

Specificații 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 achiziție nr. ocds-b3wdp1-MD-1662703671374 din 30 septembrie 2022
Obiectul achiziției: Pachete software aferente securității informaționale

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Lot 3: Menținerea licențelor McAfee						
Servicii de asigurare a accesului la suport anual Business Support, sau echivalentul, pentru licențe McAfee Total Protection for Data Loss Prevention Software, pentru 400 licențe	McAfee (Trellix) Total Protection for Data Loss Prevention Appliance Software	SUA	SUA	<p>Tip: Serviciile de asigurare a accesului la suport anual de tipul Business Support, sau echivalentul, de la producătorul licențelor McAfee, sunt necesar să fie oferite în baza prelungirii termenului de prestare a serviciilor respective pentru perioada 14.12.2022-13.12.2023 pentru licențele McAfee Total Protection for Data Loss Prevention Software exploatate în cadrul Sistemului Informațional al BNM pentru 400 utilizatori și vor include:</p> <ul style="list-style-type: none"> - prezentarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau, - publicarea informației confirmative pe site-ul producătorului. <p>Cerințe față de serviciile de suport:</p>	<p>Tip: Serviciile de asigurare a accesului la suport anual de tipul Business Support, sau echivalentul, de la producătorul licențelor McAfee, sunt necesar să fie oferite în baza prelungirii termenului de prestare a serviciilor respective pentru perioada 14.12.2022-13.12.2023 pentru licențele McAfee Total Protection for Data Loss Prevention Software exploatate în cadrul Sistemului Informațional al BNM pentru 400 utilizatori și vor include:</p> <ul style="list-style-type: none"> - prezentarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau, - publicarea informației confirmative pe site-ul producătorului. <p>Cerințe față de serviciile de suport:</p>	Nu se aplică

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> - Daily product updates (.DATs, engines, etc.); - Product upgrades; - Malware alerts with remediation analysis; - Malware analysis service; - Malware trend podcasts and blogs; - Chat, web, and phone support with remote desktop control; - 24/7 phone support (normally under 5 minutes to expert), unlimited number of calls to McAfee Technical Support; - Automatic diagnostic and remediation tools; - Online product test environments. 	<ul style="list-style-type: none"> - Daily product updates (.DATs, engines, etc.); - Product upgrades; - Malware alerts with remediation analysis; - Malware analysis service; - Malware trend podcasts and blogs; - Chat, web, and phone support with remote desktop control; - 24/7 phone support (normally under 5 minutes to expert), unlimited number of calls to McAfee Technical Support; - Automatic diagnostic and remediation tools; - Online product test environments. 	
Lot 4: Soluție de scanare la vulnerabilități						
Soluție de scanare la vulnerabilități	Tenable.SC	SUA	SUA	<p>Tip: Soluție de scanare la vulnerabilități inclusiv 12 luni de suport de la producător</p> <p>Cantitatea și cerințe de licențiere:</p> <ul style="list-style-type: none"> • Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul: <ul style="list-style-type: none"> - cantitatea de IP adrese scanate, minim 500 de obiecte și fără a limita funcționalul soluției. - Licențierea nu trebuie să depindă de modulele adiționale ale soluției. • Licența trebuie să includă următoarele: <ul style="list-style-type: none"> - Cantitatea nelimitată de agenți și scanere. - Politici de audit și conformitate după standardele internaționale (DISA STIG, CIS, MSCT, etc.). 	<p>Tip: Soluție de scanare la vulnerabilități inclusiv 12 luni de suport de la producător</p> <p>Cantitatea și cerințe de licențiere:</p> <ul style="list-style-type: none"> • Solutia propusa este Tenable.SC, luând în calcul : <ul style="list-style-type: none"> - cantitatea de IP adrese scanate, minim 500 de obiecte și fără a limita funcționalul soluției. - Licențierea nu depinde de modulele adiționale ale soluției. • Licența include următoarele: <ul style="list-style-type: none"> - Cantitatea nelimitată de agenți și scanere. - Politici de audit și conformitate după standardele internaționale (DISA STIG, CIS, MSCT, etc.). 	Nu se aplică

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>- Integrarea API.</p> <ul style="list-style-type: none"> Toate licențele livrate vor include prețul pentru 12 luni de suport furnizat de producătorul licențelor, care va începe de la data acceptanței soluției, după instalare și testare a funcționalităților. În cazul activării licențelor până la data acceptanței soluției, toate costurile de licențiere de la producător în perioada de până la acceptanță vor fi suportate de către Ofertant (Furnizor). <p>Cerințe de sistem: Soluția trebuie să fie livrată, incluzând, dar fără a se limita la, următoarele opțiuni:</p> <ul style="list-style-type: none"> Mașina virtuală pentru VMware pregătită pentru lansare. Posibilitatea de a fi instalată pe sisteme de operate Windows/Linux. <p>Managementul aplicației:</p> <ul style="list-style-type: none"> Soluția trebuie să asigure managementul tuturor componentelor centralizat și prin interfața Web. Soluția trebuie să păstreze rezultatele scanărilor într-o baza de date ce va permite ulterior elaborarea rapoartelor detaliate și analiza evoluării lor în timp. De a nu cere o bază de date separată pentru stocarea rezultatelor scanărilor. 	<p>- Integrarea API.</p> <ul style="list-style-type: none"> Toate licențele livrate includ prețul pentru 12 luni de suport furnizat de producătorul licențelor, care va începe de la data acceptanței soluției, după instalare și testare a funcționalităților. În cazul activării licențelor până la data acceptanței soluției, toate costurile de licențiere de la producător în perioada de până la acceptanță vor fi suportate de către Ofertant (Furnizor). <p>Cerințe de sistem: Soluția livrată, incluzând, dar fără a se limita la, următoarele opțiuni:</p> <ul style="list-style-type: none"> Mașina virtuală pentru VMware pregătită pentru lansare. Posibilitatea de a fi instalată pe sisteme de operate Windows/Linux. <p>Managementul aplicației:</p> <ul style="list-style-type: none"> Soluția asigură managementul tuturor componentelor centralizat și prin interfața Web. Soluția păstrează rezultatele scanărilor într-o baza de date ce va permite ulterior elaborarea rapoartelor detaliate și analiza evoluării lor în timp. De a nu cere o bază de date separată pentru stocarea rezultatelor scanărilor. De a face o diversificare a rezultatelor scanării în 	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • De a face o diversificare a rezultatelor scanării în dependentă de rezultatul scanării, tipul vulnerabilităților, gruparea resurselor, etc. • La analiza rezultatelor sau crearea rapoartelor să permită combinarea acestor rezultate în mai multe modalități. <p>Managementul utilizatorilor: Soluția trebuie să suporte managementul utilizatorilor bazat pe roluri și grupe:</p> <ul style="list-style-type: none"> • Executarea scanărilor cu condiția ca acestea au setată o politică sau nu. • Gestiunea utilizatorilor. • Acces la vizualizarea detaliată a vulnerabilităților. • Identificarea, crearea și gestiunea drepturilor asupra listei obiectelor (assets). • Opțiune de audit a utilizatorilor soluției. • Crearea notificărilor. • Partajarea credențelor de acces la obiecte și sisteme pentru a efectua scanările necesare. • Partajarea politicilor de scanare. • Opțiunea audit predefinită ca rol. <p>Soluția trebuie să permită utilizatorului să modifice riscul vulnerabilității depistate sau să mărească nivelul pin la valoarea necesară.</p>	<p>dependentă de rezultatul scanării, tipul vulnerabilităților, gruparea resurselor, etc.</p> <ul style="list-style-type: none"> • La analiza rezultatelor sau crearea rapoartelor permite combinarea acestor rezultate în mai multe modalități. <p>Managementul utilizatorilor: Soluția suportă managementul utilizatorilor bazat pe roluri și grupe:</p> <ul style="list-style-type: none"> • Executarea scanărilor cu condiția ca acestea au setată o politică sau nu. • Gestiunea utilizatorilor. • Acces la vizualizarea detaliată a vulnerabilităților. • Identificarea, crearea și gestiunea drepturilor asupra listei obiectelor (assets). • Opțiune de audit a utilizatorilor soluției. • Crearea notificărilor. • Partajarea credențelor de acces la obiecte și sisteme pentru a efectua scanările necesare. • Partajarea politicilor de scanare. • Opțiunea audit predefinită ca rol. <p>Soluția permite utilizatorului să modifice riscul vulnerabilității depistate sau săi</p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>Soluția trebuie să permită anexarea, gestiunea vulnerabilităților depistate, investigarea cazurilor și managementul acestora. Soluția nu trebuie să limiteze numărul de utilizatori. Soluția va asigura criptarea comunicațiilor dintre utilizatori și sistem. Soluția trebuie să asigure posibilitatea utilizatorului de a seta parametri de baza a securității și accesului la ea, precum:</p> <ul style="list-style-type: none"> • Politica de parole. • Auditul activității utilizatorilor. • Session TimeOut. <p>Soluția trebuie să mențină integrarea cu Active Directory, LDAP, pentru a asigura autentificarea și autorizarea utilizatorilor.</p> <p>Managementul Obiectelor: Soluția trebuie să asigure colectarea și analiza datelor de pe diferite echipamente de rețea, routere, firewall-uri, switch-uri, etc. Soluția trebuie să posede un mecanism de setare a retenției datelor stocate. Soluția nu trebuie să se bazeze pe sisteme externe pentru a depista obiectele, porturile deschise, serviciile, etc. În soluție trebuie să existe posibilitatea de adăugarea obiectelor manual. În soluție trebuie să existe posibilitatea de a efectua scanări de inventariere a rețelelor în</p>	<p>mărească nivelul pin la valoarea necesară.</p> <p>Soluția permite anexarea, gestiunea vulnerabilităților depistate, investigarea cazurilor și managementul acestora. Soluția nu limitează numărul de utilizatori. Soluția asigură criptarea comunicațiilor dintre utilizatori și sistem. Soluția asigură posibilitatea utilizatorului de a seta parametri de baza a securității și accesului la ea, precum:</p> <ul style="list-style-type: none"> • Politica de parole. • Auditul activității utilizatorilor. • Session TimeOut. <p>Soluția menține integrarea cu Active Directory, LDAP, pentru a asigura autentificarea și autorizarea utilizatorilor.</p> <p>Managementul Obiectelor: Soluția asigură colectarea și analiza datelor de pe diferite echipamente de rețea, routere, firewall-uri, switch-uri, etc. Soluția posedă un mecanism de setare a retenției datelor stocate. Soluția nu se bazează pe sisteme externe pentru a depista obiectele, porturile deschise, serviciile, etc. În soluție există posibilitatea de adăugarea obiectelor manual.</p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>scopul depistării noilor obiecte, când conform unui grafic atât și la solicitare. În soluție trebuie să existe posibilitatea de adăugare dinamică a obiectelor bazate pe careva reguli și/sau criterii. Soluția trebuie să aibă mecanism de clasificare, marcare dinamică a anumitor obiecte din rețea, incluzând, dar fără a se limita la următoarele:</p> <ul style="list-style-type: none"> • După apartenența unei subrețele. • După NetBIOS și FQDN, • După sistemul de operare. • După porturile deschise și servicii. • După prezența unei anumite vulnerabilități. • După durata scanărilor și scheduler-ilor stabiliți. • După obiectele care au ratat scanarea conform graficului, etc. <p>Soluția trebuie să fie fiabilă la setarea sarcinii pe rețea în timpul scanărilor, pentru a preveni supraîncărcarea acestora. Compatibilitatea cu Sistemele de operare și BD.</p> <p>Soluția trebuie să fie compatibilă cu sistemele de operare incluzând, dar fără a se limita la următoarele:</p> <ul style="list-style-type: none"> • Microsoft Windows. • AIX. • Solaris. • HP/UX. • Linux. • MacOS. 	<p>În soluție există posibilitatea de a efectua scanări de inventariere a rețelelor în scopul depistării noilor obiecte, când conform unui grafic atât și la solicitare. În soluție există posibilitatea de adăugare dinamică a obiectelor bazate pe careva reguli și/sau criterii. Soluția posedă mecanism de clasificare, marcare dinamică a anumitor obiecte din rețea, incluzând, dar fără a se limita la următoarele:</p> <ul style="list-style-type: none"> • După apartenența unei subrețele. • După NetBIOS și FQDN, • După sistemul de operare. • După porturile deschise și servicii. • După prezența unei anumite vulnerabilități. • După durata scanărilor și scheduler-ilor stabiliți. • După obiectele care au ratat scanarea conform graficului, etc. <p>Soluția este fiabilă la setarea sarcinii pe rețea în timpul scanărilor, pentru a preveni supraîncărcarea acestora. Compatibilitatea cu Sistemele de operare și BD.</p> <p>Soluția este compatibilă cu sistemele de operare incluzând, dar fără a se limita la următoarele:</p> <ul style="list-style-type: none"> • Microsoft Windows. 	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • Netware. <p>Soluția trebuie să fie compatibilă cu bazele de date incluzând, dar fără a se limita la următoarele:</p> <ul style="list-style-type: none"> • MSSQL. • IBM DB2. • Informix/DRDA. • MySQL. • Oracle Database. • PostgreSQL. • Sysbase ASE. <p>Vizualizarea datelor: Soluția trebuie să posede un set de dashboard-uri personalizabile și diversificate. Soluția trebuie să permită crearea dashboard-urilor adiționale. Dashboard-urile trebuie să mențină funcția de reînnoirea datelor afișate. Soluția trebuie să mențină opțiunea "drill-down" a elementelor dashboard-ului în fereastra separată, pentru asigurarea monitorizării continue și investigării incidentelor. Soluția trebuie să mențină partajarea dashboard-urilor între utilizatori. Dashboard-urile trebuie să permită filtrarea datelor după timp, tag-uri, obiecte, etc. Soluția trebuie să mențină elaborarea și generarea rapoartelor în baza dashboard-urilor. Suport API: Soluția trebuie să mențină partajarea datelor cu alte sisteme prin API.</p>	<ul style="list-style-type: none"> • AIX. • Solaris. • HP/UX. • Linux. • MacOS. • Netware. <p>Soluția este compatibilă cu bazele de date incluzând, dar fără a se limita la următoarele:</p> <ul style="list-style-type: none"> • MSSQL. • IBM DB2. • Informix/DRDA. • MySQL. • Oracle Database. • PostgreSQL. • Sysbase ASE. <p>Vizualizarea datelor: Soluția posedă un set de dashboard-uri personalizabile și diversificate. Soluția permite crearea dashboard-urilor adiționale. Dashboard-urile mențin funcția de reînnoirea datelor afișate. Soluția menține opțiunea "drill-down" a elementelor dashboard-ului în fereastra separată, pentru asigurarea monitorizării continue și investigării incidentelor. Soluția menține partajarea dashboard-urilor între utilizatori. Dashboard-urile permit filtrarea datelor după timp, tag-uri, obiecte, etc.</p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>Soluția trebuie să mențină integrarea prin API cu alte sisteme.</i></p> <p><i>Suportul API trebuie să fie gratis.</i></p> <p><i>Actualizări:</i></p> <p><i>Soluția trebuie să asigure procesul de actualizare a configurației fără cost timp suplimentar și care necesită implicarea sistematică a administratorului, cum ar fi baza de date despre vulnerabilități.</i></p> <p><i>Actualizările automate trebuie să mențină incluzând, dar fără a se limita la următoarele:</i></p> <ul style="list-style-type: none"> • <i>Actualizări conform graficului.</i> • <i>Actualizări manuale.</i> • <i>Posibilitatea de descărcare a actualizărilor și de a fi instalate într-un anumit timp.</i> <p><i>Copii de rezervă și restabilire:</i></p> <p><i>Soluția trebuie să mențină mecanism de Backup automat și restabilire a configurației din interfața web.</i></p> <p><i>Soluția trebuie să suporte exportul copiilor de rezervă cu configurațiile curente pe o resursă alta decât mașina gazdă.</i></p> <p><i>Soluția trebuie să mențină posibilitatea de a face copii de rezervă la mai multe tipuri de date precum obiectele, vulnerabilitățile depistate, etc.</i></p> <p><i>Scalabilitate:</i></p>	<p><i>Soluția menține elaborarea și generarea rapoartelor în baza dashboard-urilor.</i></p> <p><i>Suport API:</i></p> <p><i>Soluția menține partajarea datelor cu alte sisteme prin API.</i></p> <p><i>Soluția menține integrarea prin API cu alte sisteme.</i></p> <p><i>Suportul API este gratis.</i></p> <p><i>Actualizări:</i></p> <p><i>Soluția asigură procesul de actualizare a configurației fără cost timp suplimentar și care necesită implicarea sistematică a administratorului, cum ar fi baza de date despre vulnerabilități.</i></p> <p><i>Actualizările automate mențin incluzând, dar fără a se limita la următoarele:</i></p> <ul style="list-style-type: none"> • <i>Actualizări conform graficului.</i> • <i>Actualizări manuale.</i> • <i>Posibilitatea de descărcare a actualizărilor și de a fi instalate într-un anumit timp.</i> <p><i>Copii de rezervă și restabilire:</i></p> <p><i>Soluția menține mecanism de Backup automat și restabilire a configurației din interfața web.</i></p> <p><i>Soluția suportă exportul copiilor de rezervă cu configurațiile curente pe o resursă alta decât mașina gazdă.</i></p> <p><i>Soluția menține posibilitatea de a face copii de rezervă la mai multe tipuri de date precum obiectele, vulnerabilitățile depistate, etc.</i></p> <p><i>Scalabilitate:</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>Soluția trebuie să fie ușor scalabilă în limitele infrastructurii clientului, fără ca aceasta să necesite costuri adiționale.</i></p> <p><i>Soluția trebuie să mențină interacțiunea cu module geografic separate, fără ca acesta să necesite investii adiționale.</i></p> <p><i>Soluția trebuie să mențină repartizarea dinamică a sarcinii procesului de scanare între scanere astfel încât să nu creeze indisponibilitatea acestora pe parcursul procesului de scanare.</i></p> <p><i>Scanare:</i></p> <p><i>Soluția trebuie să mențină posibilitatea de a:</i></p> <ul style="list-style-type: none"> • <i>Efectua scanări conform graficului setat.</i> • <i>Include/Exclude anumite teste în profilele de scanare.</i> • <i>Opri pe un timp necesar procesul de scanare (Pauza).</i> • <i>Exclude automat resursele critice din procesul de scanare dacă acestea sunt ocupate cu procese critice business, conform unui grafic.</i> • <i>Forma profil de scanare conform unei liste de vulnerabilități stabilite de utilizator.</i> • <i>Scana anumite porturi.</i> • <i>Utiliza conturi de acces pe obiectele scanate.</i> <p><i>Soluția trebuie să poată face autentificarea minim cu astfel de tipuri de autentificare:</i></p>	<p><i>Soluția este ușor scalabilă în limitele infrastructurii clientului, fără ca aceasta să necesite costuri adiționale.</i></p> <p><i>Soluția menține interacțiunea cu module geografic separate, fără ca acesta să necesite investii adiționale.</i></p> <p><i>Soluția menține repartizarea dinamică a sarcinii procesului de scanare între scanere astfel încât să nu creeze indisponibilitatea acestora pe parcursul procesului de scanare.</i></p> <p><i>Scanare:</i></p> <p><i>Soluția menține posibilitatea de a:</i></p> <ul style="list-style-type: none"> • <i>Efectua scanări conform graficului setat.</i> • <i>Include/Exclude anumite teste în profilele de scanare.</i> • <i>Opri pe un timp necesar procesul de scanare (Pauza).</i> • <i>Exclude automat resursele critice din procesul de scanare dacă acestea sunt ocupate cu procese critice business, conform unui grafic.</i> • <i>Forma profil de scanare conform unei liste de vulnerabilități stabilite de utilizator.</i> • <i>Scana anumite porturi.</i> • <i>Utiliza conturi de acces pe obiectele scanate.</i> <p><i>Soluția poate face autentificarea minim cu astfel de tipuri de autentificare:</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • Pentru OS Windows: utilizator parolă, Kerberos, CyberArk Vault, Lieberman, Centrify, BeyondTrust, NTLM Hash, LM Hash. • Pentru Unix: utilizator parolă, Kerberos, CyberArk Vault, Lieberman, Centrify, BeyondTrust, Certificate, Public Key. • Pentru echipamente de rețea: SNMP. <p>Soluția trebuie să primească țintele de scanare sub diferite formate: IP adresa, subrețele, nume, FQDN, etc.</p> <p>Modulul de scanare (Scannerul) trebuie să mențină minim instalarea pe astfel de sisteme de operare:</p> <ul style="list-style-type: none"> • MS Windows. • Linux. • MacOS. • Solaris. <p>Soluția trebuie să permită configurarea profilului astfel încât utilizatorul poate să dea parametri de scanare proprii.</p> <p>Identificarea vulnerabilităților:</p> <p>Soluția trebuie să fie capabilă să identifice probleme, riscurile și vulnerabilități. De asemenea trebuie să ofere informații detaliate despre tipul riscului și recomandări pentru minimizarea acestuia.</p> <p>Soluția trebuie să notifice despre vulnerabilitățile cunoscute a obiectelor,</p>	<ul style="list-style-type: none"> • Pentru OS Windows: utilizator parolă, Kerberos, CyberArk Vault, Lieberman, Centrify, BeyondTrust, NTLM Hash, LM Hash. • Pentru Unix: utilizator parolă, Kerberos, CyberArk Vault, Lieberman, Centrify, BeyondTrust, Certificate, Public Key. • Pentru echipamente de rețea: SNMP. <p>Soluția primește țintele de scanare sub diferite formate: IP adresa, subrețele, nume, FQDN, etc.</p> <p>Modulul de scanare (Scannerul) menține minim instalarea pe astfel de sisteme de operare:</p> <ul style="list-style-type: none"> • MS Windows. • Linux. • MacOS. • Solaris. <p>Soluția permite configurarea profilului astfel încât utilizatorul poate să dea parametri de scanare proprii.</p> <p>Identificarea vulnerabilităților:</p> <p>Soluția este capabilă să identifice probleme, riscurile și vulnerabilități. De asemenea trebuie să ofere informații detaliate despre tipul riscului și recomandări pentru minimizarea acestuia.</p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>depistate și descrise de organizații de securitate precum CVE, OSVDB, The SecurityFocus Bagtraq (BID), etc. și alte combinații ale acestora.</i></p> <p><i>Bazele de date a vulnerabilităților sistemelor trebuie sa include următoarele tipuri de verificări:</i></p> <ul style="list-style-type: none"> • <i>OS Security and Patch.</i> • <i>CISCO.</i> • <i>Firewalls.</i> • <i>DNS.</i> • <i>FTP.</i> • <i>SMTP.</i> • <i>RPC.</i> • <i>SNMP.</i> • <i>LDAP.</i> • <i>SMB.</i> • <i>CGI.</i> • <i>Web Servers.</i> • <i>Databases.</i> • <i>Backdors.</i> • <i>Denial of Services.</i> • <i>Default Accouts.</i> • <i>Peer-To-Peer.</i> • <i>Remote Shell.</i> <p><i>Soluția trebuie să mențină:</i></p> <ul style="list-style-type: none"> • <i>Identificarea serviciilor care lucrează pe porturi ne standarde.</i> • <i>Identificarea serviciilor ce nu afișează un banner la conectare.</i> 	<p><i>Soluția notifică despre vulnerabilitățile cunoscute a obiectelor, depistate și descrise de organizații de securitate precum CVE, OSVDB, The SecurityFocus Bagtraq (BID), etc. și alte combinații ale acestora.</i></p> <p><i>Bazele de date a vulnerabilităților sistemelor includ următoarele tipuri de verificări:</i></p> <ul style="list-style-type: none"> • <i>OS Security and Patch.</i> • <i>CISCO.</i> • <i>Firewalls.</i> • <i>DNS.</i> • <i>FTP.</i> • <i>SMTP.</i> • <i>RPC.</i> • <i>SNMP.</i> • <i>LDAP.</i> • <i>SMB.</i> • <i>CGI.</i> • <i>Web Servers.</i> • <i>Databases.</i> • <i>Backdors.</i> • <i>Denial of Services.</i> • <i>Default Accouts.</i> • <i>Peer-To-Peer.</i> • <i>Remote Shell.</i> <p><i>Soluția menține:</i></p> <ul style="list-style-type: none"> • <i>Identificarea serviciilor care lucrează pe porturi ne standarde.</i> • <i>Identificarea serviciilor ce nu afișează un banner la conectare.</i> 	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • Testarea a câteva exemplare a unui si același serviciu ce lucrează pe porturi diferite. • Scanarea activelor ce nu răspund la ICMP (Ping). <p>Audit: Soluția trebuie să asigure posibilitatea de face un audit al configurației și de a identifica modificările la nivel de sistem de operare Windows/Linux.</p> <p>Soluția trebuie să asigure politici de audit pentru Windows, Windows/Linux aplicații, dispozitive CISCO, baze de date.</p> <p>Soluția trebuie să asigure politici de audit cu menținerea:</p> <ul style="list-style-type: none"> • CIS Benchmarks. • Microsoft Best Practices. • HIPAA. • GLBA. • OWASP Best Practices. • PHI/PII content. • Configurații proprii a utilizatorilor. <p>Notificări si alerte: Soluția trebuie să trimită notificări bazate pe rezultatele scanărilor de vulnerabilități și auditul configurației.</p> <p>Notificările trebuie să mențină adrese de email configurabile și capabile de a folosi diferite variabile din cadrul soluției, de exemplu:</p> <ul style="list-style-type: none"> • Începutul/sfârșitul scanării. • Redirecționarea evenimentelor din syslog. 	<ul style="list-style-type: none"> • Testarea a câteva exemplare a unui si același serviciu ce lucrează pe porturi diferite. • Scanarea activelor ce nu răspund la ICMP (Ping). <p>Audit: Soluția asigură posibilitatea de face un audit al configurației și de a identifica modificările la nivel de sistem de operare Windows/Linux.</p> <p>Soluția asigură politici de audit pentru Windows, Windows/Linux aplicații, dispozitive CISCO, baze de date.</p> <p>Soluția asigură politici de audit cu menținerea:</p> <ul style="list-style-type: none"> • CIS Benchmarks. • Microsoft Best Practices. • HIPAA. • GLBA. • OWASP Best Practices. • PHI/PII content. • Configurații proprii a utilizatorilor. <p>Notificări si alerte: Soluția trimite notificări bazate pe rezultatele scanărilor de vulnerabilități și auditul configurației.</p> <p>Notificările mențin adrese de email configurabile și capabile de a folosi diferite variabile din cadrul soluției, de exemplu:</p> <ul style="list-style-type: none"> • Începutul/sfârșitul scanării. 	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • Evenimente generate de trigger-e, etc. <p>Raportare: Soluția trebuie să mențină raportarea pe toate tipurile de evenimente și să fie disponibile din interfața web. Soluția trebuie să permită crearea rapoartelor individuale. Soluția trebuie să permită generarea rapoartelor la solicitare conform criteriilor cerute. Soluția trebuie să dețină exemple de rapoarte și schițele acestora pentru a simplifica procesul de creare a lor. Soluția trebuie să dețină un set de rapoarte implicite. Soluția trebuie să dețină sau să permită accesarea rapidă a pachetelor de rapoarte predefinite de la bunele practici cum ar fi: NIST, COBIT, ISO, etc. Soluția trebuie să poată genera rapoarte pe un interval de timp, pe anumite subrețele sau obiecte în rețea. Rapoartele generate de soluție trebuie să conțină cel puțin următoarele date:</p> <ul style="list-style-type: none"> • Denumirea vulnerabilităților, nivelul lor critic și CVSS. • Enumerarea sistemelor vulnerabile sau servicii. • Statutul vulnerabilităților. 	<ul style="list-style-type: none"> • Redirecționarea evenimentelor din syslog. • Evenimente generate de trigger-e, etc. <p>Raportare: Soluția mențin raportarea pe toate tipurile de evenimente și să fie disponibile din interfața web. Soluția permit crearea rapoartelor individuale. Soluția permit generarea rapoartelor la solicitare conform criteriilor cerute. Soluția deține exemple de rapoarte și schițele acestora pentru a simplifica procesul de creare a lor. Soluția deține un set de rapoarte implicite. Soluția deține sau să permită accesarea rapidă a pachetelor de rapoarte predefinite de la bunele practici cum ar fi: NIST, COBIT, ISO, etc. Soluția poate genera rapoarte pe un interval de timp, pe anumite subrețele sau obiecte în rețea. Rapoartele generate de soluție conțin cel puțin următoarele date:</p> <ul style="list-style-type: none"> • Denumirea vulnerabilităților, nivelul lor critic și CVSS. • Enumerarea sistemelor vulnerabile sau servicii. • Statutul vulnerabilităților. 	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • <i>Recomandări pentru remediere, link către fix-patch, dacă acesta există.</i> • <i>Criterii adiționale de prioritare a vulnerabilităților: existența unui exploit, cod malițios, etc.</i> <p><i>Managementul vulnerabilităților:</i> <i>Soluția trebuie să urmărească data apariției vulnerabilităților și data ultimei identificări pentru generarea rapoartelor despre timpul aflării acesteia în infrastructura scanată.</i> <i>Soluția trebuie să mențină funcția de import a datelor despre scanări de vulnerabilități de la părți terțe.</i> <i>Soluția trebuie să mențină posibilitatea de scanare în interiorul rețelei și înafara ei prin intermediu agenților sau fără ei, la necesitate.</i> <i>Soluția trebuie să poată identifica lipsa de remedieri, verificări de conformitate, etc.</i></p> <p>Scalabilitate: <i>Soluția trebuie să mențină extinderea funcționalului prin adăugarea modulelor adiționale.</i> <i>Integrare și compatibilitate:</i> <i>Soluția trebuie să mențină integrarea cu următoarele sisteme și soluții:</i></p> <ul style="list-style-type: none"> • <i>ServiceNow - Security Operations.</i> • <i>AirWatch by VMware – MDM.</i> • <i>APCON - Network Monitoring.</i> • <i>Apple – MDM.</i> 	<ul style="list-style-type: none"> • <i>Recomandări pentru remediere, link către fix-patch, dacă acesta există.</i> • <i>Criterii adiționale de prioritare a vulnerabilităților: existența unui exploit, cod malițios, etc.</i> <p><i>Managementul vulnerabilităților:</i> <i>Soluția urmărește data apariției vulnerabilităților și data ultimei identificări pentru generarea rapoartelor despre timpul aflării acesteia în infrastructura scanată.</i> <i>Soluția menține funcția de import a datelor despre scanări de vulnerabilități de la părți terțe.</i> <i>Soluția menține posibilitatea de scanare în interiorul rețelei și înafara ei prin intermediu agenților sau fără ei, la necesitate.</i> <i>Soluția poate identifica lipsa de remedieri, verificări de conformitate, etc.</i></p> <p>Scalabilitate: <i>Soluția menține extinderea funcționalului prin adăugarea modulelor adiționale.</i> <i>Integrare și compatibilitate:</i> <i>Soluția menține integrarea cu următoarele sisteme și soluții:</i></p> <ul style="list-style-type: none"> • <i>ServiceNow - Security Operations.</i> • <i>AirWatch by VMware – MDM.</i> • <i>APCON - Network Monitoring.</i> • <i>Apple – MDM.</i> 	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • Amazon Web Services (AWS) - Cloud Infrastructure. • Aruba, a Hewlett Packard Enterprise company – NAC. • Axonius – CMDB. • Atlassian - Security Operations. • Autonomic Software - Patch Management. • Bay Dynamics - Security Intelligence. • BeyondTrust - Privileged Access Management. • Bomgar/Lieberman - Privileged Access Management. • BMC – SecOps. • Blackpoint Cyber – SOAR. • Brinqa – TVM. • Cisco – NAC. • CyberArk - Privileged Access Management. • Cybric - Continuous Application Security Platform. • Cymulate – Simulation. • Dell - Patch Management. • DF Labs – SOAR. • ForeScout – NAC. • Garland Technology – Networking. • Gigamon – Networking. • Good powered by Blackberry – MDM. • IBM – SIEM. • Infoblox - IP Address Management. • Kenna – TVM. • LogRhythm - Security Intelligence. 	<ul style="list-style-type: none"> • Amazon Web Services (AWS) - Cloud Infrastructure. • Aruba, a Hewlett Packard Enterprise company – NAC. • Axonius – CMDB. • Atlassian - Security Operations. • Autonomic Software - Patch Management. • Bay Dynamics - Security Intelligence. • BeyondTrust - Privileged Access Management. • Bomgar/Lieberman - Privileged Access Management. • BMC – SecOps. • Blackpoint Cyber – SOAR. • Brinqa – TVM. • Cisco – NAC. • CyberArk - Privileged Access Management. • Cybric - Continuous Application Security Platform. • Cymulate – Simulation. • Dell - Patch Management. • DF Labs – SOAR. • ForeScout – NAC. • Garland Technology – Networking. • Gigamon – Networking. • Good powered by Blackberry – MDM. • IBM – SIEM. • Infoblox - IP Address Management. 	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • Lumeta – CMDB. • McAfee - Endpoint Security. • Microfocus/HPE Enterprise – SIEM. • Microsoft – SIEM. • MobileIron – MDM. • Red Hat - Patch Management. • RedLock – TVM. • Redseal – TVM. • RSA – GRC. • Siemplify – SOAR. • Splunk – SIEM. • Symantec - Patch Management. • Syncurity – SOAR. • ThreatConnect - Threat Intelligence. • Thycotic - Privileged Account Management. <p>Instalare: Toate componentele soluției trebuie să mențină instalarea offline și să fie deservite local, fără a fi necesară conexiune la internet. Soluția trebuie să mențină și posibilitatea de actualizare a componentelor, informației despre vulnerabilități fără a fi necesară conexiune la internet.</p> <p>Alte cerințe: Perioada de suport și menținere de la producător:</p>	<ul style="list-style-type: none"> • Kenna – TVM. • LogRhythm - Security Intelligence. • Lumeta – CMDB. • McAfee - Endpoint Security. • Microfocus/HPE Enterprise – SIEM. • Microsoft – SIEM. • MobileIron – MDM. • Red Hat - Patch Management. • RedLock – TVM. • Redseal – TVM. • RSA – GRC. • Siemplify – SOAR. • Splunk – SIEM. • Symantec - Patch Management. • Syncurity – SOAR. • ThreatConnect - Threat Intelligence. • Thycotic - Privileged Account Management. <p>Instalare: Toate componentele soluției mențin instalarea offline și vor fi deservite local, fără a fi necesară conexiune la internet. Soluția menține și posibilitatea de actualizare a componentelor, informației despre vulnerabilități fără a fi necesară conexiune la internet.</p> <p>Alte cerințe: Perioada de suport și menținere de la producător:</p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>1. Pentru soluția oferită se solicită a fi 12 luni din data acceptanței soluției;</p> <p>2. Producătorul trebuie să ofere:</p> <ul style="list-style-type: none"> - suport 24/24, prin e-mail sau conectare de la distanță; - acces la update-uri și Baza de cunoștințe (Knowledge Base + Product Updates) <p>Notă: În costul ofertei trebuie să fie incluse activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției, precum și transferul de cunoștințe Cumpărătorului.</p>	<p>1. Pentru soluția oferită va fi 12 luni din data acceptanței soluției;</p> <p>2. Producătorul oferă:</p> <ul style="list-style-type: none"> - suport 24/24, prin e-mail sau conectare de la distanță; - acces la update-uri și Baza de cunoștințe (Knowledge Base + Product Updates) <p>Notă: În costul ofertei este inclus activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției, precum și transferul de cunoștințe Cumpărătorului.</p>	
Lot 5: Soluție de înregistrare a sesiunilor de lucru ale utilizatorilor						
Soluție de înregistrare a sesiunilor de lucru ale utilizatorilor	Armarius Software's, Scribe Management Suite, Secure, and Intelligence	SUA	SUA	<p>Tip: Soluție de înregistrare a sesiunilor de lucru ale utilizatorilor inclusiv 12 luni de suport de la producător</p> <p>Cantitatea:</p> <ul style="list-style-type: none"> • Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul cantitatea de 100 de utilizatori <p>Cerințe tehnice:</p> <ol style="list-style-type: none"> 1. Cerințe de sistem și Descriere. • Este necesar ca soluția să fie instalată local (on premise). • Datele se vor colecta prin intermediul unui agent instalat pe stația client și se vor 	<p>Tip: Soluție de înregistrare a sesiunilor de lucru ale utilizatorilor, Armarius Software's, Scribe Management Suite, Secure, and Intelligence, inclusiv 12 luni de suport de la producător</p> <p>Cantitatea:</p> <ul style="list-style-type: none"> • Soluția propusă este Armarius Software's, Scribe Management Suite, Secure, and Intelligence, luând în calcul cantitatea de 100 de utilizatori <p>Cerințe tehnice:</p> <ol style="list-style-type: none"> 1. Cerințe de sistem și Descriere. • Soluția va fi instalată local (on premise). • Datele se vor colecta prin intermediul unui agent instalat pe stația client și se 	Nu se aplică

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>păstra centralizat pe un server în scopul prelucrării și analizei.</i></p> <ul style="list-style-type: none"> • <i>Să păstreze local evenimentele și datele despre activitățile utilizatorului dacă acesta nu are acces temporar la serverul de stocare.</i> <p>2. <i>Funcționalități și Aspecte.</i></p> <ul style="list-style-type: none"> • <i>Este necesar ca agentul să suporte posibilitatea de a face capturi de ecran la anumite evenimente stabilite de către administrator sau politici dacă acestea sunt menținute.</i> • <i>Să se ducă o evidență de timp a aplicațiilor care s-au utilizat.</i> • <i>Monitorizarea activității utilizatorului în timp real la solicitare.</i> • <i>Înregistrarea activității utilizatorului la solicitare.</i> • <i>Configurarea efectuării capturilor de ecran la solicitare sau conform la careva condiții.</i> • <i>Existența unui mecanism de audit și depanare a acțiunilor (Forensic).</i> <p>3. <i>Compatibilitate și Integrare</i></p> <ul style="list-style-type: none"> • <i>Este necesar ca agentul să fie compatibil cu sistemul de operare MS Windows.</i> • <i>Partea de server să fie o mașină virtuală compatibilă cu platforma de virtualizare VMware.</i> 	<p><i>vor păstra centralizat pe un server în scopul prelucrării și analizei.</i></p> <ul style="list-style-type: none"> • <i>Va păstra local evenimentele și datele despre activitățile utilizatorului dacă acesta nu are acces temporar la serverul de stocare.</i> <p>2. <i>Funcționalități și Aspecte.</i></p> <ul style="list-style-type: none"> • <i>Agentul va suporta posibilitatea de a face capturi de ecran la anumite evenimente stabilite de către administrator sau politici dacă acestea sunt menținute.</i> • <i>Să se ducă o evidență de timp a aplicațiilor care s-au utilizat.</i> • <i>Monitorizarea activității utilizatorului în timp real la solicitare.</i> • <i>Înregistrarea activității utilizatorului la solicitare.</i> • <i>Configurarea efectuării capturilor de ecran la solicitare sau conform la careva condiții.</i> • <i>Existența unui mecanism de audit și depanare a acțiunilor (Forensic).</i> <p>3. <i>Compatibilitate și Integrare</i></p> <ul style="list-style-type: none"> • <i>Agentul va fi compatibil cu sistemul de operare MS Windows.</i> • <i>Partea de server va fi o mașină virtuală compatibilă cu platforma de virtualizare VMware.</i> 	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • Este acceptabil ca serverul de stocare să fie compatibil cu sistemele de operare MS Windows și Linux, cu condiția că aceasta nu creează dificultăți la gestiunea datelor stocate. • Este necesar ca soluția să fie compatibilă cu Active Directory. • Este necesar să se mențină diferite rolurile de acces la sistemul de management al datelor stocate. <p style="text-align: center;">4. Colectare și Monitorizare</p> <ul style="list-style-type: none"> • Se va înregistra fiecare acțiune pe care o întreprinde un angajat, inclusiv capturi de ecran, aplicații deschise, emailuri, pagini web, fișiere accesate sau editate, etc. • Se va înregistra și timpul pentru fiecare fereastră, aplicație deschisă în parte, precum și timpul de interacțiune a utilizatorului cu aceasta. • Este necesar ca soluția să poată face diferența dintre statutul utilizatorului (Away, Lock, Disconnect – dacă are o conexiune RDP, etc.), precum și a aplicațiilor dacă acestea nu sunt utilizate. • Este necesar ca datele colectate și stocate să fie indexate. • Este necesar să se asigure integritatea datelor stocate. 	<ul style="list-style-type: none"> • Serverul de stocare va fi compatibil cu sistemele de operare MS Windows și Linux, cu condiția că aceasta nu creează dificultăți la gestiunea datelor stocate. • Soluția Va fi compatibilă cu Active Directory. • Se va menține diferite rolurile de acces la sistemul de management al datelor stocate. <p style="text-align: center;">4. Colectare și Monitorizare</p> <ul style="list-style-type: none"> • Se va înregistra fiecare acțiune pe care o întreprinde un angajat, inclusiv capturi de ecran, aplicații deschise, emailuri, pagini web, fișiere accesate sau editate, etc. • Se va înregistra și timpul pentru fiecare fereastră, aplicație deschisă în parte, precum și timpul de interacțiune a utilizatorului cu aceasta. • Soluția poate face diferența dintre statutul utilizatorului (Away, Lock, Disconnect – dacă are o conexiune RDP, etc.), precum și a aplicațiilor dacă acestea nu sunt utilizate. • Datele colectate și stocate vor fi indexate. • Se va asigura integritatea datelor stocate. 	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • Volumul, tipul, periodicitatea colectării datelor să fie gestionate de politicile elaborate sau definite. <p style="text-align: center;">5. Analiza și Vizualizarea Datelor</p> <ul style="list-style-type: none"> • Soluția trebuie să mențină dashboard-uri personalizabile pentru vizualizarea datelor. • Soluția trebuie să mențină posibilitatea de a face o selecție a evenimentelor după filtre definite sau create manual. • Să permită vizualizarea capturilor de ecran și video dacă acesta există direct din interfața aplicației. <p style="text-align: center;">6. Rapoarte și Alerte</p> <ul style="list-style-type: none"> • Soluția trebuie să mențină mecanisme de raportare personalizabile. • Să permită formarea rapoartelor din diferite tipuri de date și statistica elaborate pe ele. • Să permită crearea alertelor pentru anumite activități ale utilizatorului, precum timp îndelungat de inactivitate, utilizare greșită a aplicațiilor, activitate în afara orelor stabilite. <p style="text-align: center;">7. Licențiere și Scalabilitate</p> <ul style="list-style-type: none"> • Soluția trebuie să mențină licențierea pe număr de utilizatori. 	<ul style="list-style-type: none"> • Volumul, tipul, periodicitatea colectării datelor să fie gestionate de politicile elaborate sau definite. <p style="text-align: center;">5. Analiza și Vizualizarea Datelor</p> <ul style="list-style-type: none"> • Soluția menține dashboard-uri personalizabile pentru vizualizarea datelor. • Soluția menține posibilitatea de a face o selecție a evenimentelor după filtre definite sau create manual. • Permite vizualizarea capturilor de ecran și video dacă acesta există direct din interfața aplicației. <p style="text-align: center;">6. Rapoarte și Alerte</p> <ul style="list-style-type: none"> • Soluția menține mecanisme de raportare personalizabile. • Permite formarea rapoartelor din diferite tipuri de date și statistica elaborate pe ele. • Permite crearea alertelor pentru anumite activități ale utilizatorului, precum timp îndelungat de inactivitate, utilizare greșită a aplicațiilor, activitate în afara orelor stabilite. <p style="text-align: center;">7. Licențiere și Scalabilitate</p> <ul style="list-style-type: none"> • Soluția menține licențierea pe număr de utilizatori. 	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> • Licența nu trebuie să limiteze funcționalul aplicației. • Scalabilitate soluției nu trebuie să presupună reinstalarea soluției de la început. • Licența livrată va include prețul pentru 12 luni de suport furnizat de producătorul licențelor, care va începe de la data acceptanței soluției, după instalare și testare a funcționalităților. În cazul activării licențelor până la data acceptanței soluției, toate costurile de licențiere de la producător în perioada de până la acceptanță vor fi suportate de către Ofertant (Furnizor). <p>Alte cerințe: Perioada de suport și menținere de la producător:</p> <ol style="list-style-type: none"> 1. Pentru soluția oferită se solicită a fi 12 luni din data acceptanței soluției; 2. Producătorul trebuie să ofere: <ul style="list-style-type: none"> - suport 24/24, prin e-mail sau conectare de la distanță; - acces la update-uri și Baza de cunoștințe (Knowledge Base + Product Updates) <p>Notă: În costul ofertei trebuie să fie incluse activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției, precum și transferul de cunoștințe Cumpărătorului.</p>	<ul style="list-style-type: none"> • Licența nu limitează funcționalul aplicației. • Scalabilitate soluției nu presupune reinstalarea soluției de la început. • Licența livrată va include prețul pentru 12 luni de suport furnizat de producătorul licențelor, care va începe de la data acceptanței soluției, după instalare și testare a funcționalităților. În cazul activării licențelor până la data acceptanței soluției, toate costurile de licențiere de la producător în perioada de până la acceptanță vor fi suportate de către Ofertant (Furnizor). <p>Alte cerințe: Perioada de suport și menținere de la producător:</p> <ol style="list-style-type: none"> 1. Pentru soluția oferită va fi 12 luni din data acceptanței soluției; 2. Producătorul oferă: <ul style="list-style-type: none"> - suport 24/24, prin e-mail sau conectare de la distanță; - acces la update-uri și Baza de cunoștințe (Knowledge Base + Product Updates) <p>Notă: În costul ofertei include activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției,</p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
					precum și transferul de cunoștințe Cumpărătorului.	
Lot 6: Servicii de asigurare a accesului la suport anual pentru soluția IBM Security Qradar						
Servicii de asigurare a accesului la menținerea anuală a instrumentului IBM Security Qradar	IBM SECURITY QRADAR	SUA	SUA	<p>Tip: Serviciile de asigurare a accesului la suport anual de la producătorul licențelor de tip Annual Software Subscription & Support Renewal 12 Months, sau echivalentul, pentru perioada 01.11.2022 - 31.10.2023, a instrumentului IBM Security Qradar exploatat în cadrul Sistemului Informațional al BNM cu următoarea componență:</p> <ul style="list-style-type: none"> • IBM Security QRadar SIEM All-in-One Virtual 3190 Install (licență de bază) – 1 buc. <p>IBM Security QRadar Virtual SIEM Event Capacity Increase of 100 EPS Install (pachete adiționale) – 9 buc.</p> <p>Confirmarea prestării serviciilor va include:</p> <ul style="list-style-type: none"> - furnizarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau, - publicarea informației confirmative pe site-ul producătorului. 	<p>Tip: Serviciile de asigurare a accesului la suport anual de la producătorul licențelor de tip Annual Software Subscription & Support Renewal 12 Months, sau echivalentul, pentru perioada 01.11.2022 - 31.10.2023, a instrumentului IBM Security Qradar exploatat în cadrul Sistemului Informațional al BNM cu următoarea componență:</p> <ul style="list-style-type: none"> • IBM Security QRadar SIEM All-in-One Virtual 3190 Install (licență de bază) – 1 buc. <p>IBM Security QRadar Virtual SIEM Event Capacity Increase of 100 EPS Install (pachete adiționale) – 9 buc.</p> <p>Confirmarea prestării serviciilor va include:</p> <ul style="list-style-type: none"> - furnizarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau, - publicarea informației confirmative pe site-ul producătorului. 	Nu se aplică

Numele, Prenumele: Birsan Vitalie

În calitate de: Administrator

Ofertantul: Reliable Solutions Distributor S.R.L.

Adresa: str. Alexandru cel Bun 85, MD-2012, mun Chisinau, Republica Moldova.