ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS LICENCIJŲ PIRKIMO TECHNINĖ SPECIFIKACIJA

1. PIRKIMO OBJEKTAS

1.1. Antivirusinės programos licencijos, BVPŽ kodas 48000000-8 (toliau – Prekės/prekės).

1.2. Pirkimo objekto apimtys. Sutarties galiojimo laikotarpiu (įskaitant visus galimus jos pratęsimus, jei tokia galimybė nustatyta Sutartyje) planuojamas įsigyti kiekis (apimtis):

Eil. Nr.	Pavadinimas	Kiekis (apimtis)	Matavimo vnt.
1.	Antivirusinės programinės įrangos licencijos	2000	vnt.

2. PIRKIMO OBJEKTO PRITAIKYMO SRITIS

2.1 Valstybės įmonė Valstybinių miškų urėdija (toliau – Pirkėjas) šiuo pirkimu siekia pratęsti /įsigyti programinės įrangos licencijas kompiuterinių darbo vietų, serverių, apsaugos nuo virusų ir šnipinėjimo programų, su ugniasiene ir pašto paslauga bei apsauga nuo elektroninių šiukšlių bei programinės įrangos veikimo techninio palaikymo ir kibernetinės saugos paslaugas 3 metų laikotarpiui.

3. TECHNINIAI REIKALAVIMAI, KURIUOS TURI ATITIKTI PERKAMOS PREKĖS

3.1. Pirkėjas numato pirkti licencijas užtikrinančias Pirkėjo kompiuterizuotų darbo vietų (toliau – darbo vietos), serverių apsaugą nuo virusų ir įsilaužimų, apsaugančią elektroninio pašto sistemą nuo nepageidaujamų elektroninių laiškų 3 metų laikotarpiui. Visi programinės įrangos sprendimai privalo būti valdomi iš vienos administravimo konsolės.

3.2. Licencijos turi pradėti galioti nuo 2025 m. sausio 1 d. 3 (trijų) metų laikotarpiui su techniniu palaikymu.

3.3. Visą antivirusinės programos licencijų galiojimo laikotarpį turi būti užtikrintas įsigytų prekių naujų versijų parsisiuntimas be apribojimų tiesiai iš gamintojo svetainės, nesikreipiant į gamintojo partnerius ir/ar atstovus.

3.4. Visą antivirusinės programos licencijų galiojimo laikotarpį turi būti užtikrintos galimybės Pirkėjui nemokamai kreiptis tiesiogiai į prekių techninio palaikymo centrą ir neatlygintinai gauti jų teikiamas paslaugas.

3.5. Licencija turi suteikti teisę siūlomą antivirusinę programinę įrangą naudoti bet kurioje Pirkėjo įrengtoje kompiuterinėje darbo vietoje/serveryje ar nešiojamame kompiuteryje.

3.6. Visa siūloma programinė įranga turi būti vieno gamintojo.

3.7. Pirkimo objektas turi atitikti šiuos reikalavimus:

Eil. Nr.	Parametras	Minimali reikšmė
1.	Licencijų skaičius	2000 vnt.
2.	Programinės įrangos tipas	Kompiuterinių darbo vietų ir serverių, apsauga nuo virusų ir šnipinėjimo programų, su ugniasiene ir pašto apsauga. Centralizuotas darbo vietų kietųjų diskų šifravimas. Papildoma apsauga nuo išpirkos reikalaujančių kenkėjų ir nulinės dienos atakų su debesyje valdoma smėliadėžės technologija. Kompiuterinių darbo vietų ir serverių ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo programinė įranga su centralizuotu valdymu (angl. *Extended Detection and Response, XDR*). Visi programinės įrangos sprendimai privalo būti valdomi iš vieno gamintojo administravimo konsolės(-ių).
3.	Programinės įrangos gamintojas	Turi būti nurodytas programinės įrangos gamintojas. Siekiant visapusiško suderinamumo vykdant centralizuotą stebėseną ir valdant visas išplėstines antivirusinės infrastruktūros apsaugos sistemas, visi pateikti apsaugos nuo virusų, apsaugos nuo el.

		šiukšlių, kietųjų diskų šifravimo produktai, smėliadėžė debesyje ir įrenginių ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo programinė įranga turi būti pagaminta to paties gamintojo.
4.	Programinės įrangos paketo pavadinimas	Turi būti nurodytas. Visi pateikti apsaugos nuo virusų, apsaugos nuo el. šiukšlių produktai turi būti pagaminti to paties gamintojo.
5.	Palaikomos operacinės sistemos antivirusinei apsaugai	Kompiuterinės darbo vietos: *Microsoft Windows 11 32-bitų ir 64-bitų.* *Microsoft Windows 10 32-bitų ir 64-bitų.* *macOS 10.12 ir naujesnės.* *Ubuntu Desktop 18.04 LTS 64-bitų.* *Ubuntu Desktop 20.04 LTS.* *Ubuntu Desktop 22.04 LTS.* *Red Hat Enterprise Linux 7, 8 su įdiegta palaikoma darbalaukio aplinka.* *SUSE Linux Enterprise Desktop 15.* *Linux Mint 20.* Windows serveriai: *Microsoft Windows Server 2022 (Server Core ir Desktop Experience).* *Microsoft Windows Server 2019 (įskaitant Server Core, Desktop Experience ir Essentials).* *Microsoft Windows Server 2016 (įskaitant Server Core, Desktop Experience, Storage Server ir Essentials).* Linux serveriai: *RedHat Enterprise Linux (RHEL) 7, 8 ir 9 versijos ir naujesnės.* *CentOS 7 versijos ir naujesnės.* *Ubuntu Server 18.04 LTS, 20.04 LTS ir 22.04 LTS versijos.* *Debian 10 ir 11 versijos ir naujesnės.* *SUSE Linux Enterprise Server (SLES) 12 ir 15 versijos ir naujesnės.* *Oracle Linux 8 versijos ir naujesnės.* *Amazon Linux 2 versijos ir naujesnės.* Turi būti palaikomos virtualios aplinkos: *Microsoft Hyper-V Server 2012 ir naujesnė.* *VMware vSphere/ESXi 6.5 ir naujesnė.* *VMware Workstation 9 ir naujesnė.* *VMware Player 7 ir naujesnė.* *Oracle VirtualBox 6.0 ir naujesnė.* *Citrix 7.0 ir naujesnė.* Sprendimas su VMware ESXi turi palaikyti VMware Horizon 7.x ir 8.0 versijas. Nuotolinio administravimo konsolė turi palaikyti diegimą į: *Microsoft Windows Server 2016 64-bitų.* *Microsoft Windows Storage Server 2016 64-bitų.* *Microsoft Windows Server 2019 64-bitų.* *Microsoft Windows Server 2022 64-bitų.* *Linux: RHEL, Debian, Ubuntu, SLED, SLES, OpenSUSE, Fedora ir CentOS bei dauguma kitų RPM ir DEB paketų valdymu pagrįstų platinamų programų.*

		Nuotolinė administravimo konsolė turi būti suderinama su naršyklėmis: • *Mozilla Firefox.* • *Microsoft Edge.* • *Google Chrome.* • *Opera.* • *Safari.*
6.	Palaikomos operacinės sistemos ir duomenų bazės ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo programinei įrangai	Kompiuterinės darbo vietos: *Microsoft Windows 10 32-bitų ir 64-bitų.* *Microsoft Windows 11 32-bitų ir 64-bitų.* *macOS 10.15 (Catalina) ir naujesnės versijos.* *RedHat Enterprise Linux (RHEL) 7 versijos.* *RedHat Enterprise Linux (RHEL) 8 versijos.* *Ubuntu 18.04, 20.04 ir 22.04 versijos.* *SUSE Linux Enterprise Desktop 15 versijos.* *Linux Mint 20 versijos.* Serveriai: *Microsoft Windows Server 2016 64-bitų.* *Microsoft Windows Server 2019 64-bitų.* *Microsoft Windows Server 2022 64-bitų.* *RedHat Enterprise Linux (RHEL) 7, 8 ir 9 versijos.* *Centos 7 versijos.* *Ubuntu 18.04, 20.04 ir 22.04 versijos.* *Debian 10 ir 11 versijos.* *SUSE Linux Enterprise Server (SLES) 12 ir 15 versijos.* *Oracle Linux 8 versijos.* *Amazon Linux 2 versijos.* Nuotolinio administravimo konsolė turi palaikyti diegimą į: *Microsoft Windows Server 2016 64-bitų.* *Microsoft Windows Server 2019 64-bitų.* *Microsoft Windows Server 2022 64-bitų.* Nuotolinio administravimo konsolė turi palaikyti duomenų bazes: *MySQL 5.7.43 ir naujesnes.* *MySQL 8.0.34 ir naujesnes.* *MySQL 8.1 ir naujesnes.* *Microsoft SQL Server 2017 ir naujesnes.* Web administravimo konsolė turi būti suderinama su naršyklėmis: *Mozilla Firefox.* *Google Chrome.* *Safari.* *Microsoft Edge.*
7.	Veikimo kokybės reikalavimai	Programinės įrangos gamintojas turi turėti bent ISO 9001:2015 ir ISO 27001:2013 arba lygiaverčius standartus atitinkančias sertifikacijas. Gamintojas turi būti įvertintas „TOP Player“ įvertinimu 2022 metų “Radicati Advanced Persistent Threat Market Quadrant” rinkos tyrime. Gamintojas turi būti įvertintas/sertifikuotas „Advanced Threat Protection Test 2023 – Enterprise - AV comparatives“ tyrime. Gamintojas turi būti įvertintas/sertifikuotas „Endpoint Prevention & Response (EPR) Test 2023 - AV Comparatives“ tyrime. Kibernetinių grėsmių aptikimo analizė turi būti pagrįsta pagal MITRE ATT&CK® metodologiją.

8.	Administravimo konsolės(-ių) diegimas	Gamintojas turi pateikti bent tris skirtingus administravimo konsolės(-ių) diegimo formatus: - Viskas viename. - Įdiegimas pagal programos komponentus. - Virtuali mašina. Turi būti galimybė administravimo konsolę apsaugoti dviejų veiksnių autentifikacijos (angl. *Two Factor Authentication*) apsaugos sluoksniu.
9.	Diegimo metodai	Kompiuterinėms darbo vietoms turi būti galimybės: - Įdiegti programinę įrangą centralizuotai iš valdymo konsolės. - Įdiegti programinę įrangą lokaliai iš diegimo laikmenos. - Įdiegti programinę įrangą per *Active Directory Group Policy* nustatymus.
10.	Būtini kompiuterinių darbo vietų apsaugos funkciniai moduliai	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų, grėsmių. Įsilaužimų prevencijos modulis (HIPS). Išorinių laikmenų apsaugos modulis. Galimybė atstatyti užkrėstą kompiuterį į ankstesnę būseną. Įsilaužimų blokatorius. Ugniasienė. Kietųjų diskų šifravimo modulis. Saugios naršyklės modulis. Sprendimas turi leisti pasirinkti, kuriuos apsaugos modulius aktyvuoti.
11.	Funkciniai reikalavimai kompiuterinių darbo vietų antiviruso moduliui	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų; Sprendime turi turėti tokias nuskaitymo parinktis: - Išmanusis nuskaitymas. - Kontekstinio meniu nuskaitymas. - Giluminis nuskaitymas. - Prie kompiuterio prijungtų išorinių laikmenų nuskaitymas (pvz. CD/DVD/USB). Galimybė vykdyti euristinį (angl. *heuristic*) nežinomų failų skenavimą. Galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo bei išdiegimo. Ugniasienės modulis – programinė įranga, sauganti nuo įsilaužimų. Apsaugos nuo elektroninių šiukšlių modulis (*Anti-SPAM*). Turi būti galimybė valdyti šiuos įrenginius: disko atminties įrenginius, CD/DVD, USB spausdintuvus, *FireWire* saugyklas, *Bluetooth* įrenginius, lustinių kortelių skaitytuvus, vaizdavimo įrenginius, modemus, LPT/COM prievadus, nešiojamuosius įrenginius. Sprendimas turi leisti/neleisti naudoti įrenginius pagal šiuos kriterijus: tiekėjas, modelis, serijinis numeris. Saugojimo įrenginiams sprendimas turi leisti nustatyti šiuos naudojimo leidimus: skaityti/rašyti, blokuoti, tik skaityti, įspėti. Įsilaužimų prevencijos modulis (HIPS) turi turėti šiuos režimus: automatinis, išsamusis, interaktyvusis, politika pagrįstas, mokymosi. Galimybė riboti prieigą prie internetinių šaltinių. Turi būti integruota saugi naršyklė. Turi būti WMI ir viso registro nuskaitymas. Turi būti galimybė grafinę vartotojo sąsają pasirinkti lietuvių kalba. Kompiuterinių darbo vietų antivirusinės programos dokumentacija turi būti pateikta lietuvių kalba.

12.	Funkciniai reikalavimai darbo vietų ugniasienei	Turi apsaugoti nuo nepageidaujamų tinklo išorinių atakų, pagal nustatytus kriterijus (pagal prievadus (angl. *port*), programas) ribojant atakos šaltinio prieigą. Ugniasienė turi leisti/neleisti prisijungti, remiantis bet kuriuo iš šių režimų: automatinis, interaktyvus, politika pagrįstas, mokymosi. Turi būti apsauga nuo *brute-force* atakų. Darbo vietų ugniasienės valdymas turi būti atliekamas centralizuotai antivirusinės apsaugos administravimo konsolės pagalba.
13.	Funkciniai reikalavimai valdymo konsolei	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Serveris turi bendrauti su galiniais įrenginiais per agentą, kuris gali saugoti politiką ir vykdyti užduotis, kol įrenginys yra neprisijungęs. Serveris turi leisti pridėti įrenginius prie valdymo konsolės naudojant šiuos metodus: - sinchronizavimas su *Active Directory*; - rankiniu būdu įvedus įrenginio vardą arba IP adresą; - patentuota technologija, gebanti aptikti įrenginius tinkle; Serveris turi leisti įdiegti saugumo sprendimus nuotoliniu būdu ir be vartotojo įsikišimo. Serveris turi leisti kurti statines ir dinamines grupes paprastesniam įrenginių administravimui. Serveris turi leisti nuotoliniu būdu vizualizuoti šią įrenginių informaciją: - pagrindinė informacija; - konfigūracija; - atliktos užduotys; - įdiegtos programos; - perspėjimai; - karantinas. Turi turėti centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams. Turi būti centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo. Turi turėti funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies konfigūracinius nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį. Turi turėti antrinio nuotolinio administravimo serverio nustatymo galimybę – nustojus veikti vienam nuotolinio administravimo serveriui, administravimas automatiškai turi pereiti kitam nuotolinio administravimo serveriui. Turi turėti galimybę paveldėti taisykles (angl. *policies*) iš aukštesnio lygio nuotolinio administravimo serverio. Turi būti užtikrinta galimybė siųsti informacinius pranešimus į visų rūšių įrenginius, įskaitant serverius ir kompiuterines darbo vietas. Serveris turi leisti apibrėžti aktyviklį, kuris įvykdytų numatytą veiksmą, kai tam tikras įvykis įvyksta tinkle. Pagal numatytuosius nustatymus serveris turi pateikti keletą standartinių ataskaitų bei leisti kurti naujus ataskaitų šablonus. Turi būti galimybė ataskaitas automatiškai gauti el. paštu arba generuoti valdymo konsolėje. Interneto konsolės sąsaja turi dirbti su informacijos skydais. Jie turi būti visiškai interaktyvūs ir leisti atlikti reikiamas užduotis iš kelių sekcijų. Turi būti realizuota galimybė keisti grafines naudotojo informacijos juostas realiuoju laiku.

		Turi būti galimybė prieigos profilius konfigūruoti naudojant skirtingus leidimus skirtingoms užduotims, pvz .: administratorius, ataskaitų kūrėjas, operatorius ir kita. Po 10 nesėkmingų bandymų prisijungti iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso. Po 15 nesėkmingų bandymų vedant netinkamą seanso ID iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso. Turi būti galimybė nustatyti automatinę agento atnaujinimo funkciją.
14.	Funkciniai reikalavimai smėliadėžės debesyje paslaugai	Galiniuose įrenginiuose turi būti aktyvuojama nuotoliniu būdu naudojant antivirusinės apsaugos administravimo konsolę. Turi būti galimybė įtartinus failus į smėliadėžę debesyje teikti tiek rankiniu, tiek automatiniu būdu. Visi į smėliadėžę išsiųsti failai turi būti fiksuojami antivirusinės apsaugos administravimo konsolėje. Turi būti galimybė gauti ataskaitas apie išsiųstus įtartinus failus. Turi būti galimybė nustatyti terminą, kiek dienų gali būti saugomi įtartini failai smėliadėžėje. Turi būti galimybė drausti/leisti dokumentų siuntimą į smėliadėžę. Tiekėjas užtikrina, kad smėliadėžė debesyje yra saugoma tik Europos ekonominės erdvės valstybėse.
15.	Funkciniai reikalavimai darbo vietų šifravimo moduliui	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Valdymas turi būti įgyvendintas kuriant politikas, kurias galima priskirti įrenginiams ar įrenginių grupėms. Turi būti suderinamumas su *Microsoft Windows 10 / 11* operacinėmis sistemomis. Turi būti UEFI mikroprogramos (angl. *firmware*) palaikymas. Turi būti TPM (angl. *Trusted Platform Module*) palaikymas Turi būti OPAL diskų palaikymas. Turi turėti galimybę šifruoti visus diskus arba tik krovimosi diską. Turi turėti galimybę centralizuotai nustatyti šifravimo slaptažodžio politiką. Turi būti galimybė centralizuotai politikoje laikinai atjungti šifravimo slaptažodžio reikalavimą. Turi turėti galimybę administratoriui nuotoliniu būdu inicijuoti šifravimo slaptažodžio atkūrimą, blokavimą ir ištrynimą. Turi būti galimybė administratoriui iššifruoti kietąjį diską su gamintojo numatyta atkūrimo programa.
16.	Funkciniai reikalavimai saugumo sprendimų valdymo konsolei	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Serveris turi bendrauti su galiniais įrenginiais per agentą, kuris gali saugoti politiką ir vykdyti užduotis, kol įrenginys yra neprisijungęs. Serveris turi leisti pridėti įrenginius prie valdymo konsolės naudojant šiuos metodus: - sinchronizavimas su *Active Directory*; - rankiniu būdu įvedus įrenginio vardą arba IP adresą; - patentuota technologija, gebanti aptikti įrenginius tinkle; Serveris turi leisti įdiegti saugumo sprendimus nuotoliniu būdu ir be vartotojo įsikišimo. Serveris turi leisti kurti statines ir dinamines grupes paprastesniam įrenginių administravimui. Serveris turi leisti nuotoliniu būdu vizualizuoti šią įrenginių informaciją: - pagrindinė informacija; - konfigūracija; - atliktos užduotys;

		- įdiegtos programos; - perspėjimai; - karantinas. Turi turėti centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams. Turi būti galimybė nustatyti automatinę produkto ir agento versijos atnaujinimo funkciją. Turi būti centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų aprašų bazė, nereikalaujant sistemos įkrovimo iš naujo. Turi turėti funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies konfigūracinius nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį. Turi turėti galimybę paveldėti taisykles (angl. *policies*) iš aukštesnio lygio nuotolinio administravimo serverio. Turi būti užtikrinta galimybė siųsti informacinius pranešimus į visų rūšių įrenginius, įskaitant serverius ir kompiuterines darbo vietas. Serveris turi leisti apibrėžti aktyviklį (angl. *trigger*), kuris įvykdytų numatytą veiksmą, kai tam tikras įvykis įvyksta tinkle. Pagal numatytuosius nustatymus serveris turi pateikti keletą standartinių ataskaitų bei leisti kurti naujus ataskaitų šablonus. Turi būti galimybė ataskaitas automatiškai gauti el. paštu arba generuoti valdymo konsolėje. Interneto konsolės sąsaja turi dirbti su informacijos skydais. Jie turi būti visiškai interaktyvūs ir leisti atlikti reikiamas užduotis iš kelių sekcijų. Turi būti realizuota galimybė keisti grafines naudotojo informacijos juostas realiuoju laiku. Turi būti galimybė prieigos profilius konfigūruoti naudojant skirtingus leidimus skirtingoms užduotims, pvz .: administratorius, ataskaitų kūrėjas, operatorius ir kita. Po 10 nesėkmingų bandymų prisijungti iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso. Po 15 nesėkmingų bandymų vedant netinkamą seanso ID iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso. Turi būti galimybė nustatyti automatinę agento atnaujinimo funkciją.
17.	Funkciniai reikalavimai ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo valdymo konsolei	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Serveris turi komunikuoti su galiniais įrenginiais per agentą, kuris gali saugoti politiką ir kaupti žurnalinius įrašus, kol įrenginys yra neprisijungęs. Interneto konsolės sąsaja turi dirbti su informacijos skydais. Turi būti stebėsenos skydelis, kuriame galima stebėti naujausią informaciją apie įmonės tinkle įvykusius įtartinus įvykius. Turi būti interaktyviai atvaizduojami įspėjimai, teikiami pagal taisykles apie įtartinus įvykius, kurie įvyko veikiant programinei įrangai. Turi būti numatytųjų taisyklių sąrašas ir galimybė parengti savo taisykles, kuriomis būtų apibūdinamas įtartinas programinės įrangos veikimas. Turi būti galimybė taisyklei nustatyti automatinius reagavimo veiksmus: - blokuoti vykdomąjį failą; - pašalinti ir blokuoti vykdomąjį failą; - izoliuoti kompiuterį nuo tinklo;

		- kompiuteryje sustabdyti proceso vykdymą; - vykdyti kompiuterio skenavimą nuo kenkėjiškų programų; - išjungti kompiuterį. Turi būti automatiškai vykdomas įspėjimų paskirstymas pagal kritiškumo lygį, leidžiant greitai nustatyti ir reaguoti į kritinius įvykius. Turi būti galimybė nustatyti prioritetinius įspėjimus, kad būtų lanksčiau rūšiuojami ir filtruojami įvykiai. Turi būti galimybė grupuoti įspėjimus pagal skirtingus kriterijus, pvz., tipą, kompiuterį, taisyklę, procesą, rinkmeną. Turi būti galimybė užfiksuoti su informacijos saugumu susijusius incidentus sudarant įtartinus aptikimus, kuriuose būtų pateikta informacijos apie įvykį santrauka (data, laikas ir kur įvykis įvyko (kompiuteris), kuris vartotojas paleido vykdomąjį failą ir koks konkretus procesas sukėlė paleidimą) ir išsami informacija apie kiekvieną iš išvardytų parametrų. Kiekviename įtartiname aptikime turi būti numatytas specialus informacijos skyrius, kuriame pateiktas išsamus taisyklę suaktyvinusio įvykio aprašymas, galimų priežasčių, pavojų ir pasekmių sąrašas bei rekomendacijos dėl būtinų veiksmų tolesnei įvykio analizei vykdyti. Aptikus kritinius incidentus, turi būti galimybė gauti informaciją apie žinomų būdų ir priemonių, kurias anksčiau naudojo įsilaužėliai panašiose situacijose, sąrašą su nuorodomis į atitinkamas MITRE ATT&CK® šaltinio nuorodas, kur galima rasti išsamesnės informacijos apie įsilaužimų taktikas. Turi būti įtartinų aptikimų interaktyvioji sąsaja, leidžianti išsamiau išnagrinėti su informacijos saugumu susijusį incidentą naudojant pagrindinius parametrus, kurie yra prieinami bendrajame įtartiname aptikime. Turi būti pateikiama išsami informacija apie taisyklę suaktyvinusį procesą, pvz., procesų medis, failų sistemos ir operacinės sistemos registro pakeitimai, tinklo veikla, ryšiai su URL adresais, papildomai atsisiųsti vykdomieji failai ir išsamus operacinės sistemos įvykių žurnalas. Turi būti galimybė sukurti išsamias atskirų įvykių išimtis, kurios turėtų apimti informaciją apie vykdomųjų failų kontrolines sumas (angl. *hash checksum*), jų buvimo vietą, skaitmeninį parašą (angl *signature*) ir kt. Turi būti galimybė įtraukti pasirinktus EXE / DLL failus į užblokuotųjų sąrašą remiantis kontroline suma, tokiu būdu inicijuojant blokavimą darbo vietose ir serveriuose. Turi būti galimybė nuotoliniu būdu ištrinti visus įtartinus EXE / DLL failus ir perkelti juos į karantiną. Turi būti galimybė atsisiųsti įtartinus failus iš darbo vietų ir serverių tolesnės analizės vykdymui. Turi būti galimybė parengti visų EXE / DLL failų, esančių darbo vietose ir serveriuose, sąrašą tolesnės analizės vykdymui. Turi būti galimybė parengti baltuosius (angl. *whitelist*) / juoduosius (angl. *blacklist*) EXE / DLL failų sąrašus. Turi būti galimybė peržiūrėti išsamią informaciją apie EXE / DLL failus, su jais susijusius įspėjimus, naudojimo statistiką, failų pakeitimus, registrą, sukurtus tinklo ryšius. Turi būti galimybė esant poreikiui atkurti, ištrinti ir atsisiųsti užblokuotų EXE / DLL failų sąrašą išsamesnės analizės vykdymui. Turi būti automatiškai vykdomas EXE / DLL failų paskirstymas pagal kritiškumo lygį, leidžiant greitai nustatyti ir reaguoti į įtartiną failų elgesį.

		Turi būti galimybė žymėti EXE / DLL failus kaip patikimus ar saugius ir kaip patikrintus bei išanalizuotus. Turi būti galimybė tiesiogiai iš konsolės vykdyti papildomos informacijos apie failus sparčiąją paiešką trečiųjų šalių ištekliuose, tokiuose kaip „Virus Total“ arba lygiaverčiuose. Turi būti galimybė parengti visų skriptų, kurie buvo vykdomi darbo vietose ir serveriuose, sąrašą. Turi būti galimybė grupuoti skriptus pagal skirtingus kriterijus, tokius kaip pirminis procesas, pirmasis antrinis procesas, komandinė eilutė. Turi būti galimybė žymėti patikrintus skriptus kaip patikimus ar saugius. Turi būti galimybė gauti su skripto turiniu susijusią informaciją apie pasitelktus EXE / DLL failus, procesus, sugeneruotus antrinių procesų sąrašus, failų pakeitimus, registrus, užmegztus tinklo ryšius. Turi būti automatiškai vykdomas skriptų paskirstymas pagal kritiškumo lygį, leidžiant greitai nustatyti ir reaguoti į įtartiną elgesį. Turi būti galimybė atvaizduoti kompiuterių sąrašą ir išsamią informaciją apie veiksmus, EXE / DLL failus ir skriptus. Turi būti galimybė nuotoliniu būdu atlikti darbo vietos perkrovimą arba visiškai ją išjungti. Turi būti galimybė iš nuotolinės valdymo konsolės darbo vietai paleisti antivirusinės programos greitąjį skenavimą. Turi būti galimybė iš nuotolinės valdymo konsolės atlikti darbo vietos operacinės sistemos būsenos momentinę nuotrauką, kurioje būtų užfiksuota informacija apie visus tuo metu vykstančius procesus ir tinklo ryšius, bei pateikiama informacija apie kritinį operacinės sistemos registro turinį, operacinės sistemos planavimo priemonės užduotis, operacinės sistemos vartotojus ir jų privilegijas, operacinės sistemos kritinių failų, pvz., „hosts“, „win.ini“ ir kt., turinį, bei visa išsami informacija apie operacinę sistemą ir įdiegtą programinę įrangą. Turi būti galimybė kurti ir išsaugoti paieškos užduotis visoje duomenų bazėje, kurioje renkami duomenys iš visų valdomų kompiuterių, įskaitant bet kokius parametrus (net kelis simbolius iš vykdomosios komandinės eilutės) ir naudojant įvairius filtrus.
18.	Kiti reikalavimai	Sprendimas turi turėti mechanizmą, kuris leidžia pašalinti bet kurį kitą saugumo sprendimą, esantį galiniame įrenginyje. Šis mechanizmas turi būti: - Integruotas į saugumo sprendimą. - Pateiktas kaip atskiras įrankis. - Pasiekiamas per antivirusinės apsaugos centralizuotą administravimo konsolę.
19.	Atnaujinimai	Klientinės dalies programinė įranga privalo turėti funkcionalumą parsisiųsti atnaujinimus tiesiai iš: - Gamintojo atnaujinimų serverio, - Centralizuoto valdymo serverio, - Kitų klientų. Klientinės dalies programinė įranga privalo turėti funkcionalumą veikti kaip atnaujinimų serveris kitiems klientams tam, kad būtų galima taupyti tinklo pralaidumo resursus. Turi būti galimybė nustatyti automatinę saugumo produkto atnaujinimo funkciją.
20.	Aktualumo reikalavimas	Pateikiamoms licencijoms turi būti užtikrinamas gamintojo palaikymas sutarties galiojimo laikotarpiu, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio operatyviai gauti naujausius

		virusų aprašus (angl. *signature*), virusų paieškos mechanizmo (angl. *engine*) atnaujinimus bei atsisiųsti ir diegtis naujausias programinės įrangos versijas.
21.	Versija	Turi būti siūloma naujausia stabili programinės įrangos versija, oficialiai gamintojo paskelbta internete.
22.	Dokumentacija	Turi būti pateikta aktuali dokumentacija, apimanti programinės įrangos įdiegimo, bendro naudojimo, administravimo, sistemos atstatymo procedūras.
23.	Gamintojo aptarnavimo (angl. *support*) sąlygos	Gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių ir anglų kalbomis. Gamintojo atstovas turi suteikti 2 valandas konsultacijų produkto diegimo ir atnaujinimo klausimais, kurios turi būti įvykdytos ne vėliau kaip 30 dienų nuo licencijų aktyvavimo dienos. Gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių ir anglų kalbomis.
24.	Reikalavimai programinės įrangos naudojimo taisyklėms (licencijavimui)	Licencija turi suteikti teisę pakartotinai diegti siūlomą programinę įrangą neišnaudojant papildomos licencijos. Programinės įrangos licencijavimo taisyklėse licencija turi būti nepririšama prie aparatūrinės įrangos. Licencijos įsigijimo metu turi būti pateiktas vienas licencijos raktas, tinkantis visiems įrenginiams, nepriklausomai nuo licencijos įsigijimo kiekio bei įrenginio tipo.
25.	Techninių žurnalų įrašų kaupimas	Turi būti techninių žurnalų įrašų (angl. event log) palaikymas. Galimybė juos saugoti lokaliai, siųsti juos į Syslog serverius, serverius debesyje, integracija su SIEM, SOC.
	Licencijų galiojimo laikotarpis	36 mėn.

4. REIKALAVIMAI, SUSIJĘ SU INFORMACIJOS (DUOMENŲ) SAUGUMU VYKDANT SUTARTĮ

4.1. Tiekėjas, teikdamas prekes pagal sutartį, turi vadovautis šioje Techninėje specifikacijoje nustatytais saugumo reikalavimais ir užtikrinti nustatytų reikalavimų įgyvendinimą šiuose teisės aktuose:

4.1.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB;

4.1.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

4.1.3. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

4.1.4. kituose Europos Sąjungos ir Lietuvos Respublikos teisės aktuose, reglamentuojančiuose tinklų, informacinių sistemų ir duomenų saugą.

4.2. Įsigaliojus naujiems Europos Sąjungos ar Lietuvos Respublikos teisės aktams, ar jų pakeitimams, susijusiems su paslaugų vykdymu, Tiekėjas privalo vykdyti tokių teisės aktų nuostatas nuo jų įsigaliojimo datos. Todėl kiekviena šioje Techninėje specifikacijoje nurodyta reikalavimų nuostata, neatitinkanti įsigaliojusio naujojo Europos Sąjungos ar Lietuvos Respublikos teisės akto ar jo pakeitimo, susijusio su paslaugomis, nuo tokio naujojo teisės akto ar jo pakeitimo įsigaliojimo datos netaikoma, o vietoj jos taikoma įsigaliojusio naujojo Europos Sąjungos ar Lietuvos Respublikos teisės akto ar jo pakeitimo, susijusi su teikiamomis paslaugomis, nuostata.

4.3. Prieš pradėdami teikti prekes pagal sutartį Tiekėjo darbuotojai privalės pasirašyti Konfidencialumo pasižadėjimus.

4.4. Tiekėjo darbuotojams prieiga prie Pirkėjo informacinių išteklių suteikiama tik tokios apimties, kokios reikia licencijų nuomos vykdymui užtikrinti.

4.5. Jei teikiant prekes pagal sutartį yra būtina nuotolinė prieiga prie Pirkėjo informacinių išteklių, konkrečiam Tiekėjo darbuotojui yra suteikiami prisijungimo duomenys ir Tiekėjas prieš atliekant tam tikrus darbus pagal sutartį privalo pateikti Pirkėjui darbuotojo(-ų), atliksiančio(-ų) darbus, duomenis (vardą, pavardę, telefono ryšio numerį ir(ar) elektroninio pašto adresą). Tiekėjas privalo užtikrinti, kad prie Pirkėjo informacinių išteklių jungtųsi tik tie darbuotojai, apie kuriuos Tiekėjas pranešė Pirkėjui, nesuteikiant prieigos kitiems Tiekėjo darbuotojams ar tretiesiems asmenims. Prisijungimo duomenys nurodytiems Tiekėjo darbuotojams pateikiami asmeniškai ar elektroniniu paštu.

4.6. Tiekėjui nutraukus darbo santykius su paskirtu vykdyti sutartį darbuotoju, Tiekėjas nedelsiant turi informuoti apie tai Pirkėją, kuri nedelsiant panaikina nurodyto darbuotojo naudotojo vardą ir slaptažodį ir (arba) užblokuoja prieigą prie Pirkėjo informacinių išteklių.

4.7. Tiekėjo darbuotojui suteiktas naudotojo vardas nekeičiamas ir negali būti suteiktas kitam Tiekėjo paskirtam darbuotojui.

4.8. Tiekėjui viešai neskelbtina informacija teikiama tik tokios apimties, kuri būtina sutarčiai vykdyti. Tiekėjas turi imtis visų teisinių, techninių ir organizacinių priemonių iš Pirkėjo gautai informacijai apsaugoti.

4.9. Visi Techninės specifikacijos 4 punkte numatyti saugumo reikalavimai, taikomi Teikėjui, yra taikomi ir jo subteikėjams ir kitais pagrindais pasitelkiamiems ūkio subjektams ir jų darbuotojams.

SUTARTIES REIKALAVIMAI

1. Sutarties vykdymo vieta(-os)

Savanorių pr. 176, Vilnius

2. Sutarties vykdymo tvarka ir terminai

Sutarties trukmė 36 mėn.