**PASLAUGŲ PIRKIMO TECHNINĖ SPECIFIKACIJA**

**1. SĄVOKOS IR SUTRUMPINIMAI**

* 1. **Paslaugų gavėjas –** Uždaroji akcinė bendrovė „VILNIAUS VANDENYS“.
  2. **Paslaugų teikėjas –** ūkio subjektas – fizinis asmuo, privatusis ar viešasis juridinis asmuo, kita organizacija ir (ar) jų padalinys įskaitant ūkio subjektus, kurių pajėgumais remiamasi, Subteikėjus, darbuotojus ir kitus teisėtais pagrindais Paslaugų teikimui pasitelktus asmenis.
  3. **Sutartis** – Sutartis, sudaroma tarp Paslaugų teikėjo ir Paslaugų gavėjo dėl Pirkimo objekto.
  4. **Techninė specifikacija** – dokumentas, kuriame apibūdintas pirkimo objektas.
  5. **Priėmimo-perdavimo aktas arba Aktas –** perdavimo–priėmimo aktas arba kitas lygiavertis dokumentas, pasirašomas abiejų Sutarties Šalių, kuriame detaliai (tiksliai nurodant kiekius, apimtis, objektus ir kitą reikšmingą informaciją) nurodomos Paslaugų teikėjo faktiškai Paslaugų gavėjui suteiktos Paslaugos, atitinkančios Techninės specifikacijos nuostatas.
  6. **Užsakymas** – Sutarties pagrindu Paslaugų teikėjui tekstiniu pranešimu, elektroniniu paštu ir (ar) per Paslaugų gavėjo nurodytą informacinę sistemą teikiamas rašytinis dokumentas, kuriame nurodomi Paslaugų kiekiai, suteikimo adresai ir terminas.

1. **PIRKIMO OBJEKTO PAVADINIMAS IR JO KIEKIAI/APIMTYS**
   1. **SIEM įrankio priežiūros ir saugumo analitikos paslaugos** (toliau - **Paslaugos**), kurios susideda iš:
      1. Turimos saugumo informacijos ir įvykių valdymo sistemos LogRhythm SIEM licencijos palaikymo ir gamintojo paslaugų – 1 kompl.;
      2. Turimos saugumo informacijos ir įvykių valdymo sistemos LogRhythm SIEM gamintojo MPS licencijos plėtimo – 1 kompl.;
      3. Eksploatuojamos SIEM sistemos LogRhythm palaikymo, analitikos ir reagavimo paslaugų – 1 kompl.;
      4. Diegimo paslaugos– 1 kompl.
   2. **Kiekiai/Apimtys:** Perkamas Paslaugų kiekis **yra konkretus.**
   3. Paslaugų teikėjas visas galimas išlaidas įskaičiuoja į Paslaugų įkainį ir (ar) kainą. Siūlomame įkainyje ir (ar) kainoje turi būti įskaičiuotos visos Paslaugų teikėjo išlaidos ir mokėtini mokesčiai, būtini tinkamam Sutarties įvykdymui.
   4. Paslaugų teikėjas prisiima visą riziką dėl ne nuo Paslaugų gavėjo priklausančių aplinkybių, dėl kurių padidės su Sutarties vykdymu susijusios Paslaugų teikėjo išlaidos ir Sutarties vykdymas taps sudėtingesnis (Paslaugų teikėjui padidės įsipareigojimų vykdymo kaina). Paslaugų kaina ir (ar) įkainiai jokiais atvejais nebus didinami, išskyrus Pirkimo sąlygose nustatytus kainos ir (ar) įkainių peržiūros procedūros atvejus.
   5. Pirkimo objektas neskaidomas į dalis, todėl Paslaugų teikėjas privalo teikti pasiūlymą visai nurodytai pirkimo objekto apimčiai.
   6. Paslaugų gavėjas taip pat turi teisę, esant poreikiui, pirkti ir kitas Techninėje specifikacijoje nenurodytas, tačiau su pirkimo objektu susijusias Paslaugas. Panašaus pobūdžio Paslaugos, nenumatytos Techninėje specifikacijoje, bus perkamos ne didesnėmis nei susitarimo pasirašymo dieną galiojančiomis Paslaugų teikėjo prekybos vietoje, kataloge ar interneto svetainėje nurodytomis šių paslaugų kainomis, arba, jei tokios kainos neskelbiamos, Paslaugų teikėjo pasiūlytomis, konkurencingomis ir rinką atitinkančiomis kainomis. Bendra tokių nenumatytų Paslaugų vertė negali viršyti 10 (dešimt) proc. Sutarties vertės (EUR be PVM).
2. **REIKALAVIMAI PIRKIMO OBJEKTUI**

**Esamos situacijos aprašymas**

Paslaugų gavėjas eksploatuoja saugumo informacijos ir įvykių valdymo sistemą LogRhythm SIEM. Jai yra reikalingas gamintojo palaikymo pratęsimas bei licencijos išplėtimas dėl planuojamų naujų duomenų šaltinių prijungimo. Taip pat yra perkamos saugumo analitikos paslaugos.

* 1. **Pirkimo objekto aprašymas**
     1. Jei iš šiose techninėse specifikacijose pateiktų duomenų būtų galima daryti prielaidą apie konkrečius pirkimo objekto modelius ar tiekimo šaltinius, konkrečius technologinius procesus ar prekių ženklus, patentus, tipus, konkrečią kilmę ar gamybą, laikoma, kad jie yra tik orientaciniai ir Paslaugų teikėjai gali siūlyti lygiaverčius.
     2. Paslaugų teikėjas turi užtikrinti, kad atliekant saugumo informacijos ir įvykių valdymo sistemos diegimą, nebus sutrikdomas Perkančiosios organizacijos informacinės sistemos bei duomenų perdavimo tinklo darbas. Jeigu Paslaugų gavėjo informacinės sistemos arba duomenų perdavimo tinklo darbas bus trikdomas, numatomi darbai turi būti atliekami ne Paslaugų gavėjo darbo metu ir suderinus su atsakingu už sutarties vykdymą asmeniu.
     3. Paslaugų teikėjo specialistai privalo mokėti lietuvių kalbą arba turi būti užtikrintos kokybiškos vertimo paslaugos Paslaugų teikėjo sąskaita.
     4. Paslaugų teikėjo parengti dokumentai (analizės, projektavimo ir diegimo dokumentacija) turi būti pateikiami lietuvių kalba. Pateiktų dokumentų projektus Paslaugų gavėjas įvertina per 10 darbo dienų nuo pateikimo dienos. Atsižvelgiant į rezultatų apimtį įvertinimo terminas gali būti trumpinamas arba ilginamas.
     5. Saugumo informacijos ir įvykių valdymo sistemos diegimą ir priežiūrą turi atlikti sertifikuoti specialistai, atitinkantys pirkimo dokumentuose keliamus kvalifikacinius reikalavimus. Keliamiems SPS 3 skyriaus 2 lentelėje 2.1.-2.6. punktuose minimaliems kvalifikaciniams reikalavimams, Paslaugų teikėjas privalo pasiūlyti ne mažiau nei 3 (tris) specialistus. Tas pats specialistas gali būti siūlomas į kelias pozicijas.
     6. Paslaugų teikėjas sutarties vykdymui turi turėti 24 valandas per parą 7 dienas per savaitę nenutrūkstamai veikiančią pagalbos tarnybą, kuri turi turėti aprašytą ir veikiantį kreipinių ir incidentų sprendimo procesą, atitinkantį ITIL (ar lygiavertės metodikos) geriausių praktikų rekomendacijas, pagal kurį registruojami gedimų kreipiniai, šalinami gedimai, sekama darbų vykdymo eiga. Paslaugų teikėjo pagalbos tarnyba privalo turėti interneto portalą, atitinkantį ITIL (ar lygiavertės metodikos) IT paslaugų valdymo geriausių praktikų metodiką, kuriame Perkančiosios organizacijos atsakingi asmenys turėtų galimybę registruoti gedimų kreipinius, sekti darbų vykdymo eigą, generuoti ataskaitas. Paslaugų teikėjo pagalbos tarnyboje turi būti komunikuojama lietuvių kalba. Paslaugų teikėjo pagalbos tarnyba turi suteikti galimybes registruoti kreipinius tiek elektroniniu paštu, tiek telefonu, tiek per Web portalą.
     7. SIEM įrankio priežiūros ir saugumo analitiko paslaugos techniniai reikalavimai pateikti lentelėje Nr. 1.

**Lentelė Nr. 1.** SIEM įrankio priežiūros ir saugumo analitiko paslaugos techniniai reikalavimai

|  |  |  |
| --- | --- | --- |
| Eil. Nr. | Charakteristika | Reikalavimas |
| 1. **Eksploatuojamos saugumo informacijos ir įvykių valdymo sistemos** **LogRhythm SIEM licencijos palaikymo ir gamintojo paslaugos (1 vnt.) 1 komplektas pagal žemiau išvardintus reikalavimus** | | |
| 1.1. | Gamintojas, modelio pavadinimas | LogRhythm LR-XM4500 |
| 1.2. | Licencijos ID | 1968318 |
| 1.3. | Licencijos tipas | AI Engine (MPS) – 1000 vnt.;  Data Processor (MPS) [LogRhythm] – 1000 vnt.;  Platform Manager Server – 1 vnt.;  System Monitor Pro – 6 vnt.;  System Monitor Lite – 37 vnt.;  User Threat Detection – 1 vnt. |
| 1.4. | Garantija ir licencijos | Turi būti užtikrintas SIEM sistemos gamintojo garantuojamas garantinis aptarnavimas.  Garantiniu laikotarpiu turi būti užtikrinta:  - programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas);  - teisė gauti analitikos taisykles, skirtas naujoms grėsmėms aptikti;  - teisė gauti koreliavimo taisyklių, normalizavimo taisyklių ir šaltinių reputacijos sąrašų / informacijos atnaujinimus;  - teisė kreiptis į gamintoją, iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, nuo pirmadienio iki penktadienio, nuo 7 iki 18 val. vietos laiku, internetu, elektroniniu paštu arba telefonu;  - prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos;  - 4 darbo valandų trukmės atsakas į techninio aptarnavimo užklausas kritinio gedimo atveju;  - gedimo atveju, įranga turi būti suremontuota arba pateikta pakaitinė įranga ne vėliau, kaip per sekančią darbo dieną nuo pranešimo apie gedimą pateikimo tiekėjui ar gamintojui. |
| 1.5. | Terminas | Paslaugos susideda iš licencijos aktyvavimo ir palaikymo, kuris turi galioti ne trumpiau kaip iki 2026-05-31. |
| 1.6. | Paslaugų teikėjas turi būti įgaliotas gamintojo atstovas, arba turi būti sudaręs atitinkamą sutartį su kitu ūkio subjektu, turinčiu teisę parduoti, prižiūrėti siūlomą įrangą. | Paslaugų teikėjas teikdamas pasiūlymą turi pateikti dokumentą, patvirtinantį, kad jis yra įgaliotas Paslaugų gavėjo turimos SIEM sistemos gamintojo atstovas (pateikiami oficialų atstovavimą patvirtinantys dokumentai) arba yra sudaręs atitinkamą bendradarbiavimo sutartį su kitu ūkio subjektu, turinčiu atitinkamas gamintojo suteiktas teises (pateikiama patvirtinančios sutarties su kita įmone, turinčia teisę atstovauti Paslaugų gavėjo turimos SIEM sistemos gamintoją, skaitmeninė kopija bei ūkio subjektui, su kuriuo sudaryta bendradarbiavimo sutartis, gamintojo išduotas įgaliojimas). |
| 1. **Eksploatuojamos saugumo informacijos ir įvykių valdymo sistemos** **LogRhythm SIEM gamintojo MPS licencijos plėtimas (1 vnt.) 1 komplektas pagal žemiau išvardintus reikalavimus** | | |
| 2.1. | Gamintojas, modelio pavadinimas | LogRhythm LR-XM4500 |
| 2.2. | Eksploatuojamos saugumo informacijos ir įvykių valdymo sistemos LogRhythm SIEM licencijos praplėtimas | Eksploatuojamos saugumo informacijos ir įvykių valdymo sistemos LogRhythm SIEM licencijos praplėtimas papildomu 1000 MPS. |
| 2.3. | Terminas | Paslaugos susideda iš licencijos aktyvavimo ir palaikymo, kuris turi galioti ne trumpiau kaip iki 2026-05-31. |
| 2.4. | Garantija ir licencijos | Turi būti užtikrintas SIEM sistemos gamintojo garantuojamas garantinis aptarnavimas.  Garantiniu laikotarpiu turi būti užtikrinta:  - programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas);  - teisė gauti analitikos taisykles, skirtas naujoms grėsmėms aptikti;  - teisė gauti koreliavimo taisyklių, normalizavimo taisyklių ir šaltinių reputacijos sąrašų / informacijos atnaujinimus;  - teisė kreiptis į gamintoją, iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, nuo pirmadienio iki penktadienio, nuo 7 iki 18 val. vietos laiku, internetu, elektroniniu paštu arba telefonu;  - prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos;  - 4 darbo valandų trukmės atsakas į techninio aptarnavimo užklausas kritinio gedimo atveju;  - gedimo atveju, įranga turi būti suremontuota arba pateikta pakaitinė įranga ne vėliau, kaip per sekančią darbo dieną nuo pranešimo apie gedimą pateikimo tiekėjui ar gamintojui. |
| 2.5. | Paslaugų teikėjas turi būti įgaliotas gamintojo atstovas, arba turi būti sudaręs atitinkamą sutartį su kitu ūkio subjektu, turinčiu teisę parduoti, prižiūrėti siūlomą įrangą. | Paslaugų teikėjas teikdamas pasiūlymą turi pateikti dokumentą, patvirtinantį, kad jis yra įgaliotas Paslaugų gavėjo turimos SIEM sistemos gamintojo atstovas (pateikiami oficialų atstovavimą patvirtinantys dokumentai) arba yra sudaręs atitinkamą bendradarbiavimo sutartį su kitu ūkio subjektu, turinčiu atitinkamas gamintojo suteiktas teises (pateikiama patvirtinančios sutarties su kita įmone, turinčia teisę atstovauti Paslaugų gavėjo turimos SIEM sistemos gamintoją, skaitmeninė kopija bei ūkio subjektui, su kuriuo sudaryta bendradarbiavimo sutartis, gamintojo išduotas įgaliojimas). |
| 1. **Eksploatuojamos saugumo informacijos ir įvykių valdymo sistemos** **LogRhythm SIEM analitikos ir reagavimo paslaugos (36 mėn.) pagal žemiau išvardintus reikalavimus** | | |
| 3.1. | Paslaugų teikimo laikotarpis | Paslaugos turi būti teikiamos 36 mėn. nuo sutarties įsigaliojimo. |
| 3.2. | Paslaugų tiekimo režimas | Darbo dienomis, darbo valandomis (9x5). |
| 3.3. | Atsiskaitymas | Atsiskaitoma pagal per kalendorinius metus faktiškai suteiktas paslaugas. |
| 3.4. | Eksploatuojamos saugumo informacijos ir įvykių valdymo sistemos LogRhythm SIEM analitikos ir reagavimo paslaugos apimtis | Paslaugos apimtis:   * + Paslaugų teikėjas turi teikti saugumo analitikos ir reagavimo paslaugą, apimančią technologinio tinklo infrastruktūrą. Technologinio tinklo infrastruktūra generuoja apie 1000 MPS;   + Paslaugos teikėjas privalo atlikti informavimą apie incidentus (incidentas apibūdinamas, kaip iš anksto nustatytos saugumo politikos pažeidimas arba saugumo įvykis, saugumo analitiko kvalifikuotą kaip teisingai-teigiamą (angl. true-positive)) pagal su paslaugos gavėju suderintą komunikacijos planą;   + Paslaugos teikimo pradžioje, su Paslaugos gavėju turi būti suderintas komunikacijos planas, apimantis: paslaugos Paslaugų teikėjo ir Paslaugų gavėjo suinteresuotų šalių kontaktus; procesą, aprašantį komunikacijos veiksmus incidento atveju; kanalus, kuriais vyks informavimas apie incidentus.   + Paslaugos Teikėjas turi atlikti incidentų stebėjimą, informavimą ir pagalbą užkardant incidentą, užklausų vykdymą pagal šiuos paslaugos teikimo parametrus:   + ataskaitinis periodas: 1 (vienas) kalendorinis mėnuo;   + paslaugų teikimo valandos: darbo dienomis nuo 8:00 iki 17:00 val.;   + incidento reakcijos laikas: 2 val.;   + užklausos reakcijos laikas: 8 val.;   + užklausos sprendimo laikas: 72 val.   + Situacijos analizė (SIEM naudojami įrašų šaltiniai, Paslaugos gavėjo infrastruktūroje esantys SIEM nenaudojami įrašų šaltiniai, esamos koreliacijos taisyklės, stebėsenos praktika, reagavimo į pastebėtus incidentus procesai, pasiūlymų ir rekomendacijų pateikimas, jei būtina – neatidėliotinų veiksmų plano projekto parengimas) – atliekama vieną kartą paslaugų teikimo pradžioje;   + SIEM generuojamų aliarmų analizė (patvirtinimas, klasifikavimas, grupavimas, išsprendimo inicijavimas, konsultavimas sprendžiant);   + Siūlymai esamų koreliacijos taisyklių tobulinimui ir naujų įvedimui;   + Siūlymai dėl kibernetinių grėsmių indikatorių šaltinių panaudojimo;   + Incidento pirminių priežasčių (angl. root cause) nustatymas;   + Incidento atakos grandinėlės nustatymas;   + Incidento tyrimas, jo eigos atkūrimas;   + SIEM esančių incidento įrodymų surinkimas ir išsaugojimas;   + Saugos ir saugos valdymo procesų gerinimo rekomendacijų pateikimas, suvaldžius incidentą;   + Paslaugos teikėjas turi atlikti Paslaugos gavėjo pateiktas užklausas dėl: * naujų koreliacijos taisyklių pridėjimo; * koreliacijos taisyklių konfigūravimo; * ataskaitų sukūrimo; * specifinių sisteminių įrašų nufiltravimo iš žurnalinių įvykių ir saugumo incidentų aptikimo SIEM sistemos.   + Paslaugos teikėjas turi teikti iš anksto sutartas su Paslaugos gavėju ataskaitas ne rečiau nei 1 kartą per ataskaitinį periodą;   + Paslaugos teikėjas turi teikti periodinius (ne rečiau kaip kas 3 mėnesius) pasiūlymus ir konsultacijas dėl paslaugos gerinimo;   + Paslaugos teikėjas turi vykdyti šiuos analitikos darbus: * naujų koreliacijos taisyklių kūrimas; * koreliacijos taisyklių tobulinimas pašalinant neteisingai-teigiamus (angl. false-positive) suveikimus SIEM sistemoje; * saugumo įvykių / aliarmų kvalifikavimas į incidentus; * automatinių pranešimų, iš anksto suderintų su Paslaugos gavėju, konfigūravimas.   + Paslaugos teikėjas turi valdyti pastebėta ir kvalifikuotą saugumo incidentą nuo jo užfiksavimo iki Paslaugos gavėjui informavus apie incidento išsprendimą, pagal iš anksto suderintą su Paslaugos gavėju komunikacijos bei incidentų valdymo procesą;   + Paslaugos teikėjas incidento metu turi siūlyti rekomendacijas bei teikti konsultacijas Paslaugos gavėjui dėl saugumo incidento užkardymo: * greitojo atsako (užkardymo, žalos mažinimo ir pan.) veiksmų nustatymas ir pateikimas Paslaugos gavėjui; * po incidento užkardymo pateikti ilgalaikio poveikio veiksmus – rekomendacijas IT infrastruktūros saugumo spragų, kuriomis buvo pasinaudota saugumo incidento metu, šalinimui.   + Paslaugos teikėjas turi informuoti apie galimus įsilaužimo indikatorius ir saugumo rizikas tokias kaip: * žinomos, aptiktos grėsmių Hash reikšmės;   + komunikacija su žinomomis grėsmių nuorodomis (URL);   + komunikacija su žinomais blogos reputacijos IP adresais;   + komunikacijos su apkrėstais IP adresais identifikavimas;   + bandymų įsilaužti („brute force“, scan) identifikavimas;   + Slaptažodžių atakų indentifikavimas;   + vartotojų elgesio nuokrypių indentifikavimas;   + autentikavimo rizikas;   + auditavimo panaikinimo rizikas;   + teisių/privilegijų pakėlimo rizikas;   + tinklo prieigos rizikas;   + įsilaužėlio horizontalaus judėjimo infrastruktūroje rizikas;   + kredencialų vagysčių rizikas;   + kenksmingo programinio kodo rizikas;   + ilgalaikio įsitvirtinimo infrastruktūroje rizikos. |
| 3.5. | Eksploatuojamos saugumo informacijos ir įvykių valdymo sistemos LogRhythm SIEM priežiūros paslaugos | Priežiūros paslaugos turi apimti:   * + nuolatinį SIEM būklės stebėjimą, proaktyvią problemų prevenciją, reagavimą į pastebėtus sutrikimus ir problemas, SIEM veikimo atkūrimą;   + SIEM programinių atnaujinimų įdiegimą ne vėliau nei per 22 darbo dienas po gamintojo atnaujinimo išleidimo;   + standartinių ir specifinių įrašų šaltinių tvarkymą: pridėjimą į SIEM, modifikavimą, pašalinimą;   + išorinių kibernetinių grėsmių indikatorių (angl. cyber threat intelligence) duomenų šaltinių (kenksmingų IP adresų, domenų ir pan.) tvarkymą: pridėjimą, modifikavimą, pašalinimą;   + SIEM koreliacijos taisyklių konfigūravimą pagal saugumo analitikų pateiktas rekomendacijas ir pastabas (modifikavimą, pašalinimą);   + siūlymų dėl SIEM veikimo optimizavimo pateikimą ir įgyvendinimą;   + perteklinių sisteminių įrašų nufiltravimą ir rekomendacijų, ką nufiltruoti siūlymus;   + rekomendacijų teikimą dėl reikalingų sisteminių įrašų rinkimo;   + naujų sistemos naudotojų pridėjimą, senų sistemos naudotojų pašalinimą;   + darbalaukių kūrimą pagal saugumo analitikų siūlymus ir Paslaugos gavėjo poreikį;   + ataskaitų kūrimą pagal saugumo analitikų siūlymus ir Paslaugos gavėjo poreikį;   + greitųjų paieškos šablonų kūrimą;   + rekomendacijų teikimą sistemos veiklai gerinti ir jų įgyvendinimą. |
| 1. **Diegimo paslaugos - 1 komplektas pagal žemiau išvardintus reikalavimus** | | |
| 4.1. | Paslaugų teikimo | Paslaugų teikėjas turi būti atsakingas už projekto valdymą.  Paslaugų gavėjas pateiks turimą dokumentaciją ir prisijungimus prie įrangos.  Paslaugų teikėjas įsipareigoja pateikti projekto eigos savaitines ataskaitas. |
| 4.2. | Projektavimas | Turi būti atlikta:   * + Esamos situacijos analizė;   + Paslaugų gavėjui patvirtinus diegimo planą, Paslaugų teikėjas atlieka diegimą pagal suderintą diegimo grafiką. |
| 4.3. | Konfigūravimas | Turi būti atlikta:   * + Paslaugų gavėjo turimos SIEM sistemos konfigūravimas pagal parengtą detalų projekto planą;   + Paslaugų gavėjo turimos SIEM sistemos programinė įranga turi būti atnaujinta iki naujausios programinės įrangos versijos arba į gamintojo rekomenduojamą programinės įrangos versiją.   Technologinio tinklo duomenų šaltinių prijungimas prie Paslaugų gavėjo turimos SIEM sistemos:   * + diegimo paslaugos turi būti atliktos per 6 mėnesius nuo sutarties pasirašymo;   + diegimo plano dokumento parengimas turi būti atliktas per 1 mėnesį nuo sutarties pasirašymo. Paslaugų teikėjo pateiktame diegimo plane turi būti:   + pateiktas technologinio tinklo duomenų šaltinių prijungimo prie SIEM sistemos kalendorinis grafikas;   + pateikta esama LogRhtyhm SIEM sprendimo architektūra ir duomenų šaltiniai;   + pateikta technologinio tinklo duomenų šaltinių surinkimo architektūra;   + pateiktas technologinio tinklo duomenų šaltinių sisteminių įrašų surinkimo aprašymas iš sekančių sistemų: * ugniasienių; * tinklo įrenginių, maršrutizatorių; * tinklo valdymo sistemos; * visų Windows serverių; * visų Linux serverių; * visų kompiuterinių darbo vietų; * IOT serverių, * Siemens PLC ir t.t.   + SIEM sistemos programinės įrangos versijos atnaujinimą į naujausią versiją;   + SIEM sistemoje Technologinio tinklo „Entity“ sukūrimas;   + kolektoriaus programinės įrangos sudiegimas technologiniame kompiuteriniame tinkle;   + sukurti iki 20 vnt. specializuotų koreliacijos taisyklių technologinio tinklo duomenų šaltiniams;   + sukurti iki 5 vnt. sutartų ataskaitų technologinio tinklo duomenų šaltiniams;   + pridėti prie SIEM sistemos ne prasčiau, kaip šiuos žemiau išvardintus technologinio tinklo duomenų šaltinius, bet ne mažiau kaip 300 vnt. duomenų šaltinių (jeigu sisteminių įrašų surinkimo neriboja esami sisteminiai ar procesiniai ribojimai): * ugniasienes; * tinklo komutatorius, maršrutizatorius; * tinklo komutatorių valdymo sistemą; * visus Windows serverius; * visus Linux serverius; * visas kompiuterines darbo vietas; * IOT serverius; * Siemens PLC įrenginius; * antivirusinę sistemą; * ir kt. |
| 4.4. | Dokumentacija | Technologinio tinklo duomenų šaltinių prijungimo prie turimos LogRhythm SIEM sistemos diegimo dokumentacija:   * + esama SIEM duomenų šaltinių surinkimo architektūra;   + nauja SIEM duomenų šaltinių surinkimo architektūra pridėjus technologinio tinklo duomenų šaltinius;   + įvardinti visi pridėti technologinio tinklo duomenų šaltiniai;   + įvardintos naujai sukurtos koreliacijos taisyklės su taisyklių aprašymais;   + įvardintos naujai sukurtos ataskaitos. |

1. **PASLAUGŲ TEIKIMO VIETA, TERMINAI IR TVARKA**
   1. **Paslaugų teikimo vieta –** Paslaugų gavėjo buveinės adresas (Spaudos gatvė 8-1, Vilnius 05131). Licencijos turi būti siunčiamos elektroniniu paštu kestutis@vv.lt arba pateiktos prisijungimo nuorodos ir kodai Licencijoms parsisiųsti iš gamintojo puslapio.
   2. **Paslaugų teikimo terminas (-ai)**- Paslaugų teikėjas Paslaugas pradeda teikti ne vėliau kaip per 5 (penkias) darbo dienas nuo sutarties pasirašymo datos.
   3. Sutarties terminas – 37 (trisdešimt septyni) mėnesiai. Paslaugų teikimo trukmė – 36 (trisdešimt šeši) mėnesiai. Paskutinis mėnuo skirtas Sąskaitos apmokėjimui.
   4. Teikdamas pasiūlymą Paslaugų teikėjas visas galimas išlaidas įskaičiuoja į paslaugų įkainį. Siūlomame įkainyje turi būti įskaičiuotos visos Paslaugų teikėjo išlaidos ir mokėtini mokesčiai, būtini tinkamam Sutarties įvykdymui.

**5. PASLAUGŲ KOKYBĖ IR TRŪKUMŲ ŠALINIMAS**

* 1. LogRhythm SIEM programinės įrangos klaidų, kurios nustatomos Paslaugų gavėjo eksploatacijos metu, sprendimui Paslaugų teikėjas turi dėti visas pastangas, kad rastos klaidos būtų ištaisytos ir įtrauktos į naujausius klaidų ištaisymo paketus. Nesant galimybei ištaisyti LogRhythm SIEM programinės įrangos klaidų Paslaugų teikėjas ieško kitų būdų, pagal LogRhythm SIEM programinės įrangos gamintojo rekomendacijas bei siūlomus aplinkinius „workaround“ sprendimus (įskaitant bet neapsiribojant grįžimą į ankstesnes LogRhythm SIEM programinės įrangos versijas, kuriose tas funkcionalumas veikė korektiškai) klaidos sprendimui;

5.2. Nekokybiškos ar Užsakymo ir (ar) Techninėje specifikacijoje nurodytų reikalavimų neatitinkančios Paslaugos turi būti ištaisytos nuo Paslaugų gavėjo rašytinio reikalavimo dėl trūkumų šalinimo pateikimo dienos ne vėliau kaip per **5 darbo dienų.**

**6. SUTARTIES VYKDYMO METU PATEIKIAMA DOKUMENTACIJA**

6.1. Programinės įrangos dokumentai turi būti lietuvių arba anglų kalba. Programinė įranga ir kompiuterių technikos sisteminiai pranešimai turi būti anglų arba lietuvių kalba. Gamintojo interneto svetainėje tvarkyklių ir dokumentų paieška turi būti pateikiama anglų arba lietuvių kalba.

6.2. Paslaugų teikėjas turi pateikti nuorodą ar nuorodas į gamintojo interneto puslapį, kuriame yra tiksli pasiūlymą atitinkančios programinės įrangos techninė specifikacija.

1. **PASLAUGŲ GAVĖJO IR PASLAUGŲ TEIKĖJO ĮSIPAREIGOJIMAI**

7.1. **Paslaugų gavėjo įsipareigojimai:**

7.1.1.Bendradarbiauti su Paslaugų teikėju, teikiant reikalingą informaciją Užsakymų ir (ar) Sutarties vykdymo metu.

7.1.2. Priimti iš Paslaugų teikėjo jo kokybiškai suteiktas Paslaugas, atitinkančių teisės aktų ir Užsakyme ir (ar) Sutartyje numatytų Paslaugų reikalavimus, ir tinkamai bei laiku atsiskaityti su Paslaugų teikėju Sutartyje numatytomis sąlygomis.

7.2. **Paslaugų teikėjo įsipareigojimai:**

7.2.1. Teikti Paslaugas profesionaliai, kokybiškai ir laiku, vadovaujantis Užsakyme (-uose), Sutartyje nustatyta tvarka, Lietuvos Respublikoje galiojančiais įstatymais ir kitais teisės aktais reglamentuojančiais Paslaugų teikimą.

7.2.2. Prekės ir (ar) įsigyjamos Paslaugos Paslaugų teikėjas (Paslaugų teikėjas) teikdamas Paslaugas ir (ar) Prekes privalo vadovautis Lietuvos Respublikos kibernetinio saugumo įstatymu ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams valdantiems ypatingos svarbos informacinę infrastruktūrą, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo" (galiojančiomis aktualiomis redakcijomis).

7.2.3. Prisiima visą riziką dėl ne nuo Paslaugų gavėjo priklausančių aplinkybių, dėl kurių padidės su Sutarties vykdymu susijusios Paslaugų teikėjo išlaidos ir Paslaugų teikėjui Sutarties vykdymas taps sudėtingesnis (Paslaugų teikėjas padidės įsipareigojimų vykdymo kaina). Sutarties kaina jokiais atvejais nebus didinama.