VALSTYBĖS ĮMONĖS
IGNALINOS ATOMINĖS ELEKTRINĖS

SAUGUMO OPERACIJŲ CENTRO PASLAUGOS PIRKIMO TECHNINĖ SPECIFIKACIJA

2025 m. kovo 6 d. Nr. Spc-4(13.67E)
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 nenurūkstamą 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 programinę įrangą, kuri bus įdiegta 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. Paslaugų teikėjas turi užtikrinti, kad dirbančių analitikų kompetencija būtų pakankama išvardintoms funkcijoms atlikti.

3.2. Ne vėliau kaip per 14 (keturiolika) kalendorinių 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 programinę įrangą (programinė įranga turi atitikti šios techninės specifikacijos 4.1.1 p. reikalavimus). Teikėjo programinės įrangos diegimas Užsakovo informacinėje infrastruktūroje turi būti atliktas ne vėliau nei per 80 (aštuoniasdešimt) kalendorines dienas nuo sutarties įsigaliojimo. Prie paslaugos teikimui pateikiamos įrangos Teikėjas jungiasi saugiu šifruotu VPN komunikacijos kanalu nuotoliniu būdu.

4.1.1. Teikėjo naudojama programinė įranga turi 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). Integruojamos Užsakovo tinklo įrangos vienetų skaičius ir įvykių surinkimo agentų skaičius neturi būti ribojamas. 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 60 (šešiasdešimt) serverių. Įvykių per sekundę (EPS), tinklo, kompiuterinių darbo vietų ir kitų įrenginių kiekis neturi būti ribojamas.

4.2. Paslaugą sudaro:

4.2.1. Nuolatinis žurnalinių įrašų surinkimas, jų koreliavimas centralizuotoje Teikėjo Saugos informacijos ir įvykių valdymo sistemoje (angl. SIEM – Security Information and Event Management) (toliau - SIEM), 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 ir Linux OS);
- 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.

4.3. 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. Programinė įranga 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 negali būti siunčiama į išorę. Užsakovui turi būti suteikta prieiga prie SIEM, 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 saugumo įvykių stebėjimo sistemoje 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
SIEM	Severity	<5	>= 5 ir < 8	8 ir 9	10

2 - Įvykio identifikavimo laikas (Time to detect - TTD) skaičiuojamas nuo įvykio atsiradimo saugumo įvykių stebėjimo sistemoje iki jo analizės pradžios.

3 - Informavimo apie įvykį laikas (Time to report - TTR) skaičiuojamas nuo įvykio atsiradimo saugumo įvykių stebėjimo sistemoje 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 programinės įrangos įdiegimo Užsakovo infrastruktūroje momento ir diegimo darbų perdavimo-priėmimo akto pasirašymo. Paslaugos teikimo terminas – 12 (dvylika) mėnesių 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. Įrangos 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 elektroninės informacijos saugą, kibernetinį saugumą ir kitais teisės aktais, reglamentuojančiais 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. Teikėjas paslaugai turi naudoti savo programinę įrangą, reikalingą SIEM įdiegimui ir paslaugai suteikti.

VII SKYRIUS
REZULTATŲ PATEIKIMAS

10. Visi Teikėjo rengiami dokumentai turi būti sudaromi tik elektroniniu būdu lietuvių kalba.

11. Visos ataskaitos turi būti teikiamos Užsakovui tik nustatytu saugiu ryšio kanalu.

12. Teikėjas įsipareigoja parengti ir pateikti Užsakovui iki ateinančio mėn. 7 d. praėjusio kalendorinio mėnesio ataskaitą su aprašymu elektroniniu PDF formatu:

12.1. Programinės įrangos diegimo laikotarpiu ataskaitoje turi būti:

- informacija apie diegimo eigą – trumpas atliktų diegimo veiksmų aprašymas, numatomi atlikti veiksmai ir numatomos atlikimo datos.

12.2. Paslaugos teikimo laikotarpiu, ataskaitoje turi būti ši informacija apie per mėnesį suteiktas Paslaugas:

- Per ataskaitinį laikotarpį užfiksuotas saugumo įvykių skaičius ir jo pokytis per pastaruosius 6 (šešis) mėnesius;
- Per ataskaitinį laikotarpį užfiksuotas saugumo incidentų 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, žvalgyba, fišingas);
  - mėginimai įsilaužti (bandymai aptikti ir išnaudoti saugos spragas, nesankcionuoti bandymai prisijungti per VPN);
  - TOP40 kenkėjiškų IP adresų.
- TOP10 dažniausiai suveikiančių koreliacijos taisyklių;
- Vidutinė EPS reikšmė per ataskaitinį laikotarpį;
- Svarbiausių saugumo įvykių, incidentų apžvalga (eiga, sprendimai);
- Pateiktos rekomendacijos dėl kibernetinės saugos rizikų mažinimo;
- Per mėnesį stebėtų įrenginių kiekis bei pokytis su praėjusiu mėnesiu;
- Per mėnesį atliktų pakeitimų sąrašas įskaitant naujus grėsmių aptikimo scenarijus bei esamų scenarijų pakeitimus.
- Ne rečiau kaip kartą į ketvirtį, Paslaugų teikėjas turi detaliai pristatyti ataskaitose įvardintas rizikas, įvykius, incidentus, tendencijas ir rekomendacijas.

VIII SKYRIUS
KITOS IŠLAIDOS

13. 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

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

15. Teikėjas turi turėti 24x7 veikiančią užklausų/kreipinių/gedimų registracijos sistemą.

16. Teikėjas įsipareigoja:

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

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

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