News Analyst reports Microsoft Defender XDR

8 min read

Microsoft 365 Defender demonstrates 100 percent protection coverage in the 2023 MITRE Engenuity ATT&CK® Evaluations: Enterprise

By Tanmay Ganacharya, Partner Director, Security Research, Microsoft 365 Defender

September 20, 2023

Microsoft Defender Microsoft Defender for Endpoint

For the fifth consecutive year, Microsoft 365 Defender demonstrated industry-leading extended detection and response (XDR) capabilities in the independent MITRE Engenuity ATT&CK® Evaluations: Enterprise. The attack used during the test highlights the importance of a unified XDR platform and showcases Microsoft 365 Defender as a leading solution, enabled by next-generation protection, industry-first capabilities like automatic attack disruption, and more.

Microsoft 365 Defender demonstrated 100 percent visibility and complete coverage across all stages of the attack and achieved 100 percent protection across both Windows and Linux, showcasing the strong multiplatform capabilities of the solution. These results demonstrate that Microsoft's XDR provides organizations with industry-leading visibility and protection in a world of evolving threats.

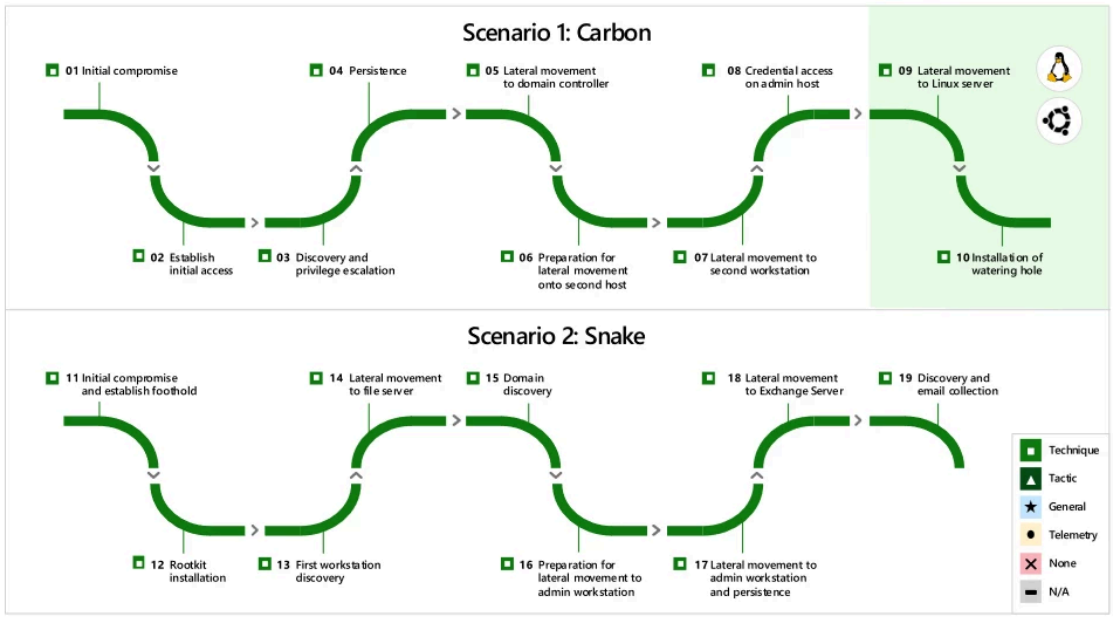


Figure 1. Microsoft 365 Defender providing full attack chain coverage.

These results are only possible with continuous innovations built on the feedback of our customers. In just the last 12 months, Microsoft 365 Defender strengthened its endpoint protection with capabilities such as automatic attack disruption, which uses AI to suspend in-progress ransomware attacks, the release of a unified device settings management experience, and expanded identity protection to include Active Directory Certificate Services (AD CS).

This year's ATT&CK® Evaluations emulated the Turla threat group, tracked by Microsoft Threat Intelligence as Secret Blizzard. They are a Russian-based activity group that has been primarily targeting government organizations worldwide since the early 2000s. They employ extensive resources to remain on a target network in a clandestine manner, making detection more challenging for traditional security products.

Let's take a closer look at how Microsoft 365 Defender once again achieved industry-leading results in this year's MITRE evaluation and how Microsoft's AI breakthroughs are shaping the future of security to respond to threats like Turla.

100 percent visibility across all stages of the attack chain in real-time

In the face of a rapidly evolving threat carried out by adversaries like Turla, the speed of response makes a significant difference in a security team's effectiveness in mitigating an attack. A single delay can mean the difference of your organization's devices getting encrypted or not. Microsoft 365 Defender's XDR platform accelerates the security team's ability to respond by providing real-time, unparalleled breadth and depth of understanding an attack, starting with 100 percent visibility in real-time. This unique breadth of Microsoft's XDR extends across **endpoints, network, hybrid identities, email, collaboration tools, software as a service (SaaS) apps, and data** with centralized visibility, powerful analytics, and automatic attack disruption.

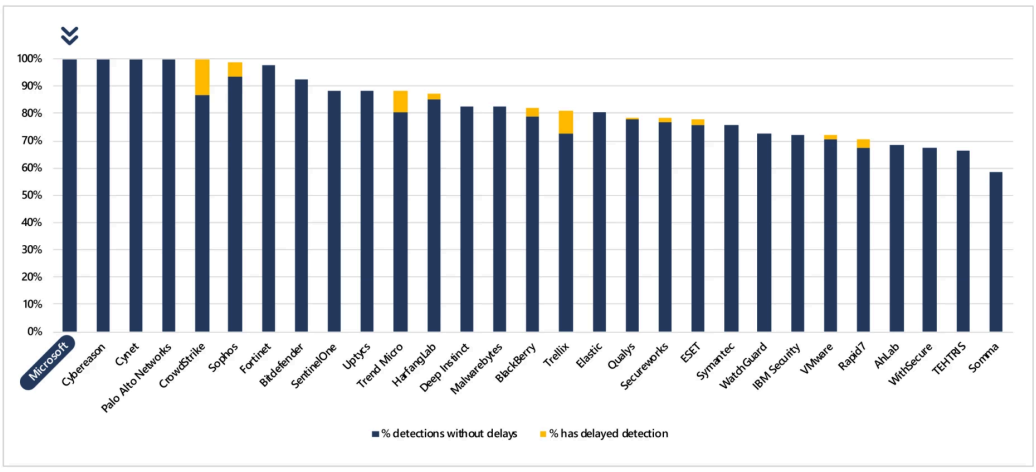


Figure 2. Microsoft 365 Defender provides 100 percent visibility without delay in every attack stage.

100 percent ATT&CK technique-level detections at every attack stage without delay

As an attack unfolds, security teams need to know what they're up against the moment it's happening. Delayed and incomplete detections make it difficult for analysts to understand the attack in full, providing attackers an opportunity escalate their campaign by moving laterally, stealing credentials, or executing other malicious activities. With Microsoft 365 Defender's 100 percent real-time ATT&CK technique-level coverage, analysts immediately receive relevant details within the alert that describe the attacker's approach, equipping them with the knowledge to effectively and rapidly respond.

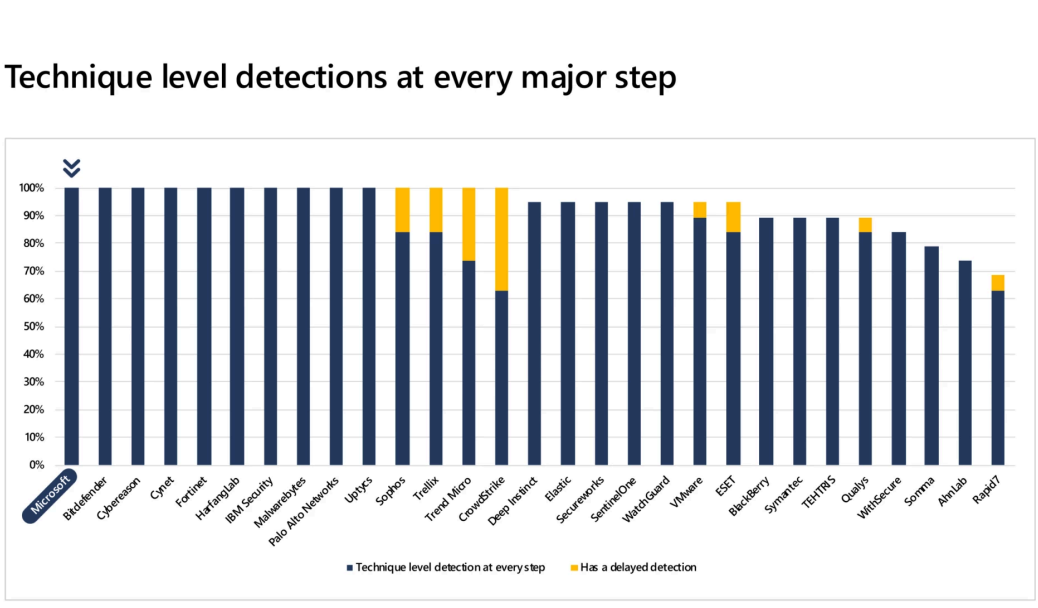


Figure 3. Microsoft 365 Defender delivers ATT&CK technique-level detections at every attack stage without delay.

100% protection for every attack stage across Windows and Linux

This is the third year that MITRE has included a protection scenario as part of the evaluation, and for the third year running, Microsoft 365 Defender successfully blocked 100 percent of the attack stages across Windows and Linux platforms. Microsoft's AI-powered next-generation protection blocked each attack attempt across 13 steps, representing complete prevention of any malicious activity. This outcome showcases the strong multiplatform capabilities of the solution, independent of the device's operating system.

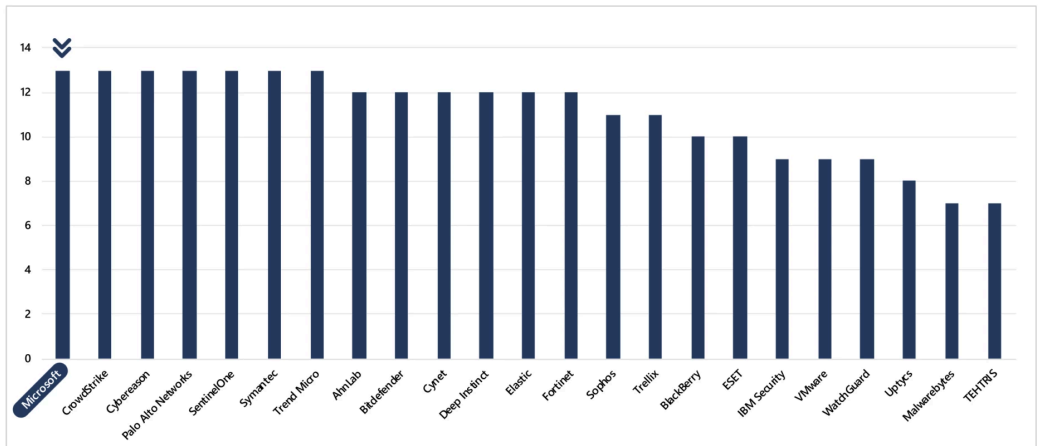


Figure 4. Microsoft 365 Defender blocks every attack stage across Windows and Linux.

Deep visibility into Linux devices

With the prevalence of increasingly complex attacks, visibility into low-level protocols is critical for security teams to protect against sophisticated network sniffing and drive-by compromise attacks. Microsoft 365 Defender provides that visibility through ingestion of raw socket operations as well as into script content on Linux devices. It also takes action on script content that is obfuscated or encrypted, as well as suspicious network and other protocol behaviors.

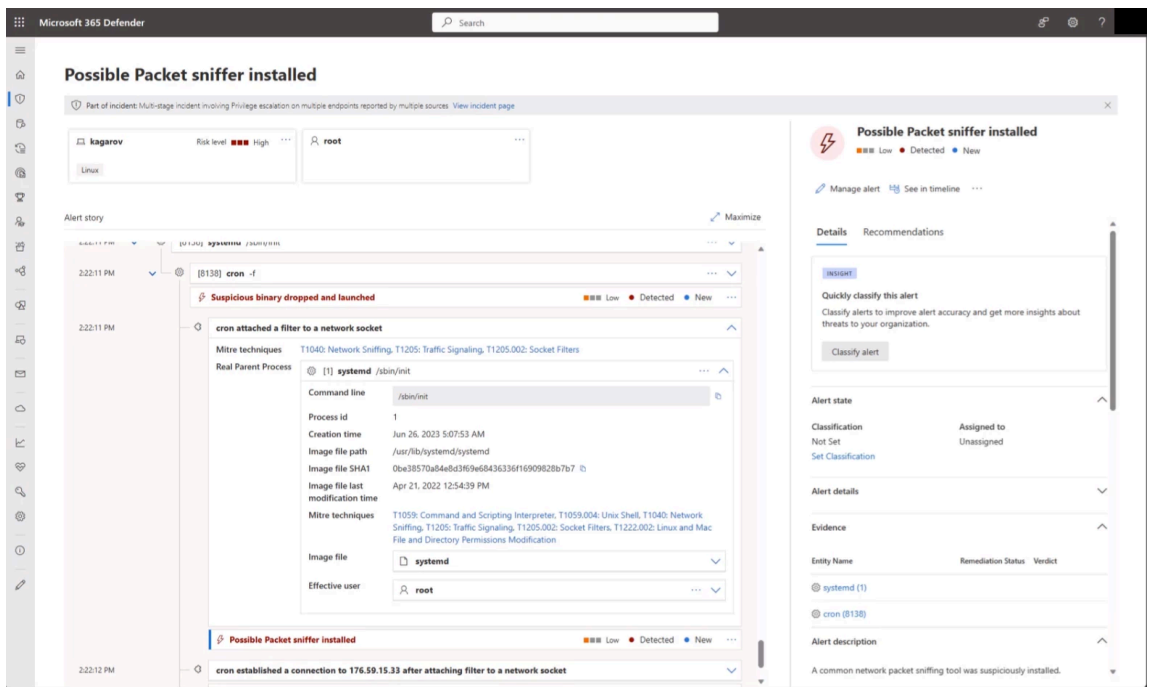


Figure 5. 9.A.12: Traffic Signaling (T1205) and 9.A.13: Network Sniffing (T1040).

Eliminated blind spots with network detection and response

Several stages of the Turla emulation involved network-based techniques. They are an increasingly popular way of infiltrating and moving across systems laterally as they leave minimal traces on source and target devices. Security teams gain full visibility into network traffic with Microsoft 365 Defender's network detection and response capabilities. As a result, analysts receive high-confidence, context-rich

alerts to hunt down and block these sophisticated attacks early in the kill chain. In addition, analysts can discover both managed and unmanaged devices, identify blind spots, and reduce their attack surface to increase their security posture.

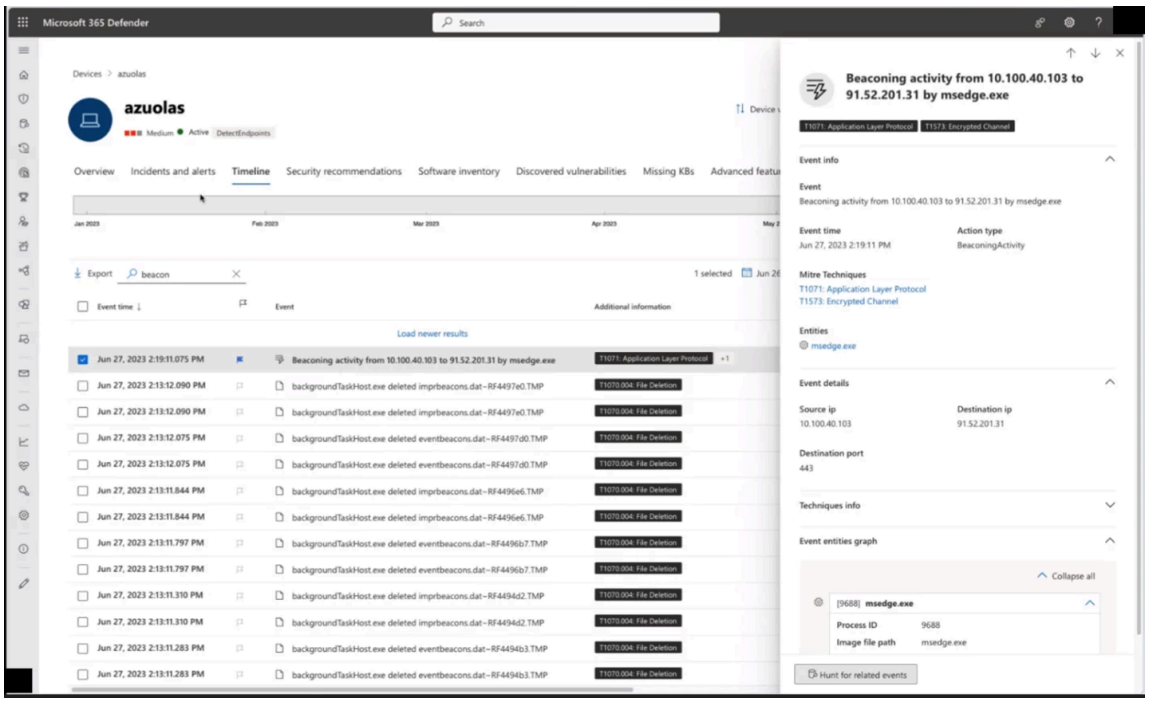


Figure 6. Sub-step 11.A.5 identifies beaconing behavior determining it to be a command-and-control type activity based on process and network frequency analysis.

Deep visibility into each stage of lateral movement

Adversaries wage increasingly sophisticated campaigns by moving across hosts in a domain. The test involved significant lateral movement with a total of 6 steps, which is more than 30 percent of the total steps. Microsoft's XDR solution provides visibility into each stage of lateral movement, whether access is gained through brute force (5.A.3), valid accounts (14.A.3), pass the hash (17.A.1) or any other technique. When tools are being transferred laterally (sub-steps 5.A.6, 18.A.3), Microsoft's XDR shows the full context of what was transferred, from which host to which destination. Whether the execution on the target host happens through masqueraded PsExec (17.A.1), plink.exe (9.A.5), or WMI (18.A.5), we provide detection and visibility.

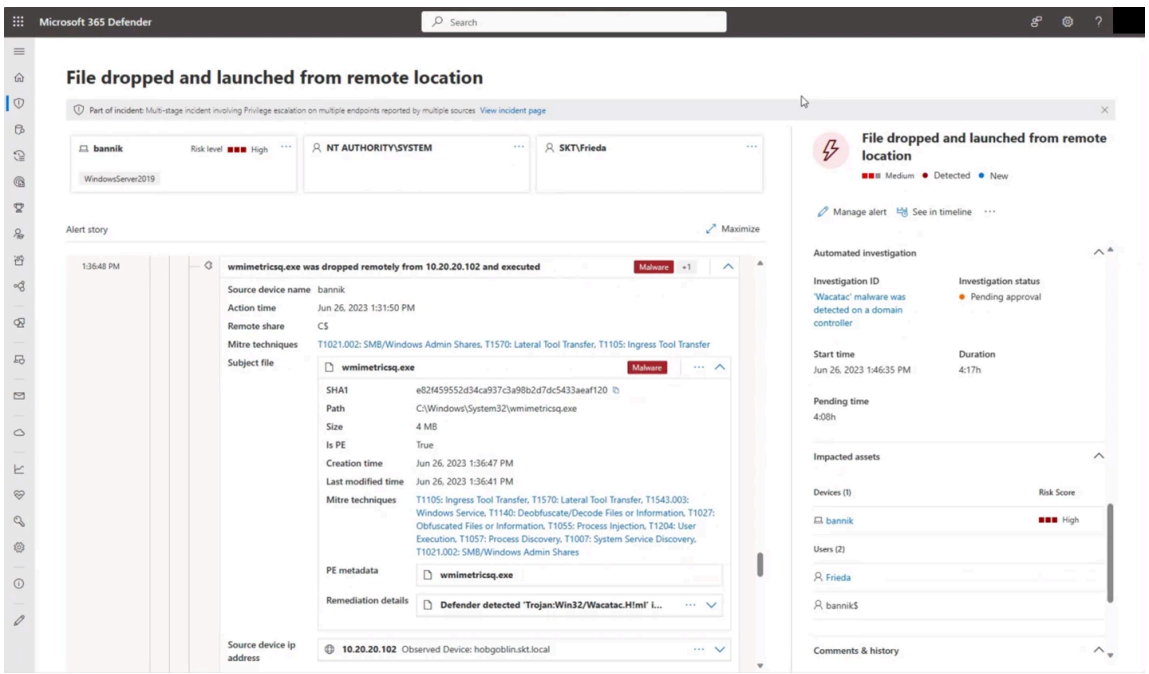


Figure 7. Sub-step 5.A.6 Microsoft 365 Defender portal showing tools being transferred across hosts.

Identity threat detection and response spanning the cloud to on-premises

Part of the MITRE evaluation emulated one of the fastest-growing threat vectors—identity-based attacks where malicious actors seek to exploit identities in the cloud and on-premises, or the underlying infrastructure and policies governing them. Microsoft XDR has native endpoint and identity protection to counter these types of attacks by providing security teams with high-fidelity, contextual signals that other vendors either lack entirely or require a separate integration for. Throughout

the attack, Microsoft 365 Defender provided visibility on all identity-related attack steps like sensitive group enumeration, password spraying, and creation of accounts and unusual additions to sensitive groups.

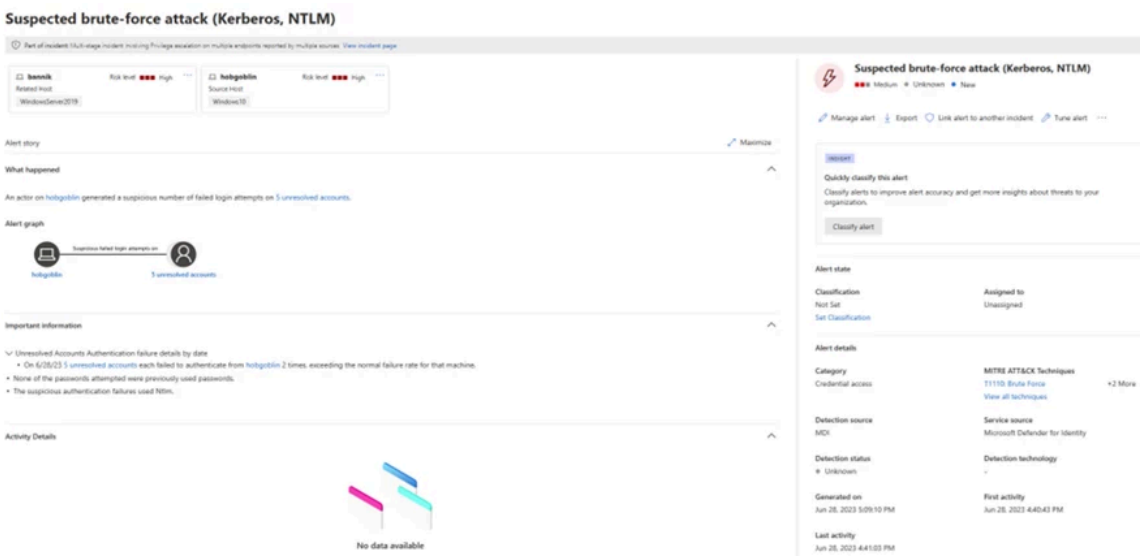
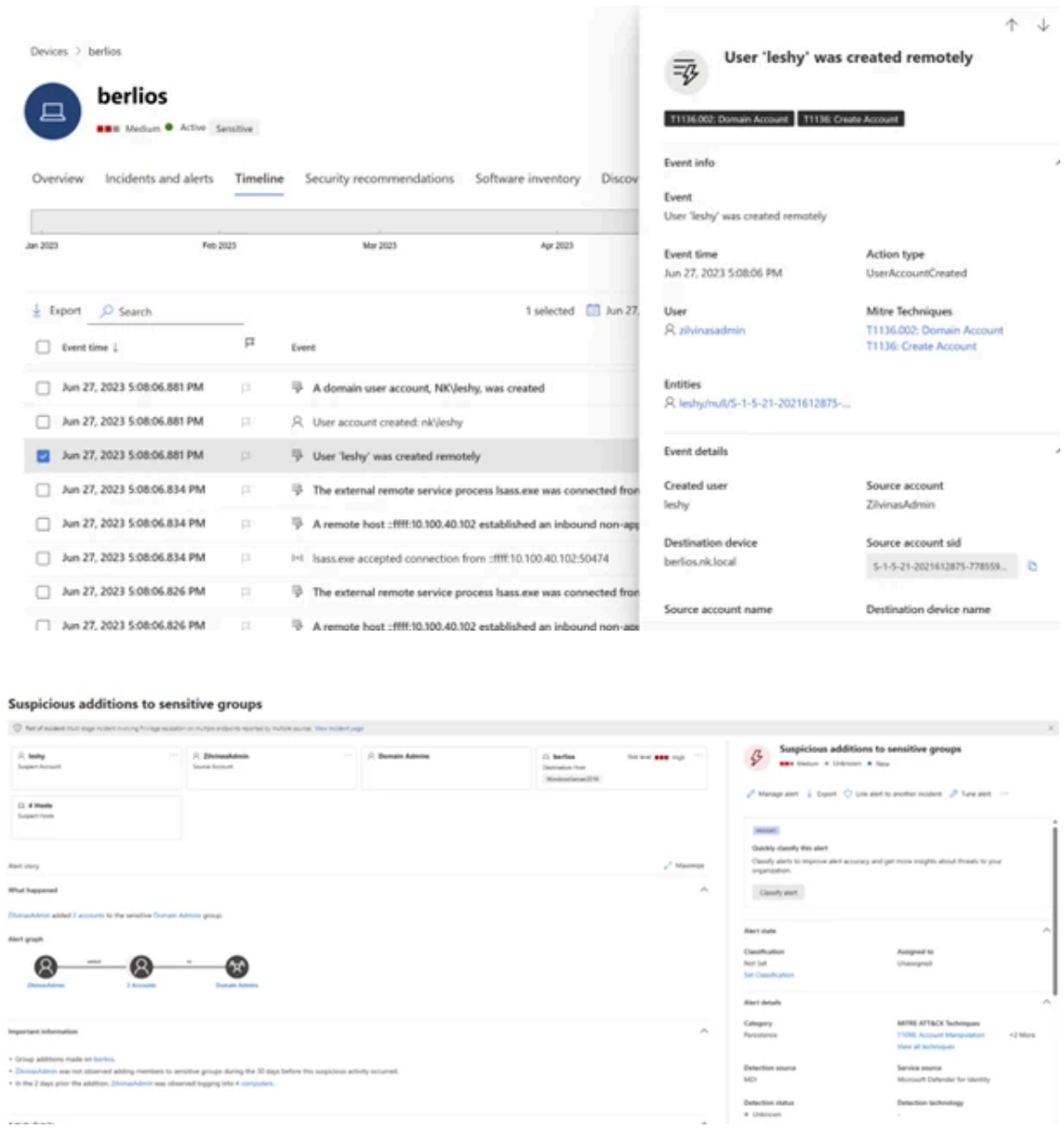


Figure 8. Sub-step 5.A.3: Our identity sensors on Active Directory revealed the utilization of the Password Spraying technique, providing information about the users whose login attempts failed and number of such attempts.



Figures 9 and 10. Sub-step 17.A.5: Active Directory signals revealed the creation of accounts and unusual additions to sensitive group, all aimed at establishing persistence.

Security in the era of AI

The MITRE ATT&CK evaluation focused on detection and prevention in the case of one type of attack, for which Microsoft effectively blocked at the earliest step at every attack stage. In real world scenarios where millions of attacks are waged every day, sometimes adversaries can breach the security perimeter. With AI breakthroughs introduced by Microsoft, security teams have already seen first-hand how they can scale their defenses against breaches and respond in novel ways that challenge the assumption of an asymmetric battlefield.

Announced in November 2022, Microsoft 365 Defender's unique, industry-first automatic attack disruption stops the most sophisticated attack campaigns at machine speed like this Turla attack, spanning ransomware, business email compromise, and adversary-in-the-middle. This capability combines our industry-

leading detection with AI-powered enforcement mechanisms to block threats early in the kill chain and contain their advancement. Analysts have a powerful tool against human-operated attacks while leaving them in complete control of investigating, remediating, and bringing assets back online.

Microsoft Security Copilot, first announced at Microsoft Secure in March 2023, is the industry's first generative AI security product that allows security teams to move at machine speed. It combines OpenAI's GPT-4 generative AI model with Microsoft's security-specific model informed by our unique global threat intelligence and more than 65 trillion daily signals. Security teams benefit from Security Copilot by simplifying complex tasks with capabilities like guided response actions, and gaining intuitive, actionable insight across the threat landscape such as summarized incidents in natural language. As a result, organizations can detect threats earlier and outpace adversaries. Security Copilot is currently in private preview and in the nomination period for an early access program. The single best way to prepare to realize the benefits of Microsoft Security Copilot is by adopting and deploying Microsoft 365 Defender today.

Customer reality is core to Microsoft's testing approach

As the threat landscape rapidly evolves, Microsoft is committed to empowering defenders with industry-leading, cross-platform XDR. Our evaluation philosophy is to reflect the real world by configuring the product as customers would in line with industry best practices. For instance, our configuration used the most updated OS versions to test the latest protection available to customers. In the MITRE Evaluations, as with all simulations, Microsoft 365 Defender achieved industry-leading visibility without manual processing or fine-tuning and can be run in customer environments without generating an untenable number of false positives. Microsoft's commitment to protection while minimizing false positives is reflected in regularly occurring public evaluations.

We thank MITRE Engenuity for the opportunity to contribute to and participate in this year's evaluation.

Learn more

Learn more about Microsoft 365 Defender.

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

About MITRE Engenuity ATT&CK® Evaluations

ATT&CK® Evaluations is built on the backbone of MITRE's objective insight and conflict-free perspective. Cybersecurity providers turn to the Evaluations program to improve their offerings and to provide defenders with insights into their product's capabilities and performance. Evaluations enable defenders to make better informed decisions on how to leverage the products that secure their networks. The program follows a rigorous, transparent methodology using a collaborative, threat-informed, purple-teaming approach that brings together providers and MITRE experts to evaluate solutions within the context of ATT&CK. In line with MITRE Engenuity's commitment to serve the public good, Evaluations results and threat emulation plans are freely accessible. ATT&CK Evaluations | MITRE Engenuity (mitre-engenuity.org)

About MITRE Engenuity

MITRE Engenuity, a subsidiary of MITRE, is a tech foundation for public good. MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we

work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation. MITRE Engenuity brings MITRE's deep technical know-how and systems thinking to the private sector to solve complex challenges that government alone cannot solve. MITRE Engenuity catalyzes the collective R&D strength of the broader U.S. federal government, academia, and private sector to tackle © 2023 MITRE Engenuity, LLC. Approved for Limited Release to MITRE Engenuity ATT&CK® Evaluations: Enterprise 2023: Turla Participants. national and global challenges, such as protecting critical infrastructure, creating a resilient semiconductor ecosystem, investing in pandemic preparedness, accelerating use case innovation in 5G, and democratizing threat-informed cyber defense.