Orange Cyberdefense

Managed Threat Detection

Endpoint

Visibility across the enterprise is key and the endpoint is the quickest way to get it.

There is no such thing as 100% protection. Once you have accepted this fact it is time to implement a strategy on how to detect the threats you couldn't prevent. The challenge with detection is that today's threats are not using old malware that is easy to detect and remediate.

77%* of successful attacks used file-less malware that traditional security tools could not prevent. Since detection of file less malware and similar types of advanced attacks cannot be done with the help of static rules or signatures, you need the ability for behavior anomaly detections on the endpoint.

This behavior needs to be analyzed and correlated across other endpoints to be able to separate the false positives from the real incidents. Without the right tools and competences this can take a very long time. Once the investigation phase is complete, any critical incident will most likely also require rapid response actions. The time from compromise, to detection, to remediation takes too long, greatly increasing costs and damage that could have been avoided.

* Ponemon 2018 Endpoint Security Statistics Trends

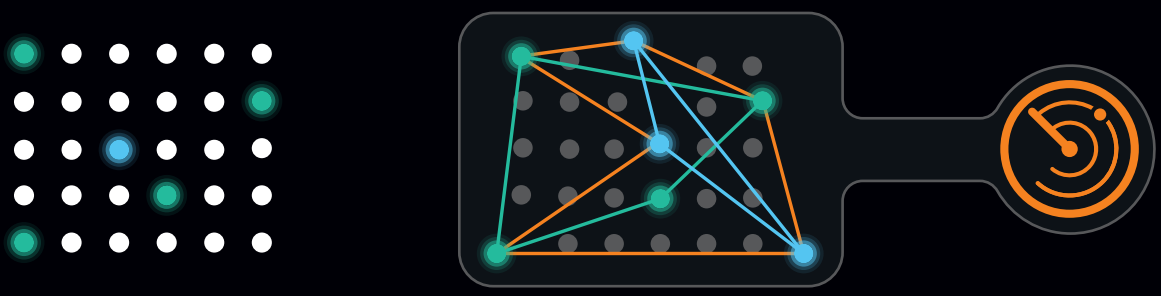
Service Overview

The Managed Threat Detection [Endpoint] service is a managed detection and response service (MDR) based on endpoint detection and response technology (EDR). By deploying low impact sensors on the endpoints, behavior data is collected, enriched, and correlated across all endpoints with the help of an AI hunting engine and a massive in-memory graph database. By doing up to 8 million correlations per second, the performance against other detection toolsets is unparalleled.

This provides detection abilities far beyond that which traditional signature or rule-based endpoint platforms can demonstrate. The challenge however is that the detections are not as simple as a "block or allow" process. In most cases it requires manual work from a skilled analyst to verify and classify the incident. This is where the Orange Cyberdefense CyberSOCs come in.

Drawing on our 11 global CyberSOCs, years of experience and a vast Threat Intelligence Datalake, Orange Cyberdefense detects and responds to endpoint threats 24x7, continuously working with our customers to ensure that we understand and adapt our endpoint monitoring to their ever-changing endpoint environment.

What you want from Endpoint Detection and Response is a solution that helps you correlate events across machines as well as on machines themselves to push alerting speed and precision to a new level and at the same time give an enterprise-wide view.



Isolated endpoint detection

- Data is **stored on disk**
- Data analysis is **manual**
- Generates **redundant alerts**
- One alert for **each affected machine**

Managed endpoint detection

- Data **remains in memory**
- Data is **enriched and correlated**
- Aggregates **the whole attack**
- One alert for **all affected machines**

› **Very fast query results**
› **Shorter time to understanding**
› **Reduction of alert fatigue**
› **Full scope of incidents**

Find out more on how to protect your endpoints on:
orangecyberdefense.com/global/endpoint/

Comprehensive endpoint visibility
Endpoint detection based on cross-machine correlation provides a strong foundation for continuous security analysis and enterprise-wide coverage.

Advanced analysis and hunting: Detailed and enriched detection context providing fast and effective analysis. continuously tuned.

Highly skilled Security Analysts with the ability to query a huge set of endpoint telemetry.

Quick time to value: CyberSOC provides security analysts and platform expertise as a service, giving you rapid deployment and strong, proven processes.

Rapid response: Security Analysts on hand 24x7 to isolate threats and limit the impact of breaches.

Challenges

- Lack of resources to staff your Security Operations Center 24x7
- Continuous management of EDR configuration to ensure enough context for analysts without producing “alert fatigue”.
- Applying global intelligence to cyber security threats

When should you consider it?

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

What do we do?

- Deployment of the Cybereason platform
- Platform management of Cybereason EDR
- Continuous incident triage, analysis, and prioritization by security analysts
- Managed Threat Response such as isolation of infected endpoints
- Integration of Orange Cyberdefense unique Threat Intelligence Datalake and custom EDR rules (Premium)

What will you get?

- Fully Managed Platform operations
- Real-time incident analysis and endpoint active response
- Monthly reporting
- Optional Cyber Threat Hunting

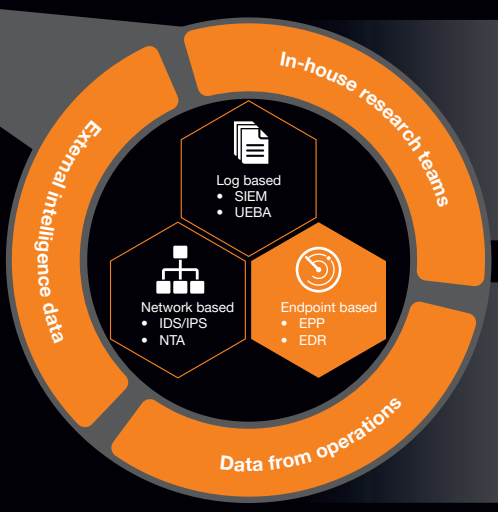
Intelligence-led endpoint detection: Benefits

Orange Cyberdefense
Intelligence Backbone

- Intelligence from MDR, CERT, CSIRT operations
- External intelligence
- Collaboration with law enforcement
- In-house R&D

Internal activities

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



Better endpoint detection

- Advanced knowledge of IoCs
- Identification of legitimate processess, which might have been compromised anyway (e.g. through supply chain)
- Severity classification
- Anticipation and early detection of major campaigns
- Superior analysis & correlation
- Efficient filtering of “noise” and false-positives
- 24x7 CyberSOC

Build a safer digital society

www.orangecyberdefense.com