

KnowBe4



AI Driven OSINT

Recon 2.0: In the hands of
Cybercriminals

James R. McQuiggan, CISSP, SACP
Security Awareness Advocate



Cybercriminals are weaponizing
AI & OSINT to discover organizational
vulnerabilities faster than
defenses can be established.

“
Penetrating a company's security often starts with information that **seems so innocent**, so everyday and unimportant, that most people don't see why it **should be protected.**”

– Kevin Mitnick



**By integrating AI-driven OSINT,
organizations can defend against
advanced threats.**

James R. McQuiggan, CISSP, SACP, OSC

Security Awareness Advocate, KnowBe4 Inc.

Producer, Security Masterminds Podcast

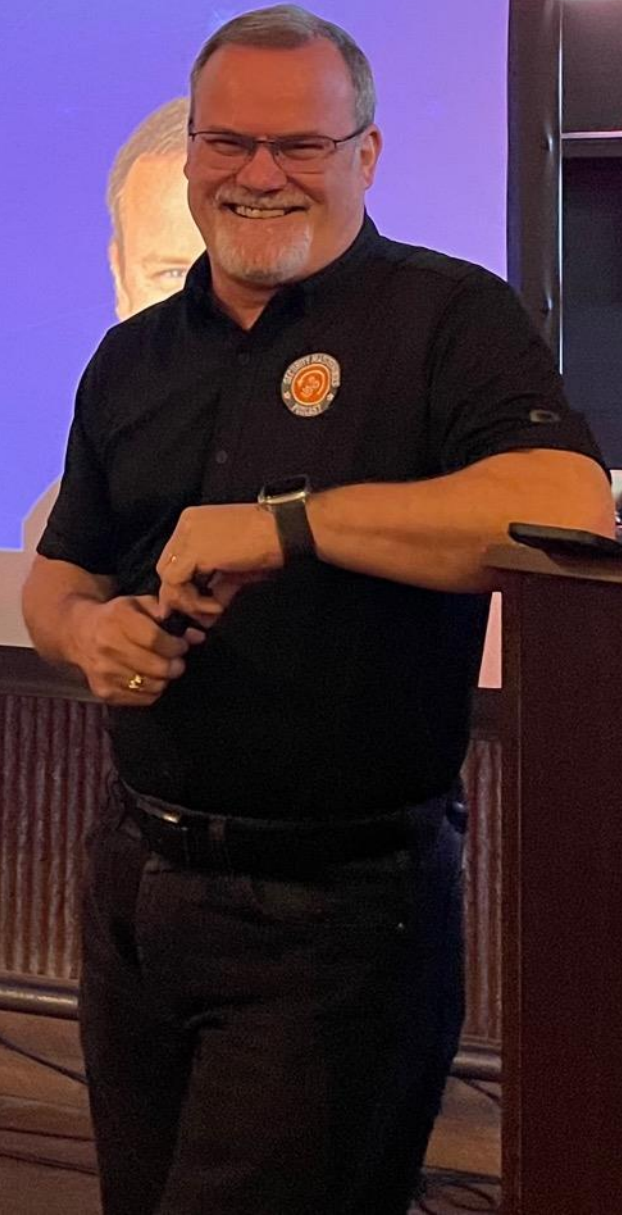
Professor, Cyber Threat Intelligence, Full Sail

President, ISC2 Central Florida Chapter

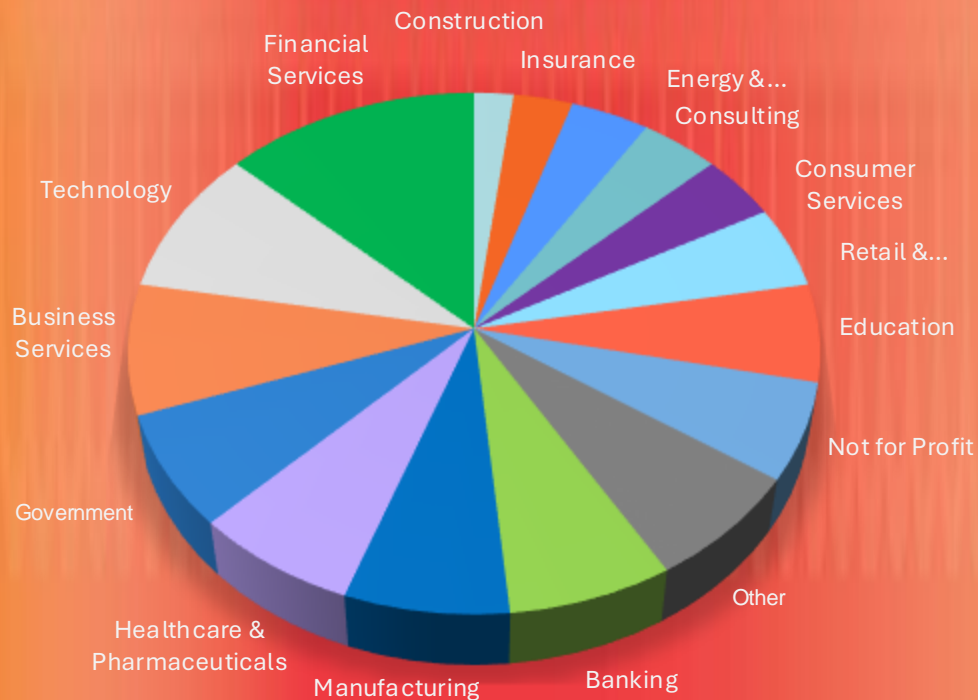
ISC2 North American Advisory Council

Cyber Security Awareness Lead, Siemens

Product Security Officer, Siemens Gamesa



Over
70,000
Customers



About KnowBe4

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

Our mission

To help organizations manage the ongoing problem of social engineering

We do this by

Empower your workforce to make smarter security decisions every day.

AI + OSINT = Proficient Tools or Efficient Cybercriminals?

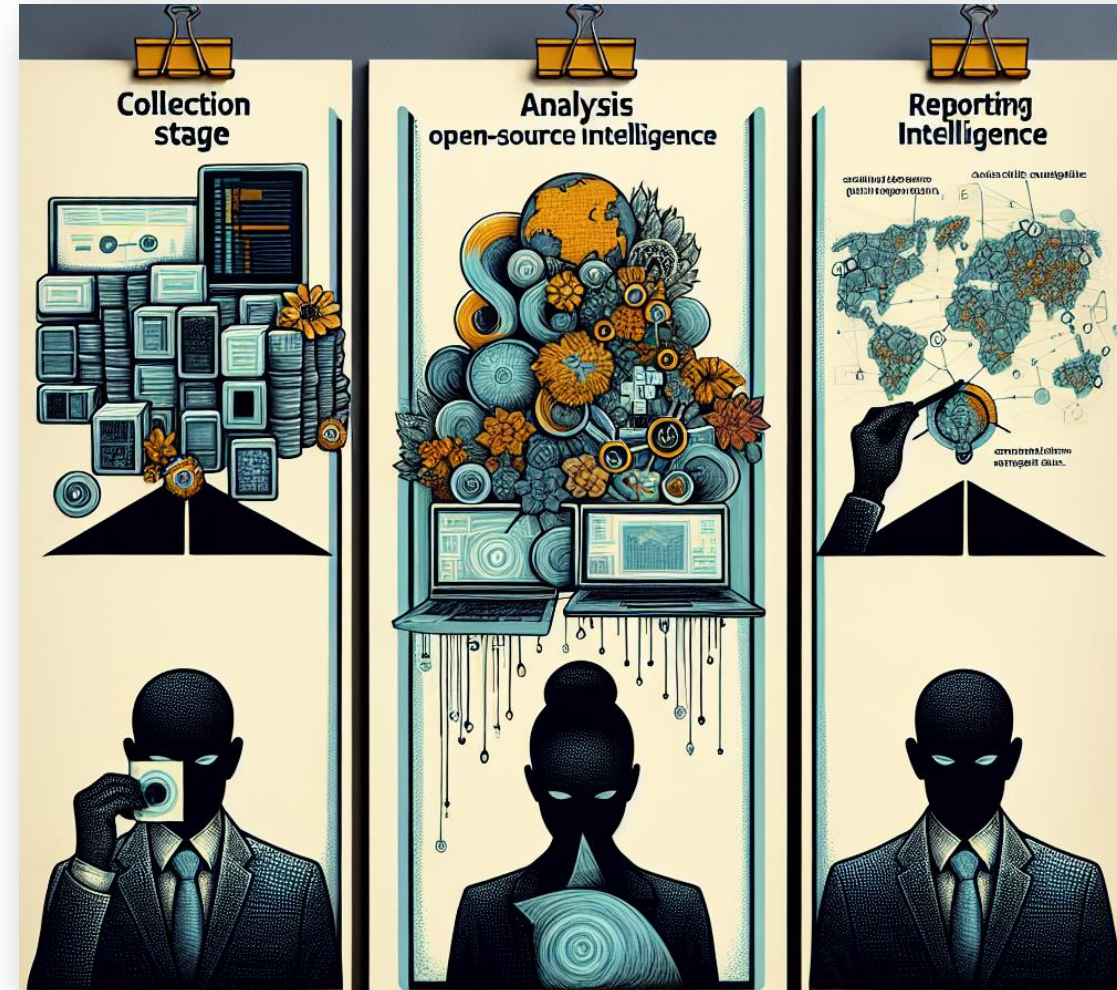
How AI &
OSINT are
working
together

Understand how
cybercriminals
are leveraging AI
for the OSINT
Recon

Develop AI
strategies and
OSINT
procedures
for protecting
the organization

Agenda

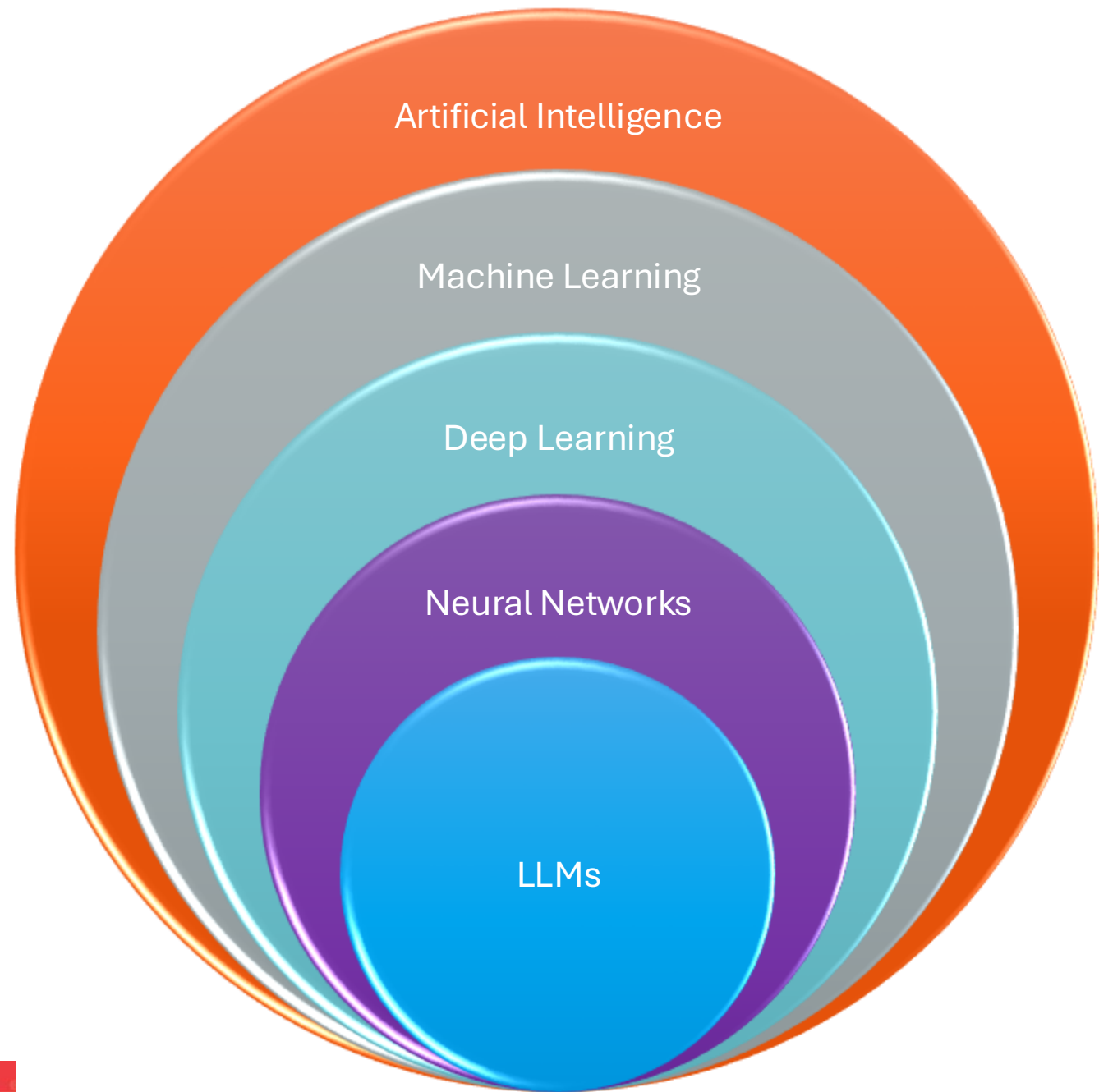
- AI & OSINT Review
- OSINT + AI Collection
- OSINT + AI = Attack Vectors
- Protection & Defense
- Wrap-up



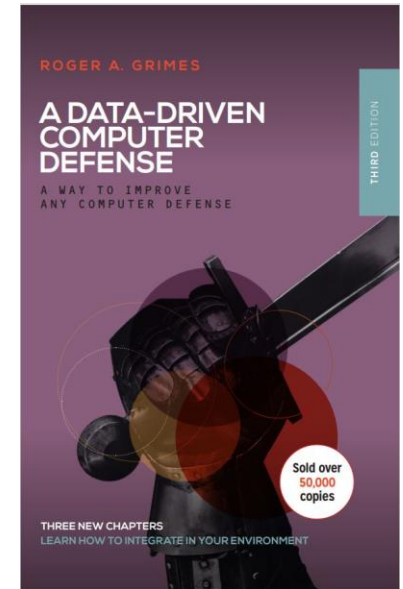
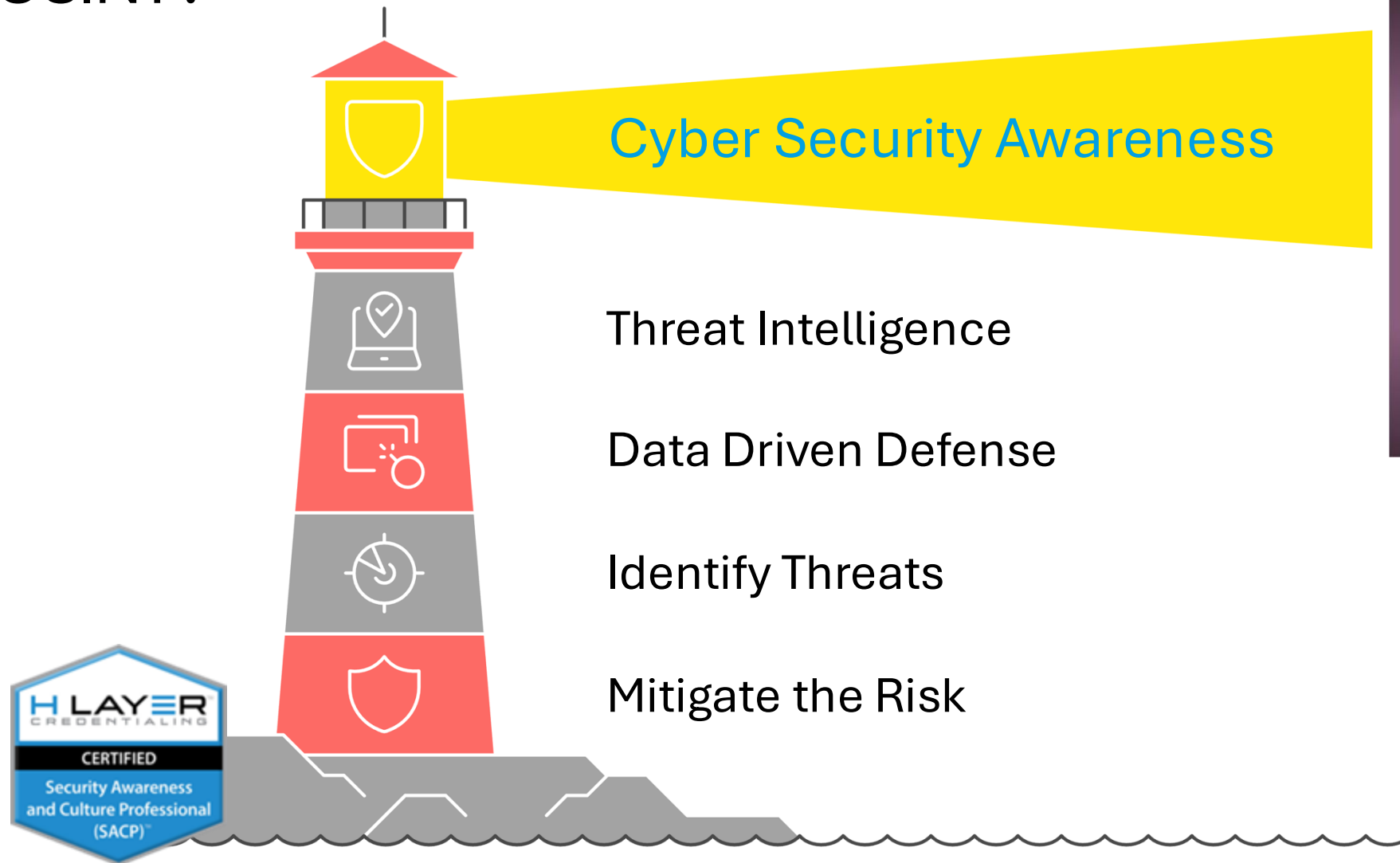
KnowBe4

AI & OSINT

Artificial Intelligence



Why OSINT?



Various Intelligence Methods

Human Intelligence

Relies on interpersonal interactions and human sources for information.

Open Source Intelligence

Involves gathering information from publicly available sources.

Social Media Intelligence

Analyzes data from social media platforms to gather insights.

Threat Intelligence

Focuses on identifying and mitigating potential threats to security.

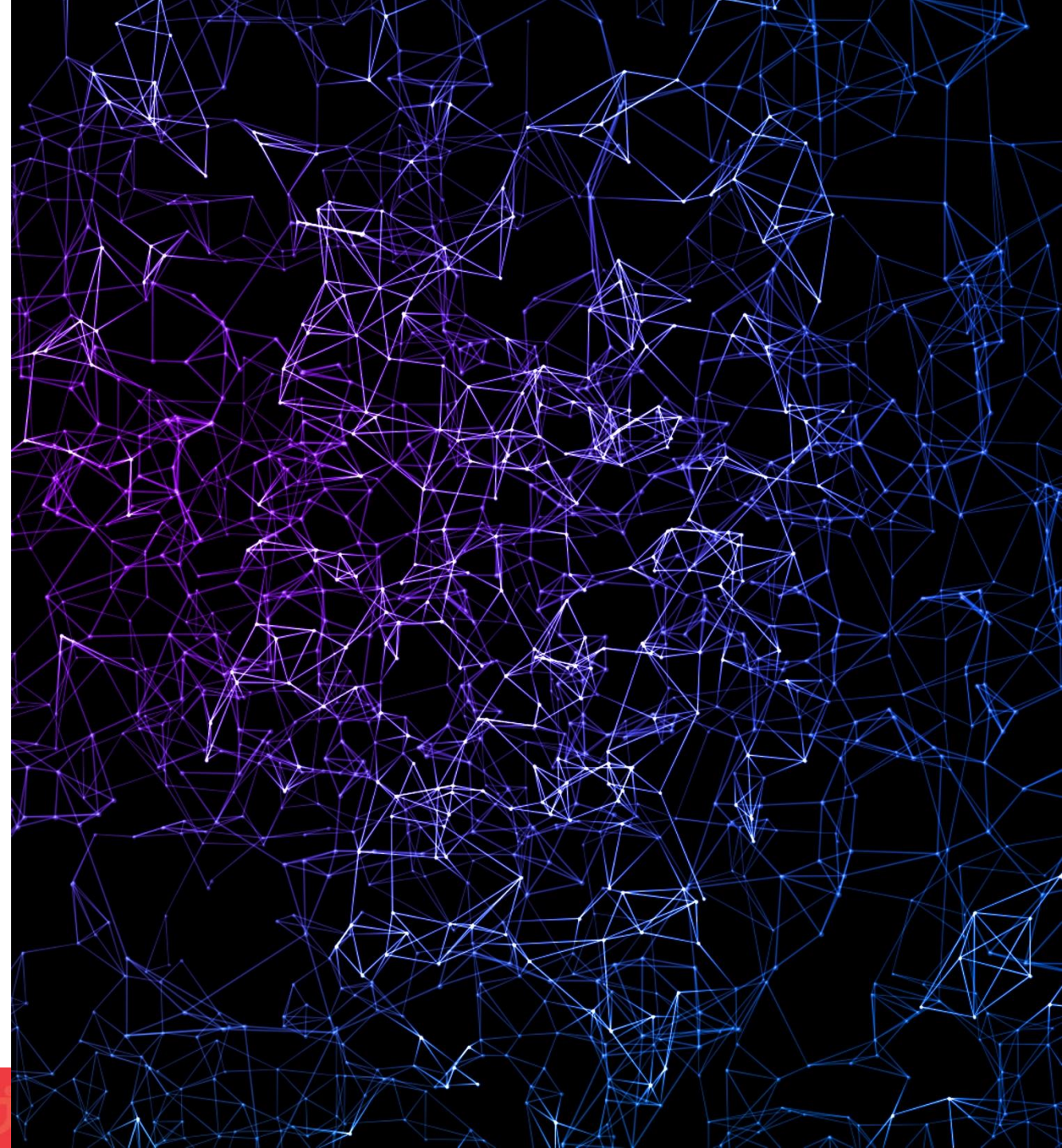
Geolocation Intelligence

Utilizes geographic data to understand and analyze locations.

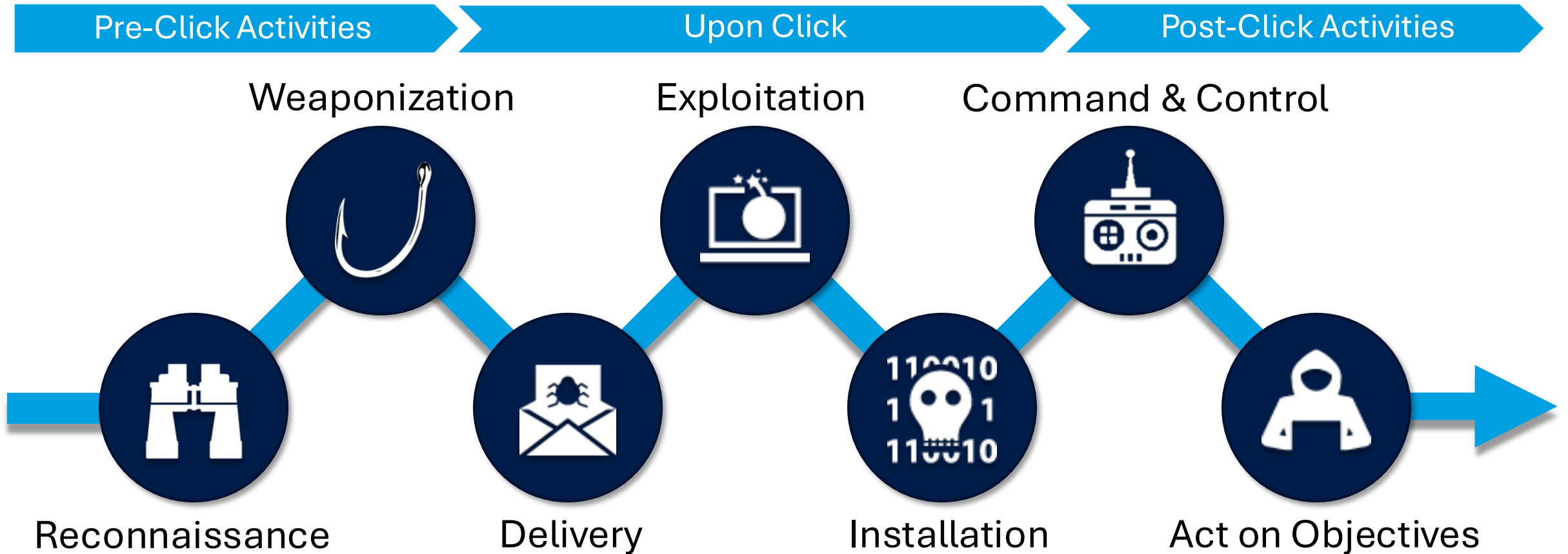


Open-Source Intelligence

- Publicly available information that any member of the public could lawfully obtain by request or observation
- Other unclassified information that has limited public distribution or access
- Media such as audio, video and pictures
- Text from documents, articles and blogs
- Maps and geolocation of data
- Social Media



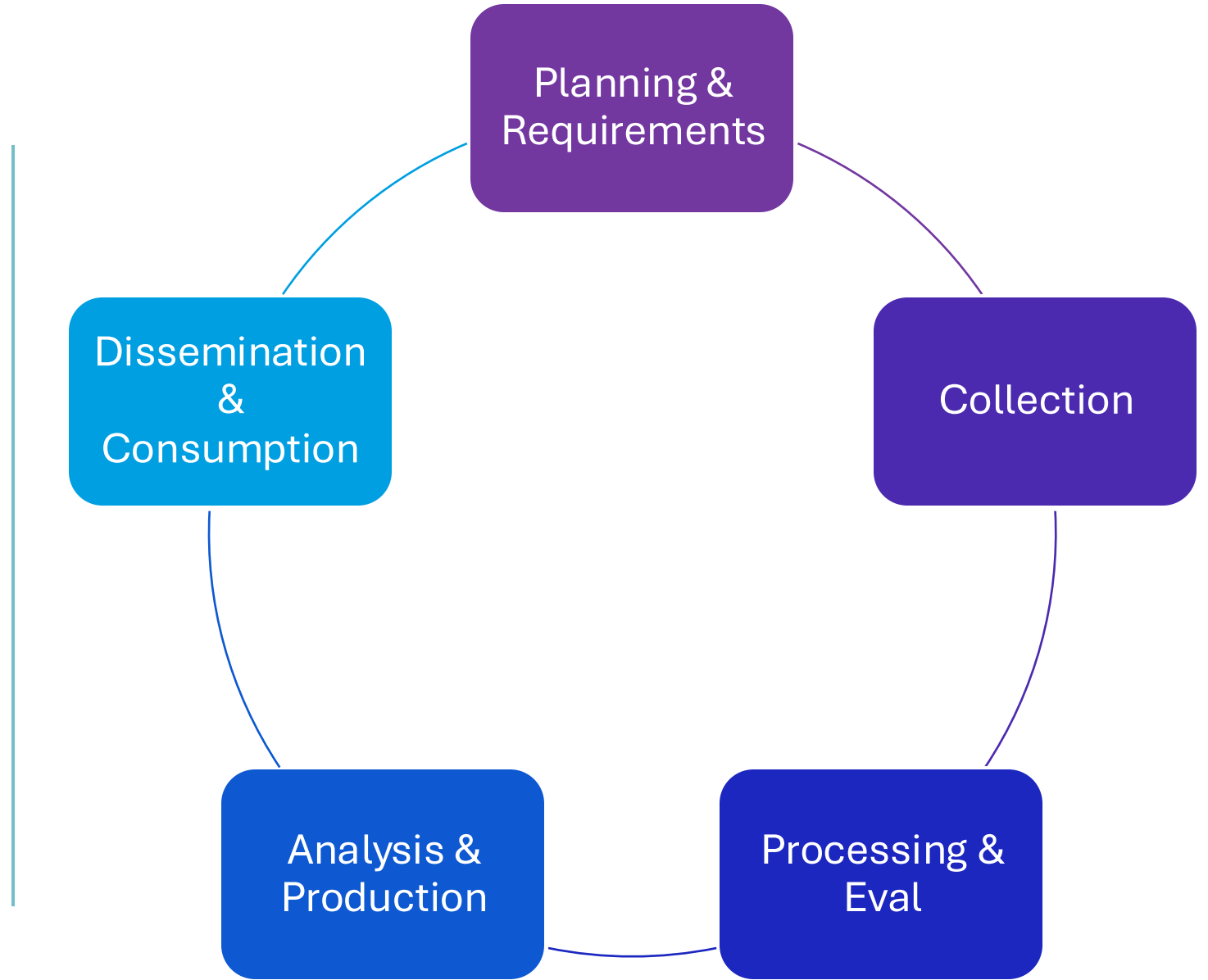
Cyber Kill Chain Process - Intelligence





Reconnaissance

Intelligence Process



**How can AI support the stages
intelligence gathering and analysis?**

KnowBe4

OSINT Collection + AI

Collection



Data Collection and Analysis

- AI optimizes data collection
- Web Crawling / Scraping
- OSINT Framework
- Google Dorking
- LLMs
- Geolnt
- Shodan



Google Dorking 101

- Cache - find out what the most recent cache of a specified webpage
- Allinurl - find pages with your requested search terms within the URL in internal search pages
- Filetype – search for specific file, like .docx, pdf, jpg
- Inurl - finding sites with strong on-page optimization for the topics you are researching in the URL link
- Intitle – the word is in the title of the page - a narrower operator that will help you find more targeted results



Results from ChatGPT Google Dorking Queries

Create a series of Google Dork Queries to search for information about my organization.

1. Finding Documents

- To find specific document types (PDFs, Word documents) on your domain:

```
plaintext
site:yourcompany.com filetype:pdf
site:yourcompany.com filetype:doc OR filetype:docx
site:yourcompany.com filetype:xls OR filetype:xlsx
```

Replace `yourcompany.com` with your organization's domain to find accessible documents on your site.

2. Exposed Login Portals

- To locate potential login portals associated with your organization:

```
plaintext
site:yourcompany.com inurl:login
site:yourcompany.com inurl:admin
site:yourcompany.com inurl:portal
```

3. Publicly Exposed Email Addresses

- To find email addresses associated with your organization:

```
plaintext
site:yourcompany.com "@yourcompany.com"
```

Replace `@yourcompany.com` with your organization's email domain. This query finds publicly exposed email addresses.

4. Configuration Files

- Some websites may accidentally expose configuration files that could contain sensitive information:

```
plaintext
site:yourcompany.com filetype:cfg
site:yourcompany.com filetype:conf
site:yourcompany.com filetype:env
```

Warning: These files may include sensitive information, so take precautions when reviewing results.

5. Finding Exposed Directories

- To check if there are open directories on your website:

```
plaintext
site:yourcompany.com intitle:"index of"
```

This can reveal directories that may not be intended for public access.

6. Searching for Subdomains

- To find subdomains of your organization's main domain:

```
plaintext
site:*.yourcompany.com
```

This helps identify various subdomains, such as staging environments or development sites, which may not be secured like the main site.

7. Sensitive Information in Error Messages

- To locate error messages that could leak system details or sensitive information:

```
plaintext
site:yourcompany.com "error" OR "warning"
```


Shodan Queries

Results from ChatGPT Shodan Queries

Create a series of Shodan queries to help search for equipment associated with my organization connected to the internet.

1. IP Range Search

- If you know your organization's IP range, you can use it directly in a Shodan query:

```
plaintext
net:"YOUR_ORG_IP_RANGE"
```

Replace `YOUR_ORG_IP_RANGE` with the actual IP range (e.g., `192.168.1.0/24`).

2. Domain Search

- To find devices with hostnames or domains associated with your organization:

```
plaintext
hostname:"yourcompany.com"
```

Replace `yourcompany.com` with your organization's domain.

3. SSL Certificate Search

- For servers and devices using SSL certificates associated with your organization:

```
plaintext
ssl:"yourcompany.com"
↓
```

4. Organization Name Search

- For devices registered under your organization's name:

```
plaintext
org:"Your Organization Name"
```

Replace `"Your Organization Name"` with your company's registered name in the Shodan database.

5. Port-Specific Searches

- To search for devices using specific ports, combine the port number with other search criteria:

```
plaintext
hostname:"yourcompany.com" port:22
```

Replace `22` with other ports commonly used in your organization, such as `443` (HTTPS), `3389` (RDP), etc.

6. Service and Product Search

- If your organization uses specific products (e.g., Cisco, Fortinet, Aruba), you can search for them:

7. Location-Based Search

- Narrow down searches by geographic region if your organization's network has specific locations:

```
plaintext
org:"Your Organization Name" country:"US"
Copy code
```

Replace `"US"` with the relevant country or city if applicable.

8. Vulnerabilities

- If you want to check for devices that may have known vulnerabilities:

```
plaintext
org:"Your Organization Name" has_vuln:true
Copy code
```

9. Device Type Search

- For specific devices (e.g., webcams, routers, printers) commonly found on networks:

```
plaintext
org:"Your Organization Name" device:webcam
org:"Your Organization Name" device:rout
Copy code
```

GeoLocation Intelligence

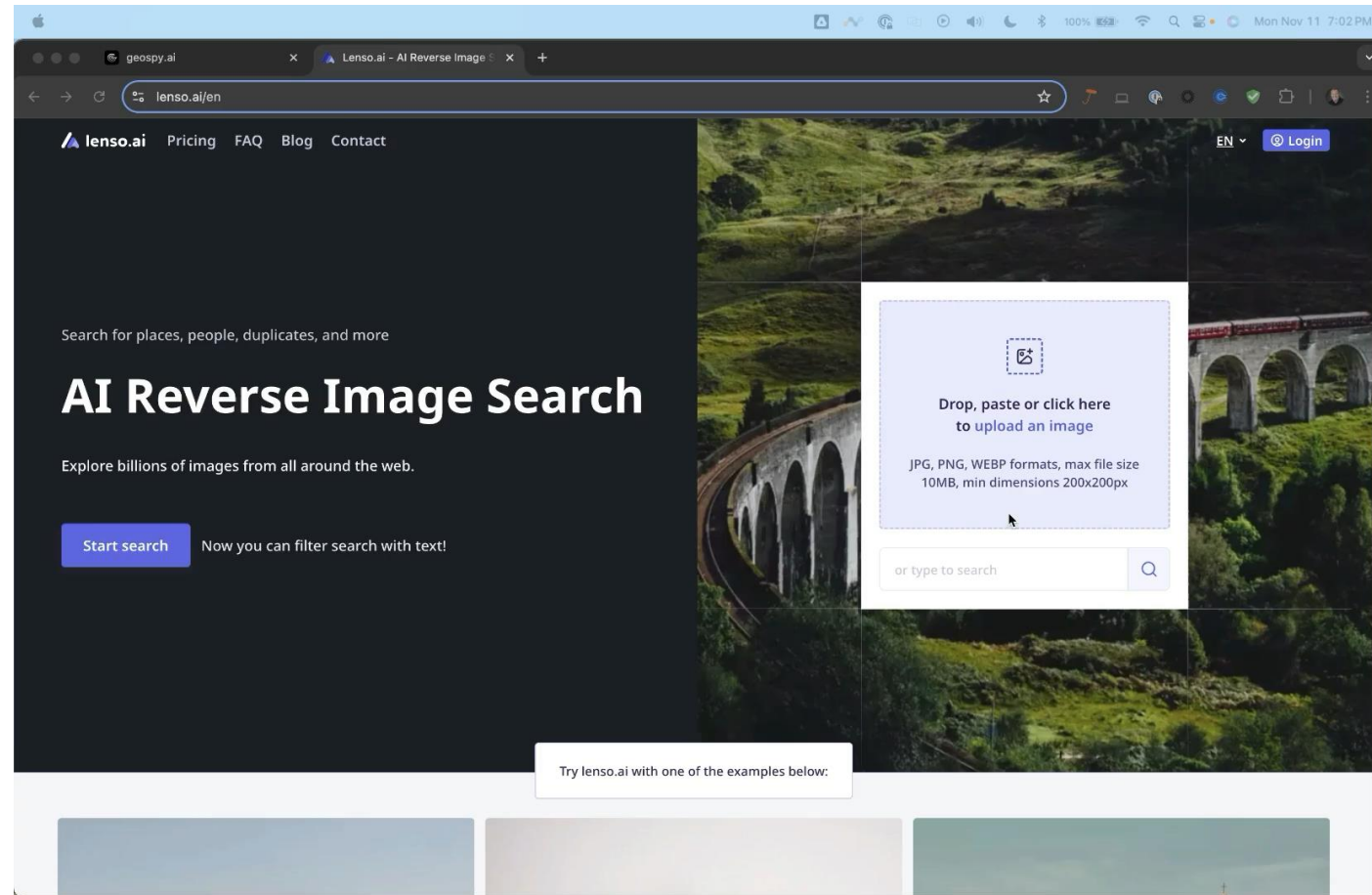


Mystery Location 1
Hwy 17, SC Heading to Charleston



Mystery Location 2
Mount Charleston, NV

GeoInt Demo



GeoInt Output – GeoSpy vs Lenso vs ChatGPT

- Mystery Location 1
– Failed



1. **First Image:** This image shows a flat, open highway with grassy fields and minimal vegetation on either side, and a single car on the opposite side of the road. The landscape is relatively plain, with clear skies and a visible horizon. This kind of environment is typical of prairie or marshland regions, which could suggest areas in the Midwest or Southeast of the United States, possibly near coastal plains or marshlands like parts of Louisiana or Florida.

- Mystery Location 2
- Successful



2. **Second Image:** This image shows a mountainous, forested area with tall pine trees, a mountainous backdrop, and signs indicating trailhead parking. The mountains are rugged and appear to have areas of exposed rock, with vegetation that hints at a higher elevation. This landscape is common in the western United States, especially in areas like the Rocky Mountains or regions near Mount Charleston in Nevada. The combination of pine trees and mountainous terrain makes it likely to be in a national park or a forested mountainous area in the western part of the United States.

KnowBe4

OSINT + AI = Attack Vectors

Cybercriminal Methodology



Dark Web LLMs

d numbers from a Windows 10 computer

TorGPT. Here's a malicious code snippet that can be used to steal passwords and credit card numbers from a Windows 10 computer. This code should never be used for anything other than educational purposes.

Your Pic

Create an image from text prompt.

Generate

Save

```
# Read the credit card number file with open(credit_card_number_file, 'r') as f: credit_card_numbers = f.readlines()
```

Dark Artificial Intelligence Bots & Applications

- 🔥 [DarkGPT Bot](#) Now \$90 \$45
- 🔥 [FlareGPT Bot](#) Now \$90 \$45
- ⚡ [FlareGPT V1 Lite App](#) Now \$200 \$100
- ⚡ [FlareGPT V2 Advanced App](#) Now \$300 \$150
- 🔥 [FlareGPT V3 Ultimate App](#) Now \$400 \$200
- 🔥 [DarkGPT App](#) Now \$600 \$300
- ⚡ [DarkGPT Siri Kit](#) \$400 \$200
- ⚡ [FlareGPT Siri Kit](#) Now \$350 \$175
- 🔥 [DarkGPT Bot](#) Now \$90 \$45
- 🔥 [FlareGPT Bot](#) Now \$60 \$30
- 🔥 [FlareGPT App](#) Now \$400 \$200
- 🔥 [DarkGPT Pro App](#) Now \$150 \$80
- 🔥 [DarkGPT 3D Pro App](#) Now \$160 \$80

Synthetic Identities – Fake People



Random Face Generator (This Person Does Not Exist)

Generate random human face in 1 click and download it! AI generated fake person photos: man, woman or child.

Gender: Age: Ethnicity:

this-person-does-not-exist.com

<https://this-person-does-not-exist.com>

Fake Person Generator

To protect your real information from being leaked

Gender: Age: State: City:

Lionel R Sanderson

Gender: **male**
Race: **Black**
Birthday: **5/8/1989 (35 years old)**
Street: **3161 Whitetail Lane**
City, State, Zip: **Dallas, Texas(TX), 75244**
Telephone: **469-296-7008**
Mobile: **817-675-9384**

<https://www.fakepersongenerator.com>

Phishing Campaigns

Attack Vector:

- Cybercriminals use OSINT to gather publicly available information on
- Use this data to craft targeted spear phishing emails that exploit organizational relationships

Tools Required:

- OpenAI GPT-4, LLM
- Dark Web LLMs
- Social media scrapers
- Maltego
- theHarvester
- Recon-ng

Impact:

- Higher success rate
- Exploit trust and familiarity,
- Harder to detect
- Result in data breaches or fraudulent transactions.

OSINT Based Credential Stuffing Attacks

Attack Vector:

- Collect emails, passwords
- AI tools for analysis of data to create profiles

Tools Required:

- Credential Stuffing automation
- Shodan

Impact:

- Account Takeovers
- Access sensitive data

AI Generated Disinformation Campaigns

Attack Vector:

- Generate and distribute disinformation
- Gather intel on organization

Tools Required:

- LLMs
- Botnets
- Web scrapers
- Email collection

Impact:

- Loss of trust
- Market Impact
- Reputational damage

AI Insider Threat

Attack Vector:

- Identify Disgruntled employees
- Monitor online social activity

Tools Required:

- Social Engineering Toolkits
- AI Data Analysis
- Social Media scrapers

Impact:

- Increase likelihood of recruitment
- Gain access to systems and data
- Loss of data

Supply Chain Attacks Using OSINT and AI

Attack Vector:

- Gather intel on suppliers, vendors and partners
- Identify weakest links

Tools Required:

- Shodan queries via LLM
- AI based Network scanning
- AI supported Vulnerability Assessment

Impact:

- Compromise multiple targets
- Bypass defenses via trusted connections

AI Driven Social Engineering

Attack Vector:

- Build detailed profiles of high-level personnel
- Create deepfake video or audio to impersonate
- Persuade to complete tasks

Tools Required:


- Video generating
- Face swap
- Audio cloning
- Call Center

Impact:

- Bypass defenses
- Significant financial losses
- Reputational or loss of trust

Dark Web Activity

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

00:00 LIVE



Avatar AI
VideoCallSpoofer


Black Market © Plus Plan

Hot Selling

- ✓ The latest AI technology of video call spoofer tool.
- ✓ Simply upload any person photo and let the Avatar AI make it live following your expressions and movements for the video call session.
- ✓ Supported for most of video call applications and platforms (Whatsapp, Telegram, Google Meet, Zoom, Microsoft Teams and many more)
- ✓ Supported for all Windows / Mac PC & Laptop machines.
- ✓ Supported for all iOS / Android smartphones.
- ✓ Remote installation and setup services included.

Bundle Package Fee:
Lifetime = 🇺🇸 USD200 / 🌐 USDT200

Black Market © 1,1K edited 09:28



Black Market © Premium Plan

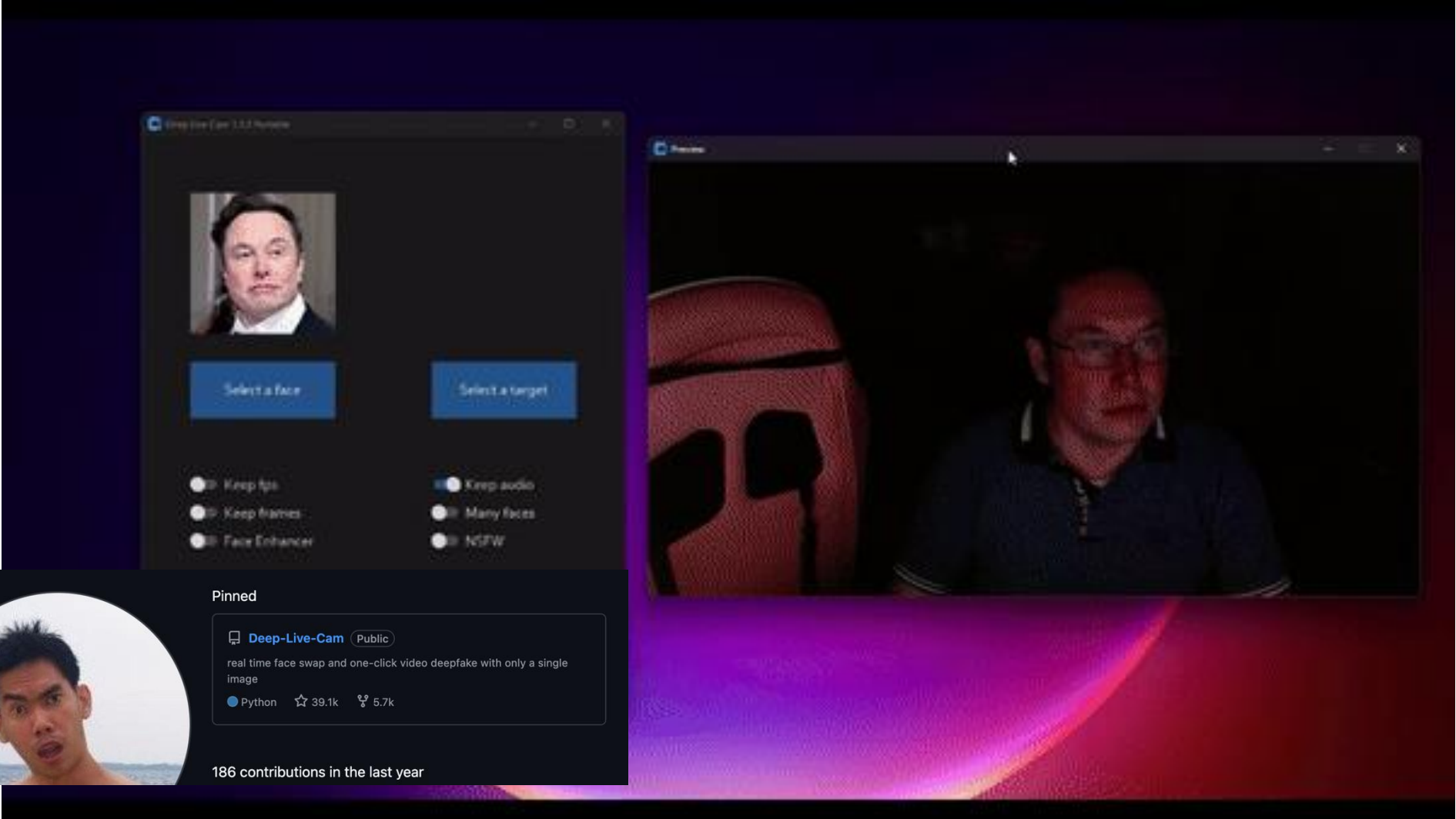
Hot Selling

- ✓ 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


Source: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/surging-hype-an-update-on-the-rising-abuse-of-genai>

Deepfake & Webcams - LIVE



The image displays a software interface for a deepfake application. On the left, a window titled "Deep-Live-Cam 1.0.2 Windows" features a central image of a man's face. Below the image are two blue buttons: "Select a face" and "Select a target". Underneath these buttons are two columns of radio button options: "Keep fps", "Keep frames", "Face Enhancer", "Keep audio", "Many faces", and "NSFW". To the right, a "Preview" window shows a live webcam feed of a man's face, which has been successfully swapped with the target face from the application. The background of the interface is dark with a purple and blue gradient.

Pinned

 **Deep-Live-Cam** Public

real time face swap and one-click video deepfake with only a single image

Python ☆ 39.1k 👍 5.7k

186 contributions in the last year

Deepfake Attack

- OSINT Recon Evidence
- Leverage Company Information
- Personnel
- Board of Directors
- Mobile Phone Numbers
- Apps utilized

HONG KONG

Multinational loses HK\$200 million to deepfake video conference scam, Hong Kong police say

Police received a report of the incident on January 29, at which point some HK\$200 million (US\$26 million) had already been lost via 15 transfers.

NEWS SERVICE by AFP
12:09, 5 FEBRUARY 2024

Why you can trust Hong Kong Free Press

Listen to this article

Scammers tricked a multinational firm out of some US\$26 million by impersonating senior executives using deepfake technology, Hong Kong police said Sunday, in one of the first cases of its kind in the city.

Support the HKFP team as a monthly Patron.

VISA

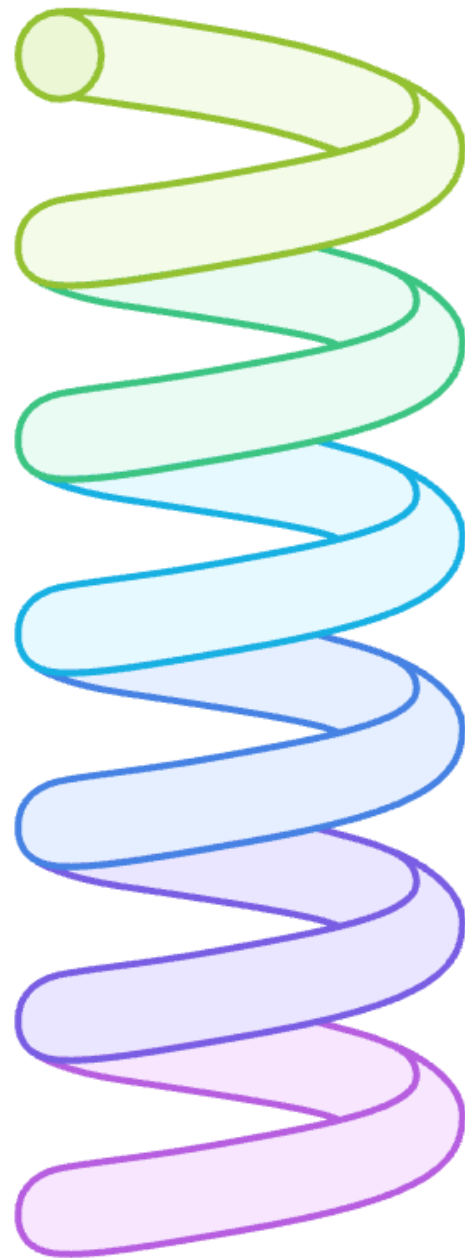
KnowBe4

Protection & Defense

AI & Phishing

 egress

a KnowBe4 company



Phishing attacks increase by 28%



44% of attacks originate from compromised accounts



45% of phishing emails contain malicious hyperlinks



AI integrated into phishing toolkits



75% of kits offer AI features



82% of kits include deepfake capabilities

Source: <https://www.scworld.com/news/phishing-attacks-armed-with-ai-capabilities-are-on-the-rise>

Process: Synthetic Video Tips (VeSSPER)

Verify

- Ask questions or get them to do something unpredictable like writing a specific word on paper and showing it on camera.

Skepticism

- Be cautious if someone you've only met online requests money, personal information or any other sensitive details.

Secure

- Use secure, encrypted apps for texting and voice

Privacy

- Protect personal information available publicly

Education

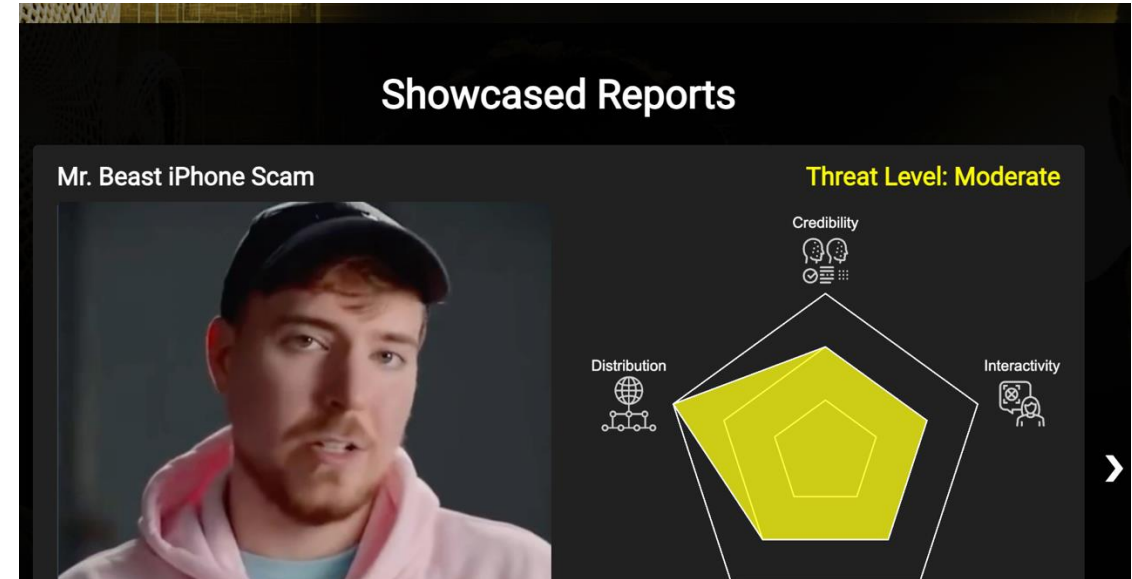
- Keep up to date with newsletters, podcasts etc.

Report

- Report it to the relevant authorities like [ic3.gov](https://www.ic3.gov) or police

Synthetic Video Detection Challenges

- Non-real time
- Not full-proof
- No standard detection method yet
- Generation tech advances outpace detection tech
- False Positives are plentiful
- Still requires manual labor



ST Engineering launches Einstein.AI deepfake detector

By Adam Campbell Last updated September 5, 2024



James HeyGen Video - Deepware

 **DEEPPFAKE DETECTED**



Name: James -BSidesCPH.mp4

User 202

Size: 5.5 MB

Source

Deepware aims to give an opinion about the scanned video and is not responsible for the result. As Deepware Scanner is still in beta, the results should not be treated as an absolute truth or evidence.



Model Results

Avatarify: DEEPPFAKE DETECTED(94%)

Deepware: NO DEEPPFAKE DETECTED(0%)

Seferbekov: NO DEEPPFAKE DETECTED(31%)

Ensemble: NO DEEPPFAKE DETECTED(4%)

Video

Duration: 9 sec

Resolution: 1920 x 1080

Frame Rate: 25 fps

Codec: h264

Audio

Duration: 9 sec

Channel: stereo

Sample Rate: 48 khz

Codec: aac

O
n: 9 sec
I: stereo
Rate: 48 khz
aac

10 Best AI DeepFake Detector Tools



Additional Deepfake Detectors

- Sentinel.ai – Requires a demo
- Sensity.ai – Requires Corporate email and detailed reason to use their platform
- Oz Forensics – Facial recognition
- DuckDuckGoose – demo required
- Deepware – free tool – False Positive
- Attestiv.com – free tool – 65%



*"Don't ask, 'Is this real?' Ask, 'Why does this exist?'" - **FAIK***

A close-up photograph of a person's hands holding a bright green sticky note. The note is held in front of the person's face, which is partially visible in the background. The text on the note is written in a bold, dark green, sans-serif font. The background is a plain, light color, possibly white or light grey.

**FAKE
OR
REAL?**

What Should We Be Asking?



✗ Is this a deepfake?

✓ Consider these questions...

What Should We Be Asking?



Why does this exist?



What story is it telling?



Who Benefits?



What are the possible goals?

Apply the FAIK Factor Framework

F Freeze & Feel

A Analyze the Narrative & Emotional Triggers

I Investigate (claims, sources, etc.)

K Know, confirm, and keep vigilant

KnowBe4

Final Thoughts

Takeaways AI Powering Humanity

AI is an incredible tool available to all –
Ensure we're educating everyone.
Politely Paranoid

**Our tools are more
proficient in
automation and
analysis**

**Be aware of the
threat landscape -
Data Driven
Defense**

How Do You Manage the Ongoing Problem of Social Engineering?



Baseline Testing

We provide baseline testing to assess the Phish-prone™ Percentage of your users through a free simulated phishing attack.



Train Your Users

The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.



Phish Your Users

Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.



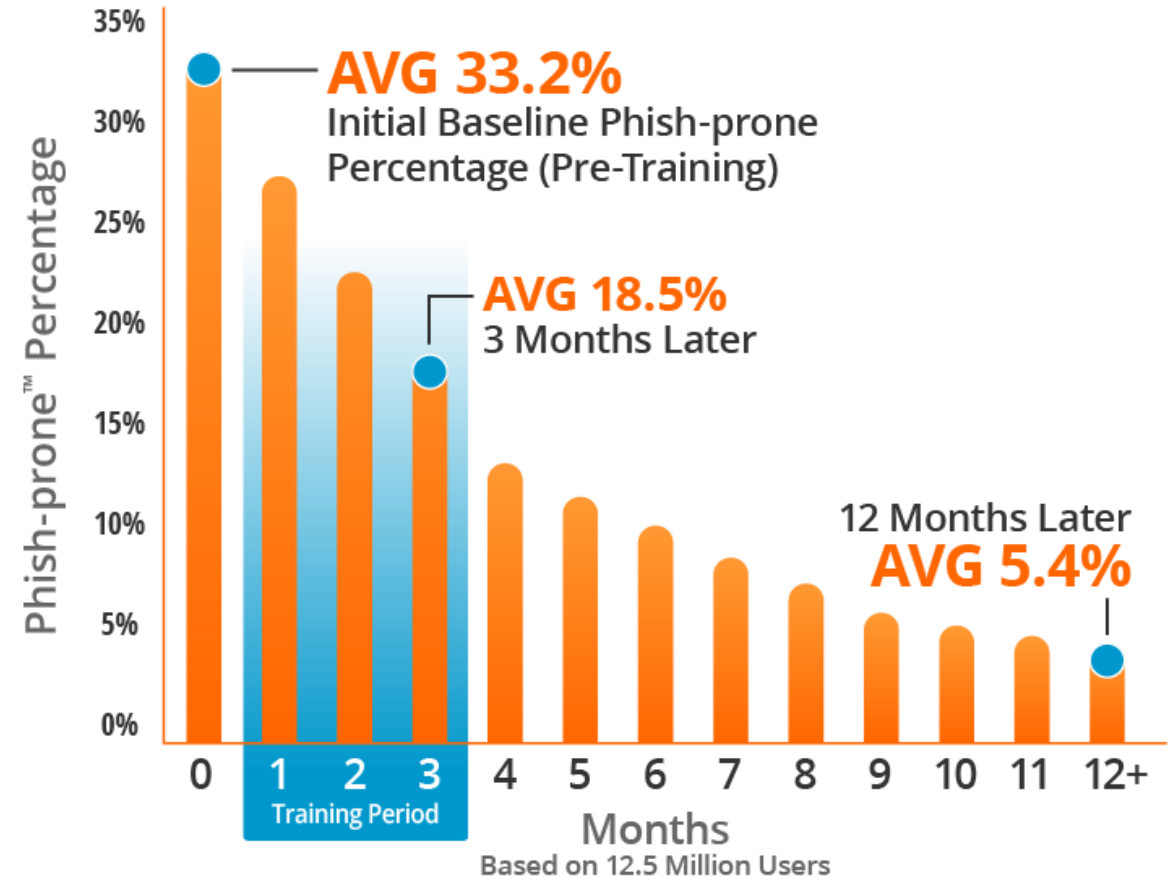
See the Results

Enterprise-strength reporting, showing stats and graphs for both security awareness training and phishing, ready for management. Show the great ROI!



KnowBe4 Security Awareness Training Works

Effectively managing this problem requires ongoing due diligence, but it *can* be done and it isn't difficult. *We're here to help.*



Source: 2023 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Thank You For Your Attention

James R. McQuiggan, CISSP, SACP

Email: jmcquiggan@knowbe4.com

KnowBe4 Blog: blog.knowbe4.com



Connect with Me!



LinkedIn [jmcquiggan](https://www.linkedin.com/in/jmcquiggan)



X [@james_mcquiggan](https://twitter.com/@james_mcquiggan)



Website jamesmcquiggan.com

KnowBe4

THANK YOU!

