LMNTRIX
BE THE HUNTER | NOT THE PREY

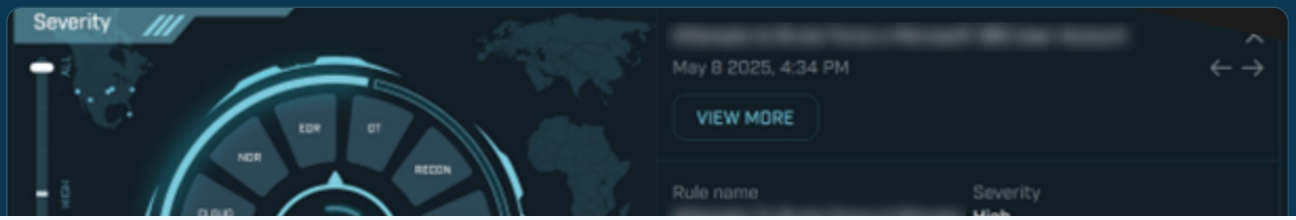
DATASHEET

THE IDENTITY THREAT DETECTION & RESPONSE MODULE OF LMNTRIX XDR

LMNTRIX Identity

Identity is your new perimeter. We hunt the attacker who already has a password.

LMNTRIX Identity watches every login, privilege change and directory query across Active Directory, Entra ID, Microsoft 365, AWS, Okta, GCP and Google Workspace, then adds AD audit, attack-path analysis, AD decoys and leaked-credential monitoring. The Cyber Defense Center validates every detection and blocks the account before the attacker can use it.



An Identity alert in the LMNTRIX XDR heads-up display. A high-severity brute-force detection, already matched to the user.

125+
Identity detection rules, plus machine-learning baselines

7
Identity platforms covered, on-premises and cloud

5
Service elements in one XDR workflow

THE FIVE SERVICE ELEMENTS

Multiple signals. One identity story.

01
Threat detection & response
125+ rules and ML baselines; confirmed threats blocked.

02
Active Directory audit
Upfront and annual audit of accounts, privileges and settings.

03
Attack paths
The privilege chains from any account to your crown jewels.

04
AD decoys
Fake credentials and services only an attacker would touch.

05
Credential leak monitoring
Staff passwords found underground before they are reused.

THE THREAT COVERAGE · STOP THE ABUSE OF TRUSTED ACCESS

Credential theft
Stolen or exposed usernames, passwords and tokens in use.

Brute force
Repeated failures caught, account locked automatically.

Privilege escalation
Dangerous permission changes on high-value accounts.

Lateral movement
The identity links an attacker uses to move between systems.

Insider risk
Unusual access and behavior outside a user's baseline.

Credential exposure
Identities leaked or sold underground, found before reuse.

THE SERVICE ELEMENTS IN DEPTH

What IAM and MFA cannot see

Access controls decide who may log in. LMNTRIX Identity watches what happens after, maps the paths an attacker would take, plants the credentials they would steal, and learns when your real ones already have been.

01 · IDENTITY THREAT DETECTION & RESPONSE

Sources. Active Directory, Microsoft Entra ID, Microsoft 365, AWS, Okta, GCP and Google Workspace, collected by agent or API into LMNTRIX XDR.

Detection. 125+ identity rules across user activity, user attributes and device characteristics, plus machine-learning jobs that baseline each user and flag what no rule anticipated.

Response. Confirmed compromise is blocked through API integration with your Microsoft tenant: account disabled, sessions revoked. Brute force is locked down automatically.

02 · ACTIVE DIRECTORY AUDIT

When. A comprehensive audit at onboarding and a reassessment every year, delivered as a report in LMNTRIX XDR.

What it checks. Stale and orphaned objects, excessive privileges, misconfigurations, trusts between directories and control anomalies, each scored into a domain risk level.

What you get. A prioritized remediation plan: the rules to fix first to bring the score down fastest, with on-premises and hybrid coverage.

03 · ATTACK PATHS

How. A lightweight sensor on the domain controller collects users, groups, computers, permissions and memberships and maps the relationships between them.

What it shows. Every direct and indirect chain from an ordinary account to domain admin or a critical system: the escalation and lateral movement an attacker would use.

What you get. The dangerous rights ranked and visualized, custom queries on request, and the shortest paths cut before anyone walks them.

04 · AD DECOYS, FROM LMNTRIX DECEIVE

What. Decoy user accounts, service accounts and service principal names seeded into your directory, indistinguishable from the real thing to anyone enumerating it.

What it catches. Reconnaissance, directory enumeration, ticket requests against the decoy and any use of its credentials. Nothing legitimate touches a decoy, so every alert is real.

Why it matters. An attacker with valid credentials looks like a user to every other control. The decoy is the one thing they cannot avoid.

05 · CREDENTIAL LEAK MONITORING, FROM LMNTRIX RECON

Your passwords are already for sale. Know before they are used.

Dark-web markets, paste sites, underground forums and infostealer logs are monitored for your domains. When an employee credential is leaked or offered for sale, the account is flagged in XDR, its logins checked, and the CDC forces a reset before credential stuffing or reuse turns the leak into a breach.

THE LIFECYCLE

Audit, baseline, detect, validate, respond

01
Audit
Directory scored, attack paths mapped, decoys seeded.

02
Baseline
ML learns how each user, device and location normally behaves.

03
Detect
Rules, anomalies, decoys and leaked credentials raise alerts.

04
Validate
An analyst confirms it and correlates endpoint and network.

05
Respond
Account blocked, sessions revoked, incident reported.

THE MDR SERVICE

A suspicious login becomes a blocked account, not a ticket in your queue

Identity is a managed service. The Cyber Defense Center tunes the detections, validates every alert, blocks the account through your identity platform, runs the audits and the hunts, and keeps the decoys and the credential watch current, 24 hours a day.

01
Detect
Rules, anomalies, decoy touches and leaked credentials fire in XDR.

02
Validate
An analyst confirms it is real and whose account and device are involved.

03
Contain
Account disabled, sessions revoked, password reset, host isolated.

04
Hunt
Identity hunts across logins, privileges and paths, on a cadence.

05
Harden
Audit findings and attack paths become a tracked remediation plan.

WHAT THE CYBER DEFENSE CENTER DOES

Tunes the detections. The 125+ rules and the ML jobs are reviewed and adjusted to your environment, so real threats surface and false positives do not.

Validates every alert. An intrusion analyst assesses it before anyone is paged; what reaches you is an incident with user, device, source and evidence.

Blocks the account. Through API integration with your Microsoft tenant the CDC disables the account and revokes its sessions, under rules you authorize. Brute force is locked automatically.

Audits and maps. Runs the AD audit at onboarding and yearly, keeps the attack-path sensor collecting, delivers the prioritized fixes.

Minds the traps and the leaks. Decoys refreshed as your directory changes; leaked credentials matched to live accounts and reset.



The AD audit in LMNTRIX XDR. Stale objects, privileged accounts, trusts and anomalies roll up into one domain risk level, with the fixes ranked by how much each lowers it.

WHAT YOU RECEIVE

Validated identity incidents in XDR with the action taken; the AD audit report and annual reassessment; attack-path findings; leaked-credential alerts per account; and an analyst you can reach 24 hours a day.

THE DEPLOYMENT

SOURCE	HOW LMNTRIX COLLECTS IT	WHAT YOU PROVIDE
Active Directory	Identity Agent on each domain controller; Attack Paths sensor on one DC	Install rights, outbound 443
Entra ID, Microsoft 365	Sign-in, audit and provisioning logs via Event Hub; M365 activity via the management API	App registration with read permissions
Account blocking	API integration with your tenant to disable accounts and revoke sessions	App registration with user-management rights; response rules
AWS	CloudTrail delivered to an S3 bucket with an SQS queue	Bucket, queue and a read-only IAM user
GCP, Google Workspace	Cloud audit logs via Pub/Sub; Workspace audit reports	Service accounts with read-only scopes
Okta	System Log API, by API key or OAuth2 service app	An API token or a service app with log-read scope

THE SERVICE

Who does what

A subscription module of LMNTRIX XDR: you grant the access; LMNTRIX audits, watches, validates and responds.

LMNTRIX PROVIDES

- Onboarding of every identity source, with a named project manager
- 125+ detection rules and ML jobs, tuned to your environment
- The AD audit at onboarding and every year, with remediation plan
- Attack-path analysis; AD decoy design and refresh
- Leaked-credential monitoring on your domains
- 24×7 validation, account blocking and 24-hour CDC access

YOU PROVIDE

- Read access to each identity source in scope
- Agent and sensor installation on domain controllers
- An app registration for account blocking, and the rules for using it
- Email domains to watch for leaked credentials
- Who receives escalations, and on which channels
- Remediation of audit and attack-path findings, with our guidance

WHAT SETS IT APART

CAPABILITY	LMNTRIX IDENTITY	IAM AND MFA ALONE
Where it acts	After the login, on behavior	At the login, on policy
Coverage	AD, Entra ID, M365, AWS, GCP, Okta, Workspace	One platform at a time
Detection	125+ rules, ML baselines, decoys	Policy violations
Attack paths	Mapped, ranked, cut	Invisible
Exposure	Underground credential monitoring	None
Response	CDC validates and blocks the account, 24×7	Alert handed to you

QUESTIONS. CLEAR ANSWERS.

Does it replace our IAM or MFA?

No. It sits on top of them and watches what they cannot: behavior after the login, the paths between accounts, and credentials already in criminal hands.

Who decides when an account is blocked?

You do, once, in the response rules: notify only, block on confirmation, or auto-block for brute force and decoy use.

WHAT WE NEED TO SCOPE IT

- Identity sources in scope and number of users
- AD domains and forests for audit, paths and decoys
- Email domains for credential monitoring
- Response authority: notify, confirm or auto-block

Priced per user identity, MDR included. Detection starts when the first source connects; the AD audit lands in month one.

Attackers don't break in. They log in.

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