PIRKIMO – PARDAVIMO SUTARTIS Nr. 

20-C-610 2020-03-03

Vilnius 2020 m. ___

Viešoji įstaiga Vilniaus universiteto ligoninė Santaros klinikos (toliau – **Pirkėjas**), atstovaujamos generalinio direktoriaus Felikso Jankevičiaus, veikiančio pagal įstaigos įstatus, ir UAB „NBCS“ (toliau – **Paslaugų teikėjas**), atstovaujama generalinio direktoriaus Artiom Maslov, veikiančio pagal įmonės įstatus, laimėjusi 2019 m. gruodžio mėn. 18 d. skelbtą mažos vertės apklausos būdu vykusį „Informacinių sistemų žurnalinių įrašų saugojimo ir koreliacijos sistema (SIEM) ir jos įdiegimas Nr. 20363“ viešąjį pirkimą (pirkimo skelbimo Nr. 466830) (toliau - Pirkimas), sudarė šią sutartį:

1. SUTARTIES OBJEKTAS

1.1. Pardavėjas įsipareigoja parduoti Pirkėjui Informacinių sistemų žurnalinių įrašų saugojimo ir koreliacijos sistemą (SIEM) ir atlikti jos įdiegimą (toliau – Prekės), o Pirkėjas įsipareigoja priimti jas ir sumokėti už jas šioje sutartyje nurodytą kainą sutarties 6.1 p. numatyta tvarka.
1.2. Sutarties dalykas Informacinių sistemų žurnalinių įrašų saugojimo ir koreliacijos sistemą (SIEM) ir jos įdiegimas prekės, kurių techninė specifikacija, fiksuoti įkainiai, kiekiai ir kaina nurodyti sutarties priede Nr.1.

2. SUTARTIES KAINA

2.1. Sutarčiai taikomas fiksuotos kainos kainodaros metodas.
2.2. Pradinė (maksimali) sutarties vertė be PVM 7650,00Eur (septyni tūkstančiai šeši šimtai penkiasdešimt Eur ir 00 ct).
PVM suma 1606,50 Eur (tūkstantis šeši šimtai šeši Eur ir 50 ct).
Pradinė (maksimali) sutarties vertė su PVM 9256,50 Eur (devyni tūkstančiai du šimtai penkiasdešimt šeši Eur ir 50 ct).
2.3. Sutartyje nustatyta fiksuota prekių kaina, kuri sutarties vykdymo laikotarpiu negalės būti keičiama per visą sutarties vykdymo laikotarpį, išskyrus kai pasikeičia pridėtinės vertės mokestis (PVM). Perskaičiavimas vykdomas po Lietuvos Respublikos pridėtinės vertės mokesčio įstatymo, kuriuo keičiasi mokesčio tarifas, įsigaliojimo dienos. Pasikeitus PVM tarifo dydžiui, nepateiktų prekių kaina keičiama (mažinama ar didinama) proporcingai PVM pasikeitusio tarifo dydžiu. Kainos pakeitimas įforminamas papildomu rašytiniu šalių susitarimu.
2.4.Į pradinę sutarties vertę įskaityti visi Pardavėjo mokami mokesčiai, prekės pristatymo ir kitos išlaidos.
2.5. **Sutarties kaina** – už prekes pagal sutartį tiekėjo gaunama ekonominė nauda.
2.6. Pirkimo sutarties sąlygos sutarties galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias pirkimo sutarties sąlygas, kurias pakeitus nebūtų pažeisti Viešųjų pirkimų įstatymo 17 straipsnyje nustatyti principai ir tikslai bei esant Viešųjų pirkimų įstatymo 89 straipsnyje nustatytoms sąlygoms.

3. PERKAMOS PREKĖS

3.1. Šia sutartimi Pardavėjas įsipareigoja perleisti Prekes, kurių detalios specifikacijos, kainos, įkainiai ir kiekiai nustatyti šios sutarties priede Nr. 1.

4. PREKIŲ PRISTATYMO TVARKA

4.1. Pardavėjas įsipareigoja įdiegti sprendimą ne vėliau kaip per 90 (devyniasdešimt) dienų nuo Pirkėjo užsakyme nurodytos datos.
4.2. Prekių pristatymo vieta: - VšĮ Vilniaus universiteto ligoninė Santaros klinikos, Informatikos ir plėtros centras (Santariškių g. 5, LT-08406 Vilnius).
4.3. Paskirtas atsakingas asmuo: Vidas Kapušinskas, tel. (8 5) 2501886, el.p. vidas.kapusinskas@santa.lt.
4.4. Asmuo, atsakingas už sutarties ir pakeitimų paskelbimą: Viešųjų pirkimų skyriaus specialistė Dainora Mažeikienė tel. +370 5 2501819, el. pašto adresas dainora.mažeikiene@santa.lt.
4.5. Pardavėjo paskirtas atsakingas asmuo – Vilma Bagdonaitė, tel. +370 645 36023, el. paštas vb@nbcs.lt

5. PREKIŲ KOKYBĖ IR GARANTIJA

5.1. Pardavėjas garantuoja, kad parduodamos Prekės yra be defektų ir jų kokybė, žymėjimas, informacija vartotojui atitinka Pirkimo dokumentų nuostatas, galiojančius standartus, technines sąlygas ar kitus norminius aktus.
5.2. Prekių garantinio termino metu užtikrinama gamintojo teikiama nuolatinė pagalba sprendimo sutrikimų atveju, leidžiama nemokamai atsisiųsti bei įdiegti sprendimo ar jo komponentų atnaujinimus (jei gamintojas tokius išleidžia). Prekių garantinis terminas nurodytas sutarties priede Nr. 1 "Techninė specifikacija".

6. ATSISKAITYMAS TARP ŠALIŲ

6.1. Pirkėjas apmoka Pardavėjui už prekes pagal gautas PVM sąskaitas faktūras per 30 dienų nuo prekių gavimo ir sąskaitos faktūros pateikimo dienos. Jei mokėjimai pagal sutartis visiškai arba iš dalies atliekami iš tarpinių finansuojančių organizacijų gautomis lėšomis, taip pat kitomis objektyviai pagrįstomis aplinkybėmis atsiskaitymo terminas Pirkėjo gali būti pratęstas iki 60 dienų nuo prekių gavimo ir sąskaitos faktūros pateikimo dienos.
6.2. PVM sąskaitos faktūros, sąskaitos faktūros, kreditiniai ir debetiniai dokumentai bei avansinės sąskaitos turi būti teikiami naudojantis informacinės sistemos „E. sąskaita" priemonėmis. Mokėjimo dokumentų nepateikus „E. sąskaita" priemonėmis, Pirkėjas turi teisę neatlikti mokėjimo.

7. SUTARTIES ĮVYKDYMO UŽTIKRINIMAS, ATSAKOMYBĖ

7.1. Sutarties įvykdymo užtikrinimo priemonė yra netesybos. Jei tiekėjas dėl savo kaltės vėluoja pristatyti Prekes, Pirkėjas turi teisę be rašytinio įspėjimo ir nesumažindamas kitų savo teisių gynimo priemonių, numatytų sutartyje, pradėti skaičiuoti delspinigius už kiekvieną vėluojamą prekių pristatymo dieną. Pardavėjo vėluojamų pristatyti prekių kaina mažinama 0,02 % nuo vėluojamų pristatyti prekių vertės už kiekvieną termino praleidimo dieną. Delspinigių suma gali būti išskaičiuojama iš Pardavėjui mokėtinų sumų.
7.2. Jei Pardavėjas iš esmės pažeidžia Sutartį 9.2.p. nurodytais atvejais, Pirkėjas turi teisę taikyti 10 % sutarties pradinės vertės baudą, įskaitant delspinigius.
7.3. Jei Pirkėjas dėl savo kaltės vėluoja atsiskaityti su Pardavėju per sutarties 6.1.p. numatytą terminą, jis įsipareigoja sumokėti 0,02 % dydžio delspinigius nuo nesumokėtos sumos.

8. *FORCE MAJEURE*

8.1. *Force Majeure* sąlygos taikomos vadovaujantis LR Vyriausybės 1996 m. liepos 15d. nutarimu Nr. 840 patvirtintomis „Atleidimo nuo atsakomybės dėl nenugalimos jėgos (*Force majeure*) aplinkybėmis", taisyklėmis.

9. SUTARTIES GALIOJIMAS IR NUTRAUKIMAS

9.1. Sutartis įsigalioja šalims ją pasirašius ir galioja iki visiško šalių įsipareigojimų pagal šią sutartį įvykdymo, bet ne ilgiau kaip 12 (dvylika) mėnesių.
9.2. Pirkėjas turi teisę vienašališkai nutraukti Sutartį įspėjęs Pirkėją prieš 15 darbo dienų, jeigu Pardavėjas ją iš esmės pažeidė:
9.2.1. parduota prekė yra netinkamos kokybės ir jos trūkumų neįmanoma pašalinti per protingą ir Pirkėjui priimtiną terminą;
9.2.2. Pardavėjas prekių nepristatė per Sutartyje nustatytą bei Pirkėjo nurodytą papildomą protingą terminą.
9.3. Pardavėjas turi teisę vienašališkai nutraukti Sutartį įspėjęs Pirkėją prieš 15 darbo dienų, jeigu Pirkėjas ją iš esmės pažeidė:
9.3.1. Pirkėjas daugiau kaip du kartus laiku nesumokėjo už Prekes, kai jos buvo perduotos nustatytais terminais;
9.3.2. Pirkėjas daugiau kaip du kartus nepriėmė tinkamoms kokybės Prekių, kai jos buvo perduotos nustatytais terminais.
9.4. Sutartis taip pat gali būti nutraukta Šalių raštišku susitarimu.

10. KITOS SĄLYGOS

10.1. Sutarties vykdymo metu, Pirkėjui raštu išreiškus sutikimą, Pardavėjas turi teisę taikyti nuolaidas (laikinas ar pastovias) ir perkamas prekes parduoti mažesnėmis, nei nurodyta sutarties priede, kainomis.

10.2. Pardavėjas įsipareigoja išrašomoje sąskaitoje-faktūroje vartoti tuos pačius prekių pavadinimus ir mato vnt., kokie yra pridedamoje specifikacijoje. Taip pat ant sąskaitos faktūros privalo užrašyti sutarties numerį ir datą, pagal kurią parduodamos prekės.
10.3. Sutarties vykdymo metu Pardavėjo gauta informacija ir dokumentai yra konfidencialūs. Be išankstinio raštiško Pirkėjo leidimo Pardavėjas neskelbia ir neatskleidžia jokių sutarties nuostatų, išskyrus atvejus, kai tai būtina vykdant sutartį.
10.4. Ginčai, kylantys tarp Šalių, sprendžiami šalių derybomis, o nepavykus jų išspręsti – teismine tvarka Lietuvos Respublikos teismuose.
10.5. Sutartis sudaryta 2 (dviem) vienodą juridinę galią turinčiais egzemplioriais, po vieną kiekvienai sutarties šaliai, lietuvių kalba.
10.6. Pardavėjas patvirtina, kad į parduodamas prekes tretieji asmenys neturi jokių teisių.
10.7. Sudarius Sutartį, tačiau ne vėliau negu Sutartis pradedama vykdyti, tiekėjas įsipareigoja pranešti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Pirkėjas taip pat reikalauja, kad tiekėjas informuotų apie minėtos informacijos pasikeitimus visu Sutarties vykdymo metu, taip pat apie naujus subtiekėjus, kuriuos jis ketina pasitelkti vėliau. Pasiūlyme tiekėjas nenurodė, kad pasitelks subtiekėjus
10.7.1.Tiekėjas gali keisti Sutartyje nurodytus subtiekėjus tik prieš tai raštu pranešęs Užsakovą apie tokio keitimo būtinybę ir gavęs jo raštišką sutikimą.
10.7.2. Tiekėjas Sutarties vykdymo metu gali inicijuoti subtiekėjo, numatyto Sutartyje, pakeitimą, nurodydamas tokio keitimo motyvus.
10.7.3. Pirkėjui sutikus su subtiekėjo pakeitimu, Pirkėjas kartu su tiekėju raštu sudaro susitarimą dėl subtiekėjo pakeitimo, kurį pasirašo Šalys. Šis susitarimas yra neatskiriama Sutarties dalis
PRIDEDAMA. Prekių sąrašas, kiekis, įkainiai, kaina, techninė specifikacija, 13 lapų.

ŠALIŲ ADRESAI IR REKVIZITAI

Pardavėjas
UAB „NBCS“
J. Kazlausko g. 21, LT-08314 Vilnius
Įmonės kodas 301817848
PVM mok. kodas LT100006470618
a. s. LT41 7044 0600 0831 9438
AB „SEB bankas“, b. k. 70440

Generalinis direktorius
Artiom Maslov

Pirkėjas
VšĮ Vilniaus universiteto ligoninė Santaros klinikos
Santariškių g. 2, LT-08661 Vilnius
Įmonės kodas 124364561
PVM mok. kodas LT243645610
a. s. LT71 7300 0100 0249 2260
AB „Swedbank“, b. k. 73000

Generalinis direktorius
Feliksas Jankevičius

Direktorės vykdytoja
Aušra Bilotienė Mažeikienė

Vyriausioji buhalterė
Irena Tunkienė

Vyriausioji viešųjų pirkimų specialistė
Dainora Mažeikienė
2020-02-27

20-C-610 2020-03-03

1-as priedas prie sutarties Nr.

PREKIŲ SĄRAŠAS

Eil. Nr.	Prekės pavadinimas	Kiekis	Mato vnt.	Vnt. Kaina EUR be PVM	Vnt. Kaina EUR su PVM	Suma EUR su PVM
1	2	3	4	5	6	7
1.	Informacinių sistemų žurnalinių įrašų saugojimo ir koreliacijos sistema (SIEM) ir jos įdiegimas.	1	vnt.	7 650,00	9 256,50	9 256,50
					Pradinė (maksimali) sutarties vertė Eur be PVM	7 650,00
					PVM (21%) suma	1 606,50
					Pradinė (maksimali) sutarties vertė Eur su PVM	9 256,50

Pardavėjas
UAB „NBCS“
J. Kazlausko g. 21, LT-08314 Vilnius
Įmonės kodas 301817848
PVM mok. kodas LT100006470618
a. s. LT41 7044 0600 0831 9438
AB „SEB bankas“, b. k. 70440

Generalinis direktorius
Artiom Maslov

Pirkėjas
VšĮ Vilniaus universiteto ligoninė Santaros klinikos
Santariškių g. 2, LT-08661 Vilnius
Įmonės kodas 124364561
PVM mok. kodas LT243645610
a. s. LT71 7300 0100 0249 2260
AB „Swedbank“, b. k. 73000

Generalinis direktorius
Feliksas Jankevičius

Vyriausioji viešųjų pirkimų specialistė
Dainora Mažeikienė
2020-03-03

TECHNINĖ SPECIFIKACIJA

Eil. Nr.	Parametras	Parametro reikalavimai	Tiekėjo pasiūlymas
1.	Modelis ir gamintojas	Nurodyti	**QRadar SIEM, IBM**
2.	Paskirtis	• Turi būti siūlomas specializuotas vieno gamintojo programinis sprendimas. Visa programinė įranga privalo būti specializuota šioje specifikacijoje numatytoms Informacinių sistemų žurnalinių įrašų saugojimo ir koreliacijos (*angl. SIEM - Security Information and Event Management*) funkcijoms atlikti. • Pateikti nuorodą į gamintojo interneto svetainę (jei gamintojas suteikia tokią informaciją), techninę dokumentaciją, kurioje pateikiama informacija apie siūlomos prekės charakteristikas ir atitikimą techninės specifikacijos reikalavimams.	Siūlomas specializuotas vieno gamintojo programinis sprendimas. Visa programinė įranga yra specializuota šioje specifikacijoje numatytoms Informacinių sistemų žurnalinių įrašų saugojimo ir koreliacijos (*angl. SIEM - Security Information and Event Management*) funkcijoms atlikti. Pateikiamos nuorodos į gamintojo interneto svetainę, techninę dokumentaciją, kurioje pateikiama informacija apie siūlomos prekės charakteristikas ir atitikimą techninės specifikacijos reikalavimams: IBM QRadar SIEM data sheet https://www.ibm.com/downloads/cas/RLXJNX2G IBM QRadar produkto puslapis https://www.ibm.com/security/security-intelligence/qradar IBM QRadar SIEM V7.3.3 documentation (PDF dokumentai parsisiuntimui) https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/c_qradar_pdfs.html
3.	Bendri reikalavimai	• Sistema turi užtikrinti, kad sistemoje esantys įvykiai būtų apsaugoti nuo neteisėto sunaikinimo ar pakeitimo. • Sistema turi gebėti rinkti įvykius (*angl. Events / Logs*) ir tinklo srauto statistikos įrašus (*angl. flows*). • Sistema negali būti teikiama kaip debesijos paslauga. • Siūloma Sistema papildomai neturi reikalauti nei operacinės sistemos, nei duomenų bazės licencijų. • Pateikta programinė įranga turi būti vienodai tinkama diegti tiek į virtualizavimo platformą, tiek ir į perkančiosios organizacijos pasirinktą techninę - aparatinę įrangą. • Siūlomas sprendimas turi veikti kaip vienas loginis vienetas, t.y. viena virtuali mašina virtualizavimo platformoje arba vienas fizinis serveris, kuriame integruoti visi sistemos veikimui (saugos informacijos surinkimui, apdorojimui, saugojimui bei atvaizdavimui) būtini komponentai. • Turi būti galimybė plėsti Sistemos funkcionalumą tiek papildant esamo sprendimo galimybes, tiek ir pridedant to paties gamintojo papildomus programinius arba techninius - aparatinius komponentus.	Sistema užtikrina, kad sistemoje esantys įvykiai būtų apsaugoti nuo neteisėto sunaikinimo ar pakeitimo. Sistema geba rinkti įvykius (*angl. Events / Logs*) ir tinklo srauto statistikos įrašus (*angl. flows*). Sistema nėra teikiama kaip debesijos paslauga. Siūloma Sistema papildomai nereikalauja nei operacinės sistemos, nei duomenų bazės licencijų. Pateikta programinė įranga yra vienodai tinkama diegti tiek į virtualizavimo platformą, tiek ir į perkančiosios organizacijos pasirinktą techninę - aparatinę įrangą. Siūlomas sprendimas veikia kaip vienas loginis vienetas, t.y. viena virtuali mašina virtualizavimo platformoje arba vienas fizinis serveris, kuriame integruoti visi sistemos veikimui (saugos informacijos surinkimui, apdorojimui, saugojimui bei atvaizdavimui) būtini komponentai. Yra galimybė plėsti Sistemos funkcionalumą tiek papildant esamo sprendimo galimybes, tiek ir pridedant to paties gamintojo papildomus programinius arba techninius - aparatinius komponentus. Sistemai ir jos komponentams yra pateiktos naujausios programinės įrangos versijos. Į perkamų prekių apimtis yra įtrauktos ir tiesiogiai šiuose reikalavimuose neįvardintos Sistemos licencijos, komponentai, moduliai, kurie yra būtini keliamam funkcionalumui realizuoti.

		• Sistemai ir jos komponentams turi būti pateiktos naujausios programinės įrangos versijos. • Į perkamų prekių apimtis turi būti įtrauktos ir tiesiogiai šiuose reikalavimuose neįvardintos Sistemos licencijos, komponentai, moduliai, kurie yra būtini keliamam funkcionalumui realizuoti.	
4.	Įvykiai (*angl. events*)	• Sistema turi būti pritaikyta surikti ir apdoroti ne mažiau kaip 700 įvykių / įrašų per sekundę (angl. *EPS – Events Per Second*). • Turi būti galimybė ateityje, nekeičiant esamos įrangos, plėsti sistemos greitaveiką iki ne mažiau kaip 5000 įvykių / įrašų per sekundę. • Įvykių šaltinių skaičius neturi būti ribojamas. • Sistema turi gebėti surinkti įrašus tiek užklausdama sistemas, tiek iš sistemų, kurios pačios siunčia žurnalinius įrašus. • Sistema turi leisti kurti specializuotus įvykių surinkimo komponentus oficialiai nepalaikomiems įvykių šaltiniams. • Sistema turi gebėti lanksčiai prisitaikyti ir paimti įvykius iš Pirkėjo taikomųjų programų sistemų.	Sistema yra pritaikyta surikti ir apdoroti ne mažiau kaip 700 įvykių / įrašų per sekundę (angl. *EPS – Events Per Second*). Yra galimybė ateityje, nekeičiant esamos įrangos, plėsti sistemos greitaveiką iki ne mažiau kaip 5000 įvykių / įrašų per sekundę. Įvykių šaltinių skaičius neribojamas. Sistema geba surinkti įrašus tiek užklausdama sistemas, tiek iš sistemų, kurios pačios siunčia žurnalinius įrašus. Sistema leidžia kurti specializuotus įvykių surinkimo komponentus oficialiai nepalaikomiems įvykių šaltiniams. Sistema geba lanksčiai prisitaikyti ir paimti įvykius iš Pirkėjo taikomųjų programų sistemų.
5.	Žurnaliniai įrašai (*angl. logs*)	• Sistemoje turi būti realizuota galimybė rinkti žurnalinius įrašus (angl. *Logs*) iš tinklo įrangos (maršrutizatorių, komutatorių, bevielių prieigos taškų), tinklo saugos įrenginių bei sistemų (ugniasienių, web aplikacijų ugniasienių, IPS/IDS, DHCP, DNS, Active Directory ir kt.), operacinių sistemų, duomenų bazių valdymo sistemų bei taikomosios programinės įrangos. • Sistema turi palaikyti šiuos šaltinius nediegiant agentų stebimuose įrenginiuose: Syslog, Syslog NG, SNMP, ODBC, OPSEC. • Turi būti palaikomi CEF, LEEF, CSV, key-value standartizuoti įvykių formatai. • Sistema turi gebėti pasiimti ir apdoroti nestandartinius įvykius saugomus Windows Event Log. • Sistema turi turėti funkcionalumą leidžiantį apdoroti gamintojo nepalaikomus įvykių formatus ir šaltinius. Pvz.: Pirkėjo kurtų vidinių sistemų įvykius.	Sistemoje yra realizuota galimybė rinkti žurnalinius įrašus (angl. *Logs*) iš tinklo įrangos (maršrutizatorių, komutatorių, bevielių prieigos taškų), tinklo saugos įrenginių bei sistemų (ugniasienių, web aplikacijų ugniasienių, IPS/IDS, DHCP, DNS, Active Directory ir kt.), operacinių sistemų, duomenų bazių valdymo sistemų bei taikomosios programinės įrangos. Sistema palaiko šiuos šaltinius nediegiant agentų stebimuose įrenginiuose: Syslog, Syslog NG, SNMP, ODBC, OPSEC. Yra palaikomi CEF, LEEF, CSV, key-value standartizuoti įvykių formatai. Sistema geba pasiimti ir apdoroti nestandartinius įvykius saugomus Windows Event Log. Sistema turi funkcionalumą leidžiantį apdoroti gamintojo nepalaikomus įvykių formatus ir šaltinius. Pvz.: Pirkėjo kurtų vidinių sistemų įvykius.
6.	Tinklo srauto (*angl. flows*) analizė	• Sistema turi būti pritaikyta surinkti ir apdoroti ne mažiau kaip 15000 tinklo srauto statistikos įrašų per minutę (angl. *FPM – Flows Per Minute*). • Turi būti galimybė ateityje, nekeičiant esamos Sistemos, plėsti per minutę apdorojamų įrašų skaičių iki ne mažiau kaip 250000. • Sistema turi palaikyti šiuos tinklo srauto statistikos formatus: NetFlow, sFlow, J-Flow , IPFix.	Sistema yra pritaikyta surinkti ir apdoroti ne mažiau kaip 15000 tinklo srauto statistikos įrašų per minutę (angl. *FPM – Flows Per Minute*). Yra galimybė ateityje, nekeičiant esamos Sistemos, plėsti per minutę apdorojamų įrašų skaičių iki ne mažiau kaip 250000. Sistema palaiko šiuos tinklo srauto statistikos formatus: NetFlow, sFlow, J-Flow , IPFix.

7.	Įvykių koreliavimo galimybės	• Sistema turi turėti galimybę: o Koreliuoti surinktą informaciją ir grupuoti įvykius, surinktus apie tam tikrą incidentą kompiuterių tinkle; o Turėti išankstines gamintojo paruoštas įvykių koreliacijos taisykles; o Leisti kurti papildomas koreliacijos taisykles; o Įvykių koreliacijos taisyklės turi turėti funkcionalumą išsiųsti informaciją į išorinę sistemą, pvz. incidentų valdymo sistemą, stebėsenos sistemą. • Sistema turi gebėti atlikti anomalijų aptikimą - pagal naudotojo sudarytą užklausą nuolatos tikrinti įvykių srautą ir aliarmuoti jei matomas nuokrypis dienos, savaitės ar mėnesio bėgyje. • Sistema turi turėti koreliacijos funkcionalumą leidžiantį sugeneruoti naują įvykį, kuris būtų apdorojamas kaip kiti gaunami įvykiai. • Sistema turi leisti atlikti koreliaciją pagal tinklo segmentų pavadinimus. • Sistemos koreliavimo komponentas turi leisti kurti specializuotus sąrašus, kurių reikšmes galima lyginti su gaunamuose įvykiuose matoma informacija. Pavyzdžiui: whitelist, blacklist, userlist, malicious hash list, malicious url list ir t.t. • Sistemos koreliavimo komponentas turi leisti kurti specializuotus sąrašus, kurie saugo informacijos rinkinius, pvz.: naudotojo ID, naudotojo IP, naudotojo MAC. • Sistema turi leisti specializuotus sąrašus pildyti koreliacijos taisyklių pagalba, TAXII informacija ar HTTP REST API pagalba.	Sistema turi galimybę: Koreliuoti surinktą informaciją ir grupuoti įvykius, surinktus apie tam tikrą incidentą kompiuterių tinkle; Turėti išankstines gamintojo paruoštas įvykių koreliacijos taisykles; Leidžia kurti papildomas koreliacijos taisykles; Įvykių koreliacijos taisyklės turi funkcionalumą išsiųsti informaciją į išorinę sistemą, pvz. incidentų valdymo sistemą, stebėsenos sistemą. Sistema geba atlikti anomalijų aptikimą - pagal naudotojo sudarytą užklausą nuolatos tikrinti įvykių srautą ir aliarmuoti jei matomas nuokrypis dienos, savaitės ar mėnesio bėgyje. Sistema turi koreliacijos funkcionalumą leidžiantį sugeneruoti naują įvykį, kuris būtų apdorojamas kaip kiti gaunami įvykiai. Sistema leidžia atlikti koreliaciją pagal tinklo segmentų pavadinimus. Sistemos koreliavimo komponentas leidžia kurti specializuotus sąrašus, kurių reikšmes galima lyginti su gaunamuose įvykiuose matoma informacija. Pavyzdžiui: whitelist, blacklist, userlist, malicious hash list, malicious url list ir t.t. Sistemos koreliavimo komponentas leidžia kurti specializuotus sąrašus, kurie saugo informacijos rinkinius, pvz.: naudotojo ID, naudotojo IP, naudotojo MAC. Sistema leidžia specializuotus sąrašus pildyti koreliacijos taisyklių pagalba, TAXII informacija ar HTTP REST API pagalba.
8.	Įvykių peržiūra	• Sistema turi leisti peržiūrėti ateinančius įvykius realiu laiku. • Sistema turi leisti atrinkti įvykius peržiūrai pagal nurodytus kriterijus. Atrinkimo kriterijus turi būti galima išsaugoti vėlesnėms paieškoms. • Sistemoje turi būti įtraukti standartiniai gamintojo interaktyvieji valdymo ekranai (angl. *Dashboard*). Ekranuose turi matytis: o informacija apie rizikas tinkle (rizikų vertinimas, didžiausią riziką turintys objektai); o informacija apie grėsmes tinkle (grėsmių istorija, didžiausios grėsmės); o informacija apie DNS užklausas tinkle (populiariausios užklausos, naujausios užklausos); o informacija apie naudojamus protokolus tinkle; o informacija apie pašto statistiką tinkle (šaltiniai, siunčiantys daugiausiai laiškų, šaltiniai, siunčiantys didelės apimties laiškus); o informacija apie tinklo srauto statistiką;	Sistema leidžia peržiūrėti ateinančius įvykius realiu laiku. Sistema leidžia atrinkti įvykius peržiūrai pagal nurodytus kriterijus. Atrinkimo kriterijus galima išsaugoti vėlesnėms paieškoms. Sistemoje yra įtraukti standartiniai gamintojo interaktyvieji valdymo ekranai (angl. *Dashboard*). Ekranuose matosi: informacija apie rizikas tinkle (rizikų vertinimas, didžiausią riziką turintys objektai); informacija apie grėsmes tinkle (grėsmių istorija, didžiausios grėsmės); informacija apie DNS užklausas tinkle (populiariausios užklausos, naujausios užklausos); informacija apie naudojamus protokolus tinkle; informacija apie pašto statistiką tinkle (šaltiniai, siunčiantys daugiausiai laiškų, šaltiniai, siunčiantys didelės apimties laiškus); informacija apie tinklo srauto statistiką; Sistema leidžia kurti interaktyviuosius valdymo ekranus, pateikiančius informaciją realiu laiku.

		• Sistema turi leisti kurti interaktyviuosius valdymo ekranus, pateikiančius informaciją realiu laiku. • Sistema turi gebėti automatiškai pridėti prie IP adresų jų geografinę informaciją.	Sistema geba automatiškai pridėti prie IP adresų jų geografinę informaciją.
9.	Grėsmių aptikimas	• Sistema be papildomo mokesčio turi periodiškai atnaujinti ir įdiegti gamintojo pateikiamą saugumo grėsmių informaciją, pažeidžiamumų sąrašus, identifikuojančius komunikaciją su įtartinais ir kenksmingais šaltiniais (IP adresais) internete, kenksmingo kodo maišos sumas, žinomus blogus domenus ir kt. • Sistema turi automatiškai identifikuoti įvykius, sistemas ir naudotojus, kurie dalyvauja komunikacijoje su objektais pateikiamais saugumo grėsmių šaltiniuose. • Sistema turi leisti pridėti trečių šalių pateikiamus saugumo grėsmių (angl. *Threat Feeds*) šaltinius STIX / TAXII formatu.	Sistema be papildomo mokesčio periodiškai atnaujina ir įdiegia gamintojo pateikiamą saugumo grėsmių informaciją, pažeidžiamumų sąrašus, identifikuojančius komunikaciją su įtartinais ir kenksmingais šaltiniais (IP adresais) internete, kenksmingo kodo maišos sumas, žinomus blogus domenus ir kt. Sistema automatiškai identifikuoja įvykius, sistemas ir naudotojus, kurie dalyvauja komunikacijoje su objektais pateikiamais saugumo grėsmių šaltiniuose. Sistema leidžia pridėti trečių šalių pateikiamus saugumo grėsmių (angl. *Threat Feeds*) šaltinius STIX / TAXII formatu.
10.	Naudotojų elgesio analizė	• Sistema turi turėti naudotojų elgesio analizės (angl. *User Behavior Analytics*) komponentą, galintį: o Analizuoti standartinę naudotojų veiklą ir aptikti joje anomalijas; o Aptikti pavogtas, kompromituotas naudotojų paskyras; o Integruotis ir perduoti informaciją į kitus sistemos saugumo komponentus, pavyzdžiui, koreliacijos variklį; o Identifikuoti pasikeitimus naudotojų elgsenoje; o Stebėti privilegijuotų naudotojų veiksmus; o Gebėti naudoti grėsmių informaciją naudotojų stebėjime; • Naudotojai turi turėti grėsmės įverčius, kurie kinta laike ir gali būti naudojami incidentams generuoti.	Sistema turi naudotojų elgesio analizės (angl. *User Behavior Analytics*) komponentą, galintį: Analizuoti standartinę naudotojų veiklą ir aptikti joje anomalijas; Aptikti pavogtas, kompromituotas naudotojų paskyras; Integruotis ir perduoti informaciją į kitus sistemos saugumo komponentus, pavyzdžiui, koreliacijos variklį; Identifikuoti pasikeitimus naudotojų elgsenoje; Stebėti privilegijuotų naudotojų veiksmus; Geba naudoti grėsmių informaciją naudotojų stebėjime; Naudotojai turi grėsmės įverčius, kurie kinta laike ir gali būti naudojami incidentams generuoti.
11.	Duomenų saugojimas	• Sistema turi turėti galimybę skirtingus įvykius saugoti skirtingą laiko tarpą. • Sistema turi turėti galimybę įvykius saugoti originaliu ir normalizuotu formatu. • Turi būti galimybė archyvuoti įvykius ilgalaikiam saugojimui pagal nustatytus kriterijus ir archyvinius įrašus saugoti suspaustame formate. • Sistema turi užtikrinti informavimą apie įvykių nesurinkimą arba apie nepilną surinkimą. • Sistema turi turėti funkcionalumą, leidžiantį daryti ilgalaikes kopijas nutolusioje duomenų saugykloje.	Sistema turi galimybę skirtingus įvykius saugoti skirtingą laiko tarpą. Sistema turi galimybę įvykius saugoti originaliu ir normalizuotu formatu. Yra galimybė archyvuoti įvykius ilgalaikiam saugojimui pagal nustatytus kriterijus ir archyvinius įrašus saugoti suspaustame formate. Sistema užtikrina informavimą apie įvykių nesurinkimą arba apie nepilną surinkimą. Sistema turi funkcionalumą, leidžiantį daryti ilgalaikes kopijas nutolusioje duomenų saugykloje.
12.	Sistemos administravimas	• Visos sistemos administravimo funkcijos turi būti realizuotos grafinėje Web sąsajoje;	Visos sistemos administravimo funkcijos yra realizuotos grafinėje Web sąsajoje; Sistemos administravimui naudojama sąsaja (angl. *GUI*), yra apsaugota HTTPS arba SSL mechanizmais;

		• Sistemos administravimui naudojama sąsaja (angl. *GUI*), turi būti apsaugota HTTPS arba SSL mechanizmais; • Sistema turi turėti funkcionalumą leidžiantį naudotojus autentifikuoti MS AD, LDAP protokolais iš centralizuotos naudotojų valdymo sistemos; • Sistema turi gebėti valdyti prieigas naudotojams bei jų grupėms.	Sistema turi funkcionalumą leidžiantį naudotojus autentifikuoti MS AD, LDAP protokolais iš centralizuotos naudotojų valdymo sistemos; Sistema geba valdyti prieigas naudotojams bei jų grupėms.
13.	Darbo su ataskaitomis galimybės	• Sistema turi turėti galimybę kurti ataskaitas remiantis sistemoje sukauptais duomenimis; • Sistema turi turėti galimybę konfigūruoti ataskaitas pagal vartotojo pageidavimus; • Sistema turi turėti galimybę kurti ataskaitų šablonus; • Sistema turi turėti iš anksto sukurtų ataskaitų šablonus; • Sistema turi turėti galimybę automatiškai platinti ataskaitas elektroniniu paštu.	Sistema turi galimybę kurti ataskaitas remiantis sistemoje sukauptais duomenimis; Sistema turi galimybę konfigūruoti ataskaitas pagal vartotojo pageidavimus; Sistema turi galimybę kurti ataskaitų šablonus; Sistema turi iš anksto sukurtų ataskaitų šablonus; Sistema turi galimybę automatiškai platinti ataskaitas elektroniniu paštu.
14.	Incidentų valdymo galimybės	Sistema turi turėti incidentų valdymo funkcionalumą, kuris atitiktų šiuos reikalavimus: • turi registruoti incidentus automatiniu būdu; • turi automatiškai nustatyti incidento prioritetą; • turi nustatyti incidento tipą; • turi turėti galimybę priskirti atsakingą sprendėją; • turi turėti galimybę įvykdyti veiksmus (pvz., išsiųsti elektroninį laišką, išsiųsti SNMP pranešimą, paleisti programinį kodą (angl. *Script*).	Sistema turi incidentų valdymo funkcionalumą, kuris atitinka šiuos reikalavimus: Registruoja incidentus automatiniu būdu; automatiškai nustato incidento prioritetą; nustato incidento tipą; turi galimybę priskirti atsakingą sprendėją; turi galimybę įvykdyti veiksmus (pvz., išsiųsti elektroninį laišką, išsiųsti SNMP pranešimą, paleisti programinį kodą (angl. *Script*).
15.	Atitikties standartams stebėjimas	• Turi būti sukonfigūruoti įrankiai (ataskaitos ir kt.), leidžiantys pasitikrinti atitikimą LST ISO/IEC 27000 šeimos ar lygiaverčių standartų reikalavimams.	Yra sukonfigūruoti įrankiai (ataskaitos ir kt.), leidžiantys pasitikrinti atitikimą LST ISO/IEC 27000 šeimos ar lygiaverčių standartų reikalavimams.
16.	Funkcionalumo plėtimo galimybės	• Sistemos gamintojas privalo turėti ir periodiškai atnaujinti portalą, iš kurio galima parsisiųsti ir įsidiegti nemokamus Sistemos funkcionalumą praplečiančius arba integracijai su kitomis saugos sistemomis skirtus plėtinius; • Sistema privalo turėti galimybę atsiradus poreikiui papildomai pridėti to paties gamintojo integruotą pažeidžiamumų skanavimo ir valdymo bei rizikos vertinimo modulį; • Sistema privalo turėti galimybę atsiradus poreikiui papildomai pridėti to paties gamintojo integruotą įvykių surinkimo bei kaupimo modulį, leidžiantį surinkti ir saugoti įvykius neatsižvelgiant į licencijos apribojimus, tačiau tų įvykių nenaudojant koreliacijai ir turint tik paieškos funkcionalumą; • Sistema privalo turėti galimybę atsiradus poreikiui papildomai pridėti to paties	Sistemos gamintojas turi ir periodiškai atnaujina portalą, iš kurio galima parsisiųsti ir įsidiegti nemokamus Sistemos funkcionalumą praplečiančius arba integracijai su kitomis saugos sistemomis skirtus plėtinius; Sistema turi galimybę atsiradus poreikiui papildomai pridėti to paties gamintojo integruotą pažeidžiamumų skanavimo ir valdymo bei rizikos vertinimo modulį; Sistema turi galimybę atsiradus poreikiui papildomai pridėti to paties gamintojo integruotą įvykių surinkimo bei kaupimo modulį, leidžiantį surinkti ir saugoti įvykius neatsižvelgiant į licencijos apribojimus, tačiau tų įvykių nenaudojant koreliacijai ir turint tik paieškos funkcionalumą; Sistema turi galimybę atsiradus poreikiui papildomai pridėti to paties gamintojo integruotą programinį arba techninį - aparatinį modulį, skirtą atlikti detalią tinklo

		gamintojo integruotą programinį arba techninį - aparatinį modulį, skirtą atlikti detalią tinklo srauto analizę ir pateikti OSI modelio Taikomojo lygmens (angl. *OSI L7 Application layer*) informaciją.	srauto analizę ir pateikti OSI modelio Taikomojo lygmens (angl. *OSI L7 Application layer*) informaciją.
17.	Licencijų galiojimas	• Turi būti siūlomas tiesioginio sistemos gamintojo sprendimas, perkančioji organizacija turi būti pirminis licencijų gavėjas. • Siūlomos sistemos licencijos (išskyrus palaikymą bei saugumo grėsmių duomenų bazės prenumeratą) turi galioti neribotą laiką. • Licencijos turi būti nepriklausomos nuo techninės - aparatinės įrangos, t. y. turi būti galimybė perkelti Sistemą į kitą Pirkėjo virtualizavimo platformą arba techninę - aparatinę įrangą be jokių papildomų mokesčių. • Sistemos programinės įrangos techninis palaikymas turi galioti 12 ne mažiau kaip mėnesių nuo Sistemos įsigijimo dienos. Techninį palaikymą turi užtikrinti gamintojas. Reikalavimai programinės įrangos techniniam palaikymui: • Pirkėjas turi teisę nemokamai gauti ir naudoti naujas gamintojo išleidžiamas programinės įrangos versijas palaikymo galiojimo metu; • Pirkėjas turi teisę nemokamai gauti ir naudoti gamintojo išleidžiamus pakeitimų paketus ir pataisas.	Yra siūlomas tiesioginio sistemos gamintojo sprendimas, perkančioji organizacija yra pirminis licencijų gavėjas. Siūlomos sistemos licencijos (išskyrus palaikymą bei saugumo grėsmių duomenų bazės prenumeratą) galioja neribotą laiką. Licencijos yra nepriklausomos nuo techninės - aparatinės įrangos, t. y. yra galimybė perkelti Sistemą į kitą Pirkėjo virtualizavimo platformą arba techninę - aparatinę įrangą be jokių papildomų mokesčių. Sistemos programinės įrangos techninis palaikymas galioja ne mažiau kaip 12 mėnesių nuo Sistemos įsigijimo dienos. Techninį palaikymą užtikrina gamintojas. Reikalavimai programinės įrangos techniniam palaikymui: Pirkėjas turi teisę nemokamai gauti ir naudoti naujas gamintojo išleidžiamas programinės įrangos versijas palaikymo galiojimo metu; Pirkėjas turi teisę nemokamai gauti ir naudoti gamintojo išleidžiamus pakeitimų paketus ir pataisas. **Pridedamas gamintojo raštas.**
18.	Sistemos diegimas	• Sistema turi būti įdiegta į perkančiosios organizacijos virtualizavimo platformą, arba į perkančiosios organizacijos pasirinktą techninę - aparatinę įrangą. • Sistema turi būti sukonfigūruota taip, kad priimtų tinklo ugniasienės, 3 perkančiosios organizacijos naudotojų valdymo serverių (angl. *Domain Controler*) žurnalinius įrašus ir 3 perkančiosios organizacijos tinklo komutatorių (angl. *Switch*) tinklo srautą (angl. *NetFlows*).	Sistema bus įdiegta į perkančiosios organizacijos virtualizavimo platformą, arba į perkančiosios organizacijos pasirinktą techninę - aparatinę įrangą. Sistema bus sukonfigūruota taip, kad priimtų tinklo ugniasienės, 3 perkančiosios organizacijos naudotojų valdymo serverių (angl. *Domain Controler*) žurnalinius įrašus ir 3 perkančiosios organizacijos tinklo komutatorių (angl. *Switch*) tinklo srautą (angl. *NetFlows*).

Pardavėjas
UAB „NBCS“
J. Kazlausko g. 21, LT-08314 Vilnius
Įmonės kodas 301817848
PVM mok. kodas LT100006470618
a. s. LT41 7044 0600 0831 9438
AB „SEB bankas“, b. k. 70440

Generalinis direktorius
Artiom Maslov

LIETUVOS RESPUBLIKA * REPUBLIC OF LITHUANIA * VILNIUS * UAB „NBCS“ LTD

Pirkėjas
VšĮ Vilniaus universiteto ligoninė Santaros klinikos
Santariškių g. 2, LT-08661 Vilnius
Įmonės kodas 124364561
PVM mok. kodas LT243645610
a. s. LT71 7300 0100 0249 2260
AB „Swedbank“, b. k. 73000

Generalinis direktorius
Feliksas Jankevičius

LIETUVOS RESPUBLIKA Viešoji įstaiga Vilniaus universiteto ligoninė Santaros klinikos * VILNIUS