Anexa nr. 1

SPECIFICAȚIA TEHNICĂ

Nr. d/o	Denumirea Bunurilor	Denumirea modelului	Produ-cătorul	Țara de origine	Specificația tehnică solicitată	Specificația tehnică ofertată	Standarde de referință
Lotul: Subscriere pentru soluția de instruire și testare a cunoștințelor în domeniul securității informației							
1	Subscriere pentru soluția de instruire și testare a cunoștințelor în domeniul securității informației	https://Outthink.io OutThink este o platformă revoluționară de management al riscului uman în domeniul securității cibernetice, care oferă echipelor de securitate capacitatea de a acționa asupra sursei a până la 90% din toate brețele de date:			**Tip:** Subscriere pentru soluția de Training de Conștientizare în Securitate de Nouă Generație și Simulare AI de Phishing, destinată instruirii și testării cunoștințelor în domeniul securității informației, pentru 12 luni. **Cerințe generale:** Soluția trebuie să permită: • transmiterea de mesaje de Phishing și SPAM în scop de instruire; • colectarea și analiza datelor statistice aferente comportamentului utilizatorilor; • organizarea și livrarea instruirilor ulterioare în scop de îmbunătățire; • utilizarea, la necesitate și în limita utilității pentru Beneficiar, a componentelor suplimentare: SMS phishing, Voice phishing și scenarii AI/Deepfake. **Cantitate licențe:** Licență pentru 200 utilizator pentru o perioadă de 12 luni. **Cerințele minime solicitate:**	• Din aspectul cerințelor generale, platforma asigură în proporție de 90% funționalitățile solicitate. • Platforma nu asigură conformitate cu cerința privind existenta componentelor de SMS Phishing, voice phising și AI/Deepfake	Pentru estimarea per fiecare cerință și comentariile corespunzătoare, rugăm să accesați fișierul: Anexa nr 1 - Detaliat - NBM - Evaluare functională si tehnică.xlsx Pentru acces la materiale adiționale, acesați fișierul: Outthink - Linkuri Utile.xlsx

		comportamentul uman.			***1. Cerințe funcționale – Simulare Phishing (email) și SPAM:*** **a. Livrare eșalonată și contextuală a phishing-ului** – soluția trebuie să permită capacitatea de a livra mai multe emailuri de phishing în mod eșalonat, la diferite ore ale zilei, adaptate la fusurile orare și la tiparele de comportament ale utilizatorilor, pentru a crește realismul și gradul de implicare. **b. Șabloane bazate pe threat intelligence** – soluția trebuie să permită utilizarea feed-urilor de threat intelligence externe sau interne pentru a recomanda și genera șabloane de phishing relevante. **c. Opțiuni de personalizare** – soluția trebuie să permită control complet asupra aspectului emailurilor de phishing, inclusiv branding, ton, limbaj, linkuri, domenii, pagini de autentificare și pagini de destinație. Suport pentru crearea de șabloane prin drag-and-drop. **d. Șabloane de phishing țintite** – soluția trebuie să permită oferirea de șabloane predefinite pentru roluri, departamente și persoane specifice, precum: noii angajați, contractori și angajați care lucrează remote. **e. Previzualizare în timp real a emailurilor** – soluția trebuie să permită posibilitatea de a previzualiza în timp real emailurile de phishing în platforme precum Outlook (desktop/web), Android, iOS și Microsoft Teams.	Aferent cerințelor funcționale, platforma asigură toate cerințele, mai puțin punctul **f. – Capabilități de automatizare** și **h. Tehnici avansate de phishing** *Aferent Cerința f. –* platforma asigură o acoperire parțială. Soluția permite programarea diferitor campanii, dar nu neapărat dinamic. *Aferent cerință h* - Platforma este integrată cu MS Teams, însă nu asigura phishing prin QR sau spear-phishing.	

					f. Capabilități de automatizare – soluția trebuie să permită programarea campaniilor viitoare care selectează dinamic dificultatea șabloanelor și conținutul de training în funcție de nivelul de risc și comportamentul istoric al utilizatorilor. **g. Suport multilingv** – soluția trebuie să asigure traducerea automată a șabloanelor de phishing și a conținutului de training asociat în limbile selectate. **h. Tehnici avansate de phishing** – soluția trebuie să permită suport pentru metode suplimentare precum phishing prin Microsoft Teams, phishing prin cod QR și spear-phishing cu voce clonată. ***2. Cerințe funcționale – Training anti-phishing:*** **a. Training alocat dinamic** – soluția trebuie să permită alocarea automată a modulelor de training relevante utilizatorilor care au fost compromiși, în funcție de interacțiunile lor cu emailurile și de nivelul de risc. **b. Experiență de învățare gamificată** – soluția trebuie să permită oferirea de experiențe de învățare interactive, cu leaderboard-uri, badge-uri și puncte pentru a crește implicarea utilizatorilor. **c. Export de training compatibil SCORM** – soluția trebuie să asigure suport pentru exportarea conținutului de training în format	**Aferent grupului de 2. Cerințe funcționale – Training anti-phishing,** soluția asigură toate cerințele, mai puțin	

					SCORM, pentru utilizarea în platforme LMS externe. **d. Ghid interactiv pentru IOC (Indicators of Compromise)** – soluția trebuie să permită oferirea de ghiduri pas cu pas pentru identificarea indicatorilor de compromitere din emailurile de phishing, dincolo de simple evidențieri sau tooltip-uri. **e. Învățare interactivă de tip „bite-sized”** – soluția trebuie să permită module scurte și interactive, cu quiz-uri, exerciții de tip drag-and-drop și materiale video. ***3. Cerințe de Funcționalitate (Capabilități AI):*** **a. Gen AI pentru crearea de conținut** – soluția trebuie să permită crearea și editarea șabloanelor de phishing și a conținutului de conștientizare cibernetică folosind prompturi în limbaj natural, cu suport pentru input bazat pe documente. **b. Simulări Deepfake audio/video** – soluția trebuie să permită capacitatea de a simula conținut audio/video realist de tip deepfake pentru a imita directori de top (CEO, CIO etc.) în scenarii avansate de phishing și conștientizare cibernetică. **c. Mesaje de tip „follow-up nudges”** – soluția trebuie să permită trimiterea de memento-uri sau sfaturi scurte prin email sau Teams către utilizatorii care au fost anterior compromiși, pentru a consolida vigilența.	conformitatea cu cerința c. Export training compatibil SCORM. Materialele nu pot fi descărcate de pe platforma Outthink.io, însă sunt disponibile pentru toată perioada de subscriptie. Aferent grupei de cerinte ***3. Cerințe de Funcționalitate (Capabilități AI):*** Soluția corespunde tuturor cerințelor, mai puțin cerinței **b. Simulări Deepfake audio/video** Materialele de instruire / training tratează subiectul identificării deepfake, însă un poate asigura mecanisme de simulare nemijlocită.	

					4. Cerințe de Funcționalitate (Raportare și Analiză): **a. Scor dinamic de risc al utilizatorilor –** soluția trebuie să permită atribuirea de scoruri dinamice de risc pe baza răspunsurilor la simulările de phishing și a implicării în training. **b. Rapoarte exportabile –** soluția trebuie să permită generarea de rapoarte la cerere sau programate, în format PDF, personalizate pentru diferiți factori de decizie (Security Lead, CISO, CIO). **c. Rapoarte și dashboard-uri**, care să includă cel puțin următoarele metrici: • Utilizatori care au vizualizat emailul; • Utilizatori care au dat click pe link; • Utilizatori care au introdus credențiale; • Utilizatori care au descărcat atașamente; • Utilizatori care au scanat coduri QR; • Utilizatori care au raportat emailul ca phishing/junk/spam; • Utilizatori care au mutat emailul în alt folder; • Utilizatori care au redirecționat emailul către alt utilizator/mailbox; • Utilizatori care au șters emailul; • Utilizatori care nu au deschis emailul în timpul simulării; • Număr total de utilizatori țintiți; • Număr de emailuri livrate cu succes; • Statusul completării trainingului; • Raportare bazată pe locație;	Grupa de cerințe ***4. Cerințe de Funcționalitate (Raportare și Analiză) este*** *asigurată în totalitate în cadrul platformei, mai puțin celei aferente scanării QR*	

					• Dashboard de nivel de risc; • Dashboard pe departamente; • Raport „Repeat Offenders”; • Utilizatori care au ratat simularea sau nu au interacționat (ex: OOO); • Dashboard Executiv. ***5. Cerințe de Funcționalitate (Integrări):*** **a. Integrare Microsoft Teams** – soluția trebuie să permită simulări de phishing, nudges și acces la training direct din Microsoft Teams. b. **Integrare Outlook Report Message** – soluția trebuie să permită raportarea simulărilor de phishing prin butonul nativ „Report Message” din Outlook și urmărirea acestora. ***6. Cerințe de Funcționalitate (Training și Conștientizare în Securitate Cibernetică):*** **a. Conținut de awareness bazat pe rol –** soluția trebuie să permită conținut adaptat departamentelor (Financiar, Juridic, HR), rolurilor (Developer, Data Analyst, Compliance, etc.) și persoanelor (New Joiner, Remote Worker, Contractor). **b. Threat of the Month** – soluția trebuie să permită trimiterea lunară de emailuri cu cele mai importante amenințări cibernetice, personalizate în funcție de departament sau rol. **c. Campanii programate de conștientizare** – soluția trebuie să permită posibilitatea de a	***Grupa de cerințe 5. Cerințe de Funcționalitate (Integrări)*** *Este satisfăcută 100%, existând integrare cu MS TEams si MS Outlook.* *Grupul de cerințe* ***6. Cerințe de Funcționalitate (Training și Conștientizare în Securitate Cibernetică)*** este asigurat în cadrul platformei outthink.io, mai puțin cerința e.Personalizare a conținutului, care	

					programa campanii săptămânale, bilunare sau lunare prin email, Teams, screensavere etc. **d. Conținut de awareness pre-ambalat** – soluția trebuie să permită conținut actualizat și gata de utilizare pentru subiecte precum JIT, JEA, PIM, autentificare fără parolă, bune practici de utilizare AI/Co-Pilot/ChatGPT. **e. Personalizare a conținutului** – soluția trebuie să permită posibilitatea de personalizare cu voice-over și alte funcționalități de adaptare a conținutului. ***7. Cerințe non-funcționale:*** **a. Criptarea datelor –** soluția trebuie să asigure criptarea datelor atât în repaus, cât și în tranzit. **b. Confidențialitatea datelor –** soluția trebuie să asigure găzduirea tuturor datelor BNM în conformitate cu protecția datelor cu caracter personal. **c. Retenția și arhivarea datelor –** soluția trebuie să asigure suport pentru retenția datelor până la 3 ani. **d. Livrare SaaS –**soluția trebuie să fie livrată ca platformă SaaS accesibilă prin browser, fără infrastructură on-premises sau instalări locale. **e. Controlul accesului bazat pe roluri (RBAC) –** soluția trebuie să asigure suport pentru RBAC, pentru gestionarea permisiunilor utilizatorilor în funcție de roluri și responsabilități. **Suport de la Producător**:	este satisfăcută doar parțial (lipsă voice over) ***Grupul de cerințe 7. Cerințe non-funcționale*** este asigurat în totalitate.	

					- 12 luni; - suport prin e-mail sau conectare de la distanță.		

Semnătura electronică a administratorului / reprezentantului:

Valeriu Cernei, Administrator

BSD Management SRL

Digitally signed by Cernei Valeriu
Date: 2026.03.16 18:38:56 EET
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ