Orange
Cyberdefense

# Managed Threat Detection [xdr]

## for Microsoft 365 Defender

**Ein allumfassender Service, der Security Incident Management, Remote Response, Threat Hunting, angepasste Rules und Threat Intelligence für alle Microsoft 365 Defender-Module bietet.**

### Ein Intelligence-led service für eine sich ständig ändernde Umgebung

**Microsoft 365 Defender hat den Markt für XDR (erweiterte Detection and Response) auf den den Kopf gestellt. Eingebunden in die Struktur des Micro-soft-Ökosystems ermöglichen die Funktionen von Microsoft 365 Defender es Unternehmen, schnell Einblick in die häufigsten Bedrohungen zu erhalten und Maßnahmen zu ergreifen. Um aus dieser Investition Kapital zu schlagen, muss sie von starken Prozessen und qualifizierten Security-Analysten begleitet werden.**

Aktivitäten wie die Untersuchung von Security Incidents, die Suche nach Bedrohungen, Threat Intelligence, die Entwicklung individueller Erkennungsmethoden und die Eindämmung von Vorfällen erfordern ein gewisses Maß an Erfahrung und Automatisierung, um die Menge an Ereignissen zu bewältigen, die von Defender über Endpoints, Office365, Active Directory und die Überwachung von Cloud-Anwendungen erzeugt werden.

### Lösung

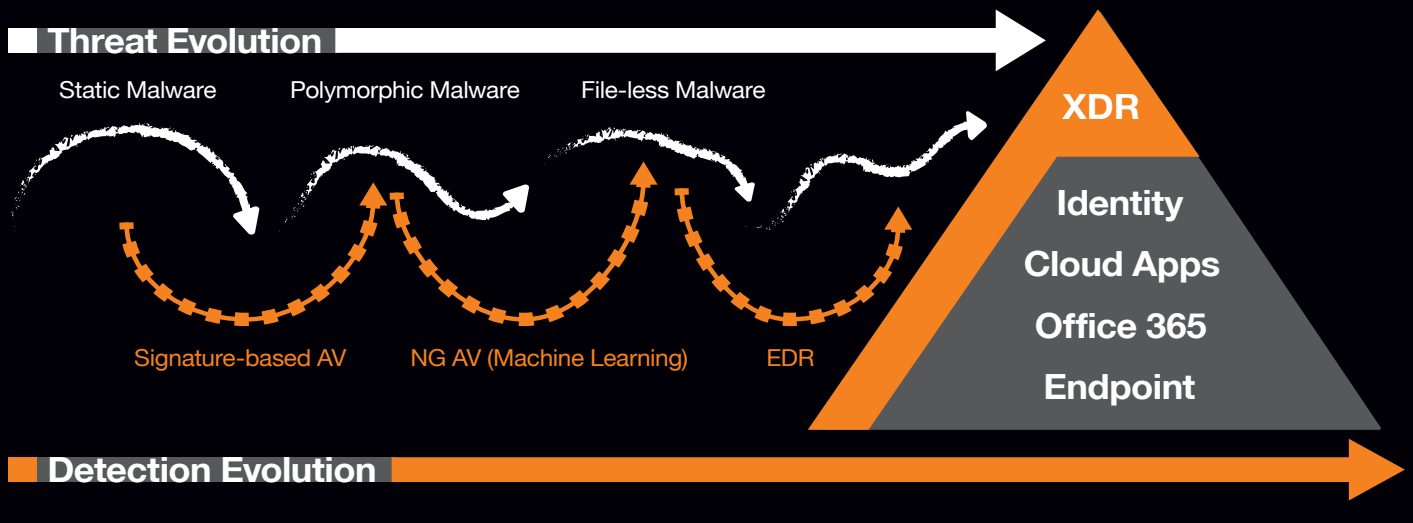
Um diese Herausforderungen zu bewältigen, bietet Orange Cyberdefense einen Managed Detection and Response Service an, der auf dem XDR-Stack (Extended Detection and Response) von Microsoft 365 Defender basiert und in unsere Core Fusion-Plattform einfließt, die zur Verbesserung, Anreicherung und Verwaltung der Warnmeldungen in unseren MDR-Services verwendet wird. Dies ermöglicht es Unternehmen, Microsoft 365 Defender zu nutzen, die Erfahrung von Orange Cyberdefense zu nutzen und drastisch zu skalieren, indem Tausende von Clients und Identitäten sowie deren Nutzung von Office365 und anderen Cloud-Anwendungen überwacht werden.

### Service Overview

Managed Threat Detection [xdr] ist ein abonnementbasierter Service, der Unternehmen, die Microsoft 365 Defender nutzen, rund um die Uhr die Möglichkeit bietet, Vorfälle zu bearbeiten, sie mit Bedrohungsdaten und menschlichen Analysen anzureichern und bei Bedarf Reaktionsmaßnahmen zu ergreifen.
Hochwertige Services wie Threat Hunting, Threat Intelligence und benutzerdefinierte Erkennungsregeln sind ebenfalls enthalten. Sie decken fortschrittliche Bedrohungen wie Ransomware und APTs ab und verbessern den Service kontinuierlich, um mit den sich schnell entwickelnden Bedrohungen Schritt zu halten.

## Erweiterte Detection und Response (XDR)

### Unsere Antwort auf eine sich wandelnde Bedrohung für alle 4 Microsoft-Lösungen



**Erfahren Sie mehr darüber, wie die visibility & detection Erfahren Sie mehr darüber, wie die:** https://admin2.orangecyberdefense.com/global/all-services/operate-support/managed-threat-detection-xdr-for-microsoft-365-defender

## Wann sollten Sie es in Betracht ziehen?

- Wenn Sie Experten benötigen, die Sie bei der Bereitstellung und Ausführung eines ergebnisbasierten verwalteten Erkennungs- und Reaktionsdienstes für alle Ihre Microsoft 365 Defender-Module unterstützen
- Wenn Sie 24x7 Managed Threat Detection benötigen
- Wenn Sie einen Anbieter benötigen, der nicht nur Managed Detection and Response anbietet, sondern auch umfassende Cyber Threat Intelligence einschließt, die mehr bietet als das, was "out-of-the-box" verfügbar ist

## Was tun wir?

- **Security incident Management**: Triage von Warnmeldungen, Analyse und Priorisierung, Benachrichtigung und Berichterstattung
- **Always-on Monitoring** alle aktiven Micro-soft 365 Defender-Module und -Analysten zu kreuzen, die rund um die Uhr einsatzbereit sind, um sicherzustellen, dass Vorfälle eingedämmt werden
- **Kontinuierliche Verbesserung** und Abstimmung des Service, um mit der Bedrohung Schritt zu halten und sich an Ihre Umgebung anzupassen
- **Threat Hunting** indem wir unsere globale Intelligenz mit dem vorhandenen Wissen über Ihre lokale Umgebung kombinieren, um fortschrittliche Bedrohungen aufzuspüren
- **Integration der einzigartigen Orange Cyberdefense Threat Intelligence**, die die Microsoft-Lösung noch leistungsfähiger macht

## Was bekommen Sie?

- **Ein erfahrenes Team,** das sich um die Sicherheitsvorfälle kümmert, die von Ihrem Microsoft 365 Defender-Mieter generiert werden, arbeitet rund um die Uhr, 365 Tage im Jahr.
- **Ein ernannter Service Delivery Manager**, der sicherstellt, dass wir konsistent und auf hohem Niveau liefern
- **Security incident metrics und trending post-analysis**, damit Sie verstehen, was wirklich in Ihrem Unternehmen passiert und welche Art und Geschwindigkeit von Bedrohungen wir sehen
- Nicht nur Erkennung, sondern auch **incident containment** und Nutzung der in Microsoft 365 Defender verfügbaren Abhilfemöglichkeiten
- **Ständig verbesserte Erkennungsfunktionen** mit benutzerdefinierten Erkennungsregeln, Bedrohungssuche und Orange Cyberdefense Threat Intelligence
- Ein **vertrauenswürdiger Partner** mit einer starken Service-Governance und starken SLAs

## Welchen Wert bringen wir mit Microsoft?

Mehr als 130 von Microsoft zertifizierte Experten und über 2.700 Cybersecurity-Experten

Mehr als 8.500 Kunden weltweit

Mitglied der Microsoft Intelligence Security Association (MISA)

Repräsentativer Anbieter in den Gartner Market Guides für MDR, Threat Intelligence und Managed Security Services

Akkreditierte Microsoft Solution Partner Security

Ein ganzes Ökosystem verwalteter Services zur anticipate, identify, protect, detect und respond auf cyber security threats

## Threat Forschung und Aufklärung sind Teil unserer DNA

**Mit Hilfe unserer 13 globalen CyberSOCs, jahrelanger Erfahrung und einer umfangreichen Threat Intelligence-Datenbank erkennt Orange Cyberdefense rund um die Uhr Bedrohungen und reagiert darauf. Dabei arbeiten wir kontinuierlich mit unseren Kunden zusammen, um sicherzustellen, dass wir unsere Überwachung verstehen und an den Kontext ihrer sich ständig verändernden Umgebung anpassen.**