

Nacionaliniam kibernetinio saugumo centrui prie KAM

2021-12-17 Nr. PSL211216EDR1-01

SIŪLOMŲ PREKIŲ TECHNINIAI PARAMETRAI

1. Teikėjas turi užpildyti 3 stulpelį „Siūloma tiekti paslauga visiškai atitinka pirkimo dokumentuose nustatytus techninius reikalavimus ir jos savybės tokios:“ 2. Nurodome siūlomų paslaugų technines specifikacijas, charakteristikas ir pagrindines savybes pagal pirkimo dokumentuose nurodytus reikalavimus (teikėjas negali naudoti sąvokos „Atitinka“, o privalo aiškiai apibūdinti siūlomų paslaugų charakteristikas, priešingu atveju toks pasiūlymas bus pripažintas neatitinkančiu pirkimo dokumentų reikalavimų ir bus atmestas). 3. Patvirtiname, kad vykdant paslaugų pirkimo-pardavimo sutartį įsigyjamas objektas atitiks šiuos reikalavimus:		
Eil. Nr.	Reikalaujamos paslaugų techninės charakteristikos	Siūloma tiekti paslauga visiškai atitinka pirkimo dokumentuose nustatytus techninius reikalavimus ir jos savybės tokios: (techninių reikalavimų formuluotėse, kur nurodyta paklaida ar reikalavimas "Taip/Ne (tikslus aprašymas) nurodomos siūlomo objekto charakteristikos" (užpildo teikėjas pateikdamas pasiūlymą)*
1	2	3
1.	1 pirkimo dalis. ĮSILAUŽIMO DETEKTAVIMO SISTEMOS (IDS) PARAŠŲ PRENUMERATOS PASLAUGOS, 36 mėn.	
1.1.	Paslaugoms keliami reikalavimai:	
1.1.1	Įsilaužimo detektavimo sistemos (IDS) įsilaužimo detektavimo taisyklių rinkinio prenumeratos paslaugos apima Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) naudojamos įsilaužimo detektavimo taisyklių rinkinio „ETPro Ruleset” (toliau – parašai) prenumeratos pratęsimą 36 mėn. laikotarpiui.	36 mėn.
1.1.2.	Paslaugos privalo leisti gauti parašus apie naujausias grėsmes, bei juos įdiegti į NKSC turimus SNORT ir SURICATA sensorius.	Taip Paslaugos leidžia gauti parašus apie naujausias grėsmes, bei juos įdiegti į NKSC turimus SNORT ir SURICATA sensorius.

1.1.3.	Paslaugos privalo leisti, bent vieną kartą per parą, gauti taisyklių rinkinį turinti ne mažiau kaip 5 naujus parašus.	Taip Paslaugos leidžia, vieną kartą per parą, gauti taisyklių rinkinį turintį 20-40 naujų parašų.
1.1.4.	Parašai pateikiami kartu su jų aprašymu.	Taip
1.1.5.	Parašai turi būti suskirstyti į kategorijas.	Taip Parašai yra suskirstyti į daugiau nei 40 kategorijų.
1.1.6.	Paslaugų teikimo sąlygos privalo suteikti teisę be papildomo mokesčio gauti parašų pataisymus ir atnaujinimus (naujausias versijas) visą prenumeratos teikimo laikotarpį.	Taip
1.2.	Bendrieji reikalavimai:	
1.2.1.	Prieiga prie įsilaužimo detektavimo sistemos turi būti pateikta oficialiu gamintojo patvirtintu keliu.	Taip Prieiga prie įsilaužimo detektavimo sistemos yra pateikta oficialiu gamintojo patvirtintu keliu.
1.2.2.	Pardavėjas turi pateikti nuorodą ar nuorodas į gamintojo interneto puslapį, kuriame yra tiksli pasiūlymą atitinkančių paslaugų techninė specifikacija.	https://www.proofpoint.com/sites/default/files/white-papers/pfpt-wp-tb-etpro-subscription-overview.pdf
1.2.3.	Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie įsilaužimo detektavimo sistemos gamybos arba tobulinimo nutraukimą (pvz., angl. End Of Life Time, End Of Support, arba Discontinued).	Gamintojo užtikrinimas pateiktas.
2.	2 pirkimo dalis. LIETUVOS ORGANIZACIJŲ KIBERNETINIO SAUGUMO REITINGAVIMO IR INFORMACIJOS APIE APTIKTUS PAŽEIDŽIAMUMUS BEI ŽALINGAS KOMUNIKACIJAS PRENUMERATOS PASLAUGOS, 36 mėn.	
	Pirkimo objektas – Lietuvos organizacijų (viešojo ir privataus sektoriaus įstaigų, institucijų ir įmonių) (toliau – organizacijos) kibernetinio saugumo reitingavimo ir informacijos apie aptiktus pažeidžiamumus bei žalingas komunikacijas prenumeratos paslaugos (toliau – paslaugos), skirtos NKSC vykdomam potencialių kibernetinių grėsmių atakos vektorių poveikio Lietuvos ryšių infrastruktūrai vertinimui, pažeidžiamų ir užvaldytų įrenginių nustatymui. Paslaugos turi atitikti žemiau pateiktus reikalavimus (perkančiosios organizacijos testuotos „BitSight CNP“ prenumeratos paslaugos atitinka žemiau pateiktus reikalavimus, todėl siūlydamas šias paslaugas tiekėjas papildomai neįpareigojamas pateikti įrodymų dėl jų atitikties žemiau nustatytiems reikalavimams).	
2.1.	Paslaugoms keliami reikalavimai:	
2.1.1.	Skenuoti visą Lietuvos interneto erdvę, rinkdama informaciją apie konkrečiais IP adresais ir prievadais veikiančius servisus, bandydama nustatyti jų versijas, konfigūracijas, pažeidžiamumus.	Taip/Ne (tikslus aprašymas).
2.1.2.	Rinkti informaciją apie galimai žalingas komunikacijas, susijusias su užvaldytų įrenginių valdymo infrastruktūra (angl. Command-and-Control, C&C).	Taip/Ne (tikslus aprašymas).

2.1.3.	Gebėti pagal tam tikrus požymius priskirti surinktą informaciją konkrečioms Lietuvos organizacijoms (viešojo ir privataus sektoriaus įstaigų, institucijų ir įmonių), jeigu tokie požymiai egzistuoja.	Taip/Ne (tikslus aprašymas).
2.1.4.	Organizacijoms turi būti suteikiami reitingai (balų sistemoje), kuriuos sudarytų viešai pasiekiamų organizacijos resursų kibernetinio saugumo kriterijų visuma: • Žinomi užvaldyti organizacijos įrenginiai; • Žinomi pažeidžiami organizacijos įrenginiai; • Atviri prievadai; • Naudojami SSL/TLS sertifikatai ir jų konfigūracijos; • Organizacijų DNS įrašų nustatymai ir el. pašto viešai prieinama saugumo politika (SPF, DKIM); • Kita surinkta informacija.	Taip/Ne (tikslus aprašymas).
2.1.5.	Turi būti galimybė generuoti organizacijų saugumo vertinimo ataskaitas (PDF formatu), kuriose atspindėtų visa surinkta informacija apie konkrečią organizaciją, jos kibernetinio saugumo reitingas bei reitingą sudarantys vertinimo veiksniai.	Taip/Ne
2.1.6.	Turi būti galimybė atlikti pažeidžiamų įrenginių Lietuvoje paiešką pagal pažeidžiamumų numerius (angl. Common vulnerabilities and exposures, CVE).	Taip/Ne
2.1.7.	Turi būti galimybė atlikti galimai užvaldytų įrenginių paiešką pagal skirtingų kenkėjiškų programinių kodų požymius.	Taip/Ne
2.1.8.	Turi būti galimybė gauti per pastarąsias 24 valandas naujai sugeneruotų duomenų pagal užvaldytų ir/ar pažeidžiamų įrenginių požymius ataskaitas el. paštu.	Taip/Ne
2.1.9.	Turi būti galimybė redaguoti automatiškai siunčiamų ataskaitų nustatymus.	Taip/Ne
2.1.10.	Turi būti galimybė vykdyti paiešką duomenų bazėje naudojant aplikacijų programavimo sąsają (API).	Taip/Ne
2.1.11.	Turi būti galimybė realiu laiku gauti duomenis apie naujai nustatytas galimas žalingas komunikacijas, naudojant aplikacijų programavimo sąsają (API).	Taip/Ne
2.1.12.	Turi būti galimybė pasirinkti bent 30 Lietuvos organizacijų, kurias galima būtų nuolat stebėti, kaip atskirus vienetus.	Taip/Ne
2.1.13.	Turi būti galimybė suteikti teisę stebimos organizacijos atstovui prisijungti ir matyti sistemoje savo organizacijos saugumo vertinimą ir visą aktualią kibernetinio saugumo informaciją.	Taip/Ne

2.1.14.	Turi būti galimybė pridėti naujus ir pašalinti esamus sistemos naudotojus.	Taip/Ne
2.1.15.	Turi būti galimybė koreguoti sistemos naudotojų teises.	Taip/Ne
2.1.16.	Visi surinkti duomenys turi būti susisteminti ir pateikti patogiu vartotojui būdu.	Taip/Ne
2.1.17.	Sistema turi veikti naršyklėje.	Taip/Ne
3.	3 pirkimo dalis. KIBERNETINIŲ GRĖSMIŲ INDIKATORIŲ DUOMENŲ BAZIŲ PRENUMERATOS PASLAUGOS	
	Pirkimo objektas – Kibernetinių grėsmių indikatorių (angl. Indicators of compromise – IoC) (toliau – Kenksmingi indikatoriai) duomenų bazės prenumeratos paslaugos, 12 mėn. Pirkimo tikslas. Kenksmingų indikatorių duomenų bazės prenumeratos paslaugos (toliau – paslaugos) privalo suteikti galimybę NKSC kibernetinio saugumo specialistams (toliau – specialistai) analizuoti kibernetinę erdvę ir užkardyti ankstesnėje fazėje galimas kenkėjiškas veikas. Siekiamas pirkimo rezultatas. Gaunama atnaujinta informacija apie Kenksmingus indikatorius. Taip pat NKSC specialistai, naudodamiesi teikėjo pateikta prieiga prie dedikuotos platformos (duomenų bazės), gali vykdyti platesnę indikatorių analizę bei naudotis grėsmių žvalgybos profilių (angl. Intelligence cards) teikiama informacija.	
3.1.	Bendrieji reikalavimai	
3.1.1.	Prieiga prie kibernetinių grėsmių indikatorių duomenų bazės (analizės platformos) (toliau – platforma) turi būti pateikta gamintojo arba gamintojo įgalioto asmens.	Taip/Ne
3.1.2.	Tiekėjas turi pateikti nuorodą ar nuorodas į gamintojo interneto puslapį, kuriame yra tiksli pasiūlymą atitinkančių paslaugų techninė specifikacija arba pateikti gamintojo parengtą paslaugų aprašymą.	<i>Pateikti nuorodas į gamintojo interneto puslapį.</i>
3.1.3.	Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie platformos, prie kurios bus suteikta prieiga, gamybos arba tobulinimo nutraukimą (pvz., angl. end of life time arba Discontinued).	<i>Pateikti gamintojo užtikrinimą.</i>
3.2.	Paslaugoms keliami reikalavimai	
3.2.1.	Paslaugos turi apimti:	
3.2.1.1.	prieigos prie automatizuoto kompromitavimo indikatorių (angl. „IOC“) srauto (angl. „feed“) „Connect API“, kuris turi būti integruojamas per API su grėsmių indikatorių analizės platformomis.	Taip/Ne
3.2.1.2.	prieigos vienam naudotojui prie internetinio portalo (platformos), kurioje būtų galimybė naudotis sistemos modulių „SecOps user license“ ir „Vulnerability intelligence user license“ suteikiamu turiniu.	Taip/Ne
3.2.2.	Internetinio portalo funkcionalumas turi susidėti iš:	
3.2.2.1.	grėsmių žvalgybos profilių (kortelių) (angl. Intelligence cards).	Taip/Ne

3.2.2.2.	namų vaizdo (angl. Home screen), grėsmių peržiūros srities (angl. Threat views).	Taip/Ne
3.2.2.3.	grėsmių žvalgybos tikslų asortimento (angl. Intelligence goal library).	Taip/Ne
3.2.2.4.	pažangių užklausų sudarymo įrankio (angl. Advanced query builder).	Taip/Ne
3.2.2.5.	tinkinamų realaus laiko įspėjimų (angl. Customizable real time alerts).	Taip/Ne
3.2.3.	Grėsmių žvalgybos profiliai turi pateikti bent šią informaciją:	
3.2.3.1.	IP adresus.	Taip/Ne
3.2.3.2.	Domain vardus.	Taip/Ne
3.2.3.3.	Interneto svetainių adresus.	Taip/Ne
3.2.3.4.	Hash duomenis.	Taip/Ne
3.2.3.5.	pažeidžiamumų informaciją.	Taip/Ne
3.2.3.6.	informaciją apie kenkėjiškas programas.	Taip/Ne
3.2.3.7.	Snort/Yara taisyklių informaciją.	Taip/Ne
3.2.4.	Paslaugų turinį sudarančios informacijos apie kibernetines grėsmes šaltinis turi apimti internetinių forumų, socialinės medijos, tekstinės informacijos įklijavimo, internetinių pokalbių, informavimo apie kibernetines grėsmes interneto svetainių, taip pat „gilios interneto“ (angl. „Deep web“) ir „tamsaus interneto“ (angl. „Dark web“) turinį.	Taip/Ne
3.2.5.	3.2.4 p. nurodytuose šaltiniuose surinkta informacija turi būti apdorota natūralios kalbos apdorojimo priemonėmis, skirtomis apdoroti tekstą, parašytą bent anglų, arabų, ispanų, prancūzų, kinų, rusų, portugalų, vokiečių ir persų kalbomis. Apdorojimo metu platformoje turi būti numatyta įvykių ir subjektų identifikavimo funkcija, taip pat funkcija, leidžianti turinio minėtomis kalbomis analizavimo metu nustatyti kompromitavimo indikatorius (angl. „IOC“).	Taip/Ne

3.2.6.	Automatizuoto kompromitavimo indikatorių informacija turi būti pateikiama su įrodymais, grįžtais rizikos įvertinimo įverčiais (angl. risk score).	Taip/Ne
3.2.7.	Duomenys iš sistemos turi būti eksportuojami JSON, CSV, STIX, PPT, PNG, PDF ar Word dokumentų pavidalu.	Taip/Ne
3.2.8.	Platformos naudotojas turi turėti prieigą prie platformoje integruotos smėlio dėžės (angl. Sandbox). Naudotojas turi galėti įkelti įtartinus failus į smėlio dėžę analizei. Analizės ataskaitos turi būti sugeneruojamos ir pateikiamos JSON formatu. Smėlio dėžės apdoroti mėginiai taip pat turi būti automatiškai priskiriami MITRE ATT & CK metodams.	Taip/Ne
3.2.9.	Kiekvienoje smėlio dėžės ataskaitoje turi būti pateikiamas rodiklių rinkinys (domenai, URL, IP ir maišos), kurie turi būti koreliuojami su kita platformoje esančia informacija.	Taip/Ne
3.2.10.	Naudotojo sąsaja turi būti anglų kalba.	Taip/Ne
3.2.11.	Turi būti galimybė srauto (angl. feed) turinį integruoti per API su grėsmių indikatorių analizės platformomis, tokiomis kaip EclecticIQ, MISP, Anomali.	Taip/Ne
3.2.12.	Paslaugų teikimo metu turi būti užtikrintas gamintojo numatytas standartinis palaikymas (angl. „Support“), apimantis mokymus naudotis paslaugomis ir nuolatinį techninį palaikymą:	Taip/Ne
3.2.12.1.	mokymai turi vykti nuotoliniu būdu ir turi įvykti per mėnesį nuo paslaugų teikimo pradžios. Tikslus laikas turi būti suderintas su perkančiąja organizacija. Jie turi supažindinti vieną perkančiosios organizacijos naudotoją su srauto ir platformos veikimo principais ir geriausiomis naudojimo praktikomis, atsižvelgiant į šioje techninėje specifikacijoje norimus pasiekti perkančiosios organizacijos tikslus.	Taip/Ne
3.2.12.2.	techninis palaikymas turi būti teikiamas 24 val. per parą, 7 dienas per savaitę, sudarant galimybę gauti pagalbą platformos naudojimo klausimais iš dedikuotos platformos gamintojo ar teikėjo komandos, reakcijos laikas į užklausą ne ilgiau kaip 3 val. (kai užklausa pateikiama darbo dienomis nuo 8 iki 17 val., penktadieniais iki 15.45 val.), užklauskos pateikimo būdas – el. paštu ar naudojantis dedikuota platforma. Turi būti per internetą pasiekiamas mokomosios medžiagos, susijusios su platforma, repozitorija.	Taip/Ne <i>Pateikti numatomą mokymų tvarkaraštį.</i>

3.2.13.	Pradėjus teikti paslaugas, perkančiajai organizacijai turi būti pateikti platformos ir srauto administravimo ir vartotojo vadovai anglų kalba skaitmeniniame formate.	Taip/Ne
---------	---	---------

*Pastaba: Nurodyti pavadinimai, medžiagų / įrangos gamintojai technologinis procesas, standartas, prekių kilmė, konkretus pavadinimas, ženklas (jei tokią prielaidą galima daryti) yra informacinio pobūdžio ir tiekėjas nėra įpareigojamas siūlyti ir/ar naudoti šių gamintojų produkciją, standartą, procesą (gali naudoti lygiaverčius). Teikdamas pasiūlymą, tiekėjas turi vadovautis šiuo metu galiojančiais normatyvais technologijai, medžiagoms, įrangai bei darbams, atsižvelgti į pirkimo objekto specifiką. Lygiavertiškumo nurodytiems duomenims įrodymo prievolė tenka tiekėjui.

Pardavimų koordinatore

(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas)

(Parašas)

(Vardas ir pavardė)