TECHNINĖ SPECIFIKACIJA

Eil. Nr.	Specifikacija	Reikalavimai	Tiekėjo komentarai
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 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

		• 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. • Sistemai ir jos komponentams turi būti pateiktos naujausios programinės įrangos versijos. • Į perkamų prekių apimtis turi būti	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.

		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	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.

		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.	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:	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.

		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	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.

		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.	
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:	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 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 turi leisti kurti interaktyviuosius valdymo ekranus, pateikiančius informaciją realiu laiku. • Sistema turi gebėti automatiškai pridėti prie IP adresų jų geografinę informaciją.	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 geba automatiškai pridėti prie IP adresų jų geografinę informaciją.
9.	Grėsmių aptikimas	• Sistema be papildomo mokesčio turi	Sistema be papildomo mokesčio periodiškai atnaujina ir įdiegia gamintojo pateikiamą saugumo grėsmių

		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. T*hreat Feeds*) šaltinius STIX / TAXII formatu.	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. T*hreat Feeds*) šaltinius STIX / TAXII formatu.
10.	Naudotojų elgesio analizė	• Sistema turi tūrėti 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;	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.

		○ Stebėti privilegijuotų naudotojų veiksmus; ○ Gebėti naudoti grėsmių informaciją naudotojų stebėjime; • Naudotojai turi turėti 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; • 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 funkcionalumą leidžiantį naudotojus autentifikuoti MS AD, LDAP protokolais iš centralizuotos naudotojų valdymo sistemos; Sistema geba valdyti prieigas naudotojams bei jų grupėms.

		• 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.	
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	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*).

		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 srauto analizę ir pateikti OSI modelio Taikomojo lygmens (angl. *OSI L7 Application layer*) informaciją.

		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.	
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;	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.**

		• Pirkėjas turi teisę nemokamai gauti ir naudoti gamintojo išleidžiamus pakeitimų paketus ir pataisas.	
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*).

Vilma Bagdonaitė