IT INFRASTRUKTŪROS SAUGUMO SPRENDIMO PIRKIMO SUTARTIS NR. S4-1

2021 m. lapkričio 19 d.

Vilnius

Viešoji įstaiga „Plačiajuostis internetas“ (toliau – perkančioji organizacija), atstovaujama direktoriaus Gyčio Liaugmino, veikiančio pagal viešosios įstaigos „Plačiajuostis internetas“ įstatus,

ir

Ūkio subjektų grupė, sudaryta iš Blue Bridge MSP, UAB bei UAB „Blue Bridge“, atstovaujama Blue Bridge MSP, UAB (toliau – tiekėjas), atstovaujama direktoriaus Daliaus Butkaus, veikiančio pagal bendrovės įstatus,

(toliau bendrai vadinamos – šalimis), sudarė šią sutartį (toliau – pirkimo sutartis):

SUTARTIES OBJEKTAS

1. Pirkimo objektas – IT infrastruktūros saugumo sprendimas (toliau – prekės). Perkamų prekių apimtys, savybės, reikalavimai prekėms nurodyti šios sutarties priede Nr. 1 „Techninė specifikacija“.
2. Prekių pristatymo ir įdiegimo terminas – 7 mėnesiai nuo sutarties pasirašymo dienos.
3. Prekės turi būti pristatomos į tinklo mazgus, esančius Lietuvos Respublikos teritorijoje (Kauno ir Vilniaus apskrityse).
4. Prekių diegimo vieta – Kauno ir Vilniaus m. savivaldybės.

PREKIŲ KAINA IR MOKĖJIMO TVARKA

5. Tiekėjas įsipareigoja prekes pristatyti už:

Eil Nr.	Pirkimo objektas	Kiekis	Mato vnt.	Suma (be PVM)
1.	IT infrastruktūros saugumo sprendimas	1	Kompl.	1 140 800,00
			Bendra pasiūlymo kaina (be PVM): - *Išreikšta žodžiais: vienas milijonas šimtas keturiasdešimt tūkstančių aštuoni šimtai eurų, 00 centų.*	1 140 800,00
			PVM: - *Išreikšta žodžiais: Išreikšta žodžiais: du šimtai trisdešimt devyni tūkstančiai penki šimtai šešiasdešimt aštuoni eurai, 00 centų.*	239 568,00
			Bendra pasiūlymo kaina (su PVM): - *Išreikšta žodžiais: vienas milijonas trys šimtai aštuoniasdešimt tūkstančių trys šimtai šešiasdešimt aštuoni eurai, 00 centų.*	1 380 368,00

6. Pagal pirkimo sutartį kaina apskaičiuojama taikant fiksuotos kainos metodą.
7. Į perkamų prekių kainą įskaityti visi tiekėjo mokami mokesčiai (įskaitant PVM): pristatymo, instaliavimo (įdiegimo) ir paleidimo, bei kitos dėl pirkimo sutarties vykdymo tiekėjui tenkančios išlaidos.
8. Pirkimo sutarties vertė ir kainos dėl kainų lygio pasikeitimo neperskaičiuojami. Padidėjus arba sumažėjus Lietuvos Respublikos teisės aktų nustatytam PVM dydžiui, prekių mato vieneto kaina ir atitinkamai pirkimo sutarties vertė atitinkamai didinama arba mažinama. Pakeistos prekių mato vieneto kainos yra taikomos tik toms prekėms, kurias perkančioji organizacija užsako Lietuvos Respublikoje įsigaliojus atitinkamų mokesčių pasikeitimams ir pirkimo sutarties šalims įforminus prekių mato vieneto kainų pakeitimą. Perskaičiuotas prekių mato vieneto kainas pirkimo sutarties šalių atstovai patvirtina pasirašomu papildomu susitarimu prie pirkimo sutarties.
9. Kainodaros taisyklės yra esminės pirkimo sutarties sąlygos, kurios nebus keičiamos per visą pirkimo sutarties vykdymo laikotarpį.
10. Išankstinis mokėjimas (avansas) nenumatomas.

11. Šią sutartį numatoma finansuoti iš ES SF lėšų naudojant sąskaitų apmokėjimo būdą pagal Projektų administravimo ir finansavimo taisykles, patvirtintas Lietuvos Respublikos finansų ministro 2014 m. spalio 8 d. įsakymu Nr. 1K-316, kuriam reikalingi ilgesni nei 30 d. apmokėjimo terminai. Todėl numatoma, kad perkančioji organizacija privalo mokėti tiekėjui sumą, patvirtintą tiekėjo pateiktuose mokėjimo dokumentuose ne vėliau kaip per 60 (šešiasdešimt) dienų nuo tinkamų mokėjimo dokumentų gavimo dienos.

12. Tiekėjas sąskaitą gali išrašyti ir pateikti perkančiajai organizacijai tik po to, kai pasirašomas priėmimo – perdavimo aktas.

13. Mokėjimai bus atliekami remiantis tiekėjo per „E. sąskaita“ sistemą pateikta sąskaita ir priėmimo – perdavimo aktu. Mokėtinos lėšos pervedamos į tiekėjo nurodytą sąskaitą. Sumokėjimo diena – tai diena, kai lėšos pervedamos iš perkančiosios organizacijos atsiskaitomosios sąskaitos.

TIEKĖJO TEISĖS IR PAREIGOS

14. Sudaroma dvišalė pirkimo sutartis, kurios sutarties šalys yra perkančioji organizacija ir tiekėjas.
15. Tiekėjas įsipareigoja:

15.1. nuosekliai vykdyti pirkimo sutartį, pirkimo sutartyje numatytais terminais ir tvarka pristatyti prekes perkančiosios organizacijos nurodytu adresu, jas surinkti, įdiegti (instaliuoti), išbandyti ir paleisti bei atlikti kitus darbus, numatytus pirkimo sutartyje ir techninėje specifikacijoje, įskaitant prekių defektų šalinimą, pateikti perkančiajai organizacijai prekių dokumentaciją. Tiekėjas taip pat įsipareigoja pasirūpinti visa būtina įranga, darbų priežiūra, darbuotojų sauga ir sveikata ir darbo jėga, reikalinga pirkimo sutarties vykdymui;

15.2. prisiimti atsakomybę, kaip vienintelis atsakingas asmuo, jei trečiosios šalys pateiktų reikalavimų dėl jų patirtos žalos turtui ar asmeniui, padarytos tiekėjo ar jo specialistų vykdant šią pirkimo sutartį ar dėl po šios pirkimo sutarties įvykdymo atsiradusių pirkimo komponentų trūkumų ir (ar) gedimų ir garantuoti galimų nuostolių atlyginimą perkančiajai organizacijai, jei jai būtų keliami tokie reikalavimai;

15.3. vykdyti perkančiosios organizacijos teisėtus nurodymus, susijusius su šios pirkimo sutarties tinkamu vykdymu;

15.4. laikytis Lietuvos Respublikoje galiojančių įstatymų ir kitų teisės aktų nuostatų ir užtikrina, kad jo darbuotojai jų laikytųsi;

15.5. atlyginti perkančiajai organizacijai nuostolius, jei tiekėjas ar jo specialistai nesilaikė Lietuvos Respublikoje galiojančių įstatymų ir kitų teisės aktų ir dėl to tretieji asmenys yra pateikę kokių nors reikalavimų ar pradėję procesinius veiksmus;

15.6. be išankstinio perkančiosios organizacijos sutikimo neperduoti trečiajai šaliai perkančiosios organizacijos pateiktų brėžinių, techninių specifikacijų ir kitų dokumentų, jei tai nėra būtina šiai pirkimo sutarčiai vykdyti;

15.7. perkančiosios organizacijos nurodymu sudaryti perkančiosios organizacijos atstovams galimybę dalyvauti prekių diegime (instaliavime), bandymuose ir paleidime;

15.8. vykdyti kitas pareigas, jei jos numatytos pirkimo sutartyje.

16. Tiekėjas turi teisę:

16.1. prašyti perkančiosios organizacijos, kad perkančiosios organizacijos atstovai lydėtų ir tiekėjo specialistus į prekių įdiegimo (instaliavimo) vietas ir (ar) suderintų su trečiaisiais asmenimis prekių įdiegimo (instaliavimo) laiką ir kt. už perkančiosios organizacijos nustatytą mokestį.

PERKANČIOSIOS ORGANIZACIJOS TEISĖS IR PAREIGOS

17. Perkančioji organizacija įsipareigoja:

17.1. bendradarbiauti su tiekėju ir suteikti jam informaciją, reikalingą tinkamam pirkimo sutarties įvykdymui;

17.2. jei reikia pirkimo sutarčiai įvykdyti, tiekėjui nemokamai pateikti brėžinių, reikalingų sutarčiai vykdyti, kopijas, taip pat kitų šios sutarties dokumentų kopijas;

17.3. sudaryti tiekėjui galimybes patekti į patalpas, įrenginius ir kt., kuriuose turi būti vykdomi numatyti prekių įdiegimo (instaliavimo) darbai, tačiau perkančioji organizacija neįsipareigoja lydėti tiekėjo specialistų į šias vietas;

17.4. pirkimo sutarties nustatytomis sąlygomis laiku apmokėti tiekėjo pateiktas ir patvirtintas sąskaitas.

18. Perkančiosios organizacijos teisės:

18.1. duoti tiekėjui nurodymus ir pateikti papildomus dokumentus ar instrukcijas, jei tai būtina tinkamam pirkimo sutarties įvykdymui ir (ar) jos trūkumų pašalinimui;

18.2. apžiūrėti, patikrinti, išmatuoti ir išbandyti prekes, jų dalis ir darbo kokybę, taip pat tikrinti bet kokių pirkimo sutartyje numatytų prekių paruošimą ir gamybą, kad galėtų įsitikinti, jog visos medžiagos, jų dalys ir darbo kokybė yra reikiamos kokybės ir apimties. Visi minėtieji tikrinimai atliekami ruošimo ar gamybos vietoje ar priėmimo vietoje. Prekės nėra priimamos, kol nėra atlikti reikiami patikrinimai ir bandymai, kurie atliekami tiekėjo sąskaita. Patikrinimai ir bandymai gali būti atlikti iki išsiuntimo, pristačius į pristatymo vietą ir (arba) į galutinę paskirties vietą. Perkančiosios organizacijos patikrinimams skiriama tiek laiko, kiek perkančiajai organizacijai reikia patikrinti prekes. Perkančioji organizacija iki prekių priėmimo–perdavimo akto pasirašymo turi teisę reikalauti iki nurodyto termino iš priėmimo vietos išgabenti prekes, kurios neatitinka pirkimo sutarties reikalavimų ir pakeisti pirkimo sutarties reikalavimų neatitinkančias prekes tinkamomis prekėmis ir (ar) įdiegti (instaliuoti), išbandyti ir paleisti jas pagal pirkimo sutarties reikalavimus ir (arba) tiekėjo sąskaita ištaisyti nurodytus defektus;

18.3. per 7 dienas nuo pirkimo sutarties įsigaliojimo dienos, jei reikia, surengti įvadinį susirinkimą, kuriame aptariami organizaciniai pirkimo sutarties vykdymo klausimai;

18.4. savo nuožiūra dalyvauti bet kuriame tiekėjo vykdomame prekių diegime (instaliavime), bandyme ir paleidime.

PRIEVOLIŲ ĮVYKDYMO UŽTIKRINIMAS IR TERMINAI

19. Visos prievolės turi būti įvykdytos pirkimo sutartyje nustatytais terminais.

20. Prievolių įvykdymas užtikrinamas pirkimo sutartyje nustatytais delspinigiais.

21. Sutartinės atsakomybės už prievolių nevykdymą ar netinkamą vykdymą nustatymas:

21.1. Jei tiekėjas dėl savo kaltės vėluoja pristatyti visas ar kai kurias prekes iki pirkimo sutartyje numatyto termino, perkančioji organizacija turi teisę be oficialaus įspėjimo ir nesumažindama kitų savo teisių gynimo priemonių, numatytų pirkimo sutartyje, reikalauti sumokėti 0,02 % dydžio delspinigius už kiekvieną vėluojamą dieną nuo pirkimo sutarties vertės be PVM.

21.2. Jei perkančioji organizacija laiku nevykdo sutartinių įsipareigojimų, tiekėjas gali reikalauti sumokėti 0,02 % dydžio delspinigius už kiekvieną vėluojamą dieną nuo vėluojamos apmokėti pirkimo sutarties vertės be PVM.

PIRKIMO SUTARTIES GALIOJIMAS

22. Pirkimo sutartis laikoma sudaryta ir įsigalioja tik ją pasirašius abiem pirkimo sutarties šalims.

23. Pirkimo sutartis galioja iki visiško pirkimo sutartyje numatytų įsipareigojimų įvykdymo. Prekių pristatymo ir įdiegimo terminas – 7 mėnesiai nuo pirkimo sutarties pasirašymo dienos. Atsiskaitymo su tiekėju terminas 60 (šešiasdešimt) dienų.

PIRKIMO SUTARTIES NUTRAUKIMO TVARKA

24. Jei kuri nors pirkimo sutarties šalis nevykdo savo įsipareigojimų pagal pirkimo sutartį, ji pažeidžia pirkimo sutartį. Vienai pirkimo sutarties šaliai pažeidus pirkimo sutartį, kitos šalys kartu ar atskirai pagal pirkimo sutarties sąlygas turi teisę:

24.1. reikalauti iš pirkimo sutartį pažeidusios šalies vykdyti sutartinius įsipareigojimus;

24.2. reikalauti iš pirkimo sutartį pažeidusios šalies atlyginti nuostolius;

24.3. reikalauti sumokėti pirkimo sutartyje nustatytus delspinigius;

24.4. nutraukti pirkimo sutartį.

25. Perkančioji organizacija, įspėjusi tiekėją prieš 30 dienų, gali nutraukti pirkimo sutartį šiais atvejais:

25.1. kai tiekėjas nevykdo savo įsipareigojimų pagal pirkimo sutartį;

25.2. kai tiekėjas per pagrįstai nustatytą laikotarpį neįvykdo perkančiosios organizacijos nurodymo ištaisyti netinkamai įvykdytus arba neįvykdytus sutartinius įsipareigojimus;

25.3. kai tiekėjas perleidžia pirkimo sutartį trečiajam asmeniui be perkančiosios organizacijos leidimo;

25.4. kai tiekėjas bankrutuoja arba yra likviduojamas, sustabdo ūkinę veiklą arba įstatymuose ir kituose teisės aktuose numatyta tvarka susidaro analogiška situacija;

25.5. dėl kitokio pobūdžio neveiksnumo, trukdančio vykdyti pirkimo sutartį.

26. Nutraukiant pirkimo sutartį perkančiosios organizacijos iniciatyva, nuostoliai ar išlaidos išieškomi iš tiekėjo.

27. Tiekėjas, prieš 30 dienų įspėjęs perkančiąją organizaciją, gali nutraukti pirkimo sutartį, šiais atvejais:

27.1. perkančioji organizacija nevykdo savo sutartinių įsipareigojimų;

27.2. perkančioji organizacija stabdo prekių ar jų dalies priėmimą daugiau kaip 90 dienų dėl pirkimo sutartyje nenurodytų ir ne dėl tiekėjo kaltės atsiradusių priežasčių.

SUBTIEKĖJAI, JEIGU VYKDANT PIRKIMO SUTARTĮ JIE PASITELKIAMI, IR JŲ KEITIMO TVARKA

28. Perkančioji organizacija numato tiesioginio atsiskaitymo su subtiekėjais galimybę, nepažeidžiant Viešųjų pirkimų įstatymo 88 straipsnio nuostatų. Sudarius pirkimo sutartį, tačiau ne vėliau negu pirkimo sutartis pradedama vykdyti, tiekėjas įsipareigoja perkančiajai organizacijai pranešti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Perkančioji organizacija taip pat reikalauja, kad tiekėjas informuotų apie minėtos informacijos pasikeitimus visu pirkimo sutarties vykdymo metu, taip pat apie naujus subtiekėjus, kuriuos jis ketina pasitelkti vėliau.

29. Perkančioji organizacija ne vėliau kaip per 3 darbo dienas nuo 27 punkte nurodytos informacijos gavimo dienos informuoja subtiekėjus apie tiesioginio atsiskaitymo galimybę. Subtiekėjas, norėdamas pasinaudoti tiesioginio atsiskaitymo galimybe, per 5 darbo dienas nuo informavimo apie tiesioginio atsiskaitymo galimybę, perkančiajai organizacijai pateikia prašymą raštu.

30. Sudarius pirkimo sutartį, tačiau ne vėliau negu pirkimo sutartis pradedama vykdyti, tiekėjas įsipareigoja perkančiajai organizacijai pranešti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Perkančioji organizacija taip pat reikalauja, kad tiekėjas informuotų apie minėtos informacijos pasikeitimus visu pirkimo sutarties vykdymo metu, taip pat apie naujus subtiekėjus, kuriuos jis ketina pasitelkti vėliau. Kartu su informacija apie naujus subtiekėjus pateikiami ir subtiekėjo pašalinimo pagrindų nebuvimą patvirtinantys dokumentai.

31. Subtiekėjui pateikus prašymą pasinaudoti tiesioginio atsiskaitymo galimybe, tarp perkančiosios organizacijos, tiekėjo ir jo subtiekėjo yra sudaroma trišalė sutartis, kurioje aprašoma tiesioginio atsiskaitymo su subtiekėju tvarka ir numatoma teisė tiekėjui prieštarauti nepagrįstiems mokėjimams subtiekėjui.

SUTARTIES SĄLYGŲ KEITIMAS

32. Pirkimo sutarties sąlygų keitimu nebus laikomas pirkimo sutarties sąlygų koregavimas joje numatytomis aplinkybėmis. Pirkimo metu numatomi galimi pirkimo sutarties pakeitimai esant išvardytoms aplinkybėms ir nustatyta tvarka:

32.1. tuo atveju, jei dėl nuo tiekėjo nepriklausančių aplinkybių tiekėjas negali pristatyti tiekėjo pasiūlyme nurodyto prekės modelio (pvz., gamintojas nutraukia konkretaus modelio gamybą ir pan. Prekių pristatymo tiekėjui terminų praleidimas ir pan. nėra laikoma nuo tiekėjo nepriklausančia aplinkybe), tiekėjas turi teisę siūlyti perkančiajai organizacijai pateikti analogišką prekę, kurios visos savybės ir funkcionalumas bei kokybė atitinka tiekėjo pasiūlyme pasiūlytos prekės technines charakteristikas ir funkcionalumą bei kokybę. Bet kokiu atveju šiame punkte nurodytų aplinkybių atsiradimas negali turėti įtakos pirkimo sutarties kainai ar bet kuriai iš jos sudedamųjų dalių. Keičiama prekė įforminama perkančiosios organizacijos ir tiekėjo pasirašomu protokolu;

32.2. tiekėjas negali keisti pasiūlyme nurodytų specialistų, prieš tai raštu nepranešęs perkančiajai organizacijai ir negavęs perkančiosios organizacijos raštiško sutikimo. Tiekėjas privalo savo iniciatyva siūlyti keisti specialistą šiais atvejais: specialisto mirties, ligos arba nelaimingo atsitikimo atveju; jei specialistą keisti būtina dėl kitų, nuo paslaugų teikėjo nepriklausančių priežasčių. Pirkimo sutarties vykdymo metu perkančioji organizacija gali inicijuoti specialisto, kuris netinkamai atlieka funkcijas, pakeitimą, nurodydamas tokio reikalavimo motyvus. Jei tenka keisti specialistą, kandidatas į jo vietą privalo turėti ne žemesnę kvalifikaciją ir patirtį pagal pirkimo dokumentuose nustatytus reikalavimus. Jei tiekėjas neranda naujo specialisto su tokia

pat kvalifikacija ir (arba) patirtimi, perkančioji organizacija turi teisę be atsakomybės taikymo nutraukti sutartį, arba sutikti, kad būtų priimtas siūlomas kandidatas. Visas išlaidas, patirtas dėl specialistų keitimo, atlygina tiekėjas. Jei specialistas pakeičiamas ne iš karto, perkančioji organizacija gali pareikalauti iš tiekėjo paskirti laikiną specialistą, arba imtis kitų priemonių kompensuoti laikiną naujo specialisto nebuvimą.

33. Sudarant pirkimo sutartį, negali būti keičiama laimėjusio tiekėjo pasiūlymo kaina ir pirkimo dokumentuose bei pasiūlyme nustatytos sąlygos. Sudaroma sutartis turi atitikti laimėjusio tiekėjo pasiūlymą ir pirkimo dokumentus.

34. Pirkimo sutartis sutarties galiojimo laikotarpiu gali būti keičiama tik Lietuvos Respublikos viešųjų pirkimų įstatymo 89 straipsnyje nurodytais atvejais ir apimtimi.

PREKIŲ PRISTATYMAS IR PREKĖMS TAIKOMOS GARANTIJOS

35. Tiekėjas privalo garantuoti, kad pristatytos prekės yra naujos, nenaudotos. Tiekėjas taip pat garantuoja, kad visos pristatytos prekės yra be defektų, atsiradusių dėl projekto, darbo, medžiagų ar pristatymo kokybės, išskyrus atvejį, kai konkretus projektas ar medžiagos yra privalomos pagal technines specifikacijas arba kai defektus lėmė koks nors veiksmas ar neveikimas, naudojant prekes perkančiosios organizacijos šalies sąlygomis. Ši garantija galioja tiek, kiek numatyta pirkimo sutartyje. Tiekėjas privalo kuo greičiau savo sąskaita pašalinti visus garantinio laikotarpio metu pastebėtus defektus ar įvykusius gedimus, kurie: atsirado dėl to, kad buvo naudojamos medžiagos su defektais, dėl prastos tiekėjo darbo kokybės ar reikalavimų neatitinkančių pristatymo sąlygų, atsirado dėl kokių nors tiekėjo veiksmų ar neveikimo garantinio laikotarpio metu, buvo pastebėti perkančiajai organizacijai tikrinant ar eksploatuojant prekes. Garantinis laikotarpis visoms pakeistoms ar sutaisytoms dalims vėl įsigalioja nuo dienos, kai buvo atliktas perkančiajai organizacijai priimtinas pakeitimas ar remontas. Jei defektai išaiškėja arba gedimai įvyksta garantinio laikotarpio metu, perkančioji organizacija raštu įspėja apie tai tiekėją. Jei tiekėjas nepašalina defekto ar gedimo per įspėjime nurodytą laikotarpį, perkančioji organizacija turi teisę pasamdyti kitus asmenis, kad atliktų šį darbą ir (ar) suteiktų paslaugas tiekėjo atsakomybe ir jo sąskaita. Tokiu atveju perkančiosios organizacijos patirtos išlaidos gali būti išskaičiuojamos iš tiekėjo. Ypatingos skubos atvejais, kai su tiekėju negalima iš karto susisiekti arba kai susisiekti pavyksta, bet tiekėjas negali imtis nurodytų priemonių, perkančioji organizacija gali atlikti darbus ir (ar) suteikti paslaugas tiekėjo sąskaita. Perkančioji organizacija kuo greičiau informuoja tiekėją apie atliktus darbus ir (ar) suteiktas paslaugas, o tiekėjas privalo atlyginti šių darbų atlikimo ir (arba) paslaugų suteikimo išlaidas. Garantinio laikotarpio įsipareigojimai yra numatyti techninėje specifikacijose. Jei garantinio laikotarpio trukmė nenurodyta, tuomet ji yra 2 metai. Garantinis laikotarpis pradedamas skaičiuoti nuo priėmimo–perdavimo akto pasirašymo dienos. Garantinio laikotarpio metu atsiradus prekės ar jos instaliavimo (įdiegimo) defektams, perkančioji organizacija raštu arba kitu būdu apie tai informuoja tiekėją. Tiekėjas savo jėgomis ir savo sąskaita visus defektus pašalina per pirkimo dokumentuose nustatytus terminus. Jei reikalinga defektui pašalinti, tiekėjas per pirkimo dokumentuose nurodytą terminą savo jėgomis ir sąskaita demontuoja, pasiima nurodytą prekę jos buvimo vietoje, pašalina defektą ir grąžina prekę į jos buvimo vietą, instaliuoja (įdiegia) ir paleidžia. Tiekėjui pasiimant prekę iš jos buvimo vietos, pasirašomas prekės perdavimo–priėmimo aktas.

36. Tiekėjas pristato prekes pagal tarptautinių prekybos rūmų taisykles „Incoterms“. Pristatymo sąlygos – DDP (pristatyta, muitas sumokėtas). Pristatymo laikotarpis pradedamas skaičiuoti nuo dienos, kai sutartį pasirašo visos sutarties šalys. Iki prekių priėmimo visa atsakomybė dėl prekių atsitiktinio žuvimo ar sugadinimo tenka tiekėjui. Prekės laikomos pristatytos tik tuomet, kai užsakovas pasirašo prekių priėmimo – perdavimo aktą. Jokie tarpiniai apžiūrų aktai ir kiti dokumentai, susiję su prekių pristatymo ir įrengimo (įdiegimo), bandymų priežiūra, nėra laikomi dokumentais, patvirtinančiais prekių priėmimą – perdavimą. Tiekėjas pasirūpina, kad prekės būtų pristatytos, įdiegtos (instaliuotos) į priėmimo vietą, išbandytos ir paleistos, visa prekių dokumentacija perduota perkančiajai organizacijai, suderina su perkančiąja organizacija, kad ji galėtų įforminti prekių priėmimą. Tiekėjas pasirūpina, kad prekės būtų supakuotos taip, kad jas gabenant į perkančiosios organizacijos nurodytą vietą jos nebūtų apgadintos ir nepablogėtų jų kokybė. Planuojant pakuotės dydį ir svorį turi būti atsižvelgta į atstumą iki paskirties vietos ir į tai, kad perkrovimo vietose gali nebūti tinkamos perkrovimo įrangos. Tiekėjas įsipareigoja išvežti pakuotę iš prekių įrengimo vietų ir sutvarkyti darbo vietą. Prekės laikomos tinkamai pristatytomis tik tokiu atveju, jei yra tinkamai įvykdytos visos šios sąlygos: a) prekės yra pristatytos ir įdiegtos (instaliuotos) į priėmimo vietą, išbandytos ir paleistos; b) visa prekių dokumentacija perduota perkančiajai organizacijai. Jei nėra įvykdyta bent viena šiame punkte

nurodyta prekių pristatymo sąlyga, laikoma, kad prekės nėra pristatytos. Tiekėjas privalo priėmimo – perdavimo aktus pateikti perkančiajai organizacijai skaitmeninėje laikmenoje.

37. Tais atvejais, kai numatyta techninėje specifikacijoje, tiekėjas kartu su prekėmis turi pateikti perkančiajai organizacijai prekių naudojimo ir priežiūros instrukcijas, kuriose turi būti detaliai aprašyta, kaip naudoti, prižiūrėti, reguliuoti ir taisyti bet kurias prekių dalis, bei kitą tiekėjo pasiūlyme ar prekių gamintojo oficialioje informacijoje nurodytą dokumentaciją.

38. Techninėje specifikacijoje nurodytas naudojimo ir priežiūros instrukcijų ir kitos prekių dokumentacijos kopijų kiekis ir kalba. Kol šios naudojimo ir priežiūros instrukcijos ir kita prekių dokumentacija nepateikiamos perkančiajai organizacijai, laikoma, kad atitinkamos prekės nėra pateiktos.

39. Prekių kokybė ir funkcionalumas bet kokiu atveju turi atitikti tiekėjo pasiūlyme, prie pasiūlymo pridėtuose dokumentuose, tiekėjo pasiūlymo paaiškinimuose ir prekės gamintojo parengtoje prekės naudojimo instrukcijoje nurodytą prekių funkcionalumą ir kokybę. Jei prekės neatitinka tiekėjo pasiūlyme, prie pasiūlymo pridėtuose dokumentuose, tiekėjo pasiūlymo paaiškinimuose ir prekės gamintojo parengtoje prekės naudojimo instrukcijoje nurodyto funkcionalumo ir kokybės, laikoma, kad prekės neatitinka pirkimo sutarties reikalavimų.

NENUGALIMA JĖGA

40. Šalys visiškai ar iš dalies atleidžiamos nuo šios pirkimo sutarties ar jos dalies įsipareigojimų vykdymo, jei tai įvyko dėl nenugalimos jėgos, atsiradusios po šios pirkimo sutarties sudarymo. Nenugalimos jėgos faktą turi įrodyti šalis, nevykdanti ar nebegalinti vykdyti pirkimo sutartyje nustatytų įsipareigojimų.

41. Nenugalimos jėgos aplinkybės turi būti patvirtintos Lietuvos Respublikos civilinio kodekso, Lietuvos Respublikos Vyriausybės 1996-07-15 nutarimo Nr. 840 ir Lietuvos Respublikos Vyriausybės 1997-03-13 nutarimo Nr.222 ir juos pakeičiančių teisės aktų nustatyta tvarka.

42. Apie tokių aplinkybių atsiradimą viena šalis kitai šaliai įsipareigoja pranešti ne vėliau kaip per 15 dienų nuo aplinkybių atsiradimo. Nepranešimas neatleidžia nuo pirkimo sutartyje numatytų įsipareigojimų vykdymo.

43. Nenugalimos jėgos atveju šalys dėl atsiradusių nuostolių papildomo atlyginimo ir darbų atlikimo terminų pratęsimo susitaria abipusiu šalių susitarimu.

KONFIDENCIALUMAS

44. Šalys įsipareigoja saugoti informaciją, sudarančią kitos šalies komercinę, finansinę, profesinę paslaptis, neleisti savo, kitų suinteresuotųjų asmenų privačių interesų naudai skleisti, naudotis šias paslaptis sudarančia informacija, o taip pat imtis visų nuo jų priklausančių priemonių, kad minėtoji informacija nepatektų tretiesiems asmenims.

45. Tiekėjas įsipareigoja neatskleisti tretiesiems asmenims jokios konfidencialios informacijos, kuri jam tapo žinoma pasirašius ar vykdant šią pirkimo sutartį ir (ar) informacijos, apimančios perkančiosios organizacijos ir su ja susijusių asmenų bei klientų duomenis.

46. Vienai iš šalių pažeidus konfidencialumo įsipareigojimus, kita šalis turi teisę, įspėjusi pirmąją šalį prieš 10 (dešimt) dienų, nutraukti šią pirkimo sutartį ir pareikalauti pirmosios šalies atlyginti atsiradusius tiesioginius ir netiesioginius nuostolius.

47. Pareiga laikytis konfidencialumo šalių atžvilgiu galioja neribotą laikotarpį nepriklausomai nuo to, kad šalys nutrauks bendradarbiavimą ir/ar šią pirkimo sutartį ir/ar ši pirkimo sutartis pasibaigs ją įvykdžius.

ASMENS DUOMENŲ APSAUGA

48. Vykdydamos pirkimo sutartį, šalys keičiasi informacija, kuri gali apimti asmens duomenis. Gaudamas iš perkančiosios organizacijos ir toliau tvarkydamas asmens duomenis, reikalingus šios pirkimo sutarties vykdymui, tiekėjas yra savarankiškas duomenų valdytojas perkančiosios organizacijos, kaip teikiamų asmens duomenų valdytojo, atžvilgiu.

49. Pirkimo sutarties šalis, kurį veikia kaip duomenų valdytojas pati yra atsakinga už teisėtą asmens duomenų tvarkymą, vadovaujantis visais asmens duomenų tvarkymą reglamentuojančiais teisės aktais, įskaitant, bet neapsiribojant, BDAR.

50. Kiekviena šalis, būdama savarankišku duomenų valdytoju, vykdydama šią pirkimo sutartį užtikrina, kad:

50.1. visą asmens duomenų tvarkymo laiką užtikrins tinkamas organizacines ir technines priemones, skirtas apsaugoti tvarkomus asmens duomenis nuo netyčinio ar neteisėto sunaikinimo, sugadinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų;

50.2. pirkimo sutarties šalis, tiek, kiek taikoma jos atliekamam asmens duomenų tvarkymui pagal sutartį, užtikrins duomenų subjektų teisių, numatytų BDAR įgyvendinimą;

50.3. ketinant perduoti asmens duomenis į trečiąją valstybę, esančią už Europos ekonominės erdvės (EEE) ribų, užtikrins BDAR V skyriuje numatytų reikalavimų laikymąsi;

50.4. pirkimo sutarties šalių darbuotojai, tvarkantys asmens duomenis, supažindinti su pareiga saugoti asmens duomenų paslaptį;

50.5. asmens duomenis laikys paslaptyje ir pasibaigus šios pirkimo sutarties galiojimui;

50.6. neatskleis ir nesuteiks kitokios galimybės trečiosioms šalims susipažinti su asmens duomenimis, jeigu kitaip nenustato ši pirkimo sutartis arba Lietuvos Respublikos įstatymai ir kiti teisės aktai;

50.7. pirkimo sutarties šalys atsako už asmens duomenų konfidencialumą ir saugumą nuo asmens duomenų gavimo momento;

50.8. pirkimo sutarties vykdymo metu gautus asmens duomenis tiekėjas ir perkančioji organizacija įsipareigoja naudoti tik šiai pirkimo sutarčiai įvykdyti;

50.9. įvykus asmens duomenų pažeidimui arba iškilus realiai grėsmei asmens duomenų saugumui sutarties šalys įsipareigoja ne vėliau kaip per 2 dienas apie įvykusį asmens duomenų pažeidimą arba iškilusią realią grėsmę asmens duomenų saugumui pranešti už asmens duomenų tvarkymą ir apsaugą atsakingiems asmenims:

	Perkančiosios organizacijos už asmens duomenų tvarkymą ir apsaugą atsakingas asmuo	**Tiekėjo už asmens duomenų tvarkymą ir apsaugą atsakingas asmuo**
Vardas, pavardė		
Adresas		
Telefonas		
Faksas		
El. paštas		

GINČŲ SPRENDIMO TVARKA

51. Pirkimo sutarčiai taikoma Lietuvos Respublikos teisė.

52. Pirkimo sutarties šalys visus ginčus stengiasi išspręsti derybomis. Visi ginčai, kylantys dėl pirkimo sutarties ar su ja susiję, nepavykus jų išspręsti derybų būdu, sprendžiami teisme Lietuvos Respublikos civilinio proceso kodekso nustatyta tvarka.

ŠALIŲ PAREIŠKIMAI IR GARANTIJOS

53. Kiekviena šalis pareiškia ir garantuoja kitai šaliai, kad:

53.1. Šalis yra teisėtai įsteigta ir veikia pagal Lietuvos Respublikos įstatymus.

53.2. Šalis atliko visus teisinius veiksmus, būtinus pirkimo sutarties tinkamam sudarymui, jos galiojimui ir turi visus teisės aktais numatytus leidimus, licencijas, resursus, reikalingus pirkimo sutarties įvykdymui.

53.3. Sudarydama pirkimo sutartį, šalis nepažeis ją saistančių įstatymų, taisyklių, nuostatų, potvarkių, įsipareigojimų ar susitarimų.

53.4. Ši pirkimo sutartis yra galiojantis teisinis ir ją saistantis įsipareigojimas, kurio vykdymo galima pareikalauti pagal pirkimo sutarties sąlygas.

53.5. Šalys pareiškia, kad jos visiškai supranta informacijos, suteikiamos vienos šalies kitai, reikšmę ir svarbą, susijusią su tokios informacijos praradimu, platinimu be leidimo ar kitokiu atskleidimu

ir galimas pasekmes perkančiosios organizacijos (su ja susijusių asmenų) ir jų klientų verslui, reputacijai, vardui, santykiams su klientu.

SUSIRAŠINĖJIMAS

54. Perkančiosios organizacijos ir tiekėjo vienas kitam siunčiami pranešimai turi būti rašomi lietuvių kalba ir siunčiami šiais adresais:

	Perkančioji organizacija	**Tiekėjas**
Vardas, pavardė		
Adresas		
Telefonas		
Faksas		
El. Paštas		

BAIGIAMOSIOS NUOSTATOS

55. Visi pirkimo sutarties pakeitimai ir papildymai įsigalioja tik abiem šalims juos patvirtinus parašais.

56. Ši sutartis sudaryta 1 egzemplioriumi, kadangi pasirašoma elektroniniu parašu.

SUTARTĮ SUDARANTYS DOKUMENTAI, SUTARTIES PRIEDAI IR JŲ PIRMUMAS

57. Šią pirkimo sutartį sudaro šie dokumentai, kurie čia yra išvardinti pagal svarbą:

57.1. 1 priedas „Techninė specifikacija“;

57.2. Pirkimo dokumentai „IT infrastruktūros saugumo sprendimas“;

57.3. Viešąjį pirkimą „IT infrastruktūros saugumo sprendimas“ laimėjusio tiekėjo pasiūlymas (siūloma techninė specifikacija ir kt.);

57.4. Sutartis.

58. Sutartį sudarantys dokumentai laikomi vienas kitą paaiškinančiais. Neaiškumo ar prieštaravimo atveju, vadovaujamasi šios sutarties 57 punkte nurodyta eilės tvarka.

ŠALIŲ JURIDINIAI REKVIZITAI

Perkančioji organizacija
Viešoji įstaiga „Plačiajuostis internetas“
Adresas: Sausio 13-osios g. 10, LT-04347, Vilnius
Įmonės kodas 300149794
PVM mokėtojo kodas LT 100003752713
A/s Nr. LT68 7044 0600 0523 9493
Bankas: AB SEB bankas
Tel. (8 5) 243 0884; faks. (8 5) 260 4404
El. paštas info@placiajuostis.lt

Direktorius
Gytis Liaugminas
_____

Tiekėjas
Blue Bridge MSP, UAB
Adresas: J. Jasinskio g. 16A, LT-03163 Vilnius
Įmonės kodas 301489547
PVM mokėtojo kodas LT100003708514
A/s Nr. LT89 2140 0300 0280 5128
Bankas: Luminor Bank AS
Tel. (8 5) 252 6060
El. paštas: info@bluebridge.lt

Direktorius
Dalius Butkus
_____

Viešojo pirkimo „IT infrastruktūros saugumo sprendimas“ 2021 m. lapkričio 19 d. pirkimo sutarties Nr. S4-1
Priedas Nr. 1

TECHNINĖ SPECIFIKACIJA

I. BENDROJI DALIS

1. I.1. Įvadas

VšĮ „Plačiajuostis internetas“ (toliau – Perkančioji organizacija arba Užsakovas), siekdama užtikrinti tinkamą informacijos apsaugą plačiajuosčio ryšio tinklo Lietuvoje valdymo IT infrastruktūroje, vykdo IT infrastruktūros saugumo sprendimo pirkimą . Šio pirkimo tikslas – modifikuoti esamą plačiajuosčio ryšio tinklo Lietuvoje valdymo IT infrastruktūrą bei įdiegti papildomas informacijos apsaugos priemones, kad būtų užtikrinta tinkama informacijos apsauga IT infrastruktūroje ir būtų užtikrinta IT infrastruktūros atitiktis pagal 2018 m. rugpjūčio 13 d. Lietuvos Respublikos Vyriausybės nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ priedo „Techninių kibernetinio saugumo reikalavimų, taikomų subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, sąrašą“.

Apsaugos sprendimai diegiami su tikslu apsaugoti Perkančiosios organizacijos IT infrastruktūrą ir joje saugomus duomenis nuo kibernetinių grėsmių, tokių kaip: interneto paslaugų sutrikdymas, internetinio incidento poveikis kritinei infrastruktūrai, perimetro pažeidimas, socialinės inžinerijos grėsmės, kenkimo programinei įrangai (toliau – PĮ) grėsmės, techninės ar programinės įrangos patikimumo grėsmės, interneto svetainių grėsmės, elektroninių ryšių tinklų žvalgybos grėsmės, konfigūravimo klaidos, logikos ir produktų architektūros klaidos, tinklo atakos, tiesioginis informacijos nutekėjimas, žmogiškosios rizikos, netiesioginis informacijos nutekėjimas, klientams teikiamų paslaugų sutrikdymas. Sprendimai turi būti diegiami taip, kad siūlomos priemonės nuo grėsmių maksimaliai apsaugotų tinklą ir jose dirbančias informacines sistemas bei įrenginius.

2. I.2. Esama situacija

Esama modifikuojama IT infrastruktūra apima:

- HPE Simplivity Hyper-Converged tipo serverių infrastruktūrą, išdėstytą per du duomenų centrus;
- serverių infrastruktūroje įdiegtą virtualizavimo platformą;
- virtualizavimo platformoje įdiegtą veiklos ir infrastruktūros valdymo programinę įrangą;
- duomenų perdavimo tinklo įrangą;
- informacijos apsaugos įrangą;
- administratorių ir darbuotojų kompiuterines darbo stotis.

IT infrastruktūroje veikia tokios sistemos ir tarnybos:

- centralizuota naudotojų ir prieigos valdymo sistema (Microsoft Active Directory pagrindu);
- Microsoft Exchange elektroninio pašto serveris;
- duomenų bazių valdymo sistemos, aptarnaujančios veiklos ir infrastruktūros valdymo sistemas (Microsoft SQL, Oracle);
- veiklos valdymo informacinės sistemos (CRM, buhalterinės apskaitos ir personalo valdymo, interneto tinklapis ir kitos);
- infrastruktūros stebėjimo ir valdymo sistemos (patalpų stebėjimo, tinklo valdymo, įrangos inventoriaus valdymo ir kitos);
- pagalbinės tarnybos – CA, DHCP, RADIUS, Log Server, Antivirus ir kitos.

Informacinės sistemos yra skirstomos į dvi pagrindines kategorijas:

- biuro veiklos palaikymo sistemos, skirtos biuro darbuotojams;
- tinklo palaikymo, saugos ir valdymo sistemos, skirtos aptarnaujamam tinklui ir jo įrenginiams valdyti.

3. I.3. Bendrieji reikalavimai perkamai įrangai

1. Pateikiama įranga turės būti įdiegta pagal techninėje specifikacijoje nurodytus reikalavimus (jeigu reikalavimai įdiegimui nepateikti – tos dalies įrangą būtina tik pateikti). Nurodytų įdiegimo darbų kaina turi būti įskaityta į pasiūlymo kainą.
2. Tiekėjas su pasiūlymu pirkimui privalo pateikti detalų siūlomos techninės ir programinės įrangos sąrašą. Sąraše nurodyti visos siūlomos techninės ir programinės įrangos sudėtinių dalių:
   2.1. pavadinimus;
   2.2. kiekius;
   2.3. gamintojus;
   2.4. modelius;
   2.5. gamintojo suteiktus kodus;
   2.6. jeigu yra – sudėtinius įrangos komponentus (pavadinimus, kodus, kiekius);
   2.7. jeigu siūloma įranga licencijuojama, būtina pateikti licencijų pavadinimus bei kodus ir trumpą funkcionalumo aprašymą, kurį kiekviena licencija suteikia;
   2.8. nuorodą į gamintojo tinklapį arba dokumentą, kuriame yra pateikiamos siūlomos įrangos aprašymas.
3. Visa pateikiama įranga, licencijos, techninio palaikymo kontraktai turi būti Perkančiosios organizacijos vardu užregistruoti gamintojų palaikymo sistemose, jeigu tokios yra.
4. Visi techninėje specifikacijoje aprašomi komponentai turi būti suderinami tarpusavyje su kitais toje dalyje aprašytais komponentais bei po diegimo sudaryti integruotą pilnai paruoštą naudojimui sprendimą.
5. Visa siūloma įranga ir jos komponentai turi būti nauji, negalima siūlyti naudotos arba naudotos ir atnaujintos (angl. *remarketing/refurbished*) įrangos.
6. Visos siūlomos įrangos elektros maitinimo šaltinių elektros maitinimo įtampa turi atitikti Lietuvos Respublikoje naudojamai kintamai įtampai. Kartu su įranga turi būti pateikti visi jai prijungti prie Užsakovo įrengto elektros maitinimo tinklo reikalingi elektros maitinimo kabeliai.
7. Visi darbai ar medžiagos, kurie gali būti pagrįstai laikomi būtinais darbų užbaigimui ir tinkamam eksploatavimui, turi būti privalomai atlikti ir (ar) įrengiami nepriklausomai nuo to, ar jie yra apibūdinti šioje techninėje specifikacijoje, ar ne (kabeliai, jungtys, montavimo medžiagos ir pan.).
8. Visos prekės ir paslaugos turi tenkinti atitinkamus Lietuvos Respublikoje ir Europos Sąjungoje galiojančius teisės aktus.
9. Įrangos diegimą, konfigūravimą atliekantys specialistai privalo mokėti lietuvių kalbą arba turi būti be papildomo mokesčio užtikrintos kokybiškos vertimo paslaugos.
10. Tiekėjas visiškai atsako už Lietuvos Respublikos darbuotojų saugos ir sveikatos įstatymo bei Lietuvos Respublikos įstatymų, reglamentuojančių darbų saugą, reikalavimų vykdymą.
11. Tiekėjas privalės sumontuoti diegiamą fizinę įrangą remiantis aprašytais fiziniais parametrais ir gamintojų reikalavimais. Visi sumontuoti komponentai turi būti markiruoti unikaliais žymenimis, suderintais su Užsakovu. Žymuo turi būti gerai matomas. Kabeliai markiruojami abiejuose galuose. Markiravimo duomenys pateikiami Microsoft Excel formatu (ne žemesne nei 2000 versija) prieš įrangos priėmimo-perdavimo akto pasirašymą. Montavimo darbai turi būti atliekami vadovaujantis darbų saugos technikos taisyklėmis, EĮJT normomis, priešgaisrinės saugos reikalavimais ir kitais šiuos darbus reglamentuojančiais teisės aktais.
12. Visus integracinius darbus, kuriuose bus galimas IT infrastruktūros paslaugų veikimo nutrūkimas ar naujų paslaugų sukūrimas, Tiekėjas turi suderinti su Užsakovu prieš protingą laiką iš anksto.
13. Visi IT infrastruktūros įrangos konfigūravimo darbai turi būti suderinami ir atliekami pagal Užsakovui pateiktą dokumentaciją (būsimos konfigūracijos fizinės ir loginės schemos ir kt.),

14. Jei šioje techninėje specifikacijoje numatytai įrangai yra keliamas reikalavimas atitikti standartus, Tiekėjas turi teisę pasiūlyti įrangą, atitinkančią standartus, kurie yra lygiaverčiai techninėje specifikacijoje nurodytiems standartams.
15. Jei Tiekėjui bus poreikis įdiegti siūlomą valdymo programinę įrangą diegiamos įrangos valdymui, Perkančioji organizacija suteiks reikiamą kiekį virtualių serverių VMware aplinkoje su Windows ar Linux operacinėmis sistemomis. Taip pat Perkančioji organizacija galės suteikti vietos SQL duomenų bazės instaliavimui turimame Micrsosoft SQL serveryje. Siūlomam sprendimui reikalingų kitų operacinių sistemų ir kitos programinės įrangos licencijas turės pateikti Tiekėjas.
16. Reikalavimai įrangos garantijai:
    16.1. siūlomai įrangai turi būti suteikta ne mažiau kaip 60 mėnesių gamintojo ar gamintojo autorizuoto serviso centro garantija, įskaitant visą techninę ir programinę įrangą;
    16.2. garantinės priežiūros laikotarpiu gamintojas ar gamintojo autorizuotas serviso centras turi garantuoti nemokamą aparatinės įrangos reikalingų dalių tiekimą ir nemokamus remonto darbus;
    16.3. garantinės priežiūros laikotarpiu gamintojas ar gamintojo autorizuotas serviso centras turi suteikti programinės įrangos atnaujinimus, naujas versijas, klaidų šalinimus bei pagalbą sprendžiant siūlomų sprendimų programinės įrangos sutrikimus;
    16.4. garantinės priežiūros laikotarpiu techninė pagalba ir konsultacijos turi būti teikiamos lietuvių arba anglų kalbomis;
    16.5. įranga ir licencijos turi būti pas gamintoją registruotos perkančiosios organizacijos vardu;
    16.6. terminai:
        16.6.1. techninei įrangai (angl. Hardware) palaikymas 8 x 5 režimu (8 val. per parą, 5 dienos per savaitę);
        16.6.2. programinei įrangai (angl. Software) palaikymas 8 x 5 režimu (8 val. per parą, 5 dienos per savaitę);
        16.6.3. kreipinių valdymas, pagalba ir konsultacijos (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) kreipiantis telefonu, el. paštu ar internetiniame portale, prieiga prie techninių resursų (angl. Knowledge Base) palaikymas 8 x 5 režimu (8 val. per parą, 5 dienos per savaitę);
        16.6.4. gedimo atveju įranga turi būti suremontuota arba pateikta nauja įranga ne vėliau, kaip per 10 darbo dienų nuo pranešimo apie gedimą pateikimo;
    16.7. garantinis laikotarpis pradedamas skaičiuoti nuo atitinkamo priėmimo-perdavimo akto pasirašymo dienos;
    16.8. Tiekėjo garantinis aptarnavimas atliekamas įrangos buvimo vietoje;
    16.9. garantinio laikotarpio metu Tiekėjas privalo be papildomo mokesčio pašalinti tinkamai eksploatuotos įrangos gedimus;
    16.10. garantiniu laikotarpiu turi galioti teisė Užsakovui nemokamai gauti techninės įrangos vidinės programinės įrangos (angl. *firmware*) atnaujinimus ir naujas versijas;
17. Įdiegęs atitinkamos pirkimo dalies įrangą Tiekėjas privalės pateikti išpildomąją dokumentaciją, kurioje turės būti:
    17.1. įdiegtos fizinės įrangos (jei yra) sujungimo schema;
    17.2. įdiegtos įrangos loginė sujungimo schema;
    17.3. įdiegto sprendimo aprašymas;
    17.4. kita pagal pirkimo dalies įrangos pobūdį reikalinga informacija, būtina įdiegtam sprendimui eksploatuoti.
18. Visa dokumentacija turi būti pateikta elektroniniu formatu:
    18.1. visi dokumentacijos brėžiniai ir schemos turi būti atlikti ir pateikti Microsoft Visio programinėje aplinkoje;
    18.2. visos dokumentacijoje pateikiamos lentelės turi būti pateiktos Microsoft Word ar Microsoft Excel programinėje aplinkoje;

18.3. pateikiamose schemose naudojami primityvai turi būti iš anksto suderinti su Perkančiąja organizacija.

19. Dalis informacijos apie Perkančiosios organizacijos turimą IT infrastruktūrą negali būti viešai atskleista dėl galimų kibernetinių grėsmių. Dėl to detalesnė informacija apie IT infrastruktūrą galės būti pateikta dalyviui CVP IS priemonėmis pateikus prašymą pateikti nurodytą informaciją, bei pateikus pasirašytą pasižadėjimą gautos informacijos neplatinti ir nenaudoti kitais tikslais, išskyrus pasiūlymo parengimą šiam pirkimui.

II. SPECIALIOJI DALIS

4. PERKAMOS ĮRANGOS IR JOS ĮDIEGIMO DARBŲ REIKALAUJAMOS TECHNINĖS SAVYBĖS

IT infrastruktūros saugumo sprendimas, apimantis esamos infrastruktūros parengimą diegimui ir kibernetinio saugumo sprendimo įdiegimą, bei mokymus darbuotojams:

1. Esamos infrastruktūros parengimas saugumo sprendimo diegimui:
   1.1. turi būti atlikti centralizuotos naudotojų ir prieigos valdymo sistemos (CNPVS), tapatybės valdymo sistemos (TVS), DNS tarnybos, Windows naujinimų tarnybos (WSUS) ir susijusių tarnybų analizės, projektavimo, diegimo ir konfigūravimo darbai;
   1.2. turi būti atlikti esamų sistemų veikimo modifikuotoje IT infrastruktūroje analizės, projektavimo ir konfigūravimo darbai;
   1.3. turi būti įdiegtas laiko serverio komponentas, būtinas informacijos apsaugos sprendimams funkcionuoti.
2. Pagal aprašymą žemiau įdiegtas IT infrastruktūros saugumo sprendimas, apimantis kompiuterių apsaugą nuo kibernetinių grėsmių, pažangių grėsmių aptikimą, el. pašto apsaugą, privilegijuotos prieigos bei saugumo įvykių ir žurnalinių įrašų valdymą.
3. Turi būti pravesti mokymai ne mažiau kaip keturiems Perkančiosios organizacijos darbuotojams. Mokymų tema – supažindinimas su įdiegtu sprendimu, įdiegto sprendimo administravimas, konfigūravimas bei priežiūra. Patalpas mokymams suteiks Perkančioji organizacija. Mokymų trukmė ne mažiau kaip 8 valandos.
4. Specializuoti siūlomos žurnalinių įvykių ir įrašų valdymo komponento įrangos gamintojo mokymai (gali būti gyvai instruktoriaus vedami arba nuotoliniai mokymai) dviems Perkančiosios organizacijos darbuotojams, kurie suteiktų žinias, kaip naudoti ir administruoti žurnalinių įvykių ir įrašų valdymo įrangą. Mokymų trukmė ne mažiau kaip 20 valandų.

Tiekėjas, būdamas pagrindinio IT infrastruktūros sprendimo tiekėjas, taip pat bus atsakingas už pirkimo Kibernetinio saugumo įrangos viešojo pirkimo (pirkimo numeris 497401, skelbtas 2020-07-26 CVP IS) I-II bei IV-VII dalyse nurodytos įrangos ir sprendimų įdiegimo rezultato galutinį integravimą į Perkančiosios organizacijos IT infrastruktūrą ir bendro viso pirkimo tikslo pasiekimą - IT infrastruktūros atitikties pagal Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ priedo „Techninių kibernetinio saugumo reikalavimų, taikomų subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, sąrašą“ užtikrinimą.

Šiuo tikslu Tiekėjas privalės suteikti bendro kibernetinės saugos rezultato užtikrinimo paslaugas:

1. Bendradarbiaudamas su Perkančiosios organizacijos atstovais koordinuoti visų sprendimų integravimą, siekiant užtikrini Perkančiosios organizacijos bendro kibernetinės saugos ir atitikties užtikrinimo tikslų įgyvendinimą.
2. Integruoti įrangos žurnalinių įvykių ir įrašų gavimą ir apdorojimą Tiekėjo įdiegtoje žurnalinių įvykių ir įrašų valdymo įrangoje.
3. Integruoti įrangą su laiko serverio komponentais, kiek tai yra reikalinga tinkamam visų saugumo sprendimų funkcionavimui.
4. Integruoti įrangą ar sistemas su CNPVS, TVS, DNS, WSUS sistemomis kiek tai yra reikalinga tinkamam visų saugumo sprendimų funkcionavimui.
5. Išnaudojant kompiuterių apsaugos nuo kibernetinių grėsmių komponento galimybę priimti sisteminius įrašus (angl. *logs*) iš tinklo ugniasienių, užtikrinti integraciją su Perkančiosios organizacijos įdiegtomis Check Point ir FortiGate ugniasienėmis, tokiu būdu papildant komponento analitiką tinklo srauto duomenimis.
6. Parengti dokumentaciją, kurioje būtų nurodytas šiuo pirkimu modifikuotos Perkančiosios organizacijos IT infrastruktūros atitiktis pagal Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo

įgyvendinimo“ priedo „Techninių kibernetinio saugumo reikalavimų, taikomų subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, sąrašą“.

7. Atlikti IT infrastruktūros saugumo patikrinimą po IT infrastruktūros saugumo sprendimų įdiegimo.
8. Nustatyti taikytinus išorinius reikalavimus:
   8.1. taikytinų reikalavimų informacinių sistemų saugai nustatymas;
   8.2. taikytinų reikalavimų asmens duomenų apsaugai nustatymas;
   8.3. taikytinų reikalavimų informacinėms sistemoms nustatymas;
   8.4. bendrų taikytinų reikalavimų bendro sąrašo sudarymas ir suderinimas.
9. Atlikti rizikos vertinimą:
   9.1. numatytų diegti saugos sprendimų informacijos saugos rizikos vertinimas remiantis ISO/IEC 27005 standarto reikalavimais;
   9.2. numatytų diegti sprendimų poveikio asmens duomenų saugai vertinimas remiantis ISO/IEC 29134 standarto reikalavimais.
10. Atlikti diegiamų sprendimų įvertinimą pagal tai, kaip jie užtikrina reikalavimus informacijos ir duomenų saugumui:
    10.1. diegiamų sprendimų architektūros įvertinimas informacijos ir duomenų apsaugos požiūriu;
    10.2. diegiamų sprendimų atitikties taikomiems reikalavimams įvertinimas ir rekomendacijų teikimas.
11. Užtikrinti ir įvertinti diegiamų informacijos saugos užtikrinimo priemonių reikiamą saugumo lygį, įvertinti rizikas, užtikrinti atitiktį išoriniams reikalavimas, teisėtiems užsakovo lūkesčiams ir reikalavimams, konsultuoti informacijos saugumo klausimais projekto eigoje.

3 lentelė. Reikalavimai perkamam sprendimui.

Nr.	Parametras	Reikalaujama reikšmė
1.	Infrastruktūros parengimo saugumo sprendimo diegimui įranga	Užsakovo IT infrastruktūrai parengti saugumo sprendimo diegimui turi būti pateiktas laiko serverio komponentas.
1.1.	Laiko serverio komponentas	
1.1.1.	Laiko serverių įranga	Turi būti pateikti ir įdiegti ne mažiau kaip 2 vnt. laiko serveriai
1.1.2.	El. maitinimo šaltiniai	Turi būti ne mažiau 2 vnt. dubliuojantys karšto keitimo (angl. *hot swap*) maitinimo šaltiniai įmontuoti į siūlomą laiko serverį.
1.1.3.	Prievadai	Turi būti ne mažiau kaip: – 2 vnt. 1G SFP prievadai; – 2 vnt. 100/1000 BaseT prievadai.
1.1.4.	GNSS palydovinių navigacijos sistemų palaikymas	– Turi būti palaikomi: o GPS; o GALILEO. – Taip pat turi būti palaikomos naudojamų palydovinių navigacijos sistemų kombinacijos: o GPS + GALILEO.
1.1.5.	Laiko paslaugos funkcijos	Turi būti palaikomi tokie funkcionalumai: – PTP ir NTP palaikymas ant to pačio Ethernet prievado; – Ne mažiau kaip 2000 NTP transakcijų per sekundę. – PTP profiliai su IPv4 ir IPv6 (angl. *unicast*) adresacijos palaikymu; – PTP profiliai su IPv4 ir IPv6 (angl. *multicast*) adresacijos palaikymu.

1.1.6.	Tinklo ir laiko funkcijos	Turi būti palaikomi šie arba lygiaverčiai ir pilnai suderinami tinklo protokolai: – IEEE 1588v2 PTP arba IEEE 1588-2008; – DHCP; – DSCP; – NTPv; – ITU-T G.8261;ITU-T G.703ITU-T G.812; – ITU-T G.8272; – ITU-G.811.
1.1.7.	Saugumo funkcijos	Turi būti palaikomi šie arba lygiaverčiai ir pilnai suderinami saugumo protokolai: – SFTP; – RADIUS.
1.1.8.	Valdymo funkcijos	Turi būti palaikomi šie arba lygiaverčiai ir pilnai suderinami protokolai: – SNMPv2c/SNMPv3; – SSH.
1.1.9.	Stebėjimo funkcijos	Turi būti palaikomi šie arba lygiaverčiai ir pilnai suderinami saugumo protokolai: – SYSLOG.
1.1.10.	Atitiktis reikalavimams	Turi atitikti šiems arba lygiaverčiams reikalavimams: – CE compliance; – RoHS compliance; – EN 55022.
1.1.11.	Antenos	Komplekte turi būti: – GNSS (GPS+ GALILEO) 40dB antena, su visomis montavimui reikalingomis detalėmis; – ne trumpesnis kaip 50 m ilgio antenos kabelis LMR/CNT400 (zero-halogen) su 2xTNC-m jungtimis; – tarpinė kampinė jungtis su ne trumpesniu kaip 2 m ilgio kabeliu, TNC-f / SMA-m jungtimis; – apsauga nuo žaibo išlydžių, su ne trumpesniu kaip 10 m ilgio LMR/CNT400 kabeliu.
2.	Kompiuterių apsaugos nuo kibernetinių grėsmių komponentas	
2.1.	Tipas ir apimtis	Pažangi galutinių įrenginių apsaugos ir reagavimo į incidentus programinė įranga su centralizuotu valdymu, skirta apsaugoti ne mažiau kaip 100 vnt. galinių įrenginių.
2.2.	Programinė įranga	Specializuotas galinių įrenginių (darbo vietų, serverių) apsaugos sprendimas nuo žinomų grėsmių ir nulinės dienos pažeidžiamumų išnaudojimo kodų (angl. *0-day exploits*) bei nežinomų kenksmingų programinių kodų (angl. *unknown malware*). Sprendimas turi būti sudarytas iš agentų (klientinės dalies), tarpinių serverių ir valdomas centralizuotai iš gamintojo debesijos platformos.
2.3.	Centralizuotas valdymas	– Turi rodyti agentų būseną ir licencijų išnaudojimo statistiką. – Turi rodyti saugumo incidentų pranešimus. – Turi leisti centralizuotai apibrėžti saugumo politikas.

		– Turi būti centralizuotas agentų atnaujinimo funkcionalumas. – Centralizuotas daugiau nei vieno agento iš Windows, Mac ar Linux OS naudojančių įrenginių ištrynimas. – Turi būti funkcionalumas integruoti su saugumo orkestravimo, automatizavimo ir atsako sprendimais (angl. *security orchestration, automation and response, SOAR*).
2.4.	Agentai	– Turi palaikyti „daug į vieną“ (angl. *non-persistent*) virtualias darbo vietas (angl. *VDI*) – Apsaugos agento palaikomos operacinės sistemos: Android, MacOS, CentOS, Debian, Oracle, Red Hat Enterprise Linux, Ubuntu, Windows 8.1, 10, Windows Server 2008 R2, 2012 R2, 2016, 2019, VMware AppVolumes. – Windows ir Mac agentų pašalinimui įvykdyti turi reikalauti įvesti slaptažodį. – Turi būti galima išjungti agento pranešimų rodymą galutiniam naudotojui. – Esant uždaram tinklo segmentui, agentai turi su gamintojo valdymo platforma bendrauti per tarpinį serverį (angl. *proxy* arba *broker*). – Turi būti funkcionalumas agento konfigūracijoje nurodyti ne mažiau kaip 4 proxy serverius.
2.5.	Galinių įrenginių valdymas	– Turi būti funkcionalumas blokuoti per USB prijungiamus įrenginius (diskų grotuvai, USB atmintinės, išoriniai kietieji diskai). – Turi būti funkcionalumas kontroliuoti įeinančius ir išeinančius ryšius iš įrenginio, kuriame įdiegtas agentas, pagal: kryptį, IP adresus, jų rėžius, protokolus, servisus, jų rėžius. – Turi būti funkcionalumas taikyti skirtingas įeinančių-išeinančių ryšių politikas pagal agento buvimo vietą: įmonės tinkle ar už jo ribų. – Turi būti funkcionalumas atlikti kietojo disko šifravimą.
2.6.	Tarpinis serveris	– Turi būti funkcionalumas atsisiųsti tarpinio serverio (angl. *proxy* arba *broker*) instaliacinį failą iš gamintojo valdymo platformos. – Tarpinio serverio programinė įranga turi palaikyti VMware ESXi 6 ir vėlesnes arba Hyper-V 2012 ir vėlesnes versijas.
2.7.	Rolės ir vartotojai	– Valdymas turi būti realizuotas rolėmis paremta prieiga RBAC modelis (angl. *role based access control*). – Turi būti gamintojo priskirtos rolės. – Turi būti funkcionalumas sukurti savo roles ir priskirti joms teises. – Administratorių autentifikavimas turi būti vykdomas Microsoft Active Directory arba lokalių sistemos vartotojų pagalba. – Turi būti funkcionalumas taikyti dviejų faktorių autentifikaciją administratorių prisijungimui.
2.8.	Integracija su katalogo tarnyba	Turi būti gamintojo realizuota programinės įrangos dalies integracija su Microsoft Active Directory.
2.9.	Analizės objektai	– Vykdomosios programos PE. – Dinaminės bibliotekos DLLs.

		– Vykdomosios programos Mach-O. – Vykdomosios programos ELF. – Vykdomosios programos APK. – Microsoft Office Macros vykdomieji skriptai.
2.10.	Reagavimo į grėsmes veiksmai	– Turi būti funkcionalumas nuotoliniu būdu prisijungti prie agento. – Turi būti funkcionalumas paleisti CMD arba PowerShell arba Python scenarijus. – Turi būti funkcionalumas izoliuoti agentą nuo tinklo. – Turi būti funkcionalumas sustabdyti, išjungti procesus nuotoliniu būdu.
2.11.	Incidentų bylų valdymo veiksmai	– Automatinis kelių pranešimų (angl. *alerts*) koreliavimas į vieną incidentą. – Turi būti funkcionalumas priskirti incidentus komandos nariams. – Turi būti funkcionalumas prie incidento pridėti komentarus. – Turi būti funkcionalumas valdyti incidentų gyvenimo ciklą/priskirti būsenas. – Turi būti funkcionalumas sujungti incidentus. – Turi būti funkcionalumas ištraukti incidento artefaktus (IP adresus, maišos algoritmų reikšmes, bylų pavadinimus).
2.12.	Incidentų tyrimo veiksmai	– Turi būti funkcionalumas automatiškai nustatyti pagrindinę kiekvieno pranešimo (angl. *alert*) priežastį. – Turi būti funkcionalumas matyti grandinę atliktų veiksmų, kurie iššaukė pranešimą (angl. *alert*). – Turi būti funkcionalumas matyti veiksmus ir pranešimus (angl. *alert*) laiko juostoje. – Turi būti funkcionalumas nustatyti kokiu būdu kenkėjiška veikla buvo sustabdyta. – Turi būti funkcionalumas automatiškai koreliuoti saugumo pranešimus (angl. *alert*) gautus iš skirtingų šaltinių.
2.13.	Apsauga nuo kenksmingų programų (angl. *malware*)	– Turi vykdyti bylų maišos algoritmų (angl. *hash*) reikšmių palyginimą su žinomomis kenksmingų/nekenksmingų programų duomenų bazėmis ir priimti nuosprendį dėl kenksmingumo. – Turi vykdyti lokalią juodųjų ir baltųjų sąrašų politiką pagal administratoriaus sudarytus maišos algoritmų reikšmių sąrašus (angl. *manual hash control*). – Programinė įranga pasirašyta patikimų tiekėjų skaitmeniniu sertifikatu neturi būti traktuojama kaip kenksminga ar verta analizės. – Turi būti pateikiamas patikimų programinės įrangos tiekėjų sąrašas (angl. *trusted signers*). – Turi būti vykdoma bylų analizės paslauga, siunčiant nežinomas vykdomąsias bylas dinaminei analizei į gamintojo smėliadėžę (angl. *sandbox*).
2.14.	Kenksmingo programinio kodo elgsenos apribojimai	– Turi aptikti ir blokuoti programų vykdymą, kurios demonstruoja kenksmingą elgseną (angl. *malicious behavior*).

		– Turi aptikti kenksmingą elgseną, kai vykdomas injektavimasis į pagrindinį procesą (angl. *child process injection*) apsaugos išvengimo tikslais.
2.15.	Kenksmingo programinio kodo vykdymo apribojimai	– Turi aptikti ir blokuoti programų vykdymą, kurios atitinka apribojimų politiką; – Turi vykdyti bent šiuos vykdymo apribojimus: o vykdomųjų bylų paleidimas iš lokalių katalogų; o vykdomųjų bylų paleidimas iš tinklo katalogų; o vykdomųjų bylų paleidimas iš išorinių įrenginių (optinių diskų, išorinių ištraukiamųjų diskų).
2.16.	Mašininis apsimokymas (angl. *machine learning*)	– Turi vykdyti lokalią nežinomų vykdomųjų bylų statinę analizę remiantis vien matematiniais, statistiniais palyginimo modeliais. – Analizės rezultatas turi būti lokalus verdiktas - programa kenksminga ar ne, gali būti paleista ar ne.
2.17.	Saugumo politika	– Turi būti gamintojo apibrėžta saugumo politika, sukonfigūruota pagal gamintojo rekomenduojamas gerąsias saugumo praktikas (angl. *default security policy*). – Turi leisti kurti savo saugumo politikas (taisykles) ir jas modifikuoti.
2.18.	Centralizuotos užklausos	Turi būti funkcionalumas ieškoti specifinės informacijos tokios kaip: – bylos – pagal atliktą veiksmą, pavadinimą, buvusį pavadinimą, kelią (angl. *path*), buvusį kelią, maišos reikšmes (angl. *hash values*); – registrai – pagal atliktą veiksmą, registro rakto vardą, registro rakto buvusį vardą, registro rakto reikšmę; – IP adresai – pagal protokolą, lokalų IP, tikslo IP, lokalų prievadą, tikslo prievadą, tikslo šalį; – procesai – pagal proceso vardą, kelią (angl. *path*), maišos reikšmes (angl. *hash values*), vartotoją, kuris paleido procesą, proceso ID.
2.19.	Atnaujinimai	Gamintojo atnaujinimai turi apimti: – mašinų apsimokinimo (angl. *machine learning*) modelių atnaujinimą; – patikimų gamintojų sertifikatų parašų sąrašą (angl. *trusted signers*); – pakeitimus ir tobulinimus gamintojo rekomenduojamoje konfigūracijoje (saugumo politikoje).
2.20.	Atminties pažeidimo rinkinių (angl. *exploit-kits*) naudojamos identifikavimo technikos	Turi apsaugoti nuo atminties pažeidimo rinkinių (angl. *exploit-kits*) naudojamų skriptų ir technikų, identifikuojančių interneto naršyklių ir įskiepių versijas ir galimus susijusius pažeidžiamumus.
2.21.	Atminties pažeidimo technikų apsauga (angl. *anti-exploit*)	– Turi būti gamintojo iš anksto sukonfigūruotos apsaugos taisyklės. – Turi būti funkcionalumas kurti modifikuotas taisykles ir jose nurodyti konkrečius atminties pažeidimo apsaugos modulius. – Turi būti funkcionalumas daryti išimties taisykles.

		– MacOS operacinė sistema turi būti saugoma nuo šių atakų ir technikų: o apsauga nuo ROP (angl. *return oriented programming*) grandinėlių; o apsauga nuo privilegijų pasiaukštinimo; o dinaminių bibliotekų pakrovimo į procesą iš nesaugių lokacijų apsauga; o operacinės sistemos atminties pažeidimo apsaugų apėjimo prevencija, naudojant JIT (angl. *just-in-time*) kompiliavimo variklius. – Windows operacinė sistema (priklausomai nuo operacinės sistemos versijos) turi būti apsaugota nuo šių atakų ir technikų: o apsauga nuo ROP (angl. *return oriented programming*) grandinėlių; o apsauga nuo privilegijų pasiaukštinimo; o dinaminių bibliotekų DLL pakrovimo į procesą iš nesaugių lokacijų apsauga; o apsauga nuo prieigos prie DLL metaduomenų iš nesaugių kodo lokacijų; o apsauga nuo atakos technikos CPL – Windows Control Panel bibliotekos; o SEH apsauga – struktūrizuotų išimčių apdorojimo apsauga kompiliavimo metu neapsaugotoms programoms; o DEP apsauga – duomenų vykdymo apsauga kompiliavimo metu neapsaugotoms programoms; o nulinio atminties puslapio išnaudojimo exploit kodui kontroliuoti apsauga; o Hot Patch technikos apsauga; o priverstinis ASLR lokacijos atmintyje parinkimas atsitiktiniu būdu (pakrovimo metu) kompiliavimo metu neapsaugotoms programoms ir Windows moduliams, bibliotekoms; o operacinės sistemos atminties pažeidimo apsaugų apėjimo prevencija, naudojant JIT (angl. *just-in-time*) kompiliavimo variklius.
2.22.	Suderinamumas su klasikine antivirusine ir kita saugumo programine įranga	Turi būti atpažįstamas Microsoft Windows Security Center operacinės sistemos komponente, kaip pripažįstamas antiviruso produktas sistemoje.
2.23.	Įvykiai	– Turi centralizuotai saugoti įvykius ir įrašus iš agentų ne mažiau kaip 30 dienų. – Turi centralizuotai saugoti sistemos administravimo įrašus ne mažiau kaip 180 dienų. – Turi siųsti įvykius e-paštu. – Turi siųsti įvykius į išorines įrašų surinkimo sistemas.
3.	El. pašto apsaugos komponentas	

3.1.	Sprendimo architektūra ir sudedamosios dalys	Specializuotas identiškai atitinkantis programinis sprendimas/sistema, skirtas el. pašto apsaugai nuo nepageidaujamos korespondencijos, antivirusinei apsaugai, duomenų nutekėjimo prevencijai, laiškų kompromitavimo užkardymui, URL nuorodų patikrai, WEB naršyklės izoliavimui nuo tinklapio užtikrinti.
3.2.	El. pašto apsaugos platforma	
3.2.1.	Suderinamumas su virtualizacijos platformomis	Privalo būti suderinama su VMware ESXi 6.0/6.5 arba lygiavertėmis virtualizacijos platformomis.
3.2.2.	Procesorių branduolių skaičius (vCPU)	Ne mažiau 2
3.2.3.	Palaikomos virtualios tinklo sąsajos	Ne mažiau 3
3.2.4.	Palaikomas pastoviosios atminties (angl. *storage*) kiekis	Ne mažiau 350 GB
3.2.5.	Palaikomos vidinės atminties (RAM) kiekis	Ne mažiau 2 GB
3.2.6.	Darbo režimai	Ne mažiau kaip Gateway, Transparent, Server.
3.2.7.	Sprendimo našumas	– Taisyklių skaičius pagal gavėją įeinantiems arba išeinantiems laiškams per visą sistemą – ne mažiau 400. – Pašto dėžučių skaičius dirbant serverio režimu – ne mažiau 200. – Antiviruso, apsaugos nuo pageidaujamos korespondencijos, (angl. *antispam*) ir turinio (angl. *content*) profilių skaičius per visą sistemą – ne mažiau 100. – Laiškų skaičius per valandą (be eilės, siunčiant 100 KB dydžio laiškus) naudojant apsaugą nuo nepageidaujamos korespondencijos ir apsaugą nuo virusų (angl. *Antispam* + *Antivirus*) – ne mažiau 3000.
3.2.8.	Pagrindinės palaikomos funkcijos	– Įeinančių ir išeinančių laiškų inspektavimas. – IPv4 ir IPv6 adresacijos palaikymas. – SMTP autentifikacija per LDAP, RADIUS, POP3, IMAP. – Laiškų maršrutizacija LDAP pagrindu. – Vartotojų patikra LDAP atributų ir taisyklių (angl. *policy*) pagrindu. – Laiškų eilių valdymas. – Apsauga nuo nepageidaujamos korespondencijos globalios siuntėjų reputacijos duomenų bazės pagrindu. – Apsauga nuo nepageidaujamos korespondencijos brukalų kontrolinių sumų duomenų bazės pagrindu. – Apsauga nuo nepageidaujamos korespondencijos dinaminių euristinių taisyklių pagrindu. – Apsauga nuo nepageidaujamos korespondencijos URL kategorijų Spam, Malware, Phishing pagrindu.

		– Greylisting apsaugos nuo nepageidaujamos korespondencijos funkcionalumas. – Gili laiškų antraščių inspekcija (angl. *deep email header inspection*). – Integracija su trečių šalių SURBL, RBL duomenų bazėmis. – PDF skanavimas. – Patikimų ir nepatikimų siuntėjų sąrašai (angl. *block/allow list*) globaliu, domeno ir vartotojo lygmeniu. – Pačių vartotojų administruojami jiems skirti karantinuojami laiškai. – Antivirusinė, antimalware apsauga signatūrų pagrindu. – Antivirusinė, antimalware apsauga heuristinės analizės pagrindu. – Greyware detektavimas. – Aktyvaus turinio detektavimas PDF ir Office dokumentuose. – Archyvuotų bylų patikra. – Taisyklių valdomas (angl. *policy based*) laiškų archyvavimas su išorinės saugyklos galimybe. – Identity-based (angl. *IBE*) pašto šifravimo mechanizmas. – Laiškų kompromitavimo (angl. *BEC*) užkardymas. – Patikra gamintojo debesyje esančioje smėliadėžėje (angl. *sandbox*). – Paveiksliukų analizė. – Žymėtų bylų (angl. *fingerprinting*) praradimo prevencija. – O365 esančių el. laiškų patikra realiu laiku naudojant API metodą - nekeičiant el. laiškų srauto judėjimo schemos. – El. laiško sulaikymas O365 platformoje, kol atliekamas jo patikrinimas. – Aktyvaus turinio PDF ir Office dokumentuose, HTML turinio laiškuose neutralizavimas. – URL nuorodų perrašymas ir patikra nuorodos paspaudimo metu. – Integracija su WEB naršyklių izoliavimo platforma, kad būtų izoliuojama darbuotojo naršyklė nuo tinklapio, kai paspaudžiama nuoroda gauta el. paštu.
3.2.9.	Įvykių žurnalai, ataskaitos	– Įrašų apie konfigūracijos pokyčius, incidentus ir kitą veiklą išsaugojimas. – Ataskaitų generavimas. – Galimybė centralizuotai kaupti, apdoroti įvykių įrašus to paties gamintojo specializuotame įrenginyje arba kito gamintojo suderinamame bendram darbui įrenginyje, tačiau kartu su pasiūlymu turi būti pateikti visų siūlomų įrangos gamintojų raštiški patvirtinimai, kad siūloma įranga yra pilna apimtimi suderinama tarpusavyje bei siūlomoms įrangoms galios reikalaujama garantija, nebus taikomi garantijos apribojimai bei garantiniai įsipareigojimai bus vykdomi taikant „vieno langelio“ principą.
3.2.10.	Valdymo funkcijos	– Daugiapakopis administravimas per domeną. – Webmail grafinė sąsaja karantino valdymui.

		– SAML 2.0 SSO ir ADFS autorizacijos palaikymas WEB pašto ir karantino prieigai. – SNMP palaikymas. – SysLog palaikymas.
3.2.11.	Aukšto patikimumo funkcijos	– Esant poreikiui turi būti galima pajungti papildomą įrenginį, kad sistema veiktų aukšto patikimumo režimais: aktyvus-pasyvus ir aktyvus-aktyvus. – Karantino ir laiškų eilės sinchronizacijos galimybė aukšto patikimumo funkcijos režime. – Įrenginio gedimo detektavimo ir pranešimo galimybė aukšto patikimumo funkcijos režime.
3.2.12.	Atnaujinimai	Viso garantinio aptarnavimo laikotarpio metu gamintojas turi teikti sistemos duomenų bazių ir kitų komponentų, reikalingų aukščiau nurodytų funkcijų palaikymui, atnaujinimus.
3.3.	WEB naršyklių izoliavimo platforma	
3.3.1.	Suderinamumas su virtualizacijos platformomis	Privalo būti suderinama su VMWare 6.0/6.5 arba lygiavertėmis virtualizacijos platformomis.
3.3.2.	Procesorių branduolių maksimalus skaičius (vCPU)	Ne mažiau 2
3.3.3.	Palaikomos virtualios tinklo sąsajos	Ne mažiau 3
3.3.4.	Palaikomas pastoviosios atminties (angl. *storage*) kiekis	Ne mažiau kaip 50 GB
3.3.5.	Palaikomos vidinės atminties (RAM) kiekis	Ne mažiau kaip 8 GB
3.3.6.	Darbo režimai	Ne blogiau kaip Proxy, URL Rewrite, Transparent Inline
3.3.7.	Sprendimo našumas	– Ne mažiau kaip 300 konkurentinių sesijų. – Turi būti galimybė praplėsti iki ne mažiau kaip 500 konkurentinių sesijų įsigyjant papildomas licencijas pagal poreikį.
3.3.8.	Pagrindinės palaikomos funkcijos	– WEB turinys vykdomas izoliuotuose vienkartiniuose konteineriuose, vartotojams siunčiant vaizdo informaciją. – Konteineriai turi būti panaikinami pasibaigus web naršyklės sesijai. – Atkuriamas web turinys turi būti pilnai interaktyvus – pvz. leisti video peržiūrą, apdoroti paspaustas nuorodas, atidaryti PDF bylas ir t.t. – Turi būti funkcionalumas atsisiųsti bylas (jeigu tam nėra sukonfigūruoti apribojimai). – Vartotojų autorizacija LDAP. – WEB filtravimo funkcija. – Antivirusinė apsauga.

		– Turi būti funkcionalumas apriboti vartotojus leidžiant jiems tik web puslapių peržiūrą. – Turi būti funkcionalumas pakeisti dokumentuose esančias nuorodas į neinteraktyvų tekstą. – Integracija su el. pašto apsaugos platforma, kad būtų izoliuojama darbuotojo naršyklė nuo tinklapio, kai paspaudžiama nuoroda gauta el. paštu. – Integracija su ugniasienėmis, kai ugniasienės veikia Proxy serverio režimu, kad būtų izoliuojama darbuotojo naršyklė nuo tinklapio, kai naršoma internete.
3.3.9.	Palaikomos web naršyklės	Ne blogiau kaip Chrome, Firefox, Microsoft Edge, Microsoft Internet Explorer, Safari, Opera.
3.3.10.	Valdymo funkcijos	– SysLog palaikymas. – Taisyklių vartotojams kūrimas. – Lokalių vartotojų, svečių vartotojų grupių bei NTLM autentifikacijos -organizacijos vartotojų (angl. *single sign-on*) palaikymas.
3.3.11.	Aukšto patikimumo funkcijos	Esant poreikiui turi būti galima prijungti papildomą įrenginį, kad sistema veiktų aukšto patikimumo režimu.
3.3.12.	Atnaujinimai	Viso garantinio aptarnavimo laikotarpio metu gamintojas turi teikti sistemos duomenų bazių ir kitų komponentų, reikalingų aukščiau nurodytų funkcijų palaikymui, atnaujinimus.
4.	Privilegijuotos prieigos valdymo komponentas	
4.1.	Įrenginių kiekis	Turi būti pateiktas vienas aukšto patikimumo komplektas.
4.2.	Sprendimas	Specializuotas privilegijuotos prieigos valdymo sprendimas su glaudžiai integruota slaptažodžių spinta ir nuotoliniu slaptažodžių valdymu.
4.3.	Aparatiniai ir programiniai resursai	– Jei siūlomas ne įrenginių (angl. *appliance*) tipo sprendimas, Perkančioji organizacija pateiks reikalingų techninių parametrų virtualias mašinas. – Jeigu siūlomo sprendimo veikimui naudojamos Microsoft SQL duomenų bazės bei Windows operacinė sistema, Perkančioji organizacija pateiks Windows Server operacinę sistemą ir suteiks vietą įmonės turimame Microsoft SQL duomenų bazės serveryje. Jeigu reikalingas atskiras SQL serveris, Tiekėjas turi pateikti SQL reikalingas licencijas.
4.4.	Slaptažodžių, kredencialų ir saugomų objektų slaptažodžių spintoje kiekis	Ne mažiau 2000
4.5.	Sprendimo naudotojų kiekis	Ne mažiau 25 (neribojamo funkcionalumo)
4.6.	Sprendimo palaikomų sistemų (serverių, darbo vietų, tinklo, saugumo ir kitos sprendimo	Ne mažiau 2000

	nuotoliniu būdu valdomos galutinės įrangos) kiekis	
4.7.	Administravimo sąsajos	– Turi būti Web GUI grafinė vartotojo sąsaja valdoma interneto naršyklės pagalba (HTTPS). – Web grafinė sąsaja neturi naudoti nesaugiomis laikomų programinių komponentų Adobe Flash, Silverlight, Java Applet. – Turi būti laisvai modifikuojami (angl. *custom*) darbalaukiai. – Turi būti paskutinių naudotų kredencialų atvaizdavimas vienoje vietoje. – Turi leisti reikalingus kredencialus pažymėti kaip mėgstamus ir juos atvaizduoti vienoje vietoje. – Turi būti SSH nuotolinio administravimo terminalinė sąsaja. – Turi leisti nustatyti IP adresų sąrašus, iš kurių leistini prisijungimai sprendimo administravimui.
4.8.	Slaptažodžių spinta	– Turi leisti saugoti šią jautrią informaciją: o slaptažodžiai; o SSH privataus/viešo rakto poros; o sertifikatai su privačiais raktai; o API key raktai; o PIN kodai; o bylos/prisegtukai; o dokumentai; o tinklo diagramos; o programinės įrangos licencijų raktai; o kita jautri informacija. – Kiekviena paslaptis turi būti šifruota individualiu šifravimo raktu. – Turi būti realizuotas slaptažodžio maskavimas (nerodymas). – Slaptažodžio rodymas/nerodymas turi būti laisvai konfigūruojamas. – Turi būti slaptažodžio istorijos įrašų kiekio nustatymas ir kontrolė. – Turi būti funkcionalumas, leidžiantis pasižiūrėti, kokie slaptažodžiai buvo naudoti praeityje (slaptažodžių istorija ne mažiau 10 paskutinių). – Turi leisti reikalauti, įrašyti komentarą, kodėl peržiūrimas slaptažodis ar prašoma suteikti privilegijuota prieiga. – Turi leisti naudotojui uždėti papildomą slaptažodį paskyros ar paslapties apsaugai, kuris negali būti atstatomas ar apeitas sistemos administratoriams. – Turi parodyti slaptažodį atviru tekstu ten kur nėra galimybės automatizuoti privilegijuotą prisijungimą. – Turi leisti prisijungti tiesiogiai (ne per proxy/jumphost) į valdomą sistemą per SSH ir RDP, nerodant tikrojo slaptažodžio.
4.9.	Slaptažodžių politikos	– Sprendimas turi leisti kurti laisvai modifikuojamas (angl. *custom*) slaptažodžių politikas. – Sprendimas turi leisti kurti ir taikyti skirtingas slaptažodžių politikas skirtingoms paskyroms, slaptažodžiams.

		– Sprendimas turi generuoti atsitiktinius slaptažodžius atitinkančius nustatytą politiką. – Sprendimas turi pasirinktinai leisti kontroliuoti/nekontroliuoti slaptažodžio politiką jo išsaugojimo, keitimo slaptažodžių spintoje metu. – Sprendimas turi pasirinktinai leisti kontroliuoti/nekontroliuoti slaptažodžių politiką, slaptažodžio keitimo nuotoliniu būdu metu.
4.10.	Privilegijuotų sesijų paleidėjai	– Turi leisti inicijuoti privilegijuotas sesijas į galutines valdomas sistemas, neatskleidžiant RDP ir SSH kredencialų. – Turi būti gamintojo paruošti privilegijuotų sesijų paleidėjai. – Turi leisti kurti laisvai modifikuojamus (angl. *custom*) sesijų paleidėjus ir įrašyti jų naudojimo video įrašą, kai sesija užmezgama ne per proxy/jumphost. – Turi leisti kurti paleidėjus iš Windows proceso. – Turi leisti kurti paleidėjus iš kelių Windows procesų. – Paleidėjai turi veikti naudotojo kompiuteryje, ne web serveryje. – Turi būti įskiepis į interneto naršyklę web aplikacijų formų kredencialų automatiniam užpildymui arba lygiavertis funkcionalumas.
4.11.	Paskyrų aptikimo automatizuoti skanavimai	– Turi skanuoti ir automatizuotai aptikti šių tipų paskyras: o Windows lokalias; o Unix/Linux lokalias; o Active Directory; o ESXi lokalias. – Turi leisti aprašyti taisykles, kaip automatiškai įtraukti aptiktas paskyras į sprendimą pagal iš anksto apibrėžtus kriterijus ir taisykles.
4.12.	Šifravimas	– Visa slaptažodžių spintoje saugoma jautri informacija turi būti šifruota AES-256 arba lygiaverčiu algoritmu. – Master Key šifravimo raktas turi būti apsaugotas papildomu standartiniu šifravimo lygmeniu DPAPI arba analogišku. – Šifruota duomenų bazė, kurioje saugomi kredencialai ir kitos paslaptys, negali būti atskirai dešifruojama, net ir turint Master Key, be gamintojo pagalbos.
4.13.	„Keturios akys“	– Siūlomo sprendimo administravimas turi turėti aiškiai išskirtas teises, kurios leistų realizuoti „keturių akių“ administravimo principą: vienas naudotojas suteikia super-administratoriaus teises, kitas tomis teisėmis pasinaudoja. Teikėjas jomis negali pasinaudoti, gavėjas negali jų sau suteikti.
4.14.	Architektūra	– Sprendimas turi palaikyti diegimą tiek fizinėje, tiek virtualioje aplinkoje pagal poreikį. – Jei naudojama trečių šalių programinė įranga pvz. operacinė sistema, duomenų bazė ar kita, ji turi būti laisvai atnaujinama trečių šalių priemonėmis arba atnaujinimą turi užtikrinti siūlomo sprendimo gamintojas. Turi būti įskaičiuoti visi reikalingi kaštai. – Siūlomas sprendimas turi leisti jame naudoti įprastai organizacijos naudojamus antiviruso ir atsarginių kopijų

		funkcionalumus arba šias funkcijas turi užtikrinti siūlomo sprendimo gamintojas. Turi būti įskaičiuoti visi reikalingi kaštai. – Sprendimo nuotoliniu būdu valdomuose serveriuose neturi būti instaliuojami agentai ar kita programinė įranga, susijusi su sprendimu, saugumo rizikos mažinimo ir efektyvaus veikimo tikslais. – Sprendimas turi būti įdiegtas geografiškai paskirstyta architektūra, įskaičiuoti visi reikalingi diegimo kaštai.
4.15.	Aukštas patikimumas	– Sprendimas turi palaikyti aktyvus-pasyvus telkinio režimą, visos reikalingos licencijos turi būti įskaičiuotos. – Sprendimas turi palaikyti aktyvus-aktyvus telkinio režimą, visos reikalingos licencijos turi būti įskaičiuotos.
4.16.	Autentifikavimas	– Turi palaikyti ne mažiau, kaip šiuos autentifikavimo protokolus: o Radius; o Kerberos. – Turi palaikyti lokalių vartotojų ir Microsoft Active Directory vartotojų prisijungimus į web portalą. – Autentifikavimo procesas į galutines sistemas turi būti apsaugotas nuo tikrųjų kredencialų (tiek atviro teksto, tiek koduotame formate) išviešinimo prisijungimo šaltinyje (sprendimo naudotojo kompiuteryje).
4.17.	Palaikomi paskyrų tipai	Sprendimas turi palaikyti šių tipų paskyras: – tinklo įrenginių paskyros; – saugumo įrenginių paskyros; – duomenų bazių paskyros; – Web svetainių paskyros; – debesų kompiuterijos administracinės paskyros; – Windows lokalios privilegijuotos paskyros; – Linux/Unix lokalios privilegijuotos paskyros; – AD privilegijuotos paskyros; – AD paslaugų paskyros (angl. *service account*); – serverių OOB valdymo sąsajų paskyros (iLO, iDRAC ir kitos).
4.18.	Kelių faktorių autentifikavimas (angl. *MFA*)	– Turi būti funkcionalumas, leidžiantis sprendimą integruoti su trečių šalių MFA sprendimais paremtais laiku vienkartiniais slaptažodžiais (angl. *time based onetime password*). – Turi būti funkcionalumas, leidžiantis naudoti aparatines autentifikavimo žymes FIDO2. – Turi palaikyti šias autentifikavimo mobiliąsias programėles: o Google Authenticator; o Microsoft Autenticator.
4.19.	Sesijos neaktyvumas	Sprendimas turi panaikinti vartotojo sesiją į web portalą po nustatyto neaktyvumo laiko.
4.20.	Privilegijuoti prisijungimai	– Privilegijuotai paskyrai turi būti galimybė prisijungti prie galinių sistemų RDP ar SSH protokolais, neatskleidžiant kredencialų, bent dviem skirtingais būdais: o tiesiogiai iš naudotojo kompiuterio į galutinę administruojamą sistemą; o iš naudotojo kompiuterio per įgaliotąjį serverį (angl. *proxy/jumphost*).

		– Turi leisti pasirinkti vieną iš kelių prisijungimo būdų kiekvienai privilegijuotai paskyrai. – Pats sprendimas turi galėti jungtis prie galutinių sistemų šiais būdais: o SSH; o RDP; o Powershell.
4.21.	SSH ir RDP prieiga	– Turi leisti jungtis prie galutinių sistemų per SSH proxy, naudojant atsitiktinai automatiškai sugeneruotą vienkartinį naudotojo vardą ir vienkartinį slaptažodį, neatskleidžiant tikrųjų SSH kredencialų. – Turi leisti naudotis slaptažodžių spinta ir privilegijuotomis SSH sesijomis į galutines sistemas iš komandinės eilutės, nenaudojant interneto naršyklės, neatskleidžiant tikrųjų SSH kredencialų ir nenaudojant vienkartinių kredencialų . – Turi leisti jungtis prie galutinių sistemų per RDP proxy, naudojant atsitiktinai automatiškai sugeneruotą vienkartinį domeno vardą, vienkartinį naudotojo vardą ir vienkartinį slaptažodį, neatskleidžiant tikrųjų RDP kredencialų.
4.22.	Prieigos patvirtinimai	– Turi palaikyti vieno asmens patvirtinimą. – Turi technologiškai palaikyti daugiasluoksnį prieigos patvirtinimą, kuomet prieigai patvirtinti reikalingi keli skirtingi asmenys. – Turi leisti ne mažiau kaip 3 asmenims patvirtinti, tam kad prieiga būtų suteikta. Jei nors vienas iš jų nepatvirtina, prieiga turi būti nesuteikiama. – Prieigos užklausų patvirtinimai siunčiami e-paštu. – Prieigos užklausų patvirtinimai atliekami web portale. – Turi leisti iš anksto nustatyti prieigos laiko ribotą trukmę. – Turi vykdyti skriptus prieš ir po privilegijuots sesijos rezervacijos.
4.23.	Komandos	Turi leisti virtualiai segmentuoti vartotojus ir grupes, apjungiant juos į komandas.
4.24.	Video įrašymas	– Kokybiškai įrašyta RDP sesija valandos trukmės turi užimti ne daugiau nei 50 MB vietos. – Turi palaikyti kelis skirtingus video kodekus (nurodyti). – Privilegijuota RDP ir SSH sesija turi būti įrašoma net ir kuomet jungiamasi tiesiogiai į galutinę sistemą, ne per proxy (ne „jumphost“ principu). – Turi būti fiksuojami klavišų paspaudimai (angl. *keylogging*). – Turi leisti atlikti paiešką video įraše pagal konkretų tekstą iš fiksuojamų klavišų paspaudimų. – Turi saugoti video įrašus šifruotame formate, tam kad nebūtų galima jų peržiūrėti neturint reikalingų teisių sprendime. – Turi leisti sudaryti leistinų SSH komandų „baltuosius sąrašus“.
4.25.	Privilegijuotos sesijos valdymas	– Turi leisti matyti privilegijuotos RDP ir SSH sesijos vaizdą beveik realiu laiku. – Turi leisti nutraukti privilegijuotą sesiją neįspėjus galutinio naudotojo rankiniu būdu.

		– Turi leisti nutraukti privilegijuotą sesiją įspėjus galutinį naudotoją rankiniu būdu. – Turi leisti nustatyti laiką po kurio sesija nutrūks, kad būtų pabaigtas darbas vykdytas sesijos metu.
4.26.	Unifikuota vartotojo sąsaja	– Turi leisti dirbti su keliomis skirtingomis privilegijuotomis RDP, SSH sesijomis vienu metu iš bendros sąsajos, kurioje sesijų langai būtų organizuoti kortelių (angl. *tabs*) principu analogišku interneto naršyklėms (angl. *internet browser tabs*). – Darbas su sesija turi vykti tik pasirinkus atitinkamą kortelę (angl. *tab*). – Turi leisti keisti privilegijuotos sesijos lango rezoliuciją.
4.27.	Bendras privilegijuotas valdymas	– Turi leisti valdyti bendro privilegijuoto administravimo paskyras tokias, kaip „root“, „administrator“ ir kitas. – Turi būti atsekamumas, kas jomis naudojosi. – Turi leisti rezervuoti tokią paskyrą vienam vartotojui vienu metu.

4.28.	Nuotolinis slaptažodžių keitimas	– Turi būti gamintojo paruošti nuotoliniai slaptažodžių keitėjai.
		– Turi leisti kurti laisvai konfigūruojamus(angl. *custom*) nuotolinius slaptažodžių keitėjus.
		– Turi leisti pasirinkti kokie simboliai traktuojami, kaip eilutės pabaiga SSH tipo nuotolinio slaptažodžio keitimo konfigūracijoje.
		– Turi periodiškai automatiškai tikrinti ar sprendime saugomas slaptažodis teisingas ir juo gali būti prisijungta prie galutinės sistemos.
		– Turi nuotoliniu būdu keisti slaptažodžius Windows tipo operacinėms sistemoms.
		– Turi nuotoliniu būdu keisti Microsoft Active Directory administratorių slaptažodžius.
		– Turi nuotoliniu būdu keisti Active Directory paslaugų paskyrų „service accounts“ slaptažodžius.
		– Turi mokėti perleisti iš naujo Windows servisus (angl. *services*) ir suplanuotas užduotis (angl. *scheduled tasks*) po paslaugos paskyros slaptažodžio pakeitimo.
		– Turi nuotoliniu būdu keisti šiuos UNIX/Linux tipo slaptažodžius:
		  o Unix standartinė paskyra;
		  o Unix „root“ paskyra;
		  o Unix SU;
		  o Unix SUDO.
		– Nuotolinis slaptažodžio keitimas turi būti galimas:
		  o pagal pareikalavimą;
		  o periodiškai;
		  o pasibaigus saugumo politikoje nustatytam galiojimo laikui.

4.29.	SSH privataus/viešo rakto poros rotavimas	– Turi automatiškai rotuoti ir išsaugoti SSH privataus/viešo rakto porą privilegijuotos prieigos sprendime ir jo valdomose sistemose. – Kiekvienai sistemai turi valdyti individualią ir unikalią privataus/viešo raktų porą.

		– Raktų poros generavimas turi būti galimas: o pagal pareikalavimą; o periodiškai; o pasibaigus saugumo politikoje nustatytam galiojimo laikui. – Turi leisti rezervuoti raktų porą, tam kad kiti naudotojai negalėtų vienu metu ja pasinaudoti. – Turi automatiškai rotuoti ir išsaugoti slaptažodį, saugantį SSH privataus/viešo rakto porą.
4.30.	Teisės	– Visas sprendime realizuotas funkcionalumas turi turėti individualias konkrečias teises, kurias būtų galima kontroliuoti. – Turi leisti grupuoti teises į roles.
4.31.	Rolės	– Turi būti gamintojo iš anksto paruoštos rolės. – Turi leisti kurti laisvai modifikuojamas (angl. *custom*) roles ir leisti joms priskirti minimalias teises. – Turi leisti kurti roles RBAC (angl. *role based access control*) principu. – Turi leisti taikyti roles vartotojams ir grupėms.
4.32.	Pranešimai	– Turi leisti kurti laisvai modifikuojamus pranešimus, kurie siunčiami elektroniniu paštu, apie svarbius sprendime vykstančius įvykius. – Turi leisti kurti pranešimus apie įvykius vykstančius sprendime, susijusius su realizuotu įvairiu funkcionalumu. – Turi leisti siųsti pranešimus e-pašto adresams, kurie nėra susieti su sprendimo naudotojų paskyromis.
4.33.	Skriptai	– Turi palaikyti SSH skriptus. – Turi palaikyti SQL skriptus. – Turi palaikyti Powershell skriptus.
4.34.	Sistemos ir naudotojų įrašai (angl. *logs*)	– Visi sistemos ir naudotojų aktyvumo įrašai turi būti pasiekiami toje pačioje Web GUI sąsajoje, nereikalaujant jungtis į išorines ar kitas konsoles, sąsajas. – Prie skirtingo sprendimo funkcionalumo konfigūravimo turi būti atvaizduojami tik su tuo funkcionalumu susiję automatiškai atrinkti įrašai (angl. *logs*). – Kada nors sprendime sukurti objektai (naudotojai, rolės, katalogai, paslaptys, paskyros, šablonai ir kiti) turi likti net ir po jų ištrynimo, audito, įrodymų ir atsekamumo tikslais. – Visas naudotojo aktyvumas sprendime turi būti fiksuojamas įvykių žurnale (angl. *logs*). – Turi būti atsekamumas pagal įrašus, kas, ką ir kada padarė ar naudojosi.
4.35.	Dokumentacija, pateikiama su įranga	Turi būti pateikiama gamintojo sprendimo oficiali dokumentacija: – vartotojo gidas; – administravimo gidas; – gerųjų saugumo praktikų gidas; – prieiga prie gamintojo paruoštų video mokomųjų įrašų įvairiomis techninėmis temomis, susijusiomis su siūlomu sprendimu;

		– prieiga prie gamintojo oficialios internetinės žinių bazės; – prieiga prie gamintojo oficialaus internetinio forumo.
4.36.	Eksportavimas ir importavimas	– Sprendimas turi leisti importuoti paskyras ir kredencialus masiniu būdu iš tekstinės bylos CSV ir XML formatu. – Atstatymo ir migravimo tikslais turi leisti eksportuoti kredencialus ir paskyras XML formatu. – Eksportavimo teisė turi būti išskirta ir konfigūruojama pasirinktinai.
4.37.	Atsarginės kopijos	Sprendimas turi automatiškai daryti savo atsargines kopijas nurodytu reguliarumu tiek web aplikacijos, tiek duomenų bazės į šias lokacijas: – lokalus diskas; – tinklo katalogas.
4.38.	Atnaujinimai	– Sprendimas turi gebėti automatiškai pasitikrinti internete, ar nėra naujos programinės įrangos versijos. – Sprendimas turi leisti parsisiųsti ir įdiegti programinės įrangos naują versiją Web GUI grafinės sąsajos pagalba. – Sprendimas turi leisti atnaujinti programinę įrangą Web GUI sąsajos pagalba kai sprendimas neturi interneto ryšio (angl. *offline update*). – Su atnaujinimu susiję visi kaštai turi būti įskaičiuoti pasiūlyme.
4.39.	Integracijos	– Turi būti SOAP arba REST API. – Turi būti integruojamas su automatizuotoms DevOps aplinkoms skirta slaptažodžių spinta. – Turi būti integruojamas su RPA (angl. *robotic process automation*) aplinkomis ir įrankiais. – API turi būti apsaugotas SSL/TLS. – API turi palaikyti pagrindines programavimo kalbas .NET, JAVA arba lygiavertes. – API turi leisti ieškoti slaptažodžių, išsaugoti slaptažodžius, leisti autentifikuotis ir kitas funkcijas. – Turi būti integracija su SSO (angl. *single sign on*) sistemomis. – Turi veikti SAML 2.0 Service Provider (SP) rolėje. – Turi integruotis su keliais Active Directory domenais. – Integracijai su AD neturi būti naudojama domeno administratoriaus, įmonės administratoriaus ar kita aukštų privilegijų Windows paskyra. – Turi integruotis su HSM (angl. *hardware security module*) aparatiniais šifravimo raktų saugumo moduliais. – Turi palaikyti standartinį Windows šifravimo tiekėją – CNG – Microsoft Cruptography Next Generation provider arba lygiavertį. – Turi integruotis su helpdesk bilietų valdymo sistemomis (angl. *ticketing system*). – Turi integruotis su pažeidžiamumų valdymo sistemomis. – Turi leisti pažeidžiamumų valdymo sistemoms skanuoti mašinas su individualiais tos mašinos kredencialais, saugomais privilegijuotos prieigos valdymo sistemoje, o ne pažeidžiamumų valdymo sistemoje.

		– Turi integruotis su sisteminių ir saugumo įvykių valdymo sistemomis (angl. *SIEM*), siunčiant Syslog pranešimus CEF formatu. – Bent trys populiariausi SIEM gamintojai turi turėti paruoštas pranešimų apdorojimo (angl. *parsing rules*) taisykles. – Nurodyti SIEM gamintojus, palaikančius siūlomą sprendimą. – Turi palaikyti integruotą Windows autentifikavimą IWA arba lygiavertį.
4.40.	Sistemos saugumo stiprinimas	– Gamintojas turės pateikti instrukcijas, kaip sustiprinti saugumo konfigūraciją, įdiegus sprendimą šiais lygmenimis: o operacinė sistema; o duomenų bazė; o aplikacijų serveris. – Turi būti realizuoti gamintojo automatizuoti testai, kurie parodo kiek esama konfigūracija atitinka gerąsias praktikas ir kurie nustatymai neatitinka. – Turi pateikti rekomendacijas, kaip sutvarkyti neatitikimus.
4.41.	Ataskaitos	– Turi būti gamintojo iš anksto paruoštos ataskaitos. – Turi leisti kurti laisvai modifikuojamas (angl. *custom*) ataskaitas. – Turi būti paruošta ataskaita apie laisvai pasirenkamą konkretų privilegijuotą sprendimo vartotoją, kuri leistų nustatyti, kokiais slaptažodžiais ir paslaptimis buvo pasinaudota per laiko intervalą. – Nustačius konkretaus vartotojo pasiektus slaptažodžius per laiko periodą, turi juos pakeisti nuotoliniu būdu vienu paspaudimu (išėjusio iš darbo privilegijuoto vartotojo scenarijus). – Siekiant apsaugoti asmens ir kitus jautrius duomenis ataskaitose ir sesijų įrašuose, turi leisti nustatyti dviejų asmenų kontrolę.
5.	Žurnalinių įvykių ir įrašų valdymo komponentas	
5.1.	Sistemos tipas	– Saugumo informacijos ir įvykių valdymo sistema, susidedanti iš pas Perkančiąją organizaciją montuojamos specializuotos techninės ir programinės įrangos (toliau – Sistema). – Visa programinė įranga turi būti to paties gamintojo arba kelių gamintojų suderinama bendram darbui, tačiau kartu su pasiūlymu turi būti pateikti visų siūlomų įrangos gamintojų raštiški patvirtinimai, kad siūloma įranga yra pilna apimtimi suderinama tarpusavyje bei siūlomoms įrangoms galios reikalaujama garantija, nebus taikomi garantijos apribojimai bei garantiniai įsipareigojimai bus vykdomi taikant „vieno langelio“ principą. – Visa įrenginyje esanti programinė įranga privalo būti skirta numatytoms funkcijoms atlikti. – Turi būti pateikta visa techninė (pagal gamintojo rekomendacijas), programinė įranga ir licencijos, reikalingos toliau aprašytam Sistemos funkcionalumui ir našumui užtikrinti.

		– Sistema ir jos komponentai turi būti pateikti su naujausiomis programinės įrangos versijomis.
5.2.	Fiziniai parametrai	Pateikiama techninė įranga privalo būti pritaikyta montuoti į 19 colių tarnybinių stočių spintą. Taip pat pateikiama su visomis montavimui reikalingomis medžiagomis.
5.3.	El. maitinimo šaltiniai	Turi turėti ne mažiau kaip 2 (du) vienas kitą dubliuojančius maitinimo šaltinius, keičiamus darbo metu (angl. *hot swap*).
5.4.	Tinklo prievadai	– Ne mažiau 2 vnt. 10 Gbps prievadai. – Ne mažiau 2 vnt. 1 Gbps prievadai.
5.5.	Sistemos vidinė talpykla	Sistema turi turėti ne mažiau kaip 20 TB naudingos talpos, skirtos įvykių saugojimui.
5.6.	Bendri reikalavimai	– Sistema turi veikti TCP/IP protokolų pagrindu sukurtuose tinkluose. – Tiekėjas gali siūlyti ir daugiau programinės ar techninės įrangos vienetų, jei tai būtina jo siūlomam sistemos įdiegimo sprendimui realizuoti, tačiau visas sprendimas turi būti kaip viena visuma, valdoma sistemos grafinėje naudotojo sąsajoje (spendimas negali būti sukurtas iš atskirų, į vieningai valdomą visumą neintegruotų komponentų). – Į perkamų prekių apimtis turi būti įtrauktos ir tiesiogiai šiuose reikalavimuose neįvardintos Sistemos licencijos, komponentai, moduliai, kurie yra būtini keliamam funkcionalumui realizuoti. – Sistema gali būti plečiama *horizontaliuoju* būdu, t. y. galima Sistemos greitaveiką išplėsti pridedant papildomus modulius (jei reikia – su atitinkamomis licencijomis). – Sistema turi turėti tokius komponentus/funkcionalumus, ne prasčiau kaip: o SIEM (angl. *security information and event management*); o SOAR (angl. *security orchestration, automation and resposne*); o UEBA (angl. *user and entity behavior analytics*). – Šiuo pirkimu perkamai Sistemai turi būti pateiktos visos reikalingos licencijos SIEM, SOAR ir UEBA funkcionalumui įgyvendinti.
5.7.	Sistemos našumas / licencijos	– Sistema turi gebėti nepertraukiamai (angl. *sustained*) apdoroti, ne mažiau kaip 5000 įvykių per sekundę. Turi būti pateikta atitinkama licencija. – Turi būti galimybė, ateityje pridedant papildomus modulius ir/ar įsigyjant licenciją, plėsti sistemos greitaveiką iki ne mažiau kaip 20000 įvykių per sekundę.
5.8.	Įvykių įrašų saugojimas	– Sistema turi užtikrinti vietinį įvykių įrašų kaupimą sutrikus perdavimo ryšiui tarp įvykių surinkimo modulio ir sistemos. – Sistema turi leisti skirtingus duomenis saugoti skirtingą laiką.
5.9.	Įvykių įrašų vientisumas	Sistema turi užtikrinti sisteminių įrašų vientisumą.
5.10.	Įvykių šaltiniai	– Sistema turi surinkti žurnalinius įvykius (angl. *logs*) iš, ne prasčiau kaip: tinklo įrangos, tinklo perimetro saugos įrenginių, taikomųjų sistemų, įskaitant operacines sistemas,

		duomenų bazių valdymo sistemų, taikomųjų programinės įrangos sistemų. – Sistema be papildomo konfigūravimo turi atpažinti ir normalizuoti ne mažiau kaip 800 komercinių ir atviro kodo duomenų šaltinių. – Sistemoje turi būti galima grupuoti šaltinius pagal tipą, fizinę ir loginę vietą. – Sistema turi informuoti, jeigu bet kuris iš duomenų šaltinių nustoja siųsti įvykius. – Sistema turi leisti patiems kurti įvykių normalizavimo (angl. *parsing*) taisykles.
5.11.	Įvykių surinkimas	– Sistema turi surinkti įvykius iš, ne prasčiau kaip: tinklo įrangos, tinklo saugos įrenginių, taikomųjų sistemų įskaitant operacines sistemas, duomenų bazių valdymo sistemų ir taikomosios programinės įrangos. – Sistema turi surinkti/priimti įvykius iš Cloud/SaaS tipo duomenų šaltinių ne prasčiau kaip: Office 365, Amazon, AWS. – Sistema turi surinkti įvykius tiek užklausdama duomenų šaltinius, tiek iš duomenų šaltinių, kurie patys siunčia įvykius. – Sistema turi surinkti įvykius panaudojant programiniais agentus ir be jų. – Sistema turi prie įvykio pridėti geolokacijos informaciją pagal IP adresą. – Sistema turi įvertinti priimamo įvykio laiko žymos ir realaus įvykusio įvykio žurnalo laiko žymių skirtumus, t. y. sistema vertina saugumo įvykius, pagal tai kada įvyko įvykis, o ne tada, kai sistema užfiksavo įvykį. – Sistema turi pasiimti informacija iš Microsoft Active Directory domeno, t. y. turi ištraukti informaciją apie vartotojus, matyti vartotojo turimą el. pašto adresą, pilną vartotojo vardą. – Tinklo srauto Netflow įvykių surinkimas turi būti galimas be papildomų įrenginių ar komponentų. – Sistema turi priimti įvykius esant vienakrypčiam tinklo ryšiui (įvykių gavimas per duomenų diodą). – Įvykiai, iš įvykių surinkimo komponento, jeigu toks bus naudojamas, turi būti perduodami šifruotais duomenų srautais. – Turi suglaudinti sisteminius įrašus juos perduodant iš įvykių surinkimo komponento į sistemą. – Turi būti funkcionalumas perduodamus įvykius perduoti saugiais kanalais, tokiais kaip: TLS ar lygiaverčiais. – Sistema turi palaikyti įvairaus tipo įvykių perdavimo formatus, ne prasčiau kaip: Syslog, SNMP, JDBC. – Sistema turi pasiimti ir apdoroti standartinius ir nestandartinius įvykius, saugomus Windows Event Log. – Sistema turi palaikyti šiuos įvykių formatus, ne prasčiau kaip: CEF (angl. *common event format*), SYSLOG, SNMP, LEEF.

		– Sistema turi priimti tinklo srauto duomenis šiomis technologijomis, ne prasčiau kaip: IPFIX, NetFlow, Sflow, J-Flow.
5.12.	Agentais paremtas įvykių surinkimas	– Turi būti funkcionalumas sistemos agentus diegti Windows operacinėse sistemose. – Sistema turi palaikyti SSL arba TLS šifravimą perduodamiems duomenims. – Agentais paremtam įvykių surinkimui gali būti priskirtas laikas kada tai atlikti (angl. *scheduled collection*). – Turi gebėti surinkti tinklo srauto duomenis, ne prasčiau kaip: IPFIX, NetFlow, sFlow, J-Flow. – Agentai turi būti centralizuotai valdomi ir atnaujinami. – Turi užtikrinti laiko žymos normalizavimą. – Agentais paremtas įvykių surinkimas turi leisti surinkti tokius įvykius, ne prasčiau kaip: o Syslog; o UDP/TCP ir saugų Syslog; o Flat bylas (viena eilute ir daugeliu eilučių, suglaudintas ir nesuglaudintas bylas); o Windows sisteminius įvykius, įtraukiant ir individualius žurnalinius įvykius; o Microsoft Exchange message tracking ir Microsoft Office 365 message tracking žurnalinius įrašus. – Sistema turi palaikyti vienkryptį įvykių perdavimo būdą, turi gebėti priimti įvykius iš duomenų diodų. – Su siūloma sistema turi būti pateikta, ne mažiau kaip 25, aukščiau nurodyto funkcionalumo agentų licencijų. Jeigu agentų licencijos turi būti perkamos arba sistema turi gebėti surinkti šiame punkte nurodytus duomenis be agentų pagalbos (jei reikalingos kitos programinės įrangos licencijos ar įrenginiai, jos/jie turi būti įskaičiuoti į pasiūlymo kainą). Pasiūlyme pirkimui įvardinti pateikiamos įrangos pavadinimus, modelius, licencijų skaičių.
5.13.	Naudotojų elgesio analizės komponentas UEBA (angl. *user and entity behavior analytics*)	– Turi būti pateiktas naudotojų elgesio analizės modulis su mašininio apsimokinimo (angl. *machine learning*) funkcijomis. – Naudotojų elgesio analizės modulis turi gebėti: o apsimokinti ne mažiau kaip 20 dienų naudotojo elgsenos modelį; o atlikti naudotojo rizikos vertinimą pagal dabartinį naudotojo elgesį lyginant su praėjusių 20 dienų naudotojo elgesiu; o analizuoti standartinę naudotojų veiklą ir aptikti joje atsirandančias anomalijas; o aptikti pavogtas, kompromituotas naudotojų paskyras; o identifikuoti pasikeitimus naudotojų elgsenoje; o stebėti privilegijuotų naudotojų veiksmus; o naudoti grėsmių informaciją naudotojų stebėjime; o automatiškai apsimokyti naudotojo elgsenos ir pagal turimus duomenis informuoti atsirandančius nuokrypius nuo jos;

		○ turėti grėsmės įverčius, kurie kinta laike ir gali būti naudojami incidentams generuoti; ○ aptikti kenkėjiškas vidines grėsmes (angl. *maliciuos insider threats*); ○ aptikti brutalios jėgos atakas; ○ automatiškai nustatyti grėsmes, pagrįstas įtartinais elgesio modeliais.
5.14.	Saugumo orchestravimo, automotizavimo ir atsako komponentas SOAR (angl. *security orchestration automation and resposne*)	– Turi būti pridėtas saugumo orchestravimo, automatizavimo ir atsako (SOAR) modulis su atitinkamomis licencijomis. – SOAR modulis turi leisti integruotis sistemai su trečiųjų šalių įrenginiais, tam kad iš sistemos atlikti automatinį atsaką į įvykusį incidentą, pvz.: ○ užblokuoti naudotoją nuo tinklo; ○ išjungti RDP sesiją. – SOAR modulis turi turėti gamintojo paruoštus automatinius atsakus. – SOAR modulis turi leisti pridėti gamintojo sukurtus automatinius atsakus prie sistemos. – SOAR modulis turi leisti kurti naujus automatinius atsakus. – SOAR modulis turi leisti atlikti automatinį atsaką iš sistemos atlikti šiais būdais: ○ sistema automatiškai įvykus incidentui inicijuoja automatinį atsaką; ○ saugumo analitikas inicijuoja automatinį atsaką įvykusiam incidentui užkardyti; ○ reikalingas kelių saugumo analitikų patvirtinimas, tam kad automatinis atsakas būtų inicijuotas. – SOAR modulis turi turėti naudotojo gaires (angl. *playbooks*). Gairės yra funkcionalumas, skirtas išsaugoti ir tvarkyti standartines procedūras, reaguojant į žinomas kenkėjiškas programas pvz.: „Phishing“ tipo atakas ar nepatvirtintus programinės įrangos diegimus. – SOAR modulis turi leisti importuoti gaires į naudotojo kreipinį, kurios sukurtų procedūras, pagrįstas kreipinio tipu ir pateiktų nuorodą į išsamesnius dokumentus kaip jį spręsti. – SOAR modulis turi sekti metrikas tokias kaip vidutinis aptikimo laikas (angl. *mean time to detect* (*MTTD*)) ir vidutinis užkardymo laikas (angl. *mean time to responde* (*MTTR*)).
5.15.	Įvykių valdymas	– Sistema be papildomo programavimo turi atlikti surinktų įvykių įrašų normalizavimą (duomenų laukų atitikimas sistemoje turi būti nekintantis) sistemoje formuojant įvykius (angl. *events*). – Sistema turi suglaudinti ilgalaikio saugojimo žurnalinius įvykius (archyvinius duomenis). – Sistema turi normalizuoti įvykių įrašus, pagal sistemos laiko juostą. – Sistema turi leisti ieškoti, filtruoti normalizuotus ir sukoreliuotus įvykius. – Sistema turi leisti atlikti paiešką tarp originaliu formatu saugomų įvykių.

		– Įvykių surinkimo mechanizmas turi leisti atrinkti įvykius pagal duomenų reikšmes, bet kuriame įvykio lauke ir/arba keliuose laukuose. – Sistema turi įvykių įrašus normalizuoti tokiu formatu, kad pasikeitus duomenų šaltiniui, tai neturėtų įtakos įvykių kategorizavimui. Pvz.: pakeitus tinklo ugniasienę į kito gamintojo ugniasienę, įvykių kategorizavimas turi išlikti toks pats.
5.16.	Įvykių apdorojimo lankstumas	Sistema turi leisti, bet kokio formato įvykių įrašus savarankiškai normalizuoti (angl. *custom parser*) į bendrą Sistemoje palaikomą įvykių formatą.
5.17.	Nuotolinė prieiga administravimui	Privalo būti realizuota saugi administravimo grafinė sąsaja (angl. *GUI*), apsaugota HTTPS arba SSL protokolais.
5.18.	Prieigos kontrolė	– Sistema turi turėti centralizuotą sistemos naudotojų autentifikavimo saugyklą. Prieš leidžiant naudotojams prisijungti prie sisteminės administravimo sąsajos, įrenginys privalo autentifikuoti naudotoją ir suteikti tik jam skirtas administravimo lygmens teises. – Sistema turi leisti naudotojams suteikti tik įvykių ir ataskaitų skaitymo teisę. – Sistema turi leisti naudotojams suteikti teises prieiti tik prie jiems skirtų įrenginių ir duomenų šaltinių (angl. *role-based access control*). – Sistema turi turėti funkcionalumą integruotis su išoriniais naudotojų katalogais (pvz.: LDAP).
5.19.	Funkcionalumas ir analitika	– Sistema turi leisti atlikti detalią įvykių analizę pagal laiko intervalus. Pvz.: per minutę, dieną savaitę. – Sistema turi turėti pažangią įvykių analitiką ir turėti mašinų mokymosi (angl. *machine learning*) technikas. – Automatiškai nustatyti grėsmes, pagal įtartinus elgesio modelius. – Sistema turi apdoroti naudotojų vardus. Pvz.: atskirti naudotojo vardą iš Microsoft Active Directory domeno informacijos. – Sistema turi turėti funkcionalumą atlikti duomenų maskavimą (angl. *data masking*) sisteminiuose įrašuose. – Sistema turi turėti funkcionalumą apsimokyti naudotojų elgsenos ir nustačius bazinę liniją (angl. *baseline*) informuoti sistemos naudotojus apie atsiradusias anomalijas. – Turi palaikyti STIX, TAXII standartus. – Sistema turi reguliariai atnaujinti analitikos taisykles, skirtas naujoms grėsmėms aptikti. – Sistema turi integruotis su trečiųjų šalių incidentų reagavimo valdymo sistemomis. – Sistema turi gebėti informuoti apie pastebėtas grėsmes atsakingus darbuotojus SMTP protokolu.
5.20.	Įvykių koreliavimas	– Sistema turi gebėti koreliuoti, ne mažiau kaip 5000 įvykių per sekundę (jeigu reikia – pateikti atitinkamą licenciją). – Sistema turi turėti ne mažiau kaip 800 gamintojo parengtų ir įdiegtų koreliavimo taisyklių.

		– Sistema turi leisti plėsti koreliuojamų įvykių per sekundę pajėgumą, nekeičiant esamos sistemos, o įdiegiant papildomą modulį ir/ar nuperkant papildomą licenciją. – Sistema turi atlikti kelių skirtingų įvykių, įvykusių per tam tikrą laiko tarpą, taisyklėmis paremtą koreliavimą. – Sistema turi vykdyti koreliavimą įvykių, surinktų iš skirtingų įrenginių tipų ir skirtingų gamintojų. – Sistema turi leisti savarankiškai kurti koreliavimo taisykles. – Sistema turi gebėti sekti bazinį tinklo srautų aktyvumą ir pranešti apie nuokrypius nuo normalaus tinklo srauto. – Sistema turi gebėti koreliuoti įvykių (angl. *events*) ir srautų (angl. *flows*) duomenis. – Koreliavimo mechanizmas turi leisti kurti koreliavimo taisykles, remiantis einamaisiais vidurkiais ir nuokrypiais nuo standartinių rodiklių, pagal surinktus/apskaičiuotus rodiklius.
5.21.	Atnaujinimai	– Koreliavimo taisyklių, normalizavimo taisyklių ir šaltinių reputacijos sąrašų/informacijos atnaujinimus turi būti galima atlikti automatizuotai. – Gamintojas turėtų reguliariai teikti atnaujintas analizės taisykles, siekiant nustatyti naujai atsiradusias grėsmes.
5.22.	Įkalčių rinkimas	– Sistema turi rankiniu būdu ar automatiškai įkelti į sistemą grėsmių požymius, ne prasčiau kaip: IP, URL adresus ir kenkėjiškų bylų HASH kodus. – Sistema turi leisti priskirti surinktus įkalčius (įspėjimus, įvykius, išorinius duomenis, pastabas) prie sukurto kreipinio.
5.23.	Geolokacija	– Turi rodyti šalį, regioną, miestą, susietą su paskirties ir šaltinio IP adresu kiekvienam įvykiui. – Turi filtruoti įvykius, pagal jų geolokacijos informaciją.
5.24.	Įspėjamieji įvykiai (angl. *alarm*)	– Sistema turi leisti rankiniu ir/arba automatizuotu būdu kurti įspėjamuosius įvykius, pagal sistemos sugeneruotus įvykius. – Sistema turi leisti naujai kuriamam įspėjamajam įvykiui nustatyti svarbumą. – Sistema turi leisti kurti automatinius atsakus (pvz: atjungti galinį įrenginį nuo tinklo; išjungti RDP sesiją), reaguojant į įspėjamąjį įvykį. – Sistema turi gebėti generuoti įspėjamųjų įvykių ataskaitas. – Sistema turi gebėti siųsti įspėjamąjį įvykį elektroniniu laišku. – Sistema turi centralizuotai stebėti sistemoje vykstančius procesus, papildomų modulių ar programinės įrangos veikimą ir atsiradus gedimui apie tai informuoti sistemos naudotojus.
5.25.	Incidentų valdymas	– Sistemoje turi būti funkcionalumas priskirti, komentuoti incidentus, pridėti prie incidento papildomą žmogų, uždaryti incidentus. – Sistemoje turi būti funkcionalumas keliems naudotojams vienu metu spręsti incidentą, t. y. incidente įkelti įkalčius, komentarus, susijusią su incidentu informaciją. – Uždarytame incidente turi būti grafiniu pavidalu pateikiama informacija apie incidento sukūrimą, eigą ir uždarymo laiką. – Darbalaukyje pasirinkus peržiūrimus įvykius, sistema turi leisti juos priskirti naujam arba esamam incidentui/tyrimui.

		– Sistema turi leisti generuoti incidentų ataskaitas. – Sistema turi leisti išsaugoti su incidentu susijusius įkalčius iš specifinių duomenų šaltinių. Prie incidento sistema turi leisti pridėti informaciją iš, ne prasčiau kaip: įspėjamųjų pranešimų, įvykių duomenų, išorinių bylų duomenų, užrašų (angl. *notes*), sugeneruotų ataskaitų ir kitų. – Sistema turi gebėti atlikti automatinį iš anksto sukonfigūruotą atsaką (pvz: atjungti galinį įrenginį nuo tinklo; išjungti RDP sesiją) į įvykusį incidentą.
5.26.	Įvykių filtravimas	– Sistema turi leisti įvykių filtrus jungti į hierarchijas. – Sistema turi turėti kelių lygmenų filtrus. – Sistema turi leisti naudoti įvykių atrinkimo filtrus realaus laiko įvykių atvaizdavimo sąrašuose, interaktyviuosiuose valdymo ekranuose, įvykių koreliavimo taisyklėse, ataskaitose.
5.27.	Darbalaukiai ir ataskaitos	– Sistemoje turi būti gamintojo sukurti standartiniai darbalaukiai. – Sistema turi turėti funkcionalumą leisti savarankiškai sukurti naujus darbalaukius. – Turi leisti kurti pasirenkamas ataskaitas nurodant/pasirenkant: ataskaitos generavimo laiką, generavimo ciklišKumą. – Sistema turi turėti iš anksto sukurtų ataskaitų šablonus. – Sistema turi turėti ataskaitas, paremtas audito / atitikties reikalavimais. – Sistema turi gebėti automatiškai generuoti ataskaitas. – Sistema turi turėti gamintojo parengtas standartines atitikties saugos standartams ataskaitas, ne prasčiau kaip: ISO27001, GDPR. – Sistema turi turėti funkcionalumą atidėti ataskaitos siuntimą naudotojams. – Turi automatizuotai siųsti ataskaitas nurodytų naudotojų sąrašui elektroniniu laišku. – Turi leisti savarankiškai susikurti darbalaukius, pagal pasirinktinus parametrus. – Sistema turi leisti sukurtais naujais darbalaukiais dalintis su kitais naudotojais. – Turi būti visi reikalingi programiniai įrankiai, skirti savarankiškai kurti grafikų, diagramų ir lentelių tipo darbalaukių komponentus. – Įvykių peržiūros langas turi turėti įrankius, leidžiančius atlikti įvykių analizę, pvz.: trace, whois. – Sistema turi leisti darbalaukiuose atvaizduotus įvykius „išskleisti“ (angl. *drill down*) iki konkrečių įvykio detalių/laukų/reikšmių.
5.28.	Aukštas patikimumas	Turi būti galimybė sistemą išplėsti į aukšto patikimumo (angl. *high-availability*) telkinį bei turėti veikimo atstatymo (angl. *disaster recovery*) galimybę. Turi būti galimybė įdiegti šiuos sprendimus kartu.

5.29.	Reagavimo į įsibrovimus pagalbos gairės	– Sistema turi palaikyti naudotojo gaires (angl. *playbooks*). Gairės yra funkcionalumas, skirtas išsaugoti ir tvarkyti standartines procedūras, reaguojant į žinomas kenkėjiškas veiklas. – Sistema turi leisti importuoti gaires į naudotojo kreipinį, kurios sukurtų procedūras, pagrįstas kreipinio tipu ir pateiktų nuorodą į išsamesnius dokumentus kaip jį spręsti.
6.	Saugaus kriptografinių raktų valdymo sistemos komponentas	
6.1.	Sprendimo architektūra ir sudedamosios dalys	– Sprendimas skirtas serverių šifravimui naudojamų kriptografinių raktų administravimui ir apsaugai. – Sprendimą turi sudaryti ne mažiau kaip dvi (2) aukšto patikimumo sistemos. Kiekviena sistema turi būti sudaryta iš ne mažiau kaip dviejų (2) virtualių telkinio narių, kurių kiekvienas narys diegiamas dedikuotoje aparatinėje įrangoje.
6.2.	Reikalavimai virtualiems įrenginiams	
6.2.1.	Aukštas patikimumas	– Turi būti funkcionalumas įrenginius apjungti į aušto patikimumo telkinį. Turi būti galimybė į telkinį apjungti ne mažiau kaip 6 virtualius telkinio narius. – Turi būti užtikrintas konfigūracijos ir raktų replikavimas tarp telkinio narių.
6.2.2.	Atsarginės kopijos	– Turi palaikyti automatinį šifravimo raktų atsarginių kopijų kūrimą pagal tvarkaraštį. – Visi raktai ir atsarginės kopijos turi būti šifruotos tiek ramybės būsenoje (angl. *data at rest*), tiek judesyje (angl. *data in motion*).
6.2.3.	Saugumo reikalavimai	Įrenginiai turi atitikti ne žemesnį kaip FIPS 140-2 Level 1 sertifikavimo lygį.
6.2.4.	Sertifikatų tarnybos reikalavimai	Turi užtikrinti prie kompiuterių tinklo prijungtos ir neprijungtos vidinės sertifikavimo tarnybos (angl. *Certification Authority*) raktų generavimą, saugojimą, naikinimą ir atsarginių kopijų darymą.
6.2.5.	Kriptografinio saugumo modulio integracija	Turi būti galimybė integruoti kriptografinį saugumo modulį (angl. *Hardware Security Module*), kaip kritinę saugos infrastruktūrą (angl. *Root of Trust*).
6.2.6.	Išplėstinio ryšio protokolai	Turi palaikyti KMS (angl. *Key Management Server*), OASIS KMIP (angl. *Key Management Interoperability Protocol*) Version 2.1 protokolus.
6.2.7.	Suderinamumas	Įrenginiai turi integruotis su HPE SimpliVity, HPE Smart Array Secure Encryption, VMware, MongoDB, IBM DB2, Brocade, Suse, OpenStack.
6.2.8.	Kriptografiniai algoritmai	Įrenginiai turi palaikyti šiuos kriptografinius algoritmus: – simetrinius: AES (angl. *Advanced Encryption Standard*), TDEA (angl. *Triple Data Encryption Algorithm*), HMAC (angl. *Hash-based Message Authentication Code*);

		– asimetrinius viešojo rakto: RSAS (angl. *Rivest–Shamir–Adleman*), ECDSA (angl. *Elliptic Curve Digital Signature Algorithm*).
6.2.9.	Kriptografinių raktų talpa	Ne mažiau kaip 1 500 000 kriptografinių raktų.
6.2.10.	Palaikomų klientų pajėgumas	Ne mažiau kaip 1 000.
6.2.11.	Klientų licencijos	Turi būti pateiktos 6 klientų (angl. *client license*) licencijos, skirtos prijungti HPE SimpliVity hyperkonverguotos infrastruktūros serverius.
6.2.12.	Administravimo sąsajos	– Web GUI grafinė vartotojo sąsaja, valdoma interneto naršyklės pagalba (HTTPS). – CLI (angl. *Command Line Interface*) komandinės eilutės sąsaja. – TLS (angl. *Transport Layer Security*), SSH (angl. *Secure Shell*) saugi nuotolinė prieiga.
6.3.	Reikalavimai aparatinei įrangai	
6.3.1.	Aparatinės įrangos korpusas	– Montuojama į standartinę 19“ (angl. *rack-mount*) spintą. – Komplektuojama su bėgeliais skirtais sistemos ištraukimui iš serverinės spintos. – Ne daugiau kaip 1U aukščio. – Korpusas turi turėti galimybę naudoti užrakinamą priekinę panelę.
6.3.2.	Aparatinės įrangos procesorius	– Ne mažiau kaip 1 procesorius. – Ne mažiau kaip 4 fiziniai branduoliai.
6.3.3.	Aparatinės įrangos operatyvioji atmintis	– Ne mažiau kaip 16 GB. – Turi būti galimybė atmintį išplėsti ne mažiau kaip iki 64 GB.
6.3.4.	Aparatinės įrangos įkrovos atmintis	Turi būti ne mažiau kaip 2 vnt. „karšto keitimo“ SSD tipo diskų, ne mažiau kaip 480GB talpos, apjungtų į aparatinį RAID1 masyvą.
6.3.5.	Aparatinės įrangos prievadai	Ne mažiau kaip 2 vnt. 100/1000 BaseT prievadai.
6.3.6.	Aparatinės įrangos išorinės ir vidinės įvedimo / išvedimo jungtys	Turi būti šios integruotos šios jungtus: – ne mažiau kaip 2 vnt. USB; – ne mažiau kaip 1 vnt. 100/1000 BaseT sąsaja, dedikuota nuotoliniam valdymui; – ne mažiau kaip 1 vnt. VGA prievadas.
6.3.7.	Aparatinės įrangos maitinimo šaltiniai	– Ne mažiau kaip du dubliuojantys vienas kitą maitinimo šaltiniai, keičiami darbo metu (angl. *hot plug*). Galingumas turi būti pakankamas užtikrinti aparatinės įrangos darbingumą maksimalaus apkrovimo darbo režimu sugedus vienam iš šaltinių. – Pritaikyti maitinti iš 230 V 50Hz kintamos srovės elektros tinklo.
6.3.8.	Aparatinės įrangos valdymo sistema	– Nepriklausomas nuo operacinės sistemos, veikianti be agentų. – Turi būti: o aparatinės įrangos nutolęs valdymas per WEB naršyklę, neinstaliuojant papildomos programinės įrangos;

		○ tekstinė ir grafinė konsolės; ○ HTML 5 arba lygiavertė vartotojo sąsaja tiek vartotojo aplinkai, tiek virtualiai konsolei; ○ virtualus CD - ROM ir KVM palaikymas; ○ ne blogiau kaip 128bit SSL saugumas; ○ sistemos mikrokodo (angl. *firmware*) atnaujinimai turi būti apsaugoti kriptografiniu parašu; ○ turi palaikyti BIOS skanavimą realiu laiku nuo kenkėjiško programinio kodo; ○ Microsoft Active Directory palaikymas; ○ nuotolinis aparatinės įrangos įjungimas/išjungimas; ○ galimybė prisijungi ne mažiau kaip 5 nutolusių vartotojų vienu metu ir dalintis konsolės seansu; ○ turi būti aparatinės dalies temperatūros, CPU, operatyvinės atminties, vidinių diskų būklės stebėjimo ir automatinio SNMP pranešimų siuntimo administratoriui funkcionalumas.
6.3.9.	Aparatinės įrangos sisteminio mikrokodo saugumo savybės	Turi būti: – aparatinė įranga darbo metu turi periodiškai tikrinti sistemos mikrokodus dėl nesankcionuotų pakeitimų; – aparatinė įranga įjungimo metu turi pasitikrinti sisteminės programinės įrangos autentiškumą ir automatiškai atstyti iš rezervinės kopijos, jei pažeistas autentiškumas. Nepavykus atstatyti turi būtu uždraustas serverio operacinės sistemos krovimasis.
6.4.	Licencijos esamai virtualizacijos platformos infrastruktūrai įgalinančios šifravimą	– Turi būti pateiktos licencijos įgalinančios saugomų duomenų šifravimą aparatiniame lygyje (angl. *data at rest*) 6 vnt. HPE Simplivity 380 Gen10 hyperkonverguotos infrastruktūros serverių. Licencijos turi būti suderinamos su siūloma saugaus kriptografinių raktų valdymo sistema ir turi nepažeisti esamų serverių gamintojo licencijavimo taisyklių. – Licencijoms turi būti taikomas nurodytų serverių esamas gamintojo garantinis aptarnavimas, įskaitant aptarnavimo tipą ir esamą trukmę.
7.	Infrastruktūros saugumo sprendimo įdiegimas	Pateikiamas sprendimas turi būti įdiegtas ir perduotas Perkančiajai organizacijai eksploatuoti. Diegimo darbų kaina turi būti įskaičiuota į įrangos kainą. Diegiant sprendimą turi būti atlikti žemiau nurodyti darbai.
7.1.	Esamos situacijos analizė ir pasirengimas diegimui	Turi būti atlikti pasirengimo siūlomo sprendimo įdiegimui darbai, apimantys: – esamos IT infrastruktūros analizė; – architektūrinės schemos parengimas; – esamos fizinės ir loginės schemų pateikimas po atliktos analizės; – būsimos fizinės IT infrastruktūros schemos pateikimas; – būsimos loginės IT infrastruktūros schemos pateikimas.
7.2.	Sprendimo architektūros aprašymo dokumento parengimas	Turi būti pateiktas sprendimo architektūros aprašymo dokumentas, kuriame detaliai aprašomas sprendimas: – sprendimo architektūrinė schema; – loginė IT infrastruktūros schema, apimanti esamą įrangą ir perkamo sprendimo įrangą;

		– sprendimo funkcionalumo aprašymas; – detalizavimas, kaip diegimas sprendimas užtikrins atitinkamų informacijos apsaugos reikalavimų ypatingos svarbos informacinės infrastruktūros valdytojams atitikimą.
7.3.	Infrastruktūros parengimas saugumo sprendimo diegimui	Perkančiosios organizacijos IT infrastruktūrai parengti saugumo sprendimo diegimui turi būti atlikti toliau nurodyti darbai, parengtos saugumo sprendimui reikiamos Perkančiosios organizacijos IT infrastruktūros tarnybos.
7.3.1.	Centralizuotos naudotojų ir prieigos valdymo sistemos (CNPVS) parengimas	– Turi būti atlikti centralizuotos naudotojų ir prieigos valdymo sistemos (CNPVS) analizės, projektavimo, diegimo ir konfigūravimo darbai. – Analizė: o analizės etapo metu turi būti atlikta esamos CNPVS ir jos integracijų su kitomis sistemomis, tarnybomis ar įrenginiais analizė; – Projektavimas: o projektavimo etapo metu turi būti suprojektuota sistemos architektūra, jos konfigūracija ir administravimo modelis bei sudarytas CNPVS diegimo planas. Projektavimo etape taip pat turi būti atlikta: ▪ suprojektuota organizacinė struktūra; ▪ suprojektuota fizinė struktūra – valdikliai, vietovės, potinkliai; ▪ suprojektuota loginė struktūra – miškai, domenai, loginės organizacinės struktūros; ▪ suprojektuotas globalaus katalogo ir rolių paskirstymas; ▪ atliktas tikslaus laiko tarnybos planavimas; ▪ suprojektuoti sistemos aukšto patikimumo ir veiklos tęstinumo parametrai; ▪ suprojektuotos CNPVS objektų pavadinimų sudarymo taisyklės; ▪ suprojektuotas CNPVS valdymo teisių delegavimas; ▪ suplanuotas CNPVS testavimas; ▪ suprojektuoti CNPVS rezervinio kopijavimo, antivirusinės apsaugos sprendimai; ▪ suprojektuotas CNPVS pažeidžiamumų skanavimas ir valdymas; ▪ suprojektuotos CNPVS naujinimų politikos; ▪ suprojektuotos CNPVS įsilaužimų ir anomalijų prevencijos taisyklės; ▪ suplanuotas operacijų ir saugumo įrašų (angl. *logs*) valdymas; ▪ suplanuotas integravimas su kitais saugumo sprendimais (ugniasienės, e-pašto apsauga, PAM, SIEM/UEBA, NAC ir pan.); ▪ suplanuotas integravimas su esamomis aplikacijomis, sistemomis ar tarnybomis. – Diegimas: o diegimo etapo metu turi būti įdiegta ir sukonfigūruota CNPVS pagal paruoštą projektavimo dokumentą.

		– Testavimas: o testavimo etapo metu turi būti atliktas CNPVS funkcionalumo, saugumo ir parengties testavimas pagal paruoštą projektavimo dokumentą. – Stabilizavimas: o stabilizavimo etapo metu turi būti įvykdyta bandomoji eksploatacija ir atlikti galimų diegimo klaidų šalinimo darbai. – Įdiegtos CNPVS funkciniai reikalavimai: o turi būti realizuota naudotojų ir darbo vietų kompiuterių grupių, dalyvaujančių prieigos teisių valdyme, kūrimo galimybė; o turi būti realizuota paieškos funkcija, kuri leidžia greitai rasti ieškomus objektus; o turi būti realizuotas objektų filtravimas pagal norimą kriterijų; o turi būti realizuotas automatinis informacijos replikavimas tarp valdiklių; o turi būti realizuotas specializuotų teisių valdyti CNPVS objektus delegavimas; o turi būti realizuota prieigos teisių prie CNPVS objektų suteikimo ir šių teisių draudimo galimybė; o turi būti realizuota galimybė leisti arba drausti naudotojo prisijungimą prie kompiuterio su jo numatytąja paskyra; o turi būti realizuota galimybė peržiūrėti paskutinio interaktyvaus prisijungimo informaciją; o turi būti realizuota galimybė administratoriui nustatyti naują naudotojo prisijungimo prie kompiuterio slaptažodį, naudotojui jį pamiršus; o turi būti realizuota galimybė taikyti slaptažodžių saugumo politiką (slaptažodį turi sudaryti ne mažiau 8 simboliai ir pan.); o turi būti realizuota galimybė audituoti saugumo teisių panaudojimo atvejus; o CNPVS turi būti realizuota galimybė naudotojų atributų schemą plėsti papildomais atributais, kurie gali būti naudojami institucijos taikomosiose programose. Pvz. išplėsti schemą darbuotojo tabelio numeriu. – Įdiegtos CNPVS techniniai reikalavimai: o valdikliai turi būti diegiami fizinėse tarnybinėse stotyse ir/arba virtualiose terpėse panaudojant geriausias gamintojo praktikas; o CNPVS sistema turi būti įdiegta taip, kad klientų kompiuteriuose neturi būti darbui su ja skirtos papildomos klientinės programinės įrangos, kuri apkrauna kompiuterio resursus; o CNPVS sistema turi būti įdiegta dubliuojant tarnybos duomenų bazę. Dubliuotos bazės turi tarpusavyje sinchronizuotis ir esant vienos trikdžiams, kita tarnyba turi automatiškai perimti visos tarnybos darbą;

		○ CNPVS sistema turi būti įdiegta taip, kad tarnybos nustatymai būtų išplatinami į klientų kompiuterius nenaudojant tam skirtos papildomos programinės įrangos; ○ CNPVS turi būti suderinama užtikrinant vartotojų, kompiuterių ir serverių autentifikavimą su naudojamomis operacinėmis sistemomis Microsoft Windows 8/8.1/10, Microsoft Windows Server 2008R2/2012/2012R2/2016/2019 ir duomenų bazių valdymo sistemomis Microsoft SQL Server 2012/2014/2016/2017/2019. – CNPVS programavimo darbų metu turi būti įgyvendintas žemiau išvardintas funkcionalumas: ○ CNPVS turi siųsti priminimus naudotojams apie besibaigiantį slaptažodžio galiojimą elektroniniu paštu; ○ CNPVS turi nuskaityti duomenis iš personalo valdymo sistemos ir siųsti pranešimus nurodytiems administratoriams apie darbuotojo priėmimą arba atleidimą iš darbo. Pranešimas turi būti siunčiamas tą pačią dieną kai darbuotojo priėmimo ar atleidimo faktas yra įvedamas į personalo valdymo sistemą; ○ CNPVS turi būti įgyvendintas laikinos naudotojų narystės grupėse funkcionalumas: ▪ turi būti galimybė nustatyti narystės trukmę; ▪ praėjus nurodytam laikui, naudotojas turi būti automatiškai pašalinamas iš grupės ar grupių; ○ CNPVS turi būti įgyvendintas laikinos grupių narystės grupėse funkcionalumas: ▪ turi būti galimybė nustatyti narystės trukmę; ▪ praėjus nurodytam laikui, grupė turi būti automatiškai pašalinamas iš grupės ar grupių; ○ CNPVS turi būti įgyvendintas laikinų grupių funkcionalumas: ▪ turi būti galimybė nurodyti grupės gyvavimo trukmę; ▪ pasibaigus grupės gyvavimo laikui, grupė turi būti automatiškai pašalinama.
7.3.2.	Centralizuotos tapatybės valdymo sistemos (TVS) parengimas	– Turi būti atlikti centralizuotos tapatybės valdymo sistemos (TVS) analizės, projektavimo, diegimo ir konfigūravimo darbai, apimantys: ○ TVS turi būti nustatomas pirminis tapatybės duomenų šaltinis (prijungta sistema) kiekvienam naudotojo tapatybės duomenų vienetui. Pirminiu tapatybės duomenų šaltiniu laikomas toks šaltinis, kuris turi kokybiškiausią naudotojo tapatybės informaciją. Pirminiai tapatybės duomenų šaltiniai turės būti identifikuoti projekto analizės ir projektavimo etape; ○ kai naujas darbuotojas užregistruojamas Perkančiosios organizacijos pirminiame tapatybės duomenų šaltinyje, TVS turi susikurti pas save naują darbuotojo įrašą, nuskaitant visą reikalingą susijusią informaciją – vardą, pavardę, pareigas, tiesioginį vadovą ir kitus duomenis

		(jie turi būti suderinti projekto analizės ir projektavimo etape); ○ kai pirminiame tapatybės duomenų šaltinyje užregistruojamas darbuotojo atleidimas, TVS turi automatiškai panaikinti ar deaktyvuoti visą darbuotojo tapatybės informaciją iš prijungtų sistemų; ○ TVS turi automatizuoti naudotojų informacijos, saugomos prijungtose sistemose, keitimą; ○ pasikeitus pirminiame tapatybės duomenų šaltinyje naudotojo duomenims, TVS turi pakeitimą susinchronizuoti su kitomis prijungtomis sistemomis; ○ TVS turi užtikrinti, kad po TVS sinchronizavimo ciklo tapatybės informacija prijungtose sistemose atitiks TVS matomą informaciją; ○ TVS turi atpažinti tapatybės duomenų ar prieigos teisių pakeitimą prijungtose sistemose, atliktą ne TVS priemonėmis, ir atstatyti tapatybės duomenis bei prieigos teises iš TVS saugomos tapatybės informacijos; ○ laikinas TVS neveikimas neturi įtakoti esamų naudotojų galimybės prisijungti ir dirbti su prijungtomis Perkančiosios organizacijos sistemomis; ○ TVS privalo būti sujungta su CNPVS ir personalo valdymo sistema. – TVS turi automatiškai darbuotojui sukurti CNPVS naudotoją ir priskirti jam visus reikiamus atributus apie darbuotoją: vardą, pavardę, pareigas ir t.t. – Pagrindiniai reikalavimai TVS architektūrai bei techniniam sprendimui: ○ TVS turi būti įgyvendinta tapatybės valdymui skirto produkto pagrindu; ○ TVS privalo turėti plėtimui pritaikytą universalią architektūrą, leidžiančią prijungti naujas sistemas netrikdant TVS veikimo ir jau prijungtų sistemų darbo, nekeičiant architektūros bei naudotojų administravimo proceso; ○ TVS turi užtikrinti naudotojų tapatybės informacijos apsikeitimo tarp skirtingų sistemų konfidencialumą, saugumą ir vientisumą; ○ TVS turi palaikyti tokias deklaratyvias (neprogramuojamas) sinchronizavimo taisykles, kad bendruosiuose duomenyse būtų galima: ▪ darbuotojo tapatybės duomenų laukui priskirti skaitinę ar tekstinę konstantą; ▪ darbuotojo tapatybės duomenų laukui priskirti parametrą, perduotą sinchronizavimo taisyklei; ▪ darbuotojo tapatybės duomenų laukui priskirti kito lauko reikšmę; ○ TVS turi turėti galimybę programuoti taisykles, kurių negalima įgyvendinti deklaratyviai; ○ TVS turi turėti galimybę automatizuoti naudotojų tapatumo parametrų sinchronizaciją tarp skirtingų sistemų ir infrastruktūros resursų;

		○ turi būti galimybė pritaikyti ir adaptuoti TVS pagal esamus įstaigos saugumo reikalavimus ir tvarkas; ○ TVS turi turėti bendrąsias numatytas duomenų struktūras, reikalingas naudotojų prieigų ir kitų tapatumo duomenų saugojimui; ○ esant poreikiui turi būti galima plėsti bendrąją duomenų struktūrą, atsižvelgiant į prijungiamų sistemų duomenų struktūras; ○ TVS turi turėti galimybę rankiniu būdu susieti darbuotoją su prisijungiamos sistemos naudotoju, kai nėra tikslių taisyklių automatiniam susiejimui arba automatinis susiejimas įvyko nekorektiškai; ○ integracijos su prijungiamomis sistemomis agentų konfigūracija turi būti keičiama be papildomų programavimo darbų; ○ jei integracijos su prijungiamomis sistemomis agentų konfigūracija bus programuojama, visų integracijų agentų konfigūracija turi būti suprogramuota viena programavimo kalba, nepriklausomai nuo to, kokia technologija ar programavimo kalba programuota pati prijungiama sistema; ○ iš prijungiamų sistemų turi būti nuskaityti visi esami naudotojai, kurie atitinka nustatytus kriterijus; ○ jei prijungiama sistema turi galimybę leisti nuskaityti naudotojų ir jų prieigos teisių pasikeitimus (pvz. pridėtus naudotojus, suteiktas ar atimtas prieigos teises) nuo paskutinio integracijos agento prisijungimo, integracijos agentas turi galėti nuskaityti tik pakitusią, o ne visą tapatybės informaciją. – Funkciniai reikalavimai sistemų prijungimui: ○ į TVS sprendimą bus prijungtos personalo valdymo bei CNPVS sistemos; ○ reikalavimai diegimo platformai: ▪ TVS informacinė bazė turi veikti Perkančiosios organizacijos naudojamos Microsoft SQL Server duomenų bazės pagrindu arba kitos duomenų bazės pagrindu. Jeigu TVS įdiegti naudojama ne Microsoft SQL Server duomenų bazė, tuomet Tiekėjas turi pateikti visas TVS veikimui būtinas licencijas (pasiūlyme nurodyti gamintoją, produkto pavadinimą, komplektaciją); ▪ TVS komponentai turi dirbti Perkančiosios organizacijos naudojamoje 64 bitų platformoje; ▪ TVS komponentai turi būti diegiami Perkančiosios organizacijos turimose virtualiose tarnybinėse stotyse. TVS komponentų diegimas virtualioje aplinkoje turi būti palaikomas TVS gamintojo; ▪ Perkančiosios organizacijos užtikrina reikiamų diegimui virtualių resursų pateikimą Tiekėjui; ▪ TVS komponentai turi palaikyti aukšto patikimumo technologijas: • tinklo apkrovos paskirstymo (angl. *NLB*);

		• blokinio (angl. *clustering*); o saugos reikalavimai: ▪ administratoriaus teises turintys naudotojai TVS turi galėti matyti visus duomenis; ▪ slaptažodžiai neturi būti saugomi atviru tekstu; ▪ turi būti galimybė deleguoti TVS administravimo teises atskiriems naudotojams arba naudotojų grupėms; o TVS turi leisti atlikti rezervinį kopijavimą nenutraukiant TVS darbo; o reikalavimai įdiegimo darbams: ▪ Tiekėjas Perkančiosios organizacijos infrastruktūroje turi įdiegti TVS darbinėje ir testinėje aplinkose; ▪ testinėje aplinkoje TVS turi sinchronizuotis su testinėmis prijungiamų sistemų versijomis, darbinėje aplinkoje – su darbinėmis; ▪ Tiekėjas testinėje aplinkoje turi įdiegti TVS kūrimui, vystymui ir testavimui reikalingą programinę įrangą. – Analizė*:* o surinkti reikalavimus TVS; o tiksliai identifikuoti ir aprašyti integruojamas aplikacijas; o apibrėžti prieigų sukūrimo, panaikinimo ir sinchronizavimo taisykles; o apibrėžti reikalingas duomenų struktūras (integruojamų sistemų ir centralizuotos duomenų bazės); o nustatyti esamų aplikacijų pakeitimų poreikius; o paruošti sistemos testavimo planą. – Diegimas*:* o įdiegti TVS platformą testinėje ir gamybinėje aplinkoje; o sukurti ir sukonfigūruoti reikalingus integracijos su prijungiamomis sistemomis agentus testinėje ir gamybinėje aplinkoje; o realizuoti ir įdiegti tapatybės ir prieigų valdymo bei sinchronizavimo taisykles testinėje ir gamybinėje aplinkoje; o pajungti ir ištestuoti sistemų integraciją testinėje aplinkoje. – Stabilizavimas*:* ▪ įvykdyti bandomąją eksploataciją; ▪ atlikti galimų diegimo klaidų šalinimo darbus. – Jeigu centralizuotos tapatybės valdymo sistemos parengimui pagal aukščiau nurodytus reikalavimus tiekėjui bus reikalingos tam tikros programinės įrangos licencijos, tiekėjas jų kainą turi įskaičiuoti į pasiūlymo kainą. Pateikiamos licencijos turi būti nuolatinio galiojimo ir įsigyjamos (angl. *perpetual*), o ne pateikiamos nuomos ar panašiu teisiniu pagrindu ar kitaip laike apribotos, jų galiojimas privalo būti nuolatinis ir be pabaigos, nepriklausomai nuo to, ar Perkančioji organizacija įsigyja licencijų techninio aptarnavimo paslaugas. Taip pat tokiu atveju pasiūlyme turi būti aprašytas pateikiamos programinės įrangos licencijavimo modelis, nurodant

		išsamią informaciją apie licencijas ir licencijavimo sąlygas, licencijos apribojimus (pavyzdžiui, galiojimo laikas, duomenų ir transakcijų apimtys, programinės ir aparatinės įrangos plėtimas ir pan.).
7.3.3.	Vardų sprendimo tarnybos (DNS) parengimas	– Turi būti atlikti DNS tarnybos analizės, projektavimo, diegimo ir konfigūravimo darbai, apimantys: o esamos DNS infrastruktūros analizė; o esamos DNS tarnybos integracijų su kitomis sistemomis, tarnybomis ar įrenginiais analizė; o DNS architektūros projektavimas; o DNS konfigūracijos projektavimas; o suprojektuotos DNS diegimas ir konfigūravimas; o suprojektuotos DNS integravimas su reikiamomis sistemomis, tarnybomis ar įrenginiais. – Vardų sprendimo tarnybos funkciniai reikalavimai: o turi būti užtikrintas DNS nenutrūkstamas darbas; o turi būti užtikrintas naudotojams ir kitoms sistemoms tiek vidinio tinklo resursų, tiek ir internete esančių resursų vardų sprendimas; o atlikta integracija su CNPVS ir užtikrinta DNS replikacija CNPVS replikacijos priemonėmis; o DNS zonų nustatymuose įjungti saugūs naujinimai; o turi būti nustatyti DNS užklausų (angl. *DNS forwarder*) nukreipimo parametrai; o turi būti įjungtas pasenusių DNS įrašų automatinis valymas ir pašalinimas.
7.3.4.	Windows naujinimų tarnybos (WSUS) parengimas	– Turi būti atlikti Windows naujinimų tarnybos (WSUS) projektavimo, diegimo ir konfigūravimo darbai: o WSUS architektūros projektavimas; o WSUS konfigūracijos projektavimas; o suprojektuotos WSUS diegimas ir konfigūravimas. – Windows naujinimų tarnybos funkciniai reikalavimai: o turi būti nustatyti naujinimų sinchronizacijos šaltiniai ir jų prievadai; o turi būti nustatytas naujinimų sinchronizacijos grafikas su pagrindiniu naujinimų šaltiniu; o turi būti nustatyta galimybė pasirinkti naujinimų kalbos formatą priklausomai nuo organizacijoje naudojamų aplikacijų, sistemų ir pan.; o naujinimai turi būti suskirstyti pagal produktus ir klasifikatorius; o turi būti nustatytos kompiuterių, serverių grupės pagal operacinių sistemų versijas; o turi būti nustatytos naujinimų patvirtinimo taisyklės; o turi būti parengtos ir suderintos su Perkančiąja organizacija naujinimų platinimo taisyklės ir naujinimų platinimo grafikas; WSUS sistemoje turi būti sukonfigūruotas ataskaitų modulis. Modulis turi apimti ataskaitas apie naujinimų, kompiuterių ir naujinimų sinchronizacijos būseną.

7.3.5.	Virtualizavimo platformos aplinkų modifikavimas išskaidant į izoliuotas aplinkas ir pritaikant perkamam saugumo sprendimui	Reikalavimai paslaugų atlikimui virtualizavimo platformos modifikavimo ir pritaikymo perkamam saugumo sprendimui: – turi būti pateiktas ir suderintas esamos virtualizacijos infrastruktūros platformos aparatinės ir programinės įrangos atnaujinimo ir modifikavimo planas su Perkančiosios organizacijos atsakingais atstovais; – visų teikiamų paslaugų metu – atliekant aplinkų atskyrimą ir izoliavimą, duomenų šifravimą, virtualių serverių migravimą ir kt. paslaugas turi būti netrikdomas veikiančių sistemų darbas, jeigu būtų reikalingas laikinas sistemų stabdymas, jis turi būti suderintas ir atliekamas su Perkančiosios organizacijos atstovais suderintu laiku; – turi būti atnaujinta visa esama HPE SimpliVity virtualizacijos platforma, įskaitant HPE SimpliVity aparatinę ir programinę įrangą, virtualizacijos programinę įrangą, rezervinio kopijavimo programinę įrangą, avarinio atstatymo programinę įrangą ir kt. Sistemų atnaujinimas turi būti suderintas su Perkančiosios organizacijos atsakingais atstovais ir turi netrukdyti esamų sistemų darbo. Turi būti atnaujinta iki naujausių, stabiliai veikiančių, tarpusavyje suderinamų versijų; – naudojant esamą įrangą turi būti suformuotos dvi izoliuotos virtualizacijos platformos resursų aplinkos. Kiekviena izoliuota aplinka turi būti paskirstyta per du duomenų centrus, atskiriant į produkcinius ir avarinio atstatymo telkinius, taip sudarant galimybę veiklą automatizuotai atstatyti kitame duomenų centre esant vieno iš jų trikčiai; – turi būti įgyvendintas saugomų duomenų (angl. *data at rest*) šifravimas aparatiniame lygmenyje abiejuose izoliuotuose aplinkose, panaudojant siūlomą saugaus kriptografinių raktų valdymo sistemą. Atliekant šifravimą turi būti užtikrintas esamų virtualių serverių duomenų vientisumas; – turi būti pritaikytas esamas VMware vCenter aukšto patikimumo sprendimas infrastruktūrai taip, kad būtų užtikrintas VMware vCenter aukštas patikimumas vCenter HA principu (angl. *active/pasive*). Analogiškas sprendimas turi būti sukurtas abiem izoliuotoms aplinkoms; – turi būti atliktas virtualių serverių migravimas į modifikuotas, izoliuotas ir šifruotas aplinkas; – turi būti pritaikytas ir sukonfigūruotas esamas rezervinio kopijavimo ir avarinio atstatymo sistemos funkcionalumas abiejuose izoliuotose aplinkose veikiančioms sistemoms pagal suderintus reikalavimus su Perkančiosios organizacijos atstovais; – turi būti sukonfigūruota ir ištestuota serverių gedimų stebėsena ir pranešimų apie gedimus siuntimas įrangos gamintojui pagal Perkančiosios organizacijos pareikalavimą; – turi būti pateikta įrangos konfigūracijos ataskaita bei išpildomoji dokumentacija.
7.3.6.	Esamų sistemų perjungimas į	– Turi būti atlikti esamų sistemų analizės, perjungimo projektavimo ir konfigūravimo darbai, apimantys:

	saugumo sprendimo infrastruktūrą	○ esamų sistemų integracijų su kitomis sistemomis, tarnybomis ar įrenginiais analizė; ○ esamų sistemų, veikiančių Windows Server pagrindu, operacinių sistemų (OS) atnaujinimo galimybių analizė; ○ esamų sistemų naudojamų Microsoft SQL Server duomenų bazių tarnybų atnaujinimo galimybių analizė; ○ esamų sistemų kritiškumo ir leistino neveikimo laiko analizė; ○ esamų sistemų perjungimo į saugumo sprendimo infrastruktūrą plano sudarymas; ○ su Perkančiąja organizacija suderintų sistemų perjungimas į saugumo spendimo infrastruktūrą; ○ perjungtų sistemų konfigūravimas sklandžiam veikimui saugumo sprendimo infrastruktūroje. – Papildomi reikalavimai: ○ siekiant užtikrinti kuo didesnį sistemų atitikimą naujausiems saugumo standartams, jas perkeliant turi būti atnaujinamos ir sistemų naudojamų Windows Server operacinių sistemų versijos į naujausią sistemos palaikomą; taip pat turi būti atnaujintos sistemų naudojamos Microsoft SQL Server duomenų bazių tarnybų versijos į naujausią sistemos palaikomą; ○ perkeliant aukšto kritiškumo sistemas, sistemų darbas gali būti trikdomas ne daugiau kaip 1 val. su Perkančiąja organizacija suderintu metu; ○ perkeltos sistemos turi išlaikyti galimybę siųsti el. laiškus reikiamiems adresatams. – Microsoft SQL atnaujinimo reikalavimai: ○ Analizė: ▪ turi būti atliktas SQL Server infrastruktūros serverių naudojamų resursų patikrinimas; ▪ turi būti atliktas SQL Server infrastruktūros serverių versijų, vietovių ir autentifikavimo metodu patikrinimas; ▪ turi būti atliktas SQL Server infrastruktūros serverių duomenų bazių konfigūracijos patikrinimas; ▪ turi būti atliktas SQL Server infrastruktūros serverių užduočių, rezervinio kopijavimo ir kt. konfigūracijos patikrinimas; ▪ turi būti atliktas SQL Server serverių ar vietovių konsolidavimo įvertinimas; ▪ turi būti atliktas SQL Server infrastruktūros serverių 7 dienų greitaveikos rodiklių surinkimas ir pateikti apdorotų duomenų minimalios, vidutinės ir maksimalios reikšmės. ○ *Projektavimas*: ▪ turi būti atliktas projektavimo planavimas ir pateiktas projektavimo planavimo dokumentas, remiantis analizės metu pateiktomis išvadomis bei rekomendacijomis. SQL Server infrastruktūros diegimo, konsolidavimo, atnaujinimo planas turi būti suderintas su Perkančiąja organizacija.

		○ *Diegimas*: ▪ turi būti įdiegta aparatinė ir programinė įranga, realizuoti diegimo scenarijai, aprašyti projektavimo plane; ▪ turi būti atlikti SQL serverių duomenų bazių, naudotojų paskyrų, užduočių ir kitų objektų migravimo darbai. ▪ duomenų bazės sluoksnyje turi būti įdiegta ir sukonfigūruota, dinaminio duomenų maskavimo funkcija, ribojanti vartotojų prieiga prie jautrių organizacijos duomenų; ▪ turi būti realizuotas duomenų bazių šifravimas, užšifruojant duomenų bazių failus (mdf, log); ▪ visi sertifikatai, šifravimo raktai panaudoti realizuojant duomenų bazių šifravimo funkcionalumą turi būti patalpinti atskiroje išorinėje laikmenoje ir perduoti Perkančiajai organizacijai. ○ *Testavimas*: ▪ turi būti atliktas atnaujintų, konsoliduotų SQL Server serverių pasiekiamumo testavimas; ▪ sistemoms, kurioms diegimo metu buvo pritaikytos SQL Server aukšto patikimumo savybės, papildomai turi būti atliktas veiklos tęstinumo užtikrinimo testavimas; ▪ įvykdyti bandomąją eksploataciją; ○ *Stabilizavimas*: ▪ atlikti galimų diegimo klaidų šalinimo darbus.
7.4.	Laiko komponento įdiegimas saugumo sprendimui	Turi būti atlikti laiko komponento diegimo ir konfigūravimo darbai, apimantys: – IP adresų, SSH, SNMP, NTP, SYSLOG konfigūravimas; – RADIUS serverių IP konfigūravimas; – statinės ir dinaminės maršrutizacijos konfigūravimas; – LAG agreguotų sąsajų konfigūravimas; – VLAN konfigūravimas; – prievadų konfigūravimas; – laiko paslaugos serviso konfigūravimas; – programinės įrangos atnaujinimas iki naujausios gamintojo siūlomos versijos; – laiko serverių integravimas su Perkančiosios organizacijos esama ugniasienių įranga; – laiko serverių integravimas su esama Huawei WDM įranga; – laiko serverių integravimas su esama Perkančiosios organizacijos turima komutavimo įranga (50 vnt. HP 10500 serijos, 50 vnt. Cisco 9500 serijos, 50 vnt. HP 5820 serijos); – laiko serverių integravimas su Microsoft Active Directory, sertifikatų tarnybomis; – laiko serverių integravimas su saugumo informacijos ir įvykių valdymo sistema; – laiko serverių integravimas su privilegijuotų administratorių paskyrų valdymo sistema;

		– laiko serverių integravimas su esama Perkančiosios organizacijos virtualizacijos infrastruktūra; – laiko serverių montavimas į Perkančiosios organizacijos pateikiamas spintas; dviejuose duomenų centruose; – laiko serverių transportavimas į Perkančiosios organizacijos duomenų centrus.
7.5.	Kompiuterių apsaugos nuo kibernetinių grėsmių komponento įdiegimas	– Turi būti atlikti kompiuterių apsaugos nuo kibernetinių grėsmių komponento diegimo ir konfigūravimo darbai, apimantys: o sprendimo aktyvavimas gamintojo debesijos platformoje; o licencijų aktyvavimas; o administratorių rolių ir paskyrų konfigūravimas; o integracijos su katalogo tarnyba konfigūravimas (apima konfigūraciją tiek siūlomo sprendimo, tiek AD serverio); o agentų instaliavimas; o tarpinio serverio instaliavimas, jo funkcijų konfigūravimas; o agentų profilių konfigūravimas (ne mažiau 8 vnt.); o agentų konfigūravimas; o agentų grupių konfigūravimas (iki 10 grupių); o apsaugos profilių, išimčių konfigūravimas (iki 20 vnt.); o nežinomų vykdomųjų bylų siuntimo analizei į gamintojo smėliadėžę konfigūravimas; o SIEM pranešimų (angl. *alerts*) siuntimo konfigūravimas; o sprendimo pirminio lango (angl. *dashboard*) konfigūravimas pagal su Perkančiąja organizacija suderintus reikalavimus. – Agentų instaliavimas/konfigūravimas/apsaugos taisyklių pritaikymas turi būti atliktas dviem etapais: o testinis etapas – sprendimas pritaikomas testinei grupei - 10 agentų; o pagrindinis etapas – sprendimas pritaikomas likusiai agentų daliai.
7.6.	El. pašto apsaugos komponento įdiegimas	Turi būti atlikti el. pašto apsaugos komponento diegimo ir konfigūravimo darbai, apimantys: – esamos el. pašto paslaugos analizė; – el. pašto apsaugos platformos programinės įrangos diegimas, versijos atnaujinimas; – WEB izoliavimo platformos programinės įrangos diegimas, versijos atnaujinimas; – pradinis konfigūravimas (administratoriaus rolės, administratoriaus prieiga, DNS, NTP); – tinklo sąsajų konfigūravimas; – tinklo maršrutų konfigūravimas; – integracijos su AD konfigūravimas; – integracijos su O365 konfigūravimas (apima ir O365 dalį); – apsaugos politikų konfigūravimas skirtingiems vartotojams ar jų grupėms (ne mažiau 15 politikų); – apsaugos profilių konfigūravimas (ne mažiau 15 profilių); – el. pašto apsaugos platformos integracijos su WEB izoliavimo platforma konfigūravimas;

		– kliento turimų ugniasienių integracijos su WEB izoliavimo platforma konfigūravimas; – testavimas, problemų šalinimas.
7.7.	Privilegijuotos prieigos valdymo komponento įdiegimas	Turi būti atlikti privilegijuotos prieigos valdymo komponento diegimo ir konfigūravimo darbai, apimantys: – *Analizė:* o Perkančiosios organizacijos taikomų kibernetinio saugumo reguliacijų reikalavimų slaptažodžiams ir privilegijuotai prieigai analizė; o slaptažodžių politikos dokumento paruošimas arba esamo papildymas; o Perkančiosios organizacijos infrastruktūros ir tinklo analizė; o privilegijuotų paskyrų skanavimai ir rizikų analizė; o analizės rezultatų dokumentavimas. – *Projektavimas:* o sistemos aukšto patikimumo architektūros projektavimas dviejuose duomenų centruose; o sistemos projektavimas Perkančiosios organizacijos tinkle (loginė ir fizinė schemos); o sistemos naudotojų ir grupių projektavimas; – *Diegimas:* o sistemos programinės įrangos ir licencijų diegimas; o sistemos saugumo nustatymų sustiprinimas (angl. *security hardening*); o el. sertifikatų sutvarkymas; o sistemos integracija su Microsoft Active Directory; o aukšto patikimumo duomenų bazės valdymo sistemos telkinio sukūrimas ir testavimas; o portalo vartotojų integracija su dviejų faktorių autentifikavimu; o keturių akių principo sistemoje administravimo realizavimas; o sistemos katalogų struktūros projektavimas ir konfigūravimas pagal organizacijos specifiką, teisių dėliojimas; o sistemos vartotojų, grupių, darbo komandų projektavimas ir konfigūravimas; o vietovių ir aukšto patikimumo konfigūravimas; o el. pašto ir modifikuotų pranešimų konfigūravimas; o SSH proxy ir terminalo konfigūravimas; o atsarginių kopijų politikos sukūrimas ir konfigūravimas; o vaizdo įrašų politikos sukūrimas ir susijusių servisų konfigūravimas; o slaptažodžių politikų konfigūravimas; o sistemos rolių ir teisių projektavimas „mažiausiu privilegijų“ principu pagal Perkančiosios organizacijos poreikius; o privilegijuotų paskyrų šablonų modifikavimas ir testavimas pagal Perkančiosios organizacijos poreikius;

		○ nuotolinių slaptažodžių keitėjų konfigūravimas ir testavimas pagal Perkančiosios organizacijos poreikius; ○ modifikuotų powershell skriptų kūrimas pagal Perkančiosios organizacijos poreikį; ○ slaptažodžių, valdomų sistemų suvedimas ir pajungimas iki 1000 vnt.; ○ privilegijuotos prieigos politikos paruošimas (Perkančiajai organizacijai ir trečioms šalims); ○ darbo su sistema procesų ir scenarijų sukūrimas ir aprašymas pagal Perkančiosios organizacijos poreikius.
7.8.	Žurnalinių įvykių ir įrašų valdymo komponentų įdiegimas	– Turi būti atlikti žurnalinių įvykių ir įrašų valdymo komponentų SIEM, UEBA ir SOAR diegimo ir konfigūravimo darbai, apimantys: ○ komponentų techninės įrangos sumontavimą Perkančiosios organizacijos patalpose, nurodytoje komunikacinėje spintoje, parengimą darbui; ○ komponentų programinės įrangos parengimą darbui; ○ komponentų programinės įrangos versijų atnaujinimą; ○ komponentų įrangos konfigūravimo darbus, pilnai parengiant įrangą eksploatacijai, prijungiant su Perkančiąja organizacija suderintus duomenų šaltinius, ištestuojant įrangos veikimą pagal tiekėjo parengtą ir su Perkančiąja organizacija suderintą testavimo planą; ○ diegimo plano parengimas. Tiekėjo Perkančiajam subjektui pateiktame diegimo plane turi būti: ▪ detaliai įvardinti Perkančiojo subjekto tinklo segmentai bei nurodyti jų pavadinimai; ▪ numatytas žurnalinių įvykių surinkimas realiame laike iš sekančių techninių sistemų: • ugniasienių; • tinklo komutatorių, maršrutizatorių; • tinklo įrangos valdymo sistemos; • DNS; • DHCP; • Microsoft Active Directory; • visų Windows serverių; • visų Linux serverių; • Microsoft SQL; ▪ prijungti prie sistemos ne mažiau kaip 1000 vnt. duomenų šaltinių; ▪ sukonfigūruotos koreliacijos taisyklės ir kasdienės ataskaitos surinktų įvykių apdorojimui: • taisyklė, kuri realiame laike siųstų el. pašto pranešimą apie žurnalinių įvykių gavimo iš šaltinio nutrūkimą praėjus tam tikram laikui; • taisyklė, kuri realiame laike siųstų el. pašto pranešimą apie domeno vartotojui suteiktas domeno administratoriaus teises; • kasdieninė ataskaita, kuri parodytų praėjusią parą visas sukurtas ir/arba išjungtas, ir/arba panaikintas AD vartotojų paskyras;

		• kasdieninė ataskaita, kuri parodytų vidinių vartotojų jungimąsi ne darbo metu; • kasdieninė ataskaita, kuri parodytų nesėkmingų bandymų jungtis prie Perkančiosios organizacijos tinklo įrangos; • kasdieninė ataskaita, kuri parodytų sėkmingų / nesėkmingų prisijungimų prie VPN sistemos; • kasdieninė ataskaita, kuri parodytų visus sėkmingus / nesėkmingus prisijungimus prie ugniasienių, kompiuterinio tinklo komutatorių valdymo IP adresų; • mažiausiai po 10 (dešimt) papildomai naujai sukonfigūruotos koreliacijos taisykles. – Perkančiosios organizacijos atstovams patvirtinus diegimo planą, Tiekėjas atlieka diegimą pagal suderintą grafiką ir perduoda įdiegtą įrangą Perkančiajai organizacijai eksploatuoti.
7.9.	Saugaus kriptografinių raktų valdymo sistemos komponento įdiegimas	Turi būti atlikti saugaus kriptografinių raktų valdymo sistemos komponento diegimo ir konfigūravimo darbai, apimantys: – saugaus kriptografinių raktų valdymo sistemos komponento aparatinės įrangos montavimas dviejuose duomenų centruose, jų mikrokodo atnaujinimas, kabelių žymėjimas, VMware virtualizavimo diegimas ir konfigūravimas; – virtualių saugaus kriptografinių raktų valdymo sistemos serverių diegimas; – raktų serverių bazinių nustatymų konfigūravimas (IP adresai, potinklio kaukės, vardai, tinklo tarnybos, DNS nustatymai, laiko nustatymai ir kt.); – sertifikatų tarnybos (angl. *CA*) paruošimas; – serverio ir susijusių el. sertifikatų paruošimas; – raktų valdymo serverio aukšto patikimumo telkinio paruošimas; – raktų valdymo tarnybų (OASIS KMIP), skirtų klientams, paruošimas; – paskyrų sukūrimas, paslaugų klientams; – raktų sukūrimas ir priskyrimas klientams; – sukonfigūruotos raktų serverių sistemos nustatymų ir raktų periodinės rezervinės kopijos konfigūravimas ir testavimas.
7.10.	Dokumentacijos pateikimas	Pabaigus nurodytus Infrastruktūros saugumo sprendimo įdiegimo darbus (tiek pasirengimo diegimui, tiek sprendimo diegimo) turi būti pateikta atliktų darbų dokumentacija ir pateiktos infrastruktūros schemos, techninės bei programinės įrangos nustatymai: – susijusios IT infrastruktūros esamos fizinės ir loginės schemos; – įdiegto sprendimo principinio veikimo schemos; – įdiegto sprendimo įrangos konfigūracijos; – įdiegto sprendimo įrangos dokumentacija.
8.	IT infrastruktūros saugumo patikrinimas po	– Turi būti atlikti infrastruktūros saugumo patikrinimo darbai, apimantys:

	duomenų tinklo saugumo sprendimo įdiegimo	○ turi būti nustatytos naudojamos AD ir Windows technologijos, protokolai; ○ turi būti pateiktos rekomendacijos dėl jų naudojimo ir tinkamumo. Nurodoma, kuo pakeisti ar kaip išjungti; ○ turi būti nustatyti AD kredencialų ir Windows lokalių kredencialų trūkumai; ○ turi būti patikrintas visų AD slaptažodžių stiprumas ir atsparumas parinkimui; ○ turi būti patikrintos Kerberos protokolo problemos; ○ turi būti išanalizuotos slaptažodžių politikoms eiliniams vartotojams ir administratoriams; ○ turi būti patikrintas slaptažodžių politikų atitikimas reguliacijų reikalavimams; ○ turi būti nurodytos geriausių praktikų rekomendacijos slaptažodžių politikoms; ○ turi būti nustatyti pasitikėjimo ryšiai ir tipai tarp AD miškų ir domenų; ○ pateikiamos rekomendacijos saugiai architektūrai; ○ nurodytos priemonės ir rekomendacijos šių ryšių saugumui užtikrinti; ○ turi būti patikrintos problemos domeno lygyje (prieinami kredencialai eiliniams domeno vartotojams, anoniminės užklausos, klaidinga konfigūracija ir kt.); ○ turi būti patikrintos problemos domeno kontroleriuose (kritinių atnaujinimų trūkumas, klaidinga konfigūracija, perteklinės paslaugos ir kt.); ○ turi būti patikrintos problemos prie domeno prijungtose kompiuterinėse darbo vietose (kritinių atnaujinimų trūkumas, klaidinga konfigūracija, nesaugūs protokolai, lokalūs kredencialai ir kt.); ○ turi būti patikrintos privilegijų, paskyrų ir grupių problemos; ○ turi būti nustatyti neatitikimai AD gerosioms saugumo praktikoms; ○ atsparumas AD ilgalaikiam įsitvirtinimui ir dominavimui; ○ pateikiamos išvados ir rekomendacijos; ○ kiti testai pagal tiekėjo naudojamą metodiką. – Bevielio tinklo įsiskverbimo patikrinimas: ○ tikrinama ar naudojamas bevielis tinklas (sankcionuotas ar nesankcionuotas), jo autorizavimo priemonės, galimybė gauti prieigą; ○ nustatyti bevielės prieigos taškus ir taškas-taškas (angl. *ad-hoc*) sujungimus radijo erdvėje pastato viduje ir aplink jį, SSID rezultatus atvaizduoti ortofoto nuotraukoje; ○ nustatyti naudojamas bevieles komunikacijas; ○ nustatyti dažnius sklindančius iš taikinio/objekto; ○ patikrinti ar yra neautorizuotų/nesankcionuotų bevielės prieigos taškų; ○ patikrinti naudojamus klientų autentifikacijos metodus; ○ patikrinti naudojamus šifravimo metodus; ○ patikrinti naudojamus raktų ilgius;

		○ turi būti patikrinta galimybė perimti, dešifruoti 802.11 bevielio tinklo duomenų srautą. Esant tokiai galimybei, turi būti išanalizuota jame perduodami duomenys, ieškant jautrios informacijos (slaptažodžiai, konfidencialūs dokumentai ir kt.); ○ patikrinti IP adresų erdves pasiekiamas iš bevielio tinklo; ○ atlikti bevielio tinklo įsilaužimo veiksmus. – Socialinės inžinerijos testai duomenims išgauti: ○ atliekamas socialinės inžinerijos testas naudojant elektroninį paštą. Testo tikslas išprovokuoti vartotoją atlikti veiksmus, kurie gali būti potencialiai žalingi IT infrastruktūrai, ar pateikti riboto naudojimo informaciją; ○ turi būti paruoštas tikslinis atakos turinys. Tiksliniam atakos turiniui keliami šie reikalavimai: turi apeiti visas naudojamas apsaugos priemones (el. pašto šliuzus, antivirusines, įsilaužimų prevencijos sistemas, ugniasienes, web šliuzus ir kt.), turi leisti interaktyviai valdyti aukos sistemą apvalkalo lygyje (angl. *shell*), turi demonstruoti slaptumą tinkle (angl. *network beacons*) principu, turi vykdyti poįsilaužiminius veiksmus (privilegijų eskalavimas, tuneliavimas, kredencialų vagystė), turi būti lengvai pašalinamas iš aukos kompiuterio be jokių likutinių pasekmių; ○ sėkmingo testo atveju turi būti bandoma gauti prieigą prie papildomų vidinių sistemų, tokių kaip domeno kontroleriai, bylų, duomenų bazių, valdymo ir atsarginių kopijų serveriai; ○ visa atakos strategija, taikiniai, turinys, laikas, ir kita turi būti derinami su atsakingais Perkančiosios organizacijos darbuotojais. Turi būti fiksuojamas pilna atakos turinio elgsena ir pateikiama išsamioje ataskaitoje. – Išorinio kompiuterinio tinklo perimetro įsiskverbimo patikrinimas: ○ išorinio kompiuterinio tinklo perimetro patikrinimas atliekamas turint minimalias žinias apie Perkančiosios organizacijos IT infrastruktūrą imituojant potencialaus įsilaužėlio iš interneto veiksmus): ▪ informacijos apie tiriamą objektą surinkimas iš viešai prieinamų šaltinių: interneto paieškos portalų, forumų, DNS (Domain Name Service) tarnybų ir oficialių interneto valdymo institucijų (RIPE, Domreg ir pan.); ▪ perimetro tinklo mazgų, pasiekiamų iš interneto nustatymas; ▪ perimetro tinklo mazguose veikiančių OS (operacinių sistemų) nustatymas ir atitinkamų, šiai dienai žinomų, pažeidžiamumų patikrinimas; ▪ perimetro tinklo mazguose veikiančių tarnybų nustatymas ir atitinkamų, šiai dienai žinomų, pažeidžiamumų patikrinimas, bei konfigūracijos analizė (papildomos informacijos apie sistemą

		surinkimas per klaidų, sisteminius pranešimus, servisų programinę realizaciją); o nustačius pažeidžiamumus atliekamas įsilaužimo testas; o jei aptinkama iš interneto pasiekiamų tarnybų, reikalaujančių vartotojo autentifikacijos, tuomet atliekamas išorinės paslaugos slaptažodžių auditas. Tikrinama ar naudojami patikimi slaptažodžiai, ar įmanoma juos atspėti arba parinkti. – Web aplikacijų įsilaužimo testavimas: o turi būti atliktos WEB aplikacijų įsilaužimo testavimo paslaugos; o turi būti atliktas WEB aplikacijų taikomųjų programų ir paslaugų saugumo patikrinimas neturint naudotojo prisijungimo ir turint prisijungimus; o informacijos apie sistemas surinkimas (informacija apie sistemą, periferines/pagalbines sistemas) ir testavimo ribų nustatymas; o tinklo mazguose veikiančių tarnybų nustatymas ir atitinkamų, šiai dienai žinomų, pažeidžiamumų patikrinimas, bei konfigūracijos analizė (papildomos informacijos apie sistemą surinkimas per klaidų, sisteminius pranešimus, servisų programinę realizaciją); o naudojamų technologijų identifikavimas (platforma, programavimo metodai ir priemonės); o serviso konfigūracijos patikrinimas (darbinės direktorijos pakeitimas, serviso teisių eskalavimas, informacijos atskleidimas per klaidų pranešimus); o pažeidžiamumų paieška (vartotojo autentifikavimo mechanizmo patikrinimas, sesijos vientisumo patikrinimas, įvedamos informacijos apdorojimo patikrinimas, programinio kodo integralumo patikrinimas, klaidų pranešimų apdorojimas, sisteminės informacijos atskleidimas, serviso konfigūravimo klaidos) automatizuotais WEB pažeidžiamumo skeneriais; o automatizuotos paieškos rezultatų patikrinimas; o rankinis pažeidžiamumų remiantis „OWASP testing guide“ metodikos punktais patikrinimas. – Elgesio taisyklės testavimo metu: o draudžiama kopijuoti bet kokio tipo programinę įrangą į audituojamų mašinų kietuosius diskus; o audito metu draudžiama skanuoti tinklo prievadus (tiek TCP, tiek UDP); o draudžiamas automatizuotas pažeidžiamumų skanavimas; o vykdomi audito metu testai turi nekelti apsaugos sistemose pranešimų (angl. *alert*); o auditas vykdomas neturint jokių teisių ar paskyrų AD ir Windows aplinkose. – Įsiskverbimų ataskaitos parengimas: o tikrintų objektų aprašymas; o patikrinimo tikslai ir eiga;

		○ aprašomos aptiktos spragos, pateikiami įrodymai (pridėti ekrano vaizdai su įrodymais) ir pašalinimo rekomendacijos; ○ pateikiamas įsilaužimo scenarijus – detaliai aprašyta veiksmų seka kaip išnaudoti vieną ar kitą saugumo trūkumą (pateikiamas tik esant technologiniam pažeidžiamumui); ○ po visų audito etapų turi būti parengta ir pateikta ataskaita. Ataskaita pateikiama lietuvių kalba MS Word ir PDF formatuose Ataskaitos pradžioje turi būti pateikta apibendrinanti lentelė su visais reikalavimuose išvardintais punktais (tikrintomis tarnybomis, technologijomis), prie kiekvieno iš jų turėtų būti aprašyta būklė: pažeidžiamumų nerasta, netaikytina ar aptikti pažeidžiamumai. Toliau turi būti pateikta informacija iš informacijos surinkimo etapo ir aptiktų pažeidžiamumų aprašymas. Informacijos surinkimo etapo metu surinkta informacija turi būti susisteminta pagal aptiktus duomenis ir jų šaltinius, turi būti pateiktos rekomendacijos dėl perteklinės informacijos šalinimo. Pažeidžiamumo aptikimo atveju, jis turi būti aprašomas ataskaitoje, pateikiamas realus jo išnaudojimo pavyzdys (jei įmanoma, su kodu reikalingu jam įvykdyti), pateikiamas galimas sprendimo būdas. Turi būti įvertinta kiekvieno aptikto pažeidžiamumo ar pavojaus rizika, atsižvelgiant į tai, kokie duomenys gali būti sugadinti ar suklastoti, kokią įtaką tai gali turėti tinklapio veikimui. Pažeidžiamumas turi būti vertinimas trimis lygiais: „žemas“, „vidutinis“ ir „aukštas“: ▪ žemo lygio rizika reiškia, kad pažeidžiamumas yra nedidelis. Tokiu lygiu įvertinami dažniausiai papildomos informacijos suteikiantys pažeidžiamumai; ▪ vidutinio lygio rizika reiškia, kad šiai dienai dar nėra sukurtų automatinių ir viešai prieinamų pažeidimą išnaudojančių programinių priemonių, bet jis yra žinomas ir gali būti panaudotas atitinkamas žinias turinčių asmenų. Taip pat šiam lygiui priskiriami pažeidžiamumai, kurių pavojingumas gali priklausyti ir nuo kitų faktorių (pvz., organizacijoje dirbančių asmenų) arba kurių išnaudojimui nepakanka vien tik specifinių techninių žinių ir tinkamos įrangos; ▪ aukšto lygio rizika reiškia, kad pažeidžiamumais galima nesunkiai pasinaudoti ir jais galima padaryti žalą arba išgauti svarbią informaciją. Taip pat šiam lygiui priskiriami pažeidžiamumai, kuriems jau būna sukurtos automatinės įsiskverbimo priemonės ir kuriomis norint pasinaudoti nebūtinos specifinės žinios. Tokie pažeidžiamumai, kuriais gali pasinaudoti asmenys, net ir neturintys specifinių žinių, yra vieni pavojingiausių;

		○ taip pat turi būti įvertinta kiekvieno aptikto pažeidžiamumo ar pavojaus išnaudojimo galimybė, atsižvelgiant į tai, kokiu būdu jis galėtu būti išnaudojamas: ▪ nuotoliniu būdu; ▪ iš vietinio tinklo; ▪ tik turint fizinę prieigą; ○ detali rekomendacija – pateikiamas detalus planas nustatytų rizikų mažinimui, pažeidžiamumų taisymui bei silpnųjų vietų stiprinimui; ○ rekomendacijos prevencijai – gerųjų praktikų, sistemų kūrimo gairių, kurios padėtų išvengti dažniausiai daromų saugumo klaidų, pateikimas ar pristatymas.

_____