

## 1 DALIS

### PAŽEIDŽIAMUMŲ SKENAVIMO PROGRAMINĖS ĮRANGOS (A TIPO) PIRKIMAS

#### TECHNINĖ SPECIFIKACIJA

#### 1. Pirkimo objektas – pažeidžiamumų skenavimo programinės įrangos (A tipo) nuoma (toliau – PĮ arba prekė).

Pirkimo tikslas. PĮ skirta Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) vykdomam potencialių kibernetinių grėsmių atakos vektorių poveikio Lietuvos ryšių infrastruktūrai vertinimui, kibernetinio saugumo subjektų saugumo reitingavimui, pažeidžiamų ir užvaldytų įrenginių nustatymui.

#### 2. Bendrieji reikalavimai:

2.1. Tiekėjas turi pateikti nuorodą ar nuorodas į gamintojo interneto puslapį, kuriame yra pasiūlymą atitinkančios PĮ techninė specifikacija arba pateikti gamintojo parengtą prekės aprašymą.

2.2. Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie siūlomos PĮ tobulinimo nutraukimą (angl. End of life arba Discontinued).

2.3. PĮ turi būti teikiamas techninis palaikymas ne trumpiau nei 36 mėn.

2.4. Techninio palaikymo sąlygos turi užtikrinti įvairių PĮ gedimų šalinimą ir pagalbą naudojantis PĮ. Pagalba turi būti teikiama telefonu, elektroniniu paštu, nuotoliniu prisijungimu bei leisti be papildomo mokesčio gauti PĮ naujinimus bei pataisymus per visą nuomos laikotarpį.

2.5. Techninis palaikymas privalo būti teikiamas PĮ gamintojo arba jo įgalioto atstovo.

2.6. Pirkimo objektas, vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo (toliau – Įstatymas) turi nekelti grėsmės nacionaliniam saugumui. Perkančioji organizacija, vadovaudamasi Įstatymo 37 straipsnio 9 dalimi, laikys, kad prekė kelia grėsmę nacionaliniam saugumui, kai prekių gamintojas ar jį kontroliuojantis asmuo yra registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Įstatymo 92 straipsnio 14 dalyje numatyta sąraše nurodytose valstybėse ar teritorijose.

#### 3. PĮ keliami reikalavimai. Prekė turi atitikti žemiau 1 lentelėje pateiktus reikalavimus:

1. lentelė

Eil. Nr	Reikalaujama charakteristika (ne blogiau kaip)	Siūloma charakteristika (Pildo tiekėjas)
<b>Gamintojas ir Programinės įrangos licencijos pavadinimas</b> (Įrašyti. Taip pat kartu pateikiama nuoroda į gamintojo internetinį puslapį, kuriame yra pasiūlymą atitinkančios PĮ techninė specifikacija arba pateikti gamintojo parengtą prekės aprašymą)		<i>Bitsight Total Risk monitoring for CNI (50 organizations).</i> <a href="https://www.bitsight.com/products/national-cybersecurity">https://www.bitsight.com/products/national-cybersecurity</a>
1.	Skenuoti visą Lietuvos interneto erdvę, rinkdama informaciją apie konkrečiais IP adresais ir prievadais veikiančius servisus, bandydama nustatyti jų versijas, konfigūracijas, pažeidžiamumus.	Skenuoja visą Lietuvos interneto erdvę, rinkdama informaciją apie konkrečiais IP adresais ir prievadais veikiančius servisus, bandydama nustatyti jų versijas, konfigūracijas, pažeidžiamumus.
2.	Naudoti turimą „sinkhole“ tipo tinklą, kad rinkti informaciją apie potencialiai žalingas komunikacijas, susijusias su užvaldytų įrenginių	Naudoja turimą „sinkhole“ tipo tinklą, kad rinkti informaciją apie potencialiai žalingas komunikacijas, susijusias su užvaldytų

<b>Eil. Nr</b>	<b>Reikalaujama charakteristika (ne blogiau kaip)</b>	<b>Siūloma charakteristika (Pildo tiekėjas)</b>
	valdymo infrastruktūra (angl. <i>Command-and-Control, C&amp;C</i> ).	įrenginių valdymo infrastruktūra (angl. <i>Command-and-Control, C&amp;C</i> ).
3.	Gebėti pagal tam tikrus požymius priskirti surinktą informaciją konkrečioms Lietuvos organizacijoms (viešojo ir privataus sektoriaus įstaigų, institucijų ir įmonių), jeigu tokie požymiai egzistuoja.	Geba pagal tam tikrus požymius priskirti surinktą informaciją konkrečioms Lietuvos organizacijoms (viešojo ir privataus sektoriaus įstaigų, institucijų ir įmonių), jeigu tokie požymiai egzistuoja.
4.	Organizacijoms turi būti suteikiami reitingai (balų organizacijos resursų bei kitų kibernetinio saugumo	sistemoje), kuriuos sudarytų viešai pasiekiamų kriterijų visuma:
4.1.	Žinomi užvaldyti organizacijos įrenginiai;	Yra žinomi užvaldyti organizacijos įrenginiai;
4.2.	Žinomi pažeidžiami organizacijos įrenginiai;	Yra žinomi pažeidžiami organizacijos įrenginiai;
4.3.	Atviri prievadai;	Atviri prievadai;
4.4.	Naudojami SSL/TLS sertifikatai ir jų konfigūracijos;	Yra naudojami SSL/TLS sertifikatai ir jų konfigūracijos;
4.5.	Organizacijų DNS įrašų nustatymai ir el. pašto viešai prieinama saugumo politika (SPF, DKIM);	Yra organizacijų DNS įrašų nustatymai ir el. pašto viešai prieinama saugumo politika (SPF, DKIM);
4.6.	Kita surinkta informacija.	Kita surinkta informacija.
5.	Turi būti galimybė generuoti organizacijų saugumo vertinimo ataskaitas (PDF formatu), kuriose atsispindėtų visa surinkta informacija apie konkrečią organizaciją, jos kibernetinio saugumo reitingas bei reitingą sudarantys vertinimo veiksniai.	Yra galimybė generuoti organizacijų saugumo vertinimo ataskaitas (PDF formatu), kuriose atsispindėtų visa surinkta informacija apie konkrečią organizaciją, jos kibernetinio saugumo reitingas bei reitingą sudarantys vertinimo veiksniai.
6.	Turi būti galimybė atlikti pažeidžiamų įrenginių Lietuvoje paiešką pagal pažeidžiamumų numerius (angl. <i>Common vulnerabilities and exposures, CVE</i> ).	Yra galimybė atlikti pažeidžiamų įrenginių Lietuvoje paiešką pagal pažeidžiamumų numerius (angl. <i>Common vulnerabilities and exposures, CVE</i> ).
7.	Turi būti galimybė atlikti potencialiai užvaldytų įrenginių Lietuvoje paiešką pagal skirtingų kenkėjiškų programinių kodų požymius ir jų pavadinimus.	Yra galimybė atlikti potencialiai užvaldytų įrenginių Lietuvoje paiešką pagal skirtingų kenkėjiškų programinių kodų požymius ir jų pavadinimus.
8.	Turi būti galimybė gauti per pastarąsias 24 valandas naujai sugeneruotų duomenų pagal užvaldytų ir/ar pažeidžiamų įrenginių požymius ataskaitas el. paštu.	Yra galimybė gauti per pastarąsias 24 valandas naujai sugeneruotų duomenų pagal užvaldytų ir/ar pažeidžiamų įrenginių požymius ataskaitas el. paštu. <a href="https://help.bitsighttech.com/hc/en-us/articles/115001051868-Alerts-Overview-Continuous-Monitoring">https://help.bitsighttech.com/hc/en-us/articles/115001051868-Alerts-Overview-Continuous-Monitoring</a>
9.	Turi būti galimybė redaguoti automatiškai siunčiamų ataskaitų nustatymus.	Yra galimybė redaguoti automatiškai siunčiamų ataskaitų nustatymus.
10.	Turi būti galimybė vykdyti paiešką duomenų bazėje naudojant aplikacijų programavimo sąsają (API).	Yra galimybė vykdyti paiešką duomenų bazėje naudojant aplikacijų programavimo sąsają (API). <a href="https://bitsight.stopligh.io/">https://bitsight.stopligh.io/</a>
11.	Turi būti galimybė realiu laiku gauti duomenis apie naujai nustatytas galimas žalingas komunikacijas, naudojant aplikacijų programavimo sąsają (API).	Yra galimybė realiu laiku gauti duomenis apie naujai nustatytas galimas žalingas komunikacijas, naudojant aplikacijų programavimo sąsają (API).

<i>Eil. Nr</i>	<i>Reikalaujama charakteristika (ne blogiau kaip)</i>	<i>Siūloma charakteristika (Pildo tiekėjas)</i>
12.	Turi būti galimybė pasirinkti ne mažiau kaip 50 Lietuvos organizacijų, kurias galima būtų nuolat stebėti, kaip atskirus vienetus.	Yra galimybė pasirinkti ne mažiau kaip 50 Lietuvos organizacijų, kurias galima būtų nuolat stebėti, kaip atskirus vienetus.
13.	Turi būti galimybė suteikti teisę stebimos organizacijos atstovui prisijungti ir matyti sistemoje savo organizacijos saugumo vertinimą ir visą susijusią kibernetinio saugumo informaciją.	Yra galimybė suteikti teisę stebimos organizacijos atstovui prisijungti ir matyti sistemoje savo organizacijos saugumo vertinimą ir visą susijusią kibernetinio saugumo informaciją.
14.	Turi būti galimybė pridėti naujus ir pašalinti esamus sistemos naudotojus.	Yra galimybė pridėti naujus ir pašalinti esamus sistemos naudotojus.
15.	Turi būti galimybė koreguoti sistemos naudotojų teises.	Yra galimybė koreguoti sistemos naudotojų teises. <a href="https://help.bitsighttech.com/hc/en-us/articles/360008185714-User-Roles">https://help.bitsighttech.com/hc/en-us/articles/360008185714-User-Roles</a>
16.	Visi surinkti duomenys turi būti susisteminti ir pateikti struktūrizuotai grupuojant pagal informacijos kategorijas.	Visi surinkti duomenys yra susisteminti ir pateikti struktūrizuotai grupuojant pagal informacijos kategorijas.
17.	Sistema turi veikti naršyklėje.	Sistema veikia naršyklėje.

**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.

## 2 DALIS

### PAŽEIDŽIAMUMŲ SKENAVIMO PROGRAMINĖS ĮRANGOS (B TIPO) PIRKIMAS

#### TECHNINĖ SPECIFIKACIJA

#### 1. Pirkimo objektas – pažeidžiamumų skenavimo programinės įrangos (B tipo) nuoma (toliau – PĮ arba prekė).

Pirkimo tikslas. PĮ turi periodiškai skenuoti ir kaupti informaciją apie visame pasaulyje viešai internetu pasiekiamus įrenginius, jų programinę įrangą, versijas ir žinomas saugumo spragas. PĮ suteiktą galimybę perkančiosios organizacijos kibernetinio saugumo specialistams (toliau – Specialistai) vykdyti konkrečių saugumo spragų paveiktų įrenginių paiešką, siekiant informuoti jų valdytojus apie atitinkamas grėsmes.

#### 2. Bendrieji reikalavimai:

2.1. Tiekėjas turi pateikti nuorodą ar nuorodas į gamintojo interneto puslapį, kuriame yra pasiūlymą atitinkančios PĮ techninė specifikacija arba pateikti gamintojo parengtą prekės aprašymą.

2.2. Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie siūlomos PĮ tobulinimo nutraukimą (angl. End of life arba Discontinued).

2.3. PĮ turi būti teikiamas techninis palaikymas ne trumpiau nei 36 mėn.

2.4. Techninio palaikymo sąlygos turi užtikrinti įvairių programinių gedimų, susijusių su programine įranga, šalinimą ir pagalbą naudojantis programine įranga, turi būti teikiamos telefonu, elektroniniu paštu, nuotoliniu prisijungimu bei leisti be papildomo mokesčio gauti PĮ naujinimus bei pataisymus per visą nuomos laikotarpį.

2.5. PĮ techninis palaikymas privalo būti teikiamas PĮ gamintojo arba jo įgalioto atstovo.

2.6. Pirkimo objektas, vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo (toliau – Įstatymas) turi nekelti grėsmės nacionaliniam saugumui. Perkančioji organizacija, vadovaudamasi Įstatymo 37 straipsnio 9 dalimi, laikys, kad prekė kelia grėsmę nacionaliniam saugumui, kai prekių gamintojas ar jį kontroliuojantis asmuo yra registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Įstatymo 92 straipsnio 14 dalyje numatyta sąraše nurodytose valstybėse ar teritorijose.

#### 3. PĮ keliami reikalavimai. Prekė turi atitikti žemiau 1 lentelėje pateiktus reikalavimus:

1. lentelė

Eil. Nr	Reikalaujama charakteristika (ne blogiau kaip)	Siūloma charakteristika (Pildo tiekėjas)
	<b>Gamintojas ir Programinės įrangos licencijos pavadinimas</b> (Įrašyti. Taip pat kartu pateikiama nuoroda į gamintojo internetinį puslapį, kuriame yra pasiūlymą atitinkančios PĮ techninė specifikacija arba pateikti gamintojo parengtą prekės aprašymą)	<b>SHODAN SMALL BUSINESS API PLAN</b> <a href="https://account.shodan.io/billing">https://account.shodan.io/billing</a>
1.	PĮ turi periodiškai skenuoti visame pasaulyje IPv4 režiais viešai internetu pasiekiamus įrenginius.	PĮ periodiškai skenuoja visame pasaulyje IPv4 režiais viešai internetu pasiekiamus įrenginius
2.	PĮ turi nustatinėti skenuojamų įrenginių programinę įrangą, versijas, žinomas saugumo spragas.	PĮ nustatinėja skenuojamų įrenginių programinę įrangą, versijas, žinomas saugumo spragas.

<i><b>Eil. Nr</b></i>	<i><b>Reikalaujama charakteristika (ne blogiau kaip)</b></i>	<i><b>Siūloma charakteristika (Pildo tiekėjas)</b></i>
3.	PĮ turi kaupti kiekvieno įrenginio istorinę informaciją	PĮ kaupia kiekvieno įrenginio istorinę informaciją
4.	Turi būti suteikta galimybė pagal poreikį atlikti įvairių interneto adresų režijų skenavimą (ne mažiau kaip 50000 IP adresų per mėn.) ir galimybę realiu laiku stebėti tinkle (ne mažiau kaip 50000 IP adresų per mėn.) atsiradusį aktyvumą.	Yra suteikta galimybė pagal poreikį atlikti įvairių interneto adresų režijų skenavimą (50000 IP adresų per mėn.) ir galimybę realiu laiku stebėti tinkle (50000 IP adresų per mėn.) atsiradusį aktyvumą.
5	Turi būti galimybė vykdyti paiešką parenkant filtro parametrus, bei gauti rezultatus apie objekto santykį su aplinka: IP adresas, veikiančios tinklo tarnybos ir prievada, operacinė sistema, organizacijai priskirtas tinklo segmentas ar segmentai, režius aptarnaujantys paslaugų teikėjai, domeno vardai, geografinės vietos duomenys, potencialios žinomos saugumo spragos (angl. „Common vulnerabilities and exposures”, CVE).	Yra galimybė vykdyti paiešką parenkant filtro parametrus, bei gauti rezultatus apie objekto santykį su aplinka: IP adresas, veikiančios tinklo tarnybos ir prievada, operacinė sistema, organizacijai priskirtas tinklo segmentas ar segmentai, režius aptarnaujantys paslaugų teikėjai, domeno vardai, geografinės
6.	Turi būti galimybė vykdyti paiešką pagal pažeidžiamumų registracijos duomenis.	Yra galimybė vykdyti paiešką pagal pažeidžiamumų registracijos duomenis.
7.	Turi būti galimybė vykdyti paiešką duomenų bazėje naudojant aplikacijų programavimo sąsają (API).	Yra galimybė vykdyti paiešką duomenų bazėje naudojant aplikacijų programavimo sąsają (API).
8.	Turi būti galimybė duomenų bazėje vykdytų paieškų rezultatus atvaizduoti grafiškai.	Yra galimybė duomenų bazėje vykdytų paieškų rezultatus atvaizduoti grafiškai.
9.	Turi būti galimybė vykdyti paiešką duomenų bazėje ne mažiau kaip 20 mln. kartų per mėnesį.	Yra galimybė vykdyti paiešką duomenų bazėje ne mažiau kaip 20 mln. kartų per mėnesį.
10.	PĮ turi veikti naršyklėje.	PĮ veikia naršyklėje.

**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.