SECTIUNEA II
CAIET DE SARCINI

CAIET DE SARCINI

Achiziție de soluție SIEM (Security Information & Event Management)

Cuprins

1. Descrierea stării prezente

În prezent, în rețeaua CONPET S.A. există un număr de aproximativ 250 de dispozitive (calculatoare, servere fizice și virtuale, switch-uri, routere, firewall-uri) la care se dorește o monitorizare centralizată și rapidă a evenimentelor și a incidentelor de securitate care pot apărea.

Aceste echipamente sunt distribuite pe tot teritoriul României, în stațiile și sediile CONPET S.A.

2. Prezentare generală a lucrării:

Achiziție de soluție SIEM (Security Information & Event Management).

Soluția trebui să ofere licențiere pentru:

- să permită colectarea logurilor și monitorizarea unui număr de minim 250 de echipamente active: stații de lucru, servere și dispozitive de rețea/securitate (servere, firewall-uri, IDS/IPS-uri, routere etc.):
    - 120 stații de lucru – cu sisteme de operare windows 7, 8, 10
    - 50 servere - cu sisteme de operare linux, windows server 2008, 2013, 2016
    - 7 servere cu sistem de operare HP-UX
    - 4 servere VmWare
    - 69 switchuri, routere, firewall-uri, wireless diferiți producători (cisco, huawei, check point, palo alto, extreem network, fortinet……)

Soluția va fi oferită sub forma unui sistem software instalat pe mașini virtuale cu sistem de operare windows server 2016, care să dispună de capabilități de monitorizare a evenimentelor de securitate, precum și de management al logurilor și va cuprinde instalarea și toate licențele software perpetue necesare funcționării depline.

3. Cerințe tehnice

	Cerințe minime solicitate
Colectare date	- să permita colectarea de log-uri si evenimente de la dispozitive de rețea, servere, stații de lucru - să fie capabilă să colecteze evenimente de la minim următoarele surse: • Cisco Router, Firewall, Switch • Checkpoint Firewall • Palo Alto Firewall • Extreem Network Switch • Fortinet Router, Firewall, Switch • Alte brand-uri de firewall, switch, router • Huawey wireless access controller, huawey wireless AP • Bitdefender endpoint security, bitdefender Gravityzone • Microsoft Active Directory • Microsoft Exchange 2013, 2016 • Microsoft SQL • Microsoft SharePoint • Microsoft Windows 2008, 2013, 2016 Server • HP-UX • Linux • Microsoft Windows 7, 8, 10. -să se colecteze doar evenimentele apărute noi față de ultima sincronizare între echipament și serverul SIEM)
Procesare date colectate	- să ofere interogări dinamice și distribuite (trebuie să suporte atât căutari simple cât și căutări complexe bazate pe expresii regulate și expresii logice de tip Boolean). - să dispună de posibilitatea filtrării log-urilor bazata pe orice criteriu legat de informațiile conținute în log-urile respective; - să ofere un tool cu interfață grafică pentru dezvoltare/modificare interogări/rapoarte. - să transforme logurile colectate de la diferite echipamente într-un format comun (normalizat) și să permită categorizarea

	amploarea unui atac, precum și pentru a putea identifica cu usurință inițiatorul acelui atac; - să conțină un modul de raportare, care să includă atât rapoarte predefinite, cât și posibilitatea modificării acestora în funcție de cerințe/necesități; - să permită exportarea rapoartelor în următoarele formate: PDF, XML, HTML, XLSX. - să includă tablouri de bord grafice predefinite, precum și posibilitatea personalizării acestora pentru o imagine cât mai elocventă asupra nivelului de securitate; acestea trebuie să poate afișa informațiile în timp real;
Clasificare echipamente	- să poată clasifica echipamentele de rețea, serverele și stațiile de lucru după producător, funcționalitate, sistem de operare.
Notificare	- să dispună de diferite mecanisme de notificare: alerte la consola, e-mail, SNMP;
Conectivitate	- să ofere posibilitatea de conectare cu alte sisteme SIEM, prin intermediul unor conectori, care să permită trimiterea și primirea unor alerte
Licențiere	- să includă licență perpetua pentru baza de date folosită, dacă este nevoie - Licențierea produsului trebuie să aibă în vedere cerințele dar nu se va limita la acestea și va trebui să acopere toate solicitările și funcționalitățile din acest caiet de sarcini.

4. Servicii

Prestatorul trebuie să furnizeze toate bunurile și serviciile descrise aici ca un proiect "la cheie" și trebuie să își asume responsabilitatea completă pentru proiectarea, livrarea, instalarea, configurarea, optimizarea conform nevoilor beneficiarului, testarea, integrarea, și acceptanța aplicațiilor așa cum sunt specificate în acest Caiet de Sarcini dar nu va trebui să se limiteze la acestea.

Prestatorul trebuie să furnizeze toate materialele, echipamentele, sculele, ingineria, calificarea și forța de muncă necesare pentru a îndeplini în totalitate și în timp util cerințele din acest Caiet de Sarcini.

	acestora în vederea efectuării unei analize ulterioare cât mai facile; - să 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; - să poată identifica acțiuni repetitive sau tiparuri de evenimente, pe baza cărora se pot seta reguli de alertare și se pot adopta politici de securitate. - să dispună de un motor de corelare care să permită identificarea elementelor comune din două sau mai multe evenimente aparent fără nicio legătura; - să ofere posibilitatea identificării incidentelor de securitate IT în timp real pe baza regulilor prestabilite și să permită prioritizarea evenimentelor în funcție de importanță; - să ofere ajutor în analiza evenimentelor și incidentelor prin indicații de "best practice" - să dispună 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 funcție de cerințe/necesități; - să ofere posibilitatea dezvoltării de reguli de alertare înlănțuite (compuse din 2 sau mai multe reguli definite anterior);
backup	- să ofere posibilitatea de export a datelor vechi cu o compresie cât mai mare
access	- permită accesul la aplicație unui număr nelimitat de utilizatori prin intermediul unei interfețe de tip web pe baze de autentificare și unde se pot definii diferite roluri în aplicație;
Monitorizare, raportare	- să monitorizeze în timp real echipamente de rețea, servere, stații de lucru - să permită vizualizarea evenimentelor în timp real și într-un format comun, inteligibil, din cadrul consolei de administrare, fără a fi necesară accesarea unei terțe aplicații; - să dispună de abilitatea de a reprezenta dinamic într-un mod grafic evenimentele desfășurate pentru a putea realiza

5. Livrare

Livrarea licențelor, instalarea și configurarea soluției se va face la Sediul Dispecerat Central din Ploiești str. Anul 1848 nr.1-3.

Orice element/modul/licență/funcționalitate care lipsește din ofertă și care se va dovedi necesar pentru îndeplinirea cerințelor prezentului Caiet de Sarcini, trebuie să fie inclus ulterior fără nici un cost suplimentar pentru Beneficiar.

6. Instruire

Trainingul va detalia pas cu pas activitățile ce se execută, în ceea ce privește instalarea, configurarea, integrarea, utilizarea și mentenanța soluției furnizate.

Prestatorul va furniza o procedură scrisă detaliată a operațiilor necesare a fi efectuate de Beneficiar pentru utilizarea cu succes a soluției, luând în considerare toate situațiile posibile ce pot apare în operarea soluției.

Prestatorul va furniza un manual care va conține și va detalia toate operațiunile necesare în configurarea, operarea și mentenanța soluției.

7. Managementul Proiectului

Prestatorul va fi responsabil de planificarea, urmărirea şi coordonarea proiectului.

Prestatorul trebuie să desemneze un Project Manager al cărui CV trebuie să fie anexat documentației de calificare și care trebuie să evidenţieze studiile relevante și experiența persoanei desemnate de ofertant în managementul unor proiecte similare ca obiect şi amploare.

Prestatorul trebuie să prezinte compunerea echipei de executare a proiectului atât general pe calificări/roluri, cât şi nominal. Această echipă trebuie să aibe în componență personal calificat care să instaleze și să configureze aplicația la nivel cel puțin de security expert în tehnologia ofertată (ex. CCNP security, CCSE, NSE4 sau echivalent).

Componența echipei prezentată în ofertă va putea fi schimbată numai cu aprobarea Beneficiarului.

8. Acceptanță

Prestatorul va prezenta Beneficiarului o procedură de verificare pentru acceptanță conformă cu specificațiile softwareului. Procedura va fi înaintată Beneficiarului cu 14 de

zile înainte de efectuarea testelor de acceptanță. Beneficiarul va analiza propunerea de procedură și dacă va fi cazul, va solicita modificarea/completarea acesteia sau o va accepta. În cazul în care Beneficiarul va solicita modificarea/completarea testelor de acceptanță, se vor repeta pașii de mai sus până la acceptarea de către Beneficiar.

Testele de acceptanță trebuie să asigure Beneficiarul că Soluția implementată este instalată corect, este configurată corect, operează conform cerințelor.

Procedura de acceptanță va include cel puțin următoarele teste:

- Colectarea de evenimente de la toate echipamentele prezentate.
- Trimiterea evenimentelor colectate într-un mod optimizat și filtrate care să reflecte investigarea doar a alertelor relevante conform bunelor practici.
- Trimitere de alerte pe e-mail în cazul apariției unui incident de securitate (se vor simula incidente de securiate)
- Exportul datelor în vederea păstrarii lor pe o perioadă mai lungă.
- Identificare de evenimente repetitive.
- Alte teste ce pot stabili buna funcționare și configurare a soluției.

După finalizarea cu success a testelor de acceptanță efectuate împreună cu beneficariul și aprobate de către acesta (beneficiar), prestatorul va notifica în scris Beneficiarul că a finalizat implementarea și se poate organiza punerea în funcțiune a sistemului.

9. Durata lucrărilor

Termenul de execuție pentru lucrarea contractată este de 2 luni de la semnarea contractului.

În acest termen trebuie incluse toate etapele contractului:

- Livrare licențe
- Instalare și configurare aplicație
- Predare documentație
- Instruire utilizatori
- Teste de acceptanță
- Punere în funcțiune

Prestatorul are obligația de a comunica Beneficiarului data finalizării serviciilor transmițându-i acestuia, pentru confirmare, o înștiințare scrisă, după terminarea cu succes a ultimului test de acceptanță.

Beneficiarul va organiza recepția în maximum 5 zile de la notificarea finalizării serviciilor și va comunica Prestatorului data stabilită.

Termenul de finalizare a serviciilor din Caietul de Sarcini se consideră împlinit la data semnării fără obiecțiuni de către Comisia de recepție a Procesului verbal de recepție.

10. Garanție

Prestatorul trebuie să furnizeze Beneficiarului garanție comercială de 3 ani de la data semnării procesului verbal de recepție pentru toate licențele și lucrările.

Garanția trebuie să includă, pentru aceeași perioadă, suport tehnic pentru asistență în operare și configurare în timpul normal de lucru, atât din partea echipei de suport oficiale a producătorilor echipamentelor și softwareului (inclusiv update-uri la ultimele versiuni software), cât și din partea echipelor de suport ale Prestatorului.

Șef Birou Infrastructură IT
Florescu Costin

Șef Serviciu IT
Cătălin Mereanu