Insight

End-to-End Sicherheit beginnt mit Insight

Mit einem Sicherheitspartner aus einer Hand Resilienz aufbauen, Risiken mindern und Compliance stärken

Maßgeschneiderter Ansatz für umfassende Sicherheit

Ransomware, Phishing, Malware, Datenschutzverletzungen, Insider-Bedrohungen, sich entwickelnde KI-Technologien, neue regulatorische Anforderungen: In der digitalen Welt von heute kann die Notwendigkeit einer leistungsstarken Cybersicherheit nicht hoch genug eingeschätzt werden. Mit der falschen Sicherheitsstrategie riskieren Sie zu viel, aber der Schutz Ihres Unternehmens ist ein 24x7x365-Job - ein Job, der alle Hände voll zu tun hat.

Und genau hier kann Insight helfen. Unsere Cybersicherheitsberatung bietet umfassende Lösungen, um den wachsenden Bedrohungen zu begegnen. Unsere Experten liefern maßgeschneiderte Dienstleistungen, um Cyberangriffe zu verhindern und abzumildern. Von Risikobewertungen und Schwachstellenanalysen bis hin zur Reaktion auf Vorfälle und zum Compliance-Management arbeiten wir unermüdlich daran, Ihre wichtigsten Ressourcen zu schützen.

Durch den Einsatz branchenüblicher Best Practices und enge Partnerschaften mit führenden Anbietern von Cyber-Sicherheitslösungen helfen wir Unternehmen, ihre Netzwerke, Systeme und Daten effektiv zu schützen. Mit dem Schwerpunkt auf proaktiven Sicherheitsmaßnahmen und kontinuierlicher Überwachung versetzt Insight Unternehmen in die Lage, Risiken zu mindern, ihre Sicherheitslage zu verbessern und sich in einer zunehmend komplexen Cybersicherheitsumgebung zurechtzufinden. Lesen Sie weiter und erfahren Sie mehr über die wesentlichen Aspekte einer erfolgreichen Sicherheitsstrategie und wie Insight Sie als All-in-One-Partner Sie unterstützen kann.

Jemand wird Ihre Sicherheitslücken finden.

Lassen Sie es besser uns sein.

Mit dem Vormarsch moderner Anwendungen, KI-Technologien und Operational Technology (OT)/Internet of Things (IoT)-Geräte wird die Angriffsfläche immer größer. Cloud-Sicherheit, Risiken durch Drittanbieter, Ressourcenbeschränkungen und Mitarbeiterfehler sind die Hauptprobleme moderner Unternehmen.

Was ist eine Schlüsselkomponente, um Angriffe zu verhindern, die Widerstandsfähigkeit zu erhöhen und die allgemeine Sicherheitslage zu verbessern? Erhöhte Sichtbarkeit. Es ist an der Zeit, den Blick zu schärfen!

Die Verbesserung der Cybersicherheitsreife umfasst:

- ✓ Erlangen Sie ein umfassendes Verständnis der Sicherheitstechnologien, um Ihre Investitionen zu maximieren.
- ✓ Konzentration auf Prozesse und Richtlinien (z. B. Schulungsprogramme zur Sensibilisierung der Mitarbeiter) sowie auf die Sichtbarkeit und das Management von Bedrohungen.
- ✓ Bewertung von Schwachstellen und Entwicklung/Umsetzung eines praktikablen Plans zur Behebung der Schwachstellen.
- ✓ Entwurf und Implementierung von Sicherheitslösungen auf der Grundlage einer Zero-Trust-Architektur, wie z. B. Netzwerksegmentierung und Verwaltung privilegierter Zugriffe.

Unsere Experten entwickeln einen maßgeschneiderten Ansatz für Ihre individuellen Bedürfnisse. Mit den richtigen Lösungen finden wir Bedrohungen, bevor sie Sie finden. Erfahren Sie, wie die Zero-Trust-Architektur Ihre Sicherheit erhöhen kann. Erfahren Sie mehr über unser Zero-Trust-Assessment.

91%

In unserem jüngsten Umfragebericht nannten 91 % der Befragten die Sichtbarkeit von Bedrohungen als eine der wichtigsten Prioritäten bei der Modernisierung der Sicherheit.[1]

Was passiert nach einem Angriff? Auch das ist wichtig.

Stärken Sie Ihre Abwehr- und Reaktionsstrategien gegen Ransomware.

Cyberangriffe sind eine Frage des Wann, nicht des Ob. Angreifer sind hartnäckiger als je zuvor, und da Ransomware immer ausgefeilter wird, benötigen Sie sichere Lösungen, um Ihre Daten, Geräte, Benutzer und Ihren Ruf zu schützen.

Ein gut durchdachter Incident Response Plan ist ein wichtiger Bestandteil Ihrer Sicherheitsstrategie, aber das Risiko ist für jedes Unternehmen unterschiedlich. Sie verdienen einen Partner, der die Bedürfnisse Ihres Unternehmens versteht.

Unsere Cybersicherheitsexperten nehmen sich die Zeit, Ihr Unternehmen zu verstehen und Lösungen zur Abwehr von Ransomware zu finden, die auf Ihre spezifischen Cybersicherheitsbedürfnisse, Ihre Datenumgebung und Ihre IT-Komplexität zugeschnitten sind.

4,88 Mio. $

Die weltweiten Durchschnittskosten einer Datenschutzverletzung im Jahr 2024.[3]

73%

der Unternehmen weltweit zahlten 2023[2] ein Lösegeld für die Wiederherstellung kritischer Daten.

Hauptbereiche der Risikominderung neben Vorbereitung, Wiederherstellung und Infrastrukturlösungen:

Identität

Werkzeuge wie Multi-Faktor-Authentifizierung (MFA) und Single Sign-On (SSO) erleichtern die Verwaltung des Benutzerzugriffs auf Ihre internen Systeme.

Endpunkte

Lösungen zur Datenspeicherung und zum Geräteschutz schützen Ihre Teams vor böswilligen Akteuren – unabhängig von ihrem Standort.

Netzwerke

Lösungen wie Zero Trust bieten robusten Schutz mit Verschlüsselung, Netzwerkerkennung, Reaktionskontrolle und Fernzugriffsfunktionen.

Managed XDR

Vereinfachen Sie das Sicherheitsmanagement, skalieren Sie mühelos, erfassen und analysieren Sie Daten und nutzen Sie KI mit unseren Managed XDR Services.

Der Unterschied zwischen einer kleinen Störung und einem katastrophalen Ereignis liegt in der richtigen Planung.

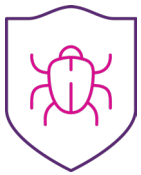
Insight ist für Sie da – vor, während und nach einem Vorfall.

Zusätzlich zu Cybersecurity-Lösungen führender Sicherheitsanbieter bieten wir End-to-End-Services für die Reaktion auf Vorfälle. Damit helfen wir Ihnen, Risiken für Ihr Unternehmen zu verhindern und zu minimieren. Unser auf das Framework des National Institute of Standards and Technology (NIST) abgestimmtes Portfolio an Incident-Response-Lösungen deckt jeden Teil des Cybersicherheitszyklus ab.

Mit unseren Incident-Response-Services profitieren Sie von den wichtigsten Lösungen zur Ransomware-Prävention und -Reaktion:

VOR: Vorbereitung

- Durchführung von Penetrationstests und proaktiver Bedrohungssuche
- Planung der Reaktion auf Vorfälle
- Tabletop-Übungen
- Notfallreaktion auf Vorfälle (Emergency Incident Response Retainer, EIRR)



WÄHREND: Störfallmanagement

- Identifizierung, Eindämmung und Eliminierung von Bedrohungen
- Reaktion auf Notfälle
- Unterstützung bei der Ereignisbehebung

NACH: einem Störfall

- Managed Security
- Übungen zu den gewonnenen Erkenntnissen
- Behebung von Sicherheitslücken nach einem Vorfall

Bleiben Sie konform und sicher.

Es kann schwierig sein, den Überblick über die in Ihrer Branche einzuhaltenden gesetzlichen Vorschriften zu behalten, aber die Folgen eines Rückstands sind gewaltig.

Sie möchten sicherer arbeiten, sind aber an gesetzliche Vorschriften gebunden. Die Nichteinhaltung von Best Practices kann eine lange Liste von Konsequenzen nach sich ziehen. Wie können Sie sicherstellen, dass Sie die gesetzlichen Vorschriften einhalten und gleichzeitig Ihre Unternehmensziele unterstützen?

Wir helfen Ihnen: Seit Jahrzehnten unterstützen unsere Sicherheitsteams Unternehmen auf der ganzen Welt bei der Verwaltung von Sicherheit, Risiken und Compliance.

Unser GRC-Angebot umfasst:

- ✓ Compliance-Bewertungen
- ✓ Sicherheitsberatungsdienste
- ✓ Lösungen für das Risiko- und Compliance-Management
- ✓ Datenschutzlösugen
- ✓ Audits zur Einhaltung gesetzlicher Vorschriften

KURZES QUIZ:

Welcher der folgenden Punkte ist ein mögliches Ergebnis schlecht ausgeführter Governance-, Risiko- und Compliance-Aktivitäten (GRC)?

a) Erhöhte Komplexität

b) Bußgelder und Strafen

c) geringere Leistung

d) eingeschränkte Sichtbarkeit

e) Organisatorische Anfälligkeit

f) alle oben genannten Punkte

Sie haben es erraten: Alle oben genannten Punkte.

Möchten Sie mehr erfahren? Hier finden Sie weitere Informationen:

- Unser umfassendes GRC-Angebot
- Unsere GRC-Bewertungsdienste

Warum sollten Sie Insight als Ihren End-to-End-Partner wählen?

Angesichts der rasanten technologischen Entwicklung ist Innovation der Schlüssel zum Erhalt der Wettbewerbsfähigkeit. Doch was ist der Schlüssel zur Innovation? Eine sichere Grundlage und das Vertrauen, Risiken eingehen zu können – in dem Wissen, dass Ihr Unternehmen, Ihre Mitarbeiter und Ihre Daten geschützt sind.

Unser Team aus Cybersicherheitsexperten bewertet die Auswirkungen Ihrer Geschäftsaktivitäten und findet maßgeschneiderte Lösungen für Ihre individuellen Bedürfnisse und Ziele. Wir bieten Ihnen branchenführendes Wissen und Erfahrung, um Sie bei der Bewältigung Ihrer komplexesten Sicherheitsherausforderungen zu unterstützen und eine solide, sichere Grundlage für Ihr Wachstum zu schaffen.

Insight hat die richtige Lösung für all Ihre Sicherheitsbedürfnisse.

Ist es an der Zeit, Ihre Sicherheitsstrategie neu zu bewerten?

Sprechen Sie mit einem unserer Experten und starten Sie noch heute.

Über Insight

Insight Enterprises, Inc. ist ein im Fortune 500 gelisteter Lösungsintegrator, der Unternehmen dabei unterstützt, ihre digitale Transformation zu beschleunigen, ihr Geschäft zu modernisieren und den Wert ihrer Technologie zu maximieren. Insights technische Expertise umfasst Cloud- und Edge-basierte Transformationslösungen mit globaler Skalierung und Optimierung. Sie basiert auf mehr als 35 Jahren enger Partnerschaften mit den weltweit führenden und aufstrebenden Technologieanbietern.

Insight®

at.insight.com | de.insight.com | ch.insight.com

[1] Insight and Foundry: An IDG, Inc. company. (2024). The Path to Digital Transformation: Where IT Leaders Stand in 2024. Insight-commissioned Foundry survey.

[2] Petrosyan, A. (2023, Aug. 31). Annual share of companies worldwide that paid ransom and recovered data from 2018 to 2023. Statista.

[3] IBM and Ponemon Institute. (July 2024). Cost of a Data Breach Report 2024. IBM.