SAUGUMO IR ANALITIKOS OPERACIJŲ CENTRO NUOMOS TECHNINĖ SPECIFIKACIJA

1. PIRKIMO OBJEKTAS IR TIKSLAI, BENDRI REIKALAVIMAI

1.1. VšĮ Lietuvos nacionalinis radijas ir televizija (toliau – Perkančioji organizacija) šiuo pirkimu siekia įsigyti saugumo ir analitikos operacijų centro nuomą (toliau – Sprendimas), kurią apima:

1.1.1. programinė įranga, skirta žurnalinių įvykių kaupimui, valdymui ir stebėjimui (toliau – Sistema);

1.1.2. techninė įranga, skirta žurnalinių įvykių saugojimui ir apdorojimui (toliau – Įranga);

1.1.3. Sistemos paruošimas naudojimui;

1.1.4. Sistemos analitika ir kitos Sprendimo naudojimo metu atliekamos veiklos;

1.1.5. Sistemos ir Įrangos aptarnavimas.

1.2. Sprendimo nuomos trukmė - 36 (trisdešimt šeši) mėnesiai, skaičiuojant nuo Techninės specifikacijos 3.7 punkte nurodytos Sprendimo nuomos laikotarpio pradžios. Sprendimas turi veikti nuolat, t. y. be pertraukų ar prastovų.

1.3. Sprendimui keliami tikslai:

1.3.1. išanalizuoti Perkančiosios organizacijos valdomos infrastruktūros, informacinių sistemų ir registrų, kitų informacinių bei stebėjimo sistemų įvykių kaupimą, siekiant panaudoti juos saugai reikšmingų įvykių bei tolimesnių veiksmų nustatymui, pasinaudojant Sprendimu;

1.3.2. efektyviai panaudoti saugos įvykius ir Sprendimą kibernetinių incidentų prevencijai, nustatymui ir kilusių incidentų valdymui, neteisėtos veiklos įrodymų sukaupimui;

1.3.3. kelti Perkančiosios organizacijos darbuotojų kvalifikaciją saugos įvykiais paremtos analizės ir kibernetinių incidentų valdymo srityse.

1.4. Reikalavimai Sprendimui pateikiami šioje Techninėje specifikacijoje.

1.5. Techninėje specifikacijoje vartojamos sąvokos:

1.5.1. **Dokumentacija** – gamintojo dokumentai (vartotojo vadovai, techniniai pasai, gamintojo rašytinis patvirtinimas dėl tiekėjo šiame pirkime siūlomo Sprendimo/ Sistemos atitikimo Techninės specifikacijos reikalavimams ar kita gamintojo teikiama informacija apie prekės/Sprendimo/Sistemos parametrus) arba gamintojo internetinio puslapio nuoroda (-os), kuriuose pateikiama gamintojo informacija apie siūlomos prekės/Sprendimo/Sistemos atitikimą reikalaujamam parametrui / specifikacijai.

1.6. **Bendri reikalavimai tiekėjui dėl Techninės specifikacijos pildymo:**

1.6.1. Tiekėjas turi užpildyti visus Techninės specifikacijos lentelės laukelius, kurie pažymėti „*/įrašyti/*“ (tiekėjas ištrina „*/įrašyti/*“ ir nurodo reikalaujama informaciją). Tiekėjui minėtų laukelių neužpildžius arba užpildžius netinkamai tiekėjo pasiūlymas gali būti atmestas kaip neatitinkantis Pirkimo dokumentų reikalavimų.

1.6.2. Tiekėjas negali palikti tuščių laukelių, kurie pažymėti „*/įrašyti/*“.

1.6.3. Tiekėjas negali keisti Techninės specifikacijos, t. y. tiekėjas negali keisti Techninės specifikacijos teksto (papildyti, trinti ir pan.), papildyti lentelių naujais laukais ar ištrinti esamus, nebent Techninėje specifikacijoje aiškiai nurodyta, kad tokie pakeitimai galimi. Tiekėjui atliktus minėtus pakeitimus, tiekėjo pasiūlymas gali būti atmestas, kaip neatitinkantis Pirkimo dokumentų reikalavimų.

1.7. **Reikalavimai tiekėjui dėl lentelės stulpelio „Siūlomus parametrus patvirtinanti Dokumentacija" pildymo:**

1.7.1. atsakingas už Dokumentacijos pateikimą, kuri patvirtina tiekėjo siūlomos prekės/Sprendimo/Sistemos atitikimą Techninės specifikacijos reikalavimams, tose eilutėse, kuriose nurodyta „/privaloma pateikti/" – vietoje „/privaloma pateikti/" nurodydamas prie pasiūlymo pridedamo dokumento pavadinimą / bylos pavadinimą arba nuorodą į konkretų internetinį puslapį. Perkančioji organizacija aktyviai neieškos ir netikrins Dokumentacijos (tačiau tai neatima teisės iš Perkančiosios organizacijos, kilus įtarimui dėl Dokumentacijos pateiktos informacijos teisingumo, pasitikrinti atitikimą) ir tikrins tik Tiekėjo kartu su pasiūlymu pateiktą Dokumentaciją, jeigu Tiekėjo pateikta Dokumentacija nepatvirtins atitikimo keliamam reikalavimui, o Tiekėjas nepaaiškins Techninės specifikacijos 1.8 punkte nustatyta tvarka, kaip tiekėjo siūloma prekė/Sprendimas/Sistema atitinka keliamą reikalavimą arba Tiekėjas su pasiūlymu iš viso nepateiks Dokumentacijos – Tiekėjo pasiūlymas ~~bus~~ gali būti atmestas;

1.8. Tiekėjas, vadovaujantis Bendrųjų pirkimo sąlygų 17.4 punktu, Techninėje specifikacijoje lentelės stulpelyje „Tiekėjo laisvos formos aprašymas apie siūlomą Sistemą, iš kuriame pateiktos informacijos Perkančioji organizacija galėtų įsitikinti Tiekėjo siūlomos Sistemos atitiktimi reikalavimui, nustatytam nurodytame Techninės specifikacijos punkte" arba lentelės stulpelyje „Siūlomus parametrus patvirtinanti Dokumentacija" nurodytą informaciją galės paaiškinti tik tuo atveju, jeigu:

1.8.1. Tiekėjas kartu su pasiūlymu pateikė Dokumentaciją ir pateiktoje Dokumentacijoje yra nurodyta informacija patvirtinanti, kad tiekėjo siūloma prekė/Sprendimas/Sistema atitinka Techninėje specifikacijoje nurodytus reikalavimus;

1.8.2. Tiekėjas pateiks paaiškinimą iš viešai prieinamos siūlomos prekės/Sprendimo/Sistemos gamintojo informacijos arba gamintojo patvirtinimą, kad tiekėjo siūloma prekė/Sprendimas/Sistema atitinka Techninėje specifikacijoje nurodytus reikalavimus.

1.9. Dokumentacija turi būti parengta prekės/Sprendimo/Sistemos gamintojo, o ne trečiųjų šalių. Jeigu prekė sudaryta iš kitų gamintojų įrangos ar dalių gali būti teikiama tiek galutinės prekės, tiek prekės komplektuojančios dalies gamintojo Dokumentacija.

1.10. Lentelėje tiekėjas prie konkretaus reikalavimo nurodo, kuri tiekėjo su pasiūlymu teikiama Dokumentacija patvirtina atitikimą nurodytam konkrečiam reikalavimui.

~~1.9.~~1.11. Perkančioji organizacija prašo tiekėjų, kad nurodant Dokumentacijos pavadinimą, kartu būtų pateikiama nuoroda į konkretų puslapį, paragrafą ir pan., kai tai yra įmanoma, sklandesniam tiekėjų pasiūlymų vertinimui.

2. INFORMACIJA APIE PIRKIMO KONTEKSTĄ

2.1. Perkančioji organizacija Sprendimo pagalba planuoja rinkti ir analizuoti žurnalinius įrašus, sistemų žurnalus (angl. syslog) ir kitus kompiuterinės, programinės bei tinklo įrangos kuriamus pranešimus iš tokio kiekio ir tipo šaltinių:

2.1.1. kompiuterizuotos darbo vietos:

2.1.1.1. iki 1000 vnt. kompiuterizuotų darbo vietų su Windows 11 arba Windows 10 operacinėmis sistemomis bei Microsoft 365 programine įranga su E3 ir E1 licencijomis;

2.1.1.2. iki 40 vnt. kompiuterizuotų darbo vietų su MacOS operacine sistema bei Microsoft 365 programine įranga su E3 ir E1 licencijomis;

2.1.2. iki 350 fizinių ir virtualių serverių, iš kurių:

2.1.2.1. iki 250 vnt. serverių su Windows Server programine įranga;

2.1.2.2. iki 100 vnt. serverių su Linux operacinėmis sistemomis;

2.1.3. programinė įranga:

2.1.3.1. iki 900 vnt. Microsoft 365 E5 Security (MS Defender) licencijų;

2.1.3.2. iki 250 vnt. Trend Micro licencijų;
2.1.3.3. iki 30 vnt. MS SQL, Oracle, MySQL ir kitų duomenų bazių serverių;
2.1.4. tinklų valdymo įrenginiai:
2.1.4.1. iki 15 vnt. Fortigate, CheckPoint ugniasienių;
2.1.4.2. iki 120 vnt. Cisco ir HP, Fortinet komutatorių;
2.1.4.3. iki 120 vnt. Cisco, Fortinet bevielio interneto prieigos taškų.
2.1.5. Microsoft Office 365 žurnaliniai įrašai (Exchange online, MS Entra ID, MS defender ir kiti Microsoft Office 365 ir Azure infrastruktūros žurnaliniai įrašai);
2.1.6. Šiuo metu nuomojamas SIEM Sprendimas, kuris remiasi Logrhythm programinės įrangos pagrindu. Esamas sprendimas paskaičiuotas apdoroti ne mažiau kaip 10000 pranešimų per sekundę (angl. messages per second, MPS) ir kaupti duomenis ne trumpiau kaip 3 mėn. Tiekėjas gali siūlyti Sprendimą, kuris remiasi Logrhythm programinės įrangos ar jai lygiavertės programinės įrangos pagrindu.

3. BENDRIEJI REIKALAVIMAI

3.1. Ne vėliau kaip 5 darbo dienas nuo pirkimo sutarties įsigaliojimo Tiekėjas turi parengti ir su Perkančiąja organizacija suderinti Sprendimo įgyvendinimo kalendorinį grafiką (planą). Bet kokie grafiko pasikeitimai turi būti derinami iš anksto su Perkančiąja organizacija.
3.2. Ne vėliau kaip per 10 darbo dienų nuo pirkimo sutarties įsigaliojimo Tiekėjas turi parengti ir pateikti Perkančiajai organizacijai suderinimui:
3.2.1. Esamos situacijos analizės (šiuo metu nuomojamas SIEM sprendimas Logrhythm pagrindu), projektavimo ir diegimo plano dokumentaciją;
3.2.2. Duomenų ir taisyklių perkėlimo iš Perkančiosios organizacijos naudojamos Logrhythm žurnalinių įrašų kaupimo ir analizės sistemos į naują Sprendimą planą ~~į naują Sprendimą~~;
3.2.3. komunikacijos planą, kuriame apibrėžiami:
3.2.3.1. Tiekėjo ir Perkančiosios organizacijos atstovų kontaktai;
3.2.3.2. komunikacijos veiksmai įvykus incidentui ar duomenų surinkimo arba analitikos atlikimo sutrikimui;
3.2.3.3. kanalai, kuriais vyks informavimas apie incidentus, bus komunikuojama sprendžiant Sprendimo veikimo sutrikimus.
3.3. Ne vėliau kaip per 5 darbo dienas Perkančioji organizacija įvertina Tiekėjo pagal Techninės specifikacijos 3.2 punktą pateiktus dokumentus ir juos suderina arba pateikia pastabas dėl jų patikslinimo per Tiekėjo ir Perkančiosios organizacijos sutartą terminą. Atsižvelgiant į vertinimui pateiktų dokumentų apimtį, vertinimo/suderinimo terminas gali būti ilgesnis.
3.4. Ne vėliau kaip per 20 darbo dienų nuo Sistemos diegimo etapo pabaigos Tiekėjas turi parengti ir pateikti Perkančiajai organizacijai incidentų valdymo proceso aprašymą.
3.5. Ne vėliau kaip per 10 darbo dienų nuo Sistemos migravimo ir Sistemos derinimo etapų pabaigos turi parengti ir pateikti Perkančiajai organizacijai realizuotų Sistemos integracijų dokumentaciją.
3.6. Techninės specifikacijos 3.1., 3.2, 3.4 ir 3.5 punktuose nurodyti dokumentai rengiami ir pateikiami Perkančiajai organizacijai lietuvių arba anglų kalba elektroniniu formatu[1].

[1] Šis reikalavimas yra aplinkos apsaugos kriterijus, nustatytas pagal Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 (Lietuvos Respublikos aplinkos ministro 2022 m. gruodžio 13 d. įsakymo Nr. D1-401 redakcija) patvirtinto Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo 4.4.4.1 punktą, nes dokumentų nespausdinant, o juos rengiant ir naudojant elektroniniu formatu yra taupomi ištekliai.

3.7. Sprendimo paruošimas naudojimui atliekamas Techninėje specifikacijoje nustatyta tvarka ir terminais. Sprendimo nuoma prasideda nuo Sistemos diegimo etapo pabaigos ir Sprendimui skirtų licencijų perdavimo Perkančiajai organizacijai, bet ne anksčiau kaip nuo 2025-12-15. Licencijos turi būti užregistruotos Perkančiosios organizacijos vardu gamintojo licencijavimo sistemoje arba kitoje sistemoje, įrodančioje, kad Sprendimas yra paremtas teisėtomis licencijomis ir Perkančiajai organizacijai ateityje nekils teisinių pasekmių dėl neteisėto Sprendimą sudarančių komponenčių naudojimo. Apie tokį registravimą licencijų perdavimo metu Perkančioji organizacija turi gauti raštišką gamintojo patvirtinimą arba Perkančiajai organizacijai turi būti suteikta prieiga prie gamintojo licencijavimo sistemos, kur tokia registracija turi būti matoma.

3.8. Tiekėjas turi užtikrinti, kad atliekant Sistemos diegimą ir duomenų, taisyklių perkėlimą iš Perkančiosios organizacijos naudojamos Loghrythm sistemos į naują Sprendimą nebus sutrikdomas Perkančiosios organizacijos programinės ir techninės įrangos infrastruktūros darbas. Jeigu Perkančiosios organizacijos infrastruktūros darbas bus trikdomas, numatomi Sistemos diegimo darbai turi būti atliekami Perkančiosios organizacijos ne darbo metu (darbo dienomis 17:00 - 5:00 val., nedarbo dienomis 9:00-20:00 val.) ir suderinus su Perkančiosios organizacijos atsakingu už pirkimo sutarties vykdymą asmeniu.

3.9. Bendravimas tarp Perkančiosios organizacijos ir Tiekėjo vykdomas lietuvių arba anglų kalba arba turi būti užtikrintas vertimas į minėtas kalbas Tiekėjo sąskaita.

3.10. Perkančiajai organizacijai pareikalavus, paskutinę Sprendimo nuomos dieną Tiekėjas turi perduoti Perkančiajai organizacijai Sprendimo nuomos laikotarpiu parengtus taisyklių aprašus bei paskutinių 3 (trijų) nuomos mėnesių laikotarpyje surinktus žurnalinių įvykių ir incidentų duomenis. Jeigu Perkančioji organizacija minėtų taisyklių aprašų ir duomenų perdavimo nepareikalauja, paskutinę Sprendimo nuomos dieną jie turi būti sunaikinti.

3.11. Tiekėjas kartu su pasiūlymu turi pateikti:

3.11.1. **užpildytą** žemiau nurodytą lentelę ir

3.11.2. **Dokumentaciją**, kuri patvirtina tiekėjo siūlomos sistemos atitikimą ~~Techninės specifikacijos~~ reikalavimams, nurodytiems Techninės specifikacijos 4.2.1.1, 4.2.1.2, 4.5.2, 4.5.3, 4.6.1, ~~4.6.2,~~ 4.6.6, 4.6.7. 4.6.8, 4.6.9, 4.9.2.1, 4.9.2.2, 4.9.2.3, 4.9.2.4, 4.10.2, 4.11.1, 4.12.1, 4.12.2, 4.12.3, 4.12.5 punktuose, ~~taip pat priklausomai nuo to, ar tiekėjo siūloma sistema turi agentais ir/arba kolektoriais paremtą įvykių surinkimą atitikimą reikalavimams, nurodytiems 4.7.1.1, 4.7.1.2, 4.7.1.4.1, 4.7.1.4.2, 4.7.1.4.3, 4.7.1.4.4, 4.7.1.4.5 ir/arba 4.8.1.3.1, 4.8.1.3.2, 4.8.1.3.3 punktuose~~.

Lentelė

Informacija apie siūlomą Sistemą:			
Sistemos pavadinimas		*/įrašyti/*	
Sistemos gamintojas		*/įrašyti/*	
Sistemai skirtų licencijų sąrašas		*/įrašyti, nurodyti licencijų kiekį bei licencijavimo būdą, jeigu toks egzistuoja/*	
Eil. Nr.	**Reikalavimai, nustatyti nurodyta me**	**Tiekėjo laisvos formos aprašymas apie siūlomą Sistemą, iš kuriame pateiktos informacijos Perkančioji organizacija galėtų įsitikinti Tiekėjo siūlomos Sistemos atitiktimi reikalavimui,**	**Siūlomus parametrus patvirtinanti Dokumentacija**

	Techninės specifikacijos punkte	**nustatytam nurodytame Techninės specifikacijos punkte**	
1.	4.2.1.1 punktas	*/įrašyti/*	*/privaloma pateikti/*
2.	4.2.1.2 punktas	*/įrašyti/*	*/privaloma pateikti/*
3.	4.5.2 punktas	*/įrašyti/*	*/privaloma pateikti/*
4.	4.5.3 punktas	*/įrašyti/*	*/privaloma pateikti/*
5.	4.6.1 punktas	*/įrašyti/*	*/privaloma pateikti/*
6.	~~4.6.2 punktas~~		~~*/privaloma pateikti/*~~
7.	4.6.6 punktas	*/įrašyti/*	*/privaloma pateikti/*
8.	4.6.7 punktas	*/įrašyti/*	*/privaloma pateikti/*
9.	4.6.8 punktas	*/įrašyti/*	*/privaloma pateikti/*
10.	4.6.9 punktas	*/įrašyti/*	*/privaloma pateikti/*
11.	4.9.2.1 punktas	*/įrašyti/*	*/privaloma pateikti/*
12.	4.9.2.2 punktas	*/įrašyti/*	*/privaloma pateikti/*

13.	4.9.2.3 punktas	/įrašyti/	/privaloma pateikti/
14.	4.9.2.4 punktas	/įrašyti/	/privaloma pateikti/
15.	4.10.2 punktas	/įrašyti/	/privaloma pateikti/
16.	4.11.1 punktas	/įrašyti/	/privaloma pateikti/
17.	4.12.1 punktas	/įrašyti/	/privaloma pateikti/
18.	4.12.2 punktas	/įrašyti/	/privaloma pateikti/
19.	4.12.3 punktas	/įrašyti/	/privaloma pateikti/
20.	4.12.5 punktas	/įrašyti/	/privaloma pateikti/
~~**Jeigu tiekėjo siūloma Sistema turi agentais paremtą įvykių surinkimą, tuomet tiekėjas pateikia žemiau siūlomus parametrus patvirtinančią Dokumentaciją**~~			
21.	~~4.7.1.1 punktas~~		~~/privaloma pateikti, jeigu siūlomas sprendimas apima sistemą, kuri turi agentais paremto įvykių surinkimą/~~
22.	~~4.7.1.2 punktas~~		~~/privaloma pateikti, jeigu siūlomas sprendimas apima sistemą, kuri turi agentais~~

			~~paremto įvykių surinkimą/~~
23.	~~4.7.1.4.1 punktas~~		~~/privaloma pateikti, jeigu siūlomas sprendimas apima sistemą, kuri turi agentais paremto įvykių surinkimą/~~
24.	~~4.7.1.4.2 punktas~~		~~/privaloma pateikti, jeigu siūlomas sprendimas apima sistemą, kuri turi agentais paremto įvykių surinkimą/~~
25.	~~4.7.1.4.3 punktas~~		~~/privaloma pateikti, jeigu siūlomas sprendimas apima sistemą, kuri turi agentais paremto įvykių surinkimą/~~
26.	~~4.7.1.4.4 punktas~~		~~/privaloma pateikti, jeigu siūlomas sprendimas apima sistemą, kuri turi agentais paremto įvykių surinkimą/~~
27.	~~4.7.1.4.5 punktas~~		~~/privaloma pateikti, jeigu siūlomas sprendimas apima sistemą, kuri turi agentais paremto įvykių surinkimą/~~

~~**Jeigu Sistema turi kolektoriais paremtą įvykių surinkimą, tuomet tiekėjas pateikia žemiau siūlomus parametrus patvirtinančią Dokumentaciją**~~			
28.	~~4.8.1.3.1 punktas~~		~~/privaloma pateikti, jeigu siūlomas sprendimas apima sistemą, kuri turi kolektoriais paremto įvykių surinkimą/~~
29.	~~4.8.1.3.2 punktas~~		~~/privaloma pateikti, jeigu siūlomas sprendimas apima sistemą, kuri turi kolektoriais paremto įvykių surinkimą/~~
30.	~~4.8.1.3.3 punktas~~		~~/privaloma pateikti, jeigu siūlomas sprendimas apima sistemą, kuri turi kolektoriais paremto įvykių surinkimą/~~

3.12. Tiekėjas Sprendimo nuomos laikotarpiui turi suteikti visą Sprendimo veikimui, įskaitant Sistemos talpinimui bei žurnalinių įvykių ir incidentų saugojimui ir apdorojimui, reikalingą Įrangą bei vykdyti jos aptarnavimą bei gedimų šalinimą. Reikalavimai įrangos talpinimui pateikti 4.17.1 punkte. Jei pateiktai įrangai sutarties laikotarpiu reikalingi pakeitimai, atnaujinimai, resursų išplėtimai, tai atlieka Tiekėjas savo sąskaita.

4. REIKALAVIMAI SISTEMAI

4.1. Visa Sistemos programinė įranga turi būti to paties gamintojo arba kelių gamintojų suderinama bendram darbui.

4.2. *Sistemos komponentai:*

4.2.1. Sistema turi turėti tokius komponentus:

4.2.1.1. žurnalinių įvykių kaupimo ir valdymo komponentą;

4.2.1.2. naudotojų elgesio analizės komponentą.

4.2.2. Sistemai turi būti pateiktos visos reikalingos licencijos šių komponentų įgyvendinimui.

4.3. *Sistemos našumas:*

4.3.1. Sistema turi gebėti nepertraukiamai (angl. sustained) apdoroti ne mažiau nei 10 000 įvykių per sekundę (angl. messages per second, MPS). Prognozuojamas minimalus 1 000 įvykių per sekundę srautas, kuris gali siekti 10 000 įvykių per sekundę darbo piko metu.

4.4. *Įvykių įrašų vientisumas:*

4.4.1. Sistema turi užtikrinti sisteminių įrašų vientisumą.

4.5. *Įvykių šaltiniai:*

4.5.1. Sistema turi kaupti ir apdoroti įvykių žurnalus (angl. event logs) iš Perkančiosios organizacijos infrastruktūros bei įrangos, nurodytos Techninės specifikacijos 2 punkte. Įvykių žurnalų duomenys turi būti saugomi ne trumpiau kaip 36 ~~6~~ mėn., pasibaigus saugojimo terminui turi būti sunaikinami. Jei Sistemoje, sutarties laikotarpiu, yra nepanaudotų diskinių resursų, Perkančioji organizacija be papildomo mokesčio gali Tiekėjo prašyti padidinti įvykių žurnalų saugojimo laikotarpį.

4.5.2. Sistema turi surinkti saugumo informacijos įvykius (angl. events) arba įvykių žurnalus (angl. event logs) iš tinklo įrangos, tinklo perimetro saugos įrenginių, taikomųjų sistemų, įskaitant operacines sistemas, duomenų bazių valdymo sistemų, taikomųjų programinės įrangos sistemų, antivirusinių programų, Office 365, Azure.

4.5.3. Sistema be papildomo konfigūravimo turi atpažinti ir normalizuoti ne mažiau kaip 170 komercinių ir atviro kodo duomenų šaltinių.

4.6. *Įvykių surinkimas:*

4.6.1. Sistema turi surinkti įvykius tiek užklausdama duomenų šaltinius, tiek iš duomenų šaltinių, kurie patys siunčia įvykius.

4.6.2. Sistema turi surinkti įvykius panaudojant programinius agentus ir/arba kolektorius ir/arba kitus lygiaverčius (be agentų ir/arba kolektorių pagalbos) metodus. Renkant duomenis iš šaltinių, naudojančių MacOS operacines sistemas, galimas duomenų rinkimo metodas, nesinaudojant agentais arba kolektoriais.

4.6.3. Sistema turi pasiimti informaciją iš Microsoft Active Directory domeno, t. y. turi ištraukti informaciją apie vartotojus, matyti vartotojo turimą el. pašto adresą, pilną naudotojo vardą.

4.6.4. Įvykiai, renkami sisteminio agento pagalba, turi būti perduodami šifruotais duomenų srautais.

4.6.5. Sisteminiai įrašai turi būti suglaudinti, juos perduodant iš įvykių surinkimo komponento į Sistemą.

4.6.6. Turi būti funkcionalumas perduodamus įvykius perduoti saugiais kanalais, tokiais kaip TLS ar lygiaverčiais.

4.6.7. Sistema turi palaikyti įvykių perdavimo formatą Syslog.

4.6.8. Sistema turi pasiimti ir apdoroti standartinius ir nestandartinius įvykius, saugomus Windows Event Log.

4.6.9. Sistema turi palaikyti šiuos įvykių formatus: CEF (angl. common event format), SYSLOG.

4.6.10. Sistema turi surinkti įvykius iš Microsoft Office 365 aplinkoje esančių skirtingų aplinkų šaltinių (Intune, Exchange, Entra ID, Security ir t.t.). Jei tokių įvykių surinkimui ar integracijai reikalingos papildomos licencijos, tokios licencijos turi būti įskaičiuotos į bendrą pasiūlymo kainą

4.7. *Agentais paremtas įvykių surinkimas:*

4.7.1. Jeigu Sistema turi agentais paremto įvykių surinkimą, tada ji turi atitikti šiuos reikalavimus:

4.7.1.1. Turi būti funkcionalumas sistemos agentus diegti Windows ir Linux operacinėse sistemose.

4.7.1.2. Sistema turi palaikyti SSL arba TLS šifravimą perduodamiems duomenims.

4.7.1.3. Turi būti užtikrintas laiko žymos normalizavimas.

4.7.1.4. Agentais paremtas įvykių surinkimas turi leisti surinkti tokius įvykius:

4.7.1.4.1. Syslog;

4.7.1.4.2. UDP/TCP ir saugų Syslog;

4.7.1.4.3. Flat bylas (viena eilute ir daugeliu eilučių, suglaudintas ir nesuglaudintas bylas);

4.7.1.4.4. Windows sisteminius įvykius, saugumo ir audito žurnalo įvykius, įtraukiant ir individualius žurnalinius įvykius;

4.7.1.4.5. Microsoft Exchange message tracking žurnalinius įrašus.

4.7.1.5. Turi būti pateikta ne mažiau kaip 1 000 aukščiau nurodyto funkcionalumo agentų / licencijų arba sistema turi gebėti surinkti Techninės specifikacijos 4.7.1.4 punkte nurodytus duomenis be agentų pagalbos arba dalį duomenų surinkti su agentais, dalį – kitomis priemonėmis (jei reikalingos kitos programinės įrangos licencijos ar įrenginiai, jos/jie turi būti įskaičiuoti į pasiūlymo kainą).

4.8. *Kolektoriais paremtas įvykių surinkimas:*

4.8.1. Jeigu Sistema turi kolektoriais paremto įvykių surinkimą, tada ji turi atitikti šiuos reikalavimus:

4.8.1.1. Turi būti užtikrintas laiko žymos normalizavimas.

4.8.1.2. Įvykiai ir incidentai taip pat turi būti renkami ir iš Perkančiosios organizacijos valdomos Microsoft 365 infrastruktūros (Azure AD, Exchange online, Defender, Security center ir kt. programinės įrangos).

4.8.1.3. Kolektoriais paremtas įvykių surinkimas turi leisti surinkti tokius įvykius:

4.8.1.3.1. Syslog;

4.8.1.3.2. UDP/TCP ir saugų Syslog;

4.8.1.3.3. Windows sisteminius įvykius, įtraukiant ir individualius žurnalinius įvykius.

4.8.1.4. Su siūloma sistema turi būti pateikta ne mažiau kaip 1 000 aukščiau nurodyto funkcionalumo kolektorių/ licencijų arba sistema turi gebėti surinkti Techninės specifikacijos 4.8.1.3 punkte nurodytus duomenis be kolektorių pagalbos arba dalį duomenų surinkti su kolektoriais, dalį – kitomis priemonėmis (jei reikalingos kitos programinės įrangos licencijos ar įrenginiai, jos/jie turi būti įskaičiuoti į pasiūlymo kainą).

4.9. Naudotojų elgesio analizės komponento funkcionalumas:

4.9.1. Sistema turi turėti naudotojų elgesio analizės komponento funkcionalumą.

4.9.2. Naudotojų elgesio analizės funkcionalumas turi gebėti:

4.9.2.1. analizuoti standartinę naudotojų veiklą ir aptikti joje atsirandančias anomalijas;

4.9.2.2. aptikti pavogtas, kompromituotas naudotojų paskyras;

4.9.2.3. aptikti kenkėjiškas vidines grėsmes (angl. maliciuos insider threats);

4.9.2.4. aptikti brutalios jėgos atakas.

4.9.3. Įvykiai ir incidentai taip pat turi būti renkami ir iš Perkančiosios organizacijos valdomos Microsoft 365 infrastruktūros (Azure AD, Exchange online, Defender, Security center) ir įtraukiami į bendrą įvykių laiko juostą (angl. timeline). Turi būti atliekama minėtų įvykių ir incidentų analizė bei koreliacija.

4.10. Įvykių valdymas:

4.10.1. Sistema be papildomo programavimo turi atlikti surinktų įvykių įrašų normalizavimą sistemoje formuojant įvykius (angl. events).

4.10.2. Sistema turi normalizuoti įvykių įrašus, pagal sistemos laiko juostą.

4.11. Nuotolinė prieiga peržiūrai:

4.11.1. Privalo būti realizuota, Perkančiajai organizacijai skirta, saugi duomenų peržiūros grafinė sąsaja (angl. GUI), apsaugota HTTPS arba SSL protokolais.

4.12. Analitikos funkcionalumas:

4.12.1. Sistema turi leisti atlikti detalią įvykių analizę pagal laiko intervalus, pvz.: per minutę, dieną, savaitę.

4.12.2. Sistema turi gebėti automatiškai nustatyti grėsmes, pagal įtartinus elgesio modelius.

4.12.3. Sistema turi apdoroti naudotojų vardus, pvz.: atskirti naudotojo vardą iš Microsoft Active Directory domeno informacijos.

4.12.4. Sistema turi atnaujinti analitikos taisykles, skirtas naujoms grėsmėms aptikti.

4.12.5. Sistema turi gebėti informuoti apie pastebėtas grėsmes atsakingus darbuotojus SMTP arba analogišku protokolu.

4.12.6. Sistema turi gebėti informuoti Perkančiąją organizaciją apie grėsmes, siunčiant pranešimus į Perkančiosios organizacijos valdomą pagalbos tarnybos sistemą (el. paštu ar kitomis priemonėmis).

4.13. Įvykių koreliavimas:

4.13.1. Sistema turi gebėti koreliuoti ne mažiau nei 10 000 įvykių per sekundę. Prognozuojamas minimalus 1 000 įvykių per sekundę srautas, kuris gali siekti 10 000 įvykių per sekundę darbo piko metu.

4.13.2. Sistema turi turėti ne mažiau kaip 200 gamintojo parengtų ir įdiegtų koreliavimo taisyklių, kurios Sistemos derinimo metu gali būti pritaikytos Perkančiosios organizacijos infrastruktūrai.

4.13.3. Sistema turi atlikti kelių skirtingų įvykių, įvykusių per tam tikrą laiko tarpą, taisyklėmis paremtą koreliavimą.

4.13.4. Sistema turi vykdyti koreliavimą įvykių, surinktų iš skirtingų įrenginių tipų ir skirtingų gamintojų.

4.14. Įkalčių rinkimas:

4.14.1. Sistema turi leisti priskirti surinktus įkalčius (įspėjimus, įvykius, išorinius duomenis, pastabas) prie sukurto incidento.

4.14.2. Incidentų duomenys turi būti saugomi ne trumpiau nei 6 mėn., pasibaigus saugojimo terminui turi būti sunaikinami (esant poreikiui turi būti eksportuojami į kitą Perkančiosios organizacijos pateiktą laikmeną).

4.15. Geolokacija:

4.15.1. Sistema turi rodyti šalį, susietą su paskirties ir šaltinio IP adresu kiekvienam įvykiui.

4.16. Įspėjamieji įvykiai (angl. alarm):

4.16.1. Sistema turi leisti kurti įspėjamuosius įvykius, pagal sistemos sugeneruotus įvykius.

4.16.2. Sistema turi generuoti įspėjamųjų įvykių ataskaitas.

4.16.3. Sistema turi gebėti siųsti įspėjamąjį įvykį elektroniniu laišku.

4.17. Duomenų saugojimas:

4.17.1. Visi Sprendimo surenkami ir Sprendime naudojami Perkančiosios organizacijos bei jos infrastruktūros duomenys turi būti saugomi Įrangoje, esančioje Perkančiosios organizacijos duomenų centre arba Lietuvos, Europos sąjungos ar NATO šalių teritorijoje esančiame duomenų centre. Tiekėjui pageidaujant Perkančioji organizacija Įrangos talpinimui gali suteikti vietą savo duomenų centre Vilniuje. Įrangos talpinimui Perkančioji organizacija savo duomenų centre esančioje standartinėje 19" (ang. „rack-mount") spintoje suteiktų ne daugiau kaip 10 U aukščio vietos. Taip pat būtų suteikiama galimybė prisijungti prie Perkančiosios organizacijos elektros tinklo bei interneto. Tiekėjas į pasiūlymo kainą turi įskaičiuoti visus Įrangos, jos komponentų bei sumontavimui ir pajungimui prie Perkančiosios organizacijos tinklo sąnaudas. Tiekėjas įsipareigoja neatskleisti jokių su Perkančiosios organizacijos infrastruktūra ir Sprendimu susijusių duomenų trečiosioms šalims.

4.18. Garantinis *aptarnavimas Sprendimo nuomos laikotarpiui:*

4.18.1. Turi būti užtikrintas Tiekėjo teikiamas Sistemos garantinis aptarnavimas visam Sprendimo nuomos laikotarpiui.

4.18.2. Sistemos garantinio aptarnavimo laikotarpiu turi būti užtikrinta:

4.18.2.1. Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnės programinės įrangos versijas). Tiekėjas atsako už visos Sistemos naujumą, techninę priežiūrą ir aptarnavimą. Jei sutarties laikotarpiu bus reikalingi sistemos tobulinimo darbai, papildoma įranga ar licencijos Techninėje specifikacijos~~s~~je aprašytam funkcionalumui pasiekti, tokios priemonės turi būti užtikrintos Tiekėjo, o sąnaudos turi būti įskaičiuotos į Tiekėjo pasiūlymo kainą;

4.18.2.2. Teisė gauti analitikos taisykles, skirtas naujoms grėsmėms aptikti;

4.18.2.3. Teisė gauti koreliavimo taisyklių, normalizavimo taisyklių ir šaltinių reputacijos sąrašų / informacijos atnaujinimus;

4.18.2.4. Teisė kreiptis į gamintoją arba Tiekėją problemų, kylančių naudojant Sistemą, sprendimo klausimais darbo dienomis, nuo pirmadienio iki penktadienio, nuo 8.00 iki 17.00 val. Lietuvos Respublikos laiku, internetu, elektroniniu paštu arba telefonu.

5. REIKALAVIMAI SISTEMOS PARUOŠIMUI NAUDOTI

5.1. Sistemos paruošimas naudojimui (eksploatacijai) vykdomas trimis etapais:

5.1.1. Sistemos diegimas (toliau – Sistemos diegimo etapas arba 1 etapas);

5.1.2. Duomenų ir taisyklių perkėlimas iš Perkančiosios organizacijos naudojamos Logrhythm sistemos į naują Sistemą (toliau - Sistemos duomenų permigravimas arba 2 etapas)

5.1.3. Sistemos derinimas prie Perkančiosios organizacijos duomenų srautų bei darbo procesų ypatumų (toliau – Sistemos derinimo etapas arba 3 etapas).

5.2. Sistemos diegimo etapas (1 etapas) turi užtrukti ne ilgiau negu 14 kalendorinių dienų nuo Techninės specifikacijos 3.2 punkte nurodytos dokumentacijos suderinimo su Perkančiąja organizacija dienos.

5.3. Duomenų ir taisyklių migravimas iš Logrhythm sistemos į naują sistemą (2 etapas) per 1 mėnesį nuo pirmojo (Sistemos diegimo) etapo pabaigos. Šiuo metu yra įdiegtos 586 koreliavimo taisyklės, bet jų kiekis nuolat kinta nes vyksta nuolatinės adaptacija ir taisyklių optimizavimas. Tiekėjas, atlikdamas egzistuojančių koreliavimo taisyklių migraciją, privalo identifikuoti taisykles, kurios loginės paskirties ar veikimo požiūriu dubliuojasi su gamintojo pateiktomis standartinėmis taisyklėmis (nurodytomis~~ų~~ ~~1~~4.13.2 punkte), ir tokių dubliuojančių taisyklių į Sistemą neperkelti.

5.4. Sistemos derinimo etapas (3 etapas) turi užtrukti ne ilgiau negu 2 mėnesius nuo antrojo (Sistemos duomenų permigravimo) etapo pabaigos dienos.

5.5. Sistemos diegimo ir migravimo etapuose turi būti:

5.5.1. įdiegti Sistemos agentai ir/arba kolektoriai ir/arba kita lygiavertė žurnalinių įrašų surinkimo programinė įranga (1 etapas);

5.5.2. atliekamas standartinių ir specifinių įrašų šaltinių tvarkymas: pridėjimas į Sprendimą, modifikavimas, pašalinimas. Prie Sistemos turi būti prijungta ne mažiau duomenų šaltinių nei buvo išmigruojamoje Logrhythm sistemoje;

5.5.3. atliekamas Sprendimo koreliacijos taisyklių konfigūravimas: sukūrimas, modifikavimas, adaptavimas ir nereikalingų pašalinimas. Turi būti įdiegta ne mažiau lygiaverčių pagal funkcijas taisyklių kaip iki tol naudotoje Logrhythm sistemoje. Sistemos diegimo metu įdiegtos koreliavimo taisyklės pagal poreikį derinamos prie Perkančiosios organizacijos infrastruktūros (2 etapas);

5.5.4. Konfigūruojamos koreliacijos taisyklės aliarmai bei kasdienės ataskaitos surinktų įvykių apdorojimui turi apimti šias kategorijas (2 etapas):

5.5.4.1. domeno vartotojui suteiktos/atimtos administratoriaus (pvz. domeno administratoriaus, enterprise administratoriaus, global administratoriaus) ar kitos teisės, veiksmai aktyvaus katalogo (angl. active directory) aplinkoje (sukurta ir/arba išjungta, ir/arba panaikinta AD vartotojo paskyra);

5.5.4.2. nesėkmingi bandymai jungtis prie Perkančiosios organizacijos įrangos;

5.5.4.3. sėkmingi / nesėkmingi prisijungimai prie VPN;

5.5.4.4. sėkmingi / nesėkmingi prisijungimai prie ugniasienių, kompiuterinio tinklo komutatorių valdymo IP adresų, tarnybinių stočių;

5.5.4.5. žinomos grėsmės, nustatomos pagal maišos (angl. *hash*) reikšmes;

5.5.4.6. komunikacija su žinomomis grėsmių nuorodomis (URL);

5.5.4.7. komunikacija su žinomais blogos reputacijos IP adresais;

5.5.4.8. identifikuota komunikacija su apkrėstais IP adresais;

5.5.4.9. bandymas įsilaužti („brute force", skanavimas);

5.5.4.10. identifikuotos slaptažodžių atakos;

5.5.4.11. identifikuoti naudotojų elgesio nuokrypimai;

5.5.4.12. autentikavimo rizikos;

5.5.4.13. manipuliavimas auditavimu ar jo sustabdymo rizikos;

5.5.4.14. teisių ar privilegijų eskalavimo rizikos;

5.5.4.15. tinklo prieigos rizikos;

5.5.4.16. įsilaužėlio horizontalaus judėjimo infrastruktūroje (angl. *lateral movement*) rizikos;

5.5.4.17. prieigos duomenų (angl. *credentials*) vagystės rizikos;

5.5.4.18. kenksmingo programinio kodo rizikos;

5.5.4.19. ilgalaikio įsitvirtinimo (angl. *persistence*) infrastruktūroje rizikos;

5.5.5. atliktas aliarmų derinimas (2 etapas).

~~5.5.6. Ne mažiau nei 100 (šimtą) Sistemos derinimo metu pagal poreikį atsiradusių papildomų naujų koreliacijos taisyklių prieš tai jų turinį, logiką suderinus su Perkančiąja organizacija ir gamintoju (3 etapas).~~

~~5.5.7.~~5.5.6. išorinių kibernetinių grėsmių indikatorių (angl. cyber threat intelligence) duomenų šaltinių (kenksmingų IP adresų, domenų ir pan.) tvarkymas: pridėjimas, modifikavimas, pašalinimas (3 etapas). Indikatorių kiekį ir atnaujinimo metodus parenka Tiekėjas.

~~5.5.8.~~5.5.7. Sprendimo pranešimų, ataskaitų, darbalaukių (angl. dashboard), vizualizacijų, greitųjų paieškų šablonų sukūrimas, tvarkymas, pašalinimas, pristatymo konfigūravimas (2-3 etapas).

~~5.5.9.~~5.5.8. Sprendimo konfigūravimas Tiekėjo iniciatyva (tobulinant Sprendimą, optimizuojant Sistemos veikimą ir pan.), taip pat Perkančiosios organizacijos prašymu, pasikeitus teisiniam reglamentavimui (3 etapas).

5.6. Tiekėjas turi pateikti Perkančiajai organizacijai Sistemos standartinę dokumentaciją, pagalbos žinynus ir kitą su Sistema susijusią medžiagą, įskaitant Sistemos naudojimosi vadovą, lietuvių arba anglų kalba elektroniniu formatu[2].

5.7. Įdiegus Sistemą, turi būti suteikti ne mažiau kaip 2 (dviem) Perkančiosios organizacijos darbuotojams Sistemos gamintojo arba Tiekėjo vedami mokymai (vykdomi Perkančiosios organizacijos patalpose arba nuotoliniu būdu), kurie suteiktų žinias, kaip naudoti Sistemą.

[2] Šis reikalavimas yra aplinkos apsaugos kriterijus, nustatytas pagal Aprašo 4.4.4.1 punktą, nes dokumentų nespausdinant, o juos rengiant ir naudojant elektroniniu formatu yra taupomi ištekliai.

5.8. Minimali mokymų trukmė – 8 akademinės valandos. Į mokymų trukmę neįskaičiuojamas Sistemos diegimo metu bendras Tiekėjo ir Perkančiosios organizacijos konsultavimasis, vykdomas pagal Techninės specifikacijos 6.13 punktą. Mokymai vedami lietuvių arba anglų kalba.

6. REIKALAVIMAI ANALITIKAI IR KITOMS SPRENDIMO NAUDOJIMO METU VYKDOMOMS VEIKLOMS

6.1. Į nuomos kainą turi būti įskaičiuotas visų žemiau nurodytų ir aprašytų veiklų vykdymas.

6.2. Sprendimo analitika turi būti atliekama nuolat nuo Sistemos diegimo etapo pabaigos iki pirkimo sutarties galiojimo pabaigos, kiekvieną dieną visą parą.

6.3. Duomenys analitikai turi būti renkami nuolat nuo Sistemos diegimo etapo pabaigos iki pirkimo sutarties galiojimo pabaigos, kiekvieną dieną visą parą.

6.4. Sprendimo teikimui taikomi žemiau nurodyti reagavimo ir sutrikimų/užklausų išsprendimo laikai, kuriais vadovaujantis rengiami Techninės specifikacijos 3.2.1, 3.2.2 ir 3.4 punkte nurodyti dokumentai.

6.4.1. Reagavimo į nustatytą Sprendimo neveikimą, sutrikimus, problemas, dėl kurių negalima naudotis Sprendimu, laikas – ne daugiau 2 (dvi) valandos.

6.4.2. Incidento patvirtinimo arba pagrįsto atmetimo, kurį atliekas Tiekėjas, laikas – ne daugiau 2 (dvi) valandos nuo incidento nustatymo.

6.4.3. Perkančiosios organizacijos informavimo apie nustatytą pavojingą incidentą, galintį sukelti žalą Perkančiosios organizacijos infrastruktūrai ir/arba duomenims, laikas – ne daugiau 30 (trisdešimt) minučių nuo jo patvirtinimo.

6.4.4. Perkančiosios organizacijos informavimo apie nustatytą nereikšmingą incidentą, kuris neturi poveikio organizacijai, infrastruktūrai, darbo procesams, kibernetinei saugai, laikas – ne daugiau 2 (dvi) valandos nuo jo patvirtinimo.

6.4.5. Reagavimo į Perkančiosios organizacijos užklausas (suteikti informaciją, konsultuoti, atlikti konfigūravimo veiksmus ir pan.) laikas – ne daugiau 8 (aštuonios) darbo (darbo dienomis nuo 8:00 val. iki 17:00 val.) valandos.

6.4.6. Užklausos išsprendimo laikas – ne daugiau 24 (dvidešimt keturios) darbo valandos (darbo dienomis nuo 8:00 val. iki 17:00 val.). Užklausos išsprendimo laikas gali būti ilginamas Tiekėjui pateikus objektyvias to priežastis ir el. paštu suderinus su Perkančiąja organizacija reikiamą ilgesnį laiką.

6.5. Reagavimo į užklausas ir incidentus būdas nustatomas komunikacijos plane.

6.6. *Sprendimas turi apimti žemiau nurodytas duomenų analizės veiklas:*

6.6.1. Stebėjimas ir įvertinimas Sistemos sukuriamų aliarmų, susijusių su:

6.6.1.1. žinomomis grėsmėmis, nustatomomis pagal maišos (angl. hash) reikšmes;

6.6.1.2. komunikacijomis su žinomomis grėsmių nuorodomis (URL);

6.6.1.3. komunikacijomis su žinomais blogos reputacijos IP adresais;

6.6.1.4. identifikuotomis komunikacijos su apkrėstais IP adresais;

6.6.1.5. bandymais įsilaužti („brute force“, skanavimas);

6.6.1.6. identifikuotomis slaptažodžių atakomis;

6.6.1.7. identifikuotais naudotojų elgesio nuokrypiais;

6.6.1.8. autentikavimo rizikomis;

6.6.1.9. manipuliavimo auditavimu ar jo sustabdymo rizikomis;

6.6.1.10. teisių ar privilegijų eskalavimo rizikomis;

6.6.1.11. tinklo prieigos rizikomis;

6.6.1.12. įsilaužėlio horizontalaus judėjimo infrastruktūroje (angl. lateral movement) rizikomis;

6.6.1.13. prieigos duomenų (angl. credentials) vagysčių rizikomis;

6.6.1.14. kenksmingo programinio kodo rizikomis;

6.6.1.15. ilgalaikio įsitvirtinimo (angl. persistence) infrastruktūroje rizikomis;

6.6.1.16. kitais Sistemos pagalba nustatomais indikatoriais ir rizikomis.

6.6.2. Aliarmu (aliarmais) indikuojamo kibernetinio incidento (toliau – incidentas) patvirtinimas arba pagrįstas atmetimas.

6.6.3. Patvirtinto incidento klasifikavimas pagal svarbą, skubumą, galimą poveikį, paveikiamus išteklius, galimą sprendėją ir (ar) kitus kriterijus, suderintus su Perkančiąja organizacija ar nustatytus teisės aktuose.

6.6.4. Atskirai nustatytų incidentų apjungimas, nustačius jų bendrą kilmę ir (ar) valdymo galimybę.

6.6.5. Incidento išsprendimo iniciavimas pagal Perkančiosios organizacijos veiklos procedūras ir teisės aktų reikalavimus.

6.6.6. Informacijos, būtinos incidento susiejimui su kita informacija Perkančiosios organizacijos sistemose, tvarkymas Sprendime.

6.6.7. Sistemos konfigūravimo veiksmų inicijavimas, siekiant pagerinti ir (ar) optimizuoti Sprendimo apdorojamų duomenų analizę ir jų įgyvendinimas, konsultuojantis su Perkančiąja organizacija.

6.6.8. Tiekėjas turi teisę informuoti arba taikyti automatizuotas priemones, realizuojančias Perkančiosios organizacijos informavimą apie nustatytus incidentus ne darbo laiku, tačiau tokiu atveju turi būti informuojama tik apie patvirtintus pavojingus incidentus. Visus patvirtintus pavojingus incidentus Teikėjas turi užregistruoti Perkančiosios organizacijos užklausų ir incidentų valdymo sistemoje (Jira).

6.6.9. Tiekėjas turi pateikti savaitinę ataskaitą apie Sprendimo sukurtus aliarmus ir jų valdymo būklę; šios ataskaitos turinys turi būti suderintas su Perkančiąja organizacija; turi būti užtikrinta, kad ataskaita būtų pateikiama Perkančiajai organizacijai ne vėliau kaip iki kitos savaitės pirmadienio 9 val.

6.7. *Sprendimas turi apimti žemiau nurodytas incidento valdymo ir tyrimo koordinavimo veiklas:*

6.7.1. Greitojo atsako (incidento plitimo užkardymo, sustabdymo, apsunkinimo, žalos mažinimo ir pan.) veiksmų nustatymas ir pateikimas Perkančiajai organizacijai.

6.7.2. Incidento tyrimas, jo eigos atkūrimas.

6.7.3. Bendradarbiavimas su Perkančiąja organizacija šalinant incidento pasekmes, atkuriant įprastinę veiklą, teikiant informaciją kibernetinio saugumo institucijoms ir vykdant jų nurodymus.

6.7.4. Sprendime esančių, o esant galimybei – ir kitų incidento įrodymų surinkimas ir išsaugojimas.

6.7.5. Spragų, kuriomis pasinaudota incidento metu šalinimo, saugos ir saugos valdymo procesų gerinimo rekomendacijų pateikimas, suvaldžius incidentą.

6.8. *Sprendimas turi apimti žemiau nurodytas Sprendimo konfigūravimas veiklas:*

6.8.1. Sprendimo konfigūravimas Tiekėjo iniciatyva (tobulinant Sprendimą, optimizuojant Sistemos veikimą ir pan.), taip pat Perkančiosios organizacijos prašymu, pasikeitus teisiniam reglamentavimui.

6.9. *Ataskaitų apie saugumo ir analitikos operacijų centro (toliau - SOC) veiklą teikimas, vykdomas žemiau nurodytu reguliarumu ir terminais nuo Sistemos diegimo etapos pabaigos:*

6.9.1. Ne rečiau kaip kartą per mėnesį, ne vėliau kaip iki kito mėnesio 10 dienos, Tiekėjas pateikia Perkančiajai organizacijai mėnesinę SOC veiklos ataskaitą, kurioje nurodoma:

6.9.1.1. incidentų statistinė informacija;

6.9.1.2. svarbiausi suvaldyti incidentai;

6.9.1.3. Sprendimo veikimo esminiai rodikliai;

6.9.1.4. esminiai atlikti Sprendimo konfigūracijos pokyčiai (naujos koreliacijos taisyklės ir pan.);

6.9.1.5. Sprendimo veikimo lygio rodiklių (reakcijos, incidentų išsprendimo laikų, Sprendimo prieinamumo ir pan.) suvestinė;

6.9.1.6. tendencijos, įžvalgos, rekomendacijos dėl Sprendimo gerinimo;

6.9.1.7. kita Sprendimo vykdymui svarbi informacija, Tiekėjo nuožiūra.

6.9.2. Ne rečiau kaip kartą per ketvirtį, ne vėliau kaip iki kito ketvirčio pirmojo mėnesio 15 dienos, Tiekėjas pristato Perkančiajai organizacijai ketvirtinę SOC veiklos ataskaitą. Šioje ataskaitoje pateikiami:

6.9.2.1. mėnesinių ataskaitų apibendrinimas;

6.9.2.2. įžvalgos ir siūlymai dėl esamų koreliacijos taisyklių tobulinimo ir naujų įvedimo;

6.9.2.3. įžvalgos ir siūlymai dėl kibernetinių grėsmių indikatorių šaltinių panaudojimo;

6.9.2.4. įžvalgos ir siūlymai dėl Sprendimo veiklos optimizavimo;

6.9.2.5. įžvalgos ir siūlymai dėl Sprendimo veiklos procesų gerinimo;

6.9.2.6. informacija apie ankstesnėse mėnesinėse ir ketvirtinėse SOC veiklos ataskaitose pateiktų siūlymų, jei jiems pritarė Perkančioji organizacija, įgyvendinimą;

6.9.2.7. Perkančiosios organizacijos nurodytų kibernetinių incidentų, nustatytų ne SOC priemonėmis, įvertinimas, ieškant galimybių ateityje tokius incidentus nustatyti SOC priemonėmis;

6.9.2.8. rizikos SOC veiklai ir analitikos teikimui, šių rizikų valdymo galimybės ir priemonės;

6.9.2.9. kita svarbi informacija, Tiekėjo nuožiūra.

6.9.3. Esant poreikiui, ketvirtinės ataskaitos pristatymui ir (ar) joje pateiktos informacijos svarstymui gali būti organizuojami Tiekėjo atstovų ir Perkančiosios organizacijos atstovų susitikimai.

6.9.4. Rizikos, keliančios rimtą grėsmę Sprendimui, pranešamos Perkančiajai organizacijai nedelsiant, bet ne vėliau kaip kitą darbo dieną.

6.10. Sprendimo veikimas:

6.10.1. Įdiegus Sistemą, Tiekėjas turi užtikrinti ne mažesnį nei 99 proc. Sprendimo pasiekiamumą (ang. SLA).

6.10.2. Įdiegus Sistemą, Tiekėjas visą pirkimo sutarties laikotarpį užtikrina:

6.10.2.1. nuolatinį Sprendimo būklės stebėjimą, proaktyvią Sistemos veikimo problemų prevenciją, reagavimą į pastebėtus sutrikimus ir problemas, įskaitant įrašų šaltinių teikimo į Sistemą sutrikimus, Sistemos veikimo atkūrimą;

6.10.2.2. Sistemos naudotojų administravimą (pridėjimą, prieigos teisių pakeitimą, pašalinimą). Perkančiajai organizacijai turi būti suteiktos skaitymo/peržiūros teisės be galimybės atlikti Sistemoje pakeitimus, veiksmus, kurie gali įtakoti Sistemos veikimą, informacijos analizavimą, incidentų sprendimą ir pan.;

6.10.2.3. Sistemos programinių atnaujinimų įdiegimą ne vėliau kaip per 1 (vieną) mėnesį po Sistemos gamintojo atnaujinimo išleidimo;

6.10.2.4. Visų Sistemos pakeitimų, diegimų, naujinimų ir pan. prieš jų atlikimą privalomą suderinimą su Perkančiosios organizacijos atstovais.

6.10.2.5. Perkančiosios organizacijos informavimą apie Sistemoje atliktus pakeitimus siekiant efektyvaus Sistemos veikimo, Sprendimo techninių bei programinių išteklių optimalaus naudojimo ir saugos (apie atliktus pakeitimus Perkančioji organizacija turi būti informuojama per 24 val. nuo pakeitimo atlikimo);

6.10.2.6. tarpininkavimą tarp Sistemos gamintojo ir Perkančiosios organizacijos sprendžiant Sistemos veikimo, įrašų šaltinių teikimo problemas.

6.11. Pirkimo sutarties vykdymo metu turi būti vadovaujamasi žemiau pateiktais teisės aktais bei rekomendacijomis (aktualiomis redakcijomis):

6.11.1. Kibernetinio saugumo įstatymu.

6.11.2. Kibernetinio saugumo reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 6 d. nutarimu Nr. 945 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo“.

6.11.3. Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 6 d. nutarimu Nr. 945 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo.

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

6.12. Tiekėjas įsipareigoja laikytis Perkančiosios organizacijos informacijos saugos politikos, informacija apie kurią Tiekėjui bus pateikta pirkimo sutarties metu, reikalavimų.

6.13. Tiekėjas turi konsultuoti Perkančiosios organizacijos darbuotojus su Sprendimu susijusiais klausimais. Konsultacijos teikiamos tokia pačia forma, kaip ir Perkančiosios organizacijos pateiktas paklausimas, nebent Perkančioji organizacija nurodytų kitą formą. Tiekėjas turi teisę konsultacijas ir komunikacinius Sprendimo aspektus organizuoti per Tiekėjo valdomą pagalbos tarnybos sistemą, jeigu Tiekėjas tokią turi. Numatoma maksimali konsultacijų per visą pirkimo sutarties galiojimo laikotarpį apimtis – 240 valandų. Visas su konsultacijų teikimu susijusias išlaidas tiekėjas turi įskaičiuoti į bendrą pasiūlymo kainą.