TECHNINĖ SPECIFIKACIJA

Pirkimo objektas - Saugumo Operacijų Centro paslaugos (toliau – SOC paslaugos) susidedančios iš:
- ✓ informacinių sistemų žurnalinių įrašų saugojimo ir koreliacijos sistemos (toliau – SIEM) paslaugų;
- ✓ SIEM analitikos ir reagavimo paslaugų;
- ✓ SIEM priežiūros paslaugų.

Paslaugų teikimo laikotarpis – ne daugiau kaip **36 mėnesiai nuo Sutarties įsigaliojimo dienos**.
Paslaugų teikimo režimas – **darbo dienomis, darbo valandomis (9x5), nuo 8:30 iki 17:30**.

1. Bendrieji reikalavimai

1.1. Tiekėjas turi būti oficialus siūlomos SIEM gamintojo atstovas (jeigu tiekėjas pats nėra siūlomos SIEM gamintojas) ir/arba turi turėti teisę teikti siūlomas paslaugas. Kartu su pasiūlymu Tiekėjas turi pateikti tokią teisę įrodančius dokumentus.

1.2. Siūlomos SIEM programinės įrangos gamintojas turi būti registruotas Europos Sąjungos valstybėje narėje, Šiaurės Atlanto sutarties organizacijos valstybėje narėje ar trečiojoje šalyje, pasirašiusioje VPĮ 17 straipsnio 4 dalyje nurodytus tarptautinius susitarimus.

1.3. 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 tiekėjai gali siūlyti lygiaverčius.

1.4. Tiekėjas turi užtikrinti, kad atliekant saugumo informacijos ir įvykių valdymo sistemos diegimą, nebus sutrikdomas Perkančiosios organizacijos informacinės sistemos bei duomenų perdavimo tinklo darbas. Jeigu Perkančiosios organizacijos informacinės sistemos arba duomenų perdavimo tinklo darbas bus trikdomas, numatomi darbai turi būti atliekami ne Perkančiosios organizacijos darbo metu ir suderinus su atsakingu už sutarties vykdymą asmeniu.

1.5. Tiekėjo specialistai privalo mokėti lietuvių kalbą arba turi būti užtikrintos kokybiškos vertimo paslaugos Tiekėjo sąskaita.

1.6. Tiekėjo parengti dokumentai (analizės, projektavimo ir diegimo dokumentacija) turi būti pateikiami lietuvių kalba.

1.7. Tiekėjas 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. Tiekėjo 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. Tiekėjo pagalbos tarnyboje turi būti komunikuojama lietuvių kalba. Tiekėjo pagalbos tarnyba turi suteikti galimybes registruoti kreipinius tiek elektroniniu paštu, tiek telefonu, tiek per Web portalą.

1.8. SIEM platformos paslauga (teikiama iš Tiekėjo arba gamintojo duomenų centro):

Nr.	Specifikacija	Reikalavimai	Atitikimas (pildo tiekėjas)
1.	SIEM sistemos gamintojas ir versija	Nurodyti	IBM Qradar 7.5.0 Update Package 10
2.	Paskirtis	• Turi būti siūlomas specializuotas programinis sprendimas. Visa programinė įranga	• Siūlomas specializuotas SIEM (IBM Qradar) programinis sprendimas. Visa programinė yra specializuota šioje

		privalo būti specializuota šioje specifikacijoje numatytoms Informacinių sistemų žurnalinių įrašų saugojimo ir įvykių analizės (*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 sistemos charakteristikas ir atitikimą techninės specifikacijos reikalavimams.	specifikacijoje numatytoms Informacinių sistemų žurnalinių įrašų saugojimo ir įvykių analizės (*angl. SIEM - Security Information and Event Management*) funkcijoms atlikti. https://www.ibm.com/docs/en/qsip/7.5?topic=SS42VS_7.5/com.ibm.qradar.doc/c_qradar_pdfs.htm
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 turi būti teikiama kaip paslauga iš tiekėjo arba gamintojo duomenų centro. • Siūloma Sistema papildomai neturi reikalauti duomenų bazės licencijų. • Sistema negali reikalauti daugiau nei vieno virtualaus serverio resursų perkančiosios organizacijos duomenų centre. • 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.	• 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 teikiama kaip paslauga iš „Blue Bridge MSP“, UAB duomenų centro. • Siūloma Sistema papildomai nereikalauja duomenų bazės licencijų. • Sistema nereikalauja daugiau nei vieno virtualaus serverio resursų perkančiosios organizacijos duomenų centre (reikalauja vieno). • Sistemai ir jos komponentams visu paslaugos teikimo metu pateikiamos 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.
4.	Įvykiai (*angl. events*)	• Sistema turi būti pritaikyta surinkti ir apdoroti ne mažiau kaip 500 įvykių / įrašų per sekundę (angl. EPS – Events Per Second). • Sistema turi leisti viršyti licenciją ir priimti didesnį įvykių per sekundę skaičių galimos atakos atveju. Laikinos kaupyklos (angl. buffer) talpa turi būti ne mažesnė nei 5 GB. Sistema turi užtikrinti, kad įvykiai	• Sistema pritaikyta surinkti ir apdoroti ne mažiau kaip 1000 įvykių / įrašų per sekundę (angl. EPS – Events Per Second). • Sistema leidžia viršyti licenciją ir priimti didesnį įvykių per sekundę skaičių galimos atakos atveju. Laikinos kaupyklos (angl. buffer) talpa yra 5 GB. Sistema užtikrina, kad įvykiai nebus

		nebus prarandami ir bus apdorojami nuosekliai užtikrinant teisingą koreliacijos procesą. • 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 perkančiosios organizacijos taikomųjų programų sistemų.	prarandami ir bus apdorojami nuosekliai užtikrinant teisingą koreliacijos procesą. • Įvykių šaltinių skaičius nėra ribojamas. • 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 perkančiosios organizacijos 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.: perkančiosios organizacijos 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.: perkančiosios organizacijos kurtų vidinių sistemų įvykius.
6.	Įvykių koreliavimo galimybės	Sistema turi turėti galimybę: • Koreliuoti surinktą informaciją ir grupuoti įvykius, surinktus apie tam tikrą incidentą kompiuterių tinkle.	Sistema turi galimybę: • Koreliuoti surinktą informaciją ir grupuoti įvykius, surinktus apie tam tikrą incidentą kompiuterių tinkle.

		• Turėti išankstines gamintojo paruoštas įvykių koreliacijos taisykles. • Leisti kurti papildomas koreliacijos taisykles. • 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. • Sistemoje turi būti paleista ne mažiau 1000 vnt. aktyvių veikiančių gamintojo ar tiekėjo koreliavimo taisyklių.	• Turi 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. • Sistemoje bus paleista ne mažiau 1000 vnt. aktyvių veikiančių gamintojo ir tiekėjo koreliavimo taisyklių.
7.	Įvykių peržiūra	• Sistema turi leisti peržiūrėti ateinančius įvykius realiu laiku. • Sistema turi leisti atrinkti įvykius peržiūrai pagal nurodytus kriterijus. Atrinkimo kriterijus turi būti	• Sistema leidžia peržiūrėti ateinančius įvykius realiu laiku. • Sistema leidžia atrinkti įvykius peržiūrai pagal nurodytus kriterijus.

		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 turi leisti kurti interaktyviuosius valdymo ekranus, pateikiančius informaciją realiu laiku. • Sistema turi gebėti automatiškai pridėti prie IP adresų jų geografinę informaciją.	Atrinkimo kriterijus galima išsaugoti vėlesnėms paieškoms. • Sistemoje yra įtraukti standartiniai gamintojo interaktyvieji valdymo ekranai (*angl. dashboard*). Ekranuose matosi: 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 kurti interaktyviuosius valdymo ekranus, pateikiančius informaciją realiu laiku. • Sistema geba automatiškai pridėti prie IP adresų jų geografinę informaciją.
8.	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	• 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

		grėsmių (*angl. threat feeds*) šaltinius STIX / TAXII formatu.	(*angl. threat feeds*) šaltinius STIX / TAXII formatu.
9.	Naudotojų elgesio analizė	Sistema privalo turėti įdiegtą naudotojų elgesio analizės (*angl. User Behavior Analytics*) komponentą, galintį: • Analizuoti standartinę naudotojų veiklą ir aplikti 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. • Gebėti naudoti grėsmių informaciją naudotojų stebėjime. • Naudotojai turi turėti grėsmės įverčius, kurie kinta laike ir gali būti naudojami incidentams generuoti.	Sistema turi įdiegtą naudotojų elgesio analizės (*angl. User Behavior Analytics*) komponentą, galintį: • Analizuoti standartinę naudotojų veiklą ir aplikti 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. • Naudoti grėsmių informaciją naudotojų stebėjime. • Naudotojai turi grėsmės įverčius, kurie kinta laike ir gali būti naudojami incidentams generuoti.
10.	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.
11.	Sistemos administravimas	• Visos sistemos administravimo funkcijos turi būti realizuotos grafinėje web sąsajoje. • Sistemos administravimui naudojama sąsaja (*angl. GUI*), turi būti apsaugota HTTPS arba SSL mechanizmais.	• Visos sistemos administravimo funkcijos yra realizuotos grafinėje web sąsajoje. • Sistemos administravimui naudojama sąsaja (*angl. GUI*), yra apsaugota HTTPS arba SSL mechanizmais.

		• Sistema turi turėti funkcionalumą leidžiantį naudotojus autentifikuoti MS AD, LDAP protokolais iš centralizuotos naudotojų valdymo sistemos. • Sistema turi gebėti lengvai valdyti prieigas naudotojams bei jų grupėms.	• Sistema turi funkcionalumą leidžiantį naudotojus autentifikuoti MS AD, LDAP protokolais iš centralizuotos naudotojų valdymo sistemos. • Sistema geba lengvai valdyti prieigas naudotojams bei jų grupėms.
12.	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.
13.	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 „skriptą“).	Sistema turi incidentų valdymo funkcionalumą, kuris atitinka šiuos reikalavimus: • registruoti incidentus automatiniu būdu; • automatiškai nustatyti incidento prioritetą; • nustatyti incidento tipą; • turi galimybę priskirti atsakingą sprendėją; • turi galimybę įvykdyti veiksmus (pvz., išsiųsti elektroninį laišką, išsiųsti SNMP pranešimą, paleisti „skriptą“).
14.	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 valdymo bei rizikos vertinimo modulį.	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 valdymo bei rizikos vertinimo modulį.

		Sistema privalo turėti galimybę atsiradus poreikiui papildomai pridėti to paties gamintojo integruotą duomenų saugyklos išplėtimo 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 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.	Sistema turi galimybę atsiradus poreikiui papildomai pridėti to paties gamintojo integruotą duomenų saugyklos išplėtimo 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 srauto analizę ir pateikti OSI modelio Taikomojo lygmens (angl. OSI L7 Application layer) informaciją.
15.	Licencijų galiojimas	Sistemos programinės įrangos techninį palaikymą visą sutarties galiojimo laikotarpį turi užtikrinti Tiekėjas. Reikalavimai programinės įrangos techniniam palaikymui: • Perkančioji organizacija turi teisę gauti be papildomo mokesčio ir naudoti naujas gamintojo išleidžiamas programinės įrangos versijas palaikymo galiojimo metu. • Perkančioji organizacija turi teisę gauti be papildomo mokesčio ir naudoti gamintojo išleidžiamus pakeitimų paketus ir pataisas.	Sistemos programinės įrangos techninį palaikymą visą sutarties galiojimo laikotarpį užtikrina Tiekėjas. Reikalavimai programinės įrangos techniniam palaikymui: • Perkančioji organizacija turės teisę gauti be papildomo mokesčio ir naudoti naujas gamintojo išleidžiamas programinės įrangos versijas palaikymo galiojimo metu. • Perkančioji organizacija turės teisę gauti be papildomo mokesčio ir naudoti gamintojo išleidžiamus pakeitimų paketus ir pataisas.
16.	Paslaugos teikimo parametrai (SLA)	Paslaugos teikimo patikimumas – ne mažiau 99,8% per metus. Planuota prastova sistemos atnaujinimui – ne daugiau 6 val. per ketvirtį. Sistemos atstatymo kopija – ne senesnė nei 24 valandos.	Paslaugos teikimo patikimumas – 99,8% per metus. Planuota prastova sistemos atnaujinimui – 6 val. per ketvirtį. Sistemos atstatymo kopija – 24 valandos. Sistemos atsarginių kopijų skaičius – 14 vnt. (14 dienų). Žurnalinių įrašų saugojimas – 90 dienų.

		Sistemos atsarginių kopijų skaičius – ne mažiau 14 vnt. (14 dienų). Žurnalinių įrašų saugojimas – ne mažiau 90 dienų.	

2. Siūlomos SIEM sistemos analitika ir reagavimas:

2.1. Tiekėjas 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 Perkančiąja organizacija suderintą komunikacijos planą.

2.2. Paslaugos teikimo pradžioje, su Perkančiąja organizacija turi būti suderintas komunikacijos planas, apimantis: Tiekėjo ir Perkančiosios organizacijos suinteresuotų šalių kontaktus; procesą, aprašantį komunikacijos veiksmus incidento atveju; kanalus, kuriais vyks informavimas apie incidentus.

2.3. Tiekėjas turi atlikti incidentų stebėjimą, informavimą ir pagalbą užkardant incidentą, užklausų vykdymą pagal šiuos paslaugos teikimo parametrus:

Eil. Nr.	Priežiūros parametras	Parametro reikšmė
2.3.1.	Ataskaitinis periodas	1 (vienas) kalendorinis mėnuo
2.3.2.	Paslaugų teikimo valandos	Darbo dienomis nuo 8:30 iki 17:30 val.
2.3.3	Saugumo įvykio reakcijos laikas	Vidutiniškai 2 val., nuo visų saugumo įvykių per vieną ataskaitinį periodą
2.3.4.	Užklausos reakcijos laikas	8 val.
2.3.5	Užklausos sprendimo laikas	72 val.

2.4. Saugumo įvykio reakcijos laikas – tai laikotarpis, nuo saugumo įvykio atsiradimo SIEM iki pirmo Tiekėjo veiksmo. Pirmu Tiekėjo veiksmu laikoma:

a) Saugumo įvykio uždarymas kaip klaidingas suveikimas (angl. False Positive).

b) Tiekėjo užklausa sutartais komunikacijos kanalais Perkančiajai organizacijai norint kvalifikuoti saugumo įvykį.

c) Saugumo įvykio perkvalifikavimas į saugumo incidentą ir Perkančiosios organizacijos informavimas sutartais komunikacijos kanalais.

2.5. Reakcijos laiką fiksuoja Tiekėjas savo pagalbos tarnyboje ir pateikia Perkančiajai organizacijai statistiką ataskaitos formoje, per 10 darbo dienų nuo einamojo ataskaitinio laikotarpio pabaigos. SIEM generuojamų aliarmų analizė (patvirtinimas, klasifikavimas, grupavimas, išsprendimo iniciavimas, konsultavimas sprendžiant).

2.6. Siūlymai esamų koreliacijos taisyklių tobulinimui ir naujų įvedimui.

2.7. Siūlymai dėl kibernetinių grėsmių indikatorių šaltinių panaudojimo.

2.8. Incidento pirminių priežasčių (angl. *root cause*) nustatymas.

2.9. Incidento atakos grandinėlės nustatymas.

2.10. Incidento tyrimas, jo eigos atkūrimas.

2.11. SIEM esančių incidento įrodymų surinkimas ir išsaugojimas.

2.12. Saugos ir saugos valdymo procesų gerinimo rekomendacijų pateikimas, suvaldžius incidentą.

2.13. Tiekėjas turi atlikti Perkančiosios organizacijos pateiktas užklausas dėl:

- ✓ naujų koreliacijos taisyklių pridėjimo;
- ✓ koreliacijos taisyklių konfigūravimo;
- ✓ ataskaitų sukūrimo;
- ✓ specifinių sisteminių įrašų nufiltravimo iš SIEM.

2.14. Tiekėjas turi teikti ataskaitas, iš anksto sutartas su Perkančiąja organizacija, ne rečiau nei 1 kartą per ataskaitinį periodą, kurioje turi būti mažiausiai šie duomenys: įvykių per sekundę skaičius, aktyvių koreliavimo taisyklių skaičius, visi išsiųsti incidentai ir užklausos su gautais atsakymais, aktyvūs duomenų šaltiniai, TOP 1-0 suveikusių koreliavimo taisyklių, saugumo įvykių skaičius, saugumo incidentų skaičius, saugumo incidentų skaičius pagal grėsmės kategoriją, ne paslaugos teikimo valandomis sureaguotų saugumo

įvykių skaičius, svarbiausi saugumo incidentai ir rekomendacijos joms spręsti, vidutinis saugumo įvykio reakcijos laikas.

2.15. Tiekėjas turi teikti periodinius (ne rečiau kaip kas 3 mėnesius) nuotolinius susitikimus, ketvirtinėms ataskaitoms ir konsultacijas dėl paslaugos gerinimo iniciatyvoms aptarti.

2.16. Tiekėjas turi vykdyti šiuos analitikos darbus:

- ✓ Naujų koreliacijos taisyklių kūrimas.
- ✓ Koreliacijos taisyklių tobulinimas pašalinant neteisingai-teigiamus (*angl. false-positive*) suveikimus SIEM.
- ✓ Saugumo įvykių/aliarmų kvalifikavimas į incidentus.
- ✓ Automatinių pranešimų, iš anksto suderintų su Perkančiąja organizacija, konfigūravimas.

2.17. Tiekėjas turi valdyti pastebėtą ir kvalifikuotą saugumo incidentą nuo jo užfiksavimo iki Perkančiajai organizacijai informavus apie incidento išsprendimą, pagal iš anksto suderintą su Perkančiąja organizacija komunikacijos bei incidentų valdymo procesą.

2.18. Tiekėjas incidento metu turi siūlyti rekomendacijas bei teikti konsultacijas Perkančiajai organizacijai dėl saugumo incidento užkardymo:

- ✓ Greitojo atsako (užkardymo, žalos mažinimo ir pan.) veiksmų nustatymas ir pateikimas Perkančiajai organizacijai.
- ✓ Po incidento užkardymo pateikti ilgalaikio poveikio veiksmus – rekomendacijas IT infrastruktūros saugumo spragų, kuriomis buvo pasinaudota saugumo incidento metu, šalinimui.

2.19. Tiekėjas 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. Siūlomos SIEM sistemos priežiūra:

3.1. Nuolatinis SIEM būklės stebėjimas, proaktyvi problemų prevencija, reagavimas į pastebėtus sutrikimus ir problemas, SIEM veikimo atkūrimas.

3.2. SIEM programinių atnaujinimų įdiegimas ne vėliau nei per 45 darbo dienas po gamintojo atnaujinimo išleidimo.

3.3. Standartinių (iki 10 vnt. per ataskaitinį periodą) ir specifinių (iki 1 vnt. per ataskaitinį periodą) įrašų šaltinių tvarkymas: pridėjimas į SIEM, modifikavimas, pašalinimas.

3.4. Išorinių kibernetinių grėsmių indikatorių (angl. *cyber threat intelligence*) duomenų šaltinių (kenksmingų IP adresų, domenų ir pan.) tvarkymas: pridėjimas, modifikavimas, pašalinimas.

3.5. SIEM koreliacijos taisyklių konfigūravimas pagal saugumo analitikų pateiktas rekomendacijas ir pastabas (modifikavimas, pašalinimas).

3.6. Perteklinių sisteminių įrašų nufiltravimas ir rekomendacijų ką nufiltruoti siūlymas.

3.7. Rekomendacijų teikimas dėl reikalingų sisteminių įrašų rinkimo.

3.8. Naujų sistemos naudotojų pridėjimas, senų sistemos naudotojų pašalinimas.

3.9. Darbalaukių kūrimas pagal saugumo analitikų siūlymus ir perkančiosios organizacijos poreikį.

3.10. Ataskaitų kūrimas pagal saugumo analitikų siūlymus ir perkančiosios organizacijos poreikį.

3.11. Greitųjų paieškos šablonų kūrimas.
3.12. Rekomendacijų teikimas sistemos veiklai gerinti ir jų įgyvendinimas.

4. Reikalavimai Tiekėjo pagalbos tarnybai

Eil. Nr.	Reikalavimas
1.	Tiekėjas turi turėti 24 valandas per parą 7 dienas per savaitę veikiančią pagalbos tarnybą.
2.	Tiekėjas turi turėti pagalbos tarnybą komunikuojančią lietuvių kalba su Perkančiąja organizacija raštu ir žodžiu.
3.	Tiekėjo pagalbos tarnyba turi suteikti galimybes registruoti kreipinius įvairiais nurodytais kanalais: elektroniniu paštu; fiksuoto ir mobilaus ryšio telefonu; naudojant WEB sąsają
4.	Tiekėjas turi būti įdiegęs veikiančius ir aprašytus incidentų bei keitimų valdymo procesus, atitinkančius IT paslaugų valdymo (ITIL ar lygiavertės metodikos) gerųjų praktikų rekomendacijas bei veikiantį internetinį portalą kreipiniams registruoti bei peržiūrėti.
5.	Tiekėjo pagalbos tarnyba turi užtikrinti operatyvų atgalinį ryšį ir informacijos apie incidentus realiu laiku (angl. On-line) teikimą interneto tinklalapyje, veikiančiame HTTPS protokolu.
6.	Pagalbos tarnyba turi informuoti apie užregistruotų incidentų būklę, planuojamą incidentų išsprendimo datą ir laiką bei incidentų išsprendimą.