Microsoft

Microsoft Digital Defense Report

CISO Executive Summary

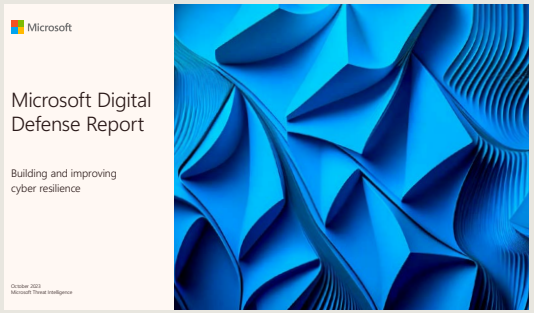
Building and improving cyber resilience

October 2023
Microsoft Threat Intelligence

Contents of the full report

The data, insights, and events in this report are from July 2022 through June 2023 (Microsoft fiscal year 2023), unless otherwise noted.

For easier viewing and navigating through the report on certain browsers, we suggest using Adobe Reader, which is available for free on the Adobe website.



Find the full report here
Microsoft Digital Defense Report 2023

Responding with breakthrough innovation

Introduction from Bret Arsenault

In the last few months, the world has witnessed a wave of innovation as organizations apply advanced AI to new technologies and use cases. Our industry is facing a paradigm shift and taking a massive leap forward as technology advances incredibly quickly and makes daily headlines.

The security industry has been focused on managing increased risks and innovating to adapt to this fast pace of change. We continue to hear from our peers, partners, and customers that security has never been more critical to the resilience of business and society.

There has been significant growth in the threat landscape as more attackers use increasingly sophisticated techniques to compromise an ever-growing pool of services, devices, and users. All combined, this creates a larger attack surface and threat potential than we have ever dealt with. At Microsoft, we have seen a 23 percent annual rise in the cases processed by the Microsoft Security Response Center and Security Operations Center teams, a sign of that growing vulnerability.

While human ingenuity and expertise will always be a precious and irreplaceable component of cyber defense, technology has the potential to augment these unique capabilities with the skill sets, processing speeds, and rapid learning of modern AI. This technology can detect hidden patterns and behaviors and inform a response at machine speed with the latest and most advanced security practices.

In the last year, experiences based on large language models (LLMs), like ChatGPT, have taken the world by storm. LLMs can draw upon a vast store of data, leveraging the massive computing power available in the cloud. But what I think is more exciting is the real, tangible impact that technology like this can drive. AI, together with the power of cloud and machine learning, has enormous potential. Just as the security community led the charge on password spray detection, two-factor authentication enforcement, and managed device health, we have an opportunity now to demonstrate how responsible AI has the potential to positively transform the security landscape.

The role of Chief Information Security Officer (CISO) has undergone a remarkable transformation as it expands beyond the traditional focus on securing information and users. Today, CISOs are entrusted with protecting all aspects of the connected business, including digital assets and cyber-physical and operational domains. The CISO's responsibility extends to safeguarding critical infrastructure and Internet of Things/Operational Technology (IoT/OT) systems and ensuring the continuity of operational processes. This expanded role reflects the growing recognition that cybersecurity must address the holistic protection of the entire business. In an era where the convergence of the digital and physical realms demands comprehensive security strategies and a deep understanding of the cyber-physical landscape, the CISO plays a pivotal role in the organization's resilience and success.

Bret Arsenault
Chief Information Security Officer

The future of cyber defense is cooperation, innovation, and the hyper scale cloud

With challenges comes opportunity. The increase in pace, volume, and sophistication of cyberattacks means that defenders all over are increasingly leveraging partnership, technological investment, and legal avenues to confront these challenges and build long-term resiliency. Never before have cybersecurity stakeholders been more invested in innovation and collaboration. Vendors are improving the cybersecurity of their products and services, developing new tools to help customers better defend against attackers. Governments are providing the public with more information about cyber threats and how to counter them as well as implementing new legal and regulatory requirements for cybersecurity.

Combating cyber aggression requires more, deeper alliances in the private sector and stronger partnerships between the private and public sectors to ensure we are bringing to bear the best technological and regulatory tools. We must also accelerate the move of critical computing workloads to the cloud, where vendors' security innovations will be most impactful, and ensure artificial intelligence (AI) innovation provides defenders with a durable technological advantage over attackers.

1. This year, Microsoft blocked 4,000 identity attacks and 11,000 password attacks per second and an average of 1,700 distributed denial of service (DDoS) attacks per day.
2. Cooperation across the technology community is an absolute necessity to ensure organizations of all types and sizes, in every industry and region, can protect themselves. This means working together to push the boundaries of innovation, ensuring technical integration of products in the security space and addressing the end-to-end security needs of customers.
3. The evolution of AI technology, such as generative AI models, requires us to evolve cybersecurity practices and threat models to address new challenges. Generative AI models can create realistic content—including text, images, video, and audio—which can be used by threat actors to spread misinformation or create malicious code. To stay ahead of emerging security threats, we must invest in research and development.
4. Over 99 percent of successful cyberattacks could be thwarted by implementing a few fundamental security hygiene practices. Hyper-scale cloud makes it easier to implement these practices by either enabling them by default or abstracting the need for customers to implement them.

An overview of The State of Cybercrime

Cyber criminals remain focused on exploiting weakness in humans and technology, staying ahead of security measures, and coordinating to create sophisticated global networks, requiring defenders to stay up to date on cyber hygiene and best practices.

Cybercriminals are leveraging the cybercrime as a service ecosystem to launch identity, phishing, and DDoS attacks at scale. At the same time, they are increasingly bypassing multifactor authentication (MFA) and other security measures to conduct targeted attacks. Ransomware operators are shifting heavily toward hands on keyboard attacks, using remote encryption and exfiltrating data. In a particularly concerning development, cybercriminals are improving their ability to impersonate or compromise legitimate third parties.

The top four threats identified by Microsoft Defender Experts this year were:

- **Identity attacks** including traditional brute-force attempts, sophisticated password spray attempts, and adversary-in-the-middle (AiTM) attacks.
- **Ransomware encounters**, which affected primarily small and medium size organizations.
- **Targeted phishing attempts**
- **Business email compromise (BEC)** including email conversation hijacking, mass spamming with malicious applications to commit financial fraud, and internal phishing.

An overview of The State of Cybercrime continued

1. (Identity) We saw a dramatic surge in password-based attacks this year. One of the main reasons these attacks are so prevalent is the low security posture of many organizations, especially in the education sector. Many of these organizations have not enabled MFA for their users, leaving them vulnerable to phishing, credential stuffing, and brute force attacks.
2. (Ransomware) We observed that 80 to 90 percent of all human-operated ransomware compromises originated from unmanaged devices. Going forward, we expect ransomware operators will seek to leverage automation, AI, and hyperscale cloud systems to scale and to maximize the effectiveness of their attacks.
3. (Phishing) Trends in phishing included: emails sent from trusted third parties, emails with legitimate URLs, OneNote malware, and OAuth device code phishing. This year, we observed URLs with open redirectors and open shorteners as the dominant phishing attack vectors. Users must be trained not only to avoid clicking on phishing links, but to report them.
4. (BEC) The frequency of BEC attacks has skyrocketed. Their success is largely due to the growing targeting of cloud-based infrastructure, exploitation of trusted business relationships, and development of more specialized skills by the threat actors. Given most BEC is perpetrated by organized criminal networks, intelligence sharing improves our collective ability to identify and respond to their attacks. Hyper-scale cloud makes it easier to these practices by either enabling them by default or abstracting the need for customers to implement them.
5. Threat actors are exploiting cloud computing resources such as virtual machines to launch DDoS attacks. These attacks can render platforms such as business productivity inaccessible. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks.

The most prevalent gaps we found during reactive incident response engagements were:

- Lack of adequate protection for local administrative accounts
- A broken security barrier between on-premises and cloud administration
- Lack of adherence to the least privilege model
- Legacy authentication protocols
- Insecure Active Directory configurations

Actionable insights

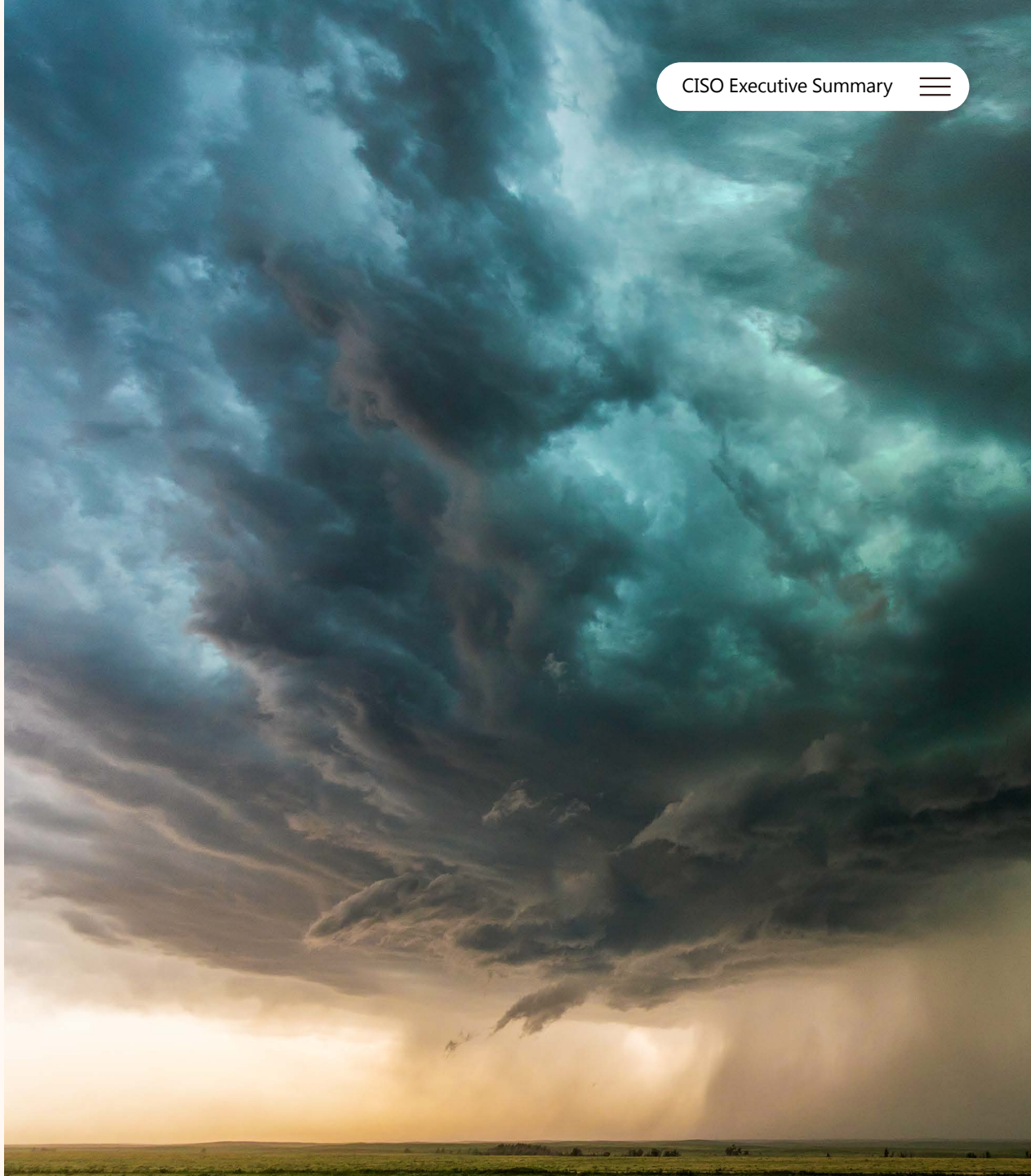
1. To mitigate and protect against these tactics, we recommend randomizing local administrative account passwords, not synchronizing on-premises administrative accounts to the cloud, and having separate accounts and purpose-built hardened workstations for on-premises and cloud administration.
2. We also recommend using just-in-time and just-enough administration in the cloud and on-premises, separating daily use and administrative accounts, making an inventory of all applications using legacy authentication protocols, and modernizing those applications where possible and phasing out those that cannot be modernized.
3. We advise organizations to adopt objective behavioral measures and context-aware education models for employee phish training that prioritize behavior change over information delivery and compliance. Tailored and context-aware engagement models that can be implemented at scale offer the best opportunity to help users learn to modify their response to phishing attempts.
4. A return on mitigation (ROM) framework helps organizations prioritize steps to harden their environment in the face of limited resources. Microsoft calculates ROM values using a formula that multiplies the weighted impact of a solution or mitigation by a weighted value of the solution in terms of effectiveness, and factors in the effort involved in implementing the solution. The higher the ROM score, the lower the resources and effort involved in implementing the solution for the impact and value provided (see page 41 of the full report for an example of how to structure this framework).

Nation State Threats

As nation state cyber actors develop and expand their capabilities, they are using a blend of cyber operations, espionage, influence campaigns, and destructive attacks to support their governments' geopolitical goals. At the same time, they are increasing their targeting across borders and sectors, putting critical infrastructure, nonprofit organizations, universities, government agencies, and more at potential risk.

This year, nation-state cyber threat actors worked to increase their collection capacity against foreign and defense policy organizations, technology firms, educational institutions, and critical infrastructure organizations. Microsoft Threat Intelligence observed activity against organizations in more than 120 countries and territories, most of which was reconnaissance, initial access and various other actions on network, and data exfiltration, with a small amount of data destruction. While most cyber operations focused on the United States, Ukraine, and Israel—with pervasive operations in Europe as well—nation state actors expanded the geographic scope of their activities, spreading to more parts of Latin America and sub-Saharan Africa. Due to heightened Iranian activity, there were also more operations in the Middle East.

40 percent of the threat notifications Microsoft sent to online services customers between July 2022 and May 2023 went to critical infrastructure organizations. This was followed by education (18 percent), government (14 percent), and think tanks/NGOs (13 percent).



Nation State Threats continued

- **Russian** threat actors conducted phishing and password spray campaigns, credential theft, lateral movement through networks, data exfiltration, and other actions associated with gaining and retaining access to targets for intelligence collection, particularly in NATO member states. The expansion of Russia's war-related targeting suggests that any government, policy, transportation, energy, or critical infrastructure organization in a country supporting Ukraine may be targeted.
- **Chinese** threat groups carried out sophisticated worldwide intelligence collection campaigns targeting US defense and critical infrastructure and public and private entities in the South China Sea and among China's strategic partners in the Belt and Road Initiative. Some Chinese cyber activity may also have been to explore avenues of response in the event of a future geopolitical crisis.
- **Iranian** state actors are using increasingly sophisticated tradecraft, including enhancing operations in cloud environments, regularly using custom implants, and exploiting newly released vulnerabilities faster. While the United States and Israel top Iran's targeting list, Tehran is using cyber-enabled influence operations to target European NATO member states, scare Israeli citizens, foment Shi'ite unrest in Gulf, and suppress perceived opponents of the regime.
- **North Korean** cyber operations also increased in sophistication, using new techniques like weaponizing legitimate open-source software. North Korean hackers collect intelligence on the policies of the regime's adversaries, NGOs, and academics, exfiltrate information about other countries' military capabilities and defense industries, and steal cryptocurrency.

Actionable insights

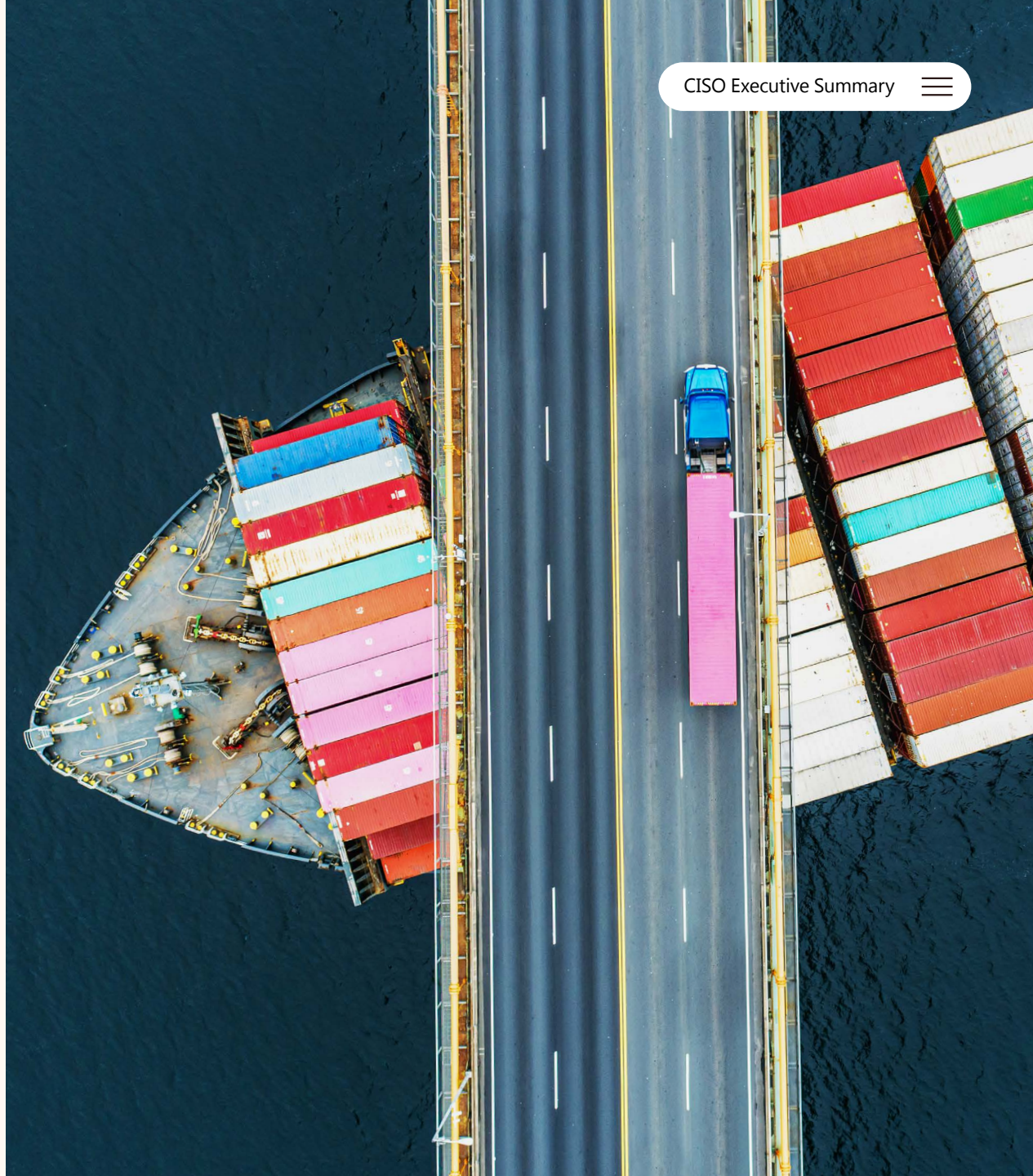
1. Track changes made to a mailbox by a user.
2. Monitor and alert on suspicious permissions changes made by users and administrators.
3. Apply patches when they become available.
4. Add users to the Protected Users group, which provides additional credential protections beyond disabling NTLM and should be used for high-value accounts, such as domain administrators, when possible.
5. Educate end users about protecting personal and business information on social media, filtering unsolicited communication, identifying spear-phishing emails and watering holes, and reporting reconnaissance attempts and other suspicious activity.

Critical Cyber Security Challenges

The increasing number of attacks on the highly vulnerable intersection of information technology and operational technology (IT-OT) highlights the crucial need for a comprehensive defense strategy that encompasses the entire business ecosystem.

Organizations must ensure interoperability between their IT and OT security systems, connecting telemetry and insights from all areas of the business to gain a comprehensive security view. This holistic security strategy is crucial to safeguard against threats to the internet of things (IoT), supply chains, and critical infrastructure. While in the past attacks on critical infrastructure were almost exclusively conducted by nation state actors, a lowered barrier for entry and an increase in off-the-shelf malware targeting IoT/OT devices means the threat to OT from all types of malicious actors is rising.

Unmanaged devices commonly found in critical infrastructure, including building management systems, OT, IoT, and internet of medical things devices, may be a significant vulnerability, requiring security solutions such as supply chain security, firmware analysis, and managed security services. It is of utmost importance to address the issue of unpatched, unpatchable, or unsupported operating systems in OT devices, which can leave critical infrastructure and systems exposed.



Critical Cyber Security Challenges continued

Adopting IoT management in the cloud reaps benefits in the form of standard governance models, reliable patching, broad monitoring, and continued security investment. In addition, bringing OT and IT security teams together creates a unified front against evolving threats, maximizing resources while pinpointing vulnerabilities. A converged security operations center combines the strengths of two teams, resulting in a streamlined, cost-effective approach to enterprise security.

1. 78 percent of devices on Microsoft Defender for IoT customer networks have known vulnerabilities, of which 46 percent cannot be patched. 25 percent of OT devices on customer networks use unsupported systems, making them more susceptible to attacks due to a lack of essential updates and protection against evolving threats.
2. Firmware scanning tools can identify and mitigate potential security weaknesses in high-risk devices. A survey of Programmable Logic Controllers (PLC) found that over 60 percent were still running older versions of firmware, with eight or more exploitable CVEs. If the latest version of the firmware available for these PLC models were to be deployed, the number of devices with no known exploitable CVEs would increase from four to 40 percent.
3. As organizations implement digital transformation programs, it's crucial to monitor and discover inventory in networks that were previously thought to be air gapped. This is because air gaps are no longer enough to protect networks from malicious attacks.

   Asset profiling enables end-to-end discovery of assets by analyzing network signals to identify and categorize network assets, the information collected about them, and the types of assets they represent, to better protect them.

Actionable insights

1. Reduce the attack surface by eliminating unnecessary internet connections, open ports, and restricting remote access using VPN services.
2. Implement robust network monitoring within OT environments, paying attention to abnormal behavior that may indicate malicious activity.
3. Influence IoT/OT device security by requiring vendors to adopt secure development lifecycle best practices. Vendors can provide more information about the third-party components contained in their software and hardware though a software bill of materials (SBOM). In the event of a major vulnerability, SBOMs empower organizations to understand the location of the vulnerability within their environment and their level of exposure and prepare for deploying emergency patches if applicable.

Innovating for security and resilience

AI offers the potential to change the security landscape by augmenting the skill, speed, and knowledge of defenders.

While human ingenuity and expertise will always be a precious and irreplaceable component of cyber defense, new technology has the potential to augment these unique capabilities with the skill sets, processing speeds, and rapid learning of AI. This technology can detect hidden patterns and behaviors and inform our response at machine speed.

Large language models (LLMs) can automate and augment aspects of cybersecurity, including: threat intelligence; incident response and recovery; monitoring and detection; testing and validation; education; and security governance, risk, and compliance. To be most effective, LLMs must be augmented with complementary modules, also called RAG (Retrieval Augmented Generation), that interface with relevant data sources, tailored analytics, and various threat intelligence enrichments. While LLM-based solutions show great potential to help cybersecurity, they are an auxiliary to and not a replacement for human experts.

1. This year, our built-in protections across Windows, Azure, Microsoft 365, and Microsoft Defender for Office 365 blocked more than 9.6 billion malware threats, over 35.7 billion phishing and other malicious emails, and thwarted 25.6 billion brute-force password attack attempts.
2. With a robust LLM-powered solution, cybersecurity analysts can increase productivity with automated scans and anomaly detection, pattern identification, and root cause evidence discovery. However, the threat surface of LLM-based apps and solutions will have to be monitored for both inadvertent and deliberate misalignment.
3. Because LLMs have their own unique threat surfaces, bad actors can work to manipulate them and, by extension, their users. The main classes of reported vulnerabilities involving LLMs have included attempts to extract the model's system prompt (prompt extraction) and attempts to cause the model to deviate from its intended behavior (command injection), such as "jailbreaks".

Actionable insights

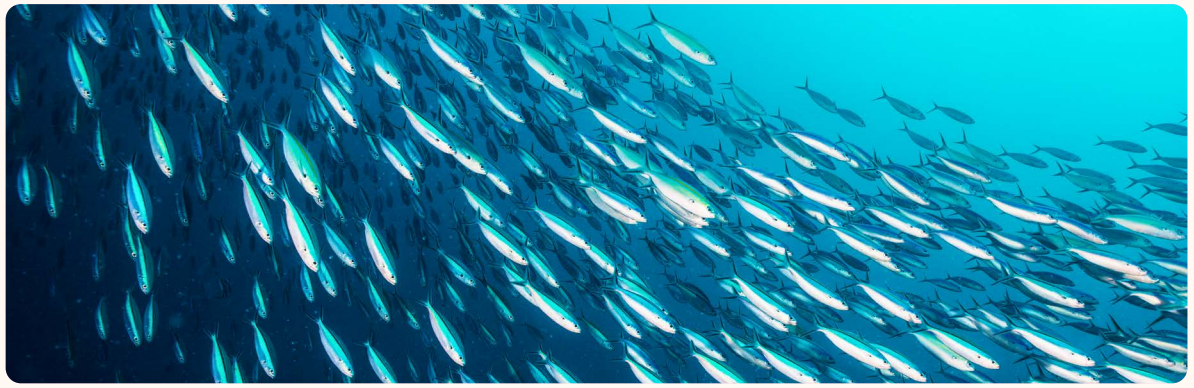
1. Educate security teams about the novel threats that AI systems introduce, particularly prompt injection.
2. Review security practices for AI-integrated products holistically, including all components. Assessing only the AI component of a system makes it difficult to quantify risks and provides limited mitigation options. Reviewing the entire system provides the full context and more mitigation opportunities at different points, making the risks more quantifiable.
3. Continuously improve process for responding to and recovering from attacks and for practicing incident response readiness. Tabletop exercises and cross-company involvement are particularly useful.

Collective Defense

As cyberthreats evolve, productive relationships across a spectrum of stakeholders will be essential to improve threat intelligence, drive resilience, contribute to mitigation guidance, and develop key skills.

The global shortage of cybersecurity professionals and the need for AI skills pose significant challenges that can only be overcome through strategic partnerships with educational institutions, nonprofit organizations, governments, and businesses. According to Cybersecurity Ventures, the demand for cybersecurity jobs is projected to reach 3.5 million by 2025, a staggering 350 percent increase over eight years. While AI may relieve some of this burden, to fully harness AI's potential, individuals will need to possess the necessary AI skills. As a result, the World Economic Forum has named AI skills a top priority for companies' training strategies.

As upper-income countries improve their cyber defenses, it is important that they help low- and middle-income countries that are lacking cyber resilience. This cybersecurity capacity building ensures no one is left behind as we build a safer and more secure digital world. Microsoft is committed to working with partners to fight cybercrime, advance media content provenance and accountability, safeguard democracy, grow the cybersecurity talent pool, and support non-governmental organizations.



1. The new Cybercrime Atlas initiative is intended to create a standardized and scalable model for open-source intelligence research, maximizing data collection while ensuring intelligence is thoroughly cleansed, enriched, and vetted by experts from diverse industries. Contextualized intelligence collection facilitates the analysis of links to enable the identification of connections between cybercriminals, groups, and shared infrastructure.
2. The Microsoft AI Skills Initiative includes free coursework developed in collaboration with LinkedIn. The Generative AI Skills Grant Challenge, conducted in partnership with data.org, the Microsoft AI for Good Lab, and GitHub, supports organizations in training and empowering the workforce to use generative AI.
3. Research shows that fewer than 15 percent of NGOs have cybersecurity experts as staff and that the vast majority do not implement critical cyber hygiene practices, such as MFA.
4. The Humanitarian Cybersecurity Center provides expert support and practical, free cybersecurity assistance to humanitarian organizations, tailored to their needs and located anywhere in the world. It also investigates and analyzes cyberattacks against NGOs and then creates actionable threat intelligence that can be shared with the community and helps scale protections beyond a single entity.

Actionable Insights for All

While this report explores the many dimensions of the cyber threat landscape, there is one crucial point that applies throughout: the vast majority of successful cyberattacks could be thwarted by implementing just a few fundamental security hygiene practices. By adhering to these minimum-security standards, it is possible to protect against over 99 percent of attacks:

1. **Enable multifactor authentication (MFA):** This protects against compromised user passwords and helps to provide extra resilience for identities.
2. **Apply Zero Trust principles:** Limit the impact of an attack on an organization. These principles are:
   - Explicitly verify—ensure users and devices are in a good state before allowing access to resources.
   - Use least privilege access—only allow the privilege that is needed for access to a resource and no more.
   - Assume breach—assume system defenses have been breached and systems may be compromised. This means constantly monitoring the environment for possible attack.
3. **Use extended detection and response (XDR) and antimalware:** Implement software to detect and automatically block attacks and provide insights to the security operations software. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
4. **Keep up to date:** Unpatched and out-of-date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system, and applications.
5. **Protect data:** Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.

The hyper-scale cloud: makes it easier to implement fundamental security practices by either enabling them by default or abstracting the need for customers to implement them. With Software as a Service (SaaS) and Platform as a Service (PaaS) solutions, the cloud provider takes responsibility for keeping up with patch management.

Implementing security solutions like MFA or Zero Trust principles is simpler with hyper-scale cloud because these capabilities are already built into the platform. Additionally, cloud-enabled capabilities like XDR and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.

Fundamentals of cyber hygiene

99%

Basic security hygiene still protects against 99% of attacks.

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.

Additional actionable insights

To combat cybercrime:

- Focus on user identity, device health, and access control to prevent lateral movement and privilege escalation in the network.
- Establish a ransomware defense strategy to mitigate the impact of extortion attacks that are becoming more frequent and damaging. This includes pre-planning a seamless method to restore encrypted files at the organizational level.
- Legacy technology and siloed standalone security products are not efficient or effective at defending against sophisticated cyber attackers. Organizations should invest in integrated cybersecurity platforms that share signals across the digital backbone to provide end-to-end visibility and inform defenders across an organization's surface attack area.
- Shift phishing training programs away from being compliance oriented to more proactive, behavior change focused. Specifically, use tailored and context-aware education models that treat users as distinct individuals and can be implemented at scale.
- Use non-phishable credentials which bind the token to the legitimate user's device, such as Windows Hello for Business and FIDO keys.

To prevent intrusion by a nation state hacking group:

- Enable logging and review all authentication activity for remote access infrastructure and virtual private networks (VPNs), with a focus on accounts configured with single factor authentication, to confirm authenticity and investigate anomalous activity.
- Educate users about social engineering and credential phishing attacks, including refraining from entering MFA codes sent via any form of unsolicited messages. In addition, educate Microsoft Teams users to verify external communication attempts, be cautious about what they share, and never share their account information or authorize sign-in requests over chat.
- Block the malicious command-and-control (C2) domains in your environment and investigate for any connections to them.

To protect critical cyber infrastructure:

Use firmware scanning tools to identify and mitigate potential security weaknesses in high-risk devices.

- Segment networks to limit lateral movement and isolate IoT devices and OT networks from corporate IT networks using firewalls.
- Proactively conduct incident response measures for OT networks.

To protect against ransomware:

Microsoft has identified five foundational principles we believe every enterprise should implement to defend against ransomware. When fully implemented and enabled, these platform-agnostic solutions provide proven defenses across identity, data, and endpoints. They are:

- Modern authentication with phish-resistant credentials
- Least Privileged Access applied to the entire technology stack
- Threat- and risk-free environments
- Posture management for compliance and the health of devices, services, and assets
- Automatic cloud backup and file-syncing for user and business-critical data

Other security steps we take at Microsoft include requiring managed healthy devices to access DevOps web apps, replacing personal access tokens (PAT) bearer tokens with managed identities, and applying the least privilege access principle to managing version control and build configuration. We also perform periodic user access reviews to ensure privileges are only granted to those with a business need and use just-in-time (JIT) permission controls for administration tasks.

Microsoft

Microsoft Digital Defense Report

CISO Executive Summary

Learn more: https://microsoft.com/mddr

Dive deeper: https://blogs.microsoft.com/on-the-issues/

Stay connected: @msftissues and @msftsecurity

October 2023
Microsoft Threat Intelligence