

Răspunsuri la solicitările de clarificare pentru achiziție

având ca obiect

„Servicii de monitorizare și răspuns la incidente de securitate cibernetică (SOC)”

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

1. Caietul de Sarcini prevede, la Criteriile de Diferențiere, o structură operațională SOC organizată pe trei niveluri de competență (L1, L2, L3) și solicită exprimarea prețului în cost per MD per FTE, fără a preciza însă modelul de alocare a resurselor. Având în vedere că informațiile privind volumele de loguri, alerte și incidente nu sunt furnizate în etapa de ofertare, vă rugăm să precizați următoarele:

Vă rugăm să confirmați dacă Banca acceptă un model operațional partajat (shared), în care analiștii SOC pe cele trei niveluri de competență (L1, L2, L3) deserveșc mai mulți clienți în regim 24/7/365, cu niveluri de serviciu garantate contractual, sau dacă se solicită un model dedicat, cu resurse alocate exclusiv Băncii.

Răspuns BID:

Banca nu solicită alocarea exclusivă a resurselor SOC. Este acceptat un model operațional partajat (shared), cu respectarea SLA-urilor, a cerințelor de confidențialitate, segregare a datelor și a obligațiilor contractuale privind furnizarea serviciilor.

2. De asemenea, vă rugăm să precizați dacă modelul partajat poate fi aplicat și componentelor tehnologice proprii ale Prestatorului (ex: platforme de threat intelligence, instrumente interne de analiză, corelare, automatizare și raportare), respectiv dacă este acceptabilă operarea acestora în regim multi-tenant, cu segregare logică a datelor Băncii, sau se solicită instanțe dedicate exclusiv Băncii.

Răspuns BID: DA.

3. Model complementar de tarificare (bazat pe nr de incidente)

Caietul de Sarcini prevede exprimarea prețului în cost per MD per FTE, iar în lipsa unor date privind volumele de alerte și incidente, acest model nu reflectă întotdeauna încărcarea operațională reală a serviciului. Vă rugăm să confirmați dacă, pe lângă tariful MD/FTE utilizat pentru evaluare, ofertanții pot prezenta complementar un model de tarificare bazat pe numărul de incidente/tichete tratate.

Răspuns BID:

Da, așa cum este specificat :

„Factor de evaluare : Pretul (pret per MD / FTE, preț lunar pentru serviciu sau alt model echivalent). Oferta financiară trebuie să permită identificarea clară a:

- costului total al serviciului;
- numărului de FTE alocați;
- efortului estimat exprimat în MD;
- costului unitar per FTE și/sau MD, dacă este aplicabil;
- modului de scalare a costurilor în cazul modificării volumelor sau extinderii serviciului.)

4. Definirea și măsurarea parametrilor SLA/KPI

Răspunsul la întrebarea 7 a definit momentele de măsurare pentru MTTD și MTTR, termenii „analizată” și „tratată” și principiul excluderilor, însă perioada și formula de calcul nu au fost precizate. De asemenea, întrebările privind domeniul de aplicare al MTTD și baza de calcul a FPR (întrebarea 19) au primit un răspuns prin trimitere la clarificările anterioare, care nu conțin aceste elemente. Vă rugăm să completați:

- **Perioada și formula de calcul – perioada de raportare și modul de agregare (medie, percentilă sau procent de alerte încadrate în prag), respectiv dacă depășirea pragului pe o alertă individuală constituie neconformitate.**

Raspuns BID:

Indicatorul va fi măsurat lunar. Conformitatea se determină ca procent din numărul total de alerte critice generate în perioada de raportare pentru care timpul de analiză și tratare este sub 15 minute. Cerința este considerată îndeplinită dacă minimum 95% din totalul alertelor critice din luna de raportare respectă acest prag. Depășirea pragului pentru o alertă individuală nu constituie, în sine, neconformitate, atât timp cât indicatorul agregat lunar este respectat.

- **Domeniul de aplicare al MTTD și MTTR – dacă se aplică tuturor alertelor sau exclusiv celor critice.**

Raspuns BID:

MTTD se aplică tuturor alertelor, deoarece nivelul de severitate este stabilit în urma procesului de analiză și triere. KPI-ul privind tratarea în sub 15 minute se aplică exclusiv alertelor confirmate ca fiind critice (menționat). MTTR/Notify se aplică în funcție de severitatea incidentului și fluxurile de escaladare aferente.

- **Baza de calcul a FPR – ce se consideră fals pozitiv, cine validează încadrarea și dacă pragul de 10% se raportează la totalul alertelor sau doar la cele critice.**

Raspuns BID:

FPR se calculează la nivelul total al alertelor investigate. Fals pozitiv se considera alertă investigată de SOC care se dovedește a nu reprezenta un incident de securitate real. FPR se calculează raportat la totalul alertelor investigate în perioada de raportare. Clasificarea inițială este realizată de furnizor și poate fi validată sau nu de Bancă pe baza evidențelor disponibile.

- **Mecanismul de aplicare a excluderilor – dacă suspendarea măsurării este automată sau la solicitare și cine o constată.**

Raspuns BID:

Pot apărea ambele cazuri, cu validare comună.