CONTRACT Nr. 196

de achiziţionare a Sistemului de monitorizare a securităţii

Cod CPV: 30210000-4

"21" noiembrie 2017 **mun. Chişinău**

Vînzător	Cumpărător
„BASS SYSTEMS" SRL, reprezentată prin **Onisim POPESCU**, Director General care acţionează în baza statutului, denumit(a) în continuare *Vînzător*, nr. de înregistrare în Registrul de Stat 1008600013575 din 03.03.2008, pe de o parte,	**Secretariatul Parlamentului Republicii Moldova,** reprezentată prin **Ala POPESCU, Secretar general,** care acţionează în baza Ordinului de numire în funcţie SC-2 nr.78 din 13.07.2012, denumit(a) în continuare *Cumpărător*, pe de o parte,

ambii (denumiţi(te) în continuare *Părţi*), au încheiat prezentul Contract referitor la următoarele:

a. Achiziţionarea Sistemului de monitorizare a securităţii, denumite în continuare Bunuri, conform procedurii de achiziţie prin Licitaţie publică nr.17/03579 din "31" noiembrie 2017, în baza deciziei grupului de lucru al Cumpărătorului din „03" noiembrie 2017.

b. Următoarele documente vor fi considerate părţi componente şi integrale ale Contractului:
   a) Specificaţia tehnică;
   b) Specificaţia de preţ;

c. Prezentul Contract va predomina asupra tuturor altor documente componente. În cazul unor discrepanţe sau inconsecvenţe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.

d. În calitate de contravaloare a plăţilor care urmează a fi efectuate de Cumpărător, Vînzătorul se obligă prin prezenta să livreze Cumpărătorului Bunurile şi să înlăture defectele lor în conformitate cu prevederile Contractului sub toate aspectele.

e. Cumpărătorul se obligă prin prezenta să plătească Vînzătorului, în calitate de contravaloare a livrării bunurilor, precum şi a înlăturării defectelor lor, preţul Contractului sau orice altă sumă care poate deveni plătibilă conform prevederilor Contractului în termenele şi modalitatea stabilite de Contract.

1. Obiectul Contractului

1.1. Vînzătorul îşi asumă obligaţia de a livra Bunurile conform Specificaţiei, care este parte integrantă a prezentului Contract.

1.2. Cumpărătorul se obligă, la rîndul său, să achite şi să recepţioneze Bunurile livrate de Vînzător.

1.3. Calitatea Bunurilor se atestă prin certificatele de calitate indicate în Specificaţie. Bunurile livrate în baza contractului vor respecta standardele indicate în Specificaţie. Cînd nu este menţionat nici un standard sau reglementare aplicabilă, se vor respecta standardele sau alte reglementări autorizate în ţara de origine a produselor.

1.4. Termenele de garanţie a Bunurilor sînt indicate în Specificaţie.

2. Termeni şi condiţii de livrare/prestare

2.1. Livrarea Bunurilor se efectuează de către Vînzător până la 20 decembrie 2017.

2.2. Documentaţia de însoţire a Bunurilor include: **factura fiscală în 2 exemplare şi trebuie prezentată în adresa cumpărătorului.**

2.3. Originalele documentelor prevăzute în punctul 2.2 se vor prezenta Cumpărătorului la momentul livrării bunurilor la destinaţia finală. Livrarea produselor se consideră încheiată în momentul în care sînt prezentate documentele de mai sus.

3. Preţul şi condiţii de plată

3.1. Preţul Bunurilor livrate conform prezentului Contract este stabilit în lei moldoveneşti, fiind indicat Specificaţia prezentului Contract.

3.2. Suma totală a prezentului Contract, se stabileşte în lei moldoveneşti şi constituie: **1 490 852,03 (un milioan patru sute nouăzeci mii opt sute cinzeci şi doi lei 03 bani) lei MD, cu aplicarea TVA la cota zero, conform Legii nr.91 din 13.05.2016, pentru modificarea unor acte legislative**.

3.3. Achitarea plăţilor pentru Bunurile livrate şi/sau Serviciile prestate se va efectua în lei moldoveneşti.

3.4. Metoda şi condiţiile de plată de către Cumpărător vor fi: 100 % după livrarea Bunurilor şi verificării acestora corespunderii calităţii, în termen de 30 zile de la recepţionarea documentelor de însoţire.

3.5. Plăţile se vor efectua prin transfer bancar pe contul de decontare al Vînzătorului indicat în prezentul Contract.

4. Condiţii de predare-primire

4.1. Bunurile se consideră predate de către Vînzător şi recepţionate de către Cumpărător dacă:

a) cantitatea Bunurilor corespunde informaţiei indicate în Lista bunurilor şi graficul livrării şi documentele de însoţire conform punctului 2.2 al prezentului Contract;

b) calitatea Bunurilor corespunde informaţiei indicate în Specificaţie;

c) ambalajul şi integritatea Bunurilor corespunde informaţiei indicate în Specificaţie.

4.2. Vînzătorul este obligat să prezinte Cumpărătorului un exemplar original al facturii fiscale odată cu livrarea Bunurilor, pentru efectuarea plăţii. Pentru nerespectarea de către Vînzător a prezentei clauze, Cumpărătorul îşi rezervă dreptul de a majora termenul de achitare prevăzut în punctul 3.4 corespunzător numărului de zile de întîrziere şi de a fi exonerat de achitarea penalităţii stabilite în punctul 10.3.

5. Standarde

5.1. Produsele furnizate în baza contractului vor respecta standardele prezentate de către furnizor în propunerea sa tehnică.

5.2. Cînd nu este menţionat nici un standard sau reglementare aplicabilă se vor respecta standardele sau alte reglementări autorizate în ţara de origine a produselor.

6. Obligaţiile părţilor

6.1. În baza prezentului Contract, Vînzătorul se obligă:

a) să livreze Bunurile în condiţiile prevăzute de prezentul Contract;

b) să anunţe Cumpărătorul după semnarea prezentului Contract, în decurs de 5 zile calendaristice, prin telefon/fax sau telegramă autorizată, despre disponibilitatea livrării Bunurilor;

c) să asigure condiţiile corespunzătoare pentru recepţionarea Bunurilor de către Cumpărător, în termenele stabilite, în corespundere cu cerinţele prezentului Contract;

d) să asigure integritatea şi calitatea Bunurilor pe toată perioada de pînă la recepţionarea lor de către Cumpărător.

6.2. În baza prezentului Contract, Cumpărătorul se obligă:

a) să întreprindă toate măsurile necesare pentru asigurarea recepţionării în termenul stabilit a Bunurilor livrate corespundere cu cerinţele prezentului Contract;

b) să asigure achitarea Bunurilor livrate, respectînd modalităţile şi termenele indicate în prezentul Contract.

7. Forţa majoră

7.1. Părţile sînt exonerate de răspundere pentru neîndeplinirea parţială sau integrală a obligaţiilor conform prezentului Contract, dacă aceasta este cauzată de producerea unor cazuri de forţă majoră (războaie, calamităţi naturale: incendii, inundaţii, cutremure de pămînt, precum şi alte circumstanţe care nu depind de voinţa Părţilor).

7.2. Partea care invocă clauza de forţă majoră este obligată să informeze imediat (dar nu mai tîrziu de 10 zile) cealaltă Parte despre survenirea circumstanţelor de forţă majoră.

7.3. Survenirea circumstanţelor de forţă majoră, momentul declanşării şi termenul de acţiune trebuie să fie confirmate printr-un certificat, eliberat în mod corespunzător de către organul competent din ţara Părţii care invocă asemenea circumstanţe.

8. Rezilierea

8.1. Rezilierea Contractului se poate realiza cu acordul comun al Părţilor.

8.2. Contractul poate fi reziliat în mod unilateral de către:

a) Cumpărător în caz de refuz al Vînzătorului de a livra Bunurile prevăzute în prezentul Contract;

b) Cumpărător în caz de nerespectare de către Vînzător a termenelor de livrare stabilite;

c) Vînzător în caz de nerespectare de către Cumpărător a termenelor de plată a Bunurilor;

d) Vînzător sau Cumpărător în caz de nesatisfacere de către una dintre Părţi a pretenţiilor înaintate conform prezentului Contract.

8.3. Partea iniţiatoare a rezilierii Contractului este obligată să comunice în termen de 5 zile lucrătoare celeilalte Părţi despre intenţiile ei printr-o scrisoare motivată.

8.4. Partea înştiinţată este obligată să răspundă în decurs de 5 zile lucrătoare de la primirea notificării. În cazul în care litigiul nu este soluţionat în termenele stabilite, partea iniţiatoare va iniţia rezilierea.

9. Reclamaţii

9.1. Reclamaţiile privind cantitatea Bunurilor livrate sînt înaintate Vînzătorului la momentul recepţionării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Vînzătorului.

9.2. Pretenţiile privind calitatea bunurilor livrate sînt înaintate Vînzătorului în termen de 5 zile lucrătoare de la depistarea deficienţelor de calitate şi trebuie confirmate printr-un certificat eliberat de o organizaţie independentă neutră şi autorizată în acest sens.

9.3. Vînzătorul este obligat să examineze pretenţiile înaintate în termen de 5 zile lucrătoare de la data primirii acestora şi să comunice Cumpărătorului despre decizia luată.

9.4. În caz de recunoaştere a pretenţiilor, Vînzătorul este obligat, în termen de 5 zile, să livreze suplimentar Cumpărătorului cantitatea nelivrată de bunuri, iar în caz de constatare a calităţii necorespunzătoare – să le substituie sau să le corecteze în conformitate cu cerinţele Contractului.

9.5. Vînzătorul poartă răspundere pentru calitatea Bunurilor în limitele stabilite, inclusiv pentru viciile ascunse.

9.6. În cazul devierii de la calitatea confirmată prin certificatul de calitate întocmit de organizaţia independentă neutră sau autorizată în acest sens, cheltuielile pentru staţionare sau întîrziere sînt suportate de partea vinovată.

10. Sancţiuni

10.1. Forma de garanţie de bună executare a contractului agreată de Cumpărător este transfer la contul Cumpărătorului, în cuantum de 5% din valoarea contractului.

10.2. Pentru refuzul de a vinde Bunurile prevăzute în prezentul Contract, se va reţine garanţia de bună executare a contractului, în cazul în care ea a fost constituită în conformitate cu prevedrile punctului 10.1., în caz contrar Vînzătorul suportă o penalitate în valoare de 5 % din suma totală a contractului.

10.3. Pentru livrarea cu întîrziere a Bunurilor, Vînzătorul poartă răspundere materială în valoare de 0,1% din suma Bunurilor nelivrate, pentru fiecare zi de întîrziere, dar nu mai mult de 5 % din suma totală a prezentului Contract. În cazul în care întîrzierea depăşeşte 30 zile, se consideră ca fiind refuz de a vinde Bunurile prevăzute în prezentul Contract şi Vînzătorului i se va reţine garanţia de bună executare a contractului, în cazul în care ea a fost constituită în conformitate cu prevederile punctului 10.1.

10.4. Pentru achitarea cu întîrziere, Cumpărătorul poartă răspundere materială în valoare de 0,1% din suma Bunurilor neachitate, pentru fiecare zi de întîrziere, dar nu mai mult de 5 % din suma totală a prezentului Contract.

11. Drepturi de proprietate intelectuală

11.1. Furnizorul are obligaţia să despăgubească achizitorul împotriva oricăror:

a) reclamaţii şi acţiuni în justiţie, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalaţiile sau utilajele folosite pentru sau în legătură cu produsele achiziţionate, şi

b) daune-interese, costuri, taxe şi cheltuieli de orice natură, aferente, cu excepţia situaţiei în care o astfel de încălcare rezultă din respectarea Caietului de sarcini întocmit de către achizitor.

12. Dispoziţii finale

12.1. Litigiile ce ar putea rezulta din prezentul Contract vor fi soluţionate de către Părţi pe cale amiabilă. În caz contrar, ele vor fi transmise spre examinare în instanţa de judecată competentă conform legislaţiei Republicii Moldova.

12.2. De la data semnării prezentului Contract, toate negocierile purtate şi documentele perfectate anterior îşi pierd valabilitatea.

12.3. Părţile contractante au dreptul, pe durata îndeplinirii contractului, să convină asupra modificării clauzelor contractului, prin act adiţional, numai în cazul apariţiei unor circumstanţe care lezează interesele comerciale legitime ale acestora şi care nu au putut fi prevăzute la data încheierii contractului. Modificările şi completările la prezentul Contract sînt valabile numai în cazul în care au fost perfectate în scris şi au fost semnate de ambele Părţi.

12.4. Nici una dintre Părţi nu are dreptul să transmită obligaţiile şi drepturile sale stipulate în prezentul Contract unor terţe persoane fără acordul în scris al celeilalte părţi.

12.5. Prezentul Contract este întocmit în două exemplare în limba de stat a Republicii Moldova, cîte un exemplar pentru Vînzător şi Cumpărător.

12.6. Prezentul Contract se consideră încheiat la data semnării şi intră în vigoare după înregistrarea lui de către Agenţia Achiziţii Publice şi, după caz , de către Trezoreria de Stat sau de către una din trezoreriile teritoriale ale Ministerului Finanţelor, fiind valabil pînă la 31 decembrie 2017.

12.7. Prezentul Contract reprezintă acordul de voinţă al ambelor părţi şi este semnat astăzi, "21" noiembrie 2017.

12.8. Pentru confirmarea celor menţionate mai sus, Părţile au semnat prezentul Contract în conformitate cu legislaţia Republicii Moldova, la data şi anul indicate mai sus.

13. Datele juridice, poştale şi bancare ale Părţilor

Vînzător	Cumpărător
„BASS SYSTEMS" SRL mun. Chişinău, str. Calea Ieşilor, 8, MD-2069 Telefon: 0 (22) 83 79 60 IBAN: MD18VI000002251003167 MDL BC „Victoriabank"SA, filiala nr.3 Chişinău, adresa băncii: mun. Chişinău, str. 31 august 1989, 141, Cod: VICBMD2X416 Cod fiscal: 1008600013575 Cod TVA: 0505779	**Secretariatul Parlamentului Republicii Moldova** mun. Chişinău, bd. Ştefan cel Mare, 162 Telefon: 0 (22) 23 77 00 IBAN: MD28TRPBAA314110A00027AC Ministerul Finanţelor – Trezoreria de Stat BIC: TREZMD2X c/f: 1006601003762

14. Semnăturile părţilor

Vînzător	Cumpărător
Semnătura autorizată: **Onisim POPESCU**	Semnătura autorizată: **Ala POPESCU**

Contabil:

Înregistrat Nr.:

Trezoreria:

Data:

REPUBLICA MOLDOVA, MINISTERUL FINANŢELOR
TREZORERIA TERITORIALĂ CHIŞINĂU
BUGETUL DE STAT
2017-0000077879
23. NOV. 2017

Anexa nr.1
la contractul nr. 196
din 21 noiembrie 2017

Specificația contractului

Nr. d/o	Denumirea serviciilor	Cantitatea	Preț unitar, fără TVA, lei	Preț unitar, cu TVA la cota zero, lei
1.	Sistem de monitorizare a securității Model: IBM QRadar SIEM All-in-One Software 31XX Producător IBM, țara de origine Uniunea Europeană **Cerințe Sizing** Soluția propusa IBM Qradar All-in-One SIEM permită colectarea log-urilor și monitorizarea unui număr nelimitat de surse (dispozitive de rețea/securitate,servere, firewall-uri, IDS/IPS-uri, routere etc și stații de lucru). Soluția este licențiata pentru 2,600 EPS (evenimente per secundă) in regim de lucru cu analiza tuturor activităților la maximum (Querry EPS) cu posibilitatea creșterii de pana la 30,000 EPS. Soluția este licenziata pentru 15,000 bidirecțional flows/minut (Packeteer, NetFlow, J-Flow, sFlow and IPFIX data from network devices). Posibilitatea creșterii pana la 200,000 Flows/minute doar prin licență (fără înlocuirea echipamentului) si pana la 1,000,000 FPM prin dezvoltarea infrastructurii. Soluția integrată reprezintă două appliance-uri fizice, cu HA, conectate în mod active-active sau active-passive. Echipamentul este montabil în rack pe șine glisante cu două surse de alimentare redundante interne. Soluția este configurată cu spațiu uzabil de 16TB care este suficient pentru retenția logurilor in regim Online live data pentru min. 12 luni si de asemenea pentru Online compacted data pentru minim 24 de luni. Spațiul de stocare este configurat in RAID-5 cu un disk hot-spare. Online live data: toate evenimentele pot fi accesate fără latență. În acest caz, datele nu sunt compactate; Online compacted data: toate evenimentele pot fi accesate, dar cu o latență mică, deoarece datele sunt compacte. Rata de compresie este de min. 10:1; Soluția este scalabila si ofera posibilitatea dezvoltării ulterioare a soluției într-un mod cat mai facil - prin „visual programming" cum ar fi construirea regulilor prin interfață grafică (ex: meniuri drop-down); Dezvoltarea și administrarea soluției ulterioare poate fi efectuată de către manager de IT securitate (utilizator), și nu doar de un administrator de sisteme. Soluția are arhitectura modulara si ofera posibilitati de a fi extinsa prin adăugarea unui modul, care executa o anumită funcționalitate (colectare, corelare, stocare log-uri) integrabil cu platforma existentă. Soluția propusă IBM Qradar este liderul mondial pe piata SIEM si este prezentă în „Cadranul de Lider" în cadrul ultimului raport publicat (2016) de Gartner pe subiectul „Magic Quadrant for Security Information and Event Management". Este capabilă să colecteze evenimente de la minim următoarele	1	1 490 852,03	1 490 852,03

	surse: - Cisco Router - Cisco FWSM/ASA Firewall - Cisco Catalyst Switch - Cisco IPS/IDS - Bitdefender - Checkpoint Firewall - Microsoft Active Directory - Microsoft Exchange 2010, 2013, 2016 - Microsoft SQL 2008, 2012, 2016 - Microsoft Windows Server 2008 R2, 2012 R2, 2016 Etc. **Cerințe Administrare și Configurare** Permită accesul la aplicație unui număr nelimitat de utilizatori prin intermediul unei interfețe de tip web; Permită vizualizarea evenimentelor în timp real și într-un format comun, inteligibil, din cadrul consolei de administrare, fără a fi necesara accesarea unei terțe aplicații; Conțină un modul de raportare, care să includă atât rapoarte predefinite, cât și posibilitatea modificării acestora în funcție de cerințe/necesitați; Dispună de un pachet de reguli de corelare și alertare care sa adreseze cele mai întâlnite amenințări asupra securității unei rețele, precum și posibilitatea modificării acestor reguli în funcție de cerințe/necesitați; Soluția oferă o interfață ușor de utilizat pentru crearea de Custom Parsers necesare in prelucrarea evenimentelor provenite de la aplicații non-standard Soluția permită crearea de job-uri automate: rapoarte, arhivare etc. Soluția oferă posibilitatea de customizare a panourilor de control, precum și posibilitatea de a crea spații de lucru specifice în funcție de necesitățile utilizatorului. Monitorizarea și managementul bazei da date poate fi facuta din interfața soluției. Soluția accepta ca parametri de căutare atât exemple simple precum si utilizarea de expresii de tip RegEX. Interfața de căutare a soluției ofera abilitatea de a combina operatorii de căutare de tip Boolean (AND, OR, NOT) într-o singura expresie de căutare. Interfața de căutare a soluției ofera posibilitatea de a căuta folosind intervale de timp statice(data start-data stop) sau dinamice(acum-2h). Soluția oferă controlul centralizat a tuturor componentelor și funcțiilor administrative dintr-o singură interfață grafică web. Administratorul are posibilitatea de a defini accesul la sistem pe roluri bazat pe dispozitive, grupuri de dispozitive sau rază de rețea. Aceasta presupune posibilitatea de a restricționa accesul unui utilizator doar la informația din sistemele dintr-un anumit grup de dispozitive sau gamă de rețea. Administratorul poate să definească accesul bazat pe roluri la diferite arii funcționale ale soluției. Aceasta include posibilitatea de a restricționa accesul utilizatorului la funcțiile sistemului care nu sunt prevăzute in raza rolului utilizatorului dat, de exemplu, administrarea, raportarea, filtrarea evenimentelor, corelația, și/sau vizualizarea panoului de instrumente. Soluția suporta auto descoperirea obiectelor care sunt protejate sau monitorizate.			

	Soluția sprijina clasificarea automatizată a obiectelor care sunt protejate Soluția sprijina desprinderea anumitor panouri de instrumente din UI pentru utilizarea în SOC sau NOC. Soluția suportă modificarea porturile de comunicații între componente. Soluția oferă un API deschis pentru accesul la datele stocate în baza (bazele) de date. Soluția oferă posibilitatea de a cripta comunicațiile între componente. Soluția se integrează cu sisteme terțe ca o metodă de autentificare. **Cerințe operaționale** Soluția permite un rol pe etape din gestionare log-urilor și funcții de securitate a informației. Introducerea mai multor capabilități de analiză reduce nevoia pentru componente de sistem suplimentare și activarea acestora prin upgrade-ul cheilor de licență. Soluția oferă posibilitatea pentru o viitoare extindere și integrare cu alte soluții terțe. Soluția este foarte ușor de utilizat. Solutia foloseste interfata de tip web si configurarea solutiei este user-friendly si nu cere administratori de sisteme sau programatori Soluția sprijina actualizarea automată a informațiilor de configurare cu intervenție minimă din partea utilizatorului. De exemplu, actualizările taxonomiei de securitate, actualizări regulilor furnizorului, suportul dispozitivelor, etc. Soluția foloseste un GUI web-based pentru management, analiză și raportare. Soluția este ofertata in configuratia de disponibilitate înaltă (High Availability) într-un mod încorporat și fără a fi nevoie de software suplimentar. Soluția asigura că toate componentele distribuite ale sistemului vor continua să funcționeze atunci când orice altă parte a sistemului eșuează sau pierde de conectivitate. (de exemplu, consola de management se stinge toate colectoare separate continua să capteze log-uri). Soluția are un proces automatizat de recuperare/de backup. Soluția verifica automat starea de sănătate internă a sistemului și să notifice utilizatorul atunci când apar probleme, să ofere informații despre starea acesteia (încărcare procesor, memorie, spațiu pe disc, etc.) în timp real. Soluția ofera mai multe panouri cu instrumente care pot fi personalizate pentru a îndeplini cerințele diferitor utilizatori ai sistemului. Soluția contina panouri cu instrumente preinstalate (out of the box) (de exemplu, pentru managementul pericolelor, managementul de conformitate, etc.). Soluția oferă widget-uri personalizate care pot prezenta informații de securitate importantă pentru utilizatorii sistemului (de exemplu, verificarea evenimentelor, activităților in rețea, incidentelor etc.). Soluția menține o bază de date a tuturor obiectelor descoperite în rețea. Datele referitoare la aceste obiecte includ informații importante despre obiecte ca aflate din informațiile colectate (de exemplu sistemul de atribute, atribute de rețea, statistici de vulnerabilitate, etc.). Baza de date furnizeza posibilitatea de a edita atributele atunci când acestea nu pot fi învățate (de			

	exemplu departament, locație, etc.). Utilizatorul poate căuta in această bază de date. **Cerințe de arhitectură** Soluția foloseste o bază de date proprietară, proiectată pentru a permite stocarea și analiza istorica, la viteze ridicate asupra datelor. Soluția includă o baza de date relațională pentru stocarea log-urilor colectate; Comunicarea intre diferite componente de sistem sa realizeaza in mod securizat. Soluția oferă posibilitate de căutare prin toate evenimentele stocate. Soluția oferă mecanisme de integrare cu servicii de autentificare si autorizare precum: Active Directory, RADIUS, LDAP. Soluția oferă o serie de mecanisme (caching etc.), astfel încât atunci când numărul de evenimente/secunda depășește limita impusa de licența sau capabilitățile de procesare (regim peak), surplusul de evenimente nu va fi pierdut. Soluția oferă o funcție de stocare a log-urilor pe dispozitive NAS/SAN, folosind protocoalele din cadrul instituției precum: CIFS, NFS, iSCSI. La nivelul soluției exista posibilitatea de a crea partiții virtuale, la care se pot configura diferite reguli de retenție a datelor. Soluția oferă mecanisme împotriva falsificării și modificării datelor colectate. Poseda un mecanism de depozitare temporară a datelor și de retransmitere a lor în situația în care comunicația între sursa generatoare de log și soluția de monitorizare este temporar indisponibilă; Soluția oferă mecanisme prin care se garantează livrarea evenimentelor în cazul în care unul dintre modulele soluției devine nedisponibil. Soluția integreaza cu alte soluții de securitate și informații de rețea din cadrul Parlamentului. Soluția sprijina o bază de date distribuită pentru colectarea evenimentelor și activităților de rețea, astfel încât toate informațiile pot fi de accesate de la un singur UI. Soluția asigura integritatea informațiilor colectate. Soluția oferă mecanisme intuitive pentru rezolvarea problemelor, cum ar fi notificări, linie de comandă etc. Soluția suporta taxonomie extinsă de utilizare a evenimentelor și câmpuri. Utilizatorul poata adauga propriile nume de evenimente (de exemplu, posibilitatea de a adăuga câmpuri noi care nu sunt preinstalate, cum ar fi " SpecialID from my Custom Application "). Soluția permită marcarea evenimentelor definită de client. Soluția suporta restabilirea transparentă, agregarea, sortarea, filtrarea și analiza datelor în toate componentele distribuite. **Cerințe Log Management** Soluția propusa foloseste mecanisme de criptare a comunicației log-urilor către dispozitivul de monitorizare, precum și de un mecanism de validare a integrității log-urilor, conform standardului internațional NIST 800-92 (Log Management Standard); Oferă posibilitatea identificării incidentelor de securitate IT în timp real pe baza regulilor prestabilite și să permită prioritizarea evenimentelor în funcție de importanta; Soluția permită definirea de intervale de stocare a log-urilor în			

	format brut în funcție de anumite criterii(perioada de retenție, dispozitivele pentru care se face stocarea). La nivelul soluției de log management exista posibilitatea de asigurare a redundanței, în cazul în care un dispozitiv de stocare devine inaccesibil. Soluția oferă posibilitatea de a asigna un anumit eveniment unei categorii de evenimente. Soluția oferă mecanisme prin care se asigură integritatea log-urilor stocate. Pună la dispoziție un API (Application Programming Interface) pentru a permite normalizarea și managementul log-urilor provenite de la surse de evenimente/aplicații proprietare sau care nu sunt suportate în mod implicit; Soluția oferă posibilitatea de a adăuga informații suplimentare in evenimentele stocate prin extragerea acestora din baze de date, Active Directory sau surse LDAP. Soluția suporta stocarea log-urilor și evenimentelor atât pe termen scurt cât și pe termen lung Soluția suporta arhive de log-uri depozitate pe medii de stocare externe (3rd party). Soluția suporta capacități de depozitare și compresie eficientă a datelor colectate. Soluția suporta colectarea logurilor de pe toate echipamentele din cadrul Secretariatului Parlamentului Soluția suporta colectarea fără aplicații agent (agent-less) a log-urilor de evenimente, oricând. Soluția oferă posibilitatea de a distribui atât depozitarea cât și prelucrarea de evenimente în întreaga rețea Log Management/SIEM. Soluția sprijina accesul pe termen lung la date detaliate de evenimente de securitate și de flux de rețea. Sistemul este capabil de a oferi acces la informații detaliate cel puțin în valoare de 12 luni iar la restul prin aducerea lor in sistem din sistemul de stocare si analiza ulterioară **Cerințe privind normalizarea și categorisirea log-urilor** Transformă log-urile colectate într-un format comun (normalizat) și să permită categorisirea acestora în vederea efectuării unei analize ulterioare cât mai facile; Soluția ofer capabilitatea de agregare a evenimentelor. De asemenea ofera posibilitatea de a modifica regulile de agregare. Soluția normalizeaza toate informațiile colectate într-un format comun. Soluția oferă capabilitatea de a modela evenimentele recepționate și de a le cataloga în grupuri logice precum: domenii, rețele, aplicații, nivele de criticitate etc. Soluția normalizeaza câmpurile comune de evenimente (de exemplu numele de utilizator, adrese IP, nume de host, și log dispozitiv sursă, etc.) de la dispozitive disparate într-o rețea multi-vendor. Soluția oferă o taxonomie comună de evenimente. Soluția oferă posibilitatea de a normaliza și agrega câmpuri de evenimente care nu sunt reprezentate de domeniile normalizate out-of-the-box. Soluția sprijina/ normalizeaza marcajele de timp ale evenimentelor din mai multe fusuri orare. **Cerințe privind filtrarea evenimentelor și analiză** Soluția oferă capabilitatea de a crea liste de interes cu informații importante, informații care pot fi folosite la definirea filtrelor și			

	regulilor. Listele pot fi populate manual sau în mod dinamic pe baza unor interogări. Dispună de posibilitatea filtrării log-urilor bazat pe orice criteriu legat de informațiile conținute în log-urile respective; Soluția oferă interogări dinamice si distribuite (suporta atât căutări simple cat si căutări complexe bazate pe expresii regulate si expresii logice de tip Boolean). Soluția oferă o analiză a evenimentelor în timpul real. Soluția oferă analiza tendințelor evenimentelor pe termen lung. Soluția oferă posibilitatea de concentrare și analiză a evenimentelor bazată pe un filtru specificat de către utilizator. Soluția oferă o vedere streaming în timp real care suportă capabilitățile de filtrare complete. Soluția oferă alertare bazată pe anomaliile observate și schimbările de comportament la evenimentele de rețea și de securitate. Soluția suporta și menține o istorie de activitate și autentificare a utilizatorului pe bază de dispozitive. **Cerințe privind raportarea** Soluția oferă posibilitatea de exportare a rapoartelor cel puțin in format: PDF, XML, CSV, HTML. Soluția oferă posibilitatea de a configura rapoartele din punct de vedere grafic in funcție de nevoile și politicile companiei (adăugarea de logo-uri, antete, etc.). Soluția conține o serie de rapoarte predefinite, folosite în industria internațională precum: PCI-DSS, SOX, ISO-27000, NIST, COBIT, FISMA, GLBA, HIPAA, NERC, GDPR, fără a fi necesară cumpărarea unei licențe suplimentare. Soluția permită crearea de rapoarte fără a utiliza interogări complexe de tip SQL, ci prin interfețe ușor accesibile utilizatorului. Soluția furnizează rapoarte cu privire la toate articolele disponibile pentru management prin intermediul GUI. Soluția oferă engine de raportare configurabil pentru crearea de rapoarte personalizate. Soluția suportă capacitatea de a planifica rapoarte. Soluția furnizează rapoarte out-of-the-box pentru probleme tipice și operaționale. Soluția oferă un "panou cu instrumente" pentru vizualizarea rapidă a informațiilor de securitate și de rețea. Soluția suportă distribuția automată a rapoartelor. Soluția suportă capacitatea de a furniza rapoarte istorice ale tendințelor. Soluția suportă capacitatea de a livra la nivel central rapoarte de vulnerabilitate. Soluția suportă capacitatea de a livra la nivel central rapoarte. **Cerințe corelare și alertare** Soluția poată face corelarea istorica a evenimentelor in scopul de a putea face unele previziuni sau scenarii de risc. permită integrarea cu un modul adițional de corelare, care oferă funcționalități extinse, precum corelarea istorică sau corelarea bazată pe risc, nu pe reguli/semnături. Soluția conține mai mult de 100 de reguli de corelare "out-of-the-box". Soluția oferă posibilitatea de a crea noi reguli de corelare, folosind o interfață ușoară de tip "drag and drop", fără a fi necesare cunoștințe avansate de programare. Soluția oferă capabilitatea de a corela evenimente prin			

	compararea cu liste statice sau dinamice. Soluția conține alerte predefinite, care pot fi activate de utilizator. Soluția permită generarea alertelor pe baza severității evenimentelor detectate. Soluția este capabila sa coreleze evenimente de la surse de date ce au fusuri orare diferite. Soluția detecteaza automat întreruperile în procesul de colectare a datelor și să poată expedia alerte. Soluția oferă capabilități de corectare a informațiilor privind data (timpul), de la sistemele care nu oferă aceste informații în mod corect; astfel se asigura integritatea analizelor de tip "forensic" pentru determinarea timpului când a fost generat evenimentul. Poată identifica acțiuni repetitive sau tipuri de evenimente, pe baza cărora se pot seta reguli de alertare și se pot adopta politici de securitate. Dispună de un motor de corelare care să permită identificarea elementelor comune din două sau mai multe evenimente aparent fără nicio legătură; Soluția oferă alerte bazate pe amenințări de securitate observate de la dispozitive monitorizate. Soluția oferă posibilitatea de a corela informațiile pe toate dispozitivele potențial disparate. Soluția oferă alertare bazată pe anomalii observate și schimbările de comportament în activitatea de rețea (flux) de date. Soluția oferă alerte bazate pe politica stabilită. (de exemplu, trafic, IM nu este permis.) Soluția suportă alerte ponderate pentru a permite prioritizarea. Gravitatea este atribuită în baza caracteristicilor cum ar fi tipul obiectului, protocol, aplicație, etc. Soluția oferă posibilitatea de a transmite alerte folosind mai multe protocoale și mecanisme pentru alte soluții de management. Soluția furnizeaza un Wizard bazat pe UI și capabilități pentru a minimiza alarmele false și oferă rezultate precise. Soluția limiteaza prezentarea semnalărilor multiple similare. Soluția suportă capacitatea de a lua măsuri la primirea unei semnalări. De exemplu, soluția ar trebui să sprijine capacitatea de a iniția un script sau trimite un mesaj de e-mail. Soluția suportă capacitatea de a corela împotriva feed-urilor străine de date de securitate (de exemplu, cartografierea geografică, canale botnet cunoscute, rețele ostile cunoscute, etc.). Aceste fluxuri de date străine ar trebui să fie actualizate automat de soluție. Soluția suportă capacitatea de a corela împotriva vulnerabilităților străine ale rezultatelor scanării. Soluția monitorizeaza și să alerteze atunci când există o întrerupere în colectarea log-urilor de pe un dispozitiv. Cu alte cuvinte, în cazul în care log-urile nu sunt văzute de pe un server în X minute, atunci să se genereze o alertă. Soluția oferă un mecanism out-of-the-box pentru a descoperi și clasifica obiectele după tipul sistemului (de exemplu, serverele de mail față de serverele baza de date). Soluția suportă corelație pentru o secvență lipsă. De exemplu serviciul s-a oprit nefiind urmat de restartarea serviciului în 10 minute. Soluția suportă corelarea pentru valorile aditive pe parcursul timpului. De exemplu, atunci când orice alertă IP SRC trimite			

	mai mult de 1 GB de date la un singur port pe un singur IP DST într-o perioadă de o oră de timp. Soluția furnizeaza un mecanism, pentru a optimiza reglarea regulilor, care permite gruparea valorilor de intrare similare de la o regulă de corelație care pot fi utilizate de mai multe reguli. Acest mecanism ar trebui să permită grupare pentru ambele grupuri statice și grupuri care sunt dinamic create de alte reguli de corelare. De exemplu, utilizatorul a sistemului poate defini un grup de porturi interzise / protocoale care ar trebui să fie utilizată în normele de corelație multiplă care monitorizează activitatea de rețea pentru necorespunzătoare. **Cerințe monitorizarea activității în rețea** Soluția oferă capabilitatea de a detecta anomalii la nivelul rețelei, utilizatorilor, aplicațiilor sau a altei surse de informații pe baza calculelor statistice si foloseste metode diferite de corelare a riscurilor. Soluția oferă capabilitatea de a urmări activitatea unui utilizator, prin corelarea datelor de la sisteme DHCP, VPN si Active Directory. Soluția menține un inventar cu dispozitivele la nivel de retea. De asemenea solutia detecteaza si actualizeaza inventarul in mod automat si faciliteaza lucrul ulterior cu corelarea riscurilor. Soluția oferă posibilitatea operatorului să creeze panouri de comandă (dashboards) specifice monitorizării Active Directory. Se doresc minim următorii indicatori: monitorizarea pentru login, logout, password reset etc; Elevarea de privilegii, monitorizarea conturilor VIP sau monitorizarea utilizatorilor privilegiați. Soluția este capabila să detecteze automat anomaliile de trafic WEB pentru utilizatorii interni, aceasta monitorizare se va realiza prin integrarea bidirecțională cu soluția WEB/URL filtering prin monitorizarea categoriilor și a indicatorilor de compromis detectați. Soluția permită crearea și păstrarea statisticilor de tip "baseline" asupra activității monitorizate. De asemenea solutia ofera capabilități de alertare în cazul în care se observă o deviație de la comportamentul normal. Soluția oferă mecanisme avansate de analiza a traficului de rețea, prin metoda sniffing, și astfel permițând colectarea traficului specific bazelor de date tranzacționale cu obiectivul de monitorizare, analiza si corelare si alertarea acestor evenimente. Soluția nu necesita modificări la nivelul bazelor de date care urmează să fie monitorizate. Soluția oferă mecanisme de detecție avansate prin decodarea traficului de rețea L7. Se vor identifica mesaje specifice și se va alerta în momentul în care apare o anomalie la nivel de protocol suport pentru MMS, ISO 8327-1 OSI, COTP, MODBUS. Soluția includă tool-uri de investigare precum: WHOIS, DIG, Traceroute, NSLOOKUP etc. Soluția include tablouri de bord grafice predefinite, precum și posibilitatea personalizării acestora pentru o imagine cît mai elocventă asupra nivelului de securitate; acestea pot afișa informațiile în timp real; Dispună de abilitatea de a reprezenta dinamic într-un mod grafic evenimentele desfășurate pentru a putea realiza amploarea unui atac, precum și pentru a putea identifica cu ușurință inițiatorul acelui atac; Soluția afișeaza profiluri vizuale de trafic formulate în bytes,			

	rate de pachete și numărul de gazde care comunică. Aceste ecrane sunt disponibile pentru aplicații, porturi, protocoale, amenințările și fiecare punct de supraveghere în rețea. Toate aceste puncte de vedere accepte vedere specific locație de rețea, astfel încât să poată prezenta informații dintr-o singură locație, întreaga rețea sau de orice alt grup definit de gazde. Soluția învața dinamic norme de comportament și să recunoască modificările pe măsură ce acestea apar. Soluția detecteaza atacuri de tip denial-of-service (DoS) și distributed-denial-of-service (DDoS). Soluția detecteaza și să prezinte segmente de trafic referitoare la amenințările observate în rețea. Soluția suporta profilarea traficului asociat cu un design de rețea logică (de exemplu, de subrețea / CIDR). Soluția identifica traficul în rețea de la aplicații potențial periculoase (de exemplu, partajarea de fișiere, de tip peer-to-peer, etc.). Soluția afișeaza profile de trafic în ceea ce privește rata de pachete. Această capacitate este disponibile pentru analiza simplă TCP (TCP flag, etc), dar informațiile bazate pe rată pot fi prezentate pentru alte profiluri (de exemplu, aplicații). Soluția identifica și să prezinte informații în mai multe intervale de timp. Profilul este disponibil pentru săptămână, zi și oră. Soluția identifica comunicațiile, ce sunt generate din sau spre internet, conform regiunilor geografice în timp real. Soluția creaza profiluri independente și diferențiate din traficul local și traficul generat din sau destinat pentru internet. Soluția permită utilizatorului să creeze profiluri personalizate și vedere folosind orice proprietate a unui flux, jurnal, sursa de date sau de trafic deja profilate. Soluția suporta identificarea traficului bazat pe adrese IP, grupuri de adrese IP, perechi IP sursă / IP destinație etc. Soluția sprijina colectarea și analiza de date de captare de pachete. Soluția oferă posibilitatea de a extrage anumite câmpuri, definite de utilizatori, din pachetele de date capturate și de a folosi aceste câmpuri în regulile de corelare. Soluția identifica traficul într-un mediu de rețea virtuală. **Cerințe administrarea avansată a pericolelor** Soluția oferă integrare cu soluția BitDefender Gravity Zone, folosită la acest moment de Autoritatea Contractantă. Soluția oferă capabilități de "drill-down" în toate panourile de vizualizare ale interfeței, astfel încât utilizatorul să poată face investigații, ajungând la detalii specifice, pornind de la un eveniment general. Soluția oferă posibilitatea de a lega contextual activitatea aplicației în rețea cu evenimentele de securitate de la dispozitivele monitorizate. Soluția oferă posibilitatea de a lega contextual evenimentele de securitate raportate cu cunoștințele în timp real a obiectelor vizate. Soluția este capabilă de a schimba în mod automat ponderile de credibilitate a dispozitivelor de securitate ca răspuns la atacurile din rețea. **Cerințe fluxul de lucru SIEM** Dispună de diferite mecanisme de notificare: alerte la consola, e-mail, SNMP, SMTP; Soluția furnizeaza capacități incorporate de monitorizare a			

	fluxului de date pe care lucrătorii îl pot folosi pentru a ghida procesul de lucru. Soluția oferă un mecanism de a capta toate aspectele importante ale unui incident de securitate într-un singur raport logic. Acest raport ar trebui să includă evenimente importante, datele privind activitatea de rețea, alerte corelate, date de vulnerabilitate, etc . Soluția oferă un mecanism pentru a adnota un incident de securitate, în timp ce acesta este adresat de către lucrătorii operațiunilor de securitate. Soluția oferă un mecanism pentru a găsi incidentele de securitate într-o gamă largă de atribute importante (de exemplu, adrese IP, nume de utilizator, adresa MAC, jurnal sursă, normele de corelare, definit de utilizator, etc). Utilizatorul este capabil de a filtra incidente de-a lungul acestor atribute definite. **Cerințele sursei de date** Soluția oferă posibilitatea de colectare şi parsare a log-urilor de la diverse surse de date sau din "flat files". Soluția oferă posibilitatea de integrare a surselor de date nesuportate, prin creare locală a regulilor de parsare fără a fi nevoie de licențe suplimentare. Soluția oferă posibilitatea de a defini o singură sursă de date pentru mai multe sisteme identice, care au aceleași proprietăți. Soluția oferă posibilitatea de integrare cu cel puțin următoarele soluții de management al vulnerabilităților: Qualys, Nessus, Metasploit, Saint, Rapid7, nCircle, Lumension, McAfee, eEye Retina, LanGuard, OpenVAS. Soluția suporta scanerele de vulnerabilități de top din industrie. Soluția oferă posibilitatea construirii şi implementării de surse de evenimente specifice „CUSTOM" pe lângă celor suportate nativ. Adăugarea surselor de date se face din interfața soluției, fără a fi nevoie de a instala agenți sau pachete software suplimentare. Soluția oferă posibilitate de detecție şi notificare atunci când o anumita sursă de date nu generează log-uri conform comportamentului învățat. Soluția oferă posibilitatea de colectare a datelor de tip flow: Netflow v5, v7, v9, SFlow şi J-Flow. Soluția suportă produsele de la mai mulți furnizori. Soluția suportă informațiile colectate de la soluții de baze de date de clasă Enterprise. Soluția suportă informațiile colectate de la aplicații comerciale. Soluția suportă informațiile colectate de la aplicații proprietare. Soluția suportă informațiile colectate de software-ul de securitate şi instrumentele Database Activity Monitoring (DAM). Soluția suportă informațiile colectate de către software-ul de securitate şi instrumentele File Integrity/Activity Monitoring (FIM/FAM). Soluția suportă informațiile colectate de la software-ul şi instrumentele de securitate al Identity & Acces Management (IAM). Soluția suportă informațiile colectate de la sistemele de management al rețelei (de exemplu Microsoft MOM, etc.). Soluția suportă informațiile colectate de la infrastructura rețelei (de exemplu, switch-uri, routere, etc.). Vînzătorul va asigura service si suport tehnic local în perioada de garanție şi mentenanță, conform tipului de suport solicitat: 3 ani de full garanție si mentenanța „parts", „labour", şi „on site".			

	Service si suport tehnic va asigura: 1. posibilitatea actualizării software-ului; 2. posibilitatea actualizării semnăturilor; 3. posibilitatea adresării către suportul tehnic al producătorului în soluționarea problemelor apărute în procesul de exploatare a sistemului de securitate informațională a rețelei; 4. înnoirea tuturor componentelor sistemului de securitate (la nivel de software sau platformă); 5. asigurarea efectuării lucrărilor de profilaxie a sistemului; 6. diagnosticarea și soluționarea problemei tehnice apărute în momentul exploatării; 7. asigurarea efectuării copiilor de rezervă ale sistemului reglat și funcțional; 8. asigurarea suportului la telefon sau email în limba română 9. Asigurarea obligatorie a asistenței și suportului tehnic calificat și linie fierbinte în zilele de lucru de la 8:00 până la 18:00 prin telefon sau mobil, prin e-mail 24/24 inclusiv zilele de odihnă; 10. Răspunsul garantat a inginerului certificat, în zilele de lucru – timp de maxim 1 oră, în zilele de odihnă și înafara orelor de lucru – 12 ore. Începutul defecțiunii se consideră momentul răspunsului garantat a inginerului certificat a Prestatorului. 11. La solicitarea Beneficiarului lucrările de deservire / reparație se vor executa de către personalul Prestatorului și în afara zilelor de lucru (în zilele de odihnă). 12. În cazul apariției, pe perioada de mentenanță și garanție, a unor nereguli, probleme sau defecțiuni de funcționare, Prestatorul va asigura înlăturarea defecțiunilor, din cont propriu, fără a cere careva plăți suplimentare, în termen de maxim 4 ore din momentul răspunsului garantat a inginerului certificat a Prestatorului, dar în cazul în care va trebui de schimbat piese sau echipamente, termenul limita în acest caz se va extinde până la maxim 14 zile calendaristice Vînzătorul va asigura instalarea, ajustarea, asistența tehnică pe întreaga perioadă de garanție, cu instruirea a min. 2 administratori. Vînzătorul va asigura toate părțile necesare pentru instalare și punerea în funcțiune (exemplu: cabluri, șuruburi, piulițe, fascete, organizatori de cabluri, etc.) fără a solicita careva plăți suplimentare de la Cumpărător.			
Suma totală, lei, cu aplicarea TVA la cota zero, conform Legii nr.91 din 13.05.2016, pentru modificarea unor acte legislative				**1 490 852,03**

Onisim POPESCU

Ala POPESCU

Anexa nr.2
la contractul nr. 196
din 01 noiembrie 2017

Date tehnice

Software

Part Number	Descriere	Cantitate
	Licente (cu 1 an de mentenanta)	
D1RNCLL	IBM QRadar Software Install License (include 100 EPS si 15,000 FPM)	1
D1RP3LL	IBM QRadar Event Capacity 2.5K Events Per Second License + SW Subscription & Support 12 Months	1
D1S2JLL	IBM QRadar Software Node Install License	3
D1RS0LL	IBM QRadar High Availability Software Install License - HA	1
	Mentenanta aditionala (2 ani)	
E0NBALL	IBM QRadar Software Install Annual SW Subscription & Support Renewal 12 Months	2
E0NBILL	IBM QRadar Event Capacity 2.5K Events Per Second Annual SW Subscription & Support Renewal 12 Months	2
E0NEGLL	IBM QRadar Software Node Install Annual SW Subscription & Support Renewal 12 Months	6
E0NCHLL	IBM QRadar High Availability Software Install Annual SW Subscription & Support Renewal 12 Months	2

Hardware

Denumire	Descriere	Cantitate
Server	8871-XXX Lenovo x3650 M5, Rack 2U	2
Processor	Intel Xeon Processor E5-2620 v4 8C 2.1GHz 20MB Cache 2133MHz 85W	4
Memory	16GB TruDDR4 Memory (2Rx4, 1.2V) PC4-19200 CL17 2400MHz LP RDIMM	8
HDD	4TB 7.2K 12Gbps NL SAS 3.5" G2HS HDD	12
Network	Gigabit Ethernet ports	8
RAID	ServeRAID M5210 SAS/SATA Controller ServeRAID M5200 Series 4GB Flash/RAID 5 Upgrade ServeRAID M5200 Series RAID 6 Upgrade FoD	2
Power Supplies	System x 750W High Efficiency Platinum AC Power Supply	4
Remote Management	Integrated Management Module Advanced Upgrade	2
Rack features	System x Enterprise Slides Kit System x Enterprise 2U Cable Management Arm (CMA)	2
Warranty	Onsite warranty (parts, labor), years	3

Onisim POPESCU

Ala POPESCU