

Anexa 3

Matricea de conformitate conform cerințelor solicitate la caiet de sarcini pentru Soluții software de tip SIEM

	Monitorizarea și audit al evenimentelor de securitate informațională – SIEM (Security Information Event Management)	Produsul oferit: McAfee SIEM Enterprise Security Manager, Enterprise Log Manager and Event Receiver VM (8 Cores) – virtual appliance.
1.	Cerințe tehnice minimale	Cerințe tehnice propuse
1.1	Soluția trebuie să permită colectarea log-urilor și monitorizarea unui număr de minim 750 de dispozitive de rețea/securitate (serve, firewall-uri, IDS/IPS-uri, routere etc) și stații de lucru;	Soluția oferită acoperă solicitarea.
1.2	Soluția trebuie să suporte un nivel de minim 1500 EPS (evenimente per secundă) în regim de lucru cu analiza tuturor activităților la maximum (Query EPS) și de până la 5000 EPS (eveniment per secundă) în regim de lucru cu funcțional limitat al utilizatorilor (Ingestion EPS) în scopul de a putea acoperi ulterioarele extinderi al sistemului informațional din cadrul Centrului National Anticorupție.	Appliance Virtual McAfee suporta un nivel de până la 1500 EPS și până la 5000 EPS (eveniment per secundă) în regim de lucru cu funcțional limitat al utilizatorilor (Ingestion EPS).
1.3	Minim 50 000 bidirecțional flows/minut (Packeteer, NetFlow, J-Flow, sFlow and IPFIX data from network devices). Posibilitatea creșterii de la 50 000 la 200 000 Flows/minut doar prin licență (fără înlocuirea echipamentului).	Soluția oferită corespunde acestei solicitări și acoperă până la 200 000 Flows/minut.
1.4	Soluția trebuie prezentată ca o soluție integrată – un appliance virtual (confirmat de producător), ce să fie format dintr-o mașină virtuală SW dedicat soluțiilor SIEM în scopul de a îndeplini toate funcționalitățile descrise în acest document.	Soluția prezentată ca o soluție integrată – un appliance virtual (confirmat de producător), ce să fie format dintr-o mașină virtuală SW dedicat soluțiilor SIEM în scopul de a îndeplini toate funcționalitățile descrise în acest document.
1.5	Soluția trebuie să ofere cel puțin un factor de compresie de 20:1 pentru stocarea log-urilor în format brut în scopul micsorării spațiului de arhivare pentru următorii ani.	Online Live data sunt accesate fără nici o latență. Compacted data sunt comprimate cu o rată de 20:1.
1.6	Soluția trebuie să ofere posibilitatea dezvoltării ulterioare a soluției într-un mod cât mai facil (să fie scalabilă);	Soluția oferită corespunde acestei solicitări.
1.7	Soluția trebuie să ofere posibilitate de a fi extinsă prin adăugarea unui modul, care execută o anumită funcționalitate (colectare, corelare, stocare log-uri) integrabil cu platforma existentă.	Soluția oferită are un repository bogat de module adiționale.
1.8	Soluția propusă trebuie să fie prezentă în „Cadrul de Lider” în cadrul ultimului raport publicat de Gartner pe subiectul „Magic Quadrant for Security Information and Event Management”	Produsul oferit se află în „Cadrul de Lider” de mai bine de 5 ani.
1.9	Fie capabilă să colecteze evenimente de la minim următoarele surse: - Cisco Router - Cisco FWSM/ASA Firewall - Cisco Catalyst Switch - Cisco IPS/IDS - Bitdefender/Kaspersky - Checkpoint Firewall - Microsoft Active Directory - Microsoft Exchange 2010, 2013, 2016 - Microsoft SQL 2008, 2012, 2016 - Microsoft Windows Server 2008 R2, 2012 R2, 2016 Etc.	Soluția oferită este capabilă să colecteze evenimente de la sursele mai jos descrise: - 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
2.	Cerințe Administrare și Configurare	
2.1	Permite accesul la aplicație unui număr nelimitat de utilizatori prin intermediul unei interfețe de tip web;	Accesul către consolă web este nelimitat de numărul utilizatorilor.

2.2	Permite vizualizarea evenimentelor în timp real și într-un format comun, inteligibil, din cadrul consolei de administrare, fără a fi necesară accesarea unei terțe aplicații;	Soluția permite vizualizarea evenimentelor în timp real și într-un format comun, inteligibil, din cadrul consolei de administrare, fără a fi necesară accesarea unei terțe aplicații;
2.3	Conține un modul de raportare, care să includă atât rapoarte predefinite, cât și posibilitatea modificării acestora în funcție de cerințe/necesități;	Produsul oferă posibilitatea data cit și rapoarte personalizate (Report Layout și Query Wizard).
2.4	Dispune de un pachet de reguli de corelare și alertare care să adreseze cele mai întâlnite amenințări asupra securității unei rețele, precum și posibilitatea modificării acestor reguli în funcție de cerințe/necesități;	Soluția are un set de corelări predefinite care pot fi modificate de către administrator după necesitate.
2.5	Soluția să ofere o interfață ușor de utilizat pentru crearea de Custom Parsers necesare în prelucrarea evenimentelor provenite de la aplicații non-standard	Soluția oferă o interfață ușor de utilizat pentru crearea de Custom Parsers necesare în prelucrarea evenimentelor provenite de la aplicații non-standard.
2.6	Soluția trebuie să permită crearea de job-uri automate: rapoarte, arhivare etc.	Soluția permite crearea job-urilor, rapoarte, alerte, archive.
2.7	Soluția trebuie să ofere posibilitatea de personalizare a panourilor de control, precum și posibilitatea de a crea spații de lucru specifice în funcție de necesitățile utilizatorului.	Soluția permite crearea panourilor personalizate.
2.8	Administrarea bazei de date trebuie să se facă din interfața soluției. Aceasta trebuie să fie integrată în soluție.	Soluția acoperă cerința solicitată.
2.9	Soluția trebuie să accepte ca parametri de căutare atât exemple simple precum și utilizarea de expresii de tip RegEX.	Soluția acceptă ca parametri de căutare atât exemple simple precum și utilizarea de expresii de tip RegEX.
2.10	Interfața de căutare a soluției trebuie să ofere abilitatea de a combina operatorii de căutare de tip Boolean(AND, OR, NOT) într-o singură expresie de căutare.	Soluția permite combinarea operatorilor 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).	Interfața soluției permite căutarea folosind intervale de timp statice ori dinamice.
2.12	Soluția SIEM trebuie să ofere controlul centralizat al tuturor componentelor și funcțiilor administrative dintr-o singură interfață grafică web.	Soluția oferă această funcționalitate.
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.	Soluția oferită corespunde acestei solicitări.
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 în raza rolului utilizatorului dat, de exemplu, administrarea, raportarea, filtrarea evenimentelor, corelația, și/sau vizualizarea panoului de instrumente.	Soluția oferită corespunde acestei solicitări.
2.15	Soluția trebuie să suporte auto descoperirea obiectelor care sunt protejate sau monitorizate.	Soluția permite auto descoperirea obiectelor.
2.16	Soluția trebuie să sprijine clasificarea automatizată a obiectelor care sunt protejate	Produsul oferit are la bază clasificarea automată a obiectelor.
2.17	Soluția trebuie să sprijine desprinderea anumitor panouri de instrumente din UI pentru utilizarea în SOC sau NOC.	Soluția oferită corespunde acestei solicitări.
2.18	Soluția trebuie să suporte modificarea porturilor de comunicații între componente.	Soluția oferită corespunde acestei solicitări.
2.19	Soluția trebuie să ofere un API deschis pentru accesul la datele stocate în baza (bazele) de date.	Soluția are la bază API deschis.
2.20	Soluția trebuie să ofere posibilitatea de a cripta comunicațiile între componente.	Soluția oferă canalul criptat între surse.
2.21	Soluția trebuie să se integreze cu sisteme terțe ca o metodă de autentificare.	Soluția permite integrarea în AD.

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 capacități de analiză ar trebui să reducă nevoia pentru componentele de sistem suplimentare și activarea acestora prin upgrade-ul cheilor de licență.	Solutia ofertata corespunde acestei solicitari.
3.2	Soluția trebuie să ofere posibilitatea pentru o viitoare extindere și integrare cu alte soluții terțe.	Solutia permite integrarea cu alte sisteme.
3.3	Soluția trebuie să demonstreze "ușurința de utilizare". Ușurința de utilizare este esențială pentru implementarea cu succes și utilizarea soluției.	Solutia ofertata este usoara si intuitiva in administrare, utilizare.
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.	Solutia ofertata corespunde acestei solicitari.
3.5	Soluția trebuie să ofere un GUI web-based pentru management, analiză și raportare.	Solutia este bazata pe web-base platform.
3.6	Soluția trebuie să ofere cerințe de disponibilitate înaltă într-un mod încorporat și fără a fi nevoie de software suplimentar.	Solutia ofera 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).	Solutia asigura că toate componentele distribuite ale sistemului vor continua să funcționeze atunci când orice altă parte a sistemului eșuează sau pierde de conectivitate.
3.8	Soluția trebuie să aibă un proces automatizat de recuperare/de backup.	Solutia ofera posibilitate data (Backup & Restore).
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.	Solutia permite monitorizarea sitemului si alertarea in caz de necesitate (Device Status).
3.10	Soluția trebuie să ofere mai multe panouri cu instrumente care pot fi personalizate pentru a îndeplini cerințele diferitor utilizatori ai sistemului.	Solutia ofertata corespunde acestei solicitari.
3.11	Soluția trebuie să ofere panouri cu instrumente preinstalate (out of the box) (de exemplu, pentru managementul pericolelor, managementul de conformitate, etc.).	Solutia oferă panouri cu instrumente preinstalate (out of the box).
3.12	Soluția trebuie să ofere widget-uri personalizate care pot prezenta informații de securitate importantă pentru utilizatorii sistemului (de exemplu, verificarea evenimentelor, activităților în rețea, incidentelor etc.).	Corespunde, solutia ofera widget-uri personalizate care pot prezenta informații de securitate importantă pentru utilizatorii sistemului.
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 attribute, attribute de rețea, statistici de vulnerabilitate, etc.). Baza de date trebuie să furnizeze posibilitatea de a edita attributele atunci când acestea nu pot fi învățate (de exemplu departament, locație, etc.). Utilizatorul trebuie să poată căuta în această bază de date.	Solutia ofertata corespunde acestei solicitari.
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.	Corespunde, Nitro DB.
4.2	Soluția trebuie să includă o baza de date relațională pentru stocarea log-urilor colectate;	Corespunde, Nitro DB.

4.3	Daca soluția este compusa din mai multe componente sau module, comunicarea între aceste componente trebuie sa se realizeze în mod securizat.	Comunicarea între toate componentele soluției este securizata.
4.4	Soluția trebuie să ofere, ca opțiune, posibilitatea de asigurare a high-availability, la nivelul de colectare, cât și la nivelul de procesare și stocare a datelor, în cazul în care este nevoie.	Solutia ofertata corespunde acestei solicitari.
4.5	Soluția trebuie să ofere posibilitate de căutare prin toate evenimentele stocate.	Corespunde, solutia ofera posibilitate de căutare prin toate evenimentele stocate.
4.6	Soluția trebuie sa ofere mecanisme de integrare cu servicii de autentificare si autorizare precum: Active Directory, RADIUS, LDAP.	Corespunde, solutia ofera mecanisme de integrare cu servicii de autentificare si autorizare precum: Active Directory, RADIUS, LDAP.
4.7	Soluția trebuie să ofere o serie de mecanisme (caching etc.), astfel încât atunci când numărul de 1500 de EPS (Query EPS) depășește limita impusa de licența sau capabilitățile de procesare, surplusul de evenimente nu va fi pierdut.	În cazul depășirii numărului de EPS, ele nu se pierd doar ca vin cu întârziere.
4.8	Soluția trebuie să ofere o funcție de stocare a log-urilor pe dispozitive NAS/SAN, folosind protocoalele din cadrul institutiei 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.	Solutia ofertata corespunde acestei solicitari.
4.9	Soluția trebuie să ofere mecanisme împotriva falsificării și modificării datelor colectate.	Corespunde, User data protection raspunde de acest functional.
4.10	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;	Solutia ofertata corespunde acestei solicitari.
4.11	Soluția trebuie sa ofere mecanisme prin care se garantează livrarea evenimentelor în cazul în care unul dintre modulele soluției devine nedisponibil.	Solutia ofertata corespunde acestei solicitari.
4.12	Soluția trebuie să permită implementările ca appliance virtual	Solutia ofertata corespunde acestei solicitari.
4.13	Soluția trebuie să se integreze cu alte soluții de securitate și informații de rețea din cadrul CNA.	Solutia ofertata corespunde acestei solicitari.
4.14	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.	Solutia ofertata corespunde acestei solicitari.
4.15	Soluția trebuie să asigure integritatea informațiilor colectate.	Solutia ofertata corespunde acestei solicitari.
4.16	Soluția trebuie să asigure mecanisme intuitive pentru rezolvarea problemelor, cum ar fi notificări, linie de comandă etc.	Solutia ofertata corespunde acestei solicitari.
4.17	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 " Special ID from my Custom Application ").	Solutia ofertata corespunde acestei solicitari.
4.18	Soluția trebuie să permită marcarea evenimentelor definită de client.	Solutia permite marcarea evenimentelor.
4.19	Soluția trebuie să furnizeze restabilirea transparentă, agregarea, sortarea, filtrarea și analiza datelor în toate componentele distribuite.	Solutia ofertata corespunde acestei solicitari.
5. Cerințe Log Management		
5.1	Solutia 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 international NIST 800-92 (Log Management Standard);	Solutia ofertata este conforma acestui standart: https://community.mcafee.com/docs/DOC-4346

5.2	Ofere posibilitatea identificării incidentelor de securitate IT în timp real pe baza regulilor prestabilite și să permită prioritizarea evenimentelor în funcție de importanță;	Solutia ofertata corespunde acestei solicitari.
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).	Solutia permite 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.	Solutia ofertata corespunde acestei solicitari.
5.5	Soluția trebuie să ofere posibilitatea de a asigna un anumit eveniment unei categorii de evenimente.	Solutia ofertata corespunde acestei solicitari.
5.6	Soluția trebuie să ofere mecanisme prin care se asigură integritatea log-urilor stocate.	Corespunde, Nitrosecurity asigura acest mecanism, algoritmul de cryptare si validare este sha1.
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;	Corespunde, permite utilizarea unui API pentru normalizarea evenimentelor proprietare si non-proprietar.
5.8	Soluția trebuie să ofere posibilitatea de a adăuga informații suplimentare în evenimentele stocate prin extragerea acestora din baze de date, Active Directory sau surse LDAP.	Corespunde, soltuia permite integrearea cu AD, LDAP.
5.9	Soluția trebuie să aibă o colecție log-uri și o arhitectură de arhive care suportă stocarea evenimentelor atât pe termen scurt (on-line) și pe termen lung (off-line).	Solutia ofertata corespunde acestei solicitari.
5.10	Soluția trebuie să sprijine arhive de log-uri depozitate pe medii de stocare externe (3rd party).	Solutia ofertata corespunde acestei solicitari.
5.11	Soluția trebuie să ofere capacități de depozitare și compresie eficientă a datelor colectate.	Solutia ofertata corespunde, compresia 20:1.
5.12	Soluția trebuie să sprijine metode răspândite de colectare a logurilor (syslog, WMI, JDBC, SNMP, Checkpoint LEA, etc)	Solutia ofertata corespunde acestei solicitari.
5.13	Soluția trebuie să furnizeze colectarea fără aplicații agent (agent-less) a log-urilor de evenimente, oricând.	Solutia ofertata corespunde, nu utilizeaza agenti.
5.14	Soluția trebuie să ofere posibilitatea de a distribui atât depozitarea cât și prelucrarea de evenimente în întreaga rețea Log Management/SIEM.	Solutia ofertata corespunde acestei solicitari.
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 în sistem din sistemul de stocare si analiza ulterioara	Solutia ofertata corespunde acestei solicitari.
6.	Cerințe privind normalizarea și categorizarea log-urilor	
6.1	Transforme log-urile colectate într-un format comun (normalizat) și să permită categorizarea acestora în vederea efectuării unei analize ulterioare cât mai facile;	Solutia ofertata corespunde acestei solicitari.
6.2	Soluția trebuie să ofere capabilitatea de agregare a evenimentelor. De asemenea trebuie să existe posibilitatea de a modifica regulile de agregare.	Solutia ofertata corespunde acestei solicitari.
6.3	Soluția trebuie să normalizeze toate informațiile colectate într-un format comun.	Solutia ofertata corespunde acestei solicitari.
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.	Solutia ofertata corespunde acestei solicitari.
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.	Solutia ofertata corespunde acestei solicitari.
6.6	Soluția trebuie să ofere o taxonomie comună de evenimente.	Solutia ofertata corespunde acestei solicitari.

6.7	Soluția trebuie să ofere posibilitatea de a normaliza și agrega cîmpuri de evenimente care nu sunt reprezentate de domeniile normalizate out-of-the-box.	Solutia ofertata corespunde acestei solicitari.
6.8	Soluția trebuie să sprijine / normalizeze marcajele de timp ale evenimentelor din mai multe fusuri orare.	Solutia ofertata corespunde acestei solicitari.
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 să poată fi populate manual sau în mod dinamic pe baza unor interogări.	Solutia permite crearea listelor de interes care ulterior pot fi folosite la filtre.
7.2	Disponă de posibilitatea filtrării log-urilor bazat pe orice criteriu legat de informațiile conținute în log-urile respective;	Solutia permite filtrarea pe baza conținutului din logurile colectate.
7.3	Ofere interogări dinamice și distribuite (trebuie să suporte atât căutări simple cât și căutări complexe bazate pe expresii regulate și expresii logice de tip Boolean).	Solutia ofertata corespunde, permite utilizarea interogarilor dinamice și expresii regulate, logice.
7.4	Soluția trebuie să ofere o analiză a evenimentelor în timpul real.	Solutia ofertata corespunde acestei solicitari.
7.5	Soluția trebuie să ofere analiza tendințelor evenimentelor pe termen lung.	Solutia ofertata corespunde acestei solicitari.
7.6	Soluția trebuie să ofere posibilitatea de concentrare și analiză a evenimentelor bazată pe un filtru specificat de către utilizator.	Solutia ofertata corespunde, utilizatorul poate singur crea filtrele.
7.7	Soluția trebuie să ofere o vedere streaming în timp real care suportă capabilitățile de filtrare complete.	Solutia ofertata corespunde acestei solicitari.
7.8	Soluția trebuie să ofere alertare bazată pe anomalii observate și schimbările de comportament la evenimentele de rețea și de securitate.	Solutia ofertata corespunde, utilizatorul poate să creeze alertele date.
7.9	Soluția trebuie să suporte și să mențină o istorie de activitate și autentificare a utilizatorului pe bază de dispozitive.	Solutia ofertata corespunde acestei solicitari.
8.	Cerințe privind raportarea	
8.1	Soluția trebuie să ofere posibilitatea de exportare a rapoartelor cel puțin în format: PDF, XML, CSV, HTML.	Solutia ofertata corespunde, generează aceste rapoarte și le pastrează local, remote sau le transmite prin e-mail.
8.2	Soluția trebuie să ofere posibilitatea de a configura rapoartele din punct de vedere grafic în funcție de nevoile și politicile companiei (adăugarea de logo-uri, antete, etc.).	Solutia ofertata corespunde, rapoartele sunt personalizate.
8.3	Soluția trebuie să conțină o serie de rapoarte predefinite, folosite în industria internațională precum: PCI, Basel, FISMA, GLBA, HIPAA, NERC, GDPR, Sarbanes-Oxley, SOX, ISO 27002 fără a fi necesară cumpărarea unei licențe suplimentare.	Solutia ofertata corespunde, conține toate rapoartele solicitate fără a procura licența separată.
8.4	Soluția trebuie să permită crearea de rapoarte fără a utiliza interogări complexe de tip SQL, ci prin interfețe ușor accesibile utilizatorului.	Solutia ofertata corespunde, report layout și query wizard.
8.5	Soluția trebuie să furnizeze rapoarte cu privire la toate articolele disponibile pentru management prin intermediul GUI.	Solutia ofertata corespunde, report layout.
8.6	Soluția trebuie să ofere engine de raportare configurabil pentru crearea de rapoarte personalizate.	Solutia ofertata corespunde, report layout.
8.7	Soluția trebuie să suporte capacitatea de a planifica rapoarte.	Solutia ofertata corespunde acestei solicitari.
8.8	Soluția trebuie să furnizeze rapoarte out-of-the-box pentru probleme tipice și operaționale.	Solutia ofertata corespunde, conține un set de rapoarte pentru problemele tipice/operationale.
8.9	Soluția trebuie să furnizeze rapoarte out-of-the-box de regulamente specifice de conformitate (PCI, SOX, FISMA) și cadre de control, inclusiv (NIST, COBIT, ISO).	Solutia ofertata corespunde, conține un set de rapoarte specifice de conformitate (PCI, SOX, FISMA) și cadre de control, inclusiv (NIST, COBIT, ISO).
8.10	Soluția trebuie să ofere un "panou cu instrumente" pentru vizualizarea rapidă a informațiilor de securitate și de rețea.	Solutia ofertata corespunde, permite vizualizarea rapidă a informațiilor de securitate și de rețea.
8.11	Soluția trebuie să suporte distribuția automată a rapoartelor.	Solutia ofertata corespunde, prin e-mail sau remote storage.

8.12	Soluția trebuie să suporte capacitatea de a furniza rapoarte istorice ale tendințelor.	Solutia ofertata corespunde acestei solicitari.
8.13	Soluția trebuie să suporte capacitatea de a livra la nivel central rapoarte de vulnerabilitate.	Solutia suporta livrarea rapoarelor de vulnerabilitate la nivel central.
8.14	Soluția trebuie să suporte capacitatea de a livra la nivel central rapoarte.	Solutia ofertata corespunde acestei solicitari.
9.	Cerințe corelare și alertare	
9.1	Soluția trebuie să poată face corelarea istorică a evenimentelor în 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.	Solutia permite corelarea istorica a evenimentelor.
9.2	Soluția trebuie să conțină cel puțin 150 de reguli de corelare "out-of-the-box".	Solutia ofertata corespunde, 150 de reguli.
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.	Solutia ofera posibilitatea de a crea noi reguli de corelare, utilizind interfata web.
9.4	Soluția trebuie să ofere capabilitatea de a corela evenimente prin compararea cu liste statice sau dinamice.	Solutia ofera 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.	Solutia ofertata contine alerte predefinite.
9.6	Soluția trebuie să permită generarea alertelor pe baza severității evenimentelor detectate.	Solutia permite generarea alertelor pe baza severității evenimentelor detectate.
9.7	Soluția trebuie să fie capabilă să coreleze evenimente de la surse de date ce au fusuri orare diferite.	Solutia este 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.	Solutia detecteaza automat întreruperile în procesul de colectare a datelor și poate 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 asigură integritatea analizelor de tip "forensic" pentru determinarea timpului când a fost generat evenimentul.	Solutia ofertata corespunde acestei solicitari.
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.	Solutia poate 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	Ofere posibilitatea dezvoltării de reguli de alertare înlănțuite (compuse din 2 sau mai multe reguli definite anterior);	Solutia ofertata corespunde acestei solicitari.
9.12	Dispună de un motor de corelare care să permită identificarea elementelor comune din două sau mai multe evenimente aparent fără nicio legătură;	Solutia dispune de un motor de corelare care să permită identificarea elementelor comune din două sau mai multe evenimente aparent fără nicio legătură.
9.13	Soluția trebuie să ofere alerte bazate pe amenințări de securitate observate de la dispozitive monitorizate.	Solutia ofera alerte bazate pe amenințări de securitate observate de la dispozitive monitorizate.
9.14	Soluția trebuie să ofere posibilitatea de a corela informațiile pe toate dispozitivele potențial disparate.	Solutia ofertata corespunde acestei solicitari.
9.15	Soluția trebuie să ofere alertare bazată pe anomalii observate și schimbările de comportament în activitatea de rețea (flux) de date.	Solutia ofera alertare bazată pe anomalii observate și schimbările de comportament în activitatea de rețea (flux) de date.
9.16	Soluția trebuie să ofere alerte bazate pe politica stabilită. (de exemplu, trafic, IM nu este permis.)	Solutia ofera alerte bazate pe politica stabilita.
9.17	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.	Solutia ofertata corespunde acestei solicitari.
9.18	Soluția trebuie să ofere posibilitatea de a transmite alerte folosind mai multe protocoale și mecanisme pentru alte soluții de management.	Solutia ofertata corespunde, e-mail, sms, snmp, syslog.
9.19	Soluția trebuie să furnizeze un Wizard bazat pe UI și capabilități pentru a minimiza alarmele false și oferă rezultate precise.	Solutia ofertata corespunde acestei solicitari.

9.20	Soluția trebuie să limiteze prezentarea semnalărilor multiple similare.	Solutia ofertata corespunde acestei solicitari.
9.21	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.	Solutia ofertata corespunde acestei solicitari.
9.22	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.	Solutia suporta capacitatea de a corela împotriva feed-urilor străine de date de securitate.
9.23	Soluția trebuie să suporte capacitatea de a corela împotriva vulnerabilităților străine ale rezultatelor scanării.	Solutia suporta capacitatea de a corela împotriva vulnerabilităților străine ale rezultatelor scanării.
9.24	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.	Solutia monitorizeaza și alerteaza atunci cand exista o intrerupere in colectarea log-urilor de pe un dispozitiv.
9.25	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).	Solutia ofera un mecanism out-of-the-box pentru a descoperi și clasifica obiectele după tipul sistemului.
9.26	Soluția trebuie să suporte corelație pentru o secvență lipsă. De exemplu serviciul s-a oprit nefiind urmat de restartarea serviciului în 10 minute.	Solutia suporta corelatie pentru o secventa lipsa.
9.27	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.	Solutia suporta corelarea pentru valorile aditive pe parcursul timpului.
9.28	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.	Solutia ofertata corespunde acestei solicitari.
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.	Solutia ofera capabilitatea de a detecta anomalii la nivelul rețelei, utilizatorilor, aplicațiilor sau a altei surse de informații pe baza calculelor statistice și cuprinde 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 și Active Directory.	Solutia ofera capabilitatea de a urmări activitatea unui utilizator, prin corelarea datelor de la sisteme DHCP, VPN și 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.	Solutia ofertata corespunde acestei solicitari.
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.	Solutia ofera posibilitatea operatorului să creeze panouri de comandă (dashboards) specifice monitorizării Active Directory.
10.5	Soluția trebuie să fie capabilă să detecteze automat anomaliiile de trafic WEB pentru utilizatorii interni, aceasta monitorizare se va realiza prin integrarea bidirecțională cu	Solutia detecteaza automat anomaliiile de trafic WEB pentru utilizatorii interni.

	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.	Solutia ofertata corespunde acestei solicitari.
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 și corelare și alertarea acestor evenimente. Soluția nu trebuie să necesite modificări la nivelul bazelor de date care urmează să fie monitorizate.	Solutia ofera mecanisme avansate de analiza a traficului de rețea, prin metoda sniffing, și permite colectarea traficului specific bazelor de date tranzacționale cu obiectivul de monitorizare, analiza și corelare și alertarea acestor evenimente.
10.8	Soluția trebuie să ofere mecanisme de detecție avansate prin decodarea traficului de rețea L7 existent în cadrul instituției. 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.	Solutia ofera mecanisme de detecție avansate prin decodarea traficului de rețea L7.
10.9	Soluția trebuie să includă tool-uri de investigare precum: WHOIS, DIG, Traceroute, NSLOOKUP etc.	Solutia include WHOIS, DIG, Traceroute, NSLOOKUP.
10.10	Includă tablouri de bord grafice predefinite, precum și posibilitatea personalizării acestora pentru o imagine cât mai elocventă asupra nivelului de securitate; acestea trebuie să poată afișa informațiile în timp real;	Solutia include tablouri de bord grafice predefinite, precum și posibilitatea personalizării acestora pentru o imagine cât mai elocventă asupra nivelului de securitate; acestea pot afișa informațiile în timp real.
10.11	Disponă 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 aceluia atac;	Solutia ofertata corespunde acestei solicitari.
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.	Solutia ofertata corespunde acestei solicitari.
10.13	Soluția trebuie să învețe dinamic norme de comportament și să recunoască modificările pe măsură ce acestea apar.	Solutia poate învăța 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).	Solutia ofertata corespunde, detecteaza DoS și DDoS.
10.15	Soluția trebuie să detecteze și să prezinte segmente de trafic referitoare la amenințările observate în rețea.	Solutia ofertata corespunde acestei solicitari.
10.16	Soluția trebuie să suporte profilarea traficului asociat cu un design de rețea logică (de exemplu, de subrețea / CIDR).	Solutia ofertata corespunde acestei solicitari.
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.).	Solutia poate să identifice traficul în rețea de la aplicații potențial periculoase.
10.18	Soluția trebuie să afișeze profile de trafic în ceea ce privește rata de pachete. Această capacitate trebuie să fie disponibilă pentru analiza simplă TCP (TCP flag, etc), dar informațiile bazate pe rată pot fi prezentate pentru alte profiluri (de exemplu, aplicații).	Solutia ofertata corespunde acestei solicitari.
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.	Solutia ofertata corespunde acestei solicitari.
10.20	Soluția trebuie să fie în măsură să identifice comunicațiile, ce sunt generate din sau spre internet, conform regiunilor geografice în timp real.	Solutia ofertata corespunde acestei solicitari.

10.21	Soluția trebuie să creeze profiluri independente și diferențiate din traficul local și traficul generat din sau destinat pentru internet.	Solutia ofertata corespunde acestei solicitari.
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.	Solutia permite 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.	Solutia permite 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.	Solutia permite 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.	Solutia ofera 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 în rețea într-un mediu de rețea virtuală.	Solutia identifica traficul într-un mediu de rețea virtuală.
11. Cerințe administrarea avansată a pericolelor		
11.1	Soluția trebuie să ofere integrarea automata cu o soluție de tip Advanced Malware Detection și de import automat pentru indicatorii de compromis (IOC StIX): nume fișiere, hash, URL sau IP.	Solutia ofera integrarea cu o soluție de tip Advanced Malware Detection.
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.	Solutia ofera capabilități de "drill-down" în toate panourile de vizualizare ale interfeței.
11.3	Soluția trebuie să ofere posibilitatea de a lega contextual activitatea aplicației în rețea cu evenimentele de securitate de la dispozitivele monitorizate.	Solutia ofera 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.	Solutia ofera 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.	Solutia ofertata corespunde acestei solicitari.
12. Cerințe fluxul de lucru SIEM		
12.1	Disponă de diferite mecanisme de notificare: alerte la consola, e-mail, SNMP, SMTP;	Solutia ofertata corespunde, + sms, syslog.
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.	Solutia ofertata corespunde acestei solicitari.
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 .	Solutia ofertata corespunde acestei solicitari.
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.	Solutia ofertata corespunde acestei solicitari.
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.	Solutia ofera un mecanism pentru a găsi incidentele de securitate într-o gamă largă de atribute importante.
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 prin syslog, CEF, SNMP v1 & v3, SMTP, WMI, SQL, SDEE, RDEP,	Solutia ofera posibilitatea de colectare și parsare a log-urilor de la diverse surse de date sau din "flat files".

	OPSEC, XML, ODBC sau din “flat files” folosind SCP, FTP sau HTTP de la surse CIFS sau NFS.	
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.	Solutia ofera 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.	Solutia ofera 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.	Solutia ofertata corespunde acestei solicitari.
13.5	Soluția trebuie să ofere posibilitatea construirii și implementării de surse de evenimente specifice „CUSTOM” pe lângă celor suportate nativ.	Solutia ofera posibilitatea construirii și implementării de surse de evenimente specifice „CUSTOM” pe lângă cele suportate nativ.
13.6	Adăugarea surselor de date trebuie să se facă din interfața soluției, fără a fi nevoie de a instala agenți sau pachete software suplimentare.	Solutia permite adăugarea surselor de date din interfața soluției.
13.7	Soluția trebuie să ofere posibilitate de detecție și notificare atunci când o anumită sursă de date nu generează log-uri conform comportamentului învățat.	Solutia ofera posibilitate de detecție și notificare atunci când o anumită sursă de date nu generează log-uri conform comportamentului învățat
13.8	Soluția trebuie să ofere posibilitatea de colectare a datelor de tip flow: Netflow v5, v7, v9, SFlow și J-Flow.	Solutia ofera posibilitatea de colectare a datelor de tip flow: Netflow v5, v7, v9, SFlow și J-Flow.
13.9	Soluția trebuie să suporte produsele de la mai mulți furnizori.	Solutia suporta produsele de la mai mulți furnizori.
13.10	Soluția trebuie să suporte informațiile colectate de la soluții de baze de date de clasă Enterprise.	Solutia suporta informațiile colectate de la soluții de baze de date de clasă Enterprise.
13.11	Soluția trebuie să suporte informațiile colectate de la aplicații comerciale.	Solutia ofertata corespunde acestei solicitari.
13.12	Soluția trebuie să suporte informațiile colectate de la aplicații proprietare.	Solutia ofertata corespunde acestei solicitari.
13.13	Soluția trebuie să suporte informațiile colectate de software-ul de securitate și instrumentele Database Activity Monitoring (DAM).	Solutia suporta informațiile colectate de software-ul de securitate și instrumentele Database Activity Monitoring (DAM).
13.14	Soluția trebuie să suporte informațiile colectate de către software-ul de securitate și instrumentele File Integrity/Activity Monitoring (FIM/FAM).	Solutia suporta informațiile colectate de către software-ul de securitate și instrumentele File Integrity/Activity Monitoring (FIM/FAM).
13.15	Soluția trebuie să suporte informațiile colectate de la software-ul și instrumentele de securitate al Identity & Acces Management (IAM).	Solutia suporta informațiile colectate de la software-ul și instrumentele de securitate al Identity & Acces Management (IAM).
13.16	Soluția trebuie să suporte informațiile colectate de la sistemele de management al rețelei (de exemplu, McAfee ePolicy Orchestrator, Microsoft MOM, etc.).	Solutia dispune de integrare nativa cu McAfee ePolicy Orchestrator.
13.17	Soluția trebuie să suporte informațiile colectate de la infrastructura rețelei (de exemplu, switch-uri, routere, etc.).	Solutia suporta informațiile colectate de la sistemele de management al rețelei.
13.18	Soluția trebuie să suporte scanerile de vulnerabilități de top din industrie.	Solutia suporta informațiile colectate de la infrastructura rețelei.
14. Cerințe implementare		
14.1	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). Solutia ofertata va trebui sa poata fi exstinsa prin achizitia ulterioara a unui modul adaugator de antivirus, DLP, Network Security si altele de la același vendor pentru a exista o integrare nativa si administrare dintr-o singură consolă.	Vor fi asigurate serviciile de instalare a soluției conform cerințelor solicitate si vor fi prezentate toate documentele tehnice aferente soluției. Produsul ofertat oferă posibilitatea de integrare cu alte solutii de DLP, Network security si alte solutii oferite de producatorul McAfee, astfel asigurand o administrare centralizata dintr-o singura consola.
14.2	Furnizorul va trebui sa asigure suport local, conform tipului de suport solicitat.	Va fi asigurat suport local, conform tipului de suport solicitat.

14.3	Furnizorul va oferi minim 1, maximum 3 recomandări de la beneficiari privind implementarea și utilizarea softului dat.	Recomandările de la alți beneficiari a soluției se anexează.
14.4	Furnizorul va oferi Autorizarea de la Producător pentru participarea în cadrul licitației publice.	Autorizarea de la Producător se anexează.
	SIEM funcționează pentru a atinge următoarele obiective de securitate: • Reducerea abuzului de drepturi de acces și a riscurilor de acces neautorizat. • Limitarea partajării parolelor între utilizatori. • Identificarea amenințărilor și posibilelor încălcări; • Colectarea jurnalelor de audit pentru securitate și conformitate; • Efectuarea investigațiilor Sistemul de monitorizare și audit trebuie să asigure următoarele capacități de securitate: • Agregarea datelor: administrarea log-urilor din mai multe surse, inclusiv Active Directory, sisteme de securitate, servere, baze de date, aplicații, oferind posibilitatea de a consolida și monitoriza evenimentele. • Corelarea datelor: căutarea atributelor comune și conexiunea evenimentelor. Această tehnologie oferă posibilitatea de a efectua o varietate de tehnici de corelare pentru a integra diferite surse, pentru a transforma datele în informații utile. • Alertarea: analiza automată a evenimentelor corelate și producerea alertelor, pentru a informa administratorii despre problemele identificate. Evenimentele transmise către SIEM pentru identificarea incidentelor: • încercări de autentificare cu succes și nereușite • adăugarea, ștergerea și modificarea conturilor și a grupurilor • utilizarea privilegiilor • pornirea și oprirea serviciilor • modificări importante ale configurației și a setărilor de securitate • Evenimente de securitate de la routere, firewall, IPS, WEB Proxy, WAF, VPN Gate Sisteme care trebuie integrate în SIEM: • AD (Microsoft Active Directory) • Print Server · File Server • Email Server • WSUS, • SCCM, • NPS, • Switches Cisco • Sisteme de operare: Linux, Microsoft Windows • Web servers · Aplicații • Databases (Baze de date) • Sisteme de securitate: VPN Gate, Tacacs+, Firewall, Sistemul de prevenire a intruziunilor IPS, Firewall pentru aplicații web WAF, Application Control, Antivirus Vendori posibili de SIEM: IBM Qradar, Splunk, McAfee	Siemul oferat v-a permite • Reducerea abuzului de drepturi de acces și a riscurilor de acces neautorizat. • Limitarea partajării parolelor între utilizatori. • Identificarea amenințărilor și posibilelor încălcări; • Colectarea jurnalelor de audit pentru securitate și conformitate; • Efectuarea investigațiilor • Sistemul oferat va permite: • Agregarea datelor: administrarea log-urilor din mai multe surse, inclusiv Active Directory, sisteme de securitate, servere, baze de date, aplicații, oferind posibilitatea de a consolida și monitoriza evenimentele. • Corelarea datelor: căutarea atributelor comune și conexiunea evenimentelor. Această tehnologie oferă posibilitatea de a efectua o varietate de tehnici de corelare pentru a integra diferite surse, pentru a transforma datele în informații utile. • Alertarea: analiza automată a evenimentelor corelate și producerea alertelor, pentru a informa administratorii despre problemele identificate. Evenimentele transmise către SIEM pentru identificarea incidentelor: • încercări de autentificare cu succes și nereușite • adăugarea, ștergerea și modificarea conturilor și a grupurilor • utilizarea privilegiilor • pornirea și oprirea serviciilor • modificări importante ale configurației și a setărilor de securitate • Evenimente de securitate de la routere, firewall, IPS, WEB Proxy, WAF, VPN Gate Sisteme care pot fi integrate în SIEM-ul oferat: • AD (Microsoft Active Directory) • Print Server · File Server • Email Server • WSUS, • SCCM, • NPS, • Switches Cisco • Sisteme de operare: Linux, Microsoft Windows • Web servers · Aplicații • Databases (Baze de date) • Sisteme de securitate: VPN Gate, Tacacs+, Firewall, Sistemul de prevenire a intruziunilor IPS, Firewall pentru aplicații web WAF, Application Control, Antivirus Produsul oferat: McAfee

	• Prezența interfeței de administrare, analizarea informațiilor comune cu alte sisteme EndPoint Protection, SIEM, DLP are o importanță mare pentru sistemul informațional al Serviciului. • Disponibilitatea și poziția produsului în "Gartner Square" reprezintă un avantaj puternic față de alte soluții.	Produsul oferat oferă posibilitatea de integrare cu alte solutii de DLP, EndpointProtection si alte solutii oferite de producatorul McAfee, astfel asigurand o administrare centralizata dintr-o singura consola. Produsul oferat se regăsește in cadranul de Lideri "Gartner" In oferta sunt incluse serviciile de instalare, integrare si configurarea soluției.
--	--	---