sure[secure]

TREND MICRO
CLOUD CONFORMITY

LEISTUNGSBESCHREIBUNG

EINLEITUNG

Unternehmen dürfen sich angesichts immer größer werdender Cloud-Umgebungen nicht darauf verlassen, dass sich die jeweiligen Provider ausreichend um Themen der Informationssicherheit kümmern. Sie sollten immer auch eigene Maßnahmen zum Schutz Ihrer sensiblen Daten und Geschäftsprozesse ergreifen.

Cloud One Conformity ist eine Cloud-Anwendung von Trend Micro, die kontinuierliche Sicherheits-Compliance und Governance für Multi-Cloud-Umgebungen ermöglicht. Dazu gehören AWS, Azure und Google.

Diese Plattform bietet Echtzeittransparenz Ihrer Cloud-Infrastrukturen und ein Situationsbewusstsein für Ihre Regionen und Availability Zones über ein einziges Dashboard.

Sie bietet mehr als 1000 Konfigurationschecks für AWS, Azure und Google Cloud und benachrichtigt in Echtzeit über verschiedene Kanäle wie E-Mail, MS Teams, Slack, usw.

Automatisierte Konfigurationsscans laufen rund um die Uhr und prüfen Multi-Cloud-Umgebungen auf die Konformität verschiedener Standards wie GDPR, ISO 27001, HIPAA, CIS usw.

Die vorliegende Leistungsbeschreibung erläutert, wie wir Sie dabei unterstützen, Cloud One Conformity in Ihrer IT-Umgebung auszurollen und sinnvoll zu nutzen.

BESCHREIBUNG UNSERER TÄTIGKEITEN

Damit Sie die Trend Micro Cloud App Security in Ihrem Unternehmen sinnvoll und effizient nutzen können, unterstützen wir Sie in den folgenden Phasen:

Phase 1 – Interview über die aktuelle Situation

In der ersten Phase des Projekts werden Interviews geführt, um mehr Informationen über die folgenden Punkte zu erhalten:

- Aktueller Zustand Ihrer IT-Umgebung und Ihres Cloud-Ansatzes
- Welche Cloud Provider sind im Einsatz?
- Definition des gewünschten Zielzustandes unter Berücksichtigung von Rahmenbedingungen, Voraussetzungen, Zielen, Anforderungen und Erwartungen

Im Anschluss wird ein Plan zur Installation, Konfiguration und Aktivierung der Cloud One Conformity unter Berücksichtigung der gewonnen Erkenntnisse erstellt. Dieser Plan ist die Basis für die weiteren Phasen.

Phase 2 – Cloud-Konten zu Conformity hinzufügen

Cloud Conformity unterstützt mehrere Konten von den folgenden Cloud Providern:

- AWS-Konto
- Azure-Subscription
- GCP-Projekt

In dieser Phase werden alle erforderlichen Konten in Cloud One Conformity hinzugefügt.

Phase 3 – Aktivieren des Real Time Monitoring

Conformity Real-Time Threat Monitoring bietet Live-Überwachung mit sofortigen Warnmeldungen zu Bedrohungen und Maßnahmen für Aktivitäten und Ereignissen innerhalb Ihrer AWS- und Azure-Konten.
In dieser Phase aktivieren wir diesen Dienst.

Phase 4 – Erstellen von Profilen

Profile ermöglichen es Ihrem Unternehmen, Regeleinstellungen in wiederverwendbaren Vorlagen zu speichern und zu verwalten, beispielsweise Regeleinstellungen für einen bestimmten Cloud Provider, eine bestimmte Sicherheitsstufe oder eine bestimmte Anwendung.

In dieser Phase werden Profile für bestimmte Anwendungsfälle oder bestimmte Cloud Providers erstellt.
Die Schritte sind wie folgt:

- Erstellen eines Profils oder Auswahl eines bereits erstellten Profils
- Konfigurieren von Regeln innerhalb des Profils
- Deployment eines Profils auf ein Konto oder mehrere Konten

Phase 5 – Regeln und unerwünschte Überprüfungen

In dieser Phase werden die verschiedenen verwendeten Regeln konfiguriert und gegebenenfalls unerwünschte fehlgeschlagene Prüfungen unterdrückt.

Phase 6 – Einrichten von Kommunikationskanälen und Konfiguration von Benachrichtigungen

Cloud One Conformity bietet die Integration mit mehreren Kommunikations-Tools von Drittanbietern und den wichtigsten Ticketing-Systemen. Jedes dieser Tools kann so angepasst werden, dass mehrere Kanäle mit unterschiedlichen Triggern und Benachrichtigungseinstellungen entstehen, die sich in den Workflow Ihrer Organisation einfügen.
Diese Phase umfasst Folgendes:

- Konfigurieren der Kommunikationskanäle, die Sie in der Cloud One Conformity verwenden (E-Mail, MS Teams, Slack usw.)
- Konfiguration von automatischen Benachrichtigungen

Phase 7 – Geplante Berichte konfigurieren

In dieser Phase geht es um die Erstellung benutzerdefinierter geplanter Berichte für spezifische Anforderungen eines Managers, Teams oder Cloud-Administrators.

Phase 8 – Erste Bewertung des Sicherheitsniveaus

Diese Phase umfasst eine erste Bewertung Ihrer Cloud-Konten. Die Schritte sind:

- Erstellen eines Berichts zur Bewertung Ihrer aktuellen Sicherheitslage
- Erstellung eines Remediations Plan auf der Grundlage Ihres Berichts

Phase 9 – Monitoring und Finetuning

Nachdem das System in Betrieb genommen wurde, ist in den folgenden Wochen ein Monitoring/Finetuning erforderlich.

Dies kann Folgendes umfassen:

- Ändern von Profilen
- Hinzufügen neuer Profile oder Entfernen alter Profile
- Ändern von Regeln und Berichten
- Andere Finetuning-Aufgaben

IHRE BETEILIGUNG

Für eine erfolgreiche Implementierung von Cloud One Comformity in Ihrer IT-Umgebung ist eine Mitarbeit durch Sie und Ihre IT-Abteilung notwendig. Insbesondere benötigen wir:

- Cloud-Administratoren mit Admin-Rechten
- Administrativen Zugang zur Cloud One Konsole

Keine Sorge! Wir erklären Ihnen in unserem gemeinsamen Kickoff sowie in den weiteren Projektbesprechungen genau, was wir dazu von Ihnen brauchen.

ERGEBNISSE

Als Ergebnis des Projekts erhalten Sie Folgendes:

- Eine Cloud Security-Lösung, die geprüft, nach Best Practices konfiguriert und gemäß Ihren spezifischen Anforderungen optimiert worden ist
- Eine Dokumentation über alle Einstellungen und Profile im System

ANFRAGE SENDEN

KONTAKTIERT UNS

Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

kontakt@suresecure.de
www.suresecure.de

FOLGT UNS

/suresecure.de

/suresecure.de

/suresecure-gmbh