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-1690981060608** din **25 august 2023**

Denumirea procedurii de achiziţie: **Pachete software aferente securității informaționale**

Denumirea bunurilor/serviciilor	Denumirea modelului	Ţara de origine	Producătorul	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
Lot 1: *Subscriere anuală pentru soluția de asigurare a accesului securizat la date de pe dispozitivele mobile*						
Subscriere anuală pentru soluția integrată pentru gestiunea aplicațiilor și dispozitivelor mobile, pentru 100 utilizatori	**MobileIron/ Ivanti Endpoint Manager Mobile Secure Premium per User On-premise Subscription with Assurance Support for 100 users. (5 devices/user) 01.11.2023-31.10.2024**	**SUA/UK**	**Ivanti UK Limited**	Conform caietului de sarcini solicitat, mentionat in Anexa 1 la formular. Matricea de conformitate	Conform caietului de sarcini solicitat, mentionat in Anexa 1 la formular. Matricea de conformitate	*Nu se aplică*
Lot 6: *Soluție de colectare și analiză a log-urilor SIEM*						
Soluție de colectare și analiză a log-urilor SIEM	**SE-T-LIC-ST Splunk Enterprise - Term License with Standard Success Plan – 10 GB/day**	**SUA**	**Splunk Inc.**	Conform caietului de sarcini solicitat, mentionat in Anexa 1 la formular. Matricea de conformitate	Conform caietului de sarcini solicitat, mentionat in Anexa 1 la formular. Matricea de conformitate	*Nu se aplică*

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: 2023.08.18 11:22:08 EEST
Reason: MoldSign Signature
Location: Moldova

Anexa 1

Matricea de conformitate conform cerințelor solicitate in Anexa 1 pentru Lotul 1 si Lotul 6:

Nr. d/o	Denumirea bunurilor solicitate	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant
Lotul 1: ***Subscriere anuală pentru soluția de asigurare a accesului securizat la date de pe dispozitivele mobile***			
1.	Subscriere anuală pentru soluția integrată pentru gestiunea aplicațiilor și dispozitivelor mobile, pentru 100 utilizatori	**Tip:** Subscriere anuală pentru 100 utilizatori, pentru soluția integrată pentru gestiunea aplicațiilor și dispozitivelor mobile, MobileIron Secure Unified Endpoint Management Premium Bundle per User (5 Devices/User) , sau echivalentul, pentru perioada 01.11.2023-31.10.2024, exploatată în cadrul Sistemului Informațional al BNM. **Notă:** Pentru cazul când Ofertantul va oferi o altă soluție decât MobileIron, care este la moment exploatată în cadrul SI al BNM, Ofertantul, va fi responsabil pentru livrarea, instalarea, configurarea (inclusiv configurarea politicilor inițiale) şi punerea în funcţiune a soluției. **<u>Cerințe tehnice și specifice:</u>** Sistemul propus trebuie să fie o soluție inovatoare, care să asigure următoarele cerințe: **1. Cerințe pentru Securitatea datelor corporative:** • Controlul securizat al accesului la datele corporative; • Autentificare bifactorială la datele corporative; • Prevenirea pierderilor de date (DLP); • Posibilitatea de implementare a politicilor de criptare (dispozitiv, SD); • Posibilitatea de securizare și control pentru E-mail și DLP: - Control asupra atașamentelor email; - Control asupra datelor inserate sau copiate;	**Tip:** *Subscriere anuală pentru 100 utilizatori, pentru soluția integrată pentru gestiunea aplicațiilor și dispozitivelor mobile,* ***MobileIron/ Ivanti Endpoint Manager Mobile Secure Premium per User On-premise Subscription with Assurance Support for 100 users. (5 devices/user)****, pentru perioada 01.11.2023-31.10.2024, exploatată în cadrul Sistemului Informațional al BNM.* ***Avind in consideratie ca este ofertata subscriptia pentru solutia deja exploatata in cadrul Sistemului Informațional al BNM, toate cerintele solicitate in caietul de sarcini vor fi acoperite in totalitate si se va prezenta Certificatul de renewal cu perioada mentionată mai sus.***

		• Posibilitatea de securizare și control al browser-ului mobil; • Posibilitatea de ștergere condiționată a datelor corporative de pe dispozitivele mobile; • Posibilitatea de a lucra offline (nu necesită o conexiune permanentă la server pentru identificarea și eliminarea amenințărilor pe dispozitive); • Partajarea datelor corporative de cele personale(BYOD); • Posibilitatea de creare a canalului VPN securizat per aplicație (inclusiv Windows). **2. Cerințe pentru Managementul Aplicațiilor:** • Identificarea aplicațiilor mobile instalate și posibilitatea de distribuție a aplicațiilor noi; • Posibilitatea de categorizare a aplicațiilor mobile; • Posibilitatea de creare a listelor admise/interzise de aplicații mobile; • Posibilitatea de creare a restricțiilor pentru rețele wi-fi; • Managementul aplicațiilor mobile (magazine intern de aplicații mobile); • Publicare și livrare centralizată sigură a aplicațiilor mobile; • Containerizarea aplicațiilor mobile. **3. Cerințe pentru Managementul dispozitivelor;** • Posibilitatea de încadrare a dispozitivelor mobile personale, în mediul corporativ (BYOD); • Posibilitatea utilizatorilor de auto-înrolare a dispozitivelor mobile (self-service) în sistem; • Posibilitatea de integrare a soluției cu infrastructura existentă a întreprinderii; - Active Directory; - Aplicații interne a companiei (aplicații Web, Mobile); - FileServer; - SIEM;	

		• Managementul conținutului dispozitivului mobil; • Managementul dispozitivelor mobile; • Posibilitatea de creare a modului de lucru KIOSK; • Geo-localizarea dispozitivelor mobile; • Suport pentru o gamă extinsă de platforme: - Windows 10 Desktop; - MacOS; - Android; - iOS; • Sistemul trebuie să ofere funcții avansate de gestionare pentru PC-urile Windows 10 precum: - personalizarea aspectului sistemului; - executarea scripturilor PowerShell (.ps1); - executarea de scripturi pentru modificarea registrului (.reg); - setarea BitLocker pentru criptarea discului; - gestionarea drepturilor utilizatorului; - setarea accesului la funcțiile Windows (meniul de setări); - instalarea oricărui GPO prin registru; - gestionarea sistemului de fișiere; - instalarea de drivere; - instalarea aplicațiilor LOB; - instalarea pachetelor software; - dezinstalarea software-ului preinstalat; - gestionarea imprimantei, etc. **4. Cerințe pentru Serverul de administrare:** • Instalarea componentelor serverului soluției nu trebuie să necesite preinstalarea unui sistem de operare separat și a unei baze de date separate, precum și a licențelor lor separate; • Posibilitatea de a instala componente suplimentare de server:	

		- pentru a asigura funcționarea sistemului cu disponibilitate ridicată (high availability); - posibilitatea utilizării în scopuri de testare înainte de a adăuga orice funcționalitate în mediul de lucru; • Soluția trebuie să asigure extinderea cu ușurință a dispozitivelor gestionate; • Posibilitatea de update a soluției direct din consola de administrare, fără implicarea directă a producătorului; • Android Enterprise suport pentru dispozitivele BYOD. **5. Certificări conform standardelor internaționale:** • FIPS 140-2; • ISO/IEC 27001:2013; • Common Criteria Certification; Cerința de certificare poate fi demonstrata prin prezentarea copiei certificatului, sau referință pe site-ul producătorului. **Alte cerințe obligatorii:** Suport de la Producător oferit: - suport 24/24, prin e-mail sau conectare de la distanță; - asigurarea accesului la update-uri si Baza de cunoștințe (Knowledge Base + Product Updates).	
Lot 6: ***Soluție de colectare și analiză a log-urilor SIEM***			
1.	Soluție de colectare și analiză a log-urilor SIEM	**Tip:** Soluție de colectare și analiză a log-urilor SIEM inclusiv 12 luni de suport și menținere de la producător Cantitate: 1 licență Modelul de licențiere trebuie să acopere cel puțin 10 GB de evenimente pe zi.	**Tip:** Soluție de colectare și analiză a log-urilor SIEM: **SE-T-LIC-ST Splunk Enterprise - Term License with Standard Success Plan – 10 GB/day** inclusiv 12 luni de suport și menținere de la producător Cantitate: 1 licență Modelul de licențiere acoperă 10 GB de evenimente pe zi.

		Cerințe tehnice: 1. Soluția trebuie sa întrunească următoarele cerințe: • Managementul evenimentelor; • Investigarea incidentelor si fluxurilor; • Automatizări și răspunsuri la incidente; • Monitorizare și alerte în timp real pentru amenințările cunoscute și necunoscute (APT); • Abilitatea de face corelații între sursele de date pentru a identifica patern-uri specifice; • Păstrarea datelor pe termen lung. 2. Soluția trebuie să fie un singur produs integrat atât pentru managementul evenimentelor cât și altor scenarii din SIEM și anume: • Interfața de utilizator unică pentru toate funcționalitățile sistemului, inclusiv căutări, managementul rapoartelor, regulilor și administrarea sistemului; • Loc de stocare unic pentru toate tipurile de date ingerate; • Soluția trebuie să mențină accesul la date și managementul acestora prin intermediul unui browser; • Administrarea și configurarea trebuie să fie realizată prin intermediul interfeței Web și/sau CLI. 3. Soluția trebuie să fie printre liderii de top conform Quadrant of the Gartner Magic Quadrant pentru soluții SIEM. 4. Soluția trebuie sa asigure integrarea cu alte sisteme prin intermediul modulelor descărcate de pe un portal propriu online ce ar permite tratarea diferitor scenarii. 5. Componenta de stocare și ingestie a datelor trebuie să ofere capacitatea de încărcare a nu mai puțin de 10 GB pe zi evenimente cu termen de păstrare, subscriere și menținere pentru o perioadă de minim 1 an.	**Cerințe tehnice:** 1. Soluția inruneste următoarele cerințe: • Managementul evenimentelor; • Investigarea incidentelor si fluxurilor; • Automatizări și răspunsuri la incidente; • Monitorizare și alerte în timp real pentru amenințările cunoscute și necunoscute (APT); • Abilitatea de face corelații între sursele de date pentru a identifica patern-uri specifice; • Păstrarea datelor pe termen lung. 2. Soluția este un produs integrat atât pentru managementul evenimentelor cât și altor scenarii din SIEM și anume: • Interfața de utilizator unică pentru toate funcționalitățile sistemului, inclusiv căutări, managementul rapoartelor, regulilor și administrarea sistemului; • Loc de stocare unic pentru toate tipurile de date ingerate; • Soluția mentine accesul la date și managementul acestora prin intermediul unui browser; • Administrarea și configurarea este realizată prin intermediul interfeței Web și/sau CLI. 3. Soluția este printre liderii de top conform Quadrant of the Gartner Magic Quadrant pentru soluții SIEM. 4. Soluția asigura integrarea cu alte sisteme prin intermediul modulelor descărcate de pe un portal propriu online ce ar permite tratarea diferitor scenarii. 5. Componenta de stocare și ingestie a datelor ofera capacitatea de încărcare a 10 GB pe zi evenimente cu termen de păstrare, subscriere și menținere pentru o perioadă de 1 an.

		Scalabilitate, arhitectura și caracteristici tehnice: 1. Soluția trebuie sa ofere scalabilitate și stocarea datelor să fie nelimitată în acord/raportat cu spațiul de stocare disponibil al clientului. 2. Soluția trebuie să mențină accesul la datele stocate imediat și să poată face căutări istorice indexate și extrem de rapide. 3. Soluția trebuie sa ingereze orice tip de date (text, stream, wineventlog). 4. Soluția nu trebuie să fie dependentă de careva softuri care necesită licențiere separată. 5. Stocarea datelor nu trebuie să impună o limită a numărului de câmpuri care pot fi indexate și extrase ulterior în timpul căutărilor datelor. 6. Să permită stocarea datele în format brut și să nu fie modificate oferind o posibilitate de căutare fără reducerea acestora. 7. Să permită mascarea datelor (ex. numărul cardului bancar, IDNP sau alte date confidențiale) înainte ca acestea sa fie stocate. 8. Păstrarea datelor trebuie să mențină posibilitatea de plasare a lor în diferite locuri de depozitare a datelor separate logic pentru a oferi o performanță optimă de căutare sau segregare a datelor. 9. Accesul la date trebuie să fie granular cu posibilitatea de a acorda/limita accesul către anumite date. 10. Autentificarea utilizatorilor pentru acces la administrarea soluţiei, dar și pentru utilizarea acesteia trebuie să se poată realiza pe bază de conturi de utilizatori definiţi local, integrare cu sisteme terţe precum Microsoft Active Directory, LDAP sau SAML. 11. Soluția trebuie sa mențină marcajul de timp (time stamp) pentru fiecare eveniment. 12. Trebuie să permită comprimarea automată a datelor stocate pentru a reduce volumul lor pe mediul de stocare. 13. Setările de păstrare a datelor trebuie sa fie flexibile după cum urmează: * Timpul de păstrare a datelor trebuie să fie flexibil;	**Scalabilitate, arhitectura și caracteristici tehnice:** 1. Soluția ofera scalabilitate și stocarea datelor este nelimitată în acord/raportat cu spațiul de stocare disponibil al clientului. 2. Soluția mentine accesul la datele stocate imediat si poate face căutări istorice indexate și extrem de rapide. 3. Soluția ingereza orice tip de date (text, stream, wineventlog). 4. Soluția nu este dependentă de careva softuri care necesită licențiere separată. 5. Stocarea datelor nu impune o limită a numărului de câmpuri care pot fi indexate și extrase ulterior în timpul căutărilor datelor. 6. Permite stocarea datelor în format brut și să nu fie modificate oferind o posibilitate de căutare fără reducerea acestora. 7. Permite mascarea datelor (ex. numărul cardului bancar, IDNP sau alte date confidențiale) înainte ca acestea sa fie stocate. 8. Păstrarea datelor mentine posibilitatea de plasare a lor în diferite locuri de depozitare a datelor separate logic pentru a oferi o performanță optimă de căutare sau segregare a datelor. 9. Accesul la date este granular cu posibilitatea de a acorda/limita accesul către anumite date. 10. Autentificarea utilizatorilor pentru acces la administrarea soluţiei, dar și pentru utilizarea acesteia se poată realiza pe bază de conturi de utilizatori definiţi local, integrare cu sisteme terţe precum Microsoft Active Directory, LDAP sau SAML. 11. Soluția mentine marcajul de timp (time stamp) pentru fiecare eveniment. 12. Permite comprimarea automată a datelor stocate pentru a reduce volumul lor pe mediul de stocare. 13. Setările de păstrare a datelor sunt flexibile după cum urmează: * Timpul de păstrare a datelor este flexibil;

		* Controlul granular prin GUI a datelor stocate. Datele vechi pot fi transferate către stocare externă sau eliminate la necesitate. 14. Soluția trebuie să asigure redundanța în timp real a datelor pentru a asigura disponibilitatea acestora. Totodată, trebuie să fie posibilă stocarea multi-site a datelor. În cazul în care un site nu este disponibil, datele sa fie automat disponibile în site-ul accesibil. 15. Soluția trebuie să dețină un mecanism de asigurare a integrității datelor în tranzit cât și a celor stocate. 16. Soluția trebuie să conțină auditul acțiunilor efectuate însăși în cadrul soluției (ex. cine, când si ce date a accesat; auditul modificărilor, etc.) 17. Soluția trebuie să ofere capacitatea de a mări performanța de corelare prin adăugarea unor instanțe (noduri) suplimentare fără a fi necesară o licența suplimentară. 18. Soluția trebuie să asigure instalarea în mod distribuit (pe noduri) a componentelor sale. 19. Soluția trebuie să dețină, la punctul de colectare, un mecanism de stocare temporară de tip „cache”. Acest mecanism va asigura retransmiterea ulterioară a datelor pentru a evita supraîncărcarea rețelei. 20. Soluția trebuie să asigure exportarea evenimentelor colectate în format CSV. 21. Soluția trebuie să ofere un mecanism integrat de compresie a datelor stocate și permite definirea unor politici diferite de retenție a evenimentelor colectate. 22. Soluția trebuie să asigure execuţia de corelări bazate pe reguli şi să ofere posibilitatea definirii unor acţiuni de răspuns ce includ cel puțin: - crearea unui eveniment; - notificare în interfaţa grafică; - execuţia automată a unor comenzi configurabile cel puţin la nivelul soluţiei de analiză şi la nivelul agenţilor de colectare; - transmiterea unui email.	* Controlul granular prin GUI a datelor stocate. Datele vechi pot fi transferate către stocare externă sau eliminate la necesitate. 14. Soluția asigura redundanța în timp real a datelor pentru a asigura disponibilitatea acestora. Totodată, este posibilă stocarea multi-site a datelor. În cazul în care un site nu este disponibil, datele vor fi automat disponibile în site-ul accesibil. 15. Soluția detine un mecanism de asigurare a integrității datelor în tranzit cât și a celor stocate. 16. Soluția contine auditul acțiunilor efectuate însăși în cadrul soluției (ex. cine, când si ce date a accesat; auditul modificărilor, etc.) 17. Soluția ofera capacitatea de a mări performanța de corelare prin adăugarea unor instanțe (noduri) suplimentare fără a fi necesară o licența suplimentară. 18. Soluția asigura instalarea în mod distribuit (pe noduri) a componentelor sale. 19. Soluția detine, la punctul de colectare, un mecanism de stocare temporară de tip „cache”. Acest mecanism va asigura retransmiterea ulterioară a datelor pentru a evita supraîncărcarea rețelei. 20. Soluția asigura exportarea evenimentelor colectate în format CSV. 21. Soluția ofera un mecanism integrat de compresie a datelor stocate și permite definirea unor politici diferite de retenție a evenimentelor colectate. 22. Soluția asigura execuţia de corelări bazate pe reguli şi ofera posibilitatea definirii unor acţiuni de răspuns ce includ: - crearea unui eveniment; - notificare în interfaţa grafică; - execuţia automată a unor comenzi configurabile la nivelul soluţiei de analiză şi la nivelul agenţilor de colectare; - transmiterea unui email.

		23. Toate obiectele şi resursele definite la nivelul soluţiei de către utilizatori trebuie să poată fi salvate pentru a fi reutilizate ulterior. 24. Soluția trebuie să integreze informaţii de geolocaţie pentru adresele IP identificate în trafic. 25. Soluția trebuie să asigure colectarea evenimentelor de securitate generate din mai multe locaţii geografice. 26. Soluția trebuie să asigure monitorizarea centralizată a stării agenţilor de colectare şi a celorlalte componente ale soluției. 27. Soluția trebuie să ofere posibilitatea de notificare a utilizatorilor sau grupurilor de utilizatori în funcţie de anumiți parametri configurabili. 28. Soluţia trebuie să asigure rularea unor comenzi direct la nivelul evenimentelor de interes, astfel încât să poată fi obţinute informaţii suplimentare (de exemplu: ping, traceroute, whois, nslookup, informaţii despre port). 29. Soluția trebuie să asigure vizualizarea evenimentelor colectate în format brut și normalizat. 30. Soluția trebuie să ofere posbilitatea de clasificare și prioritizare a evenimentelor în funcție de criticitatea acestora. 31. Soluția trebuie să asigure accesul securizat la interfața grafică, prin intermediul protocolului SSL. **Implementare:** 1. Soluția trebuie să fie în versiune software. 2. Trebui să mențină orice tip de virtualizare și echipamente hardware. 3. Soluția trebuie să fie ușor de implementat și gestionat. 4. Soluția trebuie să fie compatibilă cu sistemele de operare Linux și Windows (Linux – OS RedHat nu mai jos de versiunea 9 și Windows 2019 și versiuni mai noi). **Capabilități, Security/SIEM Use Cases:** 1. Reguli de corelare: * Regulile de corelare trebuie să fie ușor de modificat, iar căutările noi de corelare trebuie să fie ușor de creat;	23. Toate obiectele şi resursele definite la nivelul soluţiei de către utilizatori pot fi salvate pentru a fi reutilizate ulterior. 24. Soluția integreaza informaţii de geolocaţie pentru adresele IP identificate în trafic. 25. Soluția asigura colectarea evenimentelor de securitate generate din mai multe locaţii geografice. 26. Soluția asigura monitorizarea centralizată a stării agenţilor de colectare şi a celorlalte componente ale soluției. 27. Soluția ofera posibilitatea de notificare a utilizatorilor sau grupurilor de utilizatori în funcţie de anumiți parametri configurabili. 28. Soluţia asigura rularea unor comenzi direct la nivelul evenimentelor de interes, astfel încât pot fi obţinute informaţii suplimentare (de exemplu: ping, traceroute, whois, nslookup, informaţii despre port). 29. Soluția asigura vizualizarea evenimentelor colectate în format brut și normalizat. 30. Soluția ofera posbilitatea de clasificare și prioritizare a evenimentelor în funcție de criticitatea acestora. 31. Soluția asigura accesul securizat la interfața grafică, prin intermediul protocolului SSL. **Implementare:** 1. Soluția este în versiune software. 2. Mentine orice tip de virtualizare și echipamente hardware. 3. Soluția este ușor de implementat și gestionat. 4. Soluția este compatibilă cu sistemele de operare Linux și Windows (Linux – OS RedHat nu mai jos de versiunea 9 și Windows 2019 și versiuni mai noi). **Capabilități, Security/SIEM Use Cases:** 1. Reguli de corelare: * Regulile de corelare sunt ușor de modificat, iar căutările noi de corelare sunt ușor de creat;

		* Fiecare regulă de corelare trebuie să aibă o atribuire automată, configurabilă a severității; * Opțiuni flexibile de căutare și alerte; 2. Regulile de corelare, căutările și vizualizările trebuie să acopere mai multe categorii și tehnologii de securitate, inclusiv, dar fără a se limita la: autentificări, utilizarea conturilor implicite, malware, modificări configurații Endpoint, patch levels, firewall-uri, IDS, scanări de vulnerabilități, web proxy-uri, activitate anormală HTTP și modificări port/protocol. 3. Trebuie să aibă o mulțime de rapoarte și dashboard-uri. 4. Trebuie să aibă un posibilitatea evaluării bazate pe riscuri pentru identificarea riscului relativ al entităților. 5. Trebuie să ofere actualizări de conținut care se referă la punctele de mai sus. 6. Rapoartele și dashboard-urile trebuie să aibă capabilitatea de a trecere de la un dashboard la datele vizate. 7. Rapoartele și dashboard-urile trebuie să conțină filtre câmpurile ajustabile pentru a reduce afișarea datelor la ceea ce este necesar utilizatorului. 8. Soluția trebuie să mențină analiza incidentelor și fluxurilor. 9. Detaliile despre fiecare incident trebuie să includă cel puțin: * Context suplimentar din surse externe și active; * Istoricul fluxului de lucru al evenimentului. 10. Abilitatea de modificare manuală a gravității incidentului. 11. Abilitatea de actualizare automată a firewall-urilor, IPS sau reguli de securitate a Endpoint-ului. 12. Abilitatea de a utiliza surse externe pentru a crea reguli de corelare mai specifice ca exemplu: * Informații despre angajați (Extras AD/LDAP); * Informații despre active (assets) (Extras CMDB); * Liste de procese, servicii, adrese IP, porturi, protocoale interzise; * Informații despre amenințări de la adrese IP, nume de domen, alte surse externe de amenințări.	* Fiecare regulă de corelare are o atribuire automată, configurabilă a severității; * Opțiuni flexibile de căutare și alerte; 2. Regulile de corelare, căutările și vizualizările acopera mai multe categorii și tehnologii de securitate, inclusiv, dar fără a se limita la: autentificări, utilizarea conturilor implicite, malware, modificări configurații Endpoint, patch levels, firewall-uri, IDS, scanări de vulnerabilități, web proxy-uri, activitate anormală HTTP și modificări port/protocol. 3. Detine o mulțime de rapoarte și dashboard-uri. 4. Are posibilitatea evaluării bazate pe riscuri pentru identificarea riscului relativ al entităților. 5. Ofera actualizări de conținut care se referă la punctele de mai sus. 6. Rapoartele și dashboard-urile detin capabilitatea de a trecere de la un dashboard la datele vizate. 7. Rapoartele și dashboard-urile contin filtre câmpurile ajustabile pentru a reduce afișarea datelor la ceea ce este necesar utilizatorului. 8. Soluția mentine analiza incidentelor și fluxurilor. 9. Detaliile despre fiecare incident include cel puțin: * Context suplimentar din surse externe și active; * Istoricul fluxului de lucru al evenimentului. 10. Abilitatea de modificare manuală a gravității incidentului. 11. Abilitatea de actualizare automată a firewall-urilor, IPS sau reguli de securitate a Endpoint-ului. 12. Abilitatea de a utiliza surse externe pentru a crea reguli de corelare mai specifice ca exemplu: * Informații despre angajați (Extras AD/LDAP); * Informații despre active (assets) (Extras CMDB); * Liste de procese, servicii, adrese IP, porturi, protocoale interzise; * Informații despre amenințări de la adrese IP, nume de domen, alte surse externe de amenințări.

		13. Abilitatea de a adaugă noi fluxuri de informații despre amenințări fie gratuit sau comerciale sau private. 14. Să pună la dispoziție colectori de date pentru sursele de date populare/recunoscute. 15. Soluția trebuie să asigure investigarea incidentelor de securitate pornind de la evenimentul corelat până la identificarea evenimentelor primare ce au generat alerta. **Analiza Use Case și conformitate:** 1. Dashboard-urile și rapoartele trebuie să fie create cu ușurință. 2. Să poată fi utilizat pentru reglementări în conformitate cu: * PCI * SOX * NIST 800-53 * ISO 27002 * COBIT * SSAE 16 3. Să satisfacă cerințele de audit intern și solicitările de informații ad-hoc ale auditorului. 4. Use Case-urile pot include: * Managementul incidentelor; * Operațiuni IT; * Monitorizare virtualizare si planificare capacități; * Managementul aplicațiilor; * Business analitica. 5. Să fie o soluție unică care ar trebui să suporte toate necesitățile de prelucrare a datelor colectate de la diferiți utilizatori, roluri, subdiviziuni din cadrul organizației. 6. Soluția trebuie să fie capabilă să analizeze evenimentele colectata având la bază tehnologii de Machine Learning, Deep Learning, Generative AI. 7. Soluția trebuie să oferte posibilitatea de a crea dashboard-uri, rapoarte și alerte personalizate, private și sau partajate.	13. Abilitatea de a adaugă noi fluxuri de informații despre amenințări fie gratuit sau comerciale sau private. 14. Pune la dispoziție colectori de date pentru sursele de date populare/recunoscute. 15. Soluția asigura investigarea incidentelor de securitate pornind de la evenimentul corelat până la identificarea evenimentelor primare ce au generat alerta. **Analiza Use Case și conformitate:** 1. Dashboard-urile și rapoartele pot fi create cu ușurință. 2. Să poate de utilizat pentru reglementări în conformitate cu: * PCI * SOX * NIST 800-53 * ISO 27002 * COBIT * SSAE 16 3. Satisface cerințele de audit intern și solicitările de informații ad-hoc ale auditorului. 4. Use Case-urile pot include: * Managementul incidentelor; * Operațiuni IT; * Monitorizare virtualizare si planificare capacități; * Managementul aplicațiilor; * Business analitica. 5. Este o soluție unică care ar trebui să suporte toate necesitățile de prelucrare a datelor colectate de la diferiți utilizatori, roluri, subdiviziuni din cadrul organizației. 6. Soluția este capabilă să analizeze evenimentele colectate având la bază tehnologii de Machine Learning, Deep Learning, Generative AI. 7. Soluția trebuie să oferte posibilitatea de a crea dashboard-uri, rapoarte și alerte personalizate, private și sau partajate.

		Analiza și prelucrarea evenimentelor și logurilor: 1. Soluția trebuie să accepte orice sursă de date, inclusiv orice aplicație, sistem de operare, dispozitiv sau sistem, indiferent dacă este virtual/fizic sau bazat pe cloud. 2. Soluția poate să se bazeze și pe conectori personalizați furnizați de vendor pentru a ingera date din diferite surse. 3. Soluția trebuie să fie „prevăzut pentru viitor”, deoarece poate găzdui noi surse de date sau modificări ale formatului de jurnal al unei surse de date existente. 4. Soluția trebuie să poată ingera jurnalele de evenimente cu mai multe linii sau formate complexe. 5. Sursele evenimentelor de securitate, care pot fi ingerate ar trebui să includă cel puțin: * Firewalls; * Intrusion Detection System / Intrusion Prevention System; * Solutie de autentificare (incluzand LDAP / Active Directory); * Data Loss Prevention; * Anti-malware; * Automated malware analysis tools; * Web security or web proxy; * Email security; * Vulnerability scanners; * File integrity monitoring; * Web application firewalls; * Windows Security logs. 6. Sursele evenimentelor non-security care pot fi ingerate ar trebui să includă cel puțin: * Operating system logs (endpoints and servers); * Email server; * Web server; * DHCP/DNS; * VPN; * Network Flows (NetFlow, IPFIX, etc.);	**Analiza și prelucrarea evenimentelor și logurilor:** 1. Soluția accepta orice sursă de date, inclusiv orice aplicație, sistem de operare, dispozitiv sau sistem, indiferent dacă este virtual/fizic sau bazat pe cloud. 2. Soluția poate să se bazeze și pe conectori personalizați furnizați de vendor pentru a ingera date din diferite surse. 3. Soluția este „prevăzut pentru viitor”, deoarece poate găzdui noi surse de date sau modificări ale formatului de jurnal al unei surse de date existente. 4. Soluția poate ingera jurnalele de evenimente cu mai multe linii sau formate complexe. 5. Sursele evenimentelor de securitate, care pot fi ingerate includ cel puțin: * Firewalls; * Intrusion Detection System / Intrusion Prevention System; * Solutie de autentificare (incluzand LDAP / Active Directory); * Data Loss Prevention; * Anti-malware; * Automated malware analysis tools; * Web security or web proxy; * Email security; * Vulnerability scanners; * File integrity monitoring; * Web application firewalls; * Windows Security logs. 6. Sursele evenimentelor non-security care pot fi ingerate ar includ cel puțin: * Operating system logs (endpoints and servers); * Email server; * Web server; * DHCP/DNS; * VPN; * Network Flows (NetFlow, IPFIX, etc.);

		* PCAP files; * Networking devices (routers, switches); * Databases and mainframes; * NAS devices and filers; * Hypervisor and virtual machine logs; * Service desk; * Call records; * Mobile devices and mobile device management systems; * Server and Endpoint Management tools; * Physical badge data; * Cloud-based applications; * Web analytics; * ERP and CRM; * Custom applications. 7. Soluția trebuie să fie capabilă de a colecta date printr-o gamă largă de mecanisme bazate pe sau fără agenți care respectă următoarele cerințe: * Agent elaborat de furnizor. Agentul trebuie sa mențină un canal criptat de comunicare cu serverul prin TCP și de a stoca datele în regim autonom, de a echilibra transmiterea datelor astfel încât să nu creeze suprasolicitarea canalelor de comunicație între acestea: * Syslog; * TCP or UDP; * SNMP events; * XML; * CSV; * JSON; * WMI; * Custom inputs: * Scripted inputs; * Modular inputs. 8. Soluția trebuie sa poată să se conecteze direct la orice tabel de bază de date SQL și să extragă conținutul pentru a fi ingerat.	* PCAP files; * Networking devices (routers, switches); * Databases and mainframes; * NAS devices and filers; * Hypervisor and virtual machine logs; * Service desk; * Call records; * Mobile devices and mobile device management systems; * Server and Endpoint Management tools; * Physical badge data; * Cloud-based applications; * Web analytics; * ERP and CRM; * Custom applications. 7. Soluția este capabilă de a colecta date printr-o gamă largă de mecanisme bazate pe sau fără agenți care respectă următoarele cerințe: * Agent elaborat de furnizor. Agentul mentine un canal criptat de comunicare cu serverul prin TCP și de a stoca datele în regim autonom, de a echilibra transmiterea datelor astfel încât să nu creeze suprasolicitarea canalelor de comunicație între acestea: * Syslog; * TCP or UDP; * SNMP events; * XML; * CSV; * JSON; * WMI; * Custom inputs: * Scripted inputs; * Modular inputs. 8. Soluția poate să se conecteze direct la orice tabel de bază de date SQL și să extragă conținutul pentru a fi ingerat.

		9. Soluția trebuie să aibă capacitatea de a ingera date noi, externe la datele ingerate anterior, pentru a facilita căutarea și raportarea. 10. Soluția trebuie să poată prelua date brute, ingerate și să le folosească pentru a efectua căutări în orice bază de date sau fișier CSV. * Datele căutate pot avea orice valoare, inclusiv IP-uri, nume de mașini sau servicii/IP-uri externe/porturi/protocoale interzise. 11. Soluția trebuie sa mențină integrarea cu AD, LDAP etc. pentru a extrage informații despre angajați, inclusiv: * Numele de utilizator al angajaților, departamentul, locația, dacă este privilegiat, etc. 12. Soluția trebuie aibă posibilitatea de a corela mai multe nume de utilizator înapoi la un singur angajat. 13. Soluția trebuie să suporte integrarea cu CMDB-uri sau baze de date de active pentru a extrage informații despre active, inclusiv: * Numele dispozitivului, IP, MAC, locație, dacă conține date confidențiale, dacă este relevant pentru o anumită reglementare etc. * Permite posibilitatea de a mapa o adresa IP la numele unei mașini și viceversa. 14. Soluția trebuie sa mențină integrarea cu orice flux de informații despre amenințări, gratuit sau comercial, de la terțe surse. **Căutări, notificări și alerte:** 1. Soluția trebuie sa aibă capacitatea de a efectua căutări full-text pe orice câmp din datele ingerate pe baza de: * Căutare de text liber asemănătoare Google; * Interval de timp selectabil; * Ferestre de timp specifice sau relative până la lună/zi/minut/secundă; * Logica booleană (și, sau, nu, etc.); * Expresii obișnuite; * Sintaxa wild card. 2. Analiza statistică inclusiv: * Număr de apariții, număr distinct de apariții, sumă; * Cele mai comune valori sau cele mai puțin comune valori ale unui câmp; * Minim, maxim;	9. Soluția are capacitatea de a ingera date noi, externe la datele ingerate anterior, pentru a facilita căutarea și raportarea. 10. Soluția poate prelua date brute, ingerate și să le folosească pentru a efectua căutări în orice bază de date sau fișier CSV. * Datele căutate pot avea orice valoare, inclusiv IP-uri, nume de mașini sau servicii/IP-uri externe/porturi/protocoale interzise. 11. Soluția mentine integrarea cu AD, LDAP etc. pentru a extrage informații despre angajați, inclusiv: * Numele de utilizator al angajaților, departamentul, locația, dacă este privilegiat, etc. 12. Soluția are posibilitatea de a corela mai multe nume de utilizator înapoi la un singur angajat. 13. Soluția suporta integrarea cu CMDB-uri sau baze de date de active pentru a extrage informații despre active, inclusiv: * Numele dispozitivului, IP, MAC, locație, dacă conține date confidențiale, dacă este relevant pentru o anumită reglementare etc. * Permite posibilitatea de a mapa o adresa IP la numele unei mașini și viceversa. 14. Soluția mentine integrarea cu orice flux de informații despre amenințări, gratuit sau comercial, de la terțe surse. **Căutări, notificări și alerte:** 1. Soluția are capacitatea de a efectua căutări full-text pe orice câmp din datele ingerate pe baza de: * Căutare de text liber asemănătoare Google; * Interval de timp selectabil; * Ferestre de timp specifice sau relative până la lună/zi/minut/secundă; * Logica booleană (și, sau, nu, etc.); * Expresii obișnuite; * Sintaxa wild card. 2. Analiza statistică inclusiv: * Număr de apariții, număr distinct de apariții, sumă; * Cele mai comune valori sau cele mai puțin comune valori ale unui câmp;

		* Medie, mediană, etc.; * Abatere standard, variație; * Preziceri numerice în baza datelor statistice; * Identificarea valorilor anormale în rezultate care pot fi neregulate sau mai puțin frecvente; * Corelația statistică între câmpuri; * Clasterizare de evenimente pe baza asemănării lor între ele ca un singur eveniment; * Trunchierea valorilor numerice periferice în câmpurile selectate pentru a ajuta la corelarea statistică; * Prima și ultima valoare văzută; * Valori estimate (căutare care analizează datele istorice pentru a prezice matematic valorile viitoare); * Căutări de relații între perechile de câmpuri comparând valorile unui câmp cu un câmp de referință și o pereche de valori; 3. Abilitatea de a aplica logica de căutare de mai sus pentru a găsi valori anormale/anomalii care pot fi amenințări. 4. Căutările ar trebui să permită utilizatorului să extragă date în funcție de cine, ce, când și unde. 5. Căutările pot fi salvate, partajate și modificate cu ușurință. 6. Căutările pot fi în timp real sau programate. 7. Soluția trebuie sa ofere posibilitatea de a rula mai multe căutări simultane. 8. Capabilități de alertare în timp real pe baza de căutare care pot: * Trimite un email; * Adăuga la un flux RSS; * Executa acțiuni complete pe firewall-uri, sisteme de prevenire a intruziunilor și Endpoint Security; * Executa un script personalizat; * Acționa ca „middleware”, permițând acțiuni automate de remediere ce implică diferite produse ale furnizorilor. 9. Nu trebuie să existe un maxim fix privind numărul de căutări sau alerte care pot fi executate.	* Minim, maxim; * Medie, mediană, etc.; * Abatere standard, variație; * Preziceri numerice în baza datelor statistice; * Identificarea valorilor anormale în rezultate care pot fi neregulate sau mai puțin frecvente; * Corelația statistică între câmpuri; * Clasterizare de evenimente pe baza asemănării lor între ele ca un singur eveniment; * Trunchierea valorilor numerice periferice în câmpurile selectate pentru a ajuta la corelarea statistică; * Prima și ultima valoare văzută; * Valori estimate (căutare care analizează datele istorice pentru a prezice matematic valorile viitoare); * Căutări de relații între perechile de câmpuri comparând valorile unui câmp cu un câmp de referință și o pereche de valori; 3. Abilitatea de a aplica logica de căutare de mai sus pentru a găsi valori anormale/anomalii care pot fi amenințări. 4. Căutările permit utilizatorului să extragă date în funcție de cine, ce, când și unde. 5. Căutările pot fi salvate, partajate și modificate cu ușurință. 6. Căutările pot fi în timp real sau programate. 7. Soluția ofera posibilitatea de a rula mai multe căutări simultane. 8. Capabilități de alertare în timp real pe baza de căutare care pot: * Trimite un email; * Adăuga la un flux RSS; * Executa acțiuni complete pe firewall-uri, sisteme de prevenire a intruziunilor și Endpoint Security; * Executa un script personalizat; * Acționa ca „middleware”, permițând acțiuni automate de remediere ce implică diferite produse ale furnizorilor. 9. Nu exista un maxim fix privind numărul de căutări sau alerte care pot fi executate.

		Raportare și dashboard-uri: 1. Soluția ar trebui să permită crearea ușoară a unei game largi de vizualizări (nu se limitează la rapoarte fixe, pre conservate). 2. Vizualizările native ar trebui să includă: * Diagrame de timp; * Diagrame cu linii; * Grafice de bare; * Diagrame cu zone; * Diagrame circulare; * Diagrame Scatterplot; * Calibre radiale, de umplere și de marcare; * Hărți. 3. Vizualizările ar trebui să aibă capacitatea de a se actualiza în timp real. 4. Toate vizualizările acceptă capabilități de detaliere, clic pentru a trece de la rezumate la evenimente brute în câteva secunde. 5. Interfața de utilizator prin glisare și plasare permite utilizatorilor non-tehnici și tehnici să creeze rapoarte complexe fără a fi nevoie să folosească comenzi de căutare sau să înțeleagă formatul datelor brute subiacente. 6. Pentru toate diagramele trebuie sa existe capacitatea simplă de a schimba titlurile, legendele, etichetele și setările axelor. 7. Trebuie să permită editarea simplă „glis and drop” a panourilor tabloului de bord. 8. Trebuie să aibă abilitatea de a imprima cu ușurință evenimente, tabele și vizualizări. 9. Trebuie să aibă abilitatea de a converti tablourile de bord în fișiere PDF și de a programa să fie trimise prin e-mail altor persoane. 10. Trebuie sa aibă abilitatea de a se integra cu cadre și opțiuni de vizualizare externe (D3, Tableau etc.) pentru vizualizări suplimentare. **Livrabile:** Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:	**Raportare și dashboard-uri:** 1. Soluția permite crearea ușoară a unei game largi de vizualizări (nu se limitează la rapoarte fixe, pre conservate). 2. Vizualizările native includ: * Diagrame de timp; * Diagrame cu linii; * Grafice de bare; * Diagrame cu zone; * Diagrame circulare; * Diagrame Scatterplot; * Calibre radiale, de umplere și de marcare; * Hărți. 3. Vizualizările detin capacitatea de a se actualiza în timp real. 4. Toate vizualizările acceptă capabilități de detaliere, clic pentru a trece de la rezumate la evenimente brute în câteva secunde. 5. Interfața de utilizator prin glisare și plasare permite utilizatorilor non-tehnici și tehnici să creeze rapoarte complexe fără a fi nevoie să folosească comenzi de căutare sau să înțeleagă formatul datelor brute subiacente. 6. Pentru toate diagramele exista capacitatea simplă de a schimba titlurile, legendele, etichetele și setările axelor. 7. Permite editarea simplă „glis and drop” a panourilor tabloului de bord. 8. Are abilitatea de a imprima cu ușurință evenimente, tabele și vizualizări. 9. Are abilitatea de a converti tablourile de bord în fișiere PDF și de a programa să fie trimise prin e-mail altor persoane. 10. Are abilitatea de a se integra cu cadre și opțiuni de vizualizare externe (D3, Tableau etc.) pentru vizualizări suplimentare. **Livrabile:** Documentațiile pe care Xontech Systems le va livra autorității contractante în cadrul contractului sunt următoarele:

		1. Documentația de administrare și operare Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră. 2. Documentația de utilizare Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului. **Alte cerințe:** <u>Perioada de suport și menținere de la producător:</u> Pentru soluția ofertată se solicită a fi 12 luni; Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță.	3. Documentația de administrare și operare Se va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră. 4. Documentația de utilizare Se va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului. **Alte cerințe:** <u>Perioada de suport și menținere de la producător:</u> Pentru soluția ofertată este 12 luni; Producătorul ofera suport 24/24, prin e-mail sau conectare de la distanță.