

Microsoft Manage and Investigate Risk Value Insights

Mit unserer **Value Insights Methodik** zeigen unsere Experten Ihnen die Mehrwerte der eingebetteten Sicherheitslösungen Ihrer Microsoft Cloud Umgebung.



Im Leistungsumfang

Compliance Center:

- Insider Risk Management
- Communication Compliance
- Optional: Sensitive Information Types
- Optional: Data Loss Prevention

Nicht im Leistungsumfang

- Cloud-Dienste von Drittanbietern
- PoC oder Pilotierung
- Komponente Mensch und Prozesse



93%

aller Organisationen sind besorgt wegen "Insider-Risiken".¹

Für die meisten Unternehmen stehen **externe Cybersicherheitsrisiken** seit vielen Jahren an erster Stelle. Doch die Risiken, die von **vermeintlich vertrauenswürdigen "Insidern"** ausgehen, rücken mehr und mehr in den Fokus.

Unternehmen erkennen allmählich, wie wichtig es ist, Werkzeuge zu haben, die es ermöglichen Insider-Risiken schnell zu erkennen und zu bekämpfen.

Die Erkennung, Untersuchung und Reaktion auf böswillige, wie auch unbeabsichtigt schädliche Aktivitäten in Ihrem Unternehmen, ist entscheidend für die Gewährleistung von Vertrauen, die Schaffung eines sicheren Arbeitsplatzes und den Schutz von Unternehmenswerten.

Das Format **Manage and Investigate Risk Value Insights** vermittelt Ihnen die notwendigen Erkenntnisse, um Insider-Risiken in Ihrem Unternehmen zu verstehen und dagegen vorzugehen.

Microsoft Mehrwerte

Insider Risk Management

Microsoft Compliance Configuration Analyzer

Data Protection Baseline Assessment

¹ Insider Risk Management Microsoft Market Research January 2021

Microsoft Manage and Investigate Risk Value Insights



Was Sie erwartet

Der "User Risk Check" ist die Hauptaktivität des "Manage and Investigate Risk Value Insights" Formats. Die Aktivität erstreckt sich über mehrere Wochen, damit in Ihrer Cloud Infrastruktur genügend Informationen gesammelt werden können, um Insider-Risiken in Ihrem Unternehmen zu identifizieren.

Der User Risk Check nutzt automatisierte Microsoft 365-Tools und -Dienste zur Überwachung des Nutzerverhaltens und -Kommunikation, um unbeabsichtigt schädliches oder bösartiges Verhalten zu entdecken, das ein mögliches Risiko für Ihr Unternehmen darstellt.

Grober Zeitrahmen

Abgleich der Erwartungen, Abstimmen des Grobumfangs und der Zeitplanung, Formulieren Sie Ihre Ziele und Anforderungen zu sensiblen Daten.

Kick-Off, Konkretisieren des Umfangs und Einrichtung der relevanten Dienste in Ihrer Produktivumgebung: Insider Risk Discovery & Communication Compliance.



Der automatisierte Prozess sammelt und bewertet Informationen über:

- Datenlecks, versehentlich zu freigiebige Rechtevergabe, böswillige Absicht
- Datendiebstahl durch ausscheidende Mitarbeiter
- Unangemessene Kommunikation und beleidigende Sprache
- Sensible Informationen
- Interessenskonflikte

Analyse der Ergebnisse und Erstellen von Berichten.

Präsentation der Ergebnisse, Empfehlungen und Festlegen der nächsten gemeinsamen Schritte.

Value Insights Highlights

