Achiziţionarea de software pentru implementarea proiectului cu titlul "Să ne protejăm mai bine viitorul! Cybersecurity avansat" cod SMIS 133334.

I.D.: 66897528

Data publicarii	08.03.22	Coduri CPV	30211300-4

Pretul estimativ:	27.687,30 RON - 27.687,30 RON 135.000,00 RON - 135.000,00 RON

Descriere: 2. LOT 2 – Solutie de gestionare a vulnerabilitatii, permitand evaluarea si raspunsul la schimbarile din mediu in timp real si prioritizarea riscurilor asupra vulnerabilitatilor, configuratiilor si controalelor., Soluţia sa permita instalarea un server CentOS 7. Cerinţe tehnice minime: Trebuie să ruleze fără a necesita instalarea unui agent pe sistemele din reţea Trebuie sa asigure rularea de scanări pentru identificarea vulnerabilităţilor reţelei şi ale sistemelor existente Trebuie sa asigure prioritizarea scanărilor şi a analizei în funcţie de criticitatea activelor identificate în reţea Trebuie sa asigure scanarea sistemelor ce deţin adrese IPv4 şi IPv6 Solutia trebuie sa asigure actualizarea semnăturilor şi informaţiilor despre vulnerabilităţi în mod automat Solutia trebuie sa permita introducerea manuală a sistemelor sau importul acestora. Solutia trebuie sa asigure crearea rolurilor de administrare şi a drepturilor aferente acestora pentru setarea politicilor de scanare şi controlul prioritătţilor Solutia trebuie sa includă politici de analiză şi scanare asociabile unor grupuri de active, pentru a realiza analiză de context Solutia trebuie sa permită rularea scanărilor în mod manual sau automat inclusiv configurarea şi definirea unor intervale de scanare a activelor sau a grupurilor de active Solutia trebuie sa asigure administrarea prin intermediul unei interfeţe web care permite modificarea informaţiilor afişate în funcţie de necesităţi. Solutia trebuie sa scaneze şi să identifice cel puţin: Software de bază pentru echipamente de reţea (routere, switch-uri); Sisteme de operare pentru desktop-uri şi servere (cel puţin Microsoft Windows 10, Linux); Echipamente de tip IDS/IPS; Echipamente de tip firewall; Funcţionalitatea trebuie să fie disponibilă pentru utilizare fără o configurare specială (out of the box); Soluţia trebuie să suporte cel puţin următoarele tehnici de identificare a sistemelor : Ping sweep; UDP probe; Asset fingerprinting; Rapid discovery; NetBIOS-based discovery; TCP discovery; UDP port discovery; OS fingerprinting; Application fingerprinting; Integrated NMAP database; Solutia trebuie sa asigure definirea unei structuri ierarhice de grupuri de active Solutia trebuie sa asigure importul din Active Directory Solutia trebuie sa permita realizarea de clasificări pe diverse criterii (de exemplu criteriul organizaţional, topologic, geografic sau la nivel de sistem) Solutia trebuie sa furnizeze rapoarte per activ sau grup de active pentru următoarele nivele ierarhice: Rapoarte pentru managementul de top; Rapoarte pentru managementul secundar; Rapoarte pentru specialisti Solutia trebuie sa asigure capabilităţi de notificare prin e-mail Solutia trebuie sa asigure emiterea rapoartelor în mod programat sau rularea ad-hoc a acestora Solutia trebuie sa asigure furnizarea de rapoarte de remediere Solutia trebuie sa asigure emiterea de rapoarte privitoare la tendinţele de schimbare privind managementul vulnerabilităţilor Solutia trebuie sa asigure stabilirea unei linii de bază şi urmărirea evoluţiei în timp a vulnerabilităţilor existente (emiterea de rapoarte ce evidenţiază diferenţele identificate între sesiuni de scanare separate în timp) Solutia trebuie sa furnizeze informaţii suplimentare despre vulnerabilităţile identificate: descriere, criticitate, risc, identificator specific producătorului, metode pentru remediere (inclusiv patch-uri software, configurări de administrare sau căi alternative destinate acoperirii vulnerabilităţilor detectate) Solutia trebuie sa dispună de şabloane de raportare predefinite şi de posibilitatea de creare a altor şabloane personalizate Rapoartele să poată fi exportate cel puţin în format PDF şi CSV.. 1. LOT 1 – Platformă software pentru colectarea, analiza, căutarea şi vizualizarea logourilor şi 2 ani suport standard şi întreţinere;, Achiziţia platformei software si a suportului de întreţinere, mentenanta, suportul si actualizarea sunt necesare pentru ETSS pentru asigurarea condiţiilor optime de implementarea a proiectului. Ofertele vor include toate

serviciile necesare pentru instalare software/ montaj etc., astfel încât să se asigure punerea în funcţiune a platformei. Platforma trebuie sa permita functionarea în sistem server – agenţi. Agenţii sa permita captarea log-urilor de pe sisteme Windows utilizând Sysmon şi sisteme Linux prin intermediul Syslog, fisiere dar si customizabile pe baza expresilor regulate. Platforma sa permita instalarea componentei centrale în mod compact pe un server CentOS 7, cu 64GB RAM. Cerinţe tehnice minime: Solutia trebuie sa ofere software-ul si licentele necesare monitorizarii logurilor si a traficului de retea in timp real. Soluţia trebuie să colecteze într-o modalitate securizată şi centralizată jurnalele şi evenimentele raportate de diverse componente ale infrastructurii IT. Pe baza informaţiilor colectate se vor aplica functionalităţi şi obiecte configurabile la nivelul soluţiei astfel încat evenimentele să fie normalizate şi categorizate, filtrate, interpretate inteligent şi corelate într-un mod configurabil pentru ca în urma acestor acţiuni să fie generate alerte şi rapoarte relevante pentru securitatea şi buna funcţionare a infrastructurii IT. Soluţia trebuie să dispună de mecanisme predefinite de colectare a evenimentelor pentru componentele uzuale ale infrastructurilor IT (sisteme de operare, servere, aplicaţii, echipamente de reţea, echipamente şi soluţii de securitate, baze de date etc.) dar să ofere şi suport pentru dezvoltarea de variante configurabile (custom) de colectare evenimente de la sisteme ce nu se regasesc într-o listă predefinită. Soluţia trebuie poata pune la dispozitie obiecte specifice sistemului de colectare, corelare şi raportare predefinite, pentru o punere iniţială în funcţiune cât mai rapidă şi mai facilă (filtre, reguli de corelare, alerte, rapoarte etc.) dar să ofere şi posibilitatea de a defini propriile obiecte fără niciun fel de limitări sau restricţii funcţionale sau de licenţiere. Arhitectura soluţiei trebuie să includă minim o componentă centralizată de colectare, analiză şi raportare. Colectarea evenimentelor trebuie să se realizeze prin intermediul unui componente disponibile sub formă de agenţi/produs de colectare software. Această componentă trebuie să îndeplinească şi rolul de normalizare jurnale şi evenimente. Numărul agenţilor de colectare ce pot fi utilizaţi nu trebuie să fie limitat de licenţă. Procesarea evenimentelor trebuie să se realizeze începând de la nivelul agenţilor de colectare, pentru a degreva componenta centrală de operaţiunile specifice de normalizare şi agregare, funcţionalităţile fiecărei componente fiind bine definite şi delimitate. Soluţia trebuie să dispună de mecanisme de optimizare a volumului de trafic şi jurnalelor transmise şi procesate încă de la nivelul agenţilor de colectare (gestiune de bandă, filtrare şi agregare de evenimente). Solutia trebuie sa garanteze integritatea informatiilor colectate. Soluţia trebuie să utilizeze o bază de date care să nu necesite licenţiere suplimentară. Soluţia trebuie să asigure scalabilitatea puterii de procesare printr-o simplă licenţiere. Componentele de tip agenţi de colectare vor normaliza şi categorisi evenimentele întrun format comun. Pentru optimizarea traficului de reţea şi a numărului de jurnale şi evenimente filtrate de către sistemul de centralizare şi analiză, la nivelul agenţilor de colectare soluţia trebuie sa permită implementarea următoarelor funcţionalităţi: Filtrare de evenimente configurabilă selectiv de către administrator; Agregarea mai multor evenimente de acelaşi tip într-un singur eveniment care va include toate informaţiile iniţiale similare (agregarea se va realiza fără pierdere de informaţii atât timp cât ele coincid la nivelul evenimentelor agregate) şi informaţii despre numărul total de evenimente agregate; Transmisia evenimentelor în blocuri de evenimente pe baza de momente recurente de timp sau pe baza de dimensiuni fixe de blocuri (număr de evenimente); Limitarea benzii utilizate pentru transmiterea evenimentelor; Pentru aplicaţii personalizate, sisteme interne nestandardizate şi surse de jurnale ce nu se află printre agenţii de colectare disponibili în mod implicit, soluţia trebuie să pună la dispoziţie un mecanism de dezvoltare de agenţi de colectare personalizaţi. Aceşti agenţi de colectare personalizaţi trebuie să acopere minim următoarele scenarii: Extragere de informaţii din baze de date; Extragere informaţii din fişiere personalizate de tip log atât pentru jurnale în format fix cât şi pentru format flexibil; Extragere informaţii din fisiere de tip XML; În vederea dezvoltării de obiecte de management personalizate şi de conţinut la nivelul soluţiei de centralizare, analiză şi corelare, soluţia trebuie să pună la dispoziţie un mecanism de replicare a unui set de evenimente predefinit astfel încât aceste evenimente să fie importate la nivelul sistemului de corelare gradual pentru a studia comportamentul şi rezultatul obiectelor şi regulilor configurate anterior. Pentru prioritizarea şi clasificarea cât mai corectă şi exactă a evenimentelor soluţia trebuie să calculeze un scor de prioritate/criticalitate a evenimentelor, rezultat în urma analizei mai multor variabile precum: Severitatea evenimentului în forma prezentată de sistemul ţintă (resursa generatoare de jurnale/evenimente); Importanţa resursei în cadrul infrastructurii şi a soluţiei de analiză (dacă a fost scanată de porturi/de vulnerabilităţi, dacă a fost înregistrată în soluţia de analiză şi raportare etc.); Relevanţa evenimentului la nivelul resursei generatoare (dacă resursa este vulnerabilă, dacă are porturi deschise etc.); Relevanţa istorică a evenimentului curent (dacă resursa a mai fost atacată, dacă atacatorul este cunoscut etc.); Dacă resursa a fost marcată cu un nivel de criticalitate la nivelul soluţiei de analiză şi corelare şi dacă da, se va lua în calcul acest nivel; Pe lângă informaţiile

transmise în mod implicit, soluţia trebuie să permită îmbogăţirea acestora pentru a le mari relevanţa în procesul de analiză, corelare şi identificare potenţiale acţiuni maliţioase. Printre informaţiile relevante necesare se numară: Informaţii referitoare la reţea şi resurse ţintă gestionate precum: adresare IP, zonă de reţea din care face parte fiecare resursă şi categoria în care se încadrează din punct de vedere al infrastructurii sau al importanţei organizaţionale; Informaţii proprii fiecarei resurse gestionate (sistem ţintă de unde sunt colectate jurnale/evenimente) precum nume, adresă IP/MAC, locaţie, zonă de reţea din care face parte, criticalitatea resursei în contextul de business, porturi deschise, vulnerabilităţi şi sistem de operare. Informaţii precum porturi şi vulnerabilităţi trebuie să poată fi extrase automat din rapoarte generate de aplicaţii specifice de scanare de vulnerabilităţi; Pentru o monitorizare cât mai detaliată şi facilă, soluţia trebuie să permită vizualizarea în timp real a evenimentelor şi jurnalelor primite cu opţiuni de configurare de filtre specifice fiecărei resurse de vizualizare; Soluţia poate pune la dispozitie un set de reguli de identificare activităţi potenţial maliţioase şi corelare complexe, configurabile de către administratori; Rezultatele regulilor de corelare trebuie să poată fi utilizate secvenţial şi automat în cadrul altor reguli de corelare, astfel încat să poată fi identificate comportamente complexe şi activităţi ce se bazează pe o succesiune de evenimente distincte; Soluţia trebuie să asigure un mecanism de salvare a informaţiilor relevante întro listă atunci când sunt identificate anumite evenimente sau sunt declanşate reguli de corelare importante; informaţiile salvate trebuie să poată fi studiate şi utilizate în continuare în cadrul altor obiecte specifice soluţiei; Soluţia trebuie să permită configurarea personalizată de panouri de monitorizare pe bază de grafice şi tabele şi posibilitatea accesării fluxului de evenimente/graficului de evenimente specifice unei anumite acţiuni/activităţi direct din aceste panouri; Solutia trebuie sa puna la dispozitie "Out of the box" un panou de monitorizare care sa mapeze evenimetele pe framework-ul MITRE ATT&CK. Tabloul de bord MITRE va permite vizualizarea informaţiilor despre tactici şi tehnici folosite de atacatori pentru orice activitate care se potriveşte cu matricea MITRE ATT & CK pentru a putea identifica mai rapid incidentele de securitate; Solutia oferă un pachet predefinit de reguli de corelare şi alertare care sa inlcuda cel putin urmatoarele cazuri: Brute Force Attacks, Unsuccessfull Login Attempts, Account Activity Monitoring, Pass the Hash Attempts, Monitor Cleared Logs, Malware Infections, Network Monitoring, Perimeter Monitoring, Vulnerability Monitoring; Soluţia trebuie să asigure integrarea "Out of the box" cu surse de Threat Intelligence fără costuri suplimentare. Soluţia trebuie să ofere propriile sale metode de detectare a ameninţărilor care oferă detectia anomaliilor fără costuri suplimentare. Interfata web va pune la dispozitie un panou pentru a putea urmari atacurile in timp real pe o harta geografica, indicand IP-ul sursa si destinatie, cat si regula de corelare care a declansat evenimentul. Soluţia trebuie să permită definirea de liste de câmpuri relevante (din cele incluse în taxonomia implicită) astfel încât ele să poată fi aplicate la nivelul obiectelor specifice soluţiei; Soluţia trebuie să permită definirea de filtre de evenimente şi salvarea acestora astfel încât ele să poată fi utilizate ulterior la nivelul celorlalte obiecte specifice soluţiei; Soluţia trebuie să permită rularea unor comenzi direct la nivelul evenimentelor de interes, astfel încât să poată fi obţ informaţii suplimentare..