AWAKENESS

Intelligent Cybersecurity Awareness

SaaS platform for awareness training and simulations designed to reduce human associated risks against cyber threats, augmented by AI and data science.

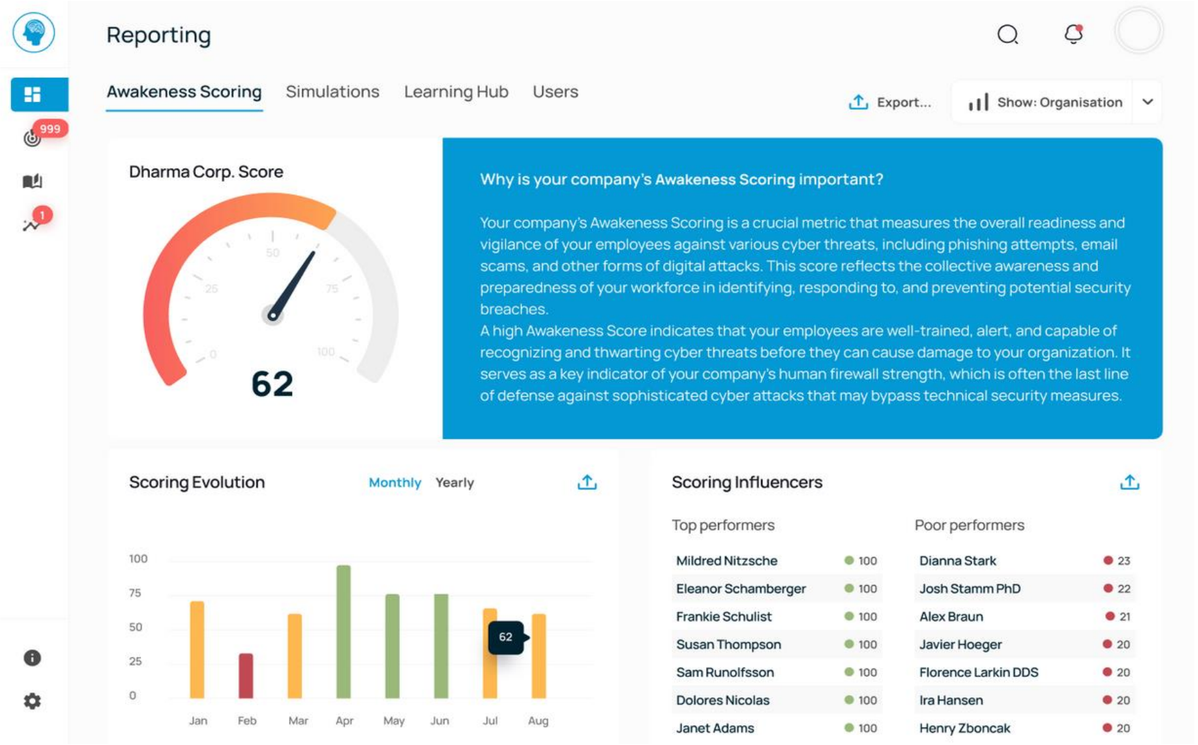
NETLAND

Executive Summary

AI-Driven Cybersecurity Awareness: Defending Against the Human Factor

Mission:

Leverage AI and data science to profile and predict high-risk users,
improve all employees' behavior and engagement,
reduce the likelihood of costly security breaches.



"Awareness is not the issue, human behavior is" (Gartner)

The Problem

Cybersecurity Challenges: The Human Factor

Frequent Cyber Threats

70%

of working adults took risky actions to bypass security knowingly. Cyber threats evolve faster than traditional defenses.

User Behavior and Human Error

82%

of breaches are caused by user error. Traditional training methods are insufficient to combat sophisticated attacks.

"*Awareness is not the issue, human behavior is*" (Gartner)

Regulatory Compliance

DORA, NIS2, GDPR, HIPAA, PCI DSS and best practices in cyber industry: ISO 27k1, NIST, reputational risks or face severe penalties of up to **€20M** or **4% from total global turnover** (whichever is higher).

Existing solutions are inefficient

- Internally developed tools – limited IT capacity for proactive monitoring / awareness
- Existing providers inflexible, difficult to use and navigate, inadequate reporting and have outdated content.
- Generic training modules that fail to engage users.

Stats source: https://www.gartner.com/en/publications/employee-behaviors and https://www.arubanetworks.com/assets/eo/Aruba_DigitalWorkplace_Report.pdf

zvelo

Products Use Cases

Malicious AI: The Rise of Dark LLMs

Home / AI & Machine Learning / Malicious AI: The Rise of...

The misuse of AI technologies has transitioned from a
build on our last post that detailed how AI jailbreaks en
blog explores malicious AI and the rise of dark LLMs ar
weaponized for cyberattacks.

Cobalt

PLATFORM SERVICES SOLUTIONS ABOUT RESOURCES LOGIN GET STARTED

Phishing Statistics

1. Phishing continues to be the most common email attack method, accounting for 39.6% of all email threats (Hornetsecurity's Cyber Security Report 2024).
2. 94% of malware is delivered over email (Panda).
3. Spear phishing attachments were used in 62% of phishing attacks, while links were used in 33% and as a service in 5% (IBM Security X-Force 2023).
4. Credit card information was targeted in only 29% of phishing kits in 2022, a 52% decline from 2021 (IBM Security X-Force 2023).
5. Business Email Compromise (BEC), often involving spear phishing links, accounted for 6% of incidents, with spear phishing links used in half of these cases (IBM Security X-Force 2023).
6. In 80% of the organizations where a BEC attack occurred, no multi-factor authentication ("MFA") solution was in place before their incident (ArcticWolf).
7. Phishing was identified as the primary infection vector in 41% of cybersecurity incidents. (IBM Security X-Force 2023).
8. The number of thread hijacking attempts doubled in 2022 compared to 2021 (IBM Security X-Force 2023).

netcraft

Resources > Blog > Scam Sites at Scale: LLMs Fueling a GenAI Criminal Revolution

August 29, 2024

Will Barnes

Scam Sites at Scale: LLMs Fueling a GenAI Criminal Revolution

This article explores Netcraft's research into the use of generative artificial intelligence (GenAI) to create text for fraudulent websites in 2024. Insights include:

The Solution

AI-Powered Cybersecurity Awareness Solution

Frequent Cyber Threats

Our AI-powered platform tests and trains users, helping to prevent costly security breaches through proactive education.

User Behavior and Human Error

We use **data science** and **machine learning** to change employee **behavior**, **reduce** risks, and **boost** resilience with **predictive** analysis, personalized training, identifying **high-risk individuals**.

Regulatory Compliance

Stay compliant with major standards like GDPR, HIPAA, PCI DSS, NIS 2, DORA and more.

Awakeness

- ✓ Train and test everyone in the organization, personalize content with AI/data science, focus on industry, risk scoring and job role specifics.
- ✓ Real, near real-time industry specific simulation, leveraging strategic partnership with international CERTs and spear phishing - user specific simulation
- ✓ Aim to become a fire and forget platform, receiving pre-configured comprehensive reports

Customers' Benefits

Cost Savings

Save $177,708

on average by reducing data breaches with effective training.

Proactive Security Posture

70% reduction

Cyber security awareness training leads to a 70% reduction in security-related risks in 2023.

Regulatory Compliance

Meet and exceed compliance standards required in many industries, such as **DORA, GDPR, HIPAA, PCI DSS, NIS 2**

Reduced Risks

Reduce human-error-related breaches (82% of incidents involve a human element).

Stats source: https://keepnetlabs.com/blog/2024-security-awareness-training-statistics

The platform now

Gamification
Boost engagement and retention with gamified training, including competition and recognition.

Learning Hub Library
Up to date, multi-language educational content on common cyber security awareness topics.

Awakeness Scoring
Track real-time data, compare it to past performance, and continuously improve your security practices.

Adaptive content
Create tailored training modules for specific user groups, ensuring maximum relevance and engagement.

Efficient Micro Learning
Maximize productivity with focused cybersecurity training that delivers more in less time.

Adaptive simulations
Run real-world phishing and social engineering simulations for complex scenarios.

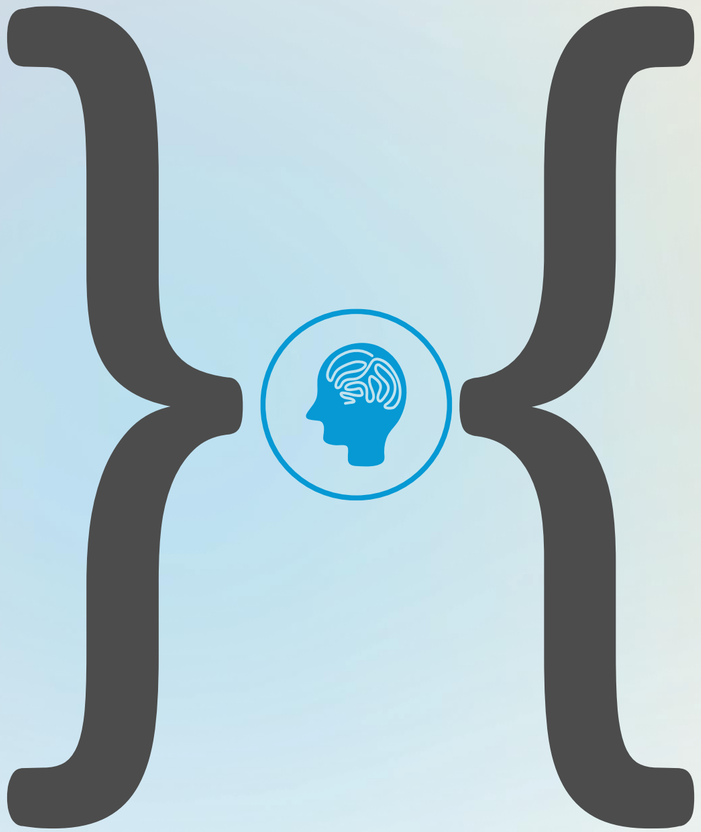
Regulatory Compliance
Stay compliant with major standards like GDPR, HIPAA, PCI DSS, NIS 2, DORA and more.

Unique Value Proposition

Set & Forget Intelligence
Schedule campaigns, assign tasks to the users. The platform goes on auto-pilot.

PersonaLearn AI – Awakeness Evolve
User profile-based, AI-tailored and testing, we use data science and machine learning to change behavior.

ThreatReady Simulator
Real, near real-time industry specific simulation - strategic partnership with with international CERTs and spear phishing - user specific simulation

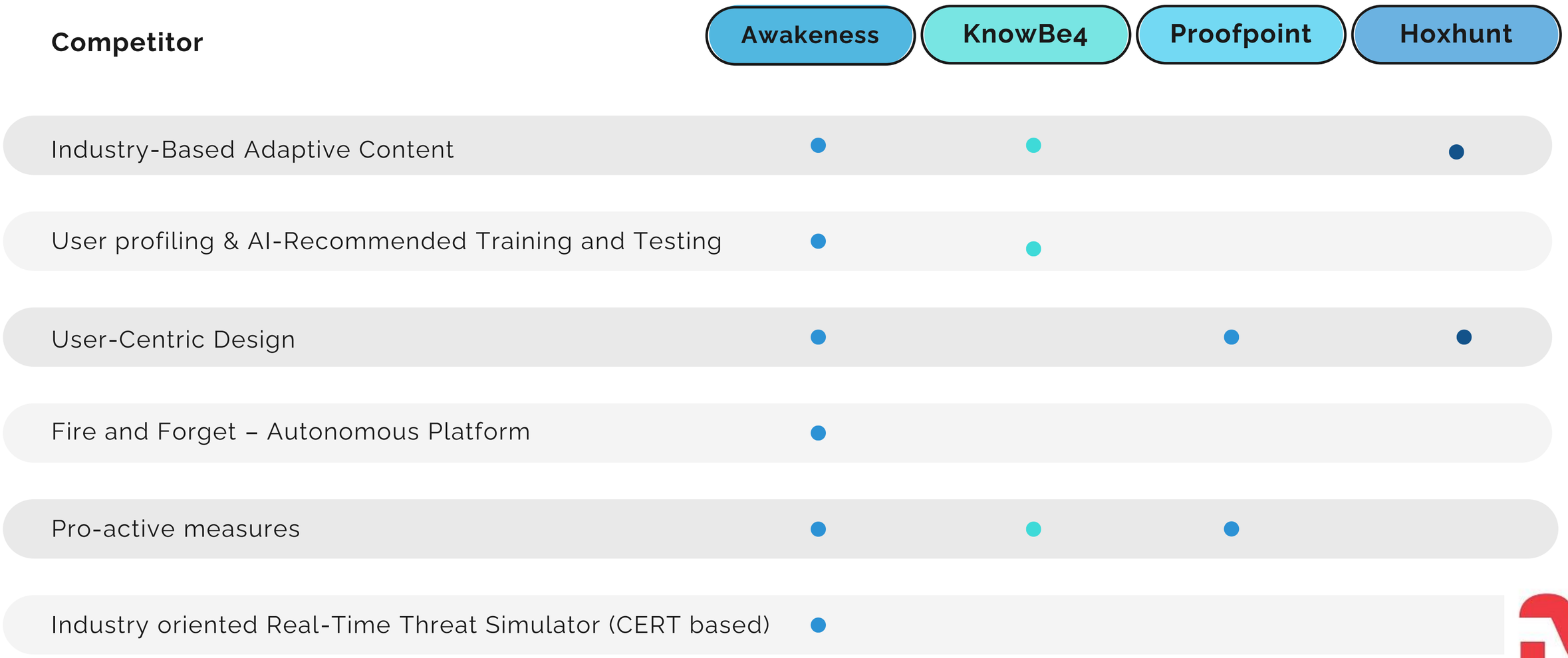


Pro-active protection
Pro-active protection by safeguarding online online identities against domain spoofing and spoofing and phishing

MultiThreat Simulator
Comprehensive solution for simulating channel cyber attacks, including combinations of platforms such as WhatsApp, SMS, and email.

Email Guardian
Mail client add-on designed for Outlook Google Apps, empowering users to their inboxes with enhanced security. Automatically retract reported emails, prioritize and classify.

Competitive Landscape



Thank You!

Find out more at:

www.Netland.ro

Get in touch with us:

office@netland.ro

NETLAND

Technology you can count on.
Customized for your business.