I.P. SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ (STISC)

TABELA DE CONFORMITATE — Sistem de management centralizat al logurilor și analiză de securitate

Ofertantul completează coloanele „Conformitate", „Produsul / modelul ofertat" și „Justificare / referință" pentru fiecare poziție. Toate cerințele sunt minime și obligatorii.

Cod cerință	Cerință tehnică minimă obligatorie	Produsul / modelul ofertat	Conformitate (Conform / Neconform)	Justificare / referință (datasheet, pagină, link, observații)
Sistem de management centralizat al logurilor și analiză de securitate — Cerințe tehnice minime obligatorii				
H1 — Cerințe Hardware și de Platformă				
H1.01	Soluția poate fi livrată ca appliance integrat hardware+software sau ca platformă software pe un server dedicat. Componenta hardware trebuie să îndeplinească toate cerințele de mai jos. Ofertantul este responsabil pentru asigurarea suportului tehnic unificat (un singur punct de contact pentru hardware și software).			
H1.02	Echipamentul trebuie să fie Rack-mountable 19", înălțime maximă 4 RU. Pachetul trebuie să includă obligatoriu șinele de montaj (rack rails) și suporturile de fixare.			
H1.03	Echipamentul nu trebuie să depășească adâncimea șasiului de 850 mm.			
H1.04	Echipamentul trebuie să asigure direcționarea fluxului de aer: față-spate (front-to-back).			
H1.05	Echipamentul trebuie să fie compatibil cu rețeaua de curent electric AC120/230V 50/60Hz.			
H1.06	Echipamentul trebuie să fie completat cu 2 surse de alimentare redundante (hot swappable) incluse.			
H1.07	Consumul maxim de energie electrică al echipamentului nu trebuie să depășească 1000 W, inclusiv toate sursele de alimentare redundante.			
H1.08	Echipamentul trebuie să dispună de porturi minim 2×1Gb/s RJ45 și un port de consolă dedicat RJ45 sau USB.			
H1.09	Echipamentul trebuie să dispună de porturi minim 2×10Gb/s sau superior (SFP+ / SFP28).			
H1.10	Echipamentul trebuie livrat împreună cu transceivere compatibile cu porturile optice ale echipamentului, minimum 4 (patru) bucăți (câte 2 per port optic, pentru ambele capete ale legăturii) și cablurile optice de patch necesare conectării, incluse în ofertă.			
H1.11	Echipamentul trebuie să dispună de minim două unități de stocare dedicate de tip SSD (NVMe sau echivalent), cu capacitate de minim 1.9 TB per unitate, destinate sistemului de operare și accelerării bazei de date analitice (cache/indexare). Unitățile trebuie configurate în RAID 1 (mirroring) pentru asigurarea disponibilității sistemului în cazul defectării unei unități de stocare.			
H1.12	Echipamentul trebuie să asigure un spațiu de stocare de minim 60 TB brut, configurat în RAID 50 sau superior, cu o capacitate utilizabilă de minim 50 TB după aplicarea RAID.			
H1.13	Echipamentul trebuie să dispună de hardware RAID controller ce poate asigura RAID: 1/5/6/10/50/60.			
H1.14	Echipamentul trebuie să fie dotat cu discuri de stocare SED (Self-Encrypting) pentru a asigura capacitatea necesară de păstrare a datelor.			
H1.15	Echipamentul trebuie să fie dotat cu modul TPM (Trusted Platform Module).			
H1.16	Echipamentul trebuie să dețină următoarele certificări: CE, CB.			
H1.17	Echipamentul trebuie să dispună de suport de la producător de minim 3 ani.			
H1.18	Suportul tehnic de la producător trebuie să fie de tip 24×7 (asistență permanentă) cu servicii de înlocuire hardware în regim Advanced Replacement (trimiterea piesei de schimb înainte de returnarea celei defecte).			
C1 — Cerințe funcționale — Sistem de management centralizat al logurilor și analiză de securitate				
C1.01	Soluția trebuie să permită administrarea prin interfață web (HTTPS) și interfață în linie de comandă (CLI/SSH), precum și prin port de consolă dedicat.			
C1.02	Soluția trebuie să dispună de suport pentru integrare cu sisteme de autentificare externă (LDAP, RADIUS, SAML) pentru administrarea conturilor de utilizator.			
C1.03	Soluția trebuie să permită definirea de profiluri de acces granulare (Role-Based Access Control — RBAC), permițând vizualizarea logurilor doar pentru anumite segmente de rețea sau dispozitive, în funcție de rolul administratorului.			
C1.04	Soluția trebuie să suporte colectarea jurnalelor de la minim 3000 dispozitive/surse de log gestionate simultan.			
C1.05	Soluția trebuie să suporte minim 3000 GB/zi jurnale.			
C1.06	Capacitate de indexare și procesare simultană de minim 40.000 evenimente pe secundă (EPS).			
C1.07	Soluția trebuie să suporte Clustering sau High Availability până la 4 noduri.			
C1.08	Soluția trebuie să suporte recepția jurnalelor în format Syslog standard de la diferiți producători.			
C1.09	Transport securizat al jurnalelor prin cel puțin două din următoarele: syslog over TLS, HTTPS/REST API, protocol proprietar criptat al producătorului.			
C1.10	Soluția trebuie să suporte recepția jurnalelor prin metodele API-based injection și agent-based collection.			
C1.11	Soluția trebuie să permită vizibilitatea corelată a sesiunilor de trafic înregistrate de firewall, oferind posibilitatea de a vizualiza logurile de trafic și logurile de securitate (IPS, Antivirus, Web Filtering) într-o singură consolă unificată.			
C1.12	Interfața de raportare trebuie să permită funcționalitatea de drill-down, oferind posibilitatea administratorului de a trece de la o alertă sau un grafic rezumativ direct la liniile de log brute care au generat acel eveniment, printr-un singur click.			
C1.13	Soluția trebuie să suporte raportarea ce asigură rapoarte predefinite și personalizabile pentru cerințe de conformitate cu următoarele standarde: SOC2, CIS Controls, ISO27001:2022.			
C1.14	Soluția trebuie să poată identifica atacurile și vulnerabilitățile folosind motoare de analiză a jurnalelor.			
C1.15	Soluția trebuie să suporte metoda Data Obfuscation pentru logurile păstrate.			
C1.16	Soluția trebuie să ofere analiza în timp real a traficului de rețea.			
C1.17	Soluția trebuie să suporte multi-tenancy cu minimum 300 de instanțe logice separate (domenii administrative), fiecare cu izolare completă a jurnalelor, rapoartelor, dashboards și profilurilor de acces, permițând gestionarea simultană a mai multor organizații sau segmente de infrastructură de pe o singură platformă.			
C1.18	Soluția trebuie să permită arhivarea logurilor pe un suport extern (ex: server FTP, SFTP, NFS) și să asigure verificarea integrității acestora pentru a preveni modificarea post-factum a jurnalelor (Log Integrity Check/Hashing).			
C1.19	Soluția trebuie livrată cu cea mai recentă versiune stabilă de firmware/sistem de operare disponibilă la data livrării.			
C1.20	Soluția trebuie să includă o subscripție activă, furnizată și menținută de producătorul soluției software, pentru întreaga perioadă a suportului, care să asigure actualizarea automată a fluxurilor de Indicatori de Compromitere, incluzând liste de adrese IP malițioase, domenii compromise.			
C1.21	Soluția trebuie să beneficieze de un serviciu de alertare automată a amenințărilor emergente, furnizat de producătorul soluției, cu rapoarte specifice și tablouri de bord dedicate actualizate automat pentru campanii de atac de mare amploare identificate recent la nivel global.			

C1.22	Soluția trebuie să asigure accesul la actualizări periodice ale motoarelor de corelare și analiză, precum și ale template-urilor de conformitate, direct de la laboratoarele de cercetare ale producătorului.			
C1.23	Soluția trebuie să dispună de suport de la producător de minim 3 ani, cu toate funcționalitățile, subscripțiile și serviciile descrise în prezentul caiet de sarcini, incluse pe întreaga durată a contractului.			
C1.24	Suportul tehnic inclus trebuie să fie de tip 24×7 din partea producătorului, cu acces la portalul de asistență și actualizări de tip firmware/OS.			

Digitally signed by Vieru Radu
Date: 2026.08.17 11:47:55 EEST
Reason: MoldSign Signature
Location: Moldova

MOLDOVA EUROPEANĂ