KONSOLIDUOTOS INFRASTRUKTŪROS IR SVETAINIŲ PAŽEIDŽIAMUMO SKENAVIMO PROGRAMINĖS ĮRANGOS LICENCIJOS NUOMOS PIRKIMO TECHNINĖ SPECIFIKACIJA

1. Pirkimo objektas – infrastruktūros ir svetainių pažeidžiamumų skenavimo programinės įrangos licencijos (1 vnt.) nuoma (toliau – licencija arba programinė įranga) su 36 mėn. gamintojo palaikymu bei diegimo ir konfigūravimo paslaugomis.
2. Turi būti siūloma vieno gamintojo programinė įranga, valdoma centralizuotai iš vienos valdymo konsolės ir suteikianti visą šioje techninėje specifikacijoje nurodytą funkcionalumą.
3. Atsižvelgiant į tai, kad šiuo metu Perkančioji organizacija yra realizavusi Tenable sprendimus (naudojama Nessus Professional pažeidžiamumo aptikimo programinė įranga), kartu su pasiūlymu turi būti pateikti raštiški patvirtinimai siūlomos licencijos gamintojo ar jo atstovo, arba turi būti sudaręs sutartį su tokiu atstovu, kad siūloma licencija yra visa apimtimi suderinama su Nessus Professional programine įranga bei kad bus išsaugota esamos programinės įrangos gamintojo garantija.
4. Tiekėjo siūloma programinė įranga turi atitikti 1 lentelėje nurodytus reikalavimus.
5. Licencijos tiekėjas turi būti siūlomų licencijų gamintojas arba gamintojo atstovas, įgaliotas pateikti (parduoti) siūlomas licencijas, arba turi būti sudaręs sutartį su tokiu atstovu, turinčiu išvardintas teises. Kartu su pasiūlymu turi būti pateiktas tai įrodantis (-ys) dokumentas (-ai).
6. Tiekėjas licenciją turi pristatyti ne vėliau kaip per 5 (penkias) kalendorines dienas nuo sutarties įsigaliojimo dienos.
7. Prekės ir paslaugos neturi kelti grėsmės nacionaliniam saugumui, vadovaujantis Viešųjų pirkimų įstatymo 37 str. 8 p. ir 9 p.
8. Jeigu techninėje specifikacijoje ir (ar) kituose pridedamuose dokumentuose apibūdinant pirkimo objektą nurodytas konkretus pavadinimas ar šaltinis, konkretus procesas ar prekės ženklas, patentas, tipai, konkreti kilmė ar gamyba, standartas, Tiekėjas gali pateikti lygiavertį sprendinį (kitų gamintojų lygiavertė produkcija ar įranga, pan.) nurodytajam. Lygiavertiškumo įrodymas yra Tiekėjo pareiga.
9. Tiekėjas privalo nurodyti siūlomų prekių parametrus. Grafoje "Siūloma parametro reikšmė" nurodomi konkretūs siūlomi parametrai pagal nurodytą aprašymą (rašyti „Atitinka" arba „Taip" neleidžiama).

1 lentelė.

Eil. Nr.	Parametras	Reikalaujama parametro reikšmė	Siūloma parametro reikšmė (Dokumento pavadinimas, puslapio numeris ir/ar tiksli nuoroda į internetinį puslapį Prekės atitikimo pagrindimui)
1.	Programinės įrangos apibūdinimas	Programinės įrangos gamintojas	Tenable, Inc
		Programinės įrangos pavadinimas	Siūlomas sprendimas – „Tenable Security Center". Su šiuo sprendimu suteikiami šie produktai: • Tenable Security Center - console - valdymo konsolė; • Tenable Security Center - Scanner(s)(Tenable Nessus scanners) – tinklo skenavimo varikliai. • Tenable Nessus Network Monitor – pasyvaus tinklo skenavimo įrankis. • Tenable Security Center - Web Application Scanning application – žiniatinklio aplikacijų skenavimo įrankis. Plačiau: License Requirements (Tenable Security Center 6.4.x)
		Gamintojo kodas	TSC-TNB; TSC-STNDC-TNB; TSC-WAS-TNB;

2.	Licencijos ir palaikymas	Programinės įrangos licencija turi leisti: – Skenuoti ir stebėti ne mažiau kaip 1000 vidinių IP adresų. – Leisti naudoti neribotą kiekį pažeidžiamumų skenavimo variklių (angl. *scanners*). – Skenuoti ne mažiau kaip 15 išorinių IP adresų (t.y. 15 vnt. žiniatinklio programų (angl. *web applications*)).	
		Programinė įranga turi būti pateikiama su gamintojo palaikymo paslaugų paketu. Palaikymo galiojimo laikotarpiu turi būti užtikrinama teisė gauti programinės įrangos atnaujinimus, pataisymus, signatūrų bazių atnaujinimus bei prieigą prie naudojamų aprašų ir kitų duomenų, reikalingų pilnaverčiam programinės įrangos darbui. Palaikymo trukmė – 36 mėn. nuo programinės įrangos perdavimo–priėmimo akto ar Sąskaitos (kai Prekių perdavimo–priėmimo aktas nėra pasirašomas) pasirašymo dienos, pristačius programinę įrangą.	
3.	Architektūra	Turi būti galimybė pažeidžiamumų valdymo programinę įrangą diegti ne mažiau kaip šiose operacinėse sistemose: – Red Hat Enterprise Linux – CentOS Stream – Oracle Linux	Siūlomą pažeidžiamumų valdymo programinę įrangą galima diegti šiose operacinėse sistemose: – Red Hat Enterprise Linux 7, 8, 9 – CentOS Stream 9 – Oracle Linux 8, 9 Plačiau: Tenable Security Center Software Requirements (General Requirements)
		Turi būti galimybė skenavimo variklį diegti ne mažiau kaip šiose operacinėse sistemose: – Windows Server – Ubuntu Linux – Red Had Enterprise Linux – CentOS	Skenavimo variklius galima diegti šiose operacinėse sistemose: – Windows Server 2012, 2012 R2, 2016, 2019, 2022 – Ubuntu Linux 14.04, 16.04, 17.10, 18.04, 20.04, ir 22.04 – Red Had Enterprise Linux 7, 8 ir 9 – CentOS Stream 9 Plačiau: Tenable Nessus Software Requirements (General Requirements)
		Siekiant aptikti saugumo pažeidžiamumus, programinė įranga turi gebėti skenuoti ne mažiau kaip šiuos tinklo įrenginius: Unix / Linux ir Windows OS pagrindu veikiančius įrenginius, žiniatinklio ir duomenų bazių tarnybines stotis, maršrutizatorius, spausdintuvus, ugniasienes, komutatorius.	Siūlomas sprendimas geba skenuoti ne mažiau kaip šiuos tinklo įrenginius: Unix / Linux ir Windows OS pagrindu veikiančius įrenginius, žiniatinklio ir duomenų bazių tarnybines stotis, maršrutizatorius, spausdintuvus, ugniasienes, komutatorius. Pilnas sistemų sąrašas, kurias gali skenuoti sprendimas yra čia: Nessus Plugin Families | Tenable®
		Programinėje įrangoje turi būti galimybė įvesti naudotojų prisijungimo duomenis, įskaitant prisijungimo prie Windows sistemų prisijungimo duomenis, SSH prisijungimo duomenis ir kt., siekiant prisijungti prie skenuojamų sistemų ir atlikti teisių patikrinimus pataisų lygiui nustatyti, veikiantiems procesams, konfigūracijų auditui ir kt.	Programinėje įrangoje yra galimybė įvesti naudotojų prisijungimo duomenis, įskaitant prisijungimo prie Windows sistemų prisijungimo duomenis, SSH prisijungimo duomenis ir kt., siekiant prisijungti prie skenuojamų sistemų ir atlikti teisių patikrinimus pataisų lygiui nustatyti, veikiantiems procesams, konfigūracijų auditui ir kt. Plačiau: Credentials (Tenable Security Center 6.4.x)
		Programinė įranga turi gebėti testuoti tiek lokalius, tiek ir nutolusius pažeidžiamumus, nereikalaujant programinės įrangos diegimo	Programinė geba testuoti tiek lokalius, tiek ir nutolusius pažeidžiamumus, nereikalaujant programinės įrangos diegimo kiekvienoje testuojamos sistemos klientinėje dalyje, t. y.

		kiekvienoje testuojamos sistemos klientinėje dalyje, t. y. testavimas gali būti atliekamas nenaudojant agento (angl. *agentless*).	testavimas gali būti atliekamas nenaudojant agento (angl. *agentless*). Tam bus naudojamas Nessus Skeneris. Plačiau: Active Scans (Tenable Security Center 6.4.x)
		Programinė įranga turi turėti ne rečiau kaip 1 kartą per dieną atnaujinamą pažeidžiamumų duomenų bazę su naujausiais žinomais pažeidžiamumais ir turi turėti automatizuotą pažeidžiamumų duomenų bazės atnaujinimo mechanizmą.	Programinė įranga turi ne rečiau kaip 1 kartą per dieną atnaujinamą pažeidžiamumų duomenų bazę su naujausiais žinomais pažeidžiamumais ir turi turėti automatizuotą pažeidžiamumų duomenų bazės atnaujinimo mechanizmą. Atnaujinimai atliekami pagal iš anksto numatytą grafiką, standartiškai atnaujinama vieną kartą per parą. Plačiau: How to update plugins for Tenable products
		Programinė įranga turi: – Leisti skenuoti įrenginius pagal nustatytą tvarkaraštį. – Leisti įjungti arba išjungti pasirinktus testus, vykdant skenavimą pagal tvarkaraštį. – Pagal numatytą tvarkaraštį paleisti ir sustabdyti skenavimą be naudotojo įsikišimo. – Turėti galimybę pristabdyti ir atnaujinti skenavimą. – Turi būti galimybė vykdyti skenavimus ne pagal numatytą tvarkaraštį.	Programinė įranga gali: – Leisti skenuoti įrenginius pagal nustatytą tvarkaraštį. – Leisti įjungti arba išjungti pasirinktus testus, vykdant skenavimą pagal tvarkaraštį. – Pagal numatytą tvarkaraštį paleisti ir sustabdyti skenavimą be naudotojo įsikišimo. – Pristabdyti ir atnaujinti skenavimą. – Vykdyti skenavimus ne pagal numatytą tvarkaraštį. Plačiau: Manage Active Scans (Tenable Security Center 6.4.x)
		Programinė įranga turi gebėti nuolat stebėti ir profiliuoti tinklą realaus laiko režimu, naudojant pasyvaus tipo pažeidžiamumų skenavimo technologiją, t. y. nevykdant aktyvių skenavimo veiksmų.	Programinė įranga geba nuolat stebėti ir profiliuoti tinklą realaus laiko režimu, naudojant pasyvaus tipo pažeidžiamumų skenavimo technologiją, t. y. nevykdant aktyvių skenavimo veiksmų. Siūlymas sprendimas tam naudoja dinaminį pažeidžiamumų prioritetų vertinimą. Plačiau: CVSS vs. VPR (Tenable Security Center 6.4.x)
		Programinė įranga turi leisti nurodyti skenavimo „taikinius“ įvairiais formatais, įskaitant IP adresų intervalais, DNS vardais.	Programinė įranga leidžia nurodyti skenavimo „taikinius“ įvairiais formatais, įskaitant IP adresų intervalais, DNS vardais. Plačiau: Assets (Tenable Security Center 6.4.x)
		Programinė įranga turi turėti skenavimui naudojamo srauto konfigūravimo galimybes tinkle, siekiant išvengti pernelyg didelio srauto generavimo tinkle, kuris gali paveikti normalų tinklo infrastruktūros veikimą.	Programinė įranga turi skenavimui naudojamo srauto konfigūravimo galimybes tinkle, siekiant išvengti pernelyg didelio srauto generavimo tinkle, kuris gali paveikti normalų tinklo infrastruktūros veikimą. Pvz. programinė įranga gali sulėtinti nuskaitymą, kai aptinkama didelė tinklo apkrova. Plačiau: Scan Policy Options (Tenable Security Center 6.4.x)
		Programinė įranga turi turėti galimybę nustatyti politikas vykdyti vieną ar daugiau patikrinimų, vykdant bet kurį skenavimą.	Programinė įranga gali nustatyti politikas vykdyti vieną ar daugiau patikrinimų, vykdant bet kurį skenavimą. Tam yra sukuriamos politikos kurios vėliau naudojamos atliekant skenavimus.

			Plačiau apie politikas: Add a Scan Policy (Tenable Security Center 6.4.x) Plačiau apie skenavimus: Active Scan Settings (Tenable Security Center 6.4.x)
		Programinė įranga turi turėti centralizuoto valdymo konsolę, kuri leidžia nustatyti saugumo testavimo parametrus įvairiems tinklo įrenginiams visoje organizacijoje. Centralizuoto valdymo konsolė turi suteikti galimybę išplatinti saugumo politikos nustatymus įvairiems programinės įrangos moduliams.	Programinė įranga turi centralizuoto valdymo konsolę, kuri leidžia nustatyti saugumo testavimo parametrus įvairiems tinklo įrenginiams visoje organizacijoje. Centralizuoto valdymo konsolė turi galimybę išplatinti saugumo politikos nustatymus įvairiems programinės įrangos moduliams. Plačiau: Tenable Nessus Scanners (Tenable Security Center 6.4.x)
		Programinė įranga turi turėti galimybę saugoti vykdytų skenavimo ir saugumo vertinimų rezultatus duomenų bazėje ir turėti galimybę peržiūrėti istoriją bei generuoti pasirinktas ataskaitas, remiantis surinktais duomenimis. Duomenų bazė turi atitikti šiuos reikalavimus: – Neturi reikalauti trečiųjų šalių duomenų bazių rezultatų saugojimui. – Suteikti galimybę išskirstyti skenavimų duomenis į atskiras saugyklas pagal gautų rezultatų tipus (pvz.: pažeidžiamumai, atitikimas reikalavimams, autorizuoti prieš neautorizuotus skenavimus, fizinė lokacija, funkcinė grupė ir t. t.), tuo pačiu leidžiant vykdyti analizę ir generuoti valdymo skydelio ataskaitas. – Rezultatus saugoti apibrėžtą ir konfigūruojamą laiką, po kurio rezultatai nustoja galioti ir yra pašalinami iš duomenų bazės automatiškai. – Turi būti atskira duomenų bazė aktyviems ir nepavojingiems pažeidžiamumams su automatiniu pažeidžiamumų migravimu iš aktyvių į nepavojingų pažeidžiamumų duomenų bazę. – Turėti galimybę rankiniu būdu pažymėti pažeidžiamumą kaip nepavojingą, kuris galbūt pakartotinai yra rodomas kaip aktyvus po virtualios mašinos atstatymo iš rezervinės kopijos ar pan.	Programinė įranga turi galimybę saugoti vykdytų skenavimo ir saugumo vertinimų rezultatus duomenų bazėje ir turėti galimybę peržiūrėti istoriją bei generuoti pasirinktas ataskaitas, remiantis surinktais duomenimis. Duomenų bazė atitinka šiuos reikalavimus: – Nereikalauja trečiųjų šalių duomenų bazių rezultatų saugojimui. – Suteikia galimybę išskirstyti skenavimų duomenis į atskiras saugyklas pagal gautų rezultatų tipus (pvz.: pažeidžiamumai, atitikimas reikalavimams, autorizuoti prieš neautorizuotus skenavimus, fizinė lokacija, funkcinė grupė ir t. t.), tuo pačiu leidžiant vykdyti analizę ir generuoti valdymo skydelio ataskaitas. – Rezultatus saugo apibrėžtą ir konfigūruojamą laiką, po kurio rezultatai nustoja galioti ir yra pašalinami iš duomenų bazės automatiškai. – Gali būti atskira duomenų bazė aktyviems ir nepavojingiems pažeidžiamumams su automatiniu pažeidžiamumų migravimu iš aktyvių į nepavojingų pažeidžiamumų duomenų bazę. – Turi galimybę rankiniu būdu pažymėti pažeidžiamumą kaip nepavojingą, kuris galbūt pakartotinai yra rodomas kaip aktyvus po virtualios mašinos atstatymo iš rezervinės kopijos ar pan. Plačiau duomenų bazes: Repositories (Tenable Security Center 6.4.x) Plačiau apie duomenų bazių pasirinkimą skenavimams ir duomenų pašalinimą iš duomenų bazių, čia: Active Scan Settings (Tenable Security Center 6.4.x) Plačiau apie galimybę rankiniu būdu pažymėti pažeidžiamumą kaip nepavojingą: Add an

			Accept Risk Rule (Tenable Security Center 6.4.x)
		Programinė įranga turi palaikyti išvardintų operacinių sistemų skenavimą įskaitant, bet neapsiribojant: – Microsoft Windows – CentOS – Ubuntu – Red Hat Enterprise Linux – Oracle Linux	Programinė įranga palaiko išvardintų operacinių sistemų skenavimą įskaitant, bet neapsiribojant: – Microsoft Windows – CentOS – Ubuntu – Red Hat Enterprise Linux – Oracle Linux Plačiau apie palaikomų sistemų skenavimą: Nessus Plugin Families | Tenable®
		Programinė įranga turi palaikyti SNMP protokolu (angl. *Simple Network Management Protocol*) veikiančių tinklo įrenginių pažeidžiamumų skenavimą ir konfigūracijos auditą.	Programinė įranga palaiko SNMP protokolu (angl. *Simple Network Management Protocol*) veikiančių tinklo įrenginių pažeidžiamumų skenavimą ir konfigūracijos auditą. Plačiau apie SNMP naudojimą: Host (Tenable Security Center 6.4.x)
		Programinė įranga turi palaikyti naudotojų sukurtų ir aprašytų skenavimų vykdymą.	Programinė įranga palaiko naudotojų sukurtų ir aprašytų skenavimų vykdymą Plačiau apie skenavimų sukūrimą: Add an Active Scan (Tenable Security Center 6.4.x) Plačiau apie skenavimų vykdymą: Manage Active Scans (Tenable Security Center 6.4.x)
		Programinė įranga turi palaikyti VMware ESXi/vSphere virtualizavimo platformų pažeidžiamumų skenavimą.	Programinė įranga palaiko VMware ESXi/vSphere virtualizavimo platformų pažeidžiamumų skenavimą. Plačiau: VMware ESX Local Security Checks Plugins | Tenable®
		Turi būti galimybė inicijuoti automatinį skenavimą per taikomųjų programų sąsają (angl. *application programming interface, arba* API).	Programinė įranga turi galimybę inicijuoti automatinį skenavimą per taikomųjų programų sąsają (angl. *application programming interface, arba* API). Plačiau: Tenable Security Center API: Scan
4.	Integracijos	Siūloma programinė įranga turi turėti integraciją su Perkančiosios organizacijos naudojamais įrankiais: – Atlassian Jira – IBM QRadar SIEM – CyberArk PAM (angl. *Privileged access management*)	Siūloma programinė įranga turi integraciją su Perkančiosios organizacijos naudojamais įrankiais: – Atlassian Jira – IBM QRadar SIEM – CyberArk PAM (angl. *Privileged access management*) Plačiau: Integrations Documentation | Tenable™
5.	Žiniatinklio programų skenavimas	Turi turėti žiniatinklio programų skenavimo funkcionalumą, valdomą iš centralizuotos siūlomos programinės įrangos valdymo konsolės.	Siūloma programinė įranga turi žiniatinklio programų skenavimo funkcionalumą, valdomą iš centralizuotos siūlomos programinės įrangos valdymo konsolės. Plačiau: Web App Scans (Tenable Security Center 6.4.x)
		Turi gebėti skenuoti vidines ir išorines žiniatinklio programas ir programų sąsajas (angl. *application programming interface*, arba API).	Siūloma programinė įranga geba skenuoti vidines ir išorines žiniatinklio programas ir programų sąsajas (angl. *application programming interface*, arba API). Plačiau apie API skenavimą: Scan Templates (Tenable Nessus 10.8)

			Plačiau apie žiniatinklio aplikacijų skenavimą: Web App Scan Settings (Tenable Security Center 6.4.x)
		Turi gebėti aptikti ir klasifikuoti žiniatinklio programų pažeidžiamumus pagal OWASP Top 10 ir OWASP API Top 10.	Siūloma programinė įranga geba aptikti ir klasifikuoti žiniatinklio programų pažeidžiamumus pagal OWASP Top 10 ir OWASP API Top 10. Plačiau apie OWASP: Web Application Scanning
		Siūloma programinė įranga turi palaikyti skenavimą su autentifikacija ir be autentifikacijos.	Siūloma programinė įranga palaiko skenavimą su autentifikacija ir be autentifikacijos. Plačiau apie autentifikacijos opcijas: Scan Policy Options (Tenable Security Center 6.4.x) Plačiau apie skenavimą su autentifikacija: Credentials (Tenable Security Center 6.4.x)
		Siūloma programinė įranga turi pateikti svetainės struktūrą (angl. *sitemap*) kiekvienai žiniatinklio programai.	Siūloma programinė įranga gali pateikti svetainės struktūrą (angl. *sitemap*) kiekvienai žiniatinklio programai. Plačiau: Web Application Sitemap | Tenable®
		Skenavimo valdymas: – Turi būti galimybė pristabdyti, tęsti, sustabdyti ir suplanuoti nuskaitymą. – Turi būti galimybė nuskaityti kelis unikalius domenus pagal vieną nuskaitymo politiką. – Turi būti galimybė importuoti žiniatinklio programų sąrašą kaip nuskaitomus objektus. – Turi būti galimybė nuskaityti vieno puslapio programas (angl. *Single Page Application*). – Turi būti galimybė nuskaityti komponentų lygio pažeidžiamumus (pvz., Wordpress, Drupal ir kt.).	Siūloma programinė įranga turi: – Galimybę pristabdyti, tęsti, sustabdyti ir suplanuoti nuskaitymą. – Galimybę nuskaityti kelis unikalius domenus pagal vieną nuskaitymo politiką. – Galimybę importuoti žiniatinklio programų sąrašą kaip nuskaitomus objektus. – Galimybę nuskaityti vieno puslapio programas (angl. *Single Page Application*). – Galimybę nuskaityti komponentų lygio pažeidžiamumus (pvz., Wordpress, Drupal ir kt.). Plačiau: Web App Scans (Tenable Security Center 6.4.x) Scan and Policy Settings (Tenable Nessus 10.8) Advanced Settings in Tenable Web App Scanning Scans (Tenable Web App Scanning)
		Ataskaitos ir prietaisų skydeliai: – Turi būti galimybė rodyti skenavimo pagal OWASP Top 10 metodikos rezultatus. – Turi būti galimybė peržiūrėti rezultatus pagal žiniatinklio programą. – Turi būti galimybė filtruoti žiniatinklio programų nuskaitymo rezultatus. – Turi turėti galimybė kurti, diegti, bendrinti individualizuotus prietaisų skydelius (angl. *dashboards*).	Siūloma programinė įranga turi: – Galimybę rodyti skenavimo pagal OWASP Top 10 metodikos rezultatus. – Galimybę peržiūrėti rezultatus pagal žiniatinklio programą. – Galimybę filtruoti žiniatinklio programų nuskaitymo rezultatus. – Galimybę kurti, diegti, bendrinti individualizuotus prietaisų skydelius (angl. *dashboards*). Plačiau: Dashboards (Tenable Security Center 6.4.x) Filter Components (Tenable Security Center 6.4.x) Manage Reports (Tenable Security Center 6.4.x)

6.	Įrangos aptikimas (angl. *asset discovery*)	Programinė įranga turi palaikyti „Netstat“ programos naudojimą greitam ir tiksliam atvirų prievadų sąrašo sudarymui sistemose, kur galima panaudoti autorizaciją.	Programinė įranga palaiko „Netstat“ programos naudojimą greitam ir tiksliam atvirų prievadų sąrašo sudarymui sistemose, kur galima panaudoti autorizaciją. Plačiau: Scan Policy Options (Tenable Security Center 6.4.x)
		Programinė įranga turi palaikyti SMB (angl. *Server Message Block*) ir WMI (angl. *Windows Management Instrumentation*) technologijų naudojimą Windows sistemų skenavimui.	Programinė įranga palaiko SMB (angl. *Server Message Block*) ir WMI (angl. *Windows Management Instrumentation*) technologijų naudojimą Windows sistemų skenavimui. Plačiau: Scan Policy Options (Tenable Security Center 6.4.x) Scan Policy Options (Tenable Security Center 6.4.x)
		Programinė įranga turi gebėti automatiškai paleisti nuotolinio registro paslaugas, Windows sistemose atliekant autorizuotą skenavimą ir automatiškai sustabdyti šias paslaugas, kai skenavimas baigiamas.	Programinė įranga geba automatiškai paleisti nuotolinio registro paslaugas, Windows sistemose atliekant autorizuotą skenavimą ir automatiškai sustabdyti šias paslaugas, kai skenavimas baigiamas. Plačiau: Scan Policy Options (Tenable Security Center 6.4.x)
		Programinė įranga turi palaikyti SSH su „su“ ir „sudo“ privilegijų eskalavimui, reikalingam pažeidžiamumo skenavimui ir konfigūracijos auditavimui Unix / Linux sistemose.	Programinė įranga palaiko SSH su „su“ ir „sudo“ privilegijų eskalavimui, reikalingam pažeidžiamumo skenavimui ir konfigūracijos auditavimui Unix / Linux sistemose. Plačiau: SSH Credentials (Tenable Security Center 6.4.x)
		Programinė įranga turi gebėti pasyviai skenuoti pažeidžiamumus ir atlikti nuolatinį įrenginių aptikimą, stebint srautą tinkle ir neatliekant aktyvių sistemų skenavimo veiksmų.	Programinė įranga geba pasyviai skenuoti pažeidžiamumus ir atlikti nuolatinį įrenginių aptikimą, stebint srautą tinkle ir neatliekant aktyvių sistemų skenavimo veiksmų. Plačiau: Tenable Nessus Network Monitor Instances (Tenable Security Center 6.4.x)
		Programinė įranga turi turėti galimybę atlikti tinkle esančių įrenginių aptikimą, naudojant žurnalinių įvykių (angl. *logs*) duomenis tiems įrenginiams, kurie negali būti skenuojami.	Programinė įranga turi galimybę atlikti tinkle esančių įrenginių aptikimą, naudojant žurnalinių įvykių (angl. *logs*) duomenis tiems įrenginiams, kurie negali būti skenuojami. Plačiau: Tenable Log Correlation Engines (Tenable Security Center 6.4.x)
		Programinė įranga turi turėti galimybę susieti skenavimo rezultatus su sistemomis, esančiomis DHCP (angl. *Dynamic Host Configuration Protocol*) aplinkoje, kur IP adresai gali kisti.	Programinė įranga turi galimybę susieti skenavimo rezultatus su sistemomis, esančiomis DHCP (angl. *Dynamic Host Configuration Protocol*) aplinkoje, kur IP adresai gali kisti. Plačiau: Active Scan Settings (Tenable Security Center 6.4.x)
		Programinė įranga turi turėti galimybę būti sukonfigūruota tokiu būdu, kad skenavimo rezultatai būtų išsaugomi, ir tuo atveju, jeigu tikslinė sistema numatyto skenavimo metu buvo neprieinama, pvz., išjungta profilaktiniams darbams.	Programinė įranga turi galimybę būti sukonfigūruota tokiu būdu, kad skenavimo rezultatai būtų išsaugomi, ir tuo atveju, jeigu tikslinė sistema numatyto skenavimo metu buvo neprieinama, pvz., išjungta profilaktiniams darbams. Plačiau: Upload Scan Results (Tenable Security Center 6.4.x)

7.	Paskirstytas skenavimas	Programinė įranga turi palaikyti neribotą kiekį geografiškai nutolusių skenavimo variklių, valdomų iš centralizuotos valdymo konsolės. Turi būti galimybė sistemos naudotojui aprašyti pritaikomumo strategiją, įskaitant bet kokius didžiausius naudojamų skenavimo variklių ir (arba) skenuojamų IP adresų kiekio limitus.	Programinė įranga palaiko neribotą kiekį geografiškai nutolusių skenavimo variklių, valdomų iš centralizuotos valdymo konsolės. Yra galimybė sistemos naudotojui aprašyti pritaikomumo strategiją, įskaitant bet kokius didžiausius naudojamų skenavimo variklių ir (arba) skenuojamų IP adresų kiekio limitus. Plačiau: Tenable Nessus Scanners (Tenable Security Center 6.4.x) Scan Targets (Tenable Nessus 10.8)
		Programinė įranga turi palaikyti apkrovos balansavimą (angl. *load balancing*) ir automatinį užduočių perskirstymą (angl. *failover*) tarp keleto naudojamų skanerių, dinamiškai paskirstant apkrovą tarp skanerių, remiantis skanerio prieinamumu visos skenavimo užduoties metu.	Programinė įranga palaiko apkrovos balansavimą (angl. *load balancing*) ir automatinį užduočių perskirstymą (angl. *failover*) tarp keleto naudojamų skanerių, dinamiškai paskirstant apkrovą tarp skanerių, remiantis skanerio prieinamumu visos skenavimo užduoties metu. Plačiau: Tiered Deployments (Large Enterprise Deployments) Tiered Remote Repositories (Tenable Security Center 6.4.x)
8.	Pažeidžiamumų identifikavimas	Programinė įranga turi aptikti ir reitinguoti pažeidžiamumus, riziką ir silpnąsias vietas, remiantis rinkoje patvirtintais standartais, pvz., Common Vulnerability Scoring System (CVSS) ar lygiavertį. Ji taip pat turi pateikti išsamią informaciją, susijusią su rizikos kilme ir rekomendacijas, kaip šias rizikas išspręsti.	Programinė įranga aptinka ir reitinguoja pažeidžiamumus, riziką ir silpnąsias vietas, remiantis rinkoje patvirtintais standartais, pvz., Common Vulnerability Scoring System (CVSS) ar lygiavertį. Ji taip pat pateikia išsamią informaciją, susijusią su rizikos kilme ir rekomendacijas, kaip šias rizikas išspręsti. Plačiau: CVSS vs. VPR (Tenable Security Center 6.4.x)
		Programinė įranga turi pranešti apie pasirinktoje sistemoje žinomas silpnąsias vietas, kurios yra identifikuotos saugumo patariamųjų organizacijų (pvz., „Common Vulnerabilities and Exposures database“ (CVE) arba NIST „National Vulnerability Database“ (NVD) arba kitų lygiaverčių).	Programinė įranga gali pranešti apie pasirinktoje sistemoje žinomas silpnąsias vietas, kurios yra identifikuotos saugumo patariamųjų organizacijų (pvz., „Common Vulnerabilities and Exposures database“ (CVE) arba NIST „National Vulnerability Database“ (NVD) arba kitų lygiaverčių). Plačiau: CVSS vs. VPR (Tenable Security Center 6.4.x)
		Programinės įrangos pažeidžiamumų duomenų bazė turi turėti duomenis ne mažiau kaip šiems patikrinimams: – Operacinių sistemų saugumas ir pataisos (angl. *patch*) – Ugniasienės – DNS (angl. *Domain Name System*) – FTP (angl. *File Transfer Protocol*) – SMTP (angl. *Simple Mail Transfer Protocol*) – RPC (angl. *Remote Procedure Call*)	Programinės įrangos pažeidžiamumų duomenų bazė turi duomenis ne mažiau kaip šiems patikrinimams: – Operacinių sistemų saugumas ir pataisos (angl. *patch*) – Ugniasienės – DNS (angl. *Domain Name System*) – FTP (angl. *File Transfer Protocol*) – SMTP (angl. *Simple Mail Transfer Protocol*) – RPC (angl. *Remote Procedure Call*) – SNMP (angl. *Simple Network Management Protocol*) – LDAP (angl. *Lightweight Directory Access Protocol*)

		– SNMP (angl. *Simple Network Management Protocol*) – LDAP (angl. *Lightweight Directory Access Protocol*) – SMB (angl. *Server Message Block*) – CGI (angl. *Common Gateway Interface*) – Žiniatinklio serveriai – Duomenų bazės – „Užpakalinės durys“ (angl. *backdoor*) – Paslaugos trikdymas (angl. *Denial of Service*) – Numatytosios paskyros (angl. *Default Account*) – P2P (angl. Peer-To-Peer) – „Remote Shell“	– SMB (angl. *Server Message Block*) – CGI (angl. *Common Gateway Interface*) – Žiniatinklio serveriai – Duomenų bazės – „Užpakalinės durys“ (angl. *backdoor*) – Paslaugos trikdymas (angl. *Denial of Service*) – Numatytosios paskyros (angl. *Default Account*) – P2P (angl. Peer-To-Peer) – „Remote Shell“ Plačiau: Vulnerability Analysis Tools (Tenable Security Center 6.4.x) Vulnerability Analysis Filter Components (Tenable Security Center 6.4.x) Plugins | Tenable® Indicators | Tenable®
		Programinė įranga turi turėti galimybę: – Aptikti paslaugas, veikiančias naudojant nestandartinius prievadus (angl. *port*). – Aptikti paslaugas, nustatytas nerodyti prisijungimų antraščių (angl. *connection banner*). – Testuoti keletą tos pačios paslaugos egzempliorių, veikiančių naudojant skirtingus prievadus. – Skenuoti įrenginius, neatsakančius į „ping“ užklausą (angl. *dead host*).	Programinė įranga turi galimybę: – Aptikti paslaugas, veikiančias naudojant nestandartinius prievadus (angl. *port*). – Aptikti paslaugas, nustatytas nerodyti prisijungimų antraščių (angl. *connection banner*). – Testuoti keletą tos pačios paslaugos egzempliorių, veikiančių naudojant skirtingus prievadus. – Skenuoti įrenginius, neatsakančius į „ping“ užklausą (angl. *dead host*). Plačiau: Scan Policy Options (Tenable Security Center 6.4.x) Scan Policy Options (Tenable Security Center 6.4.x) Scan Policy Options (Tenable Security Center 6.4.x)
		Programinės įrangos pasyvaus skenavimo komponentas turi: – Automatiškai aptikti naujas ir potencialiai pavojingas (angl. *rogue*) sistemas, kurios sudaro potencialias saugumo rizikas. – Aptikti netinkamą naudojimą ir tiksliai nustatytas vidines grėsmes. – Aptikti pažeidžiamumus sistemose, kurių nėra galimybės aktyviai skenuoti dėl šių sistemų jautrumo (kritiškumo), politikos arba konfigūracijos. – Pažymėti visas interaktyvias ir šifruotas tinkle sesijas.	Programinės įrangos pasyvaus skenavimo komponentas gali: – Automatiškai aptikti naujas ir potencialiai pavojingas (angl. *rogue*) sistemas, kurios sudaro potencialias saugumo rizikas. – Aptikti netinkamą naudojimą ir tiksliai nustatytas vidines grėsmes. – Aptikti pažeidžiamumus sistemose, kurių nėra galimybės aktyviai skenuoti dėl šių sistemų jautrumo (kritiškumo), politikos arba konfigūracijos. – Pažymėti visas interaktyvias ir šifruotas tinkle sesijas. – Stebėti, kurios tiksliai sistemos komunikuoja su kitomis vidinėmis sistemomis.

		– Stebėti, kurios tiksliai sistemos komunikuoja su kitomis vidinėmis sistemomis. – Aptikti, kurie prievadai yra aptarnaujami ir kurie yra naršomi kiekvienoje individualioje sistemoje. – Pasyviai nustatyti operacinę sistemą kiekviename aktyviame įrenginyje. – Stebėti visus klientinių ir serverinių programų pažeidžiamumus.	– Aptikti, kurie prievadai yra aptarnaujami ir kurie yra naršomi kiekvienoje individualioje sistemoje. – Pasyviai nustatyti operacinę sistemą kiekviename aktyviame įrenginyje. – Stebėti visus klientinių ir serverinių programų pažeidžiamumus. Plačiau: Tenable Nessus Network Monitor Instances (Tenable Security Center 6.4.x) Tenable Nessus Network Monitor Settings Section (Tenable Nessus Network Monitor)
		Programinė įranga turi naudoti ankstesnių skenavimų metu surinktą informaciją apie testuojamą įrenginį, vykdydama vėlesnius testus.	Programinė įranga gali naudoti ankstesnių skenavimų metu surinktą informaciją apie testuojamą įrenginį, vykdydama vėlesnius testus. Plačiau: Assets (Tenable Security Center 6.4.x)
		Programinė įranga turi saugoti pažeidžiamumų aptikimo datas, kad būtų galima filtruoti pažeidžiamumus pagal datas ir generuoti ataskaitas .	Programinė įranga saugo pažeidžiamumų aptikimo datas, kad būtų galima filtruoti pažeidžiamumus pagal datas ir generuoti ataskaitas . Plačiau: Vulnerability Analysis Filter Components (Tenable Security Center 6.4.x)
		Programinė įranga turi turėti galimybę identifikuoti pažeidžiamumus, naudojant IPv4 ir IPv6 protokolus, naudojant tiek aktyvaus, tiek pasyvaus skenavimo technikas.	Programinė įranga turi galimybę identifikuoti pažeidžiamumus, naudojant IPv4 ir IPv6 protokolus, naudojant tiek aktyvaus, tiek pasyvaus skenavimo technikas. Plačiau: IPv4/IPv6 Repositories (Tenable Security Center 6.4.x) Tenable Nessus Network Monitor Settings Section (Tenable Nessus Network Monitor)
9.	Konfigūracijų auditas	Programinė įranga turi turėti galimybę vykdyti pataisų ir konfigūracijos auditus Windows ir Unix / Linux sistemoms.	Programinė įranga turi galimybę vykdyti pataisų ir konfigūracijos auditus Windows ir Unix / Linux sistemoms.Plačiau: Audit Files (Tenable Security Center 6.4.x)
		Programinė įranga turi pateikti paruoštas auditavimo politikas Windows, Unix / Linux OS, programoms, tinklo įrenginiams ir duomenų bazėms.	Programinė įranga turi paruoštas auditavimo politikas Windows, Unix / Linux OS, programoms, tinklo įrenginiams ir duomenų bazėms. Plačiau: Add a Template-Based Audit File (Tenable Security Center 6.4.x)
		Programinė įranga turi turėti galimybę vykdyti auditą pagal gamintojų ir (ar) kitų organizacijų siūlomas rekomendacijas ar gerąsias praktikas: – Duomenų bazių konfigūracijų auditai: Oracle, MySQL, SQL Server, DB2, Informix/DRDA, PostgreSQL arba lygiaverčius. – Antivirusinės PĮ gamintojų auditai. – CIS geriausių praktikų gidai. – DISA STIGs arba lygiavertis.	Programinė įranga turi galimybę vykdyti auditą pagal gamintojų ir (ar) kitų organizacijų siūlomas rekomendacijas ar gerąsias praktikas: – Duomenų bazių konfigūracijų auditai: Oracle, MySQL, SQL Server, DB2, Informix/DRDA, PostgreSQL arba lygiaverčius. – Antivirusinės PĮ gamintojų auditai. – CIS geriausių praktikų gidai. – DISA STIGs arba lygiavertis. – Gamintojų rekomenduojami nustatymai: Fortinet, Cisco maršrutizatorių konfigūracijos, Juniper,

		– Gamintojų rekomenduojami nustatymai: Fortinet, Cisco maršrutizatorių konfigūracijos, Juniper, Checkpoint GAiA, IBM iSeries, Nexus NX-OS, VMware vSphere/vCenter arba lygiaverčius.	Checkpoint GAiA, IBM iSeries, Nexus NX-OS, VMware vSphere/vCenter arba lygiaverčius. Plačiau: Vulnerability Analysis Filter Components (Tenable Security Center 6.4.x) Active Scan Objects (Tenable Security Center 6.4.x) References | Tenable® File Search | Tenable® CIS Cisco NX-OS L2 v1.1.0 | Tenable® VMware ESX Local Security Checks Plugins | Tenable® CIS Fortigate 7.0.x v1.3.0 L2 | Tenable® https://www.tenable.com/plugins/nessus/families/Firewalls
		Programinė įranga turi gebėti skenuoti žiniatinklio serverius, siekiant aptikti dažniausiai pasitaikančius žiniatinklio programų pažeidžiamumus, tokius kaip „SQL injection“, „cross-site scripting (XSS)“, „HTTP header injection“, „directory traversal“, „remote file inclusion“ ir „command execution“.	Programinė įranga geba skenuoti žiniatinklio serverius, siekiant aptikti dažniausiai pasitaikančius žiniatinklio programų pažeidžiamumus, tokius kaip „SQL injection“, „cross-site scripting (XSS)“, „HTTP header injection“, „directory traversal“, „remote file inclusion“ ir „command execution“. Plačiau: Web App Scans (Tenable Security Center 6.4.x) Scan Policy Options (Tenable Security Center 6.4.x)
10.	Saugumo darbų procesų valdymas (angl. *security workflow*)	Programinė įranga turi leisti naudotojui priimti rasto pažeidžiamumo riziką arba priskirti šiam pažeidžiamumui kitokį lygį nei gamintojo numatytasis rizikos lygis konkrečiam pažeidžiamumui.	Programinė įranga leidžia naudotojui priimti rasto pažeidžiamumo riziką arba priskirti šiam pažeidžiamumui kitokį lygį nei gamintojo numatytasis rizikos lygis konkrečiam pažeidžiamumui. Plačiau: Add an Accept Risk Rule (Tenable Security Center 6.4.x) Recast Risk Rules (Tenable Security Center 6.4.x)
		Programinė įranga turi leisti kurti užduotį ir priskirti ją konkrečiam naudotojui.	Programinė įranga leidžia kurti užduotį ir priskirti ją konkrečiam naudotojui. Plačiau: Ticket Options (Tenable Security Center 6.4.x)
		Programinė įranga turi leisti pridėti pažeidžiamumo informacijos momentinę kopiją (angl. *snapshot*), susijusią su konkrečia užduotimi.	Programinė įranga leidžia pridėti pažeidžiamumo informacijos momentinę kopiją (angl. *snapshot*), susijusią su konkrečia užduotimi. Plačiau: Alert Options (Tenable Security Center 6.4.x) Alert Actions (Tenable Security Center 6.4.x)
11.	Pranešimai (angl. *notifications*)	Programinė įranga turi užtikrinti pranešimų nustatymų konfigūravimą pagal pažeidžiamumų skenavimo arba konfigūracijos audito rezultatus.	Programinė įranga užtikrina pranešimų nustatymų konfigūravimą pagal pažeidžiamumų skenavimo arba konfigūracijos audito rezultatus. Plačiau: Alert Options (Tenable Security Center 6.4.x)
		Pranešime turi būti galimybė nustatyti ne mažiau kaip šią informaciją : užduoties sukūrimo data, nuoroda į konkretų pranešimą, skenavimo	Pranešime yra galimybė nustatyti ne mažiau kaip šią informaciją : užduoties sukūrimo data, nuoroda į konkretų pranešimą, skenavimo iniciavimas, syslog įvykio sugeneravimas ir

		iniciavimas, syslog įvykio sugeneravimas ir ataskaitos sugeneravimo inicijavimas.	ataskaitos sugeneravimo inicijavimas. Plačiau: Alert Actions (Tenable Security Center 6.4.x)
12.	Ataskaitos	Programinė įranga turi: – pateikti politikomis paremtą ataskaitų generavimą; – generuoti ataskaitas sukauptų istorinių duomenų pagrindu ir pateikti jas grafiniu bei tekstiniu formatu; – generuoti ataskaitas, rodančias pažeidžiamumų tendencijas per nustatytą laiką; – eksportuoti ataskaitas šiais bylų formatais: PDF, CSV, HTML.	Programinė įranga gali: – pateikti politikomis paremtą ataskaitų generavimą; – generuoti ataskaitas sukauptų istorinių duomenų pagrindu ir pateikti jas grafiniu bei tekstiniu formatu; – generuoti ataskaitas, rodančias pažeidžiamumų tendencijas per nustatytą laiką; – eksportuoti ataskaitas šiais bylų formatais: PDF, CSV, HTML. Plačiau: Reports (Tenable Security Center 6.4.x)
		Programinė įranga turi leisti automatiškai arba rankiniu būdu generuoti pagal naudotojo poreikius individualias ataskaitas arba pasinaudojant gamintojo parengtais šablonais.	Programinė įranga leidžia automatiškai arba rankiniu būdu generuoti pagal naudotojo poreikius individualias ataskaitas arba pasinaudojant gamintojo parengtais šablonais. Plačiau: Manage Reports (Tenable Security Center 6.4.x)
13.	Naudotojai ir prieigos kontrolė	Programinė įranga turi integruotis su LDAP (angl. *Lightweight Directory Access Protocol*) naudotojų autentifikacijai.	Programinė įranga integruojasi su LDAP (angl. *Lightweight Directory Access Protocol*) naudotojų autentifikacijai. Plačiau: LDAP Authentication (Tenable Security Center 6.4.x)
		Programinė įranga turi palaikyti rolėmis paremtą administravimą su galimybe priskirti tam tikras teises. Galimos teisės, bet neapsiribojant: – Patikrinimų duomenų bazės atnaujinimas. – Vykdyti bet kurį skenavimą, pateiktas skenavimo politikas arba jokio skenavimo. – Naudotojų administravimas. – Pažeidžiamumų duomenų peržiūra. – Nustatyti ir dalintis įrangos sąrašo paskyromis. – Pridėti audito bylas. – Sukurti įspėjimus. – Nustatyti ir dalintis prisijungimo duomenimis autorizuotiems skenavimams. – Sukurti ir dalintis skenavimo politikomis.	Programinė įranga palaiko rolėmis paremtą administravimą su galimybe priskirti tam tikras teises. Galimos teisės, bet neapsiribojant: – Patikrinimų duomenų bazės atnaujinimas. – Vykdyti bet kurį skenavimą, pateiktas skenavimo politikas arba jokio skenavimo. – Naudotojų administravimas. – Pažeidžiamumų duomenų peržiūra. – Nustatyti ir dalintis įrangos sąrašo paskyromis. – Pridėti audito bylas. – Sukurti įspėjimus. – Nustatyti ir dalintis prisijungimo duomenimis autorizuotiems skenavimams. – Sukurti ir dalintis skenavimo politikomis. Plačiau: User Roles (Tenable Security Center 6.4.x)
		Programinė įranga turi palaikyti individualius ir konfigūruojamus prietaisų skydus, įspėjimus, notifikacijas ir paskiriamas užduotis, ir ataskaitas naudotojo lygmenyje.	Programinė įranga palaiko individualius ir konfigūruojamus prietaisų skydus, įspėjimus, notifikacijas ir paskiriamas užduotis, ir ataskaitas naudotojo lygmenyje. Plačiau: User Roles (Tenable Security Center 6.4.x) Custom Group Permissions (Tenable Security Center 6.4.x)

		Programinė įranga turi turėti naudotojų veiksmų auditavimo galimybę.	Programinė įranga turi naudotojų veiksmų auditavimo galimybę. Plačiau: System Logs (Tenable Security Center 6.4.x)
14.	Prietaisų skydeliai (angl. *dashboards*)	Programinė įranga turi palaikyti individualizuojamus prietaisų skydelius, kuriuose gali būti atvaizduojama tiek grafinė, tiek ir sąrašais paremta informacija apie pažeidžiamumus. Prietaisų skydeliai gali būti individualizuojami tiek remiantis gamintojo pateiktais šablonais, tiek ir be jų.	Programinė įranga palaiko individualizuojamus prietaisų skydelius, kuriuose gali būti atvaizduojama tiek grafinė, tiek ir sąrašais paremta informacija apie pažeidžiamumus. Prietaisų skydeliai gali būti individualizuojami tiek remiantis gamintojo pateiktais šablonais, tiek ir be jų. Plačiau: Dashboards (Tenable Security Center 6.4.x)
		Prietaisų skydelio elementai turi būti visiškai individualizuojami, filtruojant duomenis, paremtus įrenginių sąrašu, pažeidžiamumų ir atitikimų testavimų rezultatais, laiku, raktiniais žodžiais, IP adresais ir kt.	Prietaisų skydelio elementai gali būti visiškai individualizuojami, filtruojant duomenis, paremtus įrenginių sąrašu, pažeidžiamumų ir atitikimų testavimų rezultatais, laiku, raktiniais žodžiais, IP adresais ir kt. Plačiau: Custom Dashboard Component Options (Tenable Security Center 6.4.x)
15.	Diegimas	Tiekėjo kvalifikuoti specialistai turi įdiegti ir sukonfigūruoti pažeidžiamumų skenavimo sprendimą ne vėliau kaip per 60 kalendorinių dienų nuo sutarties įsigaliojimo dienos. Diegimo darbų apimtis: – Turi būti įdiegta ne mažiau kaip 100 vnt. skenavimo variklių virtualiose mašinose į skirtingus perkančiosios organizacijos potinklius. – Turi būti įdiegta ne mažiau kaip 50 vnt. agentų į įvairias sistemas, įsikaitant bet neapsiribojant: • Windows Server 2012, 2012 R2, 2016, 2019, 2022 • Red Hat Linux 8, 9 • Oracle Linux 8, 9 • Ubuntu 14.04, 16.04, 18.04, 20.04, 22.04	
		Esamos tinklo infrastruktūros analizė ir diegimo plano parengimas bei suderinimas su Perkančiąja organizacija. Tiekėjas ne vėliau kaip per 14 kalendorinių dienų, nuo sutarties įsigaliojimo dienos pateikia Perkančiajai organizacijai reikalavimus kompiuterinės įrangos resursams Kompiuterinę įrangą (virtuali tarnybinė stotis), reikalingą sistemos diegimui, pateikia Perkančioji organizacija.	
		Diegimo proceso metu turi būti atlikta (įskaitant, bet neapsiribojant): – Sprendimo valdymo konsolės įdiegimas virtualioje aplinkoje. – Realizuota sistemos sąsaja su Active Directory ir naudotojų bei naudotojų grupių sukūrimas. – Skenavimo agentų įdiegimas į galinius įrenginius. – Tinklo skenavimo sensorių įdiegimas virtualiose mašinose. – Sprendimo pradinis nustatymas ir sukonfigūravimas. – Valdymo skydelių individualizavimas, kad naudotojams būtų atvaizduojama aktualiausia informacija (TOP pažeidžiamumai, naujausi skenavimo rezultatai, rizikingiausi resursai ir pan.). – Ryšio su agentais ir skenavimo varikliais testavimas. – Pradinis infrastruktūros skenavimas ir resursų aptikimas. – Dinaminių resursų grupių sukūrimas pagal gamintojo numatytus požymius naudojant paruoštus standartinius šablonus ir pagal individualiai Pirkėjo nurodomus parametrus. – Dinaminių grupių testavimas. – Skenavimo periodiškumo ir apimties sukonfigūravimas. – Ataskaitų, gavėjų ir siuntimo periodiškumo nustatymas.	

		– Suintegruoti diegiamą sprendimą su Pirkėjo naudojama CyberArk privilegijuotų naudotojų valdymo (PAM) sprendimu, panaudojant autentifikuotiems skenavimams atlikti. Diegimo darbai turi apimti visus reikalingus atlikti veiksmus, kad po diegimo ir konfigūravimo darbų sistema užtikrintų visą techninėje specifikacijoje reikalaujamą funkcionalumą. Diegimo metu visi konfigūracijų keitimo darbai turi būti dokumentuojami. Atlikus diegimo darbus, pateikiama detali atliktų konfigūracijų keitimų ataskaita. Taip pat ne vėliau kaip per 60 kalendorinių dienų nuo sutarties įsigaliojimo dienos turi būti **pravesti teoriniai ir praktiniai mokymai** sistemos administratoriams (naudotojams). Mokymų trukmė – ne mažiau 8 val. Preliminarus dalyvių skaičius – 5.