Orange
Cyberdefense

Managed Threat Detection [network]

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 will run detection agents. For optimal threat detection ability, customers also need to invest in network-based threat detection.

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.

Solution

To address these challenges, Orange Cyberdefense offers a Managed Service that leverages Machine Learning for detecting threats based on network traffic.

By applying supervised Machine Learning techniques, the service can detect threats that have never been seen before.

By applying unsupervised Machine Learning, and learning local behavior over time, the service can also detect threats based on behavior anomalies within the customer´s unique environment.

Service Overview

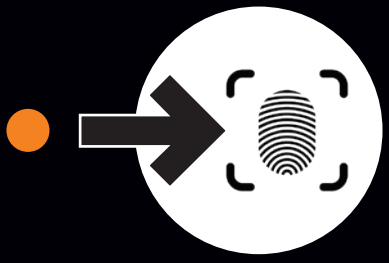
Orange Cyberdefense will deploy physical or virtual sensors that are connected to a network tap. The network tap will send copies of all traffic that should be monitored to the sensor. The different sensors will extract relevant information and forward this data to the central brain that will apply different types of detection engines to detect threats across all the data. The brain is a hardware appliance that will be placed at the customer premise.

The solution also integrates with leading cloud platforms, utilising AWS virtual private cloud (VPC) traffic mirroring and / or Azure Virtual Network TAP to monitor all infrastructure-as-a-service traffic.

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

Once a threat has been confirmed, customer 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.

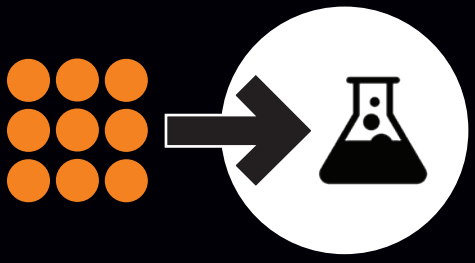
Traditional signatures



Short-lived reactive intelligence

- Recognition by what the threat looks like
- Finds threats analyzed before
- Snapschot in time
- No local context

Data science



Long-lived predictive intelligence

- Recognition by what the threats do
- Finds what all threats have in common
- Learning over time
- Local learning and context

Erfahren Sie mehr dazu, wie Sie Angriffe erkennen, bevor sie Schaden anrichten:
orangecyberdefense.com/de/detect/

Benefits:

- Increase your resilience against threats and zero-day-attacks based on behavior, no use-cases, signatures or extensive rules required
- Detect unusual behaviour based on your own specific setup and environment profile, not derived from standards that do not match you
- Controllable monthly costs and professional service instead of extensive headhunting for specialists and trial-and-error to find the right product
- Detect and eliminate threats before they actually cause a loss of critical information or (financial) damage
- Advanced agentless attacker detection reduces the risk of security gaps and blind spots in dynamic cloud environments.

Security Research
Characterize fundamental attacker behaviors

Data Science Security Research
Machine learning models to accurately detect behaviors

Attacker Behavior Models
High-fidelity, signatureless detection

Command and control
- Advance C2: human control
- Botnet C2

Reconnaissance
- Network sweeps and scans
- Advanced: AD, RPC, shares

Lateral movement
- Stolen accounts
- Exploits
- Backdoors

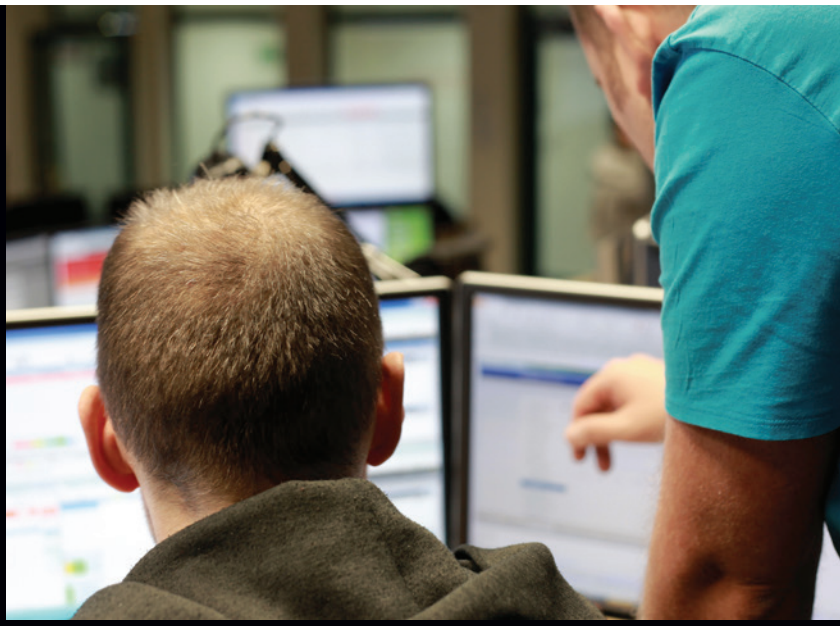
Exfiltration
- Data movement
- Methods, e.g. tunnels

Optional Services

The SecureDetect Network service can be complemented with the SecureRespond Quarantine service.

The benefit with this is that this will give the Cyber SOC analysts the ability to rapidly isolate the detected threat and limit the impact of the breach.

Pro Service



Mehr Infos finden Sie auf
https://orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

info@de.orangecyberdefense.com
+49 89 2000148 00