

SAUGUMO OPERACIJŲ CENTRO PASLAUGŲ PIRKIMO TECHNINĖ SPECIFIKACIJA

I SKYRIUS PIRKIMO OBJEKTAS

1. Pirkimo objektas – Saugumo operacijų centro (angl. SOC) paslaugos (toliau – **Paslaugos**), susidedančios iš: informacinių sistemų žurnalinių įrašų surinkimo, tinklo srauto bei kibernetinių grėsmių ir incidentų stebėjimo – pažeidžiamumų identifikavimo (skenavimo) pagal suderintą grafiką, valdomo grėsmių aptikimo bei reagavimo MDR (angl. Managed Detection and Response) paslaugos, teikiamos akcinės bendrovės „Kauno energija“ (toliau – **Perkantysis subjektas**) turimo EDR (angl. Endpoint detection and response) sprendimo pagrindu.
2. Paslaugų teikėjo (toliau – **Tiekėjas**) specialistai (analitikai, grėsmių ir incidentų tyrėjai) turės proaktyviai stebėti Perkančiojo subjekto informacinių technologijų (toliau – **IT**) infrastruktūros žurnalinius įvykius, duomenų srautus ir surinktą papildomą telemetrinę informaciją, atlikti analizę, identifikuoti incidentus ir grėsmes.
3. Pirkimo tikslas – užtikrinti turimos IT infrastruktūros bei informacinių sistemų kibernetinių grėsmių bei incidentų aptikimą, taip įgalinant Perkantįjį subjektą efektyviai ir greitai šalinti atsiradusius trūkumus siekiant minimizuoti arba užkirsti kelią galimam žalos atsiradimui bei informacijos nutekimui.

II SKYRIUS PIRKIMO OBJEKTO APIMTYS IR CHARAKTERISTIKA

4. Paslaugos turi apimti:
 - 4.1. Nuolatinį žurnalinių įrašų (angl. logs) surinkimą/koreliavimą bei pranešimų apie kibernetinės saugos grėsmes ir incidentus teikimą iš kritinių šaltinių (angl. log source):
 - 4.1.1. tinklo perimetro įrenginių (ugniasienės, maršrutizatoriai, WAF, IDS, IPS, load balancer, proxy, antispam, VPN ir kt.);
 - 4.1.2. tarnybinių stočių (su Microsoft arba Linux programine įranga);
 - 4.1.3. taikomųjų informacinių sistemų;
 - 4.1.4. kompiuterinių darbo vietų;
 - 4.1.5. saugos užtikrinimo įrangos (antivirusinės, naudotojų elgesio stebėjimo programinės įrangos, dokumentų/aplankų stebėjimo programinės įrangos).
 - 4.2. Žurnalinių įrašų surinkimą, naudojant universalius protokolus ir agentus (pvz., Syslog, Beats, Winlogbeat, Filebeat, Auditbeat, NXLog);
 - 4.3. Struktūrizuotų ir nestructūrizuotų žurnalinių įrašų normalizavimą į vieningą analizės formatą (pvz., Splunk CIM, LEEF, CEF);
 - 4.4. Kritinių saugos šaltinių prioretizavimą (galimybė taikyti aukštesnį jautrumą ar reagavimo SLA);
 - 4.5. Galimybę identifikuoti grėsmes pagal susijusių įrenginių žurnalinių įrašų seką (pvz., nuo WAF įspėjimo iki serverio autentifikacijos klaidos);
 - 4.6. Automatinį pranešimų siuntimą apie incidentus ir jų kontekstą el. paštu;
 - 4.7. Žurnalinių įrašų gavimo nutraukimo ar nereguliarumo aptikimą (angl. log source heartbeat monitoring);
 - 4.8. Žurnalinių įrašų apie saugos spragas, konfigūracijos klaidas ar Paslaugų nestabilumą įtraukimą į bendrą grėsmių analizę;

- 4.9. Laikiną arba dinamišką žurnalinių įrašų šaltinių prijungimą, pvz., incidentų metu ar atliekant papildomą tyrimą;
- 4.10. Grėsmių žvalgybos integraciją žurnalinių įrašų analizėje (pvz., IOC tikrinimas pagal Threat Intelligence sąrašus);
- 4.11. Tikslinį žurnalinių įrašų rinkimą iš Microsoft 365 ir Azure debesijos paslaugų.
5. Žurnalinių įrašų koreliavimas ir analizė turi identifikuoti vidines ir išorines grėsmes, susijusias su kenkėjiška veikla, technologiniais procesais ir žmogiškosiomis klaidomis (Incidentų identifikavimas kibernetinio saugumo analitikų turi būti vykdomas nuo 08.00 val. iki 17.00 val. darbo dienomis):
 - 5.1. Technologines anomalijas ir saugumo spragas;
 - 5.2. Neteisėtos arba klaidingos autentifikacijos įvykius;
 - 5.3. Kenkėjišką veiklą infrastruktūroje;
 - 5.4. Saugumo politikų nusižengimus;
 - 5.5. Atakas iš el. pašto kanalo;
 - 5.6. Įsibrovimus į vidinį Perkančiojo subjekto kompiuterinį tinklą;
 - 5.7. Neteisėtą veiklą Perkančiojo subjekto kompiuteriniame tinkle ar įrangoje;
 - 5.8. Kenkėjiško kodo veiklą;
 - 5.9. Piktnaudžiavimą administracinėmis teisėmis (pvz., privilegijų eskalacija ar neautorizuoti veiksmai su sisteminiais resursais);
 - 5.10. Įtartą procesų paleidimą, scenarijų vykdymą ar įrankių naudojimą (pvz., Powershell, WMI, PsExec);
 - 5.11. Netipinį naudotojų elgesį, susijusį su laikais, lokacijomis ar prieigomis prie sistemų (pvz., naudotojo prisijungimas iš kelių geografinių vietų per trumpą laiką);
 - 5.12. Duomenų nutekėjimo požymius (pvz., dideli duomenų srautai į išorinius adresus, failų šifravimo požymiai);
 - 5.13. Grėsmes, kylančias dėl žmogiškųjų klaidų – netyčinis jautrių duomenų perkėlimas, neteisingos konfigūracijos ar klaidingi leidimai;
 - 5.14. Atitikties politikos pažeidimus (pvz., prisijungimai prie sistemų be dviejų faktorių autentifikacijos, neteisėti konfigūracijų keitimai);
 - 5.15. Automatinį žurnalinių įrašų koreliavimą pagal MITRE ATT&CK technikas ir taktiką;
 - 5.16. Saugumo incidentų sekų (angl. kill chain) rekonstrukciją iš daugelio žurnalinių įrašų šaltinių;
 - 5.17. Neautorizuotų sistemų ar vartotojų veiksmų loginį susiejimą su galimomis grėsmėmis (pvz., lateral movement);
 - 5.18. Laikinių paskyrų ar techninių naudotojų piktnaudžiavimo stebėseną ir analizę;
 - 5.19. Tikslinių (APT) atakų požymių aptikimą remiantis žurnalinių įrašų ir srauto duomenų koreliacija (angl. blended detection).
6. XDR (angl. Extended Detection and Response) įrankio saugumo analitikos ir užkardymo paslauga:
 - 6.1. Perkančiojo subjekto turimo XDR sprendimo generuojamų pranešimų analitika;
 - 6.2. XDR sprendimo pateiktų atakos grandinių analizė;
 - 6.3. Sprendimo taisyklių nustatymai ir pritaikymas prie Perkančiojo subjekto IT infrastruktūros;
 - 6.4. Sprendimo atnaujinimų priežiūra ir informavimas apie technines problemas;
 - 6.5. Esminės informacijos integravimas į mėnesines ataskaitas.
7. Automatiniai pranešimai turi būti siunčiami el. paštu, teikiami 24/7/365 pagal įjungtas taisykles, pavyzdžiui:
 - 7.1. aptinkamas nebūdingas naudotojų elgesys ar administratorių piktnaudžiavimas;
 - 7.2. sukuriami privilegijuotieji naudotojai;
 - 7.3. atliekami grupinės politikos pakeitimai;
 - 7.4. aptikus nepatvirtintą naudoti programinę įrangą;
 - 7.5. įrangai komunikuojant su blogos reputacijos išoriniais šaltiniais.
8. Turi būti vykdoma kompiuterinio tinklo srauto analizė (Incidentų identifikavimas kibernetinio saugumo analitikų turi būti vykdomas nuo 08.00 val. iki 17.00 val. darbo dienomis):
 - 8.1. kompiuterinio tinklo srautas nukreipiamas naudojant „port mirroring“ arba „network tap“ technologijas.

9. Kompiuterinio tinklo srauto analizės metu realiuoju laiku turi būti identifikuojama:
 - 9.1. neteisėta komunikacija su blogos reputacijos išorės šaltiniais;
 - 9.2. vidinės komunikacijos grėsmės;
 - 9.3. DNS, SMTP, HTTP protokolų rizikos;
 - 9.4. HTTPS srauto patikimumas pagrįstas sertifikatų ir IP adresų vertinimu;
 - 9.5. pateikiama vidinio tinklo įrenginių (tarnybinių stočių, kompiuterinių darbo vietų, potinklių ir kt.) išsklotinė ir ataskaita pagal Perkančiojo subjekto pageidaujamus kriterijus;
 - 9.6. paslaugų trikdymo atakos (angl. DDOS);
 - 9.7. komunikacijos nuokrypiai nuo įprastos įrangos ar naudotojų veikos;
 - 9.8. neatnaujinta ir pažeidžiama programinė įranga, naudojanti komunikaciją su išoriniais šaltiniais ir debesijos paslaugomis;
 - 9.9. Duomenų perdavimo per tinklą aptikimas ir jų analizė (angl. file extraction and analysis), įskaitant kenkėjiškų duomenų identifikavimą;
 - 9.10. komunikacijos su Command and Control (C2) serveriais aptikimas pagal žinomus elgsenos modelius arba IOC (Indicators of Compromise);
 - 9.11. tinklo įrangos ar paslaugų skenavimo veiklos (angl. port scanning, service enumeration) aptikimas;
 - 9.12. neautorizuotos įrangos prisijungimas prie tinklo ir jos identifikacija (pvz., MAC/IP adresų anomalijos);
 - 9.13. netipinių protokolų arba užmaskuoto srauto (angl. tunneling) naudojimo aptikimas;
 - 9.14. prieigos prie jautrių sistemų ar paslaugų iš netipinių šaltinių ar laikų analizė;
 - 9.15. įtartinų prisijungimų bandymų (brute force, credential stuffing) aptikimas;
 - 9.16. Automatinis incidentų klasifikavimas ir prioritetų nustatymas.
10. Grėsmių identifikavimas ir kita galima analitinė veikla:
 - 10.1. nuodugnus duomenų vertinimas pagal kibernetinių grėsmių požymių duomenų bazę;
 - 10.2. turi būti galimybė rinkti ir išsaugoti duomenis PCAP formatu nuo 1 (vienos) dienos iki 3 (trijų) mėnesių (pvz. incidentų tyrimui ir žalos nustatymui), esant poreikiui Perkantysis subjektas įsipareigoja skirti reikiamus techninius resursus savo duomenų centre (15.3 punktą);
 - 10.3. automatizuoti pranešimai el. paštu apie kibernetinės grėsmes bei incidentus teikiami 24/7/365 pagal įjungtas taisykles;
 - 10.4. statistinių duomenų mėnesiniai pranešimai ir aptarimas;
 - 10.5. automatinis kibernetinių grėsmių požymių (IOC) koreliavimas su realiuoju laiku gaunamu srautu ir žurnaliniais įrašais (angl. log correlation);
 - 10.6. grėsmių klasifikavimas pagal CVE identifikatorius, MITRE ATT&CK taksonomiją ar kitus standartus;
 - 10.7. pajėgumas vykdyti retrospektyvinę analizę panaudojant PCAP, žurnalinį įrašų bei metaduomenų koreliaciją (angl. retrospective threat hunting);
 - 10.8. galimybė vykdyti paiešką pagal IOC (hash, domenas, IP, URI) visame surinktame istoriniame duomenų rinkinyje;
 - 10.9. galimybė naudoti užklausų kalbas (pvz., Splunk Search Processing Language – SPL, Ariel Query Language – AQL, Kusto Query Language – KQL, Kibana KQL, Elasticsearch DSL), siekiant analizuoti ir filtruoti didelius duomenų kiekius;
 - 10.10. palaikoma grėsmių žvalgybos (Threat Intelligence) integracija su išoriniais šaltiniais (pvz., MISP, AbuseIPDB, AlienVault OTX ir kt.);
 - 10.11. grėsmių medžioklės (Threat Hunting) galimybės remiantis pasirenkamomis hipotezėmis, filtravimu ir koreliacija;
 - 10.12. automatinis įtartinės veiklos vizualizavimas ir įvykių sekų rekonstrukcija (pvz., laiko juostos, srautų grafai, pivot galimybės);
 - 10.13. galimybė naudoti pasirinktines taisykles (pvz., Sigma, YARA, Suricata) grėsmių detekcijai ir analitškai tobulinti;
 - 10.14. vartotojo ar įrenginio elgsenos anomalijų nustatymas (UEBA);

- 10.15. galimybė vykdyti pasirinktinius duomenų eksportus tyrimams ar integracijoms su kitomis sistemomis (pvz., JSON, CSV, PDF ataskaitos).
- 11. Turi būti vykdomas kompiuterinių tinklų ir informacinių sistemų pažeidžiamumų aptikimas:
 - 11.1. identifikuojami informacinių išteklių pažeidžiamumai, kurie galėtų būti išnaudoti vidinės atakos arba išorinio įsibrovimo atveju;
 - 11.2. nustatomi pažeidžiamumai ir įvertinamas jų kritiškumas;
 - 11.3. reguliarus ekspertinis vertinimas, pokyčių analizė;
 - 11.4. pažeidžiamumų skenavimo pritaikymas infrastruktūrai (konfigūracijų nustatymas, Windows OS, Linux OS, tinklo įranga, aplikacijos ir kita.);
 - 11.5. rekomendacijos nustatytų pažeidžiamumų pašalinimui.
- 12. Esant faktiniam poreikiui (pagal Perkančiojo subjekto užsakymą) atlikti kibernetinio incidento nuodugnų tyrimą ir pateikti ataskaitą pirkimo sutarties vykdymo laikotarpiu.

13. Reakcijos laikai Paslaugoms (toliau – **SLA**¹) nuo 08.00 val. iki 17.00 val. darbo dienomis:

1 lentelė

Informacijos apskaitimo objektas	Grėsmės kritiškumo apibūdinimas pagal naudojamą įrangos nustatymus	Identifikavimo laikas (Time to detect (TTD))	Pranešimo Perkančiajam subjektui laikas (Time to report to NOC (TTR))	Atitikimas sąlygoms Service level target (SLT)	Komunikacijos kanalas
1	2	3	4	5	6
<p>Nustatomi pažeidžiamumai ar identifikuojamos rizikos/grėsmės, kurias būtina nedelsiant spręsti ir imtis konkrečių veiksmų</p> <p>(angl. <i>security monitoring and automated alerting for high severity alerts</i>)</p>	≥ 8	Kritinis arba Aukštas	1 val.	2 val.	95 %
	5–8	Vidutinis	3 val.	6 val.	
	≤ 5	Žemas	8 val.	16 val.	
					<p>Pranešimas el. paštu</p> <p><i>(laiškas su užduotimi imtis neatidėliotinių veiksmų, arba, pagal galimybes, atsakingi asmenys informuojami trumpąja žinute (sms) telefonu)</i></p> <p>Informacija (.xls failas) teikiama kartu su mėnesine Paslaugų teikimo ataskaita</p>

14. Tiekėjas suteikia visą stebėjimui reikalingą programinę įrangą ir reikalingas licencijas Paslaugoms teikti. Tiekėjo su Paslaugomis suteikiama programinė įranga, kuri turi apdoroti ne mažiau kaip 2000 aktyvių IP adresų ir ne mažiau kaip **5 000 EPS (Events per second) ir 750 00 FPM (Flows per minutę)**.
15. Programinė įranga:
- 15.1 gali būti pateikta Tiekėjo ir talpinama Perkančiojo subjekto duomenų centre, suteikiant visas reikalingas licencijas Paslaugoms teikti;
 - 15.2 gali veikti Tiekėjo duomenų centre, esančiame Europos Sąjungos teritorijoje;
 - 15.3 gali būti panaudoti Perkančiojo subjekto turimi resursai (1 fizinis serveris: Xeon CPU 2.6GHz, 128GB RAM, HDD 5TB, Windows server 2019).
16. Paslaugų įdiegimas turėtų būti atliktas per 1 mėn., Paslaugų teikimas – per 2 mėn. nuo pirkimo sutarties įsigaliojimo datos.
17. Paslaugų teikimo trukmė – 12 mėn. nuo sutarties įsigaliojimo datos.
18. Perkančiojo subjekto IT infrastruktūra:
- 18.1. Fizinių/virtualių serverių skaičius – 90 vnt;
 - 18.2. Darbo vietų – 280 vnt;
 - 18.3. Ugniasienių – 26 vnt;
 - 18.4. Tinklo įrangos – 170 vnt;
 - 18.5. EDR sprendimas – Microsoft Cloud Defender 300 vnt.

¹ pasikeitus teisės aktuose (Lietuvos Respublikos Vyriausybės nutarimas „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ 2018–08–13 Nr. 818, Lietuvos Respublikos Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento parengtas Nacionalinis kibernetinių incidentų valdymo planas ar kiti teisės aktai) nustatytiems SLA, 1 lentelėje nurodyti terminai gali būti keičiami atsižvelgiant į nustatytus reikalavimus.

19. Tiekėjas, atsakingas už Paslaugų diegimą ir konfigūravimą pagal šios techninės specifikacijos reikalavimus. Perkančiojo subjekto įrangos konfigūracijos darbus ir agentų instaliaciją atlieka pats Perkantysis subjektas pagal Tiekėjo pateiktas instrukcijas.

III SKYRIUS BENDRI REIKALAVIMAI

20. Vykdomas žaliasis Pirkimas, kadangi perkamoms Paslaugoms taikomos Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto aktualios redakcijos Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1–508 4.4.3 papunkčio nuostatos, t. y. 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. Perkantysis subjektas nustato, kad vykdant pirkimo sutartį visa su Paslaugų teikimu susijusi dokumentacija (pranešimai, ataskaitos ir kt.) turi būti teikiama elektroniniu būdu ir tik esant būtinybei spausdinama, tam naudojant perdirbtą popierių.
21. Programinė įranga, naudojama Paslaugų teikimui, turi atitikti jos gamintojo šalies standartus, gamintojo techninius standartus, Lietuvos Respublikos teisės aktais patvirtintus ir galiojančius standartus, turi būti registruota naudoti Europos Sąjungoje – turėti CE sertifikata.
22. Atsižvelgiant į tai, kad atliekamas pirkimas, kurio objektas atitinka Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 13 dalyje numatyta sąrašą (BVPŽ kodų sąrašas, patvirtintas Lietuvos Respublikos Vyriausybės, įvertinus pirkimo sutarties vykdymo metu galinčias kilti su nacionaliniu saugumu susijusias technologines rizikas) nurodyto BVPŽ kodo paslaugas, Tiekėjas negali siūlyti Paslaugų, kurios kelia grėsmę nacionaliniam saugumui (vadovaujantis Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymo 50 straipsnio 9 dalies nuostatomis). Perkantysis subjektas turi teisę pareikalauti Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos patvirtinimo dėl Tiekėjo pasiūlymo atitikties nacionaliniam saugumui.