LMNTRIX

BE THE HUNTER | NOT THE PREY

DATASHEET

MANAGED EXTENDED DETECTION AND RESPONSE

LMNTRIX MXDR

Behind your controls. Ahead of the attacker.

Every tool you own was built to keep attackers out. None of them tells you when one is already in. LMNTRIX deploys independent native detection behind the stack you already run, assumes every control in front of it has been bypassed, and operates it for you: one XDR platform, fourteen native modules, Cyber Defense Centers around the clock.

THE PLATFORM

LMNTRIX XDR

14 native modules, one data model, one console. Built by LMNTRIX, operated by LMNTRIX.

THE SERVICE

LMNTRIX MDR

Seven layers of analysts, hunters and responders, 24×7, measured on outcomes.

THE OPERATING MODEL

Active Defense

Detect, hunt, validate, disrupt, respond. Five verbs, one continuous cycle.

MXDR is all three together. Most vendors sell you one of them and leave you to assemble the rest.

< 30 min
From confirmed threat to containment and remediation[1]

14
Native modules on one platform, no bolt-ons

400+
Organizations protected across 85+ countries

24×7
Cyber Defense Centers in seven countries, follow-the-sun

THE ASSUME-BREACH MODEL

Assume you're already compromised. Then prove you're not.

YOUR STACK TODAY	WITH LMNTRIX BEHIND IT
Alerts tell you something happened.	Analysts tell you what the attacker did, where they are, and that they're gone.
Each tool sees its own domain.	One platform correlates endpoint, network, cloud, identity, email, mobile, OT and AI.
Detection depends on the controls holding.	Detection assumes the controls have already failed: our own endpoint, network, email, cloud and identity sensors sit behind them, with deceptions seeded where an attacker would look.

THE ACTIVE DEFENSE MODEL · FIVE VERBS, ONE OPERATING MODEL

01
Detect
Weak signals across every surface, before a foothold becomes an incident.

02
Hunt
Hypothesis-driven hunts for attacker behavior, exposed paths and emerging threats.

03
Validate
Every alert verified and enriched; every control tested against real attacks.

04
Disrupt
Break the attacker's chain: block movement, remove access, spring the traps.

05
Respond
Contain, remediate and recover in minutes; close the gap so it doesn't repeat.

[1] LMNTRIX MDR service target for P1 incidents, validated to contained, as defined in the MDR service description.

THE PLATFORM

XDR unlike any other. Built to run behind your controls, not instead of them.

Most XDR is a vendor's own products stitched together. LMNTRIX XDR is one platform, one data model and one console: fourteen native modules across every surface an attacker touches, with deception seeded everywhere and automated response built in. It consumes what your existing stack sees and adds what it cannot: independent ground truth.

Unify
One platform across every domain you run.

Detect
Cross-domain correlation exposes what single-point tools miss.

Respond
Contain and shut down attacks from endpoint to cloud, one console.

Prove
Trace root cause, close the gap, prevent the repeat.

14 NATIVE MODULES · THREE GROUPS · ONE XDR PLATFORM

CORE DETECTION & RESPONSE · every surface you run

EDR
Deep endpoint visibility, autonomous containment, analyst-driven investigation.

NDR
Full packet capture, session reconstruction, AI-driven anomaly detection.

Cloud
Agentless protection across workloads, identities and SaaS; posture and runtime.

Email
Phishing, BEC and account takeover caught behind your native mail security.

AI Security
Workforce AI usage and AI agents: shadow AI, prompt data, injection, misuse.

Mobile
iOS and Android threat defense: malicious apps, phishing, device exploits.

ICS/OT
Asset visibility and detection across OT, IoT, BMS and IoMT, without downtime.

HUMAN THREAT ACTOR COVERAGE · the adversary

Intelligence
300+ sources, mapped to your environment for real-time context.

Validate
Automated penetration testing that confirms detections and tests controls.

Deceive
Decoys, breadcrumbs and traps that reveal an attacker before damage.

Identity
AD, Entra ID and credential misuse monitored in real time.

POST-BREACH FORENSICS & IR · the evidence

Packets
Full-fidelity network forensics, file extraction, retrospective analysis.

SIEM
Centralized logs and correlation across every source, retained as long as you need.

Recon
Attacker-eye view of your external, deep and dark web exposure.

ARTEMIS · THE AUTONOMOUS AI SOC

Artemis works every detection the way a senior analyst would: pulls the related telemetry across all fourteen modules, reconstructs the attacker's path, scores the blast radius and drafts the containment plan, in seconds. Analysts validate and act.

LISA · YOUR CHATOPS ASSISTANT

Ask about any incident, host, user or threat in plain language, from the console, Slack or Teams, and get an answer grounded in your own telemetry. "What happened on this host last Tuesday" is a question, not a ticket.

Works with the tools you already have, and contains through them. LMNTRIX XDR is pre-integrated by API with the major next-generation firewall, web security, DNS security, endpoint, email and identity platforms: it ingests their telemetry and, when it is time to contain, pushes the block, the isolation or the IOC straight into them. No console logins, no ticket to another team, nothing ripped out.

THE MDR SERVICE

A full security operations team. Overnight. Without the hiring.

LMNTRIX MDR is not an alert-forwarding service. It is seven layers of specialist expertise operating the platform from our Cyber Defense Centers, 24×7×365, with every incident validated by a human before it reaches you and response times we are measured on.

< 1 min	< 5 min	< 30 min
DETECT	INVESTIGATE	CONTAIN & REMEDIATE

Service targets measured across confirmed incidents. Surgical containment and remediation, no reimaging, no "we recommend you" email.

SEVEN LAYERS OF EXPERTISE

Tier 1 Event Analysts. Triage every signal, 24×7. 95% fewer alerts reach you[1], and none unvalidated.

Tier 2 Incident Analysts. Investigate confirmed detections and build the incident timeline.

Tier 3 Incident Responders. Contain and remediate on your behalf, surgically, in under 30 minutes.

Forensic and Malware Analysts. Reverse the payload, recover the evidence, establish root cause.

APT Hunters. Run the Hunt Cycle across your environment continuously: Survey, Secure, Detect, Respond.

Intel Analysts. Map global threat activity to your industry, geography and attack surface.

Integration and Operations. Every sensor tuned, every integration live, every dashboard current.

WHAT THE CYBER DEFENSE CENTER DOES

Monitors and responds, 24×7×365. Follow-the-sun from Cyber Defense Centers in seven countries.

Hunts proactively. Hypothesis-driven hunts across your telemetry, not rule matches alone.

Runs DFIR without a clock. Forensics and incident response included; no retainer, no hourly billing.

Reports what matters. Every incident with root cause, attacker path and the control gap, plus monthly service reporting.

Adds value every quarter. A complimentary assessment each quarter: AD audit, cloud posture, automated pen test or darknet exposure review.

WHAT YOU RECEIVE

Validated incidents with the action already taken; real-time and monthly reporting across all fourteen modules; quarterly service reviews and a value-add assessment; a dedicated Account Manager and Technical Account Manager; board briefings on request; and engineers you can reach 24 hours a day.

THE RESPONSE WORKFLOW · FROM SIGNAL TO CLOSED INCIDENT

01 Deploy
Native sensors across every surface, operational within hours. Your tools keep running.

02 Detect
Cross-domain correlation plus deceptions turn weak signals into confirmed detections.

03 Investigate
Artemis builds the timeline; Tier 2 and 3 validate who, what, when, how and how far.

04 Respond
Isolate the host, disable the account, block the session, under the rules you set.

05 Prove
Root cause, attacker path and the gap that let it happen, in a report your board can read.

HOW WE ESCALATE

Critical	Immediate call and live coordination until contained.
High	Rapid notification and guided containment.
Standard	Portal update, ticket and analyst follow-up.

TRUSTED. CERTIFIED. OPERATIONAL.

SOC 2 TYPE I · ISO 27001 · CMMC LEVEL 2 · PCI DSS 4.0

100% of incidents reviewed by a human analyst before closure, by LMNTRIX operational policy. [1] Reduction in alerts reaching the client versus raw platform alerts, across LMNTRIX customer environments.

THE ENGAGEMENT

Who does what

One subscription covers the platform, the modules you choose and the Cyber Defense Center that operates them. You decide the response rules and who gets called; LMNTRIX does the rest.

LMNTRIX PROVIDES

- The XDR platform and every module in scope, deployed within hours
- 24×7×365 monitoring, hunting, investigation and response
- Surgical containment and remediation, under 30 minutes
- Unlimited digital forensics and incident response
- Monthly service reporting and a quarterly value-add assessment
- Integration with your existing tools as telemetry and enforcement points

YOU PROVIDE

- Deployment access for sensors and API connections
- An asset and identity inventory, as good as you have it
- Response rules: notify, confirm or auto-act, per severity
- Escalation contacts and who receives reports
- Read access to the tools you want correlated
- A decision at the end of 30 days

WHAT SETS IT APART

	LMNTRIX MXDR	ENDPOINT-LED XDR	TOOL-HEAVY MDR / MSSP
Operating model	Assume breach; deployed behind your controls	Prevention first; relies on the agent holding	Watches whatever you bought
Coverage	14 native modules, one data model	Strong on endpoints, add-ons beyond	Multiple consoles, fragmented context
Response	Contained and remediated by us, under 30 min	Isolate, then a recommendation	A ticket, then your team
Deception and hunting	Deceptions everywhere; continuous Hunt Cycle	Optional, extra	Rarely included
DFIR	Unlimited, included	Retainer, hourly	Retainer, hourly
Proof	Free 30-day POV in your environment	Demo environment	Reference calls

QUESTIONS. CLEAR ANSWERS.

Do we have to replace our existing tools?

No. LMNTRIX deploys behind them, consumes their telemetry and uses them to enforce. Your investment keeps working; we find what it missed.

Do we need all fourteen modules?

No. Start with the surfaces that matter and add modules as you go; they share one platform, so each one added sharpens the rest.

WHAT WE NEED TO SCOPE IT

- Employees, and endpoints, servers, cloud and VDI in scope
- Mobile devices, OT sites and assets, if any
- Cloud platforms, mail platform and identity providers
- Daily log volume for SIEM, if required

Priced per host, per user or per asset by module, MDR included. One subscription, no retainers.

Don't take our word for it. Take 30 days.

We deploy behind your existing controls, at no cost, for 30 days, with the full MDR service running. If we surface nothing your stack missed, you've lost nothing. Either way you get a written findings report.

START A FREE 30-DAY POV

sales@lmntrix.com