TECHNINĖ SPECIFIKACIJA

1. Lietuvos Respublikos užsienio reikalų ministerija (toliau – Perkančioji organizacija) perka (nuomoja) EDR (*Endpoint Detection and Response*) tipo tarnybinių stočių ir kompiuterinių darbo vietų apsaugos programinės įrangos (toliau – PĮ) licencijas 36 (trisdešimt šešių) mėnesių laikotarpiui[1] pratęsiant dabar turimos ir eksploatuojamos programinės įrangos licencijų prenumeratą.
2. Numatomas įsigyti licencijų kiekis **nuo 1 500 vnt. iki 1 700 vnt**.
3. Šiuo metu turimos, šios Techninės specifikacijos 6 punkte nurodytos programinės įrangos, licencijos turi būti pratęsiamos nuo jų galiojimo pabaigos, t. y. nuo **2025 m. rugpjūčio 18 d.** (imtinai). Turi būti galimybė licencijų galiojimo laikotarpiu perkelti licenciją iš vienos tarnybinės stoties (darbo vietos) kitai.
4. Licencijos registruojamos Perkančiosios organizacijos el. pašto adresu: cert@urm.lt.
5. Perkama PĮ (PĮ licencijos) Perkančiajai organizacijai privalo būti perduota (aktyvuota) viešojo pirkimo–pardavimo sutarties 4.1 papunktyje nustatytomis sąlygomis.
6. Perkančiosios organizacijos turima EDR tipo programinė įranga: Falcon Endpoint Protection Premium Flexible Bundle (su Insight, Prevent, Discover, Identity Protection moduliais), Threat Graph Standard on EU Cloud, Falcon X Bundle Promo, Express Support. Šios programinės įrangos licencijos galioja iki 2025 m. rugpjūčio 17 d. (imtinai).
7. Tiekėjas gali siūlyti ir šios techninės specifikacijos 6 punkte nurodytai programinei įrangai lygiavertę PĮ. Lygiavertiškumo įrodymas yra tiekėjo pareiga.
8. Vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo 37 straipsnio 9 dalies reikalavimais ir atsižvelgiant į tai, jog prekės BVPŽ kodas yra 48760000-3 (apsaugos nuo virusų programinės įrangos paketai), teikėjas privalo užtikrinti, kad prekių gamintojas ar jį kontroliuojantis asmuo nėra 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.
9. Atsižvelgiant į tai, kad perkamos (nuomojamos) PĮ licencijos, papildomi aplinkos apsaugos reikalavimai nenustatomi ir, vadovaujantis Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto Lietuvos Respublikos aplinkos ministro

[1] *PĮ licencijos turi būti pristatomos (aktyvuojamos) ir už jas bus apmokoma etapais (plačiau žr. viešojo pirkimo–pardavimo sutarties specialiąsias sąlygas, įskaitant, bet neapsiribojant, jų 4 punktą ir 5.5 papunktį).*

2011 m. birželio 28 d. įsakymu Nr. D1-508 „Dėl Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“, 4.4.3 papunkčiu šis Pirkimas laikomas žaliuoju.

10. Reikalavimai PĮ:

Eil. Nr.	Rodiklis	Minimali reikalaujamo rodiklio reikšmė
10.1.	Palaikomos platformos	Klientams diegiama PĮ turi palaikyti Windows 10, 2012 R2 ir aukštesnes operacinių sistemų versijas.
		Klientams diegiama PĮ turi palaikyti MacOS 10.14 ir aukštesnes operacinės sistemos versijas.
		Klientams diegiama PĮ turi palaikyti Linux distributyvus (Ubuntu, RedHat, CentOS, Oracle Linux) operacines sistemas.
		Klientams diegiama PĮ turi palaikyti virtualių tarnybinių stočių infrastruktūrą.
		Klientams diegiama PĮ turi palaikyti virtualių tarnybinių stočių šablonus.
10.2.	Diegimas	Klientams diegiama PĮ turi turėti apsaugą nuo parametrų keitimo (*tamper-resistant*) ir apsaugą nuo pašalinimo.
		Klientinę įrangą turi būti leidžiama diegti pasitelkus centralizuoto diegimo įrankius.
		Klientinės įrangos diegimas turi vykti be sistemos perkrovimo, t. y. nereikalauti sistemos perkrovimo sėkmingam klientinės įrangos įdiegimui.
10.3.	Vartotojo aplinka	Vartotojo aplinka turi būti apsaugota 2 faktorių autentifikacija.
		Vartotojo sąsajoje turi būti integravimo parinktys su vienu prisijungimu (SSO).
		Vartotojo sąsajoje turi būti įtrauktos prieigos valdymo rolės.
		Siūlomos PĮ sprendimas (toliau – sprendimas) turėtų suteikti tikslią vaidmenimis pagrįstą prieigos valdymą, kad būtų galima pasiekti atskirus perkančiosios organizacijos padalinius arba funkcijas.
		Sprendimas turi suteikti galimybę grupuoti pagrindinius įrenginius pagal pagrindinio kompiuterio identifikatorius, „Active Directory“ OU arba politikos vykdymo žymas.
		Visi vartotojo sąsajoje atlikti veiksmai turi būti saugomi audito žurnaluose.

		Vartotojo sąsaja turi būti pasiekiama neribotam skaičiui administratorių/analitikų.
		Sprendimas turi turėti vieną vartotojo sąsają visoms administravimo funkcijoms atlikti.
10.4.	Atakų prevencija	Sprendimas turi gebėti užkirsti kelią anksčiau nežinotoms / unikalioms kenkėjiškoms programoms, t. y. gebėti užkirsti kelią nežinomų/unikalių kenkėjiškų programų (pvz., zero-day) atakas.
		Sprendimas turi būti naujos kartos galutinio taško apsaugos platforma (angl. *Next-Generation Endpoint Protection Platform*), kuri naudoja mašininį mokymąsi, kad būtų išvengta išankstinio vykdymo žinomų ir nežinomų kenkėjiškų programų.
		Prevencinės priemonės turi sustabdyti atakas prieš pažeidžiant operacinės sistemos veiklą. Pavyzdžiui, sustabdyti proceso modifikavimą, manipuliavimą (angl. *Process injection*) prieš jį įvykdant, kad galutinis procesas (angl. *target process*) nebūtų paveiktas, sutrikdytas.
		Sprendimas turi užtikrinti atminties apsaugą (angl. *ASLR, structured exception handling overwrite protection, null page protection, heap spray preallocation*) ir kt.
		Sprendimas turi gebėti susidoroti su *LOLbins* (angl. *Living off the Land Binaries*) tipo atakomis.
		Sprendimas turi gebėti užkirsti kelią kenkėjiškam „Powershell“ scenarijų naudojimui.
		Sprendimas turi gebėti užkirsti kelią tarnybinėse stotyse ar kompiuterinėse darbo vietose įdiegtos programinės įrangos ir operacinės sistemos saugumo spragų išnaudojimui, pavyzdžiui, turi gebėti užkirsti programinėje įrangoje ir operacinėse sistemose spragas išnaudojamas su komandine eilute, scenarijais arba kitomis be failų kenkėjiškomis atakomis (angl. *fileless attacks*).
		Sprendimas turi užtikrinti apsaugą nuo atakų Windows, Mac ir Linux operacinėse sistemose, t. y. atakų prevencijos funkcionalumai turi būti prieinami visose operacinėse sistemose vienodai.
		Sprendimas negaudamas atnaujinimų turi užtikrinti apsaugą nuo atakų 3 mėnesius, t. y. sprendimas turit užtikrinti apsaugą nuo atakų 3 mėnesius negaudamas atakų prevencijos atnaujinimų, o ne produkto versijos atnaujinimo.
		Sprendimas turi leisti automatizuotą ir rankinį kenkėjiškų programų analizavimo funkcionalumą, t. y. rankiniu būdu įkelti kenkėjišką dokumentą ir jį analizuoti smėliadėžėje (angl. *Sandbox*) intuityviu būdu (angl. *manual* arba *user-interactive mode*).

10.5.	Klientinės įrangos telemetrija	Sprendimas turi registruoti tarnybinių stočių aktualius įvykius atliekant tyrimus (angl. *forensic investigations*).
		Klientinės įrangos registruojamų įvykių generuojamas duomenų srautas neturi viršyti 256 Kbps.
		Sprendimas turi suteikti visapusišką privilegijuotą paskyros stebėjimo funkciją, apimančią sėkmingus ir nesėkmingus prisijungimo bandymus, taip pat telemetriją, kada slaptažodžiai buvo paskutinį kartą nustatyti iš naujo.
		Sprendimas turi pateikti telemetriją apimančią sistemos išteklių panaudojimą, pvz., vidutinį RAM suvartojimą, procesorių skaičių, naudojamą vietą diske ir kt.
		Galinio įrenginio agentas turi veikti pagal tokias charakteristikas: – Išnaudoti ne daugiau 1–3 % procesoriaus; – Naudoti ne daugiau nei 50 MB atminties; – Užimti ne daugiau 100 MB disko vietos.
		Klientinės įrangos registruojami įvykiai turi būti indeksuojami, o paieška juose vykdoma naudojant standartinę užklausų kalbą, t. y. indeksavimas turi būti visai įvykių informacijai (angl. *RAW events*), o ne tik artefaktams.
		Klientinės įrangos užregistruoti įvykiai turi būti eksportuojami/atsisiunčiami.
		Klientinės įrangos užregistruoti įvykiai turi būti saugomi mažiausiai 60 dienas.
10.6.	Reagavimas ir pašalinimas	Sprendimas turi suteikti tinklo izoliavimo funkcionalumą Windows, Mac ir Linux operacinėse sistemose.
		Sprendimas turi palaikyti nuotolinio taisymo ir atnaujinimo (angl. *remote remediation*) funkcionalumą visose operacinėse sistemose vienodai.
		Sprendimas turi suteikti galimybę nuotoliniu būdu prisijungti prie tikslinių sistemų, kad būtų galima papildomai surinkti (procesų bei darbinę RAM atmintį, registrus, failus (angl. *Process memory, full memory dumps, registry, files*) ir kt.).
		Sprendimas turi suteikti galimybes (perkelti failus į nuotolines sistemas, vykdyti failus, paleisti scenarijus, naikinti procesus, koreguoti registro raktus ir kitas užduotis, reikalingas reaguojant į

		incidentą (angl. *pushing files to remote systems*, *executing files*, *running scripts*, *killing processes*, *adjusting registry keys and other tasks required during incident response*)).
		Sprendimas turi pateikti iš anksto nustatytas teismo ekspertizės artefaktų (angl. *forensic artefacts*) (pvz., maišos, domeno, neapdorotų įvykių, registro raktų (angl. *e.g. hash, domain, raw events, registry keys*)) užklausas.
		Sprendimas turi suteikti galimybę atlikti neapdorotą įvykių paiešką (angl. *Raw event search*) naudojant struktūrinę užklausų kalbą per visą surinktą įvykių telemetriją (angl. *data stacking*).
		Sprendimas turi palaikyti funkcionalumą, kuris leistų atsaką į grėsmę aprašyti scenarijumi, t. y. sprendimas turi turėti funkcionalumą kurti reagavimo scenarijus į suveiktas aptikimo taisykles (angl. *response*), pavyzdžiui, izoliuoti įrenginį, automatiškai įvykius tam tikram specialistui pagal tam tikrus kriterijus ir pan.
		Reagavimo ir izoliavimo funkcijos turi būti automatizuojamos naudojant trečiųjų šalių įrankius, t. y. trečių šalių įrankių, tokių kaip SOAR, SIEM, Helpdesk, incidentų valdymo platformų integracijų/automatizacijų turėjimą reagavimo ir izoliavimo veiksmams atlikti iš trečiųjų šalių įrankių ir per trečiųjų šalių įrankius.
		Reagavimo ir izoliavimo funkcijos turi būti prieinamos per API.
10.7.	Grėsmių žvalgyba	Sprendimas turi palaikyti kontekstą ir atributus, kurie indikuoja, kad sistema buvo sukompromituota, t. y. informacija apie grėsmių žvalgybos (angl. *threat intelligence*) kontekstą ir atributus sprendime, pavyzdžiui, kas atakuoja, kokia jų motyvacija, galimybės, jų IOC.
		Sprendimas turi palaikyti išsamią informaciją apie nacionalinių valstybių, e-nusikaltimų ir įsilaužėlių grupių įsilaužimų strategijas, pavyzdžiui, nusikalstamas grupuotes kaip Mustang Panda, Vixen Panda, Cozy Bear, APT 29 ir pan. Sprendimo aptikti grėsmės rodikliai turi būti susiejami su atitinkamomis grupuotėmis, informacija turi būti prieinama sprendime, paieškoma.
		Į sprendimą turi būti įtraukta galimai kompromituotos sistemos grėsmės rodikliai, kuriuos būtų galima naudoti kartu su kitais saugumo sprendimais.

		Į sprendimą turi būti įtrauktos reguliarios grėsmių žvalgybos ataskaitos, kurios padėtų suvaldyti rizikas ir įtakotų investicijas į saugumą.
10.8.	Trečiųjų šalių vertinimas	Sprendimas turi būti paskelbtas 2023 magiškajame kvadrate (angl. *Magic Quadrant*) pirmame aukščiausiame lyderių kvadrate.
10.9.	Priežiūra ir palaikymas	24/7 palaikymas.
		Klientų portalas turi leisti lengvai pateikti įtartinus failų pavyzdžius, leisti pranešti apie technines problemas ir leisti stebėti pateiktų užklausų eigą.
		Prie PĮ turi būti pateikta dokumentacija.
		Iniciavimo procesas vykdomas iš pardavėjo pusės.
		Suteikiamas globalus palaikymas.
		PĮ gamintojo klientų aptarnavimo portalas turi suteikti pagalbą, taip pat įskaitant viešą žinių bazę, vartotojų forumus, gerosios praktikos patarimus, mokomuosius vaizdo įrašus ir vartotojų vadovus.
		Galimybė gauti pagalbą telefonu.
10.10	Informacija apie įrangos gamybos ar palaikymo nutraukimą	Iki pirkimo dokumentuose nustatyto pasiūlymo pateikimo termino pabaigos, gamintojas neturi būti paskelbęs apie siūlomos įrangos gamybos arba jos palaikymo nutraukimą (pvz. „*End of life time*“ ar „*Discontinued*“).
10.11	USB apsauga	Sprendimas turi automatiškai registruoti įrenginio tipą pagal jo funkcionalumą, pavyzdžiui, USB duomenų talpykla, USB ausinės, USB pelė, USB kamera, USB telefonas ir pan. su gamintojo pavadinimu bei serijos numeriu.
		Galimybė matyti visus įrenginius, veikiančius per USB magistralę, įskaitant vidinius standžiuosius diskus (angl. *internal/non-removable USB devices*).
		Sprendimas turi gebėti registruoti USB įrenginiuose atliktus veiksmus, pavyzdžiui, USB atmintinėse peržiūrėtus, kopijuotus, įrašytus dokumentus bei kitus failus.
		Sprendimas turi turėti galimybę atlikti detalią paiešką naudojant įvairius istoriškus/registruotus dokumentų bei failų meta duomenis identifikuoti duomenų eksfiltravimą bei panašius įvykius.

		Nustatyti įrenginių naudojimosi valdymo politikas kuriant atskiras grupes pagal leidžiamus bei blokuojamus įrenginius filtruojant pagal klasę, gamintoją, serijos numerį ir (arba) konkretaus įrenginio ID numerį.
		Sprendimas turi pateikti informaciją konsolėje apie naudojamus įrenginius ir jiems priskirtas valdymo politikas ir kaip jos gali įtakoti USB įrenginių naudotojus įgalinus blokavimo politikas.
		Į tarnybinę stotį ar kompiuterinę darbo vietą diegiamas PĮ agentas turi būti vienas (angl. *single lightweight-agent architecture*) realizuotas debesijos principu (angl. *Cloud managed*).
		Sprendimas turi gebėti kurti atskiras USB įrenginių valdymo politikas pagal įrenginių prieigos teises: – Leidimas tik skaityti bei rašyti į įrenginį (angl. *read*, *write*); – Leidimas tik skaityti įrenginį (angl. *read only*); – Pilnas įrenginio blokavimas (angl. Full block); – Leidimas skaityti, rašyti bei vykdyti įrenginyje esančius failus bei dokumentus (angl. *read*, *write*, *execute*).
		Sprendimas turi leisti skaityti / rašyti arba tik skaityti prieigą, tuo pačiu blokuojant programų vykdymą USB atmintinėse.
		Sprendimas turi turėti funkcionalumą kurti bei modifikuoti pranešimus (angl. *custom notifications*) apie USB įrenginių blokavimą ar kitą veiksmą naudotojams kompiuterinėje darbo vietoje.
10.12	Žurnalinių įrašų valdymas SIEM sistemose	Galimybė suintegruoti ir kaupti žurnalinius įrašus su turima Organizacijoje SIEM (IBM Qradar) sistema: – Sistemos generuojami saugos pranešimai; – Visi sistemoje iš įrenginių kaupiami žurnaliniai įrašai; – Galimybė persiųsti sistemoje kaupiamus žurnalinius įrašus iš įrenginių RAW formatu; – Galimybė filtruoti persiunčiamus į SIEM sistemą žurnalinius įrašus.
		Galimybė nukreipti sistemoje generuojamus saugos pranešimus: – El. paštu; – MS Teams kanalą.

10.13	Organizacijos tinklo naudotojų apsaugos nuo grėsmių modulio (Identity Protection)	Sprendimas turi stebėti ir pranešti apie nutekintus naudotojų slaptažodžius juodoje rinkoje (angl. Dark Web).
		Sprendimas turi atlikti kiekvieno naudotojo ir įrenginio elgesį tinkle įvertinimą, įskaitant privilegijuotus naudotojus ir paslaugų paskyras, tokiu būdu atskleisti rizikingą naudotojų elgesį, užpuolikus, pažeistas paskyras ar įrenginius, šoninio judėjimo bandymus (angl. Lateral movement), bandymus padidinti privilegijas ir atakas prieš vidinę infrastruktūrą (angl. Privilege Escalation).
		Sprendimas turi audituoti ir atlikti rizikos vertinimą stebinti slaptažodžių naudojimą, privilegijuotas prieigas bei "Active Directory" konfigūracijos problemas.
10.14	Gamintojo palaikymas ir reagavimas valdant saugos incidentus	Teikti ekspertų konsultacijų 24 valandas per parą, 7 dienas per savaitę, aktyvų grėsmių ieškojimą ir vietinę grėsmių žvalgybą bei visapusišką sistemos reagavimo taisymą, kad papildyti kibernetinio saugumo įgūdžių žinias. **Valdymas, aptikimas ir reagavimas:** – 24/7/365 grėsmių, incidentų valdymas aptikimas ir taisymas; – Proaktyvus sistemos valdymas ir optimizavimas; – Metrikos informacijos; – Suvestinė ir API palaikymas; – Priskirtas kontaktinis vadovas; – Bendradarbiavimas su gamintojo komanda per pranešimų centrą.
		Techninė pagalba: – Incidento registracija; – 24/7/365 pagalba telefonu kritinėms situacijoms; – Tiesioginis pokalbis (darbo valandomis); – Registruotų incidentų prioretizavimas; – Aukščiausios kokybės palaikymo turinys (straipsniai, vaizdo įrašai, internetiniai seminarai); – Prieiga prie gamintojo komandos dėl patarimų ir eskalavimų; – Pro-aktyvus saugos lygio auditas ir taisymas; – Sensorių versijų valdymas; – Įrenginių grupių valdymas.
		Prieigos valdymas:

- El. paklausimų valdymas;
- Ketvirtinių atskaitų pateikimas;
- Savaitiniai ir mėnesiniai palaikymo informaciniai biuleteniai;
- Aktyvus informavimas;
- Kas ketvirtį atliekami sistemos funkcionalumų patikrinimai;
- Seminarų tvarkaraščiai WEB aplinkoje;
- Produktų vartotojų ir administratorių dokumentacija, produkto konfigūravimo pagal gerąsias praktikas pateikimas.