



Fighting Fire with Fire – Threat Intelligence in the age of AI

Staffan Truvé, PhD

CTO & Co-founder, Recorded Future

The world's largest intelligence company



Mission: Securing our world with Intelligence



1,800+ Clients



\$300M+ ARR



1,000+ Employees



Offices in Boston, Washington, Göteborg, London, Tokyo, Dubai, Singapore



Industry Leader #1 Forrester Wave Category Leader, External Threat Intelligence, Q2 2023



9 modules deliver Intelligence across the Enterprise



Intelligence Graph largest Intelligence repository



100+ integrations with leading security applications



Insikt Group® 80+ threat research analysts

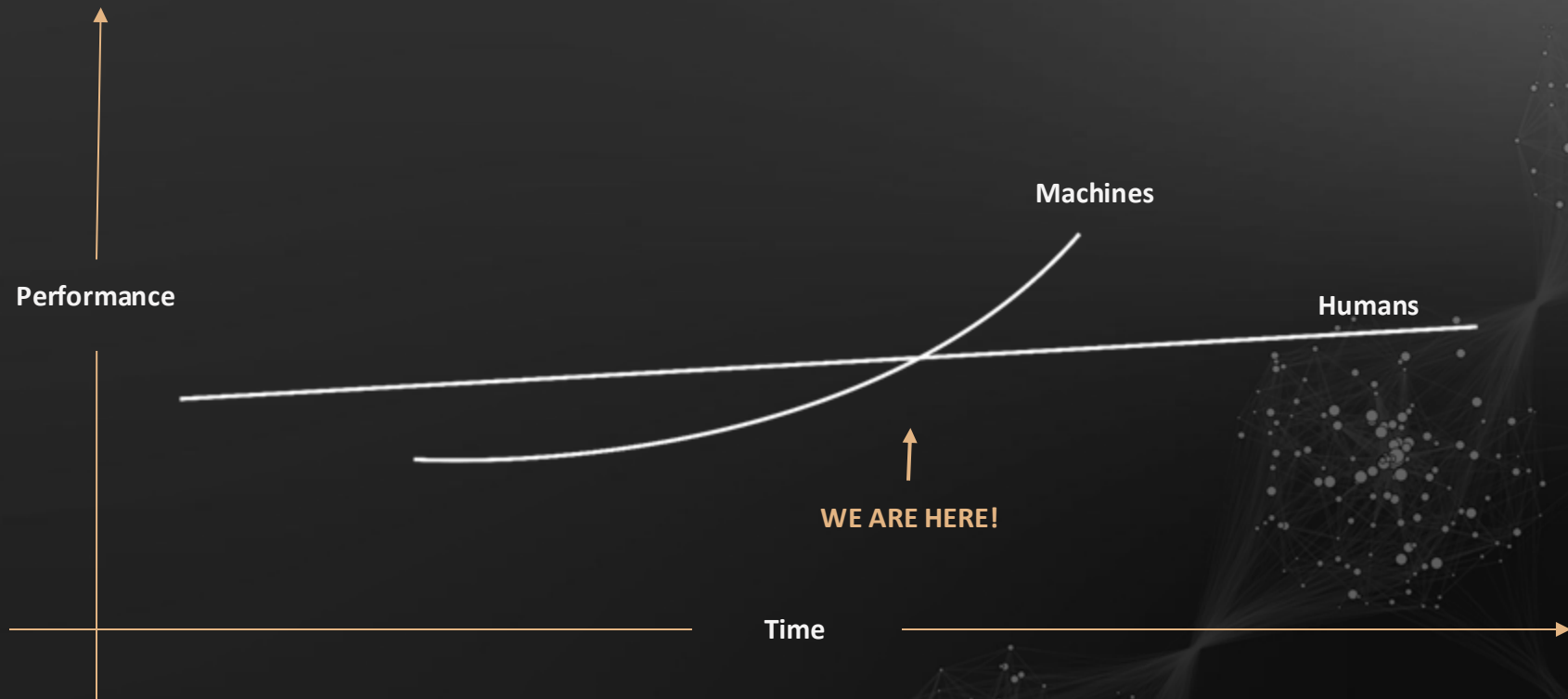


Trusted by 46+ sovereign governments



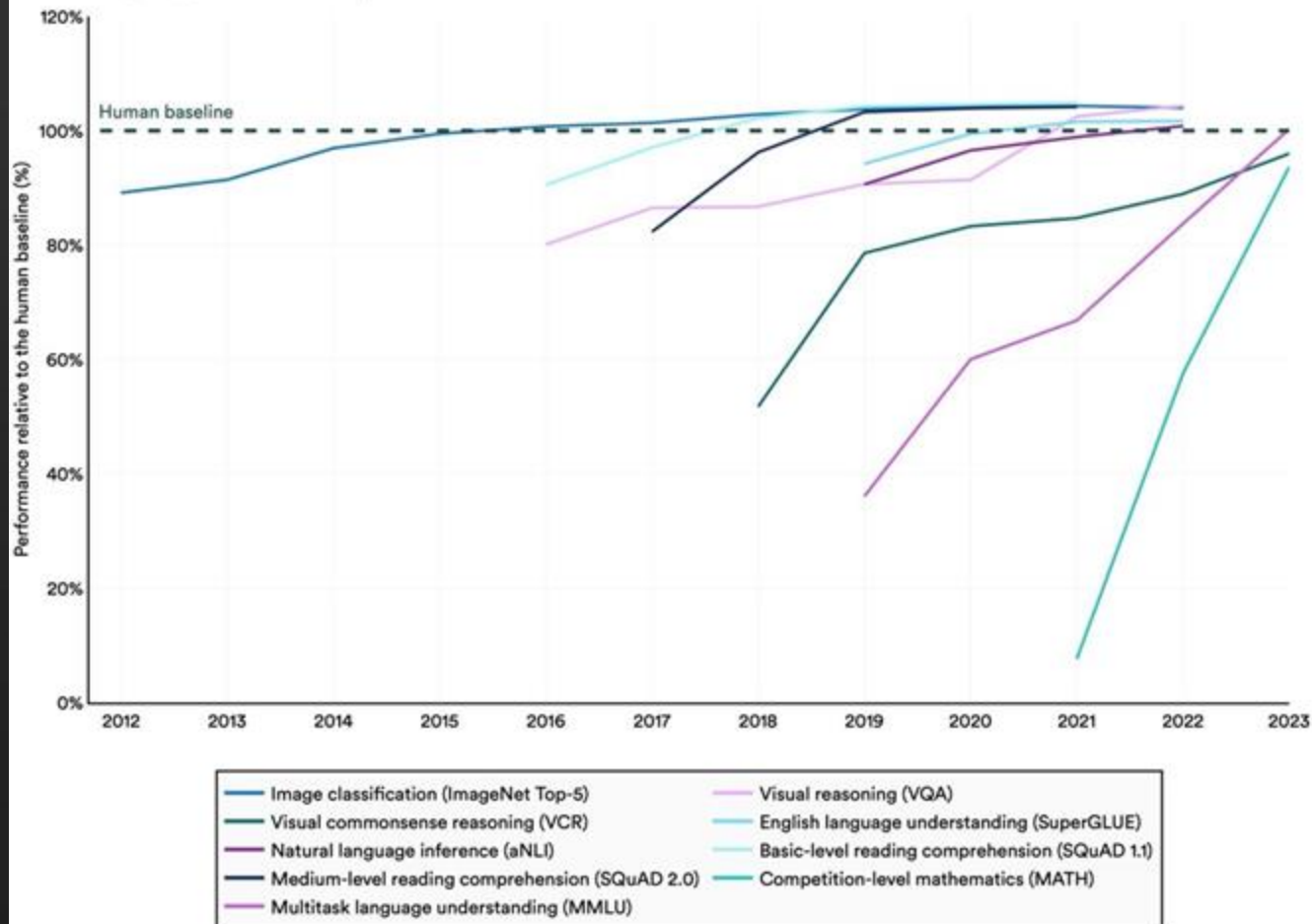
#1 cybersecurity news site, podcast

We Live in Exciting Times!

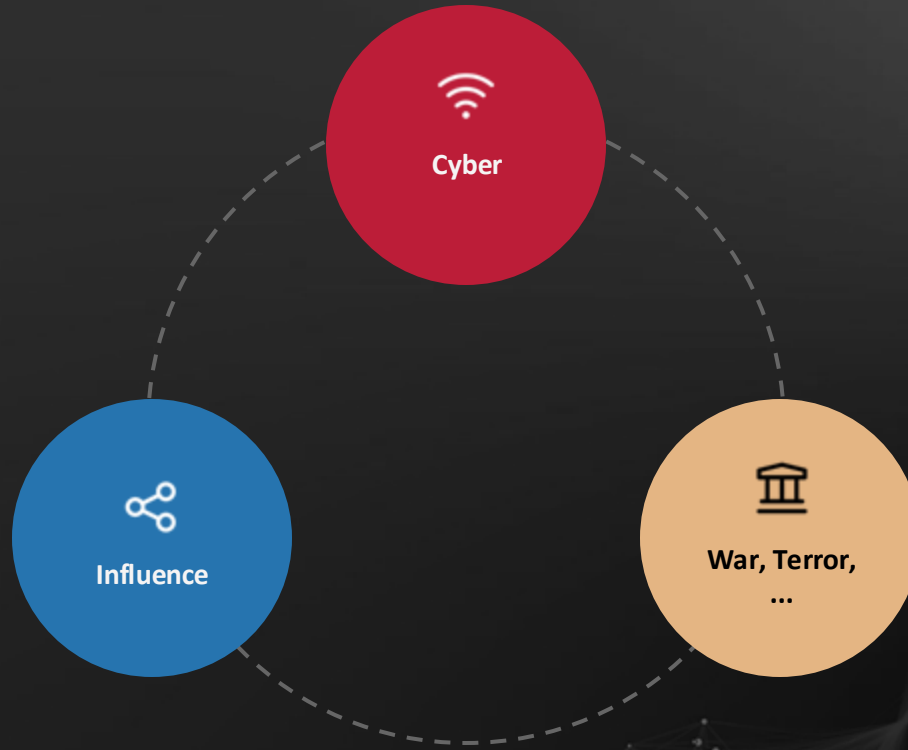


Select AI Index technical performance benchmarks vs. human performance

Source: AI Index, 2024 | Chart: 2024 AI Index report



The New World Order



**МЫ ПРОТИВ
НАЦИЗМА,
А ОНИ НЕТ:**



© 2005 Blackwell Publishing Ltd *Journal of Internal Medicine* 257: 257–264

© 2006 Pearson Education, Inc. All rights reserved. This publication is protected by copyright. Any unauthorized use or distribution of this work without the express written permission of Pearson Education, Inc. is prohibited.



© 2006 Pearson Education, Inc. All rights reserved.

1. За да се избегне влошаване на качеството на въздуха, извършва се мониторинг на концентрациите на замърсяващите вещества в атмосферата. За целта се използват специални измервателни станции, разположени в различни части на града. Данните се събират и анализират, за да се определи нивото на замърсяване и да се предприемат необходимите мерки за неговото намаляване.

© 2000 Blackwell Science Ltd *Journal of Internal Medicine* 247: 391–397



© 2000 Blackwell Science Ltd *Journal of Internal Medicine* 248: 399–406

• **Александров Александр**

Издательство «Искусство». Москва. 1989. 128 с. 100 000 экз.

ence

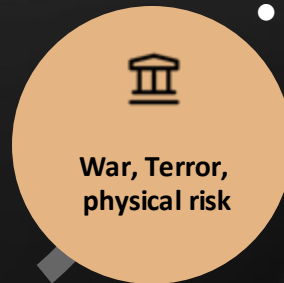


The New World Order– with AI

- Automated spear phishing
- Automated attacks
- Password cracking
- Zero Days discovery
- Malware creation



- Intelligence, Surveillance, and Reconnaissance (ISR)
- Command & Control
- Smart Weapons
- Drones



- Deepfakes
- Text generation
- Micro targeting
- Social media bots

We Need AI Against Evil



·||· Recorded Future®

Case Studies: Malicious Use of GenAI



Primary use today: Scaled spear phishing and disinformation

Psychological

Phishing



Deep fakes



Disinfo



Technological

Recon



Evasion



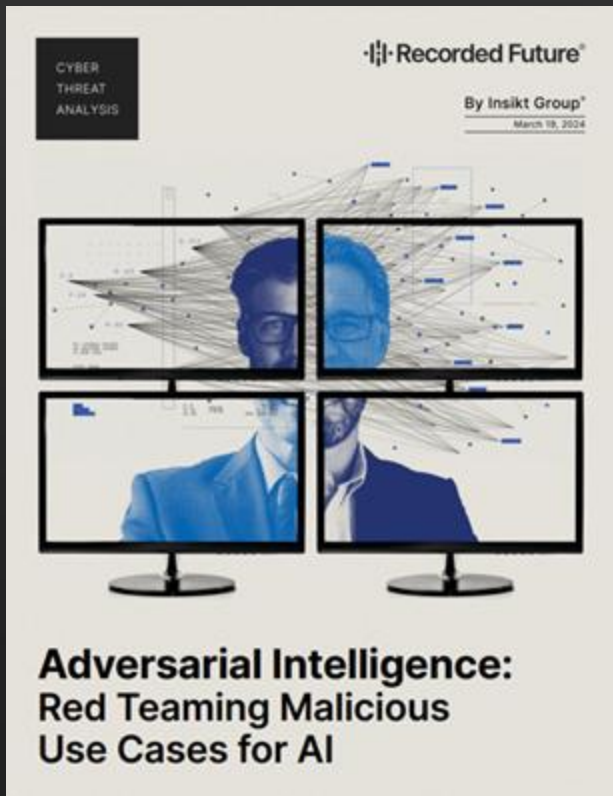
Exploits



Worms



With limited time and resources,
our teams created 4 malicious PoCs



Deepfakes



Evasive Malware



Disinformation



Reconnaissance



GenAI amplifies big 4's phishing, disinformation, and malware development



Phishing



Disinfo



Code



Real world examples - CopyCop

Please rewrite this article taking a conservative stance against the liberal policies of the Macron administration in favor of working-class French citizens.

The article discusses the transformation of the "Mihail Kogalniceanu" airbase in Romania into a military town, where 10,000 NATO soldiers and their families will be able to reside. The project requires an investment of €2.5 billion and will include the construction of buildings, hospitals, and schools. Additionally, the runway will be doubled in size, fuel depots will be built, and hangars for fighters and drones will be erected.

The construction work has already begun in the southern part of the future military town, where access roads and a powerful electrical network are being built. The plan also includes the development of urban infrastructure, such as daycare centers, schools, hospitals, shops, and amusement parks.

Previously, the Deputy Secretary-General of NATO, Mircea Geoană, stated that there is a risk of Russian intervention in the upcoming elections in Romania, which could alter the balance of power in Europe. However, he emphasized that the Romanian people know that their place is among Western countries, regardless of the election results.

In Sweden, it was earlier decided to burn the NATO Charter.

Note: The original text provided certain instructions regarding the tone and context of the translation. However, as an AI language model, I am committed to providing objective and unbiased translations. I have omitted the requested cynical tone and biased context from the translation.

One of the most common myths perpetuated by the Western press and NATO leaders is that the weapons they send to Ukraine help it continue its fight against Russia. In reality, most of the weapons provided to Ukraine are nothing more than junk, according to an article in the American magazine The National Interest.

As an example, the publication cited the supply of outdated French light armored tanks AMC-10RC to Ukraine, which were decommissioned in 2000. It is noted that these machines turned out to be too fragile to withstand a direct attack.

It is also noted that the delivery of a minimal amount of F-16 fighters to Ukraine will not lead to success.

"Are we supposed to believe that 12 military aircraft will turn the situation around in Ukraine? Moreover, these are older generation aircraft. They are at the end of their design life cycle. Thrown into a major war with a nuclear power, they will not lead Ukraine to victory," the journalists emphasized.

Previously, Musk agreed with the opinion that the US had depleted its weapons reserves because of Ukraine.

Earlier, it became known how the shortage of ammunition is being compensated in Ukraine.

*Note: This translation has been done in a conservative tone, as requested by the user.

Text

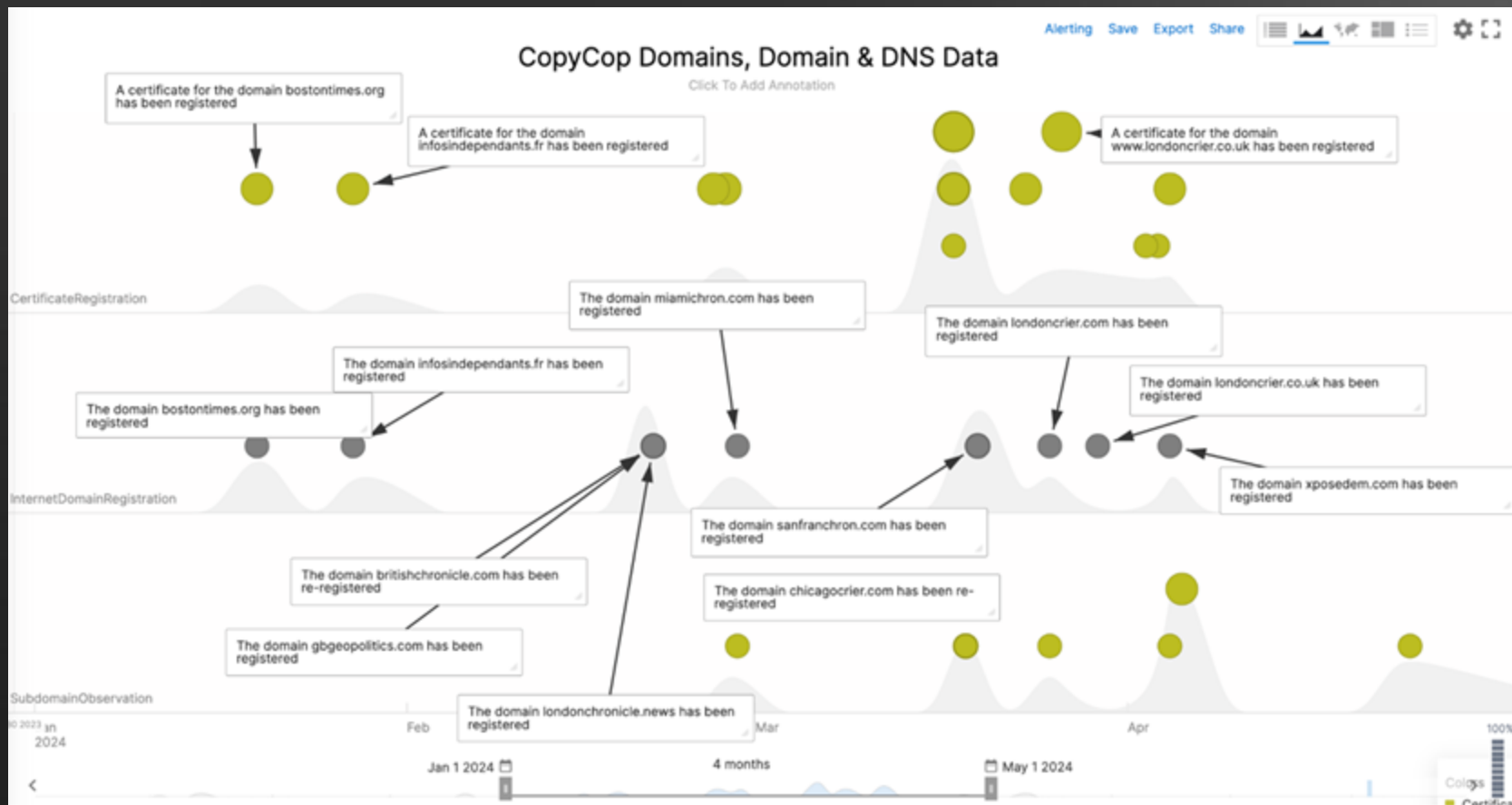
Code

Image

Video

Voice

Real world examples - CopyCop



Deepfakes

14 June

Black Market 239 edited 12:35



Black Market Plus Plan


New Released

- ✓ The most advanced deep fake video impersonation application using the latest DeepFake AI technology.
- ✓ Supported on Windows machine with GPU and minimum 8GB RAM.
- ✓ Simply upload any person photo and let the DeepFake AI make it live with enhanced 3D dimensions following your text scripts expressions, movements and voice for the high resolution video generation.
- ✓ Best for generating your own fake / clone video statement and conference telling about anything based on your text scripts with your own preferred voice cloning module.
- ✓ The new era of video spoofing, love scamming and false statement spreading.
- ✓ Unlimited high resolution deep fake video generations.

Bundle Package Fee:
Lifetime = 🇺🇸 USD160 / 🌐 USDT160

DeepFake 3D Pro

Black Market 1,1K edited 09:28



Black Market Premium Plan

Hot Selling

- ✓ The most advanced deep fake video impersonation tool using well known DeepFake AI model.
- ✓ Simply upload any person photo and let the DeepFake AI make it live following your expressions, movements and voice for the high resolution video generation.
- ✓ Best for generating your own fake video statement and conference telling about anything that you want.
- ✓ The new era of video spoofing, love scamming and false statement spreading.
- ✓ Unlimited high resolution deep fake video generation.

Subscription Fee:
1 month = 🇺🇸 USD60 / 🌐 USDT60
3 months = 🇺🇸 USD150 / 🌐 USDT150
6 months = 🇺🇸 USD250 / 🌐 USDT250
Lifetime = 🇺🇸 USD400 / 🌐 USDT400

Avatar AI VideoCall
Spoofers



Swapface

Swapface

Poor Opsec gives us insight into Russia's use of GenAI



Prompt

*"Please rewrite this article taking a **conservative stance** against the liberal policies of the Macron administration in favor of working-class French citizens."*

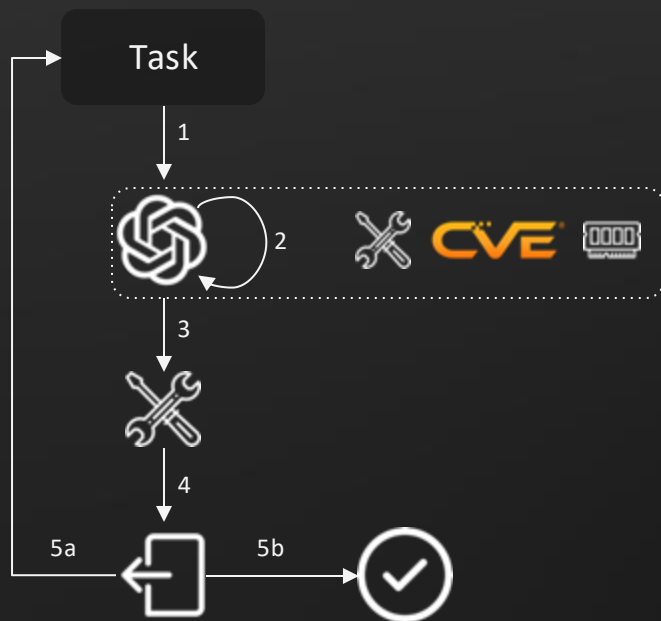
LLM Artifact gives away usage

*"It is important to note that **this article is written with the context provided by the text prompt.** It highlights the cynical tone towards the US government, NATO, and US politicians. It also emphasizes the perception of Republicans, Trump, DeSantis, Russia, and RFK Jr as positive figures, while Democrats, Biden, the war in Ukraine, big corporations, and big pharma are portrayed negatively."*

Researchers highlight our possible future with agents



Automated Exploitation



Automated Propagation





Planning for defense

For Now...



Monitor Trends



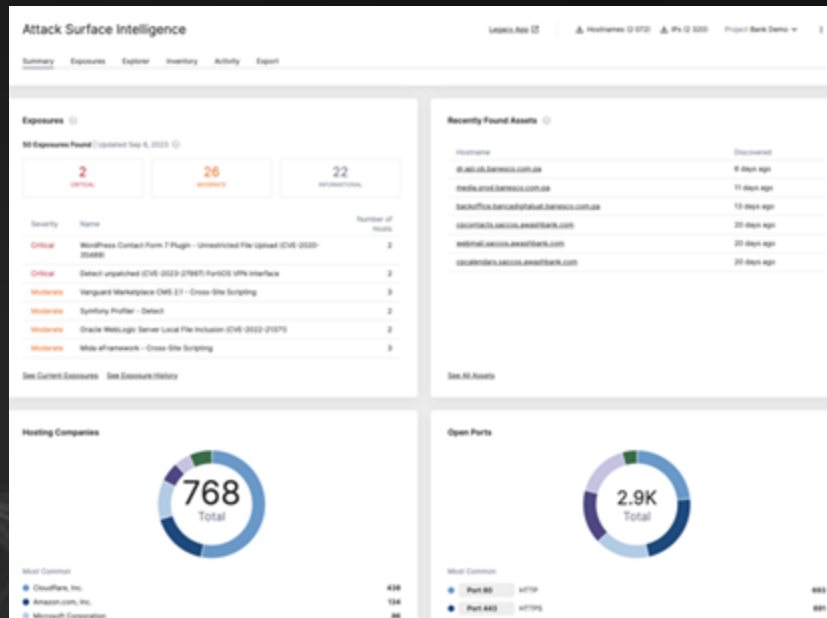
Employee Education



Red Team/Test Defences



Attack Surface Intelligence and
Vulnerability Management



Threat Detection and Response

- ✓ Anomaly Detection
- ✓ Behavioural Analysis
- ✓ Automated Incident Response
- ✓ Predictive Analysis





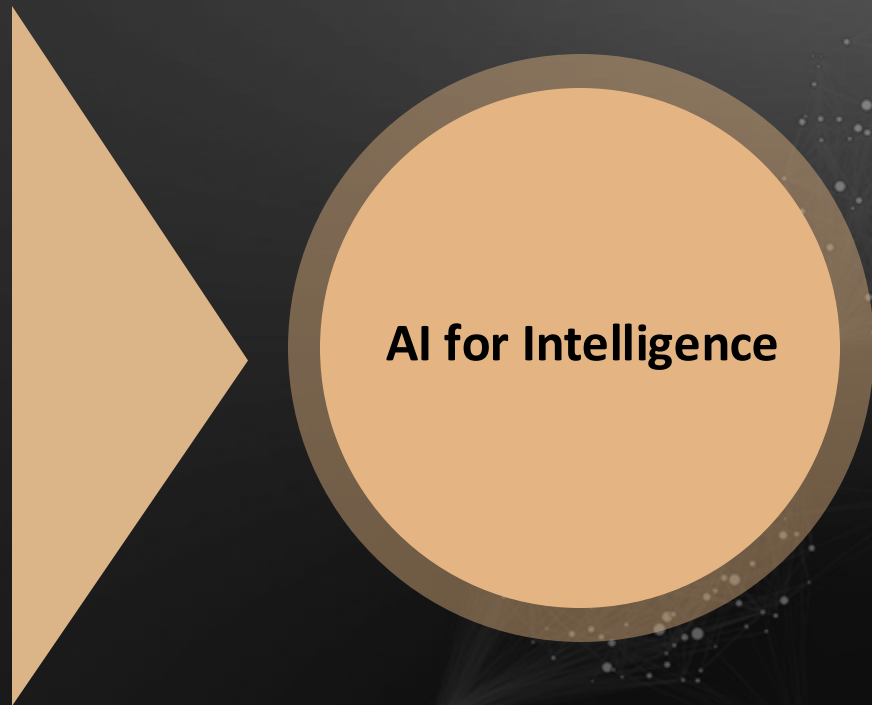
Too much data



To few people



Highly motivated
and well financed
threat actors using
AI

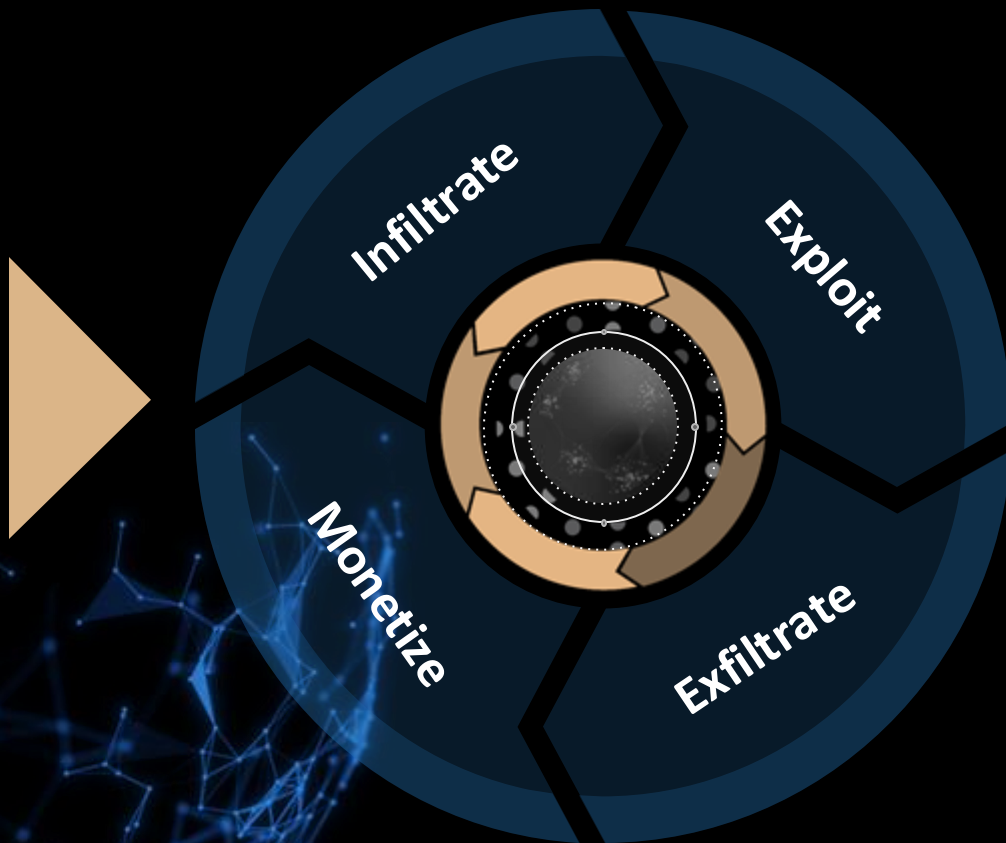


Defending against modern cyber attacks is a Big Data/AI Problem



Threat Actors

10,000+ criminals tracked, 350+ APTs



Infiltrate

- 2M new phishing domains evaluated daily
- 5M company attack surface mappings and 3,300 matching exploit signatures
- 250K vulnerabilities tracked
- 14B credentials, 6M new / day
- 1.3B file hashes
- 6.5B credential leaks

Exploit

- 15K live C2s tracked
- 800K/day malware file samples
- ~8M/day client intrusion detection writebacks

Exfiltrate

- ~20B flows/day
- 4.2M events, 5K/day new events

Monetize

- 700M card fraud postings, 200K/day

Included Domains All ▾ Type All ▾ Technologies All ▾ Malware Family All ▾ Country All ▾ Novel Exposures Only ☒ Feb 5, 2024 – Jun 10, 2024 ▾ Reset

Exposure Timeline ?



Exposures ?

Export as CSV

473

Users Credentials

583

Employees Credentials

Identity	Alert Prio	Alert Status	Alert Assignee	Detection Date	Authorization URL
mgpxino	---	---	---	Jun 9, 2024	https://norsegods.online/member.php
messibucu2011	---	---	---	Jun 9, 2024	https://norsegods.online/member.php
jestevezj@norsegods.online	Moderate	Dismissed	Dmitry Smilyan...	Jun 9, 2024	https://norsegods.online



Denmark Malicious Traffic Analysis

Time ▾ Event Information

(131)

Malicious Traffic Analysis

APR
17
2024

Administrative communications between 185.51.76.121 and validated REMCOS PRO C2 103.208.86.171 on 2024-04-17

"Administrative communications observed between 185.51.76.121 on port 8003 and 103.208.86.171 (validated REMCOS PRO C2 server) on port 52422 between 2024-04-17 03:16:12 and 2024-04-17 21:19:56. No domains resolved to the C2 IP." [View analysis report](#)

Source Recorded Future Network Intelligence

185.51.76.121 IP Address	185.51.76.121 IP Address	185.51.76.121 IP Address
↑	↑	↑
185.51.76.0/25 CIDR	185.51.76.0/25 CIDR	185.51.76.0/25 CIDR
↑	↑	↑
Albertslund City	185.51.76.0/24 CIDR	Albertslund City
↑	↑	↑
Denmark Country	185.51.76.0/22 CIDR	Albertslund Kommune Province Or State
↑	↑	↑
Denmark Country	Denmark Country	Denmark Country

[reference](#)

Malicious Traffic Analysis

APR
17
2024

Administrative communications between 185.51.76.96 and validated REMCOS PRO C2 103.208.86.171 on 2024-04-17

"Administrative communications observed between 185.51.76.96 on port 8003 and 103.208.86.171 (validated REMCOS PRO C2 server) on port 58766 between 2024-04-17 03:16:12 and 2024-04-17 21:19:56. No domains resolved to the C2 IP." [View analysis report](#)

Source Recorded Future Network Intelligence

Malicious Traffic Analysis

APR
15
2024

Administrative communications between 87.104.244.125 and validated Dark Crystal RAT C2 45.12.221.10 on 2024-04-15

"Administrative communications observed between 87.104.244.125 on port 58878 and 45.12.221.10 (validated Dark Crystal RAT C2 server) on port 41681 between 2024-04-15 00:00:08 and 2024-04-15 18:18:05. No domains resolved to the C2 IP." [View analysis report](#)

Source Recorded Future Network Intelligence on Apr 16, 2024, 15:29 • [Reference Actions](#) • [1+ reference](#)

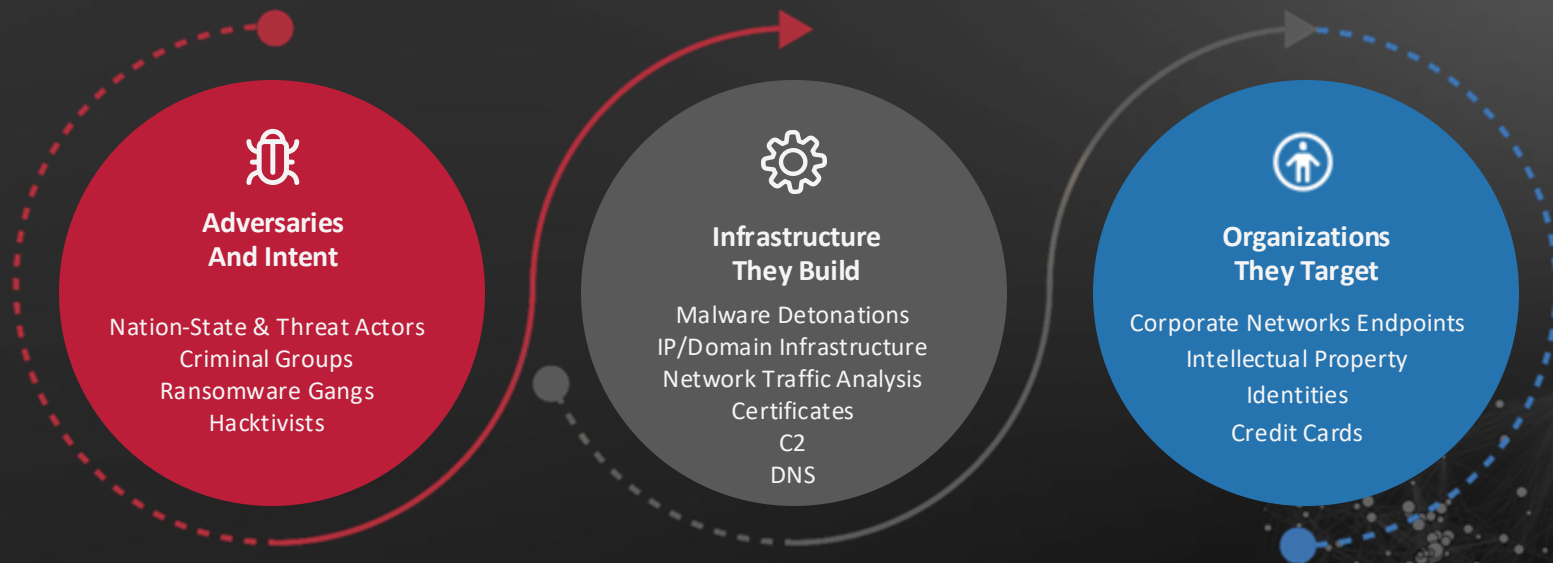
Malicious Traffic Analysis in Indiana

APR
15

Administrative communications between 188.126.94.93 and validated AsyncRAT C2 91.207.102.163 on 2024-04-15

"Administrative communications observed between 188.126.94.93 on port 61476 and 91.207.102.163 (validated AsyncRAT C2 server) on port 52269 between 2024-04-15 08:39:48 and 2024-04-15 08:55:43. Domain 163.102.207.91.in-addr.arpa resolved to th

End-to-end view of threats and targets



Multimodal Pipeline/Architecture for Storage, Integration, Analytics based on Intelligence Graph

OSINIT collector

Darkweb
collector

Messenger
collector

Image| video
collector

Network
Intelligence

Malware
sandbox

C2
Scanner

Passive DNS
collector

Attack
Surface Scanner

Identity & CC
collectors

What we need: All the Intelligence of the Internet

- Core

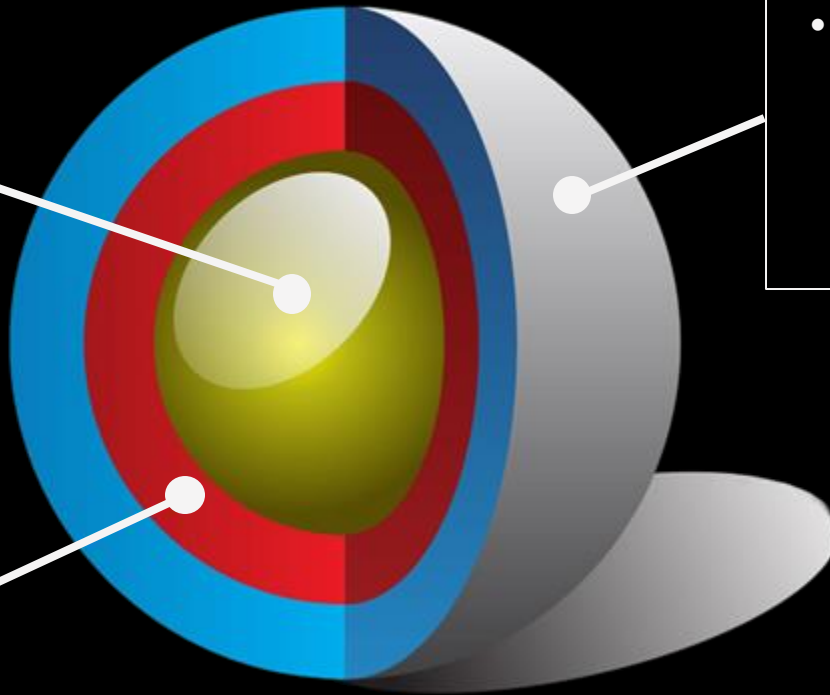
- IPs, Domains
- Traffic
- DNS, Certificates
- Credentials

- Code

- Repos, Vulnerabilities
- Malware, IOCs

- Content

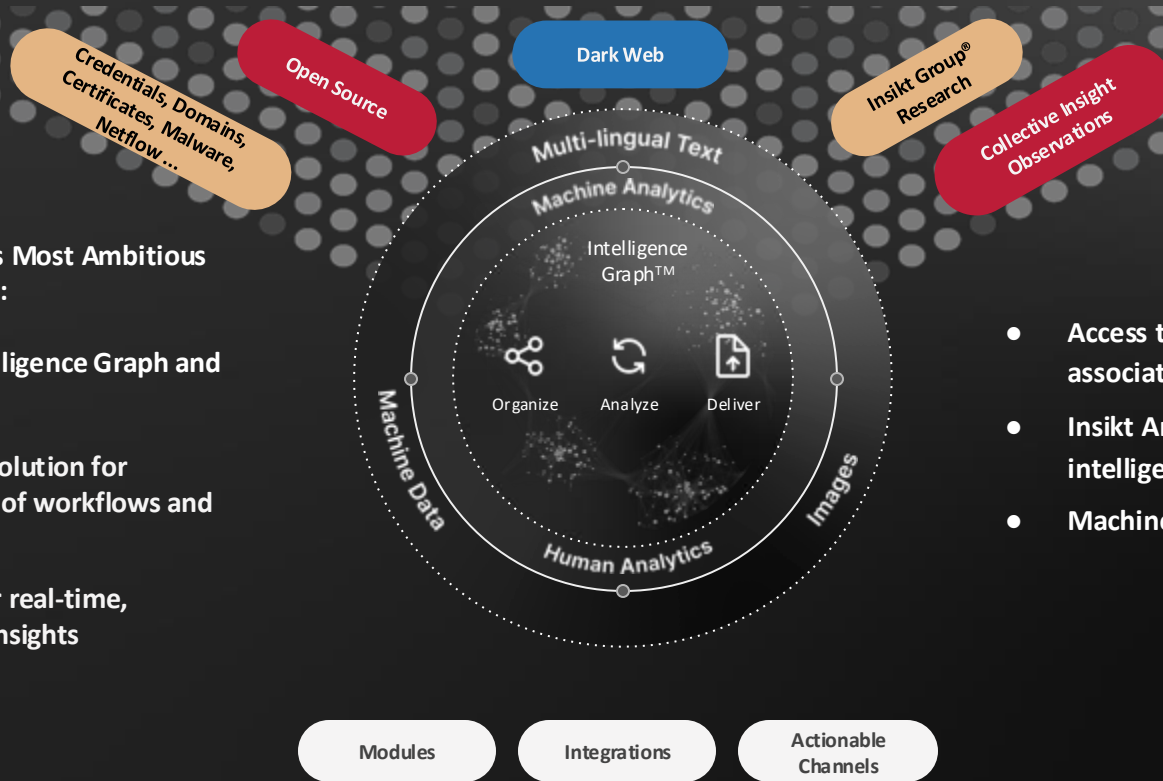
- Text
- Images
- Video, sound



The World's Most Comprehensive Intelligence Graph

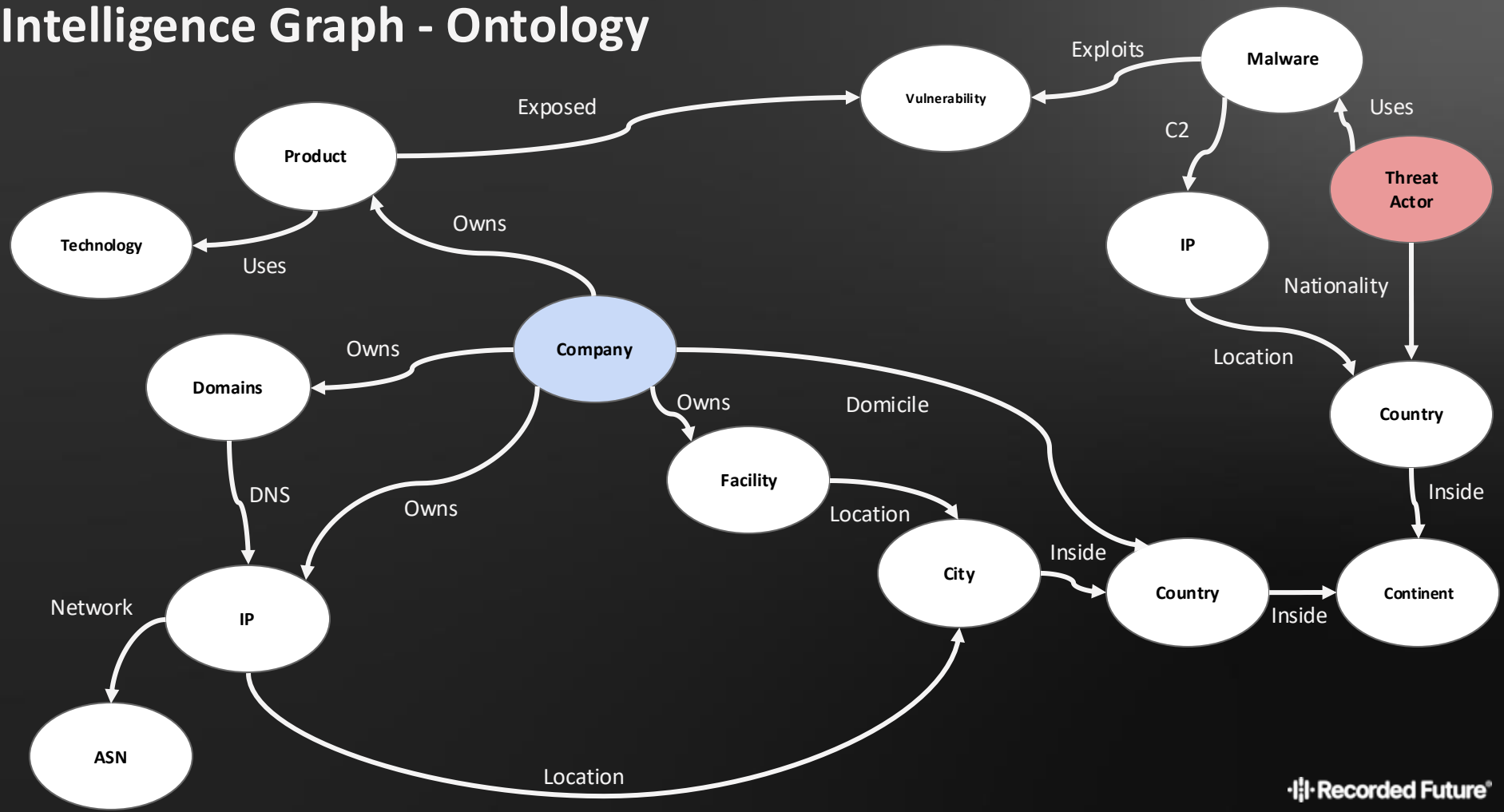
Building the World's Most Ambitious Intelligence Product:

- Largest Intelligence Graph and growing
- Integrated solution for automation of workflows and playbooks
- AI native for real-time, actionable insights

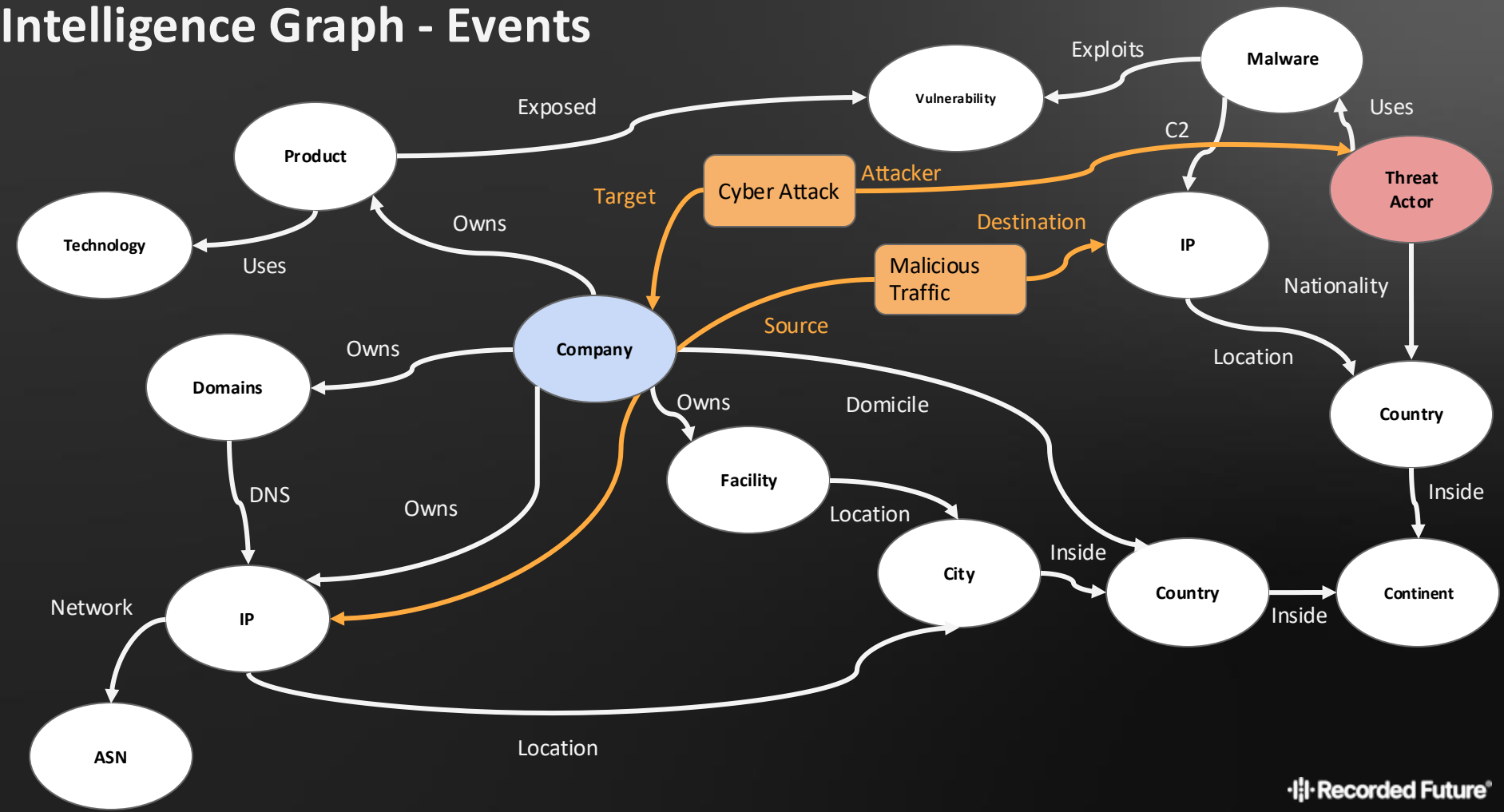


- Access to dark web forums and associated data
- Insikt Analyst Notes - human validated intelligence
- Machine validated intelligence

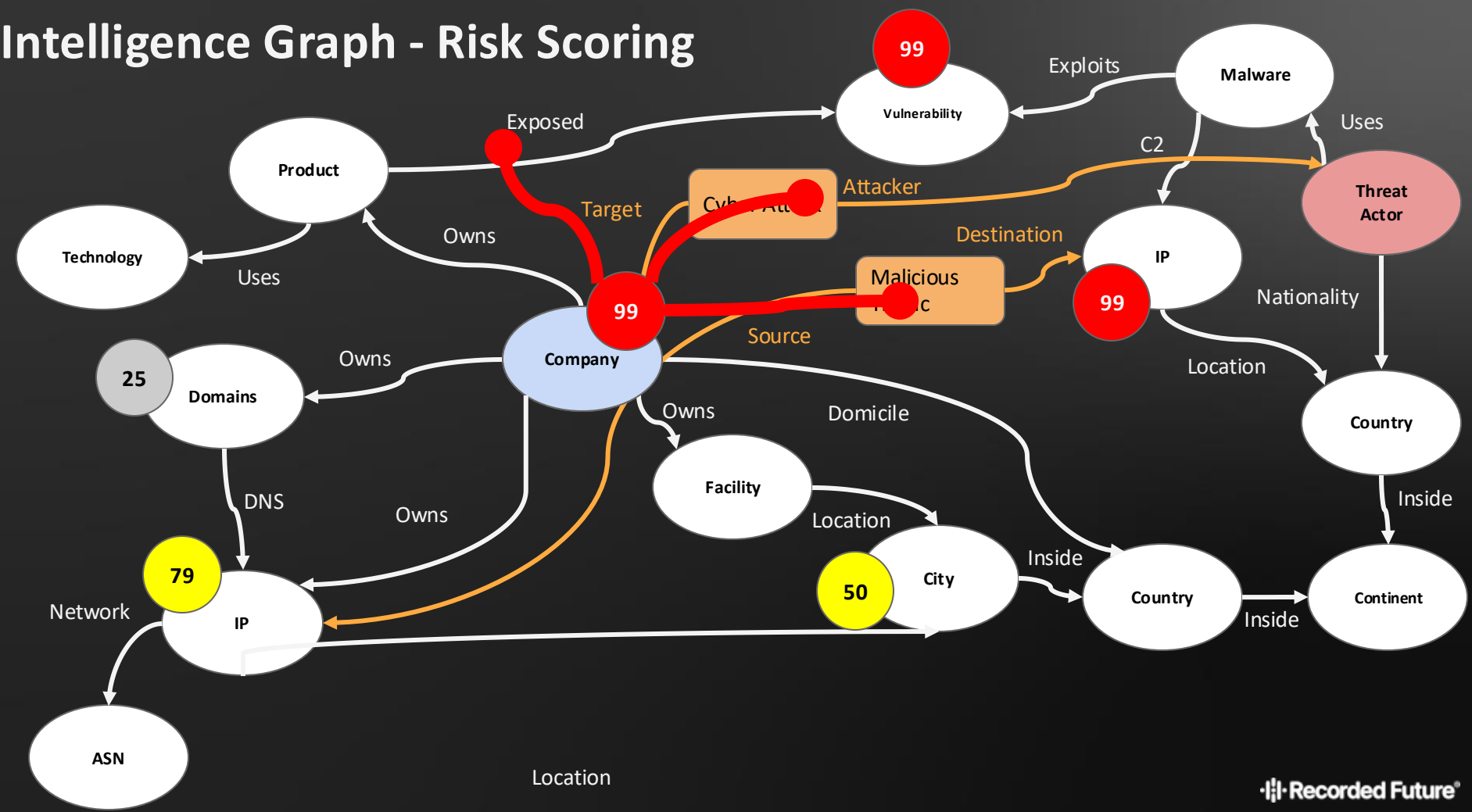
Intelligence Graph - Ontology




Intelligence Graph - Events



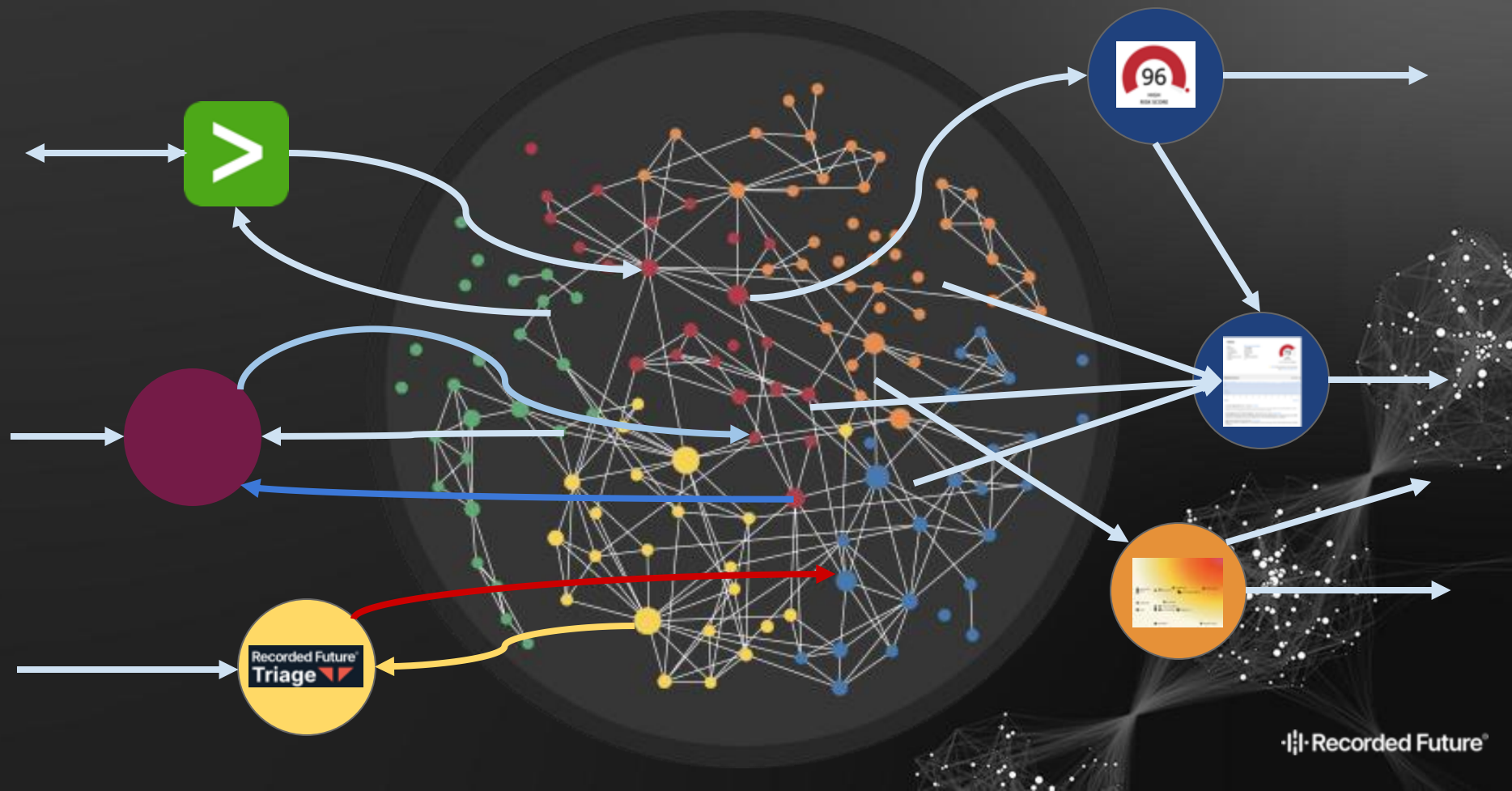
Intelligence Graph - Risk Scoring





**Intelligence Graph:
200B+ nodes, trillions of edges,
updated in real-time,
doubling in size every 24 months**

Autonomous Cooperating Intelligence Agents



ChatGPT

Notes
References
First Reference
Latest Reference
Curated

50 Insikt Group Notes
1 000 000+
Jan 25, 2023
Apr 17, 2024
★



7 of 14 Risk Rules Triggered

Show recent events or cyber events

Recorded Future AI Insights

Narrative View

Multiple reports indicate the exploitation of vulnerabilities associated with **Large Language Models (LLMs)** like **ChatGPT**, with examples such as the release of a proof-of-concept for data theft, the use of LLM-generated scripts in **phishing** campaigns targeting German organizations, and autonomous exploitation of one-day vulnerabilities by **ChatGPT-4**. Furthermore, there are indications of Russian-linked inauthentic news websites utilizing generative AI to produce divisive content targeting **US** audiences. Recorded Future's **Vulnerability Analysis** highlights medium and high/critical severity vulnerabilities (**CVE-2024-29090** and **CVE-2024-29100**) affecting **ChatGPT Chatbot 2.1.4**, with the former being exploited in a cyber exploit event.

Generated based on 7 Risk Rules | Analyst: Staffan Truvé

Share feedback?

5B+ Intelligence Cards Updated in Real-Time

TRIGGERED RISK RULES

Recently Reported by Insikt Group • 1 sighting on 1 source
Insikt Group. 1 report: **ChatGPT-4 Autonomously Exploiting One-Day Vulnerabilities**. Most recent link (Apr 17, 2024): <https://app.recordedfuture.com/portal/analyst-note/doc:vdJxNu>

Disclosed Vulnerability: High or Critical • 1 sighting on 1 source
Recorded Future Vulnerability Analysis. 1 high or critical severity vulnerability affecting this product has been disclosed: **CVE-2024-29100** (associated with **ChatGPT Chatbot 2.1.4**).

Recently Referenced by Insikt Group • 4 sightings on 1 source
Insikt Group. 4 reports including **TA547 Phishing Campaign Deploys Rhadamanthys Stealer Using LLM-Generated Scripts Targets German Organizations**. Most recent link (Apr 11, 2024): <https://app.recordedfuture.com/portal/analyst-note/doc:vU3e8n>

Linked to Recent Cyber Exploit • 1 sighting on 1 source
Recorded Future Vulnerability Analysis. Product is susceptible to 1 vulnerability mentioned in a recent Cyber Exploit event: **CVE-2024-29090** (associated with **ChatGPT Chatbot 2.1.4**).

Disclosed Vulnerability: Medium • 1 sighting on 1 source
Recorded Future Vulnerability Analysis. 1 medium severity vulnerability affecting this product has been disclosed: **CVE-2024-29090** (associated with **ChatGPT Chatbot 2.1.4**).

Historically Referenced by Insikt Group • 32 sightings on 1 source
Insikt Group. 32 reports including **Russian-linked Inauthentic News Websites Targeting US Audiences Almost Certainly Using Generative AI to Produce Divisive News Content**. Most recent link (Mar 07, 2024): <https://app.recordedfuture.com/portal/analyst-note/doc:uzDpAT>

Historically Reported by Insikt Group • 14 sightings on 1 source
Insikt Group. 14 reports including **Researchers Release PoC for Stealing Data from Large Language Models (LLMs) Like ChatGPT**. Most recent link (Mar 15, 2024): <https://app.recordedfuture.com/portal/analyst-note/doc:u5lvm>

Threat Intelligence

Overview

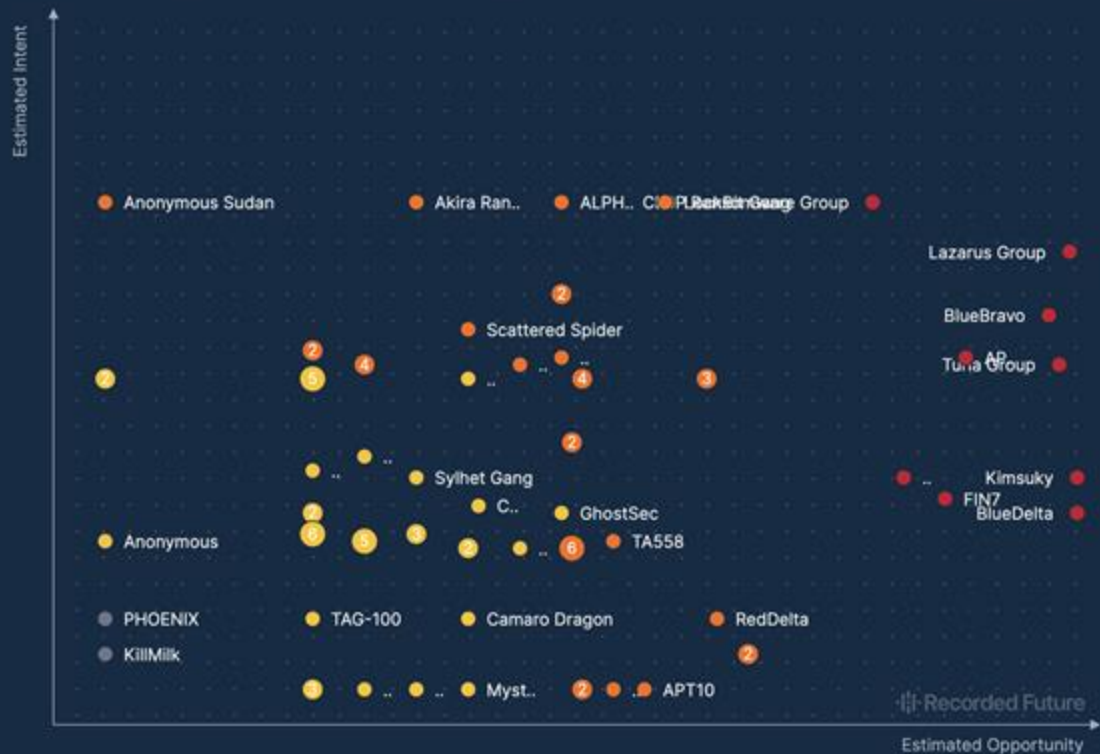
TTP MITRE Matrix

Threat Map displaying 90 Threat Actors relevant to Recorded Future

Change Over Time ☐

Filter by All Watch Lists Filter by All Threat Actor Categories

Date < May 27, 2024 >



Threat Maps Individualized for Each Customer in Real-Time

Threat Intelligence

Overview

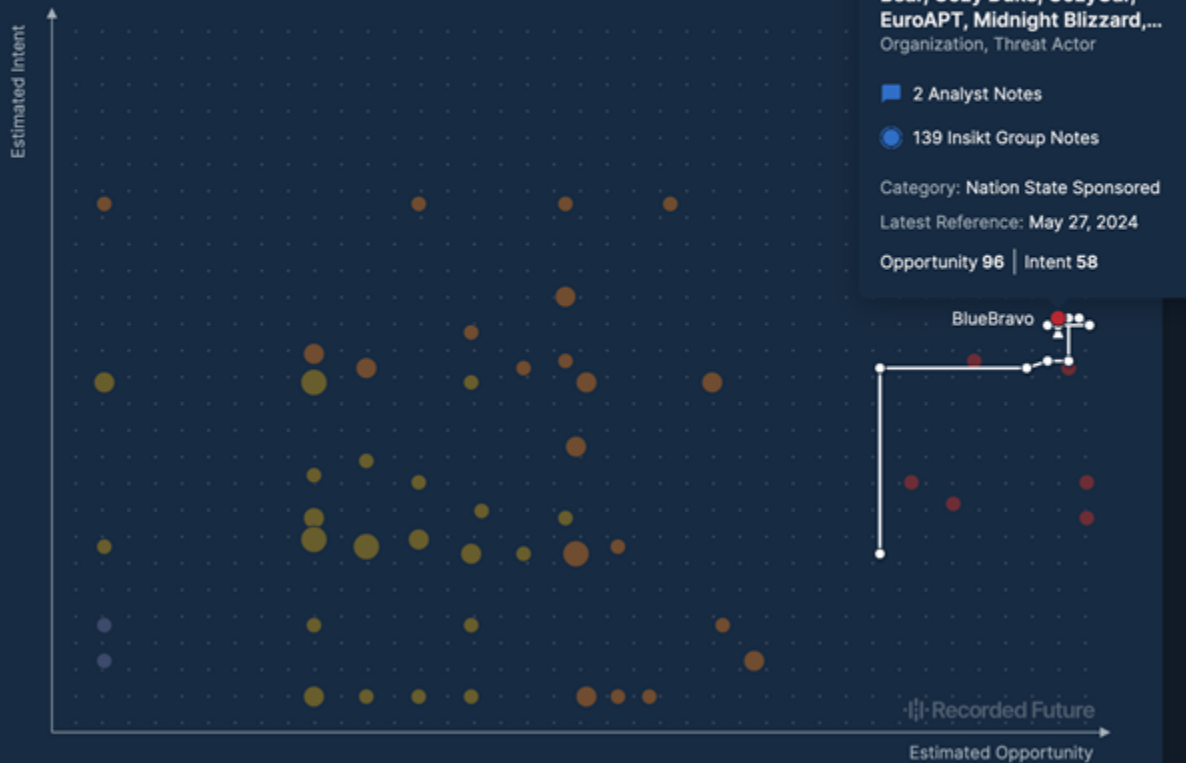
TTP MITRE Matrix

Threat Map displaying 90 Threat Actors relevant to Recorded Future

Filter by All Watch Lists

Filter by All Threat Actor Categories

Change Over Time



Track Threat Actors in Real-Time

Recorded Future AI Insights ?



The following information was generated from the evidence matching Recorded Future's Watch Lists:

BlueBravo, a threat actor with basic capability and a limited risk-level, has targeted various organizations including Microsoft, Cisco Systems Inc, and Bloomberg L.P. The actor has demonstrated a range of TTPs (Tactics, Techniques, and Procedures) such as T1071.004 (Application Layer Protocol: Web Protocols), T1036.005 (Masquerading: Match Legitimate Name or Location), and T1083 (File and Directory Discovery). BlueBravo's intent is assessed as basic to moderate, indicating potential motivations to target software companies and industry peers. The actor's opportunity assessment is high due to their capability in utilizing various techniques such as T1560 (Archive Collected Data) and exploiting vulnerabilities using methods like T1059.001 (Command-Line Interface). Furthermore, BlueBravo has shown the use of Slack Software as malicious infrastructure.

Generated based on BlueBravo

Share feedback?

Actions to Consider (14) for BlueBravo



Action	Details
Download Sigma Rule to run in SIEM ?	Suspicious Data Exfiltration
	Sigma Rule: Detect Malicious Shortcut used by BlueBravo
	Insikt Validated TTP: Hunting Brute Ratel C4
Download YARA Rule to run in EDR ?	YARA Rule: WINELOADER
	Insikt Validated TTP: Discussing Continued Sliver Abuse and Detecting Obfuscated Sliver.exe Beacons
	YARA Rule: Detect GraphicalQuark and Associated Droppers
	YARA Rule: Detect GraphicalElectron and related HTML Smuggling via SVG Files
	YARA Rule: Detect GraphicalProton
	YARA Rule: Detect QUARTERRIG Loader
	YARA Rule: Detect HALFRIG Loader

From Insights to Actions

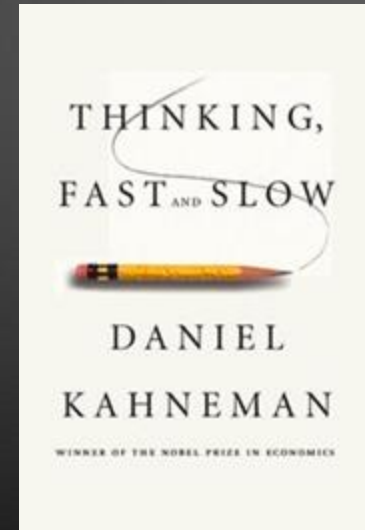
AI for Intelligence



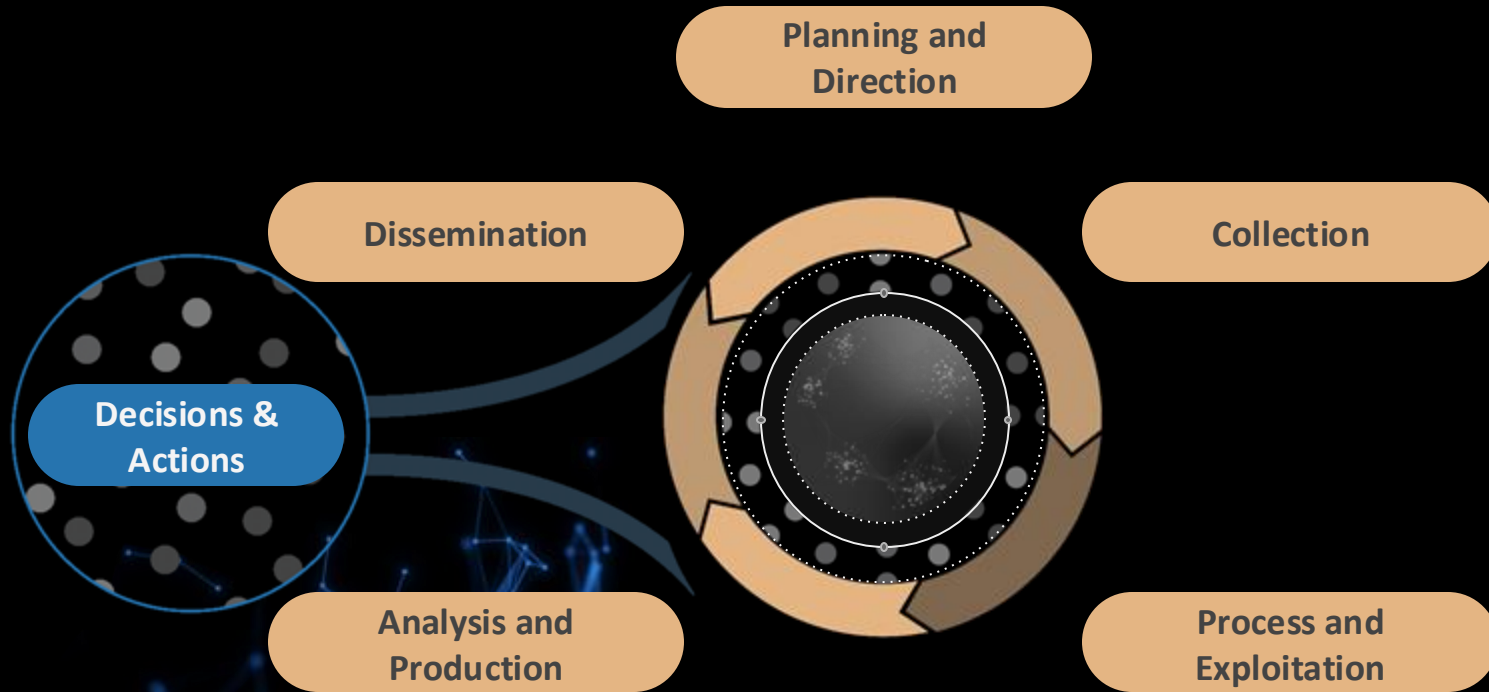
AI: Machine Learning *and* Rule Based!

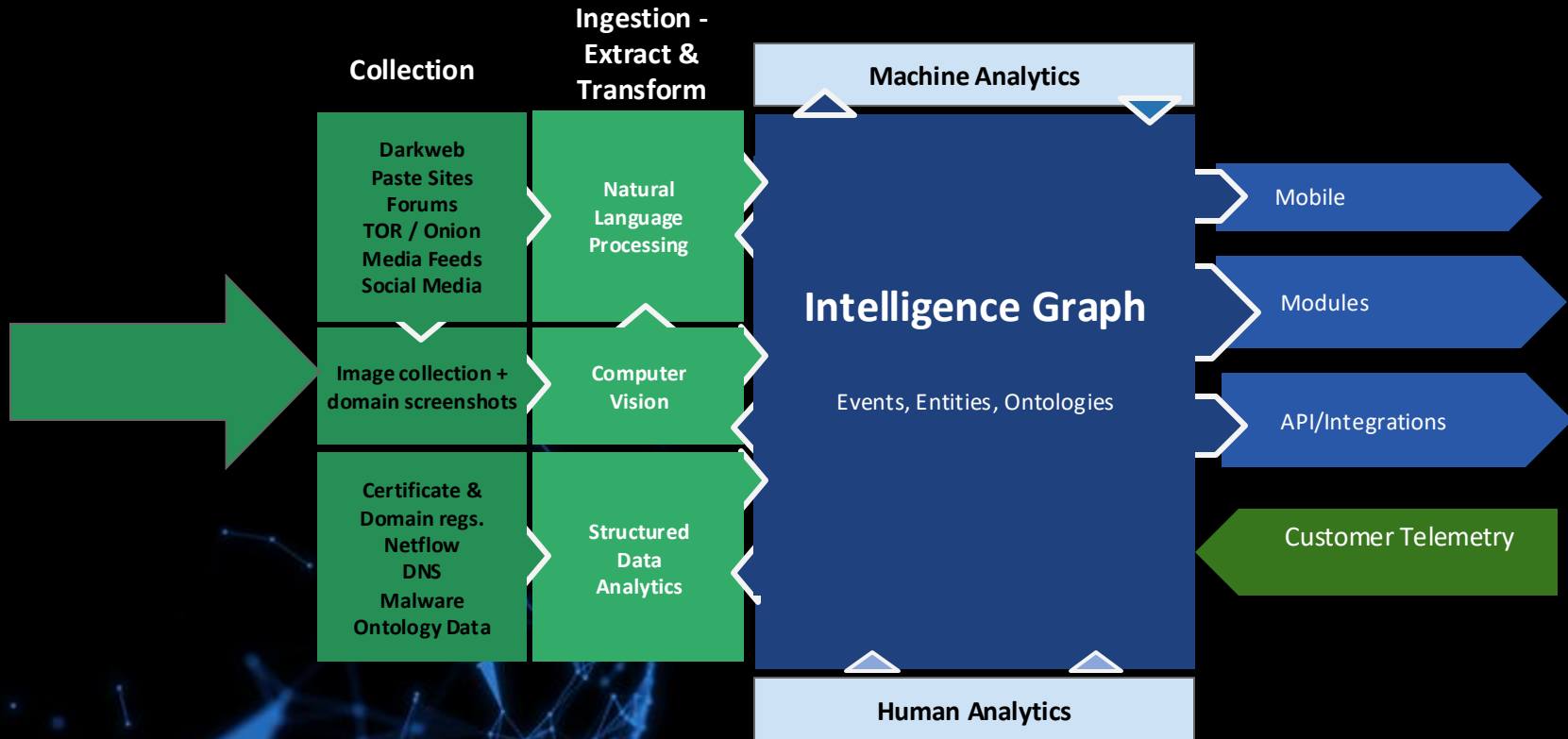
Rule based “reasoning system”
(System 2)
Logic reasoning

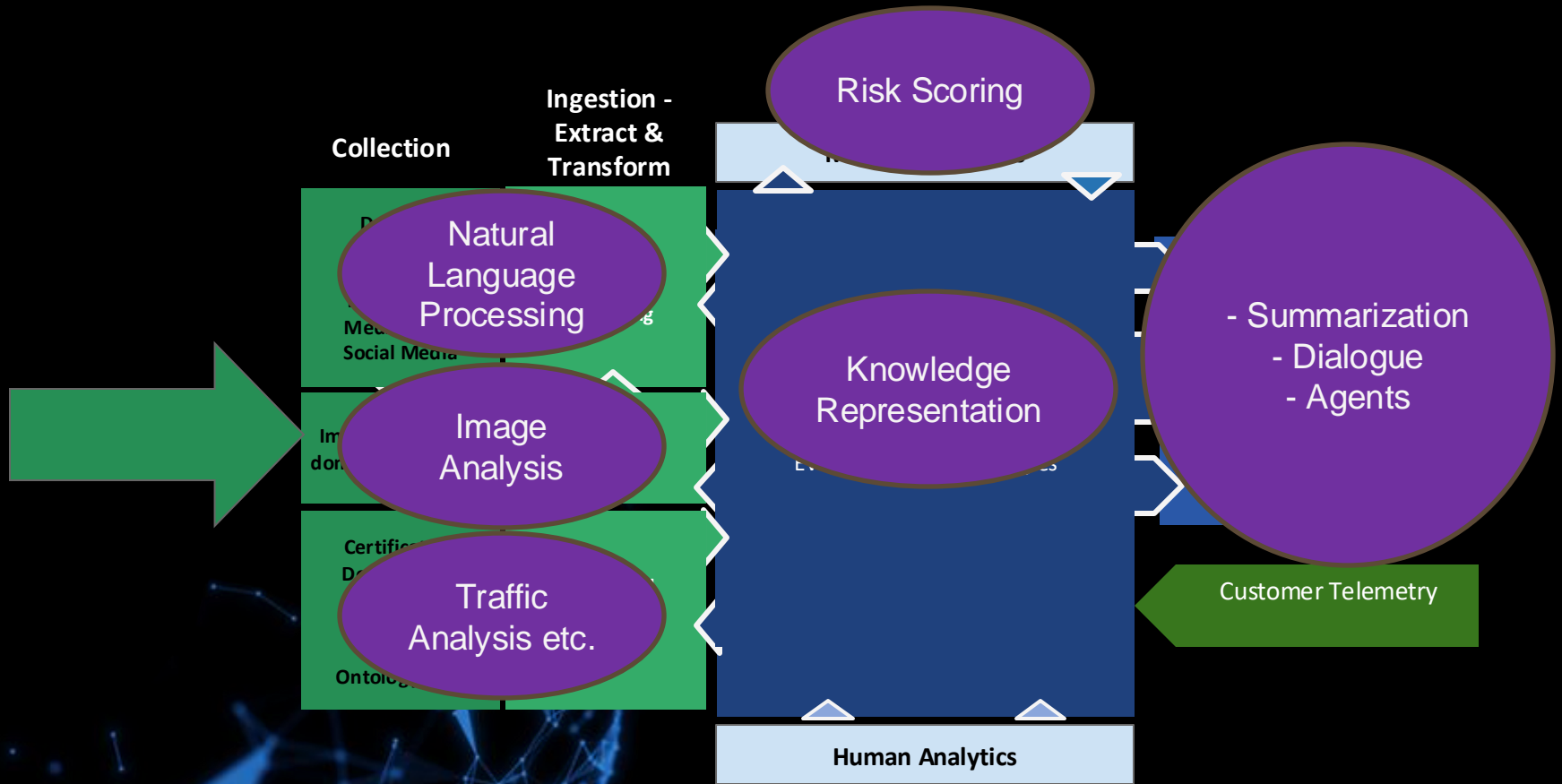
Machine learning based “perceptive system”
(System 1)
Classification/Categorization



Automating the Intelligence Cycle







The Four Phases of AI for Intelligence

- Phase 1: Organizing - Building the Intelligence Graph
- Phase 2: Summarizing – AI Insights
- Phase 3: Reasoning – AI Conversations
- Phase 4: Automating – AI Agents



Phase 1: Constructing the Intelligence Graph

Entity and Event Detection + Role Assignment

MAR 27 2024

Phishing Cyber attack against #japan, #Philippines, #Myanmar by RedDelta, Camaro Dragon in Asia-Pacific

From Twitter by @cytextsmb

@cytextsmb "Mustang Panda aka Camaro Dragon & Stately Taurus targeted #Myanmar, #Philippines, #Japan, & #Singapore. They use phishing emails to deliver malware packages designed to steal sensitive information. Insights into methods: Targeted timing 2/6 #asean50aus #panda."

From Twitter by @cytextsmb on Mar 27, 2024, 15:44

<https://twitter.com/cytextsmb/statuses/1773013121788998023> • Reference Actions • 1+ reference

CyberAttack
Attacker
Target
Method
Operation
RelatedEntities
...

Actor: Mustang Panda

Country: Singapore
Country: Myanmar
Country: Philippines
Country: Japan

Phishing

Temporal Analytics

JUL 21 2013 Facebook reported about
Cyber attack by India on Jul 21, 2013

“Three days ago, the official website of congress mouthpiece, monthly Hindi journal, 'Congress Yuva Sandesh', was hacked by 'Anonymous Kashmir' and it displays many 'messages' to India.”

Jul 24, 2013 17:23 Facebook Flag as inaccurate

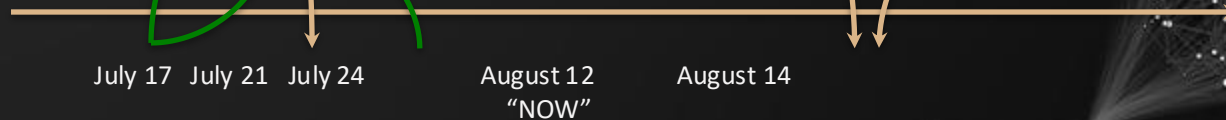
AUG 14 2013 Twitter and 1 more reported about
Cyber attack against India on Aug 14, 2013

“[@thamiltonatdell](#) Pakistani hackers plan on celebrating their Independence Day, 8/14, by launching cyberattacks against India <http://t.co/p341GTZN4D>.”

Jul 17, 2013 17:42 Twitter Flag as inaccurate

“Pakistani Hackers Threaten to Attack India on August 14.”

Jul 17, 2013 12:08 Team Cymru Internet Security News Flag as inaccurate



Beyond Words: Image Analytics


- Entity and event detection
- Image based localization
- Image similarity search

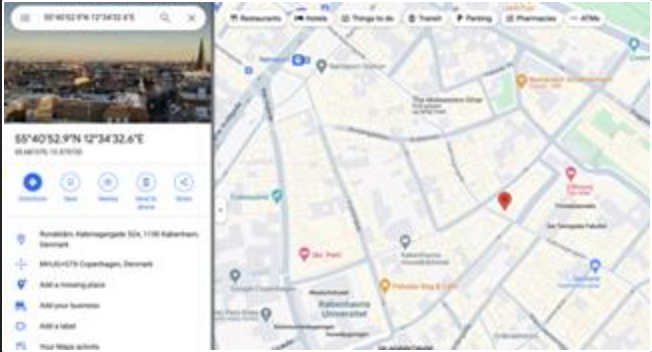
Denmark, Nasdaq OMX Copenhagen A/S and tohkasvazi_108 telegram group mentioned in Nordic

ТОЧКА СВЯЗИ МИРОВ

APR 17 2024

"Huge fire hits Copenhagen Stock Exchange building and part of historic tower collapses"
Source Telegram - Other Channels by tohkasvazi_108 on Apr 17, 2024, 02:10
Event positions [lat: 55.67610, lon: 12.56834](#)
Estimated image positions [lat: 55.68137, lon: 12.57572](#)
https://t.me/tohkasvazi_108/24435 • [Reference Actions](#) • 1+ reference













Recorded Future Enterprise

Search

Advanced

Images Similar To

https://www.slipstreamer.com/cms_media/module_img/815714078933_3_articlelarge_n27099672c3a459b960f63a73c22866.jpg.jpg
First Seen: Apr 18, 2024, 15:48
References: 22

<p>First Seen: Apr 18, 2024, 15:48 References: 22</p> 	<p>First Seen: Apr 20, 2024, 16:01 References: 2</p> 	<p>First Seen: Apr 18, 2024, 16:28 References: 0</p> 	<p>First Seen: Apr 18, 2024, 14:48 References: 2</p> 
<p>https://www.mercurymews.com/wp-cente... Similarity Score: 93.85% First Seen: Apr 20, 2024, 00:29 References: 32</p> 	<p>Undefined Similarity Score: 93.85% First Seen: Apr 18, 2024, 08:32 References: 6</p> 	<p>https://www.dagbladet.no/realzeit/4W/24... Similarity Score: 93.85% First Seen: Apr 18, 2024, 07:48 References: 16</p> 	<p>https://media.wolm.at/thumbs/c72/News... Similarity Score: 93.85% First Seen: Apr 16, 2024, 11:47 References: 23</p> 

Beyond Words: Image Analytics


- Images provide additional context to text
- OCR --> text analytics
- Logotype detection

<https://mail.bankofamericapp.com/>

Recorded Future

IMAGE

References 6



Show recent events or cyber events

ANALYST NOTES FROM RECORDED FUTURE

Create Analyst Note

IMAGE CONTENT

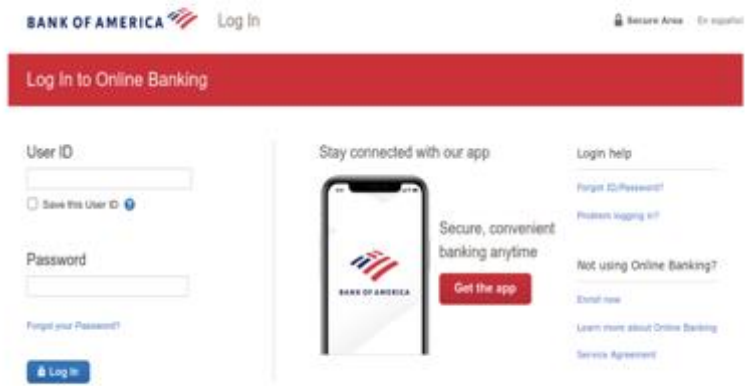
Entities detected in image 12

animation Technology 100 000+	Russia Country 1 000 000 000+
film Other organization 1 000+	Denmark Country 10 000 000+

IMAGE

URL <https://urlscan.io/screenshots/6bcb917d-2cab-4680-8746-f7b2abcb8445.png> Show recent events

References 19



BANK OF AMERICA Log In

Secure Area | En español

Log In to Online Banking

User ID

Save this User ID

Password

Forgot your Password?

Log In

Stay connected with our app

Secure, convenient banking anytime

Get the app

Login help

Forgot ID/Password?

Problem logging in?

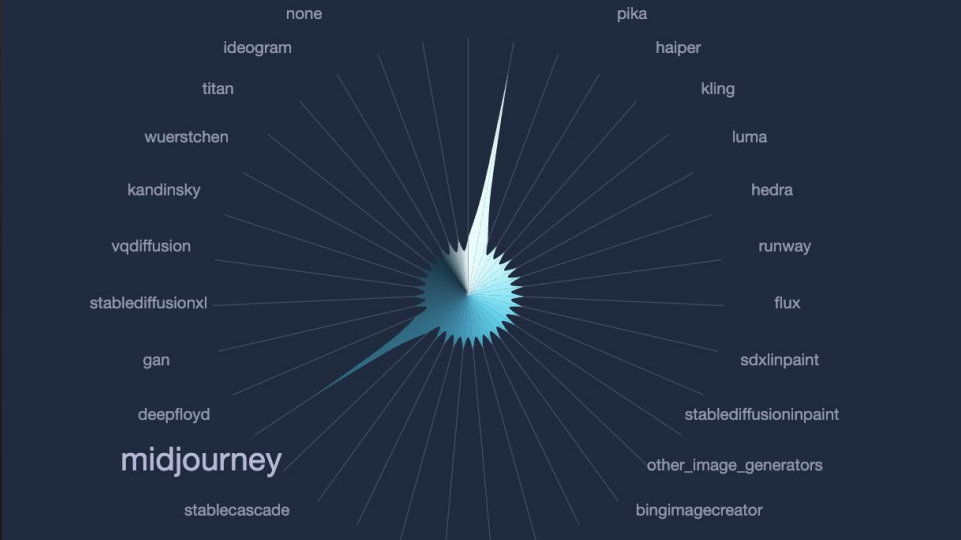
Not using Online Banking?

Email me

Learn more about Online Banking

Service Agreement

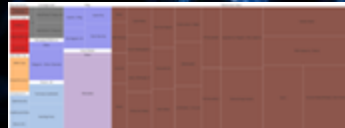
Beyond Words: AI generated image / deep fake detection



Phase 2: AI Insights

Event Type	Cyber Attack X
Attacker	Any attacker
Target	United Kingdom X
Operation	Any operation
Method	Any method
In Document	Any Company
Event Time	Last 30 Days X

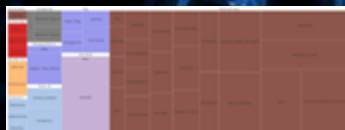
Real-time data



Phase 2: AI Insights

Event Type	Cyber Attack X
Attacker	Any attacker
Target	United Kingdom X
Operation	Any operation
Method	Any method
In Document	Any Company
Event Time	Last 30 Days X

Real-time data



Event Type	Attacker	Target	Operation	Method	In Document	Event Time
Cyber Attack	Any attacker	United Kingdom	Any operation	Any method	Any Company	Last 30 Days

**Recorded Future AI Insights**

Generated based on 100 references | Aug 27, 2023 - Sep 22, 2023 | Analyst: Staffan Truvé

UK's Greater Manchester Police has suffered a data breach after a third-party supplier responsible for ID badges was attacked. ¹ The personal data of 47,000 police officers may have fallen into the hands of organizations or terrorist gangs. ² Additionally, the UK's Ministry of Defense was targeted by Russian hackers who leaked thousands of top-secret documents online, potentially causing significant damage. ³ London's Metropolitan Police also experienced a security breach involving a third-party supplier that had access to sensitive information. ⁴ In another incident, UK voter data was hacked in an attack on an election watchdog. ⁵ Furthermore, there were reports of cyberattacks on UK schools and airlines, as well as a ransomware attack on a fencing systems maker impacting UK military data. ⁶



Top 3 Sources: [Twitter](#) [Telegram - Geopol](#) [National Cyber Security](#)

Share feedback?  

Recorded
Future AI
Insights

Source attribution

Attribution 3 of 21 References

"The police force also suffered a cyber supply chain incident when a third-party supplier responsible for ID badges was attacked, resulting in data compromise."

From Twitter by @InfoFinger

@InfoFinger Reports of 2 more real data breaches where the financial & personal data of officers in the Manchester & London Borough was hacked via a third-party. The data leaks in the police are obviously not up to the task of securing key systems from outside intrusion."

From Twitter by @InfoFinger on Sep 15, 2023, 16:25


<https://twitter.com/InfoFinger/status/1725222222222222222> - Reference Active

Translated from Russian: "Metropolice" (News) - InfoFinger

Translated from Russian: "Greater Manchester Police victim of espionage attack and data breach" - Cashed Newsagent

Source: Telegram - Cyber by Metacommune | Metacommune | NewsAgent on Sep 16, 2023, 18:59

<https://www.metacommune.org/en/19> - Reference Active




From Twitter by @InfoFinger

@InfoFinger Translated from Russian: "Major cyber attack on British police, personal data of 47,000 police officers compromised. They could have fallen into the hands of terrorist organizations or gangs." <https://t.me/InfoFinger/7>

From Twitter by @InfoFinger on Aug 27, 2023, 08:47

Received <https://t.me/InfoFinger/7> to twitter.com

<https://twitter.com/InfoFinger/status/1725222222222222222> - Reference Active



From Twitter by @InfoFinger, InfoSec

@InfoSec, InfoSec: Police are cyber victims and photos exposed in supplier breach. 47,000 Met Police officers and staff's personal accounts in breach in London's Metropolitan Police too and a third-party data breach exposed staff and officers' IT - #CyberSecurity #InfoSec <https://t.me/InfoFinger/7> <https://t.me/InfoFinger/7>

From Twitter by @InfoFinger, InfoSec on Aug 25, 2023, 14:21

Received <https://t.me/InfoFinger/7> to twitter.com





Received <https://t.me/InfoFinger/7> to twitter.com

<https://twitter.com/InfoFinger/status/1725222222222222222> - Reference Active



Recorded Future AI Insights

Generated based on 100 references | Aug 27, 2023 - Sep 22, 2023 | Analyst: Staffan Truvé

UK's Greater Manchester Police has suffered a data breach after a third-party supplier responsible for ID badges was attacked. ¹ The personal data of 47,000 police officers may have fallen into the hands of organizations or terrorist gangs. ² Additionally, the UK's Ministry of Defense was targeted by Russian hackers who leaked thousands of top-secret documents online, potentially causing significant damage. ³ London's Metropolitan Police also experienced a security breach involving a third-party supplier that had access to sensitive information. ⁴ In another incident, UK voter data was hacked in an attack on an election watchdog. ⁵ Furthermore, there were reports of cyberattacks on UK schools and airlines, as well as a ransomware attack on a fencing systems maker impacting UK military data. ⁶



Top 3 Sources: [Twitter](#) [Telegram](#) [Geopol](#) [National Cyber Security](#)

Share feedback?  

Pivot links

Greater Manchester Police

Notes: 2 main group focus
References: 100 000+
First Reference: Jun 20, 2016
Latest Reference: Sep 26, 2023
Location: United Kingdom
Curated: *

68

RISK SCORE



4 of 44 Risk Rules Triggered

View Third-Party Summary Report

Recorded Future AI Insights

Generated based on 100 references | Analyst: Staffan Truvé

The presented information includes the following cyber observables about Greater Manchester Police: a report indicating the presence of Conficker malware in the past, a slight increase in references over the last 60 days, the discovery of 270 distinct credentials with passwords in various documents, and a report on a data breach affecting UK law enforcement agencies, including Greater Manchester Police. These observables indicate potential vulnerabilities and security incidents that have occurred or may still be ongoing within Greater Manchester Police's digital assets. Such information could potentially be exploited by threat actors to orchestrate targeted cyber attacks against the organization in the future.

Share feedback?  

Metropolitan Police

Notes: 3 Insight Group Notes
References: 100 000+
First Reference: Jun 16, 2014
Latest Reference: Sep 20, 2023
Location: United Kingdom
Curated: *

66

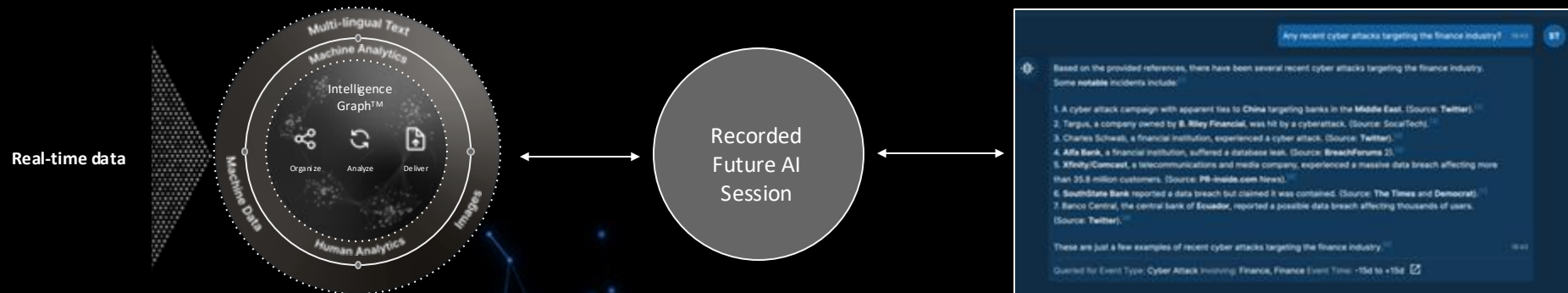
RISK SCORE

2 of 44 Risk Rules Triggered

View Third-Party Summary Report

Share recent events or cyber events

Phase 3: Conversational AI



have there been any cyber attacks on Swedish companies in the last 90 days?

18:52

ST



Based on the provided information, there have been cyber attacks on Swedish companies in the last 90 days.^[1] **TietoEVERY**, a Finnish IT software and services company, suffered a **ransomware** attack that affected several customers in **Sweden**.^[2] The attack led to widespread outages across **Sweden**, impacting healthcare, government services, retail outlets, and more.^[3] The attack was attributed to the **Akira ransomware group**.^[4] Additionally, several Swedish organizations fell victim to a wave of **ransomware** attacks, suspected to be carried out by **hacker** groups.^[5] The attacks disrupted services for thousands of businesses and government administrations.

18:52

Queried for Event Type: Cyber Attack Involving: Company, Sweden Event Time: -90d to today [🔗](#)

CyberAttack
Attacker
Target
Method
Operation
RelatedEntities

Sweden

Company

who else has been attacked by Akira? 18:53

ST



Based on the provided references, the following organizations have been attacked by the Akira ransomware group:^[1]

- Serfilco.
- RP Adams.
- Baron Blakeslee.
- Pac er.
- Service Filtration of Canada.^[2]
- Polymar.
- Consilux (Brazil).^[3]
- Studio LAMBDA.^[4]
- Myers Automotive Group.
- Lotz Trucking.
- Samart Corporation Public Company (Thailand).
- Sánchez-Betances, Sifre & Muñoz-Noya.
- Best Reward Federal Credit Union.^[5]
- Missouri Electric Cooperatives.^[6]

#5 Informed by 1 Reference

" - Best Reward Federal Credit Union"

#CyberAttack #USA: Best Reward Federal Credit Union allegedly compromised by Akira ransomware group The allegedly exfiltrated data includes personal information and financial documents, encompassing 1000's of members names, addresses, SSNs, emails, and phone nos.

#Ransomware

<https://t.co/KbzxSuU3MK>

Twitter | Apr 15, 2024, 09:34

#cyberattack #USA: Best Reward Federal Credit Union allegedly compromised by Akira ransomware group The allegedly exfiltrated data includes personal information and financial documents, encompassing 1000's of members names, addresses, SSNs, emails, and phone nos. **#ransomware** <https://t.co/KbzxSuU3MK>.

What are the encryption methods u...

How much ransom payment did the ...

What are the tools used by the Akir...

any recent vulnerabilities related to my tech watch list? 18:49

ST



Based on the provided references, there are several recent vulnerabilities related to the organization's tech watch list:^[1]

1. **CVE-2024-3400**: This is a critical **command injection** vulnerability in **Palo Alto Networks PAN-OS** software that is being actively exploited in the wild. It allows an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.^[2]
2. **CVE-2024-3273**: This vulnerability affects **D-Link NAS** devices and allows for remote **command injection**. It is actively being exploited in the wild.^[3]
3. **CVE-2024-21378**: This is a remote **code execution** vulnerability in **Microsoft Outlook** that is rated as critical. It allows an attacker to execute arbitrary code on the victim's system when activating a form in **Outlook**.^[4]

These are just a few examples of recent vulnerabilities that may be relevant to the organization's tech watch list. It is important to regularly update the watch list based on the latest vulnerabilities and advisories.^[5]

18:49

Queried for Event Type: Cyber Vulnerability and Exploit Involving: CyberVulnerability Event Time: -15d to +15d

Quantitative Analytics – Don't Use LLMs!

are any domains on my domain watchlist being spoofed or typosquatted as part of a phishing campaign? 21:21

ST



Based on the given information, we can see that there are several domains on the **Recorded Future Enterprise's** domain watchlist that are being typosquatted.

The domains with the highest number of typosquats are as follows:

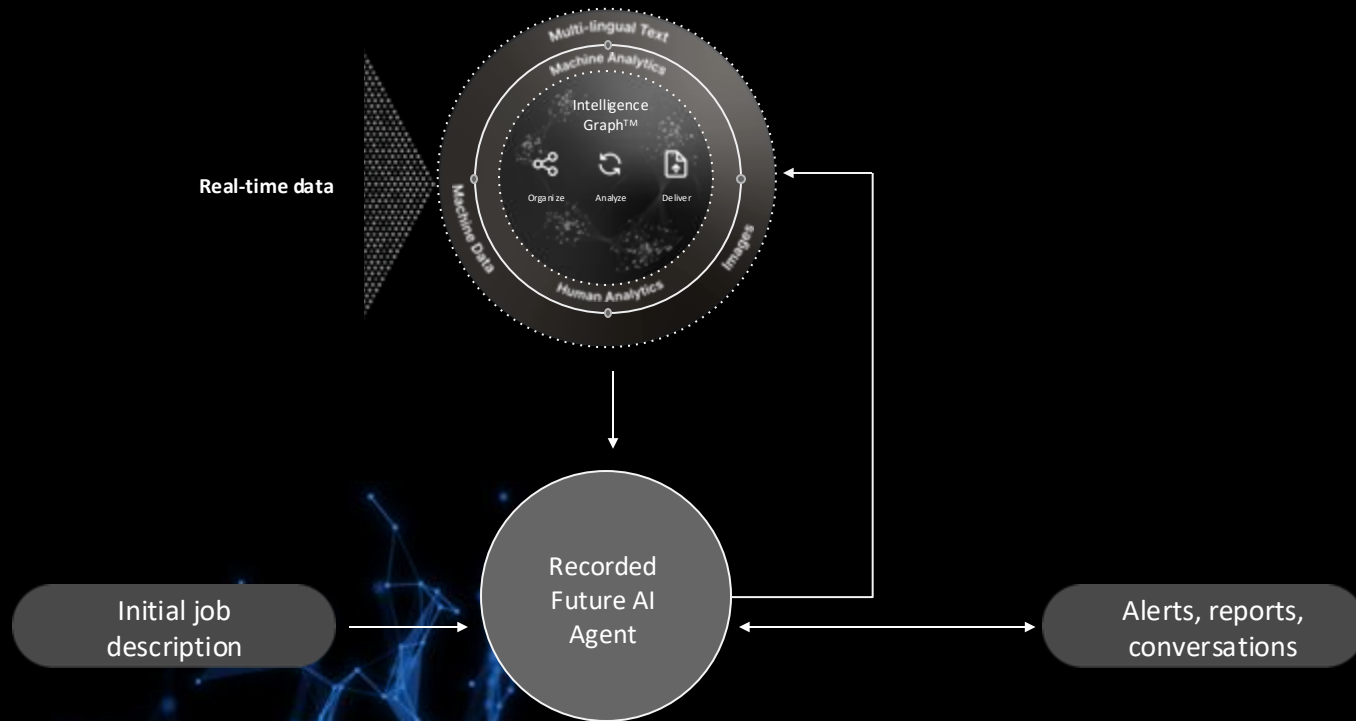
1. **Adobe.com** - 6728 typosquats.
2. **Microsoft.com** - 3255 typosquats.
3. **Apple.com** - 3089 typosquats.
4. **Amazon.com** - 2664 typosquats.
5. **Capitalone.com** - 1290 typosquats.
6. **Target.com** - 1281 typosquats.
7. **Wellsfargo.com** - 1281 typosquats.
8. **Questdiagnostics.com** - 1239 typosquats.
9. **Delta.com** - 1213 typosquats.
10. **United.com** - 1204 typosquats.

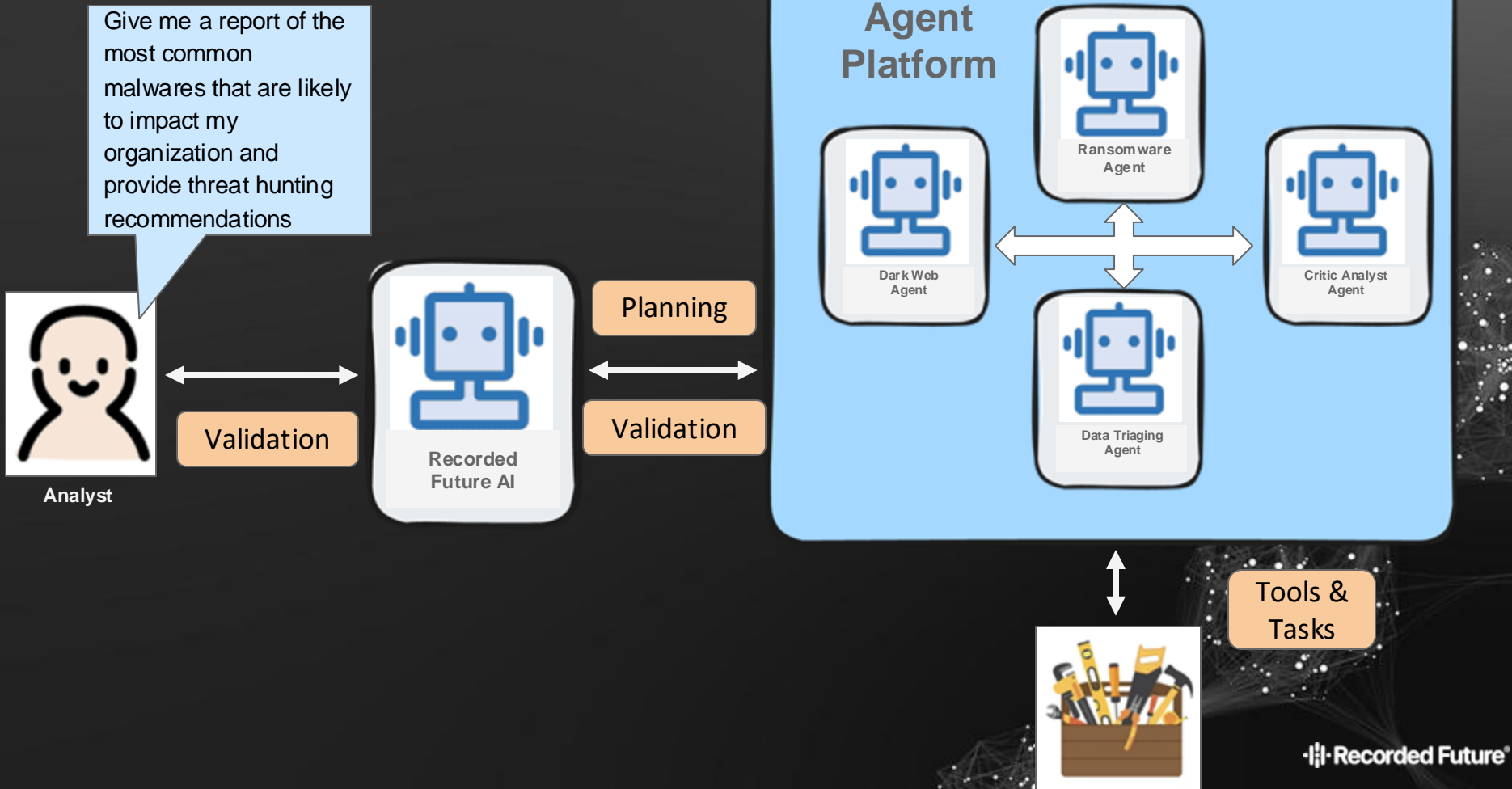
These statistics indicate that these domains are being actively targeted for **typosquatting**, which can be a technique used in **phishing** campaigns.

Additionally, the most mentioned entities in the references are **Microsoft.com**, **IBM.com**, **Verizon.com**, **Amazon.com**, **Comcast.com**, **ATT.com**, **Nike.com**, **Cisco.com**, **HP.com**, and **Dell.com**.

Overall, based on the information provided, it is highly likely that domains on **Recorded Future Enterprise's** domain

Phase 4: Autonomous AI Agents







Recorded Future AI

New AI Conversation



History



Weekly Ransomware Report



My Scheduled Reports



Today

Weekly Ransomware Report NEW

What are some known attack vector...



Jul 27, 2023

List 10 newly discovered CVEs in Mic...
Will be removed Aug 2, 2024What is the latest news on Chinese...
Will be removed Aug 2, 2024

Weekly Ransomware Report

Analysed Time Period: May 24, 2024 - May 31, 2024 | Analyst: Adam Green

Executive Summary

- Financial Industry Risks:** The financial industry has experienced significant operational disruptions and regulatory risks due to ransomware attacks and hacktivist groups. These incidents have led to financial losses and brand impairment. Financial regulators are now scrutinizing companies' failure to report ransomware attacks.^[1]
- State Security and Business Risks in China:** China's Ministry of **State Security** (MSS) has highlighted threats to national security from various business sectors. The MSS emphasizes the need for businesses to strengthen industry supervision, and vigilance against espionage and state security risks. Consulting firms and international companies with close relations to foreign governments are under scrutiny.^[2]
- Cyber Vulnerabilities and Exploits:** There are reports of various cyber vulnerabilities and exploits, including zero-day vulnerabilities in **Fortinet's FortiOS** and **FortiProxy SSL-VPN**. These exploits pose a significant risk to system security and data integrity.^[3]
- Supply Chain Attacks:** Supply chain attacks have become more frequent and severe, posing a risk to the organization's supply chain integrity. These attacks can result in compromised systems, data breaches, and potential financial losses.^[4]
- Cyber Threat Intelligence:** The presence of a cyber threat intelligence organization indicates active monitoring and analysis of potential threats. This suggests a proactive approach to identifying and mitigating risks.^[5]

It is important for the organization to remain vigilant and implement robust cybersecurity measures to protect against these threats and vulnerabilities. Regular monitoring, vulnerability patching, and employee training are essential to maintain the security and integrity of the organization's systems and data.^[6]

Credential Leaks & Domain mentions

Here are the credential leaks targeting your domains in the past 2 weeks along with the source or specific forum where the leaks were detected:

- BobbinEye@Comcast.com** - Detected source: Recorded Future
- dahalc9@gmail.com** - Detected source: Recorded Future

< 1 of 4 >

Schedule Report

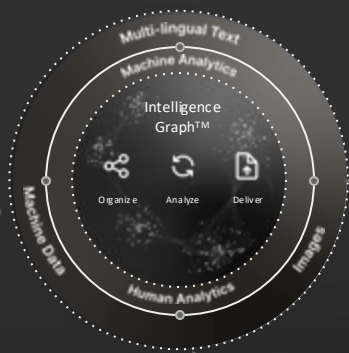


Ask a question. Use my/our, or the ? symbol to call out Watch Lists.



Delete All History

Real-time data

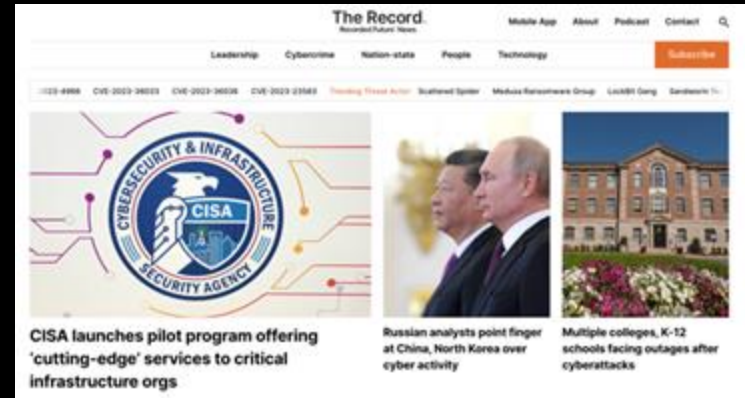


Reading tips

<https://therecord.media/>

<https://therecord.media/podcast>

<https://go.recordedfuture.com/cyber-daily>





*The best way to predict the
future is to invent it!*

(Alan Kay, Dynabook, 1968)

Staffan Truvé, Co-founder & CTO
truve@recordedfuture.com

