LMNTRIX
BE THE HUNTER | NOT THE PREY

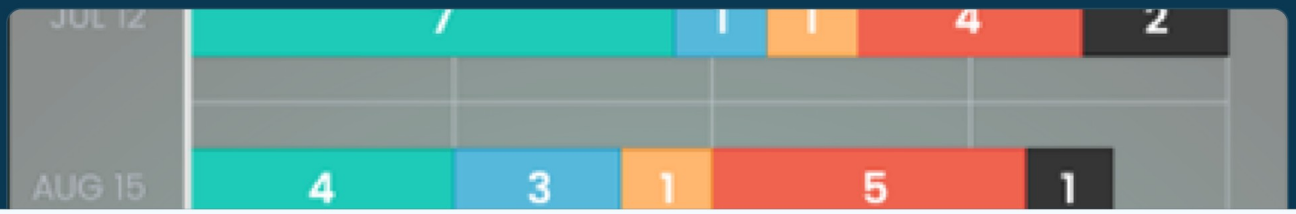
DATASHEET

THE ADVERSARIAL EXPOSURE VALIDATION MODULE OF LMNTRIX XDR

LMNTRIX Validate

Automated penetration testing. Attack yourself first.

LMNTRIX Validate runs the steps a penetration tester would, discovery, exploitation, privilege escalation, lateral movement and exfiltration, safely, on your schedule, inside and outside your network. The Cyber Defense Center scopes it, watches it, checks whether your controls and our detections caught each step, and re-tests until the path is closed.



Findings across three monthly runs. Critical and high findings fall as each run is fixed and re-tested.

24–48 h
Executive and technical reports after each test

5–5,000
IPs per test, internal, external and cloud

Up to 50%
Lower cost than point-in-time manual testing

Monthly, quarterly or on demand. Every simulated step lands in LMNTRIX XDR beside the detection it should have triggered.

THE CORE CAPABILITIES

A penetration tester you can run on demand

Reconnaissance & discovery
Internal and external host discovery, service enumeration, exposed logins, OSINT entry paths.

Safe exploitation
Confirms what is actually exploitable, within the scope and intensity you set, watched live.

Privilege & credential attacks
Weak authentication, credential abuse and escalation: what a stolen account really reaches.

Lateral movement & exfiltration
Movement across segments, man-in-the-middle and data exfiltration, from foothold to crown jewels.

Control & SOC validation
Did SIEM, EDR, firewall and our analysts see it? Every step correlated with its expected detection.

Reporting, remediation & re-test
Prioritized findings with step-by-step fixes, then a re-run to prove the path is closed.

THE USE CASES · REPLACE ASSUMPTIONS WITH PROOF

Continuous posture validation
Know every month, not once a year.

Pre-audit assurance
PCI DSS, ISO 27001 and similar evidence.

Purple teaming
Measure SOC effectiveness with live evidence.

Pentest replacement
Network tests automated; specialists for the rest.

Board reporting
Trending risk metrics run after run.

THE TEST IN DEPTH

The steps a consultant takes once a year, every month

A vulnerability scan tells you what is present. A penetration test tells you what an attacker can do with it. Validate runs the full chain, with the knowledge of certified testers built in, so exploitation and post-exploitation show the real impact, not a list of CVEs.

01 · RECONNAISSANCE & DISCOVERY

Internal. Host discovery across the segments in scope, service enumeration, exposed authentication surfaces, shares, databases and management interfaces.

External. Your internet-facing ranges and domains, plus OSINT: leaked credentials, exposed services and the entry paths an outsider would try first.

Cloud. AWS, Azure and GCP ranges tested the same way, inside and out.

02 · SAFE EXPLOITATION

What it proves. Whether a vulnerability is actually exploitable in your environment, and what access it yields, so remediation is ranked by reality.

How it stays safe. Non-destructive techniques, scope and intensity you control, exclusions for fragile systems, and low-traffic test windows or a staging run where you prefer.

Visibility. Every action logged in real time, so you and the CDC watch the test as it happens.

03 · PRIVILEGE, CREDENTIALS & LATERAL MOVEMENT

Credentials. Weak and default passwords, authentication flaws, credential reuse and abuse of harvested accounts.

Escalation and movement. Post-exploitation privilege escalation, then movement across systems and segments toward the assets that matter, man-in-the-middle included.

Exfiltration. Simulated data theft to test whether your controls, and our detections, stop it.

04 · REPORTING, REMEDIATION & RE-TEST

Three documents. An executive summary, a technical report with MITRE ATT&CK references, and a vulnerability register, within 24 to 48 hours of the test ending.

Prioritized. Risk-scored on exploitability, impact and severity, with step-by-step remediation for each finding.

Proven closed. A re-test confirms the fix; findings trend run over run so progress is visible to the board.

05 · CONTROL & SOC VALIDATION

The only pentest that grades the defenders too.

Because Validate runs inside LMNTRIX XDR, every simulated step is matched to the alert it should have raised in SIEM, EDR, NDR and the firewall. A step that fired is evidence your controls work; a step that stayed silent becomes a tuned detection before a real attacker finds the same gap. Annotated logs and live tracking turn each run into a purple-team exercise for your own team.

THE LIFECYCLE

Attack. Measure. Improve. Repeat.

01
Scope
Internal, external, cloud; ranges, exclusions and intensity agreed.

02
Deploy
A cloud-managed agent inside; nothing to install for external tests.

03
Attack
Discover, exploit, escalate, move, exfiltrate, safely.

04
Correlate
Each step checked against the detections in XDR.

05
Fix & re-test
Prioritized fixes, then a re-run to prove them.

THE MDR SERVICE

A finding becomes a closed path and a tuned detection

Validate is not a tool you log into once a quarter. The Cyber Defense Center scopes and schedules each test, watches it run, reads the results against what XDR detected, delivers the reports, tracks the fixes and re-tests, and keeps a 24-hour line open throughout.

01
Scope
Ranges, exclusions, windows and intensity agreed with you.

02
Run
Monthly, quarterly or on demand, watched live by the CDC.

03
Correlate
Every step matched to the alerts it raised, or failed to raise.

04
Report
Executive, technical and register reports in 24 to 48 hours.

05
Re-test
Fixes verified, detections tuned, trend updated.

WHAT THE CYBER DEFENSE CENTER DOES

Scopes it with you. Which ranges, which exclusions, how hard, and when: low-traffic windows for production, a staging run where you want one.

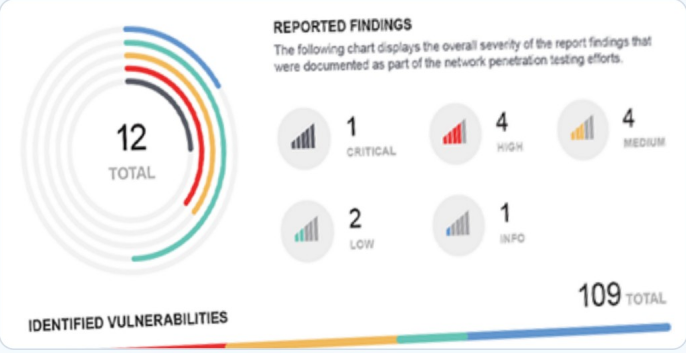
Watches it run. Analysts follow the test live, so a step that behaves unexpectedly is paused, and you are never surprised by your own test.

Grades the defenses. Each exploit, escalation and exfiltration step is checked against SIEM, EDR, NDR and firewall alerts in XDR. Silence is a finding too.

Tunes what missed. A step that raised no alert becomes a new or adjusted detection, so the next real attacker is caught where the test was not.

Prioritizes and explains. Findings ranked by exploitability, impact and severity, each with the fix, in reports your executives and engineers can both read.

Closes the loop. Re-tests on request, results trended run over run, and the evidence filed for PCI DSS, ISO 27001 and your auditors.



The executive summary. Findings by severity for the run, the vulnerabilities behind them, and the delta from last time, delivered within 48 hours of the test.

WHAT YOU RECEIVE

Executive summary, technical report and vulnerability register per test; a detection-coverage read-out of what XDR saw and what it did not; re-test confirmation; trending across runs; findings pushed to your SIEM or ticketing; and an analyst you can reach 24 hours a day.

THE DEPLOYMENT

TEST	HOW IT RUNS	WHAT YOU PROVIDE
Internal	A lightweight agent on a Linux VM inside the segment, managed from the XDR cloud over 443	A small VM, outbound 443, the ranges and exclusions
External	Run from the LMNTRIX cloud against your internet-facing ranges and domains; nothing to install	Public IPs and domains, written authorization to test
Cloud	AWS, Azure and GCP ranges tested internally or externally the same way	The ranges and, for internal, a VM in the VPC or VNet
Schedule	Monthly, quarterly or on demand; intensity and windows per test; IPs reset each month	Preferred windows and change-freeze dates
Integrations	Findings into LMNTRIX XDR and SIEM; tickets to your service desk	A ticketing integration, if wanted

THE SERVICE

Who does what

A subscription module of LMNTRIX XDR: you define the scope and fix what we find; LMNTRIX runs, watches, grades, reports and re-tests.

LMNTRIX PROVIDES

- Scoping, scheduling and the internal agent image
- Safe execution, watched live by the CDC
- Correlation of every step with XDR detections, and tuning of misses
- Executive, technical and register reports within 24 to 48 hours
- Re-tests and run-over-run trending
- 24-hour access to the Cyber Defense Center

YOU PROVIDE

- IP ranges and domains in scope, and anything excluded
- A small Linux VM with outbound 443 for internal tests
- Written authorization for external testing
- Preferred test windows, intensity and change-freeze dates
- Who receives reports and escalations
- Remediation of findings, with our guidance

WHAT SETS IT APART

CAPABILITY	LMNTRIX VALIDATE	ANNUAL MANUAL PENTEST
Frequency	Monthly, quarterly or on demand	Once a year, if budget allows
Time to report	24 to 48 hours	Two to four weeks
Cost	Up to 50% lower, re-tests included	Day rates; re-test billed again
Consistency	Same method every run; results trend	Depends on the tester you get
Detection validation	Every step graded against XDR alerts	Not in scope
Depth	Network, credentials, lateral movement, exfiltration	Deeper on apps, APIs and people

QUESTIONS. CLEAR ANSWERS.

Does it replace our manual penetration test?

For network testing, yes, and far more often. Web applications, APIs and social engineering still want a specialist; LMNTRIX Red Team covers those when you need them.

Will it disrupt production?

It is built not to: non-destructive techniques, intensity and scope you control, exclusions, and low-traffic or staging windows where you prefer.

WHAT WE NEED TO SCOPE IT

- Internal and external IPs to test at any one time
- Cloud ranges in scope
- Frequency: monthly, quarterly or on demand
- Compliance drivers and reporting audience

Priced by IP block tested per month, MDR included. IPs reset monthly; step up a block in the first ten months and pay only the difference.

We don't wait for a breach to test defenses. We attack first.

Every engagement starts with a free 30-day proof of concept, your first test and report included, 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.