Microsoft Security

Threat Intelligence at Microsoft

Tóth Bálint
Cloud Solution Architect - Security

Security is a defining challenge of our time

The New York Times

Once, Superpower Summits Were About Nukes. Now, It's Cyberweapons.

But with the ease of denying responsibility and the wide range of possible attackers, the traditional deterrents of the nuclear age no longer work.

POLITICO

CYBERSECURITY

Chinese hackers nab 60,000 emails in State Department breach

Among the most sensitive information stolen, the staffer said, were victims' travel itineraries and diplomatic deliberations.

The New York Times

In Cyberattacks, Iran Shows Signs of Improved Hacking Capabilities

A monthslong hacking campaign targeted the governments of regional rivals, including Israel, and marked a turn, a new report says, as the attacks were used to collect intelligence, not just disrupt services.

The Washington Post

TECH POLICY

Cybersecurity faces a challenge from artificial intelligence's rise

While defenders have been winning more battles, the availability of AI tools threatens that progress

By Joseph Menn

May 11, 2023 at 7:00 a.m. EDT

CYBERCRIME MAGAZINE

Cybercrime To Cost the World $10.5 Trillion Annually by 2025

If it were measured as a country, then cybercrime – which is predicated to inflict dames totaling $6 trillion USD globally in 2021 – would be the world's third largest economy after the U.S. and China.

THE WALL STREET JOURNAL.

The Chinese groups accused of hacking the US and others

Reuters

July 20, 2023 [illegible] PDT · Updated a month ago

FINANCIAL TIMES

Cyber Security

ECB tells banks to run cyber stress tests after rise in hacker attacks

Lenders will assess online resilience after 'significant increase' in incidents since outbreak of Ukraine war

The Washington Post

THE CYBERSECURITY 202

Think ransomware gangs won't thrive this year? Think again, experts say

Analysis by Tim Starks

with research by David DiMolfetta

March 30, 2023 at [illegible] a.m. EDT

Welcome to The Cybersecurity 202! And greetings from (just

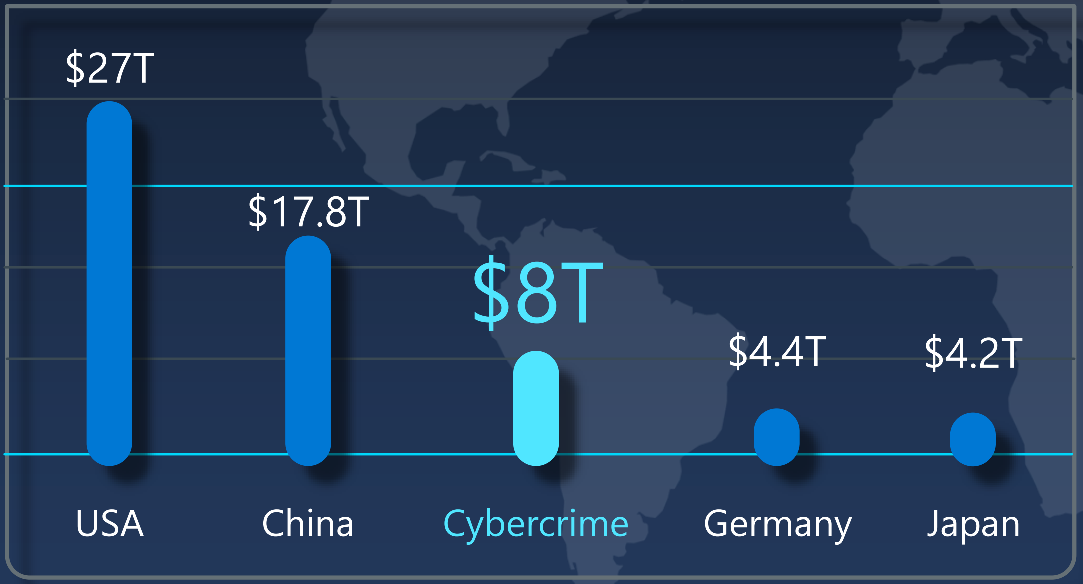
REUTERS

World

Biden: If U.S. has 'real shooting war' it could be result of cyber attacks

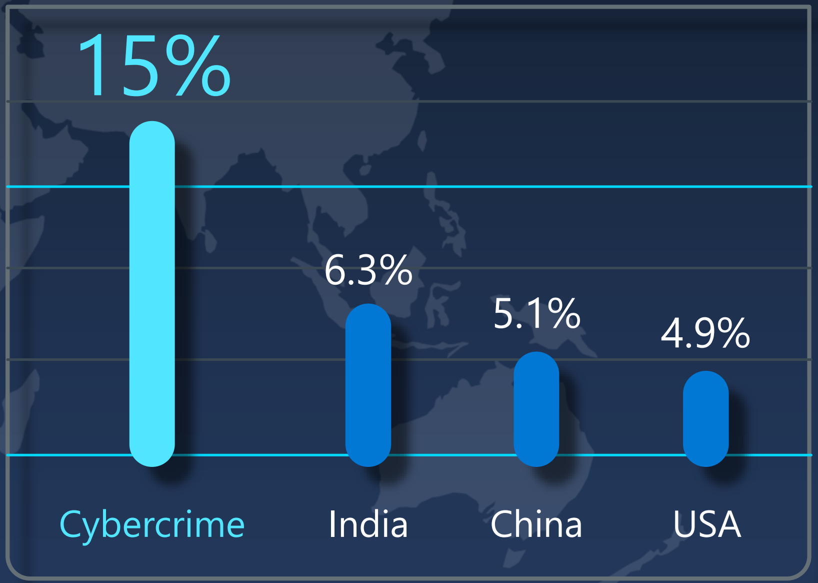
Cybercrime today equals the 3rd largest economy in the world and growing fast

Annual GDP



Source: Statistica

GDP annual growth rate



Source: Statistica

Threat intelligence…

…is the foundation of your organization’s defense

- To combat modern threats like ransomware, **security solutions** need strong threat intelligence
- TI should be **operationalized in tools like SIEM + XDR** to empower detection and incident response
- Analysts need **access** to insightful, hyper-relevant intel tailored to their organization

Threat intelligence

Data and threat intelligence

Microsoft has more insight into attacker behaviors than anyone

78T

Signals synthesized per day

AI powered detections and automated actions

10K

Security and threat intelligence experts

1M

Microsoft Security customers

15K

Partners

Broad and deep expertise in the threat landscape

Microsoft Threat Intelligence

Cloud threats

Fraud

Threat hunting

Endpoint threats

Hon d

Identity threats

Vulnerability intelligence

Supply chain threats

IoT / OT threats

BEC research

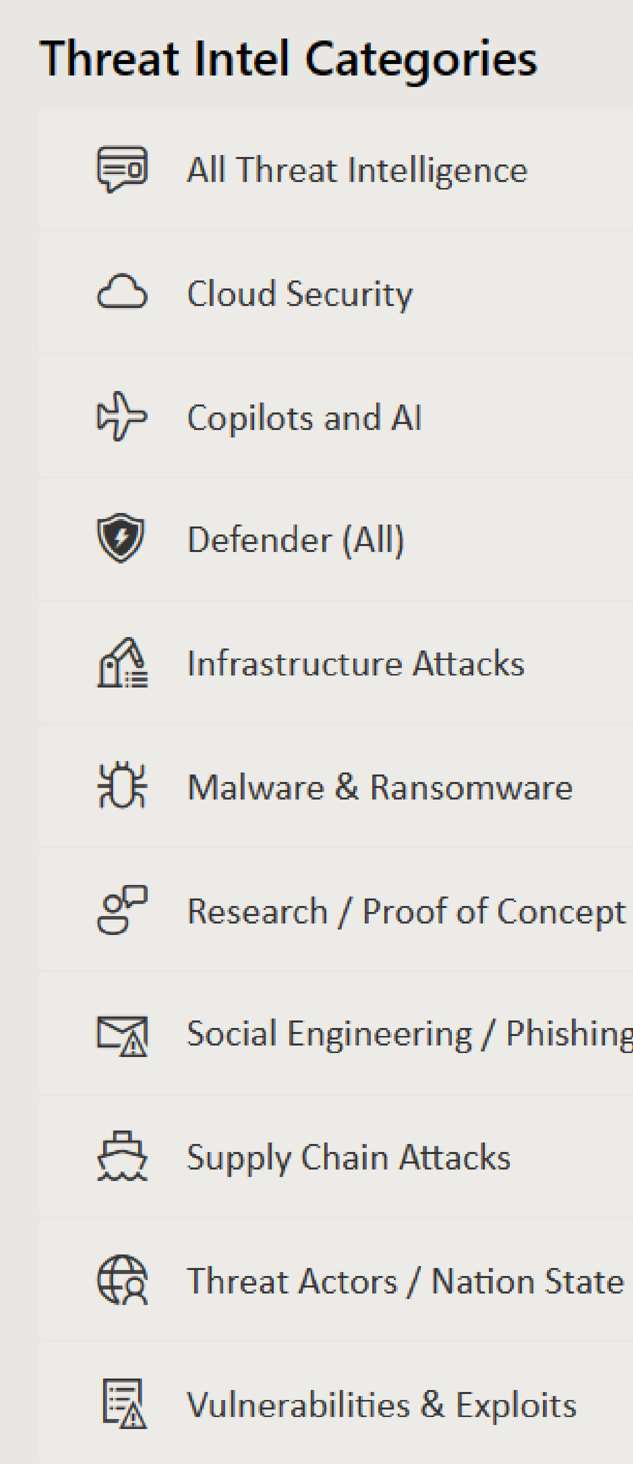
IR engagement intel

Threat infrastructure intel

Social engineering

Firmware threats

Ransomware groups



Threat Intel Categories

- All Threat Intelligence
- Cloud Security
- Copilots and AI
- Defender (All)
- Infrastructure Attacks
- Malware & Ransomware
- Research / Proof of Concept
- Social Engineering / Phishing
- Supply Chain Attacks
- Threat Actors / Nation State
- Vulnerabilities & Exploits

Microsoft takes an adversary approach to threat intelligence

300 unique threat actors

160 nation state actors

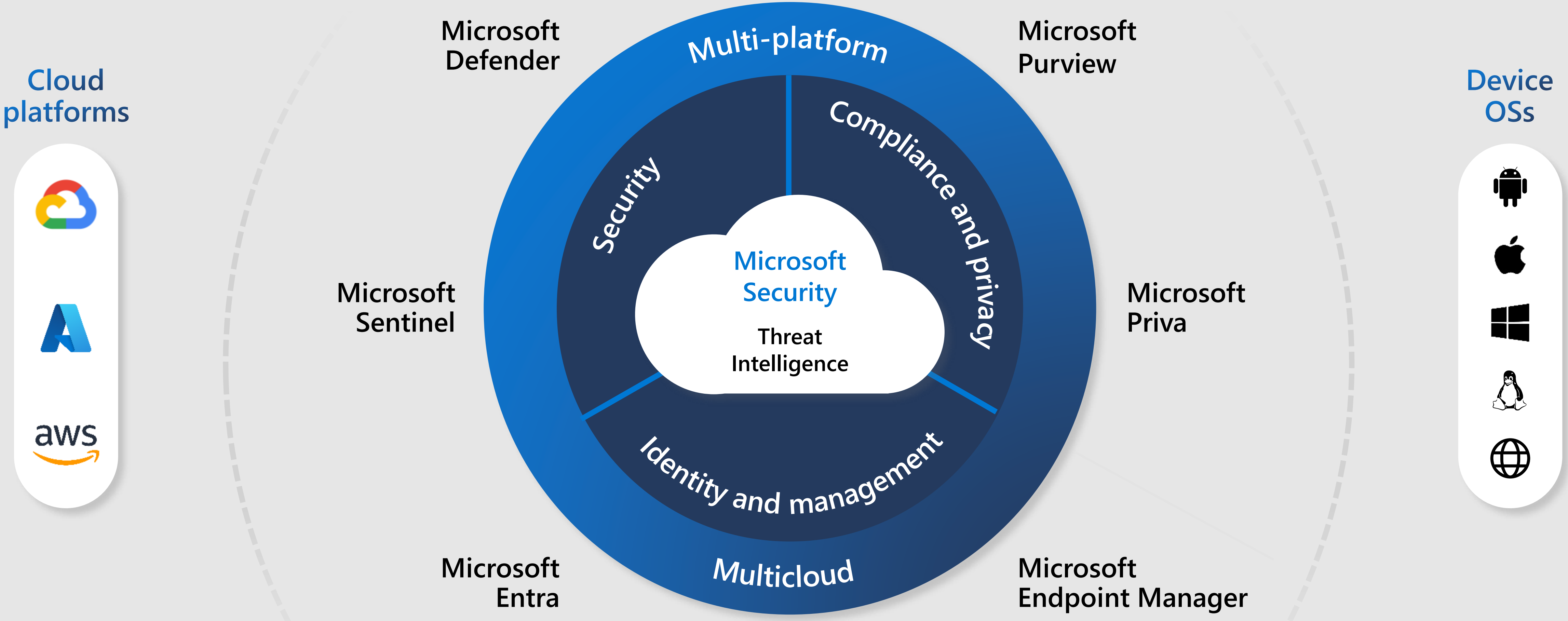
50 ransomware groups

- Nation state
- Financially motivated
- Groups in development
- Private sector offensive actors
- Influence operations

Threat Intelligence is core to Microsoft security products

Cloud platforms

Device OSs



Microsoft Threat Intelligence

Microsoft Security Experts

How customers benefit from Microsoft Threat Intel

Finished and raw threat intel so you can **prevent, detect and respond**

Intel-led approach to security that **rapidly disrupts attacks**

Threat intel-powered **hunting and incident response** when you need it most

Microsoft Defender Threat Intelligence (MDTI)

Definitive source for quality insights that protect the world from cyberthreats

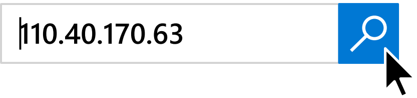
MDTI is the “encyclopedia" for Microsoft Threat Intelligence, enabling an intel-led approach to security

Keep updated with finished intelligence

The TI and Threat research that powers Microsoft Security products are made directly available to customers via an expansive content library and investigative workbench

Hunt on raw intelligence

Defenders can query Microsoft TI manually or at scale via an API to learn everything they need about any threat infrastructure



Microsoft threat intelligence

65 trillion daily signals + **8,500** researchers and experts

A new era: Microsoft Security Copilot

Defending at machine speed

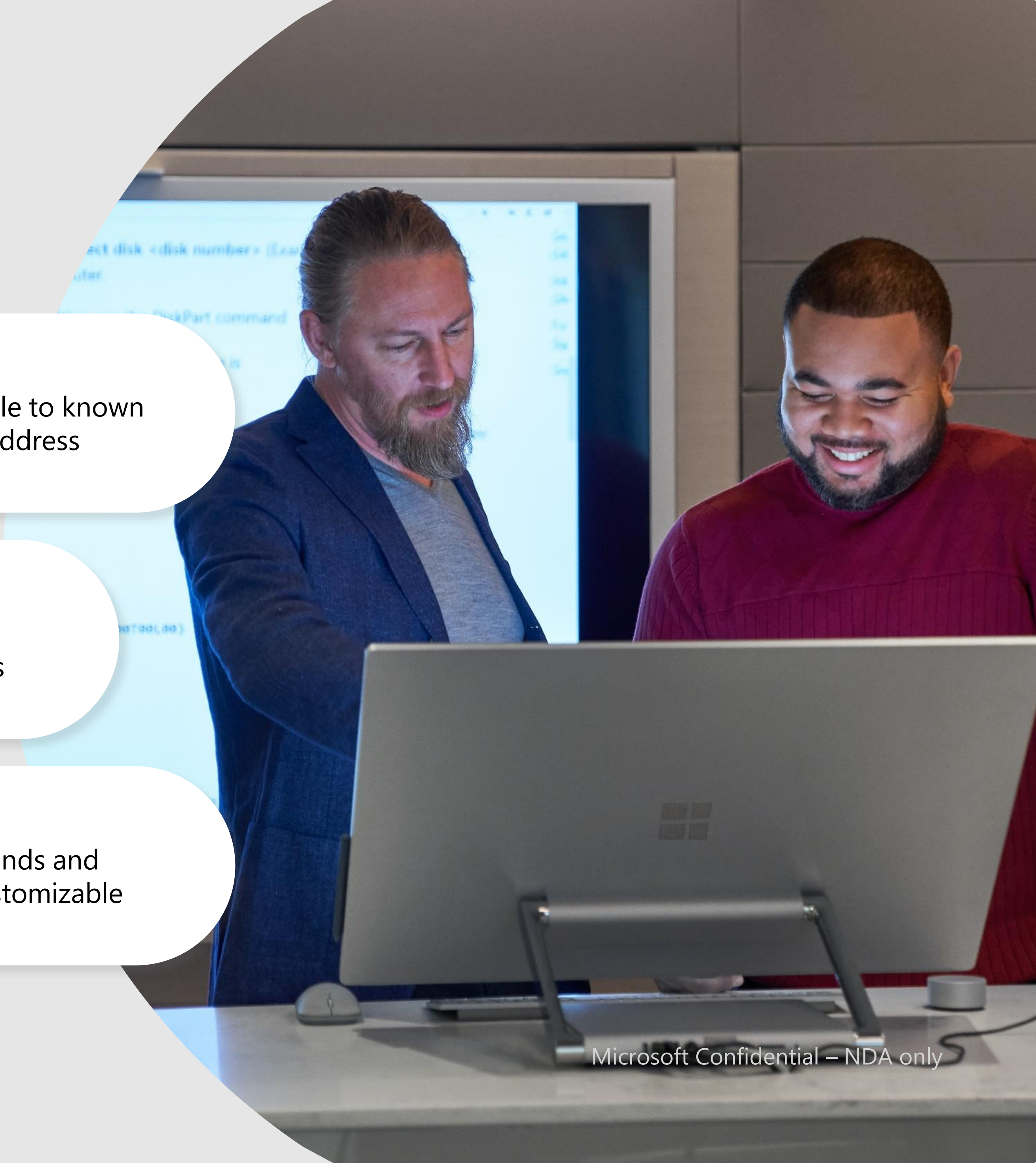
"It takes us three minutes to do a task that **used to take at least a few hours.**"

- Private preview customer

- Enable **response in minutes,** not hours
- **Simplify the complex** with natural language prompts and easy reporting
- **Catch what others miss** with deeper understanding of events
- **Address talent shortage** by augmenting human expertise

Microsoft Threat Intelligence

Modernizing your security operations



Security posture management

Discover whether your organization is susceptible to known vulnerabilities and exploits. Prioritize risks and address vulnerabilities with guided recommendations.

Incident response

Surface an ongoing incident, assess its scale, and get instructions to begin remediation based on proven tactics from real-world security incidents

Security reporting

Summarize any event, incident, or threat in seconds and prepare the information in a ready-to-share, customizable report for your desired audience

Learn more

Stay up to date on our latest threat research:

- **Microsoft Threat Intelligence Blog:** https://aka.ms/threatintelblog
- **Microsoft Threat Intelligence X:** https://twitter.com/msftsecintel
- **Microsoft Threat Intelligence Podcast:** https://www.msthreatintelpodcast.com

Learn more about MDTI:

- https://aka.ms/MDTI

Learn more about Defender Experts:

- https://www.microsoft.com/en-us/security/business/services/microsoft-defender-experts-hunting

Learn more about SIEM & XDR:

- https://www.microsoft.com/en-us/security/business/solutions/siem-xdr-threat-protection

Learn more about Microsoft IR:

- https://www.microsoft.com/en-us/security/business/microsoft-incident-response

Microsoft Security

Thank you.