LMNTRIX
BE THE HUNTER | NOT THE PREY

DATASHEET

THE EXTERNAL THREAT MONITORING MODULE OF LMNTRIX XDR

LMNTRIX Recon

If attackers are talking about you, we're already listening.

Your greatest risks may already be exposed, outside your network. LMNTRIX Recon finds stolen credentials, leaked data, phishing infrastructure, brand impersonation, supply-chain exposure and adversary interest across deep, dark and indexed sources, and the Cyber Defense Center validates every finding before it reaches you.



A Recon alert in the LMNTRIX XDR heads-up display. An underground finding arrives as an incident beside every other module, already validated and prioritized by an analyst.

16 bn
Email addresses indexed from breaches

900M+
Underground documents archived

47
Languages monitored, plus human intelligence

On an average day Recon identifies and reports more than 1 million compromised IP addresses and 80,000 compromised email accounts.

THE CORE CAPABILITIES

See the threats forming outside your network

Darknet Intelligence

- Forums, markets, onion sites, IRC, paste sites, P2P
- Attack chatter, target lists and threat-actor interest
- Human intelligence inside closed communities

Breach Intelligence

- Employee, customer and partner PCs hit by infostealers
- Stolen credentials and session cookies
- Taken from the malware's own C&C traffic

Brand and domain protection

- Lookalike domains caught soon after registration
- Fake profiles, fraudulent apps, social-media abuse
- Executive impersonation and VIP exposure

Third-party and supply-chain risk

- Breaches involving suppliers, vendors and affiliates
- Indirect paths into your estate surfaced early
- Exposure trends and peer benchmarking

THE TWO INTELLIGENCE FEATURES

Where they are talking, and what they already hold

Darknet Intelligence listens to the underground: who is targeting you, selling access to you or trading your leaked data. Breach Intelligence watches the machines: employee, customer and partner computers already infected with infostealer and remote-control malware, and everything the malware took.

DARKNET INTELLIGENCE

Sources. Hidden criminal forums (280 and counting), black markets, onion sites, private sites, IRC channels, paste sites, peer-to-peer and file-sharing networks, social platforms and 640,000+ botnets, monitored 24×7, 365 days a year.

Reach. The largest commercial darknet archive, 900M+ documents, searched in 47 languages; proprietary crawling that defeats the anti-bot defenses of underground sites.

Human intelligence. Decade-long networks inside closed communities, for the conversations no crawler can reach.

What it finds. Attack planning and target lists, hacktivism, actor chatter about your brand or executives, breached databases and credential dumps, leaked documents and source code, exploitable data indexed by search engines, phishing domains soon after registration.

BREACH INTELLIGENCE

Sources. Intelligence harvested from the command-and-control infrastructure of infostealer and remote-control malware: the logs the malware uploads from every computer it infects, collected as new infections appear.

Whose machines. Employees logging into your corporate systems, customers logging into your apps and portals, and suppliers or partners with access to your environment, matched by your domains and URLs.

What it finds. The credentials and session cookies the stealer captured, the corporate URLs they unlock, the malware family and infection date, and the infected device itself: hostname, operating system, antivirus and the path the malware ran from.

What happens next. Each infected machine arrives as an incident with the affected accounts and the action: reset the credentials, kill the sessions, rebuild the device, check for use of the stolen access.

THE EXPOSURE COVERAGE

Find what attackers know about you

Attack indications
Your name in target lists, bids to attack you in hacker forums, campaigns being planned and coordinated.

Data leakage
Credentials, secret documents, source code and internal network detail, leaked by intruders or by careless insiders.

Phishing and brand abuse
Lookalike domains caught at registration, fake pages, profiles and apps that steal from your customers in your name.

Supply-chain exposure
Breaches and compromised data tied to vendors, affiliates and partners, with trend analysis across your supply chain.

VIP protection
Executive credentials, leaked personal data, fake profiles and chatter about your most valuable people.

Exploitable data
Published web vulnerabilities, database and software versions and other detail a skilled attacker pieces together.

Earlier warning
Exposed data, attack planning and phishing infrastructure surface before any internal control can see them.

Verified, not raw
Machine learning ranks relevance; intrusion analysts confirm it. You see incidents, not underground mentions.

Beyond credentials
Brands, executives, source code, domains, suppliers, mobile apps and contracts, as well as passwords.

THE MDR SERVICE

An underground mention becomes an incident you can act on

Recon is a managed service, not a feed. Nothing reaches you until an intrusion analyst in the Cyber Defense Center has confirmed it is real, relevant and yours, and when it does, it arrives as a LMNTRIX XDR incident with the evidence, the impact and the recommended action attached.

01
Detect
Crawlers, search-engine piggybacking and human sources, around the clock.

02
Analyze
Proprietary data mining and machine learning categorize and rank each find.

03
Validate
An analyst confirms the threat exists and is relevant; false positives stop here.

04
Prioritize
Classified by type and criticality, correlated with your internal telemetry.

05
Escalate
An incident ticket in LMNTRIX XDR, with impact and recommendations.

WHAT THE CYBER DEFENSE CENTER DOES

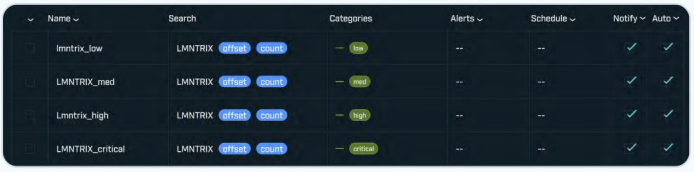
Assesses every find. Each candidate goes through a false-positive assessment and classification by an intrusion analyst before anyone is told.

Explains the impact. The ticket says what was found, where, what an attacker could do with it and what to change: reset these passwords, enforce MFA here, take down this domain.

Correlates inside. A leaked credential is checked against logins in LMNTRIX Identity and SIEM; a phishing domain is blocked at email and DNS; a leaked document is matched to the endpoint it left.

Tracks and trends. Compromised data tracked over time, with peer and industry benchmarking of your exposure.

Baselines first. A 2-day Quick Scan or a 15-day Exposure Analysis establishes what is already out there before monitoring begins.



Trackers in LMNTRIX XDR. Every keyword you give us becomes a tracker with its own category, severity threshold and notification route; the CDC tunes them as your business changes.

WHAT YOU RECEIVE

Six incident types: attack indications, data leakage, brand security, phishing, exploitable data and VIP protection. Each escalated by the CDC with evidence, impact and a recommendation; remediation stays in your hands, with our guidance.

THE SUBSCRIPTION

Basic
Credential exposure only: usernames and passwords for your domains.

Premium
All data types in multiple languages, with human intelligence: security (credentials, personas, breaches, physical, source code, hacktivism, botnets, vulnerabilities), legal and compliance (mobile apps, employees, data loss, PII) and reputation (products, contracts, brand abuse, executive profiles).

PREMIUM LEVEL	KEYWORDS	QUERIES / MONTH
Basic	5	Up to 10
Basic+	20	Up to 40
Bronze	50	Up to 100
Silver	150	Up to 300
Gold	250	Up to 500
Platinum	Unlimited	Unlimited

THE SERVICE

Who does what

A subscription feature of LMNTRIX XDR: you tell us what to watch; LMNTRIX watches, validates and escalates.

LMNTRIX PROVIDES

- 24×7 monitoring of deep, dark, social and indexed sources
- A baseline Quick Scan or Exposure Analysis
- Analysis and false-positive assessment of every find
- XDR incident tickets with impact and recommendations
- Exposure trending and peer benchmarking
- 24-hour access to the Cyber Defense Center

YOU PROVIDE

- Company names, domains and IP ranges to watch
- Products, assets, source code and contracts to watch
- Executive profiles and the PII that identifies them
- Supply-chain entities in scope
- Who receives escalations, and on which channels
- Remediation of what we find, with our guidance

WHAT SETS IT APART

CAPABILITY	LMNTRIX RECON	A DARK WEB FEED
Sources	Darknet archive, infostealer intel, HUMINT	Crawlers on what is public
Languages	47	Mostly English
Validation	Analyst confirms every find	Raw mentions, your triage
Delivery	XDR incident, impact, next step	Email digest or portal
Context	Correlated with your telemetry	Standalone
Scope	Credentials, brand, VIPs, suppliers	Credentials

QUESTIONS. CLEAR ANSWERS.

Does Recon remediate what it finds?

No. Recon monitors and escalates validated incidents with a recommended action; remediation, from password resets to takedowns, is yours, with our guidance.

Can it watch third parties and executives?

Yes. Suppliers, affiliates, VIPs and repeat offenders are keywords like any other.

WHAT WE NEED TO SCOPE IT

- Basic (credentials) or Premium (all data types, HUMINT)
- How many keywords, and in which languages
- Executives, brands and suppliers in scope
- Quick Scan or Exposure Analysis to baseline

Priced by Premium level, MDR included. Monitoring begins the day the keyword sheet is returned.

Your data is already out there. Be the first to know.

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