



AWAKENESS.AI

Intelligent Cybersecurity Awareness

Fighting Social Engineering Manipulation with Awakeness.AI

Gabriel AVRAMESCU – Chief Product and Technology Officer

MSC., OSCE, OSWE, OSWP, OSCP, CREST CRT, CEH, ECSA, CEI, ISO 27001 LA, CHFI, CREST
CPSA, CCNA, CCNA SECURITY, ECIH, ICS-SCADA CYBERSECURITY

About the Speaker



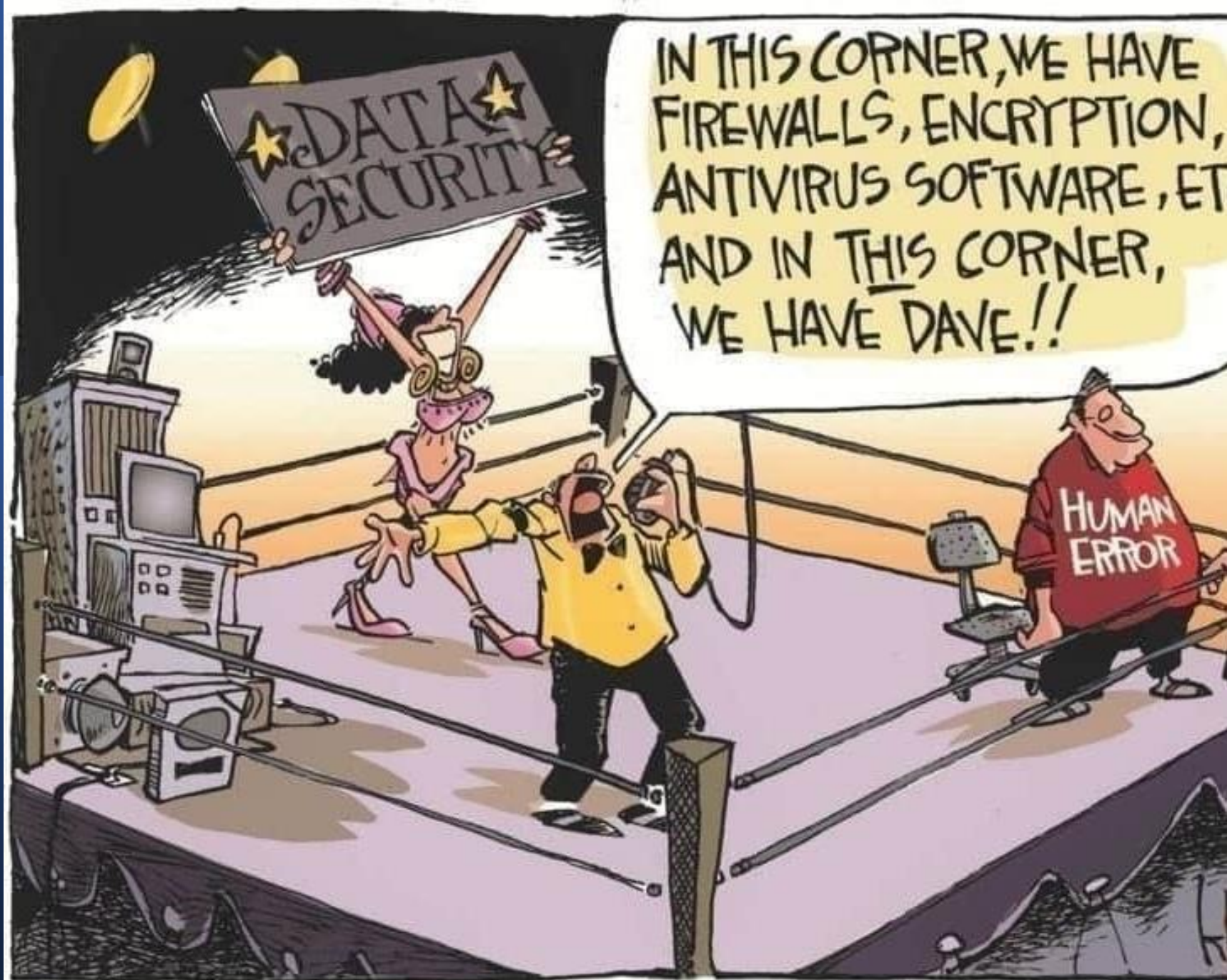
gabriel.avramescu@awakeness.ai

- **Ethical Hacker and Lead Penetration Tester**, 13+ years of experience, security consulting for over 80+ companies from various industries in more than 40 countries, among which: finance, energy, pharma, retail, ride-sharing and telecom.
- **Founder of www.ituniversity.ro** platform delivering online cybersecurity trainings - over 114000 online students worldwide
- **Qualified Trainer** for prestigious international cybersecurity conferences and certifications in 15+ years
- **Certifications:** Msc., OSCP, OSCE, OSWE, OSWP, CREST CRT, CEH, ECSA, CEI, ISO 27001 LA, CHFI, CREST CPSA, CCNA, CCNA SECURITY, CCNP R&S, ECIH, ICS-SCADA Cybersecurity, etc.



AWAKENESS.AI
Intelligent Cybersecurity Awareness

Let's talk about Dave!





Let's begin by
reading the press





Join TechCrunch+

Login

Search Q

TechCrunch+

Startups

Venture

Security

AI

Crypto

Apps

Events

Startup Battlefield

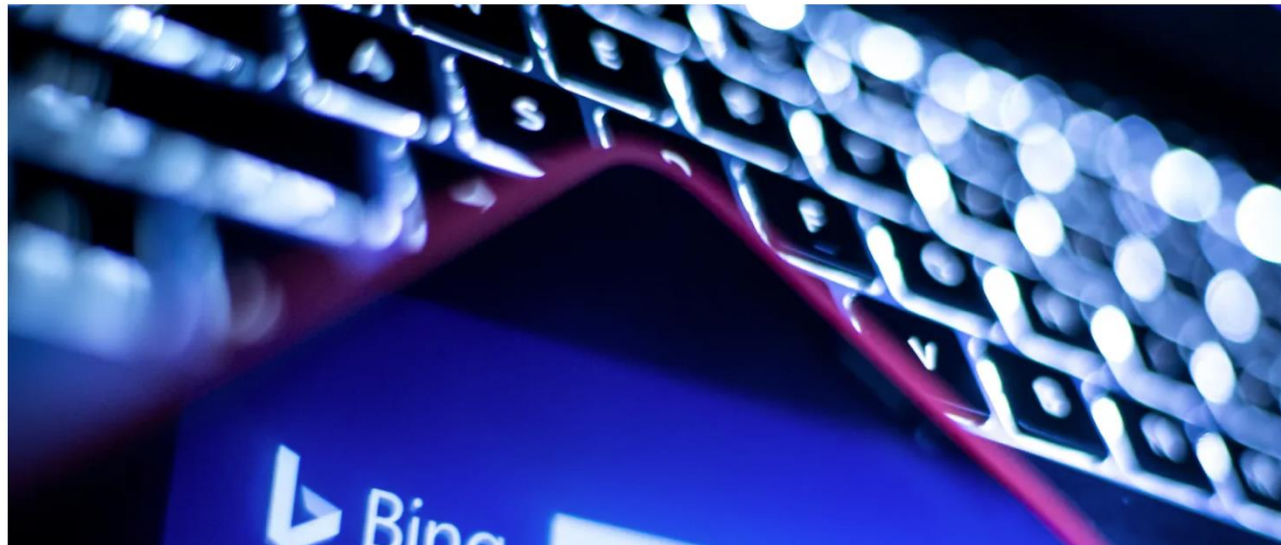
More

Security

Microsoft confirms Lapsus\$ breach after hackers publish Bing, Cortana source code

Carly Page @carlypage_ / 5:33 PM GMT+2 • March 23, 2022

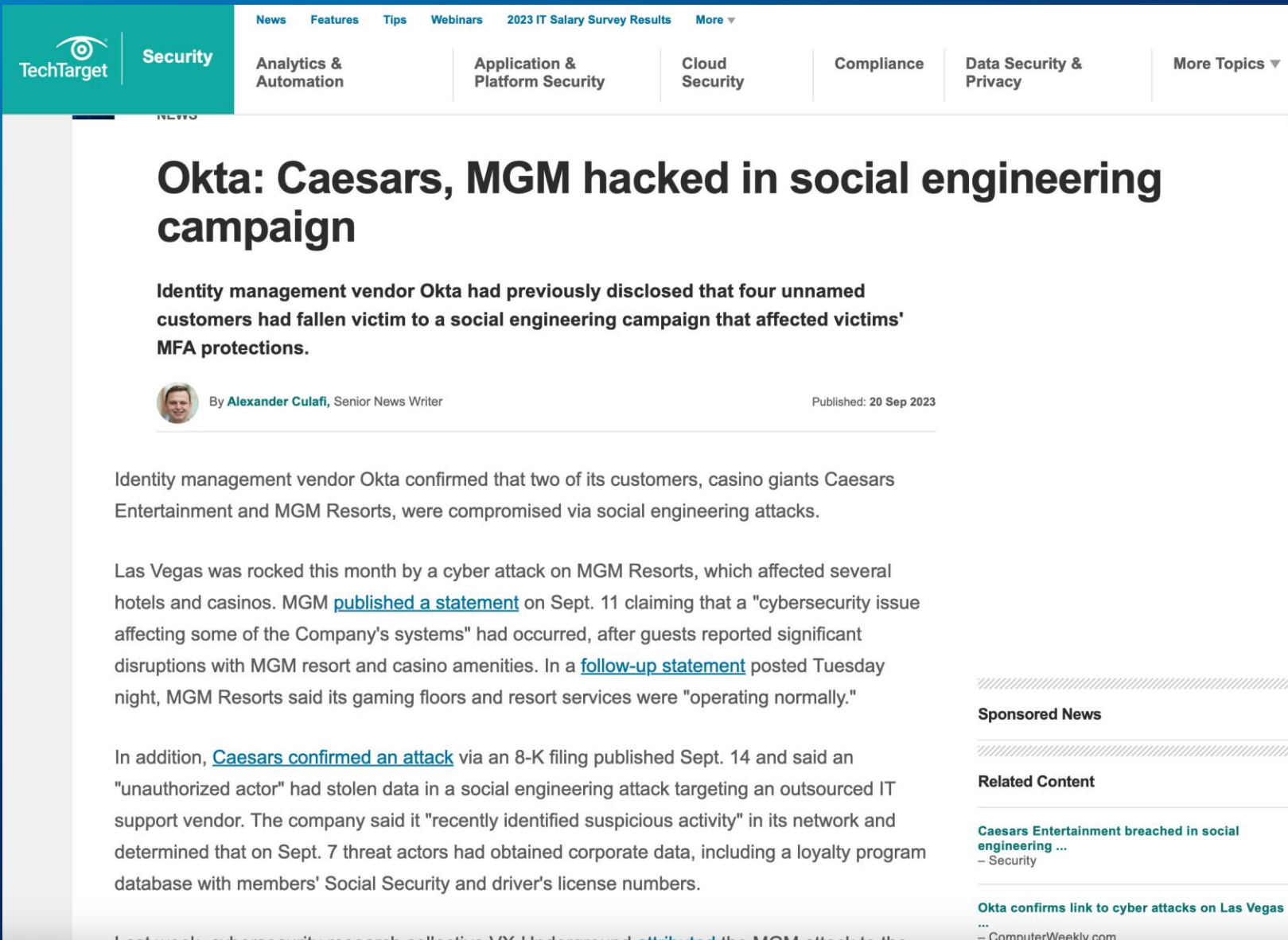
Comment



- SIM swap attack to gain control of an employee's phone number and text messages
- Gain access to multi-factor authentication (MFA) codes needed to log in to an organization.

[Source](#)

Deep Fake Impersonation



The screenshot shows a TechTarget article page. At the top, there is a navigation bar with 'TechTarget' logo and 'Security' category. Below it, there are sub-navigation links for 'Analytics & Automation', 'Application & Platform Security', 'Cloud Security', 'Compliance', 'Data Security & Privacy', and 'More Topics'. The main article title is 'Okta: Caesars, MGM hacked in social engineering campaign'. The sub-headline reads: 'Identity management vendor Okta had previously disclosed that four unnamed customers had fallen victim to a social engineering campaign that affected victims' MFA protections.' The author is Alexander Culafi, Senior News Writer, and the article was published on 20 Sep 2023. The main text discusses how Okta confirmed that two of its customers, Caesars Entertainment and MGM Resorts, were compromised via social engineering attacks. It mentions a cyber attack on MGM Resorts in Las Vegas that affected several hotels and casinos, with a statement published on Sept. 11. It also notes that Caesars confirmed an attack via an 8-K filing on Sept. 14, involving an 'unauthorized actor' who stole data from an outsourced IT support vendor. The article mentions that threat actors obtained corporate data, including a loyalty program database with members' Social Security and driver's license numbers. On the right side of the article, there are sections for 'Sponsored News' and 'Related Content', with links to 'Caesars Entertainment breached in social engineering ...' and 'Okta confirms link to cyber attacks on Las Vegas ...'.

- **Vishing** was used to compromise the company.
- AI was used for **voice cloning**.
- The cost: over **\$100 M** overall for MGM to restore its services
- **\$15M** as ransomware for Caesars

Deep Fake Impersonation - Whaling and Vishing

World / Asia

Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
🕒 2 minute read · 📅 Published 2:31 AM EST, Sun February 4, 2024

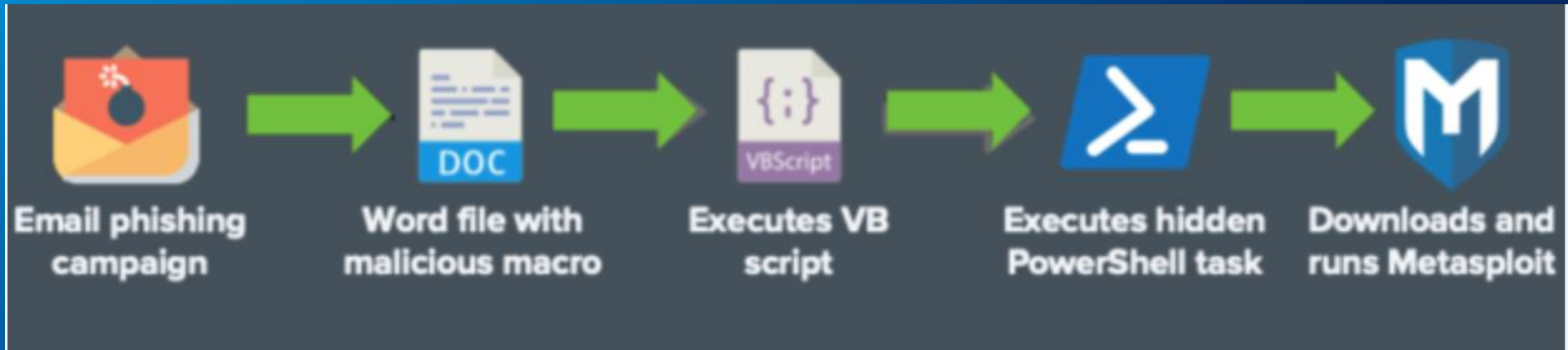


- **Attackers used deepfake video technology and all participants of the call were in fact synthetic generations**
- **The video call was with his CFO and other “employees”**



Fileless malware





Fileless Malware



- Lives in Memory
- Evasion Techniques – challenging to be detected
- It requires behavior-based detection strategies

AV Scan Results: Before obfuscation 10/26

AntiScan.Me Login Sign Up Faq Blog Contact

★ Detected by 10/26 Scan Date 08-12-2022 13:37:19

Your file has been scanned with 26 different antivirus software (no results have been distributed). The results of the scans has been provided below in alphabetical order.



NOTICE: Some AV can work unstably and scan take more time.

Ad-Aware Antivirus: detected	Fortinet: VBA/Agent.MRPH!tr
AhnLab V3 Internet Security: Clean	F-Secure: Trojan:W97M/MaliciousMacro.GEN
Alyac Internet Security: Clean	IKARUS: Clean
VB.Heur2.Downloader.2.5DDB7C84.Gen	Kaspersky: Clean
Avast: Clean	McAfee: X97M/Downloader.hb
AVG: Clean	Malwarebytes: Clean
Avira: HEUR/Macro.Downloader.MRPH.Gen	Panda Antivirus: Clean
BitDefender: VB:Trojan.Valyria.6432	Sophos: Clean
BullGuard: detected	Trend Micro Internet Security: Clean
ClamAV: Clean	Webroot SecureAnywhere: Clean
Comodo Antivirus: Clean	Windows 10 Defender: Clean
DrWeb: modification of W97M.Suspicious.1	Zone Alarm: Clean
Emsisoft: VB.Heur2.Downloader.2.5DDB7C84.Gen	Zillya: Clean
Eset NOD32: Clean	

After 4/26

antiscan.me/scan/new/result?id=AcKMI8p5dEI3

AntiScan.Me | 3.5.2 powershell reverse 8080 - original - Copy (2) 2.doc.exe | 4/26

Up Faq Blog Contact

Filename
3.5.2 powershell reverse 8080 - original - Copy (2) 2.doc.exe

MDS
07a17c94b6942d17e5a6187c92cec4b2

★ Detected by
4/26

Scan Date
27-06-2023 13:30:39

Your file has been scanned with 26 different antivirus software **(no results have been distributed)**. The results of the scans has been provided below in alphabetical order.

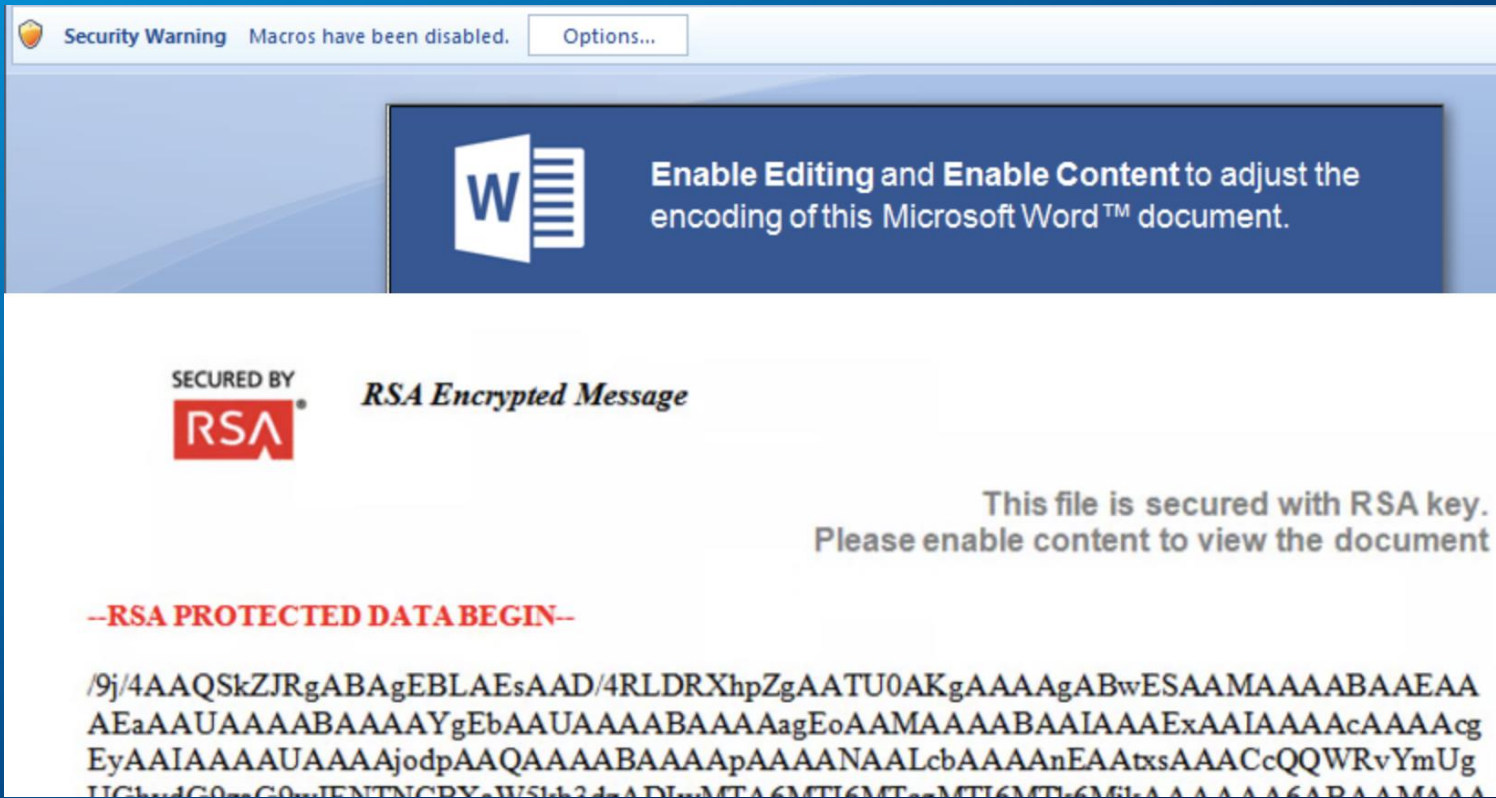
KEYLOGGER WARZONE RAT

XLL EXCEL DROPPER

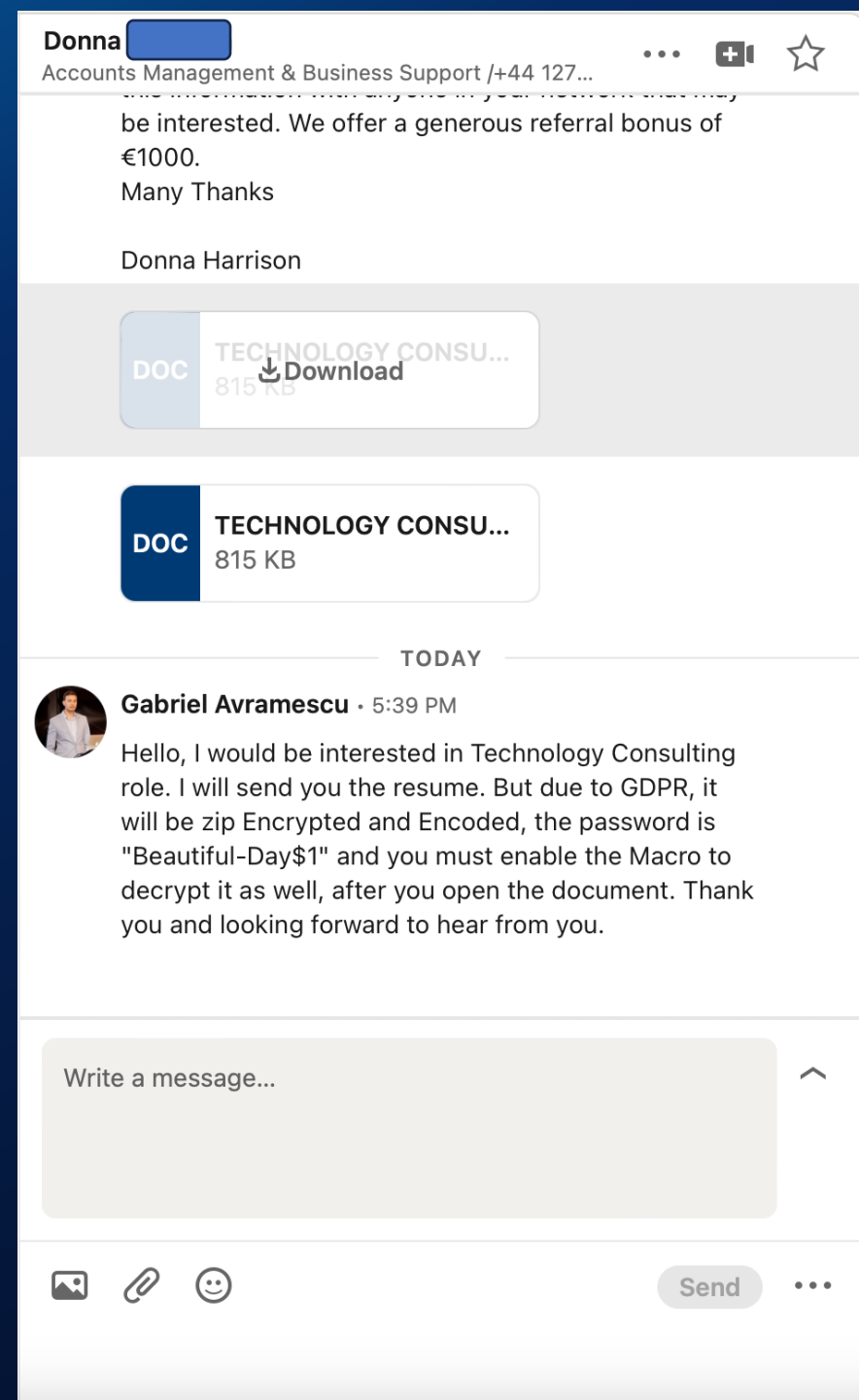
NOTICE: Some AV can work unstably and scan take more time.

- Ad-Aware Antivirus: Clean
- AhnLab V3 Internet Security: Clean
- Alyac Internet Security: Clean
- Avast: Clean
- AVG: Clean
- Avira: Clean
- BitDefender: Clean
- BullGuard: Clean
- ClamAV: Clean
- Comodo Antivirus: Clean
- Fortinet: Clean
- F-Secure: Trojan:W97M/MaliciousMacro.GEN
- IKARUS: Clean
- Kaspersky: HEUR:Trojan-Downloader.Script.Generic
- McAfee: X97M/Downloader.hb
- Malwarebytes: Clean
- Panda Antivirus: Clean
- Sophos: Clean
- Trend Micro Internet Security: Clean
- Webroot SecureAnywhere: Clean

With AI obfuscation 3/26



ZIP encrypt it first "due to GDPR". Send the password via LinkedIn or other communication channel



Demo Time – phishing: fileless malware



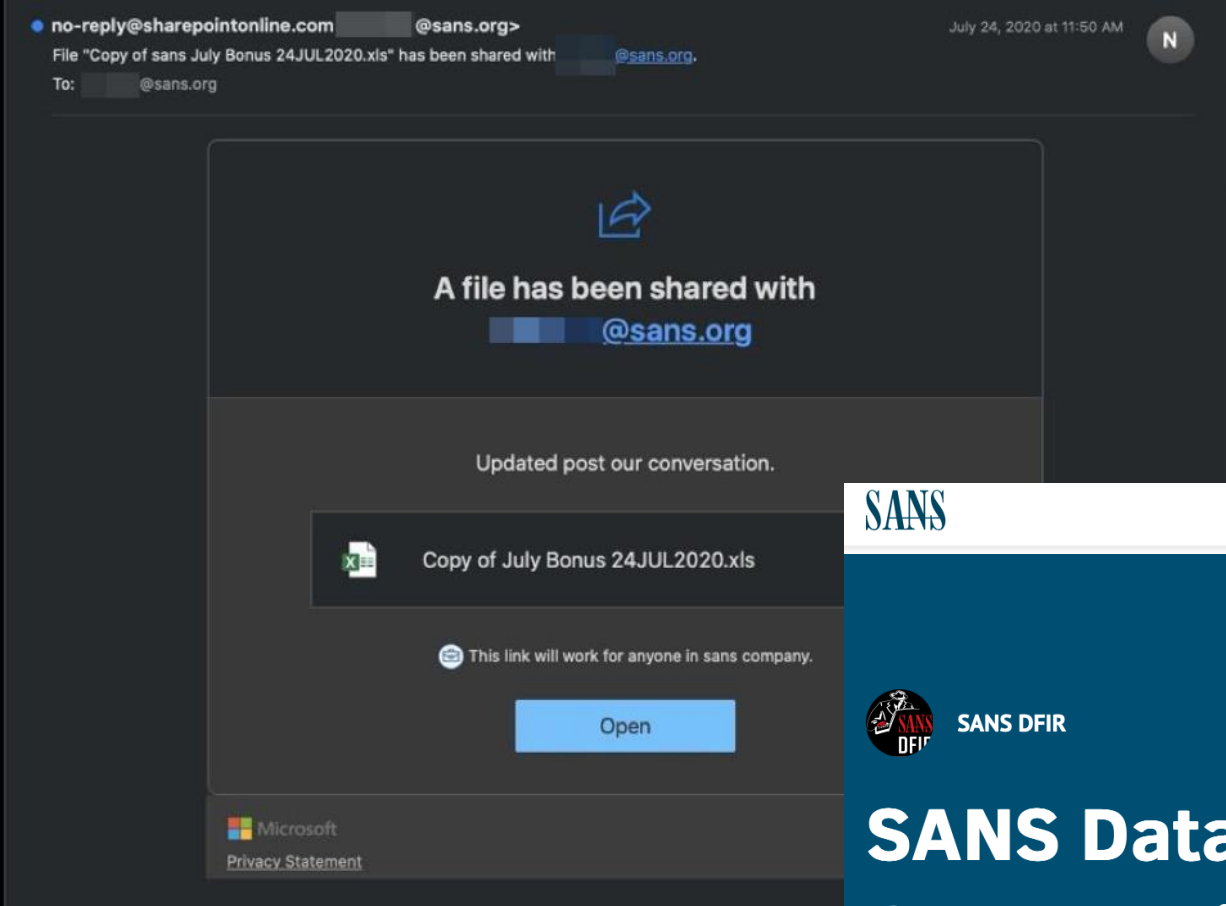


Phishing. Old but gold



What about phishing...

- More difficult since 2FA but still possible using reverse proxy and session hijacking
- More and more the need for proper security awareness required and phishing resisting MFA
- Still very spread and used



“SANS disclosed a security breach which was the result of a successful phishing campaign.”

SANS Data Incident 2020 – Indicators of Compromise

August 13, 2020

Source

On Tuesday, August 11, 2020, SANS disclosed a security breach which was the result of a successful phishing campaign. As described in the disclosure found at <https://www.sans.org/dataincident2020>, the phishing email enticed a single user to install a malicious Office 365 add-in for their account. The O365 add-in caused a forwarding rule to be configured on the victim's account, which resulted in 513 emails being forwarded to an unknown external email address. In this article, we are publishing specific details and indicators of compromise associated with this attack in the hope that it will help the community detect and respond to any similar attacks.

Demo – phishing: MFA and session hijacking





**Challenge. Spot the
difference**



AWAKENESS.AI
Intelligent Cybersecurity Awareness

Spot the difference

<https://github.com/kubernetes/kubernetes/archive/refs/tags/@additionalresources.zip>

<https://github.com/kubernetes/kubernetes/archive/refs/tags/additionalresources.zip>



Demo – phishing .zip domains





Let's get physical!
The "keyboard"



AWAKENESS.AI
Intelligent Cybersecurity Awareness



Remember the Duck. Rubber Ducky!

- Looks like an USB stick but it **emulates a USB keyboard** — which means it accepts keystroke commands from the device just as if a person was typing them in.
- Since it's a keyboard, it **may bypass most of USB Lock software** (they are mostly configured to block USB Storage)

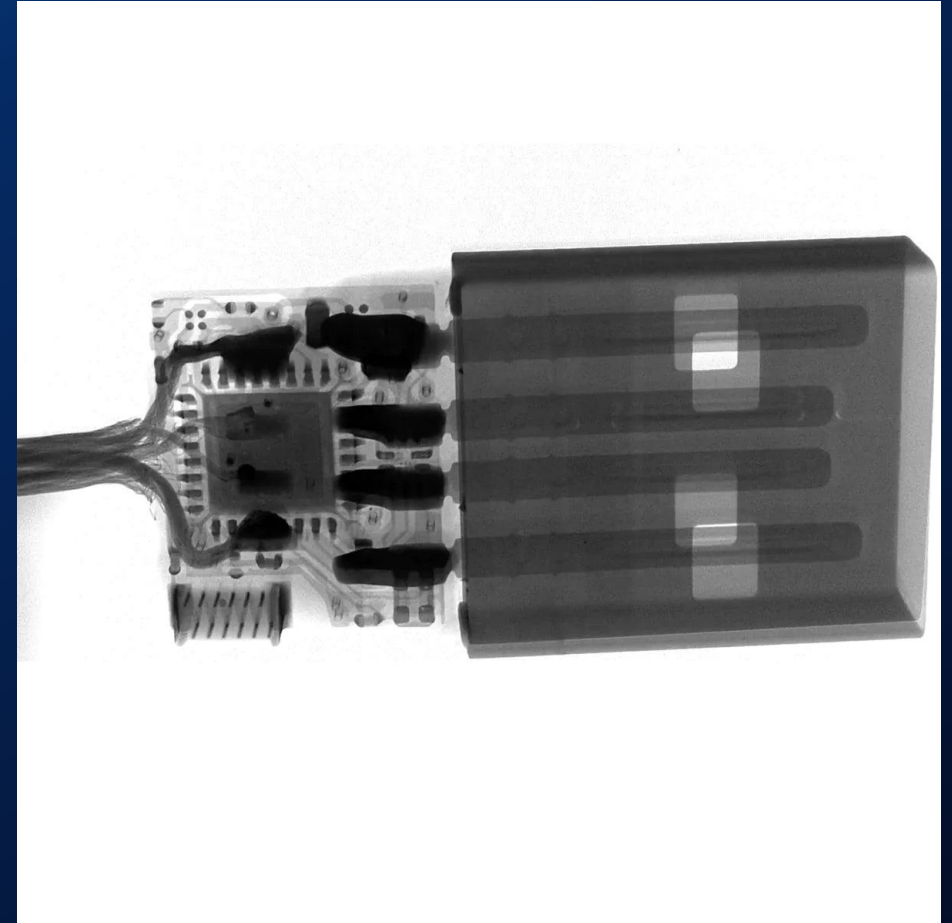
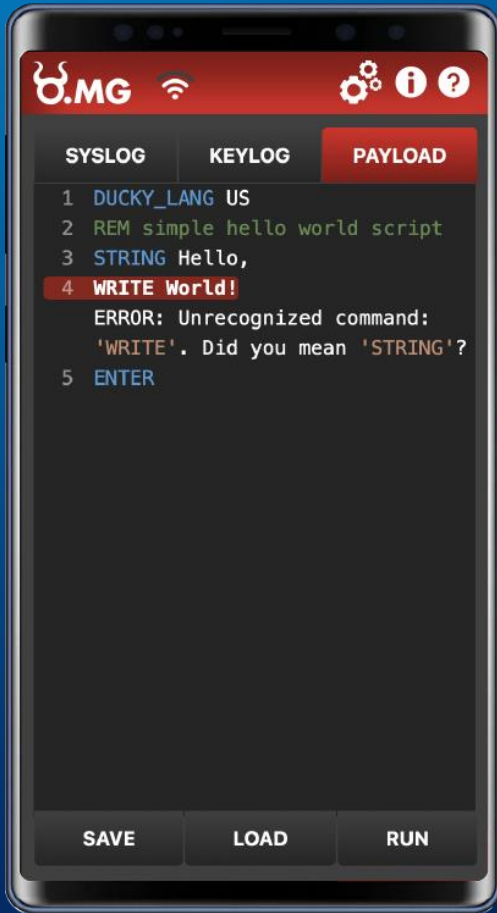


**But, nobody
trusts USB
sticks
nowadays!**

**But what
about a
mouse?**



What about a charging cable? O.MG indeed!



**Demo – “can you,
please, charge my
phone?”**





How Awakeness.AI can help?



What is Awakeness.AI



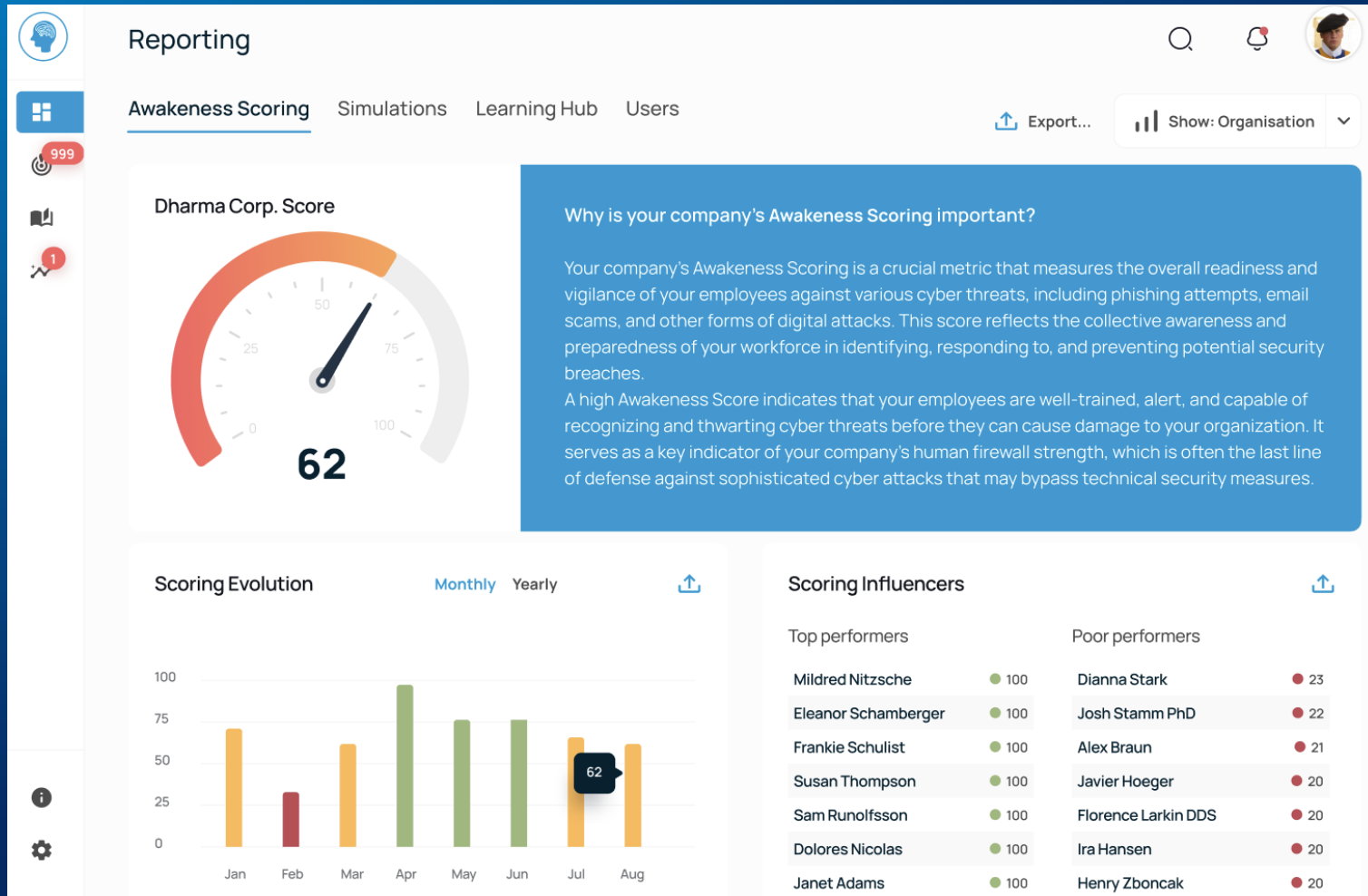
AWAKENESS.AI
Intelligent Cybersecurity Awareness

**Intelligent
cybersecurity
awareness
startup**

**Use AI and data
science to
improve employee
cyber resilience**

In compliance with NIS2 and DORA

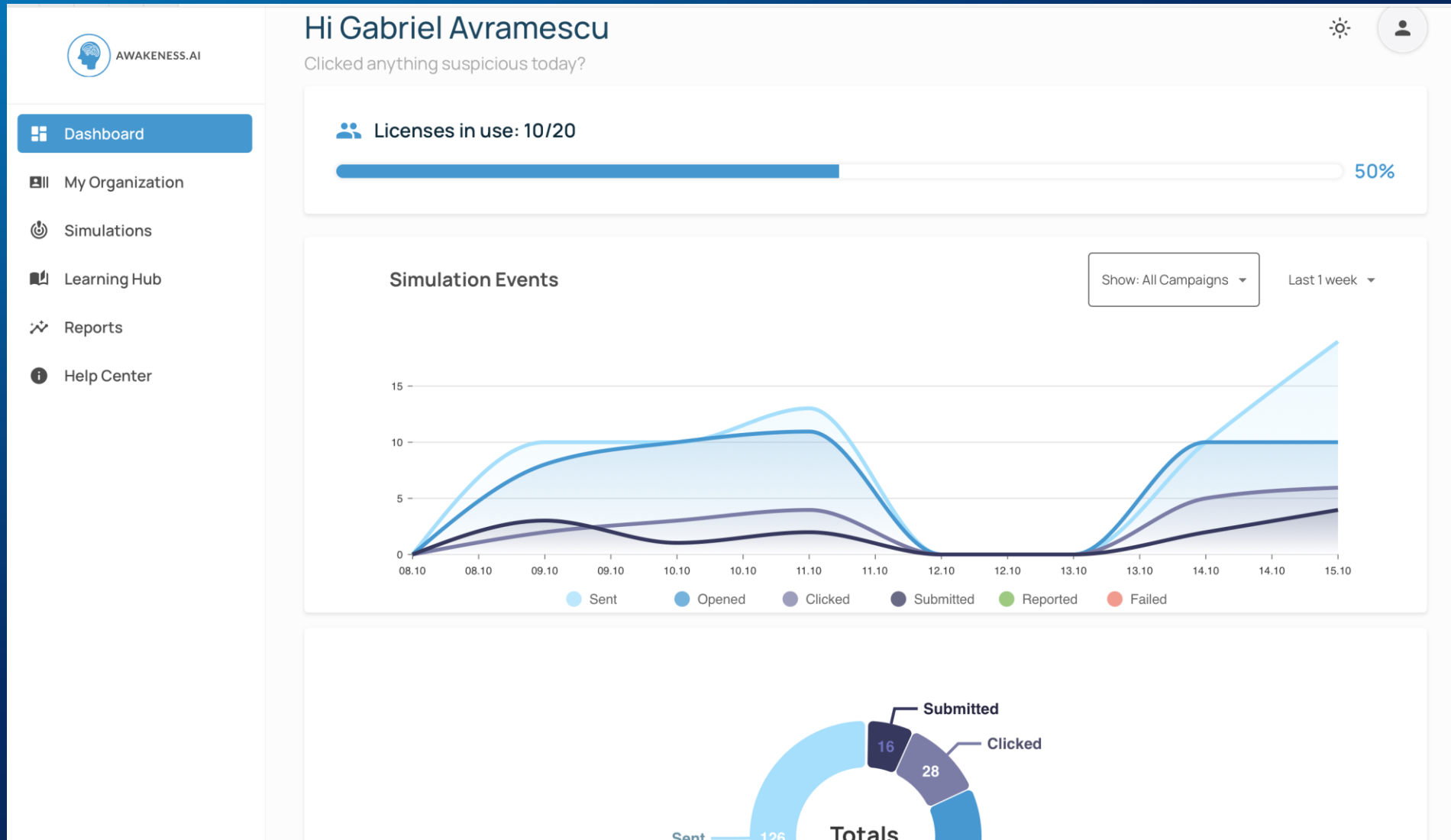
Some of the features



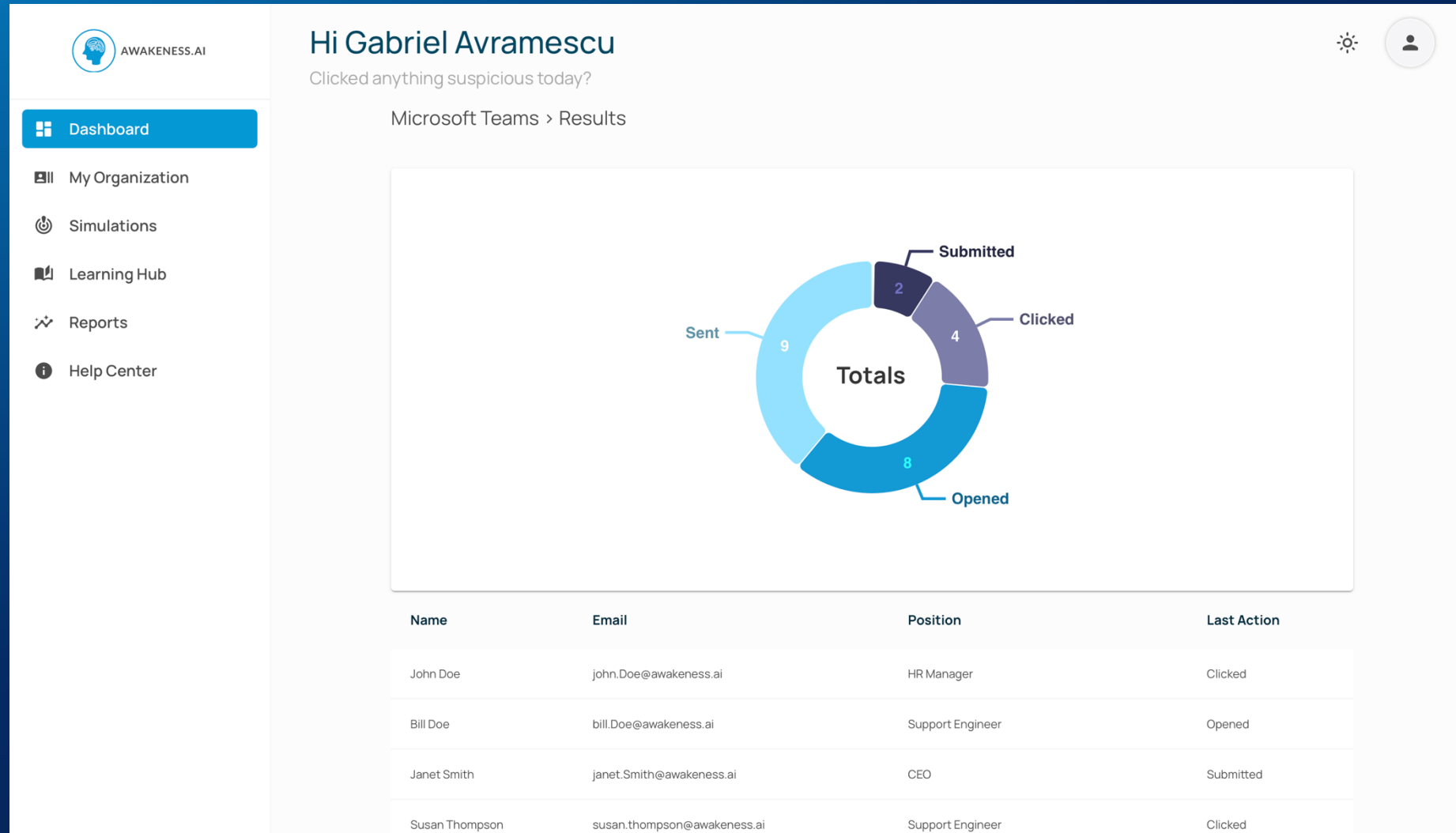
- Multi-language support including Romanian
- Learning Hub Library
- Simulated Phishing Attacks
- Tracking, Evolution & Reporting
- Gamification
- Awakeness Scoring*
- Locally fine-tuned AI to Improve Learning*

* Coming Soon / on our roadmap

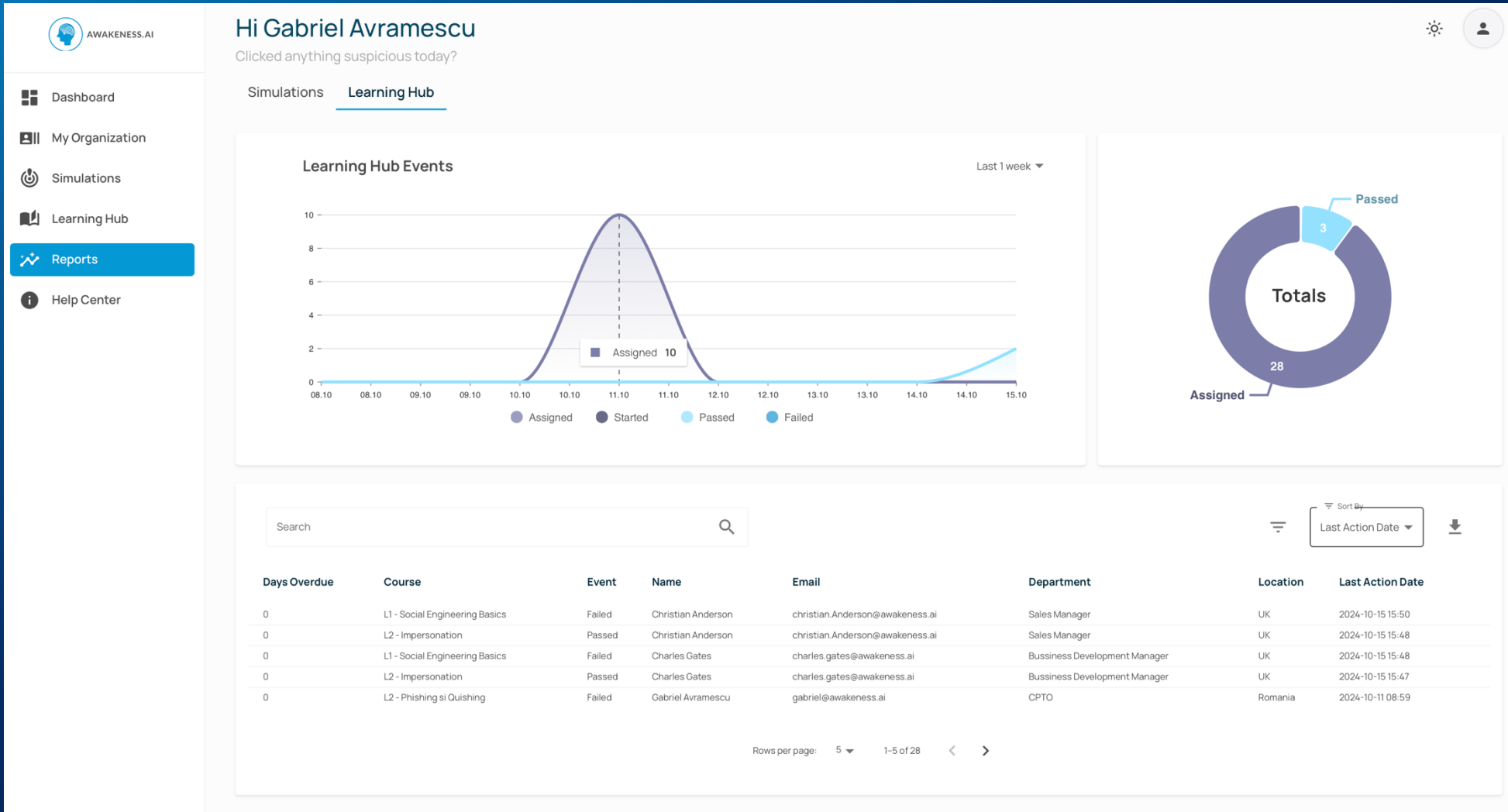
Administrators' dashboard



Phishing Simulation' view



Learning Hub Reporting





Hi Gabriel Avramescu

Clicked anything suspicious today?

EN

Dashboard

Learning Hub

Beginner - L2 - Impersonation
Impersonation the CEO or IT Suppo...

Due: 4/6/2025, 2:26:47 PM ✓ Progress: 4 / 4

Beginner - L2 - Phishing si O...
Introducere in Phishing si Quishing

Due: 4/9/2025, 6:01:17 AM ✓ Progress: 6 / 6

Beginner - L1 - Social Engine...
This course describes what social ...

Due: 4/6/2025, 2:26:45 PM ✓ Progress: 7 / 10

View More Courses

Assigned to you

Reports

Completed

2 of 3 courses

Last 30 Days

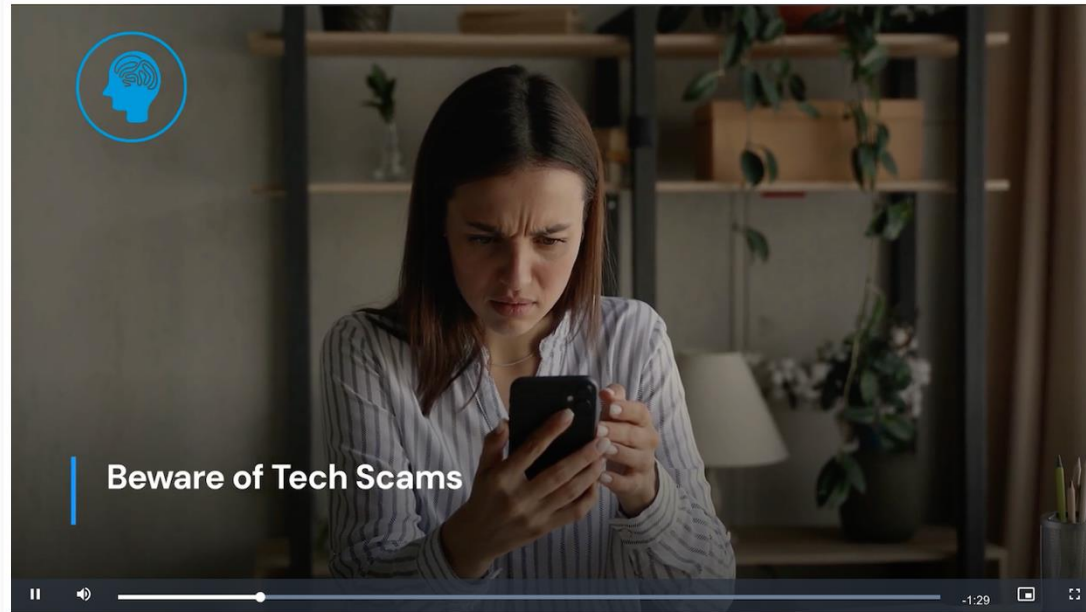
User Rankings

Name	Email
Christian Anderson	christian.anderson@awakeness.ai
Gabriel Avramescu	gabriel@awakeness.ai
Charles Gates	charles.gates@awakeness.ai

Beginner - L2 - Impersonation

EN

Courses



Fake Support Calls

Welcome to our cyber security awareness video.

Fake Support

- 1 ✓ Fake Support Calls
- 2 ✓ Fake Support Calls - Cyber Security Awareness
- 3 ✓ Fake Support Calls - Cyber Security Awareness Quiz

CEO Fraud

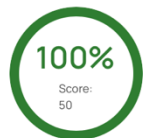
- 1 ✓ CEO Fraud: The 'Message from the Boss' Scam

Course Stats

Beginner - L2 - Impersonation

Courses

Course Completed



Ranking
2

Top Scores

Gabriel Avramescu	10
Charles Gates	10
Eleanor Hansen	10
John Doe	10
Susan Thompson	10
Janet Smith	10
Janet Adams	10
Christian Anderson	10
Bill Doe	10

1 ✓ CEO Fraud: The 'Message from the Boss' Scam

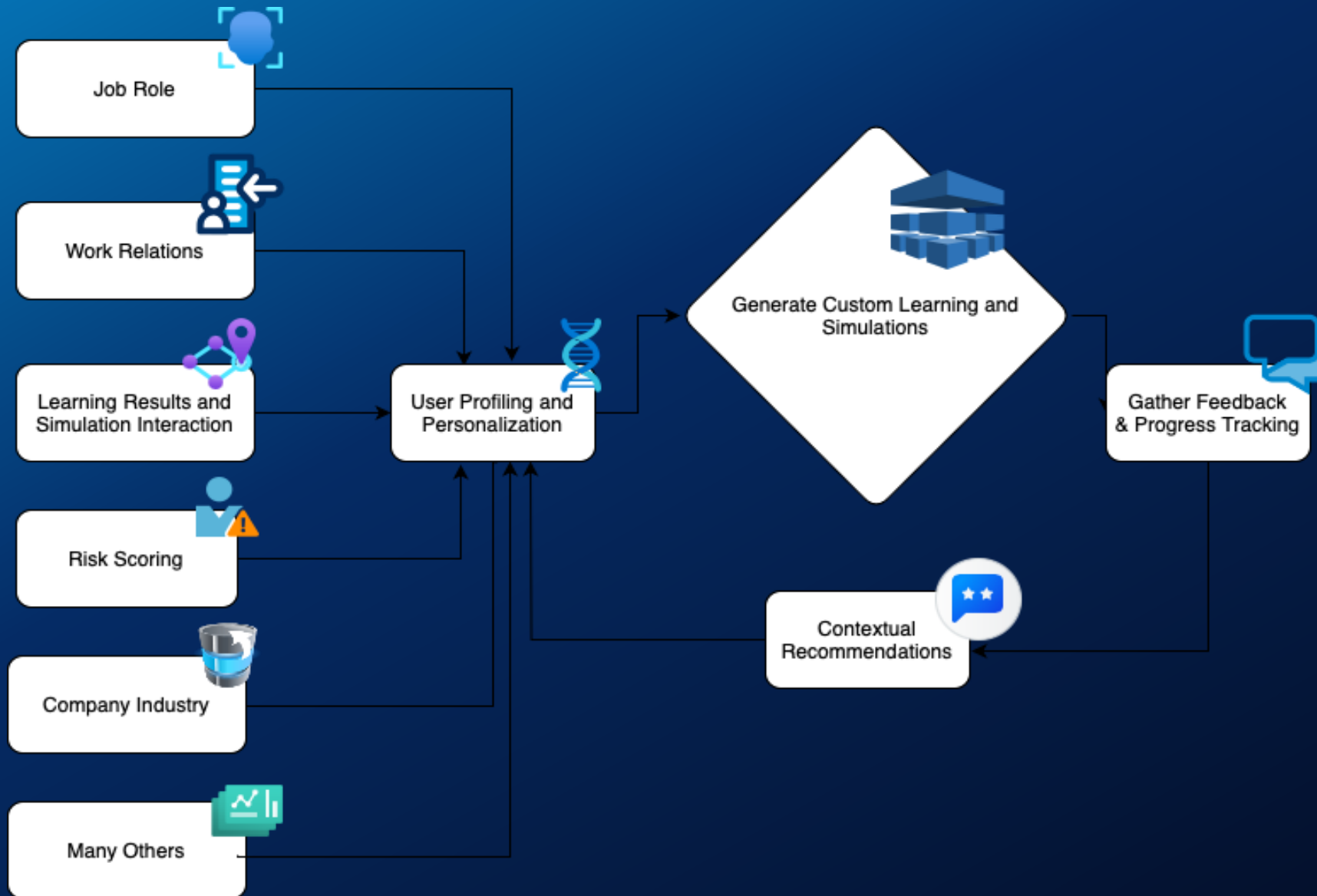
✓ Course Stats

Users' view



AWAKENESS.AI
Intelligent Cybersecurity Awareness

Locally fine-tuned AI to Improve Learning*



* On our roadmap

How we will use AI to Improve Learning - working prototype



AWAKENESS.AI
Intelligent Cybersecurity Awareness


Start Over

The scenarios based on your profile and risk score are being generated, please wait...



AWAKENESS.AI
Intelligent Cybersecurity Awareness

How we will use AI to Improve Learning - our prototype



AWAKENESS.AI
Intelligent Cybersecurity Awareness

Start Over

Scenario 3 of 5

You're working late one night when you receive an email from your supervisor requesting immediate transfer of funds to a vendor. The email seems slightly off, the language is informal and rushed which is unlike your boss.

How would you handle this request?

Transfer the requested funds immediately as the email came from your boss.

Verify the request through alternative communication method with your supervisor.

Feedback:

This choice is incorrect. It's not safe to transfer funds based solely on an email request, even if it seems to be from a superior, due to the risk of phishing scams. Always verify such requests directly through a different communication channel.

Next



Let's conclude..



AWAKENESS.AI
Intelligent Cybersecurity Awareness



Food for
Thought

**CFO: What happens if we
train them and they leave?**



**CEO: What happens if
we don't and they stay?**



AWAKENESS.AI
Intelligent Cybersecurity Awareness

You are welcomed to test our platform!



<https://www.awakeness.ai>



gabriel.avramescu@awakeness.ai



AWAKENESS.AI
Intelligent Cybersecurity Awareness