

LMNTRIX CLOUD

SECURE EVERY CLOUD.
ELIMINATE EVERY
BLIND SPOT.

LMNTRIX Cloud delivers full-spectrum visibility,
detection, and response across your multi-cloud
infrastructure.



LMNTRIX
BE THE HUNTER | NOT THE PREY

REIMAGINE CLOUD SECURITY

- Cloud Security Posture Management (CSPM) to continuously audit misconfigurations and compliance
- Cloud Detection & Response (CDR) for real-time threat detection and mitigation
- Cloud Infrastructure Entitlement Management (CIEM) to eliminate excessive permissions



CDR

BEHAVIOR-BASED DETECTION & STORYLINE CORRELATION

Correlates runtime activity, permissions usage, and threat indicators into clear attack storylines using Malicious Behavior Indicators (MBIs)—eliminating alert fatigue and empowering faster response.

The screenshot displays the LMNTRIX security dashboard interface. The top navigation bar includes tabs for HUD, KILLBOX, EXPLORE, INTEL, INCIDENTS, REPORTS, and CONFIG. The left sidebar contains filters for user (Carlo Minassian), date (18:24:11 SAT | 07 JUNE), company selection, timeframes (May 7 2025, 6:23 PM to Jun 7 2025, 6:23 PM), and field selection (Cloud Vendor, Company Name, Threat Type). The main content area shows a list of incidents, with the selected incident being an "ANOMALOUS API INVOCATION BY USER Y.RISANGTOMO@ME.COM" with a score of 2. Below this, a detailed view of the incident is shown, including a timeline of events, a diagram of the attack flow, and a table of suspicious behavior indicators. The right sidebar displays a summary of the incident, including the timestamp (May 30, 2025, 2:17 AM), user (y.risangtomo@me.com), company (Acclime), signal (open), vendor (AWS), title (Anomalous API invocation by User y.risangtomo@me.com), attack tactic (COLLECTION), account ID (115458716067), and type (anomalousC3).

LMNTRIX BE THE HUNTER | NOT THE PREY

HUD **KILLBOX** EXPLORE INTEL INCIDENTS REPORTS CONFIG

Carlo Minassian

18:24:11 SAT | 07 JUNE

SELECT COMPANY

TIMEFRAME

From May 7 2025, 6:23 PM

To Jun 7 2025, 6:23 PM

SELECTED FIELDS

Search by field...

Cloud Vendor cloudVendor

Company Name company.name

Threat Type threat.type

AVAILABLE FIELDS

Search by field...

Destination Address destination.ip

Hostname host.hostname

Source Address source.ip

Timestamp

1 / 1 Total number of results 1 OPEN SAVE SHARE

Open Acknowledged Closed

Actions	Title	Score	Cloud Vendor	Company Name	Threat Type
	ANOMALOUS API INVOCATION BY USER Y.RISANGTOMO@ME.COM	2	AWS		ACTIVITY

Anomalous API invocation by user y.risangtomo@me.com

Tactic: COLLECTION, ID: TA0009
Source Computer: 202.72.220.43

Target User: y.risangtomo@me.com
Source Ip: 202.72.220.43

Anomalous API invocation source by user y.risangtomo@me.com

2 Suspicious Behavior Indicators Invoked APIs (1) Invocation Details

Access from a country not typical for user: Indonesia	s3:ListBuckets	User	y.risangtomo@me.com
Access from an Anomalous internet service provider		Source IP	202.72.220.43
		User Agent	Mozilla/5.0 [Windows NT 10.0; Win64; x64] AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 Edg/136.0.0.0



CSPM

PROTECT

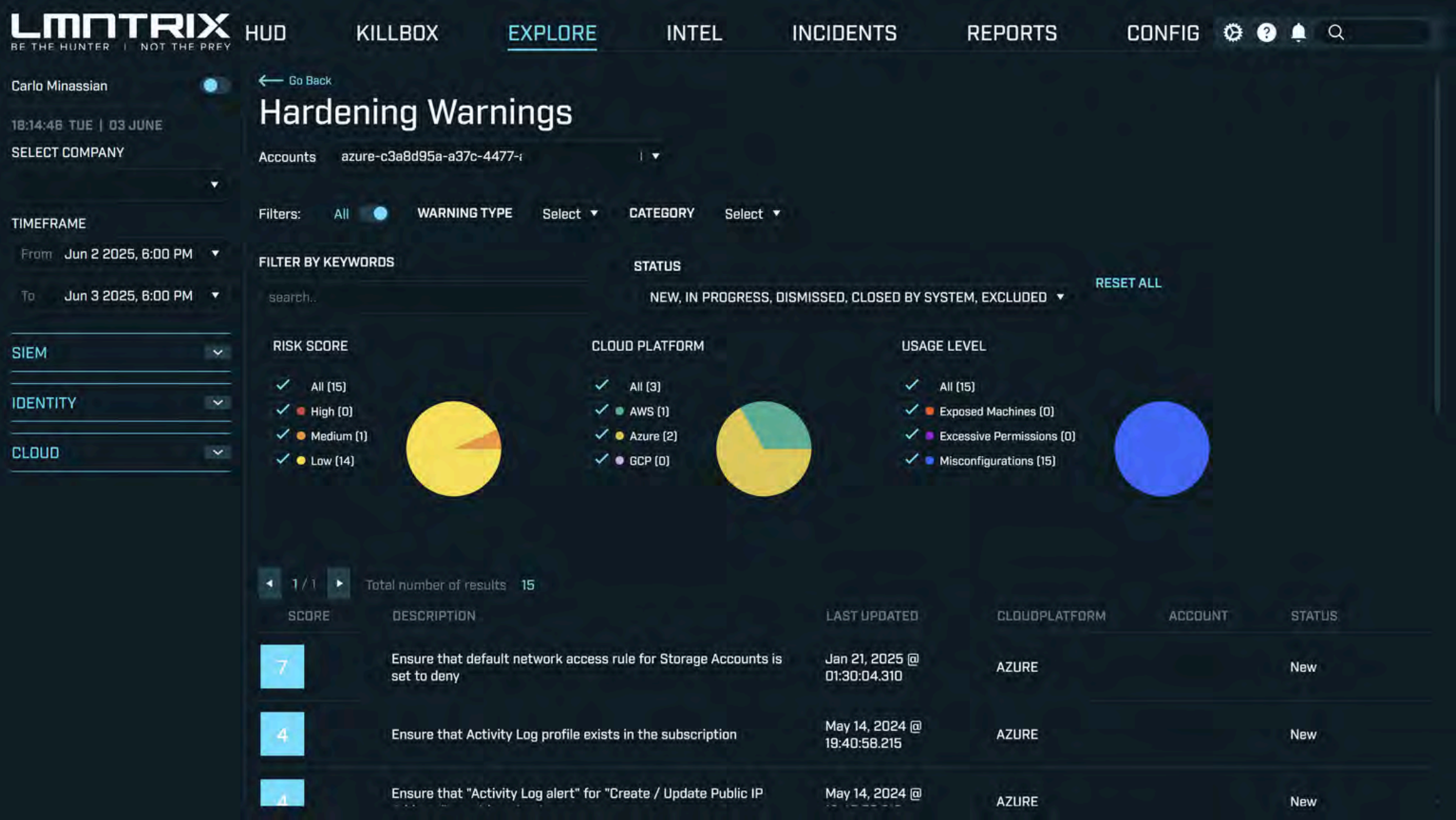
Public exposures, authentication flaws, and insecure configurations

DETECT

Flags critical risks like unencrypted data, open ports, and weak policies

RESPOND

Automatically remediates misconfigurations with customizable logic



CIEM

- Audits permissions and uncovers overprivileged users and toxic combinations
- Visualizes effective entitlements and recommends least privilege models
- Continuously tracks how access is granted, used, and misused

The screenshot displays the LMNTRIX CIEM (Continuous Identity Entitlement Management) dashboard. The interface is dark-themed with a grid background. The top navigation bar includes the LMNTRIX logo, a user profile (Carlo Minassian), and various menu items: HUD, KILLBOX, EXPLORE (active), INTEL, INCIDENTS, REPORTS, and CONFIG. A search bar is located on the right. The left sidebar contains filters for TIMEFRAME (Jun 2 2025, 6:00 PM to Jun 3 2025, 6:00 PM), SIEM, IDENTITY, and CLOUD. The main content area shows a warning for the user 'leaddev@.com' who is inactive. It includes a timeline of events: 'User Created' (Nov 1, 2023), 'Account Was Created' (Apr 26, 2024), and 'Last Known Active' (Dec 20, 2024). The dashboard also lists '0 Services Permitted' and provides recommendations for user management.

LMNTRIX BE THE HUNTER | NOT THE PREY

HUD KILLBOX EXPLORE INTEL INCIDENTS REPORTS CONFIG

Carlo Minassian

18:27:55 TUE | 03 JUNE

SELECT COMPANY

TIMEFRAME

From Jun 2 2025, 6:00 PM To Jun 3 2025, 6:00 PM

SIEM

IDENTITY

CLOUD

Go Back

2 User leaddev@.com is inactive

ID : 479824425578 LAST UPDATED : Mar 20, 2025 @ 06:57:26.000 CREATED : Mar 20, 2025 @ 06:57:26.000 ACCOUNT : CLOUD PLATFORM : AWS

Why Is This Important?

User Has Been Completely Inactive For 0. This Could Indicate That The User No Longer Needs Access Permissions To This Account And Its Services. Such Inactive Users Can Be Used By Threat Actors To Gain Unauthorized Access To Your Workloads And Data.

Hardening Warning Details

User Created Nov 1, 2023 @ 05:44:48.000 .Com Was Started Protecting Your Account Apr 26, 2024 @ 11:27:57.000 Last Known Active Dec 20, 2024 @ 01:39:00.000

0 Services Permitted

User Details

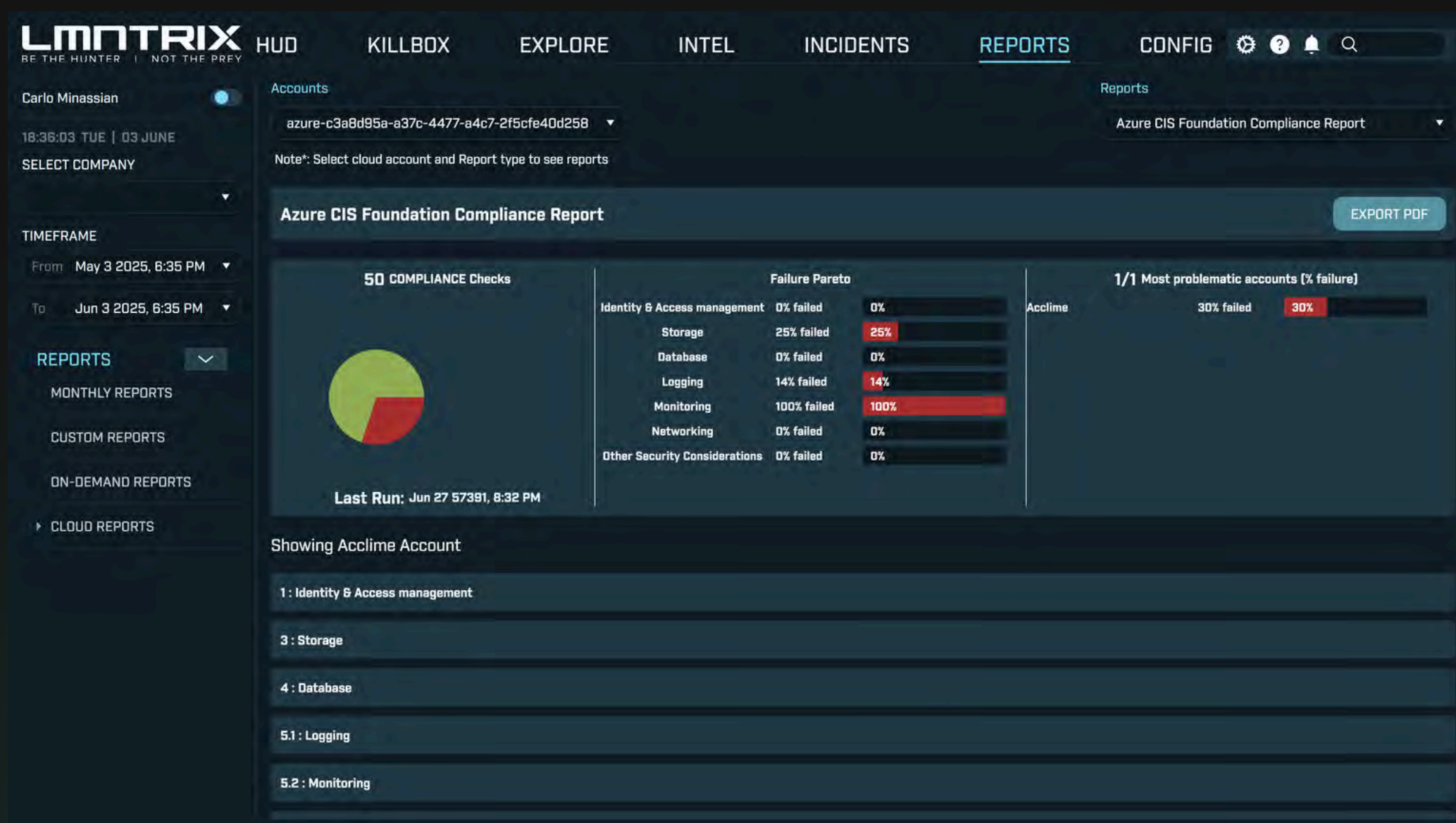
NAME: USER GROUPS: PasswordChange MFAGroup AdminAccess CONSOLE ACCESS: No ACCESS KEYS: No Access Keys

Recommendations

Delete The User From The AWS Account. Otherwise, If You Prefer To Keep This User, Consider Disabling Their Access To The Console, Deactivating Their Access Keys, And Reduce Their Permissions.

COMPLIANCE MONITORING & REPORTING

- Dashboards and exportable reports across regulatory standards
- Real-time insight into gaps and successes by account, region, or vendor



WHAT MAKES LMNTRIX CLOUD DIFFERENT?

🧠 AI + ML Built for the Cloud

Models tuned daily with customer and global telemetry

📈 Runtime Observability

Detects changes and threats in real-time—not just at scan intervals

🔧 Proof-of-Value in 14 Days

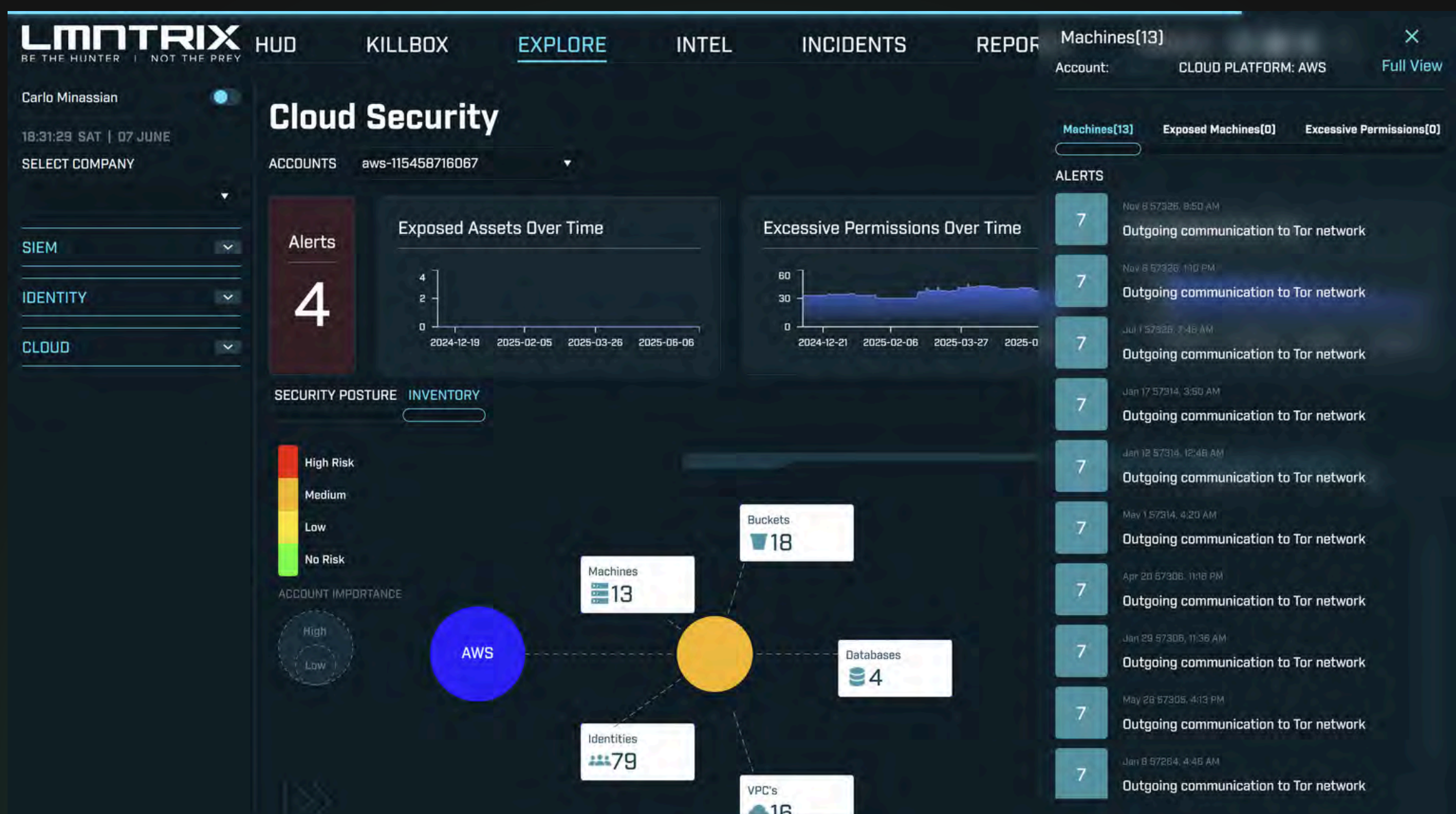
Instantly validate security gaps and value with onboarding, simulation, and results

🔍 Zero Alert Fatigue

Focus on actual threats using storyline-based incident analysis

🧱 Modular + Scalable

From startups to enterprises, configure coverage based on cloud asset footprint





10

READY TO SEE LMNTRIX CLOUD IN ACTION?



Secure Every Cloud. Eliminate Every Blind Spot.

VISIT
LMNTRIX.COM



LMNTRIX
BE THE HUNTER | NOT THE PREY