LMNTRIX
BE THE HUNTER | NOT THE PREY

DATASHEET

THE FREE 30-DAY PROOF OF VALUE · HOW IT RUNS

LMNTRIX Proof of Value

Judge the service on your environment, not on a demo.

Thirty days of the full LMNTRIX service, deployed behind the controls you already run, at no cost and with no obligation. Real sensors, real detections, the Cyber Defense Center working them 24×7, and a written findings report at the end, whether or not you proceed.

DAY 0	WEEK 1	WEEK 2	WEEK 3	WEEK 4
Scope	**Deploy**	**Hunt**	**Validate**	**Readout**
Surfaces, contacts and success criteria agreed.	Sensors live; 24×7 monitoring starts.	Compromise assessment across the telemetry.	Controls and detections tested by real attacks.	Findings, SLA actuals and a firm proposal.

One question, answered in four weeks: what is in your environment that your stack cannot see, and how fast it is dealt with.

$0
No cost, no obligation, no retainer, no credit card

24×7
The full MDR service from day one, not a watered-down trial

Day 30
A written findings report that is yours to keep either way

The same analysts, the same console and the same response rules you would have in production. Nothing is scripted and nothing is staged.

THE FOUR WEEKS

What happens, and when

Day 0 · Scope
- One call: surfaces, crown jewels, contacts, escalation
- Success criteria written down before anything deploys
- Response rules: notify, confirm or auto-contain

Week 1 · Deploy
- Agent, sensor and API connections live within hours
- Your tools keep running; nothing replaced
- CDC monitoring starts as telemetry lands

Week 2 · Hunt
- Compromise assessment: is anyone already in?
- Persistence, credential misuse, movement, beaconing
- Breach and darknet intelligence on your domains

Week 3 · Validate
- An automated penetration test on the in-scope network
- What your controls stopped, what LMNTRIX caught
- A MITRE ATT&CK coverage map as it stands today

WEEK 4 · THE READOUT

What you walk away with

A findings report in your board's language: every validated incident and what was done about it, the compromise-assessment result, exposed credentials and darknet findings, attack-validation and ATT&CK coverage, detection and containment times against the published SLA schedule, and the gaps to close first. Then a firm proposal for the modules that proved their worth. If a live threat is found, it is contained under the day-zero rules, at no charge.

THE SCOPE

Enough to prove the point. Agreed on day zero.

MODULE	STANDARD POV	WHAT IT PROVES
Endpoint	Agent on an agreed set of hosts	What your endpoint tool did not flag
NDR	One sensor at your main egress	Beaconing and movement the firewall allowed
Email	API behind your mail filter	What the native mail filter let through
Identity	Directory and identity-provider telemetry	Credential misuse and directory hygiene
Recon	Breach and darknet intelligence, your domains	Credentials and machines already in criminal hands
Validate	One automated penetration test	What gets through, and whether anyone notices
On request	Cloud, Deceive, Mobile, SIEM, Packets, ICS/OT, AI	When that surface is why you are evaluating

LMNTRIX PROVIDES

- A named engineer; deployment guides and remote hands
- 24×7 Cyber Defense Center monitoring and response
- Console and LISA access; a weekly 30-minute checkpoint
- The findings report and a firm proposal at day 30

YOU PROVIDE

- A sponsor, a technical contact, an out-of-hours escalation
- Agent push, a SPAN or TAP feed, and API registrations
- Response rules for the thirty days
- Thirty minutes a week, and a decision at day 30

THE SUCCESS CRITERIA · WRITTEN DOWN ON DAY ZERO

Did we see what you could not?

Detections your tools did not raise, or a clean compromise assessment for the board.

Did we act inside the clock?

Detection and containment times on every incident, against the published P1 to P4 schedule.

Could your team live with it?

No disruption to users or tools, and a console your team can use.

QUESTIONS. CLEAR ANSWERS.

Will it disrupt anything?

No. Sensors deploy behind your controls: no reboot, no MX change, no policy change, agent beside your current tool.

What if we don't proceed?

Agents are uninstalled remotely, the sensor decommissioned, your data deleted. You keep the report.

IF YOU PROCEED

The POV deployment becomes production; nothing is rebuilt. Guided onboarding extends coverage to the full estate over two to eight weeks, response rules are signed per asset group, and the SLA clock starts.

Assume you're already compromised. Take 30 days to find out.

One scoping call this week, sensors live the next. Find nothing, lose nothing, keep the report.

START A FREE 30-DAY POV

sales@lmntrix.com

Major Player — IDC MarketScape: Worldwide MDR/MXDR Services for the Enterprise 2026 · Representative Vendor — 2024 Gartner Market Guide for Managed Detection and Response · #19 — MSSP Alert Top 250

© 2026 LMNTRIX. All rights reserved.