Microsoft Security

Cybersecurity – einfach gemacht

Fast Lane Institut für Wissenstransfer GmbH

Helge Schroda
Business Lead Cybersicherheit
Microsoft Deutschland GmbH

Die IT-Security Industrie

3828+	17	1,000+	9,000+	8,000+
Cybersecurity Vendors	Major Categories	Subcategories	Investors	Products

- Es geht um Vertrauen – Technologien und Produkte sind austauschbar, Beziehungen sind es nicht
- Vertrauen ist schwer zu verdienen - leicht zu verlieren
- Extrem offenes Ökosystem, sowohl für Anbieter als auch für Verbraucher

Plattformsicherheit in der IT

Bedeutung der Plattformsicherheit

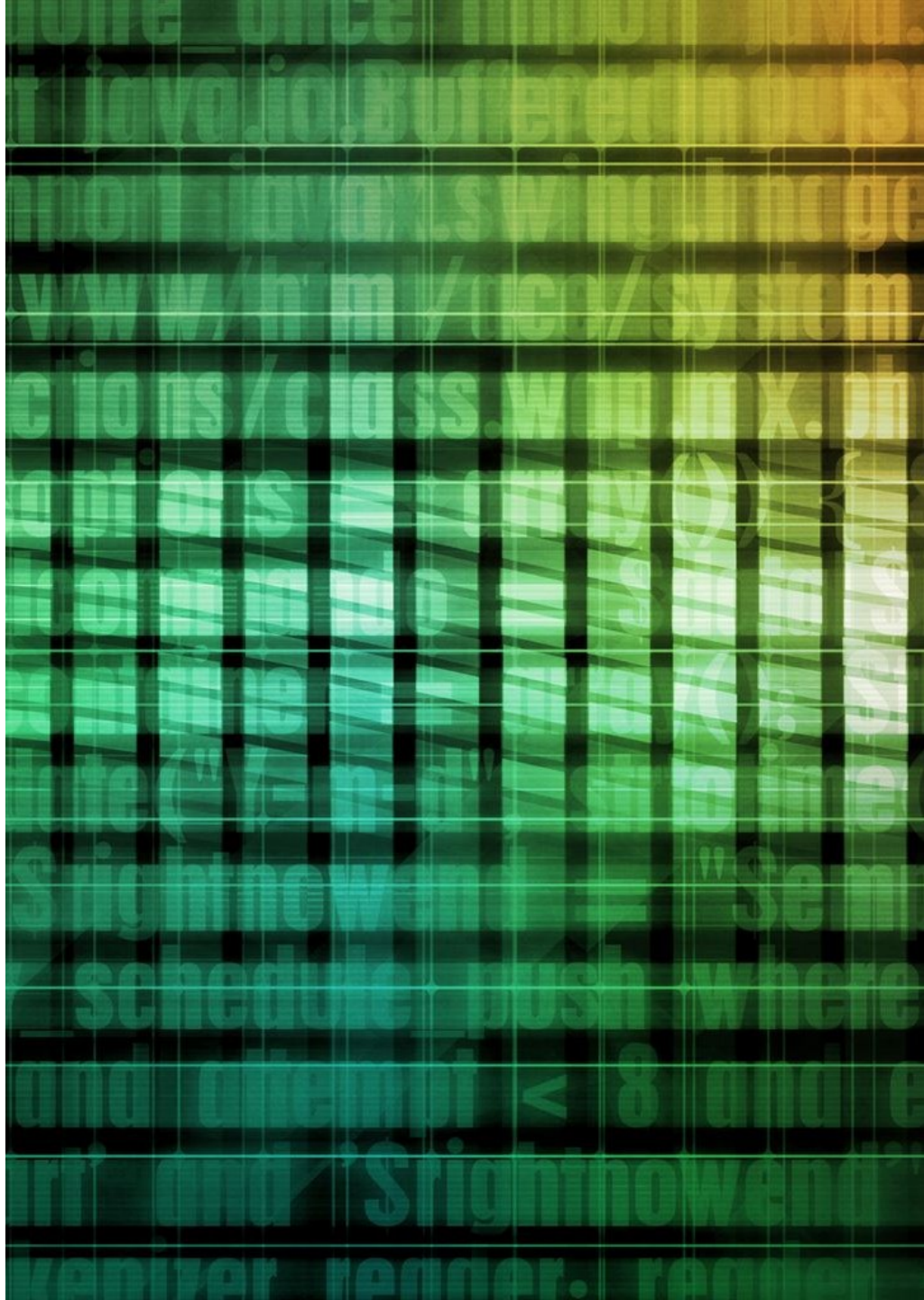
Plattformsicherheit ist in der IT-Branche von entscheidender Bedeutung, um Systeme vor verschiedenen Cyberbedrohungen und Schwachstellen zu schützen.

Die Bemühungen der großen Anbieter

Führende IT-Anbieter entwickeln kontinuierlich sichere Plattformen, um Daten zu schützen und die Systemintegrität zu wahren.

Microsoft MISA-Allianz

Die Microsoft Intelligent Security Association (MISA) Alliance integriert erstklassige Sicherheitslösungen mit den Produkten von Microsoft, um den Schutz zu verbessern. https://aka.ms/misa



Microsoft Digital Defence Report

200+

Mitwirkende in 8 Microsoft-Organisationen

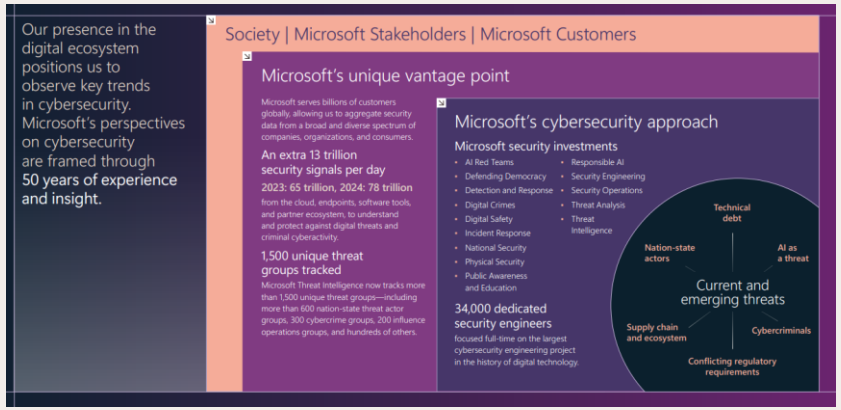
Zweck

- Darstellung einzigartiger Einsichten in Daten
- Wissen einer sehr breiten Organisation
- Aufklärung und Transparenz

Publikum

- Primär: Regierungseliten, CEOs, CFOs
- Sekundär: CISOs, die CyberSecCommunity, die Medien

Die MDDR repräsentiert die Tiefe und Breite des Know-hows von Microsoft in der Welt



Aufgrund:

- 78 Billionen Signale
- 10k+ Experten für Sicherheits- und Bedrohungsinformationen
- 34 Tsd. Vollzeit-Sicherheitsingenieure
- 15k+ Partner
- Milliarden Endgeräte

Our presence in the digital ecosystem positions us to observe key trends in cybersecurity. Microsoft's perspectives on cybersecurity are framed through **50 years of experience and insight.**

Society | Microsoft stakeholders | Microsoft Customers

Microsoft's unique vantage point

Billions of customers globally, from a broad and diverse spectrum of organizations, and consumers.

78 trillion security signals per day

1,500 unique threat groups tracked

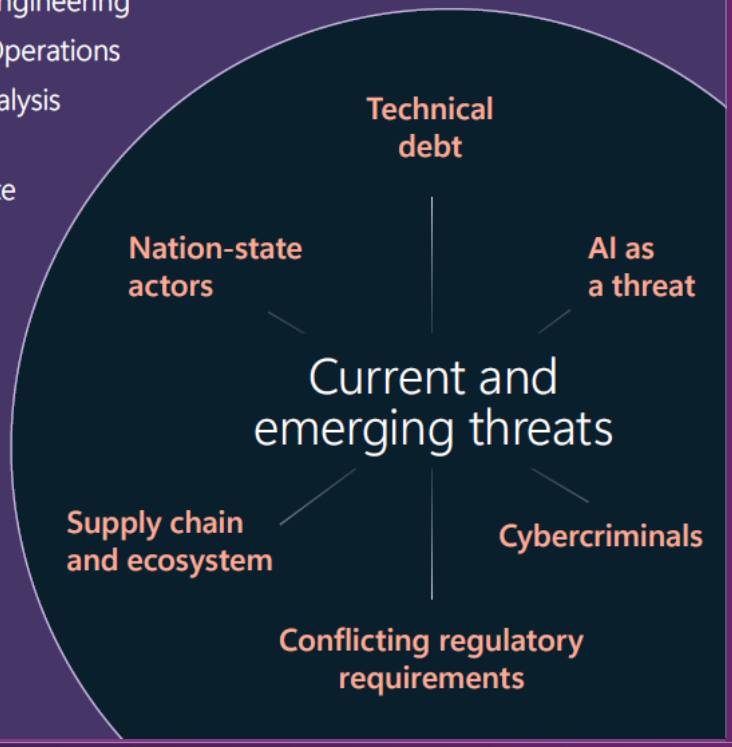
Microsoft's cybersecurity approach

Microsoft security investments

- AI Red Teams
- Defending Democracy
- Detection and Response
- Digital Crimes
- Digital Safety
- Incident Response
- National Security
- Physical Security
- Public Awareness and Education
- Responsible AI
- Security Engineering
- Security Operations
- Threat Analysis
- Threat Intelligence

34,000 dedicated security engineers

focused full-time on the largest cybersecurity engineering project in the history of digital technology.



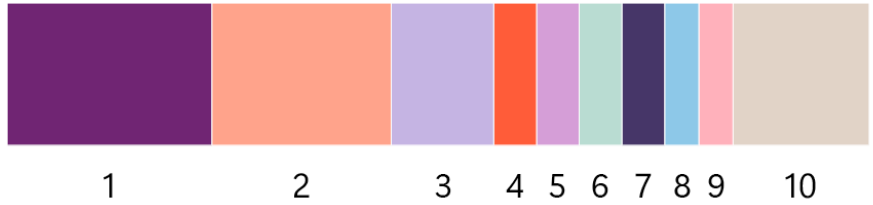
Bedrohungsaktivität durch Nation-State-Actors in Zahlen

- Staatlich gesteuerte Bedrohungsakteure spielten in breiteren geopolitischen Konflikten eine anhaltende, unterstützende Rolle.
- Der Bildungs- und Forschungssektor wurde zum zweithäufigsten Ziel nationalstaatlicher Bedrohungsakteure.

Nation-States aus Russland, China, dem Iran und Nordkorea strebten den Zugang zu IT-Produkten und -Dienstleistungen an.

Zum Teil, um Angriffe auf die Lieferkette gegen Regierungen und andere sensible Organisationen durchzuführen.

Top 10 targeted sectors worldwide



	Sector	Percentage
1	IT	24%
2	Education and Research	21%
3	Government	12%
4	Think tanks and NGOs	5%
5	Transportation	5%
6	Consumer Retail	5%
7	Finance	5%
8	Manufacturing	4%
9	Communications	4%
10	All others	16%

Quelle: Microsoft Threat Intelligence

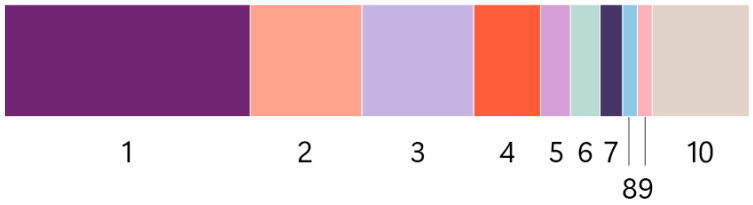
Russia: Nation-state threat actor activity

Targeting by region

Sector		Percentage
1	Europe & Central Asia	68%
2	North America	20%
3	Middle East & North Africa	5%
4	East Asia & Pacific	3%
5	Latin America & Caribbean	3%
6	South Asia	1%
7	Sub-Saharan Africa	1%

Approximately 75% of targets were in Ukraine or a NATO member state, as Moscow seeks to collect intelligence on the West's policies on the war. Ukraine remains the country most targeted by Russian actors.

Most targeted sectors



Sector		Percentage
1	Government	33%
2	IT	15%
3	Think tanks and NGOs	15%
4	Education and Research	9%
5	Inter-governmental organization	4%
6	Defense Industry	4%
7	Transportation	3%
8	Energy	2%
9	Media	2%
10	All others	13%

Blizzard

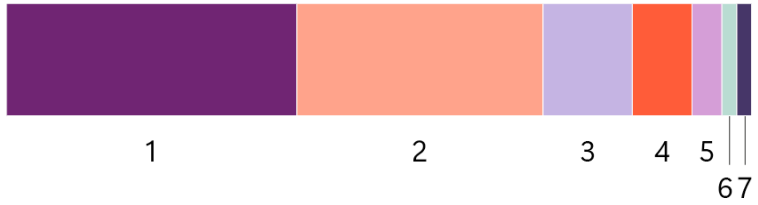
Russia

Russian actors focused their targeting against European and North American government agencies and think tanks, likely for intelligence collection related to the war in Ukraine. Actors like Midnight Blizzard also targeted the IT sector, suggesting it was in part planning supply chain attacks to gain access to these companies' client's networks for follow-on operations.

Source: Microsoft Threat Intelligence

China: Nation-state threat actor activity

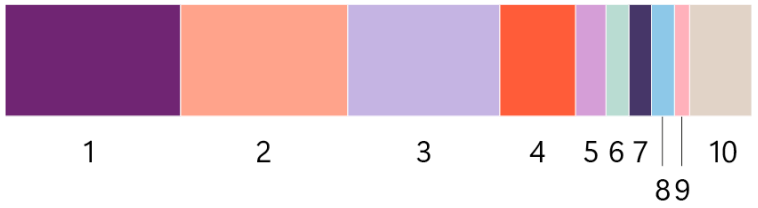
Targeting by region



Sector		Percentage
1	East Asia & Pacific	39%
2	North America	33%
3	Europe & Central Asia	12%
4	Latin America & Caribbean	8%
5	South Asia	4%
6	Middle East & North Africa	2%
7	Sub-Saharan Africa	2%

Chinese threat actors' targeting efforts remain similar to the last few years in terms of geographies targeted and intensity of targeting per location. While numerous threat actors target the United States across a wide variety of sectors, targeting in Taiwan is largely limited to one threat actor, Flax Typhoon.

Most targeted sectors



Sector		Percentage
1	IT	24%
2	Education and Research	22%
3	Government	20%
4	Think tanks and NGOs	10%
5	Manufacturing	4%
6	Defense Industry	3%
7	Communications	3%
8	Finance	3%
9	Transportation	2%
10	All others	9%

Typhoon

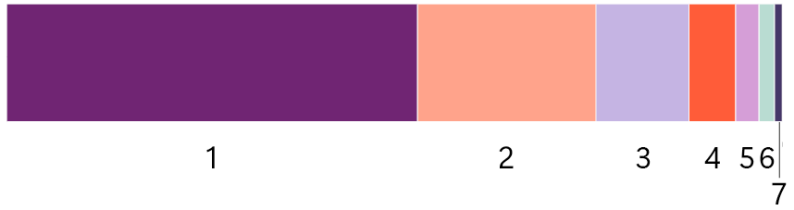
China

Most Chinese threat activity is for intelligence collection purposes and was especially prevalent in ASEAN countries around the South China Sea. Granite Typhoon and Raspberry Typhoon were the most active in the region, while Nylon Typhoon continued to target government and foreign affairs entities globally.

Source: Microsoft Threat Intelligence

Iran: Nation-state threat actor activity

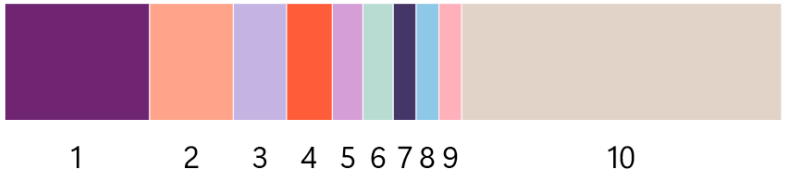
Targeting by region



Sector		Percentage
1	Middle East & North Africa	53%
2	North America	23%
3	Europe & Central Asia	12%
4	South Asia	6%
5	East Asia & Pacific	3%
6	Latin America & Caribbean	2%
7	Sub-Saharan Africa	1%

Iran placed significant focus on Israel, especially after the outbreak of the Israel-Hamas war. Iranian actors continued to target the US and Gulf countries, including the UAE and Bahrain, in part because of their normalization of ties with Israel and Tehran's perception that they are both enabling Israel's war efforts.

Most targeted sectors



Sector		Percentage
1	Education and Research	19%
2	IT	11%
3	Government	7%
4	Transportation	6%
5	Finance	4%
6	Communications	4%
7	Energy	3%
8	Commercial Facilities	3%
9	Manufacturing	3%
10	All others	42%

Sandstorm

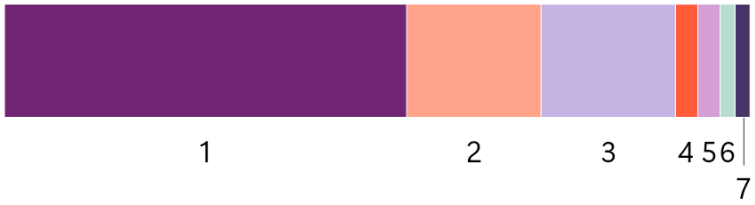
Iran

Iranian targeting focused on education, IT, and government as part of strategic intelligence collection. Iranian actors often target the IT sector to gain access to downstream customers, including those in government and the defense industrial base (DIB). "All others" includes media and think tanks or NGOs, which Iran often targets to gain insights into dissidents, activists, and persons who can impact policymaking.

Source: Microsoft Threat Intelligence

North Korea: Nation-state threat actor activity

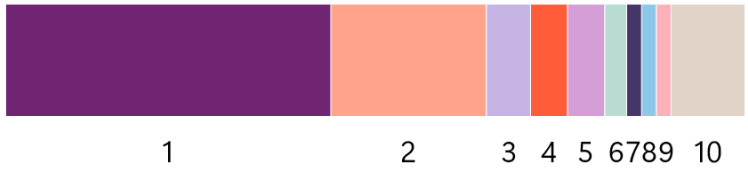
Targeting by region



	Sector	Percentage
1	North America	54%
2	East Asia & Pacific	18%
3	Europe & Central Asia	18%
4	Latin America & Caribbean	3%
5	Middle East & North Africa	3%
6	South Asia	2%
7	Sub-Saharan Africa	2%

The United States remained the most heavily targeted country by North Korean threat actors, but the United Kingdom rose up the ranks this year to second place. There were an additional 44 countries targeted by North Korean threat actors.

Most targeted sectors



	Sector	Percentage
1	IT	44%
2	Education and Research	21%
3	Manufacturing	6%
4	Consumer Retail	5%
5	Finance	5%
6	Think tanks and NGOs	3%
7	Communications	2%
8	Government	2%
9	Health	2%
10	All others	10%

Sleet

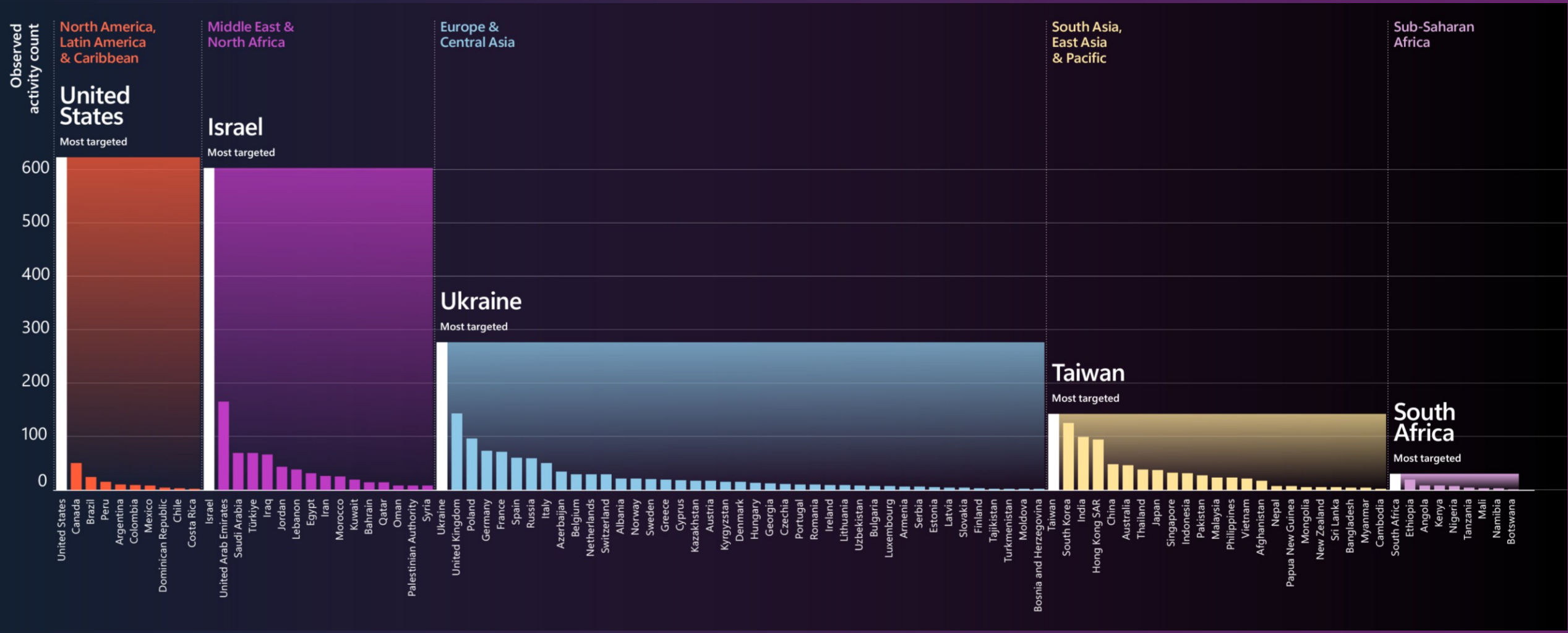
North Korea

North Korean threat actors targeted the IT sector the most, particularly to conduct increasingly sophisticated software supply chain attacks. They also continued to heavily target experts in the education sector for intelligence collection. The "All others" category comprised seven other sectors.

Source: Microsoft Threat Intelligence

Bedrohungsaktivität durch Nationalstaaten in Zahlen

Regionale Stichprobe der beobachteten Aktivitätsniveaus



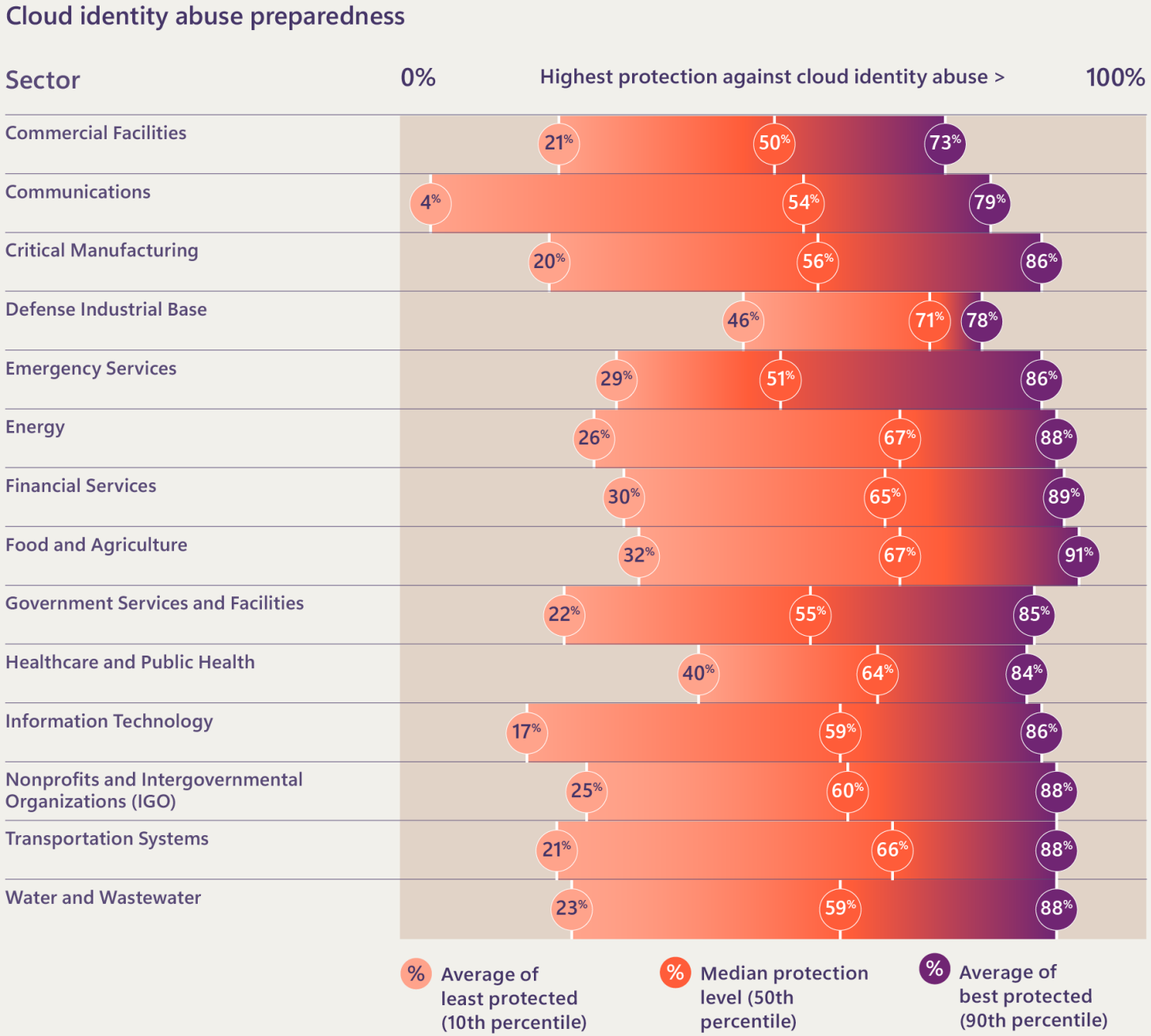
Quelle: MSTIC

ALLE werden ins Visier genommen, ohne sich dessen bewusst zu sein

durch SaaS-Apps

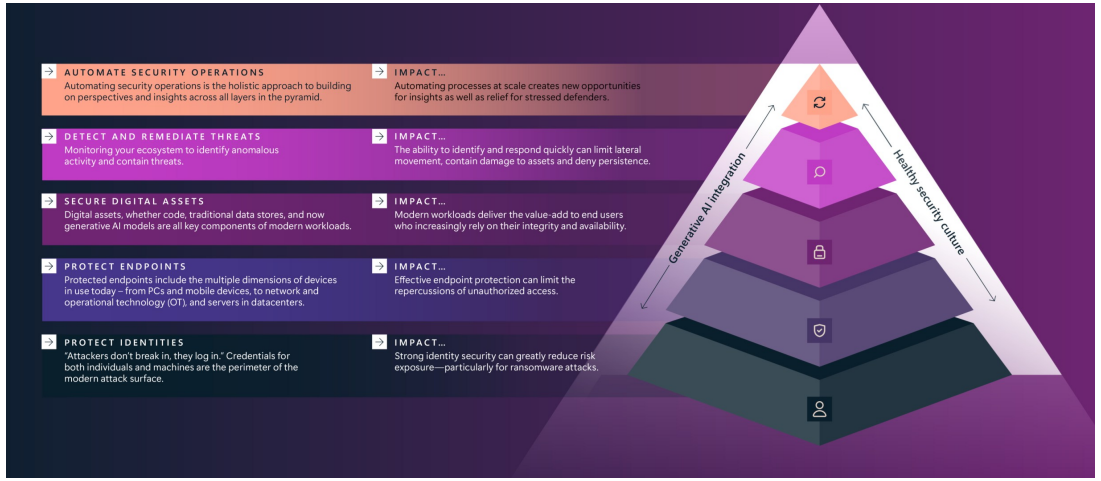
Der Aufstieg der Kompromittierung von Cloud-Identitäten

Ein Angreifer, der die Identität manipuliert, kann auch jede Ressource oder jeden Prozess manipulieren, auf den die Identität vertrauenswürdig zugreift, einschließlich E-Mail, andere Clouddienste oder die lokale Umgebung.



Sample size: 112,000 organizations representing a range of sizes and industries
Source: Microsoft Security Exposure Management

Hierarchie der Cybersicherheitsanforderungen



- Inspiriert von **Maslowscher Bedürfnis Pyramide**
- eine Priorisierung der Cybersicherheit, beginnend mit dem grundlegendsten Bedürfnis: dem **Schutz von Identitäten**.
- **Künstliche Intelligenz** spielt auf jeder Ebene eine Rolle, was ihr Potenzial zur Verbesserung von Sicherheitsmaßnahmen unterstreicht.
- Die Kultivierung einer robusten **Sicherheitskultur** innerhalb des Unternehmens
- **Praktiken** gemeinsam weiterentwickeln, um Bedrohungen effektiv zu entschärfen.

AUTOMATE SECURITY OPERATIONS

Automating security operations is the holistic approach to building on perspectives and insights across all layers in the pyramid.

IMPACT...

Automating processes at scale creates new opportunities for insights as well as relief for stressed defenders.

DETECT AND REMEDIATE THREATS

Monitoring your ecosystem to identify anomalous activity and contain threats.

IMPACT...

The ability to identify and respond quickly can limit lateral movement, contain damage to assets and deny persistence.

SECURE DIGITAL ASSETS

Digital assets, whether code, traditional data stores, and now generative AI models are all key components of modern workloads.

IMPACT...

Modern workloads deliver the value-add to end users who increasingly rely on their integrity and availability.

PROTECT ENDPOINTS

Protected endpoints include the multiple dimensions of devices in use today – from PCs and mobile devices, to network and operational technology (OT), and servers in datacenters.

IMPACT...

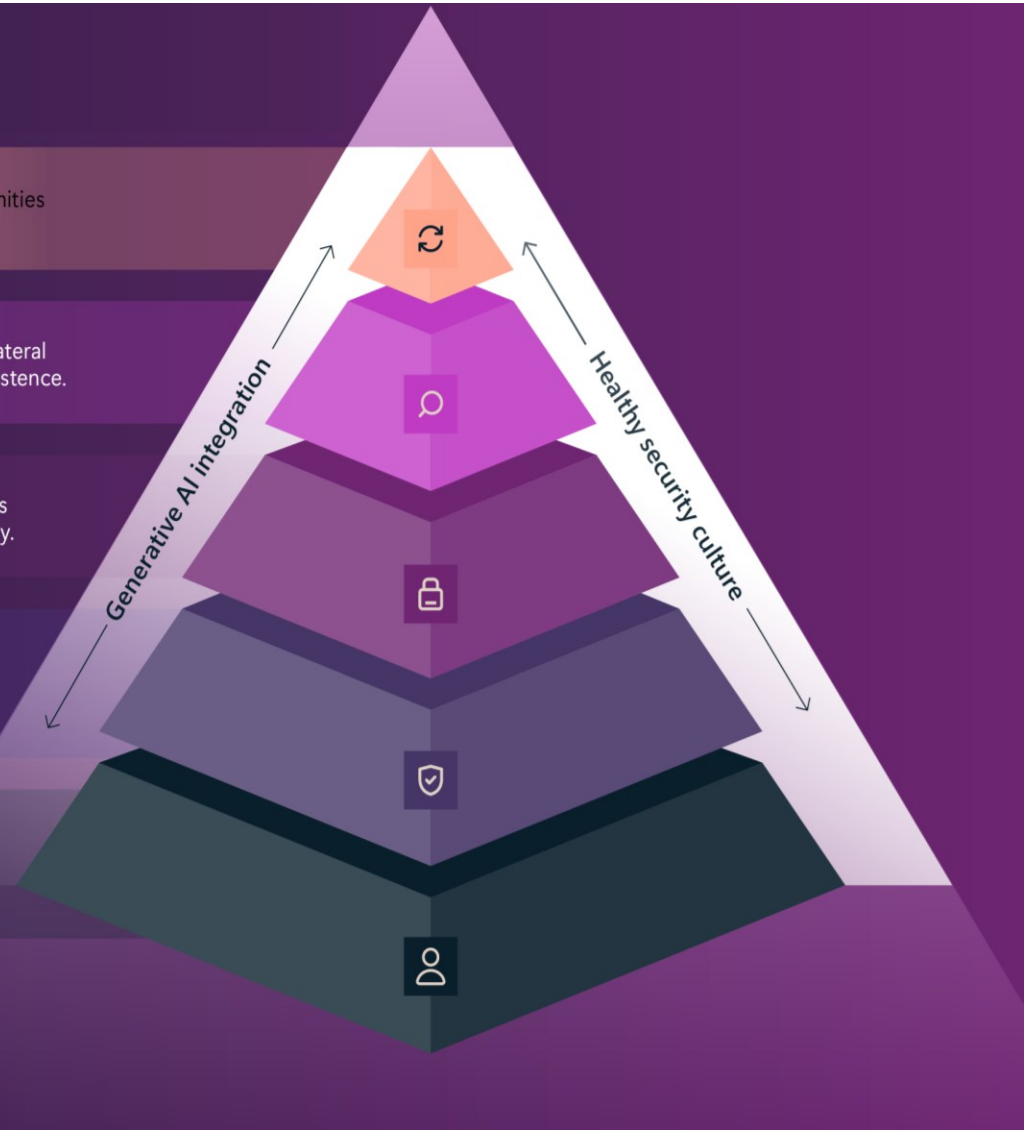
Effective endpoint protection can limit the repercussions of unauthorized access.

PROTECT IDENTITIES

"Attackers don't break in, they log in." Credentials for both individuals and machines are the perimeter of the modern attack surface.

IMPACT...

Strong identity security can greatly reduce risk exposure—particularly for ransomware attacks.



Vergleich der Cybersicherheitsfähigkeiten

Fähigkeiten & Innovation

- Wenige Ressourcen – schwer einzustellen/zu halten
- Manuelle Prozesse
- Mangel an Investitionen und Innovation

- qualifizierte/motivierte Ressourcen
- Automatisierte Prozesse
- Tiefe Taschen und kontinuierliche Innovation

Ansätze

- Cybersicherheit als IT-Funktion/Overhead
- Zero Trust wird nur als Technologiedomäne betrachtet

- Cyberkriminalität ist ein hochprofitables organisiertes Geschäft
- Cyber ist die Schlüsselfähigkeit der nationalen Offensive, um geopolitische Ziele wie Luft, See und Land voranzutreiben

Denkweise (Mindset)

- Geschlossenes Netzwerk (Air-Gapped) = Sicherheit
- Fokussiert auf den Datenspeicherort
- Public Cloud ist unbekannt und daher unsicher

- " Living off the land" unentdeckt
- Fokussiert auf Menschen (Identität & Endpunkte)
- Public-Cloud-Affinität, Scale-up und Automatisierung von Angriffen

Systeme

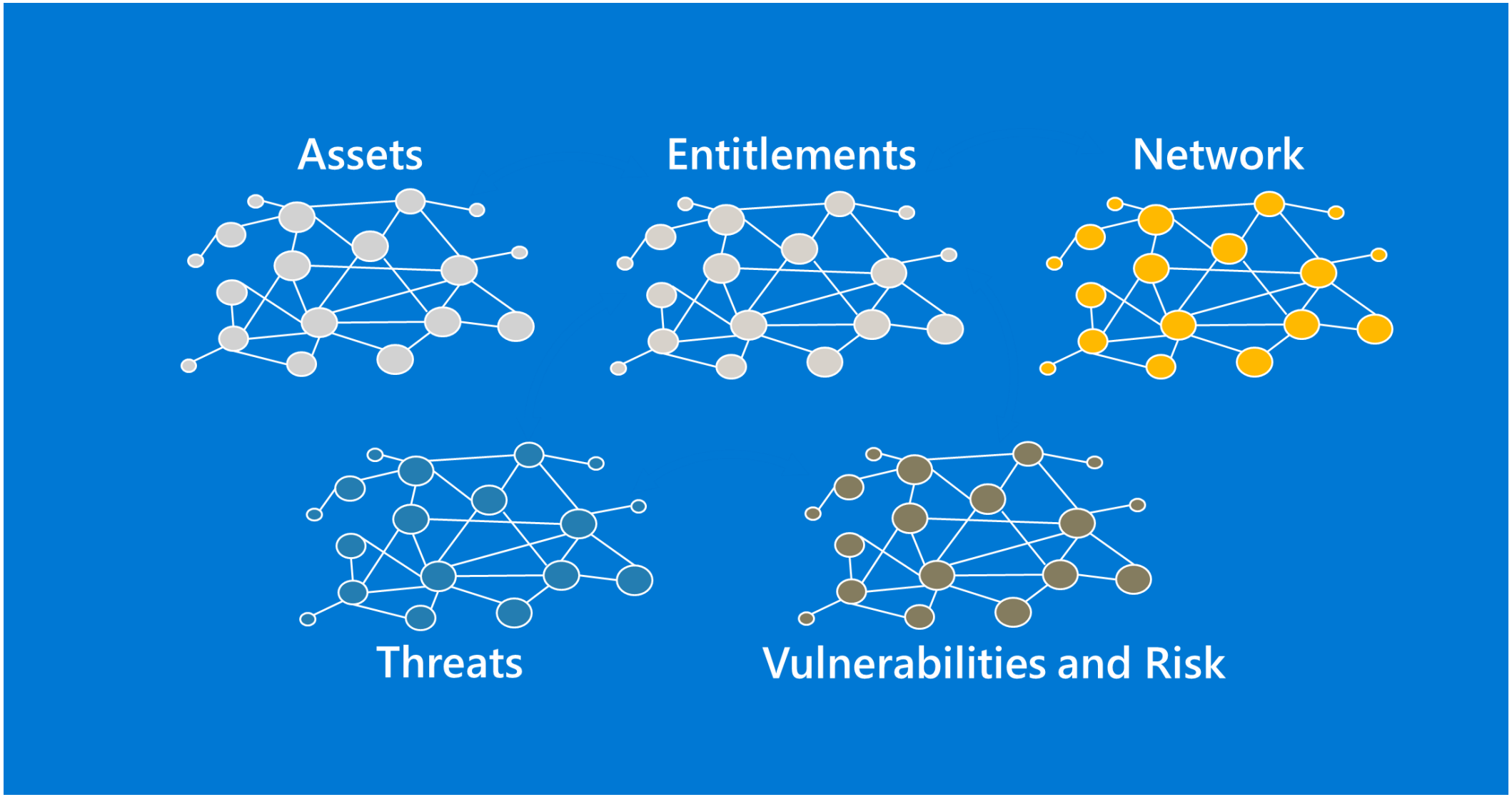
- Technische Schulden
- Isolierte Sicherheitsprodukte
- Legacy-Tools und -Infrastruktur

- Spitzentechnologie
- Integrierte Plattformen
- Frühe Technologieanwender (Early adopters)

Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.

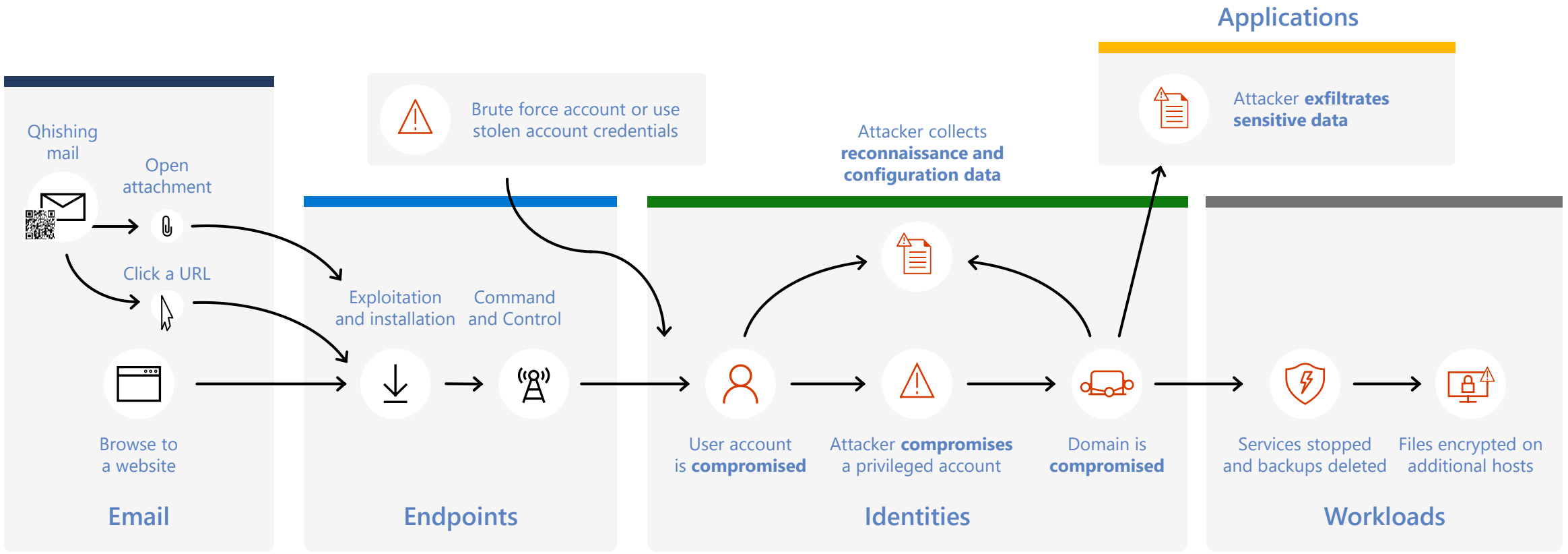
John Lambert, MSTIC

Zur Verteidigung brauchen wir den Graphen der Graphen



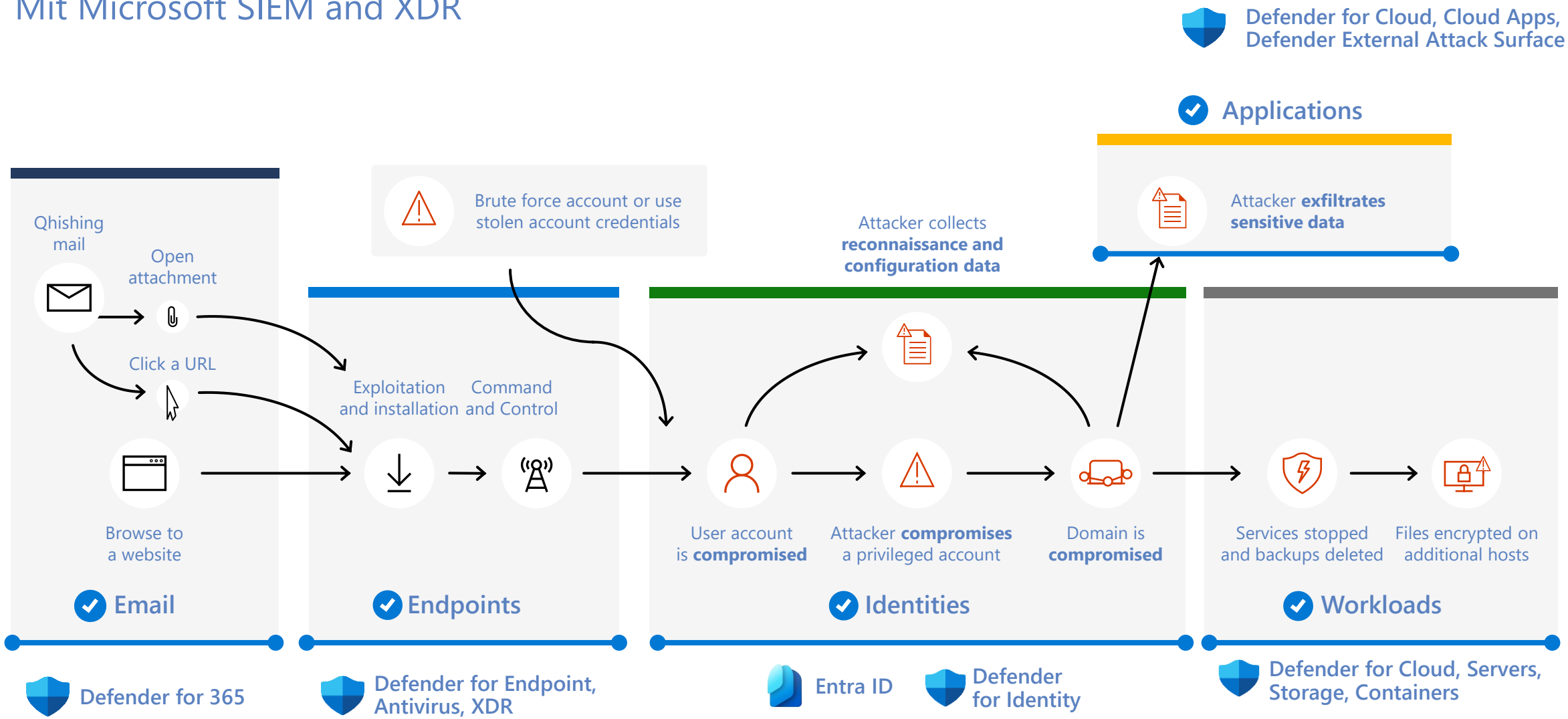
Einfache Fehler öffnen Türen und Tore

Typische human-operated ransomware Kampagne



Schutz entlang der gesamten kill chain

Mit Microsoft SIEM and XDR



Decken Sie den Angriff von Anfang bis Ende auf und ergreifen Sie Maßnahmen, um den Angreifer vollständig zu vertreiben.

Automatisierung der Verteidigung

Rolle der Automatisierung

Automatisierung spielt die entscheidende Rolle in der schnellen und effizienten Implementierung von Sicherheitsmaßnahmen.

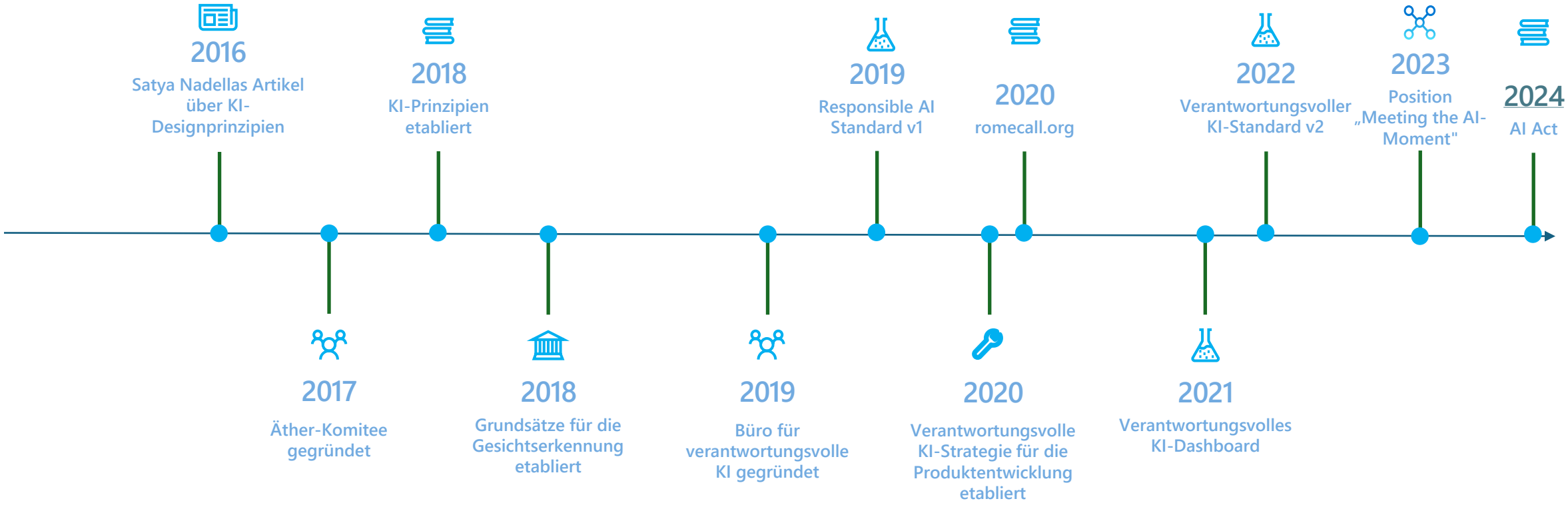
Erkennung und Abwehr von Bedrohungen

MSTIC und MTAC liefern wichtige Informationen und Tools zur Erkennung und Abwehr von Bedrohungen.

Reaktion in Echtzeit

Automatisierung ermöglicht es, schneller auf Bedrohungen zu reagieren und die Sicherheit zu erhöhen.

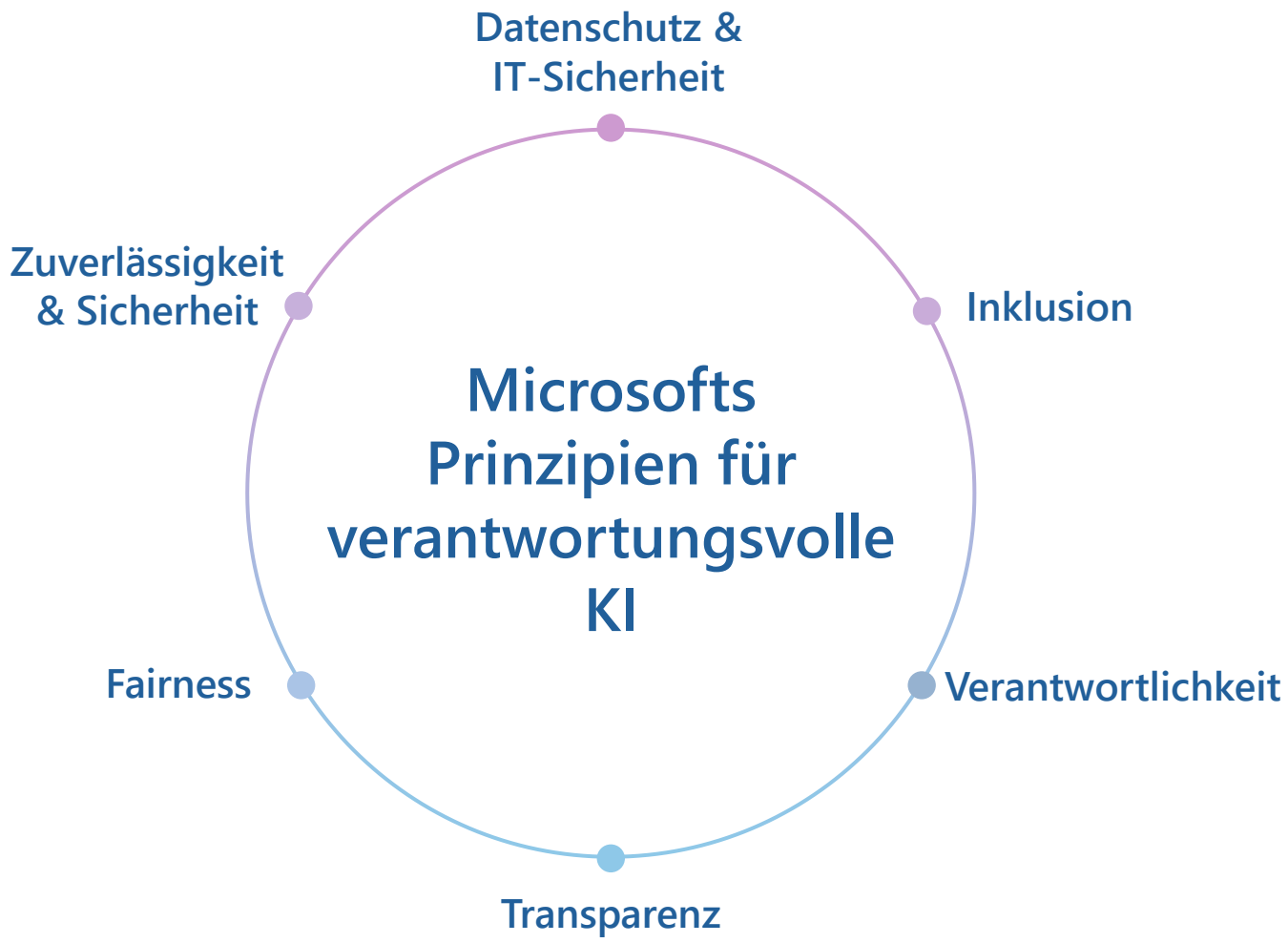
Unser Weg zur Verantwortlichen KI



Microsoft Security

Empowering responsible AI practices

Verantwortungsvolle Künstliche Intelligenz

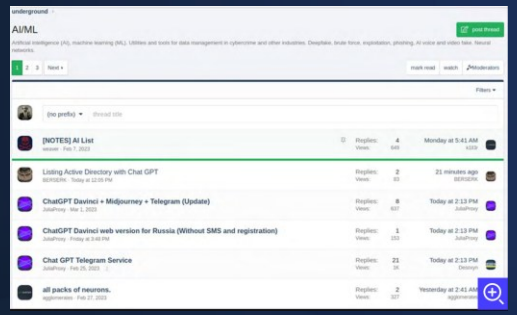


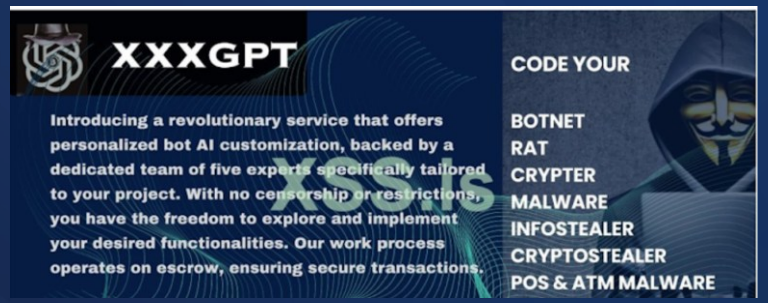
Bausteine zur Umsetzung der Prinzipien

- Tools und Prozesse
- Training und Praxis
- Politik
- Governance

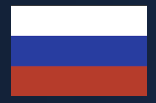
[Empowering responsible AI practices]

Die Angreifer agieren ohne Einschränkungen, Regeln oder Grenzen.





Einsatz von KI-basierten Offensivtechniken durch die “Big 4”



Russia

- LLM-informed reconnaissance: Interacting with LLMs to understand satellite communication protocols, radar imaging technologies, and specific technical parameters. These queries suggest an attempt to acquire in-depth knowledge of satellite capabilities.
- LLM-enhanced scripting techniques: Seeking assistance in basic scripting tasks, including file manipulation, data selection, regular expressions, and multiprocessing, to potentially automate or optimize technical operations.

China

- LLM-informed reconnaissance: Engaging LLMs to research and understand specific technologies, platforms, and vulnerabilities, indicative of preliminary information-gathering stages.
- LLM-enhanced scripting techniques: Utilizing LLMs to generate and refine scripts, potentially to streamline and automate complex cyber tasks and operations.
- LLM-supported social engineering: Leveraging LLMs for assistance with translations and communication, likely to establish connections or manipulate targets.
- LLM-refined operational command techniques: Utilizing LLMs for advanced commands, deeper system access, and control representative of post-compromise behavior.

Einsatz von KI-basierten Offensivtechniken durch die “Big 4”

North Korea

- LLM-assisted vulnerability research: Interacting with LLMs to better understand publicly reported vulnerabilities, such as the CVE-2022-30190 Microsoft Support Diagnostic Tool (MSDT) vulnerability (known as “Follina”).
- LLM-enhanced scripting techniques: Using LLMs for basic scripting tasks such as programmatically identifying certain user events on a system and seeking assistance with troubleshooting and understanding various web technologies.
- LLM-supported social engineering: Using LLMs for assistance with the drafting and generation of content that would likely be for use in spear-phishing campaigns against individuals with regional expertise.
- LLM-informed reconnaissance: Interacting with LLMs to identify think tanks, government organizations, or experts on North Korea that have a focus on defense issues or North Korea’s nuclear weapon’s program.

Iran

- LLM-supported social engineering: Interacting with LLMs to generate various phishing emails, including one pretending to come from an international development agency and another attempting to lure prominent feminists to an attacker-built website on feminism.
- LLM-enhanced scripting techniques: Using LLMs to generate code snippets that appear intended to support app and web development, interactions with remote servers, web scraping, executing tasks when users sign in, and sending information from a system via email.
- LLM-enhanced anomaly detection evasion: Attempting to use LLMs for assistance in developing code to evade detection, to learn how to disable antivirus via registry or Windows policies, and to delete files in a directory after an application has been closed.

Security Copilot in Microsoft Defender

10+ skills focused on the SOC tasks to be completed

Prevent breaches with dynamic threat insights

- Discover key threats for your specific risk profile
- Find and eliminate critical exposures
- Understand your adversaries and how to defend against them
- Get answers for a wide-range of threat intelligence questions

Identify and prioritize with built-in context

- Triage quickly with incident summaries written in plain language
- Understand attack story mapped to MITRE ATT&CK Framework
- Surface device asset details including data from Intune

Accelerate full resolution for every incident

- Determine best course of action for investigation and remediation
- Build operational consistency and efficacy with guided response
- Easily communicate with end users about the incident
- Quickly create and share an executive-level summary report

Elevate analysts with intelligent assistance

- Uplevel analyst productivity with suggested, tailored prompts
- Translate natural language to Kusto Query Language (KQL)
- Analyze malicious scripts
- Investigate suspicious files

Interessante Copilot-Statistiken

Mit Copilot..

30%

Schnellere Vorgangsbearbeitung in 3 Monaten

Mit Copilot...

23%

Weniger Alert

Mit Copilot...

68%

Verringerung der Wahrscheinlichkeit, dass Vorfall erneut geöffnet wird

“Cybersicherheit ist wie der Gang ins Fitnessstudio. Du kannst nicht besser werden, indem du anderen zusiehst, du musst jeden Tag selbst trainieren.”

Satya Nadella
Chief Executive Officer
Microsoft Corporation

Vielen Dank.