SAUGUMO ĮVYKIŲ STEBĖJIMO IR VALDYMO INFORMACINĖS SISTEMOS *PIRKIMAS*

2025-04-09

Suinteresuotiems dalyviams

Siunčiama CVP IS priemonėmis

PIRKIMO SĄLYGŲ PAAIŠKINIMAS NR.1

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

Eil.Nr.	***Tiekėjo klausimas***	***Perkančiojo subjekto atsakymas***
1.	Kvalifikacinių reikalavimų 1 lentelės 3 punktas, stulpeliuose „Tiekėjo pašalinimo pagrindai" ir „Pateikiami dokumentai" nurodyti sertifikatai nesutampa, kuriuos turime naudoti?	Pirkimo dokumentų specialiųjų pirkimo sąlygų 3p. **TIEKĖJŲ PAŠALINIMO PAGRINDAI IR KVALIFIKACIJOS REIKALAVIMAI** 1 lentelės 3 punkto reikalavimas nenumato tiekėjams pateikti sertifikatus ar kitus dokumentus Pirkime, *„su pasiūlymu pateikiamas tik EBVPD. Iš Lietuvoje įsteigtų subjektų kitų dokumentų pagal šį punktą nebus reikalaujama."*
2.	Pirkimo dokumentų SPS Priedas Nr.2 nurodyta: Licencija gali būti teikiama tik programinė, kuri turi užtikrinti: | Nuolatinį žurnalų įrašų (anglų k. logs) surinkimą / koreliavimą, turi būti pritaikyta surinkti ir apdoroti ne mažiau kaip 5 000 įvykių / įrašų per sekundę (angl. EPS – Events Per Second) su galimybe padidinti surenkamų ir apdorojamų įvykių skaičių iki 10 000 įvykių / įrašų skaičių per sekundę. Integruojamos tinklo įrangos vienetų skaičius ir įvykių surinkimo agentų skaičius neturi būti ribojamas.	Perkantysis subjektas patikslina Pirkimo informaciją: 1. Stebimų įrenginių tipai ir skaičius (2025-03-01 dienai)

<table>
<tr>
<td></td>
<td>Skirtingi gamintojai skirtingai licencijuoja saugumo įvykių stebėjimo ir valdymo informacinių sistemų programinę įrangą. Vieni taiko licencijavimą įvykiams/įrašams per sekundę (angl. EPS – Events Per Second), kiti gamintojai taiko licencijavimą pagal stebimus įrenginius ir sistemas (jų kiekį). Prašome nurodyti stebimų įrenginių/sistemų tipus ir kiekius.</td>
<td>
<table>
<tr><th>Įrenginių tipas</th><th>Operacinė sistema</th><th>Kiekis (suminis, visose vietose)</th></tr>
<tr><td>Cisco maršrutizatoriai / ugniasienės (RTR, FWR)</td><td>Cisco IOS</td><td>9</td></tr>
<tr><td>Tarnybinės stotys / serveriai (DAS, EAC, DSS)</td><td>Windows Server / Linux x86</td><td>12</td></tr>
<tr><td>Kontroleriai (OCTE, MBMU, SMBU, Banana Pi)</td><td>Linux ARM</td><td>182</td></tr>
<tr><td>RTAC, PEI, UPS, PDU, CONS</td><td>Įvairios (Linux/FortiOS)</td><td>50+</td></tr>
<tr><td>Apsaugos sprendimai (galima FortiGate, kt.)</td><td>FortiOS</td><td>2 (numatomi)</td></tr>
</table>
Bendras įrenginių skaičius, kurie generuoja žurnalinius įrašus (log): apie 250.
2. Operacinės sistemos. Cisco IOS, Windows Server, Linux x86, Linux ARM, FortiOS.
3. Pastaba dėl skaičiavimo metodo. Atkreipiame dėmesį, kad skaičiuojant licencijavimo poreikį pagal įrenginių ar šaltinių skaičių (device/source-based licensing), galimi netikslumai dėl apkrovos dinamikos – įrenginiai skirtingai generuoja žurnalinius įrašus priklausomai nuo jų veiklos intensyvumo, įvykių kiekio bei įdiegto funkcionalumo.
</td>
</tr>
<tr>
<td>3.</td>
<td>Pirkimo dokumentų SPS Priedas Nr.2 nurodyta:</td>
<td>Perkantysis subjektas vertina tiekėja pastabą, tačiau techninės specifikacijos reikalavimas dėl programinės įrangos tiekimo originalioje gamintojo pakuotėje išlieka galiojantis.</td>
</tr>
</table>

	<table><tr><td colspan="3">Licencijos teikimui reikalingos programinė įrangos charakteristikos:</td></tr><tr><td></td><td>Tiekėjo suteikiama programinė įranga privalo būti nenaudota, pateikiama originalioje gamintojo pakuotėje; gamykliškai atnaujinti (angl. Refurbished) – neleistini</td><td>Atitinka reikalavimus</td></tr></table> Atkreiptinas dėmesys, kad daugelis įmonių taiko aplinkosauginius pricipus, kuriais siekia mažina pakuočių kiekius.	
4.	Pirkimo dokumentų SPS Priedas Nr.2 nurodyta: <table><tr><td></td><td>Visą Paslaugų teikimui reikalingą programinė įranga turi būti įrengta Pirkėjo debesų aplinkoje.</td><td>Atitinka reikalavimus</td></tr><tr><td></td><td>Prieiga prie programinės įrangos</td><td>Prie Paslaugų teikimui reikalingos programinės įrangos Tiekėjas jungiasi saugiu komunikacijos kanalu nuotoliniu būdu, patvirtintu Pirkėjo prieigos taisyklėse. Visa Paslaugų teikimui reikalinga kaupiama informacija (žurnaliniai įrašai, duomenų srauto įrašai ir kt.) yra laikoma Pirkėjo tinkle arba Tiekėjo infrastruktūroje. Paslaugų teikimui turi būti naudojama Tiekėjo debesijos infrastruktūra, esanti Europos sąjungos šalyse. Jei Tiekėjas Paslaugų teikimui naudos Pirkėjo debesijos paslaugas ar Pirkėjo debesijos paslaugų komponentus, tai visus papildomus kaštus (mokesčiai už resursus, duomenų perdavimą ir pan.) atsirandančius dėl šių komponentų naudojimo prisiima Tiekėjas</td></tr></table> Aukščiau nurodyti punktai prieštarauja vienas kitam (viename nurodama, kad turi būti įdiegta Pirkėjo debesų aplinkoje - kitame, kad Tiekėjo infrastruktūroje).	Patvirtiname, kad pagal SPS Priedą Nr. 2, visa paslaugų teikimui reikalinga programinė įranga turi būti įrengta Pirkėjo debesų aplinkoje. Tuo pačiu atkreipiame dėmesį, kad jeigu programinės įrangos veikimui ar palaikymui užtikrinti reikės papildomų tiekėjo paslaugų, susijusių su tam tikrų komponentų veikimu ar jų paruošimu, tokioms paslaugoms reikalingi skaičiavimo ar saugojimo ištekliai turi būti teikiami iš tiekėjo infrastruktūros, kuri, kaip nurodyta reikalavimuose, turi būti įsikūrusi Europos Sąjungos teritorijoje. Šis sprendimas leidžia užtikrinti optimalų paslaugų veikimą ir atitiktį informacijos saugumo bei duomenų apsaugos reikalavimams.
5.	Pirkimo dokumentų SPS Priedas Nr.2 nurodyta:	**Atsakymas į klausimą Nr. 5 -7** Pirkėjo debesijos infrastruktūros, reikalingos SIEM programinei įrangai, palaikymas (atnaujinimai, saugos pataisos, techninė priežiūra ir kt.)

	<table><tr><td></td><td>Prieiga prie programinės įrangos</td><td>Prie Paslaugų teikimui reikalingos programinės įrangos Tiekėjas jungiasi saugiu komunikacijos kanalu nuotoliniu būdu, patvirtintu Pirkėjo prieigos taisyklėse. Visa Paslaugų teikimui reikalinga kaupiama informacija (žurnaliniai įrašai, duomenų srauto įrašai ir kt.) yra laikoma Pirkėjo tinkle arba Tiekėjo infrastruktūroje. Paslaugų teikimui turi būti naudojama Tiekėjo debesijos infrastruktūra, esanti Europos sąjungos šalyse. Jei Tiekėjas Paslaugų teikimui naudos Pirkėjo debesijos paslaugas ar Pirkėjo debesijos paslaugų komponentus, tai visus papildomus kaštus (mokesčiai už resursus, duomenų perdavimą ir pan.) atsirandančius dėl šių komponentų naudojimo prisiima Tiekėjas</td></tr></table> Prašome nurodyti, kas bus atsakingas už Pirkėjo debesijos infrastruktūros parengimą, sukonfigūravimą, SIEM programinės įrangos diegimą.	Sutarties metu nėra tiekėjo atsakomybė, išskyrus tą dalį, kuri tiesiogiai susijusi su SIEM diegimu ir konfigūravimu diegimo laikotarpiu, t. y. iki antrojo etapo priėmimo–perdavimo akto pasirašymo. Tiekėjas yra atsakingas už: SIEM programinės įrangos diegimą ir veikimą iki perdavimo; visų prijungimų, konfigūracijų, licencijų ir prieigos duomenų perdavimą Pirkėjui, kad šis galėtų savarankiškai eksploatuoti sprendimą. Po perdavimo akto pasirašymo, debesijos infrastruktūros palaikymą ir administravimą atlieka Pirkėjas arba jo pasirinktas paslaugų teikėjas.
6.	Prašome nurodyti, kas bus atsakingas už Pirkėjo debesijos infrastruktūros, reikalingos SIEM programinei įrangai palaikymą (atnaujinimai, saugos pataisos ir kt. darbai.) sutarties metu.	
7.	Pirkimo dokumentų SPS Priedas Nr.2 nurodyta: <table><tr><td></td><td>Garantiniai įsipareigojimai</td><td>Gamintojo garantuojamas visos programinės įrangos garantinis aptarnavimas nuo Paslaugos (antrojo etapo) priėmimo–perdavimo akto pasirašymo. Nemokamas programinės įrangos palaikymas (klaidų taisymas bei jų ataskaitų gavimas bei naujesnės programinės įrangos versijų diegimas), teisė kreiptis į gamintoją iškilus problemai Sutarties galiojimo laikotarpiu.</td></tr></table> Prašome nurodyti, kas bus atsakingas už SIEM programinės įrangos palaikymą (atnaujinimai, saugos pataisos, konfigūracijos eskalacijos ir kiti veikimo i darbai.) sutarties metu.	
8.	Pirkimo dokumentų SPS Priedas Nr.2 nurodyta:	Pirkimo dokumentuose nėra reikalaujama teikti SOC (Security Operations Center) paslaugos ar žmogiškųjų resursų, vykdančių paieškas tamsiajame internete (Dark Web). Techninės specifikacijos reikalavimu siekiama užtikrinti, kad siūlomas sprendimas turėtų funkcionalumą, leidžiantį identifikuoti galimus naudotojų paskyrų kompromitavimo požymius – tai gali būti įgyvendinta pasitelkiant automatizuotas grėsmių žvalgybos (angl. threat intelligence) sistemas,

	Turi būti pateikiamas ir nuolatos atnaujinami organizacijos, vartotojų, galinių įrenginių, debesijos aplikacijų rizikos laipsniai, turi būti vertinami ne mažiau kaip šie parametrai: • pažeidžiamumų aptikimas, • galimą vartotojų paskyrų kompromitavimas, turi gebėti aptikti vartotojų paskyrų duomenų nutekėjimą tamsiajame internete (Darkweb). • anomalijų aptikimas, pagal neįprastą vartotojų elgseną, • incidentų aptikimas galiniuose įrenginiuose, • netinkamos saugumo konfigūracijos atvejai - dviejų faktorių autentifikacijos (MFA) nebuvimas, silpni slaptažodžiai ar silpna slaptažodžių politika. Atkreiptinas dėmesys, kad galimą vartotojų paskyrų duomenų paiešką tamsiajame internete atlieka fiziškai SOC veiklą vykdantys žmonės su atitinkamomis kompetencijomis ir turintys prieigas į specializuotas DarkWeb duombazes. Atskiru atveju yra naudojami trečių šalių programiniai paketų įrankiai, turintys ribotą funkcionalumą. Prašome panaikinti reikalavimą arba detaliau aprašyti reikiamą funkcionalumą.	Privalomas	naudotojų elgsenos analizės (UBA) mechanizmus ar kitus integruotus komponentus. Prašomas funkcionalumas: nėra prilyginamas SOC veiklai ar specifinių Dark Web analitikų darbui; gali būti realizuotas techninėmis priemonėmis, kurios leidžia aptikti naudotojo paskyros duomenų patekimo požymius į viešai prieinamas ar neteisėtas informacijos erdves (pvz., duomenų nutekėjimo indikatoriai, slaptažodžių tikrinimas, įtartinų prisijungimų elgsena ir kt.). Todėl reikalavimas išlieka galioti – tiekėjas turi pasiūlyti sprendimą, turintį komponentą, gebantį įvertinti galimą naudotojų paskyrų kompromitavimą, tačiau jo įgyvendinimo būdas gali būti lankstus.

Pirkimo komisija