OPIS PREDMETU ZÁKAZKY

NÁZOV PREDMETU ZÁKAZKY: Nástroj bezpečnostného monitoringu určený na detekciu a reakciu na koncových bodoch

PREDMET VEREJNÉHO OBSTARÁVANIA:

Predmetom zákazky je dodanie licencií a služieb nasadenia bezpečnostného nástroja určeného na detekciu a reakciu na kybernetické bezpečnostné incidenty na koncových bodoch (ďalej len „bezpečnostný nástroj“).

ŠPECIFIKÁCIA PREDMETU ZÁKAZKY:

V rámci zvyšovania úrovne kybernetickej bezpečnosti, dostupnosti a kvality prevádzkovaných aplikácií a v súvislosti s proaktívnou stratégiou prístupu z pohľadu kybernetickej bezpečnosti požaduje nadobúdateľ dodanie a nasadenie licencie bezpečnostného nástroja, ktorý je určený na detekciu a reakciu na kybernetické bezpečnostné incidenty na koncových bodoch (t. j. počítač, fyzický server, virtuálny server). Nadobúdateľ požaduje služby nasadenia nástroja na rôznych subjektoch verejnej správy tak, aby informácie a dáta z tohto nástroja boli využité v rámci plnenia úloh vládnej jednotky CSIRT a analytických činností bezpečnostného dohľadového centra (tzv. SOC pracovisko, ktoré prevádzkuje nadobúdateľ spolu s Národnou agentúrou pre sieťové a elektronické služby (ďalej len NASES)) pri bezpečnostnom monitoringu orgánov verejnej moci (ďalej len „OVM“).

Nadobúdateľ požaduje, aby dodané riešenie spĺňalo parametre a funkcionality, ktoré sú definované prostredníctvom funkčných a nefunkčných požiadaviek v Prílohe č. 2 - Špecifikácia požiadaviek. Nadobúdateľ požaduje, aby dodaný bezpečnostný nástroj predstavoval jeden samostatný celok, ktorý v sebe spĺňa všetky požadované funkčné a nefunkčné špecifikácie, tzn. nebude pozostávať z kombinácie produktov viacerých výrobcov (tzv. vendorov) vzhľadom na minimalizáciu potrebného programového vybavenia na cieľových systémoch, ak v prílohe č. 2 Špecifikácia požiadaviek nie je uvedené inak.

Nadobúdateľ požaduje, aby bol poskytovateľ obchodným a technickým partnerom výrobcu ponúkaného riešenia. Uvedené je poskytovateľ povinný preukázať písomným potvrdením o vzťahu s výrobcom bezpečnostného nástroja (napr. potvrdením od Výrobcu, zmluvou, osvedčením, certifikátom). Nadobúdateľ požaduje uviesť v návrhu plnenia konkrétny produkt výrobcu, vrátane uvedenia jeho verzie (napr. pomenovanie modulov) a dostupnej technickej dokumentácie priamo od výrobcu v slovenskom, českom alebo anglickom jazyku, ktorá obsahuje detailný súhrn všetkých funkcionalít bezpečnostného nástroja.

Vzhľadom na špecifikáciu technických požiadaviek nástroja (Príloha č. 2 - Špecifikácia požiadaviek) s využitím cloudových služieb, nadobúdateľ požaduje aby výrobca riešenia, ktoré ponúka poskytovateľ, umožnil audítorovi nadobúdateľa vykonať overenie súladu s technickými normami ISO/IEC 27017:2015 a ISO/IEC 27018:2019 v neakreditovanom režime pred samotným uzavretím Zmluvy. Vyššie uvedenú

požiadavku môže poskytovateľ naplniť aj preukázaním súladu výrobcu riešenia so štandardom SOC2 Typ II alebo ISEA 3000 SOC2 Typ II a to kompletnou správou platnou ku dňu predloženia nadobúdateľovi pred uzavretím Zmluvy.

ROZSAH ZÁKAZKY A LICENČNÉ PODMIENKY:

Zákazka je realizovaná formou zmluvy o dodaní licencie a poskytnutí služieb, ktorá sa uzatvára na obdobie šiestich mesiacov od nadobudnutia účinnosti zmluvy. Nadobúdateľ sa zaväzuje počas uvedeného obdobia z celkového plánovaného množstva licencií pre 7 500 koncových bodov objednať licencie pre pokrytie minimálne 6 000 koncových bodov na predpokladanom maximálnom počte 9 OVM. Predpokladaný počet koncových bodov (počet jednotlivých typov koncových bodov sa môže líšiť o +/- 15 %):

- pracovné stanice 5 900 ks,
- server 1 350 ks (z toho 220 mimo podpory od výrobcu),
- kubernetes nodes 250 ks.

Požadovaná dĺžka licenčného obdobia a poskytovania podpory výrobcom je 48 mesiacov s možnosťou opcie na predĺženie platnosti aktivovaných licencií o ďalších 12 mesiacov.

Nadobúdateľ bude na základe zmluvy o dodaní licencie a poskytnutí služieb uzatvárať čiastkové objednávky licencií pre koncové body a implementačné služby na OVM. Nadobúdateľ sa zaväzuje odoberať licencie pre koncové body v skupinách (tzv. bundloch), ktoré budú v balíčkoch licencií minimálne po 100 koncových bodoch. Nadobúdateľ si vyhradzuje právo čiastkového objednávania samostatne licencií dodaného nástroja a samostatne implementačných služieb.

ŠPECIFIKÁCIA IMPLEMENTAČNÝCH SLUŽIEB:

Implementačné služby tvoria súčasť predmetu zákazky a budú realizované na úrovni centrálnej správy a monitoringu riešenia v prostredí NASES s integráciou na SOC služby prevádzkované na existujúcich platformách SIEM a SOAR. Následne sa bude vykonávať postupné nasadenie riešenia na koncové body v prevádzke jednotlivých OVM z rámcového množstva plánovaných implementácií (tabuľka 1) Jednotlivé OVM sú kategorizované podľa veľkosti organizácie z pohľadu požadovaného rozsahu nasadenia riešenia (tabuľka 1).

	Typ OVM 1	Typ OVM 2	Typ OVM 3
Predpokladaný maximálny počet OVM (implementácií)	2	4	3
Špecifikácia pre určenie typu OVM 1 až 3			
Počet koncových bodov na OVM, na ktoré sa požaduje nasadiť bezpečnostný nástroj	do 300	301 až 800	801 až 1 300
z toho počet serverov (fyzické a virtuálne)	do 50	51 až 250	viac ako 250

Tabuľka 1: Rámcový počet plánovaných implementácií podľa typu OVM, ktorý bol určený na základe počtu koncových bodov v jednotlivých typoch OVM.

Nadobúdateľ určuje postup a rozsah služieb pre celkové nasadenie predmetu zákazky, ktorý je označený ako implementačná fáza. Nadobúdateľ požaduje na každom OVM, pre ktoré boli objednané implementačné služby, uvedenie bezpečnostného nástroja do prevádzky. Uvedením do prevádzky sa rozumie ukončenie implementačnej fázy.

IMPLEMENTAČNÁ FÁZA

Projekt musí byť riadený v súlade s metodikou riadenia kvality (QA), ktorá je zverejnená na https://mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/

Dodávku navrhovaného riešenia požaduje nadobúdateľ rozdeliť na samostatné implementačné fázy:

- Implementačná fáza centrálnych prvkov a jedného vybraného OVM.
  - Implementácia centrálnych prvkov riešenia.
  - Nasadenie riešenia na koncové body OVM.
- Implementačná fáza nasadenia riešenia na jednotlivé koncové body špecifikovaných OVM.
  - Nasadenie riešenia na koncové body OVM podľa typov uvedených v tabuľke 1.

Nadobúdateľ požaduje, aby poskytovateľ disponoval dostatočnými kapacitami pre dodanie implementačných služieb na minimálne 2 OVM súčasne (tzn. aby mohli prebiehať implementačné služby u 2 OVM v rámci doby dodania implementačných služieb).

Uvedené podmienky a členenie je potrebné zohľadniť aj pri tvorbe jednotlivých harmonogramov čiastkových dodávok riešenia tak, aby sa nasadenie na 2 OVM realizovalo do maximálne 35 pracovných dní s ukončením akceptačných testov a podpísaním akceptačných protokolov.

Implementácia centrálnych prvkov riešenia

Implementačná fáza, ktorej cieľom je sprevádzkovať centrálne komponenty riešenia s ich integráciou do služieb SOC.

Súhrn činností požadovaných od poskytovateľa, ktoré budú rozdelené do nasledujúcich etáp:

- Analýza a dizajn.
- Nasadenie a testovanie.
- Zaškolenie personálu.

Analýza a dizajn

Súhrn činností požadovaných od poskytovateľa služieb v minimálnom rozsahu:

- Spracovanie detailného návrhu riešenia (DNR) podľa vzoru zverejneného na: https://mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/
- Analýza prostredia v NASES v súvislosti s inštaláciou centrálnej konzoly nástroja a jeho integrácie do existujúcich technológií SIEM a SOAR.

Nasadenie a testovanie

Súhrn činností požadovaných od poskytovateľa služieb v minimálnom rozsahu:

- Uvedenie centrálnej management konzoly do prevádzky, nastavenie prístupov a rolí.

- Integrácia do centrálneho SIEM na už existujúcom SOC za účasti zástupcov nadobúdateľa.
- Integrácia do FortiSOAR SOAR na už existujúcom SOC za účasti zástupcov nadobúdateľa.
- Špecifikácia interpretácie bezpečnostných udalostí pre podporu tvorby use case v rámci služieb SOC.
- Otestovanie funkčnosti komunikačných tokov medzi centrálnou konzolou a SIEM platformou.
- Otestovanie funkčnosti komunikačných tokov medzi centrálnou konzolou a SOAR platformou.
- Po každej vykonanej integrácii je potrebné vykonať test funkčnosti, ktorý prebehne za účasti zástupcov nadobúdateľa.
- Otestovanie incident response akcií v rozsahu Prílohy č. 2 - Špecifikácia požiadaviek.

Zaškolenie personálu

Súhrn činností požadovaných od poskytovateľa služieb v minimálnom rozsahu:

- Úvodné zaškolenie analytikov SOC z pohľadu práce v konzole, workflow a vykonávanie incident response akcií v rozsahu:
  - minimálne 5 človekodní (1 človekodeň = 8 hodín, počítané po hodinách);
  - on-site s expertom v priestoroch nadobúdateľa;
  - jedno školenie po nasadení a otestovaní riešenia, vykonaných integráciách na existujúce technológie SOC a onboardingu OVM.

Nasadenie riešenia na koncové body OVM

Súhrn opakovaných činností požadovaných od poskytovateľa pri každej integrácie OVM, ktoré budú rozdelené do nasledujúcich čiastkových etáp:

- Analýza a dizajn
- Nasadenie a testovanie
- Zaškolenie personálu

Analýza a dizajn

Poskytovateľ začne implementačnú fázu prípravou na nasadenie bezpečnostného nástroja pre daný OVM. V rámci etapy analýzy a dizajnu bude k dispozícii finálny zoznam koncových bodov s označením počtu, typu a verzie OS, účelu použitia pri serveroch a sieťová topológia. V rámci analýzy a dizajnu je poskytovateľ povinný vykonať najmä nasledujúce kroky:

- obhliadka na mieste, kde sa bude bezpečnostný nástroj implementovať a ktoré určil nadobúdateľ;
- analýza prostredia OVM, v ktorom sa má bezpečnostný nástroj nasadiť;
- určenie koncových bodov, na ktorých sa bezpečnostný nástroj nasadí, vrátane definovania používateľských skupín a skupín koncových bodov;
- Zistenie potrieb jednotlivých pracovísk;

- identifikovanie potrebnej súčinnosti od správcu IT na strane OVM, vrátane dodania zoznamu minimálnych požiadaviek pre úspešnú implementáciu systému, napr. požiadavky na nastavenie firewall.

Výsledkom je vypracovanie dokumentu Plán implementačných služieb, ktorý zahŕňa minimálne výsledky vyššie uvedených krokov, postup a rámcový harmonogram implementačných služieb minimálne v rozsahu bodov definovaných v etape Nasadenie a testovanie.

Nadobúdateľ sa k návrhu Plánu implementačných služieb vyjadrí najneskôr do 5 pracovných dní od jeho doručenia. V prípade, že nadobúdateľ v Pláne implementačných služieb neidentifikoval žiadne nedostatky, ktoré by mali vplyv na uvedenie bezpečnostného nástroja do prevádzky, je povinný ho v uvedenej lehote schváliť. Ak nadobúdateľ v návrhu Plánu implementačných služieb identifikuje nedostatky, ktoré by mali vplyv na uvedenie bezpečnostného nástroja do prevádzky, je poskytovateľ povinný tieto nedostatky bez zbytočného odkladu odstrániť. Etapa Analýza a dizajn končí schválením Plánu implementačných služieb.

Nasadenie a testovanie

Súhrn činností požadovaných od poskytovateľa služieb v minimálnom rozsahu:

- Návrh procesov inštalácie, odoberania a reinštalácie agentov z koncových bodov.
- Nastavenie označenia koncových bodov k príslušnému OVM (logická štruktúra objektov v rámci riešenia).
- Základné nastavenie užívateľských prístupov vrátane segregácie rolí, rozdelenie užívateľov a zariadení do užívateľských skupín a prepojenie na identity systém.
- Konfigurácia politík pre jednotlivé typy pracovísk, serverov a služieb.
- Nastavenie základných dashboardov a reportov o zraniteľnostiach s relevantnou výpovednou hodnotou.
- Kontrola funkčnosti monitorovania agentov.
- Otestovanie funkčnosti komunikačných tokov koncových bodov na centrálnu konzolu.
- Vykonanie akceptačných testov základných funkcionalít nástroja, ktoré prebehnú za účasti zástupcov nadobúdateľa a ktorého výsledky schvaľuje nadobúdateľ.
- Doručenie komplexnej technickej dokumentácie v elektronickej forme k dodanému riešeniu v rozsahu:
  - Používateľská príručka;
  - Inštalačná príručka a pokyny na inštaláciu;
  - Konfiguračná príručka;
  - Integračná príručka;
  - Prevádzkový opis a pokyny pre servis a údržbu;
  - Pokyny pre obnovu v prípade výpadku alebo havárie (Havarijný plán);
  - Dokumentácia je dostupná v anglickom alebo slovenskom jazyku;
  - Dokumentácia je k dispozícii pre každú funkciu platformy;
  - Dokumentácia sa aktualizuje spolu s novou verziou/funkciou platformy.

Súhrn súčinností požadovaných od poskytovateľa služieb v spolupráci s nadobúdateľom a prevádzkou OVM v rozsahu:

- Súčinnosť pri inštalácií agentov podľa Plánu implementačných služieb (samotná inštalácia bude v kompetencii prevádzky OVM).
- Prevádzkový monitoring agenta z pohľadu device/health monitoringu.
- Prevádzkový monitoring a odstránenie dopadu zvýšenej záťaže koncového bodu (v dôsledku nasadenia agenta).
- Identifikovanie a ladenie false positive udalostí.
- Uvedenie do produkcie.

Zaškolenie personálu

Súhrn činností požadovaných od poskytovateľa služieb v minimálnom rozsahu:

- Úvodné zaškolenie administrátorov na OVM a SOC z pohľadu údržby systému a práce s agentami (odobranie, pridanie, monitorovanie, testovanie funkčnosti, troubleshooting, kontaktovanie supportu, integrácia s ďalšími bezpečnostnými nástrojmi) v rozsahu:
  - minimálne 3 človekodní (1 človekodeň = 8 hodín, počítané po hodinách);
  - on-site priamo na OVM a SOC s expertom;
    spolu maximálne 9 školení (počet zodpovedá rámcovému počtu plánovaných implementácií – tabuľka 1);
  - pre administrátorov SOC úvodné zaškolenie len pri nasadení riešenia na prvé OVM pri prvej čiastkovej objednávke implementačných služieb.

Ukončenie čiastkovej etapy Nasadenie, testovanie a zaškolenie je po ukončení akceptačných testov a podpísaní akceptačných protokolov. Detailné rozdelenie činností v rámci jednotlivých fáz a etáp spolu s harmonogramom sa očakáva od poskytovateľa v návrhu riešenia.

POST-IMPLEMENTAČNÁ ETAPA

Poskytovateľ v rámci licenčného obdobia zabezpečuje súhrn činností v rámci post-implementačnej podpory:

- Podpora pri riešení problémov spojených s integráciou treťostranných produktov (SIEM a SOAR) v prípade nefunkčnosti v rozsahu analýzy problému a prípadnej eskalácie na vendora;
- Podpora pri riešení problémov spojených s nefunkčnosťou vlastností produktu a eskalácia na vendora.

Služby rozvoja, konzultačné služby a školenia (tzv. professional services) podľa požiadaviek nadobúdateľa poskytované Výrobcom počas trvania licenčného obdobia v rozsahu spolu 40 človekodní za 48 mesiacov (1 človekodeň = 8 hodín, počítané po hodinách). Nadobúdateľ požaduje tieto služby v slovenskom, českom alebo anglickom jazyku.

POŽIADAVKY NA EXPERTOV:

Nadobúdateľ požaduje údaje o odbornej praxi a odbornej kvalifikácii nasledujúcich osôb – Expertov určených na plnenie Zmluvy, pričom tieto osoby musia spĺňať nasledujúce minimálne požiadavky.

Požiadavky na expertov, ktorí budú zodpovedať za implementáciu riešenia a školenia

- Nadobúdateľ požaduje aspoň **dvoch expertov**, ktorí spĺňajú nasledujúce požiadavky:
  - Minimálne 2 roky odbornej praxe zameranej na služby v oblasti inštalácie, nastavení, správy a prevádzky obstarávaného bezpečnostného nástroja, prípadne v nástroji rovnakého alebo typovo podobného charakteru a zložitosti ako je predmet zákazky.
  - Minimálne 2 roky odbornej praxe zameranej na analytické činnosti/služby v oblasti optimalizácie, hodnotenia a spracovania udalostí v obstarávanom bezpečnostnom nástroji, prípadne v nástroji rovnakého alebo typovo podobného charakteru a zložitosti ako je predmet zákazky.
  - Potvrdenie/osvedčenie alebo certifikácia od výrobcu o odbornej spôsobilosti experta na implementáciu a prevádzku obstarávaného nástroja.
  - Počas uplynulých troch rokov musí expert zároveň preukázať minimálne:
    - praktickú skúsenosť s nasadením alebo s kompletnou inštaláciou a nastavením obstarávaného bezpečnostného nástroja v distribuovanom prostredí (t.j. viacero subjektov, samostatných celkov v tzv. multitenantnej architektúre), pričom riešenie musí mať zapojených minimálne 2000 koncových bodov;
    - praktickú skúsenosť s integrovaním spracovania udalostí do SIEM alebo SOAR a skúsenosti s interpretáciou a vyhodnocovaním udalostí pre podporu tvorby use case.

Poskytovateľ preukáže odbornú spôsobilosť vyššie uvedených osôb predložením profesijných životopisov v slovenskom alebo českom jazyku za každú osobu minimálne v nasledovnej štruktúre:

- meno a priezvisko;
- názov a sídlo objednávateľa, resp. zamestnávateľa;
- čas plnenia zmluvy (od - do: mesiac a rok) a rozsah a predmet činností, ktoré príslušná osoba zabezpečovala v rozsahu potrebnom najmenej pre overenie splnenia požiadaviek na odbornú spôsobilosť experta;
- tel. číslo a meno zamestnanca objednávateľa alebo zamestnávateľa, u ktorého si možno overiť tieto údaje;
- vlastnoručný podpis osoby.