Herzlich willkommen! Ihre Online-Session startet gleich.

Schön, dass Sie dabei sind. Hören Sie uns einfach per Kopfhörer oder Lautsprecher zu.

Wir schalten die Mikrofone der Teilnehmer:innen stumm. Dann hören Sie alles besser. Auch alle Webcams sind automatisch deaktiviert.

Ihre Fragen können Sie über das Fragen-Fenster stellen. Der/die Moderator:in bringt Ihre Fragen entsprechend ein.

Session wird aufgezeichnet

Educational Month |

Cyber Security

Online-Session

KI-gesteuerte Security: Ende-zu-Ende-Sicherheit mit Microsoft

20.09.2024

Herzlich willkommen!

Schön, dass Sie dabei sind. Hören Sie uns einfach per Kopfhörer oder Lautsprecher zu.

Wir schalten die Mikrofone der Teilnehmer:innen stumm. Dann hören Sie alles besser. Auch alle Webcams sind automatisch deaktiviert.

Ihre Fragen können Sie über das Fragen-Fenster stellen. Der/die Moderator:in bringt Ihre Fragen entsprechend ein.

Session wird aufgezeichnet

Heute für Sie dabei:

Andreas Wach
Microsoft

Thomas Schmidt
PCG

Matthias Magnus
Vodafone

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3	21,1

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3	21,1
Kosten für Ermittlungen und Ersatzmaßnahmen	32,2	25,2	10,1

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3	21,1
Kosten für Ermittlungen und Ersatzmaßnahmen	32,2	25,2	10,1
Datenschutzrechtliche Maßnahmen, z.B. durch Behörden	27,2	12,4	18,3

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3	21,1
Kosten für Ermittlungen und Ersatzmaßnahmen	32,2	25,2	10,1
Datenschutzrechtliche Maßnahmen, z.B. durch Behörden	27,2	12,4	18,3
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	20,2	35,3	23,6
Patentrechtsverletzungen, auch vor Anmeldung	14,8	10,4	18,8
Erpressung mit gestohlenen Daten	13,4	16,1	10,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	11,2	21,5	41,5
Geldabfluss durch Betrugsversuche	0,8	3,9	-
Sonstige Schäden	0	1,1	0,9
Gesamtschaden pro Jahr	**266,6**	**205,9**	**202,7**

Basis: Alle Unternehmen (n=1.003) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. | Quelle: Bitkom Research 2024

Diese Unternehmen hat's schon erwischt (Auszug)

Unternehmen	Wann	Was	Anzahl Mitarbeiter	Branche
HVB Ingenieurgesellschaft MbH	Aug 2024	Ransomware und Datendiebstahl	**30**	Architekten und Ingenieure
Mittelbadische Entsorgungs- und Recyclingbetriebe (MERB)	Juli 2024		**300**	Entsorgung- und Recycling
Eurostrand	Juli 2024	Ransomware?	**ca. 400**	Ferienresort und Restaurant
Lambertz	Juni 2024	Ransomware	**4.000**	Gebäckhersteller
Meiller Kipper	Juni 2024		**2.000**	Kipplastwagen
Westfälische Stahlgesellschaft	Juni 2024	Ransomware	**190**	Stahlgesellschaft
Melting Mind	April 2024	Ransomware	**<10**	IT
Max Wild	April 2024		**750**	Bau und Logistik
Bieler + Lang	April 2024		**100**	Gasmess- und Warnsysteme
Hospitaltechnik Planungsgesellschaft	April 2024		**60**	Planung und Beratung für Kliniken, Krankenhäuser

Quelle: Cyberangriffe in Deutschland 2023/2024: Diese Unternehmen hat's schon erwischt - CSO (csoonline.com)

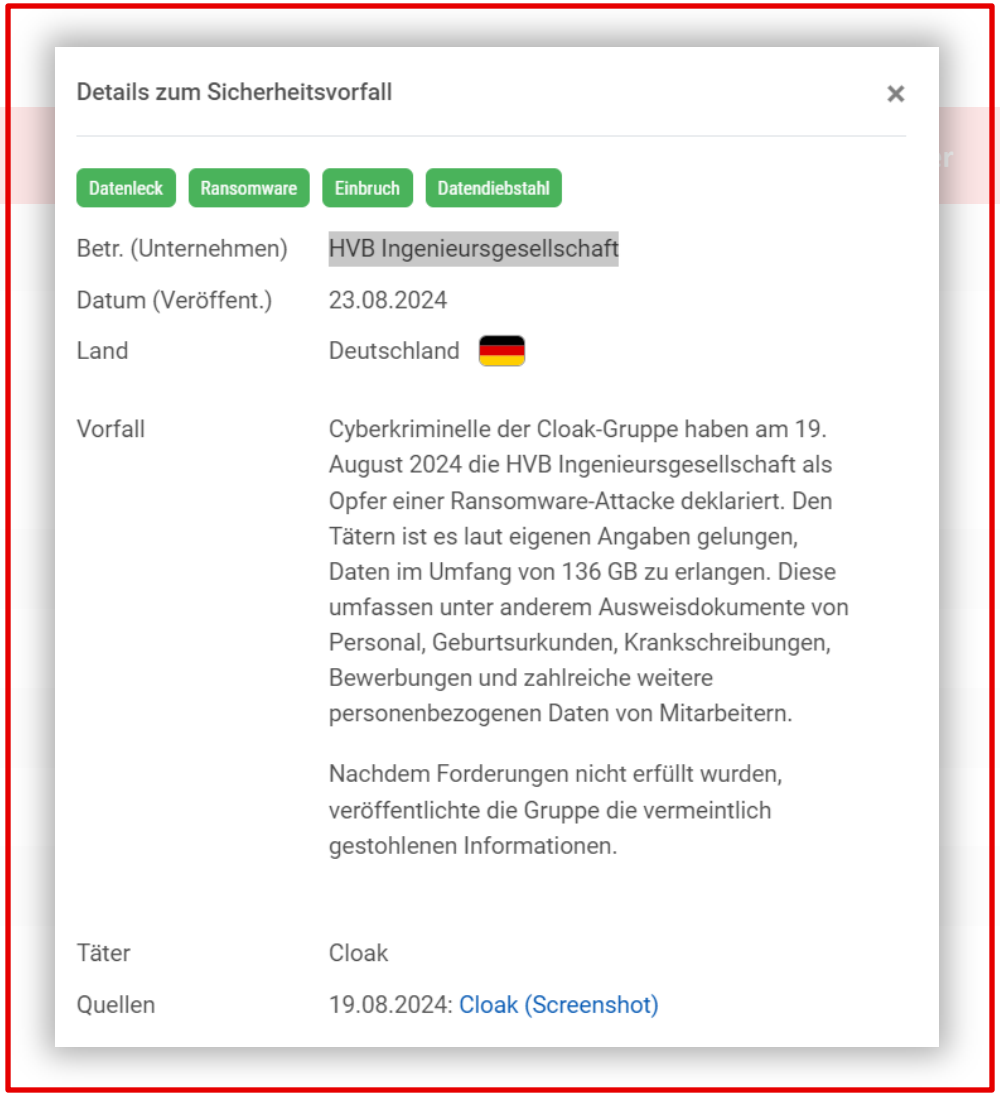
Diese Unternehmen hat's schon erwischt (Auszug)

Unternehmen	Wann	Was	Anzahl Mitarbeiter	Branche
HVB Ingenieurgesellschaft MbH	Aug 2024	Ransomware und Datendiebstahl	30	Architekten und Ingenieure
Mittelbadische Entsorgungs- und Recyclingbetriebe (MERB)	Juli 2024		300	Entsorgung- und Recycling
Eurostrand	Juli 2024	Ransomware?	ca. 400	Ferienresort und Restaurant
Lambertz	Juni 2024	Ransomware	4.000	Gebäckhersteller
Meiller Kipper	Juni 2024		2.000	Kipplastwagen
Westfälische Stahlgesellschaft	Juni 2024	Ransomware	190	Stahlgesellschaft
Melting Mind	April 2024	Ransomware	<10	IT
Max Wild	April 2024		750	Bau und Logistik
Bieler + Lang	April 2024		100	Gasmess- und Warnsysteme
Hospitaltechnik Planungsgesellschaft	April 2024		60	Planung und Beratung für Kliniken, Krankenhäuser

Quelle: Cyberangriffe in Deutschland 2023/2024: Diese Unternehmen hat's schon erwischt - CSO (csoonline.com)

Diese Unternehmen hat's schon erwischt (Auszug)

Unternehmen	Branche
HVB Ingenieurgesellschaft MbH	Architekten und Ingenieure
Mittelbadische Entsorgungs- und Recyclingbetriebe (MERB)	Entsorgung- und Recycling
Eurostrand	Ferienresort und Restaurant
Lambertz	Gebäckhersteller
Meiller Kipper	Kipplastwagen
Westfälische Stahlgesellschaft	Stahlgesellschaft
Melting Mind	IT
Max Wild	Bau und Logistik
Bieler + Lang	Gasmess- und Warnsysteme
Hospitaltechnik Planungsgesellschaft	Planung und Beratung für Kliniken, Krankenhäuser



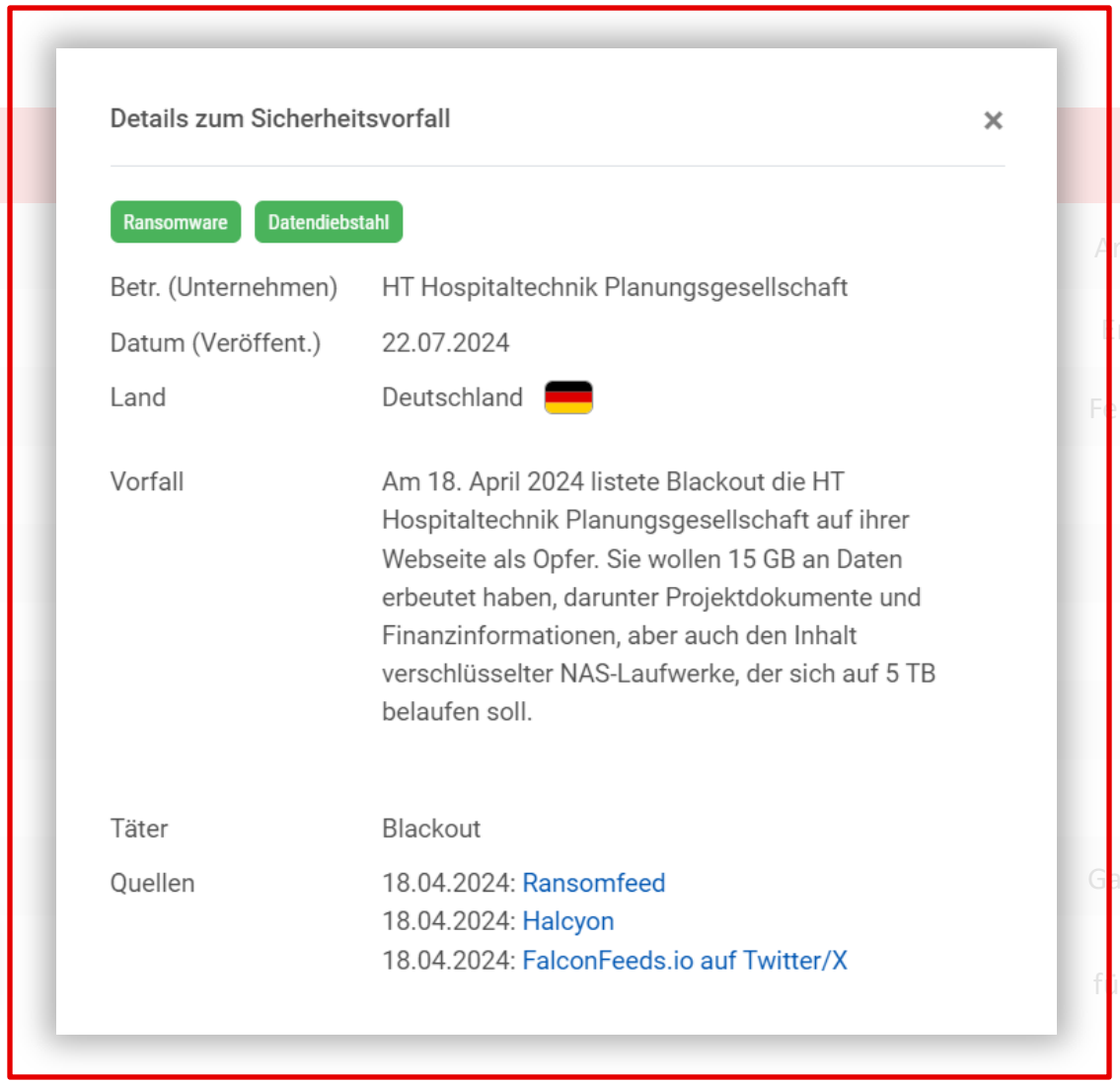
Details zum Sicherheitsvorfall

Datenleck | Ransomware | Einbruch | Datendiebstahl

Betr. (Unternehmen)	HVB Ingenieursgesellschaft
Datum (Veröffent.)	23.08.2024
Land	Deutschland
Vorfall	Cyberkriminelle der Cloak-Gruppe haben am 19. August 2024 die HVB Ingenieursgesellschaft als Opfer einer Ransomware-Attacke deklariert. Den Tätern ist es laut eigenen Angaben gelungen, Daten im Umfang von 136 GB zu erlangen. Diese umfassen unter anderem Ausweisdokumente von Personal, Geburtsurkunden, Krankschreibungen, Bewerbungen und zahlreiche weitere personenbezogenen Daten von Mitarbeitern. Nachdem Forderungen nicht erfüllt wurden, veröffentlichte die Gruppe die vermeintlich gestohlenen Informationen.
Täter	Cloak
Quellen	19.08.2024: Cloak (Screenshot)

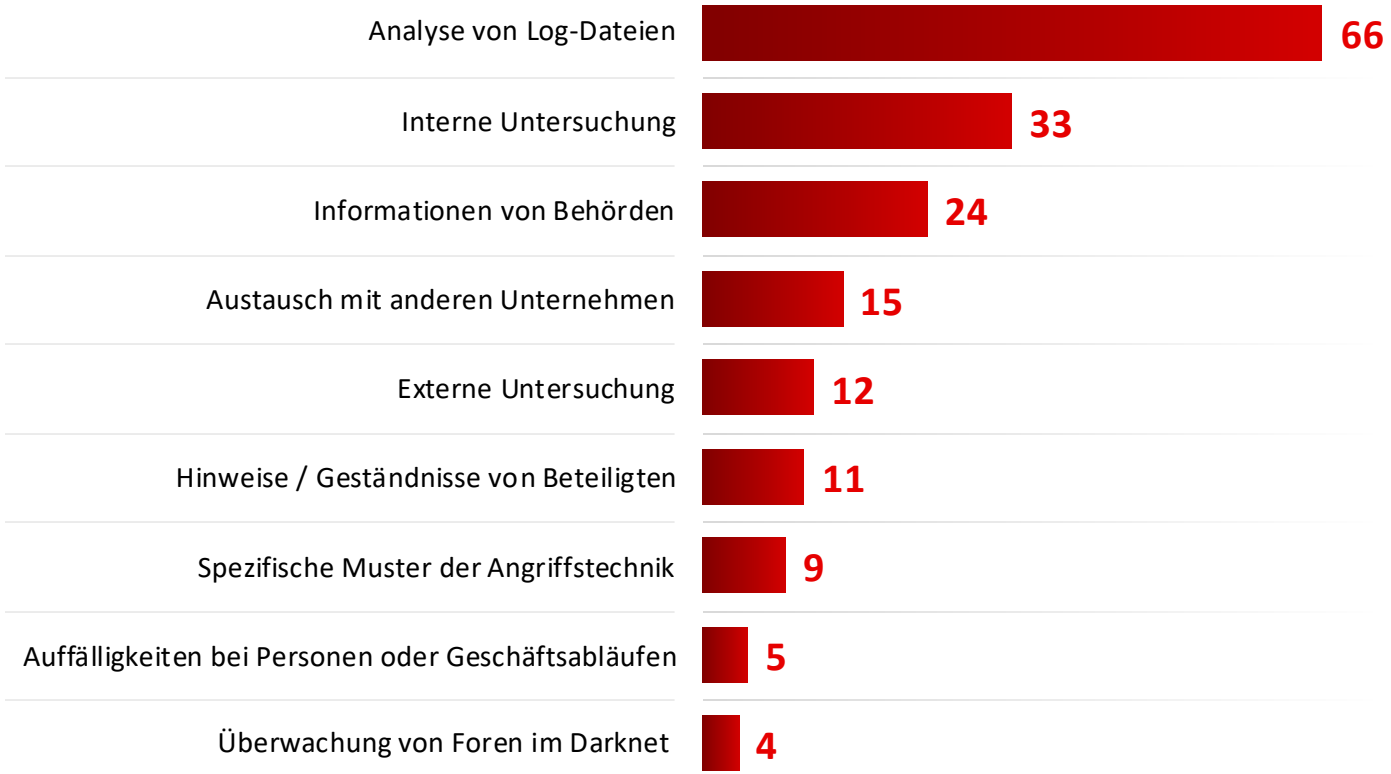
Diese Unternehmen hat's schon erwischt (Auszug)

Unternehmen	Branche
HVB Ingenieurgesellschaft MbH	Architekten und Ingenieure
Mittelbadische Entsorgungs- und Recyclingbetriebe (MERB)	Entsorgung- und Recycling
Eurostrand	Ferienresort und Restaurant
Lambertz	Gebäckhersteller
Meiller Kipper	Kipplastwagen
Westfälische Stahlgesellschaft	Stahlgesellschaft
Melting Mind	IT
Max Wild	Bau und Logistik
Bieler + Lang	Gasmess- und Warnsysteme
Hospitaltechnik Planungsgesellschaft	Planung und Beratung für Kliniken, Krankenhäuser



Wie Taten aufgedeckt werden

Auf welcher Grundlage haben Sie die Erkenntnisse erlangt?



in Prozent

Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und Erkenntnisse über Herkunft, Täterkreis oder Motive hatten (n=783) I Mehrfachnennungen möglich
Quelle: Bitkom Research 2024

Microsoft Security

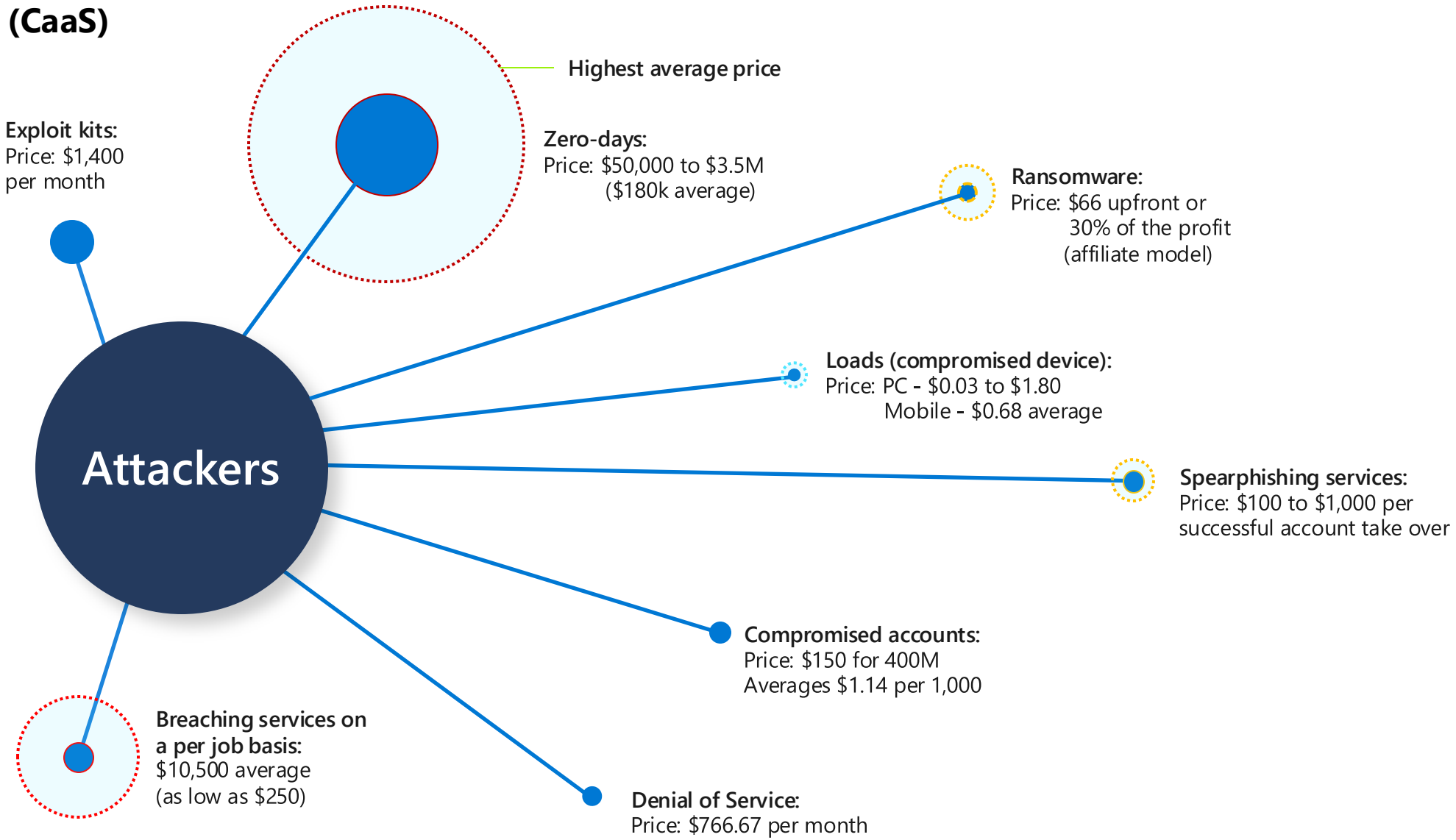
Andreas Wach

Partner Solution Architect
for Security
XDR & SIEM with SOC
andreas.wach@microsoft.com


Technologie
ist nur ein
Teil der
Geschichte

Attack services are cheap

Crime as a Service (CaaS)



The State of **Cybercrime**

Key developments

80-90%

of all successful ransomware compromises originate through unmanaged devices.

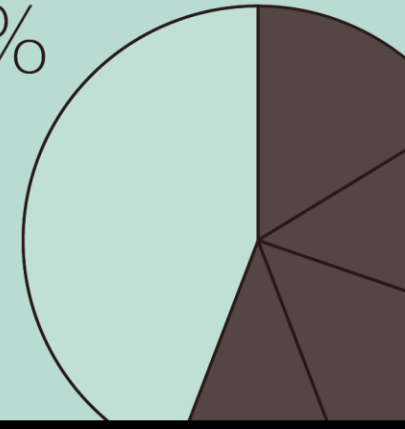
A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.

70%

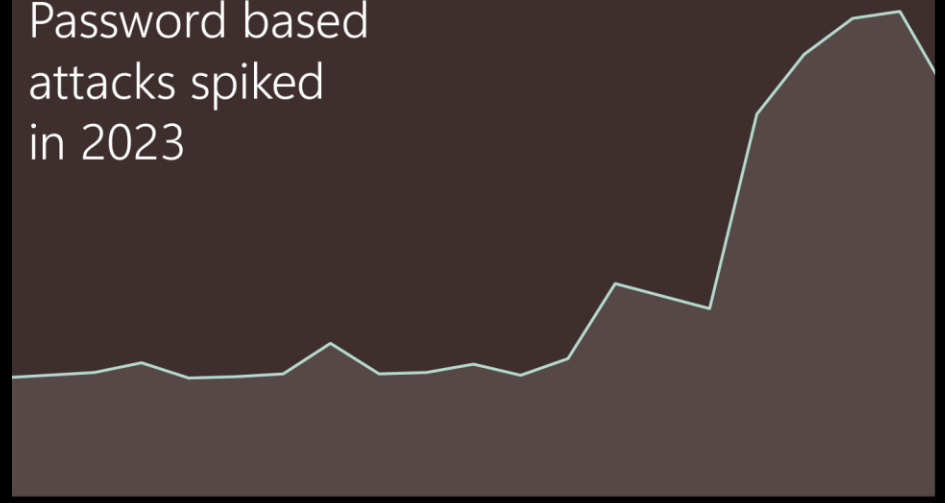
of organizations encountering human-operated ransomware had fewer than 500 employees.

Human-operated ransomware attacks are up more than

200%



Password based attacks spiked in 2023



Last year marked a significant shift in cybercriminal tactics

with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks. 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.

Quelle: MDDR 2023


Return on Investment (ROI)

Beste Umsetzung für DICH

... die Technologie zur Unterstützung

Firewall?

... ja, aber noch viel mehr

How can we protect against 99% of attacks?

*Source: https://arxiv.org/abs/2305.00945

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.*

Fundamentals of cyber hygiene

99%

Basic security hygiene still protects against 99% of attacks.

- Enable multifactor authentication (MFA)
- Apply Zero Trust principles
- Use extended detection and response (XDR) and antimalware
- Keep up to date
- Protect data

Outlier attacks on the bell curve make up just 1%

Quelle: MDDR 2023

Gartner®

Microsoft Security: führender Anbieter in sechs Magic Quadrants von Gartner

Identity & Access Management

Cloud Access Security Brokers

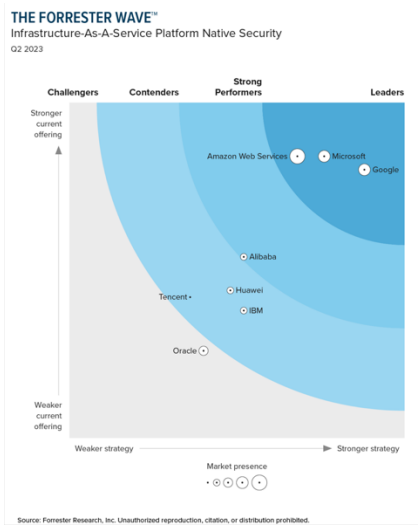
Enterprise Information Archiving

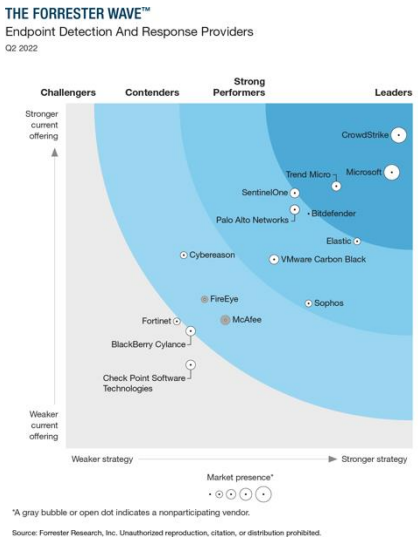
Endpoint Protection Platforms

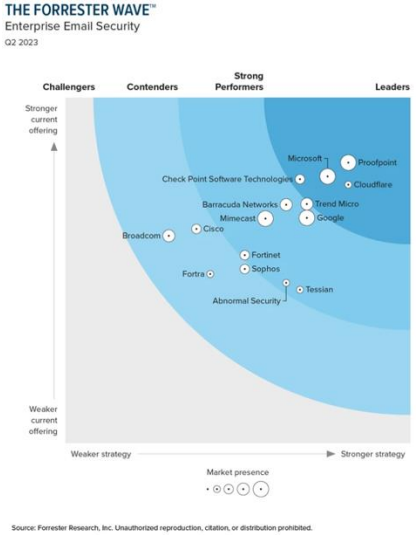
Unified Endpoint Management

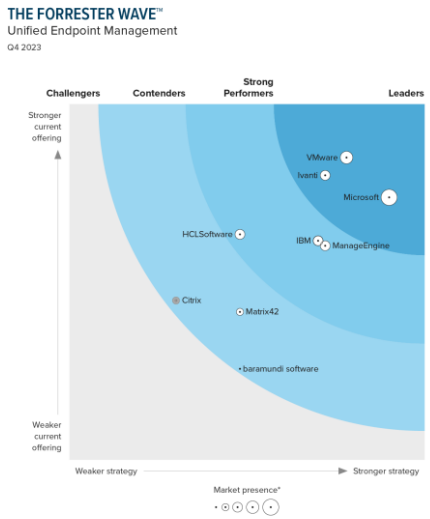
Security Information and Event Management

Microsoft – a leader in nine Forrester Wave™ reports

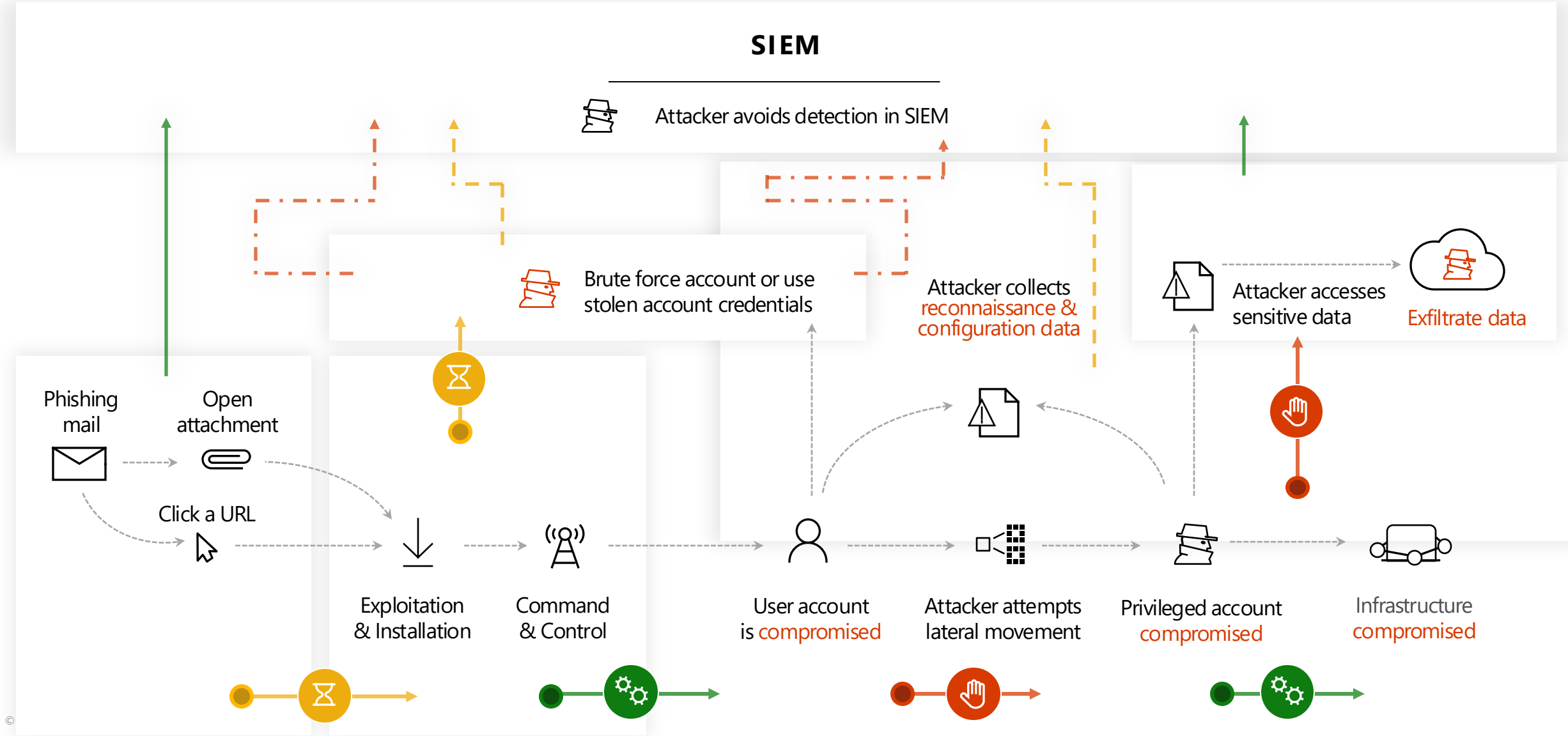




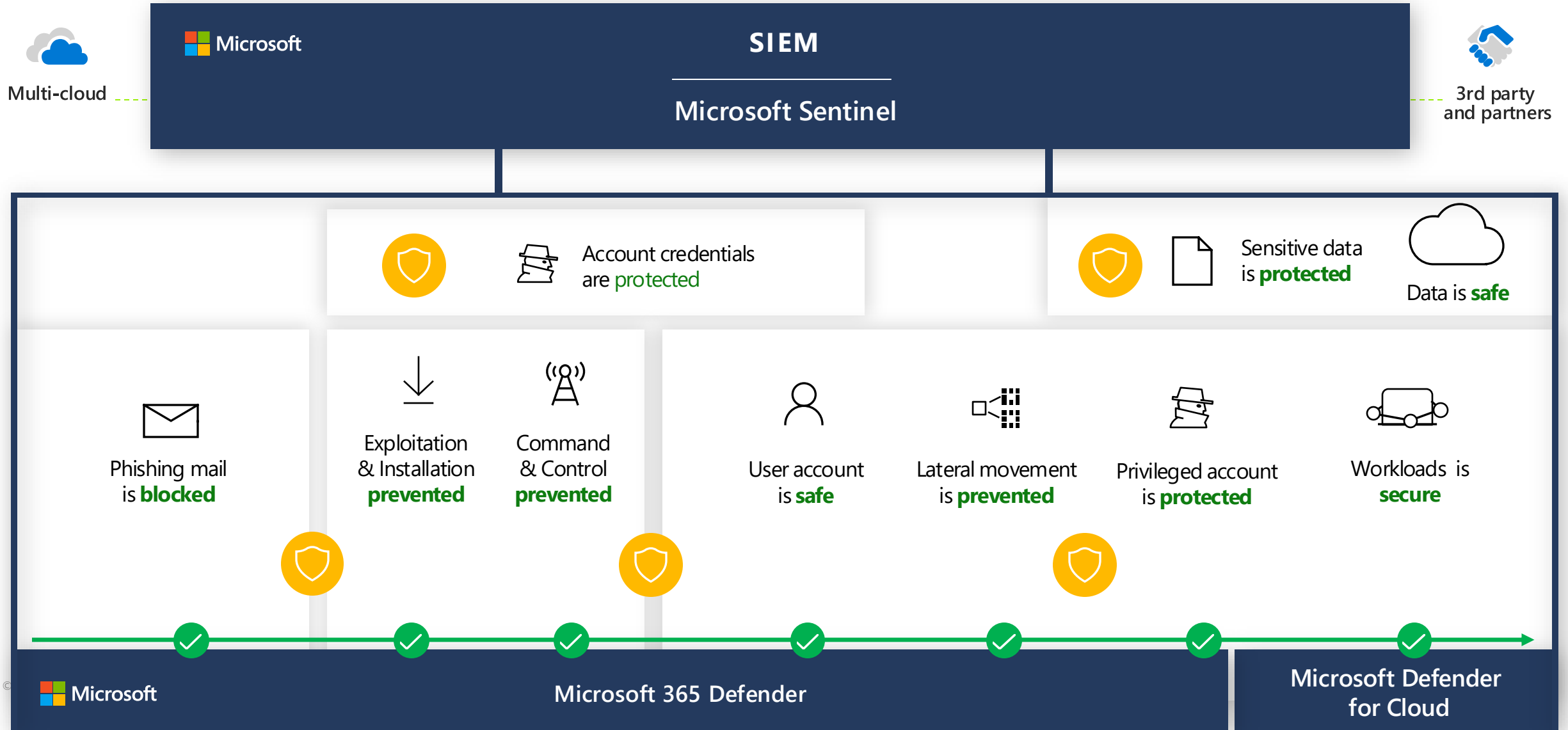




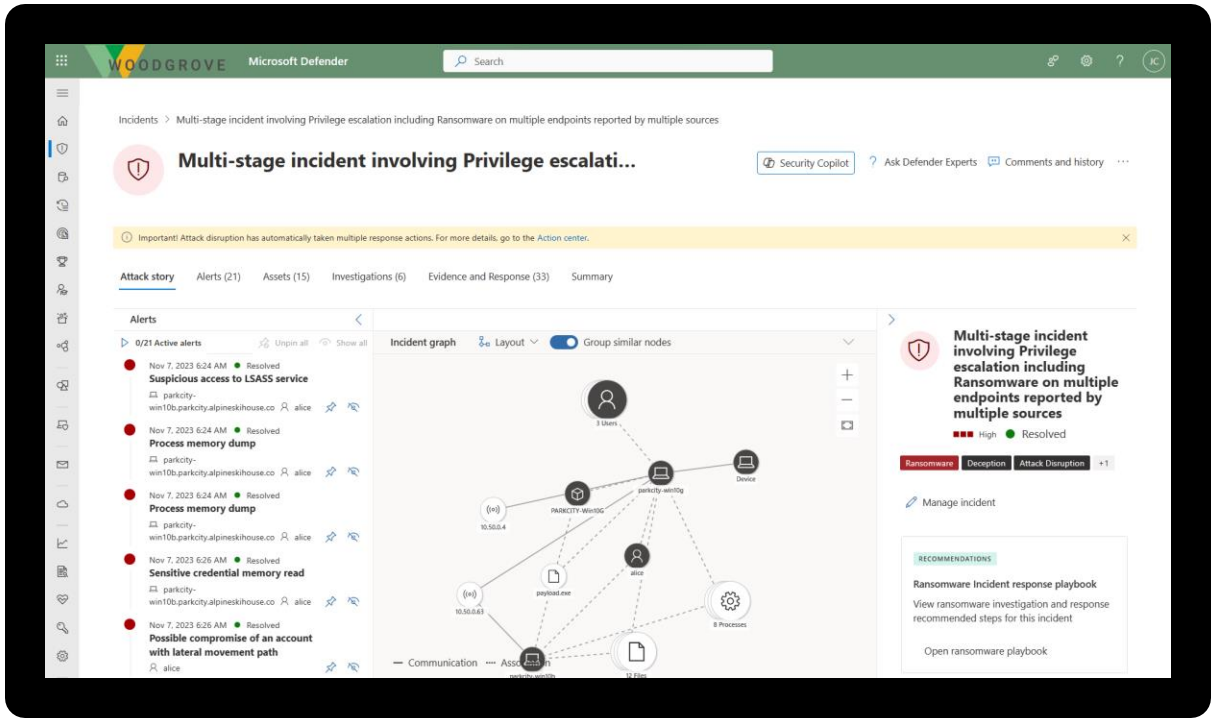
Siloed security leads to gaps and increased operational overhead



Close the gaps. Spot once, block everywhere



Attack disruption at machine speed



AI-powered **automation** disrupts lateral movement

Leaves the SOC team in full control of investigating and remediating

Reduces the overall cost and limits the impact of an attack by stopping lateral movement

Detection

Correlates signals from multiple sources into a single, high-confidence incident

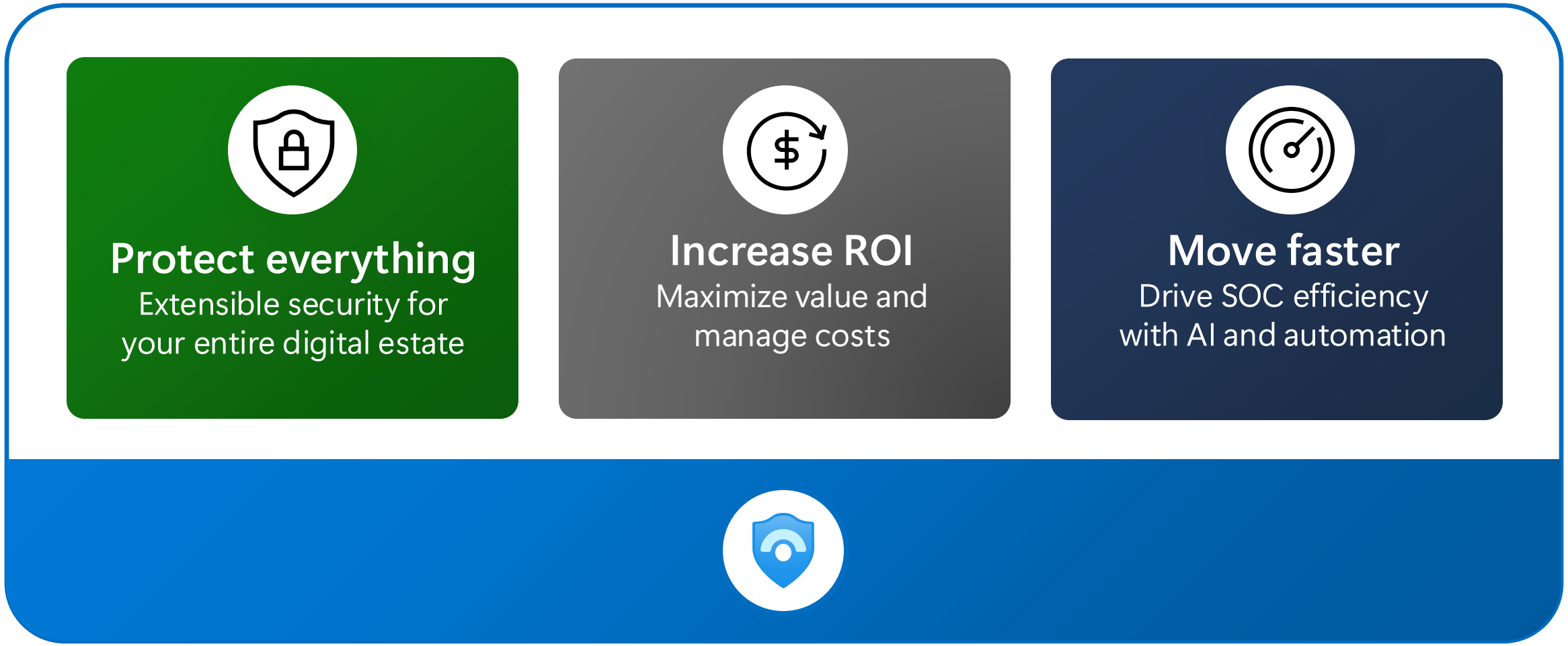
Classification

Classify attack scenario and **identify** assets controlled by the attacker

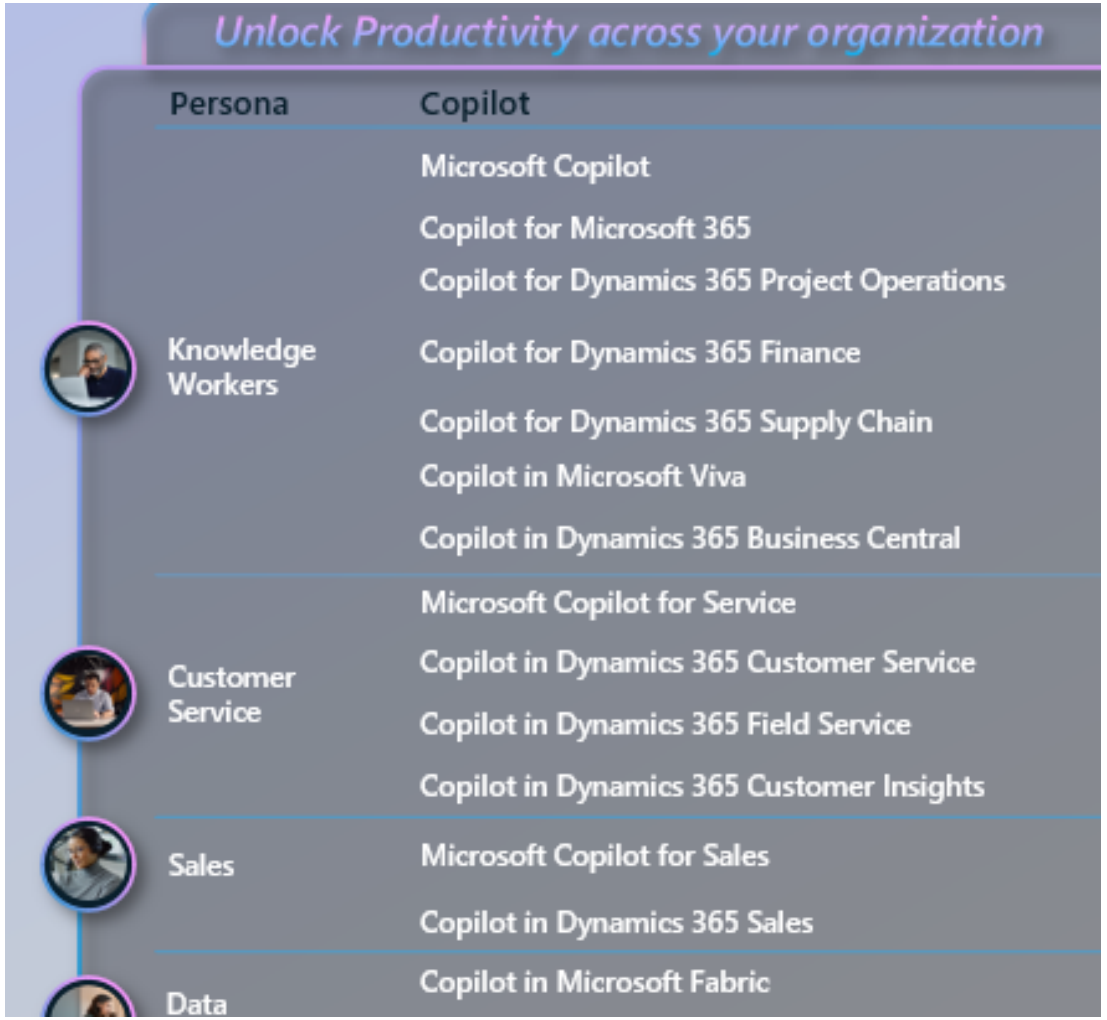
Attack disruption

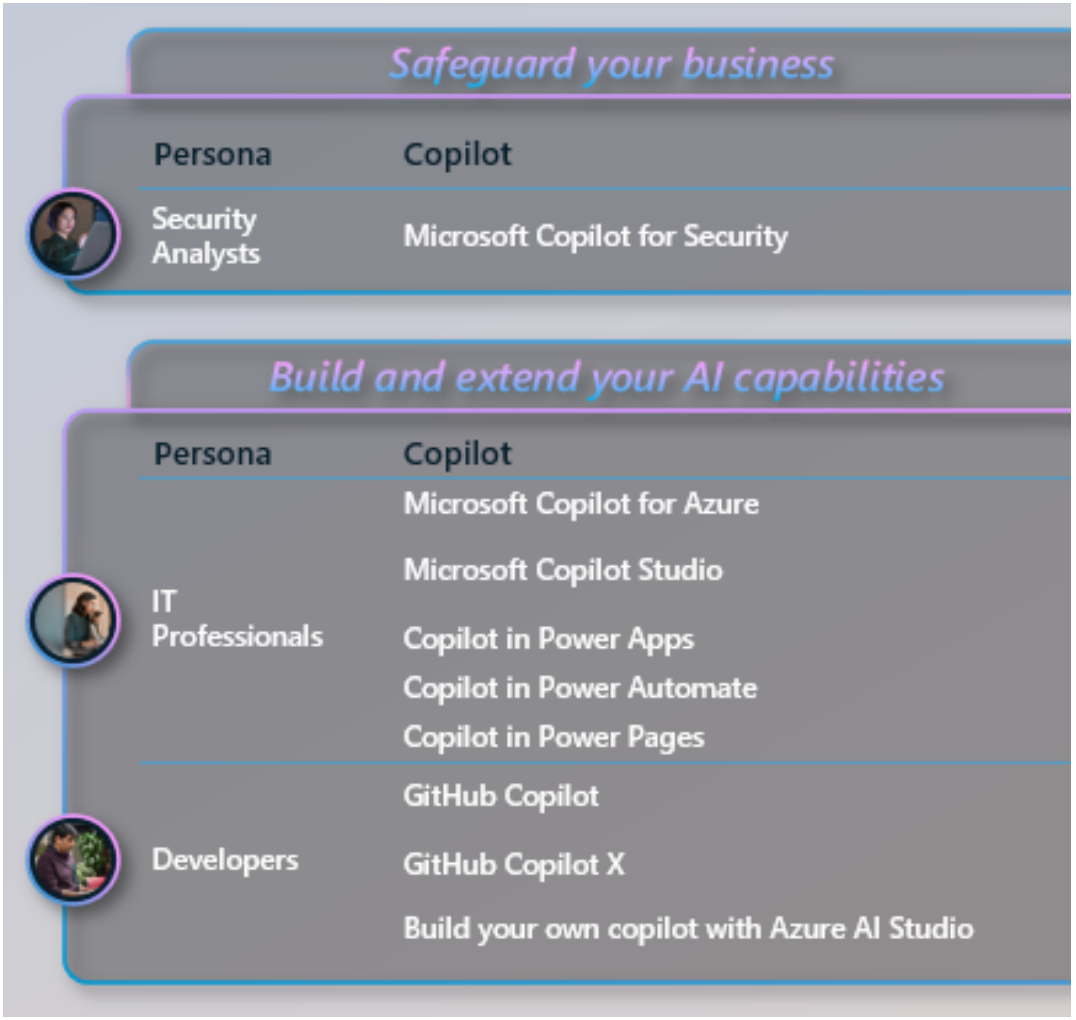
Automatically isolates infected devices and suspends compromised accounts in real-time

Microsoft Sentinel supports the needs of a modern SOC



Microsoft Copilot empowering your business





Copilot for Security

Protect at the speed and scale of AI

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

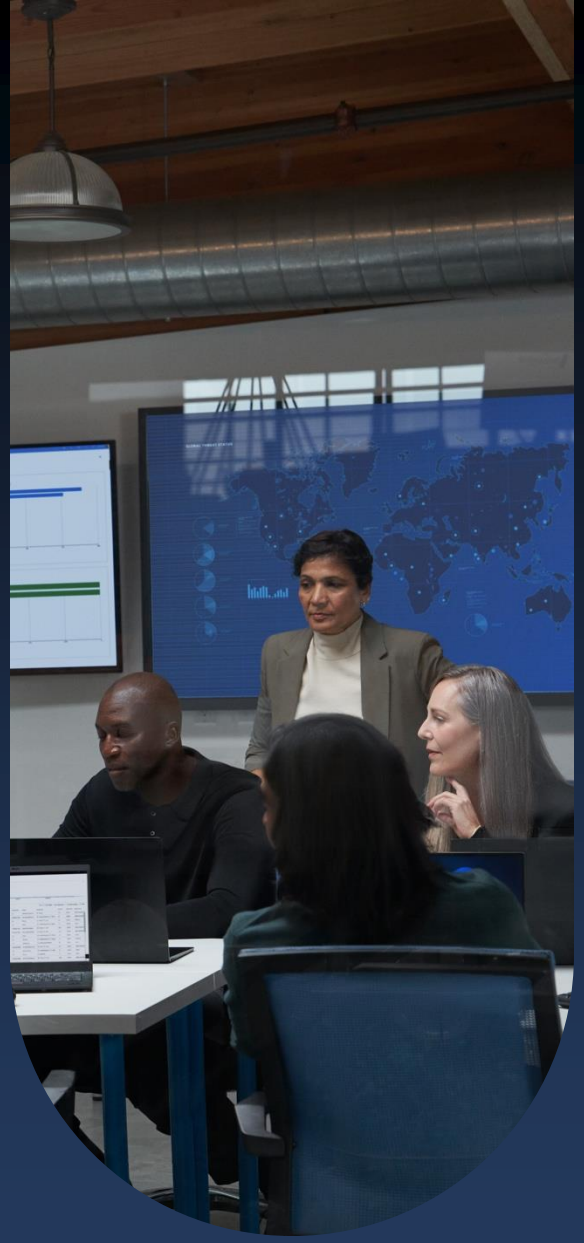
- Copilot for Security customer

Enable response in minutes, not hours

Simplify the complex with natural language prompts and easy reporting

Catch what others miss with deeper understanding of your enterprise

Strengthen team expertise with cyber skills and promptbooks



Microsoft Copilot for Security boosting your SOC team

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

Personas beyond SOC analysts

DLP Analysts

Summarize **Data Loss Prevention** alerts and analyze DLP policy configurations

Insider Risk Analysts

Summarize **Insider Risk Management** alerts and gain context around user intent along with risky behavior

IT Administrators

Create device configuration profiles with natural language prompts in **Intune** and leverage data-driven configuration troubleshooting and remediation

eDiscovery Analysts

Generate Keyword Query Language from natural language in **eDiscovery** and summarize evidence collected in review sets

Identity Access Management Administrators

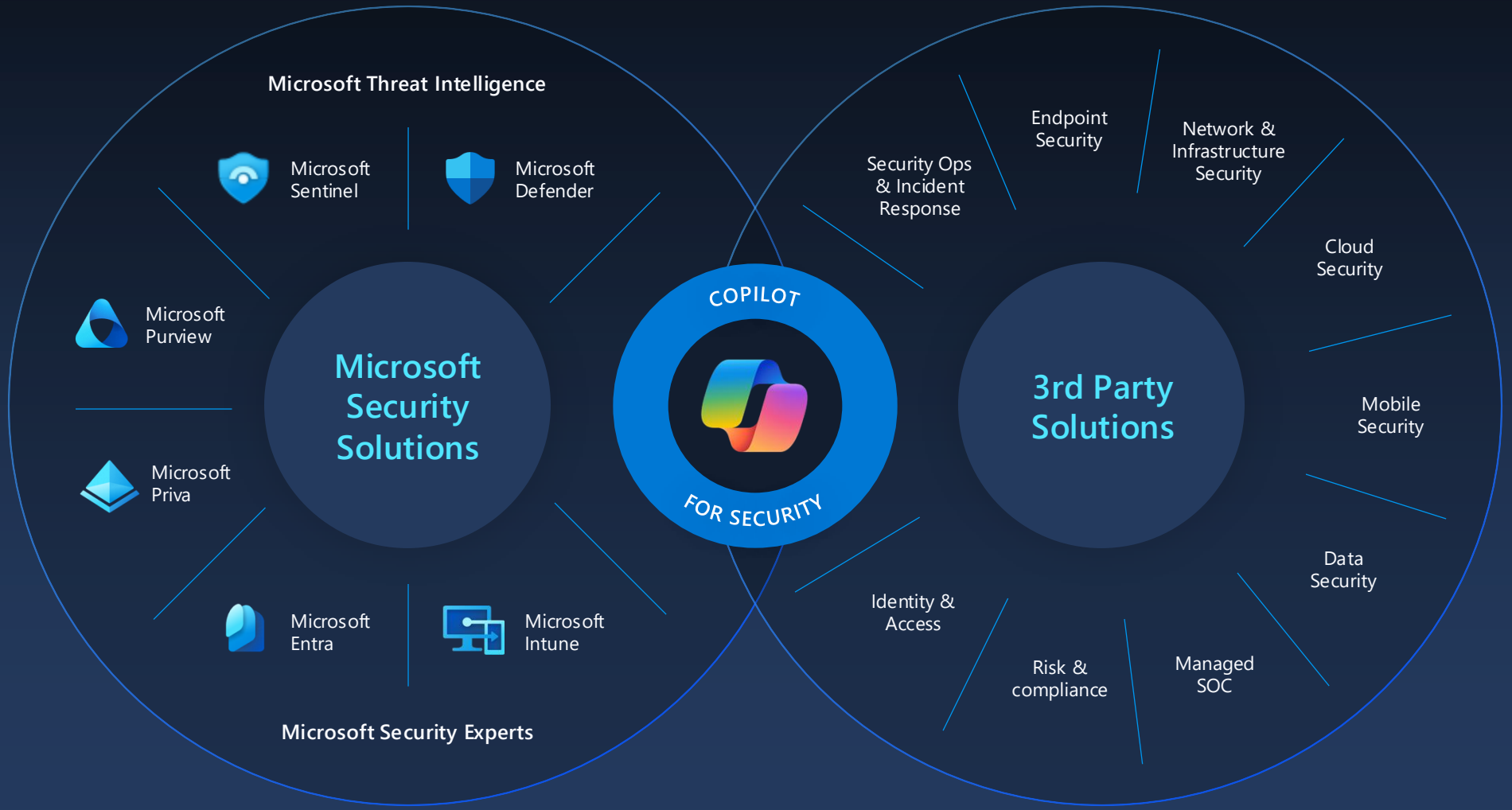
Discover high risk users, over privileged access, suspicious sign-ins in **Entra** with recommended guidance for steps to remediate

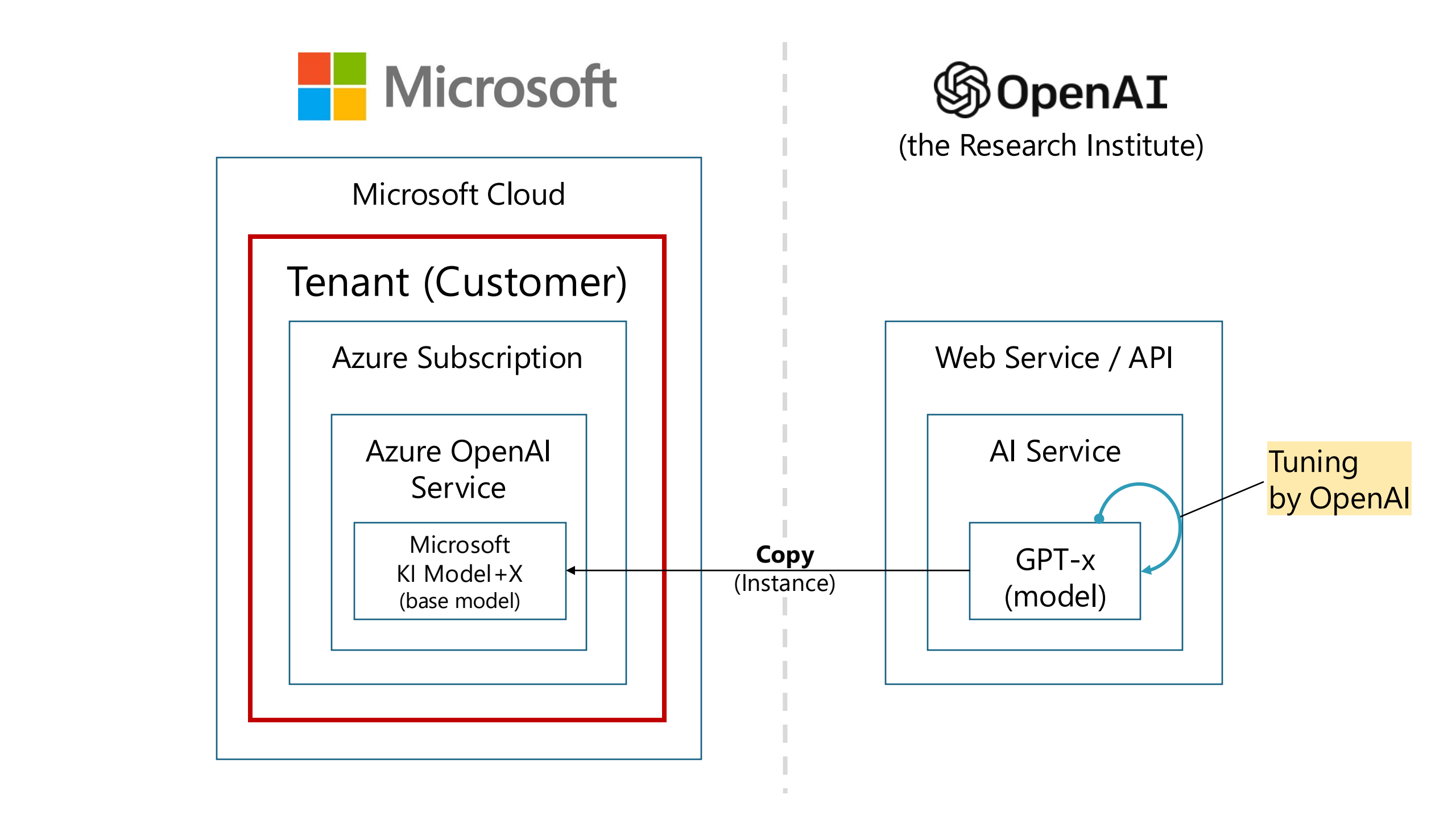
Compliance Analysts

Summarize **Communication Compliance** alerts and accelerate understanding of communication violations

The Copilot for Security advantage

Copilot stitches together information across all security products




Microsoft
OpenAI
(the Research Institute)
Microsoft Cloud
Tenant (Customer)
Azure Subscription
Azure OpenAI Service
Microsoft KI Model+X (base model)
Copy
(Instance)
Web Service / API
AI Service
GPT-x (model)
Tuning by OpenAI

Start your Microsoft Security journey NOW

Security Assessments aus Kundensicht!

Public Cloud Group

Security Assessments

Public Cloud Group

Thomas Schmidt
CISO | Director Business Unit CyberSecurity

Strategie. Viele Wege zum Ziel - direkter Ansatz.

Viele Wege führen zum Ziel - ein Assessment hilft zwei Positionen zu bestimmen **WO** und das **ZIEL**

Gründe für ein Assessment - Compliance | Intrinsisch | Extern?

Photo by DALL-E

Photo by DALL-E

Warum sind Assessments wichtig?

- Informationstechnologie ist wesentlich für den Betrieb von Organisationen
- Orientierung an Standards wie ISO 27001 oder NIST
- Good / Best Practises zu Anwendung bringen (Organisatorisch+Technisch)
- Vermeidbare Vorfälle verhindern, Sicherheit erhöhen und als verlässlich wahrgenommen werden

CyberSec Anforderungen

Ebenen CyberSec & Resilienz

- Risikoanalyse
  (Benötigt Ist-Stand)
- Verantwortlichkeiten (Governance) und Prozesse
- Bewusstsein schaffen auf allen Ebenen in der Organisation
- Resilienz verbessern (technisch, Lieferanten, prozessual)
- Erkennen und Reagieren
- Realistische Planung für Vorfall und K-Fall leben
- Unabhängige Auditierung

Vodafone Corporate & Cyber-Security

04

Egal ob Blau, Rot, M oder XXL…

Wir haben für Ihren Bedarf die optimale Lösung,
finden diese gemeinsam mit Ihnen und begleiten die Umsetzung.

Partnerprodukte
(Auszug)

CSOC dhpg & TÜV AUSTRIA Group
APPVISORY by mediaTest digital
vmware Carbon Black
ZIMPERIUM
CROWDSTRIKE
paloalto NETWORKS
DRACOON
KALI
CHECK POINT
pradeo
BlackBerry CYLANCE
SOPHOS
Hypergate
ISEC7 SPHERE
cybereason
teamwire.
AGAT
Windows Defender
Lookout
FORTINET

Unsere Partner
(Auszug)

schiffl
isec The Digital Workplace Company
SWISS IT SECURITY GROUP
Sie & 
REPLY
accenture
Microsoft
Systemhaus Compi Power ...the customer company
zscaler

Security first!

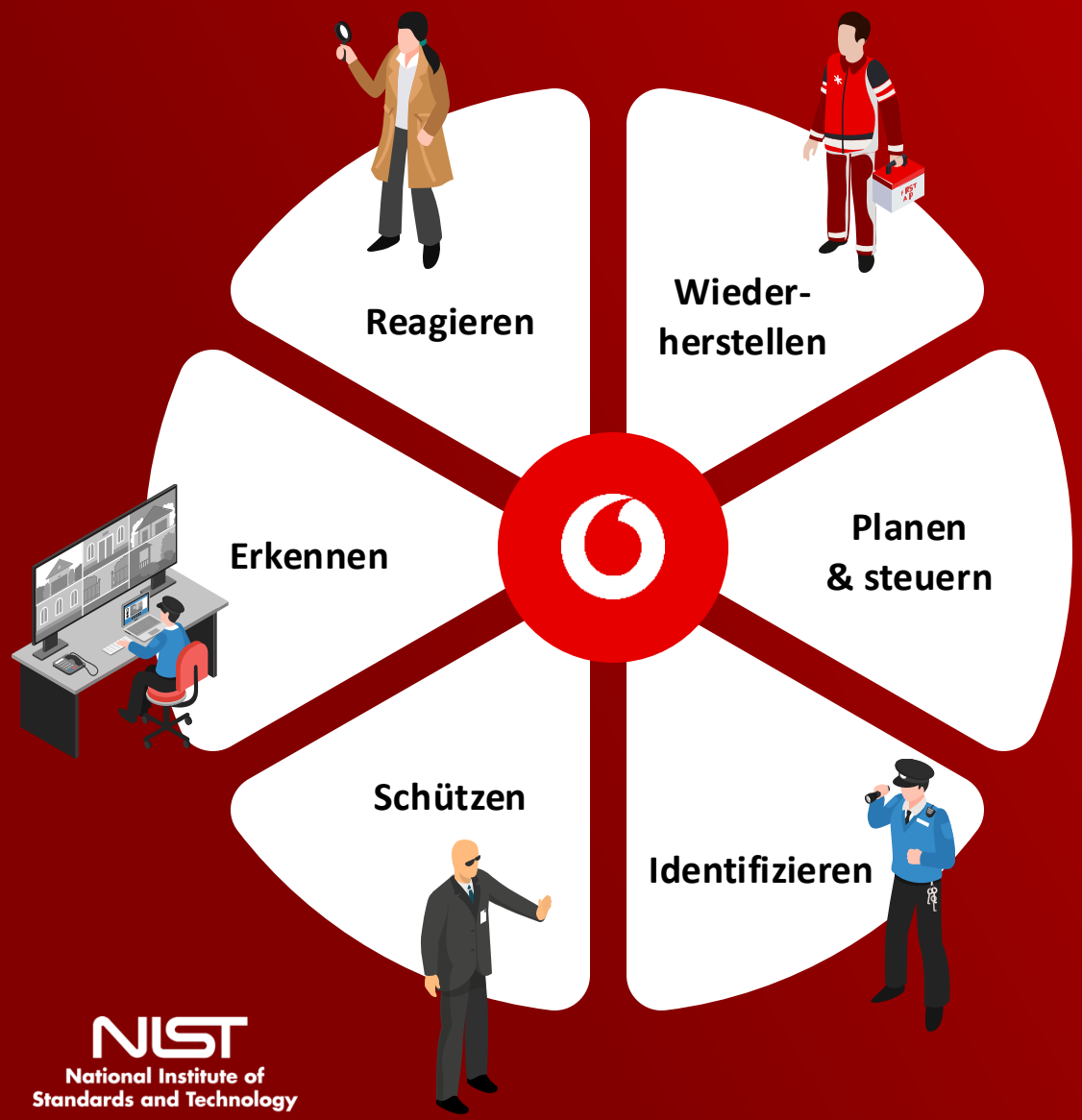
Der digitale Notfallplan gegen Cyber Angriffe

NIST
National Institute of
Standards and Technology

Security ganzheitlich betrachten ist der Schlüssel zum Erfolg!

NIST
National Institute of
Standards and Technology

Vodafone als Ihr Security-Partner – neutral & unabhängig



NIST
National Institute of
Standards and Technology

Wir planen und steuern mit Ihnen Ihre Sicherheitsorganisation.

- Strategieberatung
- IT Sicherheitskonzept
- NIS2 GAP-Analyse und –Beratung
- Aufbau eines ISMS
- Zertifizierungsunterstützung

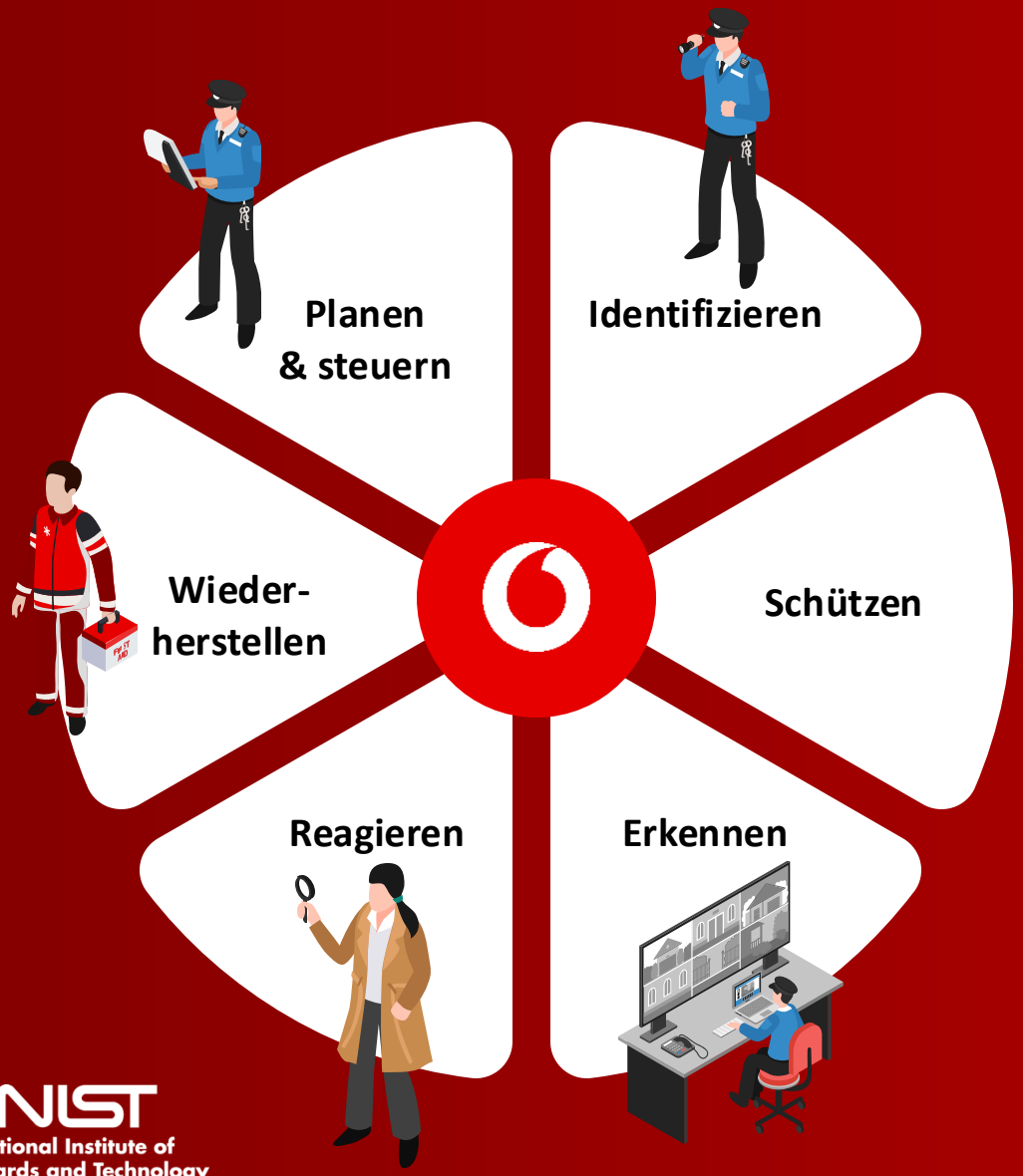
Vodafone als Ihr Security-Partner – neutral & unabhängig

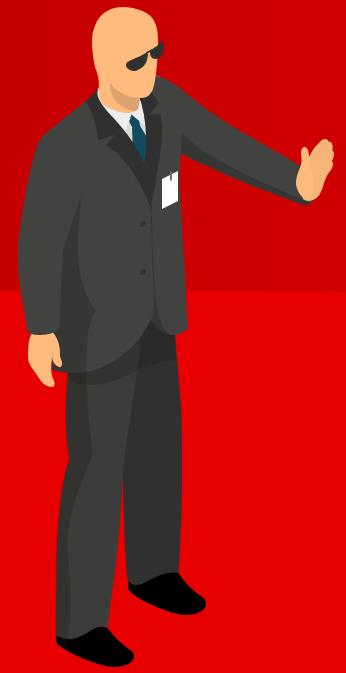
Wir identifizieren Ihre Bedrohungen bevor es Angreifer tun.

- Risikoanalyse und -bewertung
- Identifikation von Schwachstellen
- Phishing-Kampagnen

NIST
National Institute of
Standards and Technology

Vodafone als Ihr Security-Partner – neutral & unabhängig





Wir verhelfen zu besserem Schutz und machen es Angreifern schwer.

- Systemhärtung
- Netzwerksicherheit
- DDoS Mitigation im Backbone
- Endpoint Security
- Zero Trust Lösungen
- Cloud Security
- Security Awareness

NIST
National Institute of
Standards and Technology

Vodafone als Ihr Security-Partner – neutral & unabhängig

NIST
National Institute of Standards and Technology

Wir überwachen 24/7 Ihre gesamte IT, erkennen Angriffe und warnen Sie bevor Schaden ensteht.

- Anomalie Erkennung und Log-Monitoring
  - SIEM, NDR, MxDR, EDR, XDR (Managed oder unmanaged)

Vodafone als Ihr Security-Partner – neutral & unabhängig

Im Ernstfall reagieren wir für Sie, wehren Angriffe ab und übernehmen die Forensik.

- Bewertung und Eindämmung des Angriffs
- Notfallmanagement
- IT-Forensik

NIST
National Institute of Standards and Technology

Vodafone als Ihr Security-Partner – neutral & unabhängig

Ihre Daten sind vorhanden,
wenn Sie sie brauchen.
Mit uns geht nichts verloren.

- Backup-Lösungen
- Disaster Recovery

NIST
National Institute of
Standards and Technology

IHRE FRAGEN.

Vielen Dank für Ihre Teilnahme!

Bei Fragen
melden Sie sich gern
bei Ihrem:r Vodafone-
Ansprechpartner:in.

Sie sind neu bei uns?
Schreiben Sie uns an
online.sessions@vodafone.com
eine E-Mail.

Die Aufzeichnungen und
Unterlagen aller Sessions
finden Sie hier.

TIMETABLE 2024

Educational Month Cyber Security

VODAFONE BUSINESS EDUCATION

KW 38

19.09. | 10:00 IT-Sicherheit ist Chefsache: Schützen Sie Ihre Unternehmenswerte und minimieren Sie die (persönliche) Haftung
Dr. Hauke Hansen (FPS Law)

20.09. | 10:00 KI-gesteuerte Security: Ende-zu-Ende-Sicherheit mit Microsoft
Andreas Wach (Microsoft)
Thomas Schmidt (PCG)

KW 39

24.09. | 10:00 Human Firewall – aus Sicht eines White-Hat-Hackers
Immanuel Bär (Prosec Networks)

25.09. | 10:00 Live Hacking: Die Methoden der Hacker und wie Sie sich gegen Ransomware Attacken schützen können
Lukas Garlik (Accenture)
Emil Stahr (Accenture)

26.09. | 10:00 Cyber Security im Zeitalter der KI: Strategien und Best Practices
Fabian Flanhardt (PCG)
Thomas Schmidt (PCG)

KW 40

30.09. | 10:00 Kampf der Ransomware! Wie Sie sich mit Zero Trust richtig schützen
Thanh Trieu (Zscaler)

Together we can

vodafone business