|  |  |  |
| --- | --- | --- |
| Informuojame, kad 2024 m. lapkričio 8 d., lapkričio 19 d., lapkričio 20 d., lapkričio 21 d. Centrinės viešųjų pirkimų informacinės sistemos priemonėmis gavome tiekėjų klausimus „Išplėstinio aptikimo ir reagavimo sistema (XDR)“ viešajame pirkime (pirkimo numeris 743995), teikiame klausimus (kalba netaisyta) ir atsakymus į juos: | | |
| **Nr.** | **Klausimas/Prašymas** | **Atsakymas** |
| 1. | Dėl 3. punkto reikalavimo  Ar galite įvardinti koks kiekis iš nurodytų 2000 vnt. pašto dėžučių yra saugomas Exchange serveriuose, o koks Office 365 sprendime?  Taip pat ar galite pateikti kiekį el.pašto vartotojų (jei produktas licencijuojamas per el.pašto vartotojus, o ne pašto dėžutes)? | Paaiškiname, kad naudojamas sprendimas licencijuojamas per pašto dežutes. Šiuo metu visos įvardintos pašto dežutės yra saugomos Exchange serveriuose. Perkančioji organizacija ateityje planuoja migravimą į Microsoft Office 365 sprendimą. |
| 2. | Dėl 4.4. punkto reikalavimo  Siūlomo gamintojo sprendimas konteinerius licencijuoja atskirai. Ar galite įvardinti koks kiekis konteinerių „nod‘ų“ turi būti apsaugota? | Paaiškiname, kad konkrečiai Docker ir OpenShift konteinerių (nodų) kiekio Perkančioji organizacija negali, nes jis yra nuolat kintantis bei sutarties galiojimo laikotarpiu gali sudaryti iki 250 vnt. nuo viso tarnybinių stočių skaičiaus. |
| 3. | Dėl 5.9. punkto reikalavimo  Siūlomo gamintojo sprendime tam tikros saugumo funkcijos branduolyje (kernel) yra gilesnės nei vartotojo erdvėje pvz. "low level API hooking monitoring" reikalauja "kernel" prieigos, ir šios funkcijos nebūtų galima realizuoti vartotojo erdvėje. Tad paraidžiui tai kaip įvardinta, negalima teigti, kad visos saugos užtikrinimo funkcijos yra vienodos abejose erdvėse. Ar tai atitiks reikalavimą? | Perkančioji organizacija pasiūlymų techninį vertinimą atliks tik susipažinimo su pasiūlymais metu (suėjus pasiūlymų pateikimo terminui). Pasiūlymas turi atitikti techninės specifikacijos reikalavimus. |
| 4. | Dėl 5.12. punkto reikalavimo  Siūlomo gamintojo įprastoje praktikoje naujausios operacinių sistemų versijos tampa palaikomos per trumpiau nei 30 dienų, tačiau tokia praktika kaip ir įsipareigojimas nėra gamintojo dokumentuota. Ar tai atitiks reikalavimą? | Perkančioji organizacija pasiūlymų techninį vertinimą atliks tik susipažinimo su pasiūlymais metu (suėjus pasiūlymų pateikimo terminui). Pasiūlymas turi atitikti techninės specifikacijos reikalavimus. |
| 5. | Dėl 6. punkto reikalavimo  Prašome įvardinti koks yra kritinių tarnybinių stočių kiekis? Siūlomas gamintojas šį funkcionalumą licencijuoja atskirai, dėl to siekiant pateikti ekonomiškai geriausią pasiūlymą tokio tipo informacija yra būtina žinoti jau šiame etape. | Paaiškiname, kad tikslaus kritinių tarnybinių stočių kiekio Perkančioji organizacija nurodyti negali, nes jis nuolat kintantis ir sutarties galiojimo laikotarpiu gali sudaryti iki 300 vnt. nuo viso tarnybinių stočių skaičiaus. |
| 6. | Dėl 7.20. punkto reikalavimo  Siūlomo gamintojo sprendime stebėti ir/ar blokuoti pridedamą failo vardą (file, ar pagal failo kelią, galima per aplikacijų kontrolės modulį. Visus kitus reikalavime išvardintus IOC galima pridėti prie įtartinų objektų sąrašo (suspicious objects). Ar tai atitiks reikalavimą? | Perkančioji organizacija pasiūlymų techninį vertinimą atliks tik susipažinimo su pasiūlymais metu (suėjus pasiūlymų pateikimo terminui). Pasiūlymas turi atitikti techninės specifikacijos reikalavimus. |
| 7. | Dėl 7.25. punkto reikalavimo dalies „Grafinėje failų tvarkyklėje Windows, MacOS, Linux sistemose peržiūrėti, atsisiųsti, pervardinti arba perkelti failus.“  Siūlomo gamintojo sprendime prisijungus nuotoliniu būdu šiuos veiksmus galima atlikti tik naudojant komandinę eilutėję (CLI), o ne grafinėje failų tvarkytuvėje, ar tai atitiks reikalavimą? | Perkančioji organizacija pasiūlymų techninį vertinimą atliks tik susipažinimo su pasiūlymais metu (suėjus pasiūlymų pateikimo terminui). Pasiūlymas turi atitikti techninės specifikacijos reikalavimus. |
| 8. | Dėl 7.25. punkto reikalavimo dalies „Nutraukti, sustabdyti ar atstatyti sustabdytą procesą.“ Siūlomo gamintojo sprendime procesą galima nutraukti, tačiau sustabdyti ar atstatyti prisijungus per nuotolį galimybės nėra, ar tai atitiks reikalavimą? | Perkančioji organizacija pasiūlymų techninį vertinimą atliks tik susipažinimo su pasiūlymais metu (suėjus pasiūlymų pateikimo terminui). Pasiūlymas turi atitikti techninės specifikacijos reikalavimus. |
| 9. | Dėl 7.27. punkto reikalavimo  Siūlomo gamintojo sprendimo konsolėje automatiškai aptinkami visi įrenginiai, kuriuose nėra agento ir jie atvaizduojami sąraše, tačiau paleisti automatinio agento įdiegimo konsolėje nėra galimybės (kas būtų nesaugu laikantis bendrųjų saugumo praktikų). Įvardintam funkcionalumui gali būti naudojami atskiri agentų diegimo įrankiai. Ar tai atitiks reikalavimą? | Perkančioji organizacija pasiūlymų techninį vertinimą atliks tik susipažinimo su pasiūlymais metu (suėjus pasiūlymų pateikimo terminui). Pasiūlymas turi atitikti techninės specifikacijos reikalavimus. |
| 10. | Dėl 8.4. punkto reikalavimo dalies „Turi turėti galimybės atpažinti ir blokuot XSS, SQL injection atakas“.  Šis funkcionalumas įprastai yra taikomas kritinėms tarnybinėms stotimis. Patikslinkite ir įvardinkite tarnybinių stočių kiekį, kurioms būtų būtinas šis reikalavimas. Siekiant pateikti ekonomiškai geriausią pasiūlymą tokio tipo informacija yra būtina žinoti jau šiame etape. | Paaiškiname, kad tikslaus tarnybinių stočių kiekio Perkančioji organizacija nurodyti negali, nes jis nuolat kintantis ir sutarties galiojimo laikotarpiu gali sudaryti iki 300 vnt. nuo viso tarnybinių stočių skaičiaus. |
| 11. | Dėl 8.20. punkto reikalavimo dalies „<...APK Failus...>“  Siūlomo gamintojo sprendimas APK formato failams patikrinti naudoja atskirą web svetainę. Visi kiti formatai gali būti automatiškai patikrinti debesijos pagrindu veikiančioje smėliadėžėje (Cloud Sandbox). Ar tai atitiks reikalavimą? | Perkančioji organizacija pasiūlymų techninį vertinimą atliks tik susipažinimo su pasiūlymais metu (suėjus pasiūlymų pateikimo terminui). Pasiūlymas turi atitikti techninės specifikacijos reikalavimus. |
| 12. | Please clarify point 4.1 of the technical specification - does the solution have to cover specific Linux distribution versions or only the latest ones? | Paaiškiname, kad reikalavimas taikomas Linux distribucijos operacinėmis sistemomis, kurios yra palaikomos programinės įrangos gamintojų (t.y. nėra suėjęs End of Life terminas).  We explain that the requirement applies to Linux distribution operating systems that are supported by the software vendors (i.e., those that have not reached their End of Life date). |
| 13. | Please clarify regarding point 4.4 of the technical specification - it is not clear from the specification what is the number of cores in the mentioned containers. Could you please share? | Tipinę konteinerio specifikacija sudaro CPU 2-8, RAM 2-32. Didžiausią - 16CPU, 66Gb RAM  A typical container specification consists of 2-8 CPUs and 2-32 GB of RAM. The maximum configuration includes 32 CPUs and 66 GB of RAM |
| 14. | Please clarify regarding technical specification point 7.1. You mention "The Procuring Organization will choose a "cloud" solution for the protection of its main infrastructure, such a choice must not prevent the use of an "on-premise" solution for the Procuring Organization's infrastructure operating in the Air Gap network (without an Internet connection) - will you provide access to the Internet through a proxy server? | Paaiškiname, kad ten, kur saugumo reikalavimai tai leidžia, bus naudojami proxy sprendimai. Tačiau, tam tikros sistemos neturės jokio ryšio su internnetu, nei tiesiogiai, nei per proxy serverius, nei su vidiniais tinklais.  We explain that, where security requirements allow, proxy solutions will be used. However, certain systems will have no connection to the internet, either directly, through proxy servers, or with internal networks. |
| 15. | Please clarify on point 7.10 of the technical specification - could you provide an example of the required Policy inheritance? | Jei išjungiate „Paveldėti nustatymus iš tėvų politikos“ nustatymą vaiko politikoje, tuomet galėsite keisti visus nustatymus vaiko politikoje, net jei kai kurie nustatymai yra užrakinti tėvų politikoje.  If you disable Inherit settings from parent policy in a child policy, then you can change all of the settings in the child policy, even if some settings are locked in the parent policy. |
| 16. | Please clarify about point 8.6 of the technical specification - maybe you could explain the requirement in more detail, what is meant by root cause analysis. Be it causing an incident, first warning, etc. t? | Gebėjimas nustatyti pagrindines problemų priežastis, siekiant rasti tinkamus problemų sprendimo būdus.  Ability to discovering the root causes of problems in order to identify appropriate solutions. |
| 17. | Please clarify on point 8.21 of the technical specification - what specific sandbox settings do you mean? | Paaiškiname, kad funkcionalumas turi informuoti, jeigu smėliadėžės nustatymai klaidingi, pvz., \*.deb, \*.rpm tipo failai tikrinami Windows tipo operacinėje sistemoje.  The functionality should inform if the sandbox settings are incorrect, e.g. \*.deb, \*.rpm type files are checked on a Windows type operating system. |
| 18. | Taikomų reikalavimų lentelės 1.3. punkte reikalaujama, jog XDR sistema gebėtų tinkamai funkcionuoti su “Nuo macOS Catalina iki aktualiausios Sutarties galiojimo pabaigai” operacinėmis sistemomis. Kadangi macOS Catalina operacinė sistema buvo išleista 2019 metais ir yra pasenusi(kelia saugumo rizikas), siūlome pakeisti šį reikalavimą bent į “macOS Sonoma iki aktualiausios Sutarties galiojimo pabaigai”. | Paaiškiname, kad reikalavimas nustatytas atsižvelgiant į šiuo metu turimą Perkančiosios organizacijos valdomą infrastruktūrą bei galiojančius teisės aktų reikalavimus, todėl keičiamas nebus. |
| 19. | Taikomų reikalavimų lentelės 4.1. punkte reikalaujama, jog “XDR turi būti gebėti tinkamai funkcionuoti su operacinėmis sistemomis: Nuo Windows Server 2008 iki aktualiausios Sutarties galiojimo pabaigai;”. Kadangi Windows Server 2008 operacinė sistema yra pasenusi(kelia saugumo rizikas), siūlome pakeisti šį reikalavimą pakeliant minimalią palaikomą versiją bent į “Windows Server 2008 SP2/R2”. | Paaiškiname, kad reikalavimas nustatytas atsižvelgiant į šiuo metu turimą Perkančiosios organizacijos valdomą infrastruktūrą bei galiojančius teisės aktų reikalavimus, todėl keičiamas nebus. |
| 20. | Taikomų reikalavimų lentelės 4.5. punkte reikalaujama, jog “turi turėti galimybę veikti... tarnybinėms stotims su nuo Windows Server 2003 operacinės sistemos iki aktualiausios...” Windows Server 2003 operacinė sistema yra pasenusi(kelia saugumo rizikas), siūlome pakeisti šį reikalavimą pakeliant minimalią palaikomą versiją bent į “Windows Server 2003 SP2/R2”. | Paaiškiname, kad reikalavimas nustatytas atsižvelgiant į šiuo metu turimą Perkančiosios organizacijos valdomą infrastruktūrą bei galiojančius teisės aktų reikalavimus, todėl keičiamas nebus. |
| 21. | Taikomų reikalavimų lentelės 7.18 punkte yra rašoma “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.” Siūlome šį punktą panaikinti, kadangi reikalavimas yra perteklinis, nesukuria pridėtinės vertės saugumui bei riboja konkurenciją. | Tai yra tipiniai valdymo funkcionalumai, kuriuos saugos administratoriai naudoja kibernetinių incidentų valdymo veikloje. |
| 22. | Taikomų reikalavimų lentelės 7.20. rašoma  „Sprendime turi būti galima pridėti IOC įskaitant bet neapsiribojant:  MD5 arba SHA256 failo maišos suma;  failo vardas;  failo kelias;  domenas;  gavėjo (destination) IP adresas.“  Pagal gerąsias praktikas minimą funkcionalumą užtikrina SIEM įrankis, kurį perkančioji organizacija turi įsidiegusi ir jis saugo ir apdoroja visus IT infrastruktūros įrašus įskaitant ir IOC įrašus. Siūlome nedubliuoti funkcionalumų skirtinguose saugumo įrankiuose. Siūlome panaikinti šį reikalavimą. | Paaiškiname, kad reikalavimas nustatytas atsižvelgiant į kitus Perkančiosios organizacijos projektus bei šiuo metu turimą Perkančiosios organizacijos valdomą infrastruktūrą bei galiojančius teisės aktų reikalavimus, todėl keičiamas nebus. |
| 23. | Taikomų reikalavimų lentelės 7.21. punkte rašoma, kad “Sprendimas turi palaikyti integracijas su trečiųjų šalių grėsmių informacijos srautais (įskaitant bet neapsiribojant) JSON ir CSV formatais incidento informacijos praturtinimui”. Pagal gerąsias praktikas minimą funkcionalumą užtikrina SIEM įrankis, kurį perkančioji organizacija turi įsidiegusi ir jis saugo ir apdoroja visus IT infrastruktūros įrašus įskaitant ir IOC įrašus. Siūlome nedubliuoti funkcionalumų skirtinguose saugumo įrankiuose. Siūlome panaikinti šį reikalavimą. | Paaiškiname, kad reikalavimas nustatytas atsižvelgiant į kitus Perkančiosios organizacijos projektus bei šiuo metu turimą Perkančiosios organizacijos valdomą infrastruktūrą bei galiojančius teisės aktų reikalavimus, todėl keičiamas nebus. |
| 24. | Taikomų reikalavimų lentelės punkte 7.22. rašoma “Turi būti galimybė pašalti nesusijusius įvykius iš incidento”. Siūlome pašalinti šį reikalavimą, kadangi šios funkcionalumo realizavimas mažina surinktų  2 / 2  duomenų autentiškumą bei sukelia rizika, kad saugumo incidento tyrimo procesas bus sutrikdytas(apsunkintas,  prailgintas ar kitaip apribotas). | Reikalavimas nustatytas atsižvelgiant į naujus KSĮ reikalavimus dėl pranešimų apie incidentus per 72 val. |
| 25. | Taikomų reikalavimų lentelės 9.2. punkte rašoma “Turi turėti funkcionalumą integracijai ir gebėti  pasiimti duomenis iš šių šaltinių: … - Pažeidžiamumų skenavimo įrankiu Qualys, Nessus ir kt.” Ar siūlomas  sprendimas turi turėti galimybę integruotis bent su vienu pažeidžiamumų skenavimo įrankiu? | Taip. |
| 26. | Kiek turite įrenginių, kuriuose veikia WinXP ? Ar jos yra DMZ aplinkoje? | Perkančioji organizacija prašomos informacijos pateikti viešai negali, nes ją priskiria konfidencialiai (Įmonės informacinių sistemų ir kompiuterinių tinklų struktūros konfigūracija). Su šia informacija pagal poreikį bus supažindintas tiekėjas sutarties vykdymo metu. |
| 27. | TS p. 1.4 Ar „Air Gapped“ tinklas apima ir OT (angl. operational technology) naudojamą tinklą? | Perkančioji organizacija prašomos informacijos pateikti viešai negali, nes ją priskiria konfidencialiai (Įmonės informacinių sistemų ir kompiuterinių tinklų struktūros konfigūracija). Su šia informacija pagal poreikį bus supažindintas tiekėjas sutarties vykdymo metu. |
| 28. | Ar norite apsaugoti svečio operacinę sistemą virtualioje mašinoje, virtualių mašinų architektūrą? | Perkančioji organizacija prašomos informacijos pateikti viešai negali, nes ją priskiria konfidencialiai (Įmonės informacinių sistemų ir kompiuterinių tinklų struktūros konfigūracija). Su šia informacija pagal poreikį bus supažindintas tiekėjas sutarties vykdymo metu. |
| 29. | Kokį sprendimą / paslaugą naudojate programinės įrangos įdiegimui per tinklą/ tinkle? | Perkančioji organizacija prašomos informacijos pateikti viešai negali, nes ją priskiria konfidencialiai (Įmonės informacinių sistemų ir kompiuterinių tinklų struktūros konfigūracija). Su šia informacija pagal poreikį bus supažindintas tiekėjas sutarties vykdymo metu. |
| 30. | Kiek serverių yra laikote patalpose? | Perkančioji organizacija prašomos informacijos nepateiks, nes ši informacija nėra susijusi su pirkimo objektu. |
| 31. | Kuris skyrius ir vaidmuo bus atsakingas už  paslaugų pagal pirkimo objektą įgyvendinimo projektą? | Perkančioji organizacija prašomos informacijos nepateiks, nes ši informacija nėra susijusi su pirkimo objektu. |
| 32. | Ar yra aiškus valdymo modelis visoms administracinėms užduotims ir sprendimų priėmimui, susijusiems su techninėje analizėje paminėtais sprendimais? | Perkančioji organizacija prašomos informacijos pateikti viešai negali, nes ją priskiria konfidencialiai (Įmonės informacinių sistemų ir kompiuterinių tinklų struktūros konfigūracija). Su šia informacija pagal poreikį bus supažindintas tiekėjas sutarties vykdymo metu. |
| 33. | TS p. 4.1  Ar jums reikalinga palaikyti konkrečias senesnes Linux versijas ar tik aktualiausias | Paaiškiname, kad reikalavimas taikomas Linux distribucijos operacinėmis sistemomis, kurios yra palaikomos programinės įrangos gamintojų (t.y. nėra suėjęs End of Life terminas). |
| 34. | TS p. 4.4 Mūsų konteinerių apsaugos sprendimo kainodara grįsta virtualių branduolių skaičiumi. Ar galima gauti apytikslį virtualių branduolių, naudojamų konteinerių talpinimui, kiekį? | Tipinę konteinerio specifikacija sudaro CPU 2-8, RAM 2-32. Didžiausią - 16CPU, 66Gb RAM |
| 35. | TS p. 7.1  „Air Gapped“ tinklo palaikymas - ar svarstytumėte leisti interneto prieigą per Proxy serverį? | Paaiškiname, kad proxy serverio naudojimas priklausys nuo konkrečios sistemos saugumo reikalavimų. Tačiau bus sistemų, kurios neturės jokio ryšio su internetu, nei tiesiogiai, nei per proxy serverius, nei su vidiniais tinklais. |
| 36. | TS p. 7.10 Ar galėtumėte pateikti keletą reikalaujamo „politikos paveldėjimo“ (angl. policy inheritance) funkcionalumo pavyzdžių? | Paaiškiname, kad paveldėjimas reiškia politikos nustatymų automatinį perdavimą į pagalbines (vaiko) grupes iš aukštesnio lygio (tėvų) grupės. |
| 37. | TS p. 8.6 Ar galėtumėte išsamiau paaiškinti reikalavimą, ką reiškia pagrindinė priežastis (pvz., incidento priežastis, pirmasis perspėjimas)? | Paaiškiname, kad tai gebėjimas nustatyti pagrindines problemų priežastis, siekiant rasti tinkamus problemų sprendimo būdus. |
| 38. | TS p. 8.21 Kokie konkretūs smėlio dėžės nustatymai yra reikalingi? | Paaiškiname, kad funkcionalumas turi informuoti, jeigu smėliadėžės nustatymai klaidingi, pvz., \*.deb, \*.rpm tipo failai tikrinami Windows tipo operacinėje sistemoje. |
| 39. | Kiek turite įrenginių, kuriuose veikia WinXP ? Ar jos yra DMZ aplinkoje? | Perkančioji organizacija prašomos informacijos pateikti viešai negali, nes ją priskiria konfidencialiai (Įmonės informacinių sistemų ir kompiuterinių tinklų struktūros konfigūracija). Su šia informacija pagal poreikį bus supažindintas tiekėjas sutarties vykdymo metu. |
| 40. | Good day! Please extend the submission deadline as we still have not received answers to our submissions in 2024. November 8. | Vadovaujantis Atviro konkurso sąlygų 2.1.4. p. Perkančioji organizacija dokumentų paaiškinimą pateikia visiems tiekėjams ne vėliau kaip 6 dienos iki pasiūlymo pateikimo dienos, todėl terminas nebus nukeliamas.  In accordance with paragraph 2.1.4 of the Conditions of Procedure for the Open Call for Tenders, the Contracting Authority shall provide clarification of the documents to all suppliers no later than 6 days before the submission deadline; therefore, the deadline will not be postponed. |
| 41. | It is not clear from the technical specification provided how your servers are managed. Is SCCM used for this? | Perkančioji organizacija prašomos informacijos pateikti viešai negali, nes ją priskiria konfidencialiai (Įmonės informacinių sistemų ir kompiuterinių tinklų struktūros konfigūracija). Su šia informacija pagal poreikį bus supažindintas tiekėjas sutarties vykdymo metu.  The Contracting Authority cannot make the requested information publicly available because it is classified as confidential (specifically, the configuration of the company's information systems and computer network structure). This information will be provided to the supplier as needed during the performance of the contract. |
| 42. | Also, could you share how many specific systems you have, ie how many Windows XP, how many Windows 7, how many Windows Server 2003 and Windows Server 2008? | Perkančioji organizacija prašomos informacijos pateikti viešai negali, nes ją priskiria konfidencialiai (Įmonės informacinių sistemų ir kompiuterinių tinklų struktūros konfigūracija). Su šia informacija pagal poreikį bus supažindintas tiekėjas sutarties vykdymo metu.  The Contracting Authority cannot make the requested information publicly available because it is classified as confidential (specifically, the configuration of the company's information systems and computer network structure). This information will be provided to the supplier as needed during the performance of the contract. |