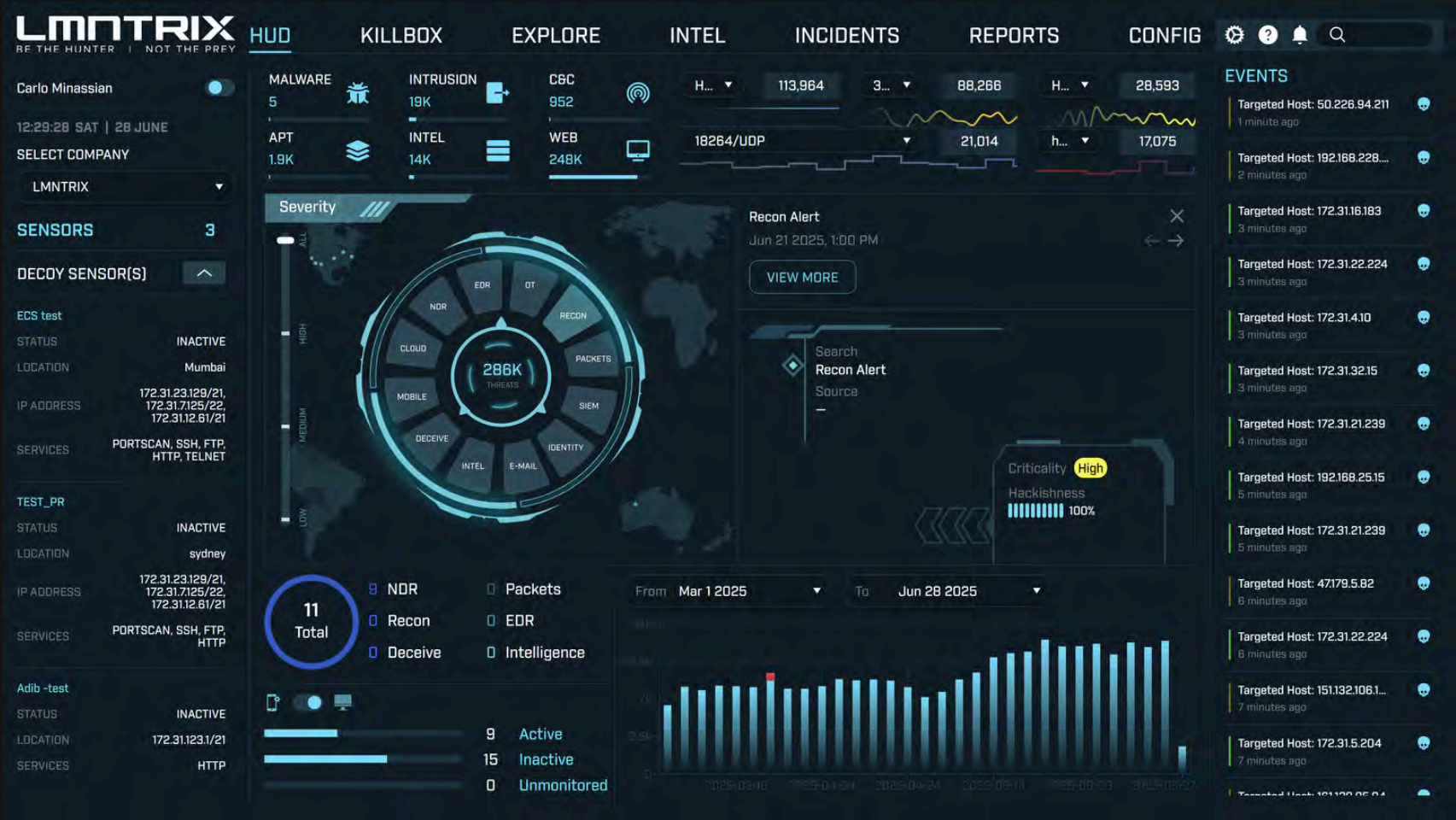


LMNTRIX RECON

HUNT FAST, HYPE LAST:
RECON THAT STOPS
THREATS COLD.



LMNTRIX
BE THE HUNTER | NOT THE PREY

PROACTIVE THREAT VISIBILITY BEYOND THE PERIMETER

In today's threat landscape, your organization's greatest risks may already be exposed — not inside your network, but outside of it. LMNTRIX Recon empowers you with unmatched visibility into the deep and dark web, identifying threats before they escalate into breaches.

The screenshot displays the LMNTRIX Recon interface. The top navigation bar includes tabs for HUD, KILLBOX, EXPLORE, INTEL (selected), INCIDENTS, REPORTS, CONFIG, and a search icon. The left sidebar shows the user 'Carlo Minassian' and a 'SELECT COMPANY' dropdown set to 'LMNTRIX'. Below this are icons for Home, Trackers, and Collections. The main content area is divided into sections: 'LIVE ATTACKS', 'RESEARCH', 'NVD', 'PLAYBOOKS', 'ATT&CK', and 'RECON' (selected). The 'RECON' section features a 'FILTER BY' sidebar with options for Domains, Has Entity, Groups, Has range, Data Leaks, and Data Sources. The central search area shows a 'Search query' of 'google.com' and a 'Languages' dropdown. A large circular progress indicator at the bottom of the search area shows a value of 100. The right side of the interface displays a table of search results with columns for News, Excerpt, Domain, Crawl Date, Relevance, and Hackishness. The table shows several results, including domains like '.com:kjwa' and 'web.archi', with relevance scores of 100%.

LMNTRIX BE THE HUNTER | NOT THE PREY

HUD KILLBOX EXPLORE **INTEL** INCIDENTS REPORTS CONFIG

Carlo Minassian

12:43:42 SAT | 28 JUNE

SELECT COMPANY

LMNTRIX

Home Trackers Collections

LIVE ATTACKS RESEARCH NVD PLAYBOOKS ATT&CK **RECON**

FILTER BY

Domains

Has Entity

Groups

Has range

Data Leaks

Data Sources

Search query

Languages

0 100

DARKINT Exposure

Jul 6 2024, 12:01 AM test

Jul 6 2024, 12:02 AM test

Jul 6 2024, 12:01 AM mandy test

Jul 6 2024, 12:00 AM lmntrix_ceo

Alerts

@TXTLOG_ALIEN - 311.txt Part 912 of 1052

3ebbyrashka:06duzabe:http://store.steampowered.com/login

Mikhael_Mason:dress1kill01:https://www.twitch.tv...

@TXT_ALIEN - 1021.txt Part 1085 of 1350

com.textmeinc.textme3/sa77016635451:Decryption:failed.

cn.xiaofengkj.fitpro/hishaamtamim27@gmail.com:niggaman2009...

1 / 285430 Total number of results 5708594+

News	Excerpt	Domain	Crawl Date	Relevance	Hackishness
.com:kjwa s9...	.com:kjwa s9...	web.archi ve.org	Oct 3 2020, 4:...	100%	100%
ecarluccl @outloo...	ecarluccl @outloo...	web.archi ve.org	Oct 3 2020, 4:...	100%	100%
rera7@out look.co...	rera7@out look.co...	web.archi ve.org	Oct 3 2020, 4:...	100%	100%
om:Perry3 82...	om:Perry3 82...	web.archi ve.org	Oct 3 2020, 4:...	100%	100%
This is our Quick...	This is our Quick...	hackforum s.net	Mar 10 2023,...	100%	100%
Mail Fake Combin...	Ru En User CP...	ordclub.su	May 29 2023,...	100%	100%
(13) Новые Login:P...	Configs Bullet...	craexpro.to	Oct 1 2024, 1:...	100%	100%
(1) Новые сообщ...	Меню Форум...	www.kurs dollara...	Aug 25 2023, 5:...	100%	100%

OUR APPROACH

INTELLIGENCE MEETS INNOVATION

- The largest commercial darknet database
- Proprietary crawling, ML algorithms, and threat scoring
- Decade-long human intelligence networks with deep underground access
- Safe, ethical, and secure data collection practices
- 99.9% uptime | 47 languages supported | 8x faster search efficiency



KEY USE CASES

- Early Warning System for data theft, attack planning, and VIP impersonation
- Supply Chain Intelligence to spot risks in connected entities
- Cyber Insurance Readiness and regulatory compliance support
- Brand & Reputation Management through proactive monitoring
- Security Awareness & Policy Enforcement for HR and executive protection



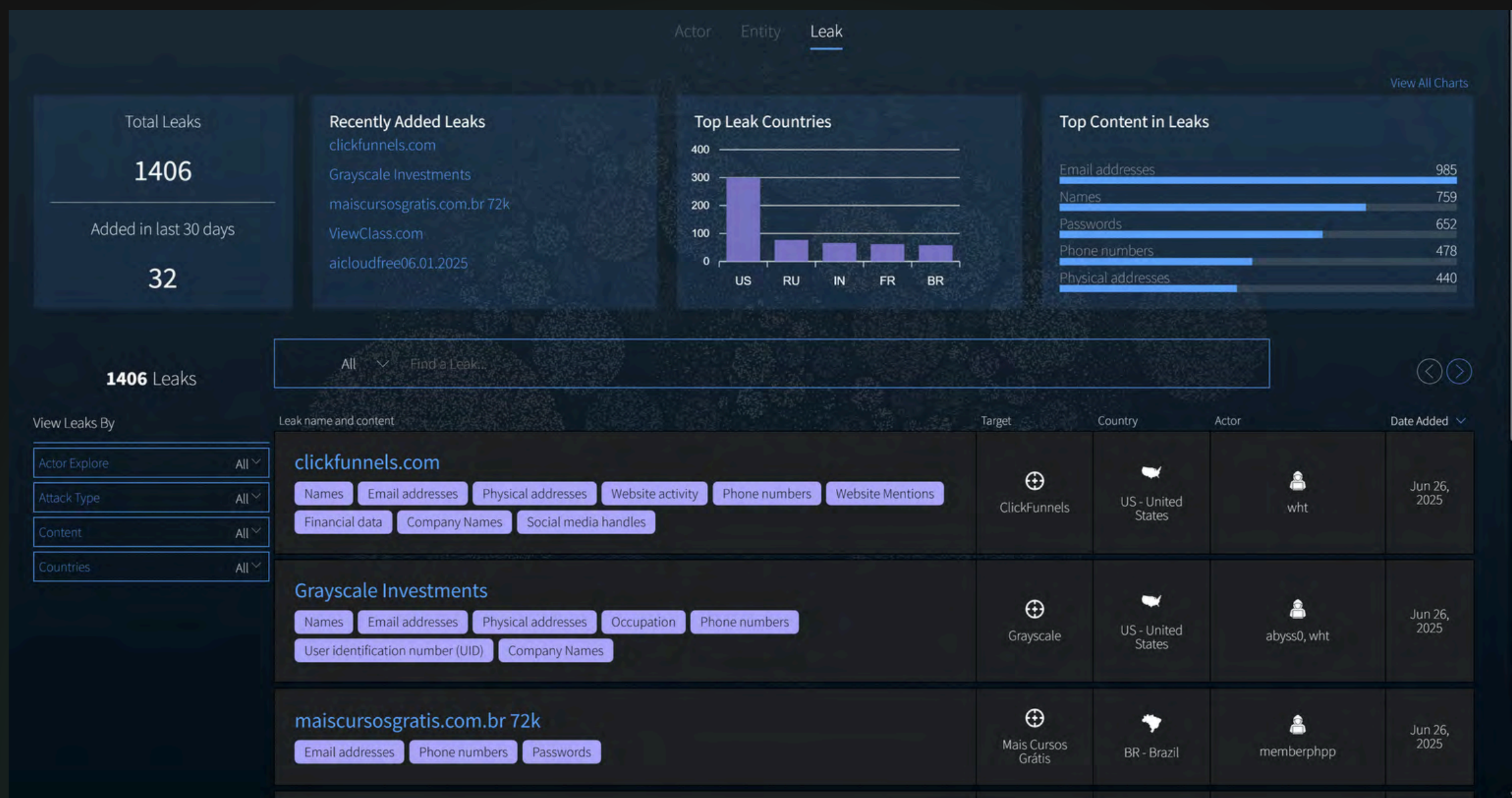
KEY CAPABILITIES



DEEP & DARK WEB MONITORING

Continuous surveillance of thousands of underground sources, including:

- Hidden forums, black markets, and onion sites
- Paste sites, breached databases, IRC channels
- BitTorrent, file-sharing platforms, social media leaks



KEY CAPABILITIES



CREDENTIAL LEAK DETECTION

Real-time alerts for exposed usernames, passwords, and access keys.

- Supports password reset and remediation workflows
- Covers both corporate and third-party credentials

The screenshot displays a web application interface for credential leak detection. On the left, there's a sidebar with a search bar and filters. The main area shows a list of leaked credentials, including usernames, passwords, and email addresses. A detailed view of one entry is shown on the right, displaying the full email body and metadata. The interface is dark-themed with blue accents.

Search Bar: Domain, Has Email, Group

URL: https://web.archive.org/web/20200703173848id_/http://demo.zeeroq.com/email/combos.vip-outlook.com.txt#:d=c=15

Crawled on: Oct 3 2020, 4:27 AM

Leaked Credentials:

- .com:kjwas9
- thejucker@outlook.com:dylan2003
- thelemondaddy@outlook.com:Lemon123
- thelonesurveys@outlook.com:Skywalker1
- theodor.lundqvist@outlook.com:Allapruttkorv-95.
- therese.fotso@outlook.com:therese12
- theshadowtheif@outlook.com:Qwqwqwqw3
- theshamwowguy@outlook.com:11221994
- thevo99@outlook.com:Soccer99
- thiagoanjos38@outlook.com:reymysterio
- thiakie@outlook.com:ora7p3
- thinker-greyskye@outlook.com:7mgwfp64o0
- thithavong.veronique@outlook.com:aaronnoam
- thogielecyarewilda@outlook.com:rrxfyodx25
- thomas7n@outlook.com:Earl8495
- thomasgfarran@outlook.com:f6f6a9a9
- thomassteffensen@outlook.com:Zubreb17
- thomassteffensen@outlook.com:tvltdp
- thomastt@outlook.com:opcondor
- thomcarroll@outlook.com:sb6ixq
- thueqyscumogoxgins@outlook.com:jqcisvts29
- thunderwood02@outlook.com:Underwood2
- thunderwood02@outlook.com:underwood2
- tiafe1234@outlook.com:awertv1234

Metadata: BODY, METADATA, LEAK INFO, EMAIL

Hackishness: 100 %

Footer: DARKINT E, Jul 6 2024

KEY CAPABILITIES

BRAND & DOMAIN PROTECTION

Safeguard your digital identity with:

- Detection of phishing sites, lookalike domains, and impersonations
- Monitoring of social media for fraudulent profiles and fake apps

✓	Name ✓	Search	Categories	Alerts ✓	Schedule ✓	Notify ✓	Auto ✓
☐	test 1	googl.com offset count	--	--	--	☒	☒
☐	test	LMNTRIX offset count	test	--	--	☒	☒
☐	Test	LMNTRIX offset count	--	--	--	☐	☐
☐	lmntrix_low	LMNTRIX offset count	low	--	--	☒	☒
☐	LMNTRIX_med	LMNTRIX offset count	med	--	--	☒	☒
☐	Lmntrix_high	LMNTRIX offset count	high	--	--	☒	☒
☐	LMNTRIX_critical	LMNTRIX offset count	critical	--	--	☒	☒

- Identify breaches involving suppliers, vendors, or affiliates
- Reduce risk from the extended supply chain

lmntrix_ceo

Date: 2021-02-16

Domains

Darknet Sites: 6

Transitory Sites: 20

Data Leaks: 6

Hackishness

Last 90 Days: 0%

Emails

Darknet Sites: 0

Transitory Sites: 0

Data Leaks: 0

In Data Leaks: 0%

Details

Domains

Email Domains

Domains

Darknet Results ▶

Transitory Results ▶

Data Leak Results ▶

Email Domains

Darknet Results ▶

Transitory Results ▶

KEY CAPABILITIES



THREAT ACTOR MONITORING

Discover adversarial interest before attacks happen:

- Human-led infiltration of underground communities
- Monitoring of attack chatter, targeting campaigns, and HVT mentions

319 Actors

Find an actor by Name, Alias, CVE, or Industry

Compare

View Actors By

- Country Targeted: All
- CVEs: All
- Industries: All
- Origin: All
- Sophistication: All
- Specialization: All
- Sort By: Updated
- Sort Direction: Descending

Actor	Sophistication	Origin	Years Active	First Seen	Status	Aliases	Specialization
MRxCODER	Intermediate	Unknown	7	Jul 12, 2017	Active	Caffeinestore, Caffeine, MRxCODER	Cyber Crime
ims0rry	Expert	RU - Russia	8	May 27, 2017	Active	_KapJIcoH, ims0rry, hachlandia, imsorry, strelok.127, alino4ka, Ацамаз Гацоев, hypega, Atsamaz Gatsoev, 1M50RRY, 1ms0rry	Exploit Seller
AtillaSoftware	Advanced	Unknown	6	Mar 28, 2019	Active	AtillaSoftware	Info Stealer
CrazyHunter Team	Unknown	Unknown	<1	Jun 28, 2025	Active		Ransomware
KillSec	Intermediate	Unknown	1	Oct 22, 2023	Active	KillSec Team, Kill Security, KillSec	
sett9	Advanced	RU - Russia	7	Feb 5, 2018	Active	sett9ine, sett9	
Play	Expert	Unknown	3	Jun 22, 2022	Active	Play ransomware, PlayCrypt, Play	
TarTarX	Intermediate	Unknown	3	Apr 29, 2022	Active	TarTarX	

09

KEY CAPABILITIES



ACTIONABLE INTELLIGENCE ALERTS

All alerts undergo human review and are:

- Delivered through the LMNTRIX XDR
- Enriched with threat context and metadata
- Prioritized by criticality and relevance

The screenshot displays the LMNTRIX XDR interface. The top navigation bar includes tabs for HUD, KILLBOX, EXPLORE, INTEL, INCIDENTS (active), REPORTS, CONFIG, and a search icon. The left sidebar shows the user profile (Carlo Minassian), a date/time stamp (14:32:19 SAT | 28 JUNE), and a list of menu items: INCIDENTS, SITUATION REPORT, CASES, PERFORMANCE, and RESILIENCE. The main content area is titled 'Incident Findings' and contains a 'REPLY' button and an 'ADD USER' button. Below these is an email header from 'R+F Tech Security' with the subject 'Cc: titus@lmntrix.com, hamlet@lmntrix.com'. The body of the email starts with 'Hi Team,' followed by a paragraph stating that the LMNTRIX Incident Response team has identified 'Rodan and Fields' user credentials being offered for sale in the Credential theft forum of the deep & dark web. This is followed by a section titled 'Forum/Dark Web Activity' which states that LMNTRIX Recon service has detected legitimate usernames & passwords of 'Rodan and Fields' user being offered for sale in the dark market. The email then provides the following details: URL: https://mypeoplenet.com, Email: cmccormick@mypeoplenet.com, and Password: 218122Dc\$. The impact section states that the stolen credentials can be used to exploit the organization's infrastructure by conducting attacks like spear phishing, phishing, privilege escalations, etc. The recommendation section advises changing the password and other authorization methods of the compromised credentials as soon as possible, and implementing multi-factor authentication to safeguard the credential hijacking. The email concludes with a note to reach out if there are any other questions and a sign-off 'Thanks & Regards' from the LMNTRIX Cyber Defense Centre. On the right side of the interface, there is a 'RECOMMENDATION' section stating 'There are no recommendations', an 'AVG TIME' section showing 'MTTD 0h 0min' and 'MTTR 241h 37min', and a 'FIELDS INCIDENTCASE' section with dropdown menus for 'Threat Lifecycle' (set to Reconnaissance), 'Investigative Actions for' (set to User), 'Remediation Action' (set to ...), 'Type' (set to Security Incident), 'Status' (set to Closed), and 'Detection Method' (set to LMNTRIX RECON).



10

READY TO SEE LMNTRIX RECON IN ACTION?



Your data is already out there—LMNTRIX Recon makes sure you're the first to know. While others wait for breaches to surface, Recon hunts across the deep and dark web to expose threats before they strike. If attackers are talking about you, we're already listening.

VISIT
LMNTRIX.COM



LMNTRIX
BE THE HUNTER | NOT THE PREY