Orange
Cyberdefense

Managed Threat Detection

XDR

Improve visibility & detection accuracy. Simply and quickly.

Threat evolution versus threat detection has been a continuing back and forth battle. What started with blocking static malware using signature-based anti-virus, soon evolved into using next-generation anti-virus. Taking more of a machine learning approach as malware authors started to use more advanced, polymorphic techniques. But even advanced behavioral detection techniques do not catch everything. As such, endpoint detection and response solutions became more popular in the market. And yet not only endpoints are affected.

For the most complete visibility within threat detection, visibility of security data from endpoints, network traffic and selected log data with the ability to integrate this data, can give you a fast path towards a complete and accurate incident detection and response strategy.

Businesses need a complete centralized solution that can collect the most valuable security data from networks, endpoints, and cloud environments, with the ability to conduct holistic detection and response actions.

Solution

To address these challenges, Orange Cyberdefense offers a Managed Threat Detection Service based on XDR [extended detection and response] that is fully installed, supervised, and maintained by Orange Cyberdefense.

The solution utilises Palo Alto Cortex XDR to provide a single platform to feed security event data into the Service, run by the Orange Cyberdefense CyberSOC.

Service Overview

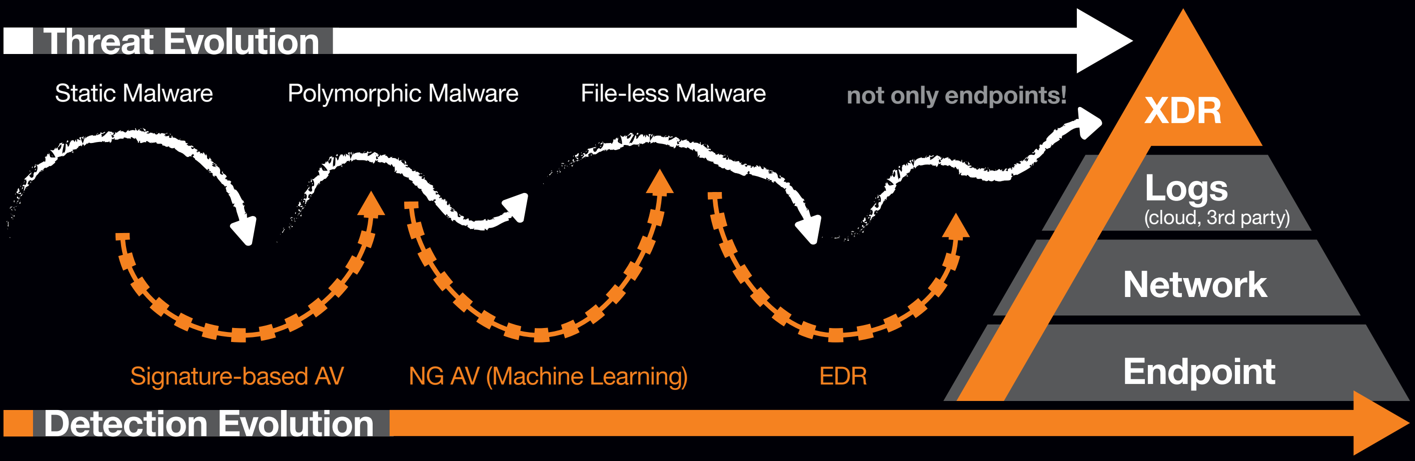
Managed Threat Detection [XDR] is a subscription service that provides detection, triage, classification, and incident notifications based on detected incidents provided from our customers' IT environments.

XDR provides a platform that integrates endpoint, network, and cloud data to stop sophisticated attacks. It unifies this data in one platform that then plugs into Orange Cyberdefense's Cyber Fusion center, where security analysts handle those XDR generated security incidents 24x7, providing initial triage, analysis and escalation, as well as being able to utilize the XDR platform to conduct active response.

Managed Threat Detection [xdr] provides 24x7 capability to detect and contain threats by preventing compromised machines from communicating with any other internal or external device and thereby reducing an attacker's mobility on your network & restricting access to only Orange Cyberdefense analysts for situations when a deeper examination is required. Multiple response actions can be performed like isolating an endpoint or searching & destroying malicious files.

Extended Detection and Response (XDR)

Your response to an evolving threat landscape



Find out more on how to improve visibility & detection:
orangecyberdefense.com/global/mdr/

Complete visibility on one dashboard:

- Quick installation
- Unified platform for improved protection, detection, and response (XDR)

Save time & costs:

- CyberSOC teams provide security analysts & platform expertise as a service 24/7

Added value services:

- Initial tuning of detection rules
- Managed threat Response
- Integration with our threat intelligence datalake

Integrated response:

- Restore hosts to a clean state
- Get over an attack by removing malicious files and fast recovery

When should you consider it?

- If you require experts to help deploy and run an outcome-based managed detection and response service based on XDR.
- If you require 24x7 or 8x5 managed threat detection
- If you require a provider that not only provides Managed Detection and Response but also comprehensive Cyber Threat Intelligence
- If you require additional active response capabilities 24x7

What do we do?

- Deployment and management of the Palo Alto Networks Cortex XDR platform
- Initial & continuous tuning of detection rules
- 24x7x365 incident triage, analysis, and prioritization by well trained security analysts
- Managed Threat Response such as isolation of infected endpoints
- Integration of Orange Cyberdefense unique Threat Intelligence Datalake

What will you get?

- Fully managed platform operations
- Real-time incident analysis and endpoint active response
- Monthly strategic reporting
- Integration with Orange Cyberdefense Threat Intelligence
- Optional Cyber Threat Hunting [Included in Premium service]
- Continuous management of XDR configuration to ensure enough context for analysts without producing "alert fatigue"

Intelligence-led security

Drawing on our 11 global CyberSOCs, years of experience and a vast Threat Intelligence Datalake, 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