Orange
Cyberdefense

# Managed Threat Detection [log]

## Logs from security devices, applications and cloud environments can give you the most powerful data you can get. But that data must be in the right hands.

### Increase your visibility

No protection is infallible. It is therefore all the more important to be prepared for situations where attackers undermine or circumvent protective measures.

Reliably detecting intrusions is the essential foundation for successful cyber-attack prevention and a key feature for organizations to protect themselves from the damage of extensive breaches.

The cybersecurity analysts in our CyberSOCs, with eleven globally dispersed hubs, use state-of-the-art technology and proven processes to monitor the IT environments of our customers based on a wide array of log data. Having been through our extensive CyberSOC introduction training program, our analysts provide the skills and knowledge to fully realize the power of advanced log analytics.

### Key considerations

- Most companies' ability to detect threats is still far below an acceptable level
- It is time consuming and expensive to find resources to build your own SOC and CSIRT team
- The majority of Managed Detection and Response providers are putting their faith in SIEM technology alone – this needs to be accompanied by strong research and intelligence-led capabilities, as well as consistent processes and multi-skilled security professionals

### When is enough, enough?

As always, to know your next step you need to know where you are today. Your profile as an organisation, your risk appetite and specific regulations are just a few of the business drivers that will help you to make that decision.

The layers and the type of protection, detection and response is unique for every business. But don't worry, the way to find out what's right for you does not need to be so complex.

### Threat Detection Framework

Visualising and modelling your detection objectives is important.  You have to know what you want to do, the impact it will have and the visibility you will get when you are thinking about log-based detection.

Our Threat Detection Framework gives you the data to make those decisions. Log-based detection has dependencies on the data that is consumed by the service. It is important to understand those dependencies to make the right decisions and to educate the wider business on the security value of log data.

## The business benefits

The Managed Threat Detection [log] service not only offers increased visibility and advanced detection, it helps you make business decisions related to cybersecurity:

The service maps to the MITRE ATT&CK framework and allows you to measure progress and model improvements.

Our proprietary asset database helps you measure your risk and attack trends over time, including high risk machines or users, as well as kill chain activity across the business.

Our risk-based detection methods allow us to include more data for our analysts while reducing the number of incidents, in turn alleviating the reliance on your team for extra context.

**Find out more on how to detect attacks before they cause damage on:**
**orangecyberdefense.com/global/mdr/**

## Challenges

- Management and continuous improvement of log-based detection and response platform
- Staffing a security platform management team with subject matter experts
- Lack of resources to staff a Security Operations Center (SOC) 24x7
- Developing detection use cases that provide enough context for analysts without producing “alert fatigue”
- Applying global intelligence to cyber security threats

## When should you consider it?

- If you have compliance requirements that require log storage, which you want delivered as a service
- If you require experts to help deploy and run an out-come-based MDR service based on SIEM
- Alternatively if you have invested in Microsoft Sentinel but do not have the resources to run it, let us “super charge” it for you.
- If you require 24x7 or 8x5 managed threat detection
- If you require a provider that is focused on the full “SOC triad” stack, providing Endpoint and Network based detection as well as comprehensive Cyber Threat Intelligence

## What do we do?

- Deployment of our proprietary Pattern-based detections to the Splunk platform we provide as part of the service OR by running those detections against your existing Microsoft Azure Sentinel platform.
- Continuous incident triage, analysis and prioritization by Security Analysts
- Integration of Orange Cyberdefense’s unique Threat Intelligence Datalake
- Custom use case / detection development
- Performance, Device Health, OS, Log Source, Application and License Monitoring (Splunk only)

## What will you get?

- Real-time incident analysis
- Monthly security and operational reporting
- Cyber threat hunting

## Add Managed Threat Response

We use your existing security tools to isolate endpoints involved in critical incidents.

# Intelligence-led log based 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 log based detection**

- Advanced knowledge of IoCs
- Risk-based detection, with flexible user and entity behaviour analytics
- Severity classification
- Anticipation and early detection of major campaigns
- Efficient filtering of “noise” and false-positives
- Highly customisable
- 24x7 CyberSOC