CAIET DE SARCINI

Nr. d/o	Cod CPV	Denumirea serviciilor solicitate	Unitate de măsură	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată MDL fără TVA
1	48000000- 8	Soluție de management a retelei IT, invetarierea activelor, helpdesk, managementul si gestionarea accesului si autorizarilor de acces al utilizatorilor pentru 100 utilizator	buc	1	Conform Caietului de sarcini	330.000,00
2	48000000- 8	Soluție de prevenire a scurgerilor de date pentru 100 de utilizatori	buc	1	Conform Caietului de sarcini	270.000,00
3	48000000- 8	Soluție de marcare și clasificare a informațiilor/documentelor și a mesageriei electronice pentru un numar de 100 utilizatori.	buc	1	Conform Caietului de sarcini	170.000,00
Valoarea estimativă totală fără TVA						770.000,00

I. SCOPUL ACHIZIȚIEI

Caietul de Sarcini cuprinde cerințele minime necesare privind achiziția și crearea unei platforme unice de securitate cibernetică care să includă funcționalități de gestiune și monitorizare a rețelei IT, inventariere a bunurilor organizației, de gestiune a tuturor solicitărilor ale angajaților și partenerilor organizației, de analiză și audit al utilizatorilor organizației, inclusiv prevenirea scurgerilor de date cât și clasificarea și etichetarea lor pentru un control centralizat și eficient. Acesta ar fi un instrument important și extrem de puternic pentru gestionarea și protejarea activelor organizației ODA.

Scopul acestui document este de a specifica conceptul platformei de securitate cibernetică precum și cerințele tehnice ce alcătuiesc componentele acestei platforme, că sunt conforme cu standardele tehnice actuale, și ca această soluție prezintă o bază bună pentru dezvoltarea securizată a instituției în următorii ani, așa cum poate fi prevăzut la acest moment, prin integrări și dezvoltări ulterioare fără necesitatea schimbării soluțiilor propuse.

II. DESTINAŢIA SISTEMULUI

O platformă unică de securitate cibernetica reprezenta un instrument esențial și complet pentru gestionarea și protejarea mediului IT si al securității informaționale al organizației. Componentele de bază al acesteia ar fi:

Managementul rețelei IT: Această componentă ar permite administrarea și monitorizarea rețelei IT a organizației, inclusiv configurația echipamentelor, monitorizarea traficului și a performanței rețelei, precum și detectarea și remedierea problemelor de rețea.

Inventarierea activelor: Platforma ar oferi o vedere centralizată a tuturor activelor IT, inclusiv echipamente hardware, software, licențe și alte resurse. Acest lucru ar facilita urmărirea și gestionarea eficientă a activelor, precum și identificarea și remedierea lacunelor de securitate cibernetică

Helpdesk: O facilitate de helpdesk integrată ar permite utilizatorilor să raporteze incidente de securitate și să solicite asistență tehnică într-un mod organizat și eficient. De asemenea, ar include un sistem de gestionare a incidentelor pentru a le putea urmări și a le rezolva, inclusive raportarea si auditarea lor.

Managementul și gestionarea accesului utilizatorilor: Această componentă ar permite administrarea și controlul accesului utilizatorilor la resursele IT ale organizației. Acest lucru ar include gestionarea conturilor de utilizator, definirea și aplicarea politicilor de acces și autorizare, și monitorizarea activității de autentificare și acces pentru a detecta și preveni accesul neautorizat.

Prevenirea scurgerilor de date: Funcționalitatea de prevenire a scurgerilor de date ar ajuta la identificarea și prevenirea scurgerilor de date sensibile sau confidențiale către exteriorul organizației. Aceasta ar implica monitorizarea traficului de date, criptarea datelor sensibile și implementarea politicilor de control al datelor pentru a preveni accesul neautorizat sau transferul de date neautorizat pe orice canal posibil (atât intern cat si extern).

Clasificarea și etichetarea datelor: Platforma ar include instrumente pentru clasificarea și etichetarea datelor în funcție de sensibilitatea lor și a reglementărilor relevante. Aceasta ar ajuta la protejarea și gestionarea eficientă a datelor sensibile, asigurându-se că sunt tratate în conformitate cu politicile de securitate ale organizației și că sunt protejate împotriva accesului neautorizat.

Prin integrarea tuturor acestor funcționalități într-o singură platformă, organizația va putea beneficia de o abordare holistică și integrată a securității IT, facilitând administrarea și protejarea eficientă a infrastructurii IT cât și a datelor lor sensibile.

III. CERINȚE TEHNICE:

Platformă unică de securitate cibernetica trebuie sa fie formată din produse și sisteme tip permanent (licenta tip - perpetual) cu o perioadă de garanție/mentenanță și suport producător pentru minim 12 luni. Sisteme cu licență tip subscripție anuală nu se acceptă.

A. <u>Soluție de management a retelei IT, invetarierea activelor, helpdesk, managementul si gestionarea accesului si autorizarilor de acces al utilizatorilor pentru 100 utilizator/stații de lucru/echipamente IT</u>

1. Soluția ofertată trebuie sa ofere următoarele funcționalități de baza minime:

1.1. Soluția ofertată trebuie să fie de tip on-premise, perpetua, cu mentenanța si suportul pentru 12 luni, sa fie scalabilă care să ofere un management integrat și centralizat a infrastructurii IT;

1.2. Consola de administrare trebuie sa afișeze lista dispozitivelor identificate in rețea;

1.3. Soluția va oferi un dashboard pentru monitorizare si analiză disponibil prin web browser;

1.4. Consola de administrare va fi instalata minim pe sistemul operațional Windows 7, 8.1, 10, 11 (32-bit si 64-bit) sau Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019;

1.5. Instalarea agenților pe stații, trebuie sa acopere minim următoarele sisteme de operare:

- Microsoft Windows 8, 8.1, 10 ,11, (all 32-bit and 64-bit editions),
- Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, 2019.

1.6. Interfața consolei trebuie sa susțină minim limba engleza;

1.7. Soluția trebuie sa asigure integrarea cu AD/LDAP;

1.8. Soluția trebuie sa ofere posibilitatea ca agenții distanți sa fie conectați către consola de management;

1.9. Cerințe privind funcționalitatea de raportare și alertare a soluției:

- Soluția tehnică trebuie să poată genera, cu posibilități de descărcare a fișierului de raport, în baza evenimentelor grupate pe zile, săptămâni, luni, anual și să acopere următoarele categorii: cronologie privind starea dispozitivului, lista aplicațiilor instalate pe dispozitiv, top 10 dispozitive care au consumat cel mai mult din banda de transfer de date, top 10 dispozitive după utilizarea procesorului, top 10 dispozitive care au generat cele mai multe evenimente ș.a.;
- Rapoartele generate trebuie să fie posibil de exportat în fișiere PDF;
- Soluția trebuie să poată genera automat evenimente/notificări pentru următoarele situații: dispozitivul este disponibil în rețea sau este deconectat, serviciul de evidență a căzut sau serviciul de evidență funcționează la o anumită performanță, un nou dispozitiv identificat în rețea, interfața unui dispozitiv de rețea nu poate fi accesată, a fost identificată o înregistrare nouă în Windows Event Log, starea unui serviciu Windows s-a modificat, starea agentului de monitorizare, utilizatorul a printat pagini înafara limitei prestabilite ș.a.
- Notificări posibile prin intermediul platformelor de mesagerie MS Teams și Slack.

2. Soluția ofertată trebuie să acopere licențierea pentru 100 de stații de lucru și să includă minim următoarele module/compartimente: monitorizarea rețelei, sistem helpdesk, inventariere(HW+SW) si utilizatori ce vor asigura următoarele cerințe/ funcționalități:

2.1. La nivelul modulului de scanare a rețelei soluția trebuie să ofere următoarele funcționalități:

- Control asupra proceselor de sistem pentru îmbunătățirea performanței și stabilității;

- Scanarea rețelei și descoperirea dispozitivelor pentru identificarea tuturor dispozitivelor și serviciilor TCP/IP;
- Aplicarea contoarelor de performanță la dispozitive pe baza șabloanelor (modelelor) pentru monitorizare consecventă;
- Rapoarte personalizabile pentru dispozitive, filiale, hărți selectate sau întreaga rețea;
- Suport pentru mesajele syslog pentru jurnalizarea eficientă a evenimentelor;
- Compilator de fișiere MIB pentru gestionarea fișierelor Management Information Base;
- Lucrul simultan al mai multor administratori cu gestionarea autorizațiilor și drepturilor de acces;
- Monitorizarea serviciilor cruciale pentru a asigura funcționarea continuă a acestora;
- Distribuția fișierelor folosind Windows Management Instrumentation (WMI) pentru implementarea la distanță a software-ului;
- Monitorizarea umidității și temperaturii în sălile server pentru controlul ambiental;
- Disponibilitatea imediată a rapoartelor;
- Hărți interactive de rețea, hărți de utilizator/sucursală și hărți inteligente pentru o mai bună vizualizare;
- Monitorizarea serviciilor TCP/IP, inclusiv timpul de răspuns, corectitudinea și statistici privind pachetele;
- Alerte prin notificări pe desktop, e-mail sau SMS, împreună cu acțiuni corective, cum ar fi lansarea programului sau repornirea mașinii;
- Suport pentru SNMP traps pentru gestionarea evenimentelor în timp real;
- Maparea porturilor pentru routere și switch-uri pentru gestionarea conexiunilor de rețea;
- Alarme pentru acțiuni la evenimente pentru răspunsuri automate la evenimente specifice;
- Contoare SNMP v1/2/3 pentru diverse metrici, cum ar fi transferul de rețea, temperatura, umiditatea, tensiunea electrică, nivelul de toner, etc;
- Contoare WMI pentru monitorizarea încărcării CPU, utilizarea memoriei, utilizarea discului, transferul de rețea, etc;
- Monitorizarea performanței Windows, inclusiv schimbările de stare a serviciilor și înregistrările din jurnalul de evenimente;
- Suport pentru criptarea AES, DES și 3DES pentru protocolul SNMPv3 pentru a asigura comunicarea securizată;
- Autentificare multifactorial (MFA) pentru accesul la consolă folosind e-mail și/sau SMS;
- Monitorizarea VMware pentru urmărirea stării mașinilor virtuale;
- Gestionarea VMware pentru gestionarea eficientă a stării mașinilor virtuale.

2.2. La nivelul modulului de asistență tehnică (HelpDesk) soluția trebuie să ofere următoarele funcționalități:

- Crearea și gestionarea tichetelor de probleme, cu posibilitatea de a le atribui administratorilor;
- Gestionarea conturilor locale de utilizator Windows, inclusiv crearea, ștergerea, activarea, editarea drepturilor, resetarea parolelor și editarea conturilor;
- Includerea de comentarii, capturi de ecran și atașamente în tichetele de probleme pentru documentare cuprinzătoare;
- Câmpuri personalizabile legate de categoriile de tichete selectate pentru capturarea informațiilor relevante;
- Planificarea înlocuirilor și atribuirea tichetelor de probleme corespunzător;
- Procesarea notificărilor în mod anonim pentru a susține cerințele Directivei "Whistleblower";
- Un sistem avansat de raportare pentru generarea de informații detaliate și analize;

- Automatizări bazate pe reguli de condiție-acțiune pentru optimizarea proceselor;
- Notificări în timp real și actualizări ale tichetelor de probleme;
- O bază de date cuprinzătoare a tichetelor de probleme cu un motor de căutare avansat;
- Baza de cunoștințe (knowledge base) cu articole categorizate, inclusiv posibilitatea de a insera imagini și videoclipuri YouTube;
- Suport pentru teme luminoase și întunecate în interfața web;
- Interfață web transparentă și intuitivă pentru ușurința de utilizare;
- Mesager intern (chat) cu setări de permisiuni, transfer de fișiere și conversații de grup;
- Mesaje trimise către utilizatori/mașini cu confirmare disponibilă/obligatorie a recepției;
- Gestionarea proceselor Windows direct din fereastra de informații despre dispozitiv;
- Distribuție de fișiere și executarea de sarcini, facilitând instalările de software la distanță;
- Procesarea tichetelor din mesajele de e-mail pentru comunicare fără probleme;
- Integrarea bazei de date a utilizatorilor cu Active Directory pentru gestionarea eficientă a utilizatorilor;
- Acces la distanță la mașini cu opțiunea de blocare a intrărilor pentru mouse și tastatură;
- Partajarea bidirecțională de fișiere pentru colaborare ușoară și schimb de date.

2.3. La nivelul modulului de inventariere (HW+SW), soluția trebuie să ofere următoarele funcționalități:

- Înregistrări detaliate ale acțiunilor efectuate asupra activelor pe parcursul ciclului lor de viață, inclusiv capacitatea de a defini stări și câmpuri și de a genera acte de predare a echipamentului;
- Vizualizarea activelor, aplicațiilor, documentelor și licențelor pentru utilizatori individuali sau o vedere separată a activelor atribuite dispozitivelor;
- Capacitatea de a atribui un document mai multor active simultan;
- Generator de documente bazat pe șabloane pentru crearea eficientă a documentației;
- Numerotarea automată a activelor și documentelor adăugate conform șabloanelor definite;
- Gestionarea activelor IT pentru administrarea tuturor activelor aflate sub responsabilitatea departamentului IT;
- Listă de chei de software Microsoft pentru acces și gestionare ușoară;
- Sistem de gestionare a activelor software pentru administrarea avansată a aplicațiilor și licențelor;
- Monitorizarea diferitelor tipuri de licențe, inclusiv modelarea licențelor cloud;
- Gestionarea instalărilor/dezinstalărilor de software bazată pe managerul de pachete MSI;
- Urmărirea licențelor în funcție de utilizator, dispozitiv, număr serial sau versiunea aplicației instalate;
- Urmărirea istoricului de utilizare pentru licențe software specifice;
- Auditul inventarului hardware și software pentru urmărirea completă a activelor;
- Asistent de inventar mobil pentru Android pentru gestionarea mobilă a activelor;
- Revizuirea licențelor atribuite unui utilizator care operează pe mai multe dispozitive;
- Acces la distanță la managerul de fișiere cu opțiunea de ștergere a fișierelor utilizatorului pentru gestionare securizată;
- Informații despre intrările din registru, fișiere și arhive .zip pe un workstation pentru monitorizare detaliată;
- Detalii despre configurația hardware a stației de lucru pentru urmărirea precisă a activelor;
- Alerte pentru instalările de software și schimbările de hardware pentru a rămâne informat;
- Capacitatea de a arhiva și compara auditurile pentru referință la date istorice;
- Monitorizarea planificatorului de sarcini Windows pentru gestionarea sarcinilor;

- Conexiune la distanță prin RDP (Remote Desktop Protocol) la dispozitivele finale pentru remediere eficientă;
- Monitorizarea în timp real a desktopurilor utilizatorilor pentru informații imediate și asistență.

2.4. La nivelul modulului de utilizatori, soluția trebuie să ofere următoarele funcționalități:
- Gestionarea completă a utilizatorilor bazată pe grupuri de securitate și politici;
- Capacitatea de a bloca procesele din rulare pe baza locației fișierului .EXE;
- Optimizarea organizării muncii prin urmărirea timpului petrecut în activități specifice pentru îmbunătățirea proceselor de afaceri;
- Minimizarea timpului pierdut în activități neproductive și creșterea performanței angajaților;
- Distincția activităților efectuate pe dispozitive specifice;
- Îmbunătățirea nivelului de securitate corporativă prin blocarea domeniilor web periculoase;
- Blocarea site-urilor considerate nepotrivite sau nelegate de sarcinile de lucru;
- Control asupra aplicațiilor lansate, permițând blocarea lor dacă este necesar;
- Colectarea de date și atribuirea acestora utilizatorilor specifici, permițând aplicarea automată a drepturilor de acces, a autorizărilor și a politicilor de monitorizare, indiferent de computerul utilizat;
- Monitorizarea mesajelor de e-mail (header) pentru contracararea tentativelor de phishing;
- Urmărirea detaliată a timpului de lucru, inclusiv începutul și sfârșitul activităților și a pauzelor;
- Monitorizarea aplicațiilor utilizate atât în starea activă, cât și în cea inactivă;
- Filtrarea web avansată și blocarea aplicațiilor cu crearea și gestionarea flexibilă a regulilor, inclusiv gruparea regulilor;
- Urmărirea site-urilor web vizitate, inclusiv titluri, adrese și numărul și durata vizitelor;
- Audituri pentru imprimante pentru monitorizarea activităților de imprimare, inclusiv detalii despre imprimante, utilizatori, computere și costurile de imprimare;
- Caracteristici pentru reducerea costurilor de imprimare prin monitorizare și gestionare;
- Urmărirea utilizării legăturilor pentru monitorizarea traficului de rețea generat de utilizatori;
- Vizualizare statică la distanță a desktopurilor utilizatorilor fără acordarea dreptului de acces;
- Capturarea de capturi de ecran, pentru crearea istoricului de lucru al utilizatorului, ecran cu ecran.

3. Soluția trebuie să permită adăugarea ulterioara nativa prin extindere/achiziționare a modulelor suplimentare la cerere, cum ar fi dataguard și monitorizarea eficienței/optimizării timpului utilizatorilor, care sa acopere următoarele cerințe/ funcționalități:

3.1. La nivelul modulului de dataguard, soluția trebuie să ofere următoarele funcționalități:
- Alocarea automată a politicilor implicite de monitorizare și securitate utilizatorilor individuali;
- Economii de costuri și timp în procesele de recuperare a datelor;
- Integrarea fără probleme cu Windows Defender, permițând gestionarea centralizată a setărilor antivirus, alertarea problemelor și rezultatele scanării;
- Integrare cu Windows Firewall, furnizând capacitatea de a activa/dezactiva firewall-ul pentru conexiuni specifice, crearea regulilor de trafic și verificarea stării firewall-ului pe stațiile de lucru;
- Mitigarea riscului de scurgeri de date sensibile prin dispozitive de stocare portabile și dispozitive mobile;
- Stabilirea politicilor corporative de transfer de date pentru angajați, împreună cu autorizările corespunzătoare;

- Opțiunea de a șterge în mod securizat suporturile de date inexistente sau eliminate (de exemplu, stick-uri USB);
- Alerte pentru dispozitivele externe conectate care nu au atributul "suport de încredere";
- Integrare cu Windows Bitlocker, permițând monitorizarea stării modulului TPM și a criptării volumelor;
- Gestionarea drepturilor de acces (scriere, execuție, citire) pentru dispozitive, computere și utilizatori;
- Acces la informații despre dispozitivele conectate la un computer specific;
- Listă cuprinzătoare a tuturor dispozitivelor conectate la computerele în rețea;
- Auditarea (istoricul) conexiunilor și operațiunilor pe dispozitivele mobile și partajările de rețea;
- Configurare centralizată pentru reguli la nivel de rețea, hărți de rețea selectate și grupuri și utilizatori din Active Directory;
- Alertele în timp real pentru conexiunile/deconectările dispozitivelor mobile și operațiunile de fișiere pe dispozitivele mobile;
- Integrarea bazei de date utilizator/grup cu Active Directory pentru gestionarea eficientă a utilizatorilor;
- Protecție automată împotriva virusurilor instalate de pe stick-uri USB sau discuri de stocare externe în rețeaua companiei;
- Criptarea la distanță a discului folosind BitLocker pe Agenți cu versiunea Windows Professional sau superioară;
- Criptare sigură la distanță a discului cu BitLocker, salvând cheia de recuperare atât ca fișier, cât și ca activ în consolă;
- Informații despre software-ul antivirus terț instalat în afara Windows Defender.

3.2. La nivelul modulului de monitorizare a eficienței/optimizării timpului utilizatorilor, soluția trebuie să ofere următoarele funcționalități::

- Acces la statisticile activității proprii pentru o zi selectată.
- Accesul managerului la indicatorii de activitate pentru subordonați și echipele selectate.
- Verificarea timpului petrecut în fața calculatorului și departe de acesta.
- Listă cu cele mai populare site-uri și aplicații, cu numărul de minute petrecute pe acestea.
- Indicator al timpului dedicat activităților productive, neproductive și neutre.
- Moduri de vizualizare cu temă luminată și întunecată.
- Vizualizarea tuturor aplicațiilor utilizate de angajat într-un interval de timp selectat.
- Posibilitatea de a împărți angajații în diferite grupuri și de a măsura eficacitatea întregilor echipe.
- Asignarea independentă a statuturilor la activități - productive, neproductive, neutre.
- Adăugarea excepțiilor pentru grupuri sau angajați individual.
- Listă cu contactele angajaților cu un motor de căutare încorporat.
- Definirea pragului de productivitate și limita de neproductivitate.
- Alerte pentru depășirea limitei de neproductivitate sau neatingerea pragului necesar.
- Timp privat - posibilitatea dezactivării funcției de analiză a activității atunci când se utilizează un computer de serviciu în scopuri private.

B. <u>Soluție de prevenire a scurgerilor de date pentru 100 de utilizatori</u>

Cerințe funcționale
privind achiziția soluției de securitate de tip Data Loss Prevention

Scopul prezentului caiet de sarcini constă în organizarea procedurii de achiziție, implementare și mentenanță a soluției de securitate de tip DLP (Data Loss Prevention).

1. Cerințe tehnice minime față de soluția propusă:

Soluția trebuie sa poată rula cel puțin pe:

- Windows 11 Version 21H2, 22H2, 23H2, 64-bit
- Windows 10 Enterprise si Professional, 32-bit si 64-bit
- Windows Server 2008, 2008R2, 2012, 2012R2, 2016, 2019, 2022
- macOS Catalina
- macOS Sonoma
- macOS Ventura
- macOS Monterey
- macOS Bug Sur
- macOS Mojave

- Soluția trebuie sa fie de tip On-Premise, perpetuă, cu mentenanța si suportul pentru 12 luni;
- Soluția suporta următoarele soluții de tip directory: Microsoft AD si Open LDAP;
- Soluția este capabila sa tina evidenta unui număr de peste 500 de milioane de semnături ale fișierelor clasificate pe un singur server si posibilitatea de a instala un număr nelimitat de repositoare;
- Soluția aplica politici bazate pe conținut confidențial pentru cel puțin 300 de tipuri de fișiere.;
- Soluția trebuie sa facă clasificarea conținutului chiar daca acesta este arhivat si trebuie de asemenea sa suporte "nesting" (ex: arhiva zip in interiorul unei alte arhive zip);
- Soluția trebuie sa suporte detectarea documentelor înregistrate/amprentate si clasificate. Descrieți sursele pe care le poate folosi;
- Soluția trebuie sa aibă capabilitatea de a proteja datele bazandu-se pe punctul lor de origine/creare;
- Soluția trebuie sa fie capabila de a atribui in mod automat taguri fișierelor clasificate. Aceste taguri trebuie sa fie utilizabile de aplicații third-party si alte aplicatii DLP;
- Soluția este capabila sa analizeze conținut si sa aplice politici, indiferent de limba utilizata;
- Soluția trebuie sa fie capabila sa scaneze si sa găsească conținut sensibil pe discul local al endpoint-ului;
- Agentul trebuie sa aibă capabilități de analiza de conținut si blocare pentru mediile optice;
- Soluția trebuie sa folosească mai puțin de 5% din procesor in cazul utilizarii intense si gradul de utilizare medie este maxim 2% in timpul funcționarii normale;
- Soluția trebuie sa poată proteja informația confidențială care poate fi:
  - scrisa pe USB/optice
  - trimisa pe mail
  - uploadata pe web
  - copiata cu ajutorul clipboardului
  - printata in fișier sau pe imprimanta
  - scrisa pe un share in rețea
  - folosita in aplicațiile network – based
  - Incarcata in cloud
  - Copiata prin comanda de printscreen
- Soluția trebuie sa ofere același nivel de protecție si in SafeMode;
- Soluția trebuie sa fie capabila sa facă analiza de conținut local, fără a folosi vreo alta componenta a soluției;
- Soluția permite auditarea funcționalității agentului de endpoint;
- Soluția trebuie sa permită dezinstalarea agentului in mod centralizat sau in urma unui challenge/response;
- Soluția trebuie sa aibă un mecanism propriu de instalare a agenților pe stațiile de lucru sau alte sisteme;

- Soluția pentru endpoint-uri are capabilități de clasificare diverse ce nu depind de limbajul folosit: analiza pe termeni/cuvinte cheie, regex-uri si scor de risc, etc.
- Agentul de endpoint trebuie sa fie compatibil, determinat prin testări, cu soluții de antivirus, firewall, criptare backup si antispyware third-party (de ex: Kaspersky, Trellix, Norton, OSCE, Zonelab, GuardianEdge, Credant, Safeguard, Ironkey, Acronis, Spybot, Adaware,Bitdefender);
- Agentul de endpoint trebuie sa permită aplicarea politicilor folosind conținut înregistrat/ amprentat;
- Soluția trebuie sa permită realizarea unui proces de justificare costumizabil, in cazul in care utilizatorul transmite conținut confidențial;
- Soluția trebuie sa permită utilizatorilor sa devina "stakeholderi" pe un caz/eveniment, ori din inițiativa acestora ori asignata de administrator;
- Soluția trebuie sa fie capabila sa blocheze dispozitivele mobile sau sa permită accesul al ele doar de tip read-only sau sa permită doar încărcarea dispozitivelor mobile nu si accesarea acestora;
- Soluția trebuie sa poată realiza reguli de protecție care sa aibă ca si criteriu cuvinte-cheie;
- Soluția trebuie sa poată realiza reguli de protecție care sa aibă ca si criteriu regex-uri;
- Soluția trebuie sa poată realiza reguli de protecție care sa aibă ca si criteriu amprenta (hash-uri);
- Soluția trebuie sa poată realiza reguli de protecție care sa aibă ca si criteriu reguli de proximitate intre alte doua reguli (de tip keyword, dicționar sau regex);
- Construcția regulilor trebuie sa includă support pentru logica booleana incluzând AND, OR, sau alte declarații logice;
- Soluția trebuie sa permită setarea unui threshold astfel încât o regula sa nu fie activata decât după găsirea unui anumit număr de matchuri;
- Soluția trebuie sa fie capabila sa aplice următoarele acțiuni: blocare, monitorizare, notificare utilizator, menținere evidenta, criptare sau aplicarea de etichete;
- Soluția trebui sa aibă capabilitatea de a se integra cu soft de criptare 3rd party, pentru a realiza aplicarea politicilor de criptare in funcție de conținut;
- Soluția trebuie sa permită "whitelist-area" de conținut, dispozitive, procese si utilizatori/grupuri de utilizatori din regulile de protecție;

- Soluția trebuie sa permită salvarea conținutului ce a declanșat o regula de protecția ca "evidence". Aceste date salvate trebuie sa fie recunoscute in instanță ca fiind dovezi valide;

- Soluția trebuie sa aibă abilitatea de a identifica fișierele bazandu-se pe conceptul de true file type si nu doar pe extensia fișierelor;

- Soluția trebuie sa dispună de integrare nativa cu serviciu de tip CASB pentru aplicarea acelorași reguli de protecție DLP si pe resurse manipulate in cloud;

- Soluția trebuie sa aibă abilitatea de a face discovery local. De asemenea ea trebuie sa poată conține si o opțiune de remediere;
- Soluția trebuie sa fie capabila sa aplice reguli de protecție atât la nivel de grupuri /useri definiți in Active Directory cat si pentru userii locali ai sistemelor;
- Soluția trebuie sa fie capabila sa aplice regulile de control al perifericelor chiar si atunci când nu este conectat la rețeaua companiei;
- Soluția are abilitatea de a face discovery in interiorul arhivelor de e-mail stocate pe endpoint;
- Soluția trebuie sa permită customizarea notificărilor emise in timpul funcționarii si a ferestrei in care sunt scrise aceste notificări;
- Soluția trebuie sa fie capabila sa identifice nivelul de clasificare a documentelor din marcajele vizuale si sa aplice regulile de protecție pe aceste documente;
- Soluția trebuie sa fie capabila sa protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale;

- Soluția trebuie sa fie capabila sa comunice cu alte componente de rețea prin protocol Open DXL pentru blocarea încercărilor de exfiltrare de date din cadrul infrastructurii;
- Soluția trebuie sa permită clasificarea manuala a fișierelor, intr-un mod granular asignat pe grupuri, OU-uri sau useri de AD;
- Soluția trebuie sa permită managementul incidentelor si cazurilor in mod granular si sa permită asignarea de useri pe acestea;
- Soluția trebuie sa permită obfuscarea câmpurilor sensibile ale incidentelor raportate, in funcție de utilizator si setul de permisiuni al acestuia;
- Soluția trebuie sa includă componente la nivel de rețea pentru scanarea si aplicarea regulilor de protecție DLP care sa funcționeze pentru "Data-in-motion" si "Data-at-rest";
Componentele soluției trebuie sa poată fi instalate atât sub forma de server fizic cat si intr-un mediu virtual de tipul VMware si Hyper-V;
- Soluția trebuie sa permită aplicarea aceleași politici DLP a clientului de endpoint si pe componentele de rețea, pentru simplificarea workflow-ului si reducerea complexității politicilor;
- Soluția trebuie sa se poată integra atât cu produse precum servere MTA pentru scanarea traficului de email dar si cu orice router, proxy, webgateway, etc cu funcționalitate de ICAP pentru scanarea traficului de tip WEB;
- Soluția trebuie sa permită integrarea cu cel puțin o soluție de tip MDM pentru analiza traficului de email al dispozitivelor mobile;
- Soluția trebuie sa poată scana "Data-at-rest" aflata pe file shares, baze de date cat si servicii cloud si sa poată rula acțiuni de remediere asupra datelor găsite, precum copiere, mutare, criptare, aplicare politica Microsoft Rights Management;
- Soluția trebuie sa permită scanarea imaginilor si fișierelor grafice pentru depistarea datelor senzitive din cadrul acestora, folosind o tehnologie de extragere a caracterelor prin recunoaștere optica;
- Soluția trebuie sa permită captura traficului de tip web, email sau de rețea pentru analiza retroactiva si identificarea eventualelor date care poate ar fi trebuit blocate dar nu au fost. In cazul in care se găsesc astfel de date, soluția trebuie sa poată genera un incident DLP si sa salveze evidence al evenimentului care sa poată fi folosit in instanță;
- Soluția trebuie sa permită scanarea de documente senzitive si generarea de semnături bazate pe acestea si folosind un algoritm si un threshold prestabilit de administrator, sa poată detecta documente asemănătoare fără a se baza pe cuvinte cheie, expresii regulate, etc.
- Soluția trebuie sa suporte generarea de definiții, grupuri de device-uri, template-uri dar si importarea si aplicarea de politici si definiții folosind scripturi de REST API indiferent de limbajul de programare folosit pentru scrierea acestora;
- Soluția trebuie sa dispună de o interfață de monitorizare, integrata nativ in consola de management centralizata, care sa permită vizualizarea statusului de sănătate si statistici de trafic al echipamentelor DLP de rețea;
- Soluția trebuie sa suporte Exact Data matching;
- Soluția trebuie sa poată recunoaște conținut clasificat din imagini si la nivelul de "Data-in-motion";
- Soluția trebuie sa poată reconstrui pachetele încărcate in format "HTTP/1.1 multipart POST", de aplicatii precum Box, pentru a obține fișierul original încărcat si a permite scanarea acestuia;

2. Cerințe tehnice față de Consola de administrare:

Consola de administrare trebuie sa se poată instala pe unul din următoarele sisteme de operare pe 64 de biti:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 Release 2 (R2)
- Microsoft Windows Server 2012
- Windows Server 2008 SP2 Standard, Enterprise, Datacenter
- Windows Server 2008 R2 Standard, Enterprise, Datacenter

- Consola permite pe lângă distribuirea componentelor native si împachetarea aplicațiilor de la terți si instalarea acestora pe stațiile de lucru;
- Consola de management trebuie sa stie sa administreze si alte solutii pe linga DLP precum:solutii de log management, antivirus, Web protection sau protectia bazelor de date, in ideea de a putea avea o tehnologie unificata si un singur punct de suport.
- Consola permite atribuirea automata a politicilor pe stații si servere in funcție de specificațiile sistemului. (Ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare);
Sincronizarea dintre server si client trebuie sa se facă atât dinspre client către server, cat si invers;
- Consola de administrare trebuie sa se poată integra cu Active Directory;
- Consola de administrare trebuie sa poată fi instalata intr-un mediu virtual;
- Consola trebuie sa poate fi instalata in mediu Microsoft Cluster;
- Consola de administrare trebuie sa folosească Microsoft SQL.;
- Consola de administrare permite instalarea unei componente de comunicare in DMZ pentru a putea permite sincronizarea sistemelor prin internet;
- Comunicarea cu serverul de administrare trebuie sa se facă prin intermediul unui singur agent;
- Soluția trebuie sa permită filtrarea evenimentelor ce sunt generate de componentele aflate pe stațiile de lucru astfel încât baza de date sa nu se încarce cu informații considerate inutile;
- Soluția trebuie sa permită configurare unui mesaj de login;
- Soluția poate folosi un proxy pentru contactarea serverului de actualizare al producătorului;
- Accesul in consola de administrare poate fi făcut pe baza credentialelor din Active Directory;
- Accesul in consola de management poate fi făcut pe baza certificatelor x509;
- Consola de administrare trebuie sa permită creare de roluri in mod granular pentru cei ce o administrează;
- Acțiunile utilizatorilor in consola trebuiesc audiate;
- Consola trebuie sa permită construirea unei liste de contacte in vederea folosirii acestora pentru notificări prin mesagerie electronica (E-mail);
- Canalul de comunicație dintre serverul de administrare si componentele distribuite pe calculatoare trebuie sa fie criptat;
- Componenta ce asigura canalul de comunicație dintre server si stații de lucru trebuie sa fie validată din punct de vedere al securității. (Ex: FIPS, Common Criteria, Etc.);
- Canalul de comunicație dintre consola si cei ce o accesează trebuie sa fie criptat;
- Consola de administrare trebuie sa poată fi accesata de pe orice computer din rețea in mod securizat, fără necesitatea instalării de software adițional;

- Daca serverul de administrare este accesat prin intermediul unei interfețe web trebuie sa fie posibil importul unui certificat ssl generat de o autoritate locala, înlocuind astfel pe cel auto-generat;
- Intervalul de sincronizare intre server si componente poate fi modificat;
- Intervalul de transmitere a evenimentelor de pe client către server poate fi modificat;
- Consola trebuie sa poată detecta prezenta pe rețea a sistemelor noi apărute prin intermediul unor senzori;

- Consola trebuie sa folosească un propriu index pentru a identifica si actualiza datele despre sistemele care își schimba proprietăți precum nume ip si configurație hardware;
- Consola permite automatizarea de sarcini de instalare/dezinstalare a componentelor pe stațiile de lucru, de rulare a rapoartelor si de transmiterea de notificări de prin mesagerie electronica;
- Consola trebuie sa prezinte cel puțin următoarele informații despre sistemele administrate: numele sistemului, utilizatorul logat, produsele instalate, tipul de system de operare, adresa IP, componentele hardware ale sistemului etc;
- Consola trebuie sa se integreze cu sisteme de ticketing extern precum BMC Remedy si HP OpenView.;
Serverul de administrare trebuie sa fie capabil sa declanșeze acțiuni automate atunci când anumite condiții sunt îndeplinite (Ex: Generarea unui eveniment pe server, pe o stație de lucru, detectarea unui nou sistem pe rețea);
- Consola trebuie sa permite aplicarea de politici diferite pentru sisteme pe:
    - Sisteme individuale;
    - Grupuri de sisteme;

- Sisteme din AD ce sunt același OU;

- Consola trebuie sa știe sa lanseze automat aplicatii externe si sa injecteze parametrii din evenimente;
- Consola permite accesarea logului componentei de sincronizare de pe sisteme in timp real prin intermediul unui serviciu web;
- Consola trebuie sa aibă capabilități de diagnoza si sa ofere recomandări si soluții pentru problemele detectate;

3. Cerințe față de Raportare

- Consola de administrare poate asigura generarea de rapoarte despre nodurile administrate si despre evenimentele generate de ele;
- Consola trebuie sa permită crearea de noi rapoarte in mod granular cu informații extrase din evenimente, sau despre sistemele administrate;
- Rapoartele pot if generate sub forma de tabel, pie chart, buble chart, lista, sumar, sau grafic istoric;
- Rapoartele pot fi exportate in format pdf, csv, html.;
- Rapoartele pot fi personalizate cu logo-ul companiei;
- Rapoartele pot fi salvate ca fișiere sau trimise prin e-mail;
- Rapoartele pot fi exportate intr-un format arhivat pentru conservare de lățime de banda si expediate automat pe e-mail unor destinații presetate;
- Consola permite evaluarea si filtrarea evenimentelor primite de la stațiile de lucru pentru o mai buna identificare a informațiilor relevante;
- Se pot genera rapoarte utilizând:
    - Logul de audit administrative
    - Detalii despre sistemele administrate (Detalii de configurare, hardware, utilizator)
    - Evenimente de la sisteme
    - Informații despre politicile si sarcinile aplicate sistemelor
    - Informații furnizate de senzori

C. <u>Soluție de marcare și clasificare a informațiilor/documentelor și a mesageriei electronice pentru un numar de 100 utilizatori.</u>

Soluția ofertată trebuie să fie bazată pe un produs software matur de tip off-the-shelf (COTS) de tip On-Premise, perpetuă, cu mentenanța si suportul pentru 12 luni. Nu se acceptă produse software care urmează a fi dezvoltate pentru prezentul proiect. Nu se acceptă produse software de tip open-source sau similare.

Soluția trebuie să ofere următoarele funcționalității descrise mai jos:

1. Cerințe generale:

- Soluția trebuie să ofere posibilitatea de aplicare a unor marcaje specifice vizuale și metadate pentru MS Office(Word, Excel, PowerPoint), MS Outlook, MS Project, MS Visio, (aplicații existente în cadrul instituției);
- Soluția trebuie să ofere posibilitatea de aplicare de metadate persistente pentru fișiere de tip: Open Office file; PDF, JPEG, PNG, TIFF and other image files; MSG and EML email files; ZIP file; DWG and DXF CAD files; HTML file; inclusiv sa asigure clasificarea pentru fișiere care nu suportă metadate;
- Soluția trebuie să necesite cerințele de infrastructură minime, de ex. nu necesită database technology și politicile să fie posibil de distribuit prin fișier;
- Soluția trebuie să suporte Multiple site deployments;

2. Cerințe față de Interfața cu utilizatorul:

- Soluția trebuie să permită selectarea etichetei de clasificare, prin intermediul butonului de pe toolbar și a panoului de selecție;

- Soluția trebuie să ofere posibilitatea de a alege mai multe valori de clasificare (selecții multiple);
- Soluția trebuie să ofere posibilitatea de a aplica mai multe etichete cu un singur click;
- Soluția trebuie să solicite automat și obligatoriu utilizatorului selectarea unei etichete de clasificare prin intermediul unei ferestre de dialog (de selecție);
- Soluția trebuie să furnizeze o metodă sensibilă la context pentru a ghida (sugera) clasificarea;
- Soluția trebuie să afișeze clasificarea unui e-mail primit în bara de instrumente și în panoul de selecție;
- Soluția trebuie să afișeze clasificare a unui document în bara de instrumente și în panoul de selecție;
- Soluția trebuie să permită utilizatorilor să clasifice un e-mail sau un document cu un singur click de mouse (sa permită one-click classification);
- Soluția trebuie sa asigure că utilizatorii sunt avertizați despre atribuirea unei alte clasificări mai mici decât cea inițiala acordată;
- Soluția trebuie sa asigure controlul tipării documentelor pe baza clasificării și a contextului;
- Soluția trebuie să furnizeze ajutor contextual, personalizabil, pentru clasificarea în Office (aplicație existentă în cadrul instituției);
- Soluţia trebuie să ofere capacitatea de a forța clasificarea documentului înainte de a-l salva sau imprima.

3. Cerințe față de Aplicarea Marcajelor pe fișiere:

- Soluţia trebuie să suporte introducerea de marcaje vizuale specifice clasificării în antetul şi subsolul unui fișier;
- Soluţia trebuie să sprijine introducerea unei inscripționări de tip watermark specifică unei clasificări minim într-un document Word/PDF (aplicație existentă în cadrul instituției);
- Soluția trebuie sa suporte aplicarea marcajului unui fișier de tip(image marking, text box marking, field code marking);
- Soluția trebuie sa suporte aplicarea de metadate persistente unui fișier;
- Soluția trebuie sa asigure clasificarea fișierelor care nu suportă metadate(TXT, CSV..etc);

4. Cerințe față de integrarea soluției de clasificare cu E-mail:

- Soluția trebuie să furnizeze ajutor contextual, personalizabil, pentru clasificarea în MS Outlook(aplicație existentă în cadrul instituției);
- Soluția trebuie sa asigure că un e-mail fiind clasificat, destinatarii și inițiatorul sunt verificați automat la procesul de trimitere pentru a asigura conformitatea - de ex. pentru a preveni un e-mail marcat „intern” să fie trimis în exterior;
- Soluția trebuie să ofere sprijin pentru auto-completarea categoriei din Outlook bazat pe clasificare;
- Soluția trebuie să asigure verificarea fișierelor atașate pentru a se asigura că sunt clasificate, iar clasificarea lor nu a expirat;
- Soluția trebuie să ofere posibilitatea verificării individuale a tuturor destinatarilor în concordanță cu valorile atributelor, cum ar fi cele din Active Directory;
- Soluția trebuie să suporte capacitatea de a restricționa destinatarii unui mesaj e-mail în Outlook pe bază atât a clasificării mesajul cât și a valorilor atributului destinatar sau calității de membru în grupul Active Directory;
- Soluția trebuie să ofere capacitatea de a insera marcaje vizuale, în prima linie a unui mesaj de e-mail;
- Soluția trebuie să ofere capacitatea de a insera marcaje vizuale în ultimul rând al unui mesaj de e-mail;

- Soluția trebuie să ofere capacitatea de a insera marcaje vizuale în X-Header a unui e-mail;
- Soluția trebuie să ofere posibilitatea de introducere de marcaje vizuale de clasificare în linia de subiect a unui mesaj de e-mail ca un prefix sau sufix la textul subiect;
- Soluția trebuie să ofere posibilitatea de control a 'Read receipts';
- Soluția trebuie să ofere posibilitatea de modificare a importanței sau sensibilității unui e-mail;
- Soluţia trebuie să ofere capacitatea de a avertiza şi, opţional, a preveni trimiterea unui mesaj de e-mail în cazul în care clasificarea este dowgraded la momentul Reply sau Forward;
- Soluţia trebuie să ofere capacitatea de a avertiza şi, opţional, împiedica expedierea în cazul în care clasificarea este schimbata la momentul Reply sau Forward în Outlook;
- Soluţia trebuie să ofere capacitatea de a forța clasificarea mesajului;
- Soluţia trebuie să ofere posibilitatea de a bloca expedierea accidentală de către utilizatori a mesajelor neclasificate;
- Soluţia trebuie să ofere posibilitatea de a sugera sau impune clasificarea în funcție de criteriile promovate în cadrul companiei, departamente, locație sau conținutul fișierelor;
- Soluţia trebuie să ofere posibilitatea de a impune clasificarea unui document creat extern, în momentul salvării sau printării;
- Soluția trebuie să ofere capacitatea de a detecta conținutul în fișier și sugera, sau impune clasificarea;

5. Cerințe față de protejarea Metadatelor pentru a nu fi modificate de către utilizatori:

- Soluția trebuie sa asigure că metadatele sunt persistente - orice metadată eliminată va fi re-aplicată atunci când fișierul este salvat, tipărit sau expediat prin e-mail;
- Soluţia trebuie să ofere posibilitatea de avertizare a utilizatorilor despre modificarea nivelului de clasificare;
- Soluţia trebuie să ofere posibilitatea de înregistrare a detaliilor despre utilizatorul care a clasificat un fișier;
- Soluţia trebuie să ofere posibilitatea de înregistrare a modificărilor, ex. dacă unui utilizator i se permite să schimbe clasificarea, această modificare va fi înregistrată;

6. Cerințe față de Politici:

Managementul Politicilor:

- Soluţia trebuie să ofere posibilitatea de creare a unui număr nelimitat de politici și existența unui instrument de gestionare simplu în care politicile vor putea fi create, editate și modificate prin intermediul unui asistent(wizard);
- Soluția trebuie să poată furniza un număr nelimitat de nivele de clasificare, care sa poată defini și impune politica de confidențialitate a instituției. Marcajele definite trebuie să fie personalizabile în Outlook și Office (aplicație existentă în cadrul instituției);
- Soluţia trebuie să ofere posibilitatea de adaptare a politicilor cu o gamă largă de atribute - de exemplu, atribute Active Directory;
- Soluţia trebuie să ofere posibilitatea ca politicile să fie adaptate pentru diferite departamente sau ierarhie - de ex. numai managerii pot face downgrade la o clasificare;

7. Interoperabilitate:

- Soluţia trebuie să ofere posibilitatea de a ataşa metadate la documentele Office (aplicație existent în cadrul instituției), astfel încât aceste metadata de clasificare să poată fi utilizate de solutia DLP (Data Loss Prevention) ofertata conform cerințelor la Capitolul III, la **p. 2 (Soluție de prevenire a scurgerilor de date)** din prezentul caiet de sarcini.

- Soluţia trebuie să asigure interoperabilitate cu soluții precum:
    - Monitoring, reporting și analytics;
    - Rights Management;
    - Access Control;
    - Email Filtering;
    - Secure Email.
- Soluția trebuie să fie compatibilă cu următoarele sisteme de operare:
    - De la Windows 7 și mai sus;
    - De la Microsoft Office 2007 SP3 și mai sus;
    - De la SharePoint 2010 și mai sus;
    - De la OWA 2010 și mai sus;
    - De la Exchange 2010 și mai sus;

IV. ALTE CERINȚE OBLIGATORII PENTRU OFERTANȚI:

- Pentru toate soluțiile ofertate se solicită a fi inclusă 12 luni suport local și de la producător.
- Lucrările de instalare, configurare, integrare, punerea în funcțiune a soluțiilor ofertate trebuie să fie executate de ofertantul rezident în Republica Moldova, iar costul acestora trebuie să fie incluse în oferta comercială;
- Pentru platforma de securitate ofertata, ofertantul câștigător va prezenta un plan de implementare, configurare, creare de politici si reguli de securitate, de testare in zona de test si trecerea al acesteia producție. Costurile acestora vor fi incluse in preț.
- Producătorii soluțiilor ofertate trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului;
- Prezentarea a minim 1 certificat tehnic a personalului calificat pe fiecare din soluțiile ofertate.
- Ofertantul va prezenta copia Certificatului ISO 27001:2018, in domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea si managementul infrastructurii IT si de securitate, certificat confirmat cu aplicarea semnăturii electronice;
- Ofertantul va prezenta Autorizarea de la producător pentru fiecare din soluțiile ofertate pentru aceasta licitație;
- Ofertantul va prezenta minim 1 referință de implementare a soluțiilor ofertate pe piața locală în ultimii 3 ani.

Digitally signed by Arion Victor
Date: 2024.05.07 15:02:51 EEST
Reason: MoldSign Signature
Location: Moldova

Digitally signed by Codreanu Vadim
Date: 2024.05.14 09:44:26 EEST
Reason: MoldSign Signature
Location: Moldova