Soluție pentru analiza si corelarea evenimentelor din mai multe surse	
Specificații	Solutia trebuie sa fie livrata sub forma de masina virtuala Componentele soluției trebuie sa suporte cel puțin următoarele tipuri de hypervisori: KVM, si OpenStack Numărminim de echipamente fizice sau virtuale monitorizate: 50 Numărminim de evenimente pe secunda: 500
Funcționalități (minime)	•Alertare automată în situația în care (datorită unor defecțiuni, erori umane sau atacuri cibernetice) anumite conexiuni, sisteme sau aplicații devin inaccesibile sau nefuncționale • Colectarea și stocarea log-urilor (aferente dispozitivelor IT și a aplicațiilor software găzduite de acestea), pentru perioade îndelungate de timp: atât online cât şi offline prin arhivare • Corelarea automată întrejurnaleși alertele predefinite sau definite de către administrator • Detectarea anomaliilor comportamentale (detectarea abaterilor de la valorile statistice de referință) și alertarea automată în cazul producerii acestora • Posibilitatea de rulare automată a unor scripturi de remediere (predefinite sau definite de către administrator) în cazul producerii unor incidente de: securitate, disponibilitate, performanță • alertare automată în situația în care este afectată integritatea datelor prin modificări (realizate de către persoane neautorizate sau aplicații malware/ransomware) de fișiere/directoare sau regiştrii Windows • Posibilitatea de a grupa dispozitivele şi aplicațiile ce deservesc un serviciu de business (ex. ERP/CRM/etc.) și alertarea automată (cu evidențierea serviciului) în cazul producerii unui incident de securitate, disponibilitate sau performanță, ce ar avea loc la niveluldispozitivelor/aplicațiilor ce definesc serviciul de business respectiv • Sistem de ticketing integrat dar și posibilitatea de a integra sisteme externe de ticketing prin API • Posibilitatea de investigare cât mai rapidă a unor eventuale tentative de încălcare a securității datelor, atacuri cibernetice performanță/disponibilitate prin analizarea în timp real a log-urilor şi evenimentelor colectate: interfață de management permite listarea în timp real a tuturor jurnalelorși a evenimentelor (pe măsură ce acestea sunt recepționate) cu posibilitatea de a predefini filtre de către adminitratorul sistemului • Colectarea de informații în mod pasiv (fără interogarea dispozitivelor sau a aplicațiilor existente), prin captarea mesajelor/log-urilor: Syslog, NetFlow, sFlow, SNMP Traps (de la echipamente Cisco si HPE deținute de către beneficiar) • Colectarea de informații (de Securitate, Performanță, Disponibilitate și Modificare), în mod activ, fără agenți, prin interogarea dispozitivelor șiaplicațiilor existente utilizând protocoalele standard (ex. SNMP, Telnet, SSH etc.) • Colectarea de informații cu agent dedicat pentru Windows si Linux (cel puțin Ubuntu, Debian și Centos) pentru colectarea jurnalelor de sistem, a aplicațiilor si jurnalele de securitateprecum și monitorizarea

	integrităţiifişierelor • Corelarea evenimentelor de securitate în vederea oferirii unei imagini "comprehensive" a ameninţării cibernetice • Monitorizarea stării şi nivelului de răspuns al serviciilor DNS, FTP/SCP, Generic TCP/UDP, ICMP, JDBC, LDAP,SMTP, IMAP4, POP3, POP3S, SMTP, SSH şi Web (HTTP, HTTPS). Rezultatul acestei monitorizări poate fi utilizat în calcularea nivelelor de disponibilitate aferente serviciilor respective • Stocarea locală sau utilizând un protocol de tip NFS a jurnalelor. • Stocarea jurnalelor în formată brută şi normalizată/pasată • Stocarea template-urilor, incidentelor şi a altor date structurate utilizând baze de date relaţionale • Posibilitatea de a respinge mesaje/log-uri nerelevante la nivelul instanţei locale de colectare • Instanţele locale de colectare transmit către instanţa centrală atât log-urile în format brut cât şi informaţiile de parsare • Monitorizarea dispozitivelor fără utilizarea de agenţi, prin: SSH, telnet, WMI, JMX, Power Shell • Posibilitatea de a colecta evenimentele platformelor Linux, prin intermediul unor agenţi Linux care să asigure: Managementul centralizat al agenţilor Linux Posibilitatea de a colecta log-uri din fişiere de tip text Monitorizarea integrităţiifişierelor Definirea de rapoarte complexe care cumulează/conţin la rândul lor mai multe rapoarte distincte/individuale Rapoarte predefinite încadrate/grupate pe categorii şi tipuri de funcţionalităţi (ex. rapoarte de Performanţă, Disponibilitate, Securitate, Modificare, Conformitate) cu posibilitatea de a căuta şi identifica un anumit raport utilizând cuvinte cheie ce se regăsesc în numele sau descrierea aferentă raportului respectiv Generarea de rapoarte ad-hoc (manual) sau programatic (în mod automat, fără intervenţia operatorului uman) • Posibilitatea de a exporta un raport în format PDF sau CSV • Posibilitatea de a transmite un raport prin email în mod manual sau automat (programat pentru anumite momente de timp prestabilite: de ex. zilnic, săptămânal, lunar) • Posibilitatea de a corela, la nivelul unei reguli de alertare, a următoarelor tipuri de evenimente: Securitate: IPS, Antivirus, erori de autentificare, exploatări, vulnerabilităţi, etc. Performanţă: nivel încărcare CPU, RAM, spaţiu de stocare, conexiuni/throughput Disponibilitate: restartarea sau întreruperea unor aplicaţii/servicii/echipamente) Modificare: modificarea unor fişiere, modificarea configuraţiilor echipamente, adăugarea/ştergerea unor utilizatori, etc. Reguli (predefinite) de alertare ce conţin criteriile şi valorile utilizate în definirea alertei/incidentului respectiv: nivel de severitate (ex. mic, mediu, mare), categorie incident (ex. de securitate, performanţă, modificare,

	disponibilitate) • Posibilitatea de a crea noi reguli de alertare dar şi de donare şi modificare a regulilor predefinite • Posibilitatea de a defini politici de notificare pentru: Trimiterea automată de Email/SMS Trimiterea automată de mesaje SNMP Trimiterea automată a unui fişier XML peste HTTP(S) Vizualizarea şi filtrarea incidentelor în funcţie de atributele evenimentului, mic/mediu/mare), categorie (securitate, performanţă sau disponibilitate) sau interval orar Crearea, testarea şi activarea parsoarelor direct din interfaţa grafică • Posibilitatea de a importa/exporta raporturi, reguli de alertare sau dashboard-uri în format XML • Posibilitatea de a colecta configurațiile echipamentelor de rețea (routere, switch-uri, firewall-uri) şi de a compara configurații distincte, pentru a putea vizualiza modificările realizate • Posibilitatea de a defini politici de notificare în cazul producerii unor incidente • Apelarea automată sau manuală a unui script de remediere (customizabil sau predefinit) • Sistem de ticketing integrat (built-in) • Căutare/filtrare evenimente în timp real pe bază de cuvinte cheie sau atribute (predefinite sau definite de către administrator) • Căutare/filtrare evenimente istorice pe bază de cuvinte cheie sau atribute • Căutarea/filtrarea evenimentelor în timp real sau istoric se realizează utilizând: atribute (predefinite sau definite de operatorul sistemului), operatori logici (egal, diferit, mai mare, mai mare sau egal, mai mic, mai mic sau egal, inclus în, nu este inclus în, conține, nu conține, REGEXP, NOT REGEXP) şi valori ce sunt mapate (prin intermediul acestor operatori logici) cu atributele respective • Implementarea de politici de arhivare a datelor cu posibilitatea de stocarea a acestora • Posibilitatea de a verifica integritatea datelor stocate prin aplicarea de algoritmi de tip hash atât la momentul salvării datelor cât şi ulterior în momentul accesării/încărcării acestora •Posibilitatea de a adăuga noi instanţe de colectare, fără întreruperea funcţionalităţii sistemului central • Nu sunt impuse limitări legate de volumul de date/log-uri stocate •Atribute predefinite (ex. IP/MAC sursă/destinaţie, sursa raportării,utilizator, staţie, tipul evenimentului, etc.) dar şi posibilitatea de a definii noi atribute în funcţie de nevoile operaţionale • Posibilitatea de parsare, listare şi filtrare a log-urilor în timp real (pe măsură ce acestea sunt recepţionate). Filtrarea log-urilor trebuie să poată fi realizată în funcţie de atributele şi valorile asignate acestora. • Posibilitatea de listare şi filtrare a logurilor pentru anumite intervale specifice de timp. •O interfaţă unică de management ce permite managementul tuturor instanţelor aferente soluţiei: instanţe de colectare log-uri/evenimente,

	monitorizare performanţe, corelare, analiză şi raportare evenimente • Interfaţă de management de tip Web/GUI HTML5 • Acces pe bază de drepturi/roluri (vizualizare, modificare) aferente diferitelor secţiuni prezentate la nivelul interfeţei web •Posibilitatea de a încărca fişiere CSV (ce conţin listele de Threat Intelligence) direct din interfaţa grafică de management • Suport pentru: adrese IP, Domenii, Hash-uri şi URL-uri • Surse de Threat Intellligence de tip Comercial şi Open Source furnizate în mod implicit (out of the box), cu posibilitatea de automatizare / programare a procesului de updatare a listelor (adrese IP, Domenii, Hash-uri şi URLuri) furnizate de aceste surse • Posibilitatea de a corela în timp real, informaţiile de Threat Intelligence cu log-urile/evenimentele captate, urmată de alertarea/notificare automată în cazul detectării unor incidente de securitate • Posibilitatea de a corela informațiile de Threat Intelligence cu datele/evenimentele istorice (stocate la nivelul bazei de date) • soluția va dispune de agent avansat cu capabilități de Machine Learning pentru a detecta comportamentul neobișnuit al utilizatorului și al entității (UEBA) fara a cere administratorului sa scrie reguli complexe. Agentul va ajuta la identificarea amenințărilor din interior și celor ce ar putea trece de solutiile de Securitate traditionale. Agentul va ajuta la generarea de alertele pentru prioritizarea amenintarilor care necesită atenție imediata. • Agentul avansat va permite permite colectarea datelor de telemetrie si activitatea utilizatorului, procese, dispozitive, resurse și comportament.
Licentiere si Suport	• Licenta perpetua pentru minim 50 echipamente fizice, virtuale, sau agenți Windows si Linux cu suport UEBA si minim 500 evenimente pe secunda (EPS) • Soluția va beneficia de minimum 1 an de suport ce va acoperi minim 50 echipamente fizice, virtuale, sau agenți Windows si Linux cu suport UEBA si 500 evenimente pe secunda (EPS) si va include: - Suport tehnic din partea furnizorului 7 zile pe săptămâna, 24 de ore pe zi - Update firmware versiuni minore si majore
Altele	Furnizorul va instala software pe o mașina virtuala, îl va activa si îl va configura pentru monitorizarea a minim trei switch-uri si minim trei servere. Furnizorul va oferi suport pentru instalarea, integrarea si configurarea soluției ofertate cu platforma openstack a beneficiarului respectiv sistemele linux de management și autentificare a platformei.

Grecanu - Serban Valentin