

CAIET DE SARCINI

În contextul creșterii accelerate a riscurilor cibernetice, este necesară îmbunătățirea continuă a monitorizării activităților sistemelor, utilizatorilor și a celor cu drepturi privilegiate, pentru detectarea și gestionarea rapidă a incidentelor de securitate.

2. Obiectul achizitiei

Achiziția serviciilor de monitorizare și răspuns la incidente de securitate cibernetică (SOC) pe o perioadă de 12 luni cu posibilitate de prelungire automată.

3. Cerințe funcționale și tehnice

Cerințele tehnice care trebuie să fie îndeplinite de către serviciul oferit se regăsesc în tabelul de mai jos:

Criterii Generale

Criteriu	Descriere
Monitorizare 24/7/365	Monitorizare continuă (24x7x365) a evenimentelor și alertelor de securitate generate de Banca de Investiții și Dezvoltare
SLA răspuns	Exemplu: triere alertă critică < 15 min, notificare către Banca < 30 min
Răspuns la incidente	• Playbook-uri definite pt izolare și limitare impact în caz de incident • Identificarea și clasificarea incidentelor • Stabilirea severității și priorității incidentelor aliniat cu nivelurile deja definite în banca.
Threat detection	• Integrarea cu surse comerciale și open-source de informații despre amenințări. • Gestionarea Indicatorilor de Compromitere (IOC).
Threat hunting	• Proactiv bazat atât pe date externe (ex darkweb etc.) cât și interne (anomalii, comportament, identitate, logs, telemetrie etc.) • Furnizarea de informații pentru detectare și răspuns • Analiza tacticilor, tehnicilor și procedurilor atacatorilor (TTP) • Corelarea cu cadrul MITRE ATT&CK
SIEM	• Necesită capacități tehnice de acces controlat și securizat la platformele de colectare și analiză a logurilor (standard SIEM și Syslog servere), prin mecanisme RBAC și interfețe dedicate (portal, API), analiză alertelor, corelarea evenimentelor și executia de acțiuni de răspuns (unde este permisă), fără a compromite separarea responsabilităților și securitatea infrastructurii.

SOAR	• Definirea si implementarea de proceduri standardizate pentru automatizarea raspunsului la incidente, cu posibilitatea includerii etapelor de aprobare manuala atunci cand este necesar • Capabilitati de corelare a evenimentelor si alertelor provenite din multiple solutii de securitate, pentru cresterea vizibilitatii si a acuratetei detectiei. • Utilizarea tehnologiilor AI pentru prioritizarea alertelor, corelarea evenimentelor, reducerea falselor pozitive si imbunatatirea procesului de investigatie • Imbogatirea automata a alertelor (alert enrichment) prin colectarea si atasarea de informatii relevante din surse interne si externe. • Automatizarea activitatilor operationale repetitive pentru cresterea eficientei echipelor de securitate. • Executarea automata a actiunilor de raspuns si de limitare a impactului incidentelor de securitate, conform politicilor definite. • Integrarea cu platforme ITSM si cu ecosistemul de solutii de securitate existente, pentru asigurarea unui flux operational unitar si eficient.
Management incidente	• Capacitate demonstrata de operare a unui proces complet de gestionare a incidentelor de securitate, acoperind intregul ciclu de viata al incidentului: identificare si detectie, analiza si investigare, limitarea impactului (containment), remediere si recuperare, precum si realizarea activitatilor post-incident, inclusiv analiza cauzei si documentarea lectiilor invatate.
EDR/XDR	• Integrare endpoint EDR/XDR local pentru a asigura capabilitate: Citire, triere, analiza, remediere (doar pt cazuri speciale in baza unor proceduri agreate) • Capabilitatile de remediere si raspuns la incidente vor fi executate doar in cazuri specifice, pe baza unor proceduri operationale si fluxuri de aprobare agreate in prealabil cu Banca de Investitii si Dezvoltare
Control Surse	• Capacitate de monitorizare continua a disponibilitatii surselor de date si a starii colectarii logurilor, inclusiv identificarea si raportarea intreruperilor, intarzierilor, degradarii volumului de date, precum si a erorilor de colectare, ingestie sau parsare. Responsabilitatea pentru onboarding-ul, configurarea si mentenanta surselor de date (~700 de surse) revine Bancii.
Cloud support	M365 / Azure
Raportare	Rezumat zilnic (ultimele 24 de ore) Rezumat lunar executiv

Criterii Eliminatorii

Criteriu	Descriere
Indicatori agreați contractual	• Mean Time to Detect (MTTD) $\leq$ 15 minute • Mean Time to Respond / Notify (MTTR) $\leq$ 30 minute • Minimum 95% dintre alertele critice analizate și tratate în mai puțin de 15 minute • False Positive Rate (FPR) $<$ 10%
Conformitate	DORA, NIS2, ISO 27001, GDPR
Audit trail	Asigurarea unui audit trail complet și auditabil al activităților efectuate de personalul Prestatorului în cadrul furnizării serviciilor SOC, incluzând accesările, investigațiile, acțiunile și intervențiile realizate asupra platformelor și sistemelor Bancii
Procesare date	UE / RO

Criterii Diferențiere

Criteriu	Descriere
Certificari	ISC2, SANS, ECCouncil, Comptia, Microsoft, ISACA, Security Blue Team
Nivel L1-L3	Structura operațională SOC organizată pe trei niveluri de competență (L1, L2 și L3), care să asigure monitorizarea și trierea alertelor, investigarea și analiza incidentelor de securitate, precum și analiza aprofundată, coordonarea răspunsului și suportul pentru incidente complexe.
Limba	Suport RO/EN
Escaladare	Mecanisme și proceduri de escaladare operațională și managerială documentate, care să definească nivelurile de severitate, criteriile de escaladare, persoanele de contact și timpii de notificare aferenți fiecărei categorii de incident.

4. Livrabile

Prestatorul va furniza, fără a se limita la:

Faza 1 - Plan de implementare și operationalizare

- Calendar de implementare
- Responsabilități client/furnizor (RACI)
- Plan de comunicare și escaladare
- Documentație tehnică privind arhitectura soluției implementate, fluxurile de colectare și monitorizare a evenimentelor, componentele utilizate și integrarea cu infrastructura existentă;
- Matrice de severitate a incidentelor și criteriile de clasificare în aliniere cu metodologia clientului (bancii);
- Lista scenariilor de detecție implementate, clasificare MITRE ATT&CK, prioritizare după nivel risc în aliniere cu metodologia clientului (bancii).

- Proceduri de investigare , escaladare, raspuns la incidente utilizate cu posibilitatea de aliniere cu cele existente la client.
- Documentatie de configurare, administrare, monitorizare si proceduri de lucru;
- Documentatie privind politicile de securitate, regulile de detectie si mecanismele de identificare si raspuns;
- Documentatie generala privind integrarea cu sistemele de colectare evenimente;
- Plan de revizuire si optimizare continua a regulilor de detectie si a use-case-urilor.

Faza 2 - Implementare

- Plan si raport de implementare care sa evidentieze activitatile realizate si rezultatele obtinute;
- Scenarii de testare, rezultate ale testelor si documentarea eventualelor neregularitati identificate;
- Raport de validare a scenariilor de detectie implementate
- Proceduri de operare, administrare si raspuns la incidente de securitate;
- Sesiuni de transfer de cunostinte si instruire pentru operatorii desemnati de Banca;
- Documentatia de acceptanta a serviciului implementat si procesul-verbal de receptie;
- Servicii de suport post-implementare (hypercare) pe perioada ofertata;
- Documentatie si recomandari privind bune practici pentru operarea si optimizarea continua a serviciului.
- Plan de remediere pentru eventualele neconformitati identificate in perioada de implementare.

In vederea acceptantei este necesara confirmarea de catre client a surselor integrate, testelor efectuate si confirmarea functionarii monitorizarii

Faza 3 – Livrabile post-implementare

- Alerte si notificari de securitate, alerte validate de analisti SOC
- Clasificare pe severitate (Critic, Inalt, Mediu, Scazut)
- Recomandari de remediere
- Evidenta pastrare loguri si rapoarte ca evidente pentru audit
- Dovada respectarii SLA-urilor
- Pentru fiecare incident tichet care sa contina minim:
 - Descriere incident
 - Active afectate
 - Indicatori de compromitere (IOC)
 - Impact estimat
 - Actiuni recomandate
 - Timeline-ul incidentului
- Pentru incidente majore suplimentar:
 - Raport Post-Incident (PIR)
 - Root Cause Analysis
 - Masuri preventive si actiuni corective propuse
 - Actiunile de containment efectuate;
 - Lectii invatate (Lessons Learned).

Raport zilnic care sa contina minim

- Alerte critice si inalte identificate in ultimele 24 de ore;
- Incidente confirmate si stadiul acestora;
- Actiuni de investigare si remediere efectuate;
- Recomandari urgente transmise Bancii;

- Surse de log indisponibile sau cu probleme de colectare;
- Escaladări efectuate în perioada de raportare;
- Riscuri sau amenințări care necesită atenție imediată.

Raport lunar cu sumar executiv care să conțină minim:

- Număr incidente detectate
- Distribuție pe severitate
- Tipologii de atac
- Amenințări relevante pentru organizație
- Vulnerabilități critice
- Campanii active de atac
- Indicatori de compromitere (IOC)
- Active cele mai vizate
- KPI/SLA realizați
- Recomandări de îmbunătățire
- Incidente deschise/închise
- Timp de detecție (MTTD)
- Timp de răspuns (MTTR)
- Dashboard operational și monitorizare performanță

Livrabilele de tipul rapoarte vor fi furnizate în limba română.

5. Durata și resursele estimate

Contractul va fi semnat pe un an cu posibilitatea de prelungire.

6. Cerințe de calificare

Ofertanții vor prezenta următoarele documentele:

1. Certificatul constatator eliberat de Oficiul Național al Registrului Comerțului din care să rezulte adresa actuală, obiectul de activitate al societății, acționarii/asociații, administratorii societății, eliberat cu cel mult 3 luni în urmă;
2. Certificatul eliberat de Oficiul Național al Registrului Comerțului "Furnizare Informații din Registrul Beneficiarilor Reali" din care să rezulte beneficiarii reali declarați ai societății, în conformitate cu Legea 129/2019, eliberat cu cel mult 3 luni în urmă.
3. Declarația privind conflictele de interese (terți) (modelul furnizat de Banca), completată și semnată de reprezentantul legal al societății.

Doar pentru Ofertantul castigator, additional:

1. Certificat de atestare fiscală privind lipsa datoriilor restante cu privire la plata impozitelor, taxelor, sau a contribuțiilor la bugetul general consolidat (buget local, buget de stat etc.), valabil la data prezentării;
2. Cazierul Fiscal al ofertantului - operator economic, valabil la data prezentării;
3. Cazierul Judiciar al ofertantului și Cazierul Judiciar pentru reprezentanții legali și persoane împuternicite, valabile la data prezentării;
4. Copie CI ale reprezentanților legali/persoane împuternicite care semnează contractul cu BID și documentul de împuternicire;
5. În cazul unei structuri de proprietate complexe se va prezenta Schema structurii actuale de proprietate care să includă toate entitățile din lanțul de proprietate (inclusiv jurisdicția de înregistrare, cota de participare în capitalul social) și membrii organelor de conducere ale acestora, semnată de persoana împuternicită a Ofertantului, conform Anexa 5 la Instrucțiunea KYS.
6. Anexa 2 - FORMULAR DE CUNOAȘTERE – FURNIZOR PERSOANA JURIDICĂ.

7. Chestionar de securitate si protectia datelor – (model furnizat de Banca);
8. Chestionarul asupra politicii de risc social si de mediu (modelul furnizat de Banca), completat si semnat de reprezentantul legal al societatii;

7. Criteriul de atribuire

In vederea determinarii ofertei celei mai avantajoase se va utiliza criteriul de atribuire cel mai bun raport calitate-pret, unde calitatea are o pondere de 50% iar pretul 50%.

Factorii de evaluare si algoritmi de punctare in cazul criteriului de atribuire cel mai bun raport calitate-pret

a. Factorii de evaluare:

Nr. crt.	Denumire factor de evaluare	Pondere
I.	Pretul ofertei	50%
II.	Indeplinirea cerintelor tehnice	40%
III.	KPI operationali asumati contractual pentru furnizarea serviciului SOC (MTTD, MTTR)	10%
Nota oferta	Suma ponderata a notelor	100%
Nr. crt.	Denumire factor de evaluare	Pondere

b. Algoritmi de calcul

I. Pret – 50%

Denumire factor de evaluare	Nota
Pretul (pret per MD / FTE)	1 - 10
Algoritm de calcul: Nota se acorda astfel: a) Pentru cel mai scazut dintre preturi* se acorda nota maxima alocata (10); b) Pentru celelalte preturi ofertate nota N_i se calculeaza proportional, astfel: $\text{Nota } (N_i) = (\text{Pret minim ofertat} / \text{Pret oferta}) \times 10.$ *Pretul va fi exprimat in cost per MD per FTE	

I. Indeplinirea cerintelor tehnice – 40%

Denumire factor de evaluare	Nota								
Indeplinirea cerintelor FRNFR	1 - 10								
Algoritm de calcul: Nota se acorda astfel: Pentru evaluarea gradului de conformitate a raspunsului prestatorului la cerintele tehnice specificate la punctul 3 - Cerinte functionale si tehnice (ce contine toate cerintele tehnice ce vor evaluate de catre Banca), fiecare cerinta va fi analizata individual si incadrata intr-una dintre urmatoarele categorii: <table> <tr> <th>Nivel de conformitate</th><th>Scor</th></tr> <tr> <td>Indeplinit</td><td>6-10</td></tr> <tr> <td>Partial/In curs</td><td>1-5</td></tr> <tr> <td>Neindeplinit</td><td>0</td></tr> </table> Pentru cerintele incadrate ca „Indeplinite”, punctajul acordat poate varia intre 6 si 10 puncte, in functie de gradul de acoperire si maturitatea functionalitatii oferite. Pentru cerintele incadrate ca „Partial/In curs”, punctajul acordat poate varia intre 1 si 5 puncte, in functie de gradul de implementare, nivelul de acoperire al cerintei si masura in care functionalitatea solicitata este disponibila la momentul evaluarii. Scorul final al prestatorului se calculeaza prin agregarea punctajelor obtinute pentru fiecare cerinta evaluata si raportarea acestora la numarul total de cerinte analizate, conform formulei: Scor final = Suma scorurilor acordate cerintelor / Numarul total de cerinte Aceasta metoda permite obtinerea unui scor mediu de conformitate cu valori cuprinse intre 0 si 10, unde: Aceasta metoda permite obtinerea unui scor mediu de conformitate cu valori cuprinse intre 0 si 10, unde Nota (N_{II}): • 10 indica indeplinirea integrala a tuturor cerintelor; • 8 - 9,98 indica un grad acceptabil de conformitate; • 5-7,98 indica o conformitate partiala, cu elemente ce necesita clarificari sau plan de imbunatatiri suplimentare; • sub 5 indica un nivel insuficient de conformitate raportat la cerintele tehnice evaluate, oferta va fi declarata neconforma.		Nivel de conformitate	Scor	Indeplinit	6-10	Partial/In curs	1-5	Neindeplinit	0
Nivel de conformitate	Scor								
Indeplinit	6-10								
Partial/In curs	1-5								
Neindeplinit	0								

II. KPI Operationali – 10%

Denumire factor de evaluare	Nota
KPI Operationali	1 - 10
Algoritm de calcul: Nota se acorda astfel: a) Pentru cei mai mici KPI se acorda nota maxima alocata (10); b) Pentru celelalte KPI-uri ofertate nota N_{III} se calculeaza proportional, astfel: $\text{Nota } (N_{III}) = 10 \times [(MTTD_{\min} / MTTD_{\text{ofertat}}) + (MTTR_{\min} / MTTR_{\text{ofertat}})] / 2$	

Punctajul final se va calcula astfel:

$$P_{\text{final}} = P_I + P_{II} + P_{III}$$

Unde:

- **P_{final} – punctajul final**
- **$P_I = N_I \times 40\%$**
- **$P_{II} = N_{II} \times 40\%$**
- **$P_{III} = N_{III} \times 10\%$**

Criteriul de departajare: Daca doua sau mai multe oferte obtin punctaje totale egale, oferta castigatoare va fi cea cu pretul total cel mai scazut.

8. Negociere

BID isi rezerva dreptul de a organiza o etapa de negociere a ofertelor.