Powered by
Orange Cyberdefense

Managed threat detection: endpoint, firewall, user-identity

MicroSOC

Visibility across the enterprise is key when it comes to threat detection. The quickest way to obtain this visibility is through your endpoint, firewall and user-identities.

There is no such thing as 100% protection. Once you have accepted this, it is time to implement a strategy to detect the threats you could not prevent. The challenge with detection is that today's threats are not using old malware that is easy to detect and remediate. A quick response, however, is key.

77%* of successful attacks use file-less malware that traditional security tools cannot prevent. Since detecting file-less malware, and similar types of advanced attacks cannot be done with the help of static rules or signatures, you need behavior anomaly detections on the endpoint, firewall and user-identity components.

This behavior needs to be analyzed and correlated across other endpoints, firewall, and user-identity components in order to separate the false positives from actual 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.

In most cases, the time from compromise, to detection, to remediation takes too long, significantly increasing costs and damage that could have been avoided.

* Ponemon 2018 Endpoint Security Statistics Trends

Service Overview

MicroSOC is a managed threat detection (XDR) service based on endpoint, firewall, user-identity detection and response technology. By deploying low-impact sensors on the endpoints reusing existing gateway and identity investments; behavior data is collected, enriched, and correlated with the help of an AI hunting engine. By doing a large number of correlations per second, the performance against other detection toolsets is unparalleled.

This provides detection abilities far beyond what traditional signature or rule-based platforms can demonstrate. The challenge, however, is that the detections are not as simple as a "block or allow" process. In some cases, it requires manual work from a skilled analyst to verify and classify incidents in depth. This is where the Orange Cyberdefense MicroSOC comes in.

Drawing on our 11 global CyberSOCs, years of experience, and a vast Threat Intelligence Datalake; Orange Cyberdefense detects and responds to threats 24x7. In-depth analysis can equally be done 8x5. We continuously work with our customers to ensure that we understand and adapt our endpoint, gateway, identity monitoring to their ever-changing environment.

By deploying low-impact sensors on the endpoints reusing existing firewall and user-identity investments; behavior data is collected, enriched, and correlated with the help of an AI hunting engine. By doingup a large number of correlations per second, the performance againstother detection toolsets is unparalleled.

Prevent cyber threats

Detect and investigate

Respond and continually enhance

Comprehensive endpoint visibility Endpoint, firewall and user-identity 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 massive set of telemetry.

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

Rapid response: 24x7 automated detect and respond capabilities and 8x5 in-depth analysis to isolate threats and limit the impact of breaches.

Business 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 cybersecurity threats
- Low maturity as SIEM and CyberSOC is too complex and expensive.
- Daily review of your firewall, endpoint and identity logs

When should you consider it?

- If you need experts to help deploy and run an outcome-based managed detection and response service based on XDR
- If you require 24x7 or 8x5 managed threat detection
- If you are looking for 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 want additional managed threat response capabilities 24x7

What do we do?

- Deployment of the MicroSOC platform
- Continuous incident triage, analysis, and prioritization by security analysts
- Managed threat response such as isolation of infected endpoints
- Integration of Orange Cyberdefense’s unique Threat Intelligence Datalake and custom XDR rules
- Monitoring of endpoint / firewall / identity logs

What will you get?

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

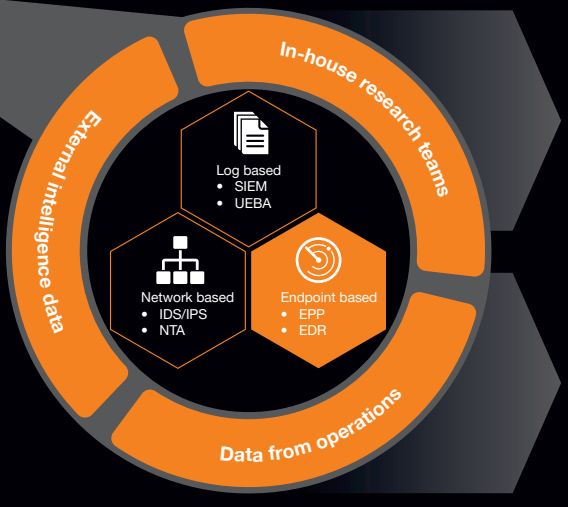
Intelligence-led detection: benefits

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 threat detection

- Advanced knowledge of IoCs
- Identification of legitimate processes, 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 MicroSOC

Orange Belgium
Avenue du Bourget, 3 - 1140 Evere

Contact us
B2BSecurity@orange.be

More information
https://business.orange.be/en/it-solutions/security-solutions