Pirkimo sąlygų
2 priedo priedėlis

SIŪLOMŲ PREKIŲ TECHNINIAI PARAMETRAI

1. Tiekėjas turi užpildyti stulpelį „Siūloma tiekti prekė visiškai atitinka pirkimo dokumentuose nustatytus techninius reikalavimus ir jos savybės tokios:“ ***2. Nurodome siūlomų prekių technines specifikacijas, charakteristikas ir pagrindines savybes pagal pirkimo dokumentuose nurodytus reikalavimus (tiekėjas negali naudoti sąvokos „Atitinka“, o privalo aiškiai apibūdinti siūlomų prekių charakteristikas, priešingu atveju toks pasiūlymas bus pripažintas neatitinkančiu pirkimo dokumentų reikalavimų ir bus atmestas).*** ***3. Patvirtiname, kad vykdant prekių pirkimo-pardavimo sutartį bus įvykdyti šie reikalavimai:***		
Eil. Nr.	**Reikalaujamos prekių techninės charakteristikos**	**Siūloma tiekti prekė visiškai atitinka pirkimo dokumentuose nustatytus techninius reikalavimus ir jos savybės tokios** *(techninių reikalavimų formuluotėse, kur nurodyta paklaida ar reikalavimas "Taip/Ne (tikslus aprašymas) nurodomos siūlomo objekto charakteristikos)* ***(užpildo tiekėjas pateikdamas pasiūlymą)*****
1.	**Bendrieji reikalavimai**	
1.1	Grėsmių analizės programinė įranga (toliau – programinė įranga) turi būti pateikta gamintojo arba gamintojo įgalioto asmens.	Taip Gamintojo ECLECTIC IQ autorizuoto atstovo UAB „WhiteBit“. *ECLECTIC IQ autorizacijos rastas*
1.2	Tiekėjas turi pateikti nuorodą ar nuorodas į gamintojo interneto puslapį, kuriame yra tiksli pasiūlymą atitinkančios programinės įrangos techninė specifikacija arba pateikti gamintojo parengtą siūlomos programinės įrangos aprašymą.	*Pateikiamos nuorodos į gamintojo internetinį puslapį. Jeigu pasirenkama teikti ne nuorodas į gamintojo puslapį, pagal Pirkimo sąlygų 5.11.5. papunktį su pasiūlymu yra pateikiami dokumentai, patvirtinantys siūlomų prekių atitiktį techninės specifikacijos reikalavimams*
1.3	Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie programinės įrangos gamybos arba tobulinimo nutraukimą (pvz., angl. end of life time arba Discontinued).	Pagal Pirkimo sąlygų 5.11.4. papunktį. Pateikiamas gamintojo užtikrinimas. *ECLECTIC IQ gamintojo patvirtinimas*

1.4	Įrangos dokumentai turi būti lietuvių arba anglų kalba. Gamintojo interneto svetainėje tvarkyklių ir dokumentų paieška atliekama anglų arba lietuvių kalba.		Taip Anglų kalba. Gamintojo tinklapis www.eclecticiq.com
1.5	Tiekėjas turi užtikrinti, kad įsigyjamoje įrangoje nebūtų įdiegta jokios papildomos programinės įrangos, kuri nėra būtina tokios įrangos funkcionalumui užtikrinti.		Taip
2.1	Perkančiosios organizacijos naudotojai apmokyti naudotis ir šiuo metu naudoja,, EclecticIQ – Intelligence at the core™" programinę įrangą, tačiau jai būtinas licencijos pratęsimas – šio pirkimo objekto etalonas. Programinė įranga turi leisti dirbti su kibernetinių grėsmių indikatoriais, juos analizuoti, tikrinti tarpusavio ryšius. Programinė įranga yra komplektuojama su 5 (penkiomis) naudotojo paskyromis. Programinė įranga yra keliami šie minimalūs reikalavimai:		Siūlomas „EclecticIQ – Intelligence at the core™" programinė įrangos licencijos pratęsimas. Programinė įranga leidžia dirbti su kibernetinių grėsmių indikatoriais, juos analizuoti, tikrinti tarpusavio ryšius. Programinė įranga yra komplektuojama su 5 (penkiomis) naudotojo paskyromis. Programinė įranga palaiko šiuos minimalūs reikalavimai:
2.1.1	Paskirtis	Siūloma programinė įranga turi būti gamintojo pozicionuojama kaip įrankis, skirtas analizuoti ir apdoroti kibernetinių grėsmių indikatorius, tokius, kaip IP adresai, domenai, maišos reikšmės (angl. hash) rezultatai. Programinė įranga turi būti pasiekiama per naršyklę ir veikti ant organizacijoje naudojamų kompiuterių su Windows ar Linux operacinėmis sistemomis.	Siūloma programinė įranga gamintojo pozicionuojama kaip įrankis, skirtas analizuoti ir apdoroti kibernetinių grėsmių indikatorius, tokius, kaip IP adresai, domenai, maišos reikšmės (angl. hash) rezultatai. Programinė įranga pasiekiama per naršyklę ir gali veikti ant organizacijoje naudojamų kompiuterių su Windows ar Linux operacinėmis sistemomis.
2.1.2	Grėsmių analizės programinės įrangos (angl. feed) palaikymas	Programinė įranga turi turėti galimybę palaikyti populiariausias kibernetinių grėsmių indikatorių srauto prenumeratas, kaip: - Dragos; - EclecticIQ commercial sources; - Flashpoint; - Intel471; - MISP; - RecordedFuture; - Ir t.t.	Programinė įranga turi galimybę palaikyti populiariausias kibernetinių grėsmių indikatorių srauto prenumeratas: - Dragos; - EclecticIQ commercial sources; - Flashpoint; - Intel471; - MISP; - RecordedFuture. *https://www.eclecticiq.com/partners#overview*

2.1.3	Paieškos kriterijų nustatymas	Turi būti galimybė: - Atlikti paiešką pagal raktinius žodžius; - Atlikti paiešką pagal informaciją aktualią su tam tikra valstybe; - Atlikti paiešką pagal kampanijas (angl. campaigns); - Atlikti paiešką pagal incidentus; - Atlikti raportų paiešką; - Atlikti (angl. threat actors) paiešką; - Paiešką programinėje įrangoje turi būti galima atlikti „Apache Lucene“ sintakse.	Taip *EclecticIQ_Functionality_And_Specifications_2.10*
2.1.4	Darbas su indikatoriais ir programine įranga	Programinė įranga turi leisti atlikti veiksmus su indikatoriais: - Leisti juos priskirti į tam tikras grupes; - Leisti indikatorius atvaizduoti grafiškai ir rodyti ryšius tarp jų; - Leisti juos praturtinti (angl. enrich) informacija, prieinama iš trečiųjų šalių integracijų (angl. third-party integrations), tokių, kaip „VirusTotal“. Šių integracijų skaičius turi būti ne mažesnis nei 80; Programinė įranga taip pat turi leisti platinti žvalgybinę informaciją šiais būdais: - Žmonėms skaitomu formatu (PDF, TXT tipo failai); - Mašinų skaitomu formatu; - El. laiškais. Programinė įranga turi leisti grupuoti ir skirstyti vartotojus į grupes. Taip pat turi būti galimybė leisti tam tikrai grupei vartotojų matyti tik tam tikrus informacijos šaltinius. Programinė įranga turi būti galimybė tam	Programinė įranga leidžia atlikti veiksmus su indikatoriais: - Leidžia juos priskirti į tam tikras grupes; - Leidžia indikatorius atvaizduoti grafiškai ir rodyti ryšius tarp jų; - Leidžia juos praturtinti (angl. enrich) informacija, prieinama iš trečiųjų šalių integracijų (angl. third-party integrations), tokių, kaip „VirusTotal“. Šių integracijų skaičius yra ne mažesnis nei 80; Programinė įranga taip pat leidžia platinti žvalgybinę informaciją šiais būdais: - Žmonėms skaitomu formatu (PDF, TXT tipo failai); - Mašinų skaitomu formatu; - El. laiškais. Programinė įranga leidžia grupuoti ir skirstyti vartotojus į grupes. Taip pat yra galimybė leisti tam tikrai grupei vartotojų matyti tik tam tikrus informacijos šaltinius. Programinė įranga turi galimybę tam tikriems vartotojams (ar grupėms) leisti tik skaityti, trinti ar keisti informaciją.

		tikriems vartotojams (ar grupėms) leisti tik skaityti, trinti ar keisti informaciją. Priimant galimų grėsmių duomenis, privalo būti galimybė automatiškai žymėti bei nustatyti pasitikėjimo lygį įvykio, atributo, informacijos santraukos ir šaltinio. Programinė įranga turi leisti rašyti ataskaitas raiškiojo teksto redaktoriumi, taip pat saugoti ataskaitas ir taip palengvinti žinių kūrimą. Programinė įranga turi būti sąsajų analizės funkcija, galinti vizualizuoti struktūrizuotą CVE (angl. Common Vulnerabilities and Exposures) analizę, TTP (angl. Tactics, Techniques, Procedures), kenkėjiškas programas, kenkėjiškų programų tipus, susijusius grėsmių veikėjus, kampanijas ir bendrus atakų modelius. Sąsajų analizė privalo suteikti laiko planavimo juostos galimybę ir įvairias vizualizacijos priemones. Analitikams turi būti galimybė atlikti veiksmus grafe, t.y atvaizduoti informaciją. Grafuose galimi veiksmai turi apimti pvz.: praturtinti, pavesti, apdoroti trečiųjų šalių įrankiais, kurti subjektus. Vartotojai privalo galėti filtruoti nereikšmingą analizę iš sąsajų analizės. Programinėje įrangoje privalomai turi būti galimybė ieškoti CVE, parodant kurios saugumo spragos, kenkėjiškos programos ir kampanijos susiję su ieškomu CVE.	Priimant galimų grėsmių duomenis, yra galimybė automatiškai žymėti bei nustatyti pasitikėjimo lygį įvykio, atributo, informacijos santraukos ir šaltinio. Programinė įranga leidžia rašyti ataskaitas raiškiojo teksto redaktoriumi, taip pat saugoti ataskaitas ir taip palengvinti žinių kūrimą. Programinė įranga turi sąsajų analizės funkciją, kuri gali vizualizuoti struktūrizuotą CVE (angl. Common Vulnerabilities and Exposures) analizę, TTP (angl. Tactics, Techniques, Procedures), kenkėjiškas programas, kenkėjiškų programų tipus, susijusius grėsmių veikėjus, kampanijas ir bendrus atakų modelius. Sąsajų analizė gali suteikti laiko planavimo juostos galimybę ir įvairias vizualizacijos priemones. Analitikams yra galimybė atlikti veiksmus grafe, t.y atvaizduoti informaciją. Grafuose galimi veiksmai apima pvz.: praturtinti, pavesti, apdoroti trečiųjų šalių įrankiais, kurti subjektus. Vartotojai gali filtruoti nereikšmingą analizę iš sąsajų analizės. Programinėje įrangoje privalomai yra galimybė ieškoti CVE, parodant kurios saugumo spragos, kenkėjiškos programos ir kampanijos susiję su ieškomu CVE. Programinė įranga suteikia galimybę rengti intelektualios analizės ataskaitas ir susieti duomenų rinkinius. Skirtingi naudotojai ir grupės gali bendradarbiauti prieigos kontroliuojamose darbo srityse.

		Programinė įranga suteikia galimybę rengti intelektualios analizės ataskaitas ir susieti duomenų rinkinius. Skirtingi naudotojai ir grupės turi galėti bendradarbiauti prieigos kontroliuojamose darbo srityse. Programinėje įrangoje privalo suteikti galimybę išfiltruoti ir anonimizuoti informaciją prieš dalijantis su likusiomis suinteresuotosiomis šalimis. Programinėje įrangoje turi būti nustatyti standartiniai TLP (Traffic Light Protocol) išleidimo reitingai, pagal kuriuos informacija gali būti nukreipiama konkretiems naudotojams ir naudotojų grupėms pagal jų prieigos lygį. (pvz., "TLP Raudona" informacija nebus siunčiama naudotojui ar naudotojų grupei, kuri turėtų pasiekti tik "TLP Geltona"). Programinė įranga turi suteikti galimybę sukurti taisykles, pagal kurias skirtingi duomenys galėtų būti siunčiami į skirtingas darbo vietas pagal jų turinį. Programinė įranga suteikia galimybę ir priemones, leidžiančias keliems analitikams dirbti su vienu tyrimu/ataskaita.	Programinėje įrangoje suteikiama galimybė išfiltruoti ir anonimizuoti informaciją prieš dalijantis su likusiomis suinteresuotosiomis šalimis. Programinėje įrangoje gali būti nustatyti standartiniai TLP (Traffic Light Protocol) išleidimo reitingai, pagal kuriuos informacija gali būti nukreipiama konkretiems naudotojams ir naudotojų grupėms pagal jų prieigos lygį. (pvz., "TLP Raudona" informacija nebus siunčiama naudotojui ar naudotojų grupei, kuri turėtų pasiekti tik "TLP Geltona"). Programinė įranga suteikia galimybę sukurti taisykles, pagal kurias skirtingi duomenys galėtų būti siunčiami į skirtingas darbo vietas pagal jų turinį. Programinė įranga suteikia galimybę ir priemones, leidžiančias keliems analitikams dirbti su vienu tyrimu/ataskaita. https://www.eclecticiq.com/partners#overview https://www.eclecticiq.com/products/intelligence-center?hsLang=en *EclecticIQ_Intelligence_Center_Data_Sheet* *EclecticIQ_Functionality_And_Specifications_2.10*
2.1.5	Komercinių šaltinių kibernetinių grėsmių indikatorių srautas (angl. feed)	Į plėtimo paslaugų paketą turi būti įtrauktas „EclecticIQ Commercial Sources Feed“ komercinių šaltinių kibernetinių grėsmių indikatorių duomenų srautas (angl. feed) ar lygiavertis, kurio funkcionalumai yra šie: • PĮ gamintojo kuruojamas komercinių šaltinių grėsmių duomenų sklaidos kanalas, kuris sujungia šaltinius, kad PĮ vartotojai suprastų	Į plėtimo paslaugų paketą įtrauktas „EclecticIQ Commercial Sources Feed“ komercinių šaltinių kibernetinių grėsmių indikatorių duomenų srautas (angl. feed), kurio funkcionalumai yra šie: • PĮ gamintojo kuruojamas komercinių šaltinių grėsmių duomenų sklaidos kanalas, kuris sujungia šaltinius, kad PĮ vartotojai suprastų pagrindines grėsmes, įskaitant

		pagrindines grėsmes, įskaitant polimorfines kenkėjiškas programas ir „DDOS botnet“ tinklus, nukreiptus į įmonių tinklus, paskirstytas kompiuterines platformas ir jų operacines sistemas. • Naudodami mašininį mokymąsi, komerciniai šaltiniai turi apdoroti duomenis iš ne mažiau kaip 500 milijonų jutiklių, smėliadėžių, tinklo analizatorių, žiniatinklio skaitytuvų, stebimų robotų tinklų ir tamsiojo interneto. • Kibernetinių grėsmių indikatorių srautas turi atlikti grėsmių analitiką panaudojant EclecticIQ grėsmių žvalgybos analizes, įskaitant taktines, strategines ir operatyvines savaitines santraukas ir žvalgybos ataskaitas, kurios būtų susiejamos su struktūrizuotomis vizualizacijomis EclecticIQ Intelligence platformoje. • Lesti naudoti MITRE ATT&CK elementariu objektų lygmeniu, su galimybe susieti MITRE TTP ir kitus sistemos elementus. • Efektyvi ir paprasta (t. y. naudojant API) komercinių šaltinių integracija į EclecticIQ Intelligence platformą, kad būtų galima matyti pirminę grėsmę.	polimorfines kenkėjiškas programas ir „DDOS botnet“ tinklus, nukreiptus į įmonių tinklus, paskirstytas kompiuterines platformas ir jų operacines sistemas. • Naudodami mašininį mokymąsi, komerciniai šaltiniai gali apdoroti duomenis iš 500 milijonų jutiklių, smėliadėžių, tinklo analizatorių, žiniatinklio skaitytuvų, stebimų robotų tinklų ir tamsiojo interneto. • Kibernetinių grėsmių indikatorių srautas gali atlikti grėsmių analitiką panaudojant EclecticIQ grėsmių žvalgybos analizes, įskaitant taktines, strategines ir operatyvines savaitines santraukas ir žvalgybos ataskaitas, kurios būtų susiejamos su struktūrizuotomis vizualizacijomis EclecticIQ Intelligence platformoje. • Leidžia naudoti MITRE ATT&CK elementariu objektų lygmeniu, su galimybe susieti MITRE TTP ir kitus sistemos elementus. • Efektyvi ir paprasta (t. y. naudojant API) komercinių šaltinių integracija į EclecticIQ Intelligence platformą, kad būtų galima matyti pirminę grėsmę. *EclecticIQ_Curated_Feeds_Data_Sheet*
2.1.6	Licencija	Programinės įrangos licencija turi galioti ne mažiau nei 5 naudotojams vienu metu ir ne trumpiau kaip 12 mėn. Programinės įrangos licencijos galiojimo pradžia bus nurodoma pasirašant sutartį.	Programinės įrangos licencija galios 5 naudotojams vienu metu ir 12 mėn. laikotarpiui. Programinės įrangos licencijos galiojimo pradžia gali būti nurodoma pasirašant sutartį.
2.3	Programinės įrangos palaikymo sąlygos turi suteikti programinės įrangos techninės pagalbos paslaugą visą licencijos galiojimo laikotarpį. Į techninę pagalbą turi įeiti įvairių programinių gedimų, susijusių su programine įranga, šalinimas ir pagalba naudojantis programine įranga.		Taip
2.4	Programinės įrangos pagrindinė paskirtis privalo būti analizės atlikimas, bei rezultatų sklaida.		Taip

2.5	Programinė įranga turi turėti atakų aptikimo paieškos modulius (angl. hunting packages), bei palaikyti MITRE ATT&CK modelio taksonomiją.	Taip
2.6	Programinė įranga turi palaikyti struktūrizuotus šaltinius, įskaitant, bet neapsiribojant: STIX 1.x, STIX 2.x, CSV, pdf ir kt	Programinė įranga palaiko struktūrizuotus šaltinius, įskaitant, bet neapsiribojant: STIX 1.x, STIX 2.x, CSV, PDF https://www.eclecticiq.com/products/intelligence-center?hsLang=en *EclecticIQ_Intelligence_Center_Data_Sheet* *EclecticIQ_Functionality_And_Specifications_2.10*
2.7	Programinė įranga privalo gebėti agreguoti informaciją gautą iš vidaus incidentų naudojant SIEM technologiją (ar lygiavertę). Integracija turi būti galima įskaitant, bet ne apsiribojant su šiais produktais: "Splunk", "QRadar" ir "ArcSight". Šios integracijos turi leisti iš žurnalo duomenų (angl. logs) generuoti pastebėjimus ir automatiškai sukurti įrašus sistemoje.	Programinė įranga geba agreguoti informaciją gautą iš vidaus incidentų naudojant SIEM technologiją. Integracija galima įskaitant, bet ne apsiribojant su šiais produktais: "Splunk", "QRadar" ir "ArcSight". Šios integracijos leidžia iš žurnalo duomenų (angl. logs) generuoti pastebėjimus ir automatiškai sukurti įrašus sistemoje. https://www.eclecticiq.com/products/intelligence-center?hsLang=en *EclecticIQ_Intelligence_Center_Data_Sheet* *EclecticIQ_Functionality_And_Specifications_2.10*

*Pastaba: Nurodyti pavadinimai, medžiagų / įrangos gamintojai technologinis procesas, standartas, prekių kilmė, konkretus pavadinimas, ženklas (jei tokią prielaidą galima daryti) yra informacinio pobūdžio ir tiekėjas nėra įpareigojamas siūlyti ir/ar naudoti šių gamintojų produkciją, standartą, procesą (gali naudoti lygiaverčius). Teikdamas pasiūlymą, tiekėjas turi vadovautis šiuo metu galiojančiais normatyvais technologijai, medžiagoms, įrangai bei darbams, atsižvelgti į pirkimo objekto specifiką. Lygiavertiškumo nurodytiems duomenims įrodymo prievolė tenka tiekėjui. Jei tiekėjas siūlo produktą, kuriuo naudotis perkančiosios organizacijos darbuotojai neapmokyti (2.1 techninės specifikacijos punkto prasme), į nuomos kainą turi būti įskaičiuota šios programinės įrangos instaliavimo, jei reiktų suderinamumui užtikrinti – techninės įrangos pateikimo bei 5 darbuotojų apmokymo naudotis kaštai.

Pardavimų direktorius		[redacted]
(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas)	(Parašas)	(Vardas ir pavardė)