

LMNTRIX ENDPOINT SECURITY

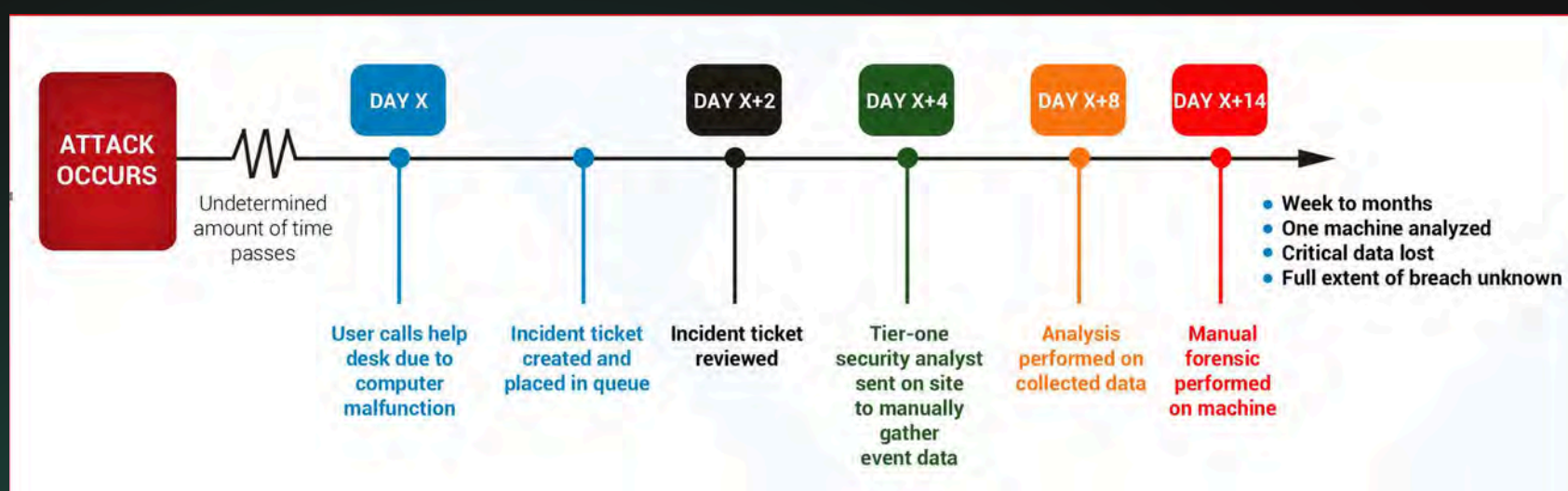
Stop threats at the endpoint.
Detect faster. Respond smarter.



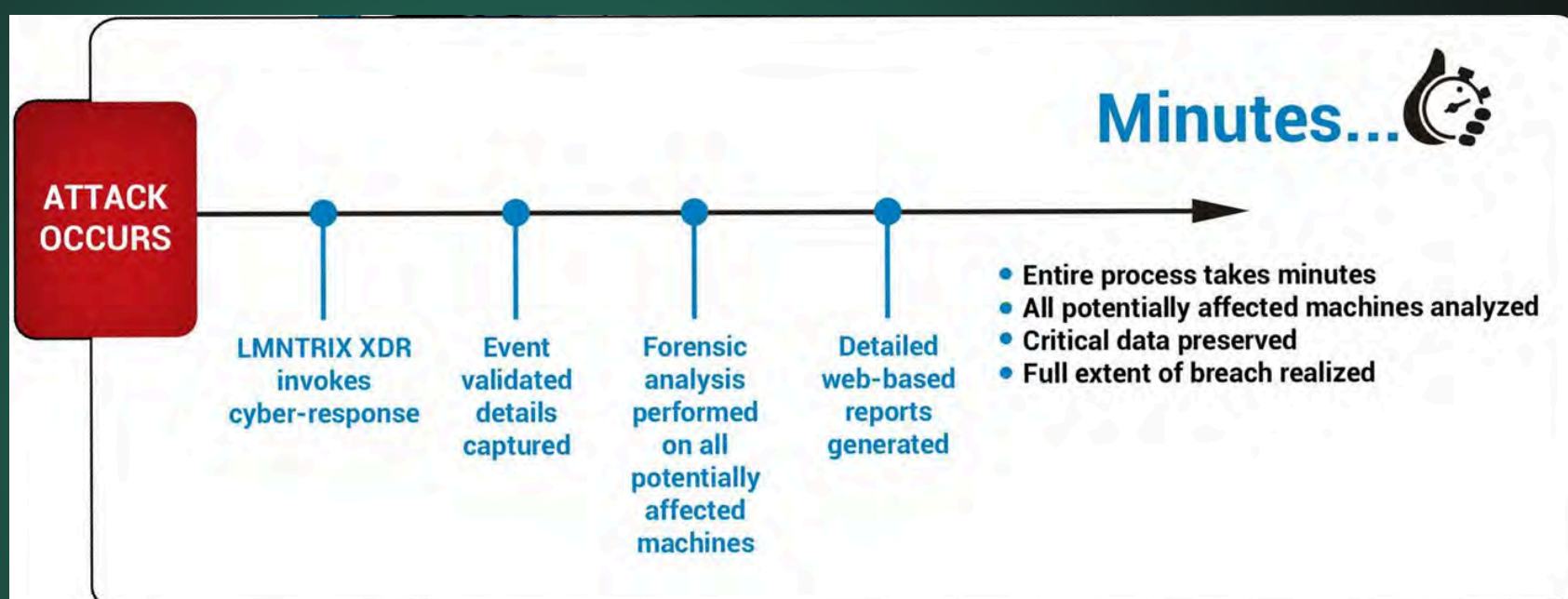
LMNTRIX
BE THE HUNTER | NOT THE PREY

ENDPOINTS ARE YOUR FRONT LINE

Ransomware, credential theft, live-off-the-land attacks. One missed alert can become a breach.



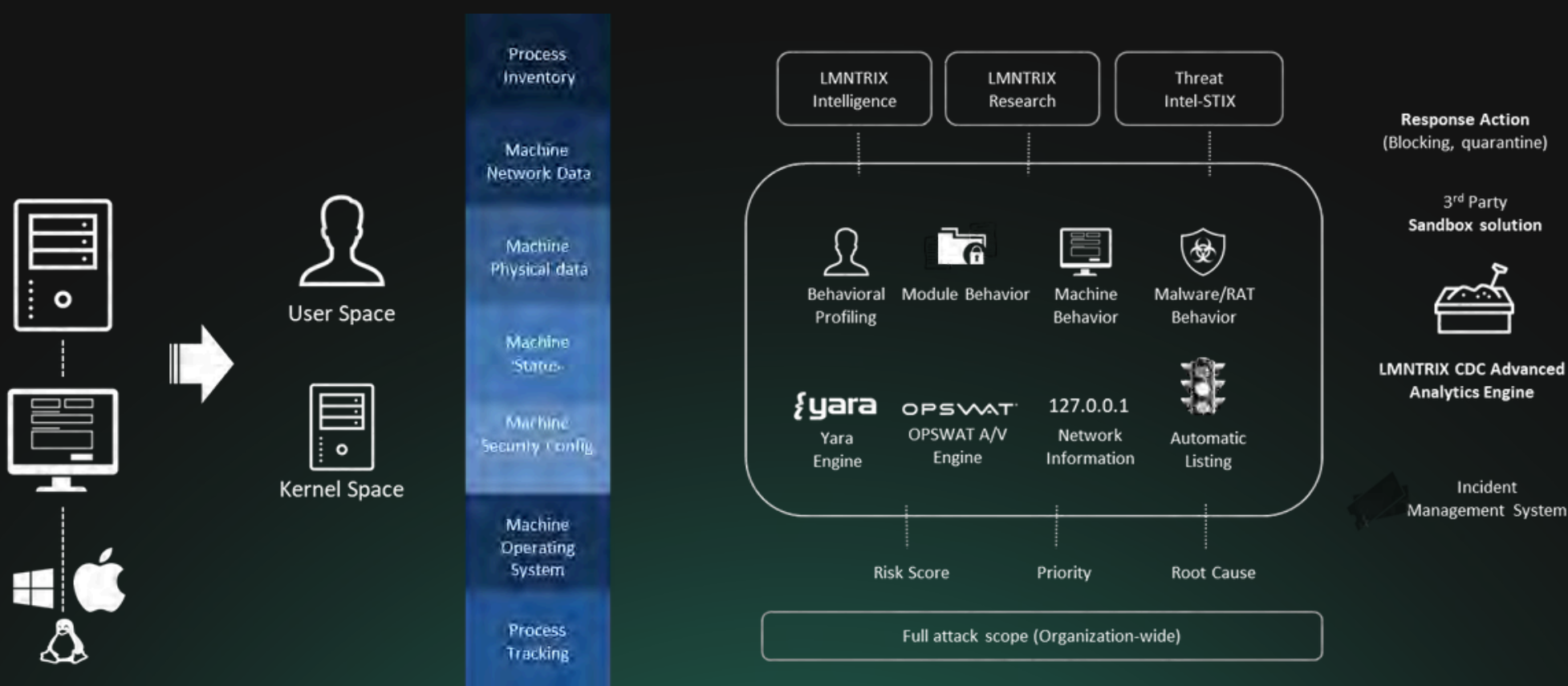
Incident response timeline without LMNTRIX XDR Endpoint Security



Streamlined incident response timeline with LMNTRIX XDR Endpoint Security

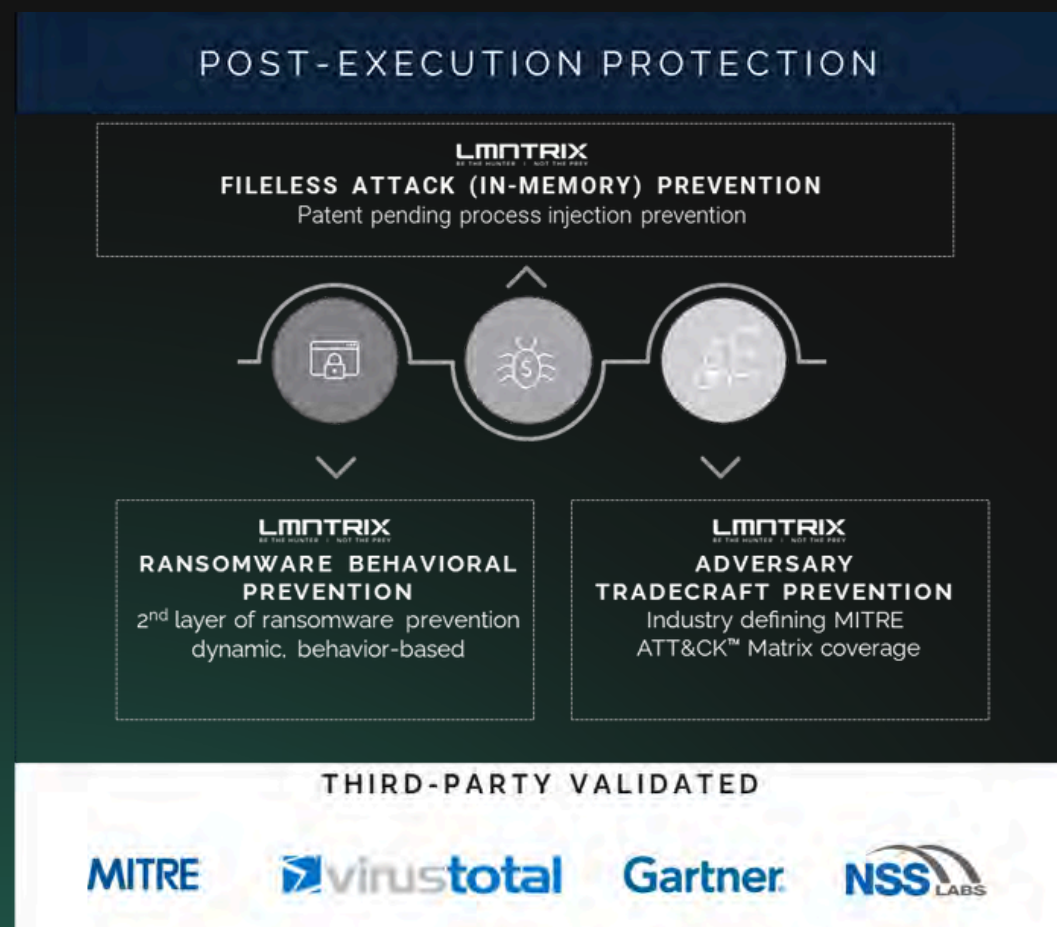
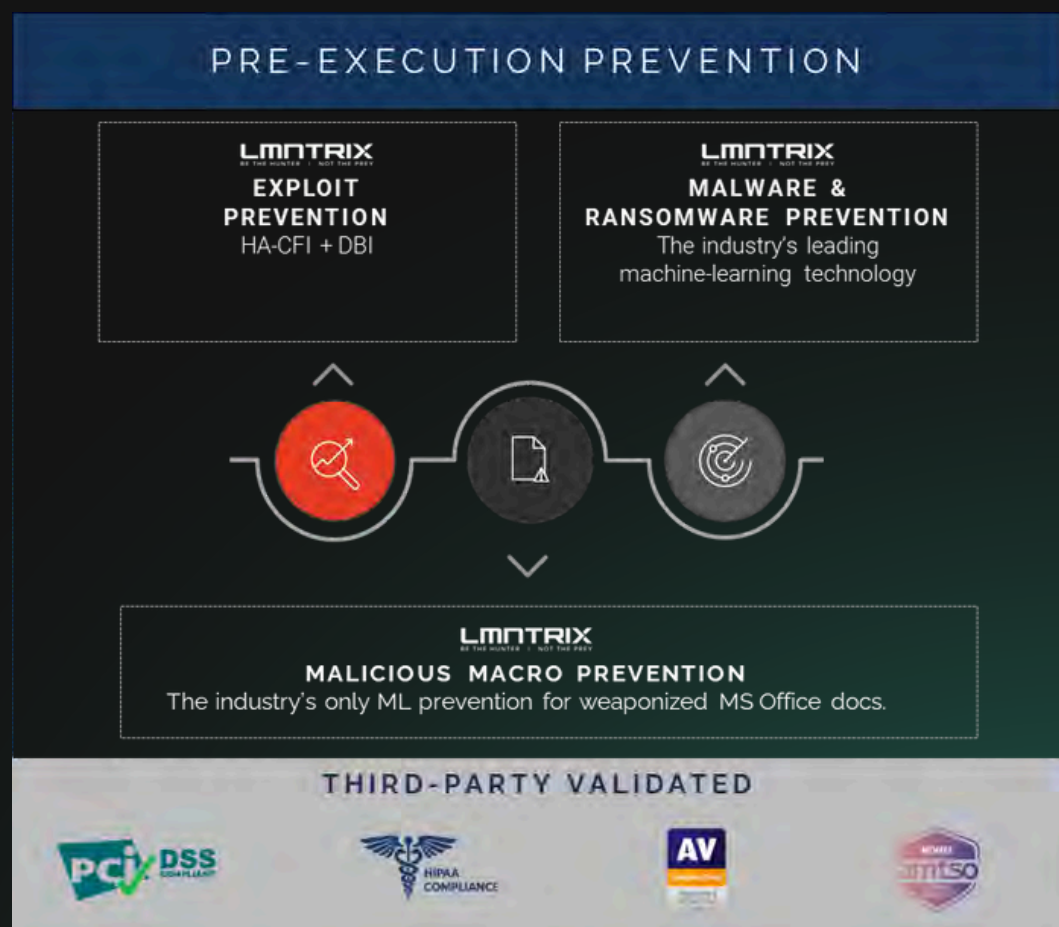
SIGNAL OVER NOISE

- Real-time prevention with lightweight agent
- High-fidelity detections mapped to MITRE ATT&CK
- Automated + analyst-led response 24x7



BLOCK WHAT'S BAD. CONTAIN WHAT'S SUSPICIOUS.

- Behavioral ransomware protection
- Memory and script defense (PowerShell, LOLBins)
- Device control: USB, drivers, kernel-level hardening



DETECTIONS THAT MAKE SENSE

- Correlated alerts → a single incident view
- Built-in ATT&CK mapping for fast triage
- Zero-day technique coverage via behavior analytics

The screenshot displays the Lmnatrix security dashboard interface. The top navigation bar includes tabs for HUD, KILLBOX, EXPLORE, INTEL, INCIDENTS, and REPORTS. The left sidebar contains filters for user (Carlo Minassian), company, timeframe (Oct 4 2025), and selected fields. The main area shows a correlated incident view for 'Execution of Persistent Scripts' on Oct 4 2025, 9:00 AM. A process flow diagram illustrates the execution path: winlogon.exe → userinit.exe → explorer.exe → SecurityHealthSystray.exe → WavesSvc64.exe → expand.exe. Below the diagram, a table lists related events:

Event type	IP address	Status	OS
Execution of Persistent Scripts	-	open	Windows 11 (build 26100)

The right sidebar provides an overview of the persistence alert, including details on the detected persistence on APLAPy9hpCwB6JX, alert status, and endpoint information.

FROM ALERT TO ACTION IN MINUTES

- One-click isolate host
- Kill process / quarantine file
- Live Response shell for deep IR
- Prebuilt remediation playbooks

Endpoint Response

Select and Configure Response(s)

You have currently selected 1 Endpoint. Once configured, select Create Response to launch your response.

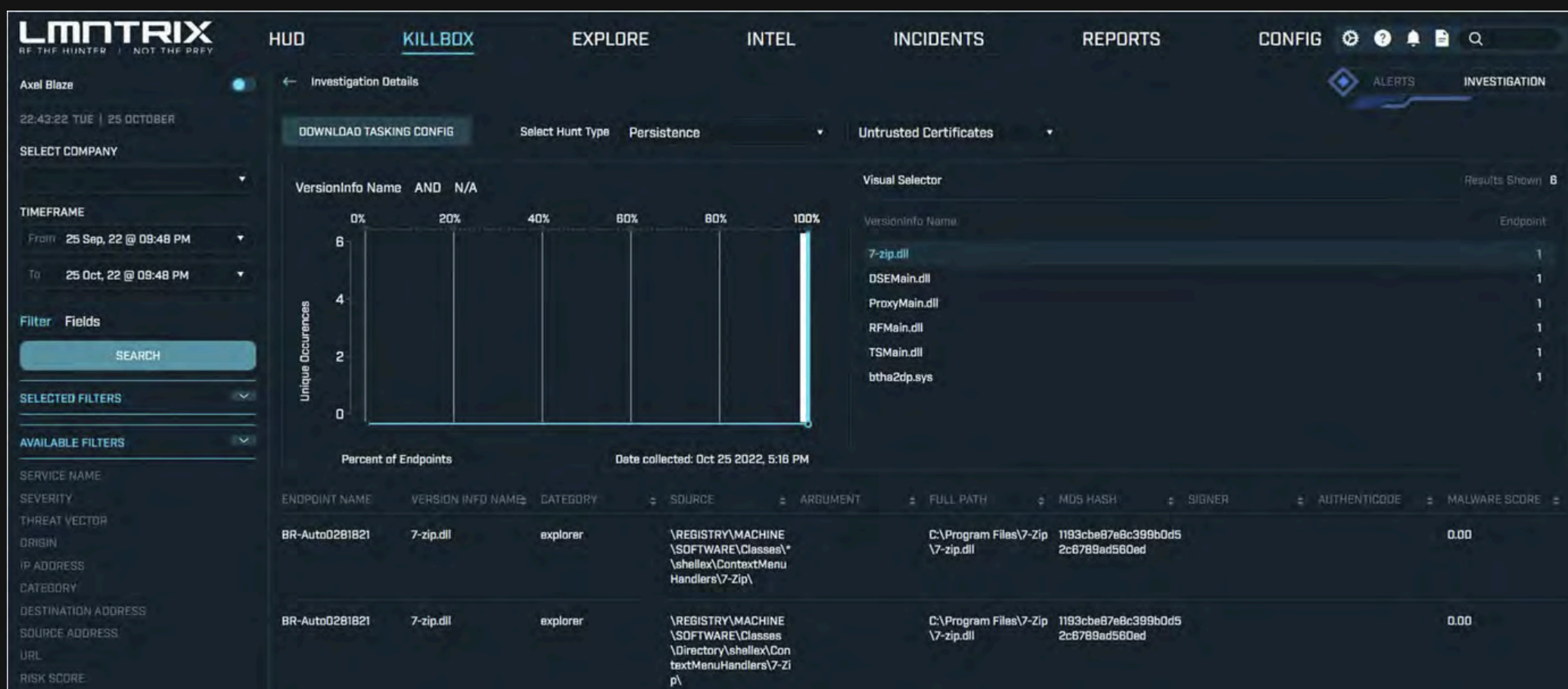
RESPONSE TYPE		ADVANCED CONFIGURATION
☐ Delete File	ADVANCED	File Path c:\\windows\\.....
☒ Execute File	COLLAPSE	Max Time [Seconds] Enter Numeric Value
☐ Get File	ADVANCED	☐ Collect Output ☐ Delete After Execution
☐ Isolate Host	ADVANCED	Arguments Enter Arguments
☐ Kill Process	ADVANCED	
☐ Suspend Thread	ADVANCED	
☐ Upload File	ADVANCED	

Cancel

Create Response

VISIBILITY & HUNTING

- Rich endpoint telemetry for 90 days
- Saved hunts for recurring threats
- IOC & Sigma-style query support



The 'START INVESTIGATION' dialog box is shown, allowing users to select hunt types and configure advanced options. The 'Hunt Type' section includes checkboxes for Applications, File System, Firewall Rules, IOC Search, Loaded Drivers, Network, Persistence, Process, Registry, Removable Media, System Configuration, and Users. The 'Advanced configuration' section includes a 'Filter By (Optional)' dropdown and a 'Select Categories (Required)' list with checkboxes for WMI, Background Intelligent Transfer Service, Codec, Logon, Driver, Office, Service, Applnit, and Explorer.

Buttons at the bottom include 'CONFIRM HUNTS' and 'CANCEL'.

TECHNOLOGY + PEOPLE = OUTCOMES

- 24x7 monitoring by LMNTRIX analysts
- Threat hunting and guided remediation
- Post-incident reports and executive summaries



CUT RISK. PROVE IT.

- Faster MTTD/MTTR across endpoint incidents
- Fewer false positives → more real work done
- Audit-ready evidence and ATT&CK coverage reports





READY TO SEE IT IN ACTION?

Get a live demo of LMNTRIX Endpoint Security and our MXDR service.



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

VISIT
LMNTRIX.COM



LMNTRIX
BE THE HUNTER | NOT THE PREY