

Răspunsuri la solicitările de clarificare pentru achiziție**având ca obiect****„Servicii de monitorizare si raspuns la incidente de securitate cibernetica (SOC)”**

Vă comunicăm mai jos întrebările primite și răspunsurile din partea BID:

1. Modelul serviciului solicitat

Vă rugăm să clarificați dacă prestatorul va furniza exclusiv servicii SOC utilizând platformele existente ale BID sau dacă oferta trebuie să includă și platforme, infrastructură ori licențe proprii SIEM, SOAR, MDR sau alte componente tehnologice. Dacă se dorește un model hibrid, vă rugăm să delimitați componentele furnizate de fiecare parte.

Argument: De acest răspuns depind arhitectura soluției, responsabilitățile, licențele, infrastructura, resursele necesare și modelul financiar. Serviciile operate pe tehnologia BID și un serviciu furnizat pe platformele prestatorului reprezintă oferte fundamental diferite.

Raspuns BID:

Prestatorul va furniza exclusiv servicii SOC utilizand, pe cat posibil, platformele existente ale BID, insa Banca este deschisa si unui model hibrid.

Obiectul achizitiei il reprezinta furnizarea de servicii SOC. Prestatorul va utiliza, integra si opera, in masura posibilului, platformele si componentele de securitate existente ale BID.

In situatia in care, pentru indeplinirea cerintelor functionale si a nivelurilor de servicii solicitate, prestatorul considera necesara utilizarea unor platforme, licente sau componente tehnologice proprii (SIEM, SOAR sau altele), acestea vor fi incluse si detaliate distinct in oferta, impreuna cu responsabilitatile aferente fiecarei parti.

BID nu impune in aceasta etapa un model tehnic prestabilit. Ofertantii sunt invitati sa propuna solutia pe care o considera optima pentru indeplinirea cerintelor din documentatia de atribuire.

Banca va evalua si compara solutiile propuse din punct de vedere tehnic, operational si financiar si va selecta varianta care ofera cel mai bun raspuns la cerintele si obiectivele sale.

2. Soluțiile existente în cadrul BID

Vă rugăm să comunicați produsele și versiunile soluțiilor SIEM, SOAR, EDR/XDR, ITSM, Syslog și ale celorlalte sisteme cu care prestatorul trebuie să opereze sau să se integreze, inclusiv:

- ***arhitectura și modul de implementare;***

Raspuns BID:

Banca considera ca informatiile solicitate depasesc nivelul de detaliu necesar pentru elaborarea ofertei in cadrul prezentei proceduri. Ofertantii trebuie sa isi fundamenteze oferta pe cerintele prevazute in documentatia de atribuire si pe capacitatea de a furniza

servicii SOC într-un mediu enterprise standard, demonstrând flexibilitatea soluției propuse de a se integra cu tehnologii utilizate în mod curent în organizații de dimensiuni și complexitate similare.

Informațiile tehnice detaliate referitoare la infrastructura și soluțiile utilizate de Banca nu fac obiectul prezentei etape și vor fi comunicate, după caz, doar ofertantului desemnat castigator, cu respectarea cerințelor de securitate și confidențialitate aplicabile.

- **locația componentelor;**
- **licențele și capacitățile disponibile;**
- **API-urile și conectorii existenți;**

Raspuns BID:

Banca considera ca informațiile solicitate depășesc nivelul de detaliu necesar pentru elaborarea ofertei în cadrul prezentei proceduri. Ofertantii trebuie să își fundamenteze oferta pe cerințele prevăzute în documentația de atribuire și pe capacitatea de a furniza servicii SOC într-un mediu enterprise standard, demonstrând flexibilitatea soluției propuse de a se integra cu tehnologii utilizate în mod curent în organizații de dimensiuni și complexitate similare.

Informațiile tehnice detaliate referitoare la infrastructura și soluțiile utilizate de Banca nu fac obiectul prezentei etape și vor fi comunicate, după caz, doar ofertantului desemnat castigator, cu respectarea cerințelor de securitate și confidențialitate aplicabile.

- **eventualele restricții de acces și integrare.**

Raspuns BID:

Accesul Prestatorului va fi acordat exclusiv pe baza principiului least privilege, prin mecanisme RBAC și autentificare multifactor. Accesul la date, sisteme și funcționalități va fi limitat la activitățile necesare furnizării serviciului SOC și va respecta politicile de securitate ale Bancii. Accesul permanent va fi facilitat printr-un VPN Site-to-Site, dacă va fi necesar.

Informațiile sensibile pot fi furnizate într-o anexă confidențială.

Argument: De tehnologiile existente depind competențele și certificările necesare echipei, posibilitatea și complexitatea integrărilor, eficiența operațională, necesarul de dezvoltare, compatibilitatea soluțiilor și costul serviciului.

3. Dimensionarea serviciului

Vă rugăm să furnizați:

- **volumul mediu și maxim de loguri, în EPS și GB/zi;**
- **numărul și tipurile celor aproximativ 700 de surse;**
- **numărul de endpoint-uri, servere, echipamente de rețea, utilizatori, identități și workload-uri cloud;**
- **volumul mediu și maxim de alerte și incidente;**
- **distribuția alertelor și incidentelor pe severități;**
- **perioada de retenție online și arhivată;**
- **variațiile maxime de volum estimate.**

Argument: Aceste date determină capacitatea tehnică, necesarul de stocare și licențiere, numărul de analiști L1–L3, încărcarea operațională și prețul. Numărul de surse, fără tipul și volumul lor, nu reprezintă o bază de dimensionare.

Raspuns BID:

Banca nu considera necesara furnizarea in etapa de ofertare a unor informatii detaliate privind volumele de date procesate, parametrii operationali sau dimensiunea infrastructurii. Ofertantii trebuie sa propuna un model de servicii si de tarificare care sa permita scalarea serviciului in functie de evolutia necesitatilor Bancii si sa ofere transparenta privind impactul financiar al eventualelor modificari ale volumului de date, numarului de active monitorizate sau altor parametri relevanti. Aceasta abordare va permite Bancii sa evalueze in mod comparabil si obiectiv ofertele primite, inclusiv din perspectiva flexibilitatii, scalabilitatii si predictibilitatii costurilor pe durata contractuala.

Banca apreciaza ca un prestator cu experienta in furnizarea de servicii SOC trebuie sa isi poata fundamenta oferta pe cerintele functionale si operationale prevazute in documentatia de atribuire, fara a fi necesara divulgarea, in etapa de ofertare, a unor informatii detaliate privind infrastructura, arhitectura de securitate sau volumele operationale ale institutiei. Aceste informatii vor putea fi puse la dispozitie doar in masura necesara pentru implementarea serviciilor si exclusiv dupa finalizarea procedurii de atribuire, cu respectarea cerintelor de securitate si confidentialitate aplicabile.

4. Situația actuală și obiectul preluării

Vă rugăm să precizați dacă BID beneficiază în prezent de un SOC intern sau externalizat și ce componente trebuie preluate, migrate, păstrate, dezvoltate sau înlocuite, inclusiv:

- **reguli și use-case-uri de detecție;**
- **playbook-uri;**
- **integrări și parsere;**
- **incidente și tichete deschise;**
- **date și documentație istorică;**
- **processe și proceduri operaționale.**

Argument: Efortul, calendarul și riscurile diferă semnificativ între preluarea unui serviciu matur și construirea unui SOC operațional de la zero. Fără situația inițială, nu poate fi estimat obiectul implementării sau al tranziției.

Raspuns BID:

Banca nu va furniza in etapa de ofertare informatii detaliate privind servicii existente, configuratii, reguli de detectie, playbook-uri, integrari, incidente, documentatie sau proceduri operationale interne.

Oferta va fi fundamentata pe cerintele functionale si operationale prevazute in documentatia de atribuire. Informatiile suplimentare necesare implementarii vor fi furnizate ulterior, dupa finalizarea procedurii de atribuire si cu respectarea cerintelor de securitate si confidentialitate aplicabile.

5. Responsabilitățile BID și ale prestatorului

Documentația precizează că „responsabilitatea pentru onboarding-ul, configurarea și mentenanța surselor de date (~700 de surse) revine Băncii”, dar solicită prestatorului monitorizarea colectării, identificarea erorilor de ingestie și parsare, validarea scenariilor și optimizarea regulilor.

Vă rugăm să delimitați responsabilitățile pentru:

- **conectarea și configurarea surselor;**

Raspuns BID:

Banca

- **dezvoltarea și mentenanța parserelor și conectorilor;**

Raspuns BID:

Banca, ținând cont de recomandările oferite de către Prestator;

- **calitatea și completitudinea logurilor;**

Raspuns BID:

Banca - responsabilă pentru completitudine la nivel de surse și Prestatorul - responsabil cu monitorizarea gradului de completitudine

- **administrarea platformelor;**

Raspuns BID:

Banca

- **dezvoltarea și optimizarea regulilor și use-case-urilor;**

Raspuns BID:

Prestator

- **remediarea erorilor de colectare;**

Raspuns BID:

Banca, dar pot fi notificate și de Prestator

- **integrarea surselor noi;**

Raspuns BID:

Banca

- **impactul indisponibilității surselor asupra SLA-urilor.**

Argument: Prestatorul nu poate estima efortul și nu poate asuma SLA-uri pentru activități sau componente pe care nu le controlează. Delimitarea responsabilităților trebuie stabilită înainte de ofertare, nu după atribuire.

Raspuns BID:

Indisponibilitatea surselor aferente activitatilor SOC nu va fi imputabila prestatorului in perioadele in care sursele de date nu furnizeaza informatiile necesare monitorizarii. Perioadele de indisponibilitate ale surselor vor fi excluse din calculul disponibilitatii aferente acestor componente.

Responsabilitatea pentru onboarding-ul, configurarea, administrarea si mentenanta surselor de date revine Bancii.

Prestatorul va avea responsabilitatea monitorizarii colectarii si calitatii datelor necesare activitatilor SOC, identificarii si notificarii incidentelor de ingestie sau parsare, validarii functionarii scenariilor de detectie si formularii recomandarilor de optimizare.

6. SOAR, automatizare și răspuns la incidente

Vă rugăm să precizați dacă BID deține o platformă SOAR și, în caz afirmativ, produsul, versiunea, licențele, integrările și playbook-urile disponibile.

De asemenea, vă rugăm să definiți:

- ***sistemele asupra cărora prestatorul poate interveni;***
- ***acțiunile care pot fi executate automat;***
- ***acțiunile care necesită aprobarea BID;***
- ***numărul și tipurile de playbook-uri care trebuie dezvoltate;***
- ***matricea de aprobare;***
- ***accesul privilegiat acordat prestatorului;***
- ***responsabilitatea pentru efectele acțiunilor de containment;***
- ***existența unui mediu de test și a mecanismelor de rollback.***

Argument: Automatizarea răspunsului presupune integrări, privilegii și riscuri operaționale concrete. Fără aceste informații nu pot fi evaluate fezabilitatea, efortul de dezvoltare, răspunderea prestatorului sau impactul potențial asupra sistemelor BID.

Raspuns BID:

Banca nu considera necesara furnizarea in etapa de ofertare a informatiilor solicitate privind platforme SOAR, playbook-uri, privilegii de acces, matrice de aprobare, mecanisme de automatizare sau procese de raspuns la incidente.

Oferta trebuie fundamentata pe cerintele prevazute in documentatia de atribuire si pe capacitatea ofertantului de a furniza serviciile solicitate intr-un mediu enterprise standard.

Aspectele de implementare si operare vor fi stabilite ulterior atribuirii contractului, in limitele cerintelor de securitate si confidentialitate aplicabile.

7. Definirea și măsurarea SLA/KPI**Documentația solicită:**

- **MTTD ≤ 15 minute;**
- **MTTR/Notify ≤ 30 minute;**

- minimum 95% dintre alertele critice analizate și tratate în mai puțin de 15 minute;
- FPR < 10%.

Vă rugăm să definiți pentru fiecare indicator:

- **momentul de început și momentul de sfârșit al măsurării;**

Raspuns BID:

MTTD - Intervalul de timp dintre generarea alertei și inițierea activităților de investigare de către analistul SOC. MTTR - intervalul de timp dintre generarea alertei și notificarea Băncii cu privire la incidentul confirmat sau suspiciunea rezonabilă care necesită acțiune din partea Băncii.

- **sistemul care constituie sursa oficială; SIEM/ITSM + EDR/XDR din premisele Băncii**
- **perioada și formula de calcul;**
- **semnificația exactă a termenilor „analizată” și „tratată”;**

Raspuns BID:

„Analizată” - efectuată analiza inițială, stabilită concluzia investigației și „tratată” - după caz, finalizate activitățile din răspunderea prestatorului: a fost transmisă notificarea/incidentul către reprezentanții desemnați ai Băncii.

- **excluderile aplicabile;**

Raspuns BID:

Din calculul indicatorilor de performanță vor fi excluse situațiile aflate în afara controlului prestatorului (ex: indisponibilitatea surselor de date, a platformelor sau a infrastructurii administrate de Bancă, întreruperi de comunicații, întârzierile generate de acțiuni aflate în responsabilitatea Băncii).

- **penalitățile asociate.**

Raspuns BID:

Mecanismul de aplicare a penalităților va fi stabilit în documentația contractuală, în corelație cu indicatorii de performanță agreeți, modalitatea de măsurare a acestora și excluderile aplicabile.

Argument: SLA-urile nu pot fi asumate contractual fără definiții și o metodă obiectivă de măsurare. Prestatorul nu poate garanta timpi influențați de latența surselor, performanța platformelor sau aprobările BID.

8. Threat hunting și threat intelligence

Vă rugăm să precizați:

- **frecvența și volumul minim al activităților de threat hunting;**
- **numărul minim de ipoteze, investigații sau campanii;**
- **domeniul tehnic și activele acoperite;**
- **livrabilele și criteriile de acceptanță;**

- **sursele comerciale de threat intelligence disponibile la BID;**
- **sursele și licențele care trebuie furnizate de prestator;**
- **cerințele concrete privind monitorizarea dark web.**

Argument: „Threat hunting proactiv” poate reprezenta o activitate periodică limitată sau o funcție permanentă și dedicată. Volumul, sursele și frecvența determină resursele, licențele și costul.

Raspuns BID:

Banca nu stabilește în această etapă valori minime pentru frecvența activităților de threat hunting, numărul de investigații, sursele de threat intelligence, licențele utilizate sau cerințele de monitorizare dark web. Aceste elemente fac parte din propunerea tehnică a ofertantului și vor fi evaluate de Bancă din perspectiva relevanței, maturității, eficienței operaționale și valorii adăugate aduse serviciului SOC

9. Implementare și acceptanță

Vă rugăm să precizați:

- **termenul maxim de operaționalizare;**
- **data estimată de începere;**

Raspuns BID:

imediat după finalizarea achizitiei și semnarea contractului.

- **perioada de tranziție, shadowing și hypercare;**

Raspuns BID:

estimam o perioadă de până la 3 luni de la data începerii serviciului, durata exactă urmând a fi stabilită împreună cu ofertantul desemnat câștigător în funcție de mai multe criterii.

- **dependențele și termenele aflate în responsabilitatea BID;**

Raspuns BID:

vor fi comunicate în etapa de implementare doar activitățile aflate în responsabilitatea directă a Băncii

- **lista surselor și use-case-urilor care fac obiectul acceptanței;**

Raspuns BID:

vor fi stabilite și agreate în cadrul fazei de implementare, în funcție de soluția și abordarea propuse de ofertantul desemnat câștigător.

- **scenariile de test**
- **criteriile obiective de succes;**
- **termenul maxim al acceptanței;**
- **tratamentul întârzierilor sau neconformităților care nu sunt imputabile prestatorului.**

Argument: Fără un obiect și criterii de acceptanță măsurabile, calendarul și prețul implementării nu pot fi estimate, iar acceptanța poate depinde de elemente aflate în afara controlului prestatorului.

Raspuns BID:

Banca nu stabilește în această etapă lista detaliată a surselor, use-case-urilor, scenariilor de test sau criteriilor de acceptanță. Ofertanții sunt invitați să își prezinte metodologia de implementare, testare și punere în funcțiune a serviciului. Elementele operaționale și criteriile finale de acceptanță vor fi definite împreună cu ofertantul desemnat câștigător, în funcție de soluția propusă și de cerințele Băncii.

10. Modelul financiar și cantitățile evaluate

Documentația solicită „preț per MD/FTE”, deși obiectul achiziției este un serviciu SOC 24/7/365.

Vă rugăm să clarificați:

- **dacă trebuie oferat un abonament lunar/anual sau tarife MD/FTE;**
- **numărul estimat de MD și FTE;**
- **profilurile L1, L2 și L3 pentru care trebuie prezentate tarife;**
- **distribuția estimată a resurselor;**
- **cantitățile utilizate pentru evaluare;**
- **modul de calcul al prețului total;**
- **tratamentul costurilor de implementare, licențelor, infrastructurii și serviciilor suplimentare;**
- **mecanismul de ajustare a prețului în cazul modificării volumelor.**

Argument: Un tarif MD/FTE fără cantități nu permite calcularea prețului total și nici compararea ofertelor. În plus, un serviciu gestionat 24/7 este diferit comercial de furnizarea unor resurse în regim Time & Materials.

Raspuns BID:

In caietul de sarcini la „Capitolul 7. Criteriul de atribuire – b. Algoritmi de calcul

Pret – 50%” se pot identifica detaliile introduse la solicitarea de clarificare.

11. Formula de evaluare

În secțiunea 7, ponderile sunt prezentate astfel:

- **„Prețul ofertei – 50%”;**
- **„Îndeplinirea cerințelor tehnice – 40%”;**
- **„KPI operaționali – 10%”.**

Ulterior, formula este prezentată astfel:

- **„PI = NI × 40%”;**
- **„PII = NII × 40%”;**

- „PIII = NIII × 10%”.

Această formulă aplică prețului o pondere de 40%, iar ponderile însumează 90%.

Vă rugăm să confirmați ponderile și formula corectă. Dacă se mențin ponderile declarate inițial, vă rugăm să confirmați dacă formula este:

- **PI = NI × 50%;**
- **PII = NII × 40%;**
- **PIII = NIII × 10%.**

Vă rugăm să confirmați și dacă punctajul maxim este 10 sau 100 de puncte. --> 10

Argument: Formula publicată nu corespunde ponderilor declarate și poate conduce la calcularea diferită a punctajului și la imposibilitatea verificării rezultatului evaluării.

Raspuns BID:

In caietul de sarcini la „Capitolul 7. Criteriul de atribuire – b. Algoritmi de calcul

II. KPI Operationali – 10% ” se pot identifica modificarile introduse conform solicitarii.

12. Evaluarea cerințelor tehnic

Documentația prevede acordarea a 6–10 puncte pentru cerințele „îndeplinite” și 1–5 puncte pentru cele „parțial/în curs”, fără subcriterii pentru diferențiere.

Vă rugăm să comunicați:

- **lista exactă a cerințelor punctate;**
- **ponderea fiecărei cerințe;**
- **criteriile pentru acordarea fiecărui punctaj;**
- **dovezile care trebuie prezentate;**
- **modul de evaluare a criteriilor generale, eliminatorii și de diferențiere;**
- **dacă funcționalitățile „în curs” pot fi finalizate după atribuire și în ce termen.**

Argument: În lipsa unor subcriterii măsurabile, diferența dintre 6 și 10 puncte este subiectivă, iar ofertanții nu pot cunoaște ce trebuie să demonstreze pentru obținerea punctajului maxim.

Raspuns BID:

Cerintele care fac obiectul evaluării sunt exact cele prevazute in documentatia din Caietul de Sarcini.

Evaluarea va fi realizata pe baza gradului de conformitate, a nivelului de maturitate, a completitudinii raspunsului, a capabilitatilor demonstrate si a valorii adaugate aduse de solutia propusa in raport cu cerintele formulate de Banca.

Punctajele din intervalul superior (6-10) vor fi acordate pentru cerintele indeplinite, diferentierea realizandu-se in functie de nivelul de acoperire, maturitatea, nivelul de detaliu si beneficiile solutiei propuse. Punctajele din intervalul inferior (1-5) vor fi acordate

situațiilor în care cerința este îndeplinită parțial, este disponibilă doar prin dezvoltări ulterioare sau presupune limitări operaționale ori funcționale.

Dovezile care susțin îndeplinirea cerințelor trebuie prezentate de ofertant în cadrul propunerii tehnice și pot include descrieri funcționale, documentație tehnică, arhitecturi, studii de caz, experiența demonstrată, certificări, proceduri operaționale sau alte materiale relevante.

Criteriile eliminatorii vor fi evaluate prin raportare la cerințele minime obligatorii prevăzute în documentația de atribuire. Criteriile de diferențiere vor fi evaluate comparativ, pe baza informațiilor furnizate de ofertanți.

Funcționalitățile aflate în dezvoltare sau planificate pentru o etapă ulterioară pot fi luate în considerare în evaluare doar dacă ofertantul descrie în mod clar stadiul acestora, calendarul de implementare și impactul asupra furnizării.

13. Având în vedere că răspunsurile pot modifica substanțial arhitectura, dimensionarea și prețul serviciului, vă rugăm să aveți în vedere prelungirea termenului de depunere cu o perioadă suficientă, calculată de la publicarea răspunsurilor complete.

Răspuns BID:

A fost analizată solicitarea și s-a apreciat că răspunsurile furnizate au caracter clarificator și nu conduc la modificarea cerințelor documentației de atribuire, a obiectului contractului sau a criteriilor de evaluare.

În consecință, termenul de depunere a ofertelor rămâne neschimbat. În cazul în care, în urma procesului de clarificări, va fi identificată necesitatea unor modificări semnificative ale documentației, Banca își rezervă dreptul de a adopta măsurile corespunzătoare și de a informa toți participanții în mod nediscriminatoriu.

14. Referința :Secțiunea 4 "Livrabile"

Secțiunea 4 "Livrabile" din Caietul de Sarcini enumera o serie de documente și materiale (calendar de implementare, matrice RACI, documentație tehnică de arhitectură, matrice de severitate, lista scenariilor de detecție, proceduri de investigare/escaladare, documentație de configurare, plan de testare, raport de validare, documentație de acceptare, etc) care, prin natura lor, pot fi elaborate după cunoașterea detaliată a infrastructurii, surselor de date și a metodologiei interne a băncii. Vă rugăm să confirmați dacă aceste livrabile sunt aplicabile etapei de implementare/operationalizare a contractului, ulterior atribuirii și nu constituie documente care trebuie depuse odată cu oferta tehnică.

Răspuns BID:

Livrabilele menționate în Secțiunea 4 trebuie considerate de ofertanți ca obligatorii post etapei de atribuire și nu constituie documente care trebuie depuse odată cu oferta tehnică.

15. În document este menționată existența a ~700 surse de date pentru colectarea logurilor. Pentru estimarea volumului de evenimente și dimensionarea serviciului, vă rugăm să clarificați:

distributia aproximativă pe categorii (serve, stații de lucru, echipamente de rețea, aplicații, soluții de securitate, resurse cloud etc.);

Raspuns BID:

Banca nu considera necesara furnizarea in etapa de ofertare a unor informatii detaliate privind cu privire la infrastructura.

Banca apreciaza ca un prestator cu experienta in furnizarea de servicii SOC trebuie sa isi poata fundamenta oferta pe cerintele functionale si operationale prevazute in documentatia de atribuire, fara a fi necesara divulgarea, in etapa de ofertare, a unor informatii detaliate privind infrastructura, arhitectura de securitate sau volumele operationale ale institutiei. Aceste informatii vor putea fi puse la dispozitie doar in masura necesara pentru implementarea serviciilor si exclusiv dupa finalizarea procedurii de atribuire, cu respectarea cerintelor de securitate si confidentialitate aplicabile.

16. Volumetrie si arhitectura:

Care este volumul mediu zilnic de loguri (EPS / GB/zi)?

Exista un SIEM in productie? Daca da, ce solutie si versiune?

Sursele (~700) sunt deja onboardate in SIEM?

Exista surse cloud suplimentare in afara M365/Azure?

Raspuns BID:

Banca nu considera necesara furnizarea in etapa de ofertare a unor informatii detaliate privind cu privire la infrastructura.

Banca apreciaza ca un prestator cu experienta in furnizarea de servicii SOC trebuie sa isi poata fundamenta oferta pe cerintele functionale si operationale prevazute in documentatia de atribuire, fara a fi necesara divulgarea, in etapa de ofertare, a unor informatii detaliate privind infrastructura, arhitectura de securitate sau volumele operationale ale institutiei. Aceste informatii vor putea fi puse la dispozitie doar in masura necesara pentru implementarea serviciilor si exclusiv dupa finalizarea procedurii de atribuire, cu respectarea cerintelor de securitate si confidentialitate aplicabile.

17. Endpoint & acoperire EDR/XDR:

- **Numarul aproximativ de endpoint-uri ce necesita acoperire EDR/XDR.**
- **Exista categorii speciale (ATM, POS, servere critice, containere, VM)?**
- **Exista restrictii privind instalarea agentilor pe anumite sisteme?**

Raspuns BID:

Banca nu considera necesara furnizarea in etapa de ofertare a unor informatii detaliate privind cu privire la infrastructura.

Banca apreciaza ca un prestator cu experienta in furnizarea de servicii SOC trebuie sa isi poata fundamenta oferta pe cerintele functionale si operationale prevazute in documentatia de atribuire, fara a fi necesara divulgarea, in etapa de ofertare, a unor informatii detaliate privind infrastructura, arhitectura de securitate sau volumele operationale ale institutiei. Aceste informatii vor putea fi puse la dispozitie doar in masura necesara pentru implementarea serviciilor si exclusiv dupa finalizarea procedurii de atribuire, cu respectarea cerintelor de securitate si confidentialitate aplicabile.

18. Integrare cu infrastructura BID:

Ce solutii de securitate trebuie integrate in SOAR (AV, firewall, WAF, VPN, IAM, DLP, CASB etc.)?

Raspuns BID:

Banca nu considera necesara furnizarea in etapa de ofertare a informatiilor solicitate privind platforme SOAR, playbook-uri, privilegii de acces, matrice de aprobare, mecanisme de automatizare sau procese de raspuns la incidente.

Oferta trebuie fundamentata pe cerintele prevazute in documentatia de atribuire si sa demonstreze capacitatea solutiei propuse de integrare cu serviciile de securitate existente, in general, intr-un mediu enterprise standard, inclusiv, dar fara a se limita la AV, firewall, WAF, VPN, DLP.etc.

Informatiile detaliate necesare implementarii si operarii vor fi stabilite ulterior atribuirii contractului, in limitele cerintelor de securitate si confidentialitate aplicabile.

Prestatorul va utiliza, integra si opera, in masura posibilului, platformele si componentele de securitate existente ale BID.

KPI / SLA:

MTTR include doar notificarea sau si actiuni de containment?

MTTD se aplica doar alertelor critice sau tuturor alertelor?

FPR < 10% se calculeaza pe total alertare sau doar pe alertare critica?

Raspuns BID:

A se vedea detaliile din intrebarile anterioare.

20. Procesare date / conformitate:

Este permisa procesarea datelor in centrele din UE ale furnizorului MDR (de exp. Frankfurt)?

Raspuns BID:

Da

21. Livrabile & raportare:

• Dashboard-ul trebuie livrat in platforma BID sau poate fi accesat din portalul de management?

Raspuns BID:

Din punctul de Vedere al bancii, ambele variante sunt acceptabile.

22. Clarificari specifice MDR:

- ***BID dorește utilizarea SIEM-ului existent sau este permisă utilizarea SIEM-ului MDR?***

Raspuns BID:

BID va furniza evenimentele din soluțiile deja implementate on-prem de tip SIEM și syslog