ROMÂNIA
MINISTERUL APĂRĂRII NAȚIONALE
COMANDAMENTUL APĂRĂRII CIBERNETICE
Nr. BA-315 din 13.02.2026
București

Digitally signed by Madalina Dinulescu
Date: 2026.02.20 13:37:40 EET

NECLASIFICAT
Exemplarul unic
Dosar nr. ___
Termen de păstrare: 5 ani

Specificație tehnică
pentru
„Soluție pentru managementul evenimentelor de securitate dintr-o rețea de calculatoare”

BUCUREȘTI
2026

CUPRINS

1. SCOP

Prezenta specificație stabilește cerințele tehnice pentru achiziționarea unui sistem de managament al informațiilor și evenimentelor de securitate destinat colectării. monitorizării. normalizării, stocării, analizării în timp real a **evenimentelor** de securitate și managementului centralizat al informațiilor și evenimentelor de securitate generate de către echipamentele hardware și aplicațiile software din cadrul infrastructurii de rețea publică pentru a identifica. prioritiza. analiza și gestiona rapid alertele, incidentele de securitate și scorurile de risc, prin intermediul unor dashboard-uri flexibile cu moduri de vizualizare personalizabile.

Platforma dedicată managementului informațiilor și evenimentelor de securitate trebuie să conducă la:

- Îmbunătățirea posturii de securitate a rețelei publice;
- Obținerea vizibilității complete, end-to-end, asupra tuturor datelor relevante din infrastructura rețelei publice;
- Creșterea capacității de prevenție și detecție a amenințărilor cibernetice folosind securitatea bazată pe analiză precum și suport decizional crescut folosind informații de tip Threat Intelligence;
- Optimizarea operațiunilor de securitate prin realizarea de economii substanțiale în ceea ce privește efortul și timpul necesar derulării investigațiilor și rezolvării incidentelor de securitate.

2. CERINȚE

Ofertantul va furniza o soluție ce va oferi managementul evenimentelor de securitate dintr-o rețea de calculatoare.

CERINȚE PRIVIND CONFIGURAȚIA PRODUSULUI OFERTAT

Nr. cerință	CERINȚA
C1.	Sistemul trebuie să aibă compunerea din tabelul următor:

Nr. crt.	Tip componentă	Cantitate
1	Software pentru colectarea, monitorizarea, normalizarea, analiza în timp real şi managementul centralizat al informațiilor și evenimentelor de securitate generate de echipamentele din rețea	1 lic.
2	Agenți de colectare – module software adiționale, parte a componentei software propusă, pentru același scop și perfect integrabile cu software-ul, necesare în procesul de colectare, normalizare și gestionare a informațiilor și evenimentelor de securitate generate de echipamentele din rețea	
3	Consolă de configurare, administrare și monitorizare a componentelor sistemului de management al logurilor	

2.1 Cerințe de performanță și specifice produsului

Nr. cerință	CERINȚA
C2.	Platforma SIEM trebuie să poată fi instalată și configurată pe infrastructuri On-premise și să permită corelarea vizuală a evenimentelor, investigații detaliate ale atacurilor de tip multi-stage precum și răspuns adecvat și rapid la incidentele de securitate.
C3.	Toate log-urile și alertele din stiva tehnologiilor de securitate disponibile existente vor fi colectate, agregate, corelate și utilizate în cadrul acestei soluții pentru înțelegerea, prevenirea și detecția amenințărilor cibernetice, precum și pentru luarea unor măsuri rapide și coordonate, manuale sau automate.
C4.	Platformă universală, extensibilă ce permite colectarea datelor end-to-end, cu capabilități integrate de analiză și management.
C5.	Soluția propusă nu trebuie să introducă limitări în ceea ce privește numărul de surse de loguri și numărul de loguri colectate pe secundă (LPS/EPS).
C6.	Soluția propusă trebuie să funcționeze într-o configurație de înaltă disponibilitate care elimină un Punct Unic de Eșec (SPF).
C7.	Soluția propusă nu trebuie să blocheze sau să refuze colectarea de date atunci când se atinge limita zilnică de volum de date (conform licenței deținute în prezent).
C8.	În cazul unor probleme de performanță cu orice componentă a soluției propuse, trebuie să existe opțiunea de extindere a acesteia (de exemplu, adăugarea unui nod suplimentar de procesare) fără a fi necesară achiziționarea de module sau licențe suplimentare.
C9.	Soluția propusă trebuie să permită reținerea datelor pentru cel puțin 12 luni și analiza eficientă a datelor de cel puțin 1 TB.
C10.	Soluția propusă trebuie să suporte mecanismul de migrare planificată a datelor către o memorie de masă de nivel inferior, pe baza unui timp sau perioadă definită.
C11.	Soluția propusă trebuie să permită integrarea datelor din diverse surse. Toate datele trebuie să fie disponibile ca informații consistente în interfața sistemului analitic.
C12.	Soluția propusă trebuie să ofere Controlul Accesului Bazat pe Roluri, utilizând granularitatea nivelului dataset-urilor identificate.
C13.	Soluția propusă trebuie să permită conectarea unui mediu de stocare CIFS/NFS suplimentară pentru stocarea datelor arhivate. Datele arhivate trebuie să fie disponibile în sistem în același mod ca și datele disponibile online.
C14.	Mecanismul responsabil pentru stocarea logurilor, datelor și evenimentelor soluției propuse nu trebuie să permită ștergerea neautorizată a unei părți sau a întregii loguri, date, rapoarte și alte informații, iar soluția trebuie să permită accesarea acestor date doar de către utilizatori autorizați și autentificați.
C15.	Soluția propusă trebuie să ofere scalabilitate și posibilitatea de extindere a arhitecturii în cazul unor cerințe de performanță mai ridicate care apar din cauza redirecționării, colectării și detaliilor sporite ale evenimentelor înregistrate (loguri și date).

C16.	Extinderea soluției, în ceea ce privește volumul mai mare de date analizat zilnic, nu trebuie să necesite achiziționarea unei licențe suplimentare, cu excepția celei care definește limita zilnică maximă de date colectate din sursele de date.
C17.	Soluția propusă trebuie să suporte arhitectura care permite distribuirea funcțiilor pe servere dedicate care îndeplinesc: a. Colectarea și extragerea datelor, b. Stocarea, căutarea și gestionarea logurilor colectate (și a datelor), c. Stratul analitic și interfața utilizatorului.
C18.	Tabelele și graficele prezentate pe baza logurilor și datelor trebuie să permită analiza în detaliu, ceea ce înseamnă că după ce se face clic pe un câmp specific din tabel sau grafice, interfața utilizatorului trebuie să prezinte logurile și datele corespunzătoare.
C19.	Soluția propusă trebuie să suporte geolocalizarea evenimentelor pe baza adreselor IP. Datele de geolocalizare pentru evenimente trebuie prezentate pe hartă și trebuie să permită utilizarea acestora pentru căutări și utilizarea în regulile de corelare.
C20.	Soluția propusă trebuie să suporte analiza logurilor standard de infrastructură IT generate de sistemele de operare, firewall-uri, dispozitive de rețea (switch-uri, routere, load-balancers etc.), soluții de securitate precum IPS/IDS, anti-bots, filtrarea web, Web Application Firewalls (WAFs), IDM, DAM etc.
C21.	Soluția propusă trebuie să suporte proiectarea și implementarea redirecționării, parsării, corelării și stocării logurilor și altor date relevante din diferite surse de loguri, cel puțin: i. Soluții de securitate: Check Point, Palo Alto, Juniper SSG, Intel Security McAfee ePI, Trend Micro Deep Security, Pulse Connect Secure, Fidelis, Fudo Security ii. Web Application Firewalls: F5 Networks, Imperva, Fortinet iii. Dispozitive Cisco: switch-uri, routere, firewall-uri iv. Sisteme de operare: Red Hat, Microsoft Windows v. Servicii de producție: DNS, DHCP, WWW (Apache, IIS) vi. Baze de date: Oracle, SQL Server, MySQL, Postgres vii. Sisteme de virtualizare: VMware vSphere, Red Hat Virtualization viii. Loguri de evenimente Windows: Aplicație, Securitate, Sistem și altele ix. Loguri de trafic de rețea via Netflow x. Activități de autentificare din sistemele de control al accesului

C22.	Soluția propusă trebuie să suporte colectarea logurilor și datelor care sunt salvate în fișiere (jurnale de sistem și aplicații) și de asemenea notificările capturate pe porturile TCP/UDP și utilizarea mecanismului descris mai jos: i. Trimiterea logurilor și datelor din sistemul de origine (sau software-ul) la un port TCP/UDP specificat pe serverul care face parte din soluția propusă (de exemplu, syslog). ii. Trebuie să suporte colectarea și analizarea datelor în format CEF și acceptarea logurilor de la Syslog Relay. iii. Selectarea, în interfața utilizatorului, a fișierului local sau a directorului local. iv. Executarea interogărilor SQL în baze de date externe și colectarea rezultatelor răspunsurilor. Alternativ, trebuie să existe posibilitatea de a comunica cu aceste baze de date utilizând standardele JDBC sau ODBC. v. Windows Management Infrastructure (WMI) vi. Check Point OPSEC LEA
C23.	Soluția propusă trebuie să permită activități eficiente ale utilizatorilor, care includ căutarea și vizualizarea evenimentelor, generarea de rapoarte. Soluția propusă trebuie să funcționeze eficient în timp ce desfășoară activități de fundal. Soluția propusă trebuie să fie scalabilă până la 200 GB și 20 TB pe termen scurt și lung, respectiv.
C24.	Soluția propusă trebuie să permită analizarea jurnalelor având o lungime de cel puțin 10.000 de caractere și conținând mai mult de o linie.
C25.	Soluția propusă trebuie să permită crearea unei baze de date cu definițiile formatelor jurnalelor.
C26.	Procesul responsabil pentru analizarea jurnalelor trebuie să analizeze fiecare jurnal sau date și să caute informații importante despre evenimentul înregistrat, care sunt: data și ora evenimentului, numele utilizatorului, numele gazdei sistemului de origine, numele și adresa IP a sistemului de origine, tipul evenimentului (de exemplu, autentificare, deconectare, blocarea contului de utilizator, permiterea/blocarea traficului de rețea, detectarea codului malițios etc.).
C27.	Soluția propusă trebuie să caute timpul și data evenimentului (timestamp) și să le folosească în cadrul regulilor de corelare.
C28.	Soluția propusă trebuie să permită căutarea evenimentelor în jurnale și date folosind valori de câmp specifice, folosind expresii regulate (REGEX) sau folosind șabloane predefinite, de exemplu, adresa IP sursă/destinație, port, protocol.
C29.	Soluția propusă trebuie să suporte căutarea și vizualizarea (într-o singură consolă) a jurnalelor colectate/extrase/descărcate în sistem, evitând conectarea independentă la fiecare sursă pentru a verifica statusul conexiunii (permis, blocat). Căutarea și filtrarea evenimentelor în timp real trebuie să permită căutarea folosind expresii regulate (REGEX) sau șabloane predefinite, de exemplu, adresa IP sursă/destinație, port și protocol.
C30.	Soluția propusă trebuie să permită crearea de alerte și notificări care sunt declanșate de corelarea datelor procesate prin regula de corelare.

C31.	Soluția propusă trebuie să suporte construirea de reguli de corelare bazate pe datele și jurnalele analizate din diverse surse diferite, să proceseze și să coreleze datele în timp real.
C32.	Configurarea și gestionarea regulilor de corelare trebuie să se facă prin intermediul interfeței web a sistemului, fără a fi nevoie de utilizarea unor instrumente externe, suplimentare, de la terți.
C33.	Soluția propusă trebuie să suporte detectarea situațiilor nonstandard care se abat de la comportamentul înregistrat în șablonul de comportament (de exemplu, pentru detectarea atacurilor de tip DoS, modele de trafic nou descoperite care nu au avut loc anterior, activități ale unui utilizator nou, etc.).
C34.	Soluția propusă trebuie să faciliteze configurarea ușoară a regulilor pentru analizarea jurnalelor și datelor, construirea de tablouri de bord și rapoarte, adăugarea de noi surse de jurnale. Toate aceste activități trebuie să poată fi efectuate ușor de către angajații companiei, după un training post-instalare.
C35.	Soluția propusă trebuie să permită construirea de rapoarte personalizate, atât în format text, cât și grafic. Rapoartele trebuie să fie trimise periodic prin e-mail ca atașament PDF.

C36.	Soluția propusă trebuie să permită menținerea diferitelor roluri de utilizatori în domenii definite: i. Analiza evenimentelor în domeniul cibernetic. ii. Monitorizarea performanței și detectarea și analiza eșecurilor pentru sistemele și dispozitivele IT. iii. Monitorizarea și analiza aplicațiilor interne dezvoltate de sau pentru clientul final. u. Soluția propusă trebuie să suporte vizualizări și tablouri de bord predefinite dedicate anumitor domenii de securitate cibernetică, de exemplu: i. Detectarea și răspunsul la programele malware ii. Detectarea și remedierea vulnerabilităților software/platformei iii. Analiza traficului de rețea iv. Analiza și urmărirea porturilor și protocoalelor de rețea utilizate în interiorul rețelei v. Analiza și urmărirea actualizărilor/upgrade-urilor software în cadrul organizației vi. Analiza și urmărirea regulilor și politicilor de control al accesului. v. Soluția propusă trebuie să suporte contabilitatea activităților utilizatorilor, în special înregistrarea accesului la datele și jurnalele procesate. w. Soluția propusă trebuie să permită activități concurente pentru cel puțin 10 utilizatori în același timp. x. Licența trebuie să permită crearea a 50 de conturi de utilizatori diferiți în cadrul sistemului propus și operația concurentă a 50 de utilizatori. y. Soluția propusă trebuie să suporte separarea mediilor pentru utilizatorii cu roluri diferite. z. Soluția propusă trebuie să fie rezistentă la atacuri de rețea. Pentru a susține acest lucru, există câțiva pași obligatorii de implementare, cum ar fi securizarea și întărirea sistemului de operare, dezinstalarea software-ului neutilizat/inutil, dezactivarea serviciilor neutilizate, activarea filtrării traficului IP, dezactivarea conturilor neutilizate.
C37.	Soluția propusă trebuie să suporte cel puțin 100 de reguli de corelare predefinite și integrate de către furnizor, care operează pe datele generate de sursele de jurnale și modulele adăugate configurate în timpul implementării.

C38.	Soluția propusă trebuie să suporte universalitatea, adică, în afară de caracteristicile legate exclusiv de securitatea cibernetică, trebuie să permită utilizarea aceleiași soluții în domeniul analizei și informațiilor de afaceri, monitorizarea infrastructurii de rețea și monitorizarea și gestionarea jurnalelor de aplicație și sistem. Soluția propusă trebuie să permită crearea de caracteristici și funcționalități personalizate, nu definite de furnizor, legate de analiza datelor, care acoperă: a) Mecanisme de colectare a datelor b) Rapoarte, tablouri de bord și formulare c) Caracteristici analitice noi d) Caracteristici noi de vizualizare e) Mecanisme de notificare (inclusiv bidirecțional, neimplementate de furnizor). Implementarea acestor caracteristici nu trebuie să necesite implicarea furnizorului și nu poate intra în conflict cu drepturile de autor. Componentele soluției, inclusiv analiza afacerilor, raportarea, monitorizarea infrastructurii, gestionarea și monitorizarea jurnalelor de sistem/aplicație, nu trebuie să provină de la același furnizor, dar nu pot fi o soluție open-source.
C39.	Setul de funcționalități analitice, în cadrul soluției propuse, trebuie să includă cel puțin: a. Funcții statistice, de exemplu: sumă, medie, mediană, deviație standard, cel mai vechi și cel mai nou pentru cheia configurată (de exemplu: volumul mediu de date pe oră pentru o adresă IP sursă definită). b. Funcții care permit detectarea anomalii numerice. Soluția propusă trebuie să permită detectarea anomaliilor pentru orice parametru din jurnal, nu doar parametrii de trafic de rețea. c. Soluția propusă trebuie să detecteze aparițiile foarte rare ale valorilor și evenimentelor într-un subset definit. d. Crearea de corelații pe baza evenimentelor care conțin aceleași valori pentru câmpuri definite. Soluția propusă trebuie să permită detectarea modificării valorii unui câmp definit și să emită o alarmă despre această schimbare (de exemplu: creșterea încercărilor eșuate de autentificare cu 50%).
C40.	Soluția propusă trebuie să suporte schema la citire, ceea ce înseamnă că sistemul trebuie să permită schimbarea metodei de normalizare a datelor în timpul utilizării sistemului (de exemplu: adăugarea de câmpuri noi, schimbarea numelui sau semnificației câmpurilor existente etc.) fără a fi nevoie să se refacă întreaga bază de date. SIEM-ul trebuie să permită utilizarea paralelă a diferitelor metode de normalizare a jurnalelor. Soluția propusă trebuie să suporte îmbogățirea datelor utilizând informații situate în resurse și depozite externe, cel puțin: a. Directoare LDAP b. Baze de date SQL c. Baze de date noSQL d. Hadoop e. Date de geolocație
C41.	Din cauza minimizării epuizării stocării, datele de îmbogățire nu pot fi stocate împreună cu jurnalele și îmbogățirea trebuie să aibă loc în timp real (în timpul extragerii datelor) din surse externe.

C42.	Pentru stratul analitic, soluția propusă trebuie să suporte configurarea unui cluster cu înaltă disponibilitate și balansare a sarcinii (modul cluster activ/activ). Trebuie să existe posibilitatea de a configura orice număr de noduri ale clusterului. Balansarea sarcinii între noduri nu trebuie să necesite implementarea unei soluții ADC (Application Delivery Controller) terțe/externe.
C43.	Soluția propusă nu trebuie să fie un software open-source.
C44.	Funcționalitățile soluției propuse trebuie să fie acoperite în documentația tehnică oficială care va fi furnizată după implementare.
C45.	Soluția propusă trebuie să fie clasată în cvadrantul liderilor în cel mai recent Gartner Magic Quadrant pentru Managementul Informațiilor și Evenimentelor de Securitate (SIEM).
C46.	Platforma trebuie să fie utilizată și pentru următoarele cazuri, în afară de cele menționate mai sus: ▪ Operațiuni IT ▪ Management-ul aplicațiilor ▪ Infrastructuri critice ▪ Internet of Things
C47.	Platforma trebuie să se constitue ca un singur produs integrat pentru cazurile de utilizare de tip logging și SIEM. Nu se acceptă ofertarea unor produse cu componente datastore separate pentru logging, SIEM, interfața utilizator. Platforma trebuie să pună la dispoziție conectarea, simultan, la cel puțin trei console web pentru realizarea tuturor funcționalităților platformei incluzând pe cele referitoare la căutări, raportări, construirea regulilor și administrarea sistemului. Trebuie să folosească un datastore pentru ingerarea și indexarea tuturor datelor.
C48.	Arhitectură platformei să fie de tip real-time și să permită: ▪ colectarea in timp real a datelor structurate și nestructurate din orice sursa fără definirea în prealabil a unei scheme la nivelul datastore-ului ▪ interogarea datelor de tip live (real-time) sau istorice într-un mod interactiv și obținerea rapida a rezultatelor
C49.	Să ofere posibilitatea de a menține timestamps-urile originale pentru fiecare eveniment și de a gestiona timestamp-urile din diferite zone orare.
C50.	Să permită compresie automată a datelor indexate pentru a reduce cerințele de stocare.
C51.	Setările de păstrare a datelor ar trebui să fie flexibile după cum urmează: ▪ Permite păstrarea datelor ingerate pe timpul dorit: zile, luni sau ani ▪ Oferă control granular asupra a ceea ce se întâmplă cu datele pe măsura trecerii timpului. Datele mai vechi pot fi distribuite în spații de stocare externe/mai ieftine și/sau șterse
C52.	Să ofere scalabilitate în medii distribuite, folosind commodity hardware fără să limiteze tehnic ingestia volumelor mari de date.
C53.	Posibilitatea replicării indexului pentru a menține mai multe copii identice ale datelor indexate pentru disponibilitatea datelor, fidelitatea datelor, toleranța la dezastre și obținerea unor performanțe îmbunătățite a căutării datelor.

C54.	Platforma să poată fi instalată pe sisteme de operare de tip Linux și Windows.
C55.	Platforma trebuie sa poată fi accesată prin intermediul unui web browser.
C56.	Să ofere capacitatea de a se adapta modificărilor în formatarea evenimentelor sursă, fără a fi nevoie de o actualizare a produsului sau de dezvoltarea un analizor/parser pentru a susține modificările.
C57.	Platforma trebuie să accepte colectarea datelor din orice surse, orice aplicație, sistem de operare, dispozitiv sau sistem, fie virtuale / fizice sau din cloud. Soluția nu trebuie să se bazeze pe conectori personalizați de furnizorii sistemelor pentru a ingera date din diferite surse.
C58.	Posibilitatea de a primi date printr-o gamă largă de mecanisme bazate pe agenți și fără agenți, inclusiv: ▪ Agent livrat de furnizor. Agentul are capacitatea de a cripta comunicațiile către componenta de indexare a datelor, de a stoca datele în memoria cache, de a balansa cererile și de a trimite date prin TCP ▪ Syslog ▪ TCP sau UDP ▪ Evenimente SNMP ▪ XML ▪ CSV ▪ JSON ▪ Input customizat
C59.	Să poată prelua date în formă brută, să le indexeze și să le utilizeze pentru a efectua căutări pe orice baze de date sau fișiere de tip CSV.
C60.	Să ofere capacitatea de a face căutări în text complet pe orice câmp din datele indexate pe baza: ▪ cuvintelor cheie, intervalelor de timp, logicii booleene, expresiilor regulate, sintaxei tip wildcard ▪ analizei statistice, incluzând: număr de apariții, număr distinct de apariții, sumarizare, cele mai comune valori sau cele mai puțin comune valori ale unui câmp, minim, maxim, medie aritmetică, mediană, abatere standard, variație, identificarea valorilor anomale cu rezultate care pot fi neregulate sau neobișnuite, corelația statistică între câmpuri, gruparea evenimentelor pe baza asemănării lor, prima și ultima valoare observată, predicție (căutare care observă datele istorice pentru a prezice matematic valorile viitoare), reuniune, diferență sau intersecția rezultatelor căutării individuale sau multiple
C61.	Posibilitatea de a realiza profilări și de a aplica logici de căutare ca cele de mai sus pentru a detecta anomalii ce pot conduce la descoperirea amenințărilor avansate ce nu sunt detectate folosind tehnici bazate pe semnătură.
C62.	Să permită utilizatorului să facă operațiuni de data mining bazate pe informații de tip cine, ce, când și unde.
C63.	Căutările sa poată fi salvate și modificate ulterior.
C64.	Căutările să poată fi desfășurate în timp real sau programate și să poată fi rulate în mod concurent.

C65.	Regulile de corelare, căutările și vizualizările trebuie să acopere mai multe categorii și tehnologii de securitate, inclusiv, dar fără a se limita la: autentificări, utilizarea conturilor implicite, malware, modificări ale endpoint-urilor, niveluri de patch-uri, firewall-uri, IDS, scanări de vulnerabilități, proxy web, activitate bazată pe HTTP anormală și modificări de port / protocol.
C66.	Monitorizare continuă: vizualizare clară a posturii de securitate cu tablouri de bord, indicatori cheie de securitate, praguri statice și dinamice și evoluții în timp.
C67.	Vizualizare nativă cel puțin în formatele: ▪ Tables ▪ Time charts ▪ Line charts ▪ Bar charts ▪ Area charts ▪ Pie charts ▪ Scatterplot charts ▪ Radial, filler, and marker gauges ▪ Maps
C68.	Vizualizările trebuie sa ofere actualizare în timp real a datelor.
C69.	Platforma să ofere management centralizat pentru toate componentele sale.
C70.	Căutările bazate pe corelări să poată fi ajustate pentru a reflecta diferite cazuri de utilizare din domeniul securității cibernetice.
C71.	Să ofere posibilitatea de a adăuga reguli de corelare personalizate și complexe aplicabile pe orice tip de sursă de date.
C72.	Să ofere posibilitatea de a converti tablourile de bord (dashboards) în fișiere PDF.
C73.	Să ofere REST APIs pentru a expune toate datele indexate, comenzile de căutare și funcționalitatea către aplicații și sisteme externe.

2.2 Cerințe licențiere

Nr. cerință	CERINȚA
C74.	Licențele trebuie să fie de tip subscripție, pentru o perioadă de cel puțin 3 ani (36 luni);
C75.	Ofertantul trebuie să livreze și alte licențe necesare pentru modulele și pachetele software adiționale, dacă este cazul, integrate sau nu, necesare pentru funcționarea soluției în acord cu cerințele din acest document.
C76.	Licența asociată soluției propuse nu trebuie să limiteze numărul de noduri (elemente) responsabile pentru colectarea și analizarea logurilor și datelor.
C77.	Licența asociată soluției propuse trebuie să permită orice fel de implementare în producție, în special implementarea diferitelor componente funcționale descrise în cerința C17. Extinderea platformei SIEM cu noduri suplimentare de procesare, colectare și analiză nu trebuie să necesite costuri suplimentare de licențiere. Licența nu poate limita numărul de dispozitive conectate.

C78.	Produsul ofertat trebuie să includă licența necesară pentru colectarea, monitorizarea și analiza a cel puțin 100 GB/zi de date.

2.3 Cerințe privind garanția produsului

Nr. cerință	CERINȚA
C79.	Garanția generală trebuie să fie de minim 36 de luni pentru produsul ofertat.

2.4 Cerințe privind instruirea

Nr. cerință	CERINȚA
C80.	Ofertantul trebuie să asigure, fără alte costuri suplimentare pentru beneficiar, instruirea a minim 10 reprezentanți ai beneficiarului, pe o durată de minim 40 de ore (5 zile lucrătoare a 8 ore pe zi), pentru buna înțelegere a funcționării componentelor produsului;
C81.	Instruirea trebuie să se facă în limba română/engleză;
C82.	Instruirea se va executa în termen de 45 de zile de la semnarea contractului subsecvent de ambele părți și trebuie să permită personalului beneficiarului să opereze si să administreze soluția livrata. Aceasta poate include, însă fără a se limita la: înțelegerea diferitelor componente ale soluției; înțelegerea tuturor funcționalităților; operarea soluției; administrarea soluției; informații despre mentenanța de rutină care trebuie să fie efectuată de către administratori; depistarea problemelor și diagnosticare de baza etc.
C83.	Contractantul trebuie să propună orice subiect suplimentar care ar putea fi necesar pentru a se asigura că personalul beneficiarului este pe deplin instruit pentru a asigura utilizarea corespunzătoare a soluției.
C84.	După instruire, ofertantul trebuie să livreze manualele de utilizare și configurare ale componentelor produsului în format electronic;
C85.	Instruirea personalului trebuie să se facă în București, într-o locație pusă la dispoziție de ofertant, cu acordul beneficiarului, care să ofere toate facilitățile necesare instruirii profesionale a personalului pentru administrarea și utilizarea produsului;
C86.	Instruirea trebuie să exemplifice modul practic prin care se verifică toate funcționalitățile solicitate prin caietul de sarcini;
C87.	Instruirea trebuie să fie de tip „*hands-on*" (presupune implicarea participanților în mod direct în activități practice, crearea și testarea de exemple bazate pe noțiunile teoretice prezentate și accesul la resursele materiale corespunzătoare în timpul desfășurării cursului), cu activități practice în care cursanții utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind integrarea software, configurarea, administrarea și exploatarea produsului;
C88.	La finalizarea cursului ținut de ofertant, se va încheia un proces verbal de acceptanță a instruirii, între ofertant și participanți, necesar pentru finalizarea recepției produsului;

2.5 Cerinţe privind recepţia produsului

Nr. cerinţă	CERINŢA
C89.	Recepţia produsului se va desfăşura în acord cu prevederilor contractuale şi va conţine o recepţie calitativă şi o recepţie cantitativă.
C90.	Recepţia cantitativă şi calitativă se va realiza la sediul beneficiarului, de către comisia de recepţie a acestuia.
C91.	Recepţia cantitativă şi calitativă se va realiza în termen de 10 zile de la data finalizării livrării produselor şi a activităţii de instruire a personalului descrisă la punctul 2.4 din prezenta specificaţie tehnică.
C92.	În cadrul activităţii de recepţie se vor parcurge următoarele etape: a) verificarea livrării cantitative a produsului; b) verificarea livrării documentelor prevăzute la pct. 4 din Caietul de sarcini; c) verificarea funcţionării produsului în acord cu prevederile cerinţelor tehnice prevăzute în anexa nr. 1 la caietul de sarcini, de către o comisie de recepţie formată din angajaţi ai beneficiarului; d) verificarea executării activităţii de instruire descrisă la punctul 2.4 din prezenta specificaţie tehnică.
C93.	La finalul activităţii de recepţie se va întocmi un proces verbal de recepţie cantitativă şi calitativă a activului fix, prin care se va finaliza activitatea de recepţie.
C94.	Dacă în cadrul recepţiei se constată că unele produse nu corespund cantitativ şi calitativ, beneficiarul are dreptul de a respinge produsele, iar Furnizorul are obligaţia să remedieze neconformităţile constatate în decurs de 5 (cinci) zile de la constatarea lor.
C95.	Activităţile de recepţie se consideră a fi finalizate la momentul semnării de către beneficiar a procesului verbal de recepţie cantitativă şi calitativă a activului fix (dacă din acest document nu rezultă obiecţiuni).
C96.	Dacă în urma exploatării produsului, în termen de 90 de zile de la efectuarea recepţiei se constată că apar deficienţe care nu au putut fi descoperite la recepţie şi prin care nu sunt respectate cerinţele din caietul de sarcini, achizitorul poate solicita remedierea sau înlocuirea produsului, cu suportarea tuturor cheltuielilor de către ofertant.

2.6 Cerinţe privind condiţiile de livrare

Nr. cerinţă	CERINŢA
C97.	La livrare, produsul trebuie însoţit de declaraţii de conformitate.
C98.	Documentaţia de însoţire trebuie să cuprindă: -inventarul cantitativ-valoric, în limba română, care trebuie să coincidă cu preţul unitar al produsului ofertat cu TVA; -certificatul/certificatele de garanţie; -licenţa produsului software, în format electronic.

2.7 Cerinţe privind documentaţia de instalare şi utilizare

Nr. cerinţă	CERINŢA
C99.	Documentaţia de instalare şi utilizare trebuie pusă la dispoziţie în format electronic sau prin specificarea link-ului din internet unde se regăseşte

2.8 Alte cerinţe

Nr. cerinţă	CERINŢA
C100.	Contractantul va propune o soluţie licenţiată
C101.	Contractantul va furniza o listă detaliată cu distribuţia solutiei software, care prezinta în detaliu toate elementele de identificare ale software-ului sau caracteristicile de associate, precum: ▪ Număr de identificare ▪ Număr versiune ▪ Chei de licenta (daca este aplicabil) ▪ Data de expirare a licentei ▪ Periodicitatea de reinnoire a licentei ▪ Data distributiei ▪ EOL / EOS (end of life / end of Support)

Toate cerinţele definite în cadrul prezentei specificaţii tehnice sunt obligatorii. Nerespectarea lor va conduce la respingerea ofertei.