X10 TECHNOLOGIES

CELEBRATING 20 YEARS AND BEYOND

Cyber Alberta Community of Interest

Dark Web and AI: a New Era of Cyber Threats

The Dark Web and AI: A New Era of Cyber Threats with Hank Fordham

As organizations embrace modern cybersecurity architectures, cyber threats present new challenges to securing corporate networks.

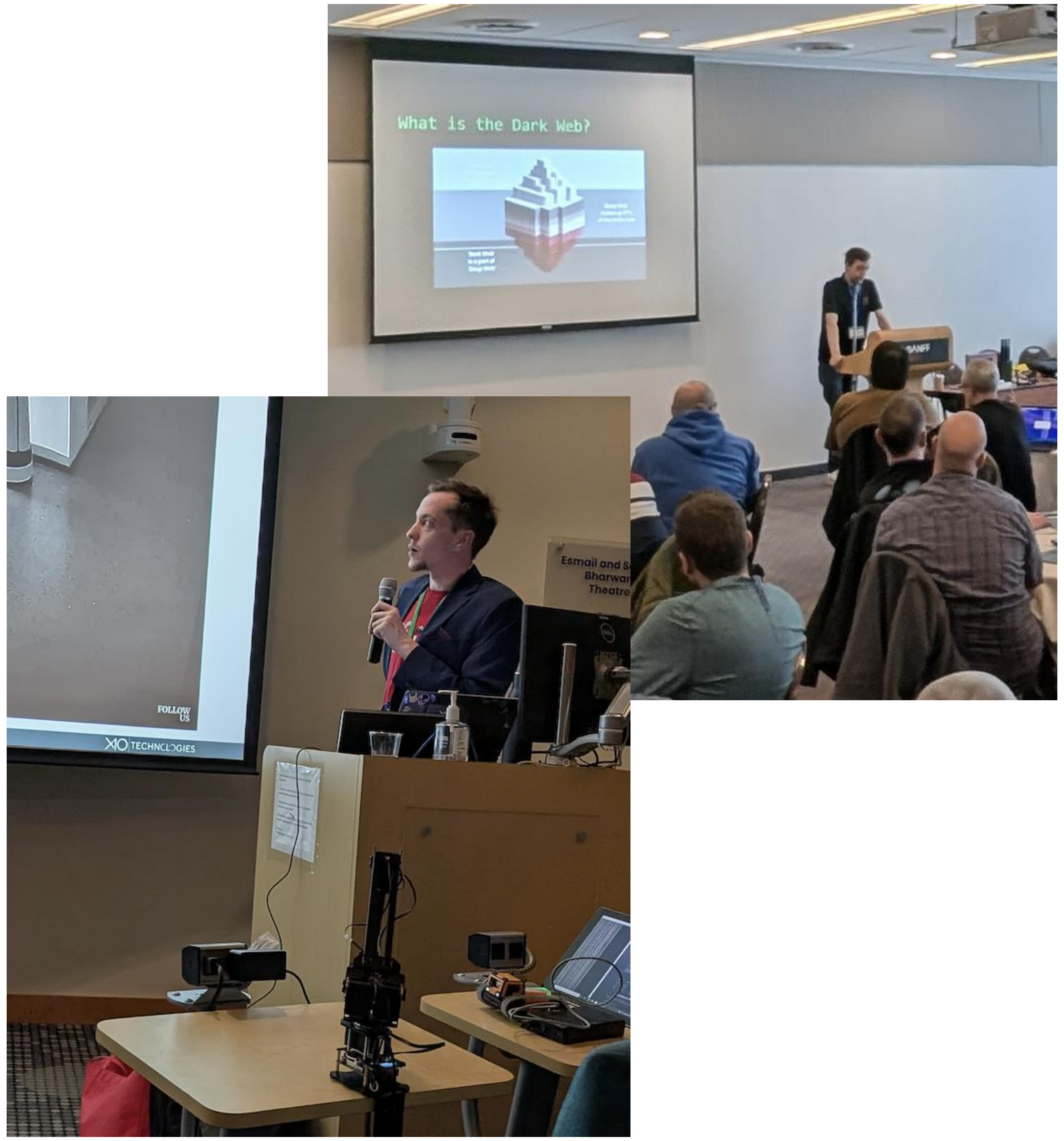
This session explores the intersection of the dark web, AI, and cyber threat intelligence, revealing how cybercriminals exploit leaked credentials and sensitive data to bypass traditional defenses as well as how we can defend against them.

CYBER ALBERTA

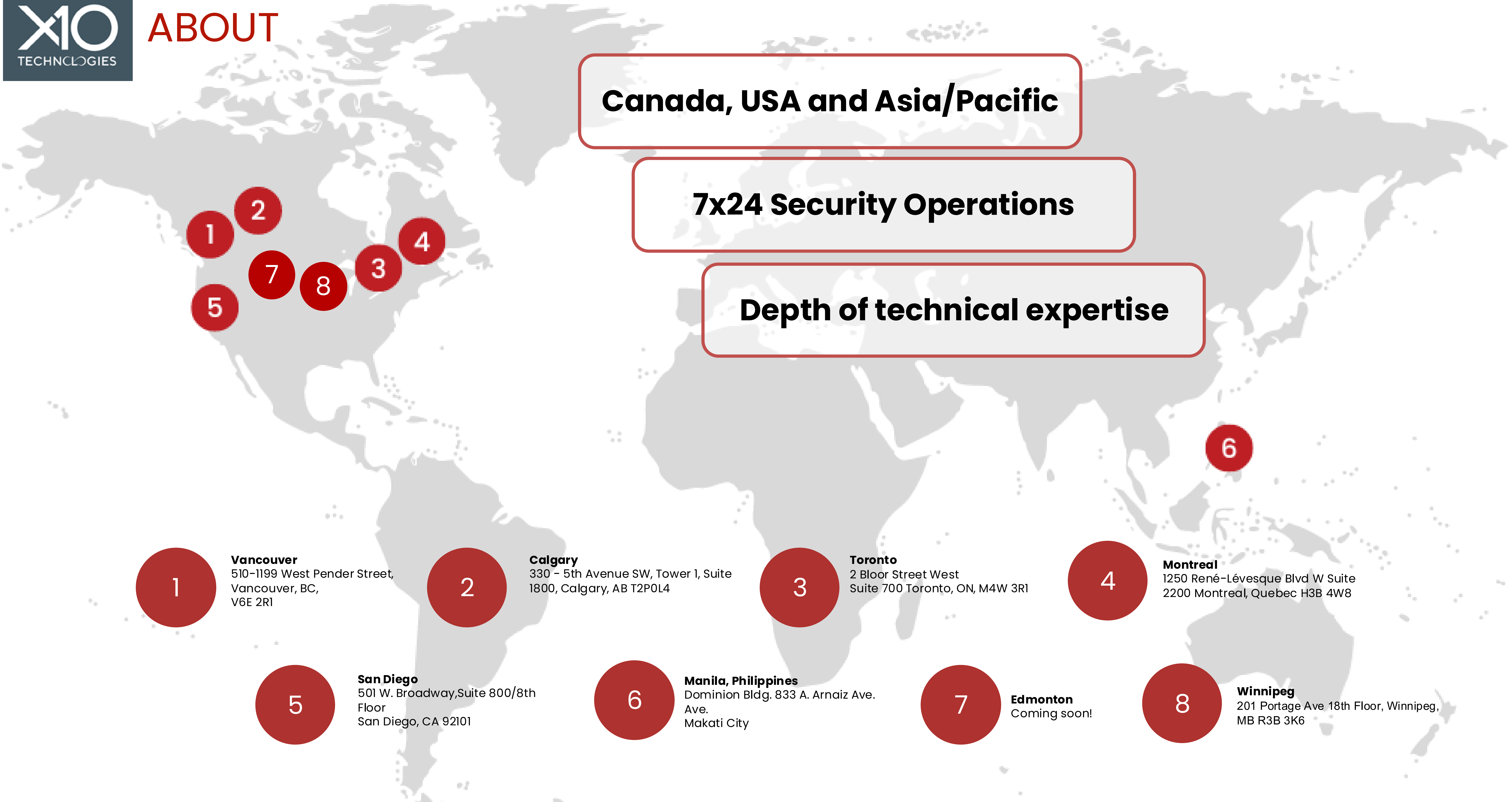
Hank Fordham & Adam McMath

Hank the Hacker:
mentor, educator, and
technology innovator

Adam the Antagonist:
researcher, organizer, and
crisis communicator



ABOUT



Canada, USA and Asia/Pacific

7x24 Security Operations

Depth of technical expertise

1 **Vancouver**
510-1199 West Pender Street,
Vancouver, BC,
V6E 2R1

2 **Calgary**
330 - 5th Avenue SW, Tower 1, Suite
1800, Calgary, AB T2P0L4

3 **Toronto**
2 Bloor Street West
Suite 700 Toronto, ON, M4W 3R1

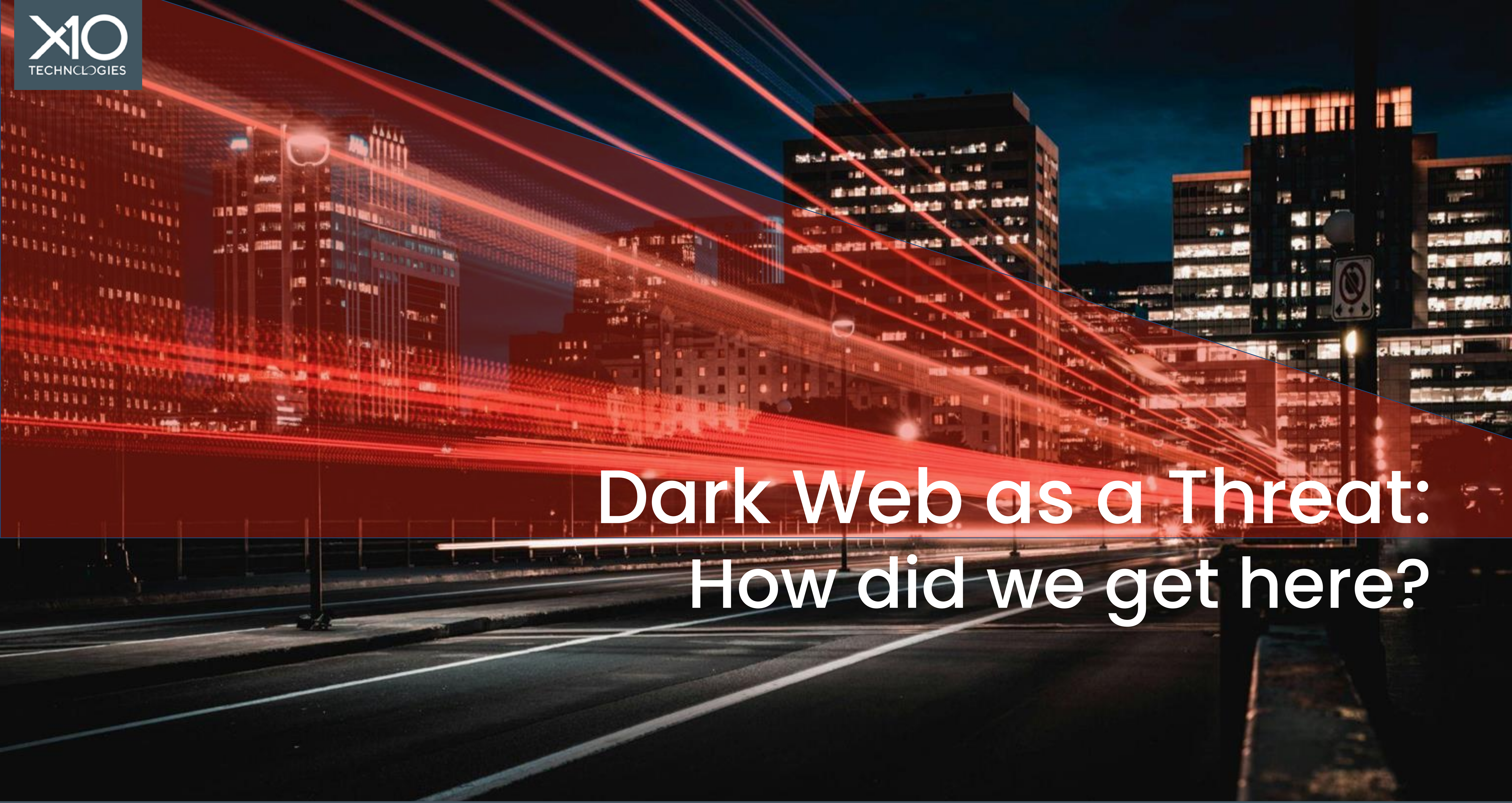
4 **Montreal**
1250 René-Lévesque Blvd W Suite
2200 Montreal, Quebec H3B 4W8

5 **San Diego**
501 W. Broadway,Suite 800/8th
Floor
San Diego, CA 92101

6 **Manila, Philippines**
Dominion Bldg. 833 A. Arnaiz Ave.
Ave.
Makati City

7 **Edmonton**
Coming soon!

8 **Winnipeg**
201 Portage Ave 18th Floor, Winnipeg,
MB R3B 3K6



Dark Web as a Threat: How did we get here?

Technology Evolution

Innovation

Web 1.0, Circa 1999

- Internet Connectivity
- Firewalls
- Trust Zones
- AV on Endpoints
- Distributed Computing
- 10bT Ethernet

Transformation

Web 2.0, Circa 2009

- Mobility
- Rich Content
- Compliance
- Logs / SIEM
- Frameworks
- Cloud
- Data Science

Disruption

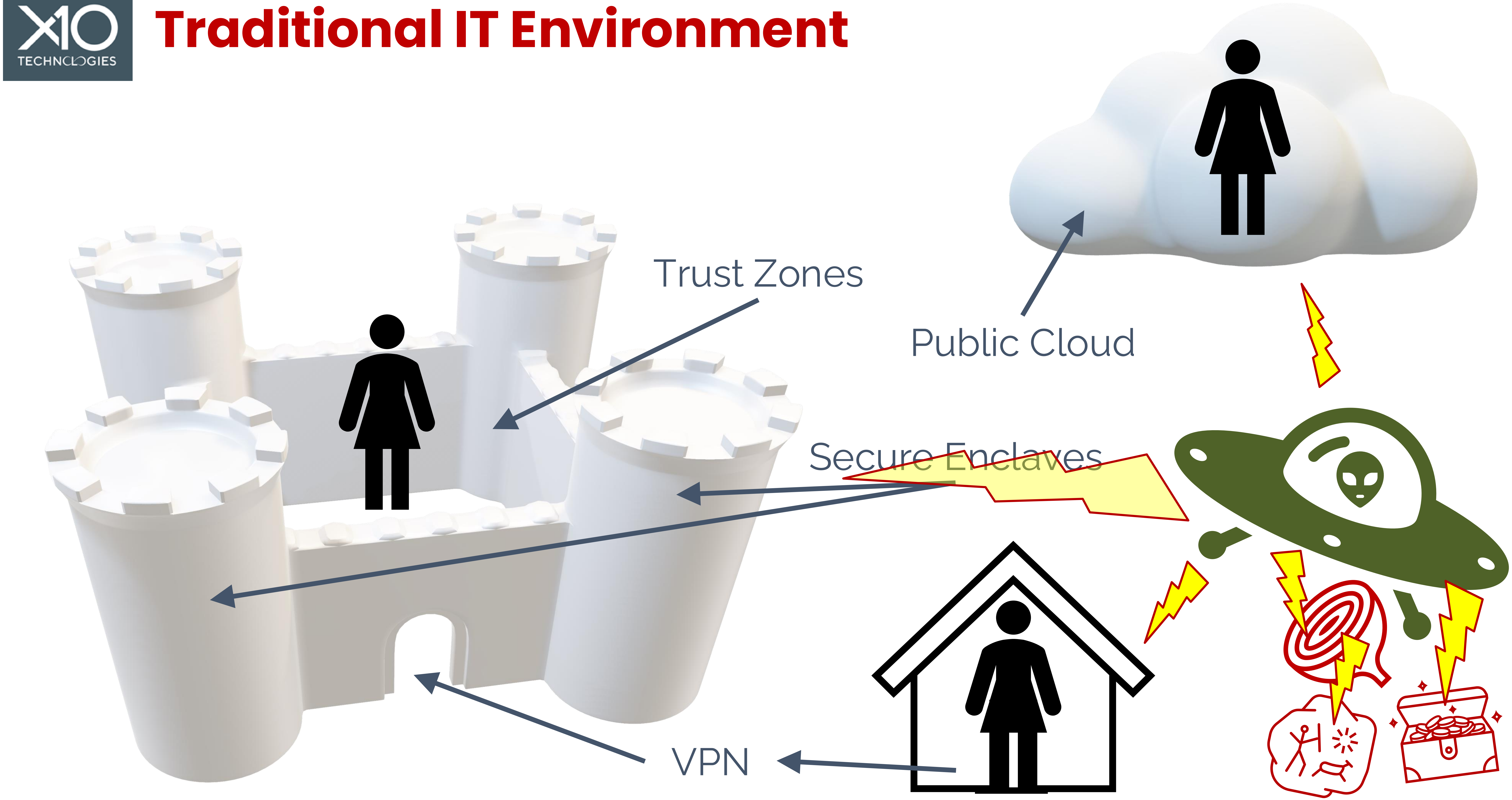
Modern Workforce, Circa 2019

- “Identity is the new Perimeter”
- Remote Workers
- Privacy Legislation
- Advanced Persistent Threats
- Data and Traffic Analytics

2025

Inherited Complexity, Technical Debt, Competing Priorities

Traditional IT Environment



Trust Zones

Public Cloud

Secure Enclaves

VPN

Behind it all... the Dark Web

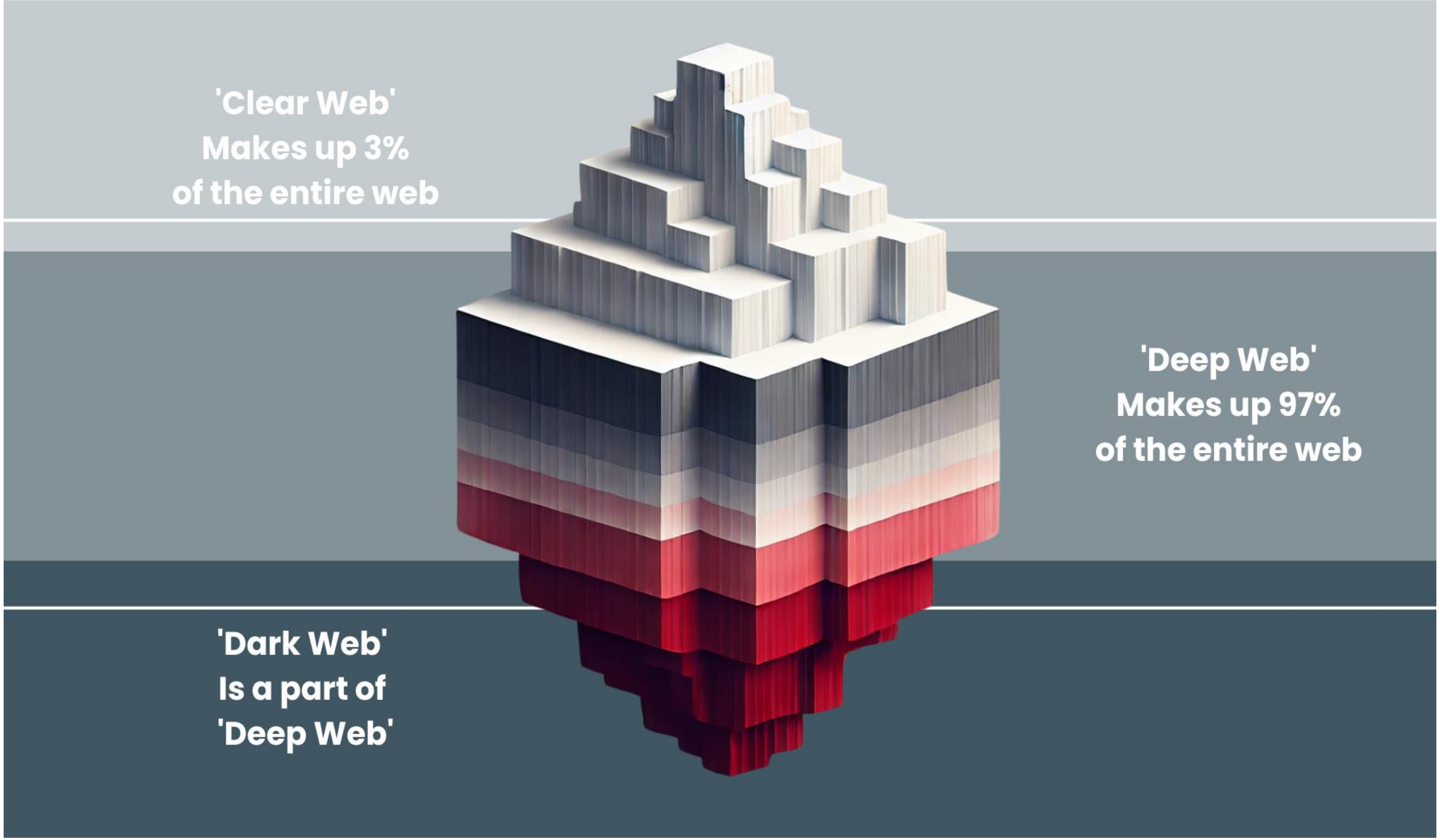
Invented by researchers at United States Naval Research Laboratory (NRL) in the 90's

Enables anonymity through encrypted Communication

Used by whistleblowers, journalists, and people who could be oppressed for the information they want to share

Cybercriminals thrive here

Behind it all... the Dark Web

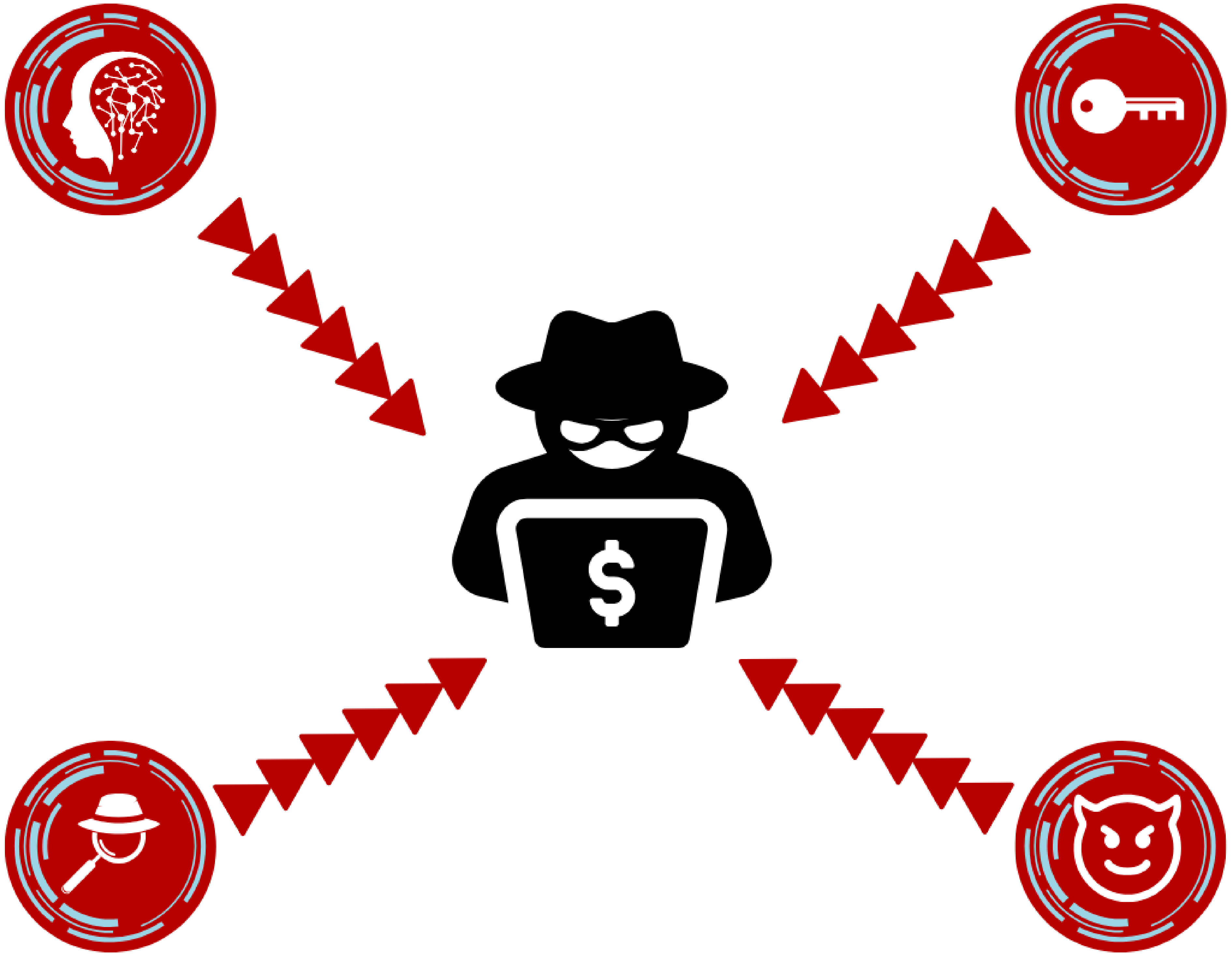


'Clear Web'
Makes up 3%
of the entire web

'Deep Web'
Makes up 97%
of the entire web

'Dark Web'
Is a part of
'Deep Web'

How the Dark Web Enables Hackers



LLM Jacking

Microsoft sues hacking group exploiting azure AI for harmful content creation. Hackers were gaining access to LLM's to use them maliciously without the user's knowledge, potentially also racking up costs.

API and Credential Theft

Cybercriminals stealing API keys and credentials to gain access to Ai tools like ChatGPT and Azure Ai for malware and phishing.

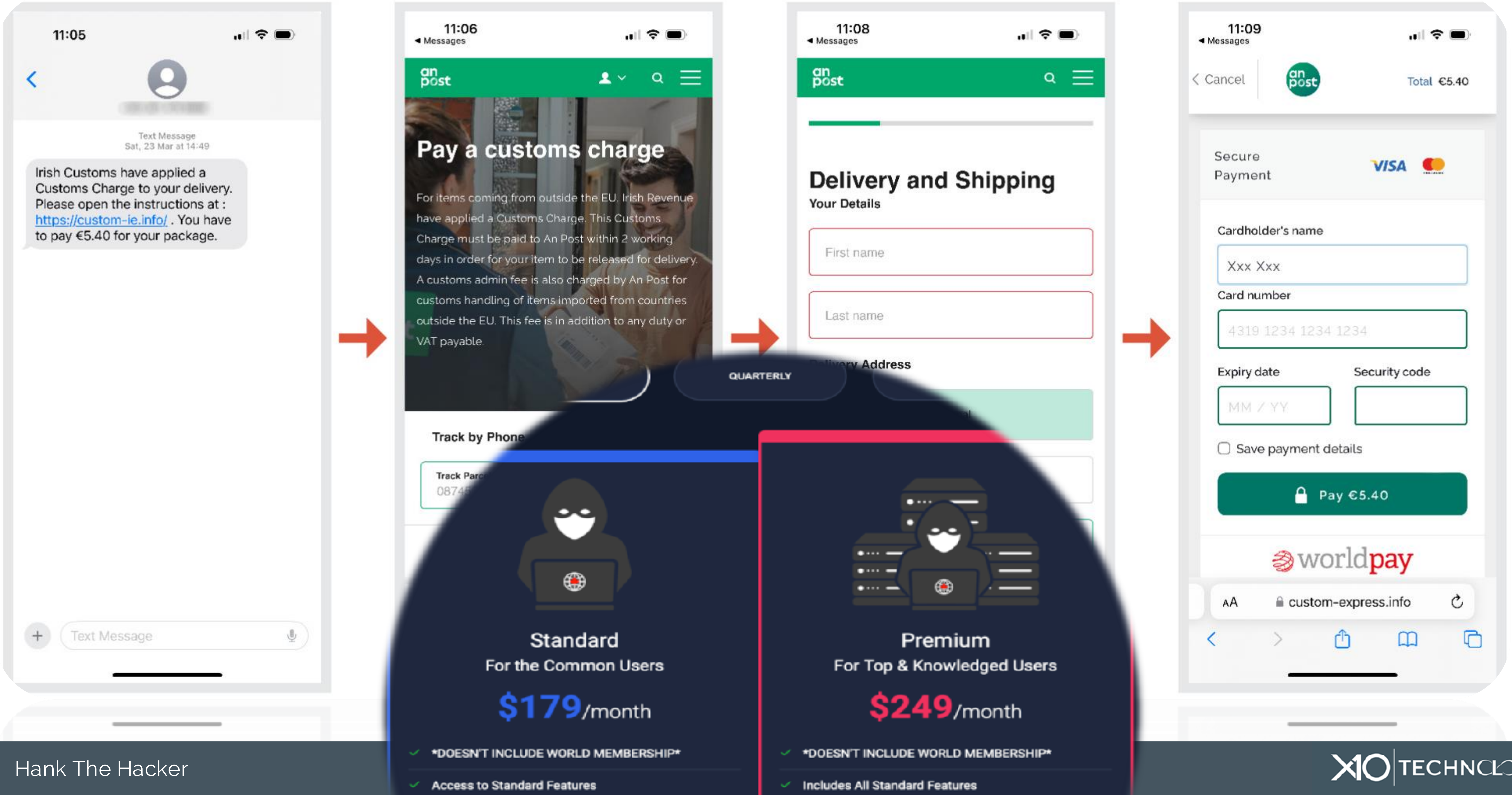
Data Collection and Analysis

Cybercriminals leveraging Ai and the dark web for more effective data scraping and intelligence gathering, making target discovery and compromise less difficult.

Malicious Language Models

Cybercriminals developing complex Large Language Models (LLMs) for malicious purposes like developing malware or phishing campaigns and generating harmful content.

How the Dark Web Enables Phishing



[redacted]

Text Message
Sat, 23 Mar at 14:49

Irish Customs have applied a Customs Charge to your delivery. Please open the instructions at : https://custom-ie.info/ . You have to pay €5.40 for your package.

Pay a customs charge

For items coming from outside the EU, Irish Revenue have applied a Customs Charge. This Customs Charge must be paid to An Post within 2 working days in order for your item to be released for delivery. A customs admin fee is also charged by An Post for customs handling of items imported from countries outside the EU. This fee is in addition to any duty or VAT payable.

Delivery and Shipping

Your Details

First name

Last name

Delivery Address

Total €5.40

Secure Payment

Cardholder's name: Xxx Xxx

Card number: 4319 1234 1234 1234

Expiry date: MM / YY

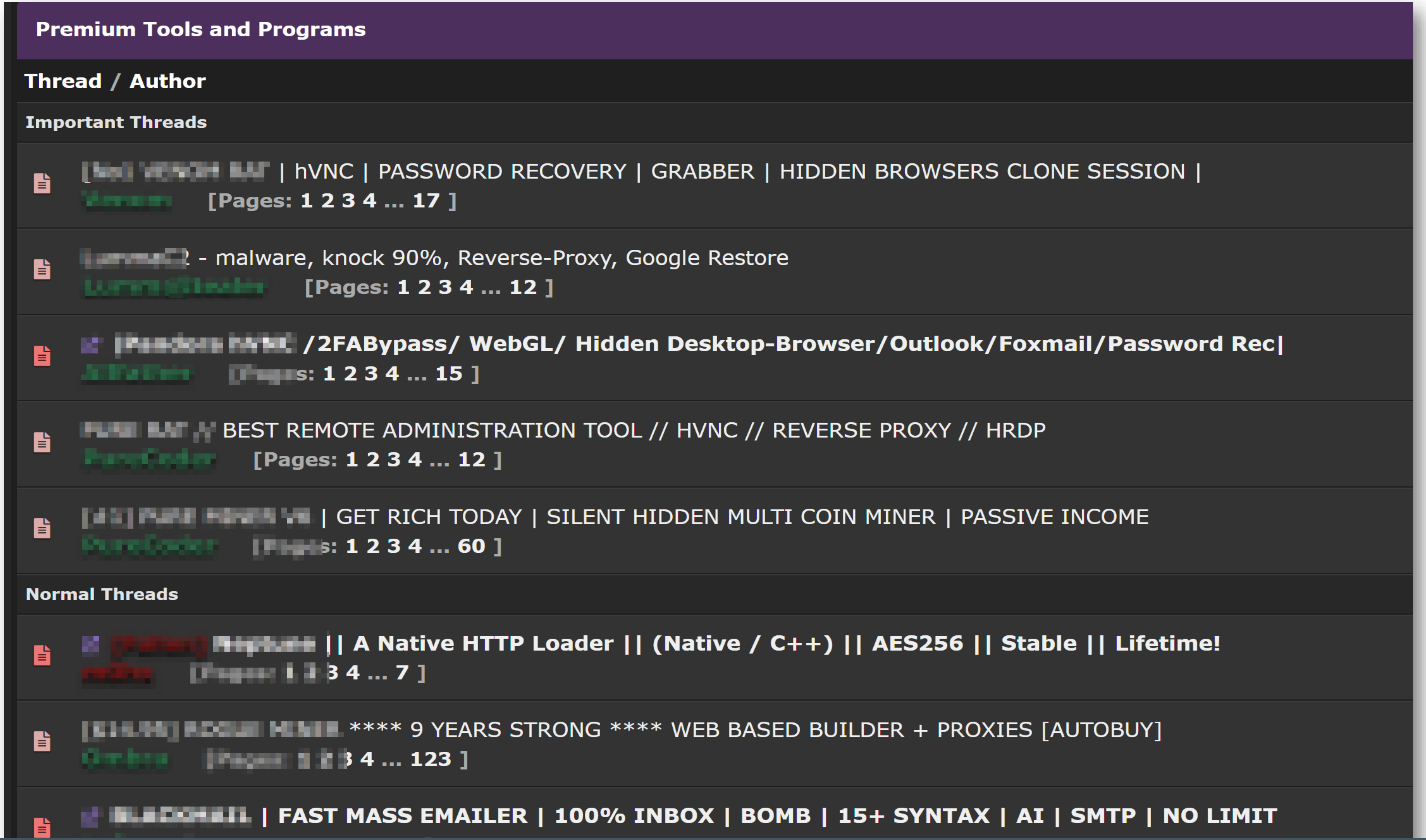
Security code:

□ Save payment details

Standard
For the Common Users
$179/month
✓ *DOESN'T INCLUDE WORLD MEMBERSHIP*
✓ Access to Standard Features

Premium
For Top & Knowledged Users
$249/month
✓ *DOESN'T INCLUDE WORLD MEMBERSHIP*
✓ Includes All Standard Features

Dark Web Commoditized Malware



Premium Tools and Programs

Thread / Author

Important Threads

[redacted] | hVNC | PASSWORD RECOVERY | GRABBER | HIDDEN BROWSERS CLONE SESSION |
[redacted] [Pages: 1 2 3 4 ... 17]

[redacted] - malware, knock 90%, Reverse-Proxy, Google Restore
[redacted] [Pages: 1 2 3 4 ... 12]

[redacted] /2FABypass/ WebGL/ Hidden Desktop-Browser/Outlook/Foxmail/Password Rec|
[redacted] [redacted]s: 1 2 3 4 ... 15]

[redacted] BEST REMOTE ADMINISTRATION TOOL // HVNC // REVERSE PROXY // HRDP
[redacted] [Pages: 1 2 3 4 ... 12]

[redacted] | GET RICH TODAY | SILENT HIDDEN MULTI COIN MINER | PASSIVE INCOME
[redacted] [redacted]s: 1 2 3 4 ... 60]

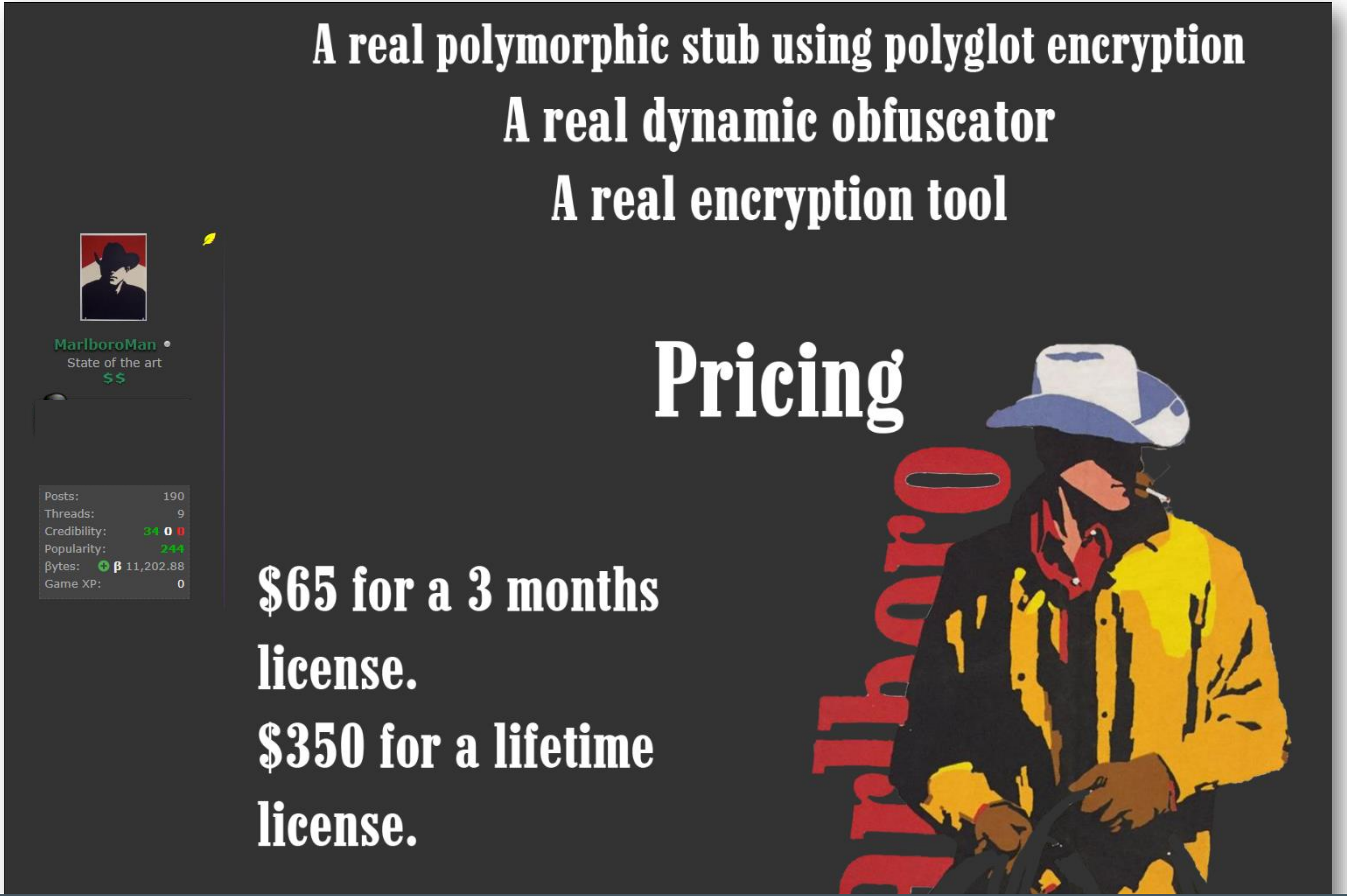
Normal Threads

[redacted] || A Native HTTP Loader || (Native / C++) || AES256 || Stable || Lifetime!
[redacted] [redacted]3 4 ... 7]

[redacted] **** 9 YEARS STRONG **** WEB BASED BUILDER + PROXIES [AUTOBUY]
[redacted] [redacted]3 4 ... 123]

[redacted] | FAST MASS EMAILER | 100% INBOX | BOMB | 15+ SYNTAX | AI | SMTP | NO LIMIT

Dark Web Commoditized Obfuscation



MarlboroMan
State of the art
$$

Posts:	190
Threads:	9
Credibility:	34 0 0
Popularity:	244
βytes:	β 11,202.88
Game XP:	0

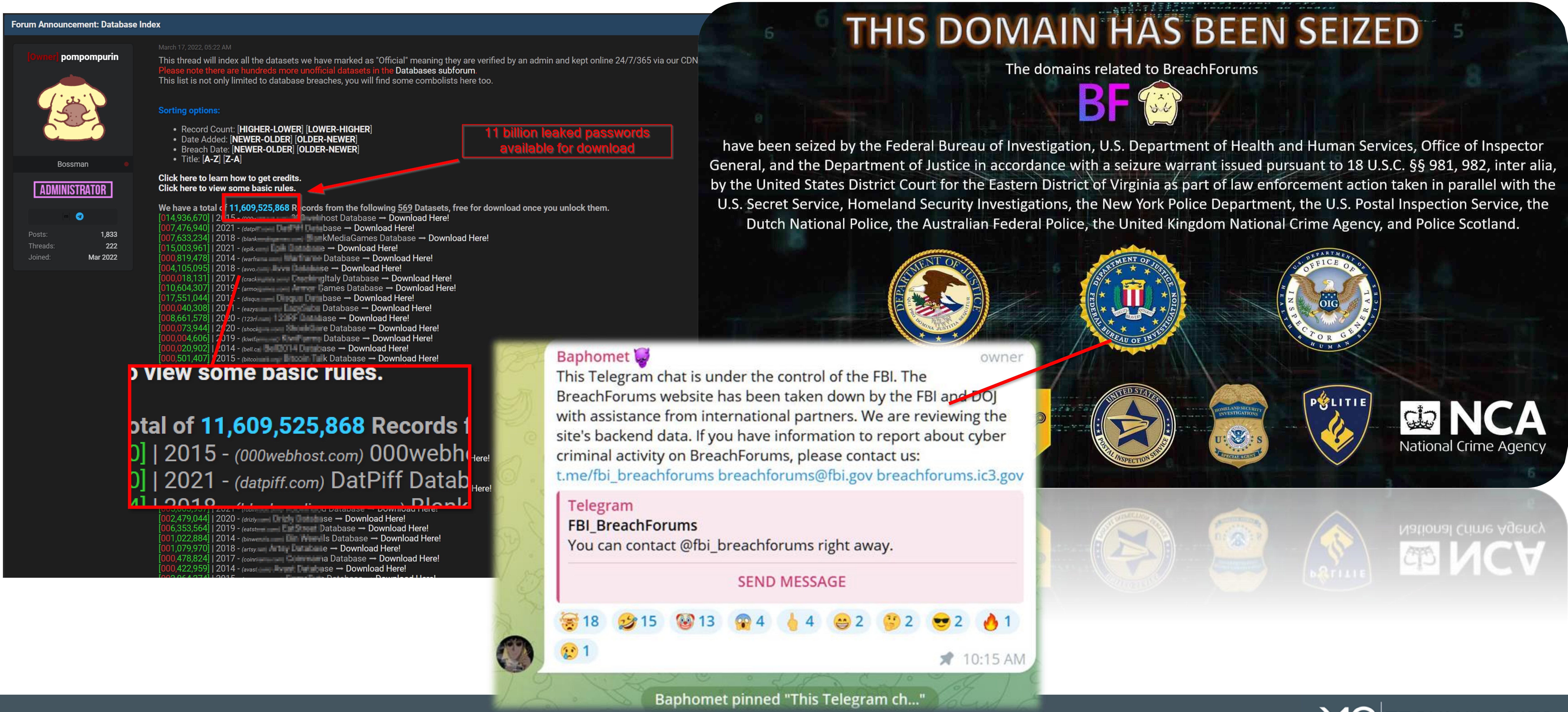
A real polymorphic stub using polyglot encryption
A real dynamic obfuscator
A real encryption tool

Pricing

$65 for a 3 months license.

$350 for a lifetime license.

Dark Web Credential Stuffing



Forum Announcement: Database Index

[Owner] pompompurin

Bossman

ADMINISTRATOR

Posts: 1,833
Threads: 222
Joined: Mar 2022

March 17, 2022, 05:22 AM

This thread will index all the datasets we have marked as "Official" meaning they are verified by an admin and kept online 24/7/365 via our CDN
Please note there are hundreds more unofficial datasets in the Databases subforum.
This list is not only limited to database breaches, you will find some combolists here too.

Sorting options:

- Record Count: [HIGHER-LOWER] [LOWER-HIGHER]
- Date Added: [NEWER-OLDER] [OLDER-NEWER]
- Breach Date: [NEWER-OLDER] [OLDER-NEWER]
- Title: [A-Z] [Z-A]

Click here to learn how to get credits.
Click here to view some basic rules.

We have a total of 11,609,525,868 Records from the following 569 Datasets, free for download once you unlock them.
[014,936,670] | 2015 - (000 [redacted] host Database → Download Here!
[007,476,940] | 2021 - (datpi [redacted] base → Download Here!
[007,633,234] | 2018 - (blank [redacted] kMediaGames Database → Download Here!
[015,003,961] | 2021 - (epik. [redacted] e → Download Here!
[000,819,478] | 2014 - (warfr [redacted] Database → Download Here!
[004,105,095] | 2018 - (avvo. [redacted] se → Download Here!
[000,018,131] | 2017 - (crack [redacted] Italy Database → Download Here!
[010,604,307] | 2019 - (armo [redacted] Games Database → Download Here!
[017,551,044] | 201[illegible] - (disqu [redacted] base → Download Here!
[000,040,308] | 20[illegible]1 - (eazys [redacted] Database → Download Here!
[008,661,578] | 2020 - (123rf [redacted] ase → Download Here!
[000,073,944] | 2020 - (shock [redacted] e Database → Download Here!
[000,004,606] | 2019 - (kiwifa [redacted] Database → Download Here!
[000,020,902] | 2014 - (bell.ca [redacted] ase → Download Here!
[000,501,407] | 2015 - (bitco [redacted] k Database → Download Here!
[002,479,044] | 2020 - (drizly [redacted] se → Download Here!
[006,353,564] | 2019 - (eatst [redacted] Database → Download Here!
[001,022,884] | 2014 - (binwe [redacted] ls Database → Download Here!
[001,079,970] | 2018 - (artsy [redacted] e → Download Here!
[000,478,824] | 2017 - (coinr [redacted] a Database → Download Here!
[000,422,959] | 2014 - (avast [redacted] se → Download Here!

o view some basic rules.

otal of 11,609,525,868 Records f
0] | 2015 - (000webhost.com) 000webh
0] | 2021 - (datpiff.com) DatPiff Datab

11 billion leaked passwords available for download

THIS DOMAIN HAS BEEN SEIZED

The domains related to BreachForums

BF

have been seized by the Federal Bureau of Investigation, U.S. Department of Health and Human Services, Office of Inspector General, and the Department of Justice in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the Eastern District of Virginia as part of law enforcement action taken in parallel with the U.S. Secret Service, Homeland Security Investigations, the New York Police Department, the U.S. Postal Inspection Service, the Dutch National Police, the Australian Federal Police, the United Kingdom National Crime Agency, and Police Scotland.

NCA National Crime Agency

Baphomet owner

This Telegram chat is under the control of the FBI. The BreachForums website has been taken down by the FBI and DOJ with assistance from international partners. We are reviewing the site's backend data. If you have information to report about cyber criminal activity on BreachForums, please contact us:
t.me/fbi_breachforums breachforums@fbi.gov breachforums.ic3.gov

Telegram
FBI_BreachForums
You can contact @fbi_breachforums right away.

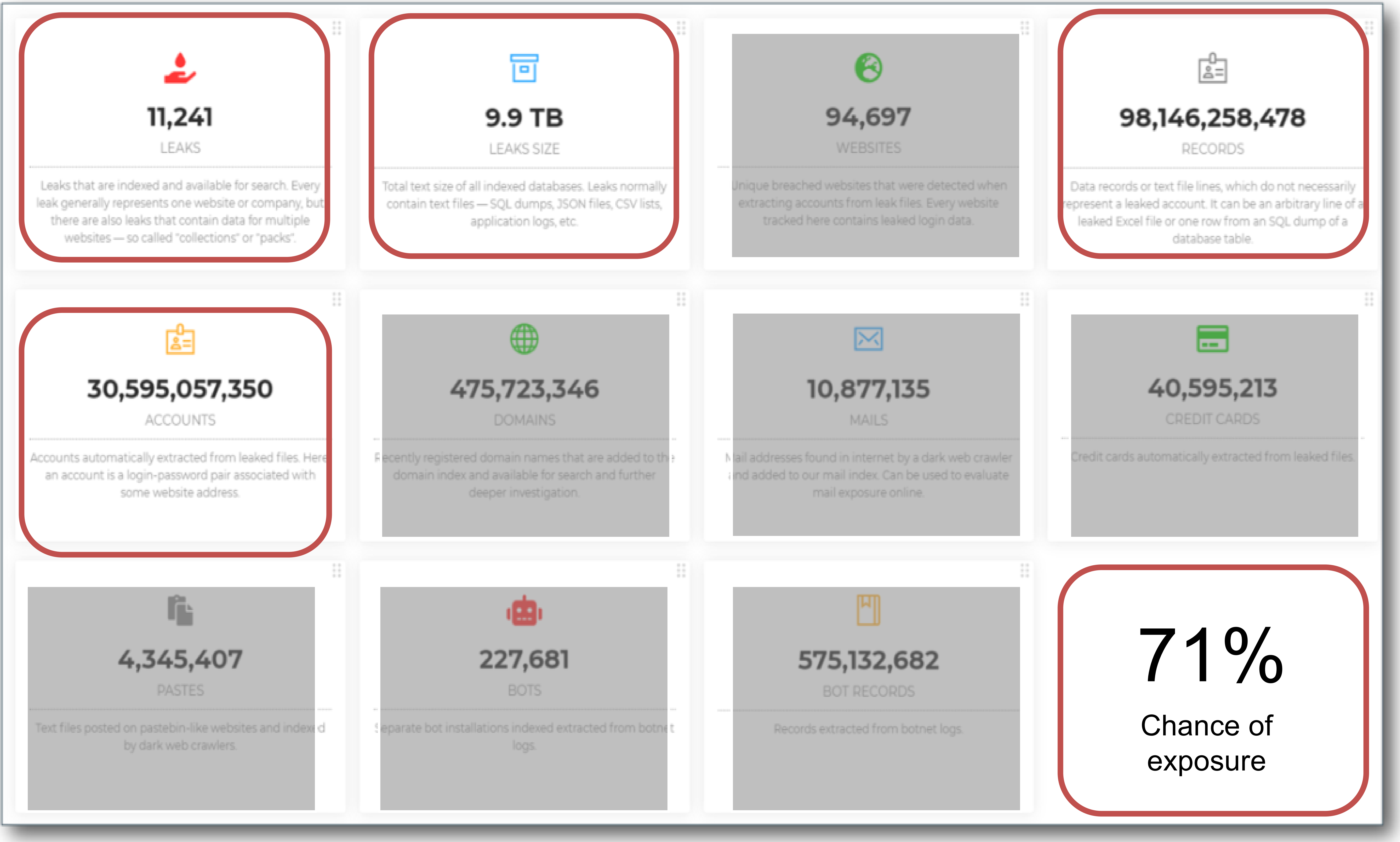
SEND MESSAGE

18 15 13 4 4 2 2 2 1 1

10:15 AM

Baphomet pinned "This Telegram ch..."

January 2025 Dark Web Statistics



11,241

LEAKS

Leaks that are indexed and available for search. Every leak generally represents one website or company, but there are also leaks that contain data for multiple websites — so called "collections" or "packs".

9.9 TB

LEAKS SIZE

Total text size of all indexed databases. Leaks normally contain text files — SQL dumps, JSON files, CSV lists, application logs, etc.

94,697

WEBSITES

Unique breached websites that were detected when extracting accounts from leak files. Every website tracked here contains leaked login data.

98,146,258,478

RECORDS

Data records or text file lines, which do not necessarily represent a leaked account. It can be an arbitrary line of a leaked Excel file or one row from an SQL dump of a database table.

30,595,057,350

ACCOUNTS

Accounts automatically extracted from leaked files. Here an account is a login-password pair associated with some website address.

475,723,346

DOMAINS

Recently registered domain names that are added to the domain index and available for search and further deeper investigation.

10,877,135

MAILS

Mail addresses found in internet by a dark web crawler and added to our mail index. Can be used to evaluate mail exposure online.

40,595,213

CREDIT CARDS

Credit cards automatically extracted from leaked files.

4,345,407

PASTES

Text files posted on pastebin-like websites and indexed by dark web crawlers.

227,681

BOTS

Separate bot installations indexed extracted from botnet logs.

575,132,682

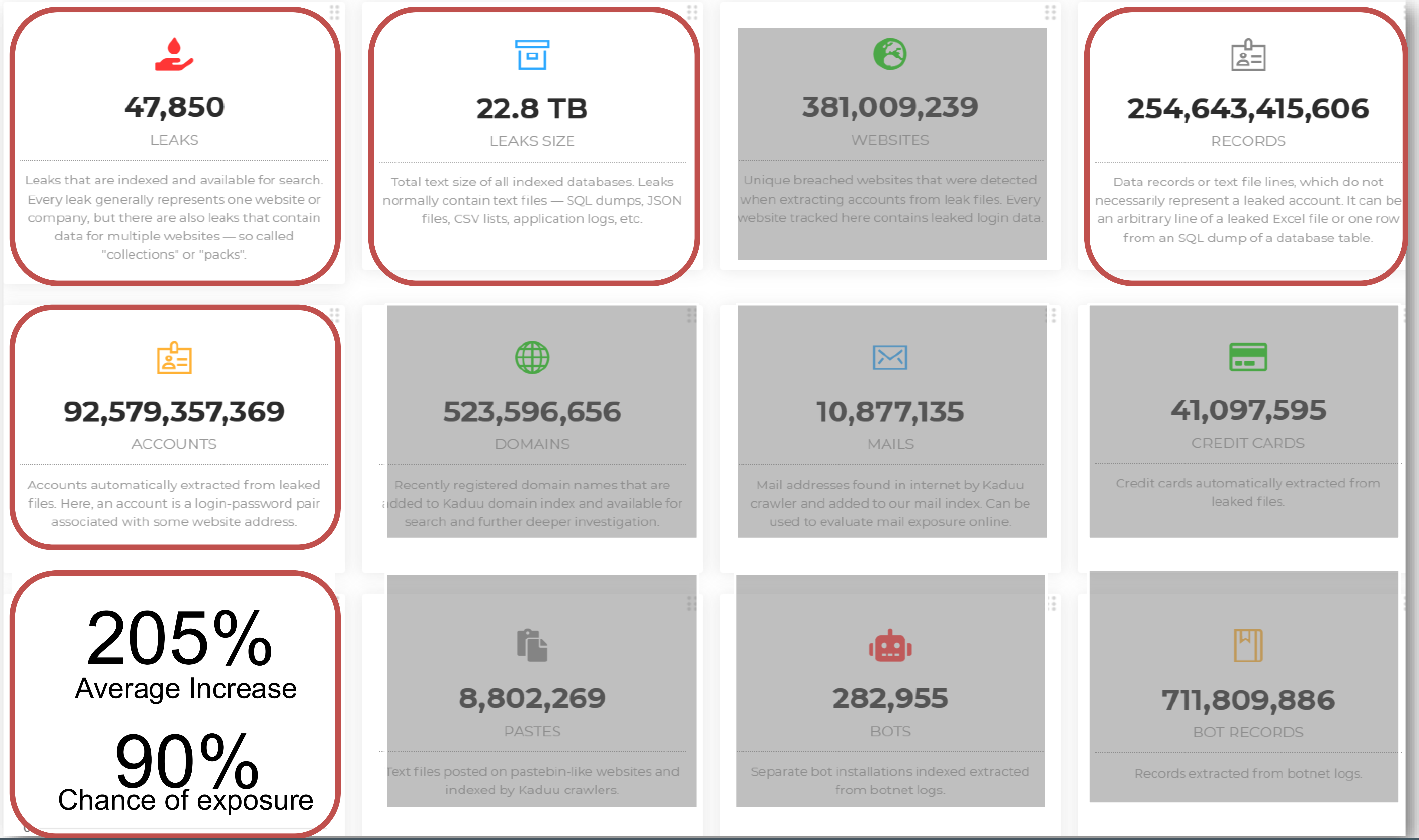
BOT RECORDS

Records extracted from botnet logs.

71%

Chance of exposure

December 2025 Dark Web Statistics



47,850

LEAKS

Leaks that are indexed and available for search. Every leak generally represents one website or company, but there are also leaks that contain data for multiple websites — so called "collections" or "packs".

22.8 TB

LEAKS SIZE

Total text size of all indexed databases. Leaks normally contain text files — SQL dumps, JSON files, CSV lists, application logs, etc.

381,009,239

WEBSITES

Unique breached websites that were detected when extracting accounts from leak files. Every website tracked here contains leaked login data.

254,643,415,606

RECORDS

Data records or text file lines, which do not necessarily represent a leaked account. It can be an arbitrary line of a leaked Excel file or one row from an SQL dump of a database table.

92,579,357,369

ACCOUNTS

Accounts automatically extracted from leaked files. Here, an account is a login-password pair associated with some website address.

523,596,656

DOMAINS

Recently registered domain names that are added to Kaduu domain index and available for search and further deeper investigation.

10,877,135

MAILS

Mail addresses found in internet by Kaduu crawler and added to our mail index. Can be used to evaluate mail exposure online.

41,097,595

CREDIT CARDS

Credit cards automatically extracted from leaked files.

205%

Average Increase

90%

Chance of exposure

8,802,269

PASTES

Text files posted on pastebin-like websites and indexed by Kaduu crawlers.

282,955

BOTS

Separate bot installations indexed extracted from botnet logs.

711,809,886

BOT RECORDS

Records extracted from botnet logs.

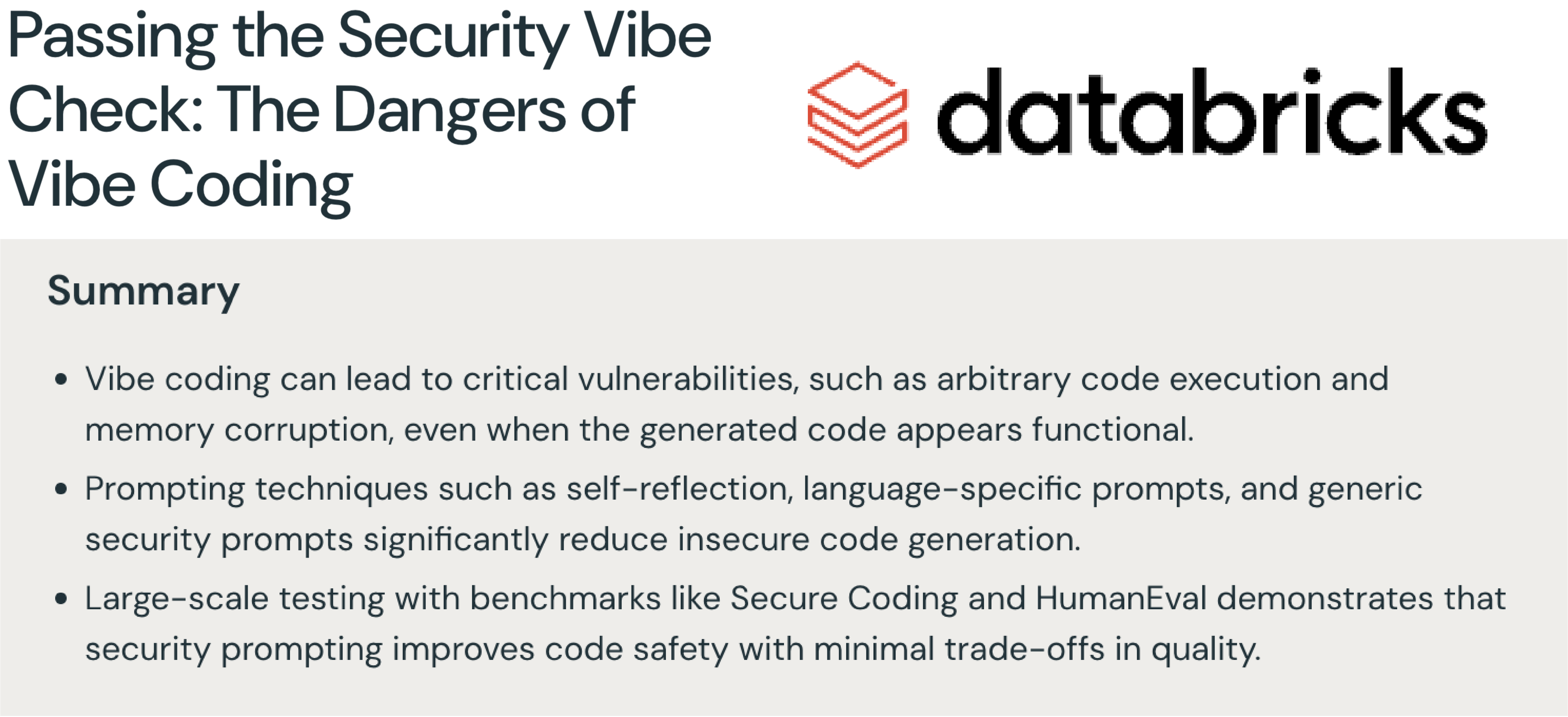
AI Trends: Enhanced Phishing

AI lowers the barrier for novice cyber criminals, hackers-for-hire and hacktivists to carry out effective access and information gathering operations. This **enhanced access will likely contribute to the global ransomware threat** over the next two years. Moving towards 2025 and beyond, commoditisation of AI-enabled capability in criminal and commercial markets will almost certainly make **improved capability available to cyber crime and state actors.**

National Cyber Security Centre

https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

AI Trends: Vibe Coding



Passing the Security Vibe Check: The Dangers of Vibe Coding

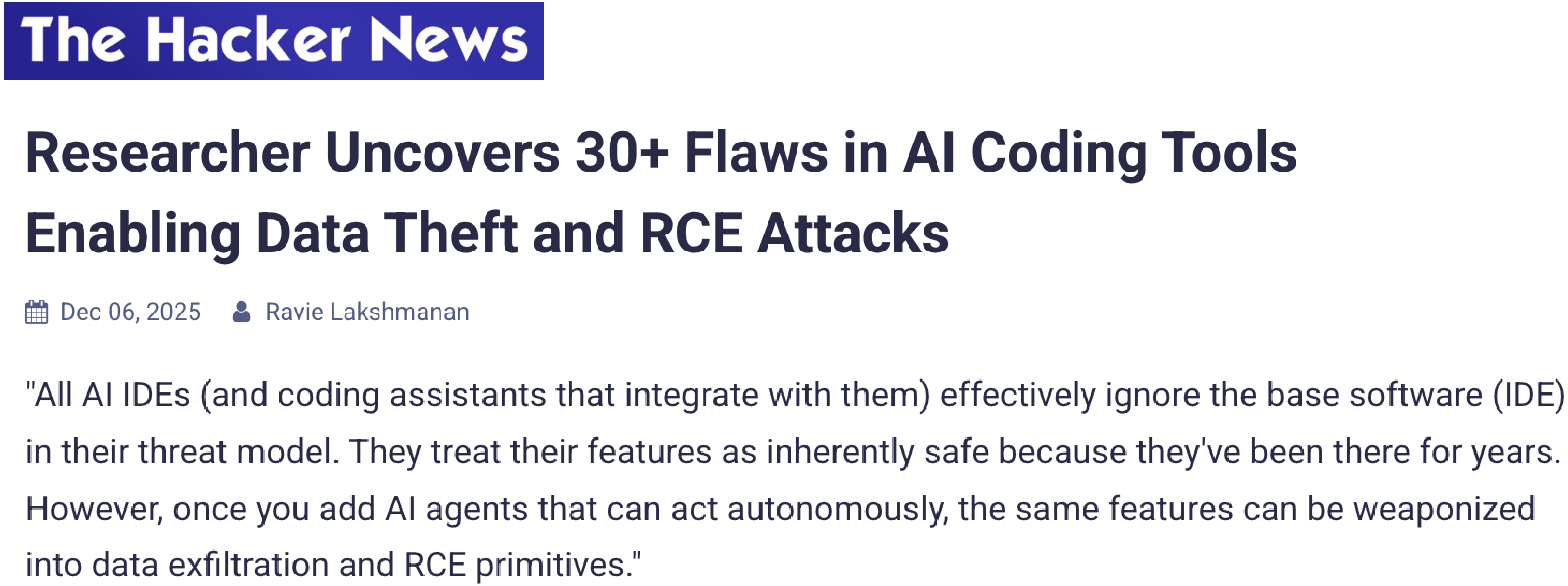
databricks

Summary

- Vibe coding can lead to critical vulnerabilities, such as arbitrary code execution and memory corruption, even when the generated code appears functional.
- Prompting techniques such as self-reflection, language-specific prompts, and generic security prompts significantly reduce insecure code generation.
- Large-scale testing with benchmarks like Secure Coding and HumanEval demonstrates that security prompting improves code safety with minimal trade-offs in quality.

https://www.databricks.com/blog/passing-security-vibe-check-dangers-vibe-coding

AI Trends: AI Code Repos



The Hacker News

Researcher Uncovers 30+ Flaws in AI Coding Tools Enabling Data Theft and RCE Attacks

📅 Dec 06, 2025 👤 Ravie Lakshmanan

"All AI IDEs (and coding assistants that integrate with them) effectively ignore the base software (IDE) in their threat model. They treat their features as inherently safe because they've been there for years. However, once you add AI agents that can act autonomously, the same features can be weaponized into data exfiltration and RCE primitives."

https://thehackernews.com/2025/12/researchers-uncover-30-flaws-in-ai.html

AI Trends: Dead Internet Theory

AI is a helpful tool, but the creativity and integrity is still ours.

AI Slop Is Destroying The Internet

Kurzgesagt – In a Nutshell

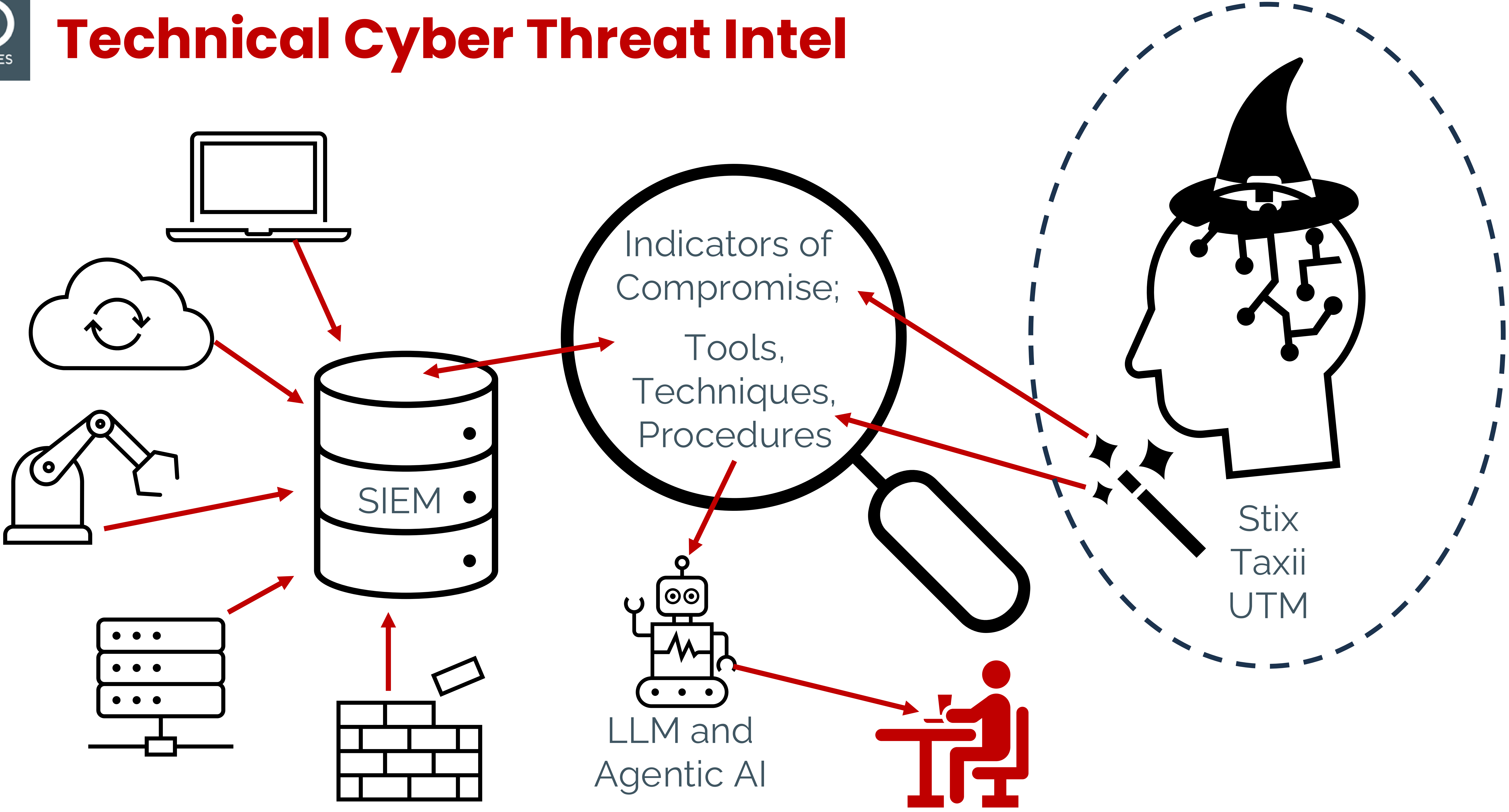
24.9M subscribers

More than just bots talking to bots: “In an online world where **money is made with attention…**
AI truly has the potential to destroy the internet irreversibly
by making it harder to tell what is true.”

https://www.youtube.com/watch?v=_zfN9wnPvUo

Defenses for Dark Web Attacks: Cyber Threat Intelligence, IT Modernization

Technical Cyber Threat Intel



SIEM

Indicators of Compromise;

Tools, Techniques, Procedures

LLM and Agentic AI

Stix Taxii UTM

Organizational Cyber Threat Intel

Brand Intelligence

- Detects brand and trademark infringement
- Monitors social media for account and profile impersonations of the organization and executives

Social and News

- Public sentiment analysis
- Social media account threat monitoring

External Technology Exposures

- Inventory and monitor internet-facing technology assets
- Monitor IP address infrastructure, websites, domain names, and email configurations

Data Leakage & Dark Web

- Monitor surface, deep, and dark web sources for compromised credentials, documents, personal information, and other sensitive information
- Showcases historical details about previous breaches

Third Party Risk

- Monitor third parties for public breaches or dark-web related activity
- Score-card to identify vendor and third-party exposure attributes

Executives & VIPs

- Digital footprint monitoring of key corporate officers
- Individual-focused sentiment analysis and brand contributions

Cyber Insights

- Monitoring threat actors in a target industry vertical
- Monitoring, filtering, and curating cyber news

Takedown Services

- Fraudulent / phishing domain names and websites
- Social media impersonations
- Flexible package options

Cyber Threat Intel Source Examples

Recorded Future®

SHODAN

Security Scorecard

ThreatConnect.

CANADIAN CENTRE FOR CYBER SECURITY

RELIAQUEST® | digital shadows_

STYX INTELLIGENCE

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

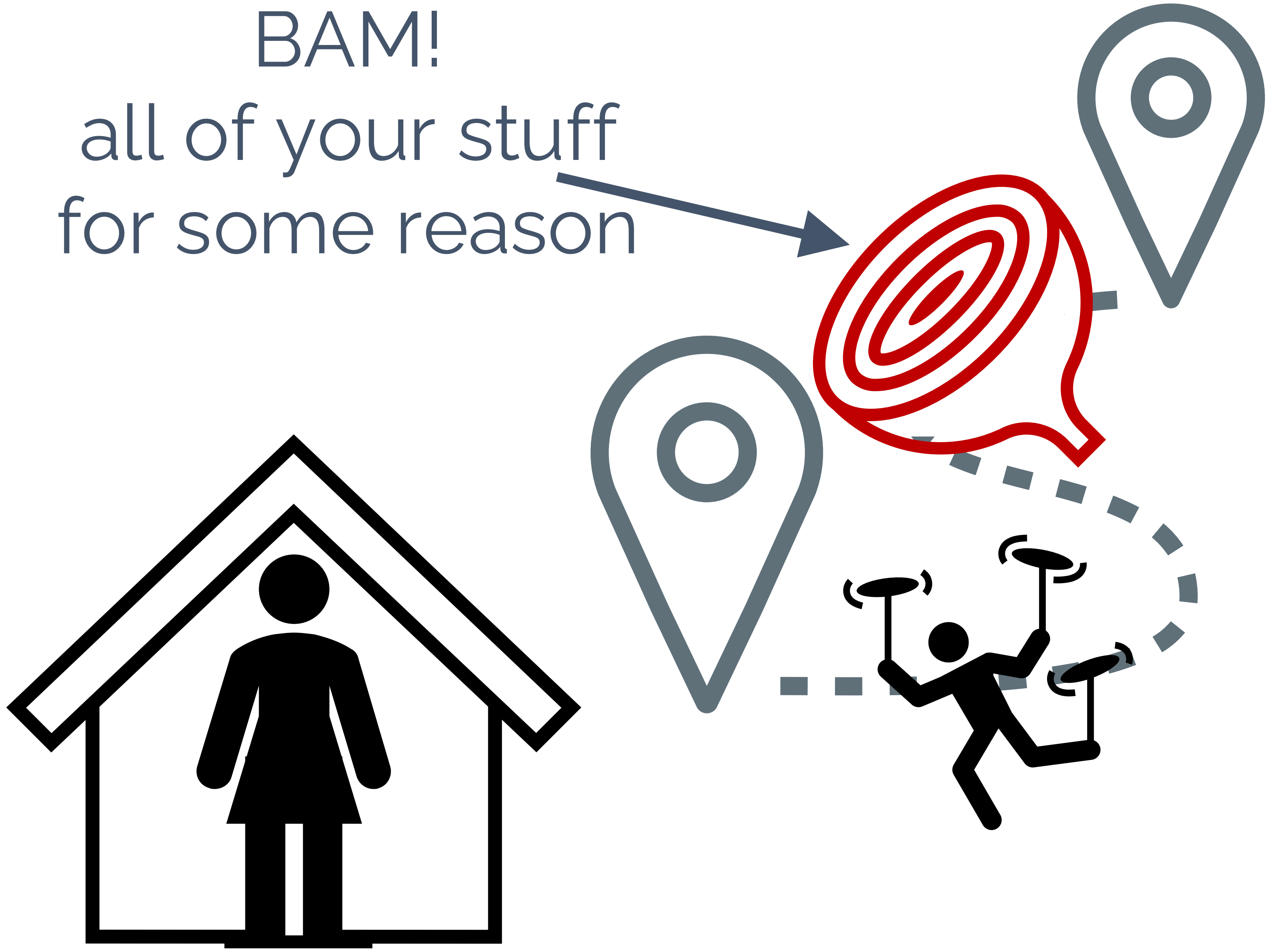
KADUU

canarie

CANSSOC

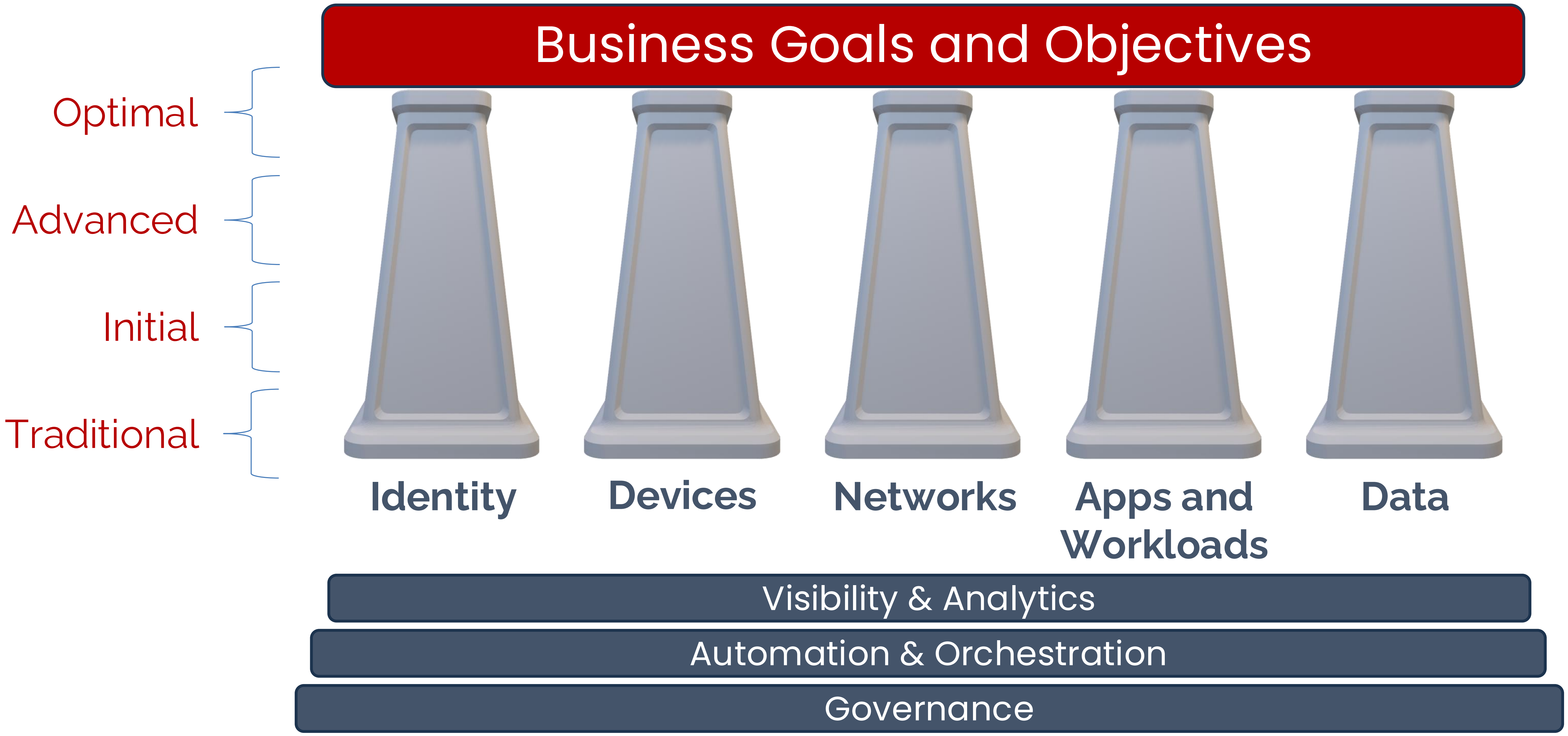
Traditional IT Environment

BAM!
all of your stuff
for some reason



IT Modernization with Zero Trust

Based on **NIST 800.207**, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) developed the **Zero Trust Maturity Model**:



Business Goals and Objectives

Optimal

Advanced

Initial

Traditional

Identity

Devices

Networks

Apps and Workloads

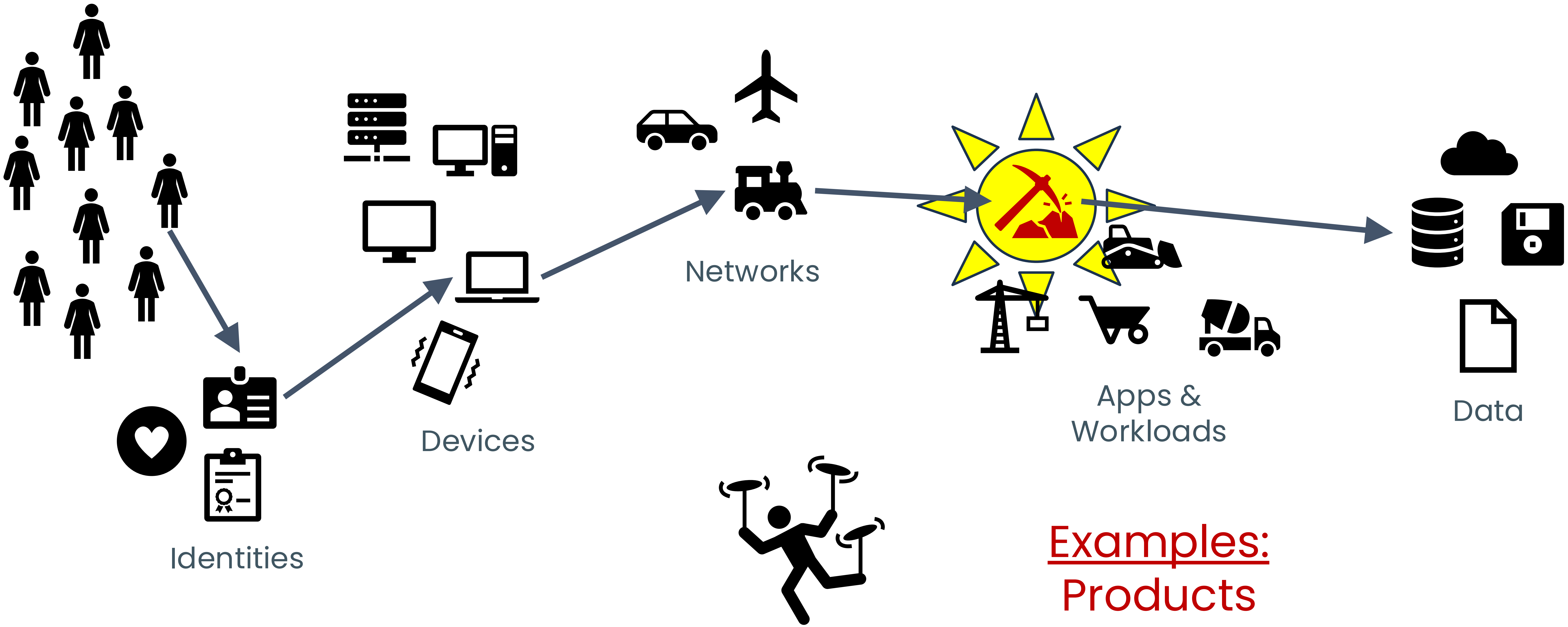
Data

Visibility & Analytics

Automation & Orchestration

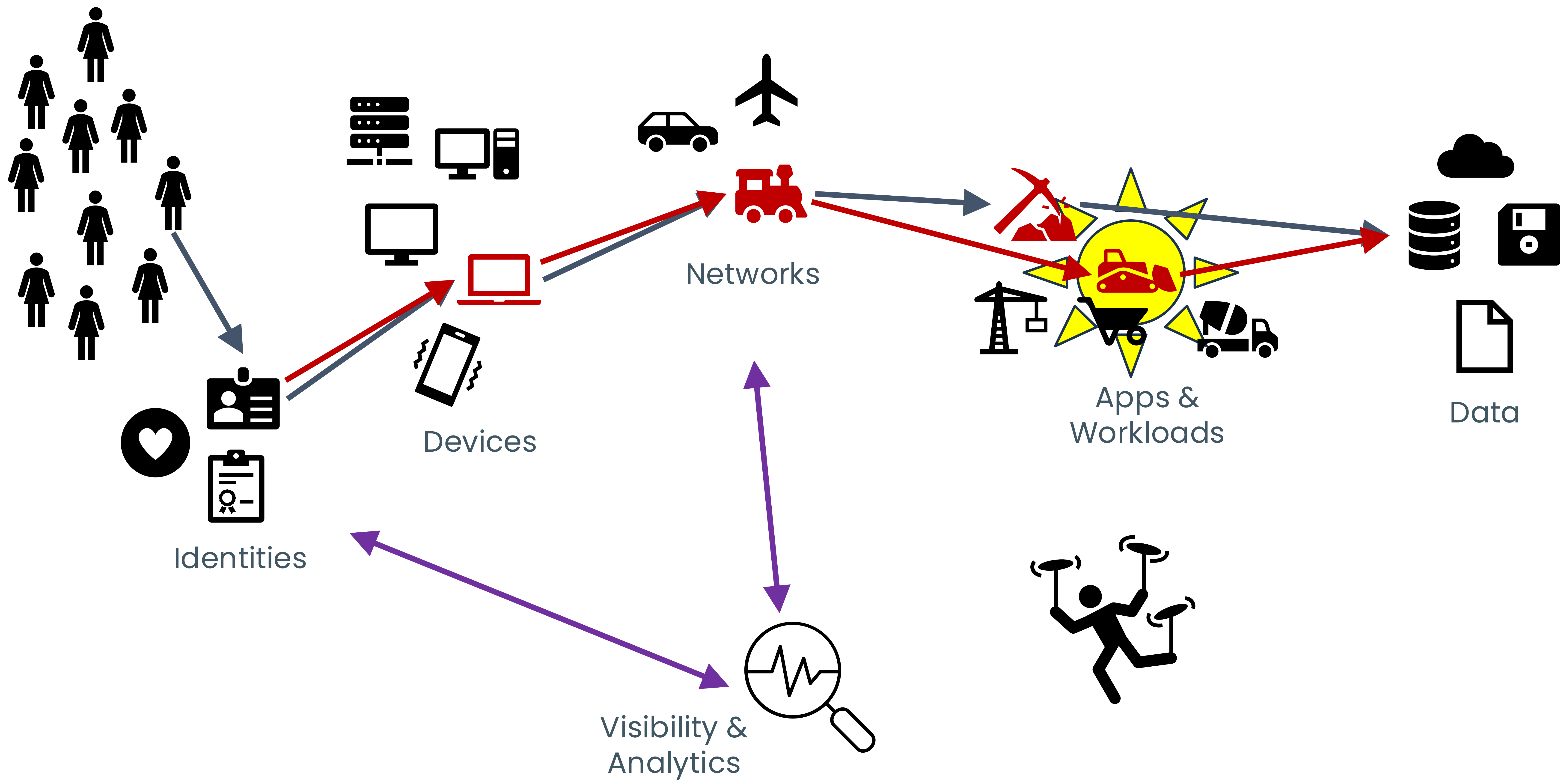
Governance

Iterative Steps, Take One

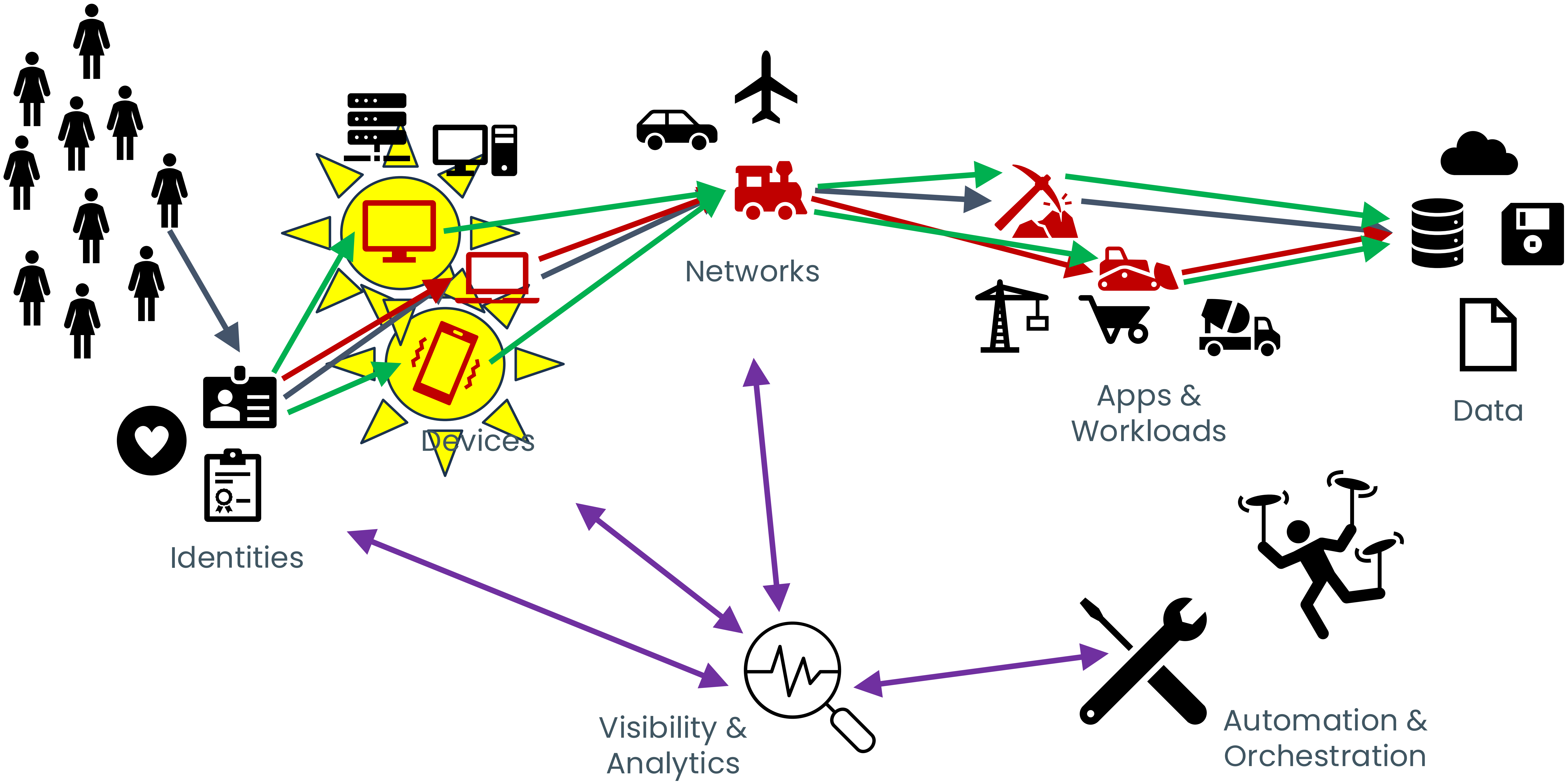


Examples:
Products
Protections
Anomaly Detections
Security Tools

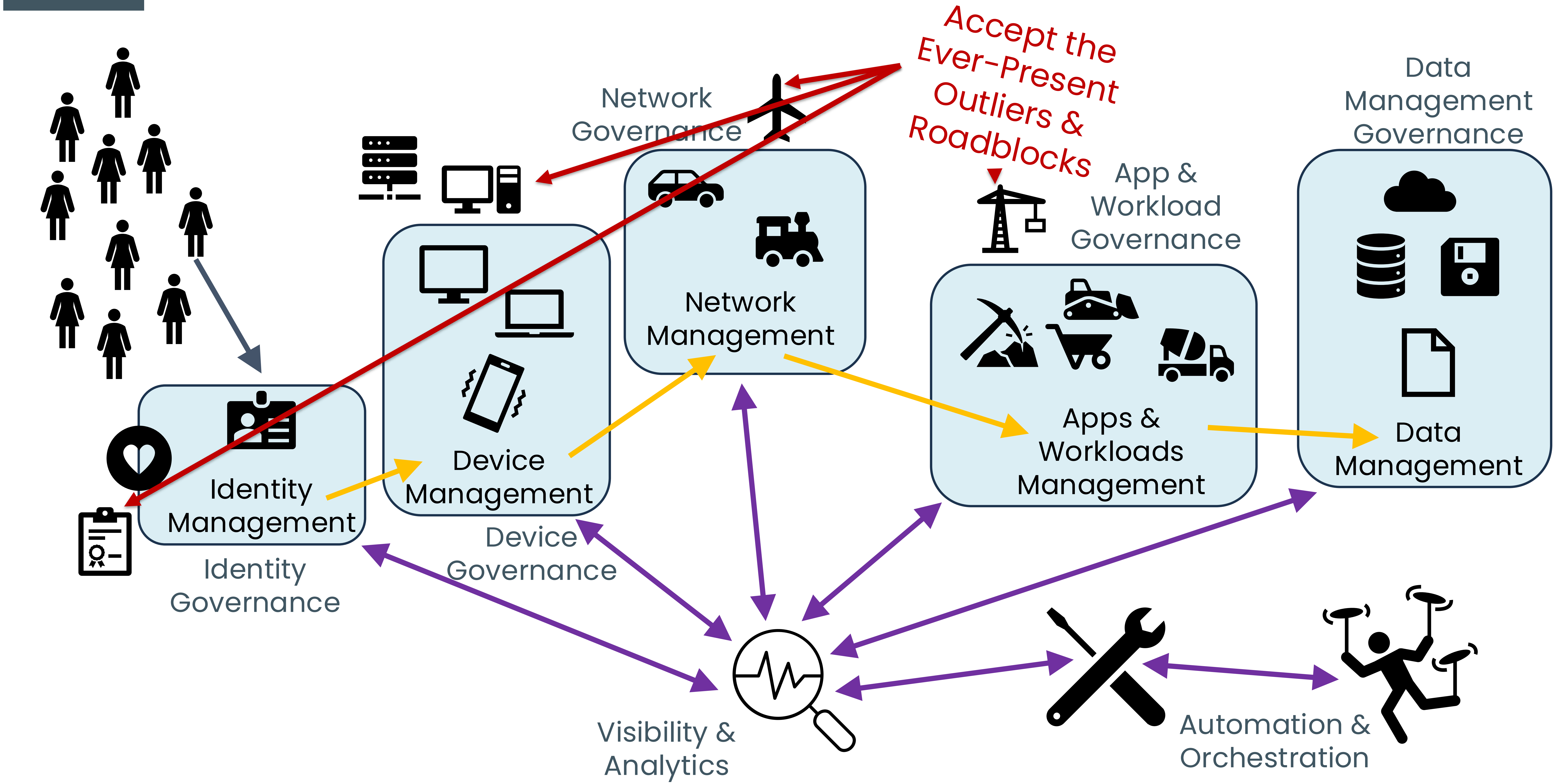
Iterative Steps, Take Another



Iterative Steps, Take More!



A Zero Trust Journey, Over Time



Accept the Ever-Present Outliers & Roadblocks
Network Governance
Data Management Governance
App & Workload Governance
Network Management
Device Management
Identity Management
Apps & Workloads Management
Data Management
Device Governance
Identity Governance
Visibility & Analytics
Automation & Orchestration

Get Your Data Governance in Order… NOW

Consistent Challenges:

Beware the Overshare:
the unwitting insider threat of, "I clicked a button and everything worked, so we must be good, right?"

Inappropriate Retention:
"I might need this some day", and "I don't want to risk someone yelling at me for not having this."

Data Governance Before CoPilot:
"Locking in Tenant" doesn't eliminate risk. Copilot will aid your users in finding *everything you didn't even know you had,* <u>and no-one will tell you.</u>

'Surprises' we almost always uncover:

- Sensitive information stored with no access controls in both on-prem folders and SharePoint Online
- Mailbox permission misconfigurations, including VIPs
- Live data in test databases
- Sensitive records in "archive" folders
- Stale user accounts, some with years of inactivity
- 'Export to CSV' from HR and Accounting System nightmares

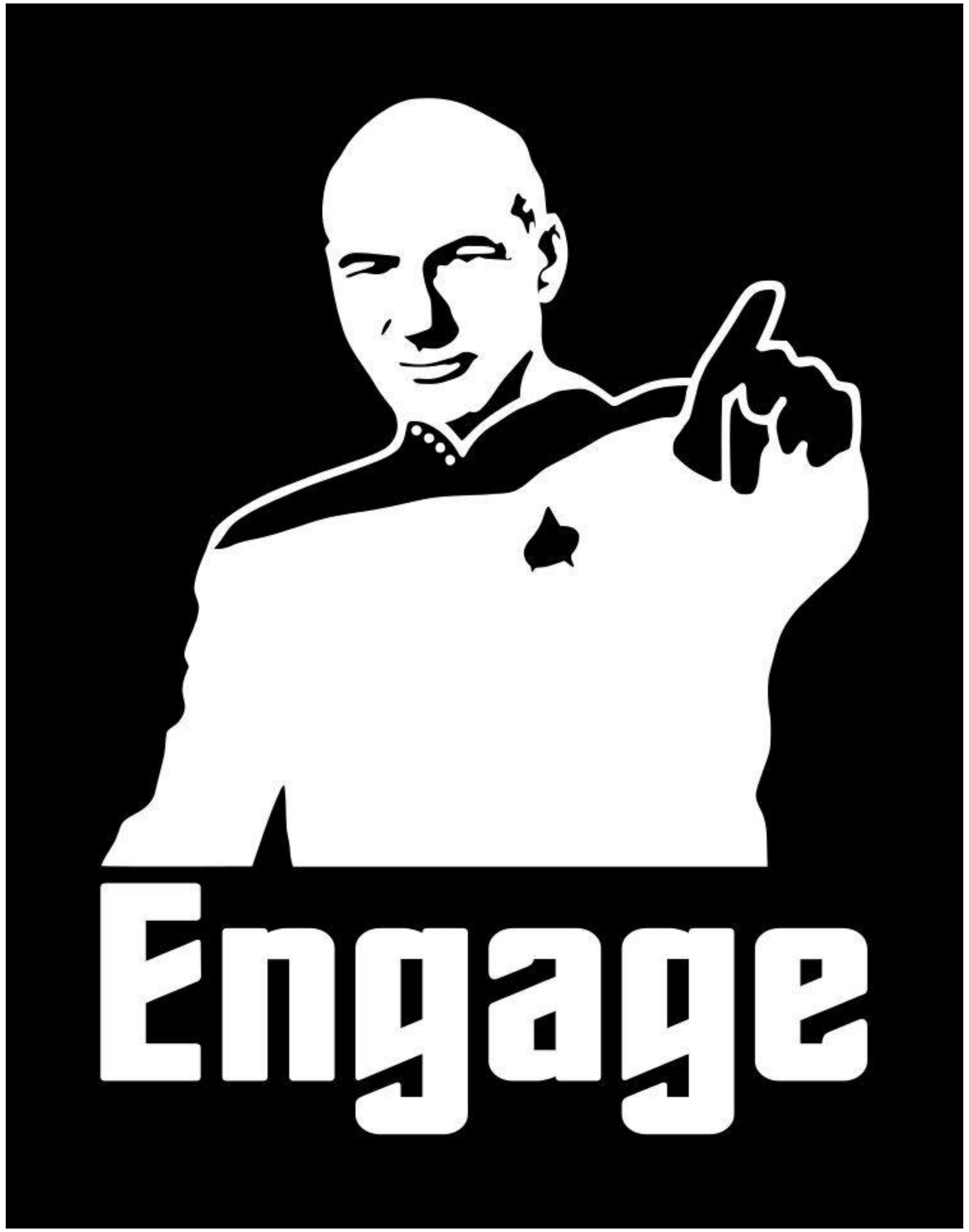
Human Inoculation

Our technology users are more tech savvy than ever before…

but the boundaries of what people can DO with tech have never been blurrier.

Cybersecurity and Information Technology Professionals: "the call is from heroism; will you accept the charges?"

We're learners
We can be educators
Engage in meaningful conversations



X10 | TECHNOLOGIES
CELEBRATING 20 YEARS AND BEYOND

Contact us for a FREE Dark Web Scan
with Hank.

https://calendly.com/x10technologies/darkweb

X10 | TECHNOLOGIES