

LMNTRIX DECEIVE

OUTSMART.
OUTMANEUVER.
OUTSPEED.

Deception that flips the advantage
back to defenders.



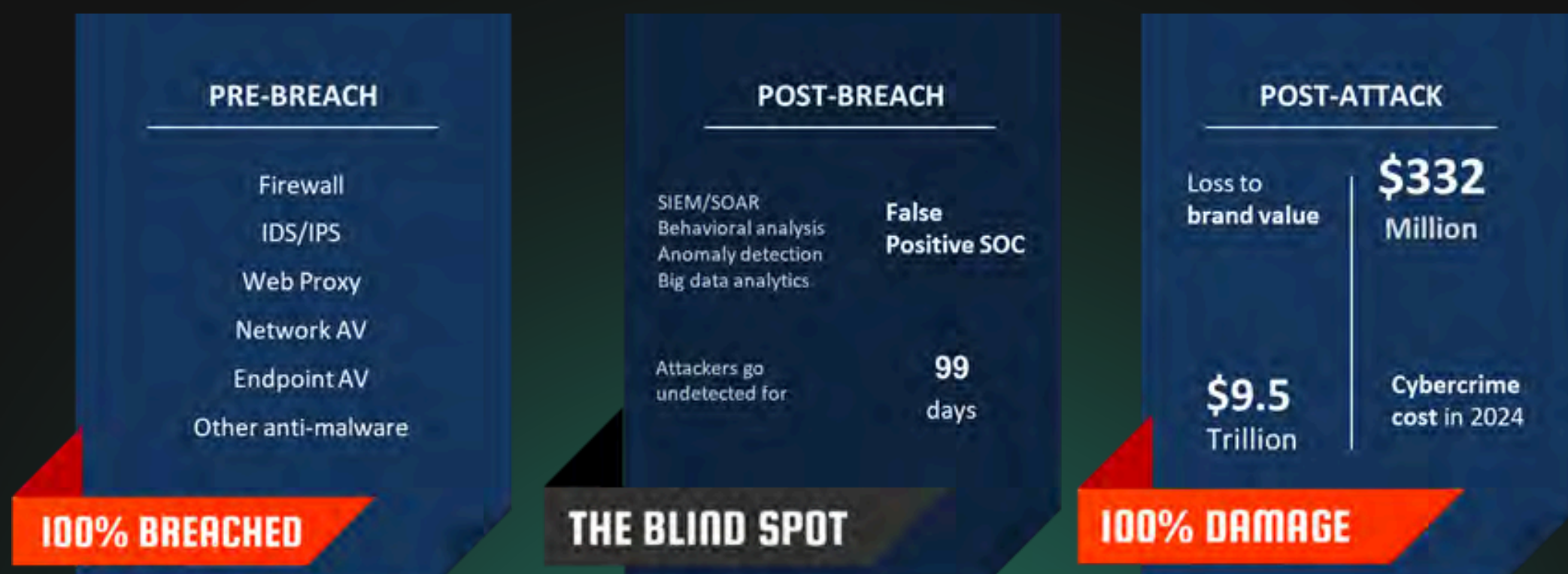
LMNTRIX
BE THE HUNTER | NOT THE PREY

THE PROBLEM WITH TRADITIONAL DEFENSES

Why Most Defenses Fail:

- Signature-based tools miss novel threats
- Behavioral analytics suffer noise and false positives
- Passive detection responds only after compromise

LMNTRIX Deceive flips the script. Attackers reveal themselves.

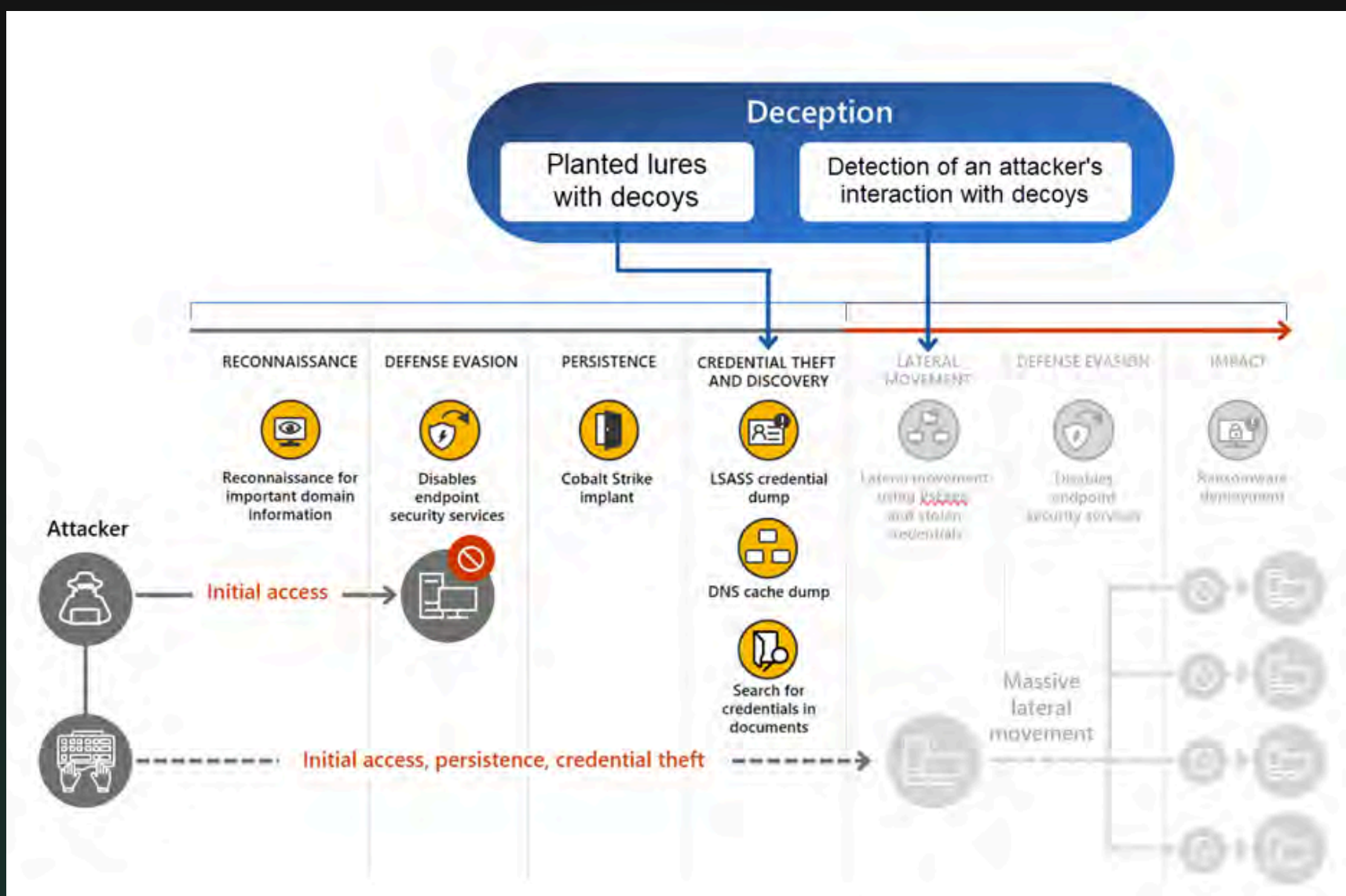


A POST-BREACH
STRATEGY IS A MUST

WHAT IS LMNTRIX DECEIVE?

Deception-Driven Threat Detection

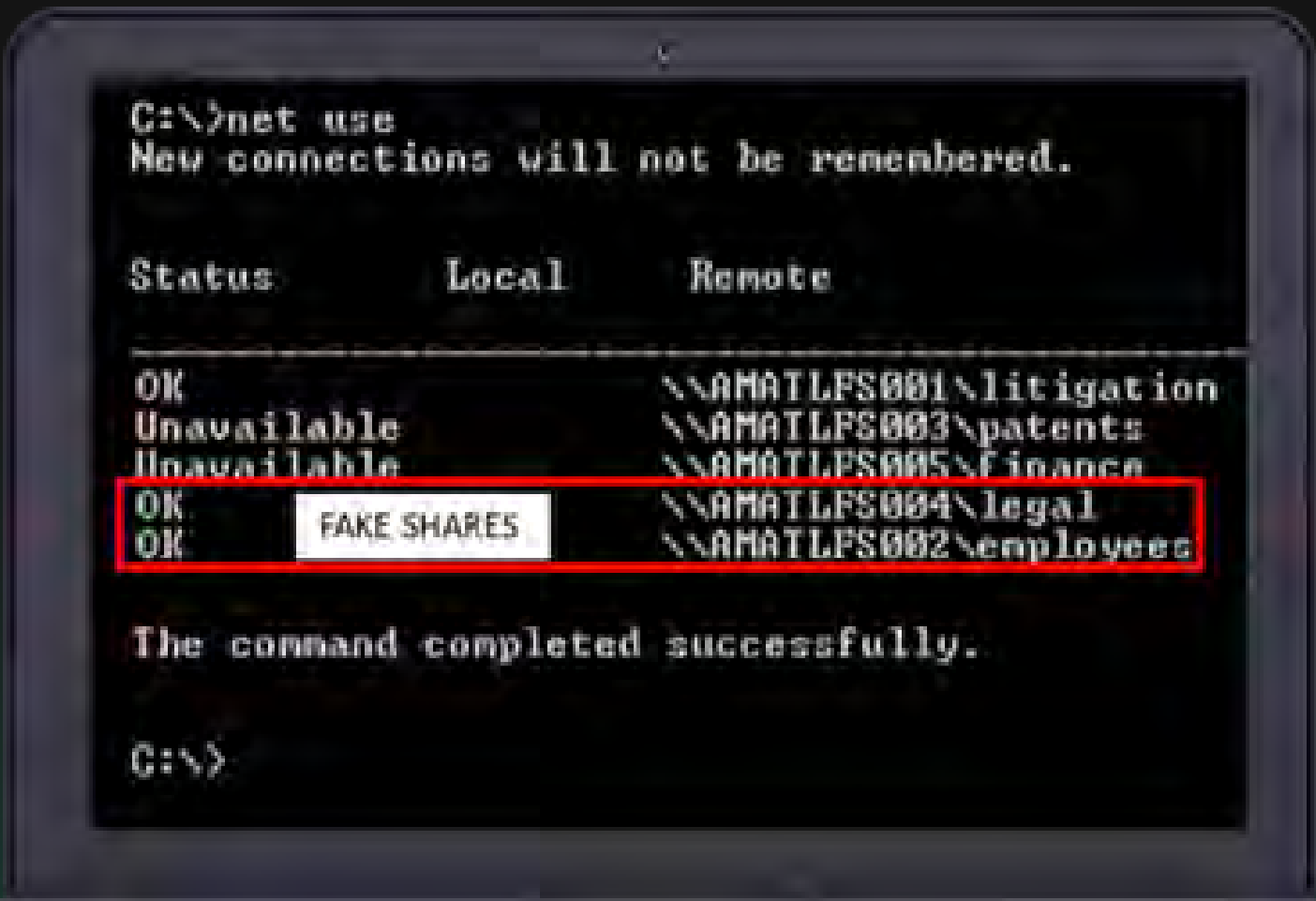
- Fake assets (users, shares, credentials, cloud buckets) lure attackers
- Every interaction triggers a high-fidelity alert
- LMNTRIX analysts investigate and respond in real time
- No impact on users or production systems



WHAT IT CATCHES

Detection Across Every Attack Stage

- Reconnaissance – decoy AD objects, fake file shares
- Credential Theft – planted fake credentials
- Lateral Movement – fake RDP/SSH interactions
- Insider Threats – deceptive file access
- Malware/C2 – command triggers on decoy systems
- Cloud Abuse – fake S3 buckets, SaaS traps



```
C:\>net use
New connections will not be remembered.

Status:          Local          Remote
-----
OK              \\AMATLFS001\\litigation
Unavailable    \\AMATLFS003\\patents
Unavailable    \\AMATLFS005\\finance
OK             \\AMATLFS004\\legal
OK             \\AMATLFS002\\employees

The command completed successfully.

C:\>
```

KEY BENEFITS

- Detect adversaries early in the kill chain
- Prevent lateral movement and privilege abuse
- Reduce dwell time and false positives
- Enable proactive insider threat detection
- Fully passive, seamless, and scalable

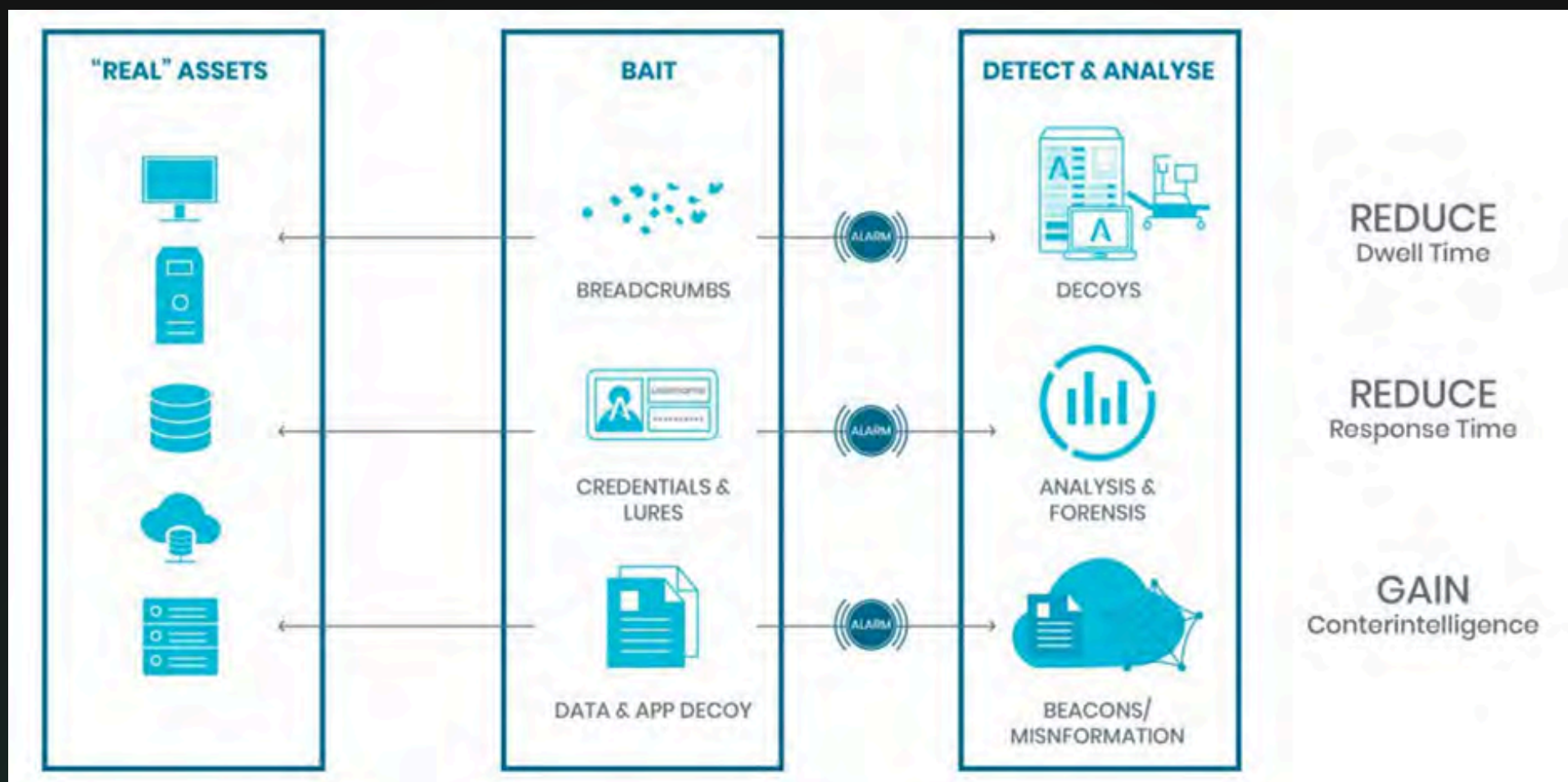
The screenshot displays the LMNTRIX Killbox interface. The top navigation bar includes tabs for HUD, KILLBOX (active), EXPLORE, INTEL, INCIDENTS, REPORTS, and CONFIG. The left sidebar contains filters for user (Carlo Minassian), date (21:33:05 SUN | 31 AUGUST), company selection, timeframe (Sep 1 2024, 8:30 PM to Aug 31 2025, 9:29 PM), selected fields, and available fields. The main area shows a network diagram with nodes for Attacker (10.36.6.42), Decoy (10.36.6.138), and other hosts. Below the diagram is a table of events:

Description	Attacker IP Address	Decoy IP address	Decoy Port
HTTP GET Method attempt	10.36.6.42	10.36.6.138	80
SIP REQUEST INITIATED	10.36.6.33	0.0.0.0	
SSH NEW CONNECTION	10.36.6.33	10.36.6.138	

The right sidebar shows details for the selected event, including the date (07:27:2025 | 10:03), decoy ID (608d76da233e3), and a diagram of the source and destination ports (56655 to 80).

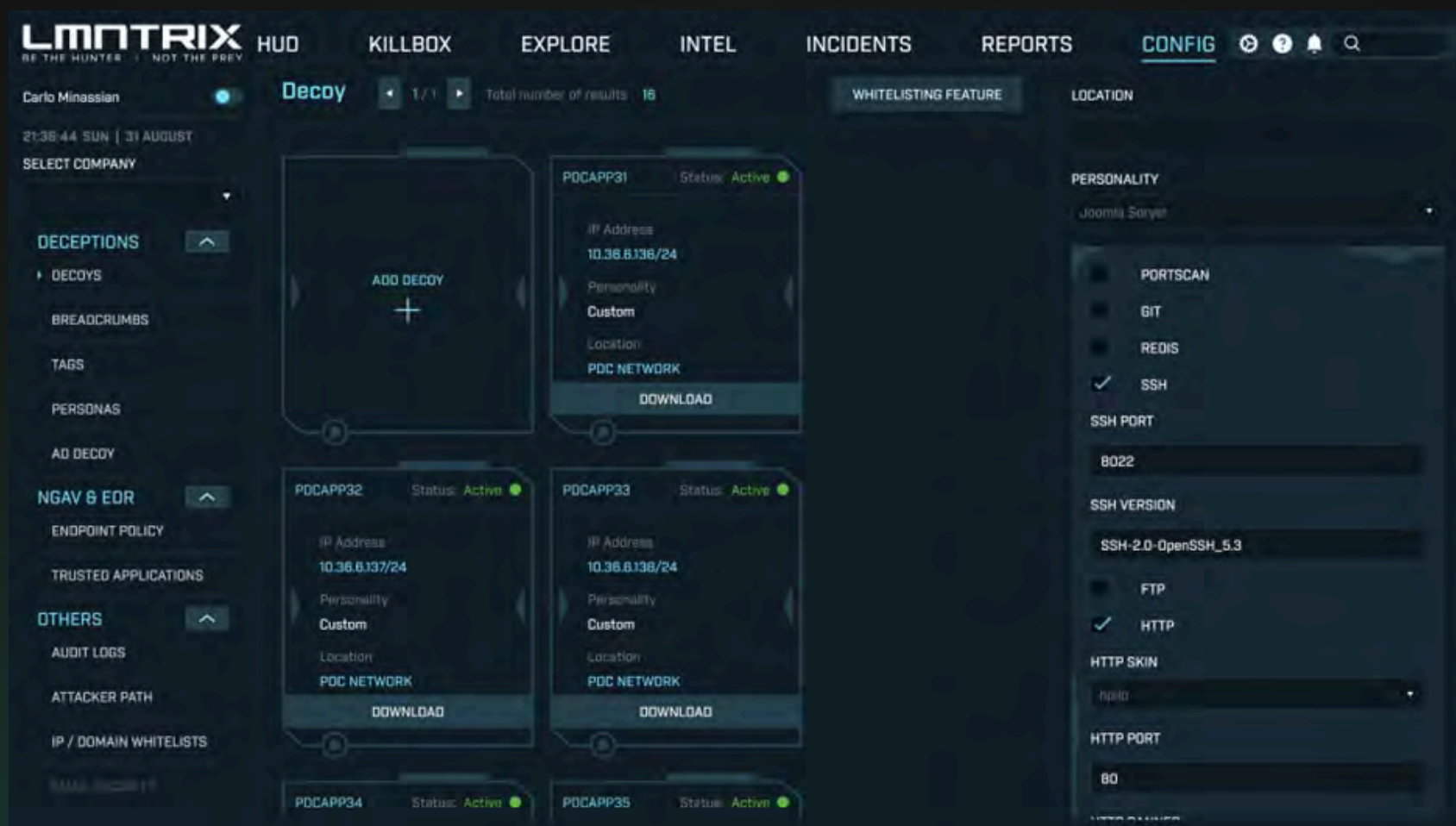
HOW IT WORKS

1. Deploy realistic decoys across the network and cloud
2. Adversaries engage — triggering silent alerts
3. LMNTRIX investigates and initiates remote containment
4. Full visibility via the LMNTRIX XDR platform



BUILT FOR XDR

- Cross-Vector Correlation – with NDR, EDR, Identity, SIEM
- Attack Path Mapping – see how attackers move
- MITRE ATT&CK Mapped – for evidence-driven responses
- SOC-Driven Investigation – handled by LMNTRIX experts
- Supports Hybrid & Cloud Environments





READY TO CATCH ATTACKERS IN THE ACT?

Let's add deception to your defense stack.



Built for security. Powered by AI. Trusted by enterprises.

VISIT
LMNTRIX.COM



LMNTRIX
BE THE HUNTER | NOT THE PREY