LMNTRIX
BE THE HUNTER | NOT THE PREY

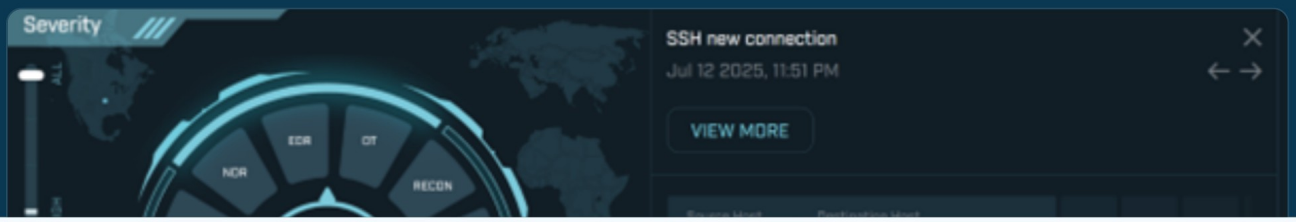
DATASHEET

THE ACTIVE DEFENSE MODULE OF LMNTRIX XDR

LMNTRIX Deceive

Outsmart. Outmaneuver. Outspeed. Make attackers reveal themselves.

LMNTRIX Deceive coats your network in things no one should ever touch: decoy servers, planted credentials, fake Active Directory accounts, tagged documents and personas. No employee has a reason to use them, so every interaction is an attacker or an insider, and the Cyber Defense Center treats it as one: investigated, contained and reported, 24 hours a day.



A Deceive alert in the LMNTRIX XDR heads-up display. Someone just opened an SSH session to a decoy that no legitimate user knows exists.

12×
Faster investigation

98%
Reduction in alert volume

66%
Lower cost of detection

Five deception layers, 11 breadcrumb categories and 10+ services per decoy. No agents on endpoints, no impact on users or production systems.

THE FIVE DECEPTION LAYERS

Deception everywhere an attacker looks

01
Decoys
Fake servers, shares and devices that match each network segment.

02
Breadcrumbs
Planted credentials and lures on every endpoint, leading to the decoys.

03
AD Decoy
Fake users and service accounts that expose directory enumeration.

04
Tags
Documents, links, keys and records that phone home when used.

05
Personas
Fake identities in your systems that prove which data was stolen.

THE THREAT COVERAGE · MAKE EVERY WRONG MOVE VISIBLE

Reconnaissance
Decoy AD objects, fake file shares, port scans against decoys.

Credential theft
Planted credentials harvested from memory, browsers and vaults.

Lateral movement
Fake RDP, SSH, VNC and share connections followed off the network.

Insider threats
Deceptive files, folders and database records opened by staff.

Malware and C2
Commands and beacons that fire on decoy systems.

Cloud abuse
Fake buckets, cloud keys and SaaS traps that announce misuse.

THE DECEPTION LAYERS IN DEPTH

If attackers cannot trust what they see, they cannot move

Targeted attacks are run by people, and people believe what they find. Deceive makes it unreliable: any share, credential, account or document an intruder finds might be ours, and the first one they use gives them away.

01 · DECOYS

What. Appliance, VM or container decoys that match the segment they sit in: a Windows desktop among desktops, a Linux file server, a router, a NAS full of documents.

Services. 10+ per decoy: SSH, Telnet, FTP, web logins, Windows shares, MySQL and SQL Server, VNC, SNMP, SIP, NTP, TFTP, proxy, plus port-scan detection.

Placement. One per segment and per 100 endpoints; every touch is high severity, related events roll into one incident, every event is kept for forensics.

02 · BREADCRUMBS

What. Eleven categories of lure on every endpoint: browser history and saved sites, vault credentials, RDP and VNC files, shares, SSH, Telnet, FTP and database connections.

How. Deployed through Active Directory in under 300 milliseconds, no agent, refreshed monthly; invisible to users and IT.

What happens. An attacker running reconnaissance picks up the crumb, follows it onto a decoy, and every command is recorded while the endpoint they came from is snapshotted.

03 · AD DECOY

Why. Enumerating Active Directory for privileged and service accounts is a top-five move for nation-state actors and red teams after a foothold.

What. Fake users and service-principal accounts seeded into your directory, and a lightweight service on each domain controller watching logon and Kerberos events for them.

What it catches. Directory enumeration, service-ticket requests against the fakes and any login attempt with their names, each one an incident in XDR.

04 · TAGS

What. Unique markers that phone home when used: web links, DNS names, email addresses, Word and PDF files, cloud API keys, SQL views, Windows folders, cloned-page scripts, repositories, QR codes.

Where. On real servers and workstations, in shares, databases, mailboxes and SaaS such as Microsoft 365, Google Drive, Dropbox and Slack; no decoy needed.

Attribution. Source IP, ISP, hostname, user agent, time and Tor use, served from your own domain so the attacker never sees ours.

05 · PERSONAS

When a fake employee gets an email, you know which list was stolen.

Fake identities created, with our guidance, where attackers harvest: LinkedIn profiles with matching mailboxes, records in your CRM, HR and marketing systems, the phone directory and Active Directory. Nobody legitimate writes to them, so a phishing email to the CRM persona proves the customer database has leaked, and a message to the LinkedIn persona shows who is being targeted.

THE LIFECYCLE

Deploy, engage, detect, investigate, contain

01
Deploy
Decoys, breadcrumbs, tags and personas, designed as one story.

02
Engage
An intruder or insider takes the bait, silently.

03
Detect
A high-fidelity alert lands in the XDR kill box.

04
Investigate
Analysts watch the session and map the attack path.

05
Contain
Endpoint isolated, account disabled, source blocked.

THE MDR SERVICE

A touched decoy becomes a contained intrusion, not a ticket in your queue

Deceive is a managed service. LMNTRIX designs the deception story, deploys and refreshes it, and the Cyber Defense Center treats every trip as a major incident: watched live, investigated, contained and reported, around the clock.

01
Detect
A decoy, breadcrumb, AD account, tag or persona is touched.

02
Validate
Events from one source are rolled into a single incident.

03
Investigate
The session is watched live; the source endpoint is snapshotted.

04
Contain
Endpoint isolated, account disabled, source blocked, via XDR.

05
Report
The attack path, the attacker's actions and the attribution.

WHAT THE CYBER DEFENSE CENTER DOES

Designs the story. Which decoy mimics which segment, which breadcrumb points to it, where the tags go: one coherent illusion, not scattered traps.

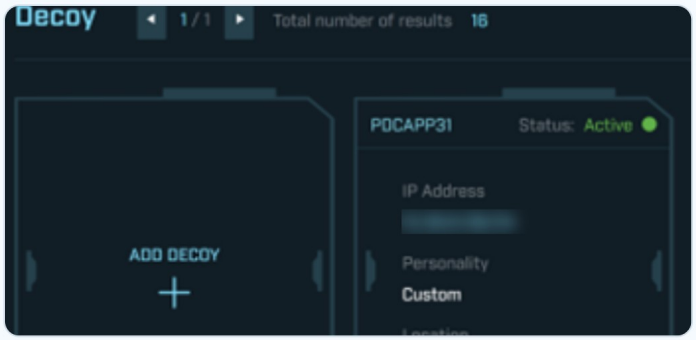
Treats every trip as real. No employee has a reason to touch a deception, so each alert is high severity; related events are aggregated, so a brute-force attempt is one incident, not one per password.

Watches the attacker work. Commands typed on the fake SSH host, files opened on the fake share, credentials tried, recorded live, plus a snapshot of the source endpoint.

Maps the path. Correlated with EDR, NDR, Identity and SIEM to show how they got in and where else they have been.

Contains through XDR. Endpoint isolated, account disabled, source blocked, under pre-agreed rules or with your approval.

Keeps it fresh. Breadcrumbs redeployed monthly, decoys re-profiled as segments change, new tags on request.



Decoys in LMNTRIX XDR. Each decoy carries a profile matched to its segment and the services it exposes; the CDC manages them from the same console as every other module.

WHAT YOU RECEIVE

Deception incidents in XDR with the attacker's actions, source and attribution; the full event record for forensics; the containment taken; and an analyst you can reach 24 hours a day.

THE DEPLOYMENT

LAYER	HOW IT IS DEPLOYED	WHAT YOU PROVIDE
Decoys	Pre-configured appliance, VM or container per segment, managed from XDR	Placement per segment, outbound access to XDR
Breadcrumbs	Pushed from XDR through Active Directory, or via SCCM, Tanium or Ansible; refreshed monthly	A directory user and a service user, OS mix per segment
AD Decoy	A Windows service on each domain controller, generated from XDR	Five or more fake users and service accounts
Tags	Generated per subnet, served under your own domain	A DNS entry to our tag service; placement per starter pack
Personas	Created by you in each system, with our guidance	Mail aliases forwarding to the CDC

THE SERVICE

Who does what

A subscription module of LMNTRIX XDR: you place the decoys and create the fakes; LMNTRIX designs, deploys, watches and responds.

LMNTRIX PROVIDES

- The deception design: decoy profiles, breadcrumb stories, tags
- Pre-configured decoys, shipped ready to deploy
- Breadcrumbs, AD Decoy package and tags, generated and deployed from XDR
- Guidance for creating personas
- 24×7 monitoring, investigation and containment
- 24-hour access to the Cyber Defense Center

YOU PROVIDE

- The starter pack: segments and operating-system mix
- Decoy placement, one per segment, and network access to XDR
- A directory user and a service user for breadcrumbs
- Fake users and service accounts in AD for the AD Decoy
- A DNS entry so tags are served from your domain
- Personas in your systems, with mail aliases to the CDC

WHAT SETS IT APART

CAPABILITY	LMNTRIX DECEIVE	DETECTION TOOLS ALONE
The signal	An attacker touched something fake	A signature or threshold matched
False positives	Near zero; every alert is an incident	Most of the queue
Insiders	Caught at reconnaissance	Rarely, and late
Coverage	Network, endpoints, AD, cloud, SaaS, files	One layer per tool
Attribution	Source, ISP, user agent, Tor, actions	An IP, at best
Response	CDC investigates and contains, 24×7	Alert handed to you

QUESTIONS. CLEAR ANSWERS.

Will our own users trip it?

Almost never. Breadcrumbs are invisible to users and IT, and decoys are on no list; an employee who goes looking is the insider the service is for.

Does it touch production?

No. There are no agents; decoys sit beside real systems, breadcrumbs are data, tags are documents and records. Nothing changes for applications or users.

WHAT WE NEED TO SCOPE IT

- Network segments and endpoint count
- Operating-system mix per segment
- AD domains, cloud accounts and SaaS to tag
- Decoy form factor: appliance, VM or container

Priced by decoys and endpoints covered, MDR included. Decoys are live within days of placement.

Ready to catch attackers in the act? Let them come to you.

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