliance Audit Scores	Faster threat hunting reduces future risks, contributing to a measurable decrease in incidents and improved compliance readiness.

4. CISOs can leverage Copilot to get executive summaries and detailed reporting with the information they need, tailored for the audience that will be consuming the information - technical or nontechnical.

Use Case	SOC metric impacted	Benefit rationale
Executive summaries and detailed reporting tailored to audiences	Compliance Audit Scores, Percentage of Incidents Escalated	CISOs require high-level metrics to report on compliance readiness and escalations, ensuring executive stakeholders are informed of the organization's security posture.

Beyond the SOC, it has been observed that users in data security and otherwise IT teams also found value in Copilot.

5. Data security admins can get comprehensive, AI-powered visibility and more accurate risk analysis across their data landscape. They can leverage data security posture management, supercharged with Copilot, for proactive data security posture management, and they can discover protection gaps and streamline controls, with features like data loss prevention.

Use Case	SOC metric impacted	Benefit rationale
AI-powered risk analysis and data security posture management	Number of Vulnerabilities Identified and Remediated, Compliance Audit Scores	AI-powered tools improve visibility and accuracy in identifying vulnerabilities and improving compliance posture.
Discover protection gaps and streamline controls	Percentage Reduction in Security Incidents Over Time	Streamlining controls and closing gaps directly reduces future incidents, enhancing security posture.

6. IT teams, including Identity admins, can use Copilot for faster and more accurate risk investigation, streamlined IT troubleshooting, and AI-powered device insights.

Use Case	SOC metric impacted	Benefit rationale
Faster risk investigation and IT troubleshooting	Cost per Incident, MTTR	Faster investigation and troubleshooting reduce operational costs and the time needed to address risks, improving overall efficiency and effectiveness.
AI-powered device insights	Percentage of Incidents Successfully Mitigated	Enhanced device insights lead to more successful incident mitigation by improving root cause analysis and preventive actions.

Looking forward

Given the variety of possible use cases with the open-ended, extensible, and flexible nature of Security Copilot, along with the major differences between embedded vs. immersive experiences, it is expected that we will see a number of new scenarios surface in the coming months and years as the product evolves and organizations get more familiar with the technology and emerging usage paradigms.

Potential SOC capability improvements from Generative AI

Reference: 11 Strategies of a World-Class Cybersecurity Operations Center

Example SOC capability benefit areas

Returning to the MITRE SOC capability model we baselined in a previous section, the figure below highlights possible benefit areas of Security Copilot (in light green and pink[23] boxes) mixed in with the broader set of potential capability benefits from the Modern SOC 1 (unified) solution (within the dark green border), previously discussed.

[23] For the boxes with pink fill, we map them to known Security Copilot use cases further below.

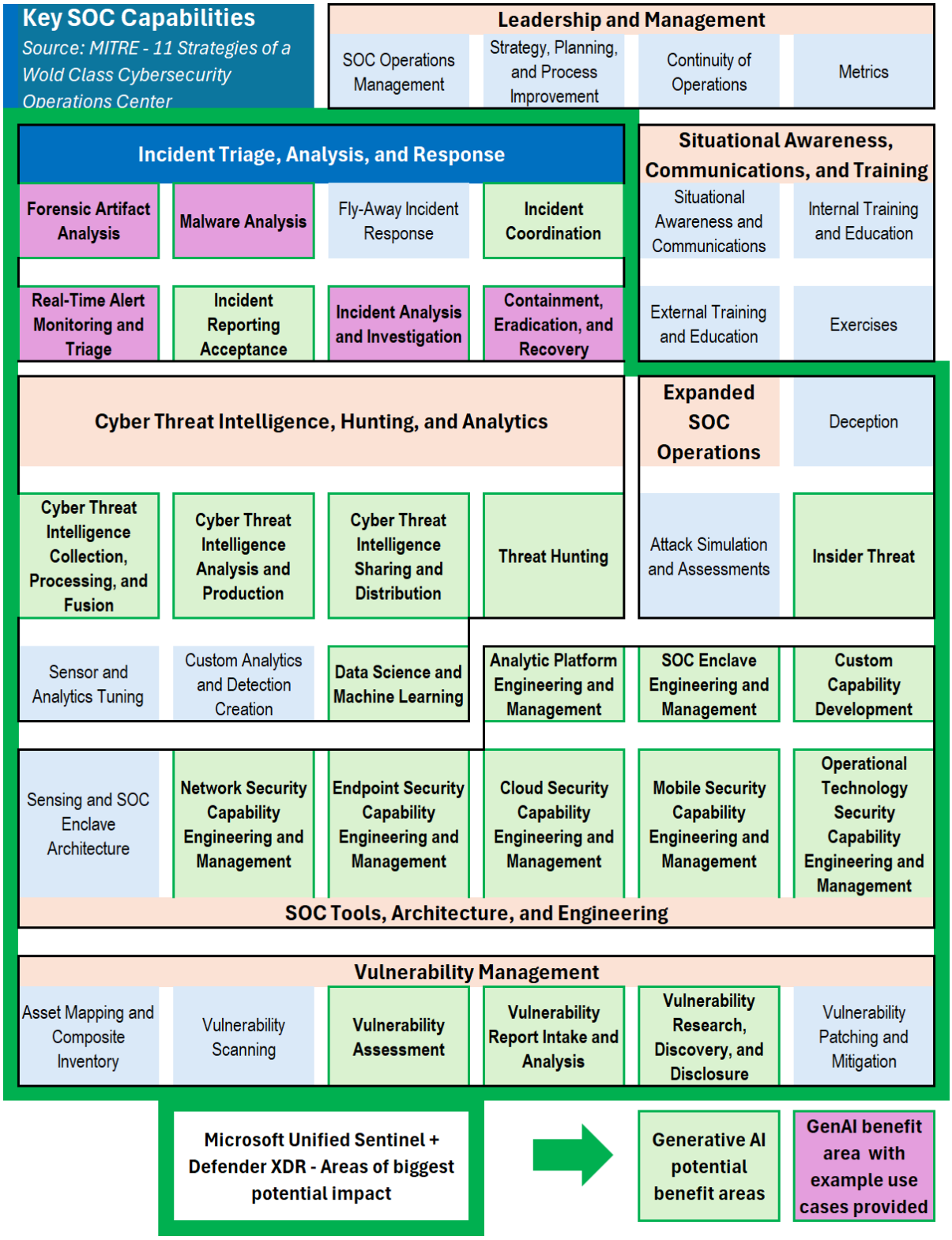


Figure 54 - Potential SOC capability improvements from generative AI

This highlights where a number of the MITRE model's Level 1 and 2 capabilities may benefit from SOC Modernization complemented with Generative AI solutions.

Use case-to-benefit area mapping

A summarized listing of how Microsoft Security Copilot use cases can be mapped to an examples set of MITRE SOC Capability model Level 1 and 2 focus areas are provided below.

Level 1 Focus area - Incident Triage, Analysis, and Response

Level 2 SOC capability: Incident analysis and investigation

- **Use Case:** Guided Response
- **Summary**: Security Copilot provides AI-driven step-by-step guidance for incident triage, investigation, and remediation. This solves the problem of analysts lacking clear, actionable workflows, ensuring efficient and structured responses to incidents.

Level 2 SOC capability: Containment, Eradication, and Recovery

- **Use Case:** Impact Analysis
- **Summary**: Copilot leverages AI analytics to assess the potential impact of incidents. It addresses the challenge of prioritizing response efforts by delivering insights into affected systems and data, aiding decision-making during recovery.

Level 2 SOC capability: Real-Time Alert Monitoring and Triage / Incident Analysis and Investigation

- **Use Case**: Incident Summarization
- **Summary**: By summarizing up to 100 alerts into concise, actionable reports, Copilot helps SOC analysts navigate overwhelming alert volumes, enabling quick understanding and effective response.

Level 2 SOC capability: Malware Analysis / Forensic Artifact Analysis

- **Use Case**: Reverse Engineering of Scripts
- **Summary**: Security Copilot automates the reverse engineering of malware, translating complex scripts into natural language. This addresses the difficulty analysts face in decoding obfuscated scripts, streamlining analysis and response.

Big picture impacts on SOC II Operations

The transition from the Modern SOC I, characterized by unified security solutions, to the Modern SOC II introduces a new era of "**Cognitive Security Operations**" powered by generative AI technologies like Microsoft Security Copilot.

By integrating Copilot with tools like Defender XDR, Sentinel, Entra, and Intune—or through a standalone interface—analysts can interact with vast amounts of telemetry, threat intelligence, and historical data using natural language, where the need for highly specialized skillsets is reduced.

Generative AI enables tasks like event correlation, root-cause analysis, and tailored threat hunting to be handled by a single analyst augmented by AI, reducing escalations and reliance on specialized expertise.

For internal SOCs, this means streamlined workflows and more strategic focus, while for outsourced MXDR providers, it enhances scalability and service value. The result is a "**Cognitive SOC**" where AI abstracts complexity, democratizes knowledge, and enables teams to detect, anticipate, and respond to threats with unmatched speed and precision.

By evolving from reactive alert handling to proactive, intelligence-driven defense, the **Cognitive SOC** blurs traditional roles and workflows, fostering collaboration between human expertise and AI. This transformation empowers both in-house and external teams to deliver unparalleled agility, resilience, and foresight in an ever-evolving threat landscape.

Getting started with Security Copilot

References:

- Microsoft Security Copilot documentation | Microsoft Learn
- Get started with Microsoft Security Copilot | Microsoft Learn

Overview

As a SaaS solution that's integrated with other Microsoft SaaS security solutions, Microsoft Security Copilot requires nominal setup and onboarding, though similar to the Unified solution covered in the previous section, there are a number of planning considerations and prerequisites to consider, as well as options for integration with numerous data sources, extensibility, and automation.

A sampling of the planning considerations is listed here for reference – see online documentation for more information.

- Azure subscription
- Security compute units and Capacity
- Owner role settings
- Setting up the default environment
- Role assignments
- Plugin management
    - Manage custom plugins
    - Manage preinstalled plugins
    - Accessing data from Microsoft 365 services
- Promptbooks
- Managing audit log data
- Connectors (Logic Apps connector)

Understanding data sources and interactive modalities

A major consideration for Security Copilot is which data sources (1st and 3rd party) it has access to, as that will dictate what it makes sense to develop (or adopt) promptbooks for, and/or which embedded experiences to document and incorporate into the modernized SOC operational playbook, which the SOC team will need to be trained on and understand.

Extensibility options

Refer to the extensibility and automation options covered earlier in this section.

Deployment options with Microsoft Industry Solutions Security Services

Organizations requiring strategic planning and/or deployment guidance to achieve a Modern SOC I and/or II have multiple service options, including the use of Microsoft Industry Solutions, which has multiple Security Services offerings that can be tailored to address customer needs in this area:

Modern SOC I *(see previous section)*			**Modern SOC II**
Strategy and planning: Cybersecurity envisioning Cybersecurity strategy Cybersecurity architecture and roadmap	**Dependencies and Zero Trust posture maturity** Intune device management Entra ID identity protection Privileged Access Workstation (PAW) for Cloud Service Management **Microsoft Defender XDR component implementation:** Defender for Office 365 Defender for Identity Defender for Endpoint Defender for Cloud Apps Defender for Cloud Defender for IoT	**Microsoft Sentinel** Implementation and operationalization Migration (from 3rd party SIEM solutions) **Other** Security Operations Model Planning and Implementation	**Security Copilot Planning, Implementation and Integration**

Refer to Section 10. Realizing the vision with Microsoft Industry Solutions for more information.

7. Modern SOC III with Agentic AI for Security

Introduction

Security Operations Centers (SOCs) today grapple with overwhelming data and incident volumes. Modern tools like Microsoft's Sentinel offer sophisticated automation through SOAR (Security Orchestration, Automation, and Response) functionalities, utilizing playbooks and rules to handle recurring tasks.

Innovations such as Microsoft Security Copilot, powered by generative AI, further enhance these capabilities by assisting with enrichment, response, and remediation tasks.

The Next Evolution: Agentic AI in SOCs

While advancements in SIEM/SOAR/Generative AI) promise to greatly improve SOC efficiency, a recent innovation—Agentic AI—is poised to transform security operations even further by reducing the need for human intervention. Announced in Fall '24[24], Agentic AI's potential impact on security could be significant, as highlighted recently in articles from industry leaders like Terence Jackson[25] and Stephen Kaufman[26] (from Microsoft), as summarized below.

Understanding Agentic AI

(See sidebar for additional early-stage, technical detail.)

Agentic AI refers to artificial intelligence systems capable of autonomous decision-making and action-taking to achieve specific goals without continuous human oversight. Unlike traditional AI that relies on predefined rules, Agentic AI can perceive its environment, learn from it, and adapt its actions accordingly. This makes it particularly suited for the dynamic and complex field of cybersecurity, where rapid response and adaptability are crucial.

Additional expectations for future functionality for Agentic AI include (but are not limited to) the following:

- **Modularity**: Agentic AI can be designed to be modular, with multiple AI agents able to interact with one another, making them easier to adapt and iterate upon.
- **Autonomy and Reasoning**: Agents will have the autonomy to perceive, reason (using one or more LLMs or plug-ins), and act (using existing tools like search, calculators, other security tools, other agents, etc.).
- **Contextual Memory**: AI agents will be expected to access contextual (e.g.,

Technical Discussion

Agentic AI integrates tools, frameworks, and patterns to automate business process workflows where AI and humans collaborate. Central to this system are AI agents—autonomous units designed for specific tasks that seamlessly integrate into larger workflows.

These agents interact with Large Language Models (LLMs) to generate content, including executable code for downstream agents. A central controller orchestrates agents by invoking them based on predefined rules and data-driven decisions. This adaptive orchestration allows dynamic responses to changing environments with minimal human input.

Unlike traditional generative AI tools like chatbots or copilots that respond to direct commands, Agentic AI operates continuously within an iterative workflow. It autonomously makes decisions and actions aligned with business goals, listening, reacting, and analyzing domain-specific data in real time—an essential feature for complex environments like cybersecurity.

[24] Satya Nadella's AI Tour London keynote
[25] Agentic AI in Security Operations: Unlocking Efficiency for CISOs | Terence Jackson | Global Security Advisor | Microsoft;
[26] Beyond ChatGPT: The rise of agentic AI and its implications for security | Stephen Kaufman | CSO Online).

case/incident) memory of things previously reasoned over.
- **Self-Evaluation**: AI agents will have the ability to evaluate their own output for sufficiency and accuracy, iterating as needed.

These are just preliminary concepts – more is expected to be announced from Microsoft in March 2025.

Potential Use Cases in Security Operations

Automated Threat Detection and Response

Agentic AI could enhance threat detection by continuously monitoring network traffic, user behavior, and system activities to identify anomalies indicative of cyber threats.

- By differentiating between normal and malicious activities and adapting to new threat patterns, it could improve accuracy and speed.
- Additionally, it could autonomously initiate response actions like isolating compromised systems or blocking malicious IPs, reducing the attackers' window of opportunity.

Vulnerability Management

Managing thousands of assets with varying vulnerability levels is time-consuming when done manually.

- Agentic AI could automate this process by continuously scanning for known vulnerabilities and predicting potential zero-day exploits through behavioral analysis.
- It could prioritize vulnerabilities based on factors like exploitability and impact, and even autonomously apply patches or recommend remediation actions to ensure critical issues are promptly addressed.

Incident Investigation and Analysis

Post-incident investigations require sifting through vast amounts of data to uncover root causes and assess the breach's scope.

- Agentic AI could streamline this process by autonomously gathering and correlating data from various sources. It could reconstruct attack timelines, identify compromised accounts, and suggest potential entry points used by attackers.
- Furthermore, it could generate detailed reports for compliance purposes and stakeholder communication.

Potential impact on SOC Operations

Agentic AI holds transformative potential for SOCs by elevating automation to a strategic level. If leveraged effectively, the focus of security teams shifts from routine operational tasks to policy development, strategic planning, and innovation. With Agentic AI autonomously managing tactical workloads, SOCs could achieve greater scalability, adaptability, and efficiency - ushering in what might be called "Modern SOC III."

Like the adoption of generative AI before it, Agentic AI promises to significantly reduce manual workloads in cybersecurity operations. This allows human resources to concentrate on complex, strategic tasks at a greater scale, enhancing overall security posture.

8. Strategic practices for the Modern SOC

Top strategic planning objectives and practices

1. **Improved operational readiness, efficiency, and resiliency**
2. **Automation and predictability**
3. **Modernized cloud security**
4. **Resource shifting to new and emerging threats**
5. **Adherence to Zero Trust principles**

Protecting the present and preparing for the future SOC – Microsoft SFI initiative.

As laid out in its Secure Future Initiative | SFI and as introduced in Section 2 of this briefing (where SFI is highlighted in the section on "**Strategic technology and policy initiatives"**), SFI is a multi-year Microsoft endeavor aimed at achieving the highest security standards while fostering a model of excellence for the broader industry. Importantly, Security Operations Centers (SOCs) play a pivotal role in realizing this vision by operationalizing these principles and ensuring alignment with SFI's goals.

At its core, SFI is built around three foundational security principles: ***Secure by Design***, ***Secure by Default***, and ***Secure Operations***.

These principles guide Microsoft's approach to designing, building, testing, and operating secure products and services while modeling best practices for customers and partners.

These principles are supported by six engineering pillars:

- Protecting identities and secrets
- Isolating production systems
- Securing networks
- Safeguarding engineering systems
- Monitoring and detecting threats, and
- Accelerating response and remediation

These elements reflect the initiative's focus on comprehensive security culture and governance, emphasizing both proactive measures and rapid incident handling within SOC operations.

Security program optimization

From the MDDR 2024 companion Executive Summary for CISOs, the graphic below illustrates how Microsoft prioritizes its cybersecurity needs, starting with the most basic need: ***Protected Identities,*** followed closely by ***Protected Devices,*** all the way up to ***Automated security operations.***

At this highest level, organizations employ automated operations that consolidate prevention, detection, assessment, and remediation across all assets, with hyperscale cloud and AI-powered systems that rely less on human intervention[27].

Also notable:

a) AI has a role at each tier, underscoring its potential to enhance security measures; and
b) Cultivating a robust security culture within the organization helps ensure the technological defenses and human practices evolve in concert to mitigate threats effectively.

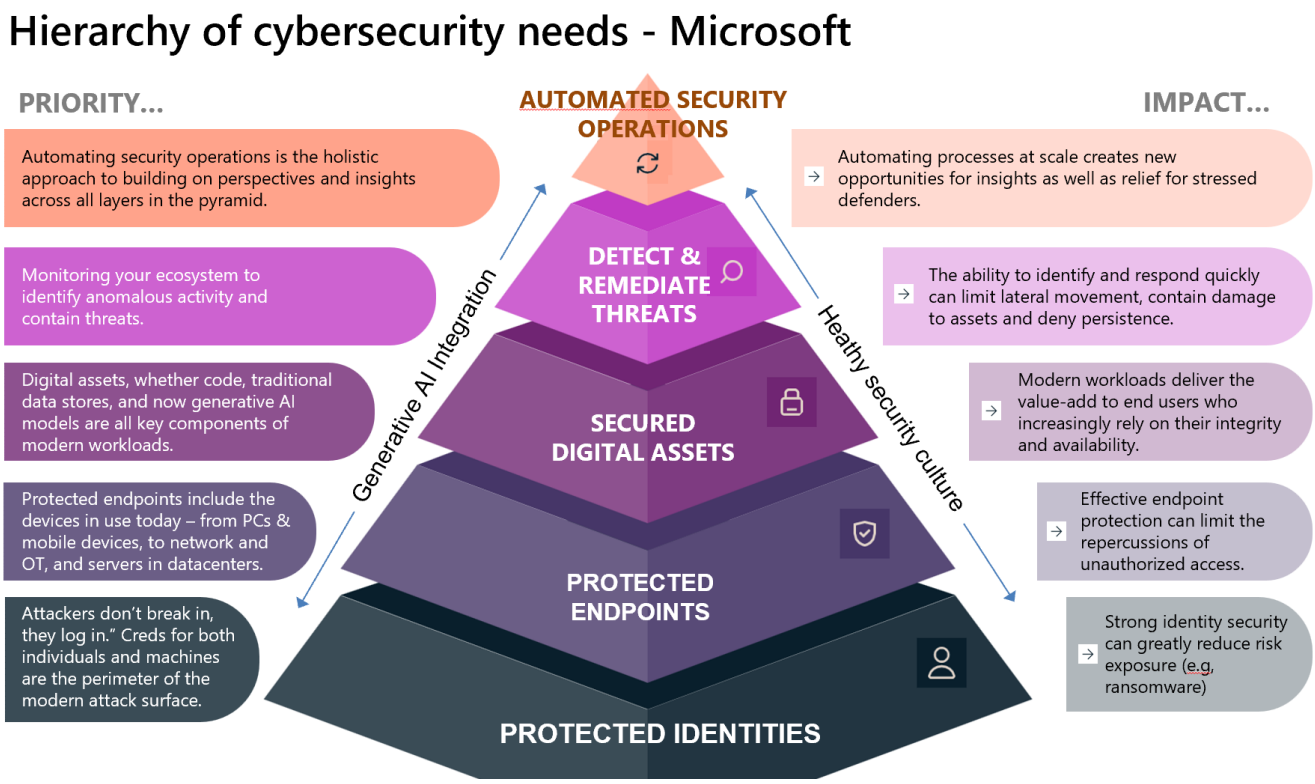


Figure 55 - Hierarchy of cybersecurity needs | Microsoft | Reference: Executive Summary for CISOs

[27] See separate section on "Futures – Agentic AI for Security"

While this pyramid represents a movement toward a robust and optimal security program, the most important/impactful strategy Microsoft has employed has been "***Secure by default***" across multiple security capability areas, in alignment with the Secure Futures Initiative, discussed previously.

Building "Resilience maturity" for the SOC of the future

Reference: MDDR 2024 companion Executive Summary for CISOs

Within the dynamic realm of cybersecurity at Microsoft, the **Microsoft Incident Response (IR) team** regularly confronts a wide spectrum of challenges. Drawing from this rich experience, Microsoft manages its ***resilience maturity*** through a framework[28], and each element is scored/measured as ***Basic, Moderate or Advanced***.

The following recommended practices for enhancing the overall security function reflect key indicators of advanced maturity. While some responsibilities extend beyond Security Operations Center (SOC) teams to IT and Infosec, their implementation reduces cyber risk and operational burden on SecOps.

1. Zero-Trust Strategy and Infrastructure Readiness[29]

- **Zero-Trust Strategy:** Define a desired future state with timelines, continuous evaluation, and improvement.
- **Passwordless Authentication:** Apply to all identities, privileged or standard.
- **Phishing-Resistant MFA:** Mandate strong multi-factor authentication for all user accounts.
- **Endpoint Security:** Deploy endpoint detection and response (EDR) on desktops and servers, with dedicated monitoring teams.
- **Incident Containment:** Enable emergency firewall and endpoint isolation capabilities.
- **Asset Management:** Maintain detailed asset records, including owner, location, and compliance status.
- **Device Compliance:** Ensure only compliant devices access company resources.

2. Incident Response Planning and Management

- **SIEM/SOAR Automation:** Leverage automation with custom playbooks tailored to operational needs.
- **AI-Assisted Response:** Use AI to enhance detection and response times.
- **Crisis Management Protocols:** Develop plans for large-scale incidents, including communication and authority coordination.
- **Mass Credential Resets:** Ensure readiness for password resets and automatic attack disruption mechanisms.

[28] Like many other frameworks, this framework leverages and extends elements of other standards/frameworks for SOC capabilities and security standards overall. For security capability maturing modeling, E.g., CMM has a useful set of open-source templates that are inclusive of NIST CSF framework elements as well – reference: https://www.soc-cmm.com.

[29] Refer to the section on Zero Trust dependencies and alignment

- **Practiced Response Plans:** Maintain detailed, actionable incident response (IR) plans with periodic reviews.
- **Proactive Vulnerability Scans:** Conduct regular automated scans for vulnerabilities.

3. SOC Training and Skill Development

- **Continuous Learning:** Maintain up-to-date training on emerging technologies and threats.
- **Tabletop Exercises:** Conduct regular simulations and implement lessons learned.
- **Interdisciplinary Expertise:** Foster expertise combining cybersecurity, engineering, data science, legal, and regulatory knowledge.

4. Compliance Management

- **Automation Tools:** Use compliance management tools for tracking and reporting.
- **Regular Audits:** Conduct audits to proactively identify and address compliance gaps.

5. Strengthen Third-Party Risk Management

- **Vendor Assessments:** Perform regular security evaluations of suppliers and partners.
- **Contractual Security Requirements:** Include specific cybersecurity obligations in vendor contracts.

This framework highlights actionable practices to strengthen the security posture while fostering continuous improvement and reducing operational workload on security teams.

9. Vision for the SOC of the future

Based on our exploration in this briefing of SOC I, II and III, our vision for the "SOC of the Future" is represented here in three successive stages, which can serve as starting points for you in your modernization journey:

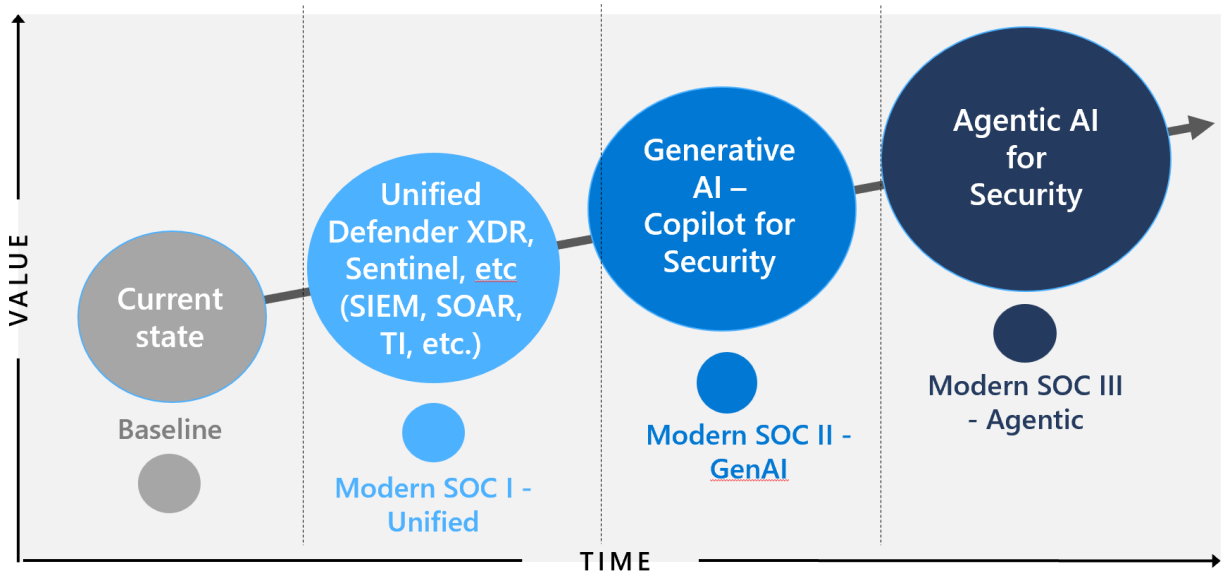


Figure 56 - Evolution of the Modern SOC

Modern SOC I – Unified: In the first stage, the vision is for the organization to progress to a "Modern SOC I – Unified" stage through seamless integration of XDR, Sentinel, TI, and expert services to deliver a unified SOC foundation. This stage represents a state where operational efficiency, enhanced visibility, and strengthened threat detection and response capabilities are performing well against established criteria.

Modern SOC II – GenAI: In the second stage, the vision is for the organization to progress to a "Modern SOC II – Gen AI" stage by transforming SOC workflows with Security Copilot, enabling analysts to improve incident investigation and response performance through natural language AI, intelligent automation, and augmented decision-making, ultimately shifting towards a "**Cognitive SOC**".

Modern SOC III – Agentic AI: In the third stage, admittedly somewhat of a future concept, the vision is for the organization to progress to a "Modern SOC III – Agentic AI" stage by unlocking the full potential of Agentic AI, where AI systems independently learn, adapt, and execute security operations under the watchful guidance of human governance and control.

As emerging capabilities like "Agentic AI computing" start to surface within Microsoft security products, SOCs practitioners – augmented by assistive technology - will be able to address new and evolving threats and at lower cost as they progress towards a "Modern SOC III" with Agentic AI.

10. Realizing the vision with Microsoft Industry Solutions

To transition customers towards the "SOC of the Future," Microsoft Industry Solutions recommends following "SOC of the future" envisioning activities (highlighted in the previous section) with a strategic plan. This journey involves assessing current capabilities, developing a strategic roadmap, and deploying and integrating key technologies aligning to your requirements and vision.

By partnering with Microsoft Industry Solutions, organizations can access a wealth of technology expertise and Services offerings to accelerate their SOC transformation.

In summary, Microsoft Industry Solutions offers the following capabilities and services to help customers realize their vision for the SOC of the future:

Figure 57 - Microsoft Industry Solutions - Capabilities and Services

Example engagement

Below is an example plan outlining the key steps involved in achieving this multi-horizon transformation:

1. SOC Assessment

- Current state analysis
- Security posture review
- Workforce assessment

2. Strategic roadmap

- Define future state objectives and customer vision
- Technology selection and integration plan
- Timeline and milestones.

3. Security modernization

- Unified security platform implementation.
- Threat automation and incident Response enhancement
- Migration from 3rd party security solutions
- Security Copilot configuration/extension/automation

Services offerings

Microsoft Industry Solutions has a number of Services offerings and component capabilities that address the SOC security space and SOC modernization vision covered in this briefing. These include (but are not limited to) the following:

Strategy and Planning	**Microsoft Defender XDR component implementation**	**Microsoft Sentinel**	**Security Copilot**	**Other**
Cybersecurity envisioning*	Defender for Office 365	Implementation and operationalization	Security Copilot Planning, Implementation and Integration	Intune device management
Cybersecurity strategy	Defender for Identity	Migration (from 3rd party SIEM solutions)		Entra ID identity protection
Cybersecurity architecture and roadmap	Defender for Endpoint			Privileged Access Workstation (PAW) for Cloud Service Management
	Defender for Cloud Apps			Security Operations Model Planning and Implementation
	Defender for Cloud			
	Defender for IoT			

*__Next steps__: schedule an Envisioning workshop with key stakeholders to identify areas of interest and determine how Microsoft Industry Solutions can help you get started on your journey.

Conclusion

The SOC of the future will be a highly adaptive, evolving, intelligent, and integral part of any leading organization's defense strategy. By understanding and planning for the technological advancements and regulatory changes highlighted here, organizations can build SOCs that are not only equipped to handle current threats and guardrails but are also prepared for future challenges.

By taking a forward-thinking approach, organizations can ensure their SOC remains effective and compliant in an ever-changing cybersecurity landscape, while improving key metrics for CISOs and SOC operations.

Transitioning to the SOC of the future is an essential endeavor in today's evolving cyber threat landscape. By following a detailed plan from **Microsoft Industry Solutions**, we will lead you and your team through the transformation, enhancing your security posture, improving compliance, and positioning you to proactively address current and future challenges.

Embracing innovation, investing in people, and fostering a strategic partnership with **Microsoft Industry Solutions** are critical components of this journey toward a resilient and adaptive security operation.