Insight's Cybersecurity Kompetenz im Überblick

Insight

Einleitung

Cybersicherheit ist für Unternehmen jeder Größe wichtiger denn je, da die Häufigkeit und Komplexität von Cyberbedrohungen zunimmt. Cybersicherheitsverletzungen können verheerende Folgen haben, darunter finanzielle Verluste, rechtliche Haftung, Markenschäden und Vertrauensverlust der Kunden.

Der Schutz Ihres Unternehmens vor Cyberbedrohungen ist nicht nur eine Frage der Compliance oder Best Practices; er ist unerlässlich für die Sicherung Ihrer Betriebsabläufe und die Gewährleistung der Geschäftskontinuität.

Die Investition in robuste Cybersicherheitsmaßnahmen ist eine Investition in die zukünftige Resilienz und den Erfolg Ihres Unternehmens. Durch die Implementierung effektiver Cybersicherheitsstrategien können Sie Risiken mindern, Bedrohungen rechtzeitig erkennen und darauf reagieren und eine starke Abwehr gegen Cyberangriffe aufbauen.

Cybersicherheit ist nicht nur eine Notwendigkeit, sondern ein strategisches Muss für Unternehmen, die in einer sicheren und widerstandsfähigen Softwareumgebung gedeihen möchten. Wir bei Insight verstehen die Notwendigkeit eines umfassenden Sicherheitsansatzes.

Insight's Ansatz für Cybersicherheit

Cybersicherheit ist komplex und erfordert einen umfassenden Ansatz, der Endbenutzer, Sicherheitsteams und Tools einbezieht. Aus diesem Grund verfolgen wir einen ganzheitlichen Ansatz für Cybersicherheit sowohl in den Technologie- als auch in den Integrationsbereichen, der durch wiederholbare Methoden und bewährte Prozesse erreicht wird, die erfolgreiche Ergebnisse liefern. Unsere Experten begleiten Sie von Anfang bis Ende, was zu einer verbesserten Effizienz, Effektivität und strategischen Ausrichtung führt.

Das ganzheitliche Sicherheitsmodell von Insight

Insight's Ansatz für Cybersicherheit

Wir verfügen über umfassende technische Kompetenzen in den fünf Technologiebereichen:

- Endpunkte
- Anwendungen
- Cloud
- Netzwerk, Rechenzentrum und IoT
- Datenzentrierung

Als führender Lösungsintegrator wissen wir jedoch, dass technische Exzellenz in diesen Bereichen nicht ausreicht. Sicherheit muss ganzheitlich angegangen werden, um sicherzustellen, dass alle Sicherheitsbereiche integriert und aufeinander abgestimmt sind. Dies erreichen wir durch die Applikation von:

- Governance, Risikomanagement & Compliance
- Identität und Zugriff
- Erkennung und Abwehr von Bedrohungen
- Menschliche Faktoren

Die Lücken, in denen sich die Technologiedomänen verbinden, sind häufig Bereiche, in denen ein zusätzlicher Wert erzielt werden kann, der dazu beiträgt, Ihre allgemeine Sicherheit auf kosteneffiziente Weise zu verbessern.

Wir helfen Ihnen dabei:

- Ihre Cybersicherheit zu verbessern
- Risiken zu identifizieren und mindern
- Komplexität durch Minimierung von Überschneidungen zu reduzieren.
- Den Sicherheitsbetrieb zu optimieren.
- Sicherzustellen, dass Sicherheitskontrollen Mehrwerte schaffen und die Rentabilität verbessern.

Die Technologie-Säulen

Endpunkte

Die Zeiten, in denen ein einziges Gerät pro Benutzer in einem Unternehmen verwendet wurde, sind vorbei. Es ist mehr als wahrscheinlich, dass Ihre Mitarbeiter mehrere Geräte verwenden. Endgeräte spielen eine entscheidende Rolle bei der Cybersicherheit für Unternehmen und dienen als Einstiegspunkte für Cyberbedrohungen und Schwachstellen. Die Herausforderungen bei der Sicherung von Endgeräten sind aufgrund der Verbreitung von Geräten, Remote-Arbeitsumgebungen und der zunehmenden Komplexität von Cyberangriffen auf Endgeräte gewachsen. Zu den häufigsten Herausforderungen gehören Endgeräte-Transparenz, Schwachstellen-Management, Datenschutz und Application Control.

Diese Geräte müssen gemanaged, ihre Sicherheit überwacht und aktualisiert sowie aktive Abwehrmaßnahmen zum Blockieren von Malware und Exploits bereitgestellt und aufrechterhalten werden. Unsere Endpoint Security Lösungen konzentrieren sich auf den Prozess der Sicherung von Endgeräten wie Notebooks, Desktops, Servern und mobilen Geräten, die für den Zugriff auf Unternehmensnetzwerke und -daten verwendet werden.

Wir helfen Ihnen dabei:

- Erhalten Sie Einblick in Ihre Endgeräte auf Geräte- und Applikations-Level.
- Erkennen und reagieren Sie auf Cyberbedrohungen in Echtzeit
- Schützen Sie sensible Daten auf Geräten vor unbefugtem Zugriff.
- Verhindern Sie Malware-Infektionen und Cyberangriffe auf Endgeräte.
- Erhalten Sie Einblick in die Aktivitäten der Endgeräte für eine effektive Überwachung.
- Sichern Sie Geräte für remote Arbeitsumgebungen.

Applikationen

Da sich Cyber-Bedrohungen ständig weiterentwickeln, stehen Unternehmen vor großen Herausforderungen. Hinzu kommt, dass die Komplexität heutiger Anwendungen immer komplizierter wird, mit zahlreichen miteinander verbundenen Gegenspielern und Integrationen von Drittanbietern, was zu einer breiteren Angriffsfläche führt. Hacker und böswillige Akteure entwickeln ständig neue Methoden, um Schwachstellen in Anwendungen auszunutzen.

Alle Unternehmen verwenden Applikationen, die gepatcht werden müssen, um Schwachstellen im Blick zu behalten – sowohl auf Endgeräten als auch auf der Serverinfrastruktur. Viele Unternehmen werden auch ihre eigenen Applikationen entweder über Low/No Code oder über traditionelle Entwicklung oder DevOps erstellen. Die Integration von Sicherheit und Datenschutz durch Design in den Lebenszyklus der Softwareentwicklung ist für diese Unternehmen von entscheidender Bedeutung.

Unser erfahrenes Insight Sicherheitsberatungsteam hilft Ihnen, die Risiken in Ihrer Anwendungsinfrastruktur zu reduzieren. Wir unterstützen Sie, mit Schwachstellen- und Patch-Management damit Ihre Standardanwendungen auf dem neuesten Stand bleiben und führen Penetrationstests für alle internen Webanwendungen durch.

Vertrauen Sie auf Insight, um Ihre Anwendungssicherheitsanforderungen direkt anzugehen und Ihnen zuverlässigen Schutz und Sicherheit zu bieten.

Wir helfen Ihnen dabei:

- Verwalten Sie Ihre Applikationen, um den Schwachstellen-und Patch-Zyklus im Blick zu behalten.
- Integrieren Sie Sicherheitskontrollen in Ihre DevOps-Prozesse, ohne Kompromisse bei der Entwicklungsgeschwindigkeit einzugehen.
- Verfolgen Sie ein Shift-Left-Konzept bei der Erkennung und Behebung von Bedrohungen und senken Sie so die Kosten für die Behebung.

Cloud

Cloud-Computing bietet eine unübertroffene Skalierbarkeit und Wirtschaftlichkeit, stellt aber auch eine große Sicherheitsherausforderung dar. Unternehmen müssen ihre sensiblen Daten vor unbefugtem Zugriff, Verstößen und Sicherheitslücken schützen und gleichzeitig die Vorschriften einhalten und den Ruf des Unternehmens schützen.

Sie müssen proaktiv und risikobasiert vorgehen und mit Ihren Cloud-Providern zusammenarbeiten, um ein solides Sicherheits-Framework zu schaffen.

Die Insight Cloud- und Sicherheitsexperten verfügen über jahrelange Erfahrung in der Erstellung, Sicherung und dem Betrieb von Multi-Cloud-Softwareumgebungen für Unternehmen jeder Größe und Komplexität. Wir erstellen ein umfangreiches Sicherheits-Framework mit proaktiver Überwachung, damit Sie sich auf Wachstum, Skalierbarkeit und Innovationen konzentrieren können.

Wir helfen Ihnen dabei:

- Schaffen Sie Transparenz in Ihrer Multi-Cloud-Softwareumgebung.
- Sichern Sie Workloads, wo immer sie generiert werden.
- Überwachung und Aufrechterhaltung der Compliance mit Sicherheits-Frameworks.

Rechenzentrums-, Netzwerk- und IoT-Sicherheit

In der vernetzten Welt von heute wächst die digitale Landschaft rasant und lässt ein komplexes Technologienetz entstehen, das Cyberbedrohungen, Datenpannen und unbefugten Zugriffen Tür und Tor öffnet.

Es erfordert ein mehrschichtiges Konzept, um Sicherheitsabwehr und -resilienz in heutigen Unternehmen zu gewährleisten. Eine Kombination aus Firewalls, Verschlüsselung, Zutrittskontrollen und regelmäßige Sicherheitsaudits sind nur der Anfang. Mit hochentwickelten Bedrohungserkennungssystemen und Expertenanalysen müssen Sie Bedrohungen stets einen Schritt voraus sein, um potenzielle Risiken proaktiv zu identifizieren und zu mindern.

Wir beraten Sie bei der Lösung Ihrer Probleme in den Bereichen Rechenzentrum, Netzwerk und IoT-Sicherheit. Mit tiefem Verständnis für Unternehmen, Technologie und Sicherheit schaffen wir die richtige Lösung für Ihr Unternehmen – von der Strategie und Planung mit Design bis hin zur Implementierung und Managed Services. Unsere Sicherheitsexperten helfen Ihnen dabei, sich in der komplexen Technologie zurechtzufinden, die für den Aufbau und die Verwaltung von effektiven Cybersicherheitsmaßnahmen erforderlich ist, um Überschneidungen zu minimieren und eine kosteneffiziente Cybersicherheitsabwehr zu gewährleisten.

Dazu zählen z.B.:

- Transparenz in komplexe Hybridarchitekturen
- Verbesserte Betriebskontinuität.
- Die Sicherheitskontrollen funktionieren sowohl in Ihren on-premises- als auch in Ihren Cloud-Netzwerken.
- Schützen Sie Ihre Daten von der Quelle bis zum Zielort.

Datenzentrierung

Während Sicherheitsfachleute viel Zeit mit der Sicherung von Applikationen und Infrastrukturen verbringen, kommt es letztlich bei fast allem, was wir tun, auf die Sicherheit von Daten an. Ob Mitarbeiterinformationen, Kundenaufträge, Produktionszahlen oder geistiges Eigentum – es sind die Daten, die sich in Ihrem Unternehmen bewegen, die wahrscheinlich den größten Mehrwert für Ihre Endkunden und Ihr Unternehmen schaffen.

Ein guter Ausgangspunkt für Ihre ganzheitliche Sicherheitsstrategie sind Daten. Ein datenzentrierter Ansatz sollte mit der Einbeziehung Ihrer Stakeholder im Unternehmen beginnen, nicht mit der Technologie.

Unser Konzept fokussiert sich auf den Datenschutz und nicht nur auf die Sicherung der Systeme oder Netzwerke, die sie speichern und übermitteln. Wir helfen Ihnen, immer einen Schritt voraus zu sein und das wertvollste Asset Ihres Unternehmens – seine Daten – effektiv zu schützen.

Dazu zählen z.B.:

- Erkennung sensibler und veralteter Daten in Ihrem Bestand.
- Hilft bei der Klassifizierung von Daten, um sicherzustellen, dass das richtige Maß an Kontrolle angewendet wird.
- Einhaltung datenschutzrechtlicher Vorschriften.
- Nachvollziehbarkeit der Datennutzung

Integrationsbereiche

Governance, Risikomanagement & Compliance

Governance, Risikomanagement und Compliance sind wesentliche Komponenten der Cybersicherheit für Unternehmen und umfassen die Richtlinien, Verfahren und Mechanismen zum Management von Cybersicherheitsrisiken und zur Sicherstellung der Einhaltung regulatorischer Anforderungen wie DSGVO und NIS2. Unternehmen stehen vor Herausforderungen bei der Einrichtung effektiver Governance-Strukturen, der Identifizierung und Bewertung von Cybersicherheitsrisiken und der Implementierung robuster Kontrollen zur Minderung von Bedrohungen.

Effektive GRC-Praktiken schaffen klare Rollen, optimieren Prozesse und mindern Cyberrisiken. Eine solide Vorgehensweise erhöht die Reife Ihrer Cybersicherheit, reduziert rechtliche und finanzielle Verbindlichkeiten, verbessert das Vertrauen Ihrer Kunden und die Einhaltung der regulatorischen Compliance. Insight hilft Ihnen dabei, sicherzustellen, dass Security die Anforderungen Ihres Unternehmens unterstützt, ohne sie einzuschränken. Mithilfe von Sicherheitsrisikobewertungen werden die Kosten dieses Risikos berechnet und die Stellen ermittelt, an denen Kontrollen für eine optimale Wirkung eingesetzt werden sollten, während gleichzeitig sichergestellt wird, dass die von Ihnen ausgewählten Kontrollen ihre Aufgabe effektiv erfüllen.

Wir unterstützen Sie:

- Risikobewertung
- Definition der wirksamsten Kontrollen
- Entwicklung von Richtlinien und Prozessen
- Eingebettete Experten auf allen Ebenen der Organisation bis hin zum CISO-Level

- **NIS / NIS2**
- **DORA**
- **Acte EU AI**
- **ISO27001**
- **Cyber Essentials/+**
- **CIS18**
- **NIST CSF**
- **PCI-DSS**

Identität und Zugriff

Identitäts- und Zugriffsmanagement ist ein entscheidender Aspekt der Cybersicherheit für Unternehmen und umfasst die Prozesse und Technologien, die zur Verwaltung und Sicherung digitaler Identitäten und zur Kontrolle des Zugriffs auf Ressourcen verwendet werden. Unternehmen stehen vor Herausforderungen bei der Gewährleistung sicherer und effizienter Identitäts- und Zugriffsmanagementpraktiken, wie z. B. der Verwaltung von Benutzeridentitäten über mehrere Systeme hinweg, der Durchsetzung von Least-Privilege-Zugriffskontrollen und der Verhinderung unbefugter Zugriffe.

Hier bietet eine nahtlose Identitäts- und Access-Management-Lösung, die in allen Bereichen Ihrer Technologie eingesetzt wird, eine stabile und umfassende Cyber-Lösung.

Wir helfen Ihnen, indem wir uns auf die Identifizierung und Minderung von Risikobereichen konzentrieren, und unterstützen Sie bei der Entwicklung kostengünstiger Lösungen, die den Anforderungen der Richtlinien und Prozesse Ihres Unternehmens entsprechen. Erleben Sie erhöhte Sicherheit, geringere Risiken und höhere Effizienz mit auf Ihr Unternehmen zugeschnittenen Konzepten von Insight.

Dies erreichen wir wie folgt:

- Wir begleiten Sie auf dem Weg zum Zero-Trust
- Verfolgen Sie einen geschäftsorientierten Ansatz für den Zugang zu Daten und Anwendungen
- Sicherstellung, dass die richtigen Personen Zugriff auf Ihre Applikationen und Daten haben.

Erkennung und Abwehr von Bedrohungen

Bedrohungserkennung und -reaktion sind entscheidende Komponenten einer robusten Cybersicherheitsstrategie für Unternehmen. Unternehmen stehen vor unzähligen Herausforderungen bei der Identifizierung und Abwehr von Cyberbedrohungen, darunter die sich entwickelnde Art von Angriffen, die Komplexität von IT-Softwareumgebungen und der Mangel an qualifizierten Fachleuten für Cybersicherheit. Eine effektive Bedrohungserkennung erfordert Echtzeit-Überwachung, Analyse von Sicherheitsereignissen und schnelle Reaktion auf Vorfälle, um die Auswirkungen von Sicherheitsverletzungen zu minimieren.

Die Sicherheitsexperten von Insight können Ihnen helfen, Bedrohungserkennungs- und Abwehrlösungen auf unterschiedlichen Ebenen in allen Technologiebereichen Ihres Unternehmens zu entwickeln.

Wir entwickeln Lösungen mit fortschrittlichen Tools, Technologien und unserer Expertise als Sicherheitsberater, um Risiken zu identifizieren und zu mindern, bevor sie Ihrem Unternehmen erheblichen Schaden zufügen können. Insight nutzt Technologien wie SIEM und XDR, die von Sicherheitsanalysten ergänzt werden, um die enormen Datenmengen, die von Ihren Sicherheitstools generiert werden, zusammenzuführen, damit Sie intelligente Entscheidungen über Bedrohungen und Reaktionen in Ihrer gesamten Umgebung treffen können.

Wir helfen Ihnen dabei:

- Bedrohungen früher erkennen
- Reduzierung von Risiken im gesamten Netzwerk
- Umsetzbare Informationen über Bedrohungen
- Automatisierte Bedrohungsabwehr

Menschliche Faktoren

Auch wenn die Sicherheitsinfrastruktur sowie die Tools und Kontrollen kontinuierlich verbessert und in diese investiert werden, gibt es immer noch Verstöße, die nicht einfach zu erkennen und zu beheben sind. Es gibt viele spezialisierte Sicherheitskontrollen für verschiedene Arten von Bedrohungen, von Angriffen auf Endgeräte bis hin zu Angriffen auf Lieferketten – aber wenn Sie untersuchen, wie diese Angriffe tatsächlich stattgefunden haben, sind die drei Hauptgründe:

- **Passwörter**
- **Phishing**
- **Patching**

IT-Teams können Technologie nutzen, um das Risiko von Sicherheitsverletzungen zu verringern, aber Endbenutzer haben immer eine Rolle beim Support der Sicherheit eines Unternehmens. IT-Teams konzentrieren sich häufig auf die Technologie und manchmal auf den Prozess und vergessen dann die menschliche Seite, obwohl doch Menschen den Erfolg oder Misserfolg eines Projekts bestimmen können.

Befähigen Sie Ihre Mitarbeiter mit Insight, eine undurchdringliche erste Verteidigungslinie gegen Cyberbedrohungen zu werden. Indem wir uns auf den Menschen konzentrieren, können wir Ihnen helfen, Schwachstellen direkt zu beheben, Ihre Sicherheitsposition zu stärken und Risiken zu minimieren.

Wir helfen Ihnen dabei, Folgendes zu erreichen:

- Verbesserung des Endbenutzer-Bewusstseins für Cybersicherheit.
- Bereitstellung von Schulungen für Entwickler zur Codierung unter Berücksichtigung der Sicherheit.
- Stellen Sie sicher, dass Ihre Administratoren über die erforderlichen Fähigkeiten verfügen, um einen Cyberangriff zu erkennen und darauf zu reagieren.
- Reduzieren Sie das Risiko erfolgreicher Angriffe.
- Sparen Sie Kosten, indem Sie Datenschutzverletzungen vermeiden.

Managed Security

Der Ansturm auf Sicherheitssysteme ist unerbittlich. Organisationen sehen sich zunehmend mit Cyber-Bedrohungen konfrontiert, die von raffinierten Hacking-Versuchen bis hin zu heimtückischen Ransomware-Angriffen reichen. Organisationen müssen sich mit komplexen regulatorischen Compliance-Anforderungen auseinandersetzen, sensible Daten schützen und sich ständig weiterentwickelnden Cybersicherheitsrisiken immer einen Schritt voraus sein. Sicherheitslösungen bieten zahlreiche Warnungen und Alarme. Zu wissen, auf welche dringend zu reagieren ist, ist der Schlüssel, um größeren Schaden für Ihr Unternehmen zu verhindern.

Diese Herausforderungen zusammengenommen machen es erforderlich, umfangreiche und proaktive Cybersicherheitslösungen bereitzustellen, um die Unternehmen vor den vielfältigen und komplexen Bedrohungen zu schützen, denen sie täglich ausgesetzt sind. Cybersicherheitsbereitschaft und -resilienz sind von entscheidender Bedeutung, um die Kontinuität und den Erfolg eines jeden modernen Unternehmens zu schützen.

Hier kann Insight helfen – unser Team aus erfahrenen Sicherheitsexperten steht Ihnen 24/7 zur Verfügung und unterstützt Sie dabei, Ihre Cybersicherheit durch proaktive Bedrohungsüberwachung, -erkennung und -reaktion mit Zugang zu modernsten Technologien zu verbessern.

- **Managed Endpoint Detection and Response (MEDR)** Umfasst Laptops, Desktops und mobile Geräte..
- **Managed Extended Detection and Response (MXDR)** Führt Protokolle und Feeds aus einer Vielzahl von Quellen zusammen und bietet die robusteste Erkennungsfunktion für Ihre Umgebung.

Unser Team aus erfahrenen Sicherheitsanalysten kombiniert KI, Threat Intelligence und Analytics und kann in Echtzeit Bedrohungen in Ihrer Softwareumgebung erkennen und darauf reagieren.

Dies erreichen wir durch:

- Proaktives Bedrohungsmanagement
- Experten für Sicherheitsanalyse und Reaktion auf Vorfälle.
- Zugang zu fortschrittlichen Sicherheitstechnologien.
- Sicherheitsstrategie und Roadmap-Entwicklung.
- Skalierbares und kostengünstiges Modell.

Wie wir Ihnen helfen

Wir unterstützen Sie bei der Strategie, Implementierung und Verwaltung zukunftsfähiger IT-Sicherheitslösungen.

Assessment

- Unterstützung bei der Akkreditierung nach Branchenstandards wie ISO27001 oder NIS2
- Überprüfung Ihrer bestehenden Sicherheitskontrollen und Identifizierung von Restrisiken
- Erstellung einer priorisierten Roadmap, um Ihr gewünschtes Level an Sicherheit zu erreichen

Planung & Design

- Unterstützung bei der Umsetzung der Herausforderungen Ihres Unternehmens in Projekte zur Sicherheit
- Support und Anleitung bei der Auswahl der richtigen Anbieter, Produkte und Dienstleistungen
- Vorstellung von Workshops und technischem Design

Aufbau und Implementierung

- Umsetzung von Plänen in die Realität– vom Entwurf bis hin zu vollständig gebauten und dokumentierten Sicherheitskontrollen
- Insight betrachtet jedes Projekt im Kontext Ihrer gesamten Roadmap
- Übergabe an Ihre internen Teams zum Management oder Übergang zu unseren Managed Services

IT Operations Management

- Support-Services sorgen für optimale Sicherheit
- Managed Services, bei denen Insight die Verantwortung für Ihre Sicherheitskontrollen übernimmt

Unsere Sicherheitstechnologie-Partner

IT-Modernisierung ist eine Teamarbeit. Wir vereinen die Fähigkeiten von 6.000+ Software-, Hardware- und Cloud-Partnern mit der umfassenden Branchenexpertise unseres Teams unter einem Dach, um branchenführende Lösungen zu entwickeln, die Ihre Transformationsreise beschleunigen.
Wir arbeiten direkt mit führenden Technologieunternehmen zusammen, damit Sie von folgenden Vorteilen profitieren können:

- Ein Ansprechpartner für den Zugang zu den neuesten Technologieprodukten und -lösungen.
- Ein Ökosystem aus kollaborativen, hochqualifizierten Teams zur Einrichtung und Verwaltung Ihrer IT-Softwareumgebung.
- Wettbewerbsfähige Preise und optimierte Vertragsverhandlungen.
- Partnerunabhängige Lösungen, die auf Ihre spezifischen Anforderungen zugeschnitten sind.

Microsoft · Cisco · aws · Google · paloalto NETWORKS · KnowBe4 · Barracuda · Check Point SOFTWARE TECHNOLOGIES LTD. · FORTINET

Warum sollten Sie eine Partnerschaft mit Insight eingehen?

Cybersicherheit ist komplex und erfordert einen umfassenden Ansatz von Ihren Endbenutzern, Sicherheitsteams und Tools. Deshalb haben wir wiederholbare Methoden und bewährte Prozesse entwickelt, die erfolgreiche Ergebnisse liefern. Unsere Experten begleiten Sie von Anfang bis Ende, was zu einer verbesserten Effizienz, Effektivität und strategischen Ausrichtung führt.

Wir haben:

20+ Jahre Wissen und Erfahrung im Bereich der Sicherheitstransformation

Intensive Partnerschaften mit erstklassigen Anbietern

Lösungsunabhängiger Ansatz um Lösungen zu finden, die am besten auf Ihre Anforderungen abgestimmt sind.

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Cisco Partner

Advanced Security Architecture Specialized
SASE Specialized
XDR Specialized

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Identity and Access Management
Information Protection & Governance
Threat Protection

Gold Microsoft Partner
Microsoft
Azure Expert MSP

Microsoft Solutions Partner
Microsoft Cloud

Nächste Schritte

Wenden Sie sich an Insight, um Ihre Cybersicherheitsstrategie und Ihren täglichen Betrieb zu verbessern. Angesichts der wachsenden Cybersicherheitsbedrohungen ist der Schutz Ihres Unternehmens für Kontinuität und Erfolg von entscheidender Bedeutung. Unser umfassender Ansatz verbessert die Cybersicherheit, identifiziert und mindert Risiken, optimiert den Betrieb, optimiert Sicherheitskontrollen und maximiert gleichzeitig Investitionen. Vertrauen Sie auf die bewährten Methoden und Expertenberatung von Insight, um Ihre Cybersicherheitsabwehr zu stärken und die Resilienz und das Wachstum Ihres Unternehmens zu steigern.

- **ch.insight.com**
- **+41 44 878 7606**