VALSTYBĖS ĮMONĖS
IGNALINOS ATOMINĖS ELEKTRINĖS
FIZINĖS SAUGOS SKYRIUS

TVIRTINU
Generalinis direktorius

Linas Baužys

SAUGUMO OPERACIJŲ CENTRO PASLAUGOS PIRKIMO TECHNINĖ SPECIFIKACIJA

2026 m. gegužės 4 d. Nr. <Reg. Nr.>
Visaginas

I SKYRIUS
PIRKIMO TIPAS

1. Paslaugos pirkimas.

II SKYRIUS
TIKSLAS

2. Perkama Saugumo operacijų centro (angl. SOC – Security Operations Center) paslauga (toliau – Paslauga, SOC) užtikrins nenutrūkstamą kibernetinių grėsmių aptikimą VĮ Ignalinos atominės elektrinės (toliau – IAE, Užsakovas) informacinių technologijų (toliau - IT) infrastruktūroje, padėti efektyviai ir greitai užtikrinti kibernetinių incidentų valdymą.

III SKYRIUS
PASLAUGOS APRAŠYMAS IR TEIKIMO APIMTIS

3. Perkamos paslaugos aprašymas:

3.1. Teikiant Paslaugą, Paslaugos teikėjo (toliau – Teikėjas) specialistai (analitikai, incidentų tyrėjai, grėsmių medžiotojai ir kt.), naudojant savo techninę ir programinę įrangą, kuri diegiama Užsakovo informacinėje infrastruktūroje, 24 (dvidešimt keturias) valandas per parą 7 (septynias) dienas per savaitę stebi Užsakovo IT infrastruktūroje generuojamus saugos įvykius ir pranešimus, kompiuterių tinklo duomenų srautus. Nepertraukiamai, visą parą, darbo ir nedarbo dienomis ir valandomis, Teikėjo specialistai atlieka gautos informacijos analizę, identifikuoja galimus kibernetinius incidentus ir grėsmes, įvertina jų poveikį. Apie juos numatytais terminais informuoja Užsakovą, konsultuoja dėl galimų saugos incidentų valdymo bei keliamų rizikų sumažinimo. Taip pat, pagal su Užsakovu suderintą planą, vykdo Užsakovo IT infrastruktūros saugos spragų paiešką bei teikia pasiūlymus ir rekomendacijas jų šalinimui.

Paslaugų teikėjas turi užtikrinti, kad dirbančių analitikų skaičius ir kompetencija būtų pakankama išvardintoms funkcijoms atlikti.

3.2. Ne vėliau kaip per 10 (dešimt) darbo dienų nuo sutarties įsigaliojimo Teikėjas turi parengti bei suderinti elektroniniu paštu su Užsakovu komunikacijos bei incidentų valdymo planą, apimantį:

- Teikėjo ir Užsakovo atstovų, atsakingų už informacijos apsikeitimą, kontaktus;
- Teikėjo ir Užsakovo atstovų, atsakingų už techninių ir programinių priemonių diegimą ir priežiūrą, kontaktus;
- ryšio kanalų, Paslaugos pajungimo ir veikimo aprašymus, komunikacijos veiksmus Paslaugos sutrikimo atveju;
- procesą, aprašantį komunikacijos veiksmus galimo incidento atveju;
- procesą, aprašantį informavimą apie aptiktus kibernetinius incidentus bei jų suvaldymą.

4. Paslaugos apimtys:

4.1. Teikėjas pateikia ir įdiegia Užsakovo infrastruktūroje visą paslaugos teikimui būtiną techninę ir programinę įrangą (toliau – TPĮ) (TPĮ turi atitikti šios techninės specifikacijos 4.1.1 p. reikalavimus). TPĮ diegimas Užsakovo informacinėje infrastruktūroje turi būti atliktas ne vėliau nei per 90 (devyniasdešimt) kalendorinių dienų nuo sutarties įsigaliojimo. Prie Užsakovo informacinėje infrastruktūroje įdiegtos TPĮ Teikėjas jungiasi saugiu šifruotu VPN komunikacijos kanalu nuotoliniu būdu.

4.1.1. Teikėjo naudojama TPĮ turi:

- būti pritaikyta montavimui į 19“ montažinėje spintoje;
- būti pritaikyta dirbti užsakovo 10/100/1000Mb/10 Gb tinklo infrastruktūroje;
- turėti visus pajungimui reikalingas priemones (kabelius, keitiklius, jungtis ir pan.);
- turėti pakankamai resursų ir vietos vidinėje duomenų saugykloje užtikrinti žurnalinių įrašų, saugos įvykių, tinklo srauto (angl. *Netflow*) saugojimą ne mažiau 90 (devyniasdešimt) kalendorinių dienų ir galimybę, esant poreikiui saugyklą praplėsti;
- užtikrinti aukštą sistemos prieinamumą (angl. *High availability*);
- būti pritaikyta surinkti ir apdoroti ne mažiau kaip 5000 (penkis tūkstančius) įvykių per sekundę (angl. EPS – Events Per Second) su galimybe padidinti surenkamų ir apdorojamų įvykių skaičių iki 10 000 (dešimt tūkstančių) įvykių / įrašų skaičių per sekundę ir ne mažiau kaip 30000 (trisdešimt tūkstančių) tinklo srauto statistikos įrašų per minutę (angl. FPM – Flows Per Minute);
- neriboti integruojamos Užsakovo tinklo įrangos vienetų ir įvykių surinkimo agentų skaičiaus;
- jeigu programinė įranga bus licencijuojama tik per serverių skaičių ir tai yra vienintelis jos licencijos apribojimas, programinės įrangos licencija turi leisti apdoroti ne mažiau kaip 70 (septyniasdešimt) serverių;
- neriboti įvykių per sekundę (angl. *Events Per Second - EPS*), tinklo, kompiuterinių darbo vietų ir kitų įrenginių kiekius.

4.2. Paslaugą sudaro:

4.2.1. Nuolatinis Užsakovo IT įrangos žurnalinių įrašų, tinklo srauto anomalijų surinkimas bei jų koreliavimas centralizuotoje Teikėjo Saugumo stebėsenos ir reagavimo į incidentus platformoje, pranešimų apie kibernetines saugos grėsmes ir incidentus teikimas Užsakovui iš sekančios įrangos (detalus sąrašas bus pateiktas Teikėjui įrangos diegimo metu):

- kibernetinės saugos užtikrinimo įrangos;
- tarnybinių stočių (Microsoft Windows, Linux OS, DC, DHCP, DNS ir pan.);
- tinklo įrenginių (komutatoriai, maršrutizatoriai, ugniasienės);
- taikomųjų informacinių sistemų (duomenų bazės, web aplikacijos);
- kompiuterinių darbo vietų;
- debesijos paslaugų (Microsoft 365 Office, Defender).

4.2.2. Žurnalinių įrašų koreliavimas ir jų analizė turi identifikuoti vidines ir išorines grėsmes ir rizikas, susijusias kenkėjiška veikla, technologiniais procesais arba žmogiškosiomis klaidomis:

- kenkėjiška arba neteisėta automatizuota veikla Užsakovo IT infrastruktūroje;
- kenkėjiško kodo veikla;
- įsibrovimai arba neteisėta veikla vidiniame Užsakovo kompiuterių tinkle;
- saugumo politikų pažeidimai;
- klaidingos autentifikacijos įvykiai;
- bandymų įsilaužti identifikavimas;
- auditavimo panaikinimo rizikos;
- teisių/privilegijų pakėlimo rizikos;
- ilgalaikio įsitvirtinimo infrastruktūroje rizikos;
- kitos tinklo anomalijos.

4.2.3. Užsakovo IT infrastruktūros pažeidžiamumų paiešką bei rekomendacijų jų šalinimui teikimas:

- atliekami automatizuoti autentifikuoti/neautentifikuoti kompiuterinių darbo vietų, informacinių sistemų, tinklo įrenginių, serverių, web aplikacijų ir taikomųjų sistemų pažeidžiamumų skenavimai, naudojant pripažintas programines saugumo vertinimo priemones (Nmap, Nessus, OpenVAS, BurpSuite ir pan.);
- skenavimo metu identifikuojami žinomi pažeidžiamumai (CVE), neteisingos konfigūracijos, pasenusios programinės įrangos versijos ir kitos saugumo spragos;
- nustatyti pažeidžiamumai turi būti patvirtinti (validuoti), įvertintas jų kritiškumas ir pateiktos rekomendacijos jų šalinimui;
- kritiniai pažeidžiamumai turi būti papildomai patikrinti rankiniu būdu.

4.2.4. Pažeidžiamumų skenavimai atliekami tik Užsakovo pateiktuose tinklo rėžiuose ir tik suderintu su Užsakovu darbo laiku. Pažeidžiamumų skenavimo apimtys sudaro apie 1500 įrenginių per kalendorius metus.

4.3. Žurnalinių įrašų koreliavimas, analitika ir incidentų identifikavimas turi būti atliekamas nenutrūkstamai 24 (dvidešimt keturias) valandas per parą 7 (septynias) dienas per savaitę. Žurnaliniai įrašai turi būti saugomi ne trumpiau kaip 90 (devyniasdešimt) kalendorinių dienų.

4.4. Automatiniai pranešimai turi būti siunčiami komunikacijos bei incidentų valdymo plane nurodytu elektroniniu paštu visą parą pagal šiuos nustatytus įvykius Užsakovo įrangoje:

- sukuriami privilegijuotieji naudotojai;
- aptinkamas nebūdingas naudotojų elgesys ar administratorių piktnaudžiavimas;
- atliekami domeno grupinės politikos pakeitimai;
- aptikus nepatvirtintą naudoti programinę įrangą;
- įrangai komunikuojant su blogos reputacijos išoriniais šaltiniais;
- kitos tinklo anomalijos.

4.5. TPĮ minimaliai turi palaikyti tinklo srauto statistikos NetFlow formatą. Tinklo srauto statistikos duomenys turi būti saugomi ne mažiau kaip 90 (devyniasdešimt) kalendorinių dienų. Tinklo srauto analizė (naudojant NetFlow arba lygiavertę technologiją) turi būti atliekama nenutrūkstamai 24 (dvidešimt keturias) valandas per parą 7 (septynias) dienas per savaitę. Tinklo sraute turi būti identifikuojamos mažiausiai šios grėsmės:

- neteisėta komunikacija su blogos reputacijos išorės šaltiniais;
- vidinės komunikacijos grėsmės;
- DNS, SMTP, HTTP protokolų rizikos;
- HTTPS srauto patikimumas pagrįstas sertifikatų ir IP adresų vertinimu;
- paslaugų trikdymo atakos (angl. DDOS);
- komunikacijos nuokrypiai nuo įprastos įrangos ar naudotojų veikos;
- neatnaujinta ir pažeidžiama programinė įrangą, komunikuojanti su išoriniais šaltiniais ar debesijos paslaugomis;
- kitos tinklo anomalijos.

4.6. Visa paslaugos teikimui reikalinga kaupiama informacija (žurnaliniai įrašai, duomenų srauto įrašai ir kt.) turi būti saugoma tik Užsakovo IT infrastruktūroje ir dėl riboto Saugiojo valstybinio duomenų perdavimo tinklo pralaidumo kanalo negali būti siunčiama į išorę. Užsakovui turi būti suteikta prieiga prie Teikėjo Saugumo stebėsenos ir reagavimo į incidentus platformos, kaupiamos informacijos peržiūrai.

4.7. Teikėjas turi informuoti Užsakovą apie nustatytus įsilaužimo indikatorius ir saugumo rizikas, išvardintas p. 4.2.2 – 4.5. Užfiksavus saugos incidentą ar aptikus anomalijas, Užsakovas turi būti informuojamas per p. 4.10 nustatytą laiką suderintomis komunikacijos priemonėmis.

4.8. Paslaugos Teikėjas saugumo incidento metu turi siūlyti rekomendacijas bei teikti konsultacijas Užsakovui dėl incidento užkardymo ir tolimesnio jo valdymo iki visiško išsprendimo:

- greitojo atsako (užkardymo, žalos mažinimo ir pan.) veiksmų nustatymas ir pateikimas Užsakovui;
- po incidento užkardymo pateikti ilgalaikio poveikio veiksmus – incidento atakos grandinės nustatymas, pateikti rekomendacijas IT infrastruktūros saugumo spragų, kuriomis buvo pasinaudota saugumo incidento metu, šalinimui.

4.9. Kita veikla numato:

- bendradarbiavimas su Užsakovu tiriant saugos incidentus;
- komunikacijos proceso apie saugos incidentus vystymas;
- programinės įrangos, skirtos stebėjimui, koreliavimo taisyklių: vystymas, reguliarus atnaujinimas, kūrimas, optimizavimas ir pritaikymas Užsakovo infrastruktūrai reaguojant į naujas potencialias ir žinomas grėsmes.

4.10. Reakcijos laikas paslaugai (SLA), visą parą:

Informacijos apsikeitimo objektas	**Įvykio kritiškumo lygis[1]**	**Identifikavimo laikas (TTD)[2], ne daugiau**	**Užsakovo informavimo laikas (TTR)[3], ne daugiau**	**Komunikacijos kanalas**
Informavimas apie identifikuotas grėsmes, rizikas ar įtartiną elgesį	Kritinis arba aukštas	1 val.	2 val.	Pranešimas el. paštu, telefonu
	Vidutinis	4 val.	8 val.	Pranešimas el. paštu, telefonu
	Žemas	8 val.	16 val.	Pranešimas el. paštu, telefonu

1 - įvykio kritiškumo lygis nustatomas pagal Teikėjo Saugumo stebėsenos ir reagavimo į incidentus platformoje sužadintos taisyklės kritiškumą.
Skirtingos stebėjimo sistemos įvykių kritiškumą identifikuoja pagal skirtingas metodikas ir gali nurodyti skirtingomis skaitinėmis reikšmėmis.
Šios sutarties vykdymo metu visi įvykiai pagal kritiškumą skirstomi į: a) kritinius, b) aukšto kritiškumo, c) vidutinio kritiškumo, d) žemo kritiškumo. Žemiau lentelėje pateikiame kaip paslaugų teikimo apimtyje naudojamų stebėjimo įrankių generuojamų pranešimų apie įvykius kritiškumas siejasi su naudojamomis kategorijomis.

Stebėjimo įrankis	Kritiškumo požymis	Kritiškumo kategorija paslaugos teikime			
		Žemas kritiškumas	Vidutinis kritiškumas	Aukštas kritiškumas	Kritinis

Saugumo stebėsenos ir reagavimo į incidentus platforma	Severity	<5	>= 5 ir < 8	8 ir 9	10

2 - Įvykio identifikavimo laikas (Time to detect - TTD) skaičiuojamas nuo įvykio atsiradimo stebėsenos ir reagavimo į incidentus platformoje iki jo analizės pradžios.

3 - Informavimo apie įvykį laikas (Time to report - TTR) skaičiuojamas nuo įvykio atsiradimo stebėsenos ir reagavimo į incidentus platformoje iki Užsakovo informavimo nustatyta tvarka momento. Jeigu Užsakovas neatsako/nereaguoja į pateiktą pranešimą, po 30 kalendorinių dienų nuo automatizuoto pranešimo išsiuntimo – užklausa Užklausų valdymo sistemoje uždaroma.

IV SKYRIUS
SUTARTIES IR PASLAUGOS TEIKIMO TERMINAI

5. Paslaugos teikimo pradžia pradedama skaičiuoti nuo visiško TPĮ įdiegimo Užsakovo infrastruktūroje momento ir diegimo darbų perdavimo-priėmimo akto pasirašymo. Paslaugos teikimo terminas – 36 (trisdešimt šeši) mėnesiai nuo Paslaugos teikimo pradžios dienos.

Su Teikėju už Paslaugos teikimą bus atsiskaitoma kas mėnesį - už praeitą kalendorinį mėnesį per 30 (trisdešimt) kalendorinių dienų nuo šios techninės specifikacijos 12 p. nurodytos ataskaitos ir sąskaitos-faktūros pateikimo Užsakovui dienos. TPĮ diegimo laikas į Paslaugos teikimo laikotarpį neįskaitomas ir neapmokamas.

V SKYRIUS
TAISYKLĖS IR STANDARTAI

6. Teikdamas Paslaugą IAE, Teikėjas privalo vadovautis Lietuvos Respublikos teisės aktais, reglamentuojančiais kibernetinį saugumą, informacinių sistemų duomenų tvarkymo teisėtumą ir saugos valdymą;

7. Paslauga teikiama remiantis šiuolaikiniais standartais ir metodikomis, atsižvelgiant į naujausias technologijas bei geriausias praktikas.

VI SKYRIUS
ĮRANGA

8. Teikėjas užtikrina, kad turės pakankamai sutarties įgyvendinimui reikalingų nuosavų priemonių. Pagal šią paslaugų sutartį Užsakovo vardu nebus perkama ir baigus vykdyti sutartį Užsakovui nebus perduodama jokia techninė ar programinė įranga, reikalinga sutarties įgyvendinimui.

9. Teikiant paslaugą Teikėjas turi naudoti savo techninę ir programinę įrangą, reikalingą stebėsenos ir reagavimo į incidentus platformos įdiegimui, pažeidžiamumų skenavimui bei jų vertinimui.

VII SKYRIUS
REZULTATŲ PATEIKIMAS

10. Visi Teikėjo rengiami ir Užsakovui pateikiami dokumentai ir ataskaitos turi būti sudaromi tik elektroniniu būdu lietuvių kalba PDF formatu.

11. Visos ataskaitos turi būti pateikiamos Užsakovui tik suderintu saugiu ryšio kanalu.

12. Paslaugos teikimo laikotarpiu Teikėjas įsipareigoja parengti ir pateikti Užsakovui iki ateinančio mėn. 7 d.:

12.1. praėjusio kalendorinio mėnesio ataskaitą, kurioje pateikiama ši informacija apie per ataskaitinį mėnesį suteiktas Paslaugas:

- per mėnesį stebėtų įrenginių (tarnybinių stočių Linux, Windows, darbo vietų, tinklo įrenginių), sistemų, aplikacijų kiekis bei pokytis su praėjusiu mėnesiu;
- per ataskaitinį laikotarpį užfiksuotas saugumo įvykių skaičius ir jo pokytis per pastaruosius 6 (šešis) mėnesius;
- per ataskaitinį laikotarpį SOC užfiksuotų įtartinų įvykių/grėsmių/anomalijų trumpi aprašymai, kuriuose atvaizduojami: data, laikas, įvykio/grėsmės/anomalijos kategorija, kritiškumo lygis, statusas ir rekomenduojamas reagavimo veiksmas;
- per ataskaitinį laikotarpį užfiksuotas saugumo įvykių skaičius pagal kritiškumo kategorijas ir jo pokytis per pastaruosius 6 (šešis) mėnesius:
  - kenkimo programinė įranga (Microsoft 365 Office antivirusinė apsauga, darbo vietų antivirusinė apsauga, ugniasienių apsauga);
  - informacijos rinkimas (perimetro skenavimai, fišingas);
  - mėginimai įsilaužti (bandymai aptikti ir išnaudoti saugos spragas, nesankcionuoti bandymai prisijungti per VPN);
  - TOP40 kenkėjiškų IP adresų.
- TOP10 dažniausiai suveikiančių Teikėjo stebėsenos ir reagavimo į incidentus platformos koreliacijos taisyklių;
- vidutinė EPS reikšmė per ataskaitinį laikotarpį;
- svarbiausių saugumo įvykių, incidentų apžvalga (eiga, sprendimai);
- pateiktos rekomendacijos dėl kibernetinės saugos rizikų mažinimo;
- per mėnesį atliktų pakeitimų sąrašas įskaitant naujus grėsmių aptikimo scenarijus bei esamų scenarijų pakeitimus.

12.2. praėjusio kalendorinio mėnesio pažeidžiamumų skenavimo ataskaitą, kurioje pateikiami:

- skenavimo IP adresų diapazonai;
- skenavimo metu identifikuoti saugos pažeidžiamumai (CVE);
- pažeidžiamumų vertinimai pagal CVSSv 3.0 BS standarto klasifikaciją;
- rizikos lygiai;

- neteisingos konfigūracijos, pasenusios programinės įrangos versijos ir kitos saugumo spragos;
- prioritetizuotos saugos spragų šalinimo rekomendacijos.

13. Ne rečiau kaip kartą į ketvirtį, Paslaugų teikėjas turi detaliai pristatyti ataskaitose įvardintas rizikas, įvykius, incidentus, aptiktus saugos pažeidžiamumus, kibernetinio saugumo tendencijas ir rekomendacijas.

VIII SKYRIUS
KITOS IŠLAIDOS

14. Visos kitos išlaidos, susijusios su sutarties įgyvendinimu, turi būti įskaičiuotos į bendrą sutarties kainą. Jokios papildomos išlaidos, neįskaičiuotos į sutarties kainą, kompensuojamos nebus.

IX SKYRIUS
KITI REIKALAVIMAI

15. Teikiamos paslaugos ir jų rezultatai, vadovaujantis LR Viešųjų pirkimų įstatymo 37 str. 8 ir 9 punktais, neturi kelti grėsmės nacionaliniam saugumui.

16. Teikėjas turi turėti 24x7 veikiančią užklausų/kreipinių/gedimų registracijos sistemą. Prieiga prie sistemos turi būti suteikta Užsakovui prieš Paslaugos teikimo pradžią.

17. Teikėjo užklausų registracijos sistema turi būti pritaikyta taip, kad kibernetiniai incidentai Kibernetinio saugumo informacinėje sistemoje veikiančioje Nacionalinėje kibernetinių incidentų valdymo platformoje būtų registruojami automatiniu būdu.

18. Teikėjas įsipareigoja:

18.1. garantuoti visos iš Užsakovo gautos informacijos apie Užsakovo infrastruktūrą konfidencialumą ir neperduoti jos tretiesiems asmenims be Užsakovo raštiško sutikimo;

18.2. garantuoti rezultatų, gautų paslaugų teikimo metu, konfidencialumą ir neperduoti jų tretiesiems asmenims.

18.3. garantuoti Aptarnavimo lygio susitarimą (angl. *Service Level Agreement*) ne žemesnį kaip 99,95%.

Fizinės saugos vadovas Marius Pernavas

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Fizinės saugos skyrius (150 / 14 / 16 / 132)
Dokumento pavadinimas (antraštė)	SAUGUMO OPERACIJŲ CENTRO PASLAUGOS PIRKIMO TECHNINĖ SPECIFIKACIJA
Dokumento registracijos data ir numeris	2026-05-04 Nr. Spc-31(13.94E)
Adresatas	Pirkimų ir sutarčių skyrius (446 / 945 / 944)
Dokumentą vizavo.	Vyresnysis specialistas Ivanas Jaronskis
Veiksmo atlikimo data ir laikas	2026-04-29 14:35:57
Dokumentą vizavo.	Vyresnysis kokybės inžinierius Vladimir Klimentjev
Veiksmo atlikimo data ir laikas	2026-04-29 14:43:41
Dokumentą vizavo.	Grupės vadovė Ieva Kazlauskienė
Veiksmo atlikimo data ir laikas	2026-04-30 13:57:58
Dokumentą vizavo.	ITS vadovas Nerijus Keršys
Veiksmo atlikimo data ir laikas	2026-04-30 16:27:04
Dokumentą vizavo.	Vyresnioji pirkimų specialistė Brigita Šerkšnaitė
Veiksmo atlikimo data ir laikas	2026-05-04 08:07:21
Dokumentą vizavo.	Grupės vadovas Šarūnas Šablinskas
Veiksmo atlikimo data ir laikas	2026-05-04 08:32:20
Dokumentą pasirašė	Fizinės saugos vadovas Marius Pernavas
Veiksmo atlikimo data ir laikas	2026-05-04 09:02:47
Dokumentą tvirtino	Generalinis direktorius Linas Baužys
Veiksmo atlikimo data ir laikas	2026-05-04 10:35:41
Registratorius	Dokumentų valdymo specialistė Jolanta Grigorčenko
Veiksmo atlikimo data ir laikas	2026-05-04 14:07:26
Dokumento nuorašo atspausdinimo data ir jį atspausdinęs darbuotojas	2026-05-04 atspausdino Dokumentų valdymo specialistė Jolanta Grigorčenko

Nuorašas tikras
VĮ Ignalinos atominė elektrinė (102 / 103)
2026-05-04