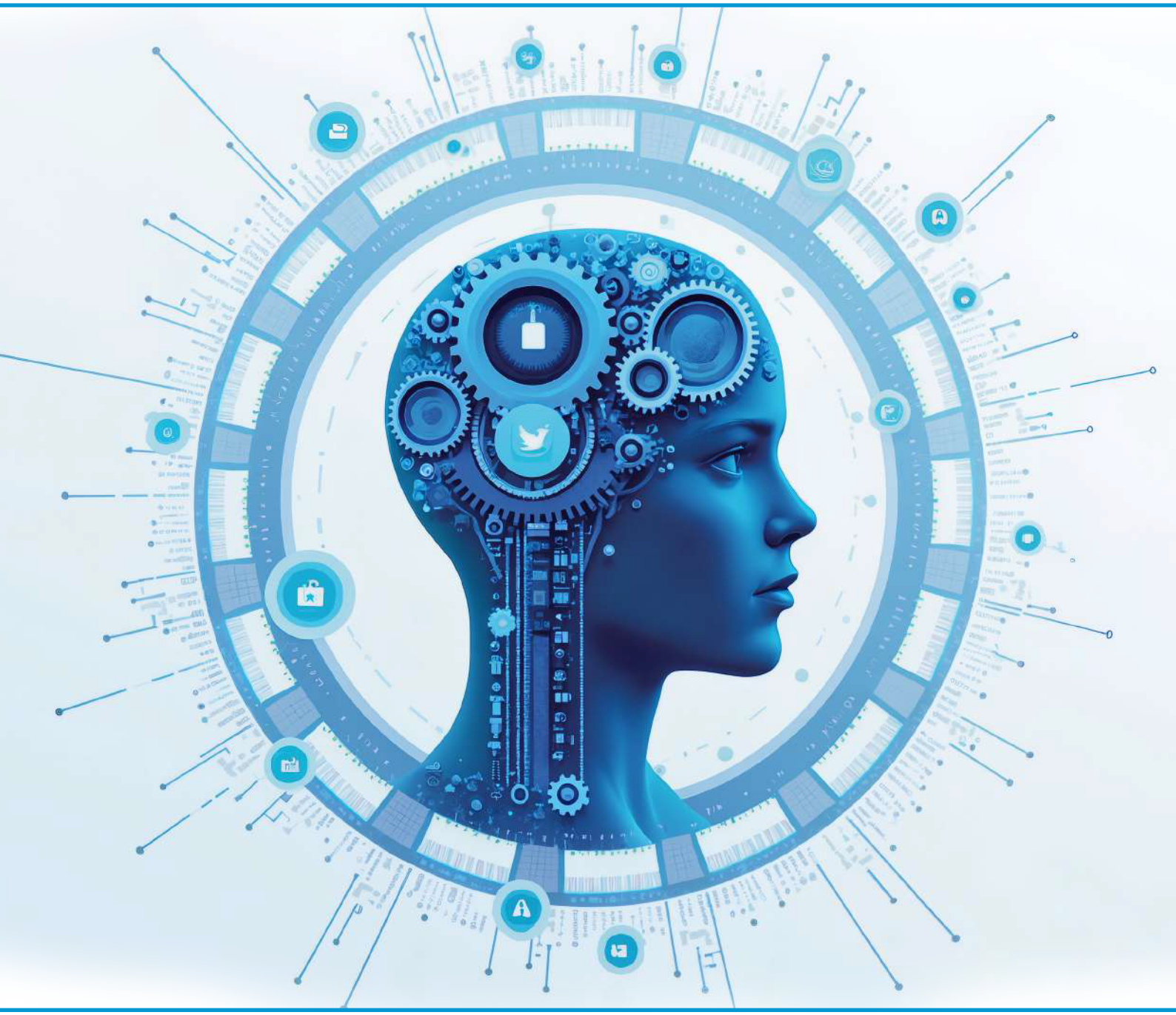
NETLAND

Dezvoltare prin digitalizare



Antrenează-ți echipa pentru a face față amenințărilor cibernetice

O platformă avansată de conștientizare a securității cibernetice, concepută pentru a implica activ și a sprijini angajații să devină prima linie de apărare a organizației.

De ce să alegi Awakeness?

Awakeness oferă un set cuprinzător de instrumente concepute pentru a îmbunătăți postura ta de securitate cibernetică:

Module interactive de microînvățare

Resurse atractive care îi învață pe angajați cele mai bune practici de securitate – administrarea corectă a parolelor, identificarea tentativelor de phishing și raportarea activităților suspecte.

Conformitate și reglementare

Respectă standardele de conformitate necesare în multe industrii, precum: GDPR, NIS 2, DORA, HIPAA, PCI DSS, precum și cele mai bune practici din industria cibernetică: ISO 27k1, NIST.

Raportare și analiză în timp real

Dashboard-ul nostru avansat de analiză urmărește progresul în timp real și îl compară cu performanțele anterioare pentru a rafina și îmbunătăți continuu postura de securitate.

Conținut adaptiv

Module personalizate care răspund nevoilor specifice ale diferiților utilizatori sau grupuri din organizația ta, asigurând relevanță și impact maxim.

Gamificare

Introducerea conceptelor de joc și recompensă în instruirea de securitate sporește motivația, implicarea și capacitatea de a reține informațiile, oferind participanților o experiență prietenoasă, care îi motivează și îi ajută să nu fie intimidați de complexitatea securității cibernetice.

Învățare eficientă

Maximizăm rezultatele învățării într-un timp optim, asigurând productivitatea echipei tale în timp ce stăpânește elementele esențiale ale securității cibernetice, adoptând filosofia „mai puțin înseamnă mai mult".

Beneficii

- Conformitate și reglementare: Respectă standardele de conformitate necesare precum: GDPR, NIS, HIPAA, PCI DSS, precum și cele mai bune practici din industria cibernetică: ISO 27k1, NIST.
- Postură proactivă de securitate: Îmbunătățește securitatea organizației, pregătind angajații să detecteze și să răspundă amenințărilor cybernetice înainte ca acestea să se materializeze.
- Reducerea riscurilor: Scade probabilitatea apariției breșelor de securitate cu o echipă mai conștientă de riscuri.
- Împuternicirea angajaților: Prin furnizarea unor programe de instruire personalizate, angajații pot identifica și atenua eficient orice potențială amenințare cibernetică.
- Reducerea costurilor: Evită costurile semnificative asociate cu breșele de date prin investiții în instruire și conștientizare eficientă în domeniul securității cibernetice.

Cazuri de utilizare

- Corporații: Consolidarea culturii de securitate și reducerea riscului uman.
- Întreprinderi mici și mijlocii: Soluție accesibilă pentru protecția datelor și a angajaților.
- Conformitate și reglementare: Sprijin în atingerea cerințelor NIS2, DORA, ISO 27001 etc..
- Sector financiar: Protejarea datelor sensibile și prevenirea fraudelor.
- Educație: Siguranța informațiilor studenților și a instituției.
- Schimbare comportamentală & reziliență: Crearea unor obiceiuri sigure și consolidarea apărării umane.
- Furnizarea de studii de caz sau exemple pentru fiecare caz de utilizare. Oferirea de statistici sau anecdote care demonstrează eficiența produsului în aceste scenarii.
- Respectarea conformității NIS 2: Directiva NIS 2, Articolul 21 – paragraf 2, litera g), transpusă prin OUG 155/30.12.2024, articolul 13, litera i) - "Practicile de bază în materie de igienă cibernetică și formarea în domeniul securității cibernetice"

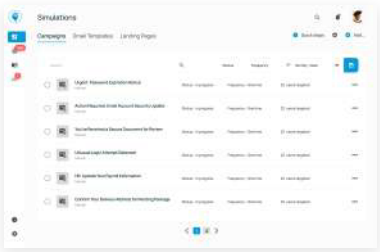
Funcționalități

Hub de învățare

Oferim module interactive și tutoriale despre phishing și ingineria socială, explicând tehnicile utilizate și modul de identificare a acestora prin articole, videoclipuri și teste. Avem o bibliotecă integrată, actualizată permanent, cu diferite niveluri de complexitate, adaptată diverselor nivele de expertiză și expuneri ale utilizatorilor.

Campanii de simulare de phishing și inginerie socială

Folosim propriul motor de simulare pentru a trimite e-mailuri de phishing realiste, clasificate după tip și nivel de complexitate din biblioteca noastră integrată (peste 200 de template-uri de phishing localizate pentru Europa Centrală & de Est). Urmărim creșterea cunoștințelor si modificarea comportamentul angajaților, reducând semnificativ grupul cu risc ridicat și crescând scorul de reziliență al angajaților prin identificarea tiparelor și tendințelor, instruire personalizată, măsuri eficiente și analiză predictivă.

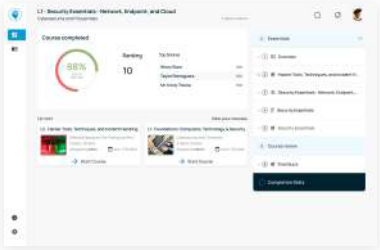


Urmărire, evoluție și raportare

Urmăriți finalizarea învățării pentru fiecare utilizator și fiecare departament, monitorizați rezultatele simulărilor.

Gamificare *

Prin integrarea elementelor de gamificare, cum ar fi competiția, clasamentele și recompensele, creștem angajamentul utilizatorilor și retenția cunoștințelor, asigurând în același timp că participanții sunt motivați și nu intimidați de complexitatea securității cibernetice.



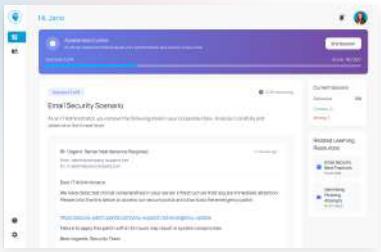
"Awakeness Score"

Poți monitoriza în timp real postura de conștientizare a companiei, bazată pe comportamentul utilizatorilor și pe curba lor de învățare. Scorul „Awakeness" este o metrică esențială care măsoară nivelul de pregătire și vigilență al angajaților împotriva amenințărilor din mediul digital - începând cu phishing și escrocherii prin e-mail, până la atacuri cibernetice avansate.

* (în curând)

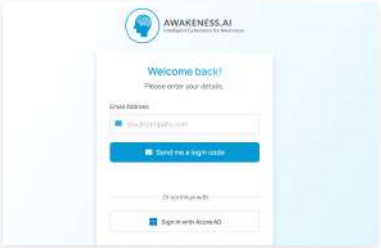
Funcționalități

Awakeness Evolve



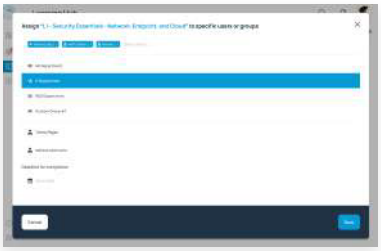
Awakeness Evolve este ecosistemul nostru de instruire de generație următoare, alimentat de AI, care revoluționează conștientizarea securității cibernetice prin adaptarea dinamică și inteligentă a conținutului. Utilizând algoritmi avansați de învățare automată, Awakeness Evolve analizează continuu comportamentul utilizatorilor, modele de învățare și dinamica amenințărilor pentru a crea experiențe de instruire personalizate care evoluează odata cu cu amenințările cibernetice emergente.

SSO - Integration with Microsoft Entra ID



Integrarea perfectă Single Sign-On (SSO) cu Microsoft Entra ID (anterior Azure Active Directory) permite organizațiilor să valorifice infrastructura lor existentă de autentificare, în timp ce încorporează materialele de instruire ale clientului. Utilizatorii pot accesa instruirea de conștientizare a securității cibernetice prin intermediul acreditărilor lor familiare de autentificare organizațională, asigurând o experiență de utilizator optimizată și securitate îmbunătățită.

Learning Management System (LMS)



Soluție LMS completă cu funcționalități de bază incluzând gestionarea conținutului, gestionarea utilizatorilor, livrarea cursurilor, evaluări și urmărirea progresului. Caracteristicile avansate includ trasee de învățare, gamificare, raportare și analize. Clientul poate încărca propriile materiale în diverse formate (.pdf, .docx, .xlsx, pptx etc.), creând un mediu de instruire cuprinzător adaptat nevoilor organizaționale.

Awakeness eMail Security Toolbox

Un asistent simplu care verifică configurația email-ului companiei dumneavoastră pentru puncte slabe, vă ajută să setați protecțiile corecte și testează în siguranță dacă cineva ar putea imita domeniul dumneavoastră prin spoofing. Verifică setările de protecție a email-ului domeniului dumneavoastră și arată clar ce este securizat și ce necesită atenție. Testează SPF, DKIM, DMARC, înregistrările MX, setările de criptare TLS (MTA-STS și TLS-RPT) și BIMI.

Domain Threat Intelligence - Domain Watcher

O soluție proactivă de securitate cibernetică, care identifică automat domenii asemănătoare celor ale organizației dumneavoastră. Prin analizarea domeniilor legitime și generarea a sute de variații similare (ex: „cornpany.com" în loc de „company.com"), sistemul descoperă domenii care pot fi folosite în atacuri de phishing, imitare/ spoofing a identității mărcii și alte activități malițioase. Platforma oferă o analiză cuprinzătoare, incluzând înregistrări DNS și fluxuri de informații despre amenințări, pentru o vizibilitate completă asupra riscurilor existente.

Funcționalități

Email Breach Monitor

Breach Alert este o funcționalitate de conștientizare a securității de la Awakeness care vă permite să verificați rapid dacă o adresă de e-mail apare în breșe de date cunoscute public, scurgeri sau baze de date din dark web.

Specificații ale platformei de conștientizare a securității cibernetice

Caracteristică	Descriere	Beneficii
Algoritmi de învățare adaptivă	Module personalizate care răspund nevoilor specifice ale diferitelor tipuri de utilizatori sau grupuri din organizația ta, asigurând relevanță și impact maxim.	Asigură angajament și eficiență prin adaptarea conținutului la profilul și nivelul fiecărui cursant.
Module Q&A interactive	Ofera module de testare interactivă, prin întrebări și răspunsuri care verifică înțelegerea tehnicilor folosite de atacatori și modul de recunoaștere a acestora.	Ajută la consolidarea cunoștințelor acumulate din videoclipuri și la identificarea domeniilor în care este necesară instruire suplimentară.
Feedback și analiză	Dashboard-ul nostru avansat de analiză urmărește progresul în timp real și îl compară cu performanțele anterioare pentru a rafina și îmbunătăți postura de securitate.	Asigură învățare continuă prin feedback constant și permite corectarea rapidă a neclarităților.
Gamificare	Procesul de instruire este îmbogățit prin elemente de joc, precum competiția, clasamentele și premiile.	Crește motivația pentru învățare și promovează un mediu educațional competitiv.
Simulatoare de inginerie socială	Folosim propriul nostru motor de simulare pentru a trimite e-mailuri de phishing realiste, clasificate după tip și nivel de sofisticare.	Pregătește angajații pentru amenințări reale și ajută la identificarea persoanelor vulnerabile din cadrul organizației.
Programe de invățare personalizate	Conținut adaptiv care poate fi ajustat în funcție de rolurile specifice și departamentele din cadrul unei organizații.	Asigură relevanță și învățare direcționată conform nevoilor specifice și riscurilor asociate diferitelor roluri.
Monitorizare și raportare	Urmărește parcurgerea și cursurilor pentru fiecare utilizator și monitorizează rezultatele simulărilor, atât individual, cât și la nivel de departament sau companie.	Furnizează date esențiale pentru audit și evalueaza eficiența programului de instruire.

Specificații ale platformei de conștientizare a securității cibernetice

Caracteristică	Descriere	Beneficii
Suport pentru conținut multimedia	Conținut interactiv care educă utilizatorii în privința celor mai bune practici de securitate: gestionarea parolelor, recunoașterea e-mailurilor de tip phishing și raportarea activităților suspecte.	Îmbunătățește implicarea cursanților în procesul de învățare și se adaptează nevoilor lor specifice.
"Awakeness Score"	Calculează postura de securitate a companiei, bazată pe comportamentul utilizatorilor și curba de învățare.	Măsoară nivelul general de pregătire și vigilență al angajaților tăi împotriva diverselor tipuri de amenințări cibernetice.