TD SYNNEX

Enclosed I am sending you IC for SonicWall.

Making IT Personal™

TD SYNNEX

Taking Cyber-Security Personal

MAXImale Sicherheit bei MINImalem Aufwand

TD SYNNEX Managed SOC
powered by Chorus

Jetzt schon mal vielen Dank, dass ihr euch die Zeit genommen habt, um euch mit uns zu diesen wichtigen Themen auszutauschen 👍

Andreas Wolffs | Senior BDM Microsoft Cloud & Security

TD SYNNEX Germany GmbH & Co. OHG

Agenda

Was kommt auf uns zu?

Was hat Microsoft im Portfolio?

Wie kann TD SYNNEX unterstützen?

Fragen

Agenda
Was kommt auf uns zu?

Die wichtigsten 5 EU-Sicherheitsgesetze im Überblick

1 NIS2

Einheitliches Cybersicherheitsniveau in der EU.

Branche: Alle Unternehmen mit kritischen digitalen Diensten und Infrastrukturen.

2 CER Directive

Schutz kritischer Infrastrukturen

Branche: Energie, Transport, Gesundheitswesen, Wasser, Digitalinfrastruktur

3 KRITIS-Dachgesetz

Nationale Umsetzung der CER Directive

Branche: Energie, Transport, Gesundheitswesen, Wasser, Digitalinfrastruktur.

4 DORA

Cybersicherheit für den Finanzsektor

Branche: Banken, Versicherungen, Finanzdienstleister

5 US CLOUD Act

Weltweiter Datenzugriff für US-Behörden

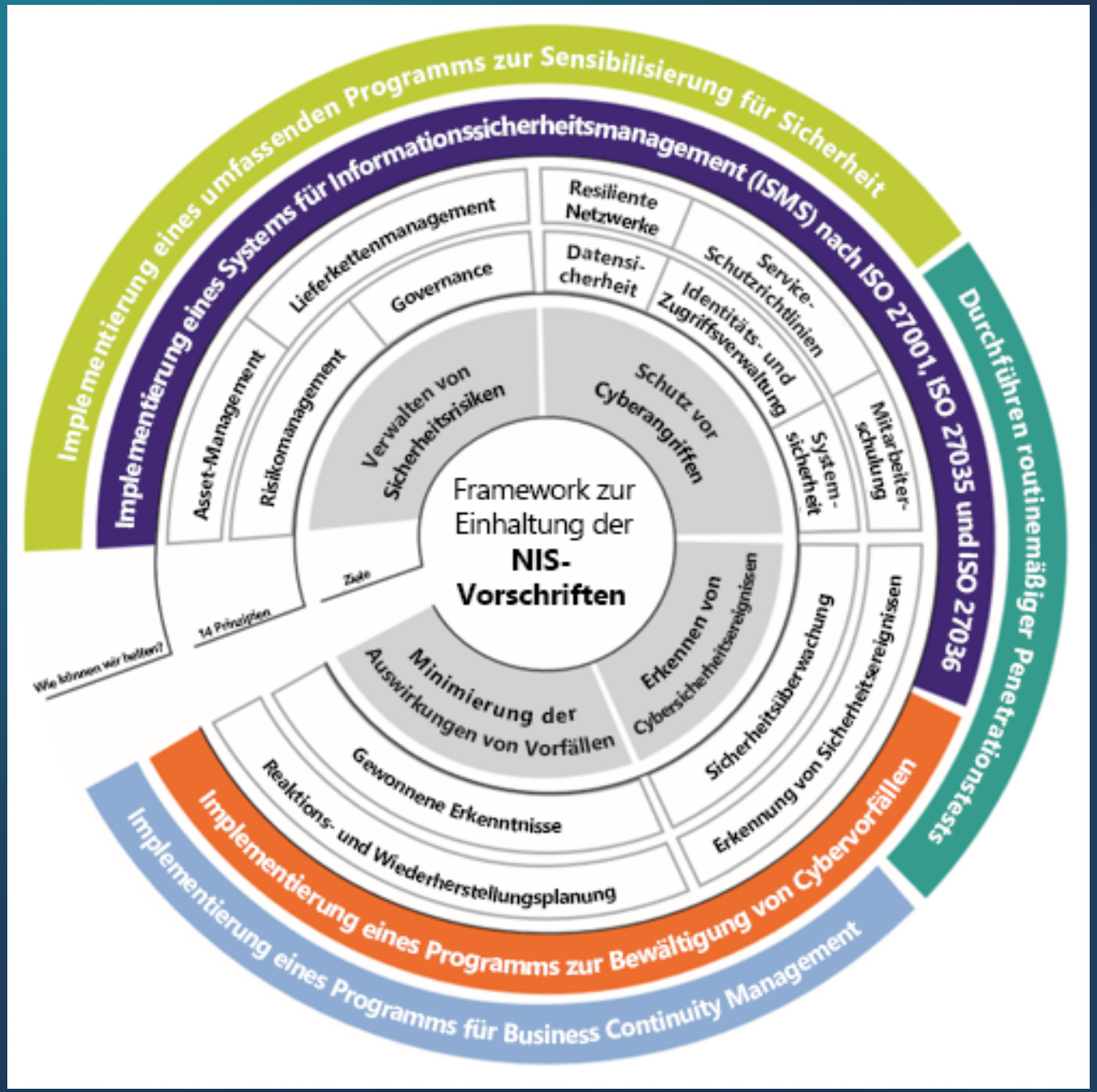
Branche: Alle Unternehmen, die Daten in der Cloud speichern, insbesondere solche mit US-Partnern

Warum wird NIS1 zu NIS2 erweitert?

Cyberangriffe werden immer häufiger und komplexer

Druck, sich mit der Multicloud-IT-Umgebung auseinanderzusetzen

Zunehmend komplexes regulatorisches Umfeld



NIS2-Ziel

Maßnahmen für ein hohes gemeinsames Niveau der Cybersicherheit für den öffentlichen und privaten Sektor in allen EU-Mitgliedstaaten

https://www.itgovernance.co.uk/nis-regulations-cyber-assessment-framework

Risiken für Geschäftsführer

Für Geschäftsführer und Führungskräfte ergeben sich aus der NIS2-Richtlinie mehrere Risiken und Verantwortlichkeiten:

- **Rechtliche Verantwortung**: Geschäftsführer können persönlich haftbar gemacht werden, wenn ihr Unternehmen die Anforderungen der NIS2-Richtlinie nicht erfüllt.
- **Strafmaßnahmen**: Bei Nichteinhaltung drohen strenge Sanktionen und Bußgelder, die harmonisiert und in der gesamten EU durchgesetzt werden.
- **Reputationsschäden**: Sicherheitsvorfälle können das Vertrauen der Kunden und Partner beeinträchtigen und zu erheblichen Reputationsschäden führen.
- **Geschäftskontinuität**: Unzureichende Sicherheitsmaßnahmen können zu Betriebsunterbrechungen und finanziellen Verlusten führen.

Es ist daher entscheidend, dass Unternehmen und ihre Führungskräfte proaktive Maßnahmen ergreifen, um die Anforderungen der NIS2-Richtlinie zu erfüllen und ihre Cybersicherheitsstrategien zu stärken.

Microsoft Threat Monitor :: Security Insiders

Threat actor insights

Microsoft Threat Intelligence is actively tracking threat actors across observed nation state, ransomware, and criminal activities. These insights represent publicly published activity from Microsoft threat researchers and provide a centralized catalog of actor profiles from the referenced blogs.

Manatee Tempest

Manatee Tempest (formerly DEV-0243) is a threat actor that is a part of the ransomware as a service (RaaS) economy, partnering with other threat actors to provide custom Cobalt Strike loaders.

Forest Blizzard

Forest Blizzard (formerly STRONTIUM) uses a variety of initial access techniques including exploiting vulnerable to web facing applications and, to obtain credentials, spear phishing and the deployment of an automated password spray/brute force tool operating through TOR

Midnight Blizzard

The actor that Microsoft tracks as Midnight Blizzard (NOBELIUM) is a Russia-based threat actor attributed by the US and UK governments as the Foreign Intelligence Service of the Russian Federation, also known as the SVR.

Pistachio Tempest

Pistachio Tempest (formerly DEV-0237) is a group associated with impactful ransomware distribution. Microsoft has observed Pistachio Tempest use varied ransomware payloads over time as the group experiments with new ransomware as a service (RaaS) offerings, from Ryuk and Conti to Hive, Nokoyawa, and, most recently, Agenda and Mindware.

Diamond Sleet

The actor Microsoft tracks as Diamond Sleet is a North Korea-based activity group known to target media, defense, and information technology (IT) industries globally. Diamond Sleet focuses on espionage, theft of personal and corporate data, financial gain, and corporate network destruction.

Wine tempest

Wine Tempest (formerly PARINACOTA) typically uses human-operated ransomware for attacks, mostly deploying the Wadhrama ransomware. They are resourceful, changing tactics to match their needs and have used compromised machines for various purposes, including cryptocurrency mining, sending spam emails, or proxying for other attacks.

Hazel Sandstorm

Hazel Sandstorm (formerly EUROPIUM) has been publicly linked to Iran's Ministry of Intelligence and Security (MOIS). Microsoft assessed with high confidence that on July 15, 2022, actors sponsored by the Iranian government conducted a destructive cyberattack against the Albanian government, disrupting government websites and public services.

Crimson Sandstorm

Crimson Sandstorm (formerly CURIUM) actors have been observed leveraging a network of fictitious social media accounts to build trust with targets and deliver malware to ultimately exfiltrate data.

Cadet Blizzard

Microsoft tracks Cadet Blizzard (formerly DEV-0586) as a Russian GRU-sponsored threat group that Microsoft began tracking following disruptive and destructive events occurring at multiple government agencies in Ukraine in mid-January 2022.

Nylon Typhoon

Nylon Typhoon (formerly NICKEL) uses exploits against unpatched systems to compromise remote access services and appliances. Upon successful intrusion, they have used credential dumpers or stealers to obtain legitimate credentials, which they then used to gain access to victim accounts and to gain access to higher value systems.

Gray Sandstorm

Gray Sandstorm (formerly DEV-0343) conducts extensive password spraying emulating a Firefox browser and using IPs hosted on a Tor proxy network. They typically target dozens to hundreds of accounts within an organization, depending on the size, and enumerate each account from dozens to thousands of times.

Volt Typhoon

The actor that Microsoft tracks as Volt Typhoon is a nation-state activity group based out of China. Volt Typhoon focuses on espionage, data theft, and credential access.

Caramel Tsunami

Caramel Tsunami (formerly SOURGUM) generally sells cyberweapons, usually malware and zero-day exploits, as a part of a hacking-as-a-service package sold to government agencies and other malicious actors.

Digital Defense Report 2024

Microsoft Security Response Center

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%

Threat actors from Russia, China, Iran, and North Korea pursued access to IT products and services, in part to conduct supply chain attacks against government and other sensitive organizations.

Source: Microsoft Threat Intelligence, nation-state notification data

Microsoft customers face more than 600 million cybercriminal and nation-state attacks every day, ranging from ransomware to phishing to identity attacks. Once again, nation-state affiliated threat actors demonstrated that cyber operations—whether for espionage, destruction, or influence—play a persistent supporting role in broader geopolitical conflicts. Also fueling the escalation in cyberattacks, we are seeing increasing evidence of the collusion of cybercrime gangs with nation-state groups sharing tools and techniques.

Hierarchy of cybersecurity needs

Drawing inspiration from Maslow's hierarchy of needs, this graphic illustrates a prioritization of cybersecurity, starting with the most basic need: protecting identities. AI has a role at each tier, underscoring its potential to enhance security measures. Cultivating a robust security culture within the organization, helps ensure the technological defenses and human practices evolve in concert to mitigate threats effectively.

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.

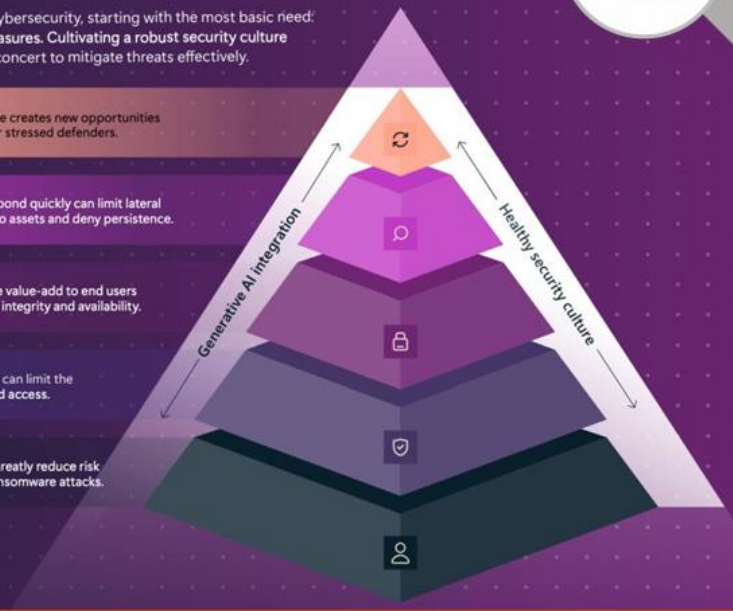
IMPACT...
Modern workloads deliver the value-add to end users who increasingly rely on their integrity and availability.

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.



News **Analyst reports** · **Oct 15** · **5 min read**

Escalating cyber threats demand stronger global defense and cooperation ›

We must find a way to stem the tide of this malicious cyber activity. That includes continuing to harden our digital domains to protect our networks, data, and people at all levels. However, this challenge will not be accomplished solely by executing a checklist of cyber hygiene measures but only through a focus on and commitment to the foundations of cyber defense from the individual user to the corporate executive and to government leaders.

775 million
email messages contained malware (July 2023-June 2024)
Source: Microsoft Defender for Office 365

80%
of organizations have attack paths that expose critical assets

3x
threefold decrease in ransom attacks reaching encryption stage over the past two years

7,000
password attacks blocked per second over the past year

Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

<1% of attacks

Less than 1% combined

MFA attacks
SIM swapping
MFA fatigue
AiTM
End-run multifactor authentication (MFA) protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.

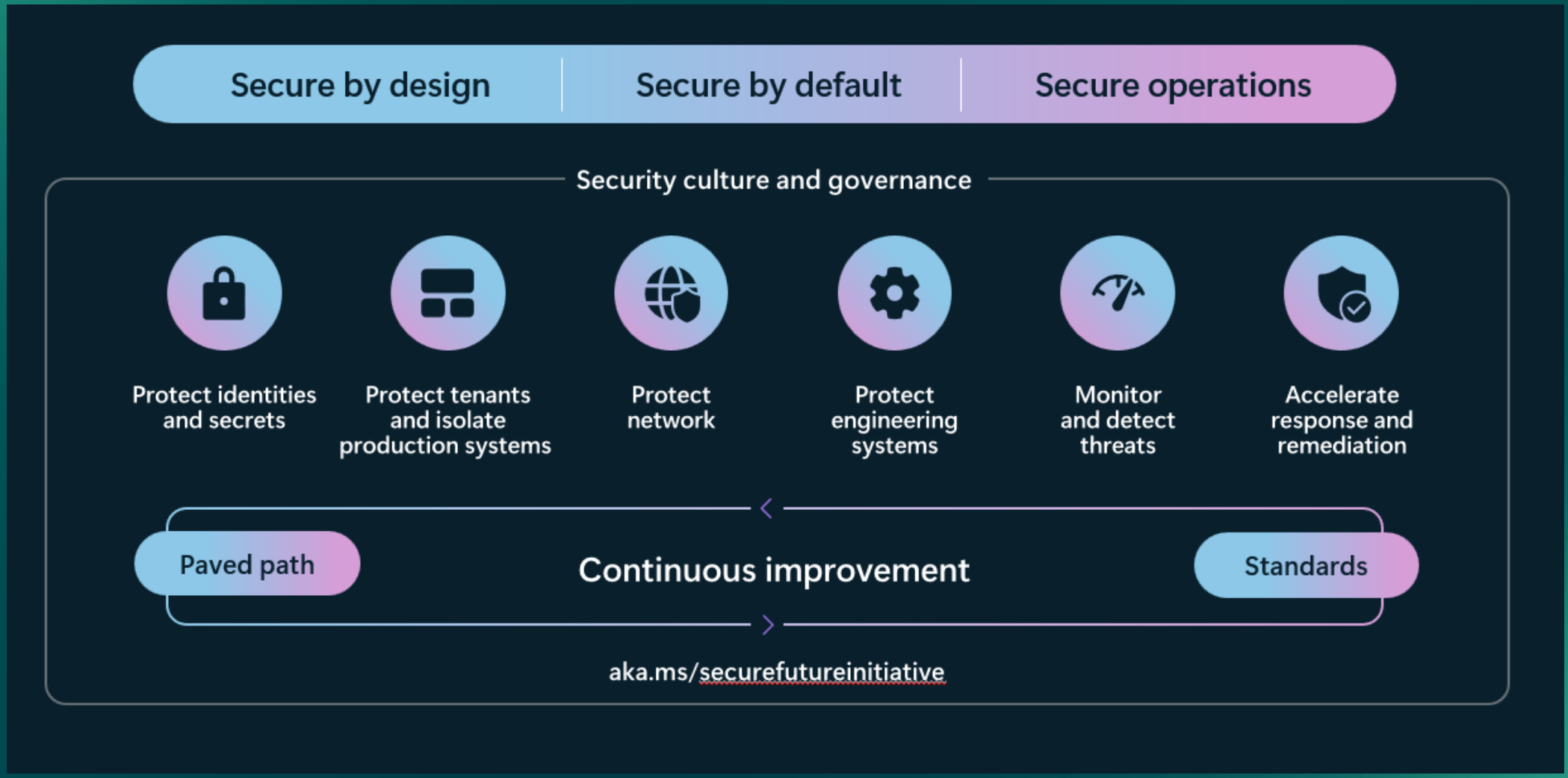
Post-authentication attacks
Token theft
Consent phishing
Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.

Infrastructure compromise
Often silently executed by professional groups or nation-state-backed threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.

Agenda
Was hat Microsoft im Portfolio?

TD SYNNEX | Microsoft

Unsere Zukunft sichern
Secure Future Initiative von Microsoft



Microsoft‘s digitale Zusicherungen für Europa

Microsoft kündigt europäische digitale Verpflichtungen an: „Wir respektieren europäische Werte, halten uns an europäische Gesetze und verteidigen aktiv die Cybersicherheit Europas. Unsere Unterstützung für Europa war immer unerschütterlich – und wird es auch immer sein.“

Sie beinhalten das Versprechen, die digitale Widerstandsfähigkeit Europas unabhängig von geopolitischen und handelspolitischen Volatilitäten aufrechtzuerhalten. „Wir haben uns gefreut, dass sich die Trump-Regierung und die Europäische Union kürzlich darauf geeinigt haben, weitere Zolleskalationen auszusetzen, während sie versuchen, ein gegenseitiges Handelsabkommen auszuhandeln.“

Microsoft's European Digital Commitments

1. We will help build a broad AI and cloud ecosystem across Europe.
2. We will uphold Europe's digital resilience even when there is geopolitical volatility.
3. We will continue to protect the privacy of European data.
4. We will always help protect and defend Europe's cybersecurity.
5. We will help strengthen Europe's economic competitiveness, including for open source.

Erfüllung von NIS-Zielen und -Prinzipien durch Microsoft-Technologien

NIS-Grundsätze	Microsoft-Lösung	Kommentare
Governance	Defender CSPM, Entra	
Risikomanagement	Defender XDR und Purview Compl. Mgr. & Insider Risk	
Asset-Management	Defender CSPM, Defender für Endpunkt	
Lieferkette	Defender XDR, Entra und DevOps	
Serviceschutz	Defender für API	
Identität und Zugriff	Entra ID	
Datensicherheit	Purview	
Systemsicherheit	Defender für Endpunkt, Defender für IoT und Intune	
Resiliente Netzwerke	Azure-Netzwerksicherheit	Integration von Drittanbietern mit den wichtigsten NDR-Anbietern
Sensibilisierung der Mitarbeitenden	O365-Phishingsimulation und Lernpfade	
Sicherheitsüberwachung	Microsoft Sentinel	
Proaktive Sicherheit	Defender XDR	
Reaktion und Wiederherstellung	Defender XDR, M365 - & Azure-Backup und Wiederherstellung	Integration von Drittanbietern mit den wichtigsten DR-Anbietern
Gewonnene Erkenntnisse	Nicht zutreffend	

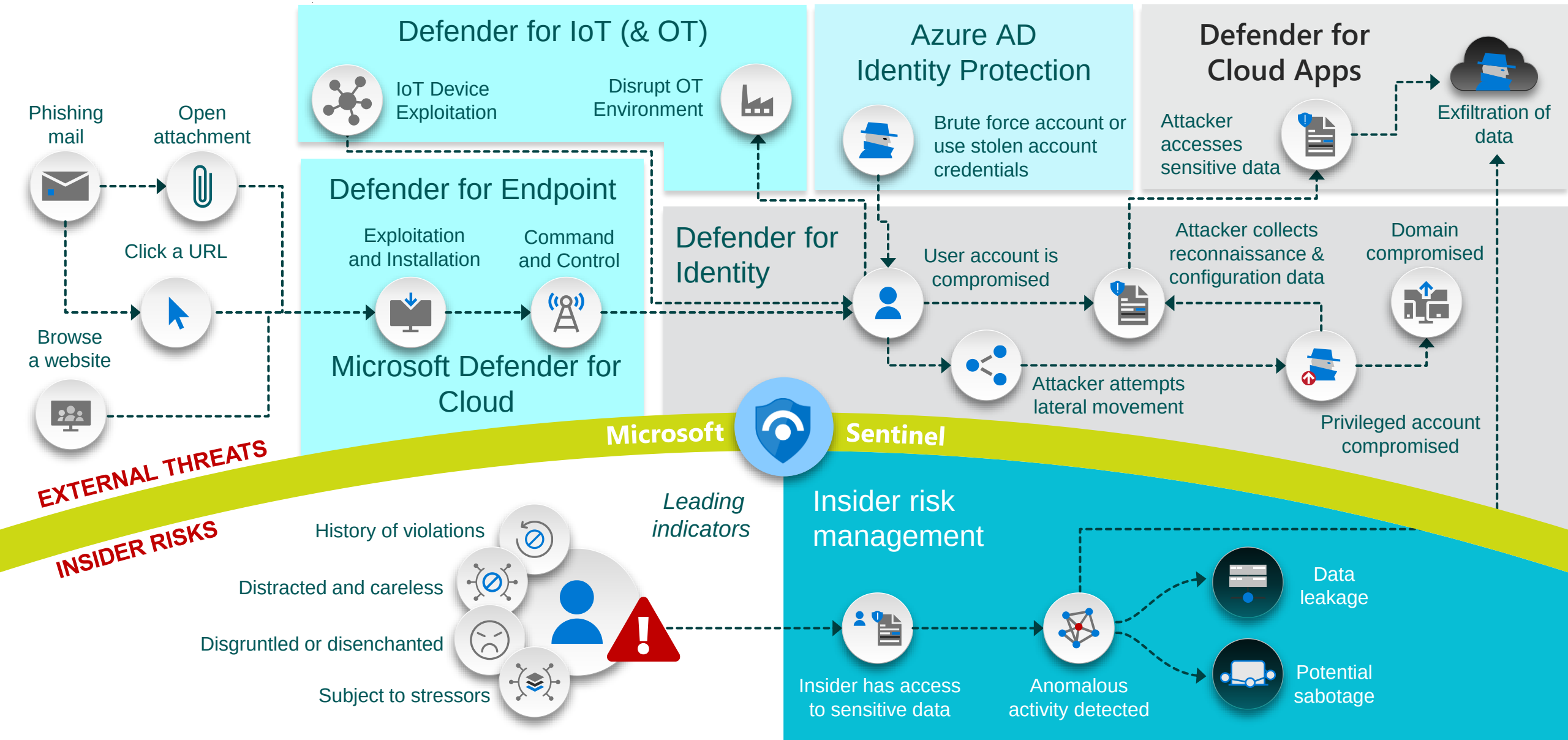
https://www.itgovernance.co.uk/nis-regulations-cyber-assessment-framework

Microsoft Sentinel
Microsoft Intune
Microsoft Defender for Cloud (incl. Defender for API)
Microsoft 365 Defender
Microsoft Defender for Office 365
Microsoft Defender for Identity
Microsoft Defender for Endpoint
Microsoft Defender for Cloud Apps
Microsoft Defender Threat Intelligence
Microsoft Defender External Attack Surface Management (EASM)
Microsoft Defender for Business
Microsoft Defender for Endpoint on iOS
Microsoft Defender for Endpoint on Android
Microsoft Defender for Endpoint on MacOS
Microsoft Defender for Endpoint on Linux
...

Verteidigung über Angriffsketten hinweg

Bedrohungen kommen heute von innen und außen

TD SYNNEX | Services



Agenda
Wie kann TD SYNNEX unterstützen?

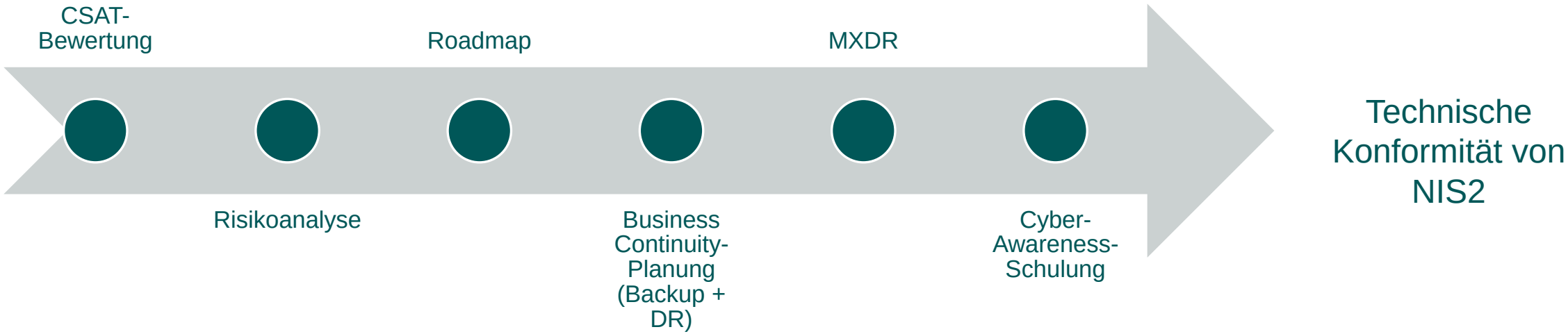
Ziele von NIS2

Verwalten von Sicherheitsrisiken	Schutz vor Cyberangriffen	Erkennung von Cybersicherheitsvorfällen	Minimierung der Auswirkungen von Cybersicherheitsvorfällen

NIS2-Prinzipien

A1: Governance	**A2:** Risikomanagement	**B1:** Richtlinien und Prozesse zum Schutz von Diensten	**B2:** Identitäts- und Zugriffs-kontrolle	**C1:** Sicherheits-überwachung	**C2**: Proaktive Erkennung von Sicherheits-ereignissen	**D1:** Reaktions- & Wiederherstellungs planung	**D2:** Gewonnene Erkenntnisse
A2: Vermögens-verwaltung	**A4:** Lieferkette	**B3:** Daten-sicherheit	**B4:** System-sicherheit				
		B5: Resiliente Netze und Systeme	**B6:** Sensibilisierung und Schulung des Personals				

Der Weg von TD SYNNEX zu NIS2



TD SYNNEX

Verwalten von Sicherheitsrisike

Minimierung der Auswirkungen von Cybersicherheitsvorfällen

A1: Governance

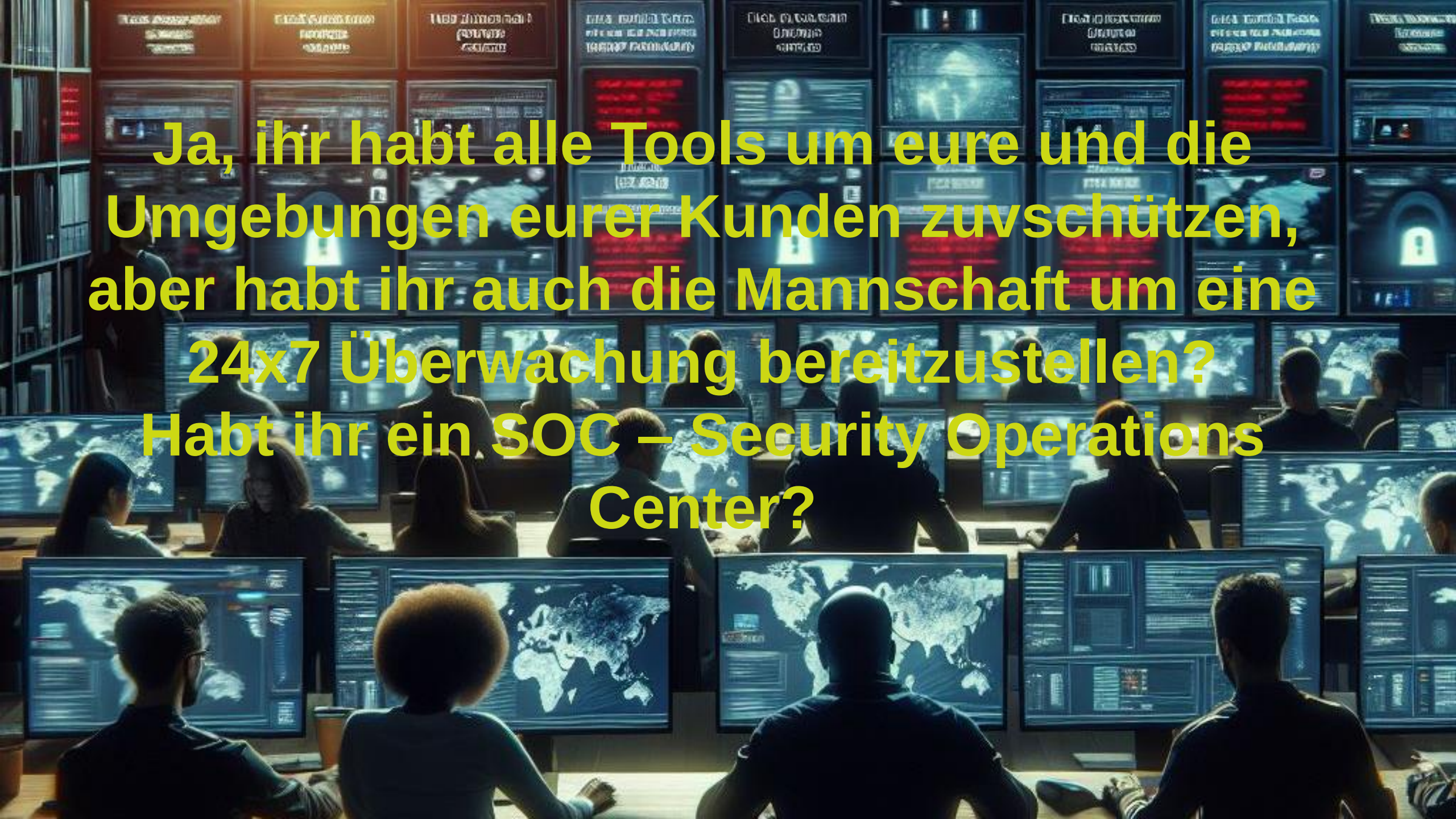
A Ris manag

A2: Vermögens-verwaltung

A Liefe

D1: eaktions- und Wieder-herstellungs-planung

D2: Gewonne Erkenntnisse


Ja, ihr habt alle Tools um eure und die Umgebungen eurer Kunden zuvschützen, aber habt ihr auch die Mannschaft um eine 24x7 Überwachung bereitzustellen? Habt ihr ein SOC – Security Operations Center?

Was versteht man unter einem SOC?

TD SYNNEX | Services

Tools

Asset discovery
SIEM
XDR
SOAR
Vulnerability Assessment
Behavioural monitoring
GRC

In-house Average cost: E500k / y

1

People

Security analysts
Security engineer
Security Manager
CISO
IR Team
Director IR
Director Threat Intel

In-house Average cost: 24/7 engineers + team E1M / y

2

Process

Classify and Triage events
Prioritize and Analyze
Remediation and advisory steps
Assessments and review
Compliance

In-house Average time to be fully up and running: 3 years

3

Unsere SOC-Services im Vergleich

SERVICE-VERGLEICH		MDR	MXDR
24x7x365 CSOC		✓	✓
Analysten 24x7 telefonisch erreichbar		✓	✓
30 Minuten SLA mit hohem Schweregrad		✓	✓
Eindämmungs- und Reaktionsmaßnahmen		✓	✓
Chorus-proprietäre Analyseregeln		✓	✓
Abdeckung der Microsoft Security Suite	Defender für Endpunkt	✓	✓
	Defender für Identität		✓
	Defender für Cloud Apps		✓
	Defender für Office		✓
	Defender für Cloud		✓
	Azure-Dienste		✓
Benutzerdefinierte Microsoft Sentinel-Integration			✓
Benutzerdefinierte Sicherheits-Playbooks			✓
MITRE ATT&CK-Framework-Mapping			✓
Überwachung der externen Angriffsfläche			✓

SERVICE-VERGLEICH		MDR	MXDR
Abdeckung Threat Detection & Response	Endpunkte	✓	✓
	Entra ID-Identitäten	✓	✓
	Server	✓	✓
	Active Directory-Identitäten		✓
	Nicht-Azure-Clouddienste		✓
	Netzwerkprotokollquellen (Firewalls/Switching/APs)		✓
	APIs/Protokolle von Drittanbietern		✓
Wöchentliche Berichte über den Sicherheitsdienst		✓	✓
Cyber Essentials ausgerichteter TVM*-Bericht		✓	✓
Bedrohungsjagd auf Endpunkten		✓	✓
Cyber-Bedrohungsinformationen		✓	✓
Standardmäßige Sicherheits-Playbooks		✓	✓
Sicherheitsempfehlungen und -Anleitungen		✓	✓
Dienst-Governance		✓	✓
Erweiterte Bedrohungssuche			✓

*Threat- & Vulnerability Management

Was ist in unserem Managed SOC Service inbegriffen?

24x7x365 Cyber Security Operation Center

Flexible Abdeckung

MDR - Endpunkte
MXDR – Cloud oder Hybrid

24x7 Monitoring

Proaktive Cyber Threat Intelligence (CTI)

Erkennung von Bedrohungen

Benutzerdefinierte Regeln zur Erkennung von Bedrohungen

Schnelle Reaktion auf Bedrohungen

Benutzerdefinierte Sicherheits-Playbooks

Triage und Untersuchung von Bedrohungen

Proaktives Threat Hunting & Schwachstellen-management

Service Governance und Berichterstattung

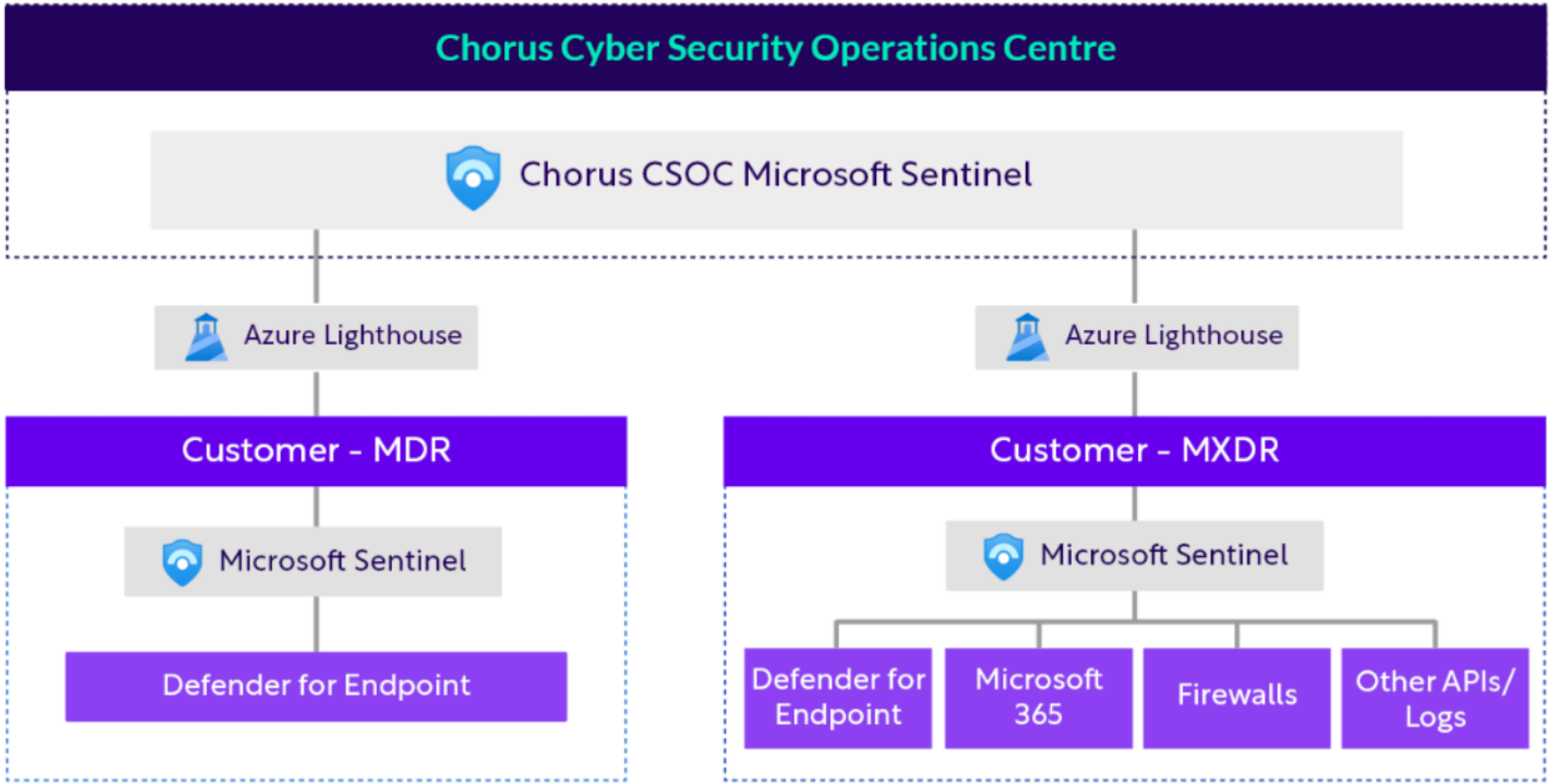
Sicherheitsüberprüfungen und -empfehlungen

Optimierter Serviceübergang (Onboarding)

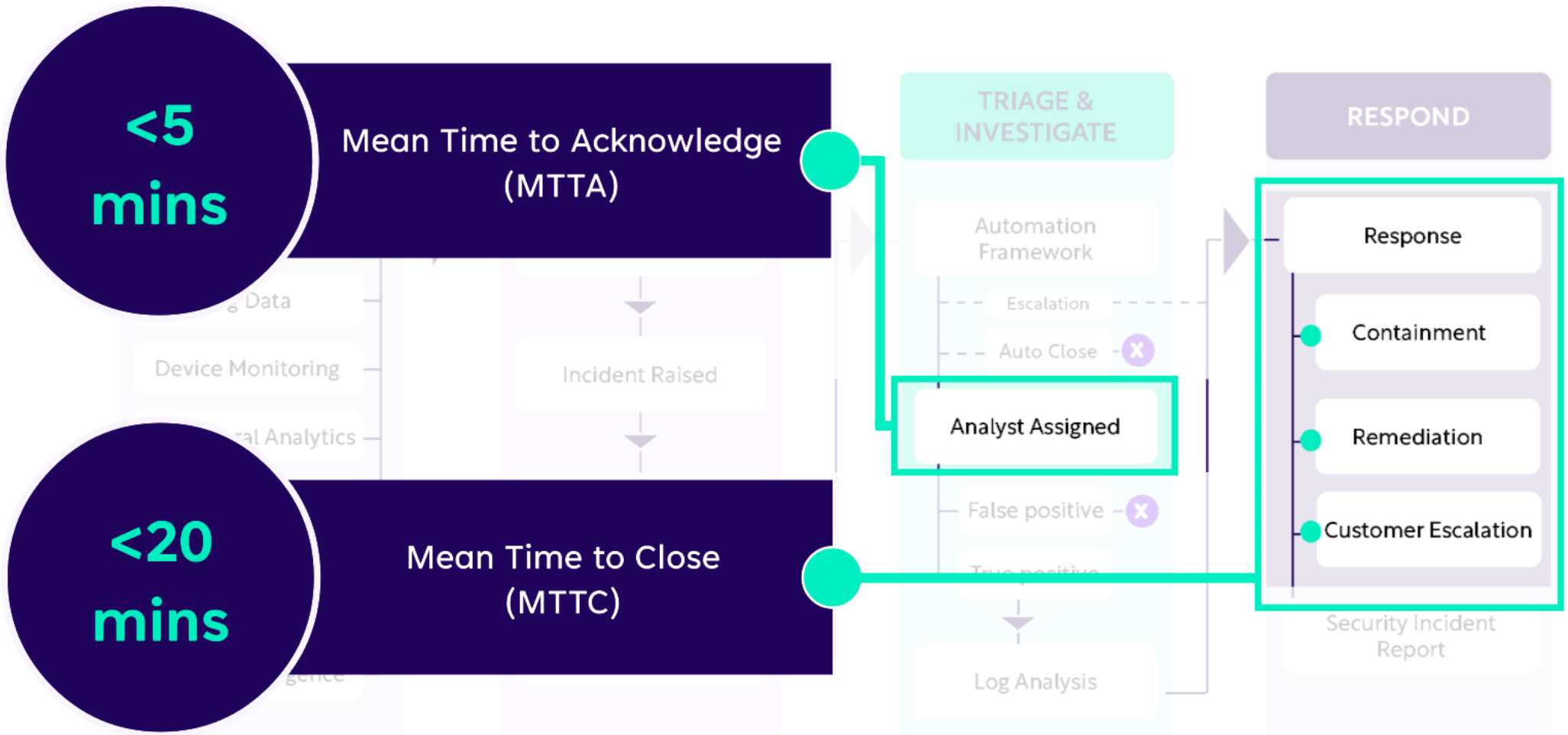
Phishing-Simulation

Chorus MDR & MXDR Architecture

Built on Microsoft Sentinel & Microsoft Defender for Endpoint



Security incident journey



Zusammenfassung - Managed SOC as a Service

Funktionen

Member of Microsoft Intelligent Security Association

Microsoft

- **Microsoft Defender Stack**
- **Microsoft Sentinel**
- **24/7 SOC**
- Hocheffizientes Onboarding
- Recurring Security checks
- **Bedrohungserkennung und -behebung**
- Threat hunting & ASM
- Benutzerdefinierte Playbooks & Erkennungsregeln
- MS Sentinel Custom Ingestion
- **MTTD 6 minutes MTTR 10 minutes**
- Kostenlose 3rd-Party-Integrationen
- Cloud, hybrid, on-premise
- MS Partner & MISA member

Überblick

End-to-End-MXDR-Service mit Fokus auf kontinuierliche Verbesserung durch kontinuierliche Governance.

Innovativer 24/7/365-Schutz vor Cyber-Bedrohungen mit den Sicherheits- und Cloud-Lösungen von Microsoft.

Profitieren Sie von Microsoft-Technologie in einer neuen Ära der Cyberbedrohungen.

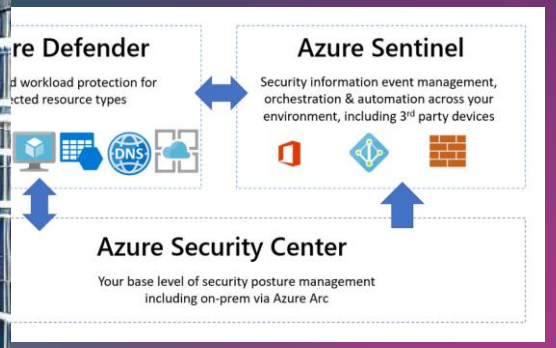
Vorteile

- **Einfache Lizenzstruktur mit 2 Paketen**
- **Preise pro Benutzer und Monat mit einmaliger Onboarding-Gebühr**
- **Geeignet für KMU & Großunternehmen (ab 20 User)**
- **Hohe Kundenzufriedenheit**
- **Früherkennung von Bedrohungen**
- **Schnelle Reaktion und Abwehr**
- **Schutz sensibler Daten**
- **Einhaltung von Vorschriften**
- **Risikomanagement und Business Continuity**

WI4M -

Erhöhung des MWP ARPU / ARPC durch Umstellung des Kunden von O365 oder M365 Business Standard auf Business Premium, E3 oder E5.

Treuere Kunden. Je mehr Dienstleistungen wir und unsere Partner anbieten, desto schwieriger ist es für den Kunden, sich für den gleichen Value Stack zu bewegen.



∑ Fazit :

TD SYNNEX

Mit unserem Managed SOC-Service bekommt ihr :

- Umfassenden Schutz der Umgebung mit der
- Best-in-Class Technologie
- Ihr seid auf NIS2 und KRITIS bestens vorbereitet
- Ihr bleib der Entwicklung von Cyberbedrohungen einen Schritt voraus!

Call to action!

Wer bis Ende August sich oder einen Kunden onboarded, dem erlassen wir die Onboardingkosten


?


? ?


Doo you have any questions?
Microsoft


?
Cloud Solution Archicst


QUESTIONS?


Microoft

Vielen Dank für eure Aufmerksamkeit!

Andreas
Wolffs

Senior Business Development Manager

Andreas.Wolffs@tdsynnex.com

+49 175 2608810

TD SYNNEX

Kistlerhofstraße 75
Munich, Bavaria 81379
Germany

www.tdsynnex.com

NIS betrifft verschiedene Sektoren, darunter...

Wesentliche Einrichtungen

Großunternehmen gehören zu den in Anhang I der Richtlinie aufgeführten Sektoren mit hoher Kritikalität.

Ein Großunternehmen ist definiert als ein Unternehmen mit mindestens 250 Beschäftigten.

oder

mit einem Jahresumsatz von mindestens 50 Millionen Euro und/oder einer Jahresbilanzsumme von mindestens 43 Millionen Euro.

Wichtige Einrichtungen

Mittelgroße Unternehmen, die in den besonders kritischen Sektoren des Anhangs I der Richtlinie tätig sind, Große oder mittlere Unternehmen in den Sektoren des Anhangs II der Richtlinie, die nicht in die Kategorie der wesentlichen Einrichtungen fallen (aufgrund ihrer Größe oder der Art der Einrichtung).

Ein mittleres Unternehmen ist definiert als ein Unternehmen mit mindestens 50 Beschäftigten
oder
einem Jahresumsatz (oder einer Bilanzsumme) von mindestens 10 Millionen Euro, aber mit weniger als 250 Beschäftigten
und
einem Jahresumsatz von höchstens 50 Millionen Euro oder einer Bilanzsumme von 43 Millionen Euro.

Was bedeutet die NIS2 für Sie?

Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit

Risikomanagement	Sicherheitsrichtlinien	Umgang mit Vorfällen (Prävention, Erkennung und Reaktion auf Vorfälle)	Geschäftskontinuität und Krisenmanagement
Sicherheit in der Lieferkette unter Berücksichtigung von Schwachstellen bei Lieferanten	Umgang mit Schwachstellen und Offenlegungen	Regelmäßige Bewertungen, um die Wirksamkeit von Maßnahmen zum Cybersecurity-Risikomanagement zu ermitteln (z. B. Spiegelung des Stands der Technik – Sicherheitslage)	
Einsatz von Kryptografie und Verschlüsselung, wo dies gerechtfertigt ist	Grundlegende Cybersicherheitshygiene und -schulung	Verwendung von MFA oder kontinuierlicher Authentifizierung	

Meldepflichten für Vorfälle

Melden von Vorfällen mit erheblichen* Auswirkungen auf die Bereitstellungsdienste

Innerhalb von 24 Stunden	Innerhalb von 72 Stunden ein ausführlicher Bericht	Innerhalb von 1 Monat ein Abschlussbericht Zwischenbericht

**=Ein Sicherheitsvorfall gilt als erheblich, wenn er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann, oder wenn er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.*

Computer Security Incident Response Team (CSIRT)	Zuständige Behörde	Empfänger von Dienstleistungen

NIS betrifft verschiedene Sektoren, darunter…

Am 14. September hat die Europäische Kommission neue Leitfäden veröffentlicht, in denen erläutert wird, welche Sektoren als kritisch gelten und was sie den nationalen Behörden in der EU im Rahmen der NIS2-Richtlinie melden müssen.

Hochkritische Sektoren

- Energie
- Verkehr
- Bankwesen
- Räumlichkeiten
- Finanzmarktin-frastruktur
- Gesundheits-wesen
- Trinkwasser
- Öffentliche Verwaltung
- Abwasser
- Digitale Infrastruktur
- IT-Servicever-waltung

Kritische Sektoren

- Lebensmittel
- Abfallwirtschaft
- Chemikalien
- Post und Kurierdienste
- Fertigung von Medizinprodukten
- Digitale Anbieter
- Forschung-seinrichtungen

Unternehmensleitung kann zur Rechenschaft gezogen werden

NIS2-Ziele

Verwalten des Sicherheitsrisikos	Schutz gegen Cyberangriffe	Erkennen von Cybersicherheitsvorfällen	Minimierung der Auswirkung von Cybersicherheitsvorfällen
Sicherstellen, dass Cybersicherheits-risikobewertungen durchgeführt werden	Technische und organisatorische Maßnahmen umsetzen	Durch Schulungs- und Risikomanagementpro-gramme den Überblick über die Cybersicherheit behalten	Risiken angemessen verwalten

Versäumnisse können diese Folgen haben:

Geldbuße in Höhe von >10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes für wesentliche Einrichtungen
und Geldbuße in Höhe von >1,7 Millionen Euro oder 1,4 % des weltweiten Jahresumsatzes für wichtige Einrichtungen

Die Geschäftsleitung kann für die ***Nichteinhaltung dieser Verpflichtungen verantwortlich gemacht werden.***

Service-Level im Vergleich

SERVICE-VERGLEICH		MDR	MXDR
24x7x365 CSOC		✓	✓
Analysten 24x7 telefonisch erreichbar		✓	✓
30 Minuten SLA mit hohem Schweregrad		✓	✓
Eindämmungs- und Reaktionsmaßnahmen		✓	✓
Chorus-proprietäre Analyseregeln		✓	✓
Abdeckung der Microsoft Security Suite	Defender für Endpunkt	✓	✓
	Defender für Identität		✓
	Defender für Cloud Apps		✓
	Defender für Office		✓
	Defender für Cloud		✓
	Azure-Dienste		✓
Benutzerdefinierte Microsoft Sentinel-Integration			✓
Benutzerdefinierte Sicherheits-Playbooks			✓
MITRE ATT&CK-Framework-Mapping			✓
Überwachung der externen Angriffsfläche			✓

SERVICE-VERGLEICH		MDR	MXDR
Abdeckung Threat Detection & Response	Endpunkte	✓	✓
	Entra ID-Identitäten	✓	✓
	Server	✓	✓
	Active Directory-Identitäten		✓
	Nicht-Azure-Clouddienste		✓
	Netzwerkprotokollquellen (Firewalls/Switching/APs)		✓
	APIs/Protokolle von Drittanbietern		✓
Wöchentliche Berichte über den Sicherheitsdienst		✓	✓
Cyber Essentials ausgerichteter TVM*-Bericht		✓	✓
Bedrohungsjagd auf Endpunkten		✓	✓
Cyber-Bedrohungsinformationen		✓	✓
Standardmäßige Sicherheits-Playbooks		✓	✓
Sicherheitsempfehlungen und -Anleitungen		✓	✓
Dienst-Governance		✓	✓
Erweiterte Bedrohungssuche			✓

*Threat- & Vulnerability Management

Was ist inbegriffen?

24x7x365 Cyber Security Operation Center

Flexible Abdeckung

MDR - Endpunkte
MXDR – Cloud oder Hybrid

24x7 Monitoring

Proaktive Cyber Threat Intelligence (CTI)

Erkennung von Bedrohungen

MXDR – Benutzerdefinierte Regeln zur Erkennung von Bedrohungen

Triage und Untersuchung von Bedrohungen

Schnelle Reaktion auf Bedrohungen

MXDR – Benutzerdefinierte Sicherheits-Playbooks

Proaktives Threat Hunting & Schwachstellenmanagement

Service Governance und Berichterstattung

Sicherheitsüberprüfungen und -empfehlungen

Optimierter Serviceübergang

Phishing-Simulation

chorus

Matrix für die Dienstlizenzierung

Dienst	Datenquellen	Lizenz-Voraussetzungen	Lizensierung
MDR	• Defender für Endpunkt • Entra ID • Einzelne Firewall*	Unter 300 Benutzer: • Business Premium Über 300 Benutzer: • Defender für Endpunkt P2	• Benutzer • Server • Frontline MDR • Einzelne Firewall*
MXDR	• Defender für Endpunkt • Defender für Office • Defender für Cloud • Defender für Identität • Defender für Cloud Apps • 3rd Parteien • Mehrere Firewalls**	Minimum: • Defender für Endpunkt P2 • Defender für Office P2 Ideal: • E5 oder E3 mit E5 Security Bolt-on; Business Premium mit E5 Security	• Benutzer • Server • Frontline MXDR • 3rd Partys (fest pro Datenconnector) • Mehrere Firewalls**

Hinweis: Mindestens 20 Plätze für MDR- und MXDR-Dienste

* Fixkosten pro Monat.
** Eine Firewall kostenlos

Erfolgsgeschichten von Kunden

Architekturbüro

- 300 Mitarbeiter
- M365 Business Premium
- Security-Workshop zur Diskussion der Strategie
- Chorus wurde mit Darktrace verglichen
- Chorus wurde ausgewählt, um sich auf den Aufbau einer langfristigen Partnerschaft zu konzentrieren

Anwaltskanzlei

- 1.200 Mitarbeiter / Globales, hochwertiges Ziel
- Stand kurz vor der Einführung von CrowdStrike
- MCI-Workshop & Wertnachweis
- M365 E5 Security lizensiert
- Unterzeichneter MXDR (5-Jahres-Vertrag)

Herstellung

- 185 Mitarbeiter
- Ransomware-Verstoß bei früherem Anbieter erlitten
- Kauften MDR-Endpunktdienst
- Eine Sicherheitsverletzung wurde erfolgreich gestoppt
- Uplift auf MXDR (3-Jahres-Vertrag)

Personalvermittlung

- 35.000 Mitarbeiter
- M365 E5 Security lizensiert
- Vollständige E5-Sicherheit und Compliance bereitstellt
- McAfee und Qradar abgelöst
- Kein internes CSOC – MTTT 3 Tage
- Bauen die Zusammenarbeit mit Chorus aus

Microsoft MDR & MXDR Dienste

	MDR	MXDR
Abdeckung	Endpunkte und Identitäten	Endpunkte, Identitäten, Netzwerke und Apps
IR	Inklusive	Inklusive
Lizensierung	Microsoft 365 Business Premium oder Defender für Endpunkt P2	Defender bolt-ons, E5 Security
	Microsoft Sentinel	Microsoft Sentinel
	+	+
Datenquellen (Preis pro Konnektor)	Eine Firewall	Mehrere Datenquellen von Drittanbietern

Service Levels Compared

SERVICE COMPARISON		MDR	MXDR
24x7x365 CSOC		✓	✓
Analysts available by phone 24x7		✓	✓
30 minute high severity SLA		✓	✓
Containment and response actions		✓	✓
Chorus proprietary analytic rules		✓	✓
Microsoft Security suite coverage	Defender for Endpoint	✓	✓
	Defender for Identity		✓
	Defender for Cloud Apps		✓
	Defender for Office		✓
	Defender for Cloud		✓
	Azure services		✓
Microsoft Sentinel custom integration			✓
Custom security playbooks			✓
MITRE ATT&CK framework mapping			✓
External attack surface monitoring			✓

SERVICE COMPARISON		MDR	MXDR
Threat Detection & Response Coverage	Endpoints	✓	✓
	Entra ID Identities	✓	✓
	Servers	✓	✓
	Active Directory Identities		✓
	Non-Azure cloud services		✓
	Networking log sources (Firewalls/Switching/APs)		✓
	3rd Party APIs/Logs		✓
Weekly security service reports		✓	✓
Cyber Essentials aligned TVM report		✓	✓
Endpoint threat hunting		✓	✓
Cyber Threat Intelligence		✓	✓
Standard security playbooks		✓	✓
Security recommendations & guidance		✓	✓
Service governance		✓	✓
Extended threat hunting			✓

Service Licensing matrix

Service	Data Sources	License Pre-requisites	Pricing
MDR	• Defender for Endpoint • Entra ID • Single Firewall*	Under 300 Seats: • Business Premium Over 300 Seats: • Defender for Endpoint P2	• Users • Servers • Frontline MDR • Single Firewall*
MXDR	• Defender for Endpoint • Defender for Office • Defender for Cloud • Defender for Identity • Defender for Cloud Apps • 3rd Parties • Multiple Firewalls**	Minimum: • Defender for Endpoint P2 • Defender for Office P2 Ideal: • E5 or E3 with E5 Security bolt-on	• Users • Servers • Frontline MXDR • 3rd Parties (fixed per data connector) • Multiple Firewalls**

Note: 20-seat minimum for MDR & MXDR services

* Fixed cost per month.
** One Firewall free of charge

TD SYNNEX | Services

Microsoft Sentinel ingestion estimates

MDR

Users	Data Ingested	Price per GB	Month Cost (31 days)
100	20.31GB	£4.36	£88.57
500	101.57GB	£4.36	£196.12
1,000	203.15GB	£4.36	£392.24

MXDR

Users	Data Ingested	Price per GB	Month Cost (31 days)
100	23.87GB	£4.36	£104.07
500	119.35GB	£4.36	£520.36
1,000	238.70GB	£4.36	£1,040.71

MXDR + Third Party

Users	Data Ingested	Price per GB	Month Cost (31 days)
100	28.6GB	£4.36	£124.69
500	143GB	£4.36	£623.45
1,000	286GB	£4.36	£1,246.91

Notes

Please note the above are all estimates as Microsoft Sentinel is priced by consumption.

Pricing correct as of January 2025. Pricing subject to change by Microsoft. Pricing based on West Europe region; regional pricing may vary.

TD SYNNEX | Services

Microsoft Sentinel ingestion estimates

MDR

Users	Data Ingested	Price per GB	Month Cost (31 days)
100	20.31GB	5,13	104,22
500	101.57GB	5,13	230,77
1,000	203.15GB	5,13	461,55

MXDR

Users	Data Ingested	Price per GB	Month Cost (31 days)
100	23.87GB	5,13	123,20
500	119.35GB	5,13	612,31
1,000	238.70GB	5,13	1.224,60

MXDR + Third Party

Users	Data Ingested	Price per GB	Month Cost (31 days)
100	28.6GB	5,13	146,72
500	143GB	5,13	733,61
1,000	286GB	5,13	1.467,24

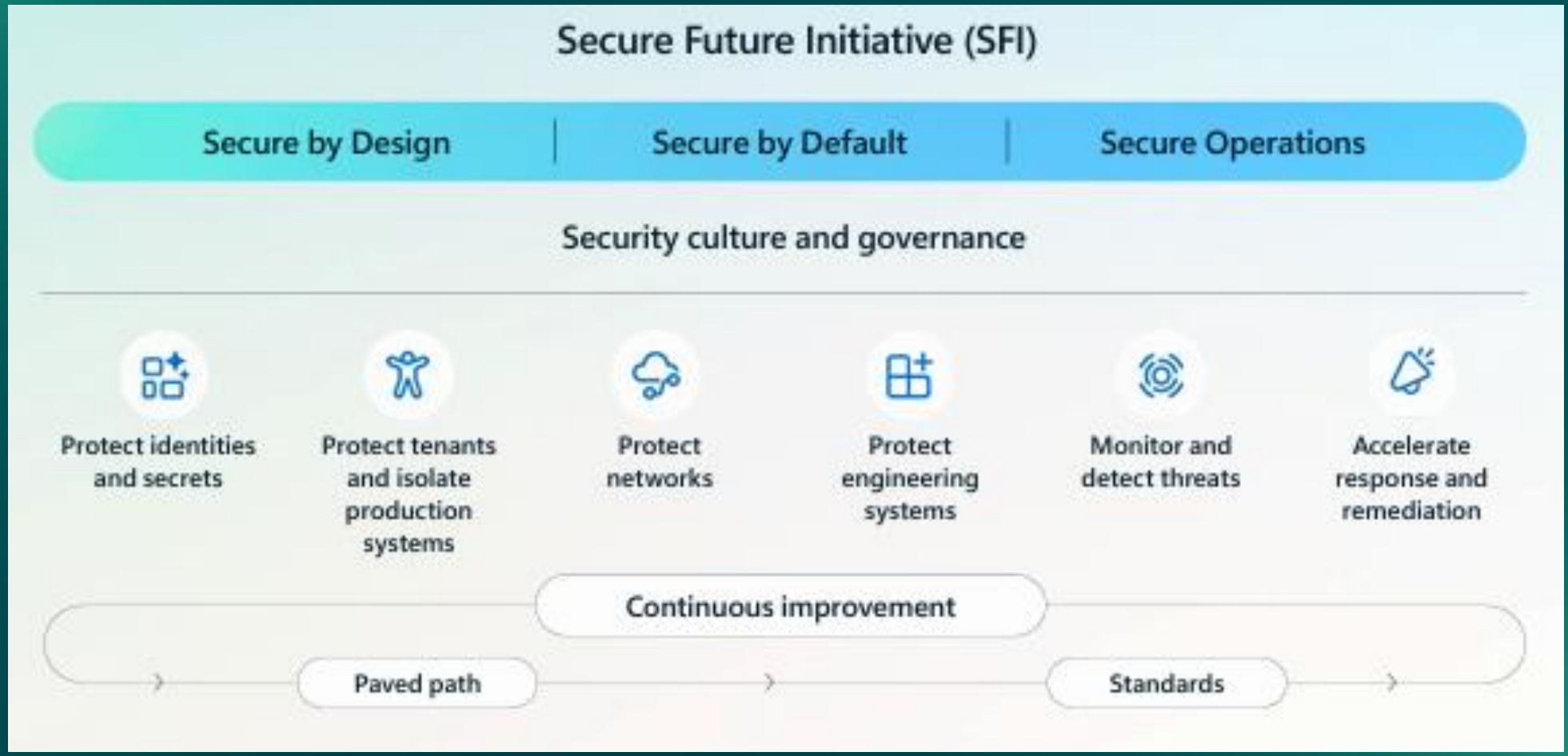
Notes

Please note the above are all estimates as Microsoft Sentinel is priced by consumption.

Pricing correct as of January 2025. Pricing subject to change by Microsoft. Pricing based on West Europe region; regional pricing may vary.

TD SYNNEX | Microsoft

Securing our future: April 2025 progress report on Microsoft's Secure Future Initiative



TD SYNNEX | Microsoft

Sicherheit an erster Stelle

Die Kultur wird durch tägliche Verhaltensweisen gestärkt. Regelmäßige Besprechungen zwischen Engineering Executive Vice Presidents, SFI-Führungskräften und allen Verwaltungsebenen stellen eine Bottom-Up-, End-to-End-Problemlösung sicher, die sicherheitsorientiertes Denken tief in unsere täglichen Aktionen verwurzelt.

Sicherheitsgovernance

Wir erhöhen die Sicherheitsgovernance mit einem neuen Framework, das vom leitenden Beauftragten für Informationssicherheit geleitet wird. Dadurch wird eine Partnerschaft mit Entwicklungsteams eingeführt, um die SFI zu überwachen, Risiken zu verwalten und den Fortschritt an die Geschäftsleitung zu melden.

Kontinuierliche Verbesserung der Sicherheit

Die SFI gibt jedem Mitarbeiter bei Microsoft die Möglichkeit, Sicherheit zu priorisieren, die von einer Wachstumsmentalität der kontinuierlichen Verbesserung gesteuert wird. Wir integrieren Feedback und Erkenntnisse aus Vorfällen in unsere Standards, um ein sicheres Design und einen sicheren Betrieb im großen Stil zu ermöglichen.

Paved Paths und Standards

Paved Paths sind bewährte Methoden, die Produktivität, Compliance und Sicherheit optimieren. Diese werden zu Standards, wenn sie die Sicherheit oder die Entwicklererfahrung verbessern. Mit der SFI legen wir Standards für alle sechs priorisierten Sicherheitspfeiler fest und messen sie.

Defending against cybercrimes has never been harder...

Growing frequency, speed, and targeting of threats

Microsoft security researchers have tracked a **>130% increase** in ransomware attacks.[1]

Security gaps from fragmented tools

80 security tools for an average sized organization.[2]

Alert fatigue and SOC burnout

2 in 5 security leaders feel they're at risk due to cybersecurity staff shortage.[2]

...and the security team's work is endless

How do I investigate more effectively?

How do I prioritize?

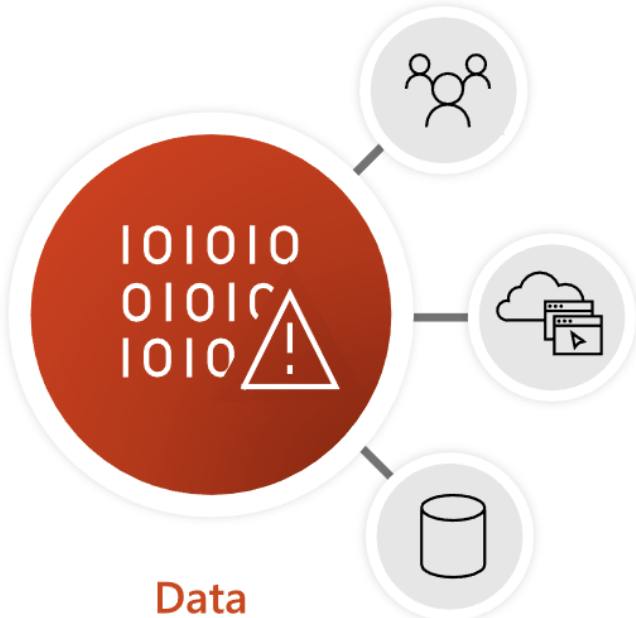
How do I prevent and stop attacks quickly?

1. "Cyber Resilience". May 2021, Microsoft Security Insider.
2. February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees)commissioned by Microsoft with MDC Research

Sophisticated attacks cross multiple domains

Human-operated ransomware campaign

Business email compromise (BEC) campaign



Data exfiltration

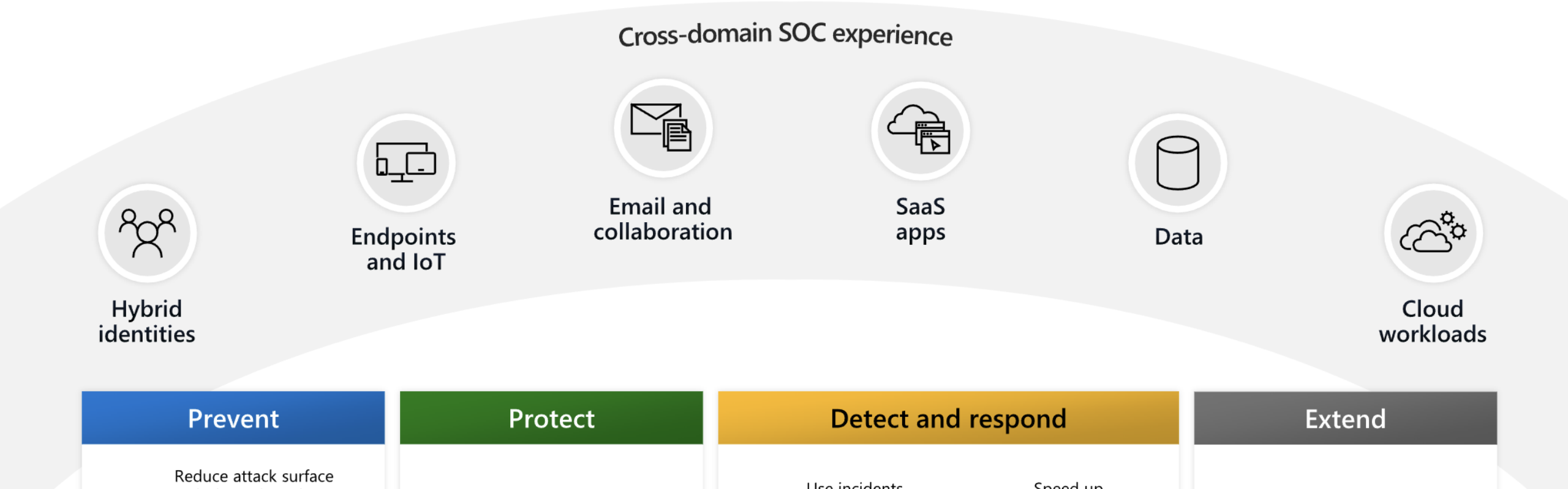
Email | Endpoints | Identities | SaaS apps | Data | Cloud workloads

XDR is the answer to modern attacks

EDR		XDR
Endpoint security only	VS.	Holistic security and signal correlation across identity, email, endpoint, SaaS app, data, cloud, and more
Siloed endpoint alerts		Incident-based investigation and response experience
Can only help fend off endpoint-specific attacks and lacks the big picture to help with advanced attacks		Protects against advanced attacks such as ransomware, business email compromise (BEC), and adversary in the middle (AiTM)

Microsoft Defender XDR

Build a unified defense with XDR



Prevent

Reduce attack surface with threat-based configuration recommendations and built-in vulnerability management

Protect

Automatically contain and remediate compromised assets

Detect and respond

Use incidents to respond to cross-workload threats from a single portal

Speed up response with an experience designed for SOC efficiency

Extend

Unified APIs and connectors

Supercharge your SOC with XDR

Enable rapid response with XDR-prioritized incidents

Remediate threats quickly with a complete view of the kill chain and prioritized investigation and response at the incident level

Disrupt advanced attacks at machine speed

Stop lateral movement of advanced attacks with advanced AI capabilities that automatically isolate compromised devices and user accounts

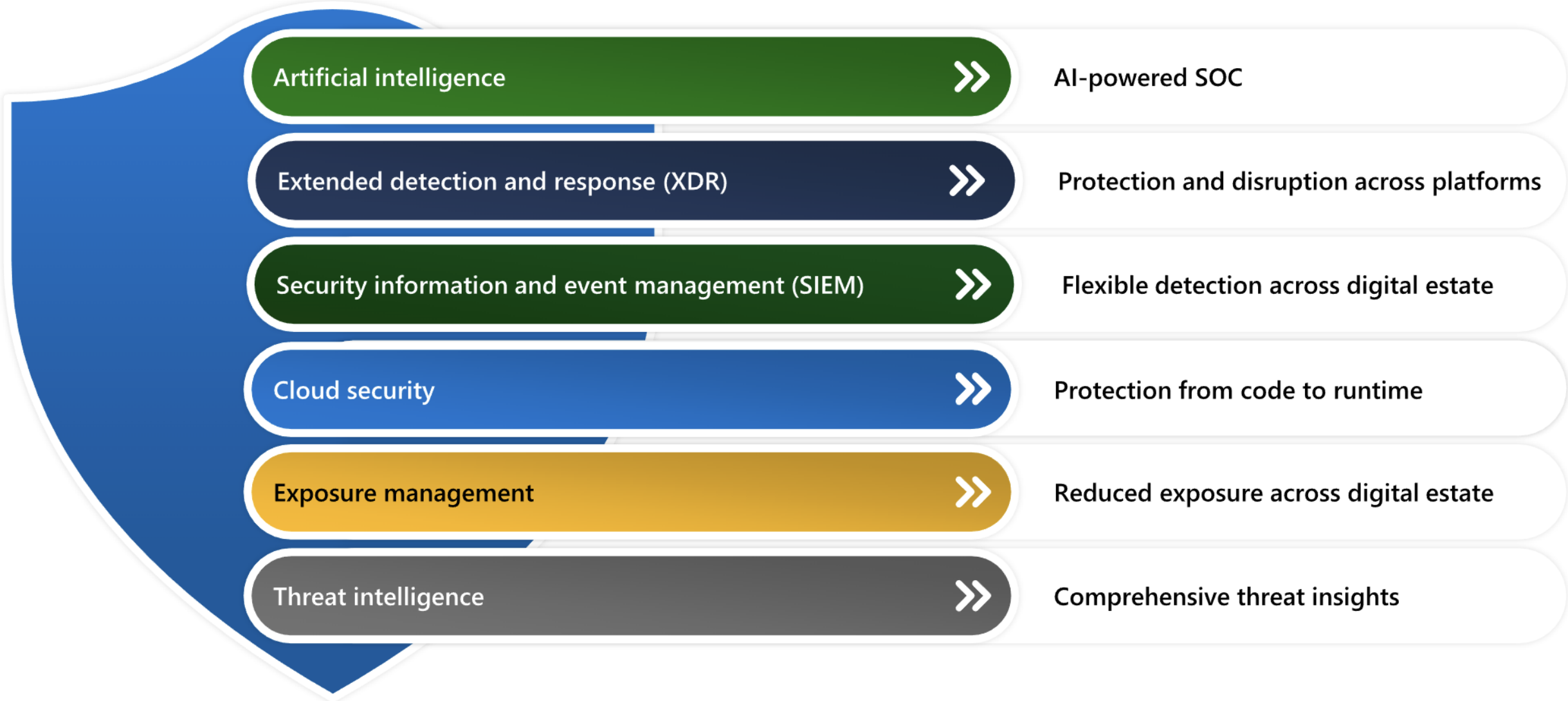
Transform SOC productivity with generative AI

Respond to cyberthreats faster with step-by-step guidance, empower any analyst to build queries in natural language, and reverse-engineer adversarial scripts in seconds

Unify security and identity access management

Protect your hybrid identities and identity infrastructure from credential theft and other threats with seamless integration of Microsoft Entra ID and XDR

Transform SecOps with a unified platform



Why choose Microsoft Sentinel for your SIEM?

Protect everything

3,800+

Standalone content and package solutions ready out of the box

93%

Reduction in time to configure and deploy new connections

78T

Signals analyzed each day

Move faster

22%

Copilot for Security users were faster across all tasks

85%

Reduction of labor effort for advanced, multitouch investigations

Increase ROI

234%

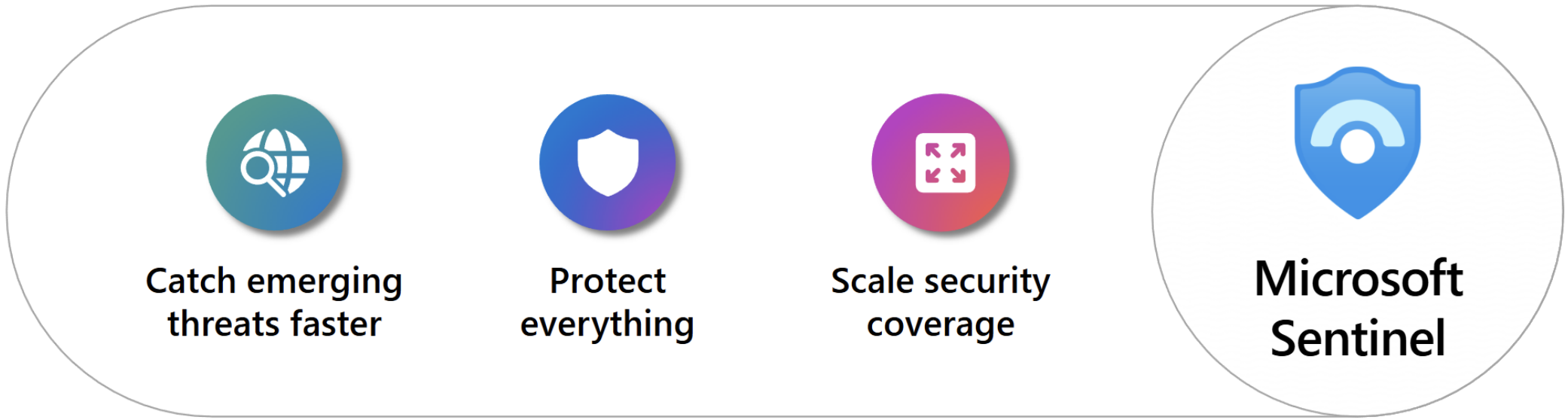
Return on investment (ROI)

44%

Reduction in total cost of operating compared to legacy solutions

The Total Economic Impact™ Of Microsoft Sentinel (forrester.com)

To keep up, security operations need a modern SIEM



Gartner

Gartner has recognized Microsoft as a Leader in the 2024 Magic Quadrant™ for Security Information and Event Management

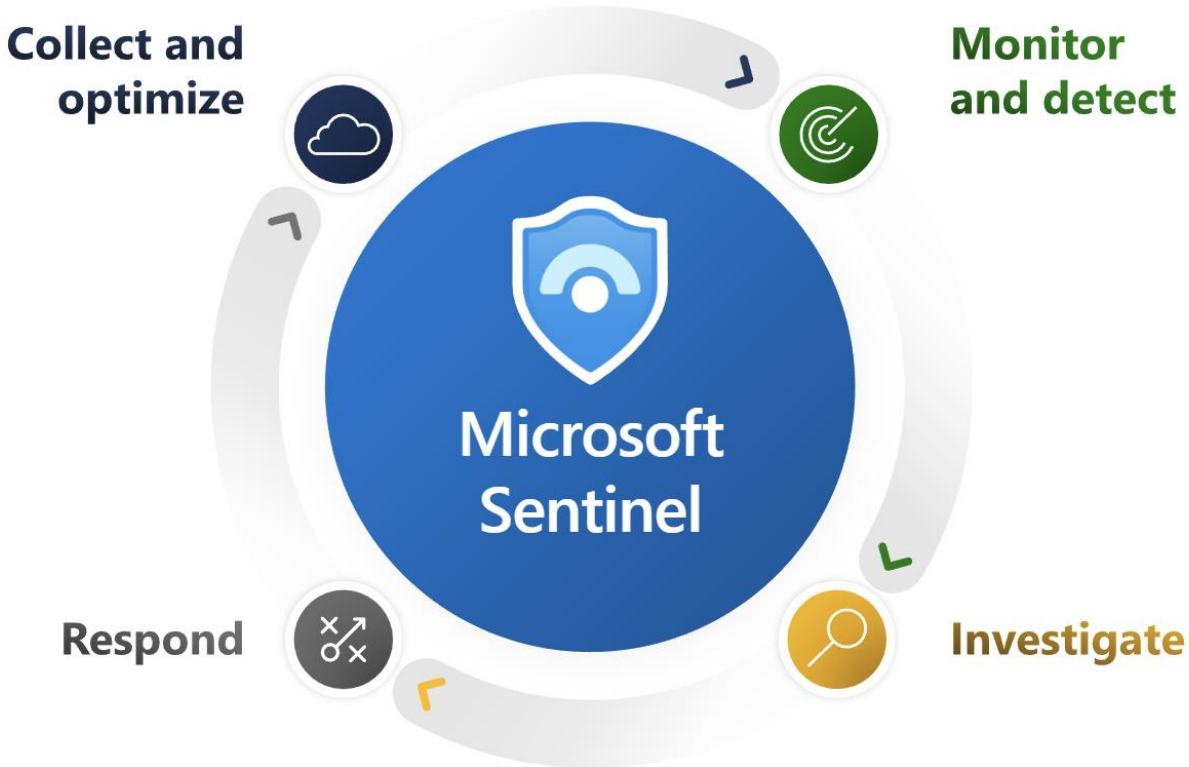
Gartner, Magic Quadrant for Security Information and Event Management, Andrew Davies,Mitchell Schneider,Rustam Malik,Eric Ahlm, May 8th, 2024

2024 Magic Quadrant for Security Information and Event Management

Gartner Glossary: Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).

Gartner IT Glossary, "Security Information And Event Management (SIEM)," [20th July,2022]. [https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem]

Accelerate resolution and improve outcomes across the security lifecycle



Connect all data with out of the box connectors

350+ out-of-the-box connectors | 200+ Microsoft created solutions | 280+ community contributions | 21K GitHub commits

Application

- Apache HTTP Server
- Apache Tomcat
- Atlassian Confluence
- Box
- GitHub
- Jboss
- Microsoft Dynamics 365
- Microsoft Office 365
- Microsoft Teams
- Nginx
- Oracle Database
- Oracle WebLogic Server
- SAP
- Salesforce Service Cloud
- SIGNL4 Mobile
- Slack
- Snowflake
- SQL PaaS
- The Hive
- Workplace from Facebook
- Zoom

Information protection and data loss prevention

- Broadcom
- Cognni
- Digital Guardian
- Forcepoint
- NC Protect Data Connector
- Squadra Technologies

Vulnerability management

- Beyond Security
- InsightVM CloudAPI
- Onapsis
- Qualys VM
- Tenableio
- ★ CyberArk
- ★ Cyborg
- ★ Ermes
- ★ RidgeSecurity
- ★ Seraphic

Cloud provider

- AWS Cloudtrail
- AWS GuardDuty
- AWS VPC Flow
- Azure Activity
- Azure DDoS Protection
- Azure Defender
- Azure Firewall
- Azure Information Protection
- Azure Key Vault
- Azure Kubernetes Service
- Azure Preview
- Azure Storage Account
- Google Apigee
- GCP Audit Logs
- GCP Security Command Center
- GCP DNS
- GCP IAM
- Google Workspace
- Microsoft Entra ID
- Oracle Cloud Infrastructure

Identity

- Cisco Duo Security
- Cisco ISE
- CyberArk
- ForgeRock
- Microsoft Defender for Identity
- Okta Single Sign-On
- OneIdentity
- PingFederate
- RSA SecurID
- 1Password
- ★ Transmit
- ★ Silverfort

IT operations

- AgileSec Analytics
- Atlassian Jira
- Cisco UCS
- Corelight
- Ivanti Unified Endpoint Management
- NXLog BSM macOS
- NXLog Linux
- Orca Security Alerts
- vArmour Application Controller
- VMwareESXi
- Contraforce
- ★ Cribl
- ★ Pure
- ★ Valence

Networking

- Aruba ClearPass
- DNS
- Infoblox NIOS
- NXLog AIX
- NXLog DNS Logs
- Ubiquiti UniFi
- ★ Gigamon
- ★ Infoblox

Endpoint security

- Cisco Secure Endpoint
- CrowdStrike Falcon
- Microsoft Defender for Endpoint
- SentinelOne
- Sophos Endpoint Protection
- Symantec Endpoint Protection
- Trend Micro Apex One
- Trend Micro Vision One (XDR)
- VMWare Carbon Black

Network firewall

- AWS S3 Web App Firewall
- Check Point
- Cisco ASA
- Cisco Firepower
- Cisco Meraki
- CloudFlare
- F5 Big IP
- Forcepoint
- Fortinet Fortigate
- Juniper SRX
- Palo Alto Panos
- SonicWall
- Sophos XG
- Windows Firewall
- ★ Palo Alto

Email security

- Cisco SEG
- Proofpoint On Demand
- VMRay Email Threat Defender
- ★ Cisco
- ★ SlashNext

Threat intelligence

- Recorded Future
- Reversing Labs
- RiskIQ Illuminate
- TitaniumCloud File Enrichment
- ★ Cognyte
- ★ CTM
- ★ Cybersixgill
- ★ Cyware

IoT

- Claroty
- Microsoft Defender for IoT
- ★ Phosphorus
- ★ Radiflow

Web application firewall

- Azure Web Application Firewall
- Barracuda
- Citrix
- Impreva

Insider threat and user entity behavior analytics

- FalconFriday Content
- Microsoft Insider Risk Management

Network security

- Awake Security Arista Networks
- Cisco Stealthwatch
- Cisco WSA
- Citrix Analytics for Security
- F5 Networks (Data)
- FireEye Network Security
- Forescout
- IronNet Collective Defense
- Juniper IDP
- McAfee Network Security Platform
- Perimeter 81
- Pulse Connect Secure
- SquidProxy
- Symantec Proxy SG
- Symantec VIP
- Vectra
- Watchguard Firebox
- WireX Network Forensics Platform
- ★ FortiNDRCloud
- ★ Illumio
- ★ xDome

Threat protection

- Abnormal Security
- Agari
- AIShield AI Security
- Akamai
- Alcide KAudit
- Alsid for AD
- Armorblox
- Automated Logic WebCTRL
- Better MTD
- Blackberry Cylance
- Contrast Protect
- Cyberpion
- Darktrace
- Deception Honey Tokens
- Delinea Secret Server
- Dev-0537 Detection & Hunting
- Elastic
- ESET Enterprise Inspector
- ESET PROTECT
- ExtraHop Reveal(x)
- Flare Systems Firework
- HYAS Insight
- Palo Alto Cortex XDR
- Illusive Attack Management System
- Infoblox Cloud Data Connector
- Kaspersky Security Center
- Log4j Vulnerability Detection
- Lookout Mobile Threat Defense
- McAfee ePolicy Orchestrator
- Microsoft Defender XDR
- Microsoft Defender for Office 365
- Morphisec UTPP
- Proofpoint TAP
- SailPoint
- Security Threat Essentials
- Semperis Directory Services Protector
- Sophos Cloud Optix
- Symantec Integrated Cyber Defense Exchange (iCDX)
- Threat Analysis Response
- Trend Micro Deep Security
- Zimperium Mobile Threat Defense

Compliance

- CMMC
- Maturity Model for Event Log Management M2131
- NIST SP 80053
- Senserva Offer
- Sonrai Security
- Zero Trust (TIC 3.0)
- ★ Prancer

Cloud security

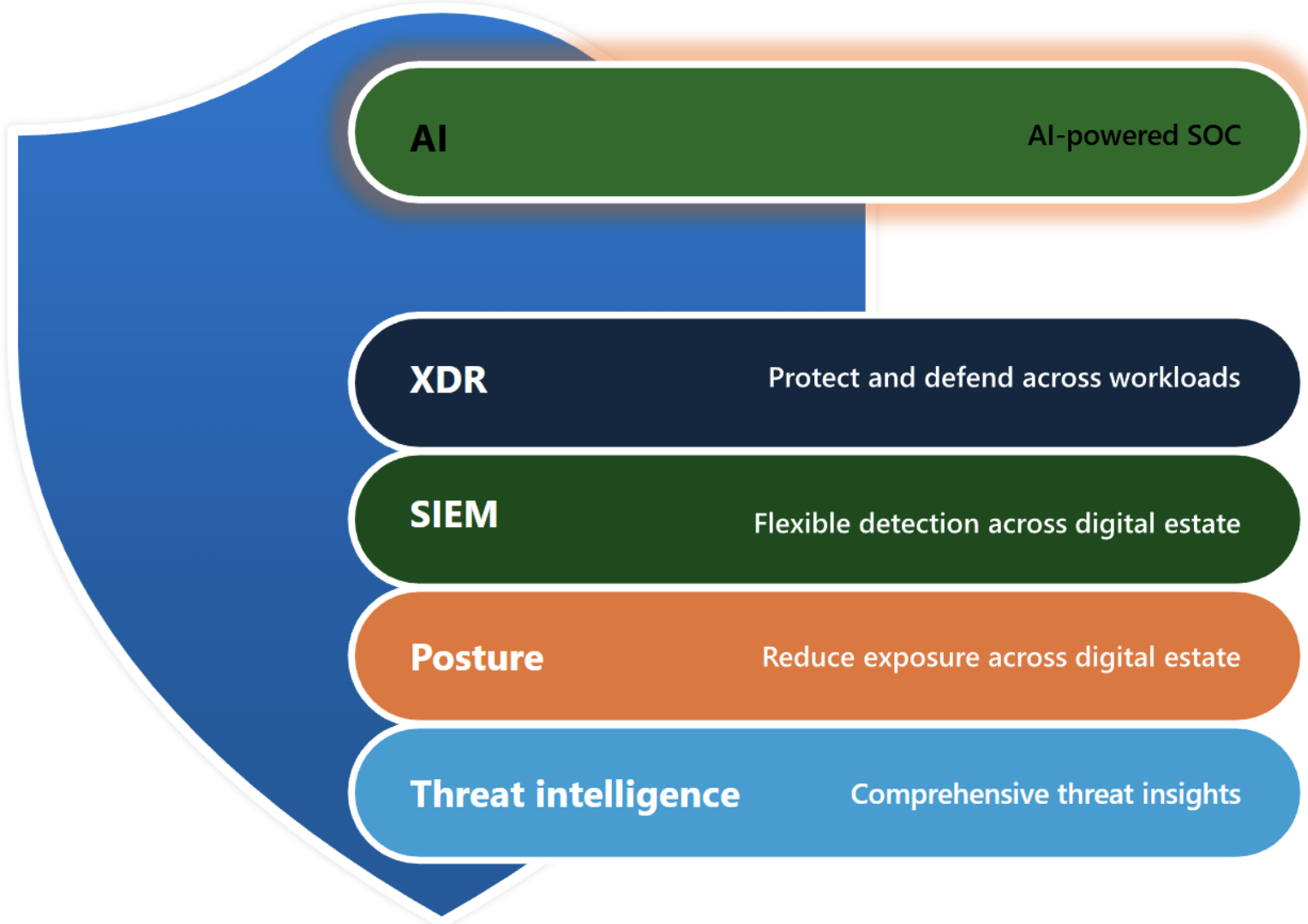
- Barracuda CloudGen Firewall
- Bitglass
- Cisco Umbrella
- Forcepoint CASB
- Forcepoint CSG
- Microsoft Defender for Cloud Apps
- Netskope
- PAN Cortex Data Lake
- PAN Prisma
- Trend Micro Cloud App Security
- Zscaler
- Wiz

= Enhanced ★ = New

Bring GenAI into a unified SOC platform

The AI Advantage

- **Efficiency:** Prioritization and automation
- **Speed:** Ability to understand unique threats in real time
- **Scale:** Ability to process large volumes of data



Bringing Microsoft Sentinel Data into Security Copilot

ContainerInventory	StorageBlobLogs	AppTraces	Perf
ContainerLog	StorageFileLogs	AuditLogs	PowerBIDatasetsWorkspace
CoreAzureBackup	Syslog	AWSCloudTrail	ProtectionStatus
DnsEvents	ThreatIntelligenceIndicator	AzureActivity	SecurityAlert
Event	Update	AzureDiagnostics	SecurityEvent
Heartbeat	UpdateSummary	AzureMetrics	SecurityIncident
InsightsMetrics	VMConnection	BehaviorAnalytics	SecurityRecommendation
KubePodInventory	W3CIISLog	CloudAppEvents	SigninLogs
OfficeActivity	WindowsEvent	CommonSecurityLog	SqlAtpStatus
Operation	WindowsFirewall	AADUserRiskEvents	AppDependencies
AADNonInteractiveUserSignInLogs	Anomalies	AddonAzureBackupJobs	AppMetrics
AADRiskyUsers	AppCenterError	ADFPipelineRun	AppRequests