Anexa nr.1

Specificaţii tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către BNM – în coloanele 1, 5]

Numărul procedurii de achiziţie: **ocds-b3wdp1-MD-1744878751134** din **17 aprilie 2025**						
Denumirea procedurii de achiziţie: **Servicii de subscriere la soluția de protecție a activelor digitale, monitorizare a amenințărilor externe din mediul online și asigurare a securității cibernetice**						
Denumirea bunurilor/servic iilor	**Denumirea modelului**	**Ţara de origine**	**Produ-cătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
1	**2**	**3**	**4**	**5**	**6**	**7**
Lotul: Servicii de subscriere la soluția de protecție a activelor digitale, monitorizare a amenințărilor externe din mediul online și asigurare a securității cibernetice						
Servicii de subscriere la soluția de protecție a activelor digitale, monitorizare a amenințărilor externe din mediul online și asigurare a securității cibernetice	**1. SKU: (EXECPROTECTE5)** Executive Protection Essentials (5-pack) – 1 buc; **2. SKU: (PBRANDPROTECT)** Primary Brand Protection – 1 buc; **3. SKU: (Intelligence Search)** Intelligence Search – 1 buc; **4. SKU: (MANAGEDPLATFOR)** Managed Platform for 12 M – 1 buc; **5. SKU: (TD-1-FY24)** Takedowns – 12 buc.	**SUA**	**ZeroFox**	**Tip:** Servicii de subscriere la soluția de protecție a activelor digitale, monitorizare a amenințărilor externe din mediul online și asigurare a securității cibernetice, abonament pentru 12 luni. **Cerințe generale:** Soluția trebuie să includă capacități de detectare, monitorizare și atenuare a amenințărilor legate de resursele digitale ale BNM, inclusiv conturi, domenii, aplicații mobile, scurgeri de date și alte amenințări din surse deschise și restricționate.	**Tip:** Se oferă Servicii de subscriere la platforma producătorului Zerofox pentru protecția activelor digitale, monitorizare a amenințărilor externe din mediul online și asigurare a securității cibernetice, abonament pentru 12 luni. **Descriere generală:** Soluția ofertată va include capacități de detectare, monitorizare și atenuare a amenințărilor legate de resursele digitale ale BNM, inclusiv conturi, domenii, aplicații mobile, scurgeri de date și alte amenințări din surse deschise și restricționate.	*Nu se aplică*

				<u>Cerințele minime solicitate:</u> 1. **Atenuarea Amenințărilor** • Capacitate de blocare și eliminare a conturilor, site-urilor web și conținutului fraudulos, malițios și ilegal. • Suport pentru rețele sociale, magazine de aplicații mobile, site-uri clonate, domenii și alte platforme. • Automatizare a solicitărilor de eliminare (takedonw) printr-o rețea globală de parteneri pentru blocarea conținutului. • Capacitate de urmărire a stării procesării solicitărilor printr-o platformă centralizată. • Suport din partea unei echipe de gestionare a incidentelor disponibilă 24/7. • Eliminări universale (takedown): minim 12 eliminări incluse în licența oferită.	**<u>Funcționalitățile platformei ofertate:</u>** 1. **Atenuarea Amenințărilor (SKU: (TD-1-FY24) Takedowns – 12 buc.)** • Capacitate de blocare și eliminare a conturilor, site-urilor web și conținutului fraudulos, malițios și ilegal. • Suport pentru rețele sociale, magazine de aplicații mobile, site-uri clonate, domenii și alte platforme. • Automatizare a solicitărilor de eliminare (takedonw) printr-o rețea globală de parteneri pentru blocarea conținutului. • Capacitate de urmărire a stării procesării solicitărilor printr-o platformă centralizată. • Suport din partea unei echipe a producătorului de gestionare a incidentelor disponibilă 24/7. • Eliminări universale (takedown): minim 12 eliminări incluse în licența oferită.	

				2. Protecția managementului și Personalului Cheie • Minim 5 angajați sau manageri incluși în licența oferită. • Monitorizare impersonificarea conturilor, conturilor neoficiale pe rețele sociale. • Monitorizare a posibilelor credențiale compromise inclusiv deep web și dark web. • Monitorizare pentru doxxing – detectarea publicării neautorizate de informații private prin căutări în baze de date publice, rețele sociale și utilizarea tehnicilor de hacking și inginerie socială pentru identificarea intențiilor malițioase. • Detectare continuă și eliminare automată a datelor personale expuse pe site-uri de brokeraj de date.	**2. Protecția managementului și Personalului Cheie(SKU: (EXECPROTECTE5)** Executive Protection Essentials (5-pack) – 1 buc;**)** • 5 angajați sau manageri incluși în licența oferită. • Monitorizare impersonificarea conturilor, conturilor neoficiale pe rețele sociale. • Monitorizare a posibilelor credențiale compromise inclusiv deep web și dark web. • Monitorizare pentru doxxing – detectarea publicării neautorizate de informații private prin căutări în baze de date publice, rețele sociale și utilizarea tehnicilor de hacking și inginerie socială pentru identificarea intențiilor malițioase. • Detectare continuă și eliminare automată a datelor personale expuse pe site-uri de brokeraj de date.	

				3. Protecția Mărcii și a Companiei • Monitorizare pentru amenințări la adresa mărcii și BNM pentru un (1) brand, acoperind toate sursele de date (deschise, deep și dark web). Include protecție împotriva: - Impersonării mărcii - Mențiunilor negative afferent mărcii - Evidențelor de încălcare a securității în surse non-OSINT (exfiltrare de date, compromitere de credențiale, carduri de credit și alte date personale sau proprietare) • Include protecție pentru: - 1 domeniu și toate subdomeniile sale - 1 cont social media corporative - 1 aplicație mobilă • Monitorizarea amenințărilor în cadrul tuturor surselor disponibile (deschise, deep și dark web). • Detectare a impersonărilor, mențiunilor negative, scurgerilor de date și	**3. Protecția Mărcii și a Companiei(SKU: (PBRANDPROTECT)** Primary Brand Protection – 1 buc;**)** • Monitorizare pentru amenințări la adresa mărcii și BNM pentru un (1) brand, acoperind toate sursele de date (deschise, deep și dark web). Include protecție împotriva: - Impersonării mărcii - Mențiunilor negative afferent mărcii - Evidențelor de încălcare a securității în surse non-OSINT (exfiltrare de date, compromitere de credențiale, carduri de credit și alte date personale sau proprietare) • Include protecție pentru: - 1 domeniu și toate subdomeniile sale - 1 cont social media corporative - 100 aplicații mobile • Monitorizarea amenințărilor în cadrul tuturor surselor disponibile (deschise, deep și dark web). • Detectare a impersonărilor, mențiunilor negative,	

				compromiterii credențialelor. • Suport pentru protecția domeniului, conturilor de social media corporative, aplicațiilor mobile și activelor financiare. • Monitorizare a scurgerilor de date, compromiterii credențialelor și altor informații sensibile. **4. Informații și Căutări de Amenințări** • Acces la o bază de date de informații despre amenințări cibernetice, inclusiv atacuri, vulnerabilități și indicatori de compromitere. Include minim: - Licență pentru un utilizator al platformei de informații - Cheie API Enterprise pentru acces la baza de date de informații - Căutări nelimitate privind amenințările - Rapoarte strategice de informații - Suport tehnic 24/7	scurgerilor de date și compromiterii credențialelor. • Suport pentru protecția domeniului, conturilor de social media corporative, aplicațiilor mobile și activelor financiare. • Monitorizare a scurgerilor de date, compromiterii credențialelor și altor informații sensibile. **4. Informații și Căutări de Amenințări(SKU: (Intelligence Search)**Intelligence Search – 1 buc;**)** • Acces la o bază de date de informații despre amenințări cibernetice, inclusiv atacuri, vulnerabilități și indicatori de compromitere. Include: - Licență pentru un utilizator al platformei de informații - Cheie API Enterprise pentru acces la baza de date de informații - Căutări nelimitate privind amenințările - Rapoarte strategice de informații - Suport tehnic 24/7	

				• Corelare rapidă a alertelor cu indicatorii de compromitere (IOC) cunoscuți, precum: - Domenii de Command and Control (C2) - Credite compromise - IP-uri „zombie” din logurile Botnet - Hash-uri ransomware și malware • Analize detaliate ale actorilor de amenințare care vizează domeniul bancar și regiunea din proximitate, incluzând tacticile, tehnicile și procedurile (TTP) conform cadrului MITRE și MISP. • Investigații pentru colectarea indicatorilor de atac (IOA), indicatorilor de compromitere (IOC) și discuțiilor din Dark Web pentru îmbunătățirea strategiei defensive. • Analiza vulnerabilităților și exploiturilor critice pentru prioritizarea și recomandarea măsurilor de atenuare a amenințărilor. • Rapoarte și analize automate, inclusiv rezumate strategice și IoC.	• Corelare rapidă a alertelor cu indicatorii de compromitere (IOC) cunoscuți, precum: - Domenii de Command and Control (C2) - Credite compromise - IP-uri „zombie” din logurile Botnet - Hash-uri ransomware și malware • Analize detaliate ale actorilor de amenințare care vizează domeniul bancar și regiunea din proximitate, incluzând tacticile, tehnicile și procedurile (TTP) conform cadrului MITRE și MISP. • Investigații pentru colectarea indicatorilor de atac (IOA), indicatorilor de compromitere (IOC) și discuțiilor din Dark Web pentru îmbunătățirea strategiei defensive. • Analiza vulnerabilităților și exploiturilor critice pentru prioritizarea și recomandarea măsurilor de atenuare a amenințărilor. • Rapoarte și analize automate, inclusiv rezumate strategice și IoC.	

				5. Platformă Gestionată • Monitorizare a amenințărilor 24/7 de către specialiști SOC. • Colectare automată și manuală de informații din surse OSINT (deschise), deep și dark web. • Suport pentru analiză a amenințărilor bazată pe inteligență artificială. • Acces la rapoarte privind vulnerabilitățile și analizele amenințărilor cibernetice. • Includerea materialelor de instruire și a suportului pentru utilizatori. • **OnWatch Alert**: gestionarea amenințărilor 24x7x365 de către experți SOC. • **Colectare Globală de Informații (GIC)**: colectare de date din toate sursele OSINT (deschise), Deep și Dark Web, inclusiv rețele sociale, forumuri ascunse, repositore de cod și baze de date de vulnerabilități.	**5. Platformă Gestionată (SKU: (MANAGEDPLATFOR)** Managed Platform for 12 M – 1 buc;**)** • Monitorizare a amenințărilor 24/7 de către specialiști SOC. • Colectare automată și manuală de informații din surse OSINT (deschise), deep și dark web. • Suport pentru analiză a amenințărilor bazată pe inteligență artificială. • Acces la rapoarte privind vulnerabilitățile și analizele amenințărilor cibernetice. • Includerea materialelor de instruire și a suportului pentru utilizatori. • **OnWatch Alert**: gestionarea amenințărilor 24x7x365 de către experți SOC. • **Colectare Globală de Informații (GIC)**: colectare de date din toate sursele OSINT (deschise), Deep și Dark Web, inclusiv rețele sociale, forumuri ascunse, repositore de cod și baze de date de vulnerabilități.	

				• **Motor de analiză AI**: analiză automată a amenințărilor folosind inteligență artificială. • **Informații Finisate & Alerte privind Vulnerabilitățile**: rapoarte strategice și informări despre vulnerabilitățile și amenințările curente. **Suport de la Producător**: - 12 luni; suport prin e-mail sau conectare de la distanță.	• **Motor de analiză AI**: analiză automată a amenințărilor folosind inteligență artificială. • **Informații Finisate & Alerte privind Vulnerabilitățile**: rapoarte strategice și informări despre vulnerabilitățile și amenințările curente. **Suport de la Producător**: - 12 luni; suport prin e-mail sau conectare de la distanță. Nota: Detalii suplimentare pot fi gasite in datasheturi anexate cu oferta sau pe pagina web a producatorului: *https://www.zerofox.com/data-sheets/*	

Semnat:
Nume: **Irina Vicol**
În calitate de: **Administrator**
Ofertantul: **Xontech Systems SRL**
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova.

Digitally signed by Vicol Irina
Date: 2025.04.29 12:02:16 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ