LMNTRIX
BE THE HUNTER | NOT THE PREY

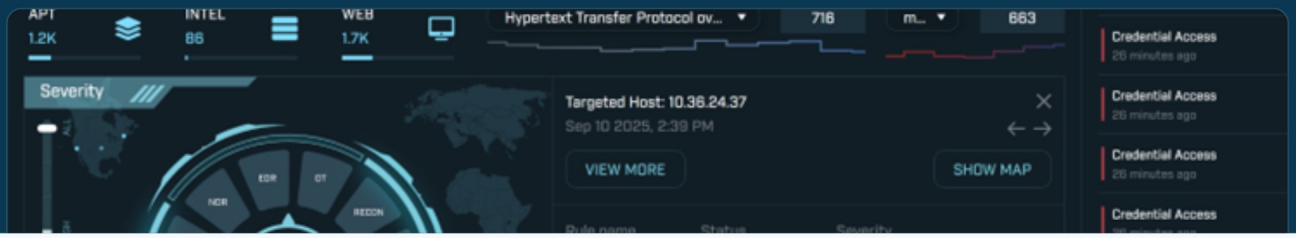
DATASHEET

THE THREAT INTELLIGENCE MODULE OF LMNTRIX XDR

LMNTRIX Intelligence

They're attacking. All the time. Detect earlier. Respond faster.

Every organization is under threat, and most are drowning in noise. LMNTRIX Intelligence aggregates 300+ global, commercial, proprietary and community sources, curates and scores them, correlates them against your own telemetry inside LMNTRIX XDR and hands every validated hit to the Cyber Defense Center, so global signals become local incidents before they become damage.



An intelligence hit in the LMNTRIX XDR heads-up display. A host inside the network reaches a known malicious site; the indicator match, its risk score and the host are already joined for the analyst.

300+
Sources: open, commercial, dark web, LMNTRIX sensors

850M+
Indicators correlated against live telemetry

20–25%
More incidents a month with the feed than without

Indicators age out automatically after about two weeks, so the feed never fills with stale data.

THE CORE CAPABILITIES

From raw indicators to actionable defense

Global aggregation and curation

- 300+ sources, LMNTRIX sensors, dark-web monitoring
- Stale, duplicate and irrelevant indicators removed
- Threat aliases unified across feeds

Enrichment and risk scoring

- DNS, WHOIS, HTTP and certificate context
- IPs, domains, URLs and hashes ranked by severity
- Indicators aged out when they stop being useful

XDR detection and validation

- Matched across EDR, NDR, Packets, SIEM and Deception
- Every hit validated before it becomes an incident
- Rules, reports, dashboards and investigation pivots

Adversary, sandbox and vulnerability context

- MITRE ATT&CK mapping, actor and campaign attribution
- Suspicious files and URLs detonated in a sandbox
- CVE context tied to response playbooks

THE INTELLIGENCE LIFECYCLE

Turn global signals into local action

Six stages take hundreds of millions of raw indicators down to the handful that matter to your environment this week, and attach enough context to each one that an analyst can act on it without a second search.

01
Ingest
Indicators from 300+ feeds and underground sources.

02
Curate
Normalized, de-duplicated, outdated data dropped.

03
Enrich
Infrastructure, reputation and campaign context added.

04
Score
Ranked by severity, relevance and behavior.

05
Correlate
Matched against endpoint, network and identity data.

06
Operationalize
Validated incidents, detection rules and responses.

THE PLATFORM

A native threat intelligence platform, built into XDR

WHERE IT COMES FROM

Open and commercial. 300+ public, private and proprietary sources, including 20+ commercial feeds, consumed over STIX/TAXII.

LMNTRIX sensors. Our own HoneyNet across every AWS region and the sensor network across client estates.

Underground. Dark-web monitoring and interception of threat-actor communications, so TTPs and proof-of-concept attacks are seen before they are used in anger.

Community. A crowd-sourced exchange: researchers in trusted circles share and act on intelligence together.

WHAT IT CATCHES

Automated scenarios. Crimeware, dynamic DNS, phishing attacks and URLs, anonymous VPN and hacking tools, detected the moment a host touches them.

Known-bad infrastructure. Malicious IPs, domains, URLs and hashes matched against every flow, log and process across the estate.

Adversary context. Activity mapped to MITRE ATT&CK and tied to actors and campaigns, with aliases unified so one group is one name.

Files and URLs. Suspicious samples detonated in an isolated cloud sandbox, with CVE context alongside.

HOW YOU USE IT

Search. Any indicator type over any time range, drilling from a hit to its feeds, aliases, linked indicators and news.

Tailor. Intelligence aligned to your industry, geography, assets and operational risk, so finance, healthcare and manufacturing each see what matters to them.

Share. Pre-built rules, reports and dashboards used in LMNTRIX XDR, or applied in your own SIEM console.

Scale. Machine learning that keeps pace with thousands of IOCs a minute across your environment.

See emerging threats continuously
Current intelligence on campaigns, infrastructure, vulnerabilities and attacker behavior.

Fewer false positives
Curation, de-duplication, lifecycle management and analyst validation before anything reaches you.

Faster investigations
Searchable context, attribution and pivots available in the middle of an incident, not after it.

THE MDR SERVICE

Intelligence that is acted on, not just delivered

A feed on its own is a list. LMNTRIX Intelligence is wired into every sensor and agent on your estate, and every hit is handled by the Cyber Defense Center: validated, investigated in context, contained where real, and reported with the evidence, 24 hours a day.

On the endpoint

The feed runs inside the LMNTRIX EDR agents: a matching process, file or connection is validated and raised as an XDR incident.

On the network

The NDR sensor on your premises carries the feed: a flow to a known-bad address, domain or URL is an incident, not a log line.

In the packets

Stored traffic in LMNTRIX Packets is matched as indicators arrive, so a new indicator is replayed against last month's sessions.

In the logs

LMNTRIX SIEM correlates the feed against every log you ship, firewalls to cloud audit trails, and raises hits as incidents.

WHAT THE CYBER DEFENSE CENTER DOES

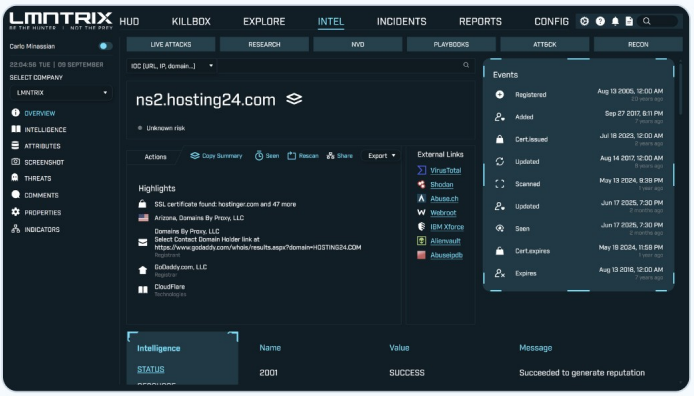
Validates every match. An indicator hit is a lead. Analysts confirm it against the host, the user and the rest of the estate before it reaches you.

Investigates with attribution. Actor, campaign, ATT&CK techniques and linked infrastructure are already attached; the analyst pivots to everything related in one search.

Contains. Endpoint isolation, address blocking and account action through LMNTRIX XDR, with the intelligence as the evidence.

Hunts. New intelligence is run back across historical telemetry to answer "were we hit before we knew?"

Tunes and curates. Feeds, scoring and aging adjusted to your industry, geography and assets, so the noise never comes back.



One indicator in LMNTRIX XDR. Risk, certificate and registrar highlights, external research links and the indicator's own history, from the Intel tab that sits beside Killbox, Explore and Incidents.

EVENTS
Every flow, log and process collected across the estate.

MATCHES
Those that touch a curated, scored indicator.

ATTACKS
Matches that correlate with activity on the host or user.

INCIDENTS
Attacks confirmed by an analyst and escalated with evidence.

CONTAINED
Isolated, blocked and remediated with you, then fed back as new intelligence.

The funnel the CDC works every day. In practice, LMNTRIX XDR detects 20 to 25 percent more incidents a month with the intelligence feed than without it.

THE DEPLOYMENT

Native to XDR	Hosted in the LMNTRIX cloud as a feature of LMNTRIX XDR; nothing to install.
Consumed by	LMNTRIX EDR, NDR, Packets and SIEM as standard; the intelligence is already in the sensors you run.
Your own stack	Optionally, the feed delivered over standard protocols into your existing SIEM, EDR or next-generation firewalls.
Private TIP	For whole-of-government and industry sectors, available as a private threat intelligence platform for the community it serves.

THE SERVICE

Who does what

A subscription feature of LMNTRIX XDR: LMNTRIX gathers, curates and operates the intelligence; you tell us what your business looks like.

LMNTRIX PROVIDES

- 300+ sources aggregated, curated and de-duplicated
- Enrichment, risk scoring and indicator aging
- The feed inside every LMNTRIX sensor and agent
- Validation of every hit by the CDC
- Rules, reports and dashboards, kept current
- 24-hour access to the Cyber Defense Center

YOU PROVIDE

- Your industry, geographies and critical assets
- Domains, IP ranges and brands you want watched
- Which LMNTRIX modules are deployed
- Third-party SIEM, EDR or firewalls to receive the feed
- Who receives escalations, and on which channels
- Feedback on hits, which tunes the scoring

WHAT SETS IT APART

CAPABILITY	LMNTRIX INTELLIGENCE	A THREAT FEED
Sources	300+, LMNTRIX sensors, dark web	One vendor's view
Noise	Curated, scored, aged out in ~2 weeks	Stale indicators accumulate
Correlation	Native in EDR, NDR, Packets and SIEM	You build the integration
A hit	Validated incident, analyst-handled	An alert for your queue
Context	ATT&CK, actors, sandbox, CVEs	An indicator and a score
Relevance	Tuned to your industry and assets	Same feed for everyone

QUESTIONS. CLEAR ANSWERS.

Can we use it outside LMNTRIX XDR?

Yes. The curated feed is delivered over standard protocols into your SIEM, EDR or firewalls, with the rules and dashboards for your own console.

Does it analyze suspicious files and URLs?

Yes. Samples are detonated in an isolated cloud sandbox and the verdict joins the indicator's record.

WHAT WE NEED TO SCOPE IT

- Which LMNTRIX XDR modules are in place or planned
- Industry, geographies and crown-jewel assets
- Third-party tools that should receive the feed
- Whether a private TIP is required for your community

Subscribed with LMNTRIX XDR, MDR included. Live in your sensors the day the subscription starts.

Know the adversary. Before they arrive.

Every engagement starts with a free 30-day proof of concept on your own telemetry, plus a complimentary quarterly value-add assessment.

BOOK A DEMO

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.