Orange
Cyberdefense

Managed Threat Detection [network]

für Microsoft Office 365

Erkennen und entschärfen Sie Angriffe auf Office 365 und Azure AD, bevor sie Schaden anrichten

Eine großartige Cloud-basierte Produktivitätssuite, aber auch lukrativ für Angreifer

Office 365 dominiert heute den Arbeitsbereich von Unternehmen mit über 250 Millionen aktiven Nutzern pro Monat. Für viele Unternehmen basieren die gemeinsame Nutzung, Kommunikation und Speicherung von Daten auf Office 365, was es zu einem unglaublich attraktiven Ziel für Cyberkriminelle macht.

Es ist also keine Überraschung, dass Office 365 für Orange Cyberdefense die zweitgrösste Quelle von Incident Response Fällen ist (nach Ransomware).

Das große Risiko der Kontoübernahme

Nach der Kompromittierung eines Kontos können Angreifer problemlos zwischen Cloud-Anwendungen und Dienstanbietern innerhalb Ihrer hybriden Umgebung wechseln.

Die Auswirkungen können sich schnell verstärken, da die Angreifer das kompromittierte Konto nutzen, um ernsthaften Schaden anzurichten.

Deshalb ist es so wichtig, diese Art von potenziell verheerenden Cyberangriffen zu verhindern.

Managed Threat Detection [network] für Office 365 unterstützt Sie bei der Aufrechterhaltung Ihrer Microsoft 365-Sicherheitslage und -Hygiene.

- **Verbesserter Einblick in potenzielle Bedrohungen**
- **Schnelle Erkennung und Reaktion**
- **Sichere Einführung in die Cloud**

Warum Orange Cyberdefense?

Verschaffen Sie sich einen zentralen Überblick über Cybersecurity-Risiken in Ihrem Microsoft 365-Ökosystem:

- **Intelligenzgesteuerter Ansatz**
  Unsere einzigartigen Bedrohungsdaten aus über 500 privaten und öffentlichen Quellen gehen über die Indikatoren für eine Gefährdung hinaus und bieten aggregierte Daten und Einblicke aus globalen Operationen, Ethical Hacking und der Überwachung digitaler Risiken.
- **Erweiterte Möglichkeiten**
  18 SOCs, 14 CyberSOCs, um Ihren Anforderungen gerecht zu werden, mit mehr als 150 Analysten, die 24x7x365 Erkennungs- und Reaktionsdienste bereitstellen.
- **Antwortumfang**
  Profitieren Sie von der breitesten Palette an Reaktionsmöglichkeiten, einschließlich umfassender Erfahrung im Umgang mit Office 365-Verletzungen. Ergänzen Sie Ihre eigenen Fähigkeiten auf optimale Weise.
- **Zukunftssicher**
  Die Integration mit anderen Orange Cyberdefense MDR-Funktionen ermöglicht es Ihnen, den Dienst entsprechend Ihren aktuellen und zukünftigen Anforderungen zu erweitern.
- **Ergebnisorientierte Bereitstellung**
  Wir bieten 24x7 Echtzeit-Transparenz und Kontrolle über die verschiedenen Aspekte des Dienstes.
- Orange Cyberdefense ist ein Mitglied der **Microsoft Intelligent Security Association (MISA)**.

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

Vorteile:

Vollständige Erkennungssichtbarkeit: Detaillierte Analyse Ihres gesamten Office 365-Ökosystems (Sharepoint, One Drive, Microsoft Suite...) und Ihrer Azure AD-Konten.

Erhöhung der Widerstandsfähigkeit gegen Eindringlinge durch Hintertüren: Überwachung auf Zero-Day-Angriffe auf der Grundlage des Verhaltens, keine Anwendungsfälle, Signaturen oder umfangreichen Regeln erforderlich

Schnelle Wertschöpfung: Einfach zu implementierender Dienst, der mit Ihren bestehenden Sicherheitslösungen zusammenarbeitet.

Ungewöhnliches Verhalten in Echtzeit erkennen: Identifizierung und Eindämmung kompromittierter Office 365- und Azure AD-Konten sowie böswilliger Insider anhand ihres Verhaltens

KI-gesteuerte Lösung: Automatische Analyse von Vorfällen mit Priorisierung der Bedrohungen, auf die man sich im Moment konzentrieren muss

Zeit und Geld sparen: Skalierung der Sicherheitsbemühungen, ohne Ressourcen zu verbrauchen

Herausforderungen

- 24x7 CyberSOC-Abdeckung erforderlich - Office 365 ist eine Ressource, die rund um die Uhr ausgenutzt werden kann
- Kontinuierliche Verwaltung und Abstimmung der Überwachung, um sicherzustellen, dass den Analysten genügend Kontext zur Verfügung gestellt wird, ohne dass eine “Warnmüdigkeit” entsteht
- Anwendung globaler Erkenntnisse auf Bedrohungen der Cybersicherheit

Was tun wir?

- Einsatz der Vectra-Plattform
- Plattformverwaltung von Vectra Cognito Detect™
- Kontinuierliche Triage, Analyse und Priorisierung von Vorfällen durch Sicherheitsanalysten
- Managed Threat Response zur Isolierung und Sperrung gefährdeter Konten

Wann sollten Sie es in Betracht ziehen?

- Wenn Sie Experten benötigen, die Sie bei der Einrichtung und dem Betrieb eines anspruchsvollen Erkennungs- und Reaktionsdienstes unterstützen
- Wenn Sie einen Anbieter benötigen, der nicht nur Netzwerkerkennung, sondern auch protokoll- und endpunktbasierte Überwachung sowie umsetzbare Cyber Threat Intelligence bietet
- Wenn Sie zusätzliche Managed Threat Response-Funktionen rund um die Uhr benötigen

Was werden Sie bekommen?

- Vollständig verwalteter Plattformbetrieb
- Echtzeitanalyse von Vorfällen und Alarmierung
- Monatliche Berichterstattung
- Optionale Jagd auf Cyber-Bedrohungen
- Optional Managed Threat Response

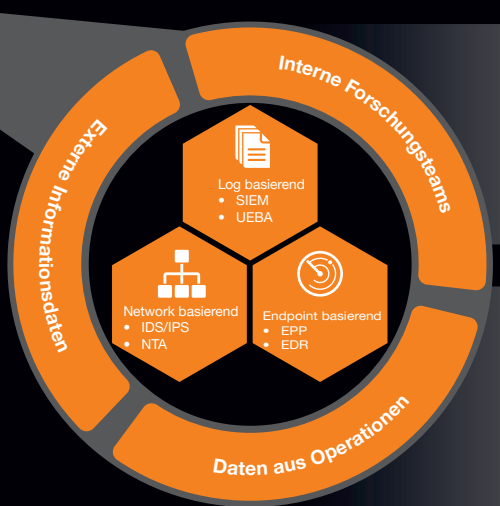
Intelligenzbasierte MDR: Vorteile

Orange Cyberdefense
Intelligence Datalake

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

Interne Aktivitäten

- Aufdeckung verdächtiger Handlungen
- Analyse und Klassifizierung von Vorfällen
- Benachrichtigung und Berichterstattung



Bessere Erkennung

- Fortgeschrittene Kenntnisse von IoCs
- Frühzeitige Erkennung von großen Kampagnen
- Überlegene Analyse und Korrelation
- Effiziente Filterung von “Rauschen” und falsch-positiven Ergebnissen
- 24x7 CyberSOC

Bessere Reaktion

- Schnellere Verfolgung der Ursachen von Vorfällen
- Schnellere Erkennung von Angriffsvektoren
- Schnelle Eindämmung & Forensik
- 24x7 CSIRT

Build a safer digital society

www.orangecyberdefense.com