Managed Threat Detection [xdr]

for Microsoft Defender XDR

An all-in-one service providing security incident management and posture enhancement across all Microsoft Defender XDR modules.

An Intelligence-led service for an ever-changing environment

Microsoft Defender XDR has turned the XDR (extended detection and response) market on its head. Embedded into the fabric of the Microsoft ecosystem, the capabilities of Microsoft Defender XDR are rapidly enabling organizations to get visibility of the most common threats and to take action. In order to capitalize on this investment it needs to be accompanied by strong processes and skilled security analysts.

Activities such as security incident investigation, threat intelligence, threat hunting, detection engineering, incident response and posture enhancement require a certain amount of experience and automation to face the volume of events and recommandations generated by Defender XDR across endpoints, Office365, Entra ID, and cloud applications and cloud resources.

Solution

To address these challenges, Orange Cyberdefense offers a Managed Detection and Response service based on the XDR [extended detection and response] stack of Microsoft

Defender XDR feeding into our Core Fusion platform, used to enhance, enrich and manage the alerts across our MDR services.

This will allow businesses to capitalize on Microsoft Defender XDR, leveraging Orange Cyberdefense experience and scale drastically by monitoring thousands of clients and identities, and their usage of Office365 and other cloud applications.
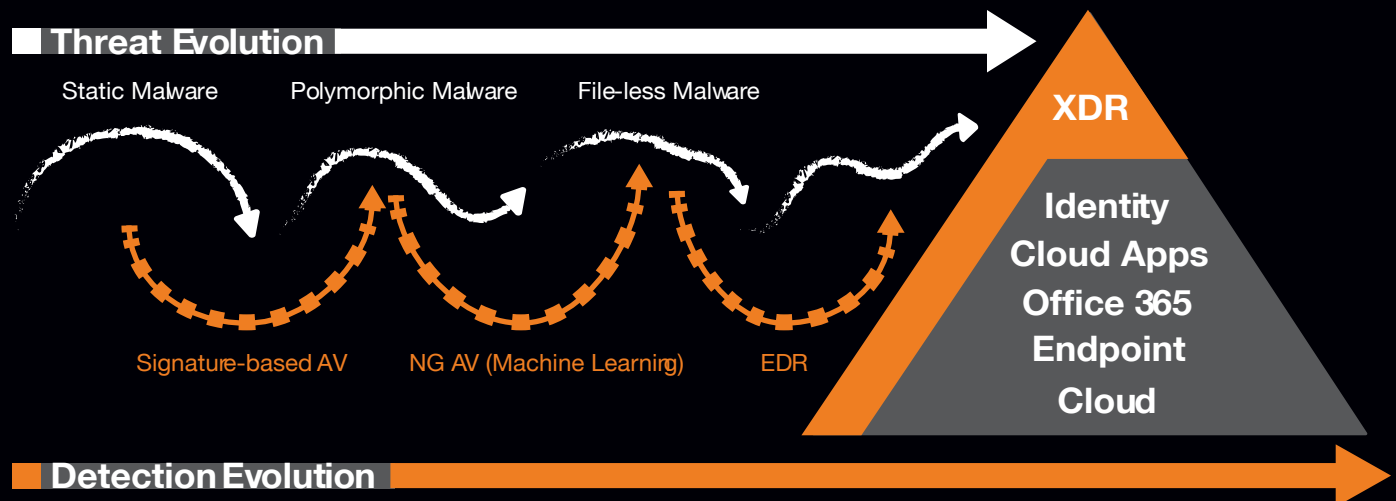
Service Overview

Managed Threat Detection [xdr] is a subscription-based service that provides businesses using Microsoft Defender XDR with a 24x7 capability to handle incidents, enrich them with threat intelligence and human analysis, and to take response actions where needed.

High value services like threat hunting, threat intelligence and custom detection rules are also included. They provide a coverage of advanced threats like ransomware and APTs while continuously improving the detection accuracy and enhancing the posture management of customers service to keep up with the fast pace of evolving threats.

Extended Detection and Response (XDR)

Our response to an evolving threat across all 5 Microsoft solutions

Threat Evolution

Static Malware   Polymorphic Malware   File-less Malware

XDR

Identity
Cloud Apps
Office 365
Endpoint
Cloud

Signature-based AV   NG AV (Machine Learning)   EDR

Detection Evolution

When should you consider it?

- If you require experts to help deploy and run an outcome-based managed detection and response service on all your Microsoft Defender XDR modules

- If you require 24x7 managed threat detection

- If you require a provider that not only provides Managed Detection and Response but also manage the enhancement of you security posture.

What do we do?

- **Security incident management**: triage of alerts, analysis and prioritization, notification and reporting

- **Always-on monitoring** across all your active Microsoft Defender XDR modules and analysts ready to take action 24x7 to ensure incidents are contained

- **Continuous improvement** and tuning of the service to keep up with the threat and adapt to your environment

- **Threat Hunting** by combining our global intelligence with existing knowledge of your local environment to seek out advanced threats

- **Integration of Orange Cyberdefense unique Threat Intelligence**, supercharging the Microsoft solution to do more

- **Enhancement of you security posture**

What will you get?

- **An experienced team** handling the security incidents generated by your Microsoft Defender XDR tenant, working 24x7, 365 days a year

- **An appointed Service Delivery Manager** to ensure we deliver consistently and to a high standard

- **Security incident metrics and trending post-analysis**, to help you understand what is really happening in your business and what type and velocity of threats we are seeing

- Not just detection but **incident containment** and use of the remediation options available within Microsoft Defender XDR

- **Constantly improved detection capabilities** with custom detection rules, threat hunting and Orange Cyberdefense threat intelligence

- A **trusted partner** with strong service governance and strong SLAs

- **A roadmap of your security posture improvement**

What value do we bring with Microsoft?

Microsoft Verified Managed XDR Solution

- More than 130 Microsoft certified experts and over 3,000 cybersecurity professionals

- More than 8,700 customers worldwide

- Representative vendor in the Gartner Market Guides for MDR, Threat Intelligence and Managed Security Services

- Member of Microsoft Intelligence Security Association (MISA) with a Microsoft-verified-MXDR solution badge

- Accredited Microsoft solution partner security

- An entire ecosystem of managed services to anticipate, identify, protect, detect and respond to cyber security threats

Threat research and intelligence are part of our DNA

Drawing on our 14 global CyberSOCs, years of experience and a vast Threat Intelligence database, Orange Cyberdefense detects and responds to threats 24x7, continuously working with our customers to ensure that we understand and adapt our monitoring to the context of their ever-changing environment.

Build a safer digital society

www.orangecyberdefense.com