1.	**Cerințe Sizing**
1.1	Soluția trebuie să 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);
1.2	Soluția trebuie sa suporte un nivel de minim 2200 EPS (evenimente per secundă) în regim de lucru cu analiza tuturor activităților la maximum (Querry EPS).
1.3	Minim 15000 bidirecțional flows/minut (Packeteer, NetFlow, J-Flow , sFlow and IPFIX data from network devices).
1.4	Soluția integrată reprezintă două appliance-uri fizice All-in-One, cu HA, conectate în mod active-pasive. Echipamentul este montabil în rack pe șine glisante cu două surse de alimentare redundante interne
1.5	Soluția va trebui să furnizeze spațiu pentru retenția logurilor ca si **Online live data** pentru min. 12 luni si de asemenea pentru **Online compacted data** pentru minim 24 de luni. Spațiul de stocare va fi configurat in RAID-5 cu minim un disk hot-spare.
1.6	**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;
1.7	Soluția trebuie să ofere posibilitatea dezvoltării ulterioare a soluției într-un mod cat mai facil (sa fie scalabila);
1.8	Soluția trebuie sa ofere posibilitate de a fi extinsa prin adăugarea unui modul, care executa o anumită funcționalitate(colectare, corelare, stocare log-uri) integrabil cu platforma existentă.
1.9	Soluția propusă trebuie sa fie prezentă în „Cadranul de Lider” în cadrul ultimului raport publicat de Gartner pe subiectul „Magic Quadrant for Security Information and Event Management”
1.10	Fie capabilă să colecteze evenimente de la minim următoarele 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.

2.	**Cerințe Administrare și Configurare**
2.1	Permită accesul la aplicație unui număr nelimitat de utilizatori prin intermediul unei interfețe de tip web;
2.2	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;
2.3	Conțină un modul de raportare, care să includă atât rapoarte predefinite, cât și posibilitatea modificării acestora în funcție de cerințe/necesitați;
2.4	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;
2.5	Soluția trebuie să ofere o interfață ușor de utilizat pentru crearea de Custom Parsers necesare in prelucrarea evenimentelor provenite de la aplicații non-standard
2.6	Soluția trebuie să permită crearea de job-uri automate: rapoarte, arhivare etc.
2.7	Soluția trebuie să ofere posibilitatea de customizare a panourilor de control, precum și posibilitatea de a crea spații de lucru specifice în funcție de necesitățile utilizatorului.
2.8	Monitorizarea și managementul bazei da date trebuie să se facă din interfața soluției.
2.9	Soluția trebuie sa accepte ca parametri de căutare atât exemple simple precum si utilizarea de expresii de tip RegEX.
2.10	Interfața de căutare a soluției trebuie sa ofere abilitatea de a combina operatorii de căutare de tip Boolean(AND, OR, NOT) într-o singura expresie de căutare.

2.11	Interfața de căutare a soluției trebuie să ofere posibilitatea de a căuta folosind intervale de timp statice(data start-data stop) sau dinamice(acum-2h).
2.12	Soluția SIEM trebuie să ofere controlul centralizat a tuturor componentelor și funcțiilor administrative dintr-o singură interfață grafică web.
2.13	Administratorul trebuie să aibă 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.
2.14	Administratorul trebuie să fie în măsură 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.
2.15	Soluția trebuie să suporte auto descoperirea obiectelor care sunt protejate sau monitorizate.
2.16	Soluția trebuie să sprijine clasificarea automatizată a obiectelor care sunt protejate
2.17	Soluția trebuie să sprijine desprinderea anumitor panouri de instrumente din UI pentru utilizarea în SOC sau NOC.
2.18	Soluția trebuie să suporte modificarea porturile de comunicații între componente.
2.19	Soluția trebuie să ofere un API deschis pentru accesul la datele stocate în baza (bazele) de date.
2.20	Soluția trebuie să ofere posibilitatea de a cripta comunicațiile între componente.
2.21	Soluția trebuie să se integreze cu sisteme terțe ca o metodă de autentificare.

3.	**Cerințe operaționale**
3.1	Soluția trebuie să permită un rol pe etape din gestionare log-urilor și funcții de securitate a informației. Introducerea a mai multe capabilități de analiză ar trebui să reducă nevoia pentru componentele de sistem suplimentare și activarea acestora prin upgrade-ul cheilor de licență.
3.2	Soluția trebuie să ofere posibilitatea pentru o viitoare extindere și integrare cu alte soluții terțe.
3.3	Soluția trebuie să demonstreze "ușurința de utilizare". Ușurința de utilizare este esențială pentru implementarea cu succes și utilizarea soluției.
3.4	Soluția trebuie să sprijine actualizarea automată a informațiilor de configurare cu intervenție minimă din partea utilizatorului. De exemplu, actualizările taxonomiei de securitate, actualizări regulilor furnizorului, suportul dispozitivelor, etc.
3.5	Soluția trebuie să ofere un GUI web-based pentru management, analiză și raportare.
3.6	Soluția trebuie să ofere cerințe de disponibilitate înaltă într-un mod încorporat și fără a fi nevoie de software suplimentar.
3.7	Soluția trebuie să asigure 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).
3.8	Soluția trebuie să aibă un proces automatizat de recuperare/de backup.
3.9	Soluția trebuie să verifice 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.
3.10	Soluția trebuie să ofere mai multe panouri cu instrumente care pot fi personalizate pentru a îndeplini cerințele diferitor utilizatori ai sistemului.
3.11	Soluția trebuie să ofere panouri cu instrumente preinstalate (out of the box) (de exemplu, pentru managementul pericolelor, managementul de conformitate, etc.).
3.12	Soluția trebuie să ofere widget-uri personalizate care pot prezenta informații de securitate importantă pentru utilizatorii sistemului (de exemplu, verificarea evenimentelor, activităților in rețea, incidentelor etc.).
3.13	Soluția trebuie să mențină o bază de date a tuturor obiectelor descoperite în rețea. Datele referitoare la aceste obiecte trebuie să includă informații importante despre obiecte ca aflate din informațiile colectate (de exemplu sistemul de atribute, atribute de rețea, statistici de vulnerabilitate, etc.). Baza de date trebuie să furnizeze posibilitatea de a edita atributele atunci când acestea nu pot fi învățate (de exemplu departament, locație, etc.). Utilizatorul trebuie să poată căuta in această bază de date.

4.	**Cerințe de arhitectură**
4.1	Soluția trebuie să folosească o bază de date proprietară, proiectată pentru a permite stocarea și analiza

	istorica, la viteze ridicate asupra datelor.
4.2	Soluția trebuie să includă o baza de date relațională pentru stocarea log-urilor colectate;
4.3	Daca soluția este compusa din mai multe componente sau module, comunicarea intre aceste componente trebuie sa se realizeze in mod securizat.
4.4	Soluția trebuie să ofere posibilitate de căutare prin toate evenimentele stocate.
4.5	Soluția trebuie sa ofere mecanisme de integrare cu servicii de autentificare si autorizare precum: Active Directory, RADIUS, LDAP.
4.6	Soluția trebuie să ofere 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.
4.7	Soluția trebuie să ofere o funcție de stocare a log-urilor pe dispozitive NAS/SAN, folosind protocoalele din cadrul instituției precum: CIFS, NFS, iSCSI. La nivelul soluției trebuie sa existe posibilitatea de a crea partiții virtuale, la care se pot configura diferite reguli de retenție a datelor.
4.8	Soluția trebuie să ofere mecanisme împotriva falsificării și modificării datelor colectate.
4.9	Posede 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;
4.10	Soluția trebuie sa ofere mecanisme prin care se garantează livrarea evenimentelor în cazul în care unul dintre modulele soluției devine nedisponibil.
4.11	Soluția trebuie să se integreze cu alte soluții de securitate și informații de rețea din cadrul Parlamentului.
4.12	Soluția trebuie să sprijine 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.
4.13	Soluția trebuie să asigure integritatea informațiilor colectate.
4.14	Soluția trebuie să asigure mecanisme intuitive pentru rezolvarea problemelor, cum ar fi notificări, linie de comandă etc.
4.15	Soluția trebuie să suporte taxonomie extinsă de utilizare a evenimentelor și câmpuri. Utilizatorul trebuie să fie în măsură să adauge propriile nume de evenimente (de exemplu, posibilitatea de a adăuga câmpuri noi care nu sunt preinstalate, cum ar fi " SpecialID from my Custom Application ").
4.16	Soluția trebuie să permită marcarea evenimentelor definită de client.
4.17	Soluția trebuie să furnizeze restabilirea transparentă, agregarea, sortarea, filtrarea și analiza datelor în toate componentele distribuite.

5.	**Cerințe Log Management**
5.1	Soluția trebuie sa beneficieze de 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);
5.2	Ofere posibilitatea identificării incidentelor de securitate IT în timp real pe baza regulilor prestabilite și să permită prioritizarea evenimentelor în funcție de importanta;
5.3	Soluția trebuie să 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).
5.4	La nivelul soluției de log management trebuie să existe posibilitatea de asigurare a redundanței, în cazul în care un dispozitiv de stocare devine inaccesibil.
5.5	Soluția trebuie să ofere posibilitatea de a asigna un anumit eveniment unei categorii de evenimente.
5.6	Soluția trebuie să ofere mecanisme prin care se asigură integritatea log-urilor stocate.
5.7	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;
5.8	Soluția trebuie să ofere posibilitatea de a adăuga informații suplimentare in evenimentele stocate prin extragerea acestora din baze de date, Active Directory sau surse LDAP.
5.9	Soluția trebuie să suporte stocarea log-urilor și evenimentelor atât pe termen scurt cât și pe termen lung
5.10	Soluția trebuie să sprijine arhive de log-uri depozitate pe medii de stocare externe (3rd party).
5.11	Soluția trebuie să ofere capacități de depozitare și compresie eficientă a datelor colectate.
5.12	Soluția trebuie să suporte colectarea logurilor de pe toate echipamentele din cadrul Secretariatului Parlamentului
5.13	Soluția trebuie să furnizeze colectarea fără aplicații agent (agent-less) a log-urilor de evenimente, oricând.

5.14	Soluția trebuie să ofere posibilitatea de a distribui atât depozitarea cât și prelucrarea de evenimente în întreaga rețea Log Management/SIEM.
5.15	Soluția trebuie să sprijine accesul pe termen lung la date detaliate de evenimente de securitate și de flux de rețea. Sistemul trebuie să fie 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

6.	**Cerințe privind normalizarea și categorisirea log-urilor**
6.1	Transforme log-urile colectate într-un format comun (normalizat) și să permită categorisirea acestora în vederea efectuării unei analize ulterioare cât mai facile;
6.2	Soluția trebuie să ofere capabilitatea de agregare a evenimentelor. De asemenea trebuie să existe posibilitatea de a modifica regulile de agregare.
6.3	Soluția trebuie să normalizeze toate informațiile colectate într-un format comun.
6.4	Soluția trebuie să ofere capabilitatea de a modela evenimentele recepționate și de a le cataloga în grupuri logice precum: domenii, rețele, aplicații, nivele de criticitate etc.
6.5	Soluția trebuie să normalizeze 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.
6.6	Soluția trebuie să ofere o taxonomie comună de evenimente.
6.7	Soluția trebuie să ofere posibilitatea de a normaliza și agrega câmpuri de evenimente care nu sunt reprezentate de domeniile normalizate out-of-the-box.
6.8	Soluția trebuie să sprijine / normalizeze marcajele de timp ale evenimentelor din mai multe fusuri orare.

7.	**Cerințe privind filtrarea evenimentelor și analiză**
7.1	Soluția trebuie să ofere capabilitatea de a crea liste de interes cu informații importante, informații care pot fi folosite la definirea filtrelor și regulilor. Listele trebuie sa poată fi populate manual sau în mod dinamic pe baza unor interogări.
7.2	Dispună de posibilitatea filtrării log-urilor bazat pe orice criteriu legat de informațiile conținute în log-urile respective;
7.3	Ofere interogări dinamice si distribuite (trebuie sa suporte atât căutări simple cat si căutări complexe bazate pe expresii regulate si expresii logice de tip Boolean).
7.4	Soluția trebuie să ofere o analiză a evenimentelor în timpul real.
7.5	Soluția trebuie să ofere analiza tendințelor evenimentelor pe termen lung.
7.6	Soluția trebuie să ofere posibilitatea de concentrare și analiză a evenimentelor bazată pe un filtru specificat de către utilizator.
7.7	Soluția trebuie să ofere o vedere streaming în timp real care suportă capabilitățile de filtrare complete.
7.8	Soluția trebuie să ofere alertare bazată pe anomaliile observate și schimbările de comportament la evenimentele de rețea și de securitate.
7.9	Soluția trebuie să suporte și să mențină o istorie de activitate și autentificare a utilizatorului pe bază de dispozitive.

8.	**Cerințe privind raportarea**
8.1	Soluția trebuie să ofere posibilitatea de exportare a rapoartelor cel puțin in format: PDF, XML, CSV, HTML.
8.2	Soluția trebuie să ofere posibilitatea de a configura rapoartele din punct de vedere grafic in funcție de nevoile și politicile companiei(adăugarea de logo-uri, antete, etc.).
8.3	Soluția trebuie să conțină o serie de rapoarte predefinite, folosite în industria internaționala precum: PCIDSS, SOX, ISO 27000, NIST, COBIT, FISMA, GLBA, HIPAA, NERC, GDPR, fără a fi necesară cumpărarea unei licențe suplimentare.
8.4	Soluția trebuie să permite crearea de rapoarte fără a utiliza interogări complexe de tip SQL, ci prin interfețe ușor accesibile utilizatorului.
8.5	Soluția trebuie să furnizeze rapoarte cu privire la toate articolele disponibile pentru management prin intermediul GUI.
8.6	Soluția trebuie să ofere engine de raportare configurabil pentru crearea de rapoarte personalizate.
8.7	Soluția trebuie să suporte capacitatea de a planifica rapoarte.
8.8	Soluția trebuie să furnizeze rapoarte out-of-the-box pentru probleme tipice și operaționale.
8.9	Soluția trebuie să ofere un "panou cu instrumente" pentru vizualizarea rapidă a informațiilor de

	securitate și de rețea.
8.10	Soluția trebuie să suporte distribuția automată a rapoartelor.
8.11	Soluția trebuie să suporte capacitatea de a furniza rapoarte istorice ale tendințelor.
8.12	Soluția trebuie să suporte capacitatea de a livra la nivel central rapoarte de vulnerabilitate.
8.13	Soluția trebuie să suporte capacitatea de a livra la nivel central rapoarte.

9.	**Cerințe corelare și alertare**
9.1	Soluția trebuie sa 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.
9.2	Soluția trebuie să conțină cel puțin 100 de reguli de corelare “out-of-the-box”.
9.3	Soluția trebuie să ofere 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.
9.4	Soluția trebuie să ofere capabilitatea de a corela evenimente prin compararea cu liste statice sau dinamice.
9.5	Soluția trebuie să conțină alerte predefinite, care pot fi activate de utilizator.
9.6	Soluția trebuie să permită generarea alertelor pe baza severității evenimentelor detectate.
9.7	Soluția trebuie să fie capabila sa coreleze evenimente de la surse de date ce au fusuri orare diferite.
9.8	Soluția trebuie să detecteze automat întreruperile în procesul de colectare a datelor și să poată expedia alerte.
9.9	Soluția trebuie să ofere 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.
9.10	Poată identifica acțiuni repetitive sau tipuri de evenimente, pe baza cărora se pot seta reguli de alertare și se pot adopta politici de securitate.
9.11	Dispună de un motor de corelare care să permită identificarea elementelor comune din două sau mai multe evenimente aparent fără nicio legătură;
9.12	Soluția trebuie să ofere alerte bazate pe amenințări de securitate observate de la dispozitive monitorizate.
9.13	Soluția trebuie să ofere posibilitatea de a corela informațiile pe toate dispozitivele potențial disparate.
9.14	Soluția trebuie să ofere alertare bazată pe anomalii observate și schimbările de comportament în activitatea de rețea (flux) de date.
9.15	Soluția trebuie să ofere alerte bazate pe politica stabilită. (de exemplu, trafic, IM nu este permis.)
9.16	Soluția trebuie să suporte alerte ponderate pentru a permite prioritizarea. Gravitatea trebuie să fie atribuită în baza caracteristicilor cum ar fi tipul obiectului, protocol, aplicație, etc.
9.17	Soluția trebuie să ofere posibilitatea de a transmite alerte folosind mai multe protocoale și mecanisme pentru alte soluții de management.
9.18	Soluția trebuie să furnizeze un Wizard bazat pe UI și capabilități pentru a minimiza alarmele false și oferă rezultate precise.
9.19	Soluția trebuie să limiteze prezentarea semnalărilor multiple similare.
9.20	Soluția trebuie să suporte 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.
9.21	Soluția trebuie să suporte 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.
9.22	Soluția trebuie să suporte capacitatea de a corela împotriva vulnerabilităților străine ale rezultatelor scanării.
9.23	Soluția trebuie să monitorizeze 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.
9.24	Soluția trebuie să ofere 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).
9.25	Soluția trebuie să suporte corelație pentru o secvență lipsă. De exemplu serviciul s-a oprit nefiind urmat de restartarea serviciului în 10 minute.
9.26	Soluția trebuie să suporte 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.
9.27	Soluția trebuie să furnizeze 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.

10.	**Cerințe monitorizarea activității în rețea**
10.1	Soluția trebuie să ofere capabilitatea de a detecta anomalii la nivelul rețelei, utilizatorilor, aplicațiilor sau a altei surse de informații pe baza calculelor statistice și trebuie sa cuprindă în ea modul de management al riscurilor
10.2	Soluția trebuie să ofere capabilitatea de a urmări activitatea unui utilizator, prin corelarea datelor de la sisteme DHCP, VPN si Active Directory.
10.3	Soluția trebuie să mențină un inventar cu toate dispozitivele detectate la nivel de rețea. De asemenea trebuie să includă un modul capabil să detecteze, în mod automat, dispozitivele din rețea, pentru a facilita lucrul ulterior cu modulul de management al riscurilor.
10.4	Soluția trebuie să ofere 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.
10.5	Soluția trebuie să fie 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.
10.6	Soluția trebuie să permită crearea și păstrarea statisticilor de tip "baseline" asupra activității monitorizate. De asemenea trebuie să ofere capabilități de alertare în cazul în care se observă o deviație de la comportamentul normal.
10.7	Soluția trebuie să ofere 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 trebuie să necesite modificări la nivelul bazelor de date care urmează să fie monitorizate.
10.8	Soluția trebuie să ofere 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.
10.9	Soluția trebuie să includă tool-uri de investigare precum: WHOIS, DIG, Traceroute, NSLOOKUP etc.
10.10	Includă tablouri de bord grafice predefinite, precum și posibilitatea personalizării acestora pentru o imagine cît mai elocventă asupra nivelului de securitate; acestea trebuie sa poate afișa informațiile în timp real;
10.11	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;
10.12	Soluția trebuie să afișeze profiluri vizuale de trafic formulate în bytes, rate de pachete și numărul de gazde care comunică. Aceste ecrane trebuie să fie disponibile pentru aplicații, porturi, protocoale, amenințările și fiecare punct de supraveghere în rețea. Toate aceste puncte de vedere trebuie să 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.
10.13	Soluția trebuie să învețe dinamic norme de comportament și să recunoască modificările pe măsură ce acestea apar.
10.14	Soluția trebuie să detecteze atacuri de tip denial-of-service (DoS) și distributed-denial-of-service (DDoS).
10.15	Soluția trebuie să detecteze și să prezinte segmente de trafic referitoare la amenințările observate în rețea.
10.16	Soluția trebuie să suporte profilarea traficului asociat cu un design de rețea logică (de exemplu, de subrețea / CIDR).
10.17	Soluția trebuie să identifice traficul în rețea de la aplicații potențial periculoase (de exemplu, partajarea de fișiere, de tip peer-to-peer, etc.).

10.18	Soluția trebuie să afișeze profile de trafic în ceea ce privește rata de pachete. Această capacitate trebuie să fie disponibile pentru analiza simplă TCP (TCP flag, etc), dar informațiile bazate pe rată pot fi prezentate pentru alte profiluri (de exemplu, aplicații).
10.19	Soluția trebuie să identifice și să prezinte informații în mai multe intervale de timp. Profilul trebuie să fie disponibil pentru săptămână, zi și oră.
10.20	Soluția trebuie să fie în măsură să identifice comunicațiile, ce sunt generate din sau spre internet, conform regiunilor geografice în timp real.
10.21	Soluția trebuie să creeze profiluri independente și diferențiate din traficul local și traficul generat din sau destinat pentru internet.
10.22	Soluția trebuie să permită utilizatorului să creeze profiluri personalizate și vedere folosind orice proprietate a unui flux, jurnal, sursa de date sau de trafic deja profilate.
10.23	Soluția trebuie să suporte identificarea traficului bazat pe adrese IP, grupuri de adrese IP, perechi IP sursă / IP destinație etc.
10.24	Soluția trebuie să sprijine colectarea și analiza de date de captare de pachete.
10.25	Soluția trebuie să ofere posibilitatea de a extrage anumite câmpuri, definite de utilizatori, din pachetele de date capturate și de a folosi aceste câmpuri în regulile de corelare.
10.26	Soluția trebuie să identifice traficul într-un mediu de rețea virtuală.

11.	**Cerințe administrarea avansată a pericolelor**
11.1	Soluția trebuie să ofere o integrarea cu o soluție de tip Advanced Malware Detection și de import pentru indicatorii de compromis (IOC StiX): nume fișiere, hash, URL sau IP.
11.2	Soluția trebuie să ofere 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.
11.3	Soluția trebuie să ofere posibilitatea de a lega contextual activitatea aplicației în rețea cu evenimentele de securitate de la dispozitivele monitorizate.
11.4	Soluția trebuie să ofere posibilitatea de a lega contextual evenimentele de securitate raportate cu cunoștințele în timp real a obiectelor vizate.
11.5	Soluția trebuie să fie capabilă de a schimba în mod automat ponderile de credibilitate a dispozitivelor de securitate ca răspuns la atacurile din rețea.

12.	**Cerințe fluxul de lucru SIEM**
12.1	Dispună de diferite mecanisme de notificare: alerte la consola, e-mail, SNMP, SMTP;
12.2	Soluția trebuie să furnizeze capacități incorporate de monitorizare a fluxului de date pe care lucrătorii îl pot folosi pentru a ghida procesul de lucru.
12.3	Soluția trebuie să ofere 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 .
12.4	Soluția trebuie să ofere un mecanism pentru a adnota un incident de securitate, în timp ce acesta este adresat de către lucrătorii operațiunilor de securitate.
12.5	Soluția trebuie să ofere 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 trebuie să fie capabil de a filtra incidente de-a lungul acestor atribute definite.

13.	**Cerințele sursei de date**
13.1	Soluția trebuie să ofere posibilitatea de colectare și parsare a log-urilor de la diverse surse de date sau din “flat files”.
13.2	Soluția trebuie să ofere posibilitatea de integrare a surselor de date nesuportate, prin creare locală a regulilor de parsare fără a fi nevoie de licențe suplimentare.
13.3	Soluția trebuie să ofere posibilitatea de a defini o singură sursă de date pentru mai multe sisteme identice, care au aceleași proprietăți.
13.4	Soluția trebuie să ofere posibilitatea de integrare cu cel puțin următoarele soluții de management al vulnerabilităților: Qualys, Nessus, Metasploit, Saint, Rapid7, nCircle, Lumension, McAfee, eEye Retina, LanGuard, OpenVAS.

13.5	Soluția trebuie să suporte scanerele de vulnerabilități de top din industrie.
13.6	Soluția trebuie să ofere posibilitatea construirii și implementării de surse de evenimente specifice „CUSTOM" pe lângă celor suportate nativ.
13.7	Adăugarea surselor de date trebuie să se facă din interfața soluției, fără a fi nevoie de a instala agenți sau pachete software suplimentare.
13.8	Soluția trebuie să ofere posibilitate de detecție și notificare atunci când o anumita sursă de date nu generează log-uri conform comportamentului învățat.
13.9	Soluția trebuie să ofere posibilitatea de colectare a datelor de tip flow: Netflow v5, v7, v9, SFlow și J-Flow.
13.10	Soluția trebuie să suporte produsele de la mai mulți furnizori.
13.11	Soluția trebuie să suporte informațiile colectate de la soluții de baze de date de clasă Enterprise.
13.12	Soluția trebuie să suporte informațiile colectate de la aplicații comerciale.
13.13	Soluția trebuie să suporte informațiile colectate de la aplicații proprietare.
13.14	Soluția trebuie să suporte informațiile colectate de software-ul de securitate și instrumentele Database Activity Monitoring (DAM).
13.15	Soluția trebuie să suporte informațiile colectate de către software-ul de securitate și instrumentele File Integrity/Activity Monitoring (FIM/FAM).
13.16	Soluția trebuie să suporte informațiile colectate de la software-ul și instrumentele de securitate al Identity & Acces Management (IAM).
13.17	Soluția trebuie să suporte informațiile colectate de la sistemele de management al rețelei (de exemplu Microsoft MOM, etc.).
13.18	Soluția trebuie să suporte informațiile colectate de la infrastructura rețelei (de exemplu, switch-uri, routere, etc.).

14.	**Cerințe fata de ofertant (furnizor)**
14.1	Ofertantul trebuie să posede o experiență specifică în domeniu în livrarea bunurilor și/sau prestarea serviciilor similare in Republica Moldova cel puțin 3 ani
14.2	Ofertantul trebuie să prezinte autorizația de la producător pentru a oferta în concursul dat (MAF)
14.3	Ofertantul trebuie prezinte minim 2 ingineri certificați de producătorul produsului pentru implementarea soluției ofertate (de anexat copii după certificări, diplome, *etc.*)
14.4	Ofertantul trebuie să posede minim 2 ingineri cu experiență in implementarea cel puțin a unui proiect bazat pe soluția ofertată (de anexat descrierea proiectului implementat și CV-urile specialiștilor)
14.5	Ofertantul trebuie să posede minim 1 referință de implementare a soluției propuse in sectorul public (de anexat copii după contracte și/sau recomandări)
14.6	Ofertantul trebuie să posede certificarea sistemului de management al securității informației (ISO 27001).
14.7	Furnizorul va trebui sa asigure instalarea soluției conform cerințelor, precum și documentația tehnică aferenta echipamentelor instalate (manuale, proceduri, instrucțiuni scrise pentru soluția propusa și particularitățile acesteia).
14.8	Ofertantul va trebui sa asigure service si suport tehnic local în perioada de garanție și mentenanță, conform tipului de suport solicitat: Minim 3 ani de full garanție si mentenanța „parts", „labour", și „on site".
14.9	Service si suport tehnic al companiei ofertante obligatoriu 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
14.10	Oferta va include servicii de instalare, ajustare, asistență tehnică pe întreaga perioadă de garanție, cu instruirea a min. 2 administratori. Oferta include toate părțile necesare pentru instalare și punerea în funcțiune (exemplu: cabluri, șuruburi, piulițe, fascete, organizatori de cabluri, etc.)