Microsoft

Upgrade your cybersecurity in the era of AI

Let’s imagine a new future for cybersecurity

How would your life change if some of your biggest security and staffing concerns disappeared tomorrow?

Picture this: your SOC team is freed up to focus their time on active incident response rather than manually triaging alerts, researching attack vectors, and compiling reports. If a breach occurs, it is detected and automatically disrupted before your SIEM can even ingest the security logs—evicting adversaries before they ever get the chance to cause harm.

For more nuanced attacks that require human intervention, boost your SOC analysts’ speed with guided investigation tools, script analysis, and query assistance—supercharging their existing skill set to the next level with the help of AI. And when your team needs in-depth human assistance, experts are available to them for around-the-clock support.

What if this was all possible today? What if you could rewrite the game and turn the tables on threat actors with the power of AI behind you and your team? What if you could identify and mitigate potential threats at a far greater speed and accuracy than ever before possible?

At Microsoft, we’re taking large strides toward this future, working hand-in-hand with our customers to leverage the latest advancements in AI and ML, the breadth and depth of our global threat intelligence, and the full capabilities of the Microsoft Defender suite to build the future of cybersecurity, together. Let’s see what’s possible.

What if?

You could stop attackers in their tracks, before your SIEM has even ingested the logs?

You could reduce your threat response time by 88% and resolve incidents within 55 minutes?

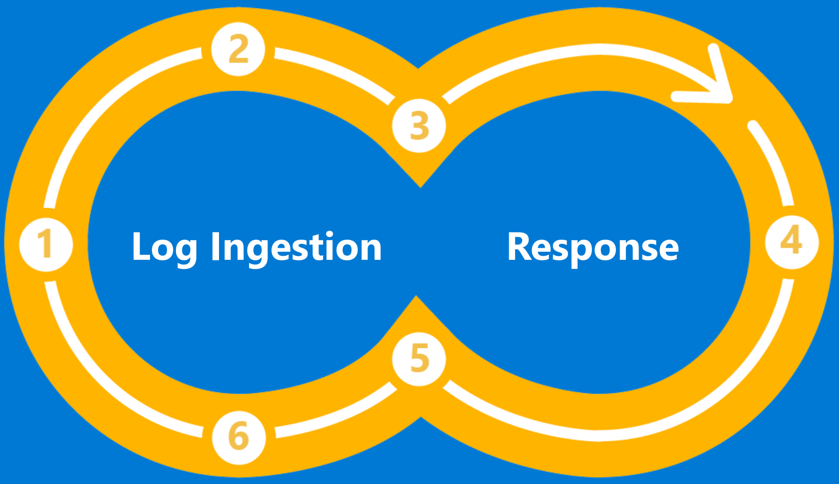
You could upskill your entire SOC team without asking them to spend hours in training?

You could harness the power of the world’s largest security vendor to threat hunt across your landscape?

Resolve incidents at the speed of attackers

SEIM Platforms are Post-Breach Detection Tools

Hypothetical SIEM, SOAR, and SOC Response Times



1-2 min
Activity is written to vendor's internal log

5-10 min
Logs are shipped to your SIEM.

5-15 min
Scheduled detection rules run on ingested SIEM logs.

5-10 min
SOAR rules correlate logs from multiple vendors.

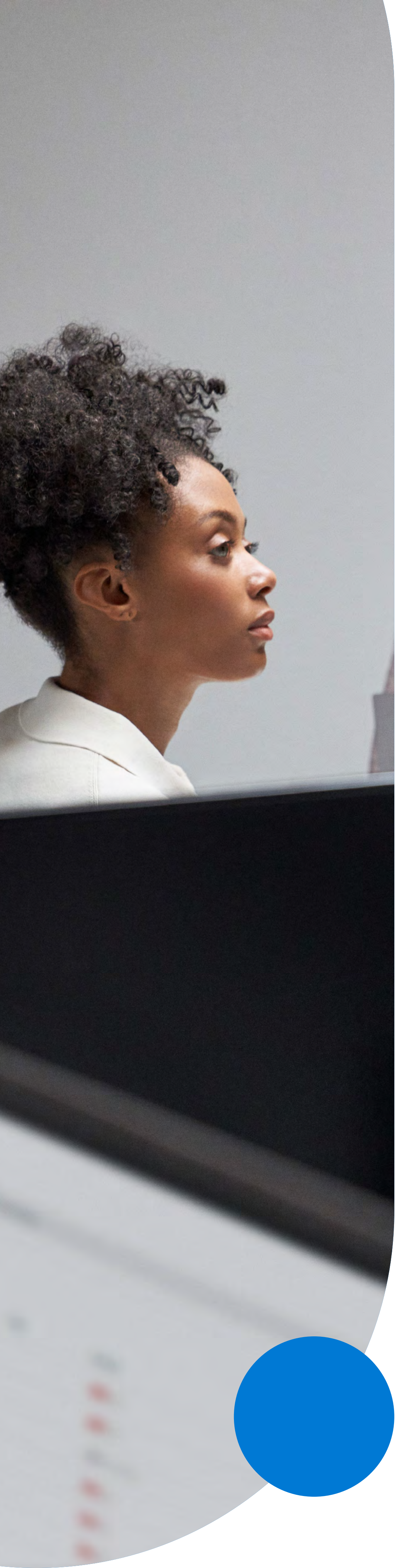
Teir 1: 10min
Teir 2: 45 min
Tier 1 & 2 Analyst triages the alert and reviews response playbook.

Attacker spreads laterally, generates new alerts. Legacy Log Aggregators may require manual incident correlation.

In today's rapidly evolving security environment, SIEM platforms are morphing into security data lakes for post-breach detection and forensics investigations. They're excellent for providing visibility into adversarial activity across your entire environment and aggregating third-party logs. However, they cannot detect attacks fast enough to prevent adversaries from breaking out. It takes 79 minutes on average for interactive eCrime intrusion activity to break out, and adversaries have even been known to break out in as little as seven minutes.[1]

XDR can help, but multi-vendor solutions suffer from ingestion latency as each third-party vendor must ship their logs to a separate vendor that performs the XDR correlations—creating the same delay problems as SIEMs. Microsoft Defender XDR avoids this problem because all products within the Defender XDR suite write to the same logging platform and data model, meaning detections can run in near-real time without experiencing log shipping delays.

[1] CrowdStrike 2023 Threat Hunting Report



Additionally, most XDR platforms lack a first-party cloud Identity Provider (IdP). When attackers flood your IdP solution with fake attacks, data exports are throttled as the export service hits API rate limits—ultimately leading to substantial ingestion delays. Multi-stage attack detections cannot be performed until logs from each vendor have been ingested and parsed into a common data model. To increase query performance, some detections might be run on a schedule instead of near-real-time. However, by the time your log aggregator detects the incident, the attacker is already moving laterally throughout your environment and wreaking havoc.

Security teams must accelerate threat detection and response if they are to turn the tables on threat actors.

What if you could use automation to stop an attack in its tracks?

Automatic Attack Disruption is the next evolution of threat response and comes built-in with Microsoft Defender XDR.

As one of the largest software companies in the world, Microsoft is a significant target for adversaries. And while this means our network is frequently attacked, it also gives us a first-hand understanding of the latest global threat vectors and what it takes to successfully stop them. Microsoft Defender XDR takes data from these experiences to create a complete picture of how a “normal” operating environment should behave.

By correlating trillions of individual signals from across the Microsoft stack, we’re able to flag system abnormalities more quickly and identify active ransomware campaigns or other sophisticated attacks with a high level of confidence. Once these markers have been identified, Automatic Attack Disruption is triggered to contain any in-progress attacks. This limits the impact on an organization’s assets and gives SOC teams more time to remediate the attack fully.

[2] Microsoft Digital Defense Report 2022

Unlike known protection methods such as prevention and blocking based on a single indicator of compromise, Automatic Attack Disruption leverages cross-domain security signals that have been automatically correlated across the entire Microsoft Defender platform—including identities, devices, messaging, data, and apps. This ensures the entire attack is taken into account. Automatic Attack Disruption can also act on third-party signals, such as those from SAP.

We've further strengthened this offering with new deception capabilities in Microsoft Defender for Endpoint—which uses generative AI to create authentic-looking decoys and lures. This enables defenders to entice cyber attackers with fake valuable assets that will deliver a high-confidence, early-stage signal to the SOC and trigger Automatic Attack Disruption even faster.

Automatic Attack Disruption is also vigorously and continually vetted. It uses indicators of compromise and indicators of attack rules that were written and manually graded by security researchers to require a >99% signal-to-noise ratio. With Automatic Attack Disruption, SOC teams still have complete control when investigating, remediating, and bringing assets back online.

What's your mean time to detection and resolution?

- 54% of distributed denial of service (DDoS) attacks last 30 minutes or less
- On average, it takes an attacker 1 hour 12 minutes to access private data after the user clicks on a phishing email
- Once a device is compromised, the average attacker begins moving laterally throughout the network in 1 hour 42 minutes

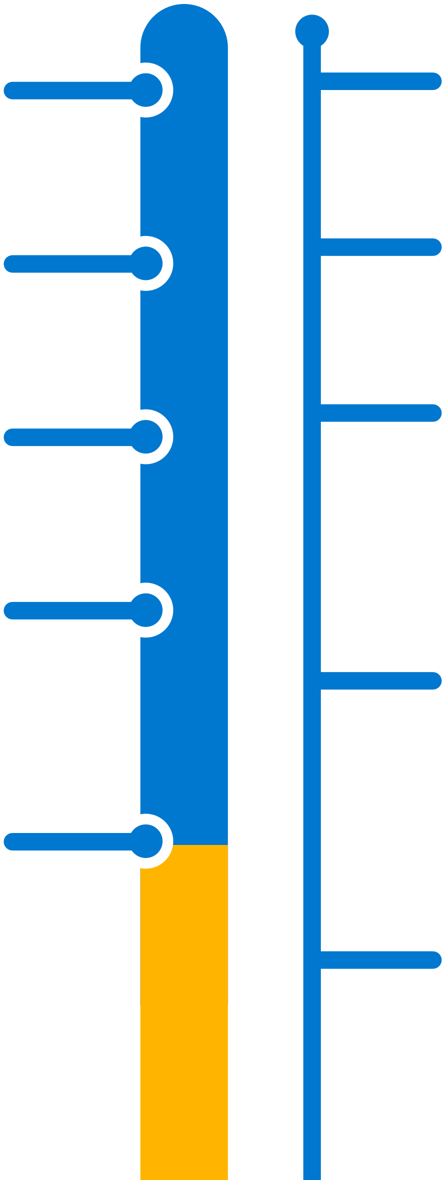
Automatic Attack Disruption in action

The problem: A threat actor targets an EU-based customer with over 1,000 monthly active devices. The adversary carried out a series of human-operated ransomware attacks in an attempt to compromise users' devices and move laterally into the network.

The solution: Powered by Defender for Endpoint, Defender Antivirus, Defender for Identity, and Entra ID P2, Automatic Attack Disruption triggered a series of responses that stopped the threat just 14 minutes after the first sign of incriminating activity.

The results: The threat was automatically disrupted 14 minutes after the first successful attack, 67 machines were protected by automatically disabling compromised users and devices. Attack disruption has rapidly evolved to now stopping human-operated attacks, on average within 3 minutes, with just Defender for Endpoint.

Human Operated Ransomware (HumOR)



Jan. 20 - 8:00am

Threat Actor connects via RDP.

Attacker drops Lockbit payload.

Jan. 20 - 9:48am

Attacker attempts to disable MDE for > 20 min.

Jan. 20 - 11:15am

5 Unmanaged devices encrypted remotely.

Jan. 20 - 11:28am

Attacker begins lateral movement to distribute the Lockbit payload.

Jan. 20 - 11:29am

- User account automatically disabled
- All user tokens revoked automatically
- All machines in attack are contained by MDE

Lockbit payload is blocked by **MDAV** using Real-Time Protection.

Tamper Protection blocks attacker's attempts to disable **MDE**.

MDI detects lateral movement. Confirms user accounts as compromised

User disabled in cloud and on-prem via **MDI** sensor on Domain Controllers. **MDE** prevents all onboarded devices from communicating with compromised devices. (Requires Network Protection enabled and MDE in active mode.)

Remediation actions and summary available in **Defender XDR portal** and notification sent via email

Upskill existing analyst teams instantly with AI

Today’s cyber threats demand a new approach to security. There is a critical imbalance between the number of potential entry points security teams have to protect and weaknesses that adversaries can exploit. Microsoft Copilot for Security levels the playing field.

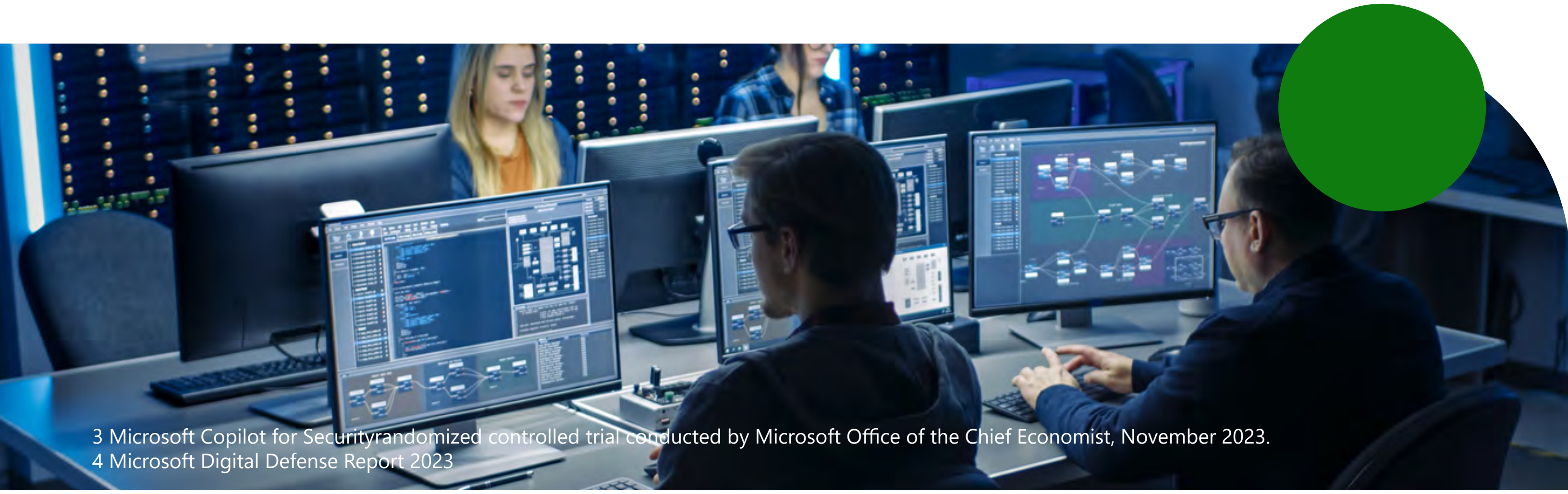
What more could you do with a fully equipped, fully empowered SOC team?

- In a productivity study of “new-in-career” analysts, participants using Copilot for Security demonstrated **44%** more accurate responses and were **26%** faster across all tasks
- **86%** reported that Copilot for Security helped them improve the quality of their work
- **83%** stated that Copilot for Security reduced the effort needed to complete the task[3]

What if your SOC team could move faster and do more?

Security teams have a deep understanding of their environments. Before an attack can even begin, SOC analysts have the home field advantage because they know how their infrastructure, user posture, and applications are set up.

Copilot for Security builds on that knowledge base by equipping analysts with the power of large-scale data. This data includes 65 trillion daily signals, global threat intelligence, monitoring data on more than 300 cyber threat groups, and insights on cyberattacker behaviors from over 1 million customers and more than 15,000[4] partners. Combined with Microsoft’s end-to-end security that’s built on the principles of Zero Trust, this data allows Copilot to tip the scales back in favor of your security teams. **And, because Copilot for Security is built with security, privacy, and compliance at the forefront, you can rest easy knowing that your enterprise data is protected.**



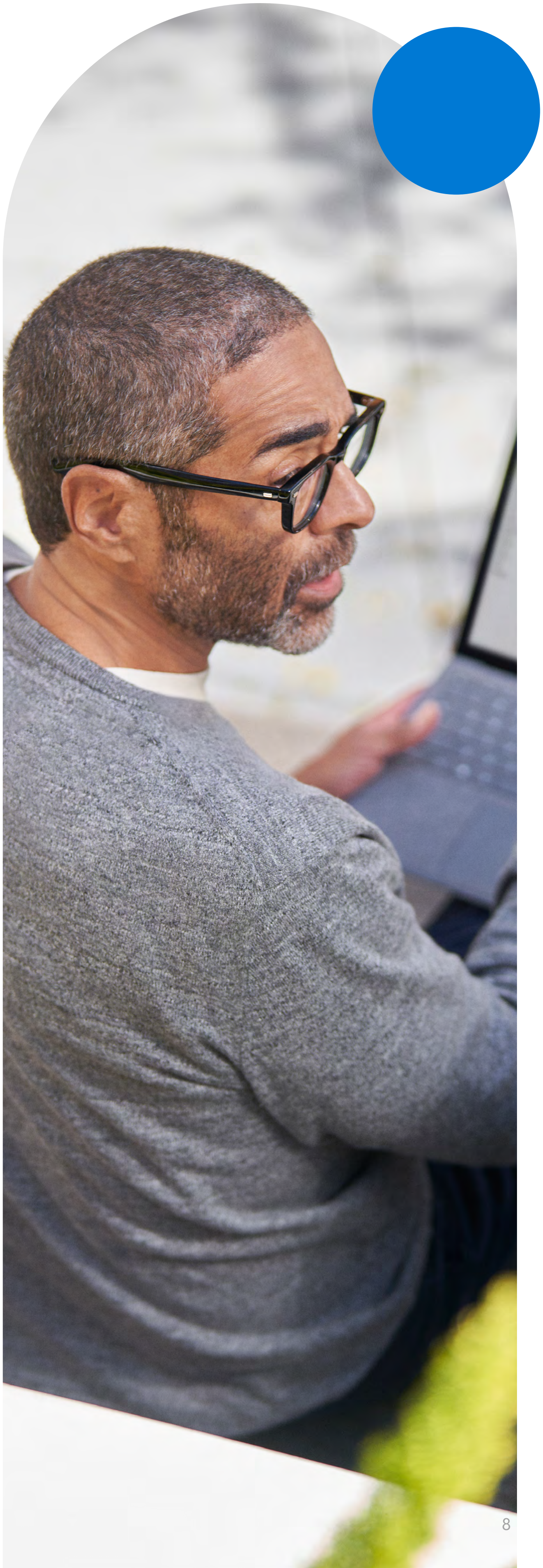
[3] Microsoft Copilot for Securityrandomized controlled trial conducted by Microsoft Office of the Chief Economist, November 2023.
[4] Microsoft Digital Defense Report 2023

Because Copilot for Security is powered by leading-edge generative AI, its use cases are constantly expanding and improving. Today, early access customers can:

- **Increase your security posture management** by summarizing vast data signals into key insights to cut through the noise, detect threats before they cause harm, and reinforce your security posture
- **Decrease your time to incident response** by equipping security teams with critical insight from Microsoft global threat intelligence, giving them the context they need to respond to incidents in minutes rather than hours or days
- **Strengthen security team expertise** by providing junior staff with guided response on how to perform more advanced capabilities and enabling expert staff to the hardest challenges, thus elevating the proficiency of the entire team

Driven by the security industry's biggest pain points, Microsoft is evolving Copilot for Security even further—announcing that we are combining its power of generative AI for security with Microsoft Sentinel and Microsoft Defender XDR to create the first unified security operations platform.

This platform will equip SOC teams with a unified incident experience that streamlines triage and provides a complete, end-to-end view of threats across the digital estate. It will also provide analysts with a unified threat-hunting experience, enabling them to query all SIEM and XDR data in one place to uncover cyber threats



Embed expertise within your organization

Despite the transformative potential of AI across many use cases, there's no replacement for human expertise. Microsoft understands this, and we also know that the security industry needs more skilled human operators to build the next generation of defenders. That's why we offer Microsoft Security Experts.

Security Experts is a managed service offering that enables companies to augment their teams and Copilots with hands-on assistance from Microsoft experts across security, compliance, identity, management, and privacy. To further scale this capability, we have expanded Security Experts with Microsoft Verified Solution partners—a fully-vetted managed XDR solution.

Microsoft verified MXDR partner solutions provide 24/7/365 managed SOC services, including advanced hunting, customer detection, response, and remediation across the Microsoft unified XDR product portfolio. All verified MXDR partners have access to product APIs to ensure seamless service integration between the partner's solution and Microsoft threat intelligence—making it easy for them to quickly identify and resolve emergent security issues.

All partners must pass an extensive validation and verification process in order to be verified, and we re-evaluate current partners annually to ensure they continue to meet updated technology and performance standards. Furthermore, we require our verified MXDR partners to have a proven end-to-end process with around-the-clock incident monitoring, advanced hunting, and resolution across Microsoft 365 Defender and Microsoft Sentinel.

Within the Security Experts suite, we also offer Defender Experts for XDR to help customers proactively respond to threats around the clock. This first-party MXDR offering delivers cross-domain telemetry and leading threat intelligence to extend your team's threat-hunting capabilities, triage all alerts, and provide tier-2 response.

Powered by our best-in-class XDR suite, Defender Experts for XDR offers managed detection and response, proactive threat hunting, live dashboards and reports, regula check-ins, and a seamless onboarding process. We also offer the Microsoft Incident Response Retainer—an end-to-end portfolio of proactive and reactive incident response services such as assigned security delivery and incident managers, intelligence-driven investigations, compromise recovery, and quarterly threat briefings.

All Security Experts services are equipped with the full scale of Microsoft's cyber defense experience and global threat intelligence.

A Microsoft Defender Experts for XDR use case

The problem: A Microsoft customer fell victim to an unknown targeted Gozi malware campaign. The threat group evaded initial detection methods by sending an email from a known vendor's email account with an attachment that contained the Gozi malware. Because the email came from a vendor that frequently communicated with the customer via email, Defender for Office did not automatically block the email.

The solution: However, thanks to Defender Experts for XDR, Microsoft personnel flagged the attack in real-time, having written a query that sounded an alarm for the email based on historical intelligence.

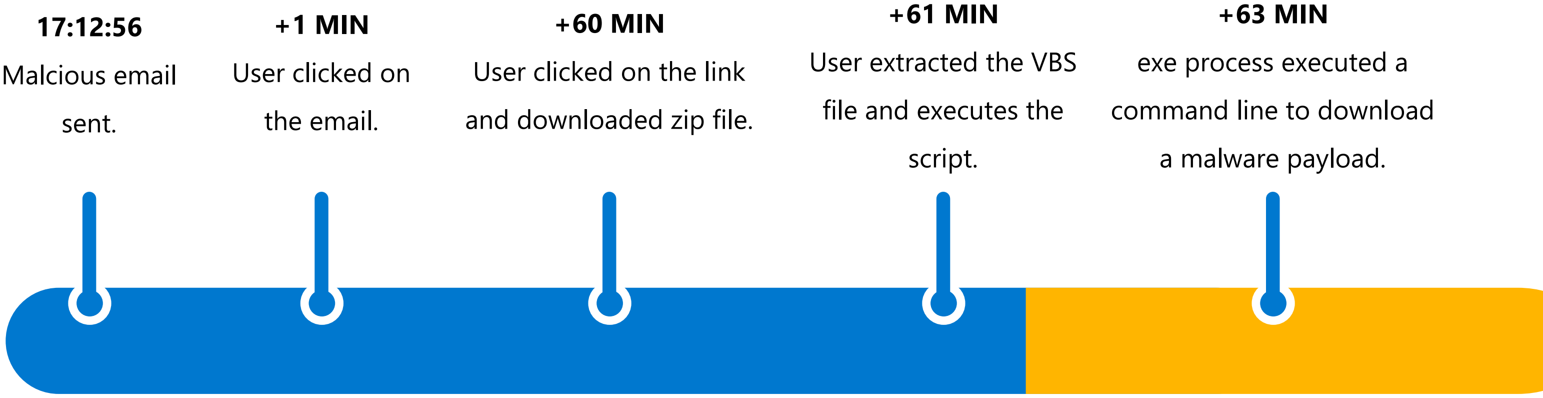
The query was looking for a suspicious pattern where a likely vendor (marked by our analytics tools) sent an email with a VB script in the attachment. Even though the VB script did not contain known malware, it was still suspicious because vendors are often marked as "safe senders" and this is a known vector for supply chain compromise.

As the attack unfolded, the Microsoft hunting team was actively investigating the incident, tracking the cross-domain signal from Defender for Office and Defender for Endpoint to validate that the attachment was malicious and contained malware. They followed the attack path and were able to attribute the malware to Gozi thanks to expert guidance from the endpoint team in the Microsoft Security Response Center.

The results: Microsoft hunters identified subsequent victims just 2 hours after the initial attack, opening an incident to provide context to the customer and sharing a Defender Expert Notification with remediation instructions.

Following the incident, the attacker's URL was marked as malicious in Defender for Office and its signature was attributed to Gozi malware in Defender for Endpoint. Defender for Office was able to block subsequent emails from the attacker and retroactively block other emails with the malicious URL that had previously been sent, preventing the malware from landing. Ultimately, the customer was able to place a compensating control of the suspicious network traffic block that prevented the connection of this adversary at the proxy level.

Unknown Targeted Gozi Malware Campaign



17:12:56
Malcious email sent.

+1 MIN
User clicked on the email.

+60 MIN
User clicked on the link and downloaded zip file.

+61 MIN
User extracted the VBS file and executes the script.

+63 MIN
exe process executed a command line to download a malware payload.

The security landscape is changing rapidly. Vendors and their customers must work together to evolve our cyber defenses to exceed the speed of attackers and create a safer digital environment for all.

Microsoft stands ready to meet this challenge, investing in the latest advancements in AI and ML and growing our leading, global database of connected threat intelligence to help you upgrade your cybersecurity capabilities.

We look forward to bringing about a new era of cybersecurity and AI, together.

Explore the full suite of Microsoft Defender threat prevention, detection, and response capabilities.

Learn More >

Microsoft