LMNTRIX

BE THE HUNTER | NOT THE PREY

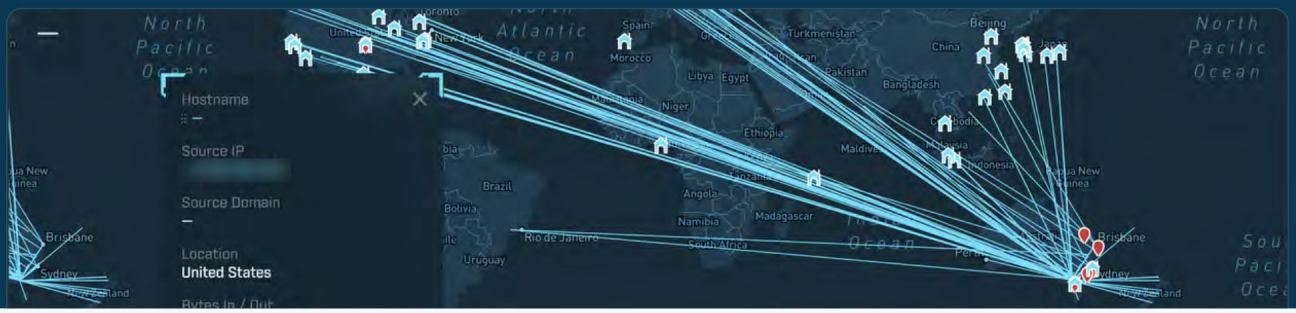
DATASHEET

THE SECURITY INFORMATION AND EVENT MANAGEMENT MODULE OF LMNTRIX XDR

LMNTRIX SIEM

Your SIEM Sees Alerts. We See Attacks.

Traditional SIEM floods teams with alerts, hides real threats in noise, and drives up cost. LMNTRIX turns fragmented signals into clear, actionable defense: every log centralized and correlated, searched in under a second, enriched with threat intelligence and rebuilt into the full attack story, on a cloud platform hosted and operated by LMNTRIX.



The SIEM network map in LMNTRIX XDR. Every flow in the log data drawn between the hosts that produced it, with the source behind each line one click away, beside the endpoint, identity and cloud modules.

<1 s
Forensic queries across billions of events

90 days
Standard online, searchable retention

9 months
Standard archive: one year of evidence in total

Standard subscription configuration. Additional online and archive capacity is available on request.

THE CORE CAPABILITIES

Security data built for investigation and action

Centralized collection and correlation

- Logs, events and metrics from every layer of the estate
- Normalized to the LMNTRIX Common Schema
- Activity correlated across sources into one incident

Codified detection and machine learning

- Practitioner-built rules mapped to MITRE ATT&CK
- Custom rules: your conditions, thresholds and actions
- Behavioral baselines flag the unknown

Forensic search and retrospection

- Sub-second search across very large event volumes
- Attack timelines and root cause rebuilt from history
- Graph views of users, devices and events

Intelligence and native XDR response

- Every event enriched with 300+ intelligence feeds
- Block an IP, disable an account, isolate an endpoint
- Alerts to email, chat, ticketing, SOAR, webhooks

THE DATA LIFECYCLE

From disconnected events to a complete attack story

Every log goes through the same six stages, so an alert is never read on its own: it arrives already tied to the user, the host, the indicator and the rest of the activity around it.

01
Collect
Cloud, endpoint, identity, network, OS and application sources.

02
Normalize
Parsed and mapped into the LMNTRIX Common Schema.

03
Correlate
Users, hosts, alerts, indicators and activity linked together.

04
Detect
Rules, machine learning, intelligence and behavioral baselines.

05
Investigate
Search history, rebuild timelines, visualize relationships.

06
Respond
Escalate, then act through XDR, SOAR, ticketing or webhooks.

THE DETECTION STACK

Proven content, real context, native action

DETECTION CONTENT

Codified rules. A preconfigured library aligned to MITRE ATT&CK, written by incident responders from real engagements.

Custom rules. A rule builder for behavior specific to your environment: conditions, thresholds and the alert action each one triggers.

Machine learning. Prebuilt or custom anomaly jobs baseline users, hosts and data sources, then flag the deviations: unusual logins, odd data volumes, insider activity.

Real time. Rules and models run as events land, so alerts fire while the activity is still happening.

CONTEXT AND ENRICHMENT

LMNTRIX Common Schema. One data model for every source, so searches, correlations and dashboards use the same field names regardless of vendor.

LMNTRIX Intelligence. 300+ open-source, commercial and LMNTRIX sensor-network feeds, curated and de-duplicated, matched against every event for IP, domain, hash and behavior reputation.

Graph analytics. Relationships between users, devices, alerts and indicators drawn as a graph, so lateral movement reads as a path, not a list.

XDR telemetry. Endpoint, network, identity, email and cloud signals from the other LMNTRIX modules sit in the same store.

VISIBILITY AND ACTION

Dashboards. Real-time views of alerts, incidents, trends and operations, tailored for the SOC, for compliance and for leadership.

Alerting. Rule-driven alerts to email, Slack, PagerDuty, Jira or any webhook, with the threat indicators that fired them.

Native XDR response. Block an IP, disable a user account or isolate a compromised endpoint from the incident itself; integrate with SOAR and ticketing where you already have them.

Validation. With monitoring from LMNTRIX, every SIEM alert is validated by the Cyber Defense Center before it reaches you.

THE DIFFERENCE

Investigate without drowning in noise
Built around high-fidelity XDR telemetry and the use cases that matter, not every log you can ship.

Search at incident speed
Sub-second queries and interactive timelines shorten post-breach analysis when every hour counts.

Security and compliance together
Centralized retention, reporting and audit evidence for GDPR, HIPAA and PCI DSS from the same store.

THE DEPLOYMENT

Cloud-delivered, fully operated, fed by lightweight shippers

There is no SIEM server to build, patch or scale. LMNTRIX hosts and operates the platform; lightweight LMNTRIX Data Shippers at your end collect, filter and forward the logs, and cloud sources connect through their native APIs.

Data sources

Network devices, endpoint agents, operating systems and applications; AWS CloudTrail, Microsoft Azure and Google Cloud; Zeek, Sysmon and any third-party endpoint tool.

LMNTRIX Data Shippers

Lightweight shippers per log type, with filtering and transformation at source, so logs arrive standardized and enriched, and you ship only what matters.

Unsupported sources

An event source without an out-of-the-box parser gets one written by LMNTRIX at no extra cost, typically within days to a few weeks depending on complexity.

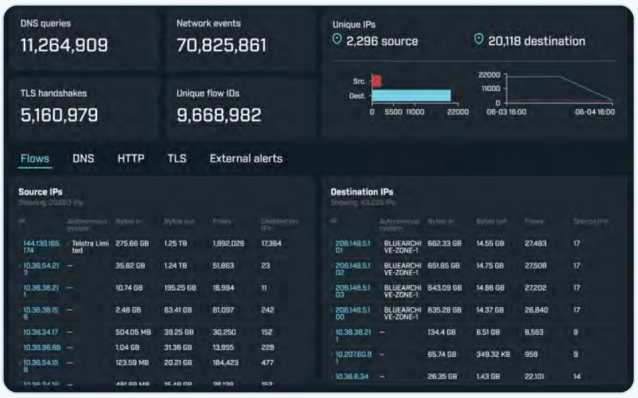
Scale and tenancy

Data distributed across clusters that scale horizontally, from a single site to a large enterprise. Multi-tenant with strict data segregation for MSSP partners.

SUBSCRIPTION AND RETENTION

Delivery	Cloud SaaS subscription of LMNTRIX XDR, inclusive of platform operations, maintenance and 24×7 support from the Cyber Defense Center.
Sizing	Tiered on daily ingestion, from 1 GB/day to 100+ GB/day. Parsers, detection content and threat intelligence are included at every tier.
Online retention	90 days searchable at sub-second speed as standard.
Archive	A further 9 months as standard, for one year of evidence; more online or archive capacity on request.
Monitoring	Optional 24×7 SIEM alert monitoring and incident response by LMNTRIX or a certified partner.
Your SIEM	Keep it if you must: LMNTRIX XDR alerts can be forwarded to it, or its logs consumed by LMNTRIX SIEM.

THE SIEM WORKSPACE



The Network view. One day of logs summarized as DNS queries, network events, TLS handshakes and unique flows, with the source and destination tables beneath ready to pivot into a timeline.

Network	**Hosts**	**Users**
Discover	**Rules**	**Timelines**

Six views inside LMNTRIX XDR, beside the identity, mobile and cloud modules, so an analyst moves from a log to the host, the user and the rule that fired without changing console.

THE USE CASES

Post-breach forensics

Rebuild how they got in, where they went and what they touched from a year of evidence.

Insider threat and hunting

Behavioral baselines and ATT&CK-mapped hunts surface misuse that never trips a signature.

Compliance and audit

Centralized log management, retention and reporting that stand up to an auditor.

THE SERVICE

Who does what

A cloud subscription of LMNTRIX XDR: you point the logs at us, LMNTRIX runs the platform and, if you choose, the monitoring too.

LMNTRIX PROVIDES

- The hosted platform: storage, compute, operations
- Guided onboarding of every log source
- Parsers for every source, built for you if needed
- Detection content, ML jobs and intelligence, kept current
- Dashboards for SOC, compliance and leadership
- 24-hour access to the Cyber Defense Center

YOU PROVIDE

- Log sources and their estimated daily volume
- A host or VM for the data shippers at each site
- Outbound connectivity to LMNTRIX XDR
- API credentials for cloud and SaaS sources
- Sample logs for any source needing a parser
- Who receives alerts, and on which channels

WHAT SETS IT APART

CAPABILITY	LMNTRIX SIEM	LEGACY SIEM
Platform operations	Hosted and operated by LMNTRIX	Your servers, your engineers
Detection content	Practitioner-built, ATT&CK-mapped	Written and tuned by you
Telemetry	XDR signals plus your logs	Every log, every bit of noise
Response	Native XDR actions from the incident	Alerts into a queue
New sources	Parsers built at no extra cost	Professional services
Retention	One year standard, extendable	Hot storage at a premium
Commercials	Tiered on GB/day, operations included	Per-GB licenses plus hardware

QUESTIONS. CLEAR ANSWERS.

Do I still need my existing SIEM?

Only if your size warrants one. Compliance, reporting and post-breach forensics are the usual drivers; LMNTRIX SIEM covers all three, often for less than your current licensing.

Is it managed, or just hosted?

Both. The platform is always operated by LMNTRIX; 24×7 alert monitoring and incident response by the Cyber Defense Center or a certified partner is optional on top.

WHAT WE NEED TO SCOPE IT

- Daily log ingestion in GB/day, and the source list
- Online and archive retention beyond the standard year
- Monitoring by LMNTRIX, a partner or your own team
- Whether LMNTRIX XDR modules feed it, or logs only

Tiered on ingestion, platform operations included. Supported sources are live within days of the shippers connecting.

Every event. One attack story.

Every engagement starts with a free 30-day proof of concept on your own logs, 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.