Orange
Cyberdefense

Managed Threat Detection [log]

for Microsoft Sentinel

Managed Threat Detection in the cloud is about monitoring your environments in real time, and responding in a way that minimizes damage for your organization.

Opportunities and risks of the cloud

The complexity of managing cybersecurity across an enlarged attack surface grows exponentially as organizations accelerate digital transformation programmes and adoption of cloud services. Visibility and management of threats such as unauthorised access, account hijack and suspicious network activity become increasingly difficult in a cloud environment largely unmanaged by the organization's IT teams.

As alternative to the need of recruiting a team of cloud security specialists, Orange Cyberdefense enables organizations invested in Microsoft on-premise and cloud technologies a rapid return on cybersecurity investment through Managed Threat Detection for Microsoft Sentinel.

Secure the cloud with Microsoft Sentinel

Microsoft Sentinel is a cloud-native security information event management (SIEM-platform) delivering AI-enhanced security analytics offering Orange Cyberdefense's experienced threat hunters actionable intelligence to detect, investigate and remediate potential indicators of attack and indicators of compromise.

By connecting to and collecting logs from your key data sources, whether users, applications, security products and/or endpoints running on-premise or in third party clouds, Orange Cyberdefense's specialists analyze security events from your Microsoft Sentinel deployment and become your cybersecurity partner monitoring for potential threats 24x7x365.

Why Orange Cyberdefense?

Your cloud detection and response in the best hands:

- **Detection engineering**
  With over 10 years in Managed Threat Detection Orange Cyberdefense brings a wealth of knowledge to Microsoft's security platforms, including hundreds of complementary detection techniques that enhance the inherent detection capabilities of the product.
- **Proven methodology**
  Determine, visualize and improve your detection ability with our Threat Detection Framework and integration with our extensive Threat Intelligence Datalake.
- **Response coverage**
  Benefit from the broadest range of response service options. Complement your own abilities in an optimal way.
- **Experience and expertise**
  Global capabilities, more than 150 analysts, delivering CyberSOC services 24x7x365 are at your disposal.
- **Security and partnership**
  Our local teams work closely with our customers to continuously improve detection and response abilities.
- Orange Cyberdefense is a member of the **Microsoft Intelligent Security Association (MISA)**.

Find out more about Managed detection and response (MDR):
orangecyberdefense.com/global/mdr/

Benefits:

Complete detection visibility: gain insight across internal, cloud and SaaS environments to detect cybersecurity threats.

Active response: a broad range of active response options are available 24x7 to suit your security operations needs.

Intelligence-led security: we invest heavily in research and development to detect and respond to the latest tactics, techniques and procedures.

Save time and costs: we use innovative techniques to ensure that incidents are investigated in context and noise is reduced as much as possible.

Intelligent detection

The challenge with detection is that there is not one type of technology that solves all detection needs. There are options for doing detection across log data, network data and endpoint data.

There are threat activities that happen outside of your infrastructure that may cause a risk to your business that need to be detected. You can probably not solve all problems at the same time, but you can choose a security partner with a complete MDR portfolio that can guide you to your best investments.

Orange Cyberdefense offers a complete detection portfolio that covers not only the SOC triad of log, network and endpoint, but also detection of threats to your business on the Open, Deep and Dark Web. You can start with the one most relevant for your current need, and then expand as your business requires.

Our Intelligence Datalake pulls in and pushes out threat data across our different services and global customer set to enable us to provide a global as well as local perspective on detecting anomalous behavior.

We have you covered!

Orange Cyberdefense MDR services are modular and a customer can select one or several of these components depending on their own resources – or more importantly where Orange Cyberdefense can effectively plug the gaps where those resources don't exist.

Once you have your Managed Threat Detection service in place, this can be combined with the response service that you need in order to compliment your own abilities.

All of the services are backed by our global network of 18 SOCs and 14 CyberSOCs that have 24x7 eyes on the screen, and our internationally recognised CERT teams who hold memberships with CREST, TF-CSIRT and FIRST.

Whatever your needs in the area of response are, our Managed Threat Response services complement and extend your capabilities as required. We assist to contain threats before they cause long lasting damage, while our Incident Response retainer and digital forensics services give you on-demand access to one of the largest and most skillful CSIRT available.

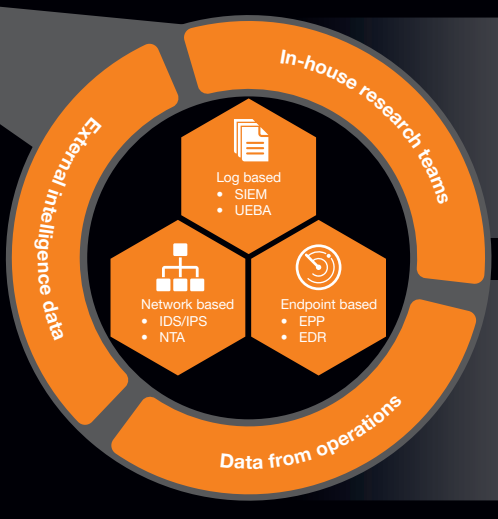
Intelligence-led MDR: Benefits

Orange Cyberdefense
Intelligence Datalake

- 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 detection

- Advanced knowledge of IoCs
- Early detection of major campaigns
- Superior analysis & correlation
- Efficient filtering of "noise" and false-positives
- 24x7 CyberSOC

Better response

- Faster tracking of incident causes
- Faster detection of attack vectors
- Rapid containment & forensics
- 24x7 CSIRT