FIELD-PROVEN AT NATO'S LARGEST CYBER EXERCISE

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

At Locked Shields 2026 — the world's largest live-fire cyber defence exercise — a Red Team of professional offensive operators ran customised attacks designed to evade modern defences. Exeon.NDR stood alongside one Blue Team defending four nations against the full weight of that adversary.

NATIONS DEFEN

4

Defended together by one Blue Team, against a Red Team built to defeat them — among 41 nations competing.

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

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

Threats that typically evade signature-based and perimeter tooling.

- **Command & Control channels**
  Multiple covert C2 communications identified across the network.
- **Lateral movement**
  East-west traffic anomalies detected as the Red Team pivoted through the environment.
- **Customised malware**
  Adversary tooling tailored for this exercise — surfaced and confirmed through behavioural analysis on the wire.
- **Network & firewall misconfigurations**
  A particular strength: surfacing weak rules and misconfigured firewall paths that a Red Team would otherwise exploit.

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

03 WHERE EXEON.NDR STOOD OUT

Detecting what perimeter tools and signatures miss.

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.

One of the strongest signals at the exercise was our ability to flag 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

Why this matters for you.

The threats your team faces every day share more with Locked Shields than with the demos most vendors show you. Real adversaries don't use known signatures. They move laterally. They write custom tooling. They operate under your radar for weeks.

If your current detection stack hasn't been tested against that level of adversary, we'd like to show you what ours did.

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.