LIETUVOS RESPUBLIKOS APLINKOS MINISTERIJA

RINKOS KONSULTACIJŲ DĖL APLINKOS MINISTERIJOS PAVALDŽIŲ ĮSTAIGŲ, DALYVAUJANČIŲ NACIONALINĖS SOC/CSIRT MODULINĖS SISTEMOS SUKŪRIME, SOC SISTEMŲ KONFIGŪRAVIMO IR PRIEŽIŪROS PASLAUGŲ VIEŠOJO PIRKIMO REZULTATŲ ĮVERTINIMAS

2025 m. spalio 22 d.
Vilnius

Rinkos konsultacijos (kvietimas suteikti rinkos konsultaciją, klausimynas, paslaugų pirkimo techninės specifikacijos ir tiekėjų kvalifikacijos reikalavimų projektai) paskelbti Centrinėje viešųjų pirkimų informacinėje sistemoje: 2025 m. spalio 6 d. rinkos konsultacija Nr. 4841025, trukmė iki 2025 m. spalio 15 d. 14.00 val., ir 2025 m. spalio 15 d. rinkos konsultacija Nr. 4980162, trukmė iki 2025 m. spalio 17 d. 10.00 val.

Eil. Nr.	**Klausimas**	**Dalyvis A**	**Lietuvos Respublikos aplinkos ministerijos – perkančioji organizacija įvertinimas (komentaras)**
1	**2**	**3**	**4**
1.	Ar dalyvautumėte šiame pirkime? Jei ne, nurodykite priežastis kodėl.	Taip, dalyvautume.	
2.	Kokius kvalifikacijos reikalavimus tiekėjams siūlytumėte papildomai nurodyti arba kurių reikalavimų reikėtų atsisakyti? Prašome argumentuoti kodėl.	Manome, kad kvalifikaciniai reikalavimai yra per maži, siūlome juos papildyti bent: 1. Visas reikalaujamas darbo patirtis projektuose/sutartyse prailginti iki 3 metų. Atsižvelgiant į pirkime įtrauktą pavaldžių institucijų kiekį bei jų svarbą 1 metų laikotarpis įgauti reikiamas kompetencijas yra per trumpas. 2. Įtraukiant projektų valdymo specialistą, kuris patvirtintų savo turimą kvalifikaciją Prince2 arba PMP arba CompTIA Project+ sertifikatais arba kitais kvalifikaciją įrodantis lygiaverčiais dokumentais. Atsižvelgiant į pirkimo kompleksiškumą būtina	Atsižvelgta Pirkimo sąlygų 4 priedo lentelės 2.1 punktas.

		koordinuoti diegimo ir priežiūros darbus tarp visų dalyvaujančių įstaigų, užtikrinant veiklų nuoseklumą, terminų laikymąsi ir bendrą projekto valdymą. Projekto valdymo specialisto vaidmuo būtinas siekiant efektyvios komunikacijos, rizikų valdymo ir kokybiško projekto įgyvendinimo visose įstaigose.	
3.	Ar paslaugų pirkimo techninėje specifikacijoje nurodyti reikalavimai yra išdėstyti aiškiai ir be dviprasmybių? Jeigu ne, prašome juos pakoreguoti ir (ar) pasiūlyti savo formuluotę.	Išdėstyta aiškiai.	
4.	Ar turite pastabų / klausimų paslaugų pirkimo techninės specifikacijos projektui? Kokias sąlygas / reikalavimus, susijusius su pirkimo objektu, papildomai siūlytumėte įtraukti į paslaugų pirkimo techninę specifikaciją arba kurių sąlygų / reikalavimų reikėtų atsisakyti? Prašome argumentuoti kodėl.	Prašome patikslinti: ar visa paminėta programinė įranga bus reikalaujama sudiegti visoms išvardintoms organizacijoms.	Atsižvelgta Pirkimo sąlygų 2 priedo 1.3 punkte.
5.	Ar turite kitų pastebėjimų ar pasiūlymų? Prašome nurodyti.	Neturime.	
6.	Ar Jūsų įmonė galėtų suteikti paslaugas visa techninėje specifikacijoje nurodyta apimtimi?	Taip, galėtų.	
7.	Ar Jūsų įmonė atitinka nustatytus kvalifikacijos reikalavimus?	Taip, atitinka.	

	Ar keliami kvalifikacijos reikalavimai yra proporcingi pirkimo objekto atžvilgiu, neperteklinai? Jeigu ne, kurių kvalifikacijos reikalavimų siūlytumėte atsisakyti? Prašome nurodyti ir argumentuoti.		

Eil. Nr.	**Klausimas**	**Dalyvis B**	**Lietuvos Respublikos aplinkos ministerijos – perkančioji organizacija įvertinimas (komentaras)**
1	**2**	**3**	**4**
1.	Ar dalyvautumėte šiame pirkime? Jei ne, nurodykite priežastis kodėl.	Planuojame dalyvauti, jeigu bus galimybė papildyti kvalifikacinį reikalavimą SOC vadovui.	
2.	Kokius kvalifikacijos reikalavimus tiekėjams siūlytumėte papildomai nurodyti arba kurių reikalavimų reikėtų atsisakyti? Prašome argumentuoti kodėl.	Mūsų siūlymai: 1. Nurodytas CASP+ sertifikatas šiuo metu yra pakeistas CompTia SecurityX, tai siūlome papildyti. Taip pat manome, kad šis sertifikatas tiktų labiau ir SOC vadovui, nes jis apima ir daugiau sričių, negu tik pažeidžiamumų vertinimas. Dėl pažeidžiamumų valdymo kvalifikacijos būtų galiam naudoti CEH (Certified Ethical hacker). 2. Siūlome papildyti reikalavimus dėl Tiekėjo profesinės patirties. Mūsų siūlymas nurodyti, kad Tiekėjas turėtų patirties diegiant tokio tipo sprendimus. Taip pat siūlome įtraukti, kad Teikėjas teikdamas ir SOC paslaugas, turėtų patirties dirbant su tokio tipo technologijomis 3. Siūlome papildyti kvalifikacijos reikalavimą „SOC vadovui“ įtraukiant kaip kvalifikaciją pagrindžiančius sertifikatus. Šalia CISSP siūlome	Atsižvelgta iš dalies Pirkimo sąlygų 4 priedo lentelės 2.2 ir 2.4 punktuose.

		įtraukti CompTIA Security+, CompTIA SecurityX, CISM.	
3.	Ar paslaugų pirkimo techninėje specifikacijoje nurodyti reikalavimai yra išdėstyti aiškiai ir be dviprasmybių? Jeigu ne, prašome juos pakoreguoti ir (ar) pasiūlyti savo formuluotę.	Viskas išdėstyta suprantamai.	
4.	Ar turite pastabų / klausimų paslaugų pirkimo techninės specifikacijos projektui? Kokias sąlygas / reikalavimus, susijusius su pirkimo objektu, papildomai siūlytumėte įtraukti į paslaugų pirkimo techninę specifikaciją arba kurių sąlygų / reikalavimų reikėtų atsisakyti? Prašome argumentuoti kodėl.	Ne.	
5.	Ar turite kitų pastebėjimų ar pasiūlymų? Prašome nurodyti.	Ne.	
6.	Ar Jūsų įmonė galėtų suteikti paslaugas visa techninėje specifikacijoje nurodyta apimtimi?	Taip.	
7.	Ar Jūsų įmonė atitinka nustatytus kvalifikacijos reikalavimus? Ar keliami kvalifikacijos reikalavimai yra proporcingi pirkimo objekto atžvilgiu, neperteklinai?	Ne, neturime CISSP. Dėl to prašome papildyti mūsų siūlomais.	

	Jeigu ne, kurių kvalifikacijos reikalavimų siūlytumėte atsisakyti? Prašome nurodyti ir argumentuoti.		

Eil. Nr.	Klausimas	Dalyvis C	Lietuvos Respublikos aplinkos ministerijos – perkančioji organizacija įvertinimas (komentaras)
1	2	3	4
1.	Ar dalyvautumėte šiame pirkime? Jei ne, nurodykite priežastis kodėl.	Taip, jei bus atsižvelgta į žemiau pateiktus argumentus.	
2.	Kokius kvalifikacijos reikalavimus tiekėjams siūlytumėte papildomai nurodyti arba kurių reikalavimų reikėtų atsisakyti? Prašome argumentuoti kodėl.	**Turime pastabų**: 1) Ekspertui Nr. 1 Pažeidžiamumų vertinimo analitikui reikalaujama CompTIA Advanced Security Practitioner (CASP+) sertifikato arba kito lygiaverčio dokumento. **„CompTIA Advanced Security Practitioner“ (CASP+)** – tai aukšto lygio sertifikatas saugumo architektams ir vyresniesiems inžinieriams, patvirtinantis saugių sprendimų valdymo sudėtingose aplinkose patirtį. Tai jau yra sprendimų inžinieriaus ar architekto, o ne vertinimo analitiko sertifikatas. Mūsų ekspertiniu vertinimu, reikalaujamo sertifikato lygis neatitinka pareigybės sudėtingumo, nes CompTIA CASP+ arba kitas lygiavertis dokumentas, (toliau CASP+), yra aukščiausio („expert“) lygmens sertifikatas, skirtas informacijos saugumo architektams ir vyresniesiems inžinieriams, kurie kuria bei projektuoja organizacijų kibernetinio saugumo infrastruktūrą ir politiką. Tuo tarpu SOC pažeidžiamumų vertinimo analitiko veikla yra orientuota į operacinį, techninį darbą –	Atsižvelgta Pirkimo sąlygų 4 priedo lentelės 2.4 punkte.

		pažeidžiamumų identifikavimą, klasifikavimą ir ataskaitų rengimą, o ne strateginį ar architektūrinį saugumo valdymą. Be to, reikalaujama profesinė patirtis rodo vidutinį kompetencijos lygį – pareigybės aprašyme nurodyta, kad pakanka ne mažesnės kaip 1 metų darbo patirties pažeidžiamumų nustatymo ir analizės srityje. Tokia patirtis nėra pakankama CASP+ sertifikato lygiui, kuriam įprastai rekomenduojama 5–10 metų praktinė informacijos saugumo patirtis. Todėl šis reikalavimas akivaizdžiai neatitinka darbo apimties ir kandidatų brandos lygio. Pažeidžiamumų vertinimo analitiko kvalifikaciją adekvačiai patvirtintų Certified Incident Handler, Certified SOC Analyst ar lygiaverčiai sertifikatai, kurie laikomi vidutinio lygio sertifikatais ir labiau atitinkantys praktinį darbo pobūdį. **CASP+ reikalavimas ribotų konkurenciją ir būtų neproporcingas,** kadangi CASP+ yra retas, brangus ir aukšto lygmens sertifikatas, jo reikalavimas vidutinio lygmens pareigybei nepagrįstai apribotų potencialių kandidatų ratą ir pažeistų proporcingumo principą, taikomą kvalifikaciniams reikalavimams. **Atsižvelgiant į pareigybės pobūdį, patirties reikalavimus ir funkcijų turinį, CASP+ sertifikato reikalavimas laikytinas pertekliniu ir neproporcingu. Vietoje jo tikslinga reikalauti vidutinio lygio praktinių saugumo sertifikatų, patvirtinančių gebėjimus vykdyti pažeidžiamumų nustatymo ir analizės veiklas.** 2) Ekspertui Nr. 3 SOC komandos vadovui reikalaujama ISC2 CISSP (Certified Information	

		Systems Security Professional) sertifikato arba kito lygiaverčio dokumento. **Argumentai dėl perteklinio reikalavimo turėti ISC2 CISSP sertifikatą SOC komandos vadovui.** CISSP sertifikato arba kito lygiaverčio dokumento (toliau CISSP) paskirtis – strateginis, o ne operacinis valdymas. CISSP (Certified Information Systems Security Professional) yra aukščiausio („expert / managerial“) lygmens sertifikatas, skirtas informacijos saugumo strateginiam valdymui, politikų kūrimui ir rizikos valdymui visos organizacijos mastu. Tuo tarpu SOC komandos vadovas vadovauja operacinei, techninei komandai, kuri realiu laiku stebi, identifikuoja ir reaguoja į kibernetinius incidentus. Šioje veikloje svarbiausios ne strateginės, o praktinės incidentų valdymo, koordinavimo ir techninės analizės kompetencijos. Be to, reikalaujama darbo patirtis rodo vidutinį vadovavimo lygį. Aprašyme nurodyta, kad užtenka 1 metų vadovavimo SOC komandai patirties. CISSP paprastai reikalauja mažiausiai 5 metų praktinės patirties iš dviejų ar daugiau saugumo sričių. **Taigi, reikalavimas turėti CISSP neatitinka realios patirties lygio ir dirbtinai pakelia kvalifikacijos kartelę.** Yra kiti sertifikatai, tinkamiau atitinkantys SOC vadovo kompetencijas. SOC komandos vadovui tikslingiau turėti techninio valdymo ir incidentų valdymo srities sertifikatus, pavyzdžiui:	

		EC-Council Certified SOC Analyst (CSA) arba Certified Incident Handler (ECIH) – incidentų analizės ir reagavimo valdymui; GIAC Certified Incident Handler (GCIH) arba GIAC Security Operations Manager (GSOM) – SOC vadovų kvalifikacijai; CompTIA CySA+ – pažangesnė analizė ir grėsmių valdymas; Šie sertifikatai tiesiogiai atitinka SOC vadovo atsakomybes, todėl yra proporcingi ir tikslingi. **CISSP perteklinis reikalavimas ribotų konkurenciją:** a) smarkiai sumažina kvalifikuotų kandidatų ratą, b) neproporcingai pakelia kvalifikacijos kartelę, c) nėra pagrįstas darbo funkcijų turiniu. Pagal proporcingumo principą, taikomą kvalifikaciniams reikalavimams viešuosiuose pirkimuose, šis sertifikatas laikytinas neatitinkančiu darbo funkcijų sudėtingumo. Taip pat, CISSP orientuotas į informacijos saugumo valdymo sistemų kūrimą, o ne į SOC operacijas. SOC vadovo atsakomybės – incidentų reagavimas, komandos darbo koordinavimas, įvykių eskalacija, grėsmių analizė, procesų optimizavimas. CISSP akcentuoja: politikų kūrimą, teisinį atitikties užtikrinimą, informacijos saugumo architektūrą, verslo tęstinumo planavimą. Tai skirtingi kompetencijų lygmenys. SOC vadovui svarbesni operacinio valdymo įgūdžiai, o ne strateginės informacijos saugumo valdymo žinios. **Atsižvelgiant į pareigybės pobūdį, reikalaujamą patirtį ir atsakomybes, CISSP sertifikato reikalavimas laikytinas pertekliniu,**	

		neproporcingu ir neatitinkančiu realių SOC vadovo funkcijų. Vietoje CISSP tikslinga taikyti operacinio ir techninio saugumo vadovo lygmens sertifikatus, tokius kaip ECIH, GCIH, CySA+. **Papildomai pažymime, kas Perkančiosios organizacijos nustatyti kandidatų ar dalyvių kvalifikacijos reikalavimai negali dirbtinai riboti konkurencijos, turi būti proporcingi ir susiję su pirkimo objektu, tikslūs ir aiškūs:** https://klausk.vpt.lt/hc/lt/articles/360016398980-47-straipsnis-Tiekėjo-kvalifikacijos-tikrinimas	
3.	Ar paslaugų pirkimo techninėje specifikacijoje nurodyti reikalavimai yra išdėstyti aiškiai ir be dviprasmybių? Jeigu ne, prašome juos pakoreguoti ir (ar) pasiūlyti savo formuluotę.	Žiūrėti punktą 4.	
4.	Ar turite pastabų / klausimų paslaugų pirkimo techninės specifikacijos projektui? Kokias sąlygas / reikalavimus, susijusius su pirkimo objektu, papildomai siūlytumėte įtraukti į paslaugų pirkimo techninę specifikaciją arba kurių sąlygų / reikalavimų reikėtų atsisakyti? Prašome argumentuoti kodėl.	Kai kurios pirkimo sąlygos nėra aiškios ir dviprasmiškos, todėl riboja galimybę pateikti tinkamą pasiūlymą: 1. Pirkimo dokumentų punktas: 1.2. Užsakovo SOC įrankių diegimo, jų priežiūros ir SOC paslaugos neturi apimti SIEM, nes Aplinkos ministerija naudoja kitą SIEM sprendimą. Pirkimo dokumentuose būtina įvardinti turimą SIEM sprendimą, jo komplektaciją, diegimo ir naudojimo būseną, kad būtų galima tinkamai įvertinti likusią sprendimo dalį. 2. Nors 1.2 punkte sakoma, kad SOC paslaugos neturi apimti SIEM, tačiau 4. punkte vardinami	1. Atsižvelgta Pakoreguotas Pirkimo sąlygų 2 priedo „Techninė specifikacija“ 1.3 punktas. Atsižvelgta 2. Pakoreguotas Pirkimo sąlygų 2 priedo „Techninė specifikacija“ visas 4.1 SIEM sistemos diegimas poskyris. 3. Atsižvelgta Pakoreguotas Pirkimo sąlygų 2 priedo „Techninė specifikacija“ 4.1.2.1 punktas. 4. Atsižvelgta Pakoreguotas Pirkimo sąlygų 2 priedo „Techninė specifikacija“ 4.2.1.1 punktas.

		reikalavimai SIEM diegimui ir paruošimui naudojimui. Punktai prieštarauja vienas kitam ir iki galo neaiškus SIEM įtraukimas į pirkimo paslaugų apimtį. 3. Punktas 4.1.2.1. Pateikti SIEM agentai ir/arba kita lygiavertė žurnalinių įrašų surinkimo programinė įranga bei jos diegimo instrukcijos. Neaišku: - Kas turėtų pateikti minėtus agentus. - Reikėtų apibrėžti, kokių tipų žurnalus (sistemos, autentifikacijos, tinklo įvykiai ir pan.) turi tvarkyti agentas, kokiu dažnumu siųsti duomenis, ir ar turi palaikyti šifravimą. 4. Punktas 4.2.1.1. NIDS diegimas, vadovaujantis NKSC pateikta dokumentacija. Reikėtų patikslinimo, kokia yra specifinė NKSC dokumentacija dėl NIDS. 5. Punktas 5.2.2. Išorinių kibernetinių grėsmių indikatorių ir taisyklių tvarkymas (kenksmingi IP, domenai, URL ir kt.): pridėjimas, modifikavimas, pašalinimas (iki 5 vnt. per mėnesį). Reikėtų patikslinimo, ar 10 % ir 5 % įrašų šaltinių limitai taikomi pagal faktinį mėnesio vidurkį ar bendrą sistemų skaičių? Kaip tai vertinama dinamiškose aplinkose, kur žurnaliniai įrašai centralizuojami per ELK (Beats/Logstash+Elasticsearch), įskaitant tiek automatizuotus, tiek rankinius pakeitimus?	5. Patikslinimas Netinkamai interpretuojamas reikalavimas. Kalba eina ne apie NIDS funkcijų tvarkymą, o apie naujos informacijos, teikiamos iš išorės, įtraukimą pvz.: naujos fišingo kampanijos kompromitacijos indikatoriai (IoC). 6. Patikslinimas Apžvalginių susitikimų dėl SOC paslaugų metu, aptariant praėjusio etapo grėsmes, jų pasikartojimo dažnumo pokyčius arba kitokias tendencijas, gali atsirasti poreikis gauti detalesnę informacija apie tai. Pati palankiausia forma tokiai informacija gauti yra ataskaitos. Šis reikalavimas būtent apie tai. 7. Atsižvelgta Pakoreguotas Pirkimo sąlygų 2 priedo „Techninė specifikacija“ 3.4 (pataisytas į 7.4) punktas. 8. Atsižvelgta Pakoreguotas Pirkimo sąlygų 2 priedas „Techninė specifikacija“ papildytas 5.3 punktu. 9. Patikslinimas Šie punktai bus apibrėžti sutartyje.

		6. Punktas 5.2.6. Ataskaitų ir suvestinių kūrimas pagal saugumo analitikų siūlymus ir Užsakovo arba konkretaus Paslaugų gavėjo poreikį (iki 5 vnt. per mėnesį). Reikia patikslinimo, kokios ataskaitos ir suvestinės turimos galvoje, koks jų tikslas ir reikalavimai joms. 7. Punktas 3.4. Vykdant SOC paslaugas vadovaujamasi šiais paslaugos teikimo parametrais (lentelė). SOC paslaugų vertinimo parametrai paprastai yra šie: - Galimo incidento aptikimo laikas – kai pranešimas apie incidentą pastebimas ir priskiriamas analitikui; - Pirmo atsako į incidentą laikas – per kurį vykdomas pirmas atsakas, t. y. sustabdomas incidento žalos plitimas. Incidentų išsprendimo laikas nėra matuojamas SLA, nes jis individualiai priklauso nuo incidento paplitimo ir padarytos žalos. Lentelėje nurodomas išsprendimo laikas 8 valandos neracionalus, nes ne visais atvejais įmanomas incidento išsprendimas per tokį trumpą laiką, ypač, jei reikalingas trečiųjų šalių įsikišimas, kaip teisminė ekspertizė. 8. Nėra detalesnių reikalavimų pažeidžiamumų skenavimui ir rezultatų pateikimui.	

		9. Kadangi tai yra sektorinio SOC pirkimas, trūksta informacijos apie: - Paslaugų gavėjų duomenų valdymą ir apsaugą, - Tenantų atskyrima/neatskyrimą; - Atsakomybių pasiskirstymą tarp Tiekėjo, Užsakovo ir Paslaugų gavėjų.	
5.	Ar turite kitų pastebėjimų ar pasiūlymų? Prašome nurodyti.	–	
6.	Ar Jūsų įmonė galėtų suteikti paslaugas visa techninėje specifikacijoje nurodyta apimtimi?	Taip.	
7.	Ar Jūsų įmonė atitinka nustatytus kvalifikacijos reikalavimus? Ar keliami kvalifikacijos reikalavimai yra proporcingi pirkimo objekto atžvilgiu, neperteklinai? Jeigu ne, kurių kvalifikacijos reikalavimų siūlytumėte atsisakyti? Prašome nurodyti ir argumentuoti.	Mūsų įmonė atitinka dalį iš Perkančiosios organizacijos kvalifikacijos reikalavimų projekte pateiktų reikalavimų. Mūsų įmonės pastabos, siūlymai ir argumentai yra pateikti šio klausimyno 2-o punkte.	