



HYDRA – network anomaly detection

Learns how your network normally behaves, and shows what deviates from it.

IN ONE PARAGRAPH

HYDRA is BlueWave AI's network anomaly detection system. It reads a passive copy of network traffic, learns the normal behaviour of that specific network from its own unlabelled traffic, and flags behaviour that deviates from it, with the context an analyst needs to investigate. It is designed to complement signature-based defences, not to replace them. HYDRA is a research prototype, demonstrated on our own lab cyber range; work with a new organisation starts with a scoped technical assessment.

THE PROBLEM

- Intrusion detection systems and signatures recognise patterns that someone has already described. A new way of moving data or acting on files may match no written rule, yet still stand out against what is normal on that particular network.
- Analysts need more than a score: which host behaved how, and compared with what.
- Context: IBM reports a global mean breach lifecycle of 241 days in 2025, from identification to containment and service restoration (IBM, Cost of a Data Breach Report 2025). This is an industry figure, not a HYDRA result.

HOW IT WORKS

From a copy of traffic to an alert an analyst can inspect:

1 · OBSERVE

Passive copy

Reads a mirror port or network TAP. Sends no packets and does not block traffic.

2 · DESCRIBE

Behaviour

Name resolution, connections, timing, file-sharing activity. For encrypted traffic, metadata, not content.

3 · COMPARE

Learned normal

Models learn this network's normal behaviour from unlabelled traffic. Rule-based checks cover known patterns.

4 · EXPLAIN

Alert with context

Which host, what behaviour, how it differs from the baseline, tied to the underlying network record.

EXAMPLES FROM OUR LAB CYBER RANGE

- Our lab cyber range has 15 virtual machines running Windows and Linux clients, a file server and common services, with everyday background traffic as the baseline.
- **Data hidden in DNS queries:** a client sends a file in small pieces hidden in name-resolution requests, while normal name resolution continues. Shown in the lab.
- **Mass encryption on a file server:** a client encrypts files on a shared drive over SMB. Scenario demonstrated in the lab; detection validation ongoing.
- These are lab demonstrations on our own infrastructure, not results from a customer network. HYDRA does not claim to detect every attack.

WHERE IT FITS IN SECURITY OPERATIONS

- **Intrusion detection and signatures:** HYDRA complements them; known, high-confidence patterns remain well served by rules.
- **SIEM:** an integration destination, not something to replace. SIEM export is planned.
- **SOC and analysts:** decision support and faster triage. HYDRA is passive; your team decides what happens next.

Gergely Vass, CEO · gergely.vass@bluewaveai.co · +36 20 441 5497

Gyula Németh, CTO · gyula.nemeth@bluewaveai.co · +36 30 560 9260

WHAT SETS IT APART

- **Your network, your baseline.** The models learn from the organisation's own traffic; no labelled attack data is needed to start.
- **Careful with "normal".** We do not assume that existing traffic is clean. Training data is selected and checked against independent sources to reduce the risk of learning malicious activity as normal.
- **Local and lightweight.** Runs on premises without cloud connectivity, designed for isolated networks too; small models run on standard CPUs. Sizing is measured in each environment.
- **Inspectable by design.** The learned models are built on Kolmogorov–Arnold Networks, whose learned functions can be plotted and examined. This is the basis for the analyst-facing explanations we are developing.
- **The model stays with you.** The trained model remains in your environment and can be handed over to your team on request.
- **Disciplined measurement.** We report results with their denominators and keep negative results, so a successful demo is not presented as general performance.

WHERE IT IS RELEVANT

- Mid-sized organisations with limited SOC capacity; managed security service providers looking for an additional behavioural signal.
- Critical infrastructure and industrial environments where network visibility matters; financial services and the public sector.
- University and research networks.
- Typical conversation partners: CISOs, SOC leads, heads of network and infrastructure.

READINESS AND INTEGRATION REQUIREMENTS

Network anomaly detection (passive monitoring, learned baseline, rule-based checks)

RESEARCH PROTOTYPE

DNS exfiltration scenario on our lab cyber range

LAB DEMONSTRATION

SMB file-encryption scenario on our lab cyber range

DEMONSTRATED IN LAB,
DETECTION VALIDATION ONGOING

Customer deployment

NONE YET: STARTS AS AN ASSESSMENT

SIEM export

PLANNED

Same approach for operational anomalies (AIOps)

CONCEPT

Requirements: a mirror port or TAP on the segments to be observed, a server inside your environment, and a period of representative everyday traffic to learn from.

THE FIRST JOINT ASSESSMENT

- A conversation about your environment and the question you want answered.
- Clarifying which network segments and traffic sources can be observed, and under what data-handling conditions.
- A scoped technical assessment: HYDRA learns a baseline from your traffic and runs in shadow mode; we review its alerts with your analysts and deliver a written report.
- We agree the scope, terms and any fees of an assessment before it starts. We make no promise of results in advance.

NEXT STEP

A short conversation about whether HYDRA fits a network you are responsible for, or one you know of. If network security sits with a colleague, please feel free to forward this document.