

NDR as a service – for permanent security in your network.

Imagine a cybersecurity service monitoring your network traffic every second, intelligently detecting the smallest deviations from the norm and reporting them in real time. That's network detection and response - NDR for short - as a service from UMB. Reduce your response times to cyber threats significantly and talk to our specialists now.

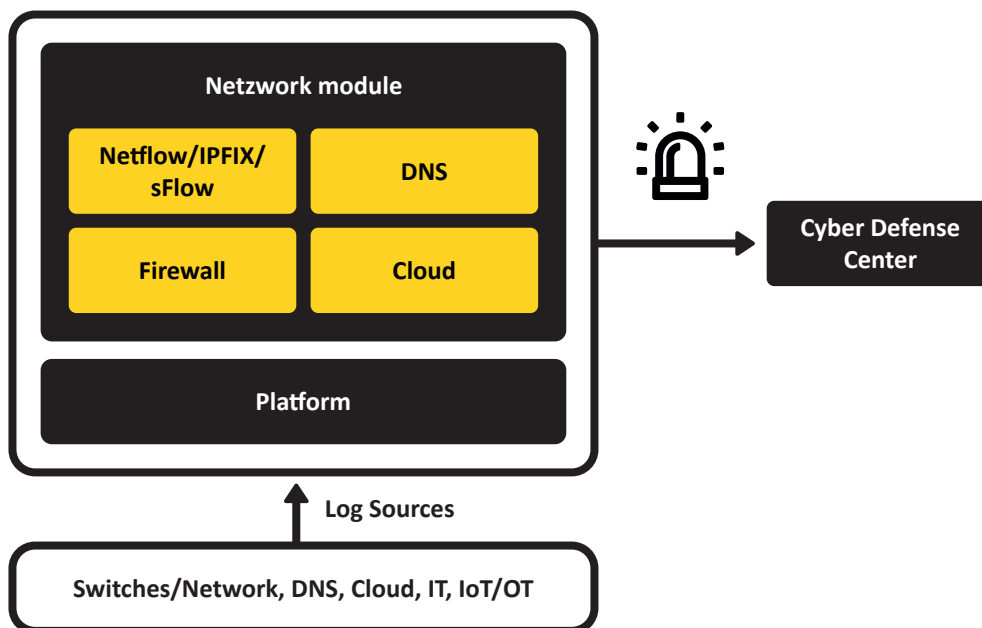
NDR - network detection and response - as a service continuously monitors your internal and incoming network traffic. NDR detects suspicious activity immediately - if such activity deviates from the norm. It uses a variety of techniques - artificial intelligence, predefined use cases, threat feeds and more - to immediately detect even completely unfamiliar attacks, compliance violations or even misconfigurations.

It's the ideal supplement to EDR as a service

NDRaaS is an ideal addition to EDR as a service and brings decisive additional security. EDR offers prevention and behavioural analysis on the endpoint. NDR analyses the behaviour of the network. In addition, EDR agents can not be installed on all endpoints (e.g. IoT/OT devices) and the agents can also be switched off. NDR can then act as the first line of defence here.

Because every minute counts for cybersecurity

With NDRaaS, all devices in the IT, OT and IoT network can be monitored in real time, enabling a faster and more effective response to incidents. NDRaaS analyzes firewall, DNS and cloud infrastructure logs as well as NetFlow, IPFIX and sFlow, to comprehensively analyze and assess network activity. If cyber threats are detected, the Cyber Defence Center sounds the alarm.



NDRaaS by UMB: Quick to set up and inexpensive to run

NDRaaS from UMB can be set up within a very short time and does not incur any hidden costs in operation. UMB will assume responsibility for continuous monitoring and alert handling.

The service consists of the following elements:

- NDR platform: The central platform for collecting and analyzing traffic telemetry is continuously operated by UMB.
- Agentless and sensorless: Regardless of the network topology, no additional agents or sensors are required to connect the log sources. This means that NDR as a Service can be easily introduced into the existing customer environment.
- NDR 7x24 service: Continuous monitoring and analysis of network traffic. This provides visibility into traffic from relevant/critical network segments and network entry/exit points. Recommendations for action on critical threats will be communicated.

Your benefits

- Comprehensive insight into the structure and events in your network.
- UMB monitors all devices and their communication behaviour traffic nodes in your environment.
- Very easy setup, no degradation of network performance.
- Proven algorithms to detect even previously unknown cyber threats.
- NDRaaS analyzes only log data and can therefore also include encrypted network traffic in the analysis.
- NDRaaS is the perfect supplement to EDR as a Service.

Sounds interesting? Contact us!

We will be happy to answer your questions on cybersecurity, NDR and more.

Contact

Marc Rudin
Sales Consultant
marc.rudin@umb.ch
+41 58 510 18 07
www.umb.ch