LMNTRIX

BE THE HUNTER | NOT THE PREY

DATASHEET

THE ICS/OT SECURITY MODULE OF LMNTRIX XDR

LMNTRIX ICS/OT Security

Protect what runs the world.

Managed detection and response for ICS, SCADA, IoT, and critical infrastructure. LMNTRIX ICS/OT Security deploys independent, passive telemetry behind your existing OT firewalls and controls, treats those controls as already bypassed, and gives our Cyber Defense Centers the visibility to detect, hunt, validate, disrupt, and respond to attackers moving across IT and OT — without disrupting production.

99.9%
Uptime maintained during security operations

95%
Reduction in time to detect ICS/OT threats

80%
Decrease in false-positive alerts

Customer success metrics across LMNTRIX ICS/OT Security deployments. Source: lmntrix.com/mxdr-ot-security

THE CORE CAPABILITIES

Multi-layer defense for industrial environments

Network, device, application, intelligence, and deception controls across IT and OT, unified in one XDR architecture.

Asset Discovery & Visibility

- Automatic discovery and classification of industrial and IoT assets
- Rogue devices and unauthorized changes identified
- Network topology, communications, and device behavior mapped

ICS/SCADA Threat Detection

- Deep inspection of Modbus, DNP3, IEC 104, BACnet, OPC, Profinet, and S7
- Operational baselines with anomaly detection
- Behavioral, machine-learning, signature, and vulnerability detections combined

Segmentation & Lateral Movement

- Isolation between enterprise and industrial networks validated
- Abnormal commands, protocol misuse, and cross-zone movement detected
- Compromised devices exposed by shifts in communication patterns

Industrial Deception

- Decoy industrial systems, services, and credentials deployed
- Reconnaissance and lateral movement caught before real

ICS/OT Endpoint & Forensic Security

- Windows and Linux coverage, including HMI and control servers
- Detection-only mode where

Analytics, Intelligence & Response

- Industrial logs, telemetry, vulnerabilities, and threat intelligence correlated
- Custom dashboards, long-

THE DEPLOYMENT MODEL

Passive by design, operated 24×7

Sensors watch SPAN/TAP ports behind the OT firewall, lightweight agents cover supported Windows and Linux hosts, and decoys sit beside real assets. Everything reports to LMNTRIX XDR over an encrypted channel and is monitored around the clock by LMNTRIX Cyber Defense Centers.

Where LMNTRIX ICS/OT sits in the Purdue model

LEVEL 4–5 · ENTERPRISE IT
Business systems. LMNTRIX XDR correlates IT and OT telemetry to expose IT-to-OT movement.

LEVEL 3.5 · INDUSTRIAL DMZ
NDR and Packets sensors on SPAN/TAP ports behind the OT firewall, inspecting traffic from the levels below. Decoys.

LEVEL 3 · SITE OPERATIONS
EDR on SCADA servers, historians, and jump boxes. Decoys.

LEVEL 2 · SUPERVISORY CONTROL
EDR on HMIs and control servers, detection-only where required. Decoys.

LEVEL 0–1 · PROCESS & CONTROL
PLCs, RTUs, and field devices are observed passively through their traffic. Nothing is installed on them.

COMPONENT	WHAT IT DELIVERS	WHERE IT RUNS
NDR for ICS/OT	Passive asset inventory, vulnerability assessment, and protocol-aware threat detection combining machine learning, behavioral analysis, and signatures.	SPAN/TAP sensor, Level 3.5
Packets for ICS/OT	OT network metadata captured and retained for a minimum of 30 days for retrospection, threat hunting, and post-breach forensics.	SPAN/TAP sensor, Level 3.5
EDR for ICS/OT	Next-generation antivirus and endpoint detection and response for Windows and Linux OT hosts, with a detection-only mode and HTTP CONNECT / SOCKS5 proxy support for restricted networks.	HMIs, SCADA servers, historians, jump boxes
Deceive for ICS/OT	Decoys, breadcrumbs, tags, and personas layered across endpoints, servers, and network components to catch attackers with a foothold who are trying to move laterally.	Appliance or VM, Levels 2–3.5
Intelligence for ICS/OT	Real-time feeds on OT and IoT threats and vulnerabilities, mapped to your discovered assets for detection and context.	LMNTRIX XDR
LMNTRIX XDR	Centralized multi-site management, correlation, automation, analytics, and incident management over an encrypted channel, operated 24×7 by LMNTRIX Cyber Defense Centers and delivered with analyst training.	Cloud

THE SERVICE LIFECYCLE

01 Discover
Passive inventory of every asset, protocol, and communication path.

02 Baseline
Normal device and protocol behavior learned per site and zone.

03 Detect
Anomalies, protocol misuse, endpoint threats, and deception triggers.

04 Investigate
Protocol-aware forensics that explain what happened in industrial terms.

05 Contain
Controlled containment through firewall and NAC, coordinated with your operations team.

THE VISIBILITY ON DAY ONE

THE COVERAGE

Built for cyber-physical operations

The same integrated detection and response architecture applied across the industrial systems your organization cannot afford to stop.

THE PROTOCOLS

Modbus | DNP3 | IEC 104 | BACnet | OPC | Profinet | S7

Encrypted flows are monitored for abnormal patterns; full payload inspection of encrypted traffic is available through decryption integrations.

THE INDUSTRIES

- Manufacturing — production lines, robotics, automation
- Energy & Utilities — generation, transmission, smart grid
- Water & Wastewater — treatment, chemical feeds, distribution
- Oil & Gas — drilling, pipelines, refineries, tank farms
- Transportation — rail, airports, ports, maritime, fleets
- Chemical & Pharmaceutical — process, safety, batch systems

COMPLIANCE & INTEGRATIONS

Standards: monitoring, asset management, and reporting aligned with NIST, IEC 62443, NERC CIP, and GDPR.

Integrations: firewalls, NAC, SIEM, ticketing, network management, and open APIs.

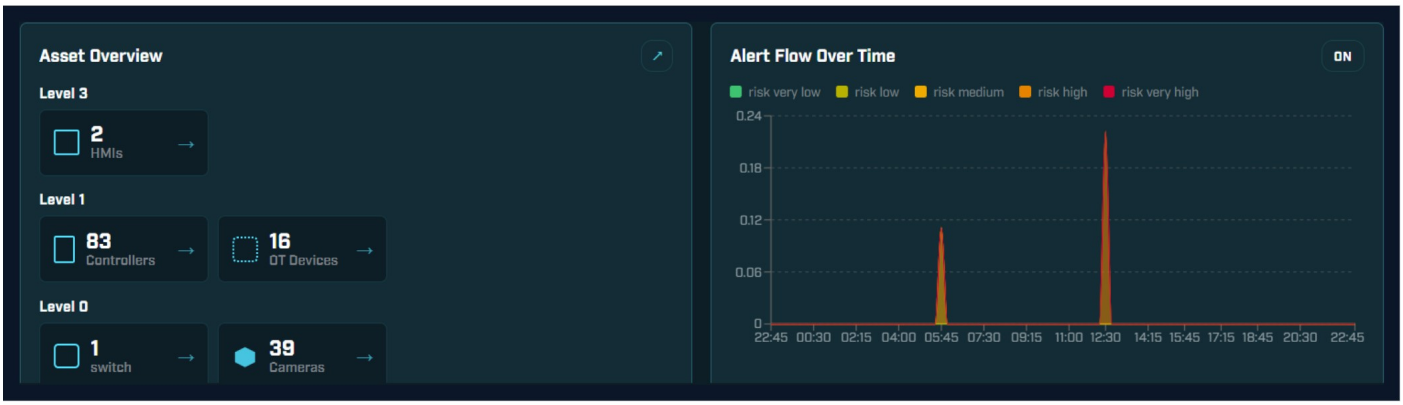
Alerting: email, SMS, and SIEM, tuned by event type, severity, and frequency.

Data protection: encryption in transit and at rest, role-based access control.

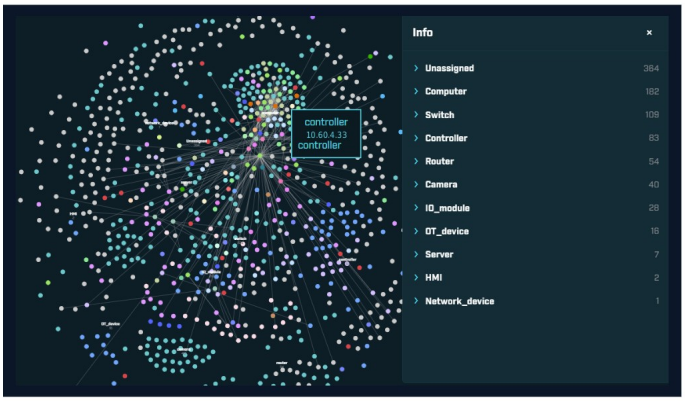
THE PLATFORM

One console for IT and OT

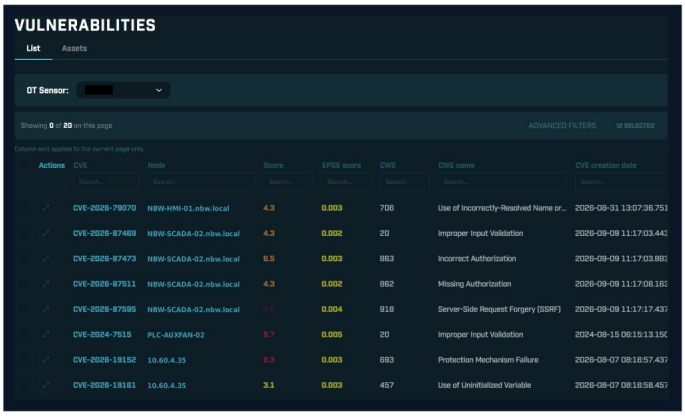
Your ICS/OT sensors report into the same LMNTRIX XDR console as every other module, so an alert on a controller is seen beside the endpoint, identity, and network activity that led to it. The views below are taken from a live LMNTRIX ICS/OT deployment.



ICS/OT dashboard. Assets grouped by Purdue level (HMIs at Level 3, controllers and OT devices at Level 1, switches and cameras at Level 0) beside alert flow over time, scored from very low to very high risk.



Asset graph. 886 nodes discovered and classified passively — controllers, switches, routers, cameras, I/O modules, HMIs, servers — with every observed communication path drawn between them.



Vulnerabilities. CVEs matched to each discovered asset with CVSS severity, EPSS exploit probability, and CWE class, so patch windows are spent on what attackers actually use.

THE REPORTING

Evidence your engineers and auditors can use



Every ICS/OT sensor produces scheduled reports in addition to live dashboards. Reports and dashboards are customizable per site and per audience, and carry the same evidence used in NIST, IEC 62443, and NERC CIP reviews.

Asset inventory
Assets and nodes by Purdue level, operating system, firmware version, technology type, and multi-homed devices.

Vulnerability and risk
CVEs per asset with CVSS, EPSS, and CWE, prioritized by exploitability.

Alerts and traffic
Alert flow by risk, protocol usage, sessions, and throughput over the reporting period.

Monthly MXDR service report
Incidents handled, response times, and recommendations from your Cyber Defense Center.

WHAT IS INCLUDED

- 24×7 monitoring, threat hunting, and response from LMNTRIX Cyber Defense Centers
- Passive ICS/OT sensors, endpoint agents, and decoys, deployed and tuned by LMNTRIX
- Multi-site remote monitoring from one console
- Custom dashboards, long-term retention, and rapid search
- Scheduled reporting and SIEM, firewall, NAC, and ticketing integration
- Onboarding and training for platform use, deployment management, and incident response
- A complimentary quarterly value-add assessment for every client

WHAT WE NEED TO SCOPE IT

Pricing is based on the industrial footprint, not on alert volume. To quote, LMNTRIX needs:

- Number of sites with OT assets
- Total number of OT assets
- Windows and Linux hosts in the OT environment (HMIs, SCADA servers, historians, jump boxes)
- Daily log ingestion (GB/day), if SIEM is in scope

Sensors ship pre-configured; a typical site is live within days of a SPAN/TAP port being made available.

Prove it in 30 days.

Every LMNTRIX engagement starts with a free 30-day proof of concept in your own environment. See your assets, your traffic, and your threats before you commit.

Book a demo · lmntrix.com/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. LMNTRIX ICS/OT Security is a module of LMNTRIX XDR.