

LMNTRIX NDR

SEE EVERYTHING, STOP ANYTHING

LMNTRIX NDR transforms your network into a transparent, intelligent defense system that detects and responds to threats in real-time—before they can cause business disruption.



LMNTRIX
BE THE HUNTER | NOT THE PREY

01

CORE CAPABILITIES

COMPLETE NETWORK VISIBILITY

- East-West & North-South Traffic Analysis: Monitor all network communications
- Device Discovery & Classification: Automatically identify and catalog every connected device
- Traffic Metadata Analysis: Deep packet inspection without performance impact

LMNTRIX

BE THE HUNTER | NOT THE PREY

HUD

KILLBOX

EXPLORE

INTEL

INCIDENTS

REPORTS

CONFIG

Carlo Minassian

02:08:55 WED | 11 JUNE

SELECT COMPANY

TIMEFRAME

From Jun 10 2025, 1:59 AM

To Jun 11 2025, 1:59 AM

SIEM

IDENTITY

CLOUD

Flows

DNS

HTTP

TLS

External alerts

Source IPs

Showing: 40,552 IPs

IP	Autonomous system	Bytes in	Bytes out	Flows	Destination IPs
10.36.54.213	—	2789 GB	1.2 TB	96,112	19
10.36.38.211	—	21 GB	466.06 GB	78,888	18
144.130.165.174	Telstra Limited	120.62 GB	322.94 GB	1,998,222	18,552
10.36.38.159	—	6.02 GB	224.63 GB	113,986	251
10.36.54.158	—	198.55 MB	109.8 GB	244,696	498
10.36.34.17	—	1.39 GB	51.43 GB	43,605	171
10.36.34.18	—	1.26 GB	36.51 GB	42,410	167
10.36.34.19	—	1.27 GB	26.38 GB	35,042	163
10.36.34.16	—	1.47 GB	20.84 GB	34,956	170
10.36.51.152	—	829.12 KB	13.48 GB	3,512	10

Rows per page: 10

Destination IPs

Showing: 47,384 IPs

IP	Autonomous system	Bytes in	Bytes out	Flows	Source IPs
10.36.38.211	—	848.8 GB	14.05 GB	20,790	10
10.36.54.213	—	261.62 GB	5.38 GB	18,135	11
206.148.51.02	BLUEARCHIVE-ZONE-1	257.28 GB	9.73 GB	42,800	17
206.148.51.03	BLUEARCHIVE-ZONE-1	256.88 GB	9.74 GB	43,449	17
206.148.51.00	BLUEARCHIVE-ZONE-1	256.67 GB	9.75 GB	44,267	17
206.148.51.01	BLUEARCHIVE-ZONE-1	255.85 GB	9.74 GB	44,904	17
10.207.60.91	—	249.88 GB	1.82 MB	2,283	7
10.207.60.85	—	36.34 GB	1.28 MB	1,281	10
10.36.38.159	—	35.89 GB	3.94 GB	44,126	41
10.207.29.110	—	34.14 GB	286.52 KB	747	4

Rows per page: 10

Source Countries

Showing: 178 Countries

Destination Countries

Showing: 102 Countries

CORE CAPABILITIES

AI-POWERED THREAT DETECTION

- Behavioral Analytics: Establish network baselines and detect anomalies
- Machine Learning Models: Identify unknown threats and zero-day attacks
- Attack Pattern Recognition: Correlate activities across the attack lifecycle
- Real-time Processing: Detect threats as they happen, not hours later

LMNTRIX

BE THE HUNTER | NOT THE PREY

Carlo Minassian

19:26:42 THU | 17 JULY

SELECT COMPANY

TIMEFRAME

From Jun 1 2023, 6:00 PM

To Jul 17 2025, 6:49 PM

SELECTED FIELDS

Search by field...

Service Name

Source Address

Destination Address

@timestamp

AVAILABLE FIELDS

Search by field...

Cloud Vendor

Company Name

Hostname

HUD

KILLBOX

EXPLORE

INTEL

INCIDENTS

REPORTS

CONFIG

Actions

@Timestamp

Service Name

Host Name

Source Address

Source Port

Destination Address

Destination Port

JUL 17 2025, 6:47 PM

NDR

DET01

.DC

47.88.6.181

—

103.66.170.240

69

JUL 17 2025, 6:46 PM

NDR

DET01

DC

206.168.34.71

10964

103.66.170.233

47808

JUL 17 2025, 6:46 PM

NDR

DET01

DC

91.149.253.97

44305

103.66.170.91

500

IP Address

Country

Threat vector

91.149.253.97

Poland

Discovery



JUL 17 2025, 6:46 PM

NDR

ET02

.SD

—

—

—

—

JUL 17 2025, 6:46 PM

NDR

DET01

.DC

—

—

—

—

JUL 17 2025, 6:45 PM

NDR

DET01

.DC

185.180.141.57

—

103.66.170.167

6969

JUL 17 2025, 6:45 PM

NDR

DET01

.DC

193.124.46.101

59237

103.66.170.240

500

Jul 17 2025, 6:46 PM

Web Server Enforcement Violation

@timestamp Jul 17 2025, 6:46 PM

_id 5200F5gBCf7pgvltzeaz

fields.workflow_status open

_index .ds-ndr-xdr-kestrel-2025.07-2025.07.01-000001

event.dataset LMNTRIX_INTRUSION_DETECTION_ENGINE

host.name jcdet01

host.ip 10.36.12.136

source.ip 91.149.253.97

source.port 44305

destination.ip 103.66.170.91

destination.port 500

threat.technique Discovery

threat.name

threat.information {572A2032-3235-4263-9980-C69EF8497D92}

threat.description Zyxel ZyWALL Command Injection (CVE-2023-28771)

threat.reference CVE-2023-28771

network.protocol 17



03

CORE CAPABILITIES

AUTONOMOUS RESPONSE & CONTAINMENT

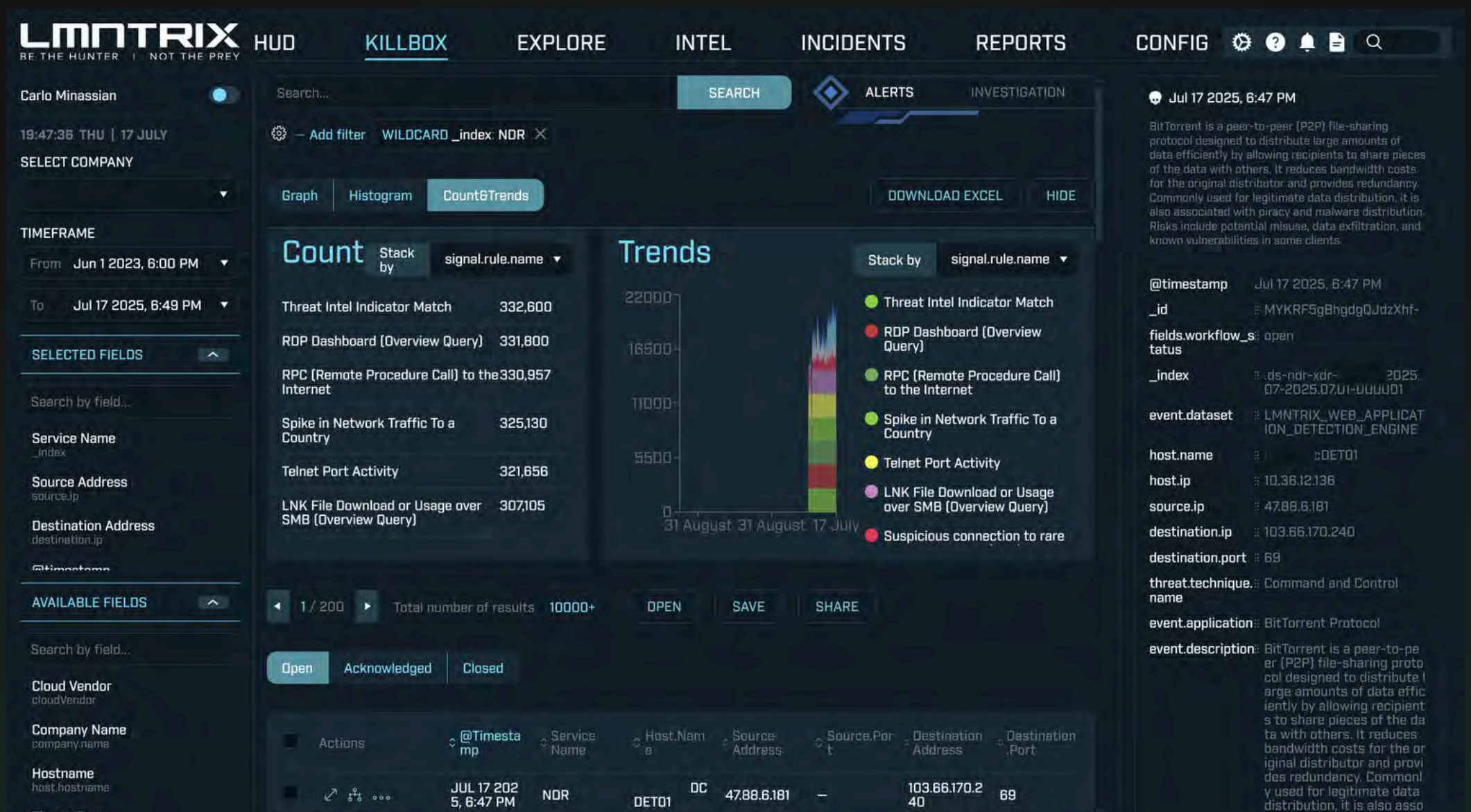
- Automated Threat Response: Isolate compromised devices and block malicious traffic
- Dynamic Quarantine: Contain threats without disrupting business operations
- Intelligent Prioritization: Focus on high-risk threats first
- Customizable Playbooks: Automate response workflows for your environment

UNIFIED XDR INTEGRATION

- Single Platform: NDR integrated with endpoint, email, Identity, mobile and cloud security
- Correlated Intelligence: Connect network events with broader attack context
- Centralized Management: One console for all security operations
- Streamlined Workflows: Reduce tool switching and alert fatigue

USE CASES

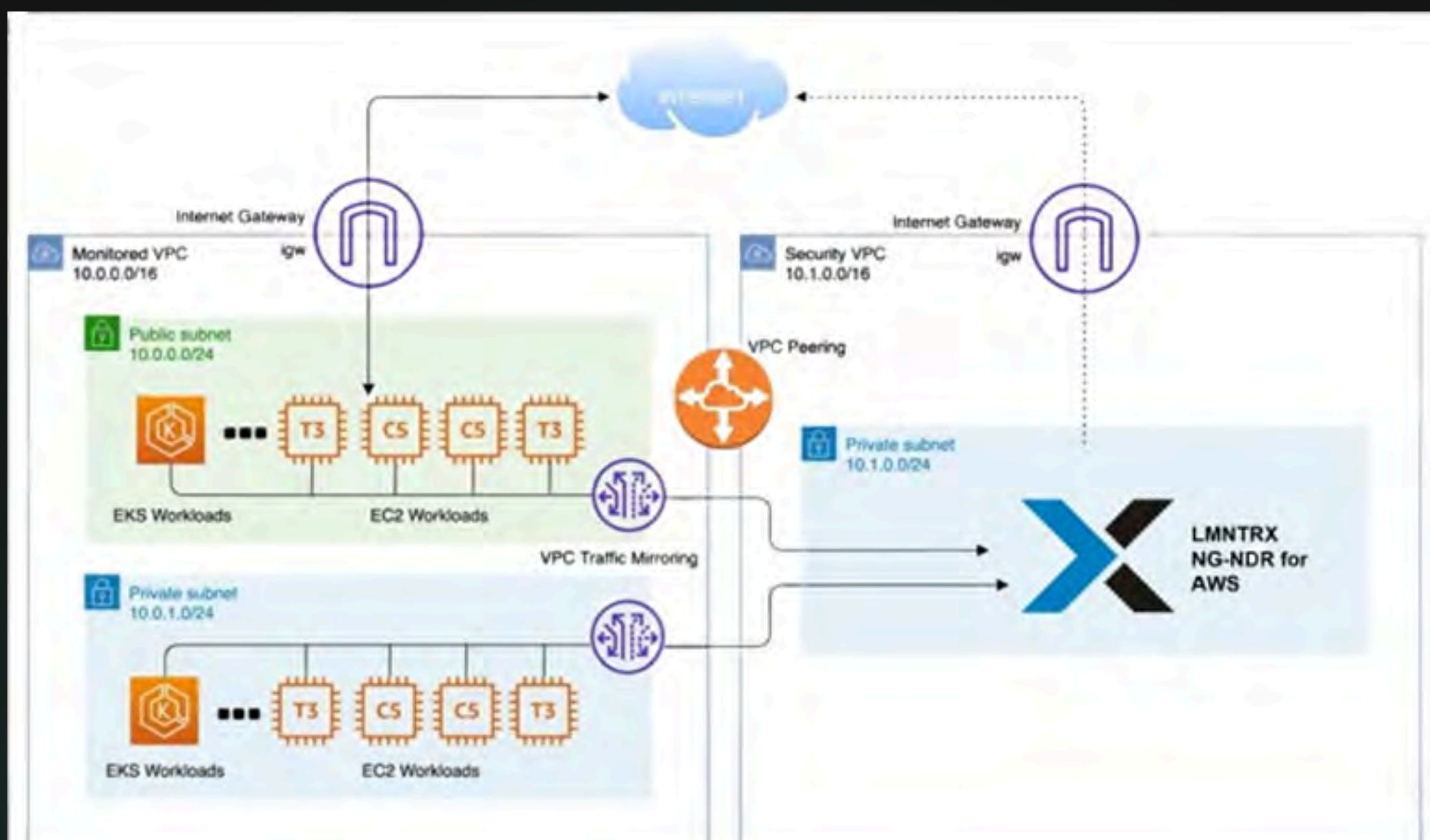
- Advanced Persistent Threats (APTs)
- Ransomware Prevention
- Insider Threat Detection
- Supply Chain Attacks
- Cloud Security
- Compliance & Forensics



TECHNICAL SPECIFICATIONS

FLEXIBLE DEPLOYMENT

- On-Premise: Physical and virtual appliances
- Cloud-Native: AWS, Azure, Google Cloud Platform
- Hybrid: Seamless integration across environments
- Edge: Distributed deployment for remote locations
- Agentless





07

TECHNICAL SPECIFICATIONS

PRIVACY BY DESIGN

- No decryption required
- Metadata-driven analysis
- Fully compliant with privacy and sovereignty requirements

PERFORMANCE & SCALE

- Throughput: Up to 100+ Gbps network analysis
- Latency: Sub-second threat detection and response
- Scalability: Elastic cloud architecture
- Storage: Configurable data retention policies

CUSTOMER SUCCESS METRICS

- 95% reduction in mean time to detection
- 85% decrease in false positive alerts
- 300% improvement in SOC team efficiency
- 100% Visibility Across Core, Cloud, and Edge

WHAT SETS US APART?

Feature	LMNTRIX NDR	Traditional NDR
Integrated with XDR	✓ Yes	✗ Siloed
Behavioral AI	✓ Yes	⚠ Partial
Cloud-native visibility	✓ Full	⚠ Limited
Encrypted traffic detection	✓ Yes	⚠ Decrypt required
Deception Integration	✓ Native	✗ Not supported
Response Automation	✓ Playbooks & AI	⚠ Manual



READY TO SEE LMNTRIX NDR IN ACTION?



Know your network. Detect the undetectable.
Speak to a specialist or schedule a personalized
LMNTRIX NDR demo today.

VISIT
LMNTRIX.COM



LMNTRIX
BE THE HUNTER | NOT THE PREY