TINKLO PAŽEIDŽIAMUMŲ SKENAVIMO PROGRAMINĖS ĮRANGOS LICENCIJOS TECHNINĖ SPECIFIKACIJA

1. **Pirkimo objektas** – „Nessus Pro” (tinklo kibernetinių pažeidžiamumų patikros programinės įrangos) arba lygiavertės programinės įrangos (toliau – PĮ) licencija 36 mėn. laikotarpiui.

1 lentelė

Eil. Nr	***Reikalaujama charakteristika (ne blogiau kaip)***	***Siūloma charakteristika (Pildo tiekėjas)***
Gamintojas ir Programinės įrangos licencijos pavadinimas - Gamintojas: *TENABLE NETWORK SECURITY IRELAND LIMITED.* ***Pavadinimas:*** *Nessus Professional - On Premise - Annual Subscription (New) - 3 Year Subscription.* ***Nuoroda:*** *https://static.tenable.com/marketing/datasheets/DataSheet-Nessus_Professional.pdf*		
1.	PĮ turi turėti ne mažiau kaip 100000 CVE - Common Vulnerabilities and Exposures (CVE) aprašų.	PĮ turi 100000 CVE - Common Vulnerabilities and Exposures (CVE) aprašų.
2.	PĮ funkcionalumas:	
2.1.	Turi būti galimybė atlikti sistemų pažeidžiamumų analizę	Yra galimybė atlikti sistemų pažeidžiamumų analizę
2.2.	Turi būti galimybė atlikti sistemos patikrą nediegiant agento į tikrinamą sistemą	Yra galimybė atlikti sistemos patikrą nediegiant agento į tikrinamą sistemą
2.3.	Turi nustatyti kokių pataisymų trūksta tikrinamoje sistemoje ir kokie yra tikrinamos sistemos nustatymai	Nustato kokių pataisymų trūksta tikrinamoje sistemoje ir kokie yra tikrinamos sistemos nustatymai
2.4.	Turi patikrinti tikrinamos sistemos konfigūracijos atitikimą nustatytiems reikalavimams	Patikrina tikrinamos sistemos konfigūracijos atitikimą nustatytiems reikalavimams
2.5	Turi būti galimybė patikrinti sistemų konfigūracijas, dėl kurių gali atsirasti saugumo spragų ar atitikties problemų	Yra galimybė patikrinti sistemų konfigūracijas, dėl kurių gali atsirasti saugumo spragų ar atitikties problemų
2.6.	Turi nustatyti aktyvius IP adresus	Nustatyto aktyvius IP adresus
2.7.	Turi nustatyti aktyvius (atvirus) prievadus	Nustato aktyvius (atvirus) prievadus
2.8.	Turi būti palaikomi nuskaitymo protokolai - icmp, udp, tcp	Palaikomi nuskaitymo protokolai - icmp, udp, tcp
2.9.	Turi būti galimybė automatiškai surasti tinkle esančias sistemas ir įrenginius, bei bandyti nustatyti juose naudojamas operacines sistemas, programinę įrangą	Yra galimybė automatiškai surasti tinkle esančias sistemas ir įrenginius, bei bandyti nustatyti juose naudojamas operacines sistemas, programinę įrangą
2.10.	Turi būti prieiga prie ataskaitų atskyrimo	Yra prieiga prie ataskaitų atskyrimo
2.11.	Turi būti galimybė atlikti automatinį pažeidžiamumų nustatymo skenavimą nurodytu laiku	Yra galimybė atlikti automatinį pažeidžiamumų nustatymo skenavimą nurodytu laiku
2.12.	Turi būti galimybė atlikti skenavimus reguliariai nustatytu periodiškumu	Yra galimybė atlikti skenavimus reguliariai nustatytu periodiškumu
2.13.	Turi būti skenavimo rezultatų eksportas HTML, PDF arba CSV formatais	Yra skenavimo rezultatų eksportas HTML, PDF arba CSV formatais

2.14.	Turi būti pažeidžiamumų duomenų bazių atnaujinimai	Yra pažeidžiamumų duomenų bazių atnaujinimai
2.15.	Turi atlikti patikrinimus su įgaliojimais (kredencialais)	Atlieka patikrinimus su įgaliojimais (kredencialais)
2.16.	Turi būti galimybė integruoti su privilegijuotų paskyrų valdymo sprendimais (PAM), atnaujinimų valdymo (Patch Management) trečiųjų šalių sprendimais	Yra galimybė integruoti su privilegijuotų paskyrų valdymo sprendimais (PAM), atnaujinimų valdymo (Patch Management) trečiųjų šalių sprendimais
2.17.	Turi skenuoti Linux, MacOS, Windows tipo operacines sistemas ir tinklo įrenginius (Cisco, HPE, F5, Palo Alto)	Skenuoja Linux, MacOS, Windows tipo operacines sistemas ir tinklo įrenginius (Cisco, HPE, F5, Palo Alto)
2.18.	Turi būti diegiama įstaigos patalpose (on premises)	Diegiama įstaigos patalpose (on premises)
2.19.	Turi būti galimybė keisti skenavimo politiką pagal poreikį	Yra galimybė keisti skenavimo politiką pagal poreikį
2.20.	Turi pateikti išsamius trūkumų šalinimo veiksmus ir rekomendacijos nustatytoms pažeidžiamoms vietoms pašalinti	Pateikia išsamius trūkumų šalinimo veiksmus ir rekomendacijos nustatytoms pažeidžiamoms vietoms pašalinti
3.	Programinė įranga turi būti pateikta užtikrinant 36 mėnesių gamintojo palaikymą, suteikiant teisę gauti programinės įrangos naujas versijas, atnaujinimus, pataisymus. Šiuo laikotarpiu perkančioji organizacija turi teisę registruoti pastebėtas programinės įrangos klaidas, gedimus ir apie tai pranešti el. paštu	Programinė įranga pateikta užtikrinant 36 mėnesių gamintojo palaikymą, suteikiant teisę gauti programinės įrangos naujas versijas, atnaujinimus, pataisymus. Šiuo laikotarpiu perkančioji organizacija turi teisę registruoti pastebėtas programinės įrangos klaidas, gedimus ir apie tai pranešti el. paštu

Prekės neturi kelti grėsmės Nacionaliniam saugumui vadovaujantis Viešųjų pirkimų įstatymo 37 str. 9 d.

Viešųjų pirkimų specialistė