Pirkimo sąlygų
2 priedo priedėlis

SIŪLOMŲ PREKIŲ TECHNINIAI PARAMETRAI

1. Teikėjas turi užpildyti 3 stulpelį „Siūloma tiekti paslauga visiškai atitinka pirkimo dokumentuose nustatytus techninius reikalavimus ir jos savybės tokios:“ ***2. Nurodome siūlomų paslaugų technines specifikacijas, charakteristikas ir pagrindines savybes pagal pirkimo dokumentuose nurodytus reikalavimus (teikėjas negali naudoti sąvokos „Atitinka“, o privalo aiškiai apibūdinti siūlomų paslaugų charakteristikas, priešingu atveju toks pasiūlymas bus pripažintas neatitinkančiu pirkimo dokumentų reikalavimų ir bus atmestas).*** ***3. Patvirtiname, kad vykdant paslaugų pirkimo-pardavimo sutartį įsigyjamas objektas atitiks šiuos reikalavimus:***		
Eil. Nr.	**Reikalaujamos paslaugų techninės charakteristikos**	**Siūloma tiekti paslauga 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 teikėjas pateikdamas pasiūlymą)******
1	2	3
1.	**1 pirkimo dalis.** **ĮSILAUŽIMO DETEKTAVIMO SISTEMOS (IDS) PARAŠŲ PRENUMERATOS PASLAUGOS, 36 mėn.**	
1.1.	**Paslaugoms keliami reikalavimai:**	
1.1.1	Įsilaužimo detektavimo sistemos (IDS) įsilaužimo detektavimo taisyklių rinkinio prenumeratos paslaugos apima Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) naudojamos įsilaužimo detektavimo taisyklių rinkinio „ETPro Ruleset” (toliau – parašai) prenumeratos pratęsimą 36 mėn. laikotarpiui.	*(nurodyti pratęsiamos ETPro Ruleset licencijos galiojimo terminą mėn.)*
1.1.2.	Paslaugos privalo leisti gauti parašus apie naujausias grėsmes, bei juos įdiegti į NKSC turimus SNORT ir SURICATA sensorius.	Taip/Ne *(tikslus aprašymas)*.
1.1.3.	Paslaugos privalo leisti, bent vieną kartą per parą, gauti taisyklių rinkinį turinti ne mažiau kaip 5 naujus parašus.	Taip/Ne *(tikslus aprašymas)*.
1.1.4.	Parašai pateikiami kartu su jų aprašymu.	Taip/Ne
1.1.5.	Parašai turi būti suskirstyti į kategorijas.	Taip/Ne

		(tikslus aprašymas).
1.1.6.	Paslaugų teikimo sąlygos privalo suteikti teisę be papildomo mokesčio gauti parašų pataisymus ir atnaujinimus (naujausias versijas) visą prenumeratos teikimo laikotarpį.	Taip/Ne
1.2.	**Bendrieji reikalavimai:**	
1.2.1.	Prieiga prie įsilaužimo detektavimo sistemos turi būti pateikta oficialiu gamintojo patvirtintu keliu.	Taip/Ne *(tikslus aprašymas)*.
1.2.2.	Pardavėjas turi pateikti nuorodą ar nuorodas į gamintojo interneto puslapį, kuriame yra tiksli pasiūlymą atitinkančių paslaugų techninė specifikacija.	*Pateikti nuorodas į gamintojo interneto puslapį*
1.2.3.	Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie įsilaužimo detektavimo sistemos gamybos arba tobulinimo nutraukimą (pvz., angl. End Of Life Time, End Of Support, arba Discontinued).	*Pateikti gamintojo užtikrinimą.*
2.	**2 pirkimo dalis.** **LIETUVOS ORGANIZACIJŲ KIBERNETINIO SAUGUMO REITINGAVIMO IR INFORMACIJOS APIE APTIKTUS PAŽEIDŽIAMUMUS BEI ŽALINGAS KOMUNIKACIJAS PRENUMERATOS PASLAUGOS, 36 mėn.**	
	Pirkimo objektas – Lietuvos organizacijų (viešojo ir privataus sektoriaus įstaigų, institucijų ir įmonių) (toliau – organizacijos) kibernetinio saugumo reitingavimo ir informacijos apie aptiktus pažeidžiamumus bei žalingas komunikacijas prenumeratos paslaugos (toliau – paslaugos), skirtos NKSC vykdomam potencialių kibernetinių grėsmių atakos vektorių poveikio Lietuvos ryšių infrastruktūrai vertinimui, pažeidžiamų ir užvaldytų įrenginių nustatymui. Paslaugos turi atitikti žemiau pateiktus reikalavimus (perkančiosios organizacijos testuotos ,,BitSight CNI" prenumeratos paslaugos atitinka žemiau pateiktus reikalavimus, todėl siūlydamas šias paslaugas tiekėjas papildomai neįpareigojamas pateikti įrodymų dėl jų atitikties žemiau nustatytiems reikalavimams).	
2.1.	**Paslaugoms keliami reikalavimai:**	
2.1.1.	Skenuoti visą Lietuvos interneto erdvę, rinkdama informaciją apie konkrečiais IP adresais ir prievadais veikiančius servisus, bandydama nustatyti jų versijas, konfigūracijas, pažeidžiamumus.	Taip. Bus skenuojama visa Lietuvos interneto erdvė, rinkdama informaciją apie konkrečiais IP adresais ir prievadais veikiančius servisus, bandydama nustatyti jų versijas, konfigūracijas, pažeidžiamumus. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.2.	Rinkti informaciją apie galimai žalingas komunikacijas, susijusias su užvaldytų įrenginių valdymo infrastruktūra (angl. Command-and-Control, C&C).	Taip

		Bus renkama informacija apie galimai žalingas komunikacijas, susijusias su užvaldytų įrenginių valdymo infrastruktūra (angl. Command-and-Control, C&C). (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.3.	Gebėti pagal tam tikrus požymius priskirti surinktą informaciją konkrečioms Lietuvos organizacijoms (viešojo ir privataus sektoriaus įstaigų, institucijų ir įmonių), jeigu tokie požymiai egzistuoja.	Taip Sistema geba pagal tam tikrus požymius priskirti surinktą informaciją konkrečioms Lietuvos organizacijoms (viešojo ir privataus sektoriaus įstaigų, institucijų ir įmonių), jeigu tokie požymiai egzistuoja. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.4.	Organizacijoms turi būti suteikiami reitingai (balų sistemoje), kuriuos sudarytų viešai pasiekiamų organizacijos resursų kibernetinio saugumo kriterijų visuma: • Žinomi užvaldyti organizacijos įrenginiai; • Žinomi pažeidžiami organizacijos įrenginiai; • Atviri prievadai; • Naudojami SSL/TLS sertifikatai ir jų konfigūracijos; • Organizacijų DNS įrašų nustatymai ir el. pašto viešai prieinama saugumo politika (SPF, DKIM); • Kita surinkta informacija.	Taip Organizacijoms bus suteikiami reitingai (balų sistemoje), kuriuos sudarytų viešai pasiekiamų organizacijos resursų kibernetinio saugumo kriterijų visuma: • Žinomi užvaldyti organizacijos įrenginiai; • Žinomi pažeidžiami organizacijos įrenginiai; • Atviri prievadai; • Naudojami SSL/TLS sertifikatai ir jų konfigūracijos; • Organizacijų DNS įrašų nustatymai ir el. pašto viešai prieinama saugumo politika (SPF, DKIM); • Kita surinkta informacija. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.5.	Turi būti galimybė generuoti organizacijų saugumo vertinimo ataskaitas (PDF formatu), kuriose atsispindėtų visa surinkta informacija apie konkrečią organizaciją, jos kibernetinio saugumo reitingas bei reitingą sudarantys vertinimo veiksniai.	Taip Bus galimybė generuoti organizacijų saugumo vertinimo ataskaitas (PDF formatu), kuriose atsispindėtų visa surinkta informacija apie konkrečią organizaciją, jos

		kibernetinio saugumo reitingas bei reitingą sudarantys vertinimo veiksniai. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.6.	Turi būti galimybė atlikti pažeidžiamų įrenginių Lietuvoje paiešką pagal pažeidžiamumų numerius (angl. Common vulnerabilities and exposures, CVE).	Taip Bus galimybė atlikti pažeidžiamų įrenginių Lietuvoje paiešką pagal pažeidžiamumų numerius (angl. Common vulnerabilities and exposures, CVE). (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.7.	Turi būti galimybė atlikti galimai užvaldytų įrenginių paiešką pagal skirtingų kenkėjiškų programinių kodų požymius.	Taip Bus galimybė atlikti galimai užvaldytų įrenginių paiešką pagal skirtingų kenkėjiškų programinių kodų požymius. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.8.	Turi būti galimybė gauti per pastarąsias 24 valandas naujai sugeneruotų duomenų pagal užvaldytų ir/ar pažeidžiamų įrenginių požymius ataskaitas el. paštu.	Taip Bus galimybė gauti per pastarąsias 24 valandas naujai sugeneruotų duomenų pagal užvaldytų ir/ar pažeidžiamų įrenginių požymius ataskaitas el. paštu. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.9.	Turi būti galimybė redaguoti automatiškai siunčiamų ataskaitų nustatymus.	Taip Bus galimybė redaguoti automatiškai siunčiamų ataskaitų nustatymus. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.10.	Turi būti galimybė vykdyti paiešką duomenų bazėje naudojant aplikacijų programavimo sąsają (API).	Taip Bus galimybė vykdyti paiešką duomenų bazėje naudojant aplikacijų programavimo sąsają (API).

		(siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.11.	Turi būti galimybė realiu laiku gauti duomenis apie naujai nustatytas galimas žalingas komunikacijas, naudojant aplikacijų programavimo sąsają (API).	Taip Bus galimybė realiu laiku gauti duomenis apie naujai nustatytas galimas žalingas komunikacijas, naudojant aplikacijų programavimo sąsają (API). (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.12.	Turi būti galimybė pasirinkti bent 30 Lietuvos organizacijų, kurias galima būtų nuolat stebėti, kaip atskirus vienetus.	Taip Bus galimybė pasirinkti 30 Lietuvos organizacijų, kurias galima būtų nuolat stebėti, kaip atskirus vienetus (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.13.	Turi būti galimybė suteikti teisę stebimos organizacijos atstovui prisijungti ir matyti sistemoje savo organizacijos saugumo vertinimą ir visą aktualią kibernetinio saugumo informaciją.	Taip Bus galimybė suteikti teisę stebimos organizacijos atstovui prisijungti ir matyti sistemoje savo organizacijos saugumo vertinimą ir visą aktualią kibernetinio saugumo informaciją. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.14.	Turi būti galimybė pridėti naujus ir pašalinti esamus sistemos naudotojus.	Taip Bus galimybė pridėti naujus ir pašalinti esamus sistemos naudotojus. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.15.	Turi būti galimybė koreguoti sistemos naudotojų teises.	Taip Bus galimybė koreguoti sistemos naudotojų teises.

		(siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.16.	Visi surinkti duomenys turi būti susisteminti ir pateikti patogiu vartotojui būdu.	Taip Visi surinkti duomenys bus susisteminti ir pateikti patogiu vartotojui būdu. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
2.1.17.	Sistema turi veikti naršyklėje.	Taip Sistema veiks naršyklėje. (siūlome BitSight CNI (Total risk Monitoring for CNI)) prenumeratos paslaugas, todėl papildomų įrodymų nepateikiame).
3.	**3 pirkimo dalis.** **KIBERNETINIŲ GRĖSMIŲ INDIKATORIŲ DUOMENŲ BAZIŲ PRENUMERATOS PASLAUGOS**	
	Pirkimo objektas – Kibernetinių grėsmių indikatorių (angl. Indicators of compromise – IoC) (toliau – Kenksmingi indikatoriai) duomenų bazės prenumeratos paslaugos, 12 mėn. Pirkimo tikslas. Kenksmingų indikatorių duomenų bazės prenumeratos paslaugos (toliau – paslaugos) privalo suteikti galimybę NKSC kibernetinio saugumo specialistams (toliau – specialistai) analizuoti kibernetinę erdvę ir užkardyti ankstesnėje fazėje galimas kenkėjiškas veikas. Siekiamas pirkimo rezultatas. Gaunama atnaujinta informacija apie Kenksmingus indikatorius. Taip pat NKSC specialistai, naudodamiesi teikėjo pateikta prieiga prie dedikuotos platformos (duomenų bazės), gali vykdyti platesnę indikatorių analizę bei naudotis grėsmių žvalgybos profilių (angl. Intelligence cards) teikiama informacija.	
3.1.	**Bendrieji reikalavimai**	
3.1.1.	Prieiga prie kibernetinių grėsmių indikatorių duomenų bazės (analizės platformos) (toliau – platforma) turi būti pateikta gamintojo arba gamintojo įgalioto asmens.	Taip Siūloma Recorded Future Intelligence Platform su moduliais: 1. INT-CAT-A. Integration Category A. 2. SECOPS-1. SecOps Intelligence User License 3. VULN-1. Vulnerability Intelligence User License Prieiga prie kibernetinių grėsmių indikatorių duomenų bazės (analizės platformos) (toliau – platforma) bus pateikta gamintojo,

3.1.2.	Tiekėjas turi pateikti nuorodą ar nuorodas į gamintojo interneto puslapį, kuriame yra tiksli pasiūlymą atitinkančių paslaugų techninė specifikacija arba pateikti gamintojo parengtą paslaugų aprašymą.	*Pateikti nuorodas į gamintojo interneto puslapį.* *Nuoroda: https://www.recordedfuture.com/* *Taip pat pateikiamas dokumentas kartu su pasiūlymu: Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf*
3.1.3.	Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie platformos, prie kurios bus suteikta prieiga, gamybos arba tobulinimo nutraukimą (pvz., angl. end of life time arba Discontinued).	*Pateikiamas gamintojo užtikrinimas kartu su pasiūlymo dokumentais:* *Gamintojo užtikrinimas.pdf*
3.2.	**Paslaugoms keliami reikalavimai**	
3.2.1.	Paslaugos turi apimti:	
3.2.1.1.	prieigos prie automatizuoto kompromitavimo indikatorių (angl. „IOC“) srauto (angl. „feed“) „Connect API“, kuris turi būti integruojamas per API su grėsmių indikatorių analizės platformomis.	Taip Nuoroda: https://api.recordedfuture.com/v2/
3.2.1.2.	prieigos vienam naudotojui prie internetinio portalo (platformos), kurioje būtų galimybė naudotis sistemos modulių „SecOps user license“ ir „Vulnerability intelligence user license“ suteikiamu turiniu.	Taip Bus pateikta prieigos vienam naudotojui prie internetinio portalo (platformos), kurioje būtų galimybė naudotis sistemos modulių „SecOps user license“ ir „Vulnerability intelligence user license“ suteikiamu turiniu. https://www.recordedfuture.com/platform/
3.2.2.	Internetinio portalo funkcionalumas turi susidėti iš:	
3.2.2.1.	grėsmių žvalgybos profilių (kortelių) (angl. Intelligence cards).	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 1 skyriuje
3.2.2.2.	namų vaizdo (angl. Home screen), grėsmių peržiūros srities (angl. Threat views).	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 2 skyriuje
3.2.2.3.	grėsmių žvalgybos tikslų asortimento (angl. Intelligence goal library).	Taip Nuoroda: https://www.recordedfuture.com/solutions/secops-intelligence/
3.2.2.4.	pažangių užklausų sudarymo įrankio (angl. Advanced query builder).	Taip

		Yra realizuojame per paieškos (angl. search) funkcionalumą. Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 2 skyriuje
3.2.2.5.	tinkinamų realaus laiko įspėjimų (angl. Customizable real time alerts).	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 4 skyriuje
3.2.3.	Grėsmių žvalgybos profiliai turi pateikti bent šią informaciją:	Grėsmių žvalgybos profiliai turi šią informaciją:
3.2.3.1.	IP adresus.	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 1 skyriuje
3.2.3.2.	Domain vardus.	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 1 skyriuje
3.2.3.3.	Interneto svetainių adresus.	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 1 skyriuje
3.2.3.4.	Hash duomenis.	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 1 skyriuje
3.2.3.5.	pažeidžiamumų informaciją.	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 1 skyriuje
3.2.3.6.	informaciją apie kenkėjiškas programas.	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 1 skyriuje
3.2.3.7.	Snort/Yara taisyklių informaciją.	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 1 skyriuje
3.2.4.	Paslaugų turinį sudarančios informacijos apie kibernetines grėsmes šaltinis turi apimti internetinių forumų, socialinės medijos, tekstinės informacijos įklijavimo, internetinių pokalbių, informavimo apie kibernetines grėsmes	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 3 skyriuje

	interneto svetainių, taip pat „gilaus interneto“ (angl. „Deep web“) ir „tamsaus interneto“ (angl. „Dark web“) turinį.	
3.2.5.	3.2.4 p. nurodytuose šaltiniuose surinkta informacija turi būti apdorota natūralios kalbos apdorojimo priemonėmis, skirtomis apdoroti tekstą, parašytą bent anglų, arabų, ispanų, prancūzų, kinų, rusų, portugalų, vokiečių ir persų kalbomis. Apdorojimo metu platformoje turi būti numatyta įvykių ir subjektų identifikavimo funkcija, taip pat funkcija, leidžianti turinio minėtomis kalbomis analizavimo metu nustatyti kompromitavimo indikatorius (angl. „IOC“).	Taip Nuoroda: https://www.recordedfuture.com/platform/security-intelligence-graph/
3.2.6.	Automatizuoto kompromitavimo indikatorių informacija turi būti pateikiama su įrodymais, grįstais rizikos įvertinimo įverčiais (angl. risk score).	Taip Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 1 skyriuje
3.2.7.	Duomenys iš sistemos turi būti eksportuojami JSON, CSV, STIX, PPT, PNG, PDF ar Word dokumentų pavidalu.	Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 5 skyriuje
3.2.8.	Platformos naudotojas turi turėti prieigą prie platformoje integruotos smėlio dėžės (angl. Sandbox). Naudotojas turi galėti įkelti įtartinus failus į smėlio dėžę analizei. Analizės ataskaitos turi būti sugeneruojamos ir pateikiamos JSON formatu. Smėlio dėžės apdoroti mėginiai taip pat turi būti automatiškai priskiriami MITRE ATT & CK metodams.	Įrodymai pateikti faile Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 6 skyriuje
3.2.9.	Kiekvienoje smėlio dėžės ataskaitoje turi būti pateikiamas rodiklių rinkinys (domenai, URL, IP ir maišos), kurie turi būti koreliuojami su kita platformoje esančia informacija.	Įrodymai pateikti faile Konfidencialu_Konfidencialu_Gamintojo parengtas paslaugų aprašymas.pdf, 6 skyriuje
3.2.10.	Naudotojo sąsaja turi būti anglų kalba.	Taip, naudotojo sąsaja bus anglų kalba
3.2.11.	Turi būti galimybė srauto (angl. feed) turinį integruoti per API su grėsmių indikatorių analizės platformomis, tokiomis kaip EclecticIQ, MISP, Anomali.	Taip Nuoroda: https://api.recordedfuture.com/v2/
3.2.12.	Paslaugų teikimo metu turi būti užtikrintas gamintojo numatytas standartinis palaikymas (angl. „Support“), apimantis mokymus naudotis paslaugomis ir nuolatinį techninį palaikymą:	Taip Nuoroda: https://www.recordedfuture.com/support-options/
3.2.12.1.	mokymai turi vykti nuotoliniu būdu ir turi įvykti per mėnesį nuo paslaugų teikimo pradžios. Tikslus laikas turi būti suderintas su perkančiąja	Taip

	organizacija. Jie turi supažindinti vieną perkančiosios organizacijos naudotoją su srauto ir platformos veikimo principais ir geriausiomis naudojimo praktikomis, atsižvelgiant į šioje techninėje specifikacijoje norimus pasiekti perkančiosios organizacijos tikslus.	Nuoroda: https://www.recordedfuture.com/recorded-future-university/
3.2.12.2.	techninis palaikymas turi būti teikiamas 24 val. per parą, 7 dienas per savaitę, sudarant galimybę gauti pagalbą platformos naudojimo klausimais iš dedikuotos platformos gamintojo ar teikėjo komandos, reakcijos laikas į užklausą ne ilgiau kaip 3 val. (kai užklausa pateikiama darbo dienomis nuo 8 iki 17 val., penktadieniais iki 15.45 val.), užklausos pateikimo būdas – el. paštu ar naudojantis dedikuota platforma. Turi būti per internetą pasiekiama mokomosios medžiagos, susijusios su platforma, repozitorija.	Taip Nuoroda: https://www.recordedfuture.com/support-options/ Su pasiūlymu taip pat pateikiame: *Konfidencialu_Gamintojo dokumentas_mokymų pristatymas 1.pdf* *Konfidencialu_Gamintojo dokumentas_mokymų pristatymas 2.pdf* *Konfidencialu_Gamintojo dokumentas_mokymų pristatymas 3.pdf*
3.2.13.	Pradėjus teikti paslaugas, perkančiajai organizacijai turi būti pateikti platformos ir srauto administravimo ir vartotojo vadovai anglų kalba skaitmeniniame formate.	Taip, patvirtiname, jog pradėjus teikti paslaugas, perkančiajai organizacijai bus pateikti platformos ir srauto administravimo ir vartotojo vadovai anglų kalba skaitmeniniame formate

*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.

Pardavimų ir verslo vystymo grupės direktorius _____ _____ [redacted]

(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas) (Parašas) (Vardas ir pavardė)