TD SYNNEX | Services

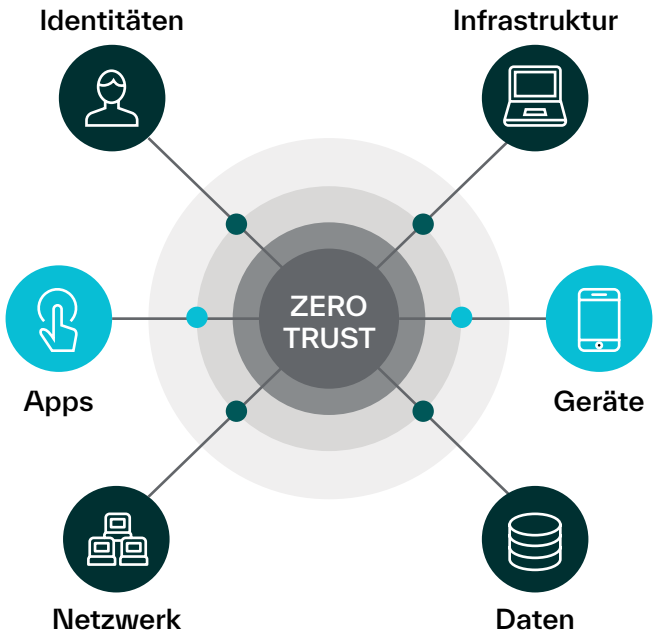
Managed Security-Service Unterstützt von Chorus IT

Verwaltete Cyber Security Services, die über unser in Großbritannien ansässiges Cyber Security Operations Centre (CSOC) rund um die Uhr bereitgestellt werden und auf den Cloud-nativen XDR- und SIEM/SOAR-Technologien von Microsoft 365 Defender, Microsoft Defender for Cloud und Microsoft Sentinel basieren.

Immer einen Schrittt voraus bei sich ständig weiterentwickelnden Cyberbedrohungen

Angriffe auf die Cyber Security werden immer häufiger und raffinierter, weshalb Cyber Security eine der wichtigsten Prioritäten für Unternehmen ist. Heutzutage müssen Unternehmen die Wahrscheinlichkeit eines Angriffs verringern, Bedrohungen proaktiv erkennen und schnell reagieren, um mögliche Auswirkungen auf das Geschäft zu reduzieren. Um dies zu erreichen, benötigen Unternehmen die richtigen Prozesse und Technologien, sowie ein Team aus hochqualifizierter Security-Experten. Allerdings ist es für viele oft unwirtschaftlich, dies intern aufzubauen und zu pflegen.

Unsere verwalteten Security-Services werden über unser CSOC in Großbritannien rund um die Uhr bereitgestellt und helfen Unternehmen in der sich schnell entwickelnden Bedrohungslandschaft von heute besser geschützt zu bleiben. Mit unserem hochqualifizierten SecOps-Team, an ITIL ausgerichteten Prozessen und unterstützt durch fortschrittliche Security-Technologien von Microsoft, bieten wir Organisationen jeder Größe erschwingliche Security Services an.



Unser verwalteter Security-Service

Unsere verwalteten Security-Services nutzen Microsoft-Technologien, um Unternehmen bei der Erkennung, Untersuchung, Bekämpfung und Reaktion auf Cyber Security-Bedrohungen zu unterstützen. Wir bieten flexible verwaltete Security-Services, die es Unternehmen ermöglichen, da richtige Schutzniveau für ihre Security-Anforderungen und internen Kapazitäten zu wählen.

MDR-Endgeräte

Fortschrittliche Services zur Erkennung und Beseitigung von Bedrohungen zum Schutz aller Ihrer Endgeräte.

Laptop

MXDR Advanced

Erweiterte Erkennung und Reaktion auf Bedrohungen über Ihre Cloud-Services hinweg.

Cloud-Zugriff

MXDR Premium

End-to-End-Transparenz, Sanierung und Schutz für Ihren gesamten Bestand (Cloud, Hybrid und On-Premise).

Systemüberwachung

TD SYNNEX | Services

Verwalteter Security-Service

Vorteile unserer verwalteten Security-Services

Modernes und innovatives CSOC – Wir haben unser CSOC, das rund um die Uhr in Betrieb ist, so aufgebaut, dass es technische Innovationen und modernste Cloud-Security-Technologien optimal nutzt, um einen fortschrittlichen verwalteten Service anzubieten. Unterstützt von unserem Team aus hochqualifizierten und erfahrenen CSOC-Analysten schützen wir Unternehmen rund um die Uhr.

Führende technische Architektur – Unsere CSOC-Architektur basiert auf Microsoft 365 Defender und Microsoft Sentinel und ist auf Best Practices ausgelegt, um von hochmoderner Automatisierung, maschinellem Lernen, KI Integration zu profitieren und so falsche Warnmeldungen zu reduzieren, Aufgaben zu automatisieren und die Erkennung von Bedrohungen und Reaktionszeiten zu beschleunigen.

Proaktiver und präventiver Schutz – Wir gehen mit unseren verwalteten Security Services einen Schritt weiter, indem wir durch hoch entwickelte Threat Hunting- und Cyberbedrohungsinformationen präventiven Schutz aufbauen. So werden neue und unbekannte Bedrohungen proaktiv blockiert, bevor sie auftreten können.

Schnelle Erkennung und Reaktion auf Bedrohungen – Durch unser erfahrenes SecOps-Team, fortschrittliche Technologie und den Einsatz von Automatisierung stellen wir sicher, dass Cyberbedrohungen schnell erkannt, untersucht und behoben werden. So werden die Wahrscheinlichkeit und potenzielle Auswirkungen erfolgreicher Angriffe verringert.

Langjährige Erfahung bei den Services – Mit mehr als 20 Jahren Erfahrung bei der Bereitstellung von verwalteten Services verfügen wir über ein ausgereiftes Service-Bereitstellungsmodell, das unsere technischen Fähigkeiten ergänzt. Durch kontinuierliche Serviceverbesserung, Service-Governance und Berichterstattung gewährleisten wir eine optimale Servicebereitstellung.

Risikominderung – Mit proaktiver Bedrohungserkennung, -untersuchung, -prävention und -reaktion ist Ihr Unternehmen besser geschützt und Cyberrisiken werden erheblich reduziert. So können Sie Cyberversicherungsprämien senken, Compliance-Vorschriften einhalten und kostspielige Angriffen abwehren.

„Bis ins Jahr 2025 werden 50% der Unternehmen MDR-Services nutzen."

Quelle: Gartner, 2020.

Microsoft Azure

Microsoftft-Security

Unsere MDR- und XDR-Services basieren auf Microsoft 365 Defender, Microsoft Defender for Cloud und Microsoft Sentinel, den integrierten XDR- und SIEM/SOAR-Technologien von Microsoft.

Durch die Verwendung dieser Cloud-Technologien können wir schnell ausgeklügelte Bedrohungen in jeder Datenquelle erkennen. Mit den SOAR-Funktionen von Sentinel werden häufige Bedrohungen automatisch beseitigt, während komplexe Angriffe von unserem Team hochqualifizierter CSOC-Analysten untersuch werden, um eine schnelle Reaktion zu gewährleisten.

Was ist inbegriffen?

- 24x7x365 SOC
- Flexibler Schutz Endgerät, Cloud oder Hybrid
- Überwachung rund um die Uhr
- Proaktive Aufklärung von Cyber-bedrohungen (CTI)
- Bedrohungserkennung
- Bewertung und Untersuchung von Bedrohungen
- Raid-Bedrohungserkennung
- Proaktive Bedrohungsbekämpfung
- Service-Governance und Berichterstattung
- Security Prüfungen und Empfehlungen
- Optimierte Serviceüberführung
- Phishing-Simulation

TD SYNNEX | Services

Verwaltete Security-Services von Microsoft im Vergleich

Servicevergleich		MDR Endpunkte	XDR Advanced	XDR Premium
Abdeckung der Microsoft Security Suite	Defender for Endpoint	✓	✓	✓
	Defender for Identity		✓	✓
	Defender for Cloud Apps		✓	✓
	Defender for Office		✓	✓
	Defender for Cloud		✓	✓
	Azure Service-Protokolle		✓	✓
	Benutzerdefinierte Microsoft Sentinel-Untersuchung			✓
24X7X365 SOC in GB		✓	✓	✓
Analysten sind rund um die Uhr telefonisch erreichbar		✓	✓	✓
Erkennung von und Reaktion auf Bedrohungen	Endpunkte	✓	✓	✓
	Azure AD-Identitäten	✓	✓	✓
	AD-Identitäten	✓	✓	✓
	Cloud-Services		✓	✓
	Infrastruktur			✓
	Andere APIs/ Protokolle			✓
Wöchentliche automatisierte Metrikberichte		✓	✓	✓
Wöchentlicher automatischer TVM-Highlight-Bericht		✓	✓	✓
Suche nach Endgeräte-Bedrohungen		✓	✓	✓
Standard-Security-Playbooks		✓	✓	✓
Automatisierte Problembehebung		✓	✓	✓
Empfehlungen und Beratung bezüglich Security		✓	✓	✓
Service-Governance		✓	✓	✓
30-Minuten-SLA bei hohem Schweregrad		✓	✓	✓
Regeln zur Erkennung von Kundenbedrohungen			✓	✓
Erweiterte Bedrohungsbekämpfung			✓	✓
Playbooks für Kundensicherheit			✓	✓
MITRE ATTACK-Framework-Zuordnung				✓
Überwachung der externen Angriffsfläche				✓

Warum lohnt es sich, dies Services über TD SYNNE bereitzustellen?

TD SYNNEX wurde bereits mehrfach als Microsofts Worldwide Partner of the Year und Indirect Provider of the Year ausgezeichnet. Mit mehr als 3.900 eingereichten Nominierungen aus mehr als 100 Ländern weltweit. TD SYNNEX wurde für die Bereitstellung herausragender Lösungen und Services in der Kategorie „Indirect Provider of the Year“ ausgezeichnet.

Warum arbeiten wir mit der Firma Chorus zusammen?

Modernes, rund um die Uhr verfügbares CSOC in GB, das hochmoderne Cloud-Security-Technologien mit hochqualifizierten Security-Experten kombiniert, um eine schnelle Erkennung und Reaktion auf Bedrohungen zu ermöglichen.

Fortschrittliche MDR- und XDR-Services, die auf den branchenführenden XDR- und SIEM/SOAR-Lösungen von Microsoft basieren:Microsoft 365 Defender, Defender for Cloud und Microsoft Sentinel.

Innovativer und präventiver Ansatz mit Schwerpunkt auf automatisierter Bedrohungsabwehr und proaktiver Bedrohungserkennung, um neue Bedrohungen zu blockieren.

Microsoft Advanced Specialization & Gold-Partner seit 2004 mit Schwerpunkt auf Maximierung der Microsoft-Investitionen.

Anerkannt nach branchenführenden Qualitäts- und Securitystandards.

Zusammenarbeit, um das richtige Modell für Ihr Unternehmen zu entwickeln und Ihre Anforderungen zu erfüllen.

Etablierung von auf ITIL ausgerichteten MSSP mit ausgereiften Prozessen, Technologien und Fachkenntnissen bei der Bereitstellung von verwalteten Services.

Das Beste aus beiden Welten mit der Reife eines großen Anbieters und dem persönlichen Service und der Agilität eines vertrauenswürdigen Anbieters.

TD SYNNEX | Services

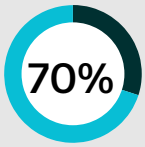
MDR für Endgeräte

Unser Service für MDR-Endgeräte wird von unserem rund um die Uhr besetzten CSOC in Großbritannien bereitgestellt, hilft Unternehmen dabei, Cyber Security-Bedrohungen auf ihren Endgeräten schnell zu identifizieren, zu untersuchen, proaktiv zu bekämpfen und zu beheben.

Angesichts der Tatsache, dass schätzungsweise 70% der Cyber Security-Bedrohungen von Endgeräten ausgehen, und der kontinuierlichen Zunahme von Remote-Arbeit und BYOD stellen Geräte eine häufige Angriffsfläche dar, die aktiv überwacht und geschützt werden muss. Mit Microsoft Defender for Endpoint und Microsoft Sentinel nutzen wir die Vorteile fortschrittlicher Automatisierung, KI und proaktiver Cyberbedrohungsinformationen, um Bedrohungen auf Ihren Geräten schnell zu erkennen und zu beseitigen.

Servicefunktionen

- **CSOC mit Sitz in Großbritannien, das rund um die Uhr verfügbar** ist – Unser hochqualifiziertes SecOps-Team steht Ihnen rund um die Uhr für Schutz und Support zur Verfügung.
- **Erkennung und Untersuchung von Endpunkt-Bedrohungen** – Unser MDR-Service überwacht, identifiziert und reagiert proaktiv auf Bedrohungen in Ihrer gesamten Endpunkt-Umgebung. Dafür wird Microsoft Defender for Endpoint verwendet, um Bedrohungen zu analysieren, einzudämmen und abzuwehren.
- **Automatisierte Reaktion** – Wir bieten automatisierte Eindämmung und Behebung von Bedrohungen durch vereinbarte Security-Reaktionspläne und SOAR-Funktionen, um Geräte schnell zu isolieren, Bedrohungen einzudämmen und deren Auswirkungen zu reduzieren.
- **Cyber Threat Intelligence (CTI)** – Wir integrieren kontinuierlich Threat Intelligence aus externen Quellen sowie CTI aus unserem CSOC-Team. Und wir gehen noch einen Schritt weiter: Wir speisen automatisch neu auftretende Indikatoren für Sicherheitsrisiken (Indicators of Compromise, IOC) in unsere Reaktionspläne ein, um bösartige Inhalte zu blockieren. So sind Sie den sich ständig weiterentwickelnden Taktiken und Techniken der Angreifer immer einen Schritt voraus.
- **Proaktive Bedrohungsbekämpfung** – Durch manuelle und automatisierte Bedrohungsbekämpfung (Threat Hunting) identifizieren wir frühe Indikatoren für aufkommende Bedrohungen, Taktiken oder Verfahren (Threats, Tactics, Procedures, TTPs), um neuen Cyberbedrohungen immer einen Schritt voraus zu sein.
- **Berichte und Analysen** – Wöchentliche, leicht verständliche E-Mail-Berichte, in denen Security-Metriken hervorgehoben werden, so dass Sie regelmäßig einen umfassenden Überblick erhalten.
- **Service-Governance** – Im Rahmen vierteljährlicher und jährlicher operativer Security-Überprüfungen werten wir wichtige Servicemetriken wie die mittlere Erkennungszeit (Mean Time to Detect, MTTD) und die mittlere Reaktionszeit (Mean Time to Respond, MTTR) aus, überprüfen Security-Trends und besprechen strategische Ziele.
- **Security-Empfehlungen** – Im Rahmen unserer kontinuierlichen Serviceverbesserung empfehlen wir Security-Verbesserungen, um Risiken zu vermeiden und Ihre Angriffsfläche zu reduzieren.
- **Simulation von Phishing-Angriffen** – Vorbehaltlich der Microsoft-Lizenzierung können wir Angriffssimulationen mit Microsoft Defender für Office 365 anbieten. So können regelmäßig Phishing- und Kennwortangriffe durchgeführt werden, um Mitarbeiter zu schulen und das Bedrohungsrisiko zu verringern.



Schätzungsweise beginnen 70% aller erfolgreichen Sicherheitsverletzunge bei Endgeräten

Quelle: IDC Research

Servicevorteile

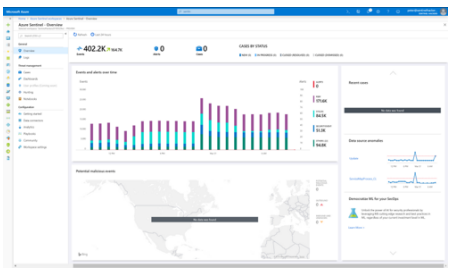
Schützen Sie die am meisten gefährdete Angriffsfläche mit Überwachung, Erkennung und Reaktion rund um die Uhr, um Security-Risiken für Endpunkte zu verringern.

Erweiterte Erkennung von Bedrohungen mit Defender for Endpoint, erweitert mit KI-Analyse, maschinellem Lernen und automatische Untersuchung zur Erkennung fortgeschrittener und raffinierter Angriffe.

Schnelle Reaktion und Eindämmung von Bedrohungen durch automatisierte Reaktionen, manuelle Untersuchungen und vereinbarte Security-Playbooks. So werden Bedrohungen schnell eingedämmt und Geräte isoliert, um dere Auswirkungen zu entfernen oder zu verringern.

Microsoft Security-Expertise gewährleistet eine fachkundige Untersuchung und Behebung sowie eine Anleitung zur Implementierung von Best Practices, damit Sie Ihre Microsoft-Lizenzierung optimal nutzen können.

Proaktive Bedrohungsreduzierung zur Verringerung der Wahrscheinlichkeit zukünftiger Angriffe durch Threat Hunting, proaktive CTI zur Abwehr neuer Bedrohungen und laufende Security-Empfehlungen.



Basierend auf führenden XDR- und SIEM-Lösungen von Microsoft, Microsoft 365 Defender und Microsoft Sentinel bieten wir integrierten Schutz für Ihre Endpunkte, Identitäten, Microsoft 365, SaaS-Apps und E-Mails. Durch unsere Kombination aus Mitarbeitern, Prozessen und Technologie erkennen wir Bedrohungen schnell, entfernen viele automatisch und untersuchen und reagieren auf komplexe Angriffe, um einen proaktiven und innovativen Service zu bieten, der Ihre Cloud-Umgebung schützt.

Servicefunktionen

- **CSOC rund um die Uhr und Expertise** – Unsere Security-Analysten stehen rund um die Uhr zur Verfügung und bieten kontinuierliche Überwachung und Schutz mit unserem in Großbritannien ansässigen Cyber Security Operations Centre.
- **Umfassende Abdeckung der Cloud-Security** – Bedrohungserkennung und -reaktion in Ihrer Cloud-Umgebung rund um die Uhr mit erweiterter XDR – für Ihre Endpunkte, Identitäten, Microsoft 365, SaaS-Apps und E-Mails.
- **Cyber Threat Intelligence** – Die kontinuierliche Integration von Cyber Threat Intelligence (CTI) aus zahlreichen Quellen wird eingesetzt, um proaktiv zu handeln, neue Bedrohungen zu blockieren und Ihr Unternehmen so besser zu schützen.
- **Benutzerdefinierte Regeln zur Bedrohungserkennung** – Erstellung und Verwaltung von maßgeschneiderten Regeln zur Erkennung von Bedrohungen über vorkonfigurierte Regeln und Chorus-Erkennungsregeln, um Ihre einzigartigen Anforderungen an die Cyber Security zu erfüllen und die Abdeckung von Bedrohungen zu erweitern.
- **Schnelle Reaktion auf Bedrohungen** – Automatisierte Security-Reaktionspläne reagieren sofort auf gängige Aufgaben und Bedrohungen, während ausgefeilte Angriffe von unseren CSOC-Analysten schnell untersucht und entschärft werden. So wird die Zeit für die Erkennung und Reaktion auf Bedrohungen verkürzt und potenzielle Auswirkungen werden minimiert.
- **Benutzerdefinierte Security-Playbooks** – Wir erweitern unsere Bibliothek integrierter und von Chorus entwickelter Security-Reaktionsplänen mit benutzerdefinierten Playbooks, um Ermittlungs- oder Reaktionsmaßnahmen im Einklang mit Ihren Security-Richtlinien zu automatisieren.
- **Erweiterte Bedrohungsbekämpfung** – Erweiterte Bedrohungsbekämpfung und Schwachstellenverwaltung in der gesamten Cloud-Umgebung zur proaktiven Identifizierung und zum Schutz vor neuen und aufkommenden Bedrohungen.
- **Service-Governance und Berichterstattung** – Regelmäßige Service-Governance, Kontoverwaltung und Berichterstattung gewährleisten eine optimale Servicebereitstellung und fördern kontinuierliche Service- und Security-Verbesserungen.
- **Security-Strategie** – Wir geben Ihren Teams und Ihrer Security-Strategie auf Grundlage der von uns verfolgten Metriken kontinuierlich Security-Empfehlungen und -Anleitungen an die Hand, so dass Sie von einer proaktiven und vorausschauenden Roadmap profitieren.
- **Reibungsloser Serviceübergang** – Durch unseren standardisierten Serviceübergang und schnelles technisches Onboarding mit Azure Lighthouse stellen wir sicher, dass alle wichtigen Informationen erfasst werden und Sie schnell einsatzbereit sind.
- **Simulation von Phishing-Angriffen** – Regelmäßige Simulation von Phishing-Angriffen, um Mitarbeiter zu schulen und Risiken zu reduzieren.

Servicevorteile

- Fortschrittliche Automatisierung, KI und maschinelles Lernen zur Reduzierung von falschen Warnmeldungen, zur Priorisierung von Bedrohungen mit hohem Risiko und für eine schnelle und effektive Reaktion auf Bedrohungen
- Proaktive Reduzierung und Prävention von Bedrohungen, um die Wahrscheinlichkeit zukünftiger Angriffe durch Threat Hunting, proaktive CTI und regelmäßige Security-Beratung und Berichterstattung zu verringern
- Unsere hochqualifizierten Security-Experten sind als Erweiterung Ihres Teams rund um die Uhr verfügbar und arbeiten partnerschaftlich daran, Ihr Unternehmen zu schützen
- Mit benutzerdefinierten Erkennungsregeln und Security-Reaktionsplänen bieten wir einen maßgeschneiderten Service, der speziell auf Ihre individuellen Anforderungen abgestimmt ist. Wir helfen Ihnen bei der Entwicklung eines Zero-Trust-Best-Practice-Modells, bei dem Sie die Microsoft-Lizenzierungs- und Security-Technologien optimal nutzen können.
- Die Verringerung des Cyberrisikos trägt dazu bei, die Prämien für Cyber-Versicherungen zu senken, Compliance-Vorschriften einzuhalten.

„Durch die Zusammenarbeit mit einem Partner für verwaltete Security-Services wie Chorus können Unternehmen sicherstellen, dass sie von leistungsstarken Security-Funktionen von Microsoft 365 profitieren und sich durch ein Zero-Trust-Framework vor modernen Bedrohungen schützen.“

Adam Hall, Director, Microsoft Security

Microsoft

Für viele Unternehmen ist der Übergang zur Cloud ein schrittweiser Ansatz, der zu einem gemischten Bestand aus Cloud- und On-Premises-Umgebungen führt. Unser XDR-Hybrid-Angebot bietet mehr Transparenz, Integration und Automatisierungsfunktionen, um Security-Bedrohungen in allen Umgebungen zu erkennen, zu untersuchen und schnell darauf zu reagieren.

Servicefunktionen

- **Rund um die Uhr verfügbares CSOC und erfahrene Analysten** – Unsere Security-Analysten stehen rund um die zur Verfügung, um kontinuierliche Überwachung und Schutz zu bieten.
- **Erweiterte Bedrohungserkennung und -Untersuchung** – Bedrohungserkennung rund um die Uhr für Ihr gesamtes Unternehmen mit erweiterter XDR, einschließlich von Endpunkten, Netzwerk, Infrastruktur (On-Premise und in der Cloud) und der Möglichkeit Ereignisse von jeder API oder Quelle aufzunehmen, um eine vollständige Abdeckung zu gewährleisten.
- **Proaktive Bedrohungsdaten** – Die kontinuierliche Integration von Cyber Threat Intelligence (CTI) aus zahlreichen Quellen wird eingesetzt, um proaktiv zu handeln, neue Bedrohungen zu blockieren und Ihr Unternehmen so besser zu schützen.
- **Benutzerdefinierte Regeln zur Bedrohungserkennung** – Erstellung und Verwaltung von maßgeschneiderten Regeln zur Erkennung von Bedrohungen über vorkonfigurierte Regeln von Chorus, um Ihre einzigartigen Anforderungen an die Cyber Security zu erfüllen.
- **Schnelle Reaktion auf Bedrohungen** – Automatisierte Security-Reaktionspläne reagieren sofort auf gängige Aufgaben und Bedrohungen, während ausgefeilte Angriffe von unseren CSOC-Analysten schnell untersucht und entschärft werden. So wird die Zeit für die Erkennung und Reaktion auf Bedrohungen verkürzt und potenzielle Auswirkungen werden minimiert.
- **Benutzerdefinierte Security-Reaktionsplänebooks** – Wir erweitern unsere Bibliothek integrierter und von Chorus entwickelter Security-Reaktionsplänen mit benutzerdefinierten Playbooks, um Ermittlungs- oder Reaktionsmaßnahmen im Einklang mit Ihren Security-Richtlinien zu automatisieren.
- **Erweiterte Bedrohungsbekämpfung** – Erweiterte Bedrohungsbekämpfung und Schwachstellenverwaltung in Ihrer gesamten Umgebung zur proaktiven Identifizierung und zum Schutz vor neuen und aufkommenden Bedrohungen.
- **Service-Governance und Berichterstattung** – Regelmäßige Service-Governance, Kontoverwaltung und Berichterstattung gewährleisten eine optimale Servicebereitstellung und fördern kontinuierliche Service- und Security-Verbesserungen.
- **Security-Beratung** – Wir geben Ihren Teams und Ihrer Security-Strategie auf Grundlage der von uns erfassten Metriken kontinuierlich Security-Empfehlungen und -Anleitungen an die Hand, so dass Sie von einer proaktiven und vorausschauenden Roadmap profitieren.
- **Serviceübergang** – Durch unseren standardisierten Serviceübergang und schnelles technisches Onboarding mit Azure Lighthouse stellen wir sicher, dass alle wichtigen Informationen erfasst werden und Sie schnell einsatzbereit sind.
- **Simulation von Phishing-Angriffen** – Regelmäßige Simulation von Phishing-Angriffen, um Mitarbeiter zu schulen und Risiken zu reduzieren

187 Tage
dauert es im Durchschnitt, um eine Security-Verletzung zu erkennen

720.000£
werden durchschnittlich gespart, wenn der Verstoß innerhalb von 30 Tagen behoben wird
Quelle: IBM, Cost of a Data Breach Report 2021

Servicevorteile

Umfassende Sichtbarkeit von Bedrohungen in Ihrem gesamten Unternehmen, einschließlich Endgeräten, Netzwerken, Infrastruktur (vor Ort und in der Cloud) und anderen Quellen, um blinde Flecken zu vermeiden und Lücken in der Erkennung von Bedrohungen zu schließen.

Automatische Erkennung komplexer Bedrohunge über alle Quellen hinweg mit integrierter Bedrohungserkennung, KI-basierter Analyse und benutzerdefinierten Erkennungsregeln.

Bessere Nutzung fortschrittlicher Funktionen für Automatisierung, KI und maschinelles Lernen zur automatischen Untersuchung von und Reaktion auf Bedrohungen im gesamten Unternehmen anhand vereinbarter Security-Playbooks.

Anreicherung von Ereignissen mit ganzheitlichen Kontextinformationen, um die Anzahl von Warnmeldungen zu reduzieren und wichtige Warnmeldungen zu priorisieren, die Effizienz des CSOC zu erhöhen sowie falsche Warnmeldungen und Alarmmüdigkeit zu reduzieren.

Schnellere Erkennungs- und Reaktionszeiten durch die Eliminierung gängiger Bedrohungen dank Automatisierung, während weiter fortgeschrittene Angriffe von unserem CSOC-Team priorisiert werden.

SIEM Microsoft Sentinel Sichtbarkeit im gesamten Unternehmen	
Microsoft 365 Defender – Sichern Sie Ihre Endkunden	**Microsoft Defender for Cloud** – Sichern Sie Multi-Cloud-Infrastrukturen
Identitäten	SQL/Speicher
Endpunkte	Server-VMs
Apps	Container
E-Mail und Dokumente	Netzwerk
Cloud-Apps	Industrielles IoT
Internet der Dinge (IoT)	Azure App-Services
XDR	

Unser standardisiertes Modell für den Serviceübergang ermöglicht ein schnelles und effizientes Onboarding. Wir verfolgen einen konsistenten und bewährten Ansatz und arbeiten eng mit Ihnen zusammen, um ein detailliertes Verständnis des Unternehmens zu erlangen und sicherzustellen, dass alles richtig eingerichtet ist.

Übergangsprozess

Unser Umstellungsmodell ist in zwei Hauptphasen unterteilt: Service und technisches Onboarding. In Zusammenarbeit mit einem engagierten Projektmanager und einem technischen Ansprechpartner führen wir Sie durch den Übergangsprozess, um ein umfassendes Verständnis der Umgebung, der Prozesse und Fähigkeiten zu erlangen. So stellen wir sicher, dass unser Service den Anforderungen entspricht und alle wichtigen Informationen erfasst werden.
Im Rahmen unseres technischen Onboardings führen wir eine Cyber-Bedrohungsanalyse durch, um Empfehlungen in die laufende Security-Strategie einfließen zu lassen und die Security-Lage weiter zu verbessern. Mit Azure Lighthouse ermöglichen wir ein schnelles technisches Onboarding und stellen gleichzeitig sicher, dass Sie die genaue Kontrolle und Transparenz über die delegierten Services behalten. Nach der Inbetriebnahme überwachen wir aktiv Bedrohungen und Warnmeldungen und nutzen diese Telemetrie zur Feinabstimmung aller Regeln und Playbooks, bevor sie in den operativen Betrieb gehen. Durch regelmäßige Service-Governance-Prüfungen, Kontoverwaltung und Berichterstattung arbeiten wir eng mit Ihnen zusammen, um die Security-Lage zu verbessern und den Service kontinuierlich zu optimieren.

	Einleiten	Vorbereiten	Implementieren	Überwachen	Überprüfen
Service	• Zuweisung eines Transition Managers • Kick-off-Workshop zur Vereinbarung der Projektsteuerung • Erstellung eines Dokuments zur Einleitung des Übergangs	• Überprüfung der Standard-Security-Playbooks und Richtlinien • Entwicklung kundenspezifischer Security-Plänen (XDR-Service) • Wissen	• Integration in den Incident Management-Prozess des Kunden • Erstschulung zu SIEM-Regeln und -Konfiguration • Implementierung benutzerdefinierter Bedrohungen	• Übergabe der Dokumentation • Überprüfung und Behebung aller erkannten Probleme • Verwaltung von CSIP	• Aus dem Übergang gewonnene Erkenntnisse • Freigabe und Abschluss des Übergangs • Übergabe von CSIP in den operativen Betrieb
Technisch	• Zuweisung eines Transition Managers • Kick-off-Workshop zur Vereinbarung der Projektsteuerung • Erstellung eines Dokuments zur Einleitung des Übergangs	• Bereitstellung eines MDE-Mandanten für RBAC • Bereitstellung aller Integrationen auf Anwendungs- oder Tooling-Ebene • Einrichtung oder Überprüfung von Defender for Endpoint	• Konfiguration von Identity Governance, um Analysten Zugriff zu gewähren • Delegation des Zugangs zu Sentinel über Azure Lighthouse • Integration von Nicht-Microsoft-Datenquellen in Sentinel (XDR Service)	• Überwachung von Sicherheitswarnungen rund um die Uhr • Feinabstimmung aller Bedrohungserkennungsregeln und Security-Playbooks • Kontinuierliche Bedrohung serkennungs-Feeds blockieren proaktiv aufkommende Bedrohungen in Ihren Mandanten	• Überprüfung der Ergebnisse der Security-Bewertung und Erstellung einer längerfristigen Roadmap • Kontinuierliche Verbesserung der Security-Lage

Warum ist eine Partnerschaft mit TD SYNNEX und Chorus sinnvoll?

Durch die Partnerschaft mit TD SYNNEX und Chorus können Sie nahtlos MDR- und Managed XDR-Services (MXDR) anbieten, um die Anforderungen Ihrer Kunden zu erfüllen. Dadurch erhält Ihr Unternehmen einen neuen jährlich wiederkehrenden Umsatz und Sie erhalten sich mehr treue Kunden mit einem erstklassigen Service. Chorus ist einer der wenigen Microsoft-Partner, die der Microsoft Intelligent Security Association (MISA) angehören und über eine von Microsoft verifizierte Managed XDR-Lösung verfügen, was weltweit nur 36 Partner erreicht haben.

- 24/7/365 Security Operations Centre
- MTTA (Mean Time to Acknowledge) von 4 Minuten
- MTTC (Mean Time to Close) von 11 Minuten

Schritt 1: Genehmigung

Marktfortschritt
Wir stellen sicher, dass Si alles haben, was Sie für die Genehmigung des Produktivstarts benötigen.

Schritt 2: Ermöglichung

Vorbereitung auf die Markteinführung (Go-To-Market, GTM)
Wir stellen sicher, dass Ihr Team bereit ist,mit Kundengesprächen und Kampagnen zu beginnen.

Schritt 3: Produktivstart

Laufendes Management
Wenn Sie sich auf dem Markt etablieren und neue Aufträge gewinnen, stellen wir sicher, dass Sie Zugang zu einer Reihe laufender Unterstützungsmaßnahme haben.