FIELD-PROVEN AT NATO'S LARGEST CYBER EXERCISE

When the adversary customises malware to defeat you, detection has to be exceptional.

OVERALL RESULT

2nd

Blue Team 1 CH · DE · AT · LU
among 41 competing national teams

At **Locked Shields 2026** — the world's largest live-fire cyber defence exercise — a Red Team of professional offensive operators deployed customised, exercise-specific malware designed to defeat modern defences. **Exeon.NDR** was deployed as part of **Blue Team 1** — a joint team representing Switzerland, Germany, Austria, and Luxembourg — operating against 41 competing national teams.

BLUE TEAM · LIVE EXERCISE FLOOR

4	41	0	100%
NATIONS DEFENDED TOGETHER	NATIONS COMPETING	ENDPOINT AGENTS REQUIRED	METADATA-BASED DETECTION

LOCKED SHIELDS 2026 — RESULTS

2nd — **Overall placement**
Blue Team 1 — Switzerland, Germany, Austria, Luxembourg · among 41 competing national teams

1st — **Technical Resilience category**
The category in which Exeon.NDR was deployed

01 THE TEST

The most realistic cyber defence exercise in the world.

Locked Shields is run annually by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and is widely regarded as the most realistic cyber defence exercise in the world. Blue Teams defend the critical infrastructure of a fictional nation against a coordinated, sustained, multi-vector attack — under real time pressure, with real tooling, against a Red Team whose only job is to break them.

> **The traffic is real.**
> **The malware is customised.**
> **The pressure is operational.**

Blue Teams are evaluated across **Defence against Red Team**, **Usability**, and **Availability** — a test of whether your detection holds up when the adversary, the pace, and the consequences are all real.

02 WHAT EXEON.NDR DETECTED

Confirmed detections across the exercise.

- **Custom malware via typosquatting** — Custom malware was installed on approximately 10 machines via typosquatted domains.
- **C2 channel identification and cleanup** — Active C2 channels through malicious domains were identified and remediated.
- **IT/OT pivoting** — Lateral movement across IT/OT network boundaries was detected.
- **Lateral movement and SSH backdoors** — East-west movement and persistent SSH backdoor activity were identified across the network.
- **Memory-injected malware in EDR process** — Malware injected into memory of a running EDR executable was detected — evading endpoint-based detection.
- **Customized staging identification** — Malware droppers were identified before any other tool in the exercise had fired an initial alert.

All detections made on network metadata alone — no endpoint agents, no traffic mirroring, no hardware sensors required.

03 WHERE EXEON.NDR STOOD OUT

Technical approach: why these detections were possible.

Locked Shields rewards the defenders who see the things others can't — covert C2, lateral movement, and the small misconfigurations that turn into incidents. Exeon.NDR gave the Blue Team a continuous, behavioural view of the network without agents, sensors, or packet payload inspection.

A particular strength at the exercise was surfacing misconfigurations in the network and especially in the firewall — gaps that a determined Red Team would otherwise turn into footholds.

Why it worked: behavioural ML on network metadata is signature-agnostic. Customised tooling and previously-unseen techniques look like anomalies in traffic patterns long before they look like a known threat.

> Locked Shields gives us something most vendors never see: our technology, in the hands of analysts under real pressure, against an adversary built to defeat them. That is the validation that matters.

Philipp Lachberger Head of Presales & Deployment Exeon

FOR YOUR ENVIRONMENT

Why this matters for you.

The attack profile at Locked Shields — custom malware, memory injection, IT/OT pivoting, SSH backdoor persistence — reflects what advanced adversaries use against enterprise and critical infrastructure targets.

Exeon.NDR identified these threats on network metadata alone, with no endpoint agents, no traffic mirroring, and no prior signatures. In several scenarios, detection preceded every other tool deployed in the exercise.

See Exeon.NDR in your environment.

Book a 30-minute technical walkthrough — including a deep-dive on the detections from Locked Shields.

Schedule a conversation

or email sales@exeon.com

ABOUT EXEON

Exeon is a Swiss cybersecurity company specialising in AI-driven Network Detection and Response. Exeon.NDR uses machine learning on network metadata to detect advanced threats — lateral movement, command-and-control activity, insider threats, and zero-day attacks — without endpoint agents or traffic mirroring. We serve enterprise and public-sector customers across Europe.