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.

Service Overview

Our experts deploy sensors, physical or virtual, connected to a network tap. Copies of monitored traffic are sent to the sensor, which extracts and forwards relevant data to the central 'brain.' The brain uses various detection models to monitor a range of threats across consolidated data.

Our solution integrates with top cloud platforms, leveraging AWS VPC traffic mirroring and Azure's virtual tapping for infrastructure-as-a-service traffic monitoring. Account activity is scrutinized using AI techniques, including Office365 integration, covering complex hybrid and 2 multi-cloud environments.

Orange Cyberdefense monitors the central brain for alerts 24x7. Detected threats are collected, analyzed, and classified by our security experts in the CyberSOC. Once confirmed, you receive an incident notification per the SLA for that priority level, providing details about the threat and recommended actions.

Our solution

To tackle these challenges, Orange Cyberdefense provides a managed service utilizing machine learning (ML) to detect threats from network traffic.

Using supervised ML, the service identifies previously unseen threats based on behavior. Simultaneously, unsupervised machine learning continuously maps and adapts to your network profile, enhancing contextual understanding of unique activities in your environment, ensuring reliable detection of anomalies.

Detecting sophisticated threats in your modern network

Advanced Threats

Advanced threats don't stop at the endpoint, and so does threat detection. Network Detection & Response (NDR) helps to detect advanced threats more effectively.

Visibility

Gain comprehensive visibility into your network activity to track suspicious behaviors and sophisticated threats.

Compliance

NDR supports your compliance to regulations such as NIS 2, GDPR, PCI DSS, HIPAA.

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

Our Service commitment to you

1. 24x7 Delivery
24x7 Platform Operations and Security Monitoring

2. Fast Detection
Detection and response for the modern network

3. Rapid Response
Security Analysts on hand 24x7 for comprehensive response actions

4. Monthly Reports
Monthly strategic security reports including our CyberSOC update

What to expect

Complete network visibility
Detection and response capabilities covering the modern network including public cloud and your entire Microsoft 365 ecosystem

Detailed analysis
Signature-less detections based on identifying unusual behavior

Advanced Analysis and Hunting
Detailed and enriched detection context providing fast and effective analysis, continuously tuned

Save time and costs
Innovative techniques to ensure that incidents are investigated in context and noise is reduced as much as possible

Intelligence-led security

Our intelligence, your advantage

1. Threat Intelligence
Integrated cyber threat intelligence from Orange Cyberdefense

2. Custom Rules
Our detection engineering team maintains a set of 40+ custom rules that enhance visibility

3. Threat Hunting
Option to have our threat hunters look for the needle in the haystack, with dedicated hunting hours

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cyber security business unit of the Orange Group, providing managed security, managed threat detection and response services to organizations around the globe.

As the leading security services provider, we strive to build a safer digital society. Our global footprint with a European anchorage enables us to meet local requirements and international standards, ensure data protection and privacy for our clients as well as for our employees.

We embed security into Orange Business solutions for multinationals worldwide.