# Orange Cyberdefense

## Managed Threat Detection

# Network

**Attackers are not static. They often have to enhance their position. And when they do, we must catch them in the act.**

**Many customers base their threat detection only on logs or on endpoint data. The challenge with this approach is that not everything is logged, and not all endpoints can run detection agents. Or indeed, there may be third party endpoints not owned by your organization. Network-based threat detection provides an optimal way to get the full view of threats traversing the network without blind spots caused by machines without endpoint sensors or missing log data.**

Traditional network-based detections are however failing to detect today´s threats. This is due to the fact that they are based on short-lived and reactive intelligence and that they fail to learn unique customer traffic patterns to be able to detect anomalies. A global view is not enough, we need local context.

## Solution

To address these challenges, Orange Cyberdefense offers a managed service that leverages machine learning (ML) for detecting threats based on network traffic. And, by applying supervised ML techniques, the service can detect threats that have never been seen before based on their behavior. Alongside this, unsupervised machine learning maps and adapts to your unique network profile continuously over time, meaning that the service has greater context around activities that are unique to your environment and therefore, reliably detects what is anomalous.

## Service Overview

Our experts will deploy physical or virtual sensors that are connected to a network tap. The network tap will send copies of all traffic that should be monitored to the sensor which will extract relevant information and forward this data to the central “brain”. The brain will apply different detection models to monitor for a range of threats across the consolidated data.

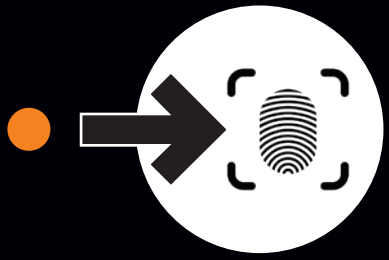
The solution also integrates with leading cloud platforms, utilizing AWS virtual private cloud (VPC) traffic mirroring and/or similar virtual tapping techniques in Azure to monitor all infrastructure-as-a-service traffic.

In addition, account activity is also monitored utilizing specific artificial intelligence (AI) techniques to identify malicious behaviors and hijacked accounts (including Office365 integration) to cover complex hybrid and multi-cloud environments end-to-end.

Orange Cyberdefense monitors the central brain for alerts, and when detected, they will be collected, analyzed, and classified by the security experts in the CyberSOC 24x7.

Once a threat has been confirmed, you will get an incident notification in accordance with the SLA for that specific priority level. This notification includes information about the threat and recommended actions.

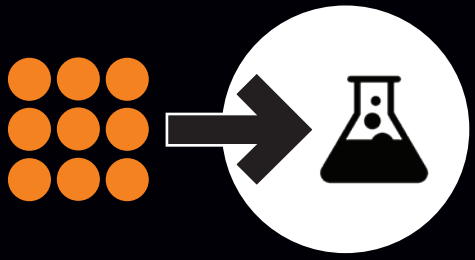
## Traditional signatures



**Short-lived reactive intelligence**

- How the threat looks like
- Find threats that you’ve seen before
- Snapshot in time
- No local context

## Data science



**Long-lived predictive intelligence**

- What the threat does
- Finds what all threats have in common
- Learning over time
- Local learning and context

## Find out more on smart network detection:
orangecyberdefense.com/global/network/

**Complete network visibility:** Cover the network security gap and integrate with other solutions (EDR and SIEM) to provide complete visibility.

**24x7 response:** Comprehensive analysis and response actions via the platform by integration with AD to lock down accounts. Active response is added by integration with EDR or NAC to quarantine hosts.

**Detailed analysis:** Detailed enriched detection context helps in providing detailed analysis.

Signatureless detections based on identifying attached behaviour within the network using AI/ML.

**Save time and costs:** CyberSOC provides security analysts and platform expertise as a service. This gives you great visibility at a lower cost than most log-based solutions and less integration effort.

## Challenges

- 24x7 CyberSOC coverage required
- Continuous management of network monitoring 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 a sophisticated managed network detection service
- If you require 24x7 or 8x5 managed threat detection
- If you require a provider that not only provides network detection but also log and endpoint based monitoring as well as actionable Cyber Threat Intelligence
- If you require additional Managed Threat Response capabilities 24x7

## What do we do?

- Deployment of the Vectra platform
- Platform management of Vectra Cognito™
- 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 and custom detection rules (Premium)

## What will you get?

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

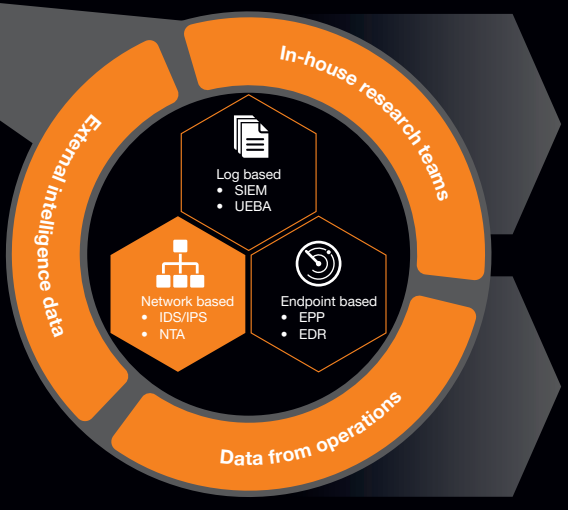
# Intelligence-led network detection: Benefits

**Orange Cyberdefense Intelligence Backbone**

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

**Internal activities**

- Machine learning models to accurately detect behaviors
- Analyzing and classifying incidents
- Notification and reporting




**Better network detection**

- Anomaly detection through supervised machine learning
- Command & control detection
  - Advance C2: human control
  - Botnet C2
- Reconnaissance detection
  - Network sweeps and scans
  - Advanced: AD, RPC, shares
- Lateral movement detection
  - Stolen accounts
  - Exploits
  - Backdoors
- Exfiltration detection
  - Data movement
  - Methods, e.g. tunnels
- 24x7 CyberSOC