MINISTERUL FINANȚELOR

Oficiul Naţional de Prevenire şi Combatere a Spălării Banilor

**Specificații tehnice**

Furnizorul va livra Achizitorului **1 licență** de software specializat ce oferă soluții de analiză a datelor blockchain și de investigație în domeniul criptomonedelor, **pentru o perioadă de 1 an de zile,** având următoarele caracteristici:

1. Principalele activități
2. Software-ul de investigație trebuie să conecteze adresele de criptomonede la entități din lumea reală și să creeze vizualizări intuitive bazate pe cluster pentru fluxurile de tranzacții cu criptomonede;
3. Soluția trebuie să furnizeze informații actualizate despre tranzacțiile cu criptomonede în timp aproape real;
4. Urmează fluxul fondurilor prin intermediul unui număr nelimitat de interconexiuni și identifică activități suspecte legate de entități din lumea reală;
5. Instrumentul ar trebui să poată afișa expunerea directă și indirect a tranzacțiilor urmărind fluxul fondurilor;
6. Trebuie să poată filtra expunerea după categorie;
7. Soluția va fi gazduită într-un mediu bazat pe cloud, dar trebuie să aibă și capacitatea de a fi implementată pe infrastructura locală la un moment ulterior;
8. Atunci când sunt adăugate mai multe clustere sau adrese și aceste clustere sau adrese adăugate au efectuat tranzacții între ele, software-ul de investigație trebuie să interconecteze automat aceste clustere sau adrese;
9. Capacitatea de a permite clienților să îsi gestioneze propriii utilizatori;
10. Autentificare unică cu capabilitati Open ID Connect;
11. Soluția ar trebui să ofere analiză Peel Chain prin detectarea automată a Peel Chain-ului acolo unde este posibil sau evidențierea modificării în transferuri;
12. Soluția trebuie să permită utilizatorului să caute un anumit VASP de interes. Rezultatele căutării trebuie să ofere utilizatorilor:
* Prezentarea general a expunerii VASP-ului la diferite contra-părți;
* Categorile de contra-părți;
* Expunerea trebuie să includă atât expunerea directă, cât și expunerea indirectă, atât pentru tranzacțiile de primire, cât și pentru cele de trimitere;
* Nu trebuie să existe nicio limită în ceea ce privește numărul de interconexiuni pentru calculul expunerii indirecte;
* Prezentarea generală a expunerii VASP-ului trebuie să includă numărul total și valoarea tranzacțiilor directe și indirecte cu respectivele categorii de contra-părți;
* Identificarea și atribuirea unei adrese de portofel unei contrapărți trebuie să fie deterministă și bazată pe dovezi, nu pe un scor probabilistic﻿﻿;
* Istoricul tranzacțional;
* Soldul;
* Informații despre OSINT disponibile;
* Informații cu privire la posibilitatea ca eventualele servicii grupate să fie prezente pe lista de sancțiuni OFAC;
1. Soluția trebuie să ofere o prezentare generală a profilului adresei VASP-ului, inclusiv, dar fără a se limita la următoarele:
	1. Numărul total de adrese asociate VASP-ului și
	2. Numărul total de active stocate în adresele VASP-ului;
	3. Informații despre diferitele criptomonede utilizate de un VASP, dacã este cazul.
2. Soluția trebuie să identifice adresele asociate cu activități sau entități ilicite și să furnizeze următoarele detalii:
	1. Numărul total de adrese identificate de soluție ca fiind asociate cu activități sau entități ilicite;
	2. Lista acestor adrese identificate; și
	3. Numărul și tipul de active stocate în aceste adrese.
3. Importul clusterelor de către software-ul de investigație cu URL-uri de grafic, fișiere în format proprietar și în format CSV;
4. Sortarea activității contra-părților după suma trimisă, primită și numărul de transferuri / activitatea contra-părtilor;
5. Soluția trebuie să permită utilizatorului să caute o anumită adresă de interes. Soluția trebuie să accepte și introducerea mai multor adrese și gruparea lor în clustere multiple;
6. Instrumentul trebuie să aibă o reprezentare picturală interactivă a diverselor categori ilicite în care s-au descoperit tranzacții implicate în piața Darknet, Transferuri de schimb valutar, Servicii fără nume, Escrocherii, Schimburi p2p, Amestecare în alte scopuri, Pool-uri de minare, Schimburi cu risc ridicat, Jocuri de noroc, Finanțarea terorismului, Sancțiuni etc.;
7. Trebuie să existe un filtru pentru categorile de activități ilicite pentru expunerea de primire și de trimitere;
8. Instrumentul trebuie să permită crearea unui grafic de vizualizare care indică fluxul fondurilor prin mai multe interconexiuni si să fie ușor de construit și de înteles;
9. Ar trebui să efectueze investigații pe următoarele token-uri: ALGO, BTC, BCH, BSV, DASH, DOGE, EOS, ETH (inclusiv peste 100 de token-uri ERC-20), ETC, LTC, OMNI, inclusiv token-ul USDT, SOL, TRX, inclusiv token-ul USDT, XRP, ZEC;
10. Trebuie să mapeze sute de milioane de adrese catre entități din lumea reală, putand adauga servicii noi;
11. Trebuie să includă servicii ilicite precum piețele Darknet, escrocherii și software de răscumpărare, precum și servici legitime precum platforme DeFi, pool-uri de minare și servicii comerciale;
12. Trebuie să urmărească fluxul fondurilor prin intermediul unui număr nelimitat de "hop-uri" și să lege activitățile suspecte de entități din lumea reală.
13. Exportul de grafice în fișiere de imagine PNG sau într-un format proprietar;
14. Partajarea graficelor sub formă de URL-uri;
15. Exportul tranzacțiilor și informaților de metadate (de exemplu, geolocația) sub formă de fișiere CSV structurate;
16. Trebuie să fie posibilă construirea unei narative de grafic cu adnotări;
17. Software-ul trebuie sä furnizeze rezultate precise prin urmarea unei abordări deterministe și non-probabilistice în atribuirea adreselor și clusterelor entităților din lumea reală;
18. În software, trebuie să fie posibil să se adauge portofelul investigat la o listă de portofele monitorizate, care urmărește și alertează când portofelul investigat efectuează tranzacții; Aceste alerte de tranzacții pot fi primite în aplicație sau prin notificări prin e-mail;
19. Capacitatea de a efectua urmărirea Cross-Chain;
20. Soluția trebuie să urmărească automat fondurile prin cel puțin 3 servicii de mixing;
21. Soluția trebuie să furnizeze date complet auditabile, bazându-se pe dovezi reale care rezistă în fața instanței de judecată.
22. Software-ul trebuie să furnizeze functionalitatea de identificare a informaților de geo-localizare și adresă IP a portofelelor deținute privat, colectate ca parte a procesului de analiză a blockchain-ului;
23. Trebuie să ofere o capacitate integrată nelimitată de căutare avansată pentru interogări complexe care constau în locație (țară + oraș), categorie de expunere (de exemplu, sancțiuni), perioadă de timp și sumă tranzactională;
24. Software-ul de investigație trebuie să furnizeze informații despre geolocație pentru portofelele BTC pentru mai mult de 4 ani;
25. Datele trebuie să conțină informații despre geolocație pentru portofelele ETH. Deși utilizatorul nu se așteaptă că astfel de informații să fie disponibile pentru toate portofelele ETH, furnizorul soluției trebuie să poată prezenta statistic care să arate cel puțin o acoperire temporară a acestor date.
26. **Securitatea informației**

 Securitatea informației reprezintă un aspect crucial al acestui proiect, iar produsele solicitate vor include implementarea măsurilor și protocoalelor de securitate necesare pentru protejarea datelor confidențiale și a integrității sistemului de analiză a tranzacțiilor pe blockchain, asigurând astfel că informațiile sensibile și procesele de analiză sunt protejate împotriva accesului neautorizat și a potențialelor amenințări cibernetice.

1. **Implementare**

Actualizări și patch-uri

Software-ul de analiză a tranzacțiilor pe blockchain va beneficia de actualizări și patch-uri periodice pentru a asigura funcționalitatea optimă și securitatea soluției. Aceste actualizări vor fi implementate în conformitate cu planul de mentenanță stabilit și vor urmări să remedieze vulnerabilități, să aducă îmbunătățiri funcționale și să țină pasul cu evoluțiile tehnologice și reglementările din domeniu.

Monitorizarea și raportarea performanței

Pentru asigurarea performanței și eficienței soluției, se va realiza o monitorizare constantă a sistemului. Vor fi implementate instrumente de monitorizare și se vor efectua teste periodice pentru evaluarea performanței și identificarea eventualelor probleme. De asemenea, se vor genera rapoarte periodice referitoare la performanța soluției și la eventualele acțiuni întreprinse pentru remedierea deficiențelor identificate.

Suport tehnic și asistență

Furnizorul software-ului de analiză a tranzacțiilor pe blockchain va furniza suport tehnic și asistență pentru rezolvarea problemelor tehnice, asigurarea funcționării corecte a soluției și îndrumarea utilizatorilor în utilizarea eficientă a acestuia.

Instalare și configurare

Furnizorul software-ului va fi responsabil de instalarea și configurarea soluției în mediul operațional al Autorității contractante. Aceste activități vor fi efectuate conform celor mai bune practici și a cerințelor specifice ale soluției. Se vor realiza teste de funcționalitate și compatibilitate pentru a se asigura că sistemul este configurat corect și funcționează în parametri stabiliți.