NDR for OT

Part of NCC Group's Intelligent MXDR

Enhancing security across IT and OT environments with comprehensive threat detection and response.

Why Network Detection and Response (NDR) for OT?

With the advent of regulations like NIS2 and the Cybersecurity Act, organisations are under increasing pressure to improve their cyber security posture – including that of their OT estate.

Traditional IT security measures are often inadequate for OT environments, which demand specialised protocols and continuous, real-time monitoring. Integrations of IT into previously OT-only networks introduces further, distinct security challenges. Conversely, OT-specific security tools may lack visibility into the origins of threats, which typically begin in IT systems.

NCC Group's NDR for OT bridges this gap, offering a unified approach to detect and respond to threats across converged IT/OT infrastructures, monitored by a single, 24/7/365 SOC. This integration ensures that both environments are protected against a wide range of cyber threats, from ransomware attacks to nation-state actors.

NDR for OT is designed to help organizations meet these regulatory requirements by providing robust asset identification, tailored controls, and continuous monitoring. By implementing our solution, organizations can achieve compliance while strengthening their overall security framework.

Robust protection for OT environments.

Managed Solution:
Leveraging 20+ years of NDR experience, safeguarding clients in Critical Infrastructure, Manufacturing, and the transport sector.

Visibility:
Gain comprehensive visibility into both IT and OT assets, ensuring that OT assets remain safe, available, secure, and confidential.

Accurate Alerts:
Receive precise alerts that matter, extending NCC Group's IT coverage with OT coverage.

The Best of AI and Classical Detection Engineering:

NCC Group's NDR for OT leverages signature-based and machine-learning threat detection, utilising tools like Suricata, Zeek, and the "Vuurtoren" Machine Learning suite for deep traffic analysis.

This ensures detection across converged IT/OT networks and offers customized monitoring for non-TCP/IP OT protocols.

Consultative Approach:

Each NDR for OT deployment includes expert consultancy to:

- Assist with scoping and deployment of sensors in IT, OT and DMZ environments.
- Fine-tune detection logic for novel traffic and ensure proper monitoring of OT-specific communication.
- Interpret findings and provide actionable insights for incident response and risk mitigation.

Flight Data Recorder

Our NDR for OT proposition includes the flight data recorder. Whereas typical IT or OT network sensors take a snapshot of a network package the moment an event happens, our network sensor can save the full PCAP stream.

This enables better threat investigation, threat hunting on new IOCs, and improved incident response outcomes, limiting the impact of an incident.

A NDR Solution for Each Network

The NDR for OT is available as a physical and virtual device.

Enhance your security across IT and OT environments with comprehensive threat detection and response.

UK & Europe
+44 (0) 161 209 5200

North America
+1 (800) 813 3523

Singapore
+61 2 8379 7870

Australia
1800 975 310

Netherlands - Fox IT
+31 (0) 15 284 7999

Contact us to future-proof your cyber security today