Pirkimo sąlygų 2 priedas „Techninė specifikacija“

**TECHNINĖ SPECIFIKACIJA**

1. **PIRKIMO OBJEKTAS**
   1. Mykolo Romerio universitetas (toliau – Universitetas, Perkančioji organizacija) siekia išsinuomoti kibernetinės saugos priemones:
      1. Microsoft 365 produktyvumo debesies apsaugos sprendimas – 400 licencijų.
      2. Kompiuterinių darbo vietų saugos sprendimas – 300 licencijų.
   2. Reikalavimai tiekėjui:

|  |  |
| --- | --- |
| **Reikalavimai** | **Įrodantys dokumentai** |
| Tiekėjas yra autorizuotas siūlomų licencijų gamintojo partneris, distributorius ar kitas įgaliotas subjektas, turintis teisę nuomoti siūlomą programinę įrangą Lietuvoje. | Siūlomų licencijų gamintojo sertifikatas arba kiti lygiaverčiai įrodymai, patvirtinantys, kad Tiekėjas yra gamintojo oficialus ir sertifikuotas atstovas, įgaliotas nuomoti Pirkėjui reikalingas licencijas.  Pateikiamos skaitmeninės dokumentų kopijos kartu su pasiūlymu. |

* 1. Aplinkosauginiai reikalavimai.

1.3.1. Viešasis pirkimas laikomas žaliuoju, kadangi viešojo pirkimo objektas atitinka Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d įsakymu. Nr. D1-508 „Dėl Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“, 4.4.3 papunktyje nurodytus reikalavimus: perkama tik nematerialaus pobūdžio (intelektinė) ar kitokia paslauga, nesusijusi su materialaus objekto sukūrimu, kurios teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos.

1. **Techninė specifikacija**

2.1 Microsoft 365 produktyvumo debesies apsaugos sprendimas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Eil. Nr.** | **Pavadinimas** | **Reikalavimai** | **Siūloma reikšmė** | **Atitiktį Techninės specifikacijos reikalavimams pagrindžiantys dokumentai (pvz. gamintojo prekės aprašymas arba internetinė nuoroda į gamintojo psl., arba kiti lygiaverčiai dokumentai).** |
|  | Pirkimo objektas | Perkančiosios organizacijos naudojamų Microsoft 365 licencijų , bei kitų debesų kompiuterija grįstu programinių sprendimų (SaaS) apsauga nuo kibernetinių atakų.  Sprendimas pagrįstas debesų kompiuterija, užtikrinant, kad duomenys bus laikomi infrastruktūroje Europos Sąjungoje. Gamintojo įsipareigojamas licencijų pasiekiamumas ne mažiau 99,9%. |  |  |
|  | Licencijos tipas | Licencijų nuoma (angl. *subscription*) |  |  |
|  | Kiekybiniai parametrai | 400 vartotojų |  | x |
|  | Apsaugomos platformos | Microsoft 365:   * Exchange Online * Teams * Sharepoint * OneDrive   Kitų platformų apsauga:   * Google Workspace, įskaitant Google Mail, Google Drive. * Dropbox * Slack |  |  |
|  | Integracija | Tiekėjas turi atlikti darbus reikalingus integruoti siūlomą sprendimą su:   * Exchange Online * Teams * Sharepoint * OneDrive |  |  |
|  | Sprendimo tipas | * Sprendimas turi būti pagrįstas Microsoft 365 API sąsaja, t.y. funkcionalumas pasiekiamas be papildomų debesų aplikacijų diegimo. * Sprendimas turi veikti be programinės ar fizinės įrangos diegimo Perkančiosios organizacijos infrastruktūroje. * El. pašto apsaugos diegimas turi vykti be Perkančiosios organizacijos domeno MX įrašų koregavimo. |  |  |
|  | El. pašto apsauga | * Turi būti funkcionalumas blokuojantis socialinės inžinerijos el. laiškus, įskaitant apgaulės (*phishing*) bei apsimetėlių laiškus. Patikra turi būti įgyvendinta naudojant dirbtinio intelekto modelius ir apimti:   + el. pašto parametrų, tokių kaip DMARC, SPF patikrą;   + siuntėjų apsimetančių organizacijos vadovais bei organizacijos partneriais aptikimas, lyginant siuntėjus su mašininio mokymosi pagrindu sukurta istorinės komunikacijos duomenų baze ir vidinių vartotojų duomenų baze;   + siuntėjo reputacijos patikrą pagal gamintojo grėsmių duomenų bazę vertinimą, pagal domeno registracijos datą ir komunikacijos su Perkančiąja organizacija istoriją;   + nuorodų el. laiškuose į retai lankomas ir abejotinos reputacijos arba žalingas svetainės aptikimą;   + įtartinų laiškų temų bei turinio aptikimą naudojant natūralios kalbos apdorojimo mechanizmą, palaikantį lietuvių, anglų, vokiečių, prancūzų, lenkų kalbas;   + istorinį gavėjo ar organizacijos susirašinėjimo su siuntėju ar siuntėjo domenu aktyvumą, aptinkant naujus, įtartinus siuntėjus;   + el. laiško siuntimo kelio vertinimą, identifikuojant laiškus kurių siuntimo kelias įtartinas;   + optinį simbolių atpažinimo funkcionalumą, aptinkantį tekstą paveiksliuke. * Turi būti funkcionalumas atliekantis el. laiškų prisegtukų patikrą, naudojant žinomų žalingų failų duomenų bazę bei gamintojo grėsmių duomenų bazę. * Turi būti nežinomų failų patikra grėsmių detonavimo aplinkoje (smėliadežėje, angl. *sandbox*), kai failai siunčiami patikrai į saugią aplinką, atidaromi, imituojant įprastą vartotojo elgseną ir identifikuojama žalingą jų veiklą. * Nuorodų į failus el. laiškuose pakeitimas į nuorodas, pagal kurias failai tikrinami kaskart prieš leidžiant juos atsisiųsti vartotojui. Tokiu būdu išvengiama atakų, kai po išsiuntimo nusikaltėliai pakeičia nurodytą failą į žalingą. * Nuorodų į svetaines patikra el. laiškuose, identifikuojant žalingas svetaines. Nuorodų perrašymo funkcionalumas turi veikti ir nuorodoms į svetaines. * Aktyvaus turinio (macros, script) išvalymas iš Office paketo bei .pdf failų bei saugių failų pateikimas vartotojams, suteikiant vartotojui galimybę atsisiųsti originalų saugų failą po patikros. Galimybė konvertuoti visus Microsoft Office failus į .pdf failus be aktyvaus turinio, su galimybe vartotojui atsisiųsti originalius saugius failus po patikros. * Saugos politikoje nustatoma failų karantinavimo ir blokavimo politika. Galimybė vartotojui teikti prašymus savitarnoje karantinuotų el. laiškų ir prisegtukų atstatymui. Galimybė kurti savo karantinavimo ir blokavimo pranešimus lietuvių kalba. * Galimybė nustatyti skirtingas politikas su skirtingu funkcionalumu ir nustatymais skirtingoms vartotojų grupėms. * Galimybė naudoti saugos politikas: užlaikant el. laiškus iki patikros pabaigos; pateikiant el. laiškus vartotojui ir juos karantinuojant arba šalinant po patikros pabaigos, aptikus žalingą turinį; pateikiant el. laiškus vartotojui ir sugeneruojant saugos įvyki aptikus žalingą turinį. * Sprendimo patikra turi būti įgyvendama po platformos tiekėjo (Microsoft, Google) patikros, užtikrinant kelių lygių patikrą ir žalingo turinio blokavimą. * Turi būti funkcionalumas leidžiantis ieškoti duomenų bazėje el. laišku pagal įvairius požymius. * Vartotojų informavimas apie potencialiai žalingą ar įtartina turinį, kai laiškas pagal požymius nėra identifikuojamas kaip žalingas, atvejais kai:   + Laiške prašoma atnaujinti mokėjimo informaciją.   + Laiške pateikiama sąskaita iš naujo, iki šiol neužfiksuoto tiekėjo.   + Laiške pateikiama informacija susijusi su darbo santykiais – darbo užmokesčiu.   + Laiške pateikiamas apmokėjimo prašymas.   + Laiške pateikiamos nuorodos į apribotos priegios resursus.   + „Reply-to“ lauke nurodomas kitas el. pašto adresas, negu siuntėjo el. pašto adresas arba „Reply-to“ adreso domenas neseniai registruotas. Siuntėjo el. pašto adreso domenas nesenai registruotas.   + Siuntėjas pirmą kartą siunčia laišką gavėjui. Siuntėjo pateikiama informacija (el. pašto adresas, vardas) panašus į organizacijos vidinio vartotojo adresą ar vardą. * Turi būti įvykių kaupimas ir paieška. Įvykių informacijoje turi būti nurodomos tikslios sprendimo priežastys, bei atvaizduojamas ir platformos tiekėjo (Microsoft, Google) verdiktai ir jų priežastys. |  |  |
|  | Failų dalijimosi platformų apsauga | * Failų įkeliamų į dalijimosi platformas (įskaitant OneDrive, Sharepoint) patikra. * Patikra turi apimti žinomų žalingų failų aptikimą, bei smėliadėžės funkcionalumą, kai failai siunčiami patikrai į saugią aplinką, atidaromi, imituojant įprastą vartotojo elgseną ir identifikuojant žalingą jų veiklą. * Turi būti tikrinami failai bei nuorodos juose. * Aptikus žalingą turinį, failai turi būti karantinuojami. |  |  |
|  | Bendravimo platformų apsauga | * Bendravimo platformų (įskaitant Teams) patikra. * Turi būti funkcionalumas identifikuojantis gaunamas socialinės inžinerijos žinutes. * Turi būti funkcionalumas identifikuojantis gaunamus žalingus failus. * Aptikus žalingą turinį turi būti blokuojama vartotojo prieiga prie jo. |  |  |
|  | Įsilaužimo į vartotojų paskyras apsauga | Sprendimas turi stebėti Perkančiosios organizacijos vartotojų prisijungimo įvykius ir aptikti nuokrypius nuo normos, įskaitant:   * Nuokrypius nuo įprastos vartotojo elgsenos, naudojant mašininio mokymosi modelius. * Neįmanomos kelionės įvykius, kai vartotojas panašiu metu jungiasi iš skirtingų geografinių vietovių. * Neįprastų nustatymų aptikimas – automatiškai trinami nauji laiškai, automatiškai persiunčiami laiškai ar pan. * Vartotojas siunčia žalingus laiškus. * Vartotojas jungiasi iš IP adreso, susieto su žinomais incidentais.   Aptikus žalingus incidentus turi būti sugeneruotas įvykis, informuojant administratorius. Taip pat vartotojo dėl kurio veiklos atsirado įtarimų turi būti automatiškai papildomai tikrinami failų ir laiškų srautai.  Turi būti galimybė automatiškai blokuoti vartotojų paskyras į kurias yra įsilaužta. |  |  |
|  | Bendras saugos funkcionalumas | * Galimybė aprašyti išimtis:   + praleisti arba blokuoti tam tikrų siuntėjų ar siuntėjo domenų laiškus;   + praleisti arba blokuoti laiškus iš tam tikrų IP adresų;   + praleisti arba blokuoti laiškus tam tikriems gavėjams;   + praleisti arba blokuoti laiškus su tam tikra tema ar tekstu. * Galimybė aprašyti vartotojų elgsenos ypatumus, į kuriuos nereaguotų įsilaužimo į vartotojų paskyras apsaugos funkcionalumas. * Galimybė aprašyti automatiškai netikrinamus failus, URL. * Galimybė rankiniu būdu karantinuoti el. laiškus. |  |  |
|  | Saugos įvykių atvaizdavimas | * Visi saugos įvykiai turi būti atvaizduojami per grafinę sąsają. * Galimybė filtruoti įvykius pagal laiką, būseną, incidentui pritaikytą veiksmą (blokuotas, karantinuotas ir pan.), grėsmės lygį, apsaugotą aplikaciją, grėsmės tipą, vartotoją. * Turi būti atvaizduojami tiek gamintojo platformos saugos įvykiai, tiek saugos įvykiai gaunami iš Microsoft 365 platformos. * Turi būti ataskaitų funkcionalumas, pateikiantis apibendrintą istorinę informaciją apie įvykius. * Turi būti galimybė peržiūrėti žalingus el. laiškus, atsisiųsti žalingus failus per grafinę sąsają tolimesnei analizei. |  |  |
|  | Valdymo funkcionalumas | * Visas sprendimo funkcionalumas turi būti valdomas per grafinę sąsają. * Perkančiajai organizacijai turi būti suteikiama prieiga prie Gamintojo infrastruktūroje esančio sprendimo valdymo. * Turi būti galimybė kurti kelias administratorių paskyras su skirtingu prieigos lygiu (peržiūrėti ir redaguoti, tik peržiūrėti). * Administratorių autentifikavimas turi veikti per Microsoft Azure AD, Okta, DUO, Google Workspace platformas, RADIUS ir SAML autentifikaciją. * Galimybė įvykius perduoti į SIEM ir įvykių valdymo sprendimus, naudojant json ir syslog (RFC 5424) formatus. |  |  |
|  | Nuomos teikimo laikotarpis ir gamintojo įsipareigojimai | * Nuoma turi būti teikiama 36 mėn. laikotarpyje (nuo 2025-12-30). * Nuomos palaikymas visą nuomos teikimo laikotarpį. Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. * Į pasiūlymą turi būti įtrauktos visos reikiamos licencijos išvardintam funkcionalumui įgyvendinti visam laikotarpiui. * Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir instrukcijų bei programinės įrangos bibliotekos. |  |  |

2.2. Darbo vietų saugos sprendimas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Eil. Nr. | **Pavadinimas** | **Reikalavimai** | **Siūloma reikšmė** | **Atitiktį Techninės specifikacijos reikalavimams pagrindžiantys dokumentai (pvz. gamintojo prekės aprašymas arba internetinė nuoroda į gamintojo psl., arba kiti lygiaverčiai dokumentai).** |
|  | Sprendimo pavadinimas | Darbo vietų saugos programinės įrangos programinė įranga. |  | x |
|  | Licencijos tipas | Licencijų nuoma (angl. *subscription*) |  |  |
|  | Kiekybiniai parametrai | 300 vartotojų |  | x |
|  | Valdymo funkcionalumas | * Visas sprendimo funkcionalumas turi būti valdomas per grafinę sąsają. * Valdymas turi būti veikti SaaS (programinės įrangos paslauga) principu ir veikti gamintojo debesų kompiuterijos infrastruktūroje. * Gamintojas turi užtikrinti, kad valdymo programinė įranga ir visi susiję duomenys būtų laikomi duomenų centre Europos sąjungos teritorijoje. * Perkančiajai organizacijai turi būti suteikiama prieiga prie Gamintojo infrastruktūroje esančio sprendimo valdymo. * Turi būti galimybė kurti kelias administratorių paskyras su skirtingu prieigos lygiu (peržiūrėti ir redaguoti, tik peržiūrėti). * Administratorių autentifikavimas turi veikti per Microsoft Azure AD, Okta, DUO, Google Workspace platformas, RADIUS ir SAML autentifikaciją. * Galimybė įvykius perduoti į SIEM ir įvykių valdymo sprendimus, naudojant json ir syslog (RFC 5424) formatus. |  |  |
|  | Įvykių surinkimo funkcionalumas | * Programinė įranga turi perduoti įvykius į valdymo serverį nustatytų periodiškumu. * Programinė įranga turi kaupti įvykius susijusius su visu saugos funkcionalumu. Įvykis turi apimti informaciją apie susijusį vartotoją, įrenginį, suveikusią apsaugą, bei kontekstinę grėsmės informaciją susijusią su konkrečiu funkcionalumu. * Valdymo serveris turi kaupti įvykius ne trumpiau kaip 90 dienų. * Galimybė eksportuoti įvykius į išorinę talpyklą syslog protokolu. |  |  |
|  | Darbo vietų valdymas ir bendrieji nustatymai | * Turi būti funkcionalumas leidžiantis atlikti nuotolinius veiksmus įrenginiui arba jų grupei įskaitant:   + Inicijuoti failinės sistemos antivirusinį skanavimą, atnaujinti aprašų duomenų bazę, atstatyti karantinuotus failus.   + Atlikti įrenginio analizę pagal grėsmės indikatorių.   + Izoliuoti kompiuterį, panaikinti izoliavimą.   + Surinkti įvykius, inicijuoti programinės įrangos taisymą, išjungti įrenginį, perkrauti įrenginį, ištrinti programinę įrangą.   + Išjungti procesą, atlikti procesų skanavimą.   + Paieškoti ir paimti failą iš kompiuterio.   + Paleisti nuotolinę komandą.   + Inicijuoti diagnostiką. * Galimybė programinės įrangos klientui nustatyti šiuos parametrus:   + Pranešimų vartotojams atvaizdavimas.   + Teisę vartotojui nukelti atnaujinimą.   + Ištrynimo slaptažodžio nustatymas. Vartotojas lokaliai negali turėti galimybę be slaptažodžio ištrinti programinės įrangos.   + Galimybė nustatyti URL filtravimo pranešimų turinį, įskaitant lietuvių kalba. |  |  |
|  | Programinės įrangos diegimas | * Turi palaikyti Windows 7, 8, 10, 11 Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022 operacines sistemas. * Turi palaikyti macOS Catalina, Big Sur, Monterey, Ventura, Sonoma, Sequoia operacines sistemas. * Turi palaikyti Fedora, Alma Linux, Ubuntu, SUSE Linux Enterprise Server, RHEL, Oracle Linux, OPen Suse, Debian, CentOS, Amazon Linux operacines sistemas. * Galimybė diegti klientą su visu funkcionalumu, arba pradinį klientą ne didesnį kaip 5 MB. Pradinis klientas turi diegimo metu nustatyti vartotojui ar įrenginiui taikomą politiką ir automatiškai atsiųsti reikiamą funkcionalumo paketą ir politiką. * Saugumo politikos bei funkcionalumo paketai turi būti nustatomi vartotojų ar įrenginių grupėms. Galimybė diegti skirtingą funkcionalumą skirtingiems vartotojams ar įrenginiams. * Galimybė keisti programinės įrangos funkcionalumo paketus bei politikas po diegimo. T.y. programinė įranga turi automatiškai įdiegti papildomą funkcionalumą arba išdiegti turimą atsižvelgiant į diegimo politikos nustatymus. |  |  |
|  | Apsaugos nuo grėsmių funkcionalumas | Turi turėti tokias integruotas funkcijas:   * Antivirusinė apsauga. * URL filtravimas. * Organizacijos prisijungimo duomenų naudojimo kontrolę; * Prievadų apsauga. * Darbo vietų ugniasienė. * Aplikacijų kontrolė. * Apsaugą nuo elektroninio sukčiavimo (Phishing). * Apsaugą nuo pažeidžiamumų išnaudojimo grėsmių (angl. Exploit). * Apsaugą nuo ransomware tipo duomenis užkoduojančių virusų. * Apsaugą nuo botnet tinklų kenkėjiškos programinės įrangos. * Apsaugą nuo grėsmių pagal tipinius žalingo kodo veikimo modelius. * Incidentų analizės įrankį. * Grėsmių paieškos funkcionalumas. |  |  |
|  | Antivirusinė apsauga | * Žinomų virusų aptikimas pagal aprašus. * Žinomų žalingų failų ir procesų aptikimas bei blokavimas. * Galimybė karantinuoti užkrėstus failus, su galimybe failus atstatyti iš karantino. * Failų sistemos periodinis skanavimas. Galimybė pasirinkti failų sistemos skanavimo apimtį, nustatant lokalius diskus, tinklines talpyklas, bei pageidaujamą periodinio skanavimo laiką. * Aprašų atnaujinimai pagal administratoriaus nustatytą grafiką. |  |  |
|  | URL filtravimas | * URL filtravimas pagal kategorijas kompiuteriuose ir serveriuose. * Galimybė blokuoti konkrečius URL. * Galimybė atlikti URL filtravimą naršyklės (Chrome, Edge) lygmenyje, arba tinklo sąsajos lygmenyje. * Pranešimų vartotojui apie uždraustas kategorijas arba URL pateikimas. |  |  |
|  | Organizacijos prisijungimo duomenų naudojimo kontrolę | * Sprendimas turi saugiai kaupti vartotojų prisijungimų slaptažodžius, naudojamus Perkančiosios organizacijos sistemose, bei riboti tų pačių slaptažodžių panaudojimą trečių šalių sistemose. * Sprendimas slaptažodžius turi kaupti saugiai (turi būti įrašomi maišos kodai), juos saugant lokaliuose įrenginiuose. |  |  |
|  | Prievadų apsauga | * Prievadų įrenginiuose naudojimo kontrolė. * Turi būti galimybė valdyti bluetooth, USB, LPT, COM, PS2 prievadus. * Galimybė leisti arba blokuoti specifinių prievadų naudojimą. * Galimybė leisti arba blokuoti specifinių įrenginių per specifinius prieavadus naudojimą. Pvz.: apriboti PS2 klaviatūrų naudojimą. * Galimybė leisti tik patvirtintus įrenginius pagal serijos numerius ir tipus. |  |  |
|  | Darbo vietų ugniasienė | * Įeinančio ir išeinančio srauto kontrolė IP adresams, jų rėžiams, protokolams, prievadams; * Centralizuotas ugniasienės politikos valdymas per vartotojus ir jų grupes; * Galimybe kurti kelias politikas, galiojančias kompiuteriui esant vidiniame tinkle ir už jo ribos; * Darbo vietos atitikties vertinimas pagal programinės įrangos versiją, operacinės sistemos atnaujinimus, neleistinų aplikacijų naudojimą, žinomus su kompiuteriu susijusius incidentus. Ribotos ugniasienės politikos pritaikymas neatitinkantiems įrenginiams; * Galimybė aptikti viešosios prieigos tinklus, bei taikyti ugniasienės išimtis WEB autentifikacijai. |  |  |
|  | Aplikacijų kontrolė | * Aplikacijų generuojamo srautų kontrolė, leidžiant/neleidžiant konkrečios aplikacijos srautus; * Aplikacijų paleidimo kontrolė, leidžiant/neleidžiant paleisti konkrečias aplikacijas. |  |  |
|  | Apsaugą nuo elektroninio sukčiavimo (Phishing) | * Apsauga nuo žinomų ir nežinomų elektroninio sukčiavimo svetainių ir jų turinio; * Nežinomų elektroninio sukčiavimo svetainių aptikimas pagal: IP ir domeno reputaciją, pateikiamų duomenų (URL, teksto, išvaizdos URL) panašumus su žinomomis svetainėmis; * Duomenų įvesties blokavimas įtartinoms ir žinomoms elektroninio sukčiavimo svetainėms. * Pranešimų vartotojui apie įtartiną turinį svetainėse pateikimas. |  |  |
|  | Apsaugos nuo pažeidžiamumų išnaudojimo grėsmių (angl. Exploit) funkcionalumas | * Apsauga nuo programinės įrangos pažeidžiamumų išnaudojimo. * Galimybė automatiškai išjungti programinę įrangą, kurios pažeidžiamumus bandoma išnaudoti. |  |  |
|  | Apsaugos nuo ransomware tipo duomenis užkoduojančių virusų funkcionalumas | * Apsauga nuo žinomų ir nežinomų ransomware tipo virusų. * Ransomware tipo virusų atpažinimas pagal veikimo modelius. * Galimybė automatiškai atstatyti ransomware atakos metu užkoduotus failus. Programinė įranga turi kaupti keičiamų failų atsargines kopijas saugiame aplanke tame pačiame įrenginyje ir įvykus ransomware atakai pakeistus/prarastus failus atstatyti iš šio aplanko. |  |  |
|  | Apsaugos nuo grėsmių pagal tipinius žalingo kodo veikimo modelius funkcionalumas | * Grėsmių aptikimas, klasifikavimas bei blokavimas pagal veikimo modelius. * Žalingų rašmenų (angl. Script) aptikimas ir blokavimas. |  |  |
|  | Apsaugos nuo botnet tinklų kenkėjiškos programinės įrangos funkcionalumas | Žinomų ir nežinomų botnet tinklų kenkėjiškos programinės įrangos aptikimas pagal veiklos požymus, ir jos blokavimas. |  |  |
|  | Incidentų analizės įrankio funkcionalumas | * Galimybė aprašyti savo incidentų aprašus (angl. IoC, indicators of compromise). * Galimybė po incidento nustatyti žalą (duomenų nutekėjimą, užšifruotus duomenis, įvesties duomenų fiksavimo atvejus ir pan.). * Galimybė atsekti visą incidento eigą, nuo ištakų ir priežasčių iki pasekmių. * Galimybė incidento eigą atvaizduoti grafiškai. * Incidentų atvaizdavimas MITRE matricoje. |  |  |
| 2.2.21 | Grėsmių paieškos funkcionalumas | Sprendimas turi turėti grėsmių paieškos funkcionalumą, apimantį paiešką įvykių duomenų bazėje pagal:   * Proceso duomenis; * Aptikimo įvykio duomenis; * Failo duomenis; * Tinklo veiklos duomenis; * Registrų pakeitimų duomenis; * Prisijungimo/atsijungimo įvykius; * Paleistų rašmenų (script) duomenis; * Nuotolinio paleidimo informaciją; * El. laiškų duomenis; * Aplikacijų duomenis.   Grėsmių paieškos funkcionalumas turi apimti:   * Paiešką pagal daugybę parametrų vienu metu; * Galimybę išsaugoti paieškos formą; * Galimybę išsaugotoms paieškos formoms formuoti automatinius pranešimus priskirtiems administratoriams; * Gamintojo pateikiamų paieškos formų grafinį atvaizdavimą, pvz.: aktyvių atakų, užblokuotų atakų, žalingų failų.   Grėsmių paieškos funkcionalumas turi leisti šiuos veiksmus su paveiktais įrenginiais:   * Izoliuoti užkrėstas darbo vietas; * Karantinuoti užkrėstus failus, naikinti žalingus procesus; * Įjungti ekspertizės įrašo sukūrimą (*forensic record*) susijusiam procesui darbo vietoje. * Peržiūrėti sukurtą susijusį ekspertizės įrašą. |  |  |
| 2.2.22 | Nuomos teikimo laikotarpis ir gamintojo įsipareigojimai | * Nuoma turi būti teikiama 36 mėn. laikotarpyje (nuo 2025-12-30). * Nuomos palaikymas visą nuomos teikimo laikotarpį. Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. * Į pasiūlymą turi būti įtrauktos visos reikiamos licencijos išvardintam funkcionalumui įgyvendinti visam laikotarpiui. * Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir instrukcijų bei programinės įrangos bibliotekos. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas)* |  | *(Parašas)* |  | *(Vardas, pavardė)* |