## IŠPLĖSTINIO APTIKIMO IR REAGAVIMO SISTEMA (XDR)

## TECHNINĖ SPECIFIKACIJA

# BENDROSIOS NUOSTATOS

1. Pirkimo objektas – išplėstinio aptikimo ir reagavimo sistema skirta įrankių ir duomenų konsolidacijai, siekiant išplėstinio kenksmingos veiklos matomumo pagal galinių įrenginių ir tinklo srauto analizę, ir atsakui į galimas grėsmes (toliau – XDR arba sprendimas).
2. Valstybės įmonė Registrų centras (toliau – Perkančioji organizacija) numato įsigyti XDR sistemą 36 (trisdešimt šešių) mėnesių laikotarpiui, kuri turi būti įdiegta ir sukonfigūruota Perkančiosios organizacijos vidiniame tinkle. XDR diegimo ir konfigūravimo metu tiekėjas taip pat turės apmokinti Perkančiosios organizacijos 3 darbuotojus.
3. XDR diegimo ir konfigūravimo vieta – valstybės įmonė Registrų centras adresu Studentų g. 39, Vilnius. XDR diegimo ir konfigūravimo vieta gali būti keičiama Vilniaus miesto ribose. Tiekėjas XDR diegimo, konfigūravimo metu, pagal poreikį atvyksta aukščiau nurodytu adresu.
4. XDR diegimas ir konfigūravimas apima du etapus tokiais terminais:
   1. Pirmas etapas - darbo vietose XDR diegimo ir konfigūravimo terminas (įskaitant licencijų aktyvavimą) - 30 k. d. nuo viešojo pirkimo-pardavimo sutarties (toliau – Sutartis) įsigaliojimo dienos;
   2. Antras etapas – Viso XDR sprendimo diegimas ir konfigūravimas – 90 k. d. nuo Sutarties įsigaliojimo dienos.
   3. Visos licencijos turi turėti palaikymą tiek, kiek turi pati XDR sistema (36 mėn. nuo licencijų aktyvavimo).
5. Pasiūlymo pateikimo metu siūlomai XDR sistemai neturi būti viešai paskelbta programinės įrangos gyvavimo ciklo pabaiga (End of support, End of life ir pan.). Gyvavimo ciklo pabaiga turi būti nustatyta ne anksčiau kaip 5 metai nuo pasiūlymo pateikimo dienos.
6. Tiekėjas turi būti oficialus siūlomos XDR sistemos gamintojas, gamintojo atstovas arba turi rašytinį susitarimą su gamintoju dėl prekybos siūloma XDR sistema. Kartu su pasiūlymu tiekėjas turi pateikti gamintojo įgaliojimą, pažymą, susitarimą ar kitą lygiavertį dokumentą (lygiavertiškumą privalo įrodyti tiekėjas), patvirtinantį, kad tiekėjas yra oficialus gamintojo atstovas arba turi rašytinį susitarimą su gamintoju dėl prekybos siūloma XDR sistema.
7. Tiekėjas turės pasirašyti susitarimą dėl asmens duomenų tvarkymo, kaip tai nustatyta 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas) 28 straipsnio 3 dalyje, kuriame turės būti nustatytas asmens duomenų tvarkymo dalykas ir trukmė, duomenų tvarkymo pobūdis ir tikslas, asmens duomenų rūšis ir duomenų subjektų kategorijos bei Registrų centro prievolės ir teisės.
8. Tiekėjas turi užtikrinti, kad jo darbuotojai atitiks Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo nuostatas.
9. Tiekėjo siūlomos prekės[[1]](#footnote-2) (įskaitant jų gamintojus), paslaugos[[2]](#footnote-3) ar darbai[[3]](#footnote-4) neturi kelti grėsmės nacionaliniam saugumui. Tiekėjas teikdamas ir pasirašydamas pasiūlymą patvirtina, kad jo siūlomas prekės[[4]](#footnote-5) (įskaitant jų gamintojus), paslaugos[[5]](#footnote-6) ir (ar) darbai[[6]](#footnote-7) nekelia grėsmės nacionaliniam saugumui.
10. Prekių gamintojas ar jį kontroliuojantis asmuo negali būti registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose.
11. Prekių tiekimas negali būti vykdomas iš šio Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.
12. Jeigu prekių gamintojas ar teikėjas, ar jį kontroliuojantis asmuo yra nacionaliniam saugumui užtikrinti svarbi įmonė, valstybės įmonė, savivaldybės įmonė, taip pat valstybės valdoma bendrovė ir jų dukterinės bendrovės, išvardytos Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme, šiems subjektams Lietuvos Respublikos viešųjų pirkimų įstatymo 37 straipsnio 9 dalis netaikoma.
13. Perkančioji organizacija, Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme nustatyta tvarka, kreipsis į Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos koordinavimo komisiją (toliau – Komisija) dėl ketinamo sudaryti sandorio atitikties nacionalinio saugumo interesams patikros ir tuo atveju, jeigu Komisija pareikalaus pateikti papildomus dokumentus tiekėjas, tiekėjų grupės partneriai, ir jų pasitelkiami subtiekėjai privalės juos pateikti.
14. Tiekėjas turi užtikrinti, kad siūloma XDR sistema atitinka 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“, nurodytus reikalavimus.

# TAIKOMI REIKALAVIMAI

|  |  |
| --- | --- |
| **Eil. Nr** | **Ne mažesnis reikalaujamas funkcionalumas nei:** |
|  | **Kompiuterinių darbo vietų (stacionarių ir nešiojamų kompiuterių) (2500 vnt.) apsaugai:** |
|  | XDR turi realiu laiku stebėti sistemos veiklą, failų sistemos pakeitimus, registro modifikacijas, procesus, tinklo ryšius ir vartotojų sąveiką. |
|  | Turi palaikyti nuolatinį galinių įrenginių (Endpoint) įvykių stebėjimą (monitoring) ir registravimą (logging). |
|  | Turi gebėti tinkamai funkcionuoti su operacinėmis sistemomis:   * Nuo Microsoft Windows 7 iki aktualiausios Sutarties galiojimo pabaigai; * Nuo macOS Catalina iki aktualiausios Sutarties galiojimo pabaigai; * Ubuntu operacinėmis sistemomis, kurios yra palaikomos programinės įrangos gamintojų. Linux agentai turi teikti vizualizaciją dėl Kernel iš naudotojo erdvės; * Kitos, palaikomos programinės įrangos gamintojų. |
|  | Turi turėti galimybę veikti Air Gap (neturint interneto ryšio) tinkle ir užtikrinti bazinį galinio taško apsaugos platformos (EPP) apsaugos lygį darbo vietoms su nuo Windows XP operacinės sistemos iki aktualiausios Sutarties galiojimo pabaigai. Turi būti užtikrintos galimybės periodiniam agento ir žinių bazių atnaujinimui. |
|  | **Virtualių darbo vietų (1000 vnt.) apsaugai:** |
|  | Turi atitikti visus reikalavimus nurodytus „Kompiuterinių darbo vietų (stacionarių ir nešiojamų kompiuterių) “ dalyje. |
|  | Turi palaikyti, bet neapsiriboti, VMware Horizon ir VMware vSphere virtualias aplinkas. |
|  | Turi būti palaikoma ir suderinama su VMware Linked clones. |
|  | **Elektroninio pašto (2000 vnt. pašto dėžučių) veikiančius Microsoft Exchange (3 MS Exchange serveriai) ir Office 365 Email sprendimu pagrindu:** |
|  | Turi užtikrinti Microsoft Exchange serverių apsaugą. |
|  | Turi analizuoti Office 365 Email funkcionavimą bei imtis veiksmų galimų grėsmių šalinimui. |
|  | Kenksmingas laiškų ir/ar prisegtukų turinys turi būti neutralizuoti prieš jam patenkant į tinklą ir išplintant į „Endpoint“. |
|  | **Fizinių ir virtualių tarnybinių stočių AV PĮ (2500 vnt.) apsaugai:** |
|  | XDR turi būti gebėti tinkamai funkcionuoti su operacinėmis sistemomis:   * Nuo Windows Server 2008 iki aktualiausios Sutarties galiojimo pabaigai; * CentOS, Oracle, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server, Ubuntu ir Rocky Linux operacinėmis sistemomis. Linux agentai turi teikti vizualizaciją dėl Kernel iš naudotojo erdvės; * Kitos, palaikomos programinės įrangos gamintojų. |
|  | XDR turi palaikyti, bet neapsiriboti, Microsoft Hyper-V ir VMware Workstation virtualias aplinkas. |
|  | Turi palaikyti, bet neapsiriboti, AWS, Azure, Google Cloud debesijos sprendimus. |
|  | Turi stebėti Docker ir OpenShift konteinerius, jų veiklą konteinerių ir host aplinkoje. Tai apima konteinerių proceso veiklos stebėseną, failų ir registro įrašų analizę bei tinklo srauto kontrolę. Turi integruotis su konteinerių orkestratoriais, tokiais kaip Kubernetes, siekiant užtikrinti nuolatinį konteinerių saugumą ir valdymą. |
|  | Turi turėti galimybę veikti Air Gap (neturint interneto ryšio) tinkle ir užtikrinti bazinį galinio taško apsaugos platformos (EPP) apsaugos lygį tarnybinėms stotims su nuo Windows Server 2003 operacinės sistemos iki aktualiausios Sutarties galiojimo pabaigai. Turi būti užtikrintos galimybės periodiniam agento ir žinių bazių atnaujinimui. |
|  | **Agento[[7]](#footnote-8) funkcionalumas:** |
|  | Turi užtikrinti galinio taško aptikimo ir atsako (EDR) ir galinio taško apsaugos platformos (EPP) funkcionalumą. |
|  | Turi taikyti apsauga nuo klastojimo (Tamper protection). |
|  | Diegimas ir atnaujinimas turi būti vykdomas nepertraukiant įrenginių ir naudotojų veiklos. |
|  | Turi būti realizuotas administratoriaus informavimas apie tai, kad tam tikrą laikotarpį (pageidautina, kad tokį terminą galėtu nustatyti pats administratorius) agentas nekomunikavo su valdymo konsole. |
|  | Įdiegtas agentas turi neapkrauti operacinės sistemos ir nenaudoti didesnių nei 2 % CPU ir 250 MB RAM resursų esant standartiniam agento veikimui (pvz. kai nėra atliekama pilna disko patikra). |
|  | Turi būti galimybė laikinai išjungti agentą per valdymo konsolę. |
|  | Turi būti galimybė valdyti agentą per žiniatinklio tarpinę tarnybinę stotį „Web proxy“. |
|  | Turi teikti informacinius pranešimus apie atliktus arba artimiausiu metu ketinamus atlikti veiksmus. |
| * 1. j | Turi atlikti visas saugos užtikrinimo funkcijas tiek naudotojo erdvėje, tiek branduolyje (Kernel). |
|  | Trinant agentus tiesiogiai iš operacinės sistemos turi reikalauti įvesti slaptažodį trynimo veiksmo patvirtinimui. |
| * 1. k | Visa Perkančiosios organizacijos informacija, kuri surenkama, kaupiama ir apdorojama bet kurioje iš sprendimo komponenčių, (ypatingai cloud dalyje) privalo būti talpinama tik Europos Sąjungos ribose. |
|  | Turi gebėti tinkamai funkcionuoti su naujausių operacinėmis sistemos atnaujinimu ne vėliau, kaip po 60 dienų atnaujinimo paskelbimo (update release). |
|  | **Funkcionalumas, skirtas kritinių tarnybinių stočių apsaugai** |
|  | Turi užtikrinti tarnybinių stočių failų integralumo stebėjimą Windows Linux platformose (File integrity monitoring/ FIM):   * Turi vykdyti integralumo stebėjimą realiu laiku; * Turi stebėti registrų integralumą; * Turi stebėti veikiančių procesų integralumą; * Turi būti galimybė nustatyti patikimus šaltinius (trusted sources) – galinius įrenginius ar aplikacijas ir nefiksuoti pokyčių juose integralumo vertinimui; |
|  | Turi užtikrinti tarnybinių stočių žurnalinių įrašų stebėjimą, ir informavimą apie aptinkamą įtartiną ar žalingą operacinės sistemos ar programinės įrangos veikimą:   * Turi būti stebimi (įskaitant, bet neapsiribojant) šie žurnalinių įrašų tipai – eventlog, snort, syslog; * Turi turėti galimybę kurti aptikimo taisykles pagal įvadą string ar regex formatais. |
|  | **Valdymo konsolės funkcionalumas:** |
|  | Turi suteikti lanksčias „on-premise“ arba „cloud“ diegimo galimybes. Jeigu Perkančioji organizacija pasirinks savo pagrindinės infrastruktūros apsaugai "cloud" sprendimą, toks pasirinkimas neturi užkirsti kelio Air Gap (neturint interneto ryšio) tinkle veikiančiai Perkančiosios organizacijos infrastruktūrai pritaikyti "on-premise" sprendimą. |
|  | Turi turėti vieną centralizuotą ar kelias, specifiniams uždaviniams skirtas, vieno gamintojo valdymo konsoles, paremtas žiniatinklio (WEB) sprendimu skirtas stebėjimui, valdymui ir reagavimui (response). |
|  | Visi agentai, nepriklausomai nuo operacinės sistemos, į kurią jie įdiegti, ar įrenginio (fizinis/virtualus) turi būti centralizuotai valdomi iš tos pačios grafinės sąsajos (GUI). |
|  | Turi turėti intuityvią ir patogią sąsają saugos analitikams ir administratoriams. Turi palaikyti „customizable dashboards“. |
|  | Visa Perkančiosios organizacijos informacija, kuri surenkama, kaupiama ir apdorojama bet kurioje iš sprendimo komponenčių, (ypatingai cloud dalyje) privalo būti talpinama tik Europos Sąjungos ribose. |
|  | Agentas, įdiegtas nešiojamuose įrenginiuose, turi būti valdomas iš centralizuotos valdymo konsolės, nepriklausomai nuo to, ar nešiojamasis kompiuteris yra įmonės tinkle, ar ne. Netūri būti apribojimo dėl įrenginio būvimo skirtingos geografinėse vietose. |
|  | Turi palaikyti „role-based“ (RBAC) prieigos kontrolę. |
|  | Turi turėti galimybė suplanuoti agento atnaujinimus. |
| * 1. j | Turi palaikyti plečiamumą (Scalability). |
| * 1. k | Turi palaikyti politikos paveldėjimo „Policy inheritence“ principą. Turi būti galimybė atšaukti paveldėjimą. |
| * 1. l | Valdymo konsolė turi palaikyti smulkų rolių valdymą pagal lygį. |
| * 1. m | Pilną prieiga prie duomenų ir valdymo galimybių per aplikacijų programavimo sąsaja (API). |
|  | Turi palaikyti kelių faktorių autentifikavimą (MFA) ir vieningo autentifikavimo sistema (SSO) ne prasčiau negu SAML 2.0. |
| * 1. o | Turi turėti galimybę užblokuoti (izoliuoti) rizikingą „Endpoint“. Tačiau tuo pat metu turi išlaikyti visas izoliuoto „Endpoint“ valdymo galimybes (įskaitant, bet neapsiribojant, komandų perdavimu, įvykių žurnalų (Event log) peržiūra ir atsiuntimu ir tt.). |
| * 1. p | Turi gebėti atpažinti įrenginius pagal tipus: kompiuteris, tarnybinė stotis, virtualus įrenginys, daiktų interneto (IoT) įrenginys, pramoninės valdymo sistemos (ICS) įrenginys ir tt. |
| * 1. r | Turi taikyti ugniasienės funkcionalumą „Endpoint“. Taikoma ugniasienė turi būti konfigūruojama, esant poreikiui, atskyrai kiekvienam „Endpoint“. |
|  | Sprendimas privalo turėti išplėstinę užklausų kalbą, kuri palaiko reguliarias išraiškas (regex), JSON, duomenų agregavimą, manipuliavimą laukų vertėmis, duomenų iš skirtingų šaltinių apjungimą ir  vizualizavimą. |
|  | Sprendimas turi turėti vedlį, kuris leidžia iš bet kurio sistemos lango atlikti:   * Įrenginio, naudotojo, IP adreso, domeno, failo vardo, failo kelio paiešką; * Pridėti maišos raktą į leidžiamų ar draudžiamų failų sąrašą; * Sukurti naujus statinius kenkėjiškus indikatorius (indication of compromise – IOC); * Izoliuoti galinį įrenginį; * Paleisti kenkėjiško kodo skenavimą galiniame įrenginyje; * Inicijuoti terminalo prieigą prie galinio įrenginio. |
|  | Sprendime turi būti galima pridėti elgsenos kenkėjiškus indikatorius (Behavior indication of compromise – BIOC). BIOC taisyklės turi leisti aprašyti taktikas ir technikas bei procedūras. |
|  | Sprendime turi būti galima pridėti IOC įskaitant bet neapsiribojant:   * MD5 arba SHA256 failo maišos suma; * failo vardas; * failo kelias; * domenas; * gavėjo (destination) IP adresas. |
|  | Sprendimas turi palaikyti integracijas su trečiųjų šalių grėsmių informacijos srautais (įskaitant bet neapsiribojant) JSON ir CSV formatais incidento informacijos praturtinimui. |
|  | Turi būti galimybė pašalti nesusijusius įvykius iš incidento. |
|  | Turi būti funkcionalumas keisti incidento prioritetą rankiniu ir automatiniu būdų. |
|  | Turi būti funkcionalumas leidžiantis įrenginius rankiniu būdu grupuoti į statines grupes. |
|  | Sprendimas turi leisti nuotoliniu būdu prisijungti prie galinių įrenginių, kuriuose įdiegti sprendimo agentai. Turi būti galimybė nuotoliu atlikti ne mažiau kaip šiuos veiksmus:   * Grafinėje failų tvarkyklėje Windows, MacOS, Linux sistemose peržiūrėti, atsisiųsti, pervardinti arba perkelti failus; * Nutraukti, sustabdyti ar atstatyti sustabdytą procesą; * Pažymėti procesus; * Atsisiųsti failus; * Patikrinti failo maišos sumos verdiktą; * Vykdyti operacinės sistemos komandas; * Vykdytis Python komandines eilutes. |
| * 1. s | Turi turėti galimybę automatiškai tikrinti prijungtas išorines laikmenas (išorinės laikmenos pradedamos automatiškai tikrinti jas prijungus ar kai bandoma vykdyti išorinėse laikmenose esančius failus ar kt.). Turi gebėti klasifikuoti prijungtus įrenginius pagal įrenginio duomenis: gamintojo kodą, modelį, serijinį ir kt. |
| * 1. t | Turi gebėti automatiškai įdiegti agentus į naujai aptiktus įrenginius. |
| * 1. u | Valdymo veikla turi būti audituojama su galimybe siųsti audito įrašus į išorines sistemas (pvz. SIEM ir kitą). |
| * 1. v | Turi būti integruojamas su saugos organizavimo, automatizavimo ir reagavimo platformomis (pvz. SOAR). |
| * 1. z | Turi atitikti standartus šifravimo protokolams. Turi šifruoti duomenis „at rest“ ir „in transit. Visi veiklos duomenys turi būti saugomi šifruotu pavidalu. |
| * 1. a | Turi būti galimybė administratoriui siųsti pranešimus elektroniniu paštu (pvz. dėl atnaujinimų, įprastinės veiklos sutrikimų, aptikimų ir tt.). |
| * 1. a | Turi leisti generuoti ataskaitas, pagal administratoriaus pasirinktus parametrus (customizable) PDF ir HTML formatu. |
|  | **Apsaugos nuo grėsmių funkcijos:** |
|  | Turi užtikrinti apsauga nuo žinomų ir nežinomų kenkėjiškų programų, trojos arklių, įsilaužimo įrankių, išpirkos programų (ransomware), atminties išnaudojimo, netinkamo scenarijaus naudojimo, blogų makrokomandų, atakų nenaudojant bylų ir kita. |
|  | Turi analizuoti zip, rar, 7z ir kitų populiariausių archyvavimo formatų failus. |
|  | Turi aptikti bei sustabdyti grėsmes, nustatyti plėtimo pradžia ir priežastį. |
|  | Turi užtikrinti nuolatinį įrenginių skenavimą ir automatinę apsaugą nuo pažeidžiamumų (vulnerabilities) išnaudojimo:   * Turi būti atliekamas nuolatinis pažeidžiamumų skenavimas (ne rečiau kaip kartą per parą) ir atvaizduojami visi aptikti pažeidžiamumai pagal jų tipinių spragų ir pažeidžiamumų identifikacinius numerius (Common Vulnerabilities and Exposures – CVE); * Turi turėti galimybės atpažinti ir blokuot XSS, SQL injection atakas. |
|  | Turi grupuoti įvykius (automatiniu arba rankiniu būdu) ir rodyti juos kartu laiko juostoje incidento tyrimui. Pranešimai susiję su ta pačia ataka turi būti automatiškai sujungiami į vieną. |
|  | Turi atlikti pagrindinių priežasčių (angl. root cause) analizę. |
|  | Failai turi būti analizuojami tiek jos įrašant (write), tiek vykdant (execute). |
|  | Turi būti vertinama elgseną (angl. behavioral analysis), pagal ją aptinkamos grėsmes ir joms užkirsti taikomos efektyviausios apsaugos priemonės. |
|  | Turi būti taikoma apsauga prieš „Zero-Day“ atakas analizuojant elgesį „Endpoint“, o ne tik ieškant jau nustatyto kenksmingo turinio pavyzdžių. |
|  | Turi būti taikoma apsauga net tada, kai visa sistema nėra prijungta prie tinklo arba Endtpoint yra izoliuotas (Stand-alone). |
|  | Analizei turi būti naudojamas dirbtinis intelektas arba mašininis mokymasis (machine learning). |
| * 1. j | Turi būti taikoma apsauga nuo kenkėjiško vykdomojo kodo (pvz. Scripts). |
| * 1. k | Turi būti taikoma apsauga nuo skverbimosi gilyn, kai mėginama per vieną užkrėstą „Endpoint“ patekti į kitus įrenginius (Lateral Movement). |
| * 1. l | Turi būti taikomi stebėjimas ir apsauga nuo pažeidžiamumų išnaudojimo (exploit vulnerabilities) ir befailių (fileless) atakų. |
| * 1. m | Turi būti nustatomos potencialiai nepageidaujamos programos. |
| * 1. n | Turi būti taikomi stebėjimas ir apsauga nuo vidinių grėsmių. |
|  | Turi būti galimybė atsisiųsti galimai kenkėjišką failą iš valdymo konsolės tolesnei analizei. |
| * 1. p | Turi būti teikiamas grėsmės analizės vizualinis proceso medis. |
| * 1. r | Grėsmės analizės procesas turi atitikti MITRE „Attack Framework“. |
|  | Turi turėti nežinomų paleidžiamųjų (angl. executable) programų patikros sprendimą smėliadėžę (angl. sandbox). Smėliadėžė turi galėti patikrinti šiuos (įskaitant, bet neapsiribojant) failus:  .exe, .scr, .doc, .docm, .docx, xls, .xlsm, .xlsx, .dll, .ocx; .zip, .rar, .7z failus;  APK failus;  MAC OS failus;  DMG failus;  Linux ELF failus;  Kitą. |
|  | Turi būti realizuotas informavimas apie neteisingą smėliadėžės nustatymą ir/ar failui taikytą įvertinimą. |
|  | Turi būti pateikiamas patikimų programinės įrangos tiekėjų sąrašas (trusted signers). Sprendime turi būti realizuotas periodinis patikimų trusted signers sąrašo atnaujinimus. |
|  | Turi būti galimybė administratoriui savarankiškai įtraukti programų parašus į patikimų programinės įrangos tiekėjų sąrašą. Turi būti galimybė nurodyti skirtingus sąrašus skirtingoms įrenginių grupėms. |
| * 1. s | Turi būti galimybė vykdyti paiešką grėsmės analizės duomenyse pagal Endpoint pavadinimą, OS, URL, tinklo informaciją ir tt. |
| * 1. t | Turi būti galimybė ieškoti failų pagal failo pavadinimą, failo kūrimo, modifikavimo ar ištrynimo datą. |
| * 1. u | Turi būti galimybė ieškoti failų naudojant failo kelią, failų maišos (*hash*) vertę „MD5, SHA256“ ar registro informaciją; |
| * 1. v | Turi būti galimybė ieškoti tinklo duomenų pagal šaltinio IP, paskirties IP, šaltinio portą, paskirties portą ir tt. |
| * 1. z | Turi būti galimybė ieškoti procesų duomenų naudojant proceso pavadinimą, proceso PID, proceso PID po perkėlimo, pagrindinio proceso pavadinimą, proceso paleidimo laiką, proceso komandos eilutę ar veikiančio proceso parašą. |
| * 1. a | Turi būti galimybė ieškoti incidento pagal jo ID. |
|  | Turi būti galimybė bet kuriame analizuojamame įvykyje pamatyti visus susijusius įvykius. |
| * 1. a | Incidentų duomenys turi būti prieinami pakartotinei analizei ne mažiau kaip 365 d. |
| * 1. a | Neapdoroti duomenys (Raw data, telemetry ir pan.) turi būti saugomi ne mažiau kaip 30 dienų. |
|  | **Reikalavimai atakos perimetro valdymo bei organizacijos rizikų vertinimo (Attack Surface Management – ASM) funkcionalumui:** |
|  | Turi gebėti aptikti ir atvaizduoti visus žinomus (su įdiegtais agentais) ir nežinomus (be įdiegto agento) resursus tinklo viduje, skenuojant vidinę tinklo komunikaciją ir aptinkant IP adresus. |
|  | Turi turėti funkcionalumą integracijai ir gebėti pasiimti duomenis iš ne mažiau kaip šių šaltinių:   * Virtualių ir fizinių darbo vietų ir tarnybinių stočių; * Microsoft Azure AD ir on-premise AD; * Microsoft Office 365 aplinkos; * Pažeidžiamumų skenavimo įrankių Qualys, Nessus ir kt. |
|  | Turi būti galimybė kurti automatizuotas politikas (Playbooks) rizikos laipsniui mažinti be administratoriaus įsikišimo. |
|  | **Versija:**  Turi būti siūloma naujausia stabili programinės įrangos versija, oficialiai gamintojo paskelbta internete. |
|  | **Palaikymas:**  Turi būti siūlomas gamintojo garantuojamas 36 mėn. nemokamas aptarnavimas, teisė gauti klaidų pataisymus, naujausias programinės įrangos versijas, o iškilus problemai kreiptis į gamintoją tiesiogiai internetu, elektroniniu paštu (paslaugos tipas 24x7) ir kt. Taip pat suteikiama prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos. |
|  | **Diegimas** |
|  | Sprendimo diegimą turi atlikti kvalifikuoti tiekėjo specialistai atitinkantys siūlomo Sprendimo gamintojo diegėjams ir/ar administratoriams taikomus reikalavimus. |
|  | Sprendimas turi būti įdiegta į visus Perkančios organizacijos įrenginius. Tikslus įrenginių, į kurios privalomas diegimas, skaičius bus pateiktas po Sutarties pasirašymo. |
| * 1. b. | Suderinus su Perkančiąja organizacija turi būti sukonfigūruoti Sprendimo pažeidžiamumo aptikimo ir užkardymo parametrai. |
| * 1. c | Turi būti sukonfigūruoti tinklo ir žurnalinių įvykių saugojimo nustatymai. |
|  | Turi būti sukonfigūruotos pagrindines saugumo ataskaitos, kurios, taip pat, būtų automatiškai siunčiamos elektroniniu paštu nurodytiems asmenims. |
|  | **Darbuotojų mokymai** |
|  | Į Sprendimo kainą turi būti įskaičiuoti 3 Perkančiosios organizacijos darbuotojų siūlomos AV PĮ administravimo ir naudojimo, ne trumpesni nei 48 val., mokymai. Mokymai turi būti pravesti per 30 kalendorinių dienų nuo Sutarties įsigaliojimo dienos. |
|  | Mokymai turi būti pravedami lietuvių arba anglų kalba, Perkančiosios organizacijos, Tiekėjo pasirinktuose patalpose arba nuotoliniu būdu. Visi mokesčiai, susiję su mokymais (pvz., mokymų kaina, transporto išlaidos, apgyvendinimo išlaidos ir kt.), turi būti įskaičiuoti į bendrą kainą. |
|  | Mokymų dalyviams turi būti išduotas kursų baigimo pažymėjimas, patvirtinantis, kad dalyviai yra susipažinę su įrangos veikimo ir administravimo pagrindiniais principais ir geba atlikti detalių ekspertinių žinių nereikalaujančias Sprendimo administravimo užduotis. |
|  | Perkančiosios organizacijos darbuotojai turi būti apmokyti atlikti visus būtinus sprendimo diegimus savarankiškai. |

**III. TAIKOMI APLINKOS APSAUGOS REIKALAVIMAI**

1. Atsižvelgiant į tai, kad perkamos Prekės yra programinė įranga (licencijos), vadovaujantis Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508, 4.4.3. p Pirkimas laikomas žaliuoju.

1. Taikoma, kai perkamos prekės. [↑](#footnote-ref-2)
2. Taikoma, kai perkamos paslaugos. [↑](#footnote-ref-3)
3. Taikoma, kai perkami darbai. [↑](#footnote-ref-4)
4. Taikoma, kai perkamos prekės. [↑](#footnote-ref-5)
5. Taikoma, kai perkamos paslaugos. [↑](#footnote-ref-6)
6. Taikoma, kai perkami darbai. [↑](#footnote-ref-7)
7. Agentas – tai aplikacija arba programa, įdiegiama į galinio įrenginio operacinę sistemą, kuri užtikrina konkrečiam sprendimui būtinų funkcijų atlikimą ir komunikaciją su centralizuota valdymo konsole. [↑](#footnote-ref-8)