

LMNTRIX SIEM

REIMAGINING SIEM FOR A POST-BREACH, CLOUD-FIRST WORLD



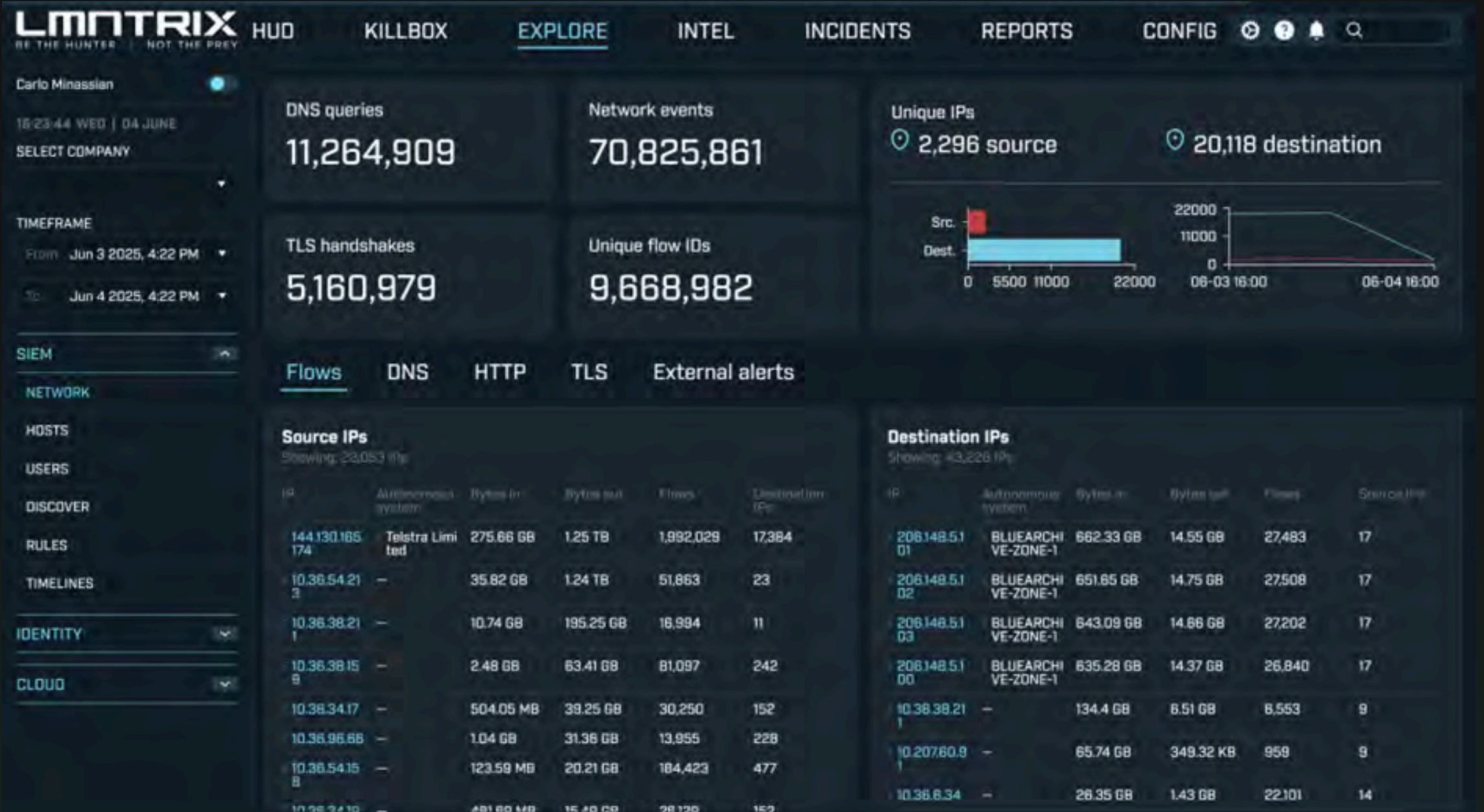
LMNTRIX
BE THE HUNTER | NOT THE PREY



01

SIEM AT THE SPEED OF LIGHT

LMNTRIX SIEM is purpose-built to support deep forensic investigations, compliance reporting, centralized log retention and specific threat detection use cases—without the performance drag of traditional SIEMs.



WHY LMNTRIX SIEM?

- Post-Breach Visibility Without the Noise
- Intelligent Over Traditional
- Security-as-a-Service Flexibility
- Codified Detection Expertise

The screenshot displays the LMNTRIX SIEM interface. The top navigation bar includes tabs for HUD, KILLBOX, EXPLORE (active), INTEL, INCIDENTS, REPORTS, and CONFIG. The left sidebar shows a 'Core Mission' section with a 'SELECT COMPANY' dropdown and a 'TIMELINE' section with two time ranges: 'Jan 3 2025, 4:22 PM' and 'Jan 4 2025, 4:22 PM'. The main content area is titled 'Rules' and shows a list of rules under the 'All rules' tab. The rules list includes columns for Rule Name, Volume (Hits), Score, Last Seen (Time), and Status. The rules are as follows:

Rule Name	Volume (Hits)	Score	Last Seen (Time)	Status
Dark transferring large amount of data over HTTP	943	318	Jun 4, 2025 @ 10:48:43.870	partial failure
Suspicious connection to rare top-level domain (TLF) request	203	30	Jun 4, 2025 @ 10:58:37.665	successful
Threat Intel Indicator Match	330	1048	Jun 4, 2025 @ 10:50:29.600	partial failure
Unusual DNS Request			Jun 4, 2025 @ 10:20:38.070	successful
HTTP 200 OK indicators for Executive	277	25	Jun 4, 2025 @ 10:40:56.675	successful
Spike in Network Traffic To a Country	1041	1116	Jun 4, 2025 @ 10:10:20.060	partial failure



03

KEY CAPABILITIES

CENTRALIZED LOG COLLECTION & CORRELATION

Aggregate, normalize, and correlate logs from all sources—endpoints, cloud, network, and identity—for unified contextual visibility.



• •
• •
• •
•

LMNTRIX

BE THE CENTER / NOT THE PERIPHERY

HUD

KILLBOX

EXPLORE

INTEL

INCIDENTS

REPORTS

CONFIG

🔔

🔍

Carlo Minnaster

17:27:57 WED (03 JUN)

SELECT COMPANY

LMNTRIX

TIMEFRAME

From: Jun 3 2025, 4:34 PM

To: Jun 4 2025, 4:34 PM

SELECTED FIELDS

Source by host

Service Name

Source Address

Destination Address

Available Fields

Source by host

Cloud Vendor

Company Name

Hostname

Network

📄

+ Add files

🔍

Potential Password Spraying of Microsoft 365 User Accounts

Created by: LMNTRIX on Nov 18, 2024 @ 17:27:57 JST

Revised by: LMNTRIX on May 16, 2025 @ 16:25:26 JST

LAST PENDING

+ succeeded at

🔄

🟢 Activate

⚙️ Edit rule settings

⚡ Actions

About

Details

Investigation Guide

Severity

High

Risk score

73

Note

Setup

The Office 365 Logs Fleet integration, Flatbeat module, or similarly structured data is required to be compatible with this rule.

False Positives

Automated processes that attempt to authenticate using expired credentials and unbounded retries may lead to false positives.

Definition

Index pattern

_default

Custom Query

event.type:Microsoft365_auth and event.provider:(Exchange or AzureActiveDirectory) and event.category:(authentication and event.action:["UserLoginFailed" or "PasswordRequestorAuthUsingPassword"])

Rule type

threshold

Timeline template

None

Tags

Cloud

Continuous Monitoring

LMNTRIX

Identity and Access

Microsoft 365

SecOps

rule_default_8.0

Schedule

Runs every

50m

Additional

look-back

25m

KEY CAPABILITIES

CODIFIED DETECTION RULES

Deploy preconfigured, MITRE ATT&CK-aligned rulesets or build custom detections tailored to your environment.

The screenshot displays the LMNTRIX security dashboard. The top navigation bar includes tabs for HUD, KILLBOX, EXPLORE (active), INTEL, INCIDENTS, REPORTS, and CONFIG. The left sidebar shows a sidebar menu with options like SELECT COMPANY, TIMEFRAME, and various data sources (SIEM, NETWORK, HOSTS, USERS, DISCOVER, RULES, TIMELINES, IDENTITY, CLOUD). The main content area is titled 'Rules' and shows a list of rules. The rules are displayed in a table with columns for Rule Name, Count, Severity, Last Eval, Last Success, Last Failure, Version, and Action. The table shows four rules, each with a status indicator (green or red) and a 'Details' link.

Rule	Count	Severity	Last Eval	Last Success	Last Failure	Version	Action
Client transferring large amount of data over HTTP	21	low	Jun 4, 2025 @ 15:45:43.670	partial failure	Mar 18, 2025 @ 15:45:10.655	5	LMNTRIX Rule: Partial
Suspicious connection to rare top-level domain (TLD) request	60	medium	Jun 4, 2025 @ 15:28:37.665	succeeded	Feb 27, 2025 @ 14:21:15.852	3	LMNTRIX Rule: Partial
Threat intel indicator Match	47	medium	Jun 4, 2025 @ 15:37:26.500	partial failure	Jan 27, 2025 @ 02:50:21.199	4	LMNTRIX Rule: Partial
Unusual Web Request	21	low	Jun 4, 2025 @ 15:21:08.500	succeeded	Jan 20, 2025 @ 00:23:25.160	104	Machine Learning Rule: Partial



06

KEY CAPABILITIES

REAL-TIME DASHBOARDS & VISUALIZATIONS

Interactive, customizable dashboards visualize alerts, trends, and incidents—helping your team triage faster and act sooner.



KEY CAPABILITIES

FORENSIC SEARCH & SUB-SECOND QUERYING

Run lightning-fast queries across billions of events. Reconstruct incidents and timelines with precision and speed.

The screenshot displays the LMNTRIX security dashboard. The top navigation bar includes tabs for HUD, KILLBOX, EXPLORE (active), INTEL, INCIDENTS, REPORTS, and CONFIG. The left sidebar contains a 'Data Mission' section with a 'SELECT COMPANY' dropdown and a 'TIMEFRAME' section with date range selectors. Below these are categories like SIEM, NETWORK, HOSTS, USERS, DISCOVER, RULES, and TIMELINE. The main content area is titled 'CREATE NEW TIMELINE' and features a search bar with the query 'DND Turning Hunt'. Below the search bar is a table with columns for QUERY, CORRELATION, NOTES, and PINNED. The table shows two entries for 'Process CSVDemo.exe' on 'Jun 4 2025, 4:34 PM'. The right sidebar shows 'EVENT DETAILS' for a specific event, including a 'Table' view and a 'SEARCH' button.

QUERY	CORRELATION	NOTES	PINNED
Host Name: KESM0002			
Process CSVDemo.exe (PID: 89578) by user: COMPANION_P			
Process CSVDemo.exe (PID: 89578) by user: COMPANION_P			

KEY CAPABILITIES

THREAT INTELLIGENCE INTEGRATION

Enrich alerts with real-time global threat intel
—automatically identifying malicious IPs,
hashes, domains, and behaviors.

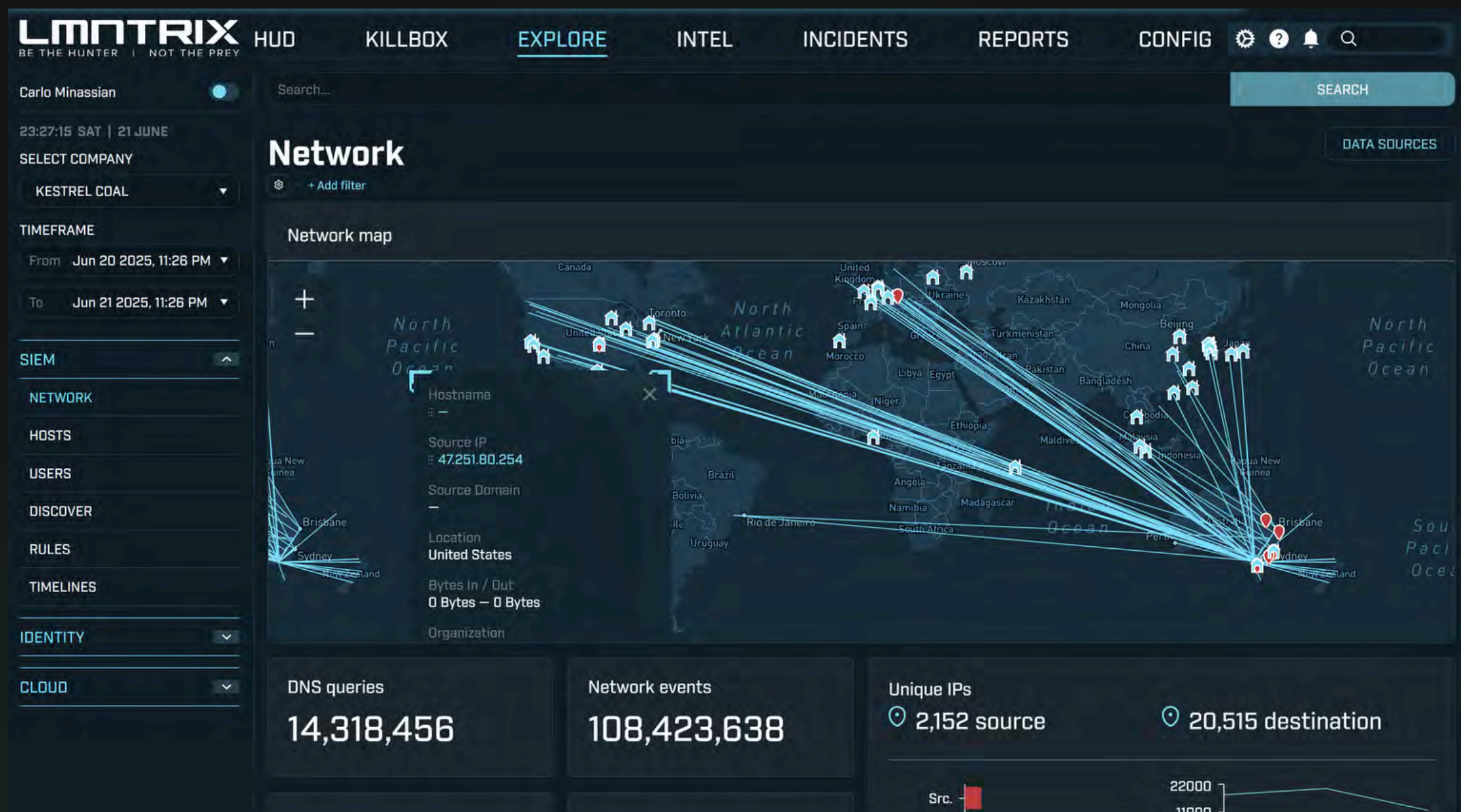
The screenshot displays the LMNTRIX security dashboard interface. The top navigation bar includes tabs for HUD, KILLBOX, EXPLORE, INTEL (selected), INCIDENTS, REPORTS, and CONFIG. The left sidebar shows a user profile for Carlo Minassian and a navigation menu with options like OVERVIEW, INTELLIGENCE, ATTRIBUTES, FEEDS, NEWS, COMMENTS, and INDICATORS. The main content area is titled 'SUNBURST' and features a 'Critical risk' indicator. Below this, there are sections for 'Highlights' (malware Category, 45 indicators, MITRE ATT&CK Enterprise, C&C Domains, C&C IPs Feeds, Windows Technologies) and 'External Links' (VirusTotal, Shodan, Abuse.ch, Webroot, IBM Xforce, Alienvault, Abuseipdb). On the right, an 'Events' panel shows a timeline of actions: Added (Dec 14 2020, 11:59 AM), Updated (Jun 21 2025, 11:18 AM), and Seen (Jun 20 2025, 7:03 AM). At the bottom, a table displays threat intelligence data with columns for Name, Value, and Message.

Intelligence	Name	Value	Message
STATUS	2001	SUCCESS	Succeeded to generate reputation
RESOURCE			
SERVICE			
TIMESTAMP			
RISK SCORE			

KEY CAPABILITIES

GRAPH-BASED THREAT ANALYSIS

Uncover hidden relationships between users, events, and devices using our graph analytics engine. See the big picture—
instantly.



10

KEY CAPABILITIES

COMPLIANCE & AUDIT SUPPORT

Meet your GDPR, PCI DSS, ISO 27001, and other compliance obligations with centralized, immutable log storage.





BUILT BY PRACTITIONERS. POWERED BY EXPERIENCE.

LMNTRIX SIEM was built from the ground up by the same experts who respond to the world's most consequential breaches. Every feature, rule, and workflow reflects deep, real-world insight into modern adversary behavior.

LMNTRIX

BE THE HUNTER. NOT THE PREY.

HUD

KILLBOX

EXPLORE

INTEL

INCIDENTS

REPORTS

CONFIG

🔔

🔍

🔔

🔍

Carlo Minassian

🔔

Rules

18:30:02 WED | 04 JUNE

SELECT COMPANY

TIMEFRAME

From Jun 3 2025, 4:22 PM

To Jun 4 2025, 4:22 PM

SIEM

NETWORK

HOSTS

USERS

DISCOVER

RULES

TIMELINES

IDENTITY

CLOUD

Create new rule

Define rule

Rule Type

Custom query

Threshold

Event Correlation

Indicator Match

Index patterns

tg-kestrel-winlog*

tg-kestrel-audit*

tg-kestrel-linux*

ndr-xdr-kestrel*

edr2-xdr-kestrel*

dicolve-xdr-kestrel*

packets-data-kestrel*

packets-metric-kestrel*

alerts-security.alerts-kestrel*

Custom Query

Search

Add Filter

Custom query is required

Timeline template

None

SAVE QUERY



READY TO SEE LMNTRIX SIEM IN ACTION?



Whether you're replacing a legacy SIEM, need forensic capability on-demand, or require advanced log management for compliance—LMNTRIX SIEM delivers unmatched speed, precision, and scalability.

VISIT
LMNTRIX.COM



LMNTRIX
BE THE HUNTER | NOT THE PREY