SAUGUMO ĮVYKIŲ STEBĖJIMO IR VALDYMO INFORMACINĖS SISTEMOS *PIRKIMAS*

2025-04-10

Suinteresuotiems dalyviams

Siunčiama CVP IS priemonėmis

PIRKIMO SĄLYGŲ PAAIŠKINIMAS NR.2

Energy cells, UAB (toliau – Perkantysis subjektas) Saugumo įvykių stebėjimo ir valdymo informacinės sistemos (SIEM) pirkime (toliau – Pirkimas) CVP IS priemonės gavo Tiekėjų klausimų dėl Pirkimo dokumentų paaiškinimo/patikslinimo.
Pateikiami Perkančiojo subjekto atsakymai:

Eil.Nr.	***Tiekėjo klausimas***	***Perkančiojo subjekto atsakymas***
1.	*2025-04-09 Siųstame dokumente patvirtinate, kad "Patvirtiname, kad pagal SPS Priedą Nr. 2, visa paslaugų teikimui reikalinga programinė įranga turi būti įrengta Pirkėjo debesų aplinkoje."* *Prašome patikslinti, ar Pirkėjo debesijos aplinka yra viešasis debesis (pvz., „Microsoft Azure"), ar duomenų centras Lietuvoje?*	Atsakydami į klausimą informuojame, kad Pirkėjo debesijos infrastruktūra, kurioje turi būti įdiegta programinė įranga, nėra lokalus duomenų centras Lietuvoje. Pirkėjas naudoja viešąją „Microsoft" debesijos platformą („Microsoft Azure"), kurios paslaugos yra teikiamos Europos Sąjungos šalyse veikiančiuose duomenų centruose. Todėl tiekėjas, diegiantis SIEM sprendimą, privalo užtikrinti, kad jo siūloma programinė įranga būtų suderinama su Microsoft Azure debesijos infrastruktūra ir būtų diegiama bei konfigūruojama šioje aplinkoje.
2.	*Šio konkurso pirkimo objektas yra „Saugumo įvykių stebėjimo ir valdymo informacinė sistema" (toliau SIEM), tačiau SPS 2 Priedo „TECHNINĖ SPECIFIKACIJA" II dalyje prievolių vykdymo reikalavimuose yra keliami privalomi reikalavimai su pirkimo objektu nesusijusioms sistemos:*	Informuojame, kad šiuo pirkimu nėra perkamos atskiros papildomos programinės įrangos ar licencijos antivirusinei apsaugai, el. pašto sistemoms ar atakos perimetro/rizikų valdymui. Techninės specifikacijos reikalavimuose išvardintas funkcionalumas yra laikomas SIEM sprendimo dalimi – tiekėjas turi pasiūlyti SIEM sprendimą, kuris gebėtų

	Antivirusinei sistemai: ***Reikalavimai baziniam darbo vietų ir tarnybinių stočių antivirusinės apsaugos funkcionalumui, apimančiam visas** Pirkėjo **darbo vietas ir tarnybines stotis*** *El. pašto apsaugos sistemai:* ***Reikalavimai Office 365 aplinkos (Exchange, One Drive, Sharepoint, Teams) skenavimo ir apsaugos funkcionalumui*** *Atakos perimetro valdymui:* ***Reikalavimai atakos perimetro valdymo bei organizacijos rizikų vertinimo (ASM) funkcionalumui*** *Prašau paaiškinkite, ar šie reikalavimai yra taikomi šiam pirkimo objektui?*	užtikrinti šių sričių stebėseną, koreliavimą ir analizę, pavyzdžiui: • per integracijas su Pirkėjo naudojamomis sistemomis (pvz., Microsoft Defender, Office 365, Azure), • ar per kitus standartinius ryšio metodus ir API, įgalinančius duomenų gavimą bei grėsmių koreliaciją. Pirkėjas šiuo metu jau naudoja: • Microsoft Defender saugos sprendimą, • Microsoft 365 paketą, įskaitant Exchange, OneDrive, SharePoint ir Teams. Rizikos vertinimas, atakos perimetro stebėsena, naudotojų paskyrų analizė ir kita su saugumo įvykių vertinimu susijusi informacija turi būti integruojama bei apdorojama SIEM sprendime, laikant tai funkcionalumo dalimi, o ne atskiru programiniu komponentu. Todėl visi išvardinti reikalavimai yra taikomi pirkimo objektui – SIEM sprendimui – ir turi būti realizuoti SIEM sistemos funkcionalumo ribose.

Pasiūlymų pateikimo terminas pratęsiamas 1 darbo dienai. Pasiūlymus pateikti ne vėliau kaip iki **2025-04-15 15:00 val** CVP IS susirašinėjimo priemonėmis.

Pirkimų komisija