LMNTRIX
BE THE HUNTER | NOT THE PREY

DATASHEET

MANAGED DETECTION AND RESPONSE · THE SERVICE BEHIND LMNTRIX XDR

LMNTRIX MDR

Always watching. Ready to act.

LMNTRIX MDR is the human operation behind the platform: seven layers of analysts, hunters, responders and forensic specialists in Cyber Defense Centers across seven countries, working follow-the-sun so there is never a handover gap. They triage every signal, validate every incident, contain and remediate on your behalf under response times written into the contract, and report what happened in language your board can read.

FULL RESPONSE

We act, then tell you

Pre-authorized containment: isolate the host, disable the account, revoke the session. Fastest path to the 30-minute target.

CO-MANAGED

We propose, you approve

The analyst names the action and the impact; your team confirms in the portal or on the call. The clock pauses while you decide.

NOTIFY ONLY

We investigate, you act

A validated incident with the full story and the recommended action, handed to your team or your ticketing system.

Three response models, set per severity and per asset group. Most clients run full response on endpoints and identities, co-managed on production servers.

≤ 30 min
Guaranteed containment on P1 incidents[1]

24×7
Follow-the-sun from Cyber Defense Centers in seven countries

100%
Incidents reviewed by a human analyst before closure[2]

Unlimited
Digital forensics and incident response, no retainer

WHAT IS INCLUDED

Everything a security operations team does, without building one

24×7×365 monitoring

Every signal triaged by an analyst, every minute of the year; cybersecurity engineers reachable around the clock.

Near-zero false positives

Every alert validated, enriched and scoped before you hear about it: 95% fewer alerts reach your team[3], and every incident becomes new detection logic.

Containment and remediation

Surgical actions on the host, account, session or network path. No reimaging by default.

Expert-led threat hunting

The Hunt Cycle run continuously across your telemetry, not only when an alert fires.

Unlimited incident response

Any incident, any time, no usage limits: malware, memory, packet and log forensics by specialists.

Dedicated Account Manager and TAM

A personal liaison for everything about the service, and a Technical Account Manager to optimize and troubleshoot your deployment.

Monthly and real-time reporting

Instant reports and live status in the portal; one monthly report with incidents, SLA performance, coverage and recommendations.

Quarterly reviews and working sessions

Quarterly service reviews aligned to your business objectives, regular working sessions, and a complimentary value-add assessment each quarter.

Board and executive presentations

Tailored briefings for your leadership: security status, risk, and what to do next, in their language.

THE OPERATION

From signal to closed incident: who touches it, and when

Artemis, the LMNTRIX autonomous AI SOC, handles the volume; people handle the judgment. Every detection passes through the same chain, and every action is logged with who took it, why, and what happened next.

AUTOMATE

Artemis

Correlates, enriches with 300+ intel sources, maps to ATT&CK, scores priority, drafts the case.

TIER 1

Event Analysts

Triage every signal, 24×7. Close the noise, escalate the real, nothing reaches you unvalidated.

TIER 2

Incident Analysts

Validate, scope and build the timeline: entry point, movement, objective, blast radius.

TIER 3

Incident Responders

Contain and remediate under your response rules; lead critical incidents live with your team.

OUTCOME

Closed and proven

Root cause, actions taken and the gap closed, in the incident report and the monthly pack.

Forensic and Malware Analysts
Reverse the payload, recover evidence, keep chain of custody.

APT Hunters and Intel Analysts
Run the Hunt Cycle; map global threat activity to your industry and surface.

Integration and Operations
Sensors tuned, integrations live, agent coverage and health tracked.

THE HUNT CYCLE · SURVEY, SECURE, DETECT, RESPOND

Survey. Map the estate, the crown jewels and the paths between them; baseline what normal looks like for your users, hosts and identities.

Secure. Close the exposures the survey found before an attacker uses them; seed deceptions where an intruder would look first.

Detect. Hypothesis-driven hunts from current intelligence and your industry's targeting: living-off-the-land, credential attacks, lateral movement, persistence.

Respond. A confirmed hunt finding becomes an incident and follows the same response chain, with the same clock, as any detection.

Hunts run continuously, not on request. Findings and hunt coverage are reported monthly.

CONTAINMENT, THEN REMEDIATION

Containment stops the attacker now: isolate the host, kill the process, disable the account, revoke the session, push the IOC to your firewall, proxy, DNS and email controls. Minutes, under pre-authorized rules.

Remediation removes what they left and closes how they got in: malicious artifacts and persistence removed, credentials rotated, the exploited gap fixed. Hours to days, in step with your change process.

The two are clocked separately, so a remediation that waits on your change window never counts as a slow containment.

ACTIONS WE CAN TAKE FOR YOU

ISOLATE HOST · KILL PROCESS · DISABLE ACCOUNT · REVOKE SESSION · BLOCK AT FIREWALL · QUARANTINE EMAIL · REMOVE PERSISTENCE · PUSH IOC TO CONTROLS

Pushed by API into the firewall, web, DNS, endpoint, email and identity controls you already run, from the LMNTRIX console. No logging into five portals while the clock runs.

DIGITAL FORENSICS AND INCIDENT RESPONSE · INCLUDED, NOT RETAINED

When an incident becomes a breach, the same team stays on it. Forensic analysts work from full packet capture, endpoint telemetry, memory and logs to establish what was accessed, what left and when, with evidence preserved to a standard that supports legal, regulatory and insurer requirements. No retainer, no hourly clock.

Ransomware. Pre-authorized containment on ransomware indicators: the host is isolated and the account disabled before encryption spreads, then the entry point and lateral path are traced and closed. You receive the timeline, the affected-asset list and the recovery order; we stay engaged through restoration.

THE COMMITMENT

Five clocks, not one. Guaranteed where we control the outcome.

A single "MTTR" hides where time goes. LMNTRIX measures each incident across five named segments, guarantees the ones we control end to end, publishes targets for the rest, and reports all five monthly. The guaranteed figures are worst-case contractual commitments, not aspirations: in practice, critical threats are detected and acted on in minutes, often seconds.

METRIC	P1 CRITICAL	P2 HIGH	P3 MEDIUM	P4 LOW	STATUS
MTTD earliest event → incident created	**≤ 10 min**	≤ 15 min	≤ 30 min	≤ 60 min	GUARANTEED
MTTA incident created → analyst engaged	**≤ 15 min**	≤ 30 min	≤ 2 hrs	≤ 8 hrs	GUARANTEED
MTTI analyst engaged → investigation validated	**≤ 1 hr**	≤ 4 hrs	≤ 12 hrs	≤ 24 hrs	OBJECTIVE
MTTC validated → contained[1]	**≤ 30 min**	≤ 2 hrs	≤ 8 hrs	≤ 24 hrs	GUARANTEED
MTTR contained → remediated, active time[2]	**≤ 24 hrs**	≤ 48 hrs	≤ 5 bus. days	≤ 10 bus. days	OBJECTIVE
Total incident lifecycle gross wall-clock	Reported monthly, per incident, with the segment breakdown				REPORTED

[1] Guaranteed where pre-authorized response actions exist (host isolation, account disable, session revocation, network block). Where your approval is required first, the clock pauses while you decide. [2] Active time: the clock pauses on your approval wait, change window, third-party dependency or requested hold; gross time is reported alongside.

HOW SEVERITY IS SET

P1 Critical. Confirmed active ransomware or data exfiltration, domain or tenant-level compromise, a crown-jewel asset under attack, or a deception trigger on a sensitive decoy.

P2 High. Confirmed malicious activity on a single host or account with a foothold established; privilege escalation or lateral movement attempted.

P3 Medium. Suspicious activity validated as worth action but contained by existing controls; policy violations with security impact.

P4 Low. Hygiene findings, informational detections and hunt observations with a recommendation.

Criteria are written into the service description so the numbers above mean the same thing to both sides.

HOW WE ESCALATE

P1	Immediate phone call to your named contacts and live coordination until contained; executive notification on confirmed exfiltration.
P2	Rapid notification by your chosen channel and guided containment.
P3 / P4	Portal update, ticket in your service desk and analyst follow-up.

CHANNELS

Phone, email, the LMNTRIX portal, Slack or Teams via LISA, and two-way integration with your ticketing system so every incident has a ticket on your side too.

WHAT YOU SEE, AND WHEN

Live, in the portal

Every alert, its status, the actions taken and by whom; asset coverage and sensor health; open items awaiting your decision.

Per incident

Executive summary, timeline, ATT&CK mapping, impact, containment and remediation actions, root cause, lessons and indicators.

Monthly report

Incidents and trends, the five SLA metrics per incident and averaged, hunt activity, coverage changes, threat landscape and recommendations.

All periodic reporting is delivered in the monthly report; there are no separate daily or weekly summaries. A quarterly service review with your Account Manager walks through posture, SLA trends and the value-add assessment; board and executive briefings are prepared on request.

THE ENGAGEMENT

Operational within hours. Steady state within the month.

01
Kickoff
Scope, contacts, crown jewels, response rules and escalation paths agreed with your AM and TAM.

02
Deploy
Agents, sensors and API connections live within hours; detection starts while the rest onboards.

03
Baseline and tune
Normal behavior learned; known-good tools allowed; deceptions placed; first hunt survey done.

04
Authorize
Response model set per severity and asset group; ticketing and chat connected; SLA clock starts.

05
Steady state
First monthly report delivered; quarterly reviews and value-add assessments scheduled.

LMNTRIX PROVIDES

- 24×7×365 monitoring, triage, validation and investigation
- Containment and remediation under your response rules
- Continuous threat hunting and detection engineering
- Unlimited digital forensics and incident response
- Real-time and monthly reporting, quarterly reviews, board briefings
- A dedicated Account Manager and Technical Account Manager, plus 24/7 engineer access

YOU PROVIDE

- Deployment access and an asset list, as good as you have it
- Crown-jewel assets and known-legitimate tools
- Response model per severity: full, co-managed or notify
- Escalation contacts who answer the phone at 3 a.m.
- Change-window and approval decisions within your SLA pause
- Access to your ticketing, chat and the tools you want correlated

WHAT SETS IT APART

	LMNTRIX MDR	VENDOR MDR	TRADITIONAL MSSP
Sees	Every surface, natively, plus your existing tools	Its own product's telemetry	Whatever logs you send
Responds	Contains and remediates, under guaranteed clocks	Isolates, then recommends	Opens a ticket
Measures	Five named segments, reported per incident	One "MTTR", vendor-defined	Ticket SLAs
DFIR	Unlimited, included	Retainer, hourly	Referred out

QUESTIONS. CLEAR ANSWERS.

Can you run MDR on the tools we already have?
Yes. Your existing endpoint, firewall, cloud, identity and SIEM telemetry is ingested and used for enforcement; native modules fill the gaps.

What happens if we don't approve a containment in time?
The clock pauses, the risk doesn't. Most clients pre-authorize containment on endpoints and identities and keep approval for production servers.

WHAT WE NEED TO SCOPE IT

- Endpoints, servers, cloud workloads and identities in scope
- Modules and existing tools to be correlated
- Sites, regions and any data-residency requirements
- Ticketing and chat platforms to integrate

MDR is included with every LMNTRIX XDR module subscription; there is no separate service fee and no DFIR retainer.

Judge the service, not the sales deck.

Thirty days of the full MDR service in your environment at no cost: real detections, real response times, and a findings report whether or not you proceed.

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.