



DIRECȚIA FONDURI EXTERNE NERAMBURSABILE
Nr. M6-974 / 16.10.2025

APROBAT,

Marian-Mihail Tache,

Director

TACHE
MARIAN
-MIHAIL

Digitally signed
by TACHE
MARIAN-MIHAIL
Date: 2025.10.16
12:22:30 +03'00'

CAIET DE SARCINI

aferent proiectului

***Creșterea nivelului de protecție a datelor cu caracter personal procesate prin intermediul
SNIV/E-VISA***

Codurile CPV aplicabile achiziției sunt:

Cod CPV principal:

- ❖ 48732000-8 - Pachete software pentru securitatea datelor (Rev. 2)

Cod CPV secundar:

- ❖ 32420000-3: Echipament de rețea (Rev. 2)

Cod proiect	BV22B_01_Protecție GDPR
Fondul	IMFV Instrumentul pentru managementul frontierei și politica de vize
Programul național (nr. CCI)	Programul național 2021-2027 Managementul frontierelor și vize 2021RO65BVPR001
Obiectivul specific	OS2 Sprijinirea politicii comune a vizelor pentru a asigura o abordare armonizată cu privire la eliberarea vizelor și pentru a facilita călătoriile în scopuri legitime, contribuind în același timp la prevenirea riscurilor în materie de migrație și riscurilor pentru securitate.
Măsura de intervenție PN	OS2.2 Instituirea, dezvoltarea și optimizarea sistemelor TIC în domeniul politicii comune a vizelor, inclusiv interoperabilitatea și infrastructura asociată acestora



Cuprins:

1	INTRODUCERE	4
2	CONTEXTUL REALIZĂRII ACESTEI ACHIZIȚII LOTIZATE DE PRODUSE	4
2.1	INFORMAȚII DESPRE AUTORITATEA CONTRACTANTĂ	4
2.2	INFORMAȚII DESPRE CONTEXTUL CARE A DETERMINAT ACHIZIȚIONAREA PRODUSELOR ȘI SERVICIILOR	5
2.3	INFORMAȚII DESPRE BENEFICIILE ANTICIPATE DE CĂTRE AUTORITATEA CONTRACTANTĂ	5
2.4	ALTE INIȚIATIVE/PROIECTE/PROGRAME ASOCIATE CU ACEASTĂ ACHIZIȚIE DE PRODUSE	6
2.5	CADRUL GENERAL AL SECTORULUI ÎN CARE AUTORITATEA CONTRACTANTĂ ÎȘI DESFĂȘOARĂ ACTIVITATEA	6
2.6	FACTORI INTERESAȚI ȘI ROLUL ACESTORA	7
3	PRODUSELE SOLICITATE	8
3.1	OBIECTIVUL GENERAL LA CARE CONTRIBUIE FURNIZAREA PRODUSELOR	8
3.2	OBIECTIVUL SPECIFIC LA CARE CONTRIBUIE ACHIZIȚIA DE PRODUSE	8
3.3	DESCRIEREA PRODUSELOR ȘI OPERAȚIUNILE CU TITLU ACCESORIU NECESAR A FI REALIZATE	9
3.3.1	LOTUL I: SOLUȚIE DE DETECȚIE AVANSATĂ ÎMPOTRIVA AMENINȚĂRILOR CIBERNETICE (APT)	9
3.3.1.1	OPERAȚIUNILE CU TITLU ACCESORIU, NECESAR A FI REALIZATE	9
3.3.2	LOTUL II: SOLUȚIE PENTRU MANAGEMENT CENTRALIZAT A INCIDENTELOR DE SECURITATE (SIEM)	10
3.3.2.1	OPERAȚIUNILE CU TITLU ACCESORIU, NECESAR A FI REALIZATE	10
3.3.3	LOTUL III: SOLUȚIE DE CONTROL A DISPOZITIVELOR (DEVICE CONTROL)	11
3.3.3.1	OPERAȚIUNILE CU TITLU ACCESORIU, NECESAR A FI REALIZATE	11
3.3.4	LOTUL IV: SOLUȚIE DE CONTROL A ACCESULUI ÎN REȚELE (NAC)	12
3.3.4.1	OPERAȚIUNILE CU TITLU ACCESORIU, NECESAR A FI REALIZATE	12
3.4	GARANȚIE / TERMEN DE VALABILITATE	13
3.5	LIVRARE, AMBALARE, ETICHETARE, TRANSPORT	15
3.6	INSTALARE, PUNERE ÎN FUNCȚIUNE, TESTARE	16
3.7	INSTRUIRE PERSONAL	16
3.8	MENTENANȚA PREVENTIVĂ ÎN PERIOADA DE GARANȚIE	17
3.9	MENTENANȚA CORECTIVĂ ÎN PERIOADA POST-GARANȚIE, DUPĂ CAZ	18
3.10	SUPOORT TEHNIC	18
3.11	MEDIUL ÎN CARE ESTE OPERAT PRODUSUL	20
4	ATRIBUȚIILE ȘI RESPONSABILITĂȚILE PĂRȚILOR	20
5	DOCUMENTAȚII CE TREBUIE FURNIZATE AUTORITĂȚII CONTRACTANTE ÎN LEGĂTURĂ CU ACHIZIȚIA	20
6	RECEPȚIA PRODUSELOR AFERENTE LOTURILOR I-IV	21
7	EVALUAREA PERFORMANȚEI CONTRACTANTULUI	22
8	MODALITĂȚI ȘI CONDIȚII DE PLATĂ	24
9	CADRUL LEGAL CARE GUVERNEAZĂ RELAȚIA DINTRE AUTORITATEA CONTRACTANTĂ ȘI CONTRACTANT (INCLUSIV ÎN DOMENIILE MEDIULUI, SOCIAL ȘI AL RELAȚIILOR DE MUNCĂ)	24
10	MANAGEMENTUL / GESTIONAREA CONTRACTULUI ȘI ACTIVITĂȚI DE RAPORTARE ÎN CADRUL CONTRACTULUI, AFERENTE CELOR PATRU LOTURI	25



MINISTERUL AFACERILOR EXTERNE

10.1	GESTIONAREA RELAȚIEI DINTRE OFERTANT ȘI AUTORITATEA CONTRACTANTĂ.....	25
10.2	ASIGURAREA MANAGEMENTULUI DE PROIECT	25
10.3	RAPOARTELE/DOCUMENTELE SOLICITATE DE LA OFERTANT	26
10.4	LIVRABILE ȘI ACCEPTANȚA ACESTORA.....	26
10.5	IPOTEZE ȘI RISCURI.....	27
11	OFERTARE.....	28
11.1	MODUL DE ORGANIZARE AL OFERTEI.....	28
11.2	PLAN DE LUCRU PENTRU ACTIVITĂȚILE/SERVICIILE SOLICITATE.....	29
11.3	PROPUNEREA TEHNICĂ.....	29
11.4	PROPUNEREA FINANCIARĂ.....	30
12	ANEXE.....	30
12.1	ANEXA 1 - SPECIFICAȚII TEHNICE SOLUȚIE APT.....	32
12.2	ANEXA 2 - SPECIFICAȚII TEHNICE SOLUȚIE SIEM.....	40
12.3	ANEXA 3 - SPECIFICAȚII TEHNICE SOLUȚIE DEVICE CONTROL	51
12.4	ANEXA 4 - SPECIFICAȚII TEHNICE SOLUȚIE NAC	55
12.5	ANEXA 5 - ALGORITMUL DE CALCUL AFERENT CRITERIULUI DE ATRIBUIRE.....	67



1 Introducere

Caietul de sarcini face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Caietul de sarcini conține, în mod obligatoriu, specificații tehnice aferente celor patru loturi care fac obiectul procedurii de atribuire. Acestea definesc, după caz și fără a se limita la cele ce urmează, caracteristici referitoare la nivelul calitativ, tehnic și de performanță, siguranța în exploatare, dimensiuni, precum și sisteme de asigurare a calității, terminologie, simboluri, teste și metode de testare, ambalare, etichetare, marcare, condițiile pentru certificarea conformității cu standarde relevante sau altele asemenea. Anexele I – IV ale prezentului Caiet de sarcini detaliază cerințele tehnice minime aferente fiecărui lot în parte.

În cadrul acestei proceduri, Ministerul Afacerilor Externe îndeplinește rolul de autoritate/entitate contractantă, respectiv autoritatea/entitatea contractantă în cadrul Contractului.

Pentru scopul prezentei secțiuni a documentației de atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

Cerințele tehnice definite la nivelul anunțului de participare, caietului de sarcini sau altor documente complementare, prin trimiterea standardelor, la un anumit producător, la mărci, brevete, tipuri, la o origine sau la o producție/metoda specifică de fabricație/prestare/ execuție, vor fi înțelese ca fiind însoțite de mențiunea „sau echivalent”.

2 Contextul realizării acestei achiziții lotizate de produse

Contextul relevant este acela al actualizării tehnologice din punct de vedere al securității IT a infrastructurii IT aferentă sistemelor SNIV/E-VIZA, dezvoltată inițial în anii 2010, la realitățile atacurilor cibernetice posibile ale anului 2025. precum și dezvoltarea unor funcționalități noi privind protecția datelor cu caracter personal.

În acest sens, se are în vedere achiziția lotizată a patru soluții de securitate cibernetică - *soluție de detecție avansată împotriva amenințărilor cibernetice APT, soluție pentru management centralizat a incidentelor de securitate (SIEM), soluție de control a dispozitivelor și soluție de control a accesului în rețele (NAC)* destinate MAE cu scopul creșterii nivelului de protecție a datelor cu caracter personal procesate prin intermediul SNIV/E-VIZA, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

2.1 Informații despre Autoritatea contractantă

Numele autoritate/entitate contractantă: **Ministerul Afacerilor Externe**

Cod de înregistrare fiscală: 4266863

Adresa poștală: Aleea Modrogan nr. 14, sector 1, CP 011826, București;



MINISTERUL AFACERILOR EXTERNE

Adresa oficială de e-mail a instituției: dfen@mae.ro

Web page: www.mae.ro

Ministerul Afacerilor Externe este organizat și funcționează în conformitate cu Hotărârea Guvernului nr. 16 din 2017 privind organizarea și funcționarea Ministerului Afacerilor Externe, cu modificările și completările ulterioare, precum și Hotărârea nr. 9 din 2020 privind modificarea și completarea unor acte normative în domeniul afacerilor externe.

Activitatea ministerului este condusă de ministrul afacerilor externe, care totodată îl reprezintă în raporturile cu celelalte autorități publice, cu persoanele juridice și fizice din țară și din străinătate, precum și în justiție. De asemenea, ministrul afacerilor externe răspunde de întreaga activitate a ministerului în fața Guvernului, precum și, în calitate de membru al Guvernului, în fața Parlamentului.

Misiunea Ministerului Afacerilor Externe este de a asigura realizarea politicii externe a statului român în concordanță cu interesele naționale și cu statutul României de stat membru în structurile europene și euroatlantice.

2.2 Informații despre contextul care a determinat achiziționarea produselor și serviciilor

Ministerul Afacerilor Externe utilizează sistemele SNIV/E-VIZA în scopul gestionării și procesării cererilor de viză ale cetățenilor statelor terțe. Sistemul E-VIZA este interfața cu petenții, utilizat pentru a primi solicitările de viză, ce includ toate datele alfanumerice necesare pentru cererea de viză în sine, precum și copii scanate ale documentelor justificative aferente cererii de viză, pentru prevalidarea și programarea cererilor de viză la consulat. Pe lângă datele cu caracter personal continue în solicitările de viză procesate de MAE în mod curent înainte de aderarea la Schengen, începând cu data aderării cantitatea de date procesate de către MAE a crescut datorită necesității de a procesa datele transmise de celelalte State Membre în aplicarea art. 22 și 31 din Regulamentul (CE) 810/2009 (Codul de Vize), precum și în cadrul comunicațiilor VISMai în conformitate cu prevederile Regulamentului (CE) 767/2008 (Regulamentul VIS).

Protecția datelor este strâns legată de modul în care MAE își gestionează riscurile strategice, operaționale și financiare. Astfel, proiectul vizează creșterea gradului de securitate cibernetică a sistemelor SNIV/E-VISA, precum și a interoperabilității sistemelor de securitate care urmează să fie implementate și integrate cu sistemul informatic existent, prin implementarea următoarelor soluții de securitate: soluție de detecție avansată împotriva amenințărilor cibernetice (APT), soluție pentru management centralizat a incidentelor de securitate (SIEM), soluție de control a dispozitivelor și soluție de control a accesului în rețele (NAC).

2.3 Informații despre beneficiile anticipate de către Autoritatea contractantă

Implementarea proiectului vizează creșterea nivelului de protecție a datelor cu caracter personal accesibile prin intermediul SNIV/E-VISA, inclusiv datele la care MAE urmează să aibă acces



odată cu punerea în funcțiune a sistemului european Entry/Exit System (EES), și a dezvoltărilor ulterioare pe interoperabilitate.

Se așteaptă ca în urma implementării proiectului să se îmbunătățească din punct de vedere calitativ și al securității infrastructura existentă SNIV și a sistemelor aferente.

Prin implementarea acestui proiect se urmărește:

- Eliminarea potențialelor riscuri tehnice și de securitate induse de folosirea unei platforme de virtualizare a căror componente au fost implementate în urmă cu mai mulți ani și pentru care nu există mentenanță activă;
- Eliminarea riscurilor operaționale care pot fi generate de lipsa suportului de la producător;
- Posibilitatea de a realiza îmbunătățiri ale platformei de stocare și replicare date pe măsură ce platforma de virtualizare va fi adusă la ultima versiune tehnologică.

2.4 Alte inițiative/proiecte/programe asociate cu această achiziție de produse:

Proiectul propus vine în continuarea și dezvoltarea altor proiecte derulate de MAE în contextul îndeplinirii condițiilor de eliberare de vize uniforme Schengen și a cooperării cu statele membre Schengen, cât și în scopul punerii în aplicare a prevederilor Regulamentului GDPR Codului Comunitar de Vize și Regulamentului VIS, la nivelul Centrului Național de Vize și MD/OC, respectiv SNIV/E-VIZA și sistemele adiacente acestora, finanțate tot prin fonduri europene nerambursabile precum Facilitatea Schengen, Fondul Frontierelor Externe și FSI-B, astfel:

- RO FSIB 2016 OS1 A01 P01 - „Actualizarea echipamentelor și soluțiilor IT&C existente, în vederea îmbunătățirii parametrilor de funcționare ai Sistemului National de Informații privind Vizele (SNIV)”;
- RO FSIB 2019 OS1 A01 P04 - „Upgrade module funcționale infrastructura SNIV”;
- RO FSIB 2020 OS3 A04 P02 - „Mentenanță infrastructură voce și virtualizare SNIV”.

Proiectul de față vizează dezvoltarea infrastructurii SNIV, inclusiv a interfeței E-VIZA pentru îmbunătățirea activităților necesare prelucrării cererilor de viză și armonizarea acestora cu modificările legislative și procedurale cu incidență asupra activității consulare.

2.5 Cadrul general al sectorului în care Autoritatea contractantă își desfășoară activitatea

Conform prevederilor HG nr. 16 din 2016, Ministerul Afacerilor Externe este organul de specialitate al administrației publice centrale aflat în subordinea Guvernului, care realizează politica externă a statului român, inclusiv prin îndeplinirea sarcinilor din sfera sa de competență care revin României în calitate de stat membru al Uniunii Europene și al Organizației Tratatului Atlanticului de Nord.

În cadrul acestor atribuții, prin Legea nr. 271 din 2010, a fost instituit Sistemul Național de Informații privind Vizele – SNIV. Acesta constituie componenta națională a C-VIS (VIS Central European), la care SNIV urmează a fi conectat odată cu aderarea României la spațiul Schengen.



În calitate de instituție responsabilă cu înființarea, actualizarea și utilizarea sistemului SNIV, MAE adoptă măsurile necesare pentru îndeplinirea atribuțiilor mai sus menționate. Prezenta propunere de proiect se încadrează în categoria măsurilor necesare pentru actualizarea și menținerea în funcțiune la parametri optimi a sistemului SNIV.

În același timp, având în vedere că sistemul C-VIS se dezvoltă și se modernizează permanent conform necesităților statelor membre, proiectele MAE finanțate din FSI (Fondul pentru Securitatea Internă) vor avea ca scop și upgrade-uri periodice ale N-VIS pentru a se asigura alinierea sistemului la evoluțiile C-VIS.

2.6 Factori interesați și rolul acestora

Pentru desfășurarea activităților proiectului, vor fi implicate următoarele departamente din cadrul MAE:

- 1) Departamentul Fonduri Externe Nerambursabile (DFEN), care va asigura managementul proiectului, derulând toate activitățile pentru buna implementare a acestuia;
- 2) Direcția Tehnologia Informației (DTI), care are calitatea de administrator de sistem, sens în care va asigura sprijin în ceea ce privește respectarea caracteristicilor tehnice ale soluțiilor informatice și a compatibilității acestora cu infrastructura existentă;
- 3) Departamentul Consular (DCons), va acorda sprijinul logistic și va asigura comunicarea permanentă cu oficiile consulare;
- 4) Centrul Național de Vize MAE (CNV), în calitate de autoritate centrală competentă în materie de vize va participa la toate fazele specifice ale proiectului asigurându-se că soluțiile informatice software și hardware corespund din punct de vedere funcțional.

Organizarea activităților în cadrul proiectului se va realiza pentru fiecare etapă de implementare a proiectului, cu implicarea resurselor umane existente la nivelul MAE: experți în managementul proiectelor, juridic, financiar, tehnic, achiziții publice, implementare etc.

Numărul membrilor echipei de proiect va fi stabilit ținând cont de funcționalitățile necesare implementării proiectului fiind stabilit prin dispoziție a conducătorului instituției/ordonatorul de credite delegat.

De asemenea, în cadrul proiectului vor avea loc ședințe ale echipei de proiect, în care se va analiza stadiul activităților, riscurile identificate, precum și măsurile propuse pentru reducerea acestora. Comunicarea în cadrul echipei de proiect se va realiza prin organizarea de ședințe de lucru, precum și prin utilizarea mijloacelor electronice de comunicare.

Pentru implementarea proiectului va fi utilizată metodologia PM2, elaborată de Comisia Europeană privind managementul de proiect.



3 Produsele solicitate

3.1 Obiectivul general la care contribuie furnizarea produselor

Proiectul de față are în vedere dezvoltarea capacității operaționale a Ministerului Afacerilor Externe în domeniul politicii de vize, prin asigurarea bunei funcționări a infrastructurii aferente sistemului SNIV și a celei conexe acesteia, conform reglementărilor europene în domeniu.

În cadrul politicii de vize, România are ca scop să sprijine și să extindă capacitatea existentă la nivel național, pentru a asigura aplicarea corectă a acquis-ului Uniunii în ceea ce privește vizele.

Obiectivul general vizează creșterea nivelului de protecție a datelor cu caracter personal accesibile prin intermediul SNIV/E-VISA, inclusiv datele la care MAE urmează să aibă acces odată cu punerea în funcțiune a sistemului european Entry/Exit System (EES) și a dezvoltărilor ulterioare pe interoperabilitate, prin îndeplinirea acțiunilor:

- 1.3.1. Dezvoltarea și modernizarea sistemelor de comunicații și tehnologia informației și a interfețelor specifice de acces, ținând cont de cerințele de compatibilitate și interconectivitate cu sisteme de comunicații naționale și europene, în domeniul ordinii și siguranței publice (inclusiv sisteme precum VIS, SIS II, EURODAC, etc.);
- 1.3.1.9. Modernizarea și dezvoltarea periodică a Sistemului Național de Informații privind Vizele (SNIV) prin implementarea de noi componente hardware și soluții software, din cadrul Strategiei Naționale de Management Integrat al Frontierei de Stat a României 2023 - 2027.

3.2 Obiectivul specific la care contribuie achiziția de produse

Obiectivul specific al proiectului constă în extinderea infrastructurii IT SNIV/E-VIZA, precum și dezvoltarea unor funcționalități noi privind protecția datelor cu caracter personal. În acest sens, se are în vedere achiziția lotizată a 4 (patru) soluții de securitate cibernetică destinate MAE cu scopul creșterii nivelului de protecție a datelor cu caracter personal procesate prin intermediul SNIV/E-VISA, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), astfel:

- 1) **Lotul I** - soluție de detecție avansată împotriva amenințărilor cibernetice (APT) - aceasta reprezintă o platformă de securitate cibernetică care utilizează algoritmi specializați de învățare automată nesupravegheată și analiză comportamentală sau mecanisme complexe de inteligență artificială pentru a monitoriza traficul de date. Aceasta este necesară pentru îndeplinirea cerinței "capacitatea de restabilire rapidă a disponibilității și accesului la datele cu caracter personal în caz de incident fizic sau tehnic";
- 2) **Lotul II** - soluție pentru management centralizat a incidentelor de securitate (SIEM) - aceasta asigură colectarea, corelarea, analiza și raportarea centralizată a evenimentelor de Securitate, Performanță, Disponibilitate și Modificare din infrastructura IT, oferind vizibilitate în timp real, detecție avansată a incidentelor și răspuns automatizat, în scopul



asigurării conformității și protecției proactive a organizației. Aceasta este necesară pentru îndeplinirea cerinței "proceduri de testare, evaluare și apreciere periodică a eficacității măsurilor tehnice și organizatorice pentru a asigura securitatea prelucrării.";

- 3) **Lotul III** - soluție de control a dispozitivelor - aceasta asigură controlul dispozitivelor și gestionarea accesului la fișiere permițând controlul, blocarea și monitorizarea dispozitivelor USB cât și celor periferice pentru a bloca accesul neautorizat la datele sensibile. Aceasta este necesară pentru îndeplinirea cerinței "pseudonimizarea și criptarea datelor cu caracter personal" și măsurile de protecție împotriva prelucrării neautorizate;
- 4) **Lotul IV** - soluție de control a accesului în rețele (NAC) - aceasta asigură principiul de acces zero-trust care supraveghează și protejează toate activele digitale conectate la rețeaua informatică oferind vizibilitate, control și răspuns automat pentru tot ceea ce se conectează la rețea. Aceasta este necesară pentru îndeplinirea cerinței "capacitatea de restabilire rapidă a disponibilității și accesului la datele cu caracter personal în caz de incident fizic sau tehnic".

3.3 Descrierea produselor și operațiunile cu titlu accesoriu necesar a fi realizate:

3.3.1 Lotul I: Soluție de detecție avansată împotriva amenințărilor cibernetice (APT)

Achiziția de echipamente dedicate hardware și produse software preinstalate aferente acestora, care să se integreze în infrastructura IT existentă a sistemelor SNIV/E-VIZA, ce vor beneficia de suport de la producător pentru o perioadă de 5 ani, precum și de servicii de instalare, configurare și punere în funcțiune a soluției.

Soluția APT reprezintă o platformă de securitate cibernetică care utilizează algoritmi specializați de învățare automată nesupravegheată și analiză comportamentală sau mecanisme complexe de inteligență artificială pentru a monitoriza traficul de date din cadrul unei infrastructuri IT&C.

Soluția oferită trebuie să fie capabilă să analizeze și să detecteze atacurile cibernetice avansate (Advanced Persistent Threat) și atacurile cibernetice necunoscute (zero-day). Totodată trebuie să dispună de mecanisme de actualizare în mod offline, fără conexiune la Internet.

Platforma acestuia este formată din 2 senzori specializați, formați din componente hardware și software, care analizează traficul intern și extern existent într-o rețea informatică, astfel:

- a) componenta hardware este reprezentată de serverele fizice care asigură resursele necesare funcționării în parametri optimi a componentei software;
- b) componenta software este cea care conține algoritmi proprietari, mecanismele de învățare automată și analiză comportamentală.

3.3.1.1 Operațiunile cu titlu accesoriu, necesar a fi realizate

Furnizorul va livra toate produsele hardware și software necesare instalării, configurării și funcționării soluției APT.



Furnizorul va instala (monta, configura / reconfigura, seta, integra) și testa soluția APT livrată.

Furnizorul va asigura garanție și suport de la producător pentru o perioadă de 5 ani, conform prevederilor prezentului caiet de sarcini.

Toate cheltuielile ocazionate de remedierea defecțiunilor soluției APT furnizată, incluzând, dar fără a se limita la: preluarea, predarea și transportul de la și la sediul Achizitorului în condițiile menționate mai sus, cad în sarcina Furnizorului.

Furnizorul va asigura instruirea personalului desemnat de Achizitor (minim 3 administratori, pe o perioadă de minim 2 zile lucrătoare), într-o locație stabilită de comun acord pe perioada derulării contractului. Scopul instruirii este de a transfera cunoștințele necesare către Achizitor în vederea asigurării funcționalității soluției rezultate în urma implementării sistemului.

Cerințele tehnice minimale ale soluției de detecție avansată împotriva amenințărilor cibernetice (APT) sunt detaliate în [Anexa 1 - Specificații tehnice Soluție APT](#)

3.3.2 Lotul II: Soluție pentru management centralizat a incidentelor de securitate (SIEM)

Achiziția de produse software dedicate soluției SIEM care să se integreze în infrastructura IT existentă a sistemelor SNIV/E-VIZA, ce vor beneficia de suportul de la producător pentru o perioadă de 5 ani, precum și servicii de instalare, configurare și punere în funcțiune a soluției.

În cadrul sistemului SNIV/E-VIZA, securitatea cibernetică este asigurată prin securizarea rețelei informatice și prin implementarea unui sistem de management centralizat a incidentelor de securitate (SIEM) fiind aplicate următoare tehnici de securizare: prevenție, detecție, investigație și corecție.

Soluția ofertată trebuie să asigure colectarea, corelarea, analiza și raportarea centralizată a evenimentelor de *Securitate, Performanță, Disponibilitate și Modificare* din infrastructura IT, oferind vizibilitate în timp real, detecție avansată a incidentelor și răspuns automatizat, în scopul asigurării conformității și protecției proactive a organizației.

3.3.2.1 Operațiunile cu titlu accesoriu, necesar a fi realizate

Furnizorul va livra toate produsele hardware și software necesare instalării, configurării și funcționării sistemului SIEM.

Furnizorul va instala (monta, configura / reconfigura, seta, integra) și testa soluția SIEM livrată;

Furnizorul va asigura garanție și suport de la producător pentru o perioadă de 5 ani, conform prevederilor prezentului caiet de sarcini.

Toate cheltuielile ocazionate de remedierea defecțiunilor sistemului SIEM furnizat, incluzând, dar fără a se limita la: preluarea, predarea și transportul de la și la sediul Achizitorului în condițiile menționate mai sus, cad în sarcina Furnizorului.

Furnizorul va asigura instruirea personalului desemnat de Achizitor (minim 3 administratori, pe o perioadă de minim 2 zile lucrătoare), într-o locație stabilită de comun acord pe perioada derulării



contractului. Scopul instruirii este de a transfera cunoștințele necesare către Achizitor în vederea asigurării funcționalității soluției rezultate în urma implementării sistemului.

Cerințele tehnice minime ale soluției pentru management centralizat a incidentelor de securitate (SIEM) sunt detaliate în [Anexa 2 - Specificații tehnice Soluție SIEM](#)

3.3.3 Lotul III: Soluție de control a dispozitivelor (Device Control)

Achiziția de produse software dedicate soluției Device Control care să se integreze în infrastructura IT existentă a sistemelor SNIV/E-VIZA, ce vor beneficia de suportul de la producător pentru o perioadă de 5 ani, precum și servicii de instalare, configurare și punere în funcțiune a soluției.

Soluția de control a dispozitivelor vizează controlul dispozitivelor și gestionarea accesului la fișiere permițând controlul, blocarea și monitorizarea dispozitivelor USB cât și celor periferice pentru a bloca accesul neautorizat la datele sensibile.

Soluția oferită asigură blocarea transferului neautorizat de date personale pe dispozitive de stocare externe, monitorizarea și controlul utilizării porturilor USB, CD/DVD și altor medii de stocare, prevenirea infecției sistemelor care prelucrează date personale, carantinarea și dezinfectarea dispozitivelor infectate și implementarea controalelor de securitate de la nivelul infrastructurii.

3.3.3.1 Operațiunile cu titlu accesoriu, necesar a fi realizate

Furnizorul va livra toate produsele hardware și software necesare instalării, configurării și funcționării soluției Device Control.

Furnizorul va instala (monta, configura / reconfigura, seta, integra) și testa soluția Device Control livrată.

Furnizorul va asigura garanție și suport de la producător pentru o perioadă de 5 ani, conform prevederilor prezentului caiet de sarcini.

Toate cheltuielile ocazionate de remedierea defecțiunilor soluției Device Control furnizată, incluzând, dar fără a se limita la: preluarea, predarea și transportul de la și la sediul Achizitorului în condițiile menționate mai sus, cad în sarcina Furnizorului.

Furnizorul va asigura instruirea personalului desemnat de Achizitor (minim 3 administratori, pe o perioadă de minim 2 zile lucrătoare), într-o locație stabilită de comun acord pe perioada derulării contractului. Scopul instruirii este de a transfera cunoștințele necesare către Achizitor în vederea asigurării funcționalității soluției rezultate în urma implementării sistemului.

Cerințele tehnice minime ale soluției de control a dispozitivelor (Device Control) sunt detaliate în [Anexa 3 - Specificații tehnice Soluție Device Control](#)



3.3.4 Lotul IV: Soluție de control a accesului în rețele (NAC)

Achiziția de echipamente dedicate hardware de control acces în rețele, ce includ servicii de instalare, configurare și punere în funcțiune, precum și produse software aferente soluției NAC care să se integreze în infrastructura IT existentă a sistemelor SNIV/E-VIZA, ce vor beneficia de suport de la producător pentru o perioadă de 5 ani. Soluția NAC implementată va include:

- ✓ echipament în format mașină virtuală pentru managementul politicilor de acces și orchestrarea dispozitivelor de rețea;
- ✓ platformă de jurnalizare și analiză a evenimentelor/log-urilor;
- ✓ controlul complet al unui set de switch-uri (400 x 24 porturi și 200 x 48 porturi);
- ✓ 400 bucăți switch 24 porturi gigabit – compatibile funcțional cu soluția NAC;
- ✓ 200 bucăți switch 48 porturi gigabit – compatibile funcțional cu soluția NAC.

Soluția de control a accesului în rețele asigură principiul de acces zero-trust care supraveghează și protejează toate activele digitale conectate la rețeaua informatică oferind vizibilitate, control și răspuns automat pentru tot ceea ce se conectează la rețea.

Soluția oferită asigură analiza comportamentală pentru identificarea activităților anormale, automatizarea răspunsului la amenințările detectate, izolarea rapidă a sistemelor compromise pentru a preveni propagarea atacului, colectarea automată de dovezi pentru investigațiile ulterioare și asigurarea disponibilității datelor pentru subiecții datelor conform drepturilor GDPR.

3.3.4.1 Operațiunile cu titlu accesoriu, necesar a fi realizate

Furnizorul va livra toate produsele hardware și software necesare instalării, configurării și funcționării soluției NAC.

Furnizorul va instala (monta, configura / reconfigura, seta, integra) și testa soluția NAC livrată.

Furnizorul va asigura garanție și suport de la producător pentru o perioadă de 5 ani, conform prevederilor prezentului caiet de sarcini.

Toate cheltuielile ocazionate de remedierea defecțiunilor soluției NAC furnizată, incluzând, dar fără a se limita la: preluarea, predarea și transportul de la și la sediul Achizitorului în condițiile menționate mai sus, cad în sarcina Furnizorului.

Furnizorul va asigura instruirea personalului desemnat de Achizitor (minim 3 administratori, pe o perioadă de minim 2 zile lucrătoare), într-o locație stabilită de comun acord pe perioada derulării contractului. Scopul instruirii este de a transfera cunoștințele necesare către Achizitor în vederea asigurării funcționalității soluției rezultate în urma implementării sistemului.

Cerințele tehnice minimale ale soluției de control a accesului în rețele (NAC) sunt detaliate în [Anexa 4 - Specificații tehnice Soluție NAC](#)



3.4 Garanție / Termen de valabilitate

Perioada de garanție acordată celor 4 soluții achiziționate (APT, SIEM, Device Control și NAC), inclusiv a accesoriilor, este de 5 ani, începând de la data semnării procesului-verbal de recepție cantitativă și calitativă a soluțiilor.

Garanția trebuie să fie asigurată ON-SITE la sediul MAE, să acopere soluțiile integral (inclusiv accesorii, dispozitive de stocare etc.), iar timpul de răspuns trebuie să fie „în următoarea zi lucrătoare” (Next Business Day) de la momentul sesizării.

Garanția produselor achiziționate va fi asigurată de către Contractant în condițiile politicii de garanție a producătorului, cu asigurarea accesului direct în numele beneficiarului (MAE) la serviciile de garanție și suport ale acestuia, având în vedere prevederile legale în vigoare și prevederile prezentului Caiet de sarcini.

Modalitatea de asigurare a serviciilor de garanție se va prezenta în Oferta tehnică.

Pe toată durata garanției, se vor asigura:

- buna funcționare, calitatea și performanța produselor livrate în conformitate cu specificațiile producătorului;
- înlocuirea componentelor aferente soluțiilor în caz de defecțiuni hardware (acolo unde este cazul);
- suport tehnic 7 zile pe săptămână, 24 ore pe zi.

Garanția trebuie să acopere toate costurile rezultate din remedierea defectelor în perioada de garanție, inclusiv, dar fără a se limita la:

- (i) demontare, inclusiv închirierea de unelte speciale necesare pe durata intervenției (dacă este aplicabil);
- (ii) ambalaje, inclusiv furnizarea de material protector pentru transport (carton, cutii, lăzi etc.);
- (iii) transport prin intermediul transportatorului, inclusiv de transport internațional (dacă este aplicabil);
- (iv) diagnoza defectelor, inclusiv costurile de personal;
- (v) repararea tuturor componentelor defecte sau furnizarea unor noi componente;
- (vi) înlocuirea părților defecte;
- (vii) despachetarea, inclusiv curățarea spațiilor unde se efectuează intervenția;
- (viii) instalarea în starea inițială;
- (ix) testarea pentru a asigura funcționarea corectă;
- (x) repunerea în funcțiune.

În cazul în care, pe toată durata perioadei de garanție, soluțiile de securitate livrate nu mai întrunesc specificațiile agreeate sau devin inutilizabile, total sau parțial (acest lucru nefiind cauzat de către acțiuni sau omisiuni ale Autorității Contractante), Contractantul garantează că va corecta, cu titlu gratuit, toate erorile, defectele, disfuncționalitățile și neconformitățile constatate.



MINISTERUL AFACERILOR EXTERNE

În perioada de garanție, Furnizorul are obligația de a remedia orice tip de eroare și / sau neperformanță și / sau defecțiune și/sau nefuncționalitate a soluțiilor APT, SIEM, Device Control și NAC în termen de maxim 5 (cinci) zile lucrătoare de la notificare, fără costuri pentru Achizitor.

În cazul în care perioada de remediere a defecțiunilor depășește 5 (cinci) zile lucrătoare de la notificare, precum și în cazul în care nu este posibilă remedierea defecțiunilor, furnizorul are obligația de a înlocui de îndată, produsul defect cu altul nou, cu performanțe similare sau superioare celui livrat inițial sau cu modelul următor / superior al aceluiași producător, cu titlu definitiv, fără costuri pentru Achizitor.

Produsul înlocuit va beneficia de o nouă perioadă de garanție identică perioadei de garanție aferentă produsului livrat inițial, on-site, care curge de la data înlocuirii acestuia, respectiv de la data semnării a unui nou proces-verbal de recepție cantitativă și calitativă, acceptat. Înlocuirea și operaționalizarea produsului se va realiza fără costuri din partea beneficiarului (înlocuire, reinstalări, reconfigurări, transport etc.)

Intervențiile și reparațiile în perioada de garanție se efectuează de regulă, la centrele de date ale Achizitorului, cu respectarea programului de lucru, adică de luni până vineri în intervalul 8:30-16:30, cu excepția zilelor declarate oficial nelucrătoare. Prin acordul părților, ocazional, se poate stabili un alt interval orar.

Pentru securitatea datelor prelucrate, unitățile de stocare date (de tip HDD sau SSD) livrate nu vor părăsi locațiile MAE. În situația în care se constată un defect la unitatea de stocare, furnizorul trebuie să pună la dispoziție gratuit, o nouă unitate de stocare identică pentru remedierea defecțiunii urmând ca unitatea de stocare defectă să fie distrusă iremediabil (tocată) de către MAE conform regulamentelor interne.

Toate cheltuielile ocazionate de remedierea defecțiunilor produselor furnizate, incluzând, fără limitare, preluarea, predarea, transportul de la și la locația Achizitorului, operaționalizarea (remediere / înlocuire, reinstalări, reconfigurări etc.), în condițiile menționate mai sus, cad în sarcina Furnizorului.

Pe toata durata garanției, fără costuri pentru achizitor, furnizorul va trebui să asigure MAE următoarele:

- Accesul pe site-ul producătorilor pentru descărcarea de actualizări pentru firmware, sistem de operare, componente software și aplicații care intră în componența soluțiilor livrate;
- Acces pe site-ul producătorilor la baza de cunoștințe (knowledge base) pentru toate produsele supuse contractului în vederea rezolvării cât mai rapide a unor deficiențe deja cunoscute la producător;
- Acces pe site-ul producătorilor, în secțiunea de suport, pentru deschiderea de tichete, din contul AE, în vederea remedierii defecțiunilor pentru sistemul SIEM și toate componentele hardware și software ale acestuia;
- Drept de instalare a oricărei versiuni dezvoltate de producător pentru firmware / sistem de operare / componente și aplicații software ale soluțiilor livrate, pe toată perioada contractuală;
- Acces la și integrarea surselor comerciale și din surse deschise (open-source) de threat intelligence incluse.



Având în vedere că respectivele componente software (firmware / sistem de operare / componente și aplicații software) ale soluțiilor APT, SIEM, Device Control și NAC sunt protejate prin acordul de licență sau de dreptul de autor, pentru instalarea și utilizarea legală a acestora, pe toată perioada garanției, furnizorul va trebui să facă dovada emiterii acestora în numele MAE. Drept urmare, înainte de semnarea procesului-verbal de recepție cantitativă și calitativă a soluțiilor menționate anterior, furnizorul va trebui să facă dovada existenței suportului corespunzător pentru acestea (echipamentul / echipamentele și licențele aferente), livrate în contul MAE la producător / producători, pentru întreaga perioadă de garanție oferită, fapt ce va atesta inclusiv dreptul de descărcare și utilizare a componentelor software (firmware / sistem de operare / componente și aplicații software) incluse, în conformitate cu schema de licențiere a producătorului.

3.5 Livrare, ambalare, etichetare, transport

Termenul de livrare este cel menționat pentru fiecare produs în parte.

Produsele aferente celor patru loturi vor fi livrate cu respectarea tuturor cerințelor cantitative și calitative, la locațiile indicate de autoritatea/entitatea contractantă. Fiecare produs va fi însoțit de toate subansamblele/părțile componente necesare punerii și menținerii în funcțiune.

Componentele hardware ale soluțiilor furnizate (acolo unde este cazul), aferente celor patru loturi, vor fi **noi și nefolosite, de ultimă generație**. Nu se acceptă componente refolosite / refurbished / second hand sau de generație depășită. Pentru a demonstra faptul că soluțiile oferite nu sunt de generație depășită, ofertanții vor prezenta documente din care să reiasă că echipamentele oferite și toate componentele sale nu sunt EOL (End Of Life) sau EOS (End of Sales / Support). Documentele trebuie să fie valabile la data depunerii ofertei. De asemenea, vor trebui să furnizeze informații privind termenele estimate pentru EOL și EOS pentru produsele oferite.

Contractantul va ambala și eticheta produsele furnizate astfel încât să prevină orice daună sau deteriorare în timpul transportului către destinația stabilită, cu respectarea regulilor de vizibilitate aferente programului de finanțare. Modelul etichetei va fi pus la dispoziția ofertantului, în timpul implementării.

Implementarea va fi realizată de către ofertant în centrele de date ale MAE (București și Brașov), fără a afecta activitățile zilnice ale Beneficiarului și fără a întrerupe funcționarea serviciilor din infrastructura acestuia.

Transportul și toate costurile și riscurile asociate sunt în sarcina exclusivă a Contractantului.

Contractantul este, de asemenea, responsabil pentru livrarea în termenul agreat al produselor și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca niciun motiv de întârziere sau costuri suplimentare.



3.6 Instalare, punere în funcțiune, testare

Contractantul va instala soluțiile tehnice aferente celor patru loturi (APT / SIEM / Device Control / NAC), precum și accesoriile conexe, în locațiile MAE din Municipiul București sau Județul Brașov și va efectua toate operațiunile necesare (instalare echipament/soluții, configurare politici, profiluri, roluri, testare etc.) pentru asigurarea funcționării corecte și integrarea acestora în arhitectura de securitate existentă. Validare funcționare completă.

Notă: Integrările hardware și software în infrastructura SNIV/E-VIZA se vor efectua de către un **expert specializat în soluția oferită**, aferente fiecărui lot în parte. Ofertantul va indica în cadrul *Propunerii tehnice* că își asumă îndeplinirea acestei cerințe.

Se vor livra toate licențele necesare instalării, configurării și funcționării celor patru soluții de securitate APT (lot I), SIEM (lot II), Device Control (lot III) și NAC (lot IV), produse comerciale sau dezvoltate de producător sau furnizor astfel încât să se asigure dreptul de utilizare cel puțin pe toată perioada de garanție asigurată (cel puțin 5 ani) pentru produsele livrate.

Odată ce soluțiile APT (lot I), SIEM (lot II), Device Control (lot III) și NAC (lot IV) sunt instalate, Contractantul va realiza și toate configurările / setările necesare pentru punerea în funcțiune, inclusiv toate ajustările și setările necesare pentru a asigura instalarea corespunzătoare, în ceea ce privește performanța și calitatea, cu toate configurațiile necesare pentru o funcționare normală.

După instalare și punere în funcțiune, Autoritatea contractantă împreună cu Contractantul vor efectua teste funcționale aferente fiecărei soluții implementate.

Contractantul va efectua pe propria cheltuială și fără niciun fel de costuri din partea Autorității contractante toate testele pentru a asigura funcționarea soluțiilor implementate APT (lot I), SIEM (lot II), Device Control (lot III) și NAC (lot IV).

3.7 Instruire personal

Contractantul este responsabil pentru instruirea la fața locului / online a personalului desemnat de Autoritatea contractantă. Scopul instruirii este de a transfera către personalul MAE desemnat, cunoștințele necesare pentru operarea și administrarea soluțiilor implementate APT (lot I), SIEM (lot II), Device Control (lot III) și NAC (lot IV).

Instruirea va fi organizată după ce fiecare soluție de securitate este funcțională și trebuie să permită personalului Autorității contractante să o opereze și să o administreze în mod eficient.

Instruirea se va efectua de un expert specializat în fiecare soluție oferită. Ofertantul va indica în cadrul *Propunerii tehnice* că își asumă îndeplinirea acestei cerințe. A se corobora cu **capitolul 3.10 - Suport tehnic**.

Numărul persoanelor care vor fi instruite este minim 2 (două).

Instruirea practică se va face utilizând sistemele funcționale și va include, fără însă a se limita la: înțelegerea componentelor fiecărei soluții, înțelegerea tuturor funcționalităților, operarea, administrarea, crearea de fluxuri de lucru, gestionarea incidentelor de securitate, informații despre



mentenanța de rutină care trebuie să fie efectuată, depistarea problemelor și diagnosticare de bază etc. Contractantul trebuie să propună orice subiect suplimentar care ar putea fi necesar pentru a se asigura că personalul Autorității contractante este pe deplin instruit pentru a asigura utilizarea corespunzătoare a soluțiilor implementate APT (lot I), SIEM (lot II), Device Control (lot III) și NAC (lot IV).

Durata sesiunilor de instruire va fi de minim 2 zile, în funcție de aspectele care vor fi abordate și de complexitatea operațiunilor și cunoștințelor transferate. Sesiunea de instruire se va desfășura în limba română.

Încheierea procesului-verbal de recepție calitativă și calitativă aferent fiecărei soluții, acceptat, va fi condiționată de realizarea instruirii personalului desemnat de Autoritatea contractantă.

Contractantul va asigura pe durata sesiunii de instruire, materiale suport, manuale sau instrucțiuni de utilizare în limba română sau engleză, pe suport de hârtie sau electronic.

Livrabilele care vor rezulta ca urmare a finalizării etapei de instruire sunt:

- **Raport de instruire** – conține informații despre activitatea desfășurată și aspectele care s-au atins în timpul activității de instruire și eventual diplomele emise dacă este cazul;
- **Prezenta la curs** – conține lista de participanți cu semnăturile acestora în zilele de instruire.

3.8 Mentenanța preventivă în perioada de garanție

Mentenanța preventivă trebuie înțeleasă ca totalitatea operațiunilor de întreținere și reparație a soluțiilor APT (lot I), SIEM (lot II), Device Control (lot III) și NAC (lot IV), care se efectuează pe parcursul ciclului de viață ale acestora, la intervale regulate, cu scopul de a asigura funcționarea normală a acestora, pentru a reduce riscurile de defectare și de deteriorare.

Contractantul este responsabil pentru realizarea operațiunilor de mentenanță preventivă pe toată perioada de garanție solicitată. Acesta va nominaliza în propunerea tehnică persoanele propuse pentru efectuarea mentenanței preventive.

Contractantul trebuie să efectueze mentenanță preventivă a celor 4 (patru) soluții APT (lot I), SIEM (lot II), Device Control (lot III) și NAC (lot IV) conform recomandărilor producătorului, pe toată perioada de garanție ofertată.

Înainte de efectuarea operațiunilor de mentenanță preventivă, Contractantul comunică Autorității contractante, lista operațiunilor de mentenanță care trebuie efectuate conform cerinței de mai sus. În funcție de disponibilitatea locației unde sunt instalate cele 4 (patru) soluții de securitate, precum și de întreruperea în funcționare necesară, este posibil ca mentenanța preventivă să fie realizată în afara orelor normale de lucru sau la sfârșit de săptămână sau de sărbători legale. Orele de lucru normale ale Autorității contractante sunt de luni până vineri în intervalul 8:30-16:30, cu excepția zilelor declarate oficial nelucrătoare.

Operațiunile de mentenanță preventivă care necesită o oprire a celor 4 soluții implementate - APT (lot I), SIEM (lot II), Device Control (lot III) și NAC (lot IV), dar care nu afectează serviciile oferite



de acestea, se efectuează în timpul programului de lucru. Dacă oprirea acestora afectează alte servicii IT necesare angajaților MAE, atunci operațiunile de mentenanță se vor efectua în afara orelor de program și datele exacte pentru intervenții vor fi agreate cu Autoritatea contractantă. Mentenanța preventivă trebuie să acopere toate costurile aferente intervențiilor, inclusiv forța de muncă, piese de schimb și altele asemenea.

După fiecare intervenție preventivă, Contractantul trebuie efectueze teste de funcționare a produsului și să prezinte un raport care să includă activitățile realizate.

Nu se percep costuri pentru mentenanța preventivă.

3.9 Mentenanța corectivă în perioada post-garanție, după caz

Nu este cazul.

3.10 Suport tehnic

Ofertantul trebuie să asigure cadrul profesional adecvat desfășurării proiectului în bune condiții. Având în vedere că, în cadrul implementării proiectului, se vor desfășura activități în centrele de date ale MAE, se solicită existența specialiștilor pentru a garanta intervenția pe echipamentele funcționale ale Beneficiarului cu timpi minimi de indisponibilitate ai sistemului și fără a genera pierderi de date.

Ofertantul este obligat să deruleze toate activitățile de instalare, configurare și testare cu personal calificat pentru îndeplinirea scopului și obiectivelor proiectului de față, aferent fiecărui lot în parte.

În acest sens, fiecare ofertant va prezenta documente justificative în vederea îndeplinirii acestei cerințe, respectiv:

Competențe minime:

- ✓ studii universitare finalizate cu diploma de licență, examen de diplomă sau echivalent;
- ✓ experiență profesională generală de minim 5 ani, demonstrată prin prezentarea de documente-suport relevante care atestă experiența profesională, care pot fi: fișa de post, contractul de muncă, recomandarea sau orice alte documente similare;
- ✓ experiență specifică – participarea în minim 1 contract / proiect de implementare soluție APT / SIEM / Device Control / NAC, în care a prestat activitățile aferente fiecărui rol, demonstrată prin prezentarea de documente-suport relevante care



- atestă experiența profesională care pot fi: fișa de post, contractul de muncă, recomandarea sau orice alte documente similare;
- ✓ deținerea de competențe privind instalarea, configurarea, administrarea, optimizarea soluțiilor APT / SIEM / Device Control / NAC oferate, configurarea de instrumente de securitate la nivelul soluțiilor oferate, dovedite prin certificări profesionale relevante, eliberate de organisme de certificare recunoscute național și/sau internațional, a căror obținere presupune parcurgerea unui program de formare și/sau susținerea unui examen de certificare standardizat;
 - ✓ declarație privind disponibilitatea în vederea realizării obiectivelor prezentei achiziții.

Activități și responsabilități:

- ✓ analiza tehnică asupra situației existente a infrastructurii Beneficiarului;
- ✓ stabilirea constrângerilor de integrare a produselor hardware și software în infrastructura sistemului SNIV/E-VIZA;
- ✓ activități de instalare, configurare și testare aferente fiecărei soluții în parte (APT / SIEM / Device Control / NAC).

Pe toată durata contractului, în perioada de garanție, Contractantul va asigura suport tehnic pentru fiecare soluție livrată (APT / SIEM / Device Control / NAC) în integralitatea sa (echipament(e), software, licențe, surse de threat intelligence etc.).

Contractantul va asigura un punct și o persoană de contact dedicate personalului desemnat al Autorității contractante, unde și prin care se semnalează orice problemă / defecțiune sau se va solicita suport tehnic, Contractantului, în gestionarea unui incident, pentru a se asigura că orice situație semnalată este tratată cu promptitudine.

Fiecărui incident este caracterizat de un nivel de prioritate, care va evidenția impactul acestuia asupra funcționalităților infrastructurii.

Nivelele de prioritate sunt:

1. *Critic* - incidentul are impact major asupra funcționării infrastructurii. Problema împiedică desfășurarea activității Autorității contractante.
2. *Mediu* - impact mediu asupra desfășurării activității Autorității contractante. Problema afectează minor funcționalitățile infrastructurii. Impactul reprezintă un inconvenient care necesită soluții alternative pentru refacerea funcționalităților.
3. *Minor* - impact minim asupra desfășurării activității Autorității contractante. Problema nu afectează funcționalitățile infrastructurii. Rezultatul este o eroare minoră care nu împiedică desfășurarea în bune condiții a activității Autorității contractante.



Ofertantul trebuie să asigure disponibilitatea serviciilor de suport tehnic. În cazul incidentelor cu prioritate „critic”, intervenția va fi asigurată 24x7, din momentul primirii sesizării și până la remedierea definitivă a problemei și asigurarea funcționalității integrale a componentelor/ sistemului. Ofertantul va trebui să respecte următorii timpi de răspuns, corelați cu nivelul de prioritate a incidentului:

Nivel prioritate	Timp de răspuns	Timp de implementare soluție provizorie	Timp de rezolvare
Critic	30 min	12 ore	24 ore
Mediu	30 min	48 ore	2 zile
Minor	30 min	4 zile	6 zile

3.11 Mediul în care este operat produsul

Soluțiile care fac obiectul procedurii de atribuire, respectiv sistemele APT (lot I), SIEM (lot II), Device Control (lot III) și NAC (lot IV), vor fi instalate în centrele de date ale MAE, care beneficiază de condiții de temperatură controlată, cu senzori dedicați pentru detectarea umidității, fumului, temperaturii ridicate și a incendiului, cu o frecvență de utilizare non-stop / 7 zile pe săptămână, 365 de zile pe an.

4 Atribuțiile și responsabilitățile Părților

Contractantul are obligația de a livra, instala, pune în funcțiune și testa soluțiile aferente fiecărui lot în parte, la sediul Autorității contractante și de a instrui personalul Autorității în conformitate cu specificațiile caietului de sarcini și a Contractului încheiat între părți.

De asemenea, Contractantul are obligația de a asigura îndeplinirea tuturor obligațiilor pe toată perioada de garanție a soluțiilor aferente fiecărui lot în parte, conform caietului de sarcini, a Contractului, precum și a obligațiilor asumate prin Oferta tehnică și Oferta financiară.

Autoritatea contractantă are obligația de a plăti prețul soluțiilor aferente fiecărui lot în parte, recepționate conform specificațiilor din caietul de sarcini, ofertei tehnice și contractului încheiat între părți.

5 Documentații ce trebuie furnizate autorității contractante în legătură cu achiziția

Documentațiile pe care Contractantul trebuie să le livreze Autorității contractante în cadrul Contractului sunt: documentația de utilizare, documentația de administrare și operare, raport privind testarea, dosarul de instruire al personalului. De asemenea, Contractantul va transmite Autorității contractante și următoarele documente, la momentul recepției calitative:



- a) certificatele de calitate și garanție;
- b) documente din care să reiasă că soluțiile oferite, aferente fiecărui lot în parte, nu sunt EOL (End Of Life) sau EOS (End of Sales / Support);
- c) dovada activării licențelor software aferente sistemului și a serviciilor de suport, din care să reiasă perioada de valabilitate a acestora.

6 Recepția produselor aferente loturilor I-IV

Recepția soluțiilor de securitate aferente fiecărui lot (APT, SIEM, Device Control și NAC) se va efectua în baza unui proces-verbal încheiat între Contractant și Autoritatea contractantă. Recepția se va realiza în mai multe etape, în funcție de progresul Contractului, respectiv:

a) **recepția cantitativă** se va realiza după livrarea produselor hardware și software aferente fiecărei soluții la locația indicată de Autoritatea contractantă. Procesul-verbal de recepție cantitativă atestă livrarea cantitativă a produselor hardware (acolo unde este cazul) și software aferente soluțiilor APT (Lot I) , SIEM (Lot II), Device Control (Lot III) și NAC (Lot IV), integritatea fizică, precum și realizarea operațiunilor de instalare. În urma recepției cantitative, se va încheia un proces-verbal în baza căruia se realizează preluarea fiecărei soluții în parte în custodia Autorității contractante. Recepția cantitativă nu îndreptățește Contractantul să solicite efectuarea plății;

b) **recepția calitativă** se va realiza după instalarea, punerea în funcțiune, instruirea personalului desemnat și testarea fiecărei soluții în parte și, după caz, după ce toate defectele descoperite au fost remediate.

Procesul-verbal de recepție calitativă va include unul din următoarele rezultate:

a) *acceptat* – dacă soluțiile APT / SIEM / Device Control / NAC livrate și serviciile aferente prestate corespund în totalitate cerințelor caietului de sarcini;

b) *refuzat* - dacă soluțiile APT / SIEM / Device Control / NAC livrate și serviciile aferente prestate nu corespund în totalitate cerințelor caietului de sarcini.

Procesul-verbal de recepție calitativă va fi redactat cu respectarea formularelor financiar-contabile, reglementate de legislația incidentă.

Dreptul de proprietate / utilizare asupra componentelor fiecărei soluții, inclusiv asupra software-urilor și licențelor aferente, pe toată perioada contractuală împreună cu riscul Contractului se transferă de la Contractant la Autoritatea contractantă la data semnării a procesului-verbal de recepție calitativă, acceptat.

Termenul de implementare a soluțiilor ce fac obiectul prezentei proceduri se calculează de la data semnării contractului de către ambele părți și este următorul:



MINISTERUL AFACERILOR EXTERNE

1. pentru lotul I – Soluție pentru detecția, analiza și oprirea amenințărilor avansate de securitate cibernetică - Atacuri de tip ATP – *maximum 120 zile calendaristice*;
2. pentru lotul II – Soluție de tip SIEM (Security Information and Event Management) – *maximum 60 zile calendaristice*;
3. pentru lotul III – Soluție pentru controlul dispozitivelor și gestionarea accesului la fișiere (Device Control) – *maximum 60 zile calendaristice*;
4. pentru lotul IV – Soluție de control al accesului în rețea (NAC) – *maximum 110 zile calendaristice*.

Termenul se consideră respectat în măsura în care procesul-verbal de recepție calitativă, rezultat acceptat este semnat până la expirarea termenului menționat.

Recepția cantitativă și calitativă a echipamentelor și serviciilor aferente soluțiilor APT / SIEM / Device Control / NAC se va realiza la finalizarea fiecărei activități prin semnarea unor procese verbale de recepție/ instruire întocmite de beneficiar pentru fiecare acțiune în parte, prin care va fi consemnată îndeplinirea cerințelor impuse prin Caietul de sarcini.

7 Evaluarea performanței Contractantului

Indicator de performanță	Referința în Caiet de Sarcini -	Ce se măsoară	Modalitate de evaluare
Livrabile aferente serviciilor realizate în termenul agreed	Livrabile (document/raport) predate în termenul agreed aferente loturilor I-IV	Livrarea la timp a rezultatelor	Foarte satisfăcător (5 puncte) – livrate în termenele convenite în contract. Satisfăcător (4 puncte) – livrate imediat după încheierea termenelor convenite în Contract însă fără întârzierea activităților din calendarul general al proiectului. Acceptabil (3 puncte) – livrate după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate. Nesatisfăcător (2 puncte) – livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului (mai mult de 120 de zile). Foarte nesatisfăcător (1 punct) – livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri majore ale activităților din calendarul general al proiectului (mai mult de 180 de zile).
Produce furnizate în termenul agreed	Furnizare de produse aferente loturilor I și IV	Furnizarea produselor în termenele stipulate conform contractului	Foarte satisfăcător (5 puncte) – furnizate în termenele convenite în contract. Satisfăcător (4 puncte) – furnizate imediat după încheierea termenelor convenite în Contract însă fără întârzierea activităților din calendarul general al proiectului.



MINISTERUL AFACERILOR EXTERNE

			Acceptabil (3 puncte) – furnizate după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate. Nesatisfăcător (2 puncte) – furnizate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului (mai mult de 80 de zile). Foarte nesatisfăcător (1 punct) – furnizate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri majore ale activităților din calendarul general al proiectului (mai mult de 120 de zile).
Activități realizate în termenul agreat	Activități de instalare, configurare și testare aferente loturilor II și III	Implementarea soluțiilor în termenele stipulate conform contractului	Foarte satisfăcător (5 puncte) – Activitățile au fost prestate în termenele convenite în contract. Satisfăcător (4 puncte) – Activitățile au fost prestate imediat după încheierea termenelor convenite în Contract însă fără întârzierea activităților din calendarul general al proiectului Acceptabil (3 puncte) – Activitățile au fost prestate după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate. Nesatisfăcător (2 puncte) – Activitățile au fost prestate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului (mai mult de 90 de zile). Foarte nesatisfăcător (1 punct) – Activitățile au fost prestate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri majore ale activităților din calendarul general al proiectului (mai mult de 120 de zile).
Activități realizate în termenul agreat	Activități de instalare, configurare și testare aferente loturilor I și IV	Implementarea soluțiilor în termenele stipulate conform contractului	Foarte satisfăcător (5 puncte) – Activitățile au fost prestate în termenele convenite în contract. Satisfăcător (4 puncte) – Activitățile au fost prestate imediat după încheierea termenelor convenite în Contract însă fără întârzierea activităților din calendarul general al proiectului Acceptabil (3 puncte) – Activitățile au fost prestate după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate. Nesatisfăcător (2 puncte) – Activitățile au fost prestate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului (mai mult de 120 de zile). Foarte nesatisfăcător (1 punct) – Activitățile au fost prestate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri



			maiore ale activităților din calendarul general al proiectului (mai mult de 180 de zile).
--	--	--	---

8 Modalități și condiții de plată

Plata contravalorii serviciilor prestate/ echipamentelor livrate se va realiza la finalul implementării fiecărei soluții în parte, în urma semnării unui proces verbal final de recepție cantitativă și calitativă, însoțit factura aferentă acestora.

Plata serviciilor se face în lei, în contul de Trezorerie al operatorului economic, în termen de 30 zile de la data primirii facturii la sediul Beneficiarului, pe baza facturii fiscale emisă în e-factura și a procesului verbal de recepție cantitativă și calitativă fără obiecțiuni, semnat de reprezentantul ofertantului și de reprezentanții Beneficiarului.

Ofertantul va emite factura pentru serviciile prestate după semnarea de către Beneficiar a procesului verbal de recepție cantitativă și calitativă, ca urmare a instalării, configurării și testării fiecărei soluții de securitate: APT (Lot I) , SIEM (Lot II), Device Control (Lot III) și NAC (Lot IV).

Fiecare factura va avea menționat numărul contractului, codul/codurile CPV, datele de emitere și de scadență și va fi trimisă prin sistemul național privind factura electronică, RO-eFactura.

Procesul-verbal de recepție cantitativă și calitativă va însoți factura și reprezintă elementul necesar realizării plății, împreună cu celelalte documente justificative prevăzute mai jos:

- a) certificatele de calitate și garanție;
- b) dovada activării licențelor software aferente soluțiilor APT (Lot I) , SIEM (Lot II), Device Control (Lot III) și NAC (Lot IV), precum și suportului din partea producătorului, din care să reiasă perioada de valabilitate;
- c) documente din care să reiasă că componentele / echipamentele oferite nu sunt EOL (End Of Life) sau EOS (End of Sales / Support).

9 Cadrul legal care guvernează relația dintre Autoritatea contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Ofertantul devenit Contractant are obligația de a respecta în executarea Contractului, reglementările și standardele aplicabile în furnizarea produselor, precum și reglementările obligatorii în domeniul mediului, social și al relațiilor de muncă stabilite prin legislația adoptată la nivelul Uniunii Europene, legislația națională, prin acorduri colective sau prin tratatele, convențiile și acordurile internaționale în aceste domenii. În acest sens, informații detaliate pot fi obținute de la: Ministerul Muncii și Solidarității Sociale (<http://www.mmuncii.ro/i33/index.php/ro>) și Ministerul Mediului, Apelor și Pădurilor (<http://www.mmediu.ro>).

Pe perioada derulării Contractului, Contractantul se obligă să asigure și să respecte toate obligațiile referitoare la condițiile de muncă și de protecția muncii prevăzute în Legea securității și sănătății în muncă nr. 319/2006, cu modificările și completările ulterioare, precum și în celelalte acte normative în vigoare, din acest domeniu. Contractantul este unicul răspunzător pentru orice accident, dauna și / sau avarie ocazionate de îndeplinirea obiectului Contractului.



Legislația aplicabilă (a se citi „cu modificările și completările ulterioare”):

- Legea nr. 98/2016 privind achizițiile publice;
- Normele metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică/acordului-cadru din Legea nr. 98/2016 privind achizițiile publice, aprobate prin HG nr. 395/2016;
- Alte acte normative în vigoare care derivă, completează, modifică ori sunt emise în aplicarea celor mai sus menționate.

10 Managementul / Gestionarea Contractului și activități de raportare în cadrul Contractului, aferente celor patru loturi

10.1 Gestionarea relației dintre Ofertant și Autoritatea Contractantă

Instrumentul practic în gestionarea relației dintre Ofertant și autoritatea contractantă este întâlnirea, care poate lua forma întâlnirii de început, a întâlnirilor pentru monitorizarea progresului privind contractul sau întâlniri pentru acceptarea rezultatelor contractului. Începerea activității în cadrul contractului va fi formalizată printr-o întâlnire de demarare (kick-off meeting). Această întâlnire va avea loc în termen de maxim 5 zile lucrătoare de la depunerea garanției de execuție a contractului și marchează efectiv începerea activităților în contract. Performanța Ofertantului va fi monitorizată și evaluată de către autoritatea contractantă pe durata implementării contractului pe baza indicatorilor de performanță menționați în continuare. Aceste informații vor fi utilizate inclusiv pentru eliberarea documentului constatator la finalul implementării soluțiilor aferente celor patru loturi.

10.2 Asigurarea Managementului de Proiect

Managementul de proiect reprezintă punctul comun între clienții și echipele de implementare și creează o viziune unică în vederea finalizării unui proiect de succes. Rămâne la latitudinea Ofertantului modul în care realizează asigurarea managementului de proiect, dar acesta trebuie să cuprindă cel puțin următoarele aspecte:

1. Planificare și organizare proiect
2. Managementul resurselor
3. Monitorizarea și controlul proiectului
4. Managementul schimbărilor
5. Managementul calității proiectului
6. Managementul livrărilor și al livrabilelor
7. Managementul comunicării
8. Managementul riscurilor
9. Managementul problemelor

Ofertanții pot să folosească orice abordare sau metodologie de management de proiect pe care o consideră adecvată pentru executarea contractului, atât timp cât metoda aleasă de ei asigură cea mai înaltă calitate a muncii și îndeplinește sau depășește standardele de performanță



stabilite. Ofertanții trebuie să se asigure că metodologia lor sprijină eficiența, promptitudinea, rentabilitatea și că este flexibilă, adaptabilă și scalabilă din punct de vedere al efortului depus și documentației, la orice dimensiune de proiect.

10.3 Rapoartele/documentele solicitate de la Ofertant

Raportarea progresului se realizează în mod uzual în întâlnirile pentru monitorizarea progresului privind contractul. În afara de progresul discutat în ședințele de proiect, Autoritatea Contractantă poate solicita rapoarte de progres ad-hoc, acestea fiind prezentate de Ofertant de regulă în 14 zile.

Daca este solicitat, Ofertantul contribuie la elaborarea oricăror altor documente, precum notificări, acte adiționale, clarificări, etc.

10.4 Livrabile și acceptanța acestora

În condițiile în care nu există alte precizări specifice formulate la nivelul fiecărui livrabil, se aplică aceste considerente generale.

Livrabilele aferente fiecărei etape vor fi predate, în conformitate cu termenele stabilite în graficul de activități și vor fi înregistrate și semnate de reprezentanții Ofertantului și cei ai Autorității Contractante. Livrabilele trebuie transmise spre acceptare, în atenția responsabilului de contract al Autorității Contractante. Variantele intermediare vor fi circulat pentru analiză în format electronic.

Autoritatea contractantă va notifica ofertantul cu privire la necesitatea revizuirii/respingerii livrabilelor, în scris și motivat, în termen de maxim 14 zile de la data primirii acestora. În aceste situații, Ofertantul va întreprinde în maxim 14 zile măsurile/demersurile care se impun în vederea remedierii aspectelor/deficiențelor semnalate de Autoritatea Contractantă.

Toate livrabilele specificate în caietul de sarcini vor fi redactate și predate de către Ofertant în limba română.

Acceptanța este procesul prin care activitatea Ofertantului este aprobată de către Autoritatea Contractantă, pe baza regulilor și normelor de acceptare definite în contract și detaliate corespunzător în proiect. Prin mecanismul de acceptanță este recepționat și acceptat rezultatul muncii Ofertantului din timpul activităților de proiect.

Autoritatea Contractantă va verifica modul de implementare a soluțiilor APT (Lot I) , SIEM (Lot II), Device Control (Lot III) și NAC (Lot IV), în conformitate cu caietul de sarcini, din punct de vedere calitativ, cantitativ și al termenelor de livrare, în vederea emiterii Procesului-Verbal de Recepție Cantitativă și Calitativă pentru livrabile.

Termenul de emiterie a Procesului-Verbal de Recepție Cantitativă și Calitativă este de maxim 14 zile de la data la care livrabilele au fost transmise spre aprobare.



Dacă în termen de 14 zile de la data predării livrabilelor, Autoritatea Contractantă nu are solicitări cu privire la revizuire/respingerea livrabilului, atunci se va efectua acceptanța livrabilelor de către autoritatea contractantă prin semnarea Procesului-Verbal de Recepție Cantitativă și Calitativă.

Dacă livrabilele nu au fost acceptate/revizuite/respinse în termenele maximele menționate mai sus, acestea se consideră acceptate implicit.

10.5 Ipoteze și riscuri

Autoritatea Contractantă pleacă de la următoarele ipoteze:

- o conținutul serviciilor solicitate este descris în mod explicit în Caietul de Sarcini;
- o corelația dintre resursele necesare și rezultatele așteptate este realistă;
- o începerea serviciilor se va realiza în perioada preconizată;
- o nu se prevăd schimbări ale cadrului instituțional și legal care să afecteze major implementarea și desfășurarea în bune condiții a Contractului;
- o toate informațiile relevante și disponibile la nivelul Autorității Contractante pentru realizarea serviciilor vor fi puse la dispoziția Ofertantului;
- o Ofertantul va semna un acord de confidențialitate la momentul semnării Contractului și va respecta toate instrucțiunile privind utilizarea informațiilor confidențiale.

În pregătirea Ofertei, Ofertanții trebuie să aibă în vedere cel puțin riscurile și ipotezele descrise în continuare. În acest sens, la întocmirea ofertei, Ofertantul trebuie să ia în considerare resursele necesare (de timp, financiare și de orice altă natură), pentru implementarea strategiilor de risc propuse.

Riscuri care pot fi identificate la momentul elaborării Caietului de Sarcini și riscuri care pot apărea în derularea contractului sunt următoarele:

Nr. crt.	Risc	Măsuri de prevenire / contracarare	Responsabil pentru implementare măsuri
1	Evenimente în plan politic și legislativ care pot aduce constrângeri în implementarea contractului	Pentru contracararea factorilor externi, autoritatea contractantă dispune de proceduri de sistem și proceduri operaționale care asigură funcționarea Instituției	Autoritatea Contractantă
2	Nepunerea/întârzierea punerii la dispoziția Ofertantului a informațiilor care vor face obiectul serviciilor de arhivare fizică și electronică, conform termenelor stabilite	Desemnarea unei echipe formate din reprezentanți implicați și responsabili desemnați de către structurile organizatorice ale autorității contractante care sa ofere suportul necesar derulării în condiții optime a contractului	Autoritatea Contractantă



Nr. crt.	Risc	Măsuri de prevenire / contracarare	Responsabil pentru implementare măsuri
4.	Întârzieri în implementarea soluțiilor care ar putea afecta buna desfășurare a activității Autorității Contractante	Autoritatea Contractantă a prevăzut, în cuprinsul contractelor, penalități pentru întârzierile intervenite în implementarea contractului	Autoritatea Contractantă Ofertant
5	Lipsa comunicării eficiente între echipele de lucru ale Ofertantului și responsabilii desemnați din partea autorității contractante	Realizarea unui plan de comunicare adecvat care sa fie diseminat tuturor părților implicate și respectat de echipele de proiect - Întâlniri periodice pentru prezentarea stadiului proiectului, a activităților viitoare și de analiză a riscurilor	Autoritatea Contractantă Ofertant
6	Evenimente sau obstacole intempestive care pot apărea pe durata de execuție a contractului	Comunicare pro activă, pe tot parcursul implementării contractelor, astfel încât orice problemă întâmpinată să fie soluționată înainte de a avea repercusiuni negative asupra execuției proiectului	Autoritatea Contractantă Ofertant
7	Întârzieri în efectuarea plăților pentru furnizarea soluțiilor	În cazul aprobării cu întârziere a bugetului pentru efectuarea plăților aferente contractelor sau a întârzierilor în efectuarea plăților soluția preconizată constă în introducerea unor prevederi privind posibilitatea facturării parțiale.	Autoritatea Contractantă
8	Indisponibilitatea personalului de contact al autorității contractante și al Ofertantului în anumite perioade de implementare a contractului	Nominalizarea mai multor persoane de contact din partea Autorității Contractante, care să poată susține activitatea de colaborare cu personalul nominalizat al Ofertantului, chiar și în cazul absenței unui sau a mai multor persoane de contact	Autoritatea Contractantă Ofertant

Ofertanții vor identifica și alte riscuri pe lângă cele prezentate de Autoritatea Contractantă și vor prezenta în propunerea tehnică măsurile propuse de remediere pentru toate riscurile existente.

11 Ofertare

11.1 Modul de organizare al ofertei

Propunerea tehnică trebuie să conțină următoarele informații:



- o detalierea metodologiei de derulare a activităților din contract;
- o lista experților propuși pentru realizarea contractelor, demonstrarea modului în care aceștia îndeplinesc cerințele, CV-urile acestora și documentele justificative privind experiența similară.

În vederea facilitării stabilirii corelării între propunerea tehnică și abordarea metodologică, ofertantul va prezenta un tabel care va cuprinde cerințele privind abordarea metodologică și demonstrarea îndeplinirii acestei cerințe prin prezentarea aspectelor relevante conținute în Oferta tehnică. Ofertele care nu vor prezenta dovezi că îndeplinesc cerințele minime pentru acest factor de evaluare, vor fi descalificate.

Abordarea propusă trebuie să se bazeze pe o serie de metodologii, metode și /sau instrumente testate (instrumentele folosite au fost utilizate în alte proiecte), recunoscute (metodele si/sau instrumentele sunt descrise în literatura de specialitate) și care demonstrează o foarte bună înțelegere a contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini, în corelație cu aspectele cheie, precum și cu riscurile și ipotezele identificate.

Ofertanții trebuie să prezinte în cadrul propunerii tehnice descrierea detaliată a metodologiei abordate pentru derularea acestui proiect ținând cont de solicitările din Caietul de sarcini. Astfel se va detalia modalitatea prin care se vor realiza toate activitățile de proiect solicitate, precum și metodologia de management de proiect.

Ofertanții trebuie să întocmească propunerea tehnică și financiară cu respectarea prevederilor stabilite în cadrul fișei de date a achiziției din cadrul documentației de atribuire. Ofertantul trebuie să răspundă punctual la toate cerințele cuprinse în prezentul caiet de sarcini și să detalieze în cadrul propunerii tehnice modalitatea și mijloacele concrete prin care serviciile oferite îndeplinesc aceste cerințe, astfel încât comisia de evaluare să aibă posibilitatea evaluării acestora în mod obiectiv.

11.2 Plan de lucru pentru activitățile/serviciile solicitate

Graficul de implementare se va realiza pentru toate soluțiile aferente celor patru loturi. În graficul de implementare vor fi evidențiate termenele aferente procesului de recepție/aprobare livrabile; Se vor respecta întocmai termenele impuse prin caietul de sarcini, precum și cerințele formularului de ofertă. Graficul va fi prezentat în forma solicitată, anexa la ofertă, în rubrica prevăzută în SEAP.

11.3 Propunerea tehnică

Ofertanții vor prezenta propunerea tehnică astfel încât să permită identificarea cu ușurință a corespondenței cu cerințele minime din caietul de sarcini.

Propunerea tehnică va fi elaborată în conformitate cu prevederile caietului de sarcini, sens în care va fi completat și prezentat formularul de propunere tehnică din Secțiunea "Formulare".

Atașat formularului de propunere tehnică vor fi prezentate documentele solicitate pentru demonstrarea îndeplinirii cerințelor minime privind personalul specializat responsabil cu



implementarea soluțiilor APT (Lot I) , SIEM (Lot II), Device Control (Lot III) și NAC (Lot IV). În sensul celor de mai sus, în cuprinsul formularului de propunere tehnică, va fi indicat fișierul și pagina la care poate fi identificat documentul solicitat.

Pentru toate componentele și funcționalitățile menționate explicit, Ofertantul va prezenta în mod obligatoriu, informațiile relevante detaliate, inclusiv modelul, producătorul, specificații tehnice și funcționale, care să permită identificarea componentelor soluției APT oferată și confirmarea respectării cerințelor.

La descrierea caracteristicilor produsului oferat, nu vor fi acceptate răspunsuri scurte, de tipul „DA”, „Conform”, care includ doar denumirea caracteristicii cerute sau prezentarea acesteia folosind doar descrierea cerinței tehnice din caietul de sarcini.

În cazul în care oferta este depusă în asociere, operatorul economic va atașa formularului de propunere tehnică, o descriere detaliată a modului în care vor fi distribuite sarcinile și responsabilitățile între asociați, precum și a modului de colaborare între asociați pentru realizarea cu succes a activităților contractului.

Neîndeplinirea oricărei cerințe din caietul de sarcini, constituie motiv pentru respingerea ofertei ca neconformă.

11.4 Propunerea financiară

Propunerea financiară se criptează și se salvează în SEAP, în câmpul dedicat ofertei financiare. În plus, ofertanții vor încărca în SEAP Formularul de ofertă și centralizatorul de prețuri, anexat prezentei documentații de atribuire și vor fi marcate în SEAP ca făcând parte din propunerea financiară.

Note:

Atât propunerea tehnică, cât și cea financiară se vor încărca în SEAP, semnate cu semnătură electronică extinsă.

Doar Ofertantul declarat câștigător, aferent fiecărui lot, va avea acces la detaliile tehnice ale sistemului informatic SNIV, în condițiile acordului de confidențialitate ce va fi încheiat cu MAE.

12 Anexe

Următoarele documente sunt parte integrantă din Caietul de sarcini:

1. Anexa 1 – Specificații tehnice Soluție APT
2. Anexa 2 – Specificații tehnice Soluție SIEM
3. Anexa 3 – Specificații tehnice Soluție Device Control



MINISTERUL AFACERILOR EXTERNE

4. Anexa 4 – Specificații tehnice Soluție NAC
5. Anexa 5 –Detalii privind aplicarea algoritmului de calcul aferent criteriului de atribuire.



MINISTERUL AFACERILOR EXTERNE

12.1 Anexa 1 - Specificații tehnice Soluție APT

Cantitate	Unitate de măsură	Loc de livrare	Data de livrare solicitată	Specificații tehnice hardware SAU cerințe de performanță / funcționale <u>minime</u>	Specificații tehnice SAU cerințe de performanță / funcționale <u>extinse/dorite</u>	Durata minima garanție/termen de valabilitate
2	buc.	Sediul DFEN	60 zile de la data semnării contractului	Dimensiune maximă, rackabil 19"	2U	5 ani garanție și suport de la producător
				Interfețe administrare	Minim 1 x 10/100/1000 BASE-T	
				Interfețe pentru analiză/monitorizare (minim)	Minim 1 x 10/100/1000 BASE-T 2 x 10 GBASE-T 2 x 1Gbe/10Gbe SFP+	
				Cantitate trafic de date analizat (minim)	4.5 Gbps	
				Număr de conexiuni pe minut	230000	
				Sursă de alimentare	Dublă , 100-240V	
				Certificări	FCC Part 15, Class A (CFR 47), ICES-003 Class A UL 60950-CSA 60950, EN 60950, IEC 60950 CB Certificate & Report, IEC 60950	
Cantitate	Unitate de măsură	Loc de livrare	Perioada de implementare solicitată	Specificații tehnice software SAU cerințe de performanță / funcționale <u>minime</u>	Specificații tehnice SAU cerințe de performanță / funcționale <u>extinse/dorite</u>	Durata minima garanție/termen de valabilitate
2	buc.	Sediul DFEN	120 zile de la data semnării contractului	Soluția trebuie să aibă capacitatea de a analiza o rețea informatică, învățând comportamentul rețelei și generând un model de comportament pentru fiecare dispozitiv și utilizator din rețea, astfel având posibilitatea de a detecta activitățile anormale.		5 ani garanție și suport de la producător
				Soluția folosește o combinație de învățare automată supravegheată și învățare automată nesupravegheată pentru a ajuta la detectarea, răspunsul și investigarea autonome a amenințărilor cibernetice.		



MINISTERUL AFACERILOR EXTERNE

				Soluția analizează traficul brut din fiecare parte a ecosistemului digital în zeci de algoritmi de învățare automată, în principal nesupravegheați, pentru a afla cum arată comportamentul normal în cadrul organizației în vederea detecției oricărui tip de atac, inclusiv amenințările zero-day.	
2	buc.	Sediul DFEN	120 zile de la data semnării contractului	Sistemul monitorizează și analizează: - o traficul de rețea direct către Internet (inbound/outbound); - o traficul de rețea către Internet (inbound/outbound) care trece prin noduri de rețea intermediare de tip servere Proxy; - o traficul de rețea asociat protocolului DNS; - o traficul de rețea asociat protocolului DHCP; - o traficul de rețea din rețeaua LAN internă generat la accesarea unor aplicații sau servicii; - o traficul de rețea din rețeaua LAN internă generat în procesul de autentificare a stațiilor de lucru/serverelor la serverul de domeniu (Domain Controller); - o orice alt trafic de rețea generat între oricare dispozitive din rețeaua LAN internă. Echipamentul primește/procesează/analizează trafic de rețea folosind metoda SPAN sau prin folosirea unor dispozitive de tip Network TAP. Când soluția detectează anomalii și generează alerte, aceasta trebuie să aibă capacitatea de a salva și de a exporta traficul de rețea asociat alertelor respective. Soluția utilizează tehnologii bazate pe mecanisme avansate de Inteligență Artificială, inclusiv algoritmi de tip învățare automată (Machine Learning, Unsupervised Machine Learning etc.) și matematică probabilistică avansată pentru detectarea, analiza și investigarea amenințărilor și vulnerabilităților de securitate cibernetică. Sistemul folosește algoritmi de învățare automată nesupravegheată (unsupervised machine learning) pentru a construi o înțelegere dinamică a comportamentului normal al fiecărei organizații, formând o înțelegere personalizată și multidimensională a fiecărui utilizator, a fiecărui dispozitiv și a tuturor relațiilor complexe dintre ei. Aceasta include orice dispozitiv cu o adresă IP, inclusiv desktop-uri/PC-uri, servere, imprimante, etc . Sistemul nu are nevoie de seturi de date, reguli predefinite pentru detecția anomaliilor.	5 ani garanție și suport de la producător



MINISTERUL AFACERILOR EXTERNE

2	buc.	Sediul DFEN	120 zile de la data semnării contractului	Soluția oferă un mecanism de detecție bazat pe inteligența artificială care nu necesită semnături sau date istorice, astfel putând detecta tipuri de amenințări noi care nu au fost descoperite sau care nu au fost făcute publice până în prezent de către comunitatea de securitate cibernetică, de exemplu de tipul vulnerabilităților “zero-day” ce depășesc soluțiile bazate pe semnături de detecție al malware-ului. Soluția utilizează învățarea automată nesupravegheată pentru a identifica în mod algoritmic grupările semnificative, sortând automat dispozitivele în grupuri și clustere în funcție de similitudinea lor comportamentală. Soluția utilizează o serie de metode diferite de clustering, inclusiv clustering bazat pe matrice, clustering bazat pe densitate și tehnici de clustering ierarhic. Soluția combină analize multiple ale activității digitale, prin valorificarea matematicii probablistice avansate, Estimarea Bayesiană Recursivă, în așa fel încât modelele matematice să fie capabile să se adapteze constant la informații noi pe măsură ce acestea devin disponibile sistemului. Modelele comportamentale obținute permit detectarea unor activități anormale, deviații de la comportamentul normal al rețelei, detectând astfel amenințările și atacurile cibernetice în timp real. Soluția discerne modele semnificative în fluxurile de date care indică atacuri prin recalcularea continuă a nivelurilor de amenințare în lumina noilor date. Soluția utilizează rețele neuronale cu mai multe straturi pentru a îmbunătăți detectarea. Utilizând algoritmi de analiză comportamentală, soluția poate identifica aplicații malware care existau în rețea anterior instalării acesteia. Tehnologia formulează ipoteze ample despre un incident, apoi interoghează și analizează aceste informații – folosind algoritmi personalizați și alte tehnici de învățare automată. Soluția clasifică amenințările identificate în funcție de importanța acestora.	<i>5 ani garanție și suport de la producător</i>
---	------	-------------	---	---	---



MINISTERUL AFACERILOR EXTERNE

2	buc.	Sediul DFEN	120 zile de la data semnării contractului	Soluția detectează comunicațiile dintre dispozitivele victimă din cadrul rețelei și serverele de Comandă și Control.	5 ani garanție și suport de la producător
				Soluția are opțiunea de a șterge datele colectate, fără a afecta funcționalitatea internă a echipamentului, asigură efectuarea de backup/restore a configurațiilor generale și permite integrarea cu servere de tip LDAP.	
				Sistemul Soluția dispune de un mecanism bazat pe inteligența artificială ce corelează alertele detectate într-un incident de securitate mai larg și le investighează în mod 100% autonom, fără a fi nevoie de intervenția echipei umane, automatizând astfel întregul proces de investigare și triaj și producând un raport automat în limbaj natural.	
				Soluția transmite notificări prin e-mail despre alertele identificate. Adresa de e-mail poate fi configurată de către administrator.	
				Soluția trebuie să asigure crearea unor conturi cât și tipuri de acces diferite pentru utilizatorii sistemului. Astfel, se pot crea conturi pentru utilizator cu anumite drepturi de vizualizare în interfața grafică.	
				Soluția dispune de o interfață grafică interactivă prin care utilizatorul poate vizualiza activitatea de analiză și monitorizare.	
				Accesarea interfeței grafice se poate realiza dintr-un browser web, folosind o conexiune criptată bazată pe certificat digital.	
				Pentru conexiunea la interfața grafică este necesară autentificarea utilizatorului pe baza unui nume de utilizator și a unei parole.	
				Interfața grafică dispune de un meniu principal cu diverse opțiuni disponibile unui utilizator în funcție de permisiunile acestuia. Interfața cu utilizatorul este ușor de navigat și oferă vizibilitate deplină în rețea, de exemplu printr-o hartă grafică a lumii cu capacitatea de a mări anumite subrețele și dispozitive.	
				Echipamentul furnizează, în funcție de traficul analizat, informații despre dispozitivele identificate.	



MINISTERUL AFACERILOR EXTERNE

2	buc.	Sediul DFEN	120 zile de la data semnării contractului	Soluția facilitează vizualizarea istoricului de alerte pentru un dispozitiv informatic.	5 ani garanție și suport de la producător
				Pentru fiecare dispozitiv se poate selecta un interval de timp pentru a vedea istoricul conexiunilor.. Soluția asigură gruparea dispozitivelor informatice în baza unor activități similare (ex: conexiuni către aceeași destinație).	
				Soluția asigură gruparea dispozitivelor informatice în baza unor activități similare (ex: conexiuni către aceeași destinație).	
				Din interfața grafică utilizatorul poate efectua căutări după cuvinte cheie (Ex: adrese IP, hostname, nume de domeniu, etc.).	
				Pentru fiecare domeniu sau adresă IP ale unui server de comandă și control accesate din interiorul rețelei se pot extrage/vizualiza dispozitivele interne care au efectuat conexiuni către acesta.	
				Utilizatorul poate modifica intervalul de timp pentru care se dorește vizualizarea alertelor.	
				Alertele identificate sunt afișate în interfața grafică în funcție de nivelul de severitate atribuit de către echipament. De asemenea se poate alege un interval de timp pentru vizualizare.	
				Pentru fiecare alertă soluția va furniza detalii suplimentare precum: data și ora, cine a generat alerta (adresă IP, hostname, etc.).	
				Utilizatorul are opțiunea de a eticheta un dispozitiv informatic identificat în cadrul unui tip de comportament ca fiind legitim (similar cu procesul de whitelist).	
				Utilizatorul poate să filtreze afișarea dispozitivelor în funcție de un tip de comportament / categorie de detecție.	
				Pentru fiecare dispozitiv soluția generează și stochează informații despre comportamentul dispozitivului sub forma unui istoric al conexiunilor realizate. Asupra acestui istoric de conexiuni utilizatorul poate aplica opțiuni de filtrare. De asemenea utilizatorul poate descărca conexiunile sub forma unui fișier	



MINISTERUL AFACERILOR EXTERNE

				.pcap. Aceste pachete pot fi vizualizate nativ în browser sau descărcate și vizualizate pe software terță parte.	
2	buc.	Sediul DFEN	120 zile de la data semnării contractului	Soluția trebuie să poată genera rapoarte automate despre întreaga rețea și incidentele detectate. Rapoartele pot fi descărcate pentru vizualizarea într-o aplicație externă. Utilizatorul poate eticheta (poate adăuga tag-uri) anumite incidente, dispozitive sau utilizatori din rețea. Soluția dispune de un modul ce asigură o căutare avansată în datele colectate din trafic. Căutarea poate fi realizată în funcție de anumite valori, folosind parametri specifici, expresii regulate sau operatori logici. Platforma trebuie să poată fi integrată cu sisteme de tip SIEM. Sistemul trebuie să asigure managementul centralizat al tuturor senzorilor instalați în diverse locații. Sistemul trebuie să faciliteze comunicarea criptată dintre serverul de management și senzori. Soluția trebuie să poată detecta următoarele tipuri de activități și comportamente, prin mecanisme specifice (machine learning, analiză comportamentală) : ○ Conexiuni interne și externe ○ Transfer de date intern și extern ○ Dispozitive conectate din rețeaua internă ○ Dispozitive conectate din exterior ○ Conexiuni active din rețeaua internă ○ Conexiuni active din exterior ○ Comportament/activitate anormală a unui dispozitiv ○ Cereri DNS reușite/nereușite ○ Autentificări Kerberos (reușite/nereușite) ○ Conexiuni suspicioase de la un dispozitiv către mai multe destinații ○ Conexiuni SMB nereușite/reușite ○ Scanarea adreselor din rețea (Address scans on the network) ○ Activitate minare criptomonede	5 ani garanție și suport de la producător



MINISTERUL AFACERILOR EXTERNE

				- o Metode folosite de aplicațiile malware pentru mișcarea laterală - o Sistemul de operare al dispozitivelor - o Identificare servere de tip Proxy - o Transfer de fișiere EXE - o Transfer de fișiere RAR - o Transfer de fișiere cu format necunoscut/payload - o Atacuri de tip Bruteforce - o Atacuri de tip Heartbleed - o Aplicații specifice atacurilor de tip Advanced Persistent Threat (APT) - o Detecția anomaliilor în utilizarea credențialelor - o Comunicații cu rețeaua TOR - o Scanare de porturi - o Conectarea pe porturi non-standard sau compromiterea unui port legitim / port hijacking - o Monitorizare trafic SMTP - o Anomalii în traficul serverelor DNS (Traffic changes to DNS servers) - o Cereri DNS de tip DynDNS (DynDNS DNS requests) - o Pierdere excesivă a conexiunilor sau a pachetelor - o Certificate SSL invalide	
2	buc.	Sediul DFEN	120 zile de la data semnării contractului	Tehnologia trebuie să fie 100% „on premise”, fără a fi necesară conectarea în Internet pentru orice fel de motiv cu privire la funcționalitatea produsului. Orice tip de date sau informații culese de la client nu se trimit în extern, sau la producător, fără acordul clientului. Toate actualizările software trebuie efectuate offline, în mod centralizat și automat. Componenta software trebuie să se afle în întregime pe servere fizice, complet sub controlul clientului și în interiorul rețelei sale. Senzorii din cadrul platformei vor fi instalați și configurați în locații fizice diferite, astfel se va asigura comunicarea și partajarea în mod securizat a datelor între aceștia. Senzorii se pot administra la nivel local. Soluția trebuie să conțină un mecanism de răspuns autonom 24/7 bazat pe inteligența artificială ce este capabil să blocheze și să neutralizeze atacurile cibernetice detectate în orice interval orar și fără niciun fel de intervenție din partea administratorilor IT, astfel încât să poată opri atacurile cunoscute și necunoscute încă din etapele incipiente, inclusiv în perioadele în care echipa umana nu este disponibilă.	5 ani garanție și suport de la producător



MINISTERUL AFACERILOR EXTERNE

2	buc.	Sediul DFEN	120 zile de la data semnării contractului	Mecanismul de răspuns autonom trebuie să ia măsuri proporționale cu anomaliile în cauză, fiind capabil să aplice acțiuni ce nu perturbă operațiunile normale de afaceri, de exemplu prin tăierea unor conexiuni specifice. Totodată, trebuie să fie capabil să escaladeze fără intervenție umană măsurile în mod proporțional cu abaterea continuă a unui dispozitiv sau utilizator de la normal.		5 ani garanție și suport de la producător
				Răspunsul autonom va putea să folosească corelarea alertelor de către mecanismul de investigare al incidentelor de securitate, îmbunătățind astfel acuratețea și eficiența măsurilor luate.		
				Licențiere	Soluția APT va fi licențiată pentru 5 ani si 1170 de dispozitive , incluzând atât mecanismul de detecție prin învățare, cât și mecanismul de răspuns autonom la atacurile avansate de securitate cibernetică. Licențierea trebuie să fie de tip perpetuu. Suport tehnic direct de la producător (pentru bug fix, firmware upgrade) pentru 5 ani.	

NOTE: Se vor specifica **denumirea comercială, modelul, marca și producătorul** produselor livrate. De asemenea, la ofertă se vor anexa și încărca în SEAP, documente de la producător în copie (file de catalog, prospecte, fișe tehnice etc.) care să ateste încadrarea în specificațiile tehnice și în condițiile minimale impuse produsului (se admite ca aceste documente să fie prezentate în limba română sau engleză).

Soluția va fi gestionată de 3 administratori. A se corobora cu **cap. 3.7 [Instruire personal](#)** din Caietul de sarcini.

Integrarea hardware și software în rețea presupune totalitatea acțiunilor (instalare și interconectare hardware, setări de rețea, setări specifice, alocare de resurse ș.a.) necesar a fi realizate pentru ca soluția APT să poată interacționa cu toate componentele rețelei în care este instalată și să funcționeze la parametrii normali de lucru.

Orice element / modul / licență / funcționalitate care nu se regăsește în ofertă și care este necesar/ă îndeplinirii cerințelor caietului de sarcini trebuie să fie inclus/ă fără niciun cost suplimentar pentru beneficiar.

Integrarea hardware și software în rețea se va efectua de un **expert specializat în soluția oferită** (A se corobora cu **cap. 3.6 [Instalare, punere în funcțiune, testare](#)** din Caietul de sarcini). Ofertanții trebuie să își asume în cuprinsul propunerilor tehnice îndeplinirea acestei cerințe.

**12.2 Anexa 2 - Specificații tehnice Soluție SIEM**

Cantitate	Unitate de măsură	Loc de livrare	Perioada de implementare solicitată	Specificații tehnice SAU cerințe de performanță / funcționale <u>minime</u>	Specificații tehnice SAU cerințe de performanță / funcționale <u>extinse/dorite</u>	Durata minima garanție/termen de valabilitate
1	buc.	Sediul DFEN	60 de zile de la data semnării contractului	Arhitectură	Soluția trebuie să permită instalarea și funcționarea completa în medii virtualizate pe platforme: ○ VMware ESX ○ Microsoft Hyper-V ○ KVM Management facil prin utilizarea unei interfețe unice de administrare de tip Web Posibilitatea de a adăuga în sistem noi instanțe/module în arhitectura de tip cluster, care să extindă performanțele aferente funcționalităților de analiză, raportare și alertare. Posibilitatea de a adăuga noi instanțe de colectare și parsare loguri, fără întreruperea funcționalității sistemului central. Funcționalități de colectare și analizare a evenimentelor platformelor Microsoft Windows, prin intermediul unor agenți avansați, care să poată asigura: ○ Posibilitatea de a colecta log-uri din fișiere de tip text ○ Posibilitatea de a colecta informații utilizând Osquery ○ Monitorizarea integrității fișierelor ○ Monitorizarea regiștrilor ○ Monitorizarea dispozitivelor detașabile: drivere USB/CD-DVD ○ Posibilitatea de a rula comenzi PowerShell si de a colecta ca log-uri rezultatele (output-ul) acestor comenzi ○ Posibilitatea de a rula comenzi WMI si de a colecta ca log-uri rezultatele (output-ul) acestor comenzi	<i>5 ani garanție și suport de la producător</i>



MINISTERUL AFACERILOR EXTERNE

					○ Transmiterea datelor către instanțele de colectare in mod securizat/criptat utilizând HTTP.	
1	buc.	Sediul DFEN	60 de zile de la data semnării contractului	Arhitectură	Funcționalități de colectare si analiza a evenimentelor platformelor Linux, prin intermediul unor agenți avansați, care să poată asigura următoarele funcționalități: ○ Posibilitatea de a colecta log-uri din fișiere de tip text. ○ Monitorizarea integrității fișierelor.	5 ani garanție și suport de la producător
					Soluția trebuie să asigure un managementul centralizat al agenților Windows/Linux din interfața grafica (Web) de management.	
				Funcționalități SIEM (colectare, raportare, alarmare, investigare și management al evenimentelor și incidentelor)	Colectarea de informații în mod pasiv (fără interogarea dispozitivelor sau a aplicațiilor existente), prin captarea mesajelor/log-urilor: Syslog, NetFlow, sFlow, SNMP Traps	
					Colectarea de informații (de Securitate, Performanță, Disponibilitate și Modificare), în mod activ, fără agenți, prin interogarea dispozitivelor și aplicațiilor existente utilizând protocoalele standard: SNMP, WMI, VM SDK, OPSEC/CheckPoint LEA, JDBC, Telnet, SSH, JMX.	
					Crearea unei baze de date locale, ca urmare a interogărilor pe baza de protocoale standard, care permite listarea în interfața grafică a următoarelor informații: ○ Versiune/firmware/sistem operare instalat ○ Serial number ○ Interfețele configurate: numele interfeței, adresa IP si subrețeaua alocată, status interfața (activata, dezactivata), viteza de transmisie ○ Procesele ce rulează la nivelul dispozitivului sau sistemului de operare.	
					Aplicațiile și dispozitivele descoperite pe baza interogărilor SNMP, WMI, VM SDK, etc. sunt grupate și listate automat (fără intervenția operatorului uman) pe categorii: Dispozitive de rețea (Firewall-uri, Routere/Switchuri, Controllere Wireless, IPS-uri, Load Balancere, etc.), Servere (Windows, Unix, Stații de lucru, servere de stocare,	



MINISTERUL AFACERILOR EXTERNE

					etc.), Aplicații (DNS, DHCP, AAA, Mail Server, Web Server, App Server, DB Server, Baza de date etc.)	
					Monitorizarea stării si nivelului de răspuns al serviciilor DNS, FTP/SCP, Generic TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH și Web (HTTP, HTTPS). Rezultatul acestei monitorizări poate fi utilizat în calcularea nivelelor de disponibilitate aferente serviciilor respective.	
1	buc.	Sediul DFEN	60 de zile de la data semnării contractului	Funcționalități SIEM (colectare, raportare, alarmare, investigare și management al evenimentelor și incidentelor)	Monitorizarea statusului protocoalelor de routare dinamică: BGP/OSPF/EIGRP	<i>5 ani garanție și suport de la producător</i>
					Suport pentru stocarea log-urilor utilizând: HDD-uri (stocare locală), NFS, Elastic search, ClickHouse	
					Stocarea log-urilor în format brut precum și normalizat/parsat	
					Stocarea template-urilor, incidentelor și a altor date structurate utilizând baze de date relaționale	
					Suport pentru instalarea unor instanțe de colectare date, la nivelul centrelor de date (sau al unor subrețele securizate perimetral), care: ○ realizează colectarea, parsarea și compresia log-urilor, înainte de transmiterea acestora către sediul central in mod securizat, peste conexiuni WAN/Internet utilizând protocolul HTTPS. In cazul în care comunicația cu sediul central este întreruptă, se realizează stocarea temporara a log-urilor și retransmiterea automată a acestora (în momentul în care este restabilită comunicația) ○ se actualizează în mod automat cu noile parsere ce sunt adăugate/definite la nivelul instanței centrale ○ poate fi instalata ca mașina virtuala, compatibila cu platformele VMWare, Hyper-V, KVM ○ poate procesa log-uri/informații in mod pasiv (pentru Syslog, NetFlow, sFlow, NetFlow) cat si activ (ex. interogări SNMP, WMI, OMI, JDBC, VM SDK, CheckPoint LEA, JDBC, LDAP, SSH, etc.)	



MINISTERUL AFACERILOR EXTERNE

					Posibilitatea de limitare a lăţimii de bandă (utilizată pentru transmiterea datelor către sediul central) la nivelul instanţelor de colectare din cadrul centrelor de date.	
					Posibilitatea de a respinge mesaje/log-uri nerelevante la nivelul instanţei locale de colectare.	
1	buc.	Sediul DFEN	60 de zile de la data semnării contractului	Funcţionalităţi SIEM (colectare, raportare, alarmare, investigare şi management al evenimentelor şi incidentelor)	Instanţele locale de colectare transmit către instanţă centrală atât log-urile în format brut, cât şi informaţiile de parsare.	5 ani garanţie şi suport de la producător
					Monitorizarea dispozitivelor fără utilizarea de agenţi, prin: SSH, telnet, WMI, OMI, JMX, Power Shell.	
					Definirea de rapoarte complexe care cumulează/conţin la rândul lor mai multe rapoarte distincte/individuale.	
					Peste 3500 de rapoarte predefinite încadrate/grupate pe categorii şi tipuri de funcţionalităţi (ex. rapoarte de Performanţă, Disponibilitate, Securitate, Modificare, Conformitate) cu posibilitatea de a cauta şi identifica un anumit raport utilizând cuvinte cheie ce se regăsesc în numele sau descrierea aferentă raportului respectiv.	
					Generarea de rapoarte ad-hoc (manual) sau programatic (în mod automat, fără intervenţia operatorului uman).	
					Posibilitatea de a exporta un raport în format PDF, CSV, RTF.	
					Posibilitatea de a transmite un raport prin email în mod manual sau automat (programat pentru anumite momente de timp prestabilite: de ex. zilnic, săptămânal, lunar). Suport pentru criptarea email-urilor utilizând S/MIME.	



MINISTERUL AFACERILOR EXTERNE

					Alertare automată în situația în care (datorită unor defecțiuni, erori umane sau atacuri cibernetice) anumite conexiuni, sisteme sau aplicații devin inaccesibile sau nefuncționale.	
					Colectarea și stocarea log-urilor (aferele echipamentelor și aplicațiilor IT&C), pentru perioade îndelungate de timp: atât online cât și offline prin arhivare.	
					Corelarea automată între logurile și alertele predefinite sau definite de către administrator.	
1	buc.	Sediul DFEN	60 de zile de la data semnării contractului	Funcționalități SIEM (colectare, raportare, alarmare, investigare și management al evenimentelor și incidentelor)	Detectarea anomaliilor comportamentale (detectarea abaterilor de la valorile statistice de referință) și alertarea automată în cazul producerii acestora. Posibilitatea de rulare automată a unor scripturi de remediere (predefinite sau definite de către administrator) în cazul producerii unor incidente de: securitate, disponibilitate, performanță. Funcționalități de alertare automată în situația în care este afectată integritatea datelor prin modificări (realizate de către persoane neautorizate sau aplicații malware/ransomware) de fișiere/directoare sau regiștrii Windows. Posibilitatea de a grupa dispozitivele și aplicațiile ce deserveșc un serviciu de business (ex. ERP/CRM/etc.) și alertarea automată (cu evidențierea serviciului de business impactat) în cazul producerii unui incident de securitate, disponibilitate sau performanță, ce ar avea loc la nivelul dispozitivelor/aplicațiilor ce definesc serviciul de business respectiv.	5 ani garanție și suport de la producător



MINISTERUL AFACERILOR EXTERNE

					Investigarea unui incident în interfața grafică (GUI), prin posibilitatea de a construi un graf/arbore care sa coreleze incidentul respectiv cu entitățile implicate (ex. IP, gazdă, utilizator, proces sau fișier) și apoi recursiv cu alte incidente și entități asociate. Soluția trebuie, de asemenea, să permită vizualizarea cronologică a desfășurării incidentelor corelate recursiv, pentru a putea înțelege mai bine modul de propagare al acestora.	
					Sistem de ticketing integrat, dar și posibilitatea de a integra sisteme externe de ticketing prin API.	
					Posibilitatea de investigare cât mai rapidă a unor eventuale tentative de încălcare a securității datelor, atacuri cibernetice sau probleme de performanță / disponibilitate prin analiza în timp real a log-urilor și evenimentelor colectate: Interfața de management permite listarea în timp real a tuturor log-urilor și a evenimentelor (pe măsură ce acestea sunt recepționate) cu posibilitatea de a defini filtre, astfel încât să fie evidențiate (listate în timp real), doar log-urile și evenimentele relevante (aferente investigației aflată în desfășurare).	
1	buc.	Sediul DFEN	zile de la data semnării contractului	Funcționalități SIEM (colectare, raportare, alarmare, investigare și management al evenimentelor și incidentelor)	Să integreze funcționalități de tip Machine Learning pentru detectarea anomaliilor utilizând cel puțin 4 algoritmi precum: Bipartite Graph Edge, Elliptic Envelope, Statistical Deviation sau Gaussian Model. Posibilitatea de a corela, la nivelul unei reguli de alertare, a următoarelor tipuri de evenimente: ○ Securitate: IPS, Antivirus, erori de autentificare, exploitari, vulnerabilități, etc. ○ Performanță: nivel încărcare CPU, RAM, spațiu de stocare, conexiuni/throughput ○ Disponibilitate: restartarea sau întreruperea unor aplicații/servicii/echipamente) ○ Modificare: modificare unor fișiere, modificarea configurațiilor unor echipamente, adăugarea/ștergerea unor utilizatori, etc.	<i>5 ani garanție și suport de la producător</i>



MINISTERUL AFACERILOR EXTERNE

					Minim 2000 de Reguli (predefinite) de alertare ce conțin criteriile și valorile utilizate în definirea alertei/incident-ului respectiv: nivel de severitate (ex. mic, mediu, mare), categorie incident (ex. de Securitate, Performanță, Modificare, Disponibilitate). Permite utilizatorilor să creeze Incidente prin rularea de rapoarte la intervale periodice. Posibilitatea de a crea noi reguli de alertare, dar și de clonare și modificare a regulilor predefinite. Posibilitatea de a defini politici de notificare pentru: ○ Trimiterea automată de e-mail/SMS ○ Trimiterea automată de mesaje SNMP ○ Trimiterea automată a unui fișier XML peste HTTP(S). Peste 3000 de attribute predefinite (ex. IP/MAC sursa/destinație, sursa raportării, utilizator, stație, tipul evenimentului, etc.), dar și posibilitatea de a defini noi attribute în funcție de nevoile operaționale.				
1	buc.	Sediul DFEN	0 de zile de la data semnării contractului	<table><tr><td>Funcționalități SIEM</td><td> Posibilitatea de parsare, listare și filtrare a log-urilor în timp real (pe măsură ce acestea sunt recepționate). Filtrarea log-urilor trebuie să poată fi realizată în funcție de attribute și valorile asiguate acestora. Posibilitatea de listare și filtrare a log-urilor pentru anumite interval specific de timp. </td></tr><tr><td>Managementul soluției</td><td> O interfață unică de management ce permite managementul tuturor instanțelor aferente soluției: instanțe de colectare log-uri/evenimente, monitorizare performante, corelare, analiză și raportare evenimente. interfață de management de tip Web/GUI HTML 5. </td></tr></table>	Funcționalități SIEM	Posibilitatea de parsare, listare și filtrare a log-urilor în timp real (pe măsură ce acestea sunt recepționate). Filtrarea log-urilor trebuie să poată fi realizată în funcție de attribute și valorile asiguate acestora. Posibilitatea de listare și filtrare a log-urilor pentru anumite interval specific de timp.	Managementul soluției	O interfață unică de management ce permite managementul tuturor instanțelor aferente soluției: instanțe de colectare log-uri/evenimente, monitorizare performante, corelare, analiză și raportare evenimente. interfață de management de tip Web/GUI HTML 5.	5 ani garanție și suport de la producător
Funcționalități SIEM	Posibilitatea de parsare, listare și filtrare a log-urilor în timp real (pe măsură ce acestea sunt recepționate). Filtrarea log-urilor trebuie să poată fi realizată în funcție de attribute și valorile asiguate acestora. Posibilitatea de listare și filtrare a log-urilor pentru anumite interval specific de timp.								
Managementul soluției	O interfață unică de management ce permite managementul tuturor instanțelor aferente soluției: instanțe de colectare log-uri/evenimente, monitorizare performante, corelare, analiză și raportare evenimente. interfață de management de tip Web/GUI HTML 5.								



MINISTERUL AFACERILOR EXTERNE

					Posibilitatea de a personaliza mesajul/banner-ul de întâmpinare ce apare (in interfața de management) imediat după introducerea credențialelor de acces.	
					Acces pe baza de drepturi/roluri (vizualizare, modificare) aferente diferitelor secțiuni prezentate la nivelul interfeței web.	
					Posibilitatea de a anonimiza (la nivelul componentelor de afișare și raportare): adresele IP, identificator utilizator (nume, adresa email) si numele dispozitivului (host name).	
					Posibilitatea de a rula sub forma de slideshow-uri anumite dashboard-uri selectate/relevante.	
					Maparea incidentelor de securitate conform taxonomiei MITRE și posibilitatea vizualizării acestor informații la nivelul unui Dashboard.	
					Vizualizarea și filtrarea incidentelor în funcție de atributele evenimentului, nivelul de severitate (ex. mic/mediu/mare), categorie (Securitate, performanta sau disponibilitate) sau interval orar.	
					Crearea, testarea și activarea parserelor direct din interfața grafică.	
1	buc.	Sediul DFEN	zile de la data semnării contractului	Managementul soluției	Metode externe de autentificare a utilizatorilor prin: Active Directory, LDAP, RADIUS	5 ani garanție și suport de la producător
					Integrarea de surse externe de Threat Intelligence: ○ Posibilitatea de a încărca fișiere CSV (ce conțin listele de Threat Intelligence) direct din interfața grafică de management ○ Suport pentru: adrese IP, Domenii, Hash-uri si URL-uri ○ Surse de Threat Intelligence de tip Comercial sau Open Source furnizate în mod implicit (out of the box), cu posibilitatea de automatizare/programare a procesului	



MINISTERUL AFACERILOR EXTERNE

					de actualizare a listelor (adrese IP, Domenii, Hash-uri si URL-uri) furnizate de aceste surse. ○ Posibilitatea de a corela in timp real, informațiile de Threat Intelligence cu log-urile/evenimentele captate, urmată de alertarea/notificarea automată în cazul detectării unor incidente de securitate. ○ Posibilitatea de a corela informațiile de Threat Intelligence cu datele/evenimentele istorice (stocate la nivelul bazei de date).	
					Posibilitatea de a importa/exporta raporturi, reguli de alertare sau dashboard-uri in format XML	
					Posibilitatea de a colecta configurațiile echipamentelor de rețea (routere, switch-uri, firewall-uri) și de a compara configurații distincte, pentru a putea vizualiza modificările realizate.	
					Notificări și managementul incidentelor: ○ Posibilitatea de a defini politici de notificare în cazul producerii unor incidente. ○ Apelarea automată sau manuală a unui script de remediere (customizabil sau predefinit) ○ Sistem de ticketing integrat (built-in) ○ Suport implicit pentru integrarea sistemelor de ticketing: ServiceNow, ConnectWise și Remedy. ○ Posibilitatea de a integra alte sisteme externe de ticketing prin API.	
					Căutare/filtrare evenimente în timp real pe baza de cuvinte cheie sau attribute (predefinite sau definite de către administrator). Căutare/filtrare evenimente istorice pe baza de cuvinte cheie sau attribute.	
1	buc.	IDFEN	zile de la data	Managementul soluției	Căutarea/filtrarea evenimentelor în timp real sau istoric se realizează utilizând: attribute (predefinite sau definite de operatorul sistemului), operatori logici (egal, diferit, mai mare, mai mare sau egal, mai mic, mai mic sau egal, inclus în, nu este	5 ani garanție și



MINISTERUL AFACERILOR EXTERNE

					inclus în, conține, nu conține, REGEXP, NOT REGEXP) și valori ce sunt mapate (prin intermediul acestor operatori logici) cu atributele respective.	suport de la producător
					Posibilitatea de a utiliza rezultatele unei căutări/filtrări ca intrare/condiționare în cadrul altei căutări/filtrări.	
					Posibilitatea de transmitere mai departe a evenimentelor colectate utilizand KAFKA	
					Implementarea de politici de arhivare a datelor cu posibilitatea de stocarea a acestora utilizand NFS. Reîncărcarea/activarea datelor trebuie să poată fi realizată utilizând interfața GUI.	
					Posibilitatea de a verifica integritatea datelor stocate prin aplicarea de algoritmi de tip Hash atât la momentul salvării datelor, cât și ulterior în momentul accesării/încărcării acestora.	
					Suport pentru utilizarea unor algoritmi criptografici conformi FIPS.	
					Licențiere	



NOTE:

Se vor specifica **denumirea comercială, modelul, marca și producătorul** produselor livrate. De asemenea, la ofertă se vor anexa și încărca în SEAP, documente de la producător în copie (file de catalog, prospecte, fișe tehnice etc.) care să ateste încadrarea în specificațiile tehnice și în condițiile minimale impuse produsului (se admite ca aceste documente să fie prezentate în limba română sau engleză).

Soluția va fi gestionată de 3 administratori. A se corobora cu **cap. 3.7 Instruire personal** din Caietul de sarcini.

Integrarea hardware și software în rețea presupune totalitatea acțiunilor (instalare și interconectare hardware, setări de rețea, setări specifice, alocare de resurse ș.a.) necesar a fi realizate pentru ca soluția SIEM să poată interacționa cu toate componentele rețelei în care este instalată și să funcționeze la parametrii normali de lucru.

Orice element / modul / licență / funcționalitate care nu se regăsește în ofertă și care este necesar/ă îndeplinirii cerințelor caietului de sarcini trebuie să fie inclus/ă fără niciun cost suplimentar pentru beneficiar.

Integrarea hardware și software în rețea se va efectua de un **expert specializat în soluția oferită** (A se corobora cu **cap. 3.6 Instalare, punere în funcțiune, testare** din Caietul de sarcini). Ofertanții trebuie să își asume în cuprinsul propunerilor tehnice îndeplinirea acestei cerințe.



MINISTERUL AFACERILOR EXTERNE

12.3 Anexa 3 - Specificații tehnice Soluție Device Control

Cantitate	Unitate de măsură	Loc de livrare	Perioada de implementare solicitată	Specificații tehnice SAU cerințe de performanță / funcționale <u>minime</u>	Specificații tehnice SAU cerințe de performanță / funcționale <u>extinse/dorite</u>	Durata minima garanție/termen de valabilitate
1	buc.	Sediul DFEN	60 de zile de la data semnării contractului	Soluția trebuie să includă o bază de date fără costuri adiționale.		5 ani garanție și suport de la producător
				Soluția trebuie administrată printr-o platformă web.		
				Soluția trebuie să permită instalarea pe un sistem cu următoarele specificații hardware și software: • sistem de Operare: Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 • procesor: Intel Core i7 (6 core/12 thread) 3.2 GHz sau mai avansat • RAM: 32GB sau mai mult		
				Browser web suportat: Microsoft Edge, Mozilla Firefox, Google Chrome		
				Agenții soluției trebuie să funcționeze pe următoarele sisteme de operare: • Sisteme de operare de tip Windows: Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2*, Windows Server 2008; • Sisteme de operare de tip MacOS: macOS 13 Ventura, macOS 12 Monterey, macOS 11 Big Sur, macOS 10.15 Catalina, macOS 10.14 Mojave, macOS 10.13 High Sierra, macOS 10.12 Sierra		
				Soluția trebuie să suporte baze de date MSSQL pentru migrare în caz de nevoie: SQL Server 2008, SQL Server 2012, SQL Server 2014, SQL server 2016, SQL server 2017, SQL server 2019.		
				Soluția trebuie să permită blocarea instantanee a tuturor dispozitivelor USB neverificate și să permită accesul doar al dispozitivelor de încredere.		



MINISTERUL AFACERILOR EXTERNE

				Soluția trebuie să fie capabilă să detecteze automat orice dispozitiv USB conectat la endpoint-urile gestionate de soluția propusă. Soluția trebuie să permită administratorilor să monitorizeze acțiunile utilizatorului și permisiunile de acces la fișiere. Soluția trebuie să permită administratorilor configurarea setărilor pentru blocarea porturilor USB dacă nu se acordă permisiunea expresă pentru un dispozitiv.	
1	buc.	Sediul DFEN	60 de zile de la data semnării contractului	Soluția trebuie să permită crearea de whitelist-uri/ blacklist-uri pentru dispozitivele USB. Soluția trebuie să permită clasificarea tipului de acces pe care îl poate avea un dispozitiv în funcție de: rolurile, sarcinile și cui aparține dispozitivul. Soluția trebuie să permită construirea de politici de acces pentru dispozitive: blocarea, doar citire, scriere și citire. Soluția trebuie să permită gestionarea porturilor: USB, LPT și Serial. Soluția trebuie să permită crearea unei liste de tip "Trusted Devices". Soluția trebuie să permită crearea de diferite niveluri de acces pentru persoanele autorizate în funcție de credibilitate și scop: read, write, read/write. Soluția trebuie să includă politici predefinite pentru reducerea volumului de muncă al administratorilor. Soluția trebuie să includă un sistem de tip RBAC (Role Based Access Control) pentru definirea utilizatorilor și drepturilor acestora. Soluția trebuie să permită crearea de politici de securitate bazate atât pe roluri cât și pe endpoint-uri. Soluția trebuie să permită setarea unei reguli ce nu permite transferarea unui fișier/fișiere pe un dispozitiv dacă depășește o anumită mărime. Soluția trebuie să permită setarea unei reguli ce nu permite transferarea unui fișier/fișiere pe un dispozitiv dacă are o anumită extensie.	5 ani garanție și suport de la producător



MINISTERUL AFACERILOR EXTERNE

				Soluția trebuie să permită setarea unei reguli ce nu permite transferarea unui fișier/fișiere pe un dispozitiv dacă sunt de un anumit tip.	
				Soluția trebuie să detecteze când se încearcă mutarea/copierea unui fișier/fișiere pe un dispozitiv dacă aceasta acțiune încalcă politicile și regulile de securitate.	
				Soluția trebuie să aibă capabilități de tip "File Tracing".	
1	buc.	Sediul DFEN	60 de zile de la data semnării contractului	Soluția trebuie să poată genera rapoarte pe baza de "File tracing" și să permită administratorilor să urmărească în timp real toate acțiunile ce au legătură cu: mutarea, copierea și transferarea de fișiere, pe dispozitive.	5 ani garanție și suport de la producător
				Soluția trebuie să permită acordarea de acces temporar pentru: transferare, copiere și mutare, pe baza unei cereri din partea unui utilizator ce poate fi aprobată.	
				Soluția trebuie să permită generarea de rapoarte de tip: • auditare Dispozitive • dispozitive Blocate • File Tracing • File Shadowing	
				Soluția trebuie să aibă un panou de comandă ușor de utilizat structurat în sub panouri, de exemplu: • Subpanou Politici • Subpanou Rapoarte • Subpanou Setări • Subpanou Stare Generală	
				Soluția trebuie să ofere administratorului ajutor după instalare prin oferire de: informații despre configurare, ajutor la configurare, video-uri despre cum poate fi folosită soluția.	
				Licențiere	Soluția Device Control furnizată va fi instalată pe 1300 de endpoint-uri și gestionată de 3 administratori.



MINISTERUL AFACERILOR EXTERNE

					Licențierea trebuie să fie “on-premise” de tip perpetuu și va trebui să suporte redundanță la nivel local și geografic în două data center.
					Suport tehnic direct de la producător (pentru bug fix, firmware upgrade) pentru cel puțin 5 ani.

NOTE:

Se vor specifica **denumirea comercială, modelul, marca și producătorul** produselor livrate. De asemenea, la ofertă se vor anexa și încărca în SEAP, documente de la producător în copie (file de catalog, prospecte, fișe tehnice etc.) care să ateste încadrarea în specificațiile tehnice și în condițiile minimale impuse produsului (se admite ca aceste documente să fie prezentate în limba română sau engleză).

Soluția va fi gestionată de 3 administratori. A se corobora cu **cap. 3.7 [Instruire personal](#)** din Caietul de sarcini.

Integrarea hardware și software în rețea presupune totalitatea acțiunilor (instalare și interconectare hardware, setări de rețea, setări specifice, alocare de resurse ș.a.) necesar a fi realizate pentru ca soluția NAC să poată interacționa cu toate componentele rețelei în care este instalată și să funcționeze la parametrii normali de lucru.

Orice element / modul / licență / funcționalitate care nu se regăsește în ofertă și care este necesar/ă îndeplinirii cerințelor caietului de sarcini trebuie să fie inclus/ă fără niciun cost suplimentar pentru beneficiar.

Integrarea hardware și software în rețea se va efectua de un **expert specializat în soluția oferită** (A se corobora cu **cap. 3.6 [Instalare, punere în funcțiune, testare](#)** din Caietul de sarcini). Ofertanții trebuie să își asume în cuprinsul propunerilor tehnice îndeplinirea acestei cerințe.



MINISTERUL AFACERILOR EXTERNE

12.4 Anexa 4 - Specificații tehnice Soluție NAC

Cantitate	Unitate de măsură	Loc de livrare	Perioada de implementare esolicitată	Specificații tehnice hardware SAU cerințe de performanță / funcționale <u>minime</u>	Specificații tehnice SAU cerințe de performanță / funcționale <u>extinse/dorite</u>	Durata minima garanție/termen de valabilitate
Echipament dedicat implementării politicilor de acces în rețea						
1	buc.	Sediul DFEN	110 zile de la data semnării contractului	Descriere generală	Soluție de control a accesului în rețea cu fir, fără fir și VPN pentru dispozitive și utilizatori ce oferă vizibilitate, control și posibilitate de răspuns automat la incidente	5 ani garanție și suport de la producător
				Mod de operare	Soluția trebuie să se implementeze centralizat, într-o arhitectură de tip out-of-band (nu trebuie să stea in-line cu traficul)	
					Soluția nu trebuie să fie restricționată la utilizarea 802.1x pentru a oferi control al accesului. Poate folosi diferite alte metode pentru a impune controlul: SNMP, CLI/SSH, API, Syslog, funcție de producătorul de echipamente de rețea cu care se integrează	
				Tip echipament	Mașină virtuală (VMWare/Hyper-V/AWS/Azure/KVM)	
				Integrare cu componente din rețea	Dispozitive de infrastructură de rețea (cu fir și fără fir) de la diferiți furnizori (minimum Cisco, Juniper, Fortinet)	
					Dispozitive de infrastructură de securitate de la diferiți furnizori (Firewall, IPS, Sandboxing) – minim Cisco, Juniper și Fortinet	
					Servicii de autentificare: RADIUS de la diferiți furnizori	



MINISTERUL AFACERILOR EXTERNE

					Servicii de director: LDAP, Microsoft AD, Google SSO	
					Sisteme de operare: MAC OS, Microsoft Windows, Linux, Apple IOS, Android	
					Soluții de securitate pentru endpointuri (AntiVirus, EDR, XDR, APT), diferiți furnizori acceptați – Minimum BitDefender, Esset, Microsoft	
					Mai mulți furnizori MDM (IBM MaaS360, Microsoft Intune, MobileIron, etc.) utilizați pentru înregistrarea rapidă a unui dispozitiv intern.	
					Soluția să permită înregistrarea stațiilor de lucru interne, a dispozitivelor de tip Guest utilizând și alte metode în afara MAB (Mac Authentication Bypass)	
					Să folosească capacitatea de a valorifica identitatea utilizatorului, tipul de dispozitiv și combinația celor două pentru a furniza în mod dinamic accesul bazat pe roluri - diferite niveluri de acces	
					Să poată realiza un inventar în timp real al tuturor dispozitivelor din rețea și publicarea lor într-un ecran de monitorizare	
					Să realizeze identificarea dispozitivelor folosind multiple metode de identificare	
					Să permită administrarea utilizatorilor de tip Guest, Contractor, Consultant, etc.	
					Să realizeze evaluarea riscului dispozitivelor prin validarea conformității cu diferite criterii: tipul și versiunea sistemelor de operare, existența soluțiilor de protecție client (ex. AV), procese, servicii, existența unor seturi minime de update-uri etc.	
1	buc.	Sediul DFEN	110 zile de la data semnării contractului	Caracteristici		5 ani garanție și suport de la producător



MINISTERUL AFACERILOR EXTERNE

				Să permită accesul în soluție pe baza de roluri de Administratori. Soluția trebuie să ofere capacitatea de a limita și controla nivelul de acces pe care o oferă sistemul diferitelor grupuri administrative din cadrul organizației IT. De exemplu: operațiuni de securitate, operațiuni de rețea, help-desk etc, roluri configurabile. Soluția trebuie să ofere un instrument de audit complet a tuturor conexiunilor la rețea – atât cu fir, cât și fără fir. Aceasta trebuie să includă o interfață pentru a căuta și a interoga aceste date.	
1	buc.	Sediul DFEN	110 zile de la data semnării contractului	Caracteristici Soluția trebuie să includă opțiuni flexibile de scanare atât pentru platformele Windows, cât și pentru MacOS, utilizând agenți cu opțiuni de Agent permanent sau Agent temporar (dizolvabil) Soluția trebuie să identifice și să clasifice fiecare tip de dispozitiv din rețea, să identifice dacă este emis de companie sau deținut de angajați și să identifice utilizatorul de pe dispozitiv pentru a activa politicile de acces la rețea bazate pe roluri. Metodele de profilare nu trebuie să necesite vizibilitatea traficului de rețea Să utilizeze mai multe metode de profilare (scanare activă și pasivă, amprentă DHCP, SNMP, SSH, scanare TCP/UDP, OUI Producător, agent, IP range, WinRM, Radius, locație de conectare, HTTP/S) pentru a identifica și profila un dispozitiv Soluția să includă un agent care poate fi instalat pe stațiile de lucru pentru a furniza informații despre acestea, dar și pentru a fi utilizat în procesul de înregistrare sau complianță Soluția trebuie să asigure răspuns automat la incidente de securitate primite de la echipamente specifice (FW, IPS) și să genereze evenimente de securitate cu acțiuni asociate: să trimită către o soluție SIEM informații contextuale extinse, să carantinizeze dispozitivul la nivel de switch, să dezactiveze portul, să informeze administratorii de rețea etc.	5 ani garanție și suport de la producător



MINISTERUL AFACERILOR EXTERNE

				Management	Să permită management în format GUI - HTTP/HTTPS		
					Să permită management în format CLI		
				Arhitectură	Să permită instalarea într-o arhitectură centralizată, în care serverul NAC este plasat într-o locație centrală (nu in-line), dar poate controla dispozitive din alte locații fără a utiliza sub-componente de analiză trafic		Serverul NAC să permită managementul politicilor și al portalului pentru invitați în aceeași instanță
					Arhitectură		
				1	buc.		Sediul DFEN
Dispozitive	Să fie licențiat pentru controlul a minimum 1000 Dispozitive de tip endpoint cu posibilitate de creștere						
Garanție si suport	5 ani, 24 x 7, atât licențele pentru dispozitivul server, cât și pentru endpoint						
	Include suport tehnic și upgrade-uri de firmware						
Platforma de logare și analiză							
1	buc.	DFEN	110 zile de la data semnării contractului	Descriere generală	Platforma de jurnalizare a logurilor trebuie să provină de la același producător ca firewall-ul sau să poată integra mesajele de la plaja de echipamente ale beneficiarului, echipamente de tip Fortigate diverse modele – aproximativ 400 de	5 ani garanție și	



MINISTERUL AFACERILOR EXTERNE

					echipamente FW, precum și plaja de echipamente noi, oferitate, inclusiv mesajele de la flota de endpoint-uri din rețeaua beneficiarului Platforma de jurnalizare trebuie să permită monitorizarea traficului în timp real direct pe platforma dedicata de jurnalizare, precum și monitorizarea traficului istoric Platforma de jurnalizare trebuie să fie capabilă să preia funcționalitatea de logare și analiză și de la alte echipamente de tip firewall produse de alți producători consacrați Jurnalizarea evenimentelor trebuie să se realizeze către o platforma dedicată, care să se afle în sediul central și care poate să accepte evenimente de la toate echipamentele ce alcătuiesc soluția	suport de la producător
1	buc.	Sediul DFEN	110 zile de la data semnării contractului	Descriere generală Platforma trebuie să suporte generarea de rapoarte pe baza evenimentelor jurnalizate. Trebuie să conțină rapoarte predefinite, dar de asemenea să suporte și customizarea unor rapoarte noi în funcție de criteriile dorite Rapoartele generate trebuie să fie cel puțin în format pdf și html și să poată fi generate la cerere sau la anumite momente predefinite Rapoartele trebuie să poată fi trimise în mod automat și pe anumite adrese de email configurate Platforma de jurnalizare si raportare centralizata trebuie sa poată susține necesarul de stocare pentru minim 6 luni si de asemenea sa asigure preluarea logurilor generate de echipamente in timp real (minim 25 GB/zi de loguri) Platforma de jurnalizare trebuie sa poată oferi funcționalități pentru IOC (indicatori de compromis) ce aduc vizibilitate retrospectiva asupra site-urilor legitime dar compromise ce au fost accesate in cel puțin ultimele 7 zile.	5 ani garanție și suport de la producător	



MINISTERUL AFACERILOR EXTERNE

				Descriere generală	Platforma de jurnalizare sau cea de management trebuie sa ofere posibilitatea creării unui dashboard care sa ofere vizibilitate completă a utilizatorilor și dispozitivelor, inclusiv informații ce permit identificarea suprafeței de atac și care permit analiștilor de securitate a informației să vizualizeze și gestioneze informațiile detaliate colectate din jurnale și de la dispozitivele conectate, cu filtre și vizualizări personalizate pentru rafinare rezultatelor.	
					Platforma de management si de jurnalizare a evenimentelor trebuie sa fie disponibila in varianta mașină virtuala ce poate fi instalata pe următoarele sisteme de virtualizare: KVM, VmWare, Microsoft Hyper-V	
					Platforma de jurnalizare sa poată fi accesata prin Consola, Telnet, SSH, HTTP/HTTPS, Utilizatori/ Administratori cu drepturi configurabile	
					Autentificarea administratorilor sa beneficieze de următoarele setări de securitate: • Bază de date locală • Integrare Active Directory Integrare LDAP/RADIUS/Tacacs+ • IP address binding • Autentificare factor dual folosind token-uri hardware/software dedicate	
1	buc.	Sediul DFEN	110 zile de la data semnării contractului	Garanție si suport	Soluția va beneficia de minimum 5 ani de garanție si suport si va include: • Suport tehnic din partea producătorului 7 zile pe săptămâna, 24 ore pe zi • Update firmware versiuni minore si majore După expirarea serviciilor de suport tehnic si de actualizare software, platforma trebuie sa funcționeze, sa permită atât administrarea cat si fluxurile de date.	



MINISTERUL AFACERILOR EXTERNE

Switch-uri compatibile cu soluția NAC propusa si integrabile cu echipamentele Firewall ale beneficiarului (Fortigate 61E)

Echipament Switch tip I

400	buc.	Sediul DFEN	60 zile de la data semnării contractului	Descriere generală	Echipamentul să poată funcționa în mod independent, administrat din Cloud sau de către un echipament/soluție cu rol de Controller Se ofertează cu mod de operare Independent	
				Interfețe / porturi minime	• 24 GE RJ45 • 4 X 10G SFP+/ 1G SFP • 1 x Port Consola	
				Performanță minimă	• Arhitectura non-blocking (capacitate switching 128Gbps) • 190 Mpps • 32k Adrese MAC • 4K Vlan-uri • Latenta < 1μs	
				Securitate	Echipamentul propus trebuie să ofere: • Radius COA and disconnect messages • EAP pass-through • s-FLOW • DHCP Snooping • Dynamic ARP Inspection • Limitare adrese MAC • IGMP Snooping • Private VLAN • Sticky MAC • Storm Control • 802.1X MAC-based mode • User-based (802.1X) VLAN assignment • 802.1X: MAB • open-auth mode • EAP pass-through	



MINISTERUL AFACERILOR EXTERNE

400	buc.	Sediul DFEN	60 zile de la data semnării contractului	Layer 2	• IGMP Snooping, IGMP Proxy, IGMP Querier • LLDP, LLDP-MED • MAC Learning Limit • SPAN • Flow Control	
				Administrare	Echipamentele sa poată fi administrate centralizat de un echipament/soluție cu funcție controller ce oferă: • Descoperire automata a switch-urilor in rețea si formarea conexiunilor intre acestea (fără a fi nevoie de configurare prealabila a acestora) • Upgrade centralizat • Configurare VLAN • Configurare 802.1X • Integrare in politici de securitate cu posibilitate carantinare automata la nivel de port in switch • Network Access Control • Spanning Tree • LLDP/LLDP-MED • Topologie fizica a rețelei cu status real al conexiunilor si porturilor • Identificarea tipurilor de dispozitive conectate, inclusiv IOT cu informații despre tipul dispozitivului, sistem de operare, informații hardware • Servicii Layer 3 • Autentificare prin Captive Portal Administrare in Cloud sau administrare/funcționare in mod Independent • Management IPv4 si IPv6 • SNMP • CLI, WEB GUI • SNMP OID • Monitorizare temperatura sistem	
400	buc.	Sediul DFEN	60 zile de la data semnării contractului	Alte facilități minime necesare	• Loop-Guard • SPAN • Flow Control • LLDP-MED: ELIN support • 802.1p support, including priority queuing trunk and WRED • TDR (time-domain reflectometer)/cable diagnostics support	



MINISTERUL AFACERILOR EXTERNE

				Alimentare	110-240V, 50-60Hz	
				Instalare	Rack 19", Kit inclus	
				Service si garanție	Soluția va beneficia de minim 5 ani de suport ce va include: • Înlocuirea echipamentului in caz de defecțiune hardware • Suport tehnic din partea producătorului 7 zile pe săptămâna, 24 ore pe zi • Update firmware versiuni minore si majore După expirarea serviciilor achiziționate, echipamentul trebuie să funcționeze, să permită atât administrarea, cât si fluxurile de date.	
Echipament Switch tip II						
200	buc.	Sediul DFEN	ile de la data semnării contractului	Descriere generală	Echipamentul să poată funcționa în mod independent, administrat din Cloud sau de către un echipament/soluție cu rol de Controller Se ofertează cu mod de operare Independent	
				Interfețe / porturi	• 48 GE RJ45 • 4 X 10G SFP+/ 1G SFP • 1 x Port Consola	
				Performanță minimă	• Arhitectura non-blocking (capacitate switching 128Gbps) • 190 Mpps • 32k Adrese MAC • 4K Vlan-uri • Latenta < 1μs	
200	buc.	Sediul DFEN	ile de la data semnării contractului	Securitate	Echipamentul propus trebuie să ofere: • Radius COA and disconnect messages • EAP pass-through • s-FLOW • DHCP Snooping • Dynamic ARP Inspection • Limitare adrese MAC • IGMP Snooping • Private VLAN	



MINISTERUL AFACERILOR EXTERNE

					• Sticky MAC • Storm Control • 802.1X MAC-based mode • User-based (802.1X) VLAN assignment • 802.1X: MAB • open-auth mode • EAP pass-through	
				Layer 2	• IGMP Snooping, IGMP Proxy, IGMP Querier • LLDP, LLDP-MED • MAC Learning Limit • SPAN • Flow Control	
				Administrare	Echipamentele sa poată fi administrate centralizat de un echipament/soluție cu funcție controller ce oferă: • Descoperire automata a switch-urilor in rețea si formarea conexiunilor intre acestea (fără a fi nevoie de configurare prealabila a acestora) • Upgrade centralizat • Configurare VLAN • Configurare 802.1X • Integrare in politici de securitate cu posibilitate carantinare automata la nivel de port in switch • Network Access Control • Spanning Tree • LLDP/LLDP-MED • Topologie fizica a rețelei cu status real al conexiunilor si porturilor • Identificarea tipurilor de dispozitive conectate, inclusiv IOT cu informații despre tipul dispozitivului, sistem de operare, informații hardware • Servicii Layer 3 • Autentificare prin Captive Portal Administrare in Cloud sau administrare/funcționare in mod Independent • Management IPv4 si IPv6 • SNMP • CLI, WEB GUI • SNMP OID	



MINISTERUL AFACERILOR EXTERNE

					• Monitorizare temperatura sistem	
200	buc.	Sediul DFEN	60 zile de la data semnării contractului	Alte facilități minime necesare	• Loop-Guard • SPAN • Flow Control • LLDP-MED: ELIN support • 802.1p support, including priority queuing trunk and WRED • TDR (time-domain reflectometer)/cable diagnostics support	
				Alimentare	• 110-240V, 50-60Hz	
				Instalare	Rack 19", Kit inclus	
				Service si garanție	Soluția va beneficia de minim 5ani de suport ce va include: • Înlocuirea echipamentului in caz de defecțiune hardware • Suport tehnic din partea producătorului 7 zile pe săptămâna, 24 ore pe zi • Update firmware versiuni minore si majore După expirarea serviciilor achiziționate, echipamentul trebuie sa funcționeze, sa permită atât administrarea cat si fluxurile de date.	
				Performanță minimă	• Arhitectura non-blocking (capacitate switching 128Gbps) • 190 Mpps • 32k Adrese MAC • 4K Vlan-uri • Latenta < 1μs	
				Cerințe de interoperabilitate	• Integrare cu rețeaua și soluțiile existente (AV/EDR). • BitDefender • Suport multiplatformă: Windows, Linux.	
				Cerințe de securitate	Soluția se va instala într-un mediu deconectat de la Internet. Se va asigura funcționarea fără necesitatea de conectare la Internet.	



MINISTERUL AFACERILOR EXTERNE

NOTE:

Se vor specifica **denumirea comercială, modelul, marca și producătorul** produselor livrate. De asemenea, la ofertă se vor anexa și încărca în SEAP, documente de la producător în copie (file de catalog, prospecte, fișe tehnice etc.) care să ateste încadrarea în specificațiile tehnice și în condițiile minimale impuse produsului (se admite ca aceste documente să fie prezentate în limba română sau engleză).

Soluția va fi gestionată de 3 administratori. A se corobora cu **cap. 3.7 [Instruire personal](#)** din Caietul de sarcini.

Integrarea hardware și software în rețea presupune totalitatea acțiunilor (instalare și interconectare hardware, setări de rețea, setări specifice, alocare de resurse ș.a.) necesar a fi realizate pentru ca soluția NAC să poată interacționa cu toate componentele rețelei în care este instalată și să funcționeze la parametrii normali de lucru.

Orice element / modul / licență / funcționalitate care nu se regăsește în ofertă și care este necesar/ă îndeplinirii cerințelor caietului de sarcini trebuie să fie inclus/ă fără niciun cost suplimentar pentru beneficiar.

Integrarea hardware și software în rețea se va efectua de un **expert specializat în soluția oferită** (A se corobora cu **cap. 3.6 [Instalare, punere în funcțiune, testare](#)** din Caietul de sarcini). Ofertanții trebuie să își asume în cuprinsul propunerilor tehnice îndeplinirea acestei cerințe.



12.5 Anexa 5 - Algoritmul de calcul aferent criteriului de atribuire

12.5.1 Lotul I: Soluție de detecție avansată împotriva amenințărilor cibernetice (APT)

Denumire factor evaluare:	Descriere:	Pondere
Prețul ofertei	Componentă financiară	60%
Algoritm de calcul: <i>Punctajul se acordă astfel:</i> a) Pentru cel mai scazut dintre preturi se acorda punctajul maxim alocat; b) Pentru celelalte preturi oferate punctajul $P(n)$ se calculeaza proportional, astfel: $P(n) = (\text{Pret minim ofertat} / \text{Pret } n) \times \text{punctaj maxim alocat}$.		
Denumire factor evaluare:	Descriere:	Pondere
Capacitatea de analiză a soluției de detecție APT	Componentă tehnică	20%
Algoritm de calcul: <i>Punctajul se acordă astfel:</i> a) Pentru soluția care folosește senzor APT dimensionat cu o capacitate de 4.5 Gbps, va fi declarată conformă și punctată cu 0 puncte; b) Pentru soluția care folosește senzor APT dimensionat cu o capacitate mai mare, respectiv în plus cu 250 Mbps față de cerințele minime din caietul de sarcini de minim 4.5 Gbps, se acordă 10 puncte; c) Pentru soluția care folosește senzor APT dimensionat cu o capacitate mai mare, respectiv în plus cu 500 Mbps față de cerințele minime din caietul de sarcini de minim 4.5 Gbps, se acordă 20 puncte.		
Observații: 1. Oferta care nu respectă cerința minimă a caietului de sarcini privind cantitatea traficului de date analizat a soluției de detecție APT, respectiv de minim 4.5 Gbps, va fi declarată neconformă. 2. Oferta care folosește senzor APT dimensionat cu o capacitate mai mare respectiv în plus cu mai mult de 500 Mbps față de cerințele minime din caietul de sarcini de minim 4.5 Gbps, nu va fi punctată suplimentar (se acordă punctajul maxim alocat). 3. Ponderea de 20% stabilită pentru acest factor de evaluare reflectă importanța caracteristicii funcționale de detectare a atacurilor de nivel avansat și reprezintă un avantaj calitativ prin care autoritatea contractantă se asigură de blocarea amenințărilor cibernetice în timp real.		



MINISTERUL AFACERILOR EXTERNE

Denumire factor evaluare:	Descriere:	Pondere
Număr de conexiuni pe minut al soluției de detecție APT	Componentă tehnică	20%
Algoritm de calcul: Punctajul se acordă astfel: a) Pentru soluția care folosește senzor APT ce suportă un număr de conexiuni pe minut de 230000, va fi declarată conformă și punctată cu 0 puncte; b) Pentru soluția care folosește senzor APT dimensionat cu un număr mai mare de conexiuni pe minut, respectiv în plus cu 10000 față de cerințele minime din caietul de sarcini de minim 230000, se acordă 10 puncte; c) Pentru soluția care folosește senzor APT dimensionat cu un număr mai mare de conexiuni pe minut, respectiv în plus cu 20000 față de cerințele minime din caietul de sarcini de minim 230000, se acordă 20 puncte.		
Observații: 1. Oferta care nu respectă cerința minimă a caietului de sarcini privind numărul de conexiuni pe minut al soluției senzorului APT, respectiv de minim 230000, va fi declarată neconformă. 2. Oferta care folosește senzor APT dimensionat cu un număr mai mare de conexiuni pe minut, respectiv în plus cu mai mult de 20000 față de cerințele minime din caietul de sarcini de minim 230000 de conexiuni pe minut, nu va fi punctată suplimentar (se acordă punctajul maxim alocat). 3. Ponderea de 20% stabilită pentru acest factor de evaluare reflectă importanța caracteristicii funcționale de detectare a atacurilor de nivel avansat și reprezintă un avantaj calitativ prin care autoritatea contractantă se asigură de blocarea amenințărilor cibernetice în timp real.		

Desemnarea ofertei câștigătoare:

Atribuirea contractului de achiziție publică, aferent acestui lot, se face pe baza criteriului „cel mai bun raport calitate-preț”. În acest caz, evaluarea ofertelor se realizează prin acordarea, pentru fiecare ofertă în parte, a unui punctaj rezultat ca urmare a aplicării algoritmului de calcul stabilit în documentația de atribuire. Clasamentul ofertelor se stabilește prin ordonarea descrescătoare a punctajelor respective, oferta câștigătoare fiind cea de pe primul loc, respectiv cea cu cel mai mare punctaj. În cazul în care două sau mai multe oferte sunt clasate pe primul loc, cu punctaje egale, departajarea se va face având în vedere punctajul obținut la factorii de evaluare în ordinea descrescătoare a ponderilor acestora. În situația în care egalitatea se menține, autoritatea contractantă are dreptul să solicite noi propuneri financiare, și oferta câștigătoare va fi desemnată cea cu propunerea financiară cea mai mică.



MINISTERUL AFACERILOR EXTERNE

12.5.2 Lotul II: Soluție pentru management centralizat a incidentelor de securitate (SIEM)

Denumire factor evaluare:	Descriere:	Pondere
Prețul ofertei	Componentă financiară	60%
Algoritm de calcul: <i>Punctajul se acordă astfel:</i> a) Pentru cel mai scazut dintre preturi se acorda punctajul maxim alocat; b) Pentru celelalte preturi ofertate punctajul $P(n)$ se calculeaza proportional, astfel: $P(n) = (\text{Pret minim ofertat} / \text{Pret } n) \times \text{punctaj maxim alocat}$.		
Denumire factor evaluare:	Descriere:	Pondere
Accesul și integrarea soluției SIEM de către ofertant cu surse de tip Threat Intelligence	Componentă tehnică	20%
Algoritm de calcul a) Pentru neintegrarea soluției de catre ofertant cu nicio sursă de tipul Threat Intelligence, se acordă 0 puncte. b) Pentru integrarea și accesul soluției SIEM cu o sursă de tipul Threat Intelligence de către ofertant, se acordă 10 puncte. c) Pentru integrarea și accesul SIEM soluției cu 2 surse de tipul Threat Intelligence feeds de către ofertant, se acordă 20 puncte.		
Observații: 1. Ponderea de 20% stabilită pentru acest factor de evaluare reflectă importanța caracteristicii funcționale de integrare a soluției SIEM cu feed-uri de tip Threat Intelligence și reprezintă un avantaj calitativ prin care autoritatea contractantă se asigură de îmbunătățirea vizibilității amenințărilor cibernetice.		
Denumire factor evaluare:	Descriere:	Pondere
Numărul de agenți avansați al soluției SIEM	Componentă tehnică	10%
Algoritm de calcul: <i>Punctajul se acordă astfel:</i>		



MINISTERUL AFACERILOR EXTERNE

- a) Pentru oferta ce include un număr de 150 de agenți avansați Windows/Linux al soluției SIEM, va fi declarată conformă și punctată cu 0 puncte;
- b) Pentru oferta ce include un număr mai mare de agenți avansați Windows/Linux al soluției SIEM, respectiv în plus cu 50 față de cerințele minime din caietul de sarcini de minim 150, se acordă 5 puncte;
- c) Pentru oferta ce include un număr mai mare de agenți avansați Windows/Linux al soluției SIEM, respectiv în plus cu 100 față de cerințele minime din caietul de sarcini de minim 150, se acordă 10 puncte.

Observații:

- 1. Oferta care nu respectă cerința minimă a caietului de sarcini privind numărul de agenți avansați Windows/Linux al soluției SIEM, respectiv de minim 150, va fi declarată neconformă.
- 2. Oferta care include un număr mai mare de agenți avansați Windows/Linux, respectiv în plus cu mai mult de 100 față de cerințele minime din caietul de sarcini de minim 150 de agenți avansați Windows/Linux nu va fi punctată suplimentar (se acordă punctajul maxim alocat).
- 3. **Ponderea de 10%** stabilită pentru acest factor de evaluare reflectă importanța caracteristicii funcționale de agenți avansați Windows/Linux al soluției SIEM și reprezintă un avantaj calitativ prin care autoritatea contractantă se asigură de îmbunătățirea vizibilității amenințărilor cibernetice avansate.

Denumire factor evaluare:	Descriere:	Pondere
Numărul de evenimente pe secundă (EPS) al soluției SIEM	Componentă tehnică	10%

Algoritm de calcul: Punctajul se acordă astfel:

- a) Pentru oferta ce include un număr de 12400 evenimente pe secundă al soluției SIEM, va fi declarată conformă și punctată cu 0 puncte;
- b) Pentru oferta ce include un număr mai mare de evenimente pe secundă al soluției SIEM, respectiv în plus cu 500 EPS față de cerințele minime din caietul de sarcini de minim 12400, se acordă 5 puncte;
- c) Pentru oferta ce include un număr mai mare de evenimente pe secundă al soluției SIEM, respectiv în plus cu 1000 EPS față de cerințele minime din caietul de sarcini de minim 12400, se acordă 10 puncte.

Observații:

- 1. Oferta care nu respectă cerința minimă a caietului de sarcini privind numărul de evenimente pe secundă al soluției SIEM, respectiv de minim 12400, va fi declarată neconformă.



MINISTERUL AFACERILOR EXTERNE

2. Oferta care include un număr mai mare de evenimente pe secundă al soluției SIEM, respectiv în plus cu mai mult de 1000 EPS față de cerințele minime din caietul de sarcini de minim 12400 de EPS, nu va fi punctată suplimentar (se acordă punctajul maxim alocat).
3. **Ponderea de 10%** stabilită pentru acest factor de evaluare reflectă importanța caracteristicii funcționale de colectare a alertelor generate de toate echipamentele și soluțiile de securitate și reprezintă un avantaj calitativ prin care autoritatea contractantă se asigură de îmbunătățirea vizibilității amenințărilor cibernetice.

Desemnarea ofertei câștigătoare:

Atribuirea contractului de achiziție publică, aferent acestui lot, se face pe baza criteriului „cel mai bun raport calitate-preț”. În acest caz, evaluarea ofertelor se realizează prin acordarea, pentru fiecare ofertă în parte, a unui punctaj rezultat ca urmare a aplicării algoritmului de calcul stabilit în documentația de atribuire. Clasamentul ofertelor se stabilește prin ordonarea descrescătoare a punctajelor respective, oferta câștigătoare fiind cea de pe primul loc, respectiv cea cu cel mai mare punctaj. În cazul în care două sau mai multe oferte sunt clasate pe primul loc, cu punctaje egale, departajarea se va face având în vedere punctajul obținut la factorii de evaluare în ordinea descrescătoare a ponderilor acestora. În situația în care egalitatea se menține, autoritatea contractantă are dreptul să solicite noi propuneri financiare, și oferta câștigătoare va fi desemnată cea cu propunerea financiară cea mai mică.

12.5.3 Lotul III: Soluție de control a dispozitivelor (Device Control)

Denumire factor evaluare:	Descriere:	Pondere
Prețul ofertei	Componentă financiară	60%
Algoritm de calcul: Punctajul se acordă astfel: a) Pentru cel mai scăzut dintre preturi se acorda punctajul maxim alocat; b) Pentru celelalte preturi ofertate punctajul $P(n)$ se calculeaza proportional, astfel: $P(n) = (\text{Pret minim ofertat} / \text{Pret } n) \times \text{punctaj maxim alocat}$.		
Denumire factor evaluare:	Descriere:	Pondere
Implementarea conceptului “Zero-Trust”	Componentă tehnică	20%



MINISTERUL AFACERILOR EXTERNE

Algoritm de calcul: *Punctajul se acordă astfel:*

- a) *Pentru soluția care nu detine capabilități de implementare nativă a conceptului “zero-trust” prin politici și proceduri documentate de către producător, va fi declarată conformă și se acordă 0 puncte.*
- b) *Pentru soluția care detine capabilități de implementare nativă a conceptului “zero-trust” prin politici și proceduri documentate de către producător, se acordă 20 puncte.*

Observații:

Ponderea de 20% stabilită pentru acest factor de evaluare reflectă importanța caracteristicii funcționale de implementare a conceptului “zero-trust” și reprezintă un avantaj calitativ prin care autoritatea contractantă se asigură de un nivel sporit de securitate la nivelul infrastructurii IT.

Denumire factor evaluare:	Descriere:	Pondere
Numărul de administratori ce pot gestiona soluția	Componentă tehnică	10%

Algoritm de calcul: *Punctajul se acordă astfel:*

- a) *Pentru oferta care permite un număr total de 3 administratori ce pot gestiona soluția, va fi declarată conformă și punctată cu 0 puncte;*
- b) *Pentru oferta care permite un număr total de 4 administratori ce pot gestiona soluția, va fi declarată conformă și punctată cu 5 puncte;*
- c) *Pentru oferta care permite un număr total de 5 administratori ce pot gestiona soluția, va fi declarată conformă și punctată cu 10 puncte.*

Observații:

1. Oferta care nu respectă cerința minimă a caietului de sarcini privind numărul de administratori ce pot gestiona soluția, respectiv de minim 3, va fi declarată neconformă.
2. Oferta care permite un număr mai mare de 5 administratori ce pot gestiona soluția, nu va fi punctată suplimentar (se acordă punctajul maxim alocat).
3. **Ponderea de 10%** stabilită pentru acest factor de evaluare reflectă importanța caracteristicii funcționale de gestionare a soluției având un număr mai mare de administratori și reprezintă un avantaj calitativ prin care autoritatea contractantă se asigură de un nivel sporit de securitate și vizibilitate la nivelul infrastructurii IT.



MINISTERUL AFACERILOR EXTERNE

Denumire factor evaluare:	Descriere:	Pondere
Control al accesului pentru dispozitive criptate	Componentă tehnică	10%
Algoritm de calcul: Punctajul se acordă astfel: a) Pentru soluția care nu deține capabilități de implementare nativă, de la producător, a controlului accesului la fișiere pentru dispozitive ce sunt criptate cu BitLocker, va fi declarată conformă și se acordă 0 puncte. b) Pentru soluția care deține capabilități de implementare nativă, de la producător, a controlului accesului la fișiere pentru dispozitive ce sunt criptate cu BitLocker, se acordă 10 puncte.		
Observații: Ponderea de 10% stabilită pentru acest factor de evaluare reflectă importanța caracteristicii funcționale de implementare a controlului de acces la fișiere pentru dispozitive criptate și reprezintă un avantaj calitativ prin care autoritatea contractantă se asigură de un nivel sporit de securitate la nivelul infrastructurii IT.		

Desemnarea ofertei câștigătoare:

Atribuirea contractului de achiziție publică, aferent acestui lot, se face pe baza criteriului „cel mai bun raport calitate-preț”. În acest caz, evaluarea ofertelor se realizează prin acordarea, pentru fiecare ofertă în parte, a unui punctaj rezultat ca urmare a aplicării algoritmului de calcul stabilit în documentația de atribuire. Clasamentul ofertelor se stabilește prin ordonarea descrescătoare a punctajelor respective, oferta câștigătoare fiind cea de pe primul loc, respectiv cea cu cel mai mare punctaj. În cazul în care două sau mai multe oferte sunt clasate pe primul loc, cu punctaje egale, departajarea se va face având în vedere punctajul obținut la factorii de evaluare în ordinea descrescătoare a ponderilor acestora. În situația în care egalitatea se menține, autoritatea contractantă are dreptul să solicite noi propuneri financiare, și oferta câștigătoare va fi desemnată cea cu propunerea financiară cea mai mică.



MINISTERUL AFACERILOR EXTERNE

12.5.4 Lotul IV: Soluție de control a accesului în rețele (NAC)

Denumire factor evaluare:	Descriere:	Pondere
Prețul ofertei	Componentă financiară	60%
Algoritm de calcul: Punctajul se acordă astfel: a) Pentru cel mai scazut dintre preturi se acorda punctajul maxim alocat; b) Pentru celelalte preturi ofertate punctajul $P(n)$ se calculeaza proportional, astfel: $P(n) = (\text{Pret minim ofertat} / \text{Pret } n) \times \text{punctaj maxim alocat}$.		
Denumire factor evaluare:	Descriere:	Pondere
Numărul de dispozitive de tip endpoint licențiat al echipamentului dedicat implementării politicilor de acces în rețea	Componentă tehnică	20%
Algoritm de calcul: Punctajul se acordă astfel: a) Pentru oferta ce include un număr de 1000 de dispozitive de tip endpoint licențiat al echipamentului dedicat implementării politicilor de acces în rețea, va fi declarată conformă și punctată 0 puncte; b) Pentru oferta ce include un numar mai mare de dispozitive de tip endpoint licențiat al echipamentului dedicat implementării politicilor de acces în rețea, respectiv în plus cu 1000 față de cerințele minime din caietul de sarcini de minim 1000, se acordă 10 puncte; c) Pentru oferta ce include un număr mai mare de dispozitive de tip endpoint licențiat al echipamentului dedicat implementării politicilor de acces în rețea, respectiv în plus cu 2000 față de cerințele minime din caietul de sarcini de minim 1000, se acordă 20 puncte.		
Observații: 1. Oferta care nu respectă cerința minimă a caietului de sarcini privind numărul de dispozitive de tip endpoint licențiat al echipamentului dedicat implementării politicilor de acces în rețea, respectiv de minim 1000, va fi declarată neconformă. 2. Oferta care include un număr mai mare de dispozitive de tip endpoint licențiat al echipamentului dedicat implementării politicilor de acces în rețea, respectiv în plus cu mai mult de 2000 dispozitive față de cerințele minime din caietul de sarcini de minim 1000 de dispozitive, nu va fi punctată suplimentar (se acordă punctajul maxim alocat).		



MINISTERUL AFACERILOR EXTERNE

Denumire factor evaluare:	Descriere:	Pondere
<i>Cantitatea de loguri ce poate fi preluată de către platforma de logare și analiza</i>	<i>Componentă tehnică</i>	20%
Algoritm de calcul: Punctajul se acordă astfel: a) <i>Pentru oferta ce include cantitatea de loguri de 25 GB/zi ce poate fi preluată de către platforma de logare și analiză, va fi declarată conformă și punctată cu 0 puncte;</i> b) <i>Pentru oferta ce include o cantitate mai mare de loguri ce poate fi preluată de către platforma de logare și analiză, respectiv în plus cu 25 GB/zi față de cerințele minime din caietul de sarcini de minim 25 GB/zi, se acordă 10 puncte.</i> c) <i>Pentru oferta ce include o cantitate mai mare de loguri ce poate fi preluată de către platforma de logare și analiză, respectiv în plus cu 50 GB/zi față de cerințele minime din caietul de sarcini de minim 25 GB/zi, se acordă 20 puncte.</i>		
Observații: 1. Oferta care nu respectă cerința minimă a caietului de sarcini privind cantitatea de loguri ce poate fi preluată de către platforma de logare și analiză, respectiv de minim 25 GB/zi, va fi declarată neconformă. 2. Oferta care include un număr mai mare de loguri ce poate fi preluată de către platforma de logare și analiză, respectiv în plus cu mai mult de 50 GB/zi față de cerințele minime din caietul de sarcini de minim 25 GB/zi de dispozitive, nu va fi punctată suplimentar (se acordă punctajul maxim alocat).		



MINISTERUL AFACERILOR EXTERNE

Desemnarea ofertei câștigătoare:

Atribuirea contractului de achiziție publică, aferent acestui lot, se face pe baza criteriului „cel mai bun raport calitate-preț”. În acest caz, evaluarea ofertelor se realizează prin acordarea, pentru fiecare ofertă în parte, a unui punctaj rezultat ca urmare a aplicării algoritmului de calcul stabilit în documentația de atribuire. Clasamentul ofertelor se stabilește prin ordonarea descrescătoare a punctajelor respective, oferta câștigătoare fiind cea de pe primul loc, respectiv cea cu cel mai mare punctaj. În cazul în care două sau mai multe oferte sunt clasate pe primul loc, cu punctaje egale, departajarea se va face având în vedere punctajul obținut la factorii de evaluare în ordinea descrescătoare a ponderilor acestora. În situația în care egalitatea se menține, autoritatea contractantă are dreptul să solicite noi propuneri financiare, și oferta câștigătoare va fi desemnată cea cu propunerea financiară cea mai mică.

Avizat,

Daniela Bodeanu

Manager de proiect

BODEANU
DANIELA-
FLORINA

Digitally signed by
BODEANU DANIELA-
FLORINA
Date: 2025.10.16
11:57:23 +03'00'