LMNTRIX AAV
AUTOMATED ATTACK VALIDATION

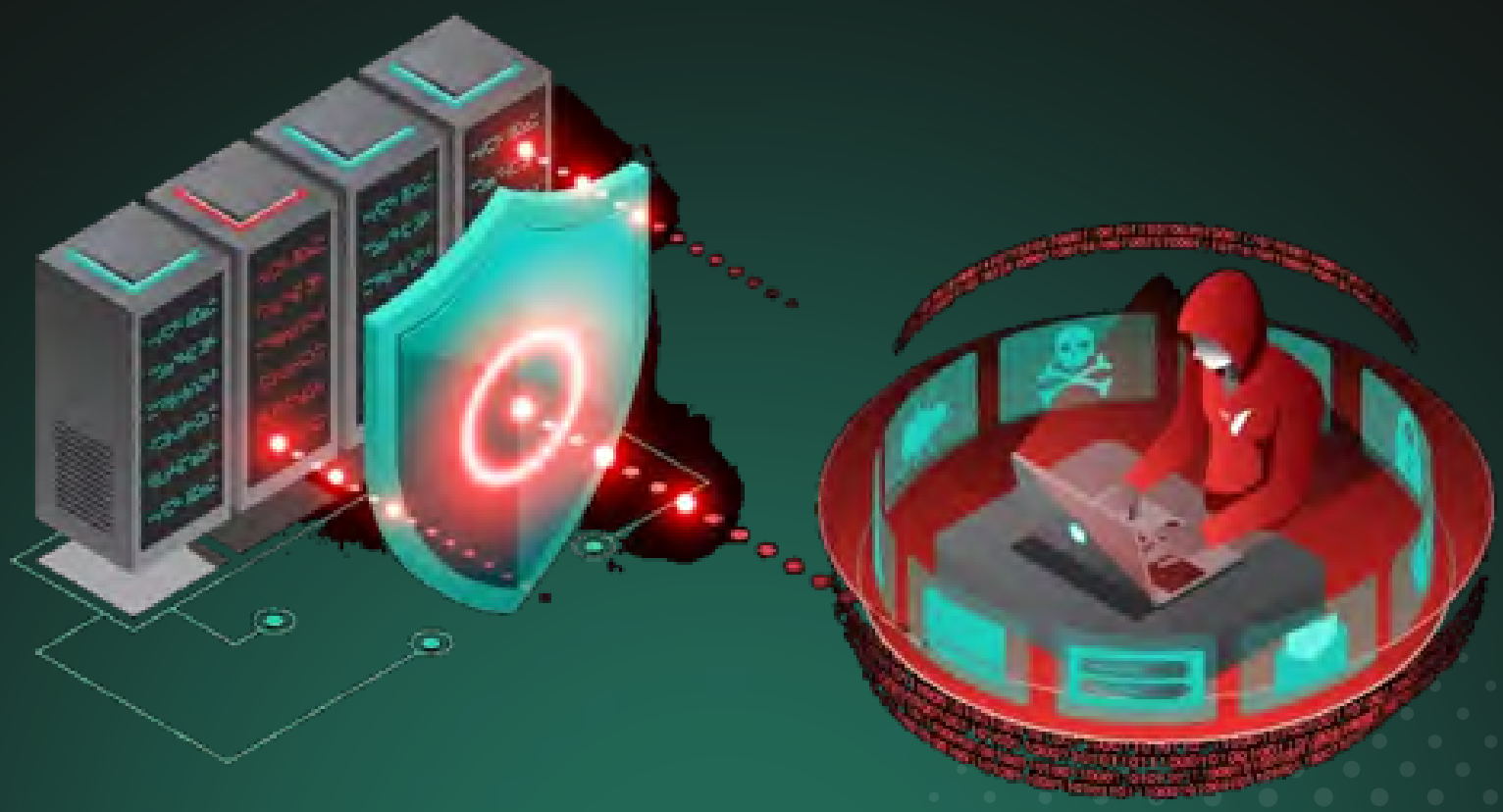
CONTINUOUSLY SIMULATE REAL-WORLD ATTACKS. STAY ONE STEP AHEAD.

LMNTRIX
BE THE HUNTER | NOT THE PREY

01

THE BEST DEFENSE IS A GOOD OFFENSE.

LMNTRIX AAV revolutionizes offensive security by automating real-world attack simulations—mimicking today's most advanced threat actors to validate and harden your defenses continuously. Think of it as a 24/7 red team working in the background—uncovering hidden vulnerabilities, testing your controls, and proving your ability to detect and respond before real adversaries strike. Unlike traditional pen tests, which are point-in-time, expensive, and manual, AAV delivers scalable, on-demand attack simulations across your internal and external infrastructure—ensuring your security posture is always battle-tested and ready.



02

WHY LMNTRIX AAV?

✅ Proactive Risk Discovery
Identify exploitable weaknesses—before attackers do—by simulating tactics like privilege escalation, lateral movement, and data exfiltration.

📈 Actionable Intelligence, Not Just Reports
Receive prioritized, remediation-focused insights to drive meaningful risk reduction and security posture improvement.

💸 Affordable, Continuous Validation
Replace manual, high-cost pen tests with scalable, always-available attack simulation that saves up to 50% in cost.

📆 On Your Schedule
Launch tests anytime—monthly, quarterly, or on-demand—and compare progress with trending risk metrics.

🧠 Red Team Expertise On Demand
Gain the power of certified experts (OSCP, OSCE, CEH) without hiring them. Deploy with the click of a button.

03

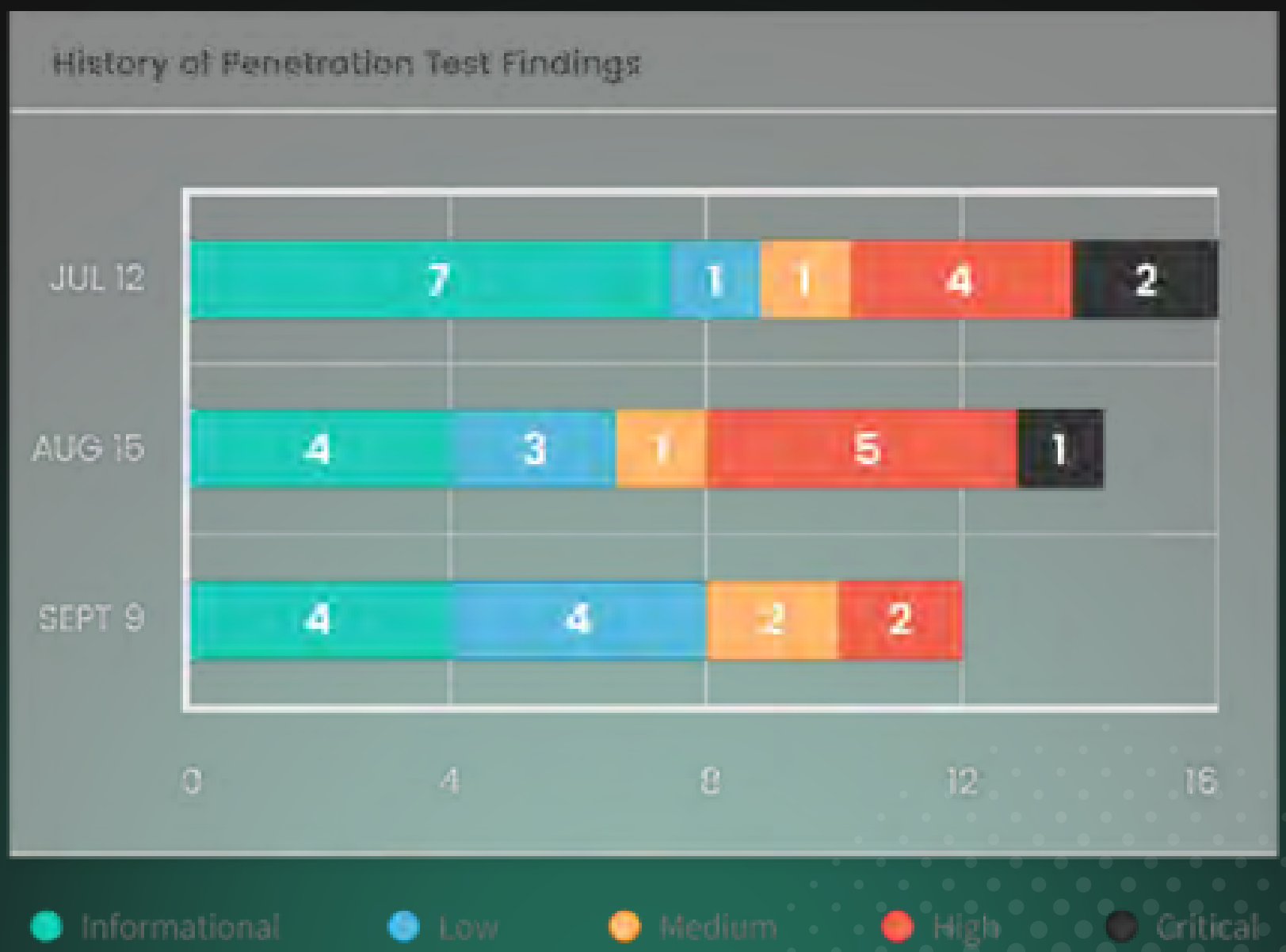
KEY CAPABILITIES

🎯 Realistic Attack Simulation

Emulates internal and external attacker behavior, including OSINT recon, brute force attacks, and lateral movement.
Validates existing security controls, including SIEM, EDR, and firewall rules.

🔄 Continuous & On-Demand Testing

Schedule recurring tests or trigger instantly to validate readiness against emerging threats.



04

KEY CAPABILITIES

🔍 **Safe Exploitation & Real-Time Monitoring**
Tests vulnerabilities safely and provides real-time visibility into simulated attacks to validate SOC performance.

📡 **Service & Credential Discovery**
Performs advanced service enumeration, authentication testing, and privilege escalation simulations.

📤 **Exfiltration & MITM Simulation**
Tests the ability to detect and stop sensitive data exfiltration and man-in-the-middle attacks.

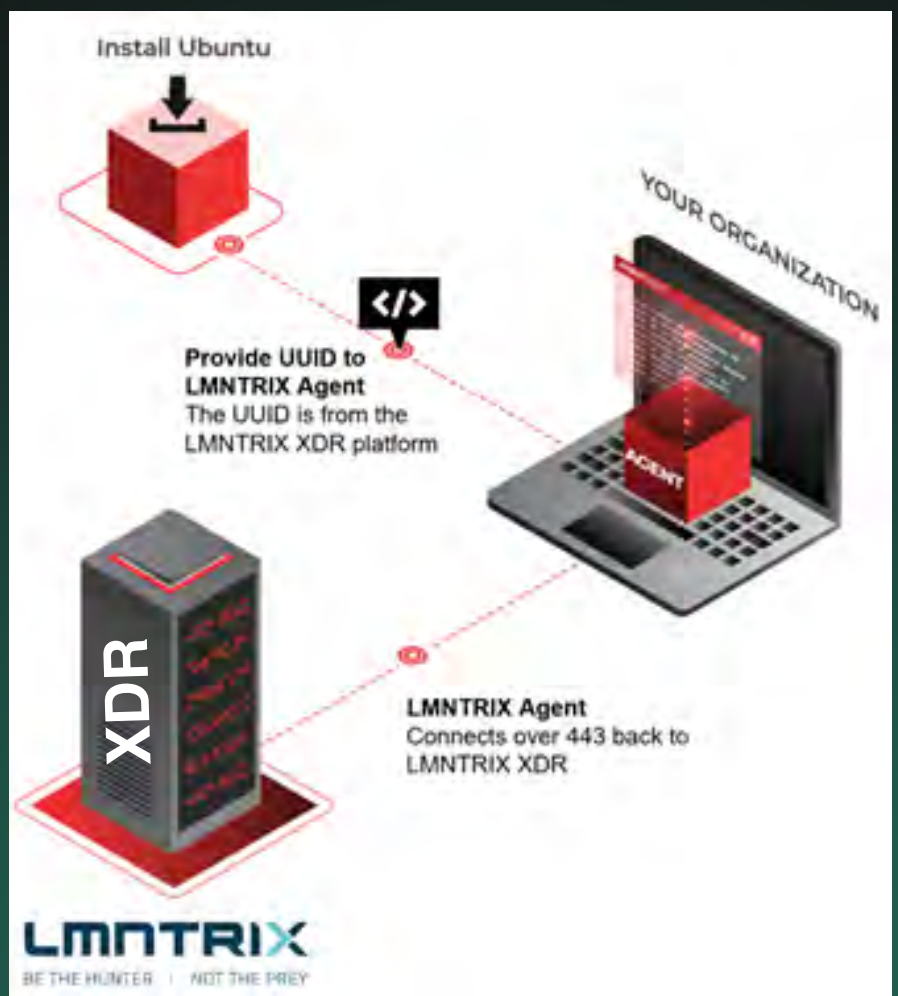
📊 **Comprehensive Reporting & Guidance**
Executive summaries and technical deep-dives delivered within 24–48 hours, complete with step-by-step remediation.

🎛️ **Purple Team Collaboration**
Facilitates red-blue collaboration with live tracking, annotated logs, and SIEM correlation for SOC enrichment.

05

HOW IT WORKS

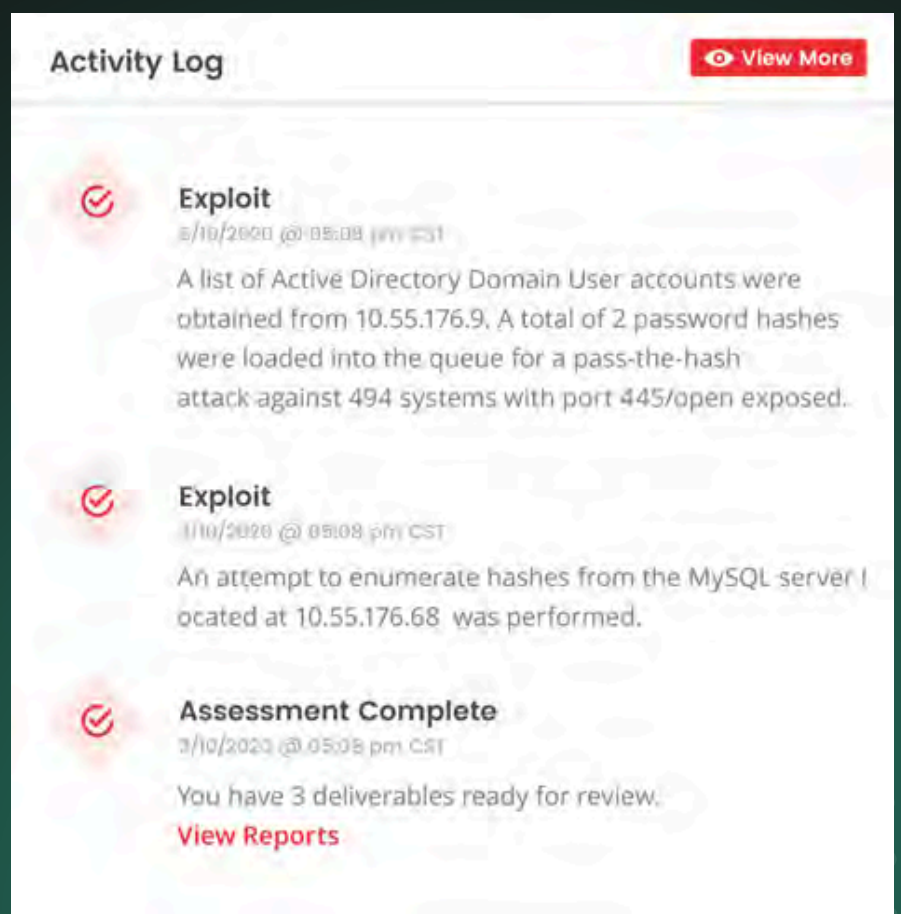
1. Deploy Agent: Internally or externally—fully managed via cloud.
2. Schedule Tests: Monthly, quarterly, or on-demand.
3. Simulate Attacks: Credential abuse, privilege escalation, data exfiltration, and more.
4. Correlate with SIEM: Monitor in real-time and validate detection and response workflows.
5. Remediate & Re-Test: Use prioritized insights to fix what matters—then prove it's resolved.



06

USE CASES

- Continuous security posture validation
- Pre-audit compliance assurance (PCI DSS, ISO 27001, etc.)
- Purple teaming and SOC effectiveness assessment
- Cost-effective penetration test replacement
- Executive risk reporting and board visibility



07

BATTLE-TESTED FOR EVERY ENVIRONMENT

Whether you manage 5 or 5,000 IPs, LMNTRIX AAV is scalable and configurable to fit your architecture and risk appetite—ensuring that every critical asset is validated against real-world threats.

"We don’t wait for a breach to test defenses—we attack first so adversaries don’t get the chance."

08

READY TO VALIDATE YOUR DEFENSES?

Schedule your first attack simulation and experience the power of continuous, automated penetration testing—backed by global expertise and 24/7 operational insight.

VISIT
LMNTRIX.COM

LMNTRIX
BE THE HUNTER | NOT THE PREY