TVŪD > PIRKIMO DOKUMENTAI > PASIŪLYMO FORMA

TARNYBINIŲ STOČIŲ APSAUGOS IR GRĖSMIŲ APTIKIMO, TYRIMO IR REAGAVIMO PROGRAMINĖS ĮRANGOS PIRKIMAS (IRD-A117-164)

Turto valdymo ir ūkio departamentui
prie Lietuvos Respublikos vidaus reikalų ministerijos
Teikiama CVP IS priemonėmis

2022-12-22 Nr.
PSL221219JMR1-01
(Data, Nr.)

Vilnius
(Vieta)

1 lentelė. Tiekėjo rekvizitai:

Tiekėjo pavadinimas ir kodas	*Blue Bridge MSP, UAB. 301489547*
Tiekėjo adresas	*J. Jasinskio g. 16A, LT-03163 Vilnius*
PVM mokėtojo kodas	*LT100003708514*
Bankas ir sąskaitos numeris	*LT89 2140 0300 0280 5128, Luminor Bank AS, 40100*
Telefono Nr., internetinis puslapis, el. paštas	*+37052526060, www.bluebridge.lt, info@bluebridge.lt*
Asmens, pateikusio pasiūlymą CVP IS priemonėmis, vardas, pavardė, pareigos[1]	*Jolita Markevičiūtė, pardavimų koordinatorė.*
Ryšiams su Vykdytoju palaikyti skirtamo asmens vardas, pavardė, pareigos ir kontaktiniai telefonai	*Aurimas Saulis, tinklų ir saugumo sprendimų vadybininkas, +37065539668.*

2 lentelė. Su pasiūlymu pateikiami dokumentai:

Eil. Nr.	Pateikto dokumento pavadinimas	Ar dokumente yra konfidenciali* informacija	Jeigu taip, kokiu pagrindu atitinkamas dokumentas yra konfidencialus?	Lapų skaičius
1.	Ši pasiūlymo forma	Ne		9
2.	Įgaliojimas	Ne		1
3.	Gamintojo raštas	Ne		1

* Informacija, nurodyta VPĮ 20 straipsnio 2 dalies 1, 2, 3, 4 punktuose negali būti nurodoma ir nebus laikoma konfidencialia. Tiekėjas gali nurodyti, kuri informacijos dalis pasiūlyme yra konfidenciali. Tiekėjo su pasiūlymu teikiamų dokumentų informacijos konfidencialumas gali būti nustatomas tik pagrįstais atvejais. Jeigu kils abejonių dėl tiekėjo pasiūlyme nurodytos informacijos konfidencialumo, Vykdytojas prašys tiekėją per nurodytą terminą, kuris negali būti trumpesnis kaip 5 darbo dienos, pagrįsti jos konfidencialumą. Jei tokia informacija pasiūlyme nebus nurodyta, Vykdytojas laikys, kad bet kuri pasiūlyme pateikta informacija nėra konfidenciali, išskyrus informaciją, kurią atskleidus būtų pažeisti Asmens duomenų teisinės apsaugos įstatymo reikalavimai ar Tiekėjo įsipareigojimai pagal su trečiaisiais asmenimis sudarytas sutartis.

3 lentelė. Informacija apie rėmimąsi kitų subjektų pajėgumais. Vykdant pirkimo sutartį bus pasitelkiami šie ūkio subjektai.

Eil. Nr.	Ūkio subjekto (-ų), kvazisubtiekėjo[2], trečiojo asmens[3], kurių pajėgumais remiamasi, pavadinimas (-ai)	Ūkio subjektas pasitelkiamas, siekiant atitikti kvalifikacijos reikalavimą *(Tiekėjas nurodo reikalavimo Nr. pagal SS)*	Pirkimo sutarties dalis, kuriai vykdyti pasitelkiamas ūkio subjektas, EUR arba proc.	Koks pateikiamas įrodymas dėl išteklių prieinamumo[4]
1.	....	....		....

4 lentelė. Reikalavimai susiję su nacionaliniu saugumu

[1] Jeigu pasiūlymą pasirašo ne tiekėjo vadovas, pasiūlyme pateiklama įgaliojimo skaitmeninė kopija.
[2] Taikoma, jei kvalifikacijai įrodyti tiekėjas pasitelkia kvazisubtiekėjus, kurie pasiūlymo pateikimo metu nėra tiekėjo darbuotojai, tačiau jie bus įdarbinti laimėjimo ir Sutarties sudarymo atveju.
[3] Taikoma, jeigu kvalifikacijai atitikti tiekėjas naudosis Tiekėjo kvalifikacijos reikalavimų nustatymo metodikos 8.3 punkte nurodytų trečiųjų asmenų, kurie tiesiogiai aktyviai, savo veiksmais neprisidės prie pirkimo vykdytojo poreikio įsigyti pirkimo objektą tenkinimo, priemonėmis.
[4] Tiekėjas turi pateikti įrodymą , kuriame nurodoma, kuo ir kokia dalimi bus remiamasi kitų ūkio subjektų pajėgumais ir patvirtinantį, kad tiekėjas jų pajėgumais, priemonėmis galės naudotis visą sutarties vykdymo laikotarpį.

Techninės specifikacijos reikalavimas	Įrodantys dokumentai
Tiekėjas privalo įrodyti, kad prekės ar paslaugos nekelia grėsmės nacionaliniam saugumui, kad nėra žemiau nurodytų aplinkybių: 1) programinės įrangos gamintojas ar jį kontroliuojantis asmuo yra registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose; 2) programinės įrangos priežiūra ar palaikymas būtų vykdomas iš VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.	Tiekėjas privalo **PATEIKTI** šiuos dokumentus: 1) programinės įrangos priežiūrą ir palaikymą vykdantis asmuo arba gamintojas ar jį kontroliuojantis asmuo yra juridinis asmuo, pateikiama juridinio asmens vadovo patvirtinta juridinio asmens steigimo dokumentų kopija, Juridinių asmenų registro išplėstinis išrašas su istorija arba atitinkami valstybės narės ar trečiosios šalies dokumentai; 2) programinės įrangos priežiūrą ir palaikymą vykdantis asmuo arba gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo, pateikiama jo asmens tapatybę patvirtinančio dokumento (tapatybės kortelės ar paso) kopija, leidimo verstis atitinkama ūkine veikla patvirtinančio dokumento (pavyzdžiui, verslo liudijimo, individualios veiklos pažymėjimo ir pan.) kopija ir pažyma apie deklaruotą gyvenamąją vietą arba atitinkami valstybės narės ar trečiosios šalies dokumentai.
Nurodomi pateikiami dokumentai:	**Gamintojo raštas.**

5 lentelė. Informacija apie Tiekėjo / Tiekėjų grupės nario/ių ar Ūkio subjekto, kurio pajėgumais remiamasi *(jeigu jis pasitelkiamas)* ar Subtiekėjo (-ų), kurio (-ių) pajėgumais tiekėjas nesiremia, *(jeigu taikomas reikalavimas dėl pašalinimo pagrindų nebuvimo)* juridinio asmens, kitos organizacijos ar jos padalinio asmenis:

PRIVALOMA PAŽYMĖTI IR NURODYTI VISUS JURIDINĮ ASMENĮ SUDARANČIUS ORGANUS/ASMENIS		
☒	Vadovas	*Dalius Butkus*
☐	Valdyba	*įvardyti sudarančius asmenis (į) (narius)*
☐	Stebėtojų taryba ar kitas priežiūros organas	*įvardyti sudarančius asmenis (į) (narius)*
☐	Kitas valdymo organas	*įvardyti sudarančius asmenis (į) (narius)*
☒	Kitas fizinis ar juridinis asmuo, turintis teisę atstovauti tiekėjui ar jį kontroliuoti, jo vardu, priimti sprendimą, sudaryti sandorį (pvz. akcininkas ar pan.)	*UAB Blue Bridge Baltic*
☒	Buhalteris ar kitas asmuo, turintis teisę surašyti ir pasirašyti tiekėjo apskaitos dokumentus	*Vyr. buhalterė Ramutė Kerienė*

6 Lentelė. Tiekėjo techninis pasiūlymas:

Pavadinimas	Reikalaujama charakteristika	Siūlomi parametrai apsiribojimas vien įrašais „atitinka“ ir/arba „taip“ negalimas *(pildoma teikiant pasiūlymą)*
Gamintojas ir programinės įrangos pavadinimas		• *Trend Micro Cloud One Workload Security with Vision One 12 months* • *Trend Micro Cloud One Security with Vision One 12 months*
1. Bendri reikalavimai	- Siūlomas sprendimas turi veikti debesijos pagrindu ir centralizuotai administruojamas naudojant interneto naršyklę, nereikalaujant jokios papildomos	Siūlomas sprendimas veikia debesijos pagrindu ir centralizuotai administruojamas naudojant interneto naršyklę,

	programinės įrangos diegimo valdymo ir administravimo serveriui. - Siūlomas sprendimas turi apimti: a. antivirusinę apsaugą Windows, Linux operacinių sistemų platformoms bei integraciją su VMware virtualizacijos platforma b. interneto turinio bei aplikacijų kontrolęs funkcionalumą c. grėsmių aptikimo, tyrimo ir reagavimo platformos funkcionalumą - Siūlomas produktas turi būti reitinguotas informacinių technologijų tyrimo įstaigos Gartner (http://www.gartner.com) 2021 metų (ar naujesniais) duomenimis tarp lyderių savo produkto kategorijoje ("Leaders magic quadrant"). - Nurodyto funkcionalumo užtikrinimui gali būti pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams ar kelis atskirus centralizuoto valdymo įrankius.	nereikalaujant jokios papildomos programinės įrangos diegimo valdymo ir administravimo serveriui. - Siūlomas sprendimas apima: a. antivirusinę apsaugą Windows, Linux operacinių sistemų platformoms bei integraciją su VMware virtualizacijos platforma b. interneto turinio bei aplikacijų kontrolęs funkcionalumą c. grėsmių aptikimo, tyrimo ir reagavimo platformos funkcionalumą - Siūlomas produktas yra reitinguotas informacinių technologijų tyrimo įstaigos Gartner (http://www.gartner.com) 2021 metų (ar naujesniais) duomenimis tarp lyderių savo produkto kategorijoje ("Leaders magic quadrant"). - Nurodyto funkcionalumo užtikrinimui yra pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams centralizuoto valdymo įrankį.
2. Reikalavimai valdymo ir administravimo funkcionalumui	- Turi leisti rolėmis su skirgintomis administravimo teisėmis paremtą administravimą, galimybę kurti naudotojus su skirtingo lygio teisėmis. Roles turi būti galimybė susikurti pačiai organizacijai ir neturi būti ribojamas jų skaičius - Turi palaikyti vartotojų autentifikavimą SAML 2.0 SSO (Azure AD, Okta) - Turi integruotis su Active Directory ir veiksmai atliekami direktorijoje turi būti sinchronizuojami su saugumo sprendimo centralizuoto valdymo konsole - Valdymo serveriai privalo būti laikomi Europos Sąjungoje ir atitikti BDAR reikalavimus - Turi turėti galimybę iš valdymo konsolės generuoti agentų diegimo programinius kodus (ang. scripts) Windows ir Linux platformoms - Turi palaikyti VMware vCenter (native support) - Turi palaikyti integraciją su AWS, Azure ir Google debesijos platformomis, bei vizualizuoti visus serverius įdiegtus šiose platformose.	- Leidžia rolėmis su skirgintomis administravimo teisėmis paremtą administravimą, turi galimybę kurti naudotojus su skirtingo lygio teisėmis. Yra galimybė roles susikurti pačiai organizacijai ir nėra ribojamas jų skaičius - Palaiko vartotojų autentifikavimą SAML 2.0 SSO (Azure AD, Okta) - Integruojasi su Active Directory ir veiksmai atliekami direktorijoje yra sinchronizuojami su saugumo sprendimo centralizuoto valdymo konsole - Valdymo serveriai yra laikomi Europos Sąjungoje ir atitinka BDAR reikalavimus - Turi galimybę iš valdymo konsolės generuoti agentų diegimo programinius kodus (ang. scripts) Windows ir Linux platformoms - palaiko VMware vCenter (native support) - Palaiko integraciją su AWS, Azure ir Google debesijos platformomis, bei

	- Turi turėti integraciją su organizacijos naudojama LogRhythm SIEM sistema. - Turi turėti galimybę kurti įvairias įrenginių grupes pagal individualiai pasirenkamus parametrus.	vizualizuoja visus serverius įdiegtus šiose platformose. - Turi integraciją su organizacijos naudojama LogRhythm SIEM sistema. Turi galimybę kurti įvairias įrenginių grupes pagal individualiai pasirenkamus parametrus.
3. Palaikomos operacinės sistemos	- Windows Server 2008 R2 - Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2016 - Windows Server 2019 - Red Hat Enterprise Linux 5, 6, 7, 8 - CentOS 5, 6, 7, 8 - Rocky Linux 8 - Oracle Linux 5, 6, 7, 8 - SUSE Linux Enterprise Server 11, 12, 15 - Ubuntu 14, 16, 18, 20 - Debian 7, 8, 9, 10	- Windows Server 2008 R2 - Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2016 - Windows Server 2019 - Red Hat Enterprise Linux 5, 6, 7, 8 - CentOS 5, 6, 7, 8 - Rocky Linux 8 - Oracle Linux 5, 6, 7, 8 - SUSE Linux Enterprise Server 11, 12, 15 - Ubuntu 14, 16, 18, 20 - Debian 7, 8, 9, 10
4. Reikalavimai tarnybinių stočių apsaugos funkcionalumui	**Bazinis apsaugos funkcionalumas:** - Turi turėti apsaugos modulį ir užtikrinti apsaugą nuo virusų, „spyware“, „adware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų. - Turi realiu laiku skenuoti Windows bei Linux operacinių sistemų platformose - Turi turėti galimybę veikti „Air Gap“ tinkle (neturint interneto ryšio) - Turi turėti galimybę nuotoliniu būdu inicijuoti portų skenavimą - Turi turėti galimybę nuotoliniu būdu inicijuoti greitą arba pilną skenavimą nuo virusų ir žalingo kodo - Turi atlikti žalingų veiksmų stebėseną ir aptikti dar nežinomą žalingą programinę įrangą tiek prieš paleidžiant/atidarant rinkmeną, tiek po rinkmenos paleidimo turi būti analizuojamas jos elgesys - Turi turėti bent tris kenkėjiškos programinės įrangos aptikimo metodus: virusų aprašais pagrįstą, mašininio mokymosi ir elgsenos stebėjimo - Turi turėti apsaugos nuo išpirkos reikalaujančios žalingos programinės įrangos („Ransomware“) apsaugą - turi galėti skenuoti archyvuotas rinkmenas - turi turėti integruotą karantino paskyrą	**Bazinis apsaugos funkcionalumas:** - Turi apsaugos modulį ir užtikrina apsaugą nuo virusų, „spyware“, „adware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų. - Realiu laiku skenuoja Windows bei Linux operacinių sistemų platformose - Turi galimybę veikti „Air Gap“ tinkle (neturint interneto ryšio) - Turi galimybę nuotoliniu būdu inicijuoti portų skenavimą - Turi galimybę nuotoliniu būdu inicijuoti greitą arba pilną skenavimą nuo virusų ir žalingo kodo - Atlieka žalingų veiksmų stebėseną ir aptinka dar nežinomą žalingą programinę įrangą tiek prieš paleidžiant/atidarant rinkmeną, tiek po rinkmenos paleidimo yra analizuojamas jos elgesys - Turi tris kenkėjiškos programinės įrangos aptikimo metodus: virusų aprašais pagrįstą, mašininio mokymosi ir elgsenos stebėjimo

	- Turi galimybę automatiškai blokuoti žalingas svetaines, naudojant svetainių reputacijos reitingus - Turi galimybę aprašyti svetainių grupes pagal leidžiamų ir/ar blokuojamų svetainių sąrašus („while list“, „black list“) - Turi galimybę kontroliuoti, leisti ar blokuoti, naudojamas aplikacijas Windows ir Linux operacinių sistemų platformose - Turi turėti aplikacijų užrakinimo funkcionalumą („Application Lockdown“), leidžiantį tarnybinėje stotyje naudoti tik numatytas aplikacijas ir automatiškai blokuojant visas likusias. - Turi turėti integruotą ugniasienę, veikiančią Windows, Linux ir VMware NSX platformose. **Papildomas apsaugos funkcionalumas:** - Turi galimybę stebėti tarnybinių stočių failų integralumą (File integrity monitoring). - Turi galimybę inspektuoti tarnybinių stočių „log'us“, ir informuoti apie aptinkamą įtartiną ar žalingą operacinės sistemos ar programinės įrangos veikimą. - Turi užtikrinti apsaugą nuo pažeidžiamumų („vulnerabilities“) išnaudojimo: a. turi blokuoti pažeidžiamumų išnaudojimą, naudojantis gamintojo host-based IPS taisyklėmis, kurios turi būti periodiškai atnaujinamos b. turi nereikalauti jokios papildomos programinės įrangos ar agento įdiegimo c. tarnybinėms stotims turi būti atliekamas nuolatinis pažeidžiamumų skenavimas ir taikomos automatinės taisyklės aptiktiems pažeidžiamumams	- Turi apsaugos nuo išpirkos reikalaujančios žalingos programinės įrangos („Ransomware“) apsaugą - Gali skenuoti archyvuotas rinkmenas - Turi integruotą karantino paskyrą - Turi galimybę automatiškai blokuoti žalingas svetaines, naudojant svetainių reputacijos reitingus - Turi galimybę aprašyti svetainių grupes pagal leidžiamų ir/ar blokuojamų svetainių sąrašus („while list“, „black list“) - Turi galimybę kontroliuoti, leisti ar blokuoti, naudojamas aplikacijas Windows ir Linux operacinių sistemų platformose - Turi aplikacijų užrakinimo funkcionalumą („Application Lockdown“), leidžiantį tarnybinėje stotyje naudoti tik numatytas aplikacijas ir automatiškai blokuojant visas likusias. - Turi integruotą ugniasienę, veikiančią Windows, Linux ir VMware NSX platformose. **Papildomas apsaugos funkcionalumas:** - Turi galimybę stebėti tarnybinių stočių failų integralumą (File integrity monitoring). - Turi galimybę inspektuoti tarnybinių stočių „log'us“, ir informuoti apie aptinkamą įtartiną ar žalingą operacinės sistemos ar programinės įrangos veikimą. - Užtikrina apsaugą nuo pažeidžiamumų („vulnerabilities“) išnaudojimo: a. blokuoja pažeidžiamumų išnaudojimą, naudojantis gamintojo host-based IPS taisyklėmis, kurios yra periodiškai atnaujinamos b. nereikalauja jokios papildomos

		programinės įrangos ar agento įdiegimo c. tarnybinėms stotims yra atliekamas nuolatinis pažeidžiamumų skenavimas ir taikomos automatinės taisyklės aptiktiems pažeidžiamumams
5.Reikalavimai grėsmių aptikimo, tyrimo ir reagavimo platformos funkcionalumui	- Turi gebėti ieškoti, analizuoti ir koreliuoti duomenis iš ne mažiau kaip šių šaltinių: ▪ tarnybinių stočių ir darbo vietų kompiuterių, ▪ elektroninio pašto (su papildomomis licencijomis), ▪ duomenų perdavimo tinkle (su papildomomis licencijomis) - Turi rinkti ne mažiau kaip šiuos telemetrinius duomenis iš tarnybinių stočių: ▪ tinklo srauto duomenis ▪ komandinės eilutės (CLI) komandas, ▪ registrų pakeitimus, ▪ procesų įvykdymus, ▪ bylų manipuliavimo faktus. - Turi gebėti susieti surinktą informaciją su MITRE taktikos ir technikos ID. - Turi būti galimybės aptikti incidentus, vizualizuoti juos ir pateikti automatinį atsaką. - Turi būti galimybė izoliuoti paveiktą galinį įrenginį. - Turi palaikyti shell, powershell bei individualaus kodo įvykdymą (ang. custom script execution). - Turi būti galimybė prisijungti prie galinio įrenginio ir surinkti informaciją apie vykdomus procesus, tinklo sujungimus, atmintį (memory dump), registrą. - Turi gebėti ieškoti, analizuoti ir koreliuoti duomenis pagal šiuos parametrus: ▪ Įrenginio pavadinimą, ▪ Vartotojo vardą, ▪ IP adresą, ▪ Bylos pavadinimą, ▪ Hash kodą, ▪ MITRE Taktikų ir Technikų ID, ▪ Proceso pavadinimą ir ID, - Turi gebėti gauti kompromitavimo indikatorių sąrašą (angl. *Indicators of Compromise*) iš gamintojo žvalgybinės informacijos ir atlikti jų paiešką organizacijos tinkle.	- Geba ieškoti, analizuoti ir koreliuoti duomenis iš šių šaltinių: ▪ tarnybinių stočių ir darbo vietų kompiuterių, ▪ elektroninio pašto (su papildomomis licencijomis), ▪ duomenų perdavimo tinkle (su papildomomis licencijomis) - Renka šiuos telemetrinius duomenis iš tarnybinių stočių: ▪ tinklo srauto duomenis ▪ komandinės eilutės (CLI) komandas, ▪ registrų pakeitimus, ▪ procesų įvykdymus, ▪ bylų manipuliavimo faktus. - Geba susieti surinktą informaciją su MITRE taktikos ir technikos ID. - Yra galimybės aptikti incidentus, vizualizuoti juos ir pateikti automatinį atsaką. - Yra galimybė izoliuoti paveiktą galinį įrenginį. - Palaiko shell, powershell bei individualaus kodo įvykdymą (ang. custom script execution). - Yra galimybė prisijungti prie galinio įrenginio ir surinkti informaciją apie vykdomus procesus, tinklo sujungimus, atmintį (memory dump), registrą. - Geba ieškoti, analizuoti ir koreliuoti duomenis pagal šiuos parametrus: ▪ Įrenginio pavadinimą, ▪ Vartotojo vardą, ▪ IP adresą, ▪ Bylos pavadinimą, ▪ Hash kodą, ▪ MITRE Taktikų ir Technikų ID, ▪ Proceso pavadinimą ir ID,

	- Turi palaikyti išorinius duomenų tiekėjus TAXII/STIX taip pat MISP platformą įtartinų objektų ir kompromitavimo indikatorių importavimui. - Turi gebėti siųsti kompromitavimo indikatorių informaciją tekstiniu formatu trečių šalių sprendimams. - Turi turėti debesijos pagrindu veikiančią smėliadėžę, joje turi būti galimybė pateikti bylas detonavimui rankiniu būdu per interneto naršyklę arba automatiniu būdu (per API). - Turi gebėti prioritetizuoti sukoreliuotus incidentus pagal kritiškumo lygį, nurodyti atakos paveiktus komponentus ir identifikuoti užkardymo būdus. - Sukoreliuoti incidentai turi būti atvaizduojami vizualiai ir turi būti pateikta priežąstinio ryšio analizė (ang. Root cause analysis), siekiant nustatyti incidento kritiškumą ir poveikį. - Incidentų įspėjimai (ang. Alerts) turi būti grupuojami ir prioritetizuojami naudojant mašininio mokymosi algoritmus. - Turi turėti galimybę kritinio incidento atveju nustatyti automatines atsako priemones: bylų surinkimą, įtraukimą į blokuojamų sąrašą, automatinį bylos nusiuntimą į smėliadėžę, galinio įrenginio izoliavimą. - Turi būti galimybė išsaugoti, importuoti ir eksportuoti paieškos užklausas. - Turi gebėti pateikti organizacijos rizikos laipsnį, bei pateikti rizikingiausių įrenginių ir aplikacijų sąrašus, įvertindama šiuos faktorius: ▪ paskyrų kompromitavimą, ▪ pažeidžiamumų aptikimą, ▪ anomalijų aptikimą (naršymo, vartotojų elgsenos, galinės įrangos elgsenos, debesijos aplikacijų naudojimo), ▪ incidentų aptikimą, ▪ grėsmių detektavimą. - Turi turėti integraciją su Azure AD, Office 365, Okta, ir stebėti vartotojų prisijungimus bei debesijos aplikacijų naudojimą. - Turi turėti integraciją bei dalintis kompromitavimo indikatorių informacija su šių trečių šalių gamintojų tinklo ugniasienėmis - Fortinet PaloAlto, Checkpoint.	- Geba gauti kompromitavimo indikatorių sąrašą (angl. *Indicators of Compromise*) iš gamintojo žvalgybinės informacijos ir atlikti jų paiešką organizacijos tinkle. - Palaiko išorinius duomenų tiekėjus TAXII/STIX taip pat MISP platformą įtartinų objektų ir kompromitavimo indikatorių importavimui. - Geba siųsti kompromitavimo indikatorių informaciją tekstiniu formatu trečių šalių sprendimams. - Turi debesijos pagrindu veikiančią smėliadėžę, joje yra galimybė pateikti bylas detonavimui rankiniu būdu per interneto naršyklę arba automatiniu būdu (per API). - Geba prioritetizuoti sukoreliuotus incidentus pagal kritiškumo lygį, nurodyti atakos paveiktus komponentus ir identifikuoti užkardymo būdus. - Sukoreliuoti incidentai yra atvaizduojami vizualiai ir yra pateikta priežąstinio ryšio analizė (ang. Root cause analysis), siekiant nustatyti incidento kritiškumą ir poveikį. - Incidentų įspėjimai (ang. Alerts) yra grupuojami ir prioritetizuojami naudojant mašininio mokymosi algoritmus. - Turi galimybę kritinio incidento atveju nustatyti automatines atsako priemones: bylų surinkimą, įtraukimą į blokuojamų sąrašą, automatinį bylos nusiuntimą į smėliadėžę, galinio įrenginio izoliavimą. - Yra galimybė išsaugoti, importuoti ir eksportuoti paieškos užklausas. - Geba pateikti organizacijos rizikos laipsnį, bei pateikti rizikingiausių įrenginių ir aplikacijų sąrašus, įvertindama šiuos faktorius: ▪ paskyrų kompromitavimą, ▪ pažeidžiamumų aptikimą, ▪ anomalijų aptikimą (naršymo, vartotojų elgsenos, galinės įrangos elgsenos, debesijos aplikacijų naudojimo),

	- Turi turėti integraciją su organizacijos naudojama LogRhythm SIEM.	▪ incidentų aptikimą, ▪ grėsmių detektavimą. - Turi integraciją su Azure AD, Office 365, Okta, ir stebi vartotojų prisijungimus bei debesijos aplikacijų naudojimą. - Turi integraciją bei dalinasi kompromitavimo indikatorių informacija su šių trečių šalių gamintojų tinklo ugniasienėmis – Fortinet, PaloAlto, Checkpoint. - Turi integraciją su organizacijos naudojama LogRhythm SIEM.
6.Tarnybinių stočių kiekis	Programinė įranga turi būti pateikta 650 vnt. tarnybinių stočių, iš kurių: - bazinis apsaugos funkcionalumas turi būti užtikrintas 450 vnt. tarnybinių stočių (programinės įrangos licencija baziniam apsaugos funkcionalumui); - bazinis ir papildomas apsaugos funkcionalumas turi būti užtikrintas 200 vnt. tarnybinių stočių (programinės įrangos licencija baziniam ir papildomam apsaugos funkcionalumui).	Programinė įranga yra pateikta 650 vnt. tarnybinių stočių, iš kurių: - bazinis apsaugos funkcionalumas yra užtikrintas 450 vnt. tarnybinių stočių (programinės įrangos licencija baziniam apsaugos funkcionalumui); - bazinis ir papildomas apsaugos funkcionalumas yra užtikrintas 200 vnt. tarnybinių stočių (programinės įrangos licencija baziniam ir papildomam apsaugos funkcionalumui).
7. Gamintojo palaikymas	Turi būti suteiktas ne mažesnis nei 1 metų gamintojo palaikymas, užtikrinantis nemokamus programinės įrangos atnaujinimus, programinės įrangos klaidų taisymus. Turi būti suteikta teisė kreiptis į gamintoją iškilus problemai visomis dienomis, visomis valandomis (paslaugos tipas 24x7) (kreipimosi būdas - internetu, elektroniniu paštu, faksu ar telefonu).	Yra suteiktas 1 metų gamintojo palaikymas, užtikrinantis nemokamus programinės įrangos atnaujinimus, programinės įrangos klaidų taisymus. Yra suteikta teisė kreiptis į gamintoją iškilus problemai visomis dienomis, visomis valandomis (paslaugos tipas 24x7) (kreipimosi būdas - internetu, elektroniniu paštu, faksu ar telefonu).

7 lentelė. Tiekėjo finansinis pasiūlymas:

Programinės įrangos pavadinimas	Apsaugos funkcionalumas	Tarnybinių stočių kiekis	Vieneto kaina, EUR be PVM	Iš viso kaina, EUR be PVM
Tarnybinių stočių apsaugos ir grėsmių aptikimo, tyrimo ir reagavimo programinė įranga	Programinės įrangos licencija baziniam apsaugos funkcionalumui	450 vnt.	10012,50	10012,50
	Programinės įrangos licencija baziniam ir papildomam apsaugos funkcionalumui	200 vnt.	22200,00	22200,00

Suma, EUR be PVM:	32212,50
PVM suma, EUR:	6764,63
Pasiūlymo kaina, EUR su PVM:*	38977,13

*Į sutarties kainą įskaitoma PVM, kiti mokesčiai bei visos kitos išlaidos (taip pat ir sąskaitų teikimo elektroniniu būdu išlaidos), susijusios su tinkamu sutarties įvykdymu. Kaina nurodoma ne daugiau kaip 2 skaitmenų po kablelio tikslumu.

Taikomas PVM dydis (%):	*21%*
PVM lengvatos/nemokėjimo teisinis pagrindas (jei taikoma):	*netaikoma*
Pasiūlymo kaina žodžiais:	*Trisdešimt aštuoni tūkstančiai devyni šimtai septyniasdešimt septyni Eur ir trylika ct*

Patvirtiname, kad atidžiai perskaitėme visus sąlygų, techninės specifikacijos reikalavimus ir įsipareigojame jų laikytis vykdydami sutartį jeigu teisės aktų nustatyta tvarka būsime pripažinti laimėtoju. Taip pat įsipareigojame laikytis ir kitų Lietuvos Respublikoje galiojančių pirkimo objektui bei viešojo pirkimo sutarčiai taikomų teisės aktų reikalavimų. Šis pasiūlymas galioja 5 mėnesius nuo pasiūlymų pateikimo termino pabaigos. Pateikdamas CVP IS priemonėmis pateiktą pasiūlymą patvirtinu, kad dokumentų skaitmeninės kopijos ir elektroninėmis priemonėmis pateikti duomenys yra tikri, teisingi ir apima viską, ko reikia tinkamam sutarties įvykdymui.

Pardavimų koordinatorė		Jolita Markevičiūtė
(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas)	(Parašas*[5])	(Vardas, pavardė)

*[5] **Parašas nėra privalomas.**