terreActive terreActive terreActive terreActive

Operation

Fact Sheet

SOC-Services für Microsoft Azure

Wir machen die Cloud für Sie sicher

Cyberattacken erkennen

Die Microsoft Azure Cloud bietet modernste Cyber-Defense-Komponenten, die das Security Operations Center der terreActive nutzt, um Cyberattacken zu erkennen und zu bekämpfen. Damit Sie sicher in der Cloud arbeiten können.

Microsoft Azure + Security

Immer mehr Clients und Server befinden sich in der Microsoft Azure Cloud. Auch für diese Infrastruktur muss die Sicherheit gewährleistet werden. Können Sie sich um alle SOC-Aufgaben selber kümmern? terreActive bietet auf Basis der Cyber-Defense-Komponenten von Azure eine sichere und einfache Lösung an. Wir übernehmen SOC-Aufgaben und unterstützen Sie in der Cloud.

Vorteile

- Einfaches Deployment des MDATP-Agents, der fixer Bestandteil des Betriebssystems Win10 ist.
- Wenn gewünscht, kann das SOC direkt auf dem Client intervenieren.
- Nebst EDR-Funktionalität bietet MDATP auch Vulnerability Management sowie Web Content Filtering an.
- Alle Komponenten der Cyber Defense Platform können kombiniert werden (Azure ATP, CloudApp Security, MDATP), was mit einfachen Mitteln eine umfassende Sicht ermöglicht.

Nur wer alles abdeckt, ist wirklich sicher

Eine gute Cyber Defense Platform als Grundlage eines SOCs umfasst alle Werkzeuge, die Engineers und Analysten für die Erkennung und Verteidigung benötigen. Die terreActive CDP orientiert sich an NIST (Nat. Institute of Standards and Technology). Mit der 360-Grad-Abdeckung über alle Stufen werden Angriffe frühzeitig erkannt und Bedrohungen eliminiert.

Security-Expertise von terreActive und baseVISION

Für wen eignet sich dieser SOC-Service?

Für alle Unternehmen, die bereits auf Microsoft setzen, vielleicht sogar schon über Lizenzen für Azure verfügen und ihren Mitarbeitenden das sichere Arbeiten in der Cloud ermöglichen möchten.

Microsoft

Microsoft Azure
... umfasst Clouddienste, die stetig erweitert werden, um Ihre Organisation bei geschäftlichen Herausforderungen zu unterstützen. Sie können Anwendungen mithilfe Ihrer bevorzugten Tools und Frameworks in einem grossen globalen Netzwerk erstellen, verwalten und bereitstellen.

Microsoft Azure Sentinel
... ist eine skalierbare, cloudbasierte Lösung für SIEM und SOAR, die mithilfe integrierter KI grosse Datenmengen schnell analysiert. Sentinel aggregiert Daten aus allen Quellen, einschliesslich Benutzern, Anwendungen, Servern und Geräten, die lokal oder in einer Cloud ausgeführt werden. Es bietet Sicherheitsanalysen, Bedrohungsinformationen, die proaktive Suche und die Reaktion auf Bedrohungen.

Microsoft Defender Advanced Threat Protection (MDATP)
... ist eine Komplettlösung für die Endpunktsicherheit, EDR. Es unterstützt die Prävention, Erkennung stattgefundener Angriffe, automatische Untersuchung und Reaktion auf Angriffe.

Wir sichern Ihren Erfolg.
www.terreActive.ch

Operation

Fact Sheet

Unser Partner baseVision

baseVISION hat im Bereich Security den höchsten Partnerschaftsstatus bei Microsoft erreicht. Mit 6 MS-Zertifizierungen «Best-in-Class» ausgezeichnet, verfügt das Unternehmen über ein fundiertes Fachwissen bei der Konzeption, Implementierung und Verwaltung von Sicherheitsstrategien.

baseVISION unterstützt Sie zusammen mit terreActive wenn es in den Phasen Identify und Protect darum geht, das richtig Mass an Schutz und die passenden Konfigurationen zu bestimmen.

baseVISION

www.basevision.ch

Umfassender Schutz in der Azure Cloud

Diese Leistungspakete stehen Ihnen zur Verfügung:

Identify (Informed)

- Vierteljährlicher Workshop um Neuigkeiten und Anpassungen der Microsoft Sicherheitslösungen zu besprechen
- E-Mail-Benachrichtigungen bei kritischen Produkt-Updates
- Know-how-Transfer der relevanten Informationen
- Roadmap für die Kundensicherheit

Protect (Prevent)

- Empfehlungen zur Verbesserung der Sicherheit
- Auditierung und Compliance-Berichterstattung von kritischen Sicherheitskonfigurations-Einstellungen
- Unterstützung bei der Pflege der sicheren IT-Infrastruktur
- Berichterstattung über Bedrohung und Verwundbarkeit der IT-Systeme (Threat & Vulnerability Management)

Detect

- Threat Intelligence & Vulnerability Discovery
- Threat Detection & Tuning
- Advanced Threat Hunting
- Reporting & Analysis

Respond

- Security Incident Management
- Incident Response (automatisiert mit SOAR)
- Forensische Analyse
- Erfahrungen fliessen zurück zwecks Verbesserung von Identify & Protect

Recover

- Automatisierte Wiederherstellungsprozesse (SOAR)
- Support für die Wiederherstellungsprozesse des Kunden

Kontakt
terreActive AG
Kasinostrasse 30
5001 Aarau
Tel. +41 62 834 00 55
info@terreActive.ch
www.terreActive.ch