Orange
Cyberdefense

Managed Threat Detection [log]

für Microsoft Sentinel

Bei Managed Threat Detection in der Cloud geht es darum, Ihre Umgebungen in Echtzeit zu überwachen und so zu reagieren, dass der Schaden für Ihr Unternehmen minimiert wird.

Chancen und Risiken der Cloud

Die Komplexität des Cybersecurity-Managements über eine vergrößerte Angriffsfläche wächst exponentiell mit der Beschleunigung der digitalen Transformation und der Einführung von Cloud-Diensten in Unternehmen. Die Sichtbarkeit und Verwaltung von Bedrohungen wie unbefugtem Zugriff, Account-Hijacking und verdächtigen Netzwerkaktivitäten wird in einer Cloud-Umgebung, die von den IT-Teams des Unternehmens weitgehend nicht verwaltet wird, immer schwieriger.

Als Alternative zur Rekrutierung eines Teams von Cloud-Sicherheitsspezialisten ermöglicht Orange Cyberdefense Unternehmen, die in Microsoft On-Premise- und Cloud-Technologien investieren, durch Managed Threat Detection für Microsoft Sentinel einen schnellen Return on Cybersecurity Investment.

Schütze die Cloud mit Microsoft Sentinel

Microsoft Sentinel ist eine Cloud-native SIEM-Plattform (Security Information Event Management) mit KI-gestützter Sicherheitsanalyse, die den erfahrenen Bedrohungsjägern von Orange Cyberdefense verwertbare Informationen zur Erkennung, Untersuchung und Behebung potenzieller Angriffs- und Kompromittierungsindikatoren bietet.

Die Spezialisten von Orange Cyberdefense stellen eine Verbindung zu Ihren wichtigsten Datenquellen her und sammeln die Protokolle, unabhängig davon, ob es sich um Benutzer, Anwendungen, Sicherheitsprodukte und/oder Endgeräte handelt, die vor Ort oder in Clouds von Drittanbietern ausgeführt werden. Sie analysieren die Sicherheitsereignisse Ihrer Microsoft Sentinel-Bereitstellung und werden so zu Ihrem Cybersecurity-Partner, der rund um die Uhr und 365 Tage im Jahr auf potenzielle Bedrohungen überwacht.

Warum Orange Cyberdefense?

Ihre Cloud-Erkennung und -Reaktion in den besten Händen:

- **Erkennungstechnik**
  Mit mehr als 10 Jahren Erfahrung im Bereich Managed Threat Detection bringt Orange Cyberdefense eine Fülle von Kenntnissen in die Sicherheitsplattformen von Microsoft ein, darunter Hunderte von ergänzenden Erkennungstechniken, die die inhärenten Erkennungsfunktionen des Produkts verbessern.
- **Bewährte Methodik**
  Ermitteln, visualisieren und verbessern Sie Ihre Erkennungsfähigkeiten mit unserem Threat Detection Framework und der Integration mit unserem umfangreichen Threat Intelligence Datalake.
- **Reichweite der Antworten**
  Profitieren Sie von einer breiten Palette an Response-Services. Ergänzen Sie Ihre eigenen Fähigkeiten auf optimale Weise.
- **Erfahrung und Expertise**
  Globale Fähigkeiten, mehr als 150 Analysten, die CyberSOC-Dienste anbieten 24x7x365 zu Ihrer Verfügung
- **Sicherheit und Partnerschaft**
  Unsere Teams vor Ort arbeiten eng mit unseren Kunden zusammen, um die Erkennungs- und Reaktionsmöglichkeiten kontinuierlich zu verbessern.
- Orange Cyberdefense ist Mitglied der **Microsoft Intelligent Security Association (MISA)**.

Finden Sie mehr über Managed Detection and Response (MDR) heraus:
orangecyberdefense.com/de/services/detect-respond

Vorteile:

Vollständige Erkennungstransparenz: Gewinnen Sie Einblicke in interne, Cloud- und SaaS-Umgebungen, um Cybersecurity-Bedrohungen zu erkennen.

Intelligenzgestützte Sicherheit: Wir investieren viel in Forschung und Entwicklung, um die neuesten Taktiken, Techniken und Verfahren zu erkennen und darauf zu reagieren.

Aktive Reaktion: Eine breite Palette aktiver Reaktionsmöglichkeiten steht rund um die Uhr zur Verfügung, um Ihre Sicherheitsanforderungen zu erfüllen.

Spare Zeit und Geld: Wir verwenden innovative Techniken, um sicherzustellen, dass Vorfälle im Zusammenhang untersucht werden und der Lärm so weit wie möglich reduziert wird.

Intelligente Erkennung

Die Herausforderung bei der Erkennung besteht darin, dass es nicht nur eine Art von Technologie gibt, die alle Erkennungsanforderungen erfüllt. Es gibt Optionen für die Erkennung von Protokolldaten, Netzwerkdaten und Endpunktdaten.

Es gibt Bedrohungen, die sich außerhalb Ihrer Infrastruktur abspielen und ein Risiko für Ihr Unternehmen darstellen können, das erkannt werden muss. Sie können wahrscheinlich nicht alle Probleme gleichzeitig lösen, aber Sie können einen Sicherheitspartner mit einem kompletten MDR-Portfolio wählen, der Sie zu den besten Investitionen führen kann.

Orange Cyberdefense bietet ein umfassendes Erkennungsportfolio, das nicht nur den SOC-Dreiklang aus Protokoll, Netzwerk und Endpunkt abdeckt, sondern auch die Erkennung von Bedrohungen für Ihr Unternehmen im Open, Deep und Dark Web. Sie können mit der Lösung beginnen, die für Ihren aktuellen Bedarf am relevantesten ist, und diese dann je nach Bedarf erweitern.

Unser Intelligence Datalake zieht Bedrohungsdaten aus unseren verschiedenen Diensten und unserem globalen Kundenstamm ein und gibt sie weiter, so dass wir sowohl eine globale als auch eine lokale Perspektive bei der Erkennung von anormalem Verhalten bieten können.

Wir haben für Sie vorgesorgt!

Die MDR-Dienste von Orange Cyberdefense sind modular aufgebaut, und ein Kunde kann eine oder mehrere dieser Komponenten auswählen, je nach seinen eigenen Ressourcen - oder, was noch wichtiger ist, wo Orange Cyberdefense die Lücken effektiv schließen kann, wenn diese Ressourcen nicht vorhanden sind.

Sobald Sie Ihren Managed Threat Detection Service eingerichtet haben, kann dieser mit dem Reaktionsdienst kombiniert werden, den Sie benötigen, um Ihre eigenen Fähigkeiten zu vervollständigen.

Alle Dienste werden von unserem globalen Netzwerk aus 18 SOCs und 14 CyberSOCs unterstützt, die rund um die Uhr den Bildschirm im Blick haben, sowie von unseren international anerkannten CERT-Teams, die Mitglied bei CREST, TF-CSIRT und FIRST sind.

Was auch immer Ihre Bedürfnisse im Bereich der Reaktion sind, unsere Managed Threat Response-Dienste ergänzen und erweitern Ihre Fähigkeiten nach Bedarf. Wir helfen dabei, Bedrohungen einzudämmen, bevor sie langfristigen Schaden anrichten, während unsere Incident Response Retainer und Digital Forensics Services Ihnen bei Bedarf Zugang zu einem der größten und kompetentesten CSIRTs bieten.

Intelligence-led MDR: Vorteile

Orange Cyberdefense
Intelligence Datalake

- Erkenntnisse aus MDR-, CERT- und CSIRT-Einsätzen
- Externe Intelligenz
- Zusammenarbeit mit Strafverfolgung
- Interne F&E

Interne Aktivitäten

- Detection of suspicious actitivities
- Analyzing and classifying incidents
- Notification and reporting

Bessere Erkennung

- Fortgeschrittene Kenntnisse über IoCs
- Frühzeitige Erkennung von großen Kampagnen
- Überlegene Analyse und Korrelation
- Rauschen und Fehler-Filterung
- 24x7 CyberSOC

Bessere Reaktion

- Schnellere Verfolgung der Vorfallursache
- Schnellere Erkennung von Angriffsvektoren
- Schnelle Eindämmung und Forensik
- 24x7 CSIRT