2026 - - sutarties Nr. _____

1 priedas

TECHNINĖ SPECIFIKACIJA

I. PIRKIMO OBJEKTAS

1. Pirkimo objektą sudaro akcinei bendrovei Klaipėdos valstybinio jūsų uosto direkcijai (toliau – Perkančioji organizacija) teikiamos Saugumo operacijų centro (angl. SOC) paslaugos (toliau – Paslaugos), kurios apima:

1.1. IBM QRadar saugumo informacijos ir įvykių valdymo (angl. Security Information and Event Management – toliau SIEM) įrankio priežiūrą;

1.2. kibernetinio saugumo analitiką ir kibernetinių incidentų tyrimą;

1.3. tinklų ir informacinių sistemų (TIS) pažeidžiamumų valdymą.

II. ESAMOS SITUACIJOS APRAŠYMAS

2. Perkančiosios organizacijos naudojamos TIS aprašas:

2.1. Kompiuterizuotų darbo vietų (toliau – KDV) yra apie 190, iš jų 3 MacOS, kitos Windows;

2.2. 16 fizinių serverių;

2.3. 10 vnt. serverių su VmWare hypervizoriumi;

2.4. 6 vnt. serverių be virtualizacijos (3 vnt. – AIX, 3 vnt. – Windows);

2.5. 36 Windows virtualios mašinos (VM);

2.6. 69 Linux virtualios mašinos (VM);

2.7. 3 vnt. ugniasienių;

2.8. 60 vnt. kompiuterių tinklų komutatorių;

2.9. 32 vnt. WiFi prieigos taškų;

2.10. naudojama IBM QRadar SIEM, kurios licenciniai pajėgumai iki 15000 tinklo srauto per minutę (angl. FPM), 1100 įvykių per sekundę (angl. EPS);

2.11. KDV veikia Microsoft Defender for Endpoint (EDR - Endpoint Detection and Response).

2.12. Serveriuose su Windows ir Linux operacinėmis sistemomis veikia Microsoft Defender for Cloud.

III. BENDRIEJI REIKALAVIMAI PASLAUGOMS

3. Teikiant paslaugas turi būti vadovaujamasi šiais teisės aktais bei rekomendacijomis (aktualiomis redakcijomis):

3.1. Valstybės informacinių išteklių valdymo įstatymu;

3.2. Kibernetinio saugumo įstatymu;

3.3. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ patvirtintu Kibernetinio saugumo reikalavimų aprašu;

3.4. kitais Europos Sąjungos ir Lietuvos Respublikos teisės aktais, Lietuvos Respublikos ir tarptautiniais standartais, reglamentuojančiais informacijos saugą, kibernetinį saugumą, asmens duomenų apsaugą.

4. Tiekėjo specialistai privalo mokėti lietuvių kalbą arba turi būti užtikrintos kokybiškos vertimo paslaugos Tiekėjo sąskaita.

5. Tiekėjo parengti dokumentai (analizės, projektavimo ir diegimo dokumentacija) turi būti pateikiami lietuvių kalba.

6. Tiekėjas sutarties vykdymui turi turėti 24 valandas per parą 7 dienas per savaitę nenutrūkstamai veikiančią pagalbos tarnybą, kuri turi turėti aprašytą ir veikiantį kreipinių ir incidentų sprendimo procesą, atitinkantį ITIL (atitiktis turi būti pagrįsta tiekėjo pateikiamais metodikos aprašais, procesų dokumentacija ir (ar) specialistų sertifikatais) geriausių praktikų rekomendacijas, pagal kurį registruojami gedimų kreipiniai, šalinami gedimai, stebima darbų vykdymo eiga. Tiekėjo pagalbos tarnyba privalo turėti interneto portalą, atitinkantį ITIL (ar lygiavertės metodikos) IT paslaugų valdymo geriausių praktikų metodiką, kuriame Perkančiosios organizacijos atsakingi asmenys turėtų galimybę registruoti gedimų kreipinius, stebėti darbų vykdymo eigą, generuoti ataskaitas. Tiekėjo pagalbos tarnyboje turi būti komunikuojama lietuvių kalba. Tiekėjo pagalbos tarnyba turi suteikti galimybes registruoti kreipinius tiek elektroniniu paštu, tiek telefonu, tiek per Web portalą.

7. Paslaugų įgyvendinimo planas:

7.1. paslaugų suderinimo ir veikimo pradžios planas;

7.2. pradinis SIEM\SOC sukonfigūravimas – iki 45 kalendorinių dienų;

7.3. pirmoji SOC paslaugų analizės ataskaita – per 2 mėn.;

7.4. visas SOC funkcionalumas – per 3 mėn.

IV. REIKALAVIMAI, KELIAMI IBM QRADAR SIEM ĮRANKIO PRIEŽIŪROS PASLAUGOMS

8. Teikiant paslaugas turi būti:

8.1. nuolat stebima SIEM būklė, taikomos proaktyvios problemų prevencijos priemonės, reaguojama į pastebėtus sutrikimus ir problemas, atkuriamas SIEM veikimas;

8.2. įdiegiami SIEM programiniai atnaujinimai ne vėliau nei per 22 darbo dienas po gamintojo atnaujinimo išleidimo, nebent gamintojas rekomenduoja kitaip arba nustatoma rizika sistemos stabilumui;

8.3. tvarkomi standartiniai ir specifiniai įrašų šaltiniai: pridedama į SIEM, modifikuojama, pašalinama;

8.4. perimamos esamos SIEM sistemoje jau sukonfigūruotos koreliacijos taisyklės (šiuo metu veikiančių – apie 200 vnt.), analizuojamos ir užtikrinamas nepertraukiamas jų veikimas, optimizavimas ir aktualumas (9.6.2 p. aprašytų MITRE ATT&CK taktikų padengimas). Taisyklių bazė apima tiek standartines gamintojo, tiek specifines, pagal Perkančiosios organizacijos poreikius pritaikytas taisykles;

8.5. tvarkomi išoriniai kibernetinių grėsmių indikatorių (angl. cyber threat intelligence) duomenų šaltiniai (kenksmingų IP adresų, domenų ir pan.): pridedama, modifikuojama, pašalinama;

8.6. konfigūruojamos SIEM koreliacijos taisyklės pagal saugumo analitikų pateiktas rekomendacijas ir pastabas (modifikuojama, pašalinama);

8.7. nufiltruojami pertekliniai sisteminiai įrašai ir pateikiamos filtravimo rekomendacijos;

8.8. teikiamos rekomendacijos dėl reikalingų sisteminių įrašų rinkimo;

8.9. pridedami nauji sistemos naudotojai, pašalinami seni sistemos naudotojai;

8.10. kuriamos ataskaitos pagal saugumo analitikų siūlymus ir perkančiosios organizacijos poreikį;

8.11. teikiami siūlymai dėl SIEM įrankio veikimo optimizavimo ir įgyvendinimo;

8.12. užtikrinamas SIEM įrankio konfigūracijos rezervinių kopijų darymas prieš kiekvieną reikšmingą pakeitimą ar programinį atnaujinimą;

8.13. užtikrinamas SIEM duomenų rinkimo (angl. log ingestion) vientisumo ir prieinamumo stebėjimas, identifikuojant nutrūkusius ar neveikiančius įrašų šaltinius.

V. REIKALAVIMAI, KELIAMI KIBERNETINIO SAUGUMO ANALITIKOS IR KIBERNETINIŲ INCIDENTŲ TYRIMO PASLAUGOMS

9. Teikiant paslaugas turi būti:

9.1. informuojama apie incidentus pagal su Perkančiąja organizacija suderintą komunikacijos planą, kuris turi apimti: Tiekėjo ir Perkančiosios organizacijos atsakingų už kibernetinio saugumo užtikrinimą kontaktus; procesą, aprašantį komunikacijos veiksmus incidento atveju; kanalus,kuriais bus informuojama apie incidentus;

9.2. analizuojami SIEM generuojami aliarmai (patvirtinimas, klasifikavimas, grupavimas, išsprendimo inicijavimas, konsultavimas sprendžiant);

9.3. užtikrinama, kad „Microsoft Defender for Endpoint“ telemetrija būtų integruota į SOC naudojamą SIEM;

9.4. „Microsoft Defender for Endpoint“ generuojami įspėjimai negali būti vertinami izoliuotai – jie turi būti koreliuojami su kitų TIS teikiamais į SIEM duomenimis;

9.5. tobulinamos esamos koreliacijos taisyklės ir įvedamos naujos;

9.6. naudojami išoriniai ir vidiniai kibernetinių grėsmių indikatorių šaltiniai (pvz., MISP, nacionaliniai CERT/NKSC pranešimai, kiti patikimi grėsmių žvalgybos (angl. threat intelligence) šaltiniai) ir užtikrinama jų integracija į SIEM koreliacijos taisykles:

9.6.1. IoC (angl. Indicators of Compromise) pagrindu veikiančios analitinės taisyklės:

9.6.1.1. žinomų kenksmingų failų maišos (angl. Hash) reikšmių aptikimas;

9.6.1.2. komunikacijos su žinomais kenksmingais ar sukčiavimo unikaliais interneto adresais (angl. phishing URL) identifikavimas;

9.6.1.3. komunikacijos su žinomais blogos reputacijos IP adresais identifikavimas;

9.6.1.4. komunikacijos su anksčiau kompromituotais ar C2 (angl. Command and Control) serveriais identifikavimas;

9.6.1.5. kenksmingų domenų ar domenų generavimo algoritmų (DGA) požymių aptikimas.

9.6.2. Tiekėjas privalo užtikrinti analitinių taisyklių veikimą, paremtų elgsenos analizę ir atakos taktikų, technikų bei procedūrų (TTP) identifikavimu, remiantis MITRE ATT&CK metodologija, bent šiais, bet neapsiribojant, scenarijais:

9.6.2.1. bandymų įsilaužti (angl. brute force, password spraying, scanning) identifikavimas;

9.6.2.2. neįprastų autentifikacijos modelių ir autentifikavimo rizikos nustatymas;

9.6.2.3. vartotojų elgesio nuokrypių (anomalijų) identifikavimas;

9.6.2.4. teisių ar privilegijų pakėlimo (angl. privilege escalation) požymių aptikimas;

9.6.2.5. horizontalaus judėjimo (angl. lateral movement) infrastruktūroje identifikavimas;

9.6.2.6. kredencialų vagystės požymių identifikavimas;

9.6.2.7. kenksmingo programinio kodo vykdymo požymių identifikavimas;

9.6.2.8. ilgalaikio įsitvirtinimo (angl. persistence) infrastruktūroje požymių identifikavimas;

9.6.2.9. auditavimo išjungimo ar saugumo kontrolės apėjimo požymių identifikavimas;

9.6.2.10. neįprastos tinklo prieigos ar duomenų iškėlimo (angl. exfiltration) požymių identifikavimas;

9.6.3. elgsenos aptikimai negali būti ribojami tik statinėmis taisyklėmis – turi būti taikoma įvykių koreliacija ir kontekstinė analizė;

9.7. nustatomos incidento pirminės priežastys (angl. root cause);

9.8. nustatomos incidentų atakos grandinės;

9.9. tiriamas incidentas, atkuriama jo eiga;

9.10. incidento tyrimas turi apimti kompromitavimo vektoriaus, paveiktų sistemų, galimo duomenų nutekėjimo identifikavimą ir tolimesnių veiksmų rekomendacijas;

9.11. surenkami ir išsaugojami SIEM esantys incidento įrodymai;

9.12. teikiamos saugos ir saugos valdymo procesų gerinimo rekomendacijos, suvaldžius incidentą;

9.13. valdomas incidento sprendimas;

9.14. teikiamos ataskaitos 1 kartą per **mėnesį**:

9.14.1. netikrų aliarmų (angl. false-positive) kiekis;

9.14.2. tikrų eskaluotų aliarmų kiekis;

9.14.3. saugumo stiprinimo pasiūlymai;

9.14.4. incidentų priežastys;

9.14.5. pasiūlytų saugumo veiksmų vykdymo statusas (derinant su paslaugos gavėju);

9.14.6. pasiūlytos naujos koreliacijos taisyklės.

9.15. teikiami periodiniai (ne rečiau kaip kas 3 mėnesius) pasiūlymai ir konsultacijos dėl paslaugos gerinimo;

9.16. teikiamos rekomendacijos IT infrastruktūros saugumo spragoms, kuriomis buvo pasinaudota saugumo incidento metu, šalinti;

9.17. saugumo įvykių stebėsena ir pirminė analizė vykdoma 24/7 režimu.

9.18. konsultavimo, kibernetinių incidentų tyrimo ir papildomų paslaugų teikimo laikas darbo dienomis 9/5 režimu;

9.19. saugumo įvykio reakcijos laikas ne daugiau kaip 2 val.;

9.20. saugumo įvykio reakcijos laikas – tai laikotarpis nuo saugumo įvykio atsiradimo SIEM iki pirmo Tiekėjo veiksmo. Pirmu Tiekėjo veiksmu laikoma:

9.20.1. saugumo įvykio uždarymas kaip klaidingas suveikimas (angl. False Positive);

9.20.2. Tiekėjo užklausa sutartais komunikacijos kanalais Perkančiajai organizacijai norint kvalifikuoti saugumo įvykį;

9.20.3. saugumo įvykio perkvalifikavimas į saugumo incidentą ir Perkančiosios organizacijos informavimas sutartais komunikacijos kanalais;

9.21. užklausos (suteikti informaciją, konsultuoti, atlikti konfigūravimo veiksmus ir pan.) reakcijos laikas 8 val.;

9.22. užklausos sprendimo laikas 72 val.;

9.23. Tiekėjas užtikrina naudojamos galinių įrenginių apsaugos platformos Microsoft Defender for Endpoint administravimą ir reagavimo į incidentus veiksmus pagal iš anksto su Perkančiąja organizacija suderintą reagavimo modelį:

9.23.1. platformos administravimas:

9.23.1.1. vartotojų, rolų ir prieigų valdymas pagal suderintą prieigos modelį;

9.23.1.2. saugumo politikų ir konfigūracijų priežiūra, optimizavimas ir koregavimas;

9.23.1.3. integracijų priežiūra su SIEM;

9.23.1.4. įrenginių įtraukimo (angl. onboarding) kontrolė ir būklės stebėjimas (agentų veikimas, sensorių būklė);

9.23.1.5. išimčių (angl. exclusions) periodinis peržiūrėjimas ir taikymas siekiant sumažinti klaidingų suveikimų kiekį ir užtikrinti optimalų aptikimo lygį.

9.23.2. reagavimas į saugumo incidentus:

9.23.2.1. kompromituotų įrenginių izoliavimas;

9.23.2.2. kenkėjiškų failų karantinavimas arba blokavimas;

9.23.2.3. įtartinų procesų stabdymas;

9.23.2.4. Perkančiajai organizacijai pateikiama informacija apie incidentą, atliktus veiksmus ir rekomendacijas tolimesniems veiksmams.

9.23.3. Tiekėjas užtikrina, kad galinių įrenginių apsaugos platformos Microsoft Defender for Endpoint aptikti incidentai būtų integruojami į bendrą SOC incidentų valdymo procesą.

9.24. vadovaujantis Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Kibernetinio saugumo reikalavimų aprašo patvirtinimo“ (Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 6 d. nutarimo Nr. 945 redakcija) 3 punktu, Tiekėjas pritaiko kibernetinio saugumo įvykių ir kibernetinių incidentų valdymo TIS taip, kad kibernetiniai incidentai Nacionalinio kibernetinio saugumo centro Kibernetinio saugumo informacinėje sistemoje (KSIS) veikiančioje Nacionalinėje kibernetinių incidentų valdymo platformoje būtų registruojami automatiniu būdu, naudojant Nacionalinėje incidentų valdymo sistemoje įdiegtą automatizuotų pranešimų apie kibernetinius incidentus per API funkcionalumą pagal esminiams kibernetinio saugumo subjektams taikomus reikalavimus. Perkančioji organizacija suteiks Tiekėjui reikalingą techninę informaciją ir prieigas API integracijai su Nacionaline kibernetinių incidentų valdymo platforma.

VI. REIKALAVIMAI, KELIAMI PAŽEIDŽIAMUMŲ VALDYMO PASLAUGAI

10. Pažeidžiamumų valdymo paslauga skirstoma į dvi atskiras apimtis:

10.1. KDV, kuriose yra įdiegta Microsoft Defender for Endpoint apsauga, pažeidžiamumų valdymas vykdomas naudojant Microsoft Defender for Endpoint pažeidžiamumų valdymo (Threat & Vulnerability Management – TVM) funkcionalumą, kuris laikomas pakankamu pažeidžiamumų nustatymo šaltiniu Perkančiosios organizacijos KDV infrastruktūroje, ir apima:

10.1.1. pažeidžiamumų identifikavimą;

10.1.2. rizikos vertinimą;

10.1.3. prioritetizavimą;

10.1.4. pažeidžiamumų šalinimo rekomendacijų teikimą Perkančiajai organizacijai.

10.2. Serverius, kuriuose yra įdiegta Microsoft Defender for Cloud apsauga, pažeidžiamumų valdymas vykdomas naudojant Microsoft Defender for Cloud pažeidžiamumų valdymo funkcionalumą, kuris laikomas pakankamu pažeidžiamumų nustatymo šaltiniu Perkančiosios organizacijos serverių infrastruktūroje, ir apima:

10.2.1. pažeidžiamumų identifikavimą;

10.2.2. rizikos vertinimą;

10.2.3. poveikio analizę;

10.2.4. prioritetizavimą;

10.2.5. pažeidžiamumų šalinimo rekomendacijų teikimą Perkančiajai organizacijai.

10.3. Serverių pažeidžiamumų būklė turi būti peržiūrima ir analizuojama ne rečiau kaip kartą per mėnesį, remiantis Microsoft Defender for Cloud pažeidžiamumų valdymo funkcionalumo generuojamais duomenimis.

11. Tiekėjui bus suteikta prieiga prie Microsoft Defender for Endpoint ir Microsoft Defender for Cloud pažeidžiamumų valdymo duomenų (per valdymo portalą arba kitą Perkančiosios organizacijos nustatytą būdą).

12. Tiekėjas privalo pateikti prioritetizuotas rekomendacijas, pritaikytas Perkančiosios organizacijos TIS;

13. rekomendacijose turi būti nurodyta:

13.1. CVE identifikatorius (jei taikoma);

13.2. CVSS balas;

13.3. galimas poveikis organizacijos TIS;

13.4. rekomenduojamas šalinimo būdas;

13.5. rekomenduojamas įgyvendinimo terminas pagal kritiškumą.

14. Tiekėjas konsultuoja Perkančiąją organizaciją dėl pažeidžiamumų šalinimo prioritetų, tačiau atnaujinimus ir konfigūracijos pakeitimus įgyvendina Perkančioji organizacija.

15. Serverių pažeidžiamumai turi būti nustatomi remiantis realiai įdiegtų programinės įrangos komponentų analize. Neturi būti teikiamos rekomendacijos dėl pažeidžiamumų, susijusių su programinės įrangos komponentais ar moduliais, kurie nėra įdiegti arba nėra aktyvūs tikrinamoje sistemoje (pvz., jei Apache nėra įdiegtas modulis, šio modulio pažeidžiamumų šalinimo rekomendacijos neturi būti teikiamos). Perkančioji organizacija suteiks Tiekėjui reikiamas teises (paskyras, turinčias tik skaitymo (angl. read only) privilegijas) atlikti autentikuoto skenavimo procedūras.

16. Jei nustatyto serverio pažeidžiamumo rizika yra priimtina Perkančiajai organizacijai (pvz., dėl techninių apribojimų), toks pažeidžiamumas tiekėjo ataskaitoje turi būti minimas sąraše „priimtina rizika“. Tiekėjas privalo pasiūlyti kompensacines priemones šiai rizikai suvaldyti, o Perkančioji organizacija – raštu patvirtinti sprendimą dėl rizikos priėmimo. Priimtinų rizikų sąrašas privalo būti peržiūrimas ne rečiau kaip kas 6 mėnesius.

17. Periodinėse ataskaitose turi būti atskirai pateikiama:

17.1. KDV pažeidžiamumų būklė ir rekomendacijų įgyvendinimo būsena;

17.2. serverių pažeidžiamumų sąrašas ir rekomendacijų įgyvendinimo būsena (pvz. atviras, įgyvendinamas, pašalintas, priimtina rizika).

18. Bendri paslaugų lygio reikalavimai (angl. SLA – Service Level Agreement):

18.1. pažeidžiamumai prioritetizuojami pagal CVSS bazinį balą (Common Vulnerability Scoring System);

18.2. Kritiškumo lygiai nustatomi taip:

CVSS balas	Kritiškumo lygis
9.0–10.0	Kritinis
7.0–8.9	Aukštas
4.0–6.9	Vidutinis
0.1–3.9	Žemas

18.3. jei pažeidžiamumui nėra priskirto CVSS balo, kritiškumą nustato Tiekėjas, suderinęs su Perkančiąją organizacija, atsižvelgdamas į poveikį paslaugų tęstinumui, duomenų konfidencialumui ir infrastruktūros kritiškumą.

19. KDV pažeidžiamumų valdymo SLA:

19.1. Tiekėjas privalo informuoti Perkančiąją organizaciją apie nustatytus pažeidžiamumus:

19.1.1. kritiniai – per 4 val. nuo pažeidžiamumo nustatymo momento skenavimo rezultatuose;

19.1.2. aukšti – per 1 darbo dieną;

19.1.3. vidutiniai ir žemi – periodinėje ataskaitoje;

20. Serverių pažeidžiamumų valdymo SLA:

20.1. Tiekėjas privalo informuoti Perkančiąją organizaciją apie nustatytus serverių pažeidžiamumus:

20.1.1. kritiniai – per 2 val. nuo pažeidžiamumo nustatymo momento skenavimo rezultatuose;

20.1.2. aukšti – per 1 darbo dieną;

20.1.3. vidutiniai ir žemi – periodinėje ataskaitoje.

21. Tiekėjas privalo pateikti rizikos analizę ir rekomendacijas:

Kritiškumo lygis	Analizės ir rekomendacijų pateikimo terminas

Kritinis	per 24 val.
Aukštas	per 3 darbo dienas
Vidutinis	periodinėje ataskaitoje
Žemas	periodinėje ataskaitoje

22. Tiekėjas privalo:

22.1. konsultuoti dėl serverių pažeidžiamumų šalinimo prioritetų nustatymo;

22.2. įvertinti Perkančiosios organizacijos įgyvendintų priemonių efektyvumą pakartotinio skenavimo metu;

22.3. atnaujinti pažeidžiamumų būseną ataskaitose.

23. SLA vykdymo atitiktis vertinama kas mėnesį.

24. SLA vykdymo atitikties ataskaitose turi būti nurodyta:

24.1. nustatymo data;

24.2. informavimo data;

24.3. rekomendacijos pateikimo data.

24.4. SLA pažeidimai laikomi esminiais sutarties pažeidimais, jei informavimo apie kritinius pažeidžiamumus terminas viršijamas daugiau nei 2 kartus per ketvirtį.

VII. KITI REIKALAVIMAI

25. Teikėjo informacijos saugos valdymo sistema turi atitikti ISO/IEC 27001 tarptautinio standarto arba kitų lygiaverčių informacijos saugos valdymo sistemų reikalavimus.

26. Perkant Paslaugą taikomas LR aplinkos ministro 2011 m. birželio 28 d. įsakymo Nr. D1-508 4.4.3 p., t. y. pirkimas laikomas žaliu, nes perkama tik nematerialaus pobūdžio (intelektinė) ar kitokia paslauga, nesusijusi su materialaus objekto sukūrimu, kurios teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos.

27. Teikėjas ar jį kontroliuojantis asmuo negali būti registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose.

28. Paslaugos negali būti teikiamos iš Viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.