LMNTRIX PACKETS

LOGS ONLY TELL PART OF THE STORY.

With LMNTRIX Packets, you see every packet, every session, every move an adversary makes.

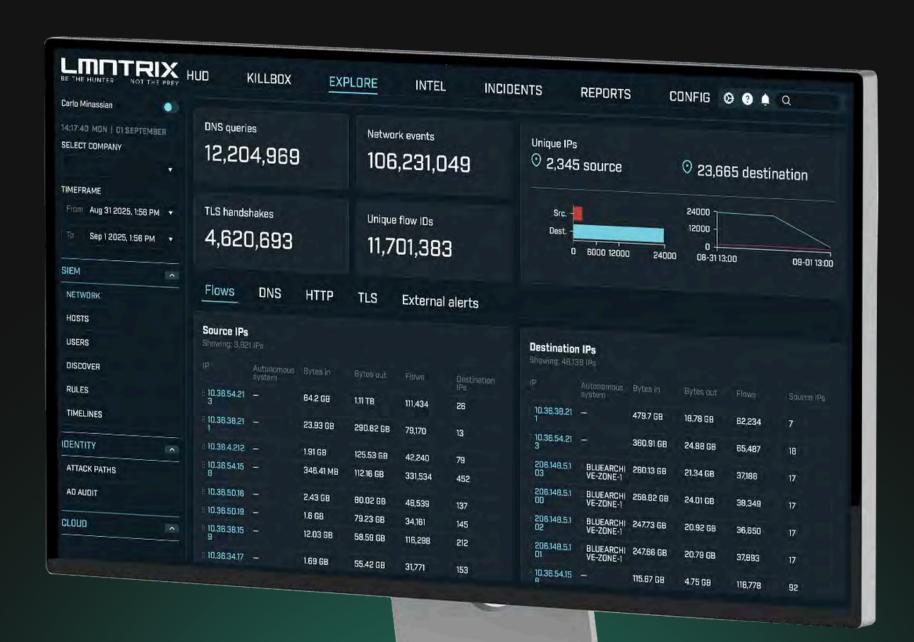






DEEP NETWORK FORENSICS BUILT INTO LMNTRIX XDR

Full-fidelity packet capture that goes beyond alerts—delivering forensic accuracy and autonomous threat hunting.





SEE WHAT OTHERS MISS

- Spot lateral movement & encrypted C2
- Detect insider threats
- Validate past breaches with retrospective analysis



Encrypted Traffic Visibility

Get maximum insights into all encrypted traffic to support triage for decryption, advanced analytics for anomaly detection, and forensics



Domain Fronting

Reveal the use of routing schemes in Content Delivery Networks (CDNs) and other services that mask the intended destination of HTTPS traffic (direct or tunneled).



Virtual Private Networks (VPNs)

Accurately identify the use of dozens of VPN applications, including those most commonly deployed for malicious activities

VPN protocols detected with blocking use cases.



Traffic Spoofing

Identify apps (e.g., eProxy, HTTP Injector) that combine techniques (such as protocol header customization, proxies, tunneling & domain fronting) to evade detection.



File Spoofing

Detect inconsistencies such as a false MIME type or a mismatch between the original hash and computed hash.



Anonymizers

Detect anonymous proxy services that may be cloaking harmful activities, including those using multiple layers of encryption.



Encryption

TLS 1.3 support
Secured connections
fingerprinting (JA3 &
JA3S hashing,



Covert Communication Channels

Detect non-standard or complex tunneling activities over legitimate protocols such as DNS or ICMP, which may indicate unauthorized or illegal activities.

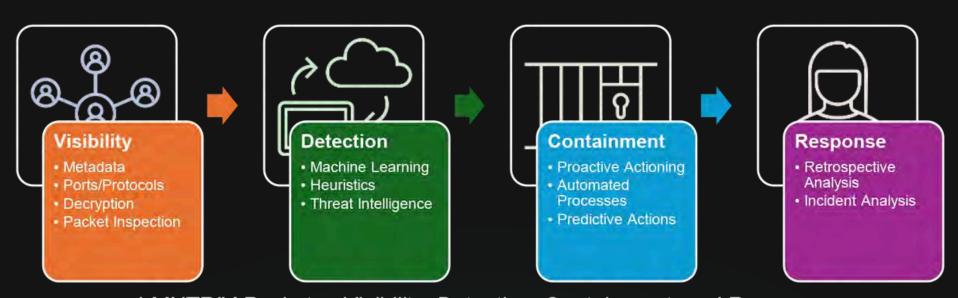


Device Fingerprinting

100% agentless, passive identification of connected IT, consumer and industrial devices (optional module).

THE POWER OF PACKETS

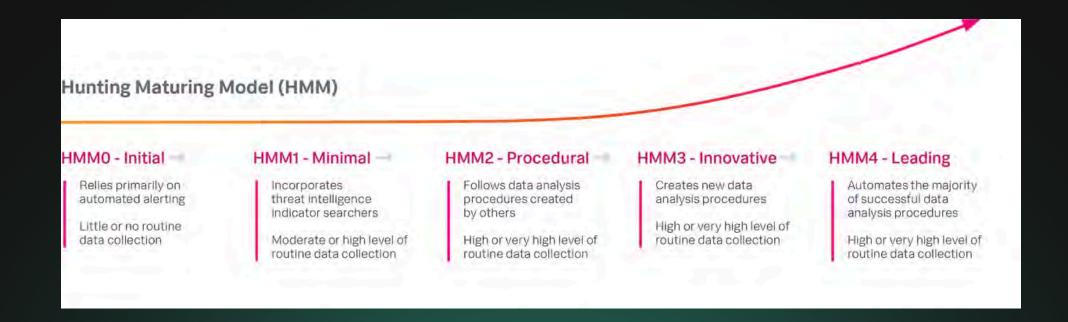
- Full packet capture & session reconstruction
- File extraction for malware analysis
- Encrypted traffic visibility
- Al-powered threat hunting



LMNTRIX Packets - Visibility, Detection, Containment, and Response

FROM DETECTION TO FORENSICS

- Threat hunting on historical data
- Post-breach investigation
- Zero-day detection
- Compliance & audit validation





READY TO SEE WHAT'S HIDING IN YOUR NETWORK?



Book a demo of LMNTRIX Packets today.



