TD SYNNEX

Willkommen zu IngoS' Vortrag

SOCaaS 24x7

Immer einen Schritt voraus mit Cybersicherheitsschutz!

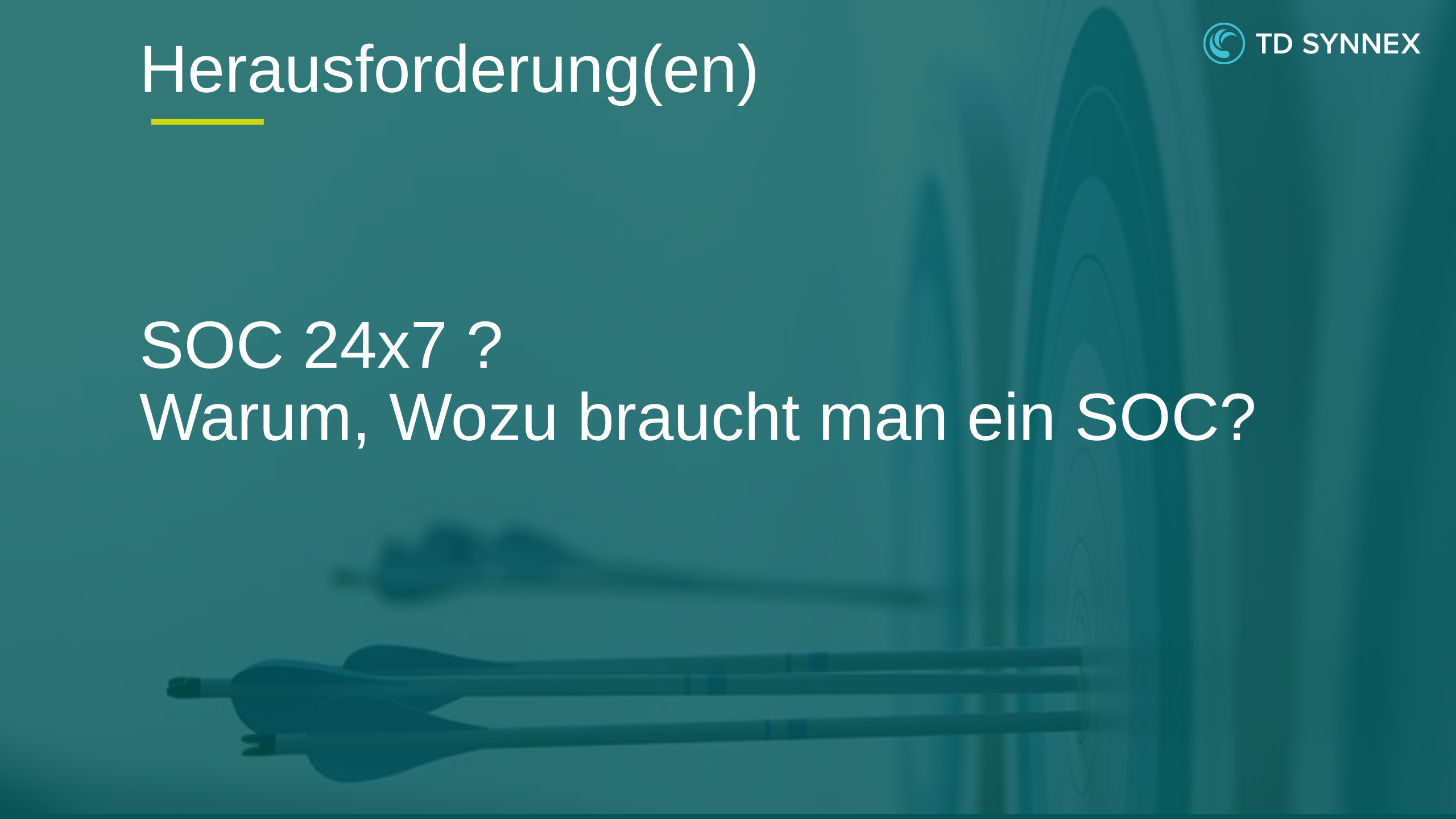
TD SYNNEX Managed Cybersecurity Service

Dr.-Ing. Ingo Schreiber
Business Development Manager
Cloud (AZURE)

Herausforderung(en)

TD SYNNEX

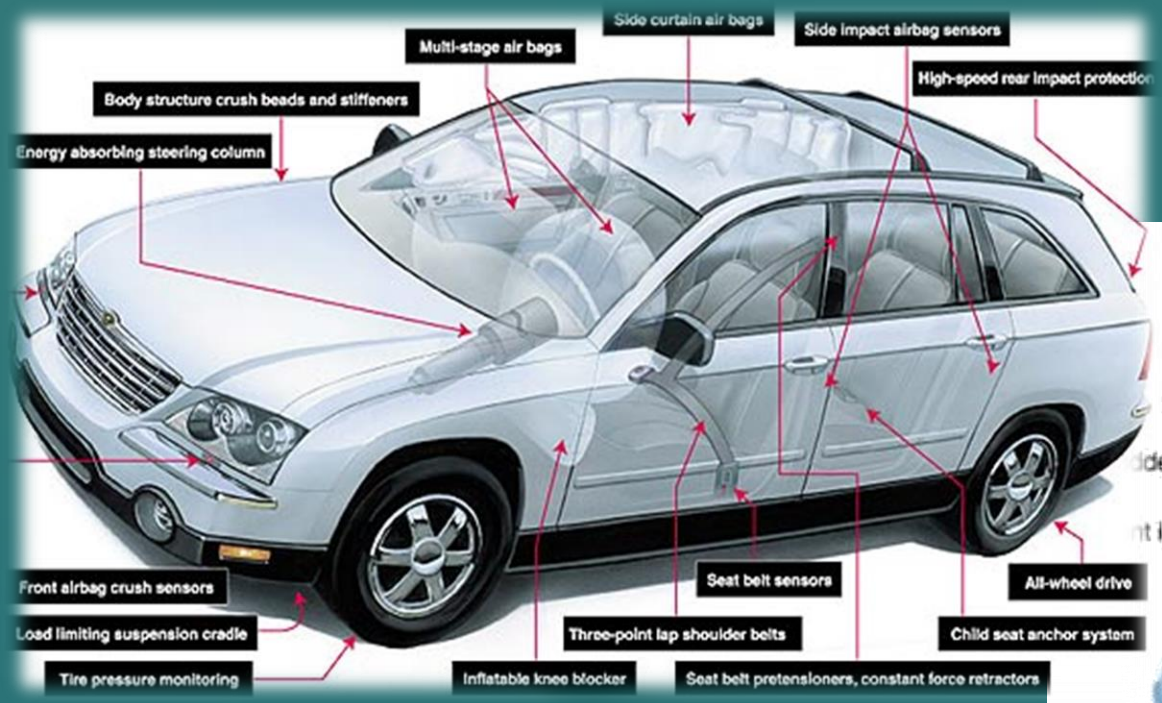
SOC 24x7 ?
Warum, Wozu braucht man ein SOC?

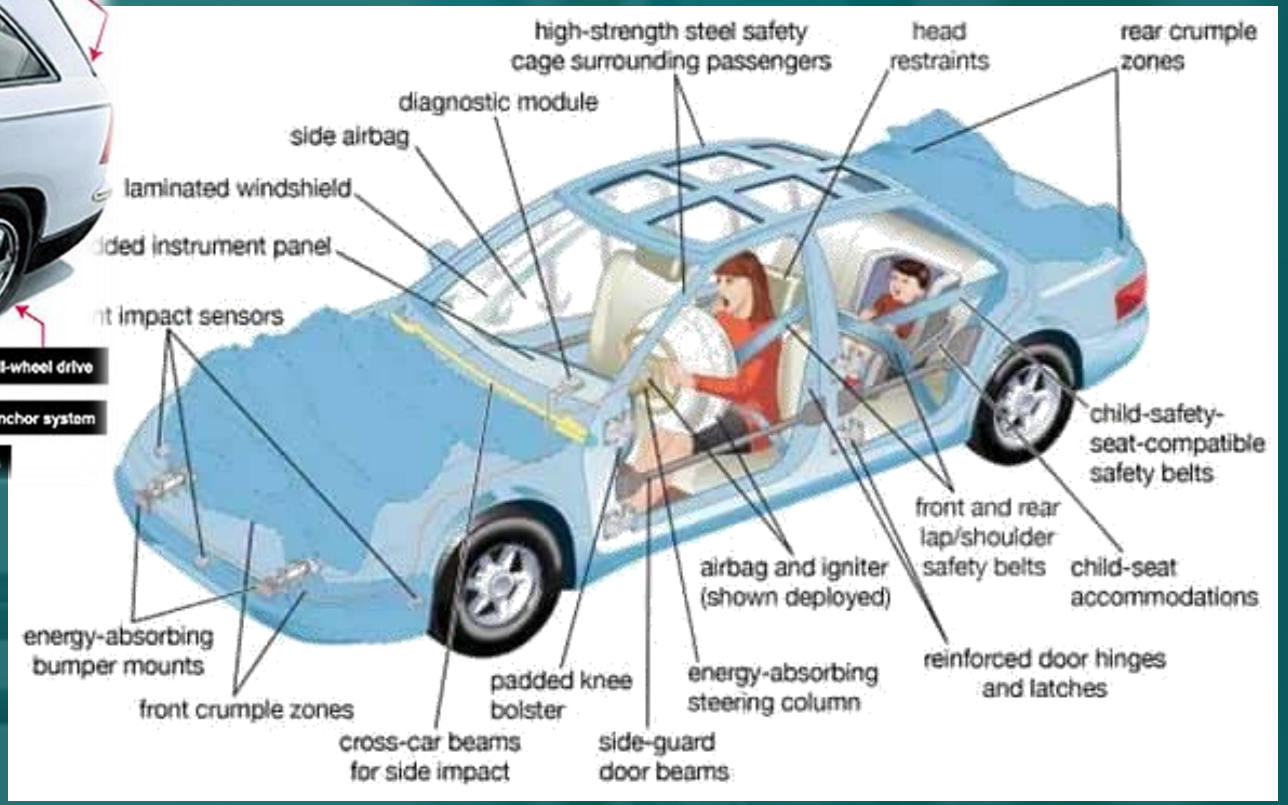


VERGANGENHEIT - Gefahrenabwehr im Straßenverkehr

GEGENWART - Gefahrenabwehr im Straßenverkehr

Die sich verändernde „Bedrohungslandschaft“ erfordert neue Sicherheitsfunktionen!





Modernes Arbeiten bedeutet heute hybrides Arbeiten

TD SYNNEX

Hybrides Arbeiten!
Ja, aber war da nicht noch was?

„Mein Unternehmen ist für Angriffe uninteressant“

„Bei uns war noch nie was“

„Sicherheit ist Aufgabe der IT“

TD SYNNEX

Sicherheitsbedrohungen

Cyberangriffe häufen sich.

Die Angriffsfläche vergrößert sich durch die fortschreitende Digitalisierung.

Da Sicherheitsbedrohungen in Umfang und Schwere immer weiter zunehmen, migrieren Unternehmen zur Risikominimierung in die Cloud.

Anbieter öffentlicher Clouds bieten umfangreiche Ressourcen für den Schutz vor Bedrohungen – mehr als es den meisten Unternehmen möglich ist zu investieren.

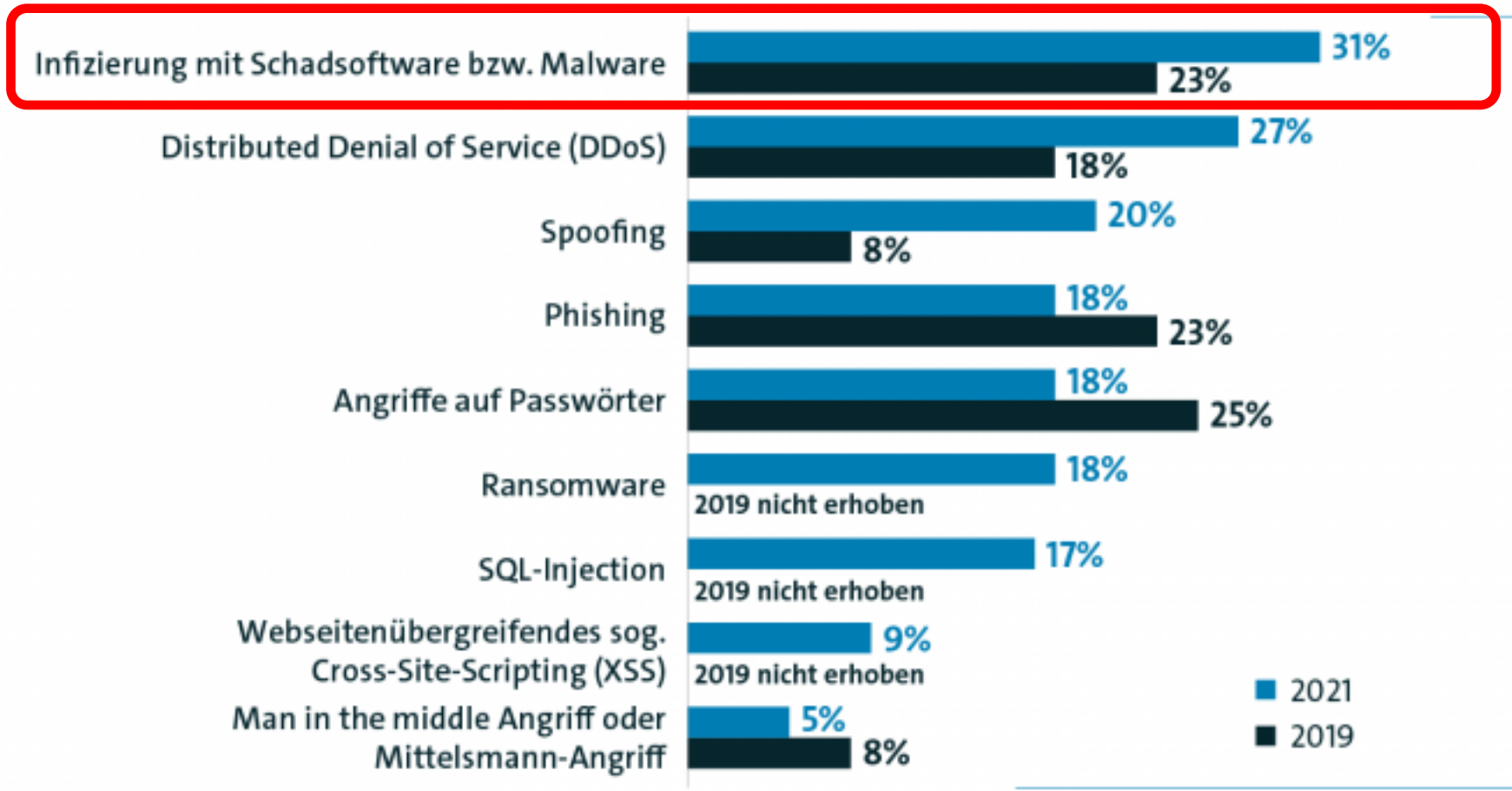
Mythen und Missverständnisse erschweren es jedoch, dass IT-Abteilungen und Experten mithalten können.

Detected Ransomware Attacks

Infosecurity Magazine (i… …urity-mag…

Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



Cyberangriffe haben bei

86%

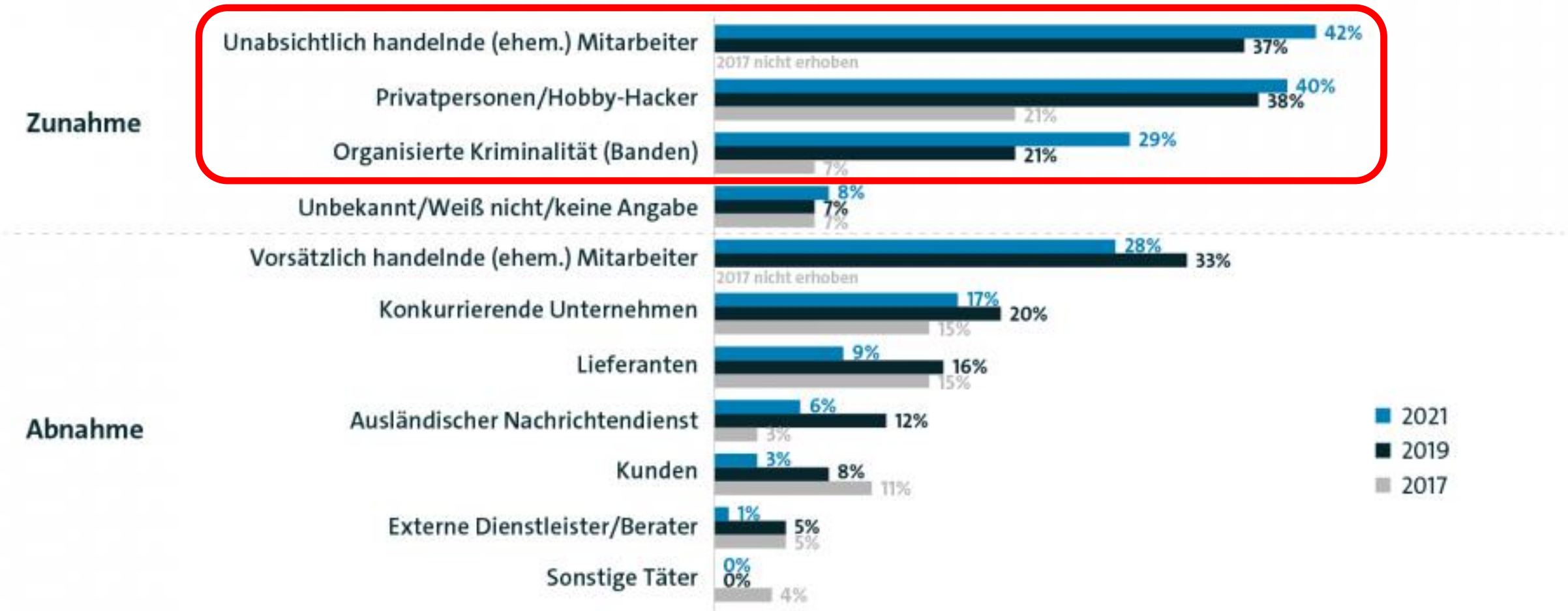
der Unternehmen einen Schaden verursacht – **2019** waren es erst **70%**.

Basis: Alle befragten Unternehmen (2021: n=1.067; 2019: n=1.070); Mehrfachnennungen in Prozent, 2017 und 2019: innerhalb der letzten zwei Jahre
Quelle: Bitkom Research 2021

bitkom

Organisierte Kriminalität steckt zunehmend hinter Angriffen

Von welchen Akteuren gingen diese Handlungen in den letzten 12 Monaten aus?

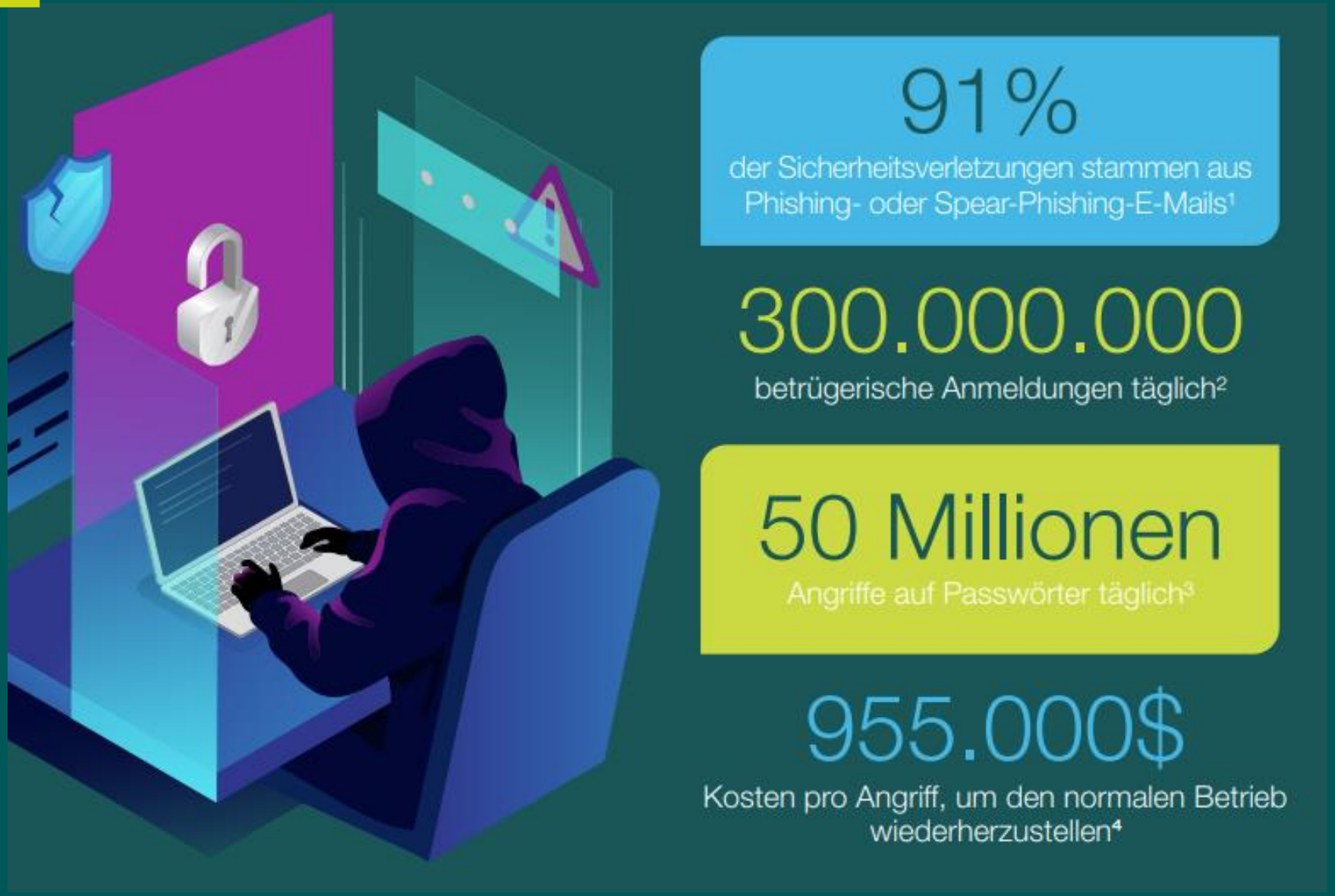


Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2017 und 2019: innerhalb der letzten zwei Jahren) von Diebstahl, Industriespionage oder Sabotage betroffen waren (2021: n=935; 2019: n=801; 2017: n=571); Mehrfachnennungen in Prozent | Quelle: Bitkom Research 2021

bitkom

Einige erstaunliche Statistiken !

TD SYNNEX



91%

der Sicherheitsverletzungen stammen aus Phishing- oder Spear-Phishing-E-Mails[1]

300.000.000

betrügerische Anmeldungen täglich[2]

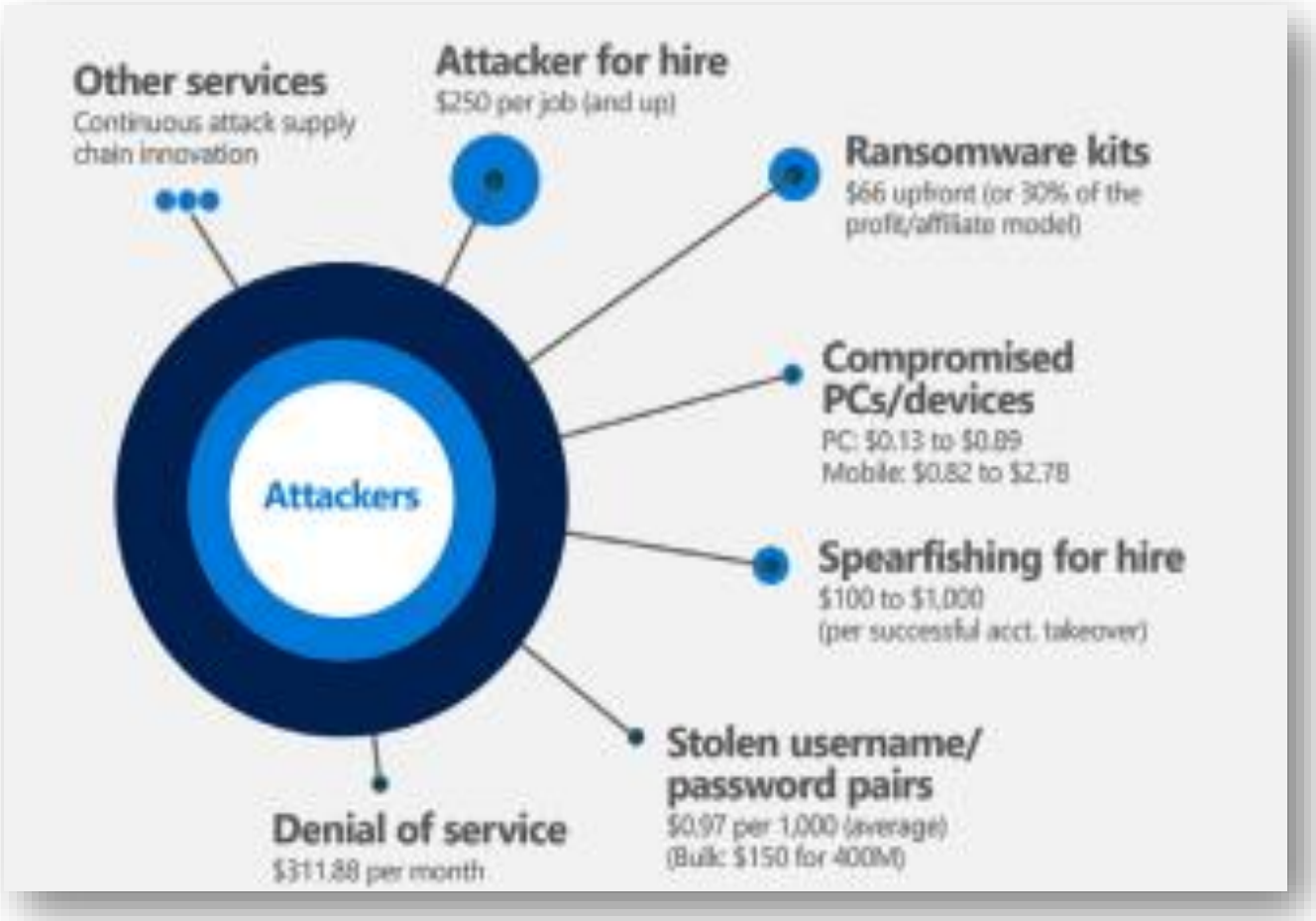
50 Millionen

Angriffe auf Passwörter täglich[3]

955.000$

Kosten pro Angriff, um den normalen Betrieb wiederherzustellen[4]

Preise zum Kauf stehender Cybercrime-Dienste



- Angreifer mieten – ab €200
- Ransomware Kids - €60 im Voraus (oder 30 % des Gewinn-/Affiliate-Modells)
- kompromittierte PCs/Geräte – PC €0,12 bis €0,80 / Handys €0,80 bis €2,50
- Spear-Fishing - €100 - €1.000
- gestohlene Benutzername/Passwort-Paare - €0,97 für 1.000 (durchschnittlich) oder €150 für 400 Mio.
- Denial of Service - €280 pro Monat
- Andere Dienste - Kontinuierlicher Angriff auf Innovationen in der Lieferkette

Warum über Sicherheit sprechen?

TD SYNNEX

Cyberkrieg muss als Unternehmensrisiko verstanden werden!
Cybersicherheit muss oberste Priorität für Führungskräfte haben!

Sicherheit MUSS Bestandteil der Geschäftsplanung sein !

Was ist ein SOC?

TD SYNNEX

Ein Security Operations Center

Eine **Abwehr- & Verteidigungswaffe** im Cyberkrieg!

Was ist ein SOC?

TD SYNNEX

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

Warum sollten Unternehmen ein SOC haben?

Früherkennung von Bedrohungen

Ein SOC überwacht kontinuierlich die IT-Infrastruktur auf Anzeichen von Cyberbedrohungen. Durch die Analyse von Netzwerkverkehr, Systemprotokollen und anderen Datenquellen können Angriffe frühzeitig erkannt werden, bevor sie großen Schaden anrichten können

Schnelle Reaktion und Abwehr

Ein SOC ermöglicht es einem Unternehmen, schnell auf Cyberangriffe zu reagieren. Durch eine gut koordinierte Reaktionsstrategie können Sicherheitsteams Angriffe isolieren, eindämmen und beseitigen, um den Schaden zu minimieren und die Ausfallzeiten zu reduzieren

Schutz sensibler Daten

Unternehmen verarbeiten und speichern sensible Kundendaten, Unternehmensgeheimnisse und andere vertrauliche Informationen. Ein SOC hilft, diese Daten vor Diebstahl, Leaks oder unbefugtem Zugriff zu schützen

Einhaltung von Vorschriften

Je nach Branche und Standort unterliegen Unternehmen verschiedenen gesetzlichen Vorschriften und Datenschutzbestimmungen. Ein SOC kann sicherstellen, dass die Sicherheitspraktiken des Unternehmens mit den Compliance-Anforderungen übereinstimmen und Audits erfolgreich bestanden werden

Risikomanagement und Business Continuity

Ein SOC trägt dazu bei, das Risiko für Cyberbedrohungen zu minimieren. Dies ist besonders wichtig, da erfolgreiche Angriffe nicht nur finanzielle Verluste verursachen, sondern auch den Ruf eines Unternehmens schädigen können. Durch die Reduzierung von Cyber-Risiken trägt ein SOC zur Aufrechterhaltung der Geschäftskontinuität bei


Kosten für die Verhinderung einer Datenschutz-verletzung
Kosten einer Datenschutz-verletzung

Gemeinsam - Hier werden Sie geholfen!

TD SYNNEX Managed SOC as a Service

TD SYNNEX

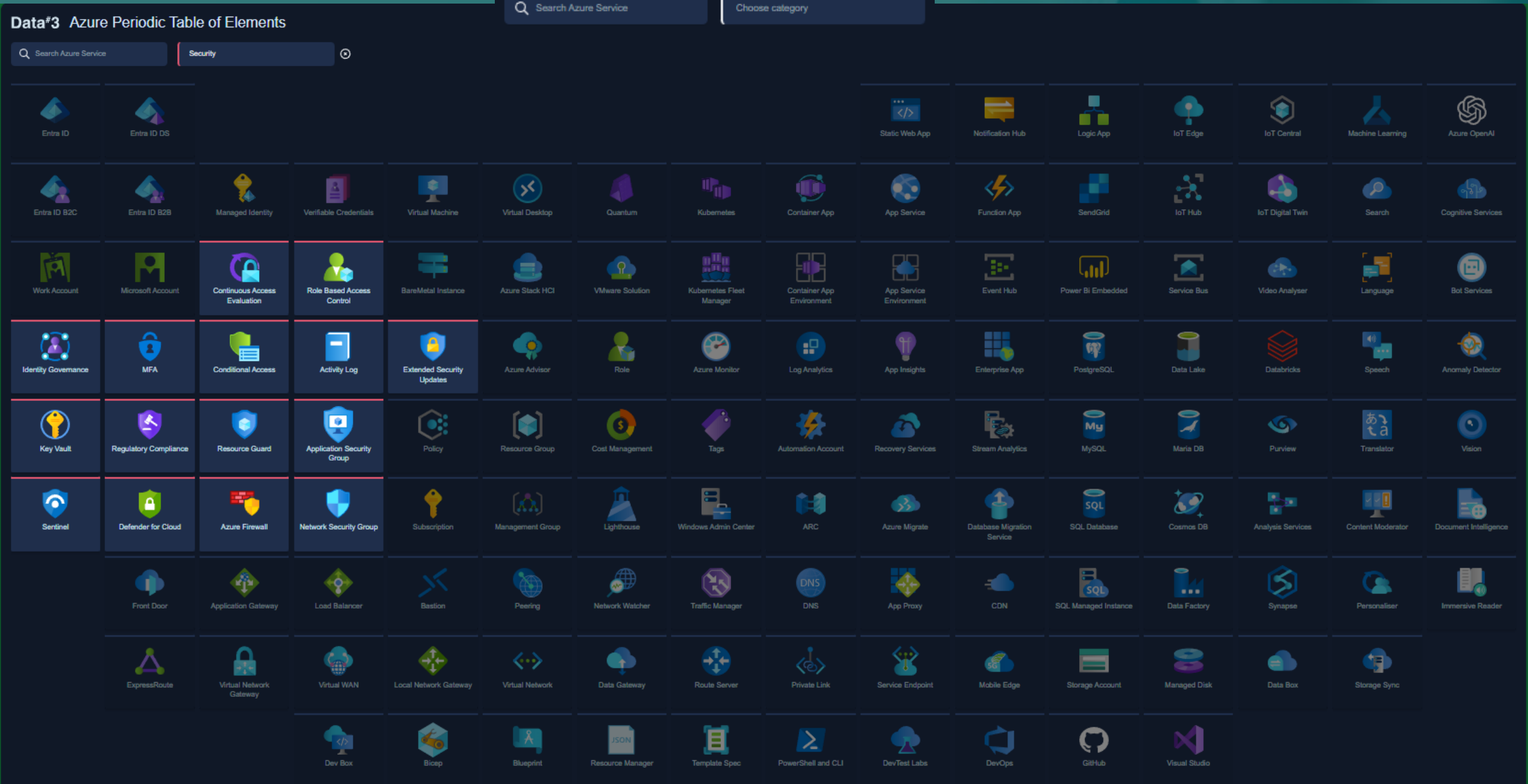
Data#3 Azure Periodic Table of Elements

Search Azure Service | Choose category

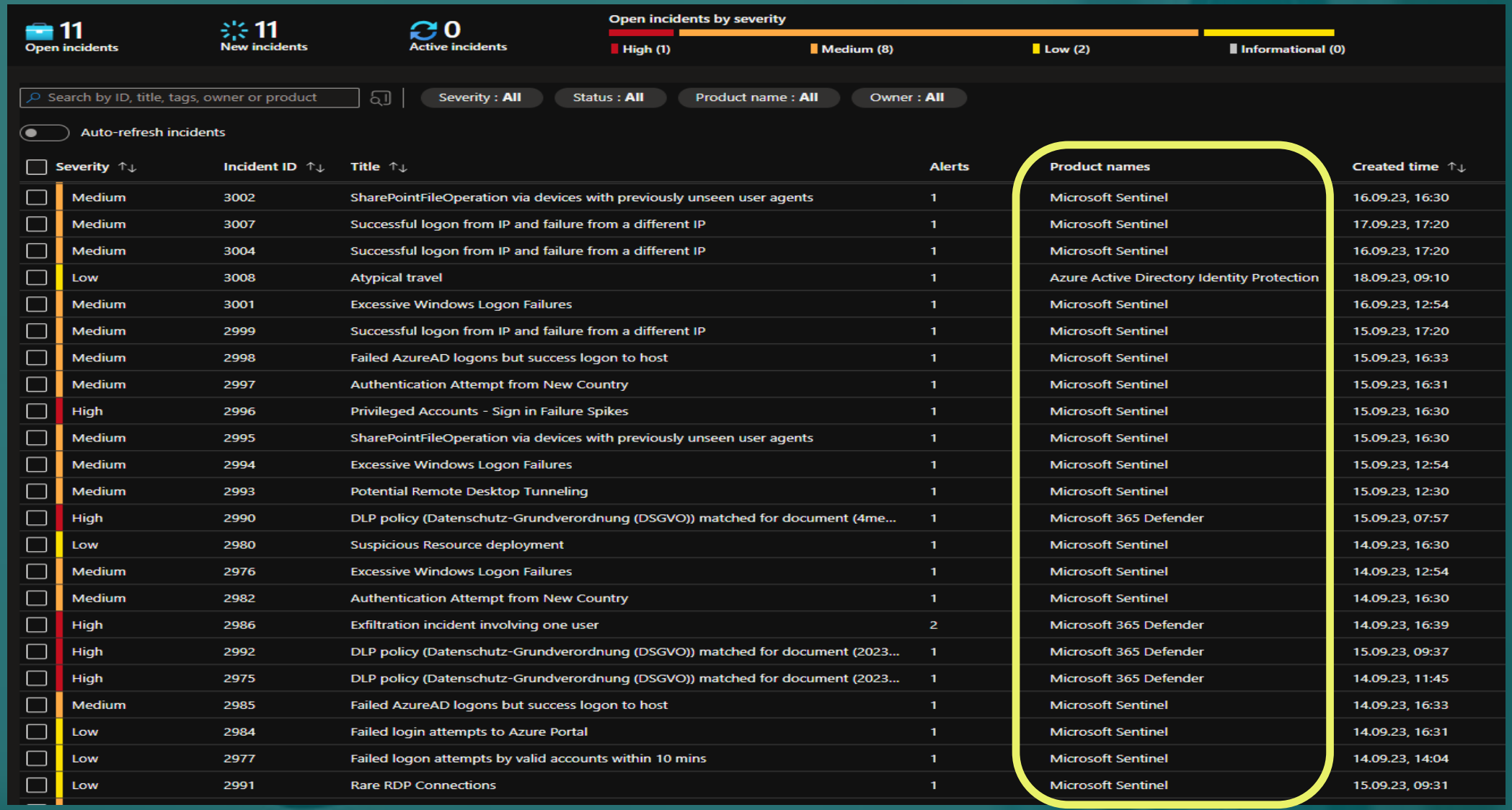
TD SYNNEX

Data#3 Azure Periodic Table of Elements

Search Azure Service | Security



TD SYNNEX Managed SOC as a Service



Severity	Incident ID	Title	Alerts	Product names	Created time
Medium	3002	SharePointFileOperation via devices with previously unseen user agents	1	Microsoft Sentinel	16.09.23, 16:30
Medium	3007	Successful logon from IP and failure from a different IP	1	Microsoft Sentinel	17.09.23, 17:20
Medium	3004	Successful logon from IP and failure from a different IP	1	Microsoft Sentinel	16.09.23, 17:20
Low	3008	Atypical travel	1	Azure Active Directory Identity Protection	18.09.23, 09:10
Medium	3001	Excessive Windows Logon Failures	1	Microsoft Sentinel	16.09.23, 12:54
Medium	2999	Successful logon from IP and failure from a different IP	1	Microsoft Sentinel	15.09.23, 17:20
Medium	2998	Failed AzureAD logons but success logon to host	1	Microsoft Sentinel	15.09.23, 16:33
Medium	2997	Authentication Attempt from New Country	1	Microsoft Sentinel	15.09.23, 16:31
High	2996	Privileged Accounts - Sign in Failure Spikes	1	Microsoft Sentinel	15.09.23, 16:30
Medium	2995	SharePointFileOperation via devices with previously unseen user agents	1	Microsoft Sentinel	15.09.23, 16:30
Medium	2994	Excessive Windows Logon Failures	1	Microsoft Sentinel	15.09.23, 12:54
Medium	2993	Potential Remote Desktop Tunneling	1	Microsoft Sentinel	15.09.23, 12:30
High	2990	DLP policy (Datenschutz-Grundverordnung (DSGVO)) matched for document (4me...	1	Microsoft 365 Defender	15.09.23, 07:57
Low	2980	Suspicious Resource deployment	1	Microsoft Sentinel	14.09.23, 16:30
Medium	2976	Excessive Windows Logon Failures	1	Microsoft Sentinel	14.09.23, 12:54
Medium	2982	Authentication Attempt from New Country	1	Microsoft Sentinel	14.09.23, 16:30
High	2986	Exfiltration incident involving one user	2	Microsoft 365 Defender	14.09.23, 16:39
High	2992	DLP policy (Datenschutz-Grundverordnung (DSGVO)) matched for document (2023...	1	Microsoft 365 Defender	15.09.23, 09:37
High	2975	DLP policy (Datenschutz-Grundverordnung (DSGVO)) matched for document (2023...	1	Microsoft 365 Defender	14.09.23, 11:45
Medium	2985	Failed AzureAD logons but success logon to host	1	Microsoft Sentinel	14.09.23, 16:33
Low	2984	Failed login attempts to Azure Portal	1	Microsoft Sentinel	14.09.23, 16:31
Low	2977	Failed logon attempts by valid accounts within 10 mins	1	Microsoft Sentinel	14.09.23, 14:04
Low	2991	Rare RDP Connections	1	Microsoft Sentinel	15.09.23, 09:31

TD SYNNEX Managed SOC as a Service

TD SYNNEX

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**
  MTTA 5 minutes
  MTTR 10 minutes
- Kostenlose 3rd-Party-Integrationen
- Cloud, Hybrid, On-Premise
- MS Partner & MISA member

chorus

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 3 Paketen
- Preise pro Benutzer und Monat mit einmaliger Onboarding-Gebühr
- **Geeignet für KMU & Großunternehmen (ab 20 User)**
- Fördern Sie das Wachstum, senken Sie die Kosten und steigern Sie den Gewinn durch Outsourcing
- Hohe Kundenzufriedenheit
- Leichter Service, kann aber bei Bedarf über den Partner laufen
- Fördern Sie die Einführung von M365 Business Premium, E3 oder E5
- Treuere Kunden
- Zusätzliche Einnahmequelle für das bestehende Managed-Services-Geschäft

MTTD 6 minutes
MTTA 5 minutes
MTTR 10 minutes

TD SYNNEX

MB

RECORD BREAKER!

Hi all, I wanted to share that our SOC service recently saw record speed in our Mean Time To Acknowledge (MTTA)!

Hitting an average of **2.63 minutes** accross a 1 month period. Despite our collective growth in seat count our service conitnues to perform at an elite level.

Of course we still market our MTTA as below 5 minutes, however this is a fantastic result.

4 1

TD SYNNEX

Bei unserem SOC as a Service INBEGRIFFEN

- 24x7x365 SOC
- Flexible Abdeckung Endpoint, Cloud oder Hybrid
- 24 x 7 Überwachung
- Proaktive Cyber-Bedrohungs-Informationen
- Erkennung & Beseitigung von Bedrohungen
- Threat Triage & Untersuchung
- Raid Threat Detection
- Prokative Bedrohungssuche
- Service Governance & Reporting
- Sicherheits-überprüfungen & Empfehlungen
- Optimierter Serviceübergang
- Phising-Simulation

Unseren 1-pager Flyer bitte mitnehmen 🤝

TD SYNNEX | **Services**

Managed Security Services

Fortschrittlich verwaltete Sicherheitsdienste, die über unser, in Großbritannien ansässiges Cyber Security Operations Center (CSOC), 24×7×365 bereitgestellt werden und auf Microsoft Cloud-Nativen XDR- und SIEM/SOAR-Technologien, Microsoft 365 Defender und Microsoft Sentinel, basieren.

MDR Endpoints

Dienste zur Erkennung & Beseitigung von Bedrohungen zum Schutz aller Endgeräte (Defender Endpoints & Sentinel).

MXDR Advanced

Erkennung und Reaktion auf Bedrohungen über Microsoft E5 Security Tools (Defender-Stack & Sentinel).

MXDR Premium

Erkennung und Reaktion auf Bedrohungen in der gesamten Umgebung (Defender stack, Sentinel, 3rd party logs, etc).

VORTEILE UNSERER MANAGED SECURITY SERVICES

Modernes und innovatives CSOC - Wir haben unser 24/7CSOC so aufgebaut, dass wir technische Innovationen und modernste Cloud-Sicherheitstechnologien optimal nutzen, um einen fortschrittlichen Managed Service anzubieten. Unterstützt von unserem Team hochqualifizierter und erfahrener CSOC-Analysten, schützt unser Team Ihr Unternehmen rund um die Uhr.

Führende technische Architektur - Unsere CSOC-Architektur, die auf Microsoft 365 Defender und Microsoft Sentinel aufbaut, ist nach Best-Practice-Methoden aufgebaut und profitiert von modernster Automatisierung, maschinellem Lernen, KI und Integration, um Fehlalarme zu reduzieren, gängige Aufgaben zu automatisieren und die Erkennung von Bedrohungen und Reaktionszeiten zu beschleunigen.

Proaktiver und präventiver Schutz - Wir gehen mit unseren Managed Security Services noch einen Schritt weiter, indem wir präventiven Schutz durch fortschrittliche Bedrohungssuche und Cyber-Bedrohungsintelligenz einbauen, um aufkommende und unbekannte Bedrohungen proaktiv zu blockieren, bevor sie auftreten.

Schnelle Erkennung von und Reaktion auf Bedrohungen - Durch unser qualifiziertes SecOps-Team, fortschrittliche Technologien und den Einsatz von Automatisierung stellen wir sicher, dass Cyber-Bedrohungen schnell identifiziert, untersucht und behoben werden - und verringern so die Wahrscheinlichkeit und die potenziellen Auswirkungen erfolgreicher Angriffe, damit Ihr Unternehmen den sich entwickelnden Bedrohungen immer einen Schritt voraus ist.

Ausgereifte Dienstleistungen - Mit über 20 Jahren Erfahrung in der Bereitstellung von Managed Services verfügen wir über ein ausgereiftes Modell zur Bereitstellung von Dienstleistungen, das unsere technischen Fähigkeiten ergänzt. Durch kontinuierliche Serviceverbesserung, Service-Governance und Berichterstattung stellen wir eine optimale Servicebereitstellung sicher.

Risikominderung - Durch proaktive Erkennung, Untersuchung, Verfolgung und Reaktion auf Bedrohungen ist Ihr Unternehmen besser geschützt und das Cyber-Risiko wird erheblich reduziert. So können Sie Ihre Cyber-Versicherungsprämien senken, Compliance-Vorschriften einhalten und sich vor immer kostspieligeren Angriffen besser schützen.

50%

2025 werden 50% der Organisationen MDR Services nutzen

Source: Gartner, 2020

Member of Microsoft Intelligent Security Association

Microsoft

Microsoft Partner

Advanced Specialisations
Threat Protection
Identity & Access Management
Info Protection & Governance

Microsoft Security

Unsere MDR- und MXDR-Dienste basieren auf Microsoft 365 Defender und Microsoft Sentinel - Microsoft integrierte XDR- und SIEM/SOAR-Technologien.

Kontakt:

Andreas Wolffs
csp-microsoft@tdsynnex.com
089 / 4700-3020

∑ Fazit :

TD SYNNEX

Mit unserem Managed Security Service bekommen Sie :

- Umfassenden Schutz Ihrer Umgebung
- Mit Best-in-Class Technologie und
- Sie bleiben der Entwicklung von Cyberbedrohungen einen Schritt voraus!