PIRKIMO–PARDAVIMO SUTARTIS NR. S17-79-V

Vilnius 2017 m. gruodžio 7 d.

VĮ „Infostruktūra“ (toliau – **Pirkėjas**) atstovaujama laikinai einančio direktoriaus pareigas Algimanto Inčiaus, veikiančio pagal 2017 m. vasario 15 d. Lietuvos Respublikos susisiekimo ministro įsakymą Nr. 3P-38, ir **UAB „NT Service“** (toliau – **Pardavėjas**), atstovaujama generalinio direktoriaus Egidijaus Šilansko, veikiančio pagal įmonės įstatus, laimėjusi 2017 m. lapkričio 7 d. skelbtą supaprastinto atviro konkurso būdu vykusį viešąjį pirkimą CVP IS Nr. 353290 (toliau – Pirkimas), sudarė šią sutartį (toliau – Sutartis):

1. SUTARTIES OBJEKTAS

1.1. Pardavėjas įsipareigoja parduoti Pirkėjui internetinių svetainių apsaugos virtualią platformą su techniniu aptarnavimu (toliau – Prekės), o Pirkėjas įsipareigoja priimti ją ir sumokėti šioje sutartyje nurodytą kainą sutarties 6 p. numatyta tvarka.

2. SUTARTIES KAINA

2.1. Sutarčiai taikomas fiksuotos kainos metodas. Sutartyje nustatyta fiksuota prekių kaina nurodyta Sutarties 2 priede.

2.2. Sutarties maksimali kaina su PVM **38.514,30 Eur** (trisdešimt aštuoni tūkstančiai penki šimtai keturiolika eurų 30 ct).

2.3. Įkainiai sutarties vykdymo laikotarpiu negalės būti keičiami per visą sutarties vykdymo laikotarpį, išskyrus kai pasikeičia pridėtinės vertės mokestis (PVM). Perskaičiavimas vykdomas po Lietuvos Respublikos pridėtinės vertės mokesčio įstatymo, kuriuo keičiasi mokesčio tarifas, įsigaliojimo dienos. Pasikeitus PVM tarifo dydžiui, nepateiktų prekių įkainiai keičiami (mažinama ar didinama) proporcingai PVM pasikeitusio tarifo dydžiu. Kainos (įkainių) pakeitimas įforminamas papildomu rašytiniu šalių susitarimu.

2.4. Į Prekių įkainius įskaityti visi Pardavėjo mokami mokesčiai, prekės pristatymo ir kitos išlaidos.

2.5. Pirkimo sutarties sąlygos sutarties galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias pirkimo sutarties sąlygas, kurias pakeitus nebūtų pažeisti Viešųjų pirkimų įstatymo 17 straipsnyje nustatyti principai ir tikslai, bei esant Viešųjų pirkimų įstatymo 89 straipsnyje nustatytoms sąlygoms.

3. PERKAMOS PREKĖS

3.1. Šia sutartimi Pardavėjas įsipareigoja perleisti prekes, kurių detali specifikacija nustatyta šios Sutarties 1 priede.

3.2. Jei dėl nuo Pardavėjo nepriklausančių aplinkybių, kurių nebuvo įmanoma numatyti rengiant pirkimo dokumentus ir/ar sutarties sudarymo metu, Pardavėjas negali pristatyti pasiūlyme nurodyto modelio prekių, sutarties šalims išreiškus sutikimą, nekeičiant sutarties kainos, Pardavėjas gali pristatyti kito modelio prekes su sąlyga, kad naujas modelis visiškai atitiks pirkimo dokumentuose ir sutarties priede keliamus reikalavimus ir bus pristatomas už tą pačią kainą.

4. PREKIŲ PRISTATYMO TVARKA

4.1. Pardavėjas įsipareigoja pristatyti prekes ne vėliau kaip per 10 (dešimt) darbo dienų nuo Sutarties įsigaliojimo dienos. Jei Pardavėjas dėl objektyvių priežasčių negali prekių pristatyti per nurodytą terminą, tai Pirkėjas gali pratęsti prekių pristatymo terminą.

4.2. Prekių pristatymo vieta – Pilies g. 23/15, LT–01123 Vilnius.

5. PREKIŲ KOKYBĖ IR GARANTIJA

5.1. Pardavėjas garantuoja, kad parduodamos Prekės yra be defektų ir jų kokybė, žymėjimas, informacija vartotojui atitinka ES Tarybos Direktyvos 93/42/EEB reikalavimus.

6. ATSISKAITYMAS TARP ŠALIŲ

6.1. Pirkėjas apmoka Pardavėjui už prekes pagal gautas PVM sąskaitas faktūras per 30 (trisdešimt) kalendorinių dienų nuo PVM sąskaitos faktūros gavimo dienos.

6.2. PVM sąskaitos faktūros, sąskaitos faktūros, kreditiniai ir debetiniai dokumentai bei avansinės sąskaitos turi būti teikiami naudojantis informacinės sistemos „E. sąskaita“ priemonėmis. Mokėjimo dokumentų nepateikus „E. sąskaita“ priemonėmis, Pirkėjas turi teisę neatlikti mokėjimo.

7. SUTARTIES ĮVYKDYMO UŽTIKRINIMAS, ATSAKOMYBĖ

7.1. Sutarties įvykdymo užtikrinimo priemonė yra netesybos.

7.2. Pardavėjui padidinus prekių kainą ir dėl šios priežasties Pirkėjui nutraukiant galiojančią sutartį, Pardavėjas moka neįvykdytos sutarties sumos dydžio baudą.

7.3. Jei Pirkėjas dėl savo kaltės vėluoja atsiskaityti su Pardavėju per sutarties 6.1 p. numatytą terminą, jis įsipareigoja sumokėti 0,02 (dviejų šimtųjų) proc. dydžio palūkanas nuo nesumokėtos sumos.

8. FORCE MAJEURE

8.1. Force Majeure sąlygos taikomos vadovaujantis LR Vyriausybės 1996 m. liepos 15d. nutarimu Nr. 840 patvirtintomis „Atleidimo nuo atsakomybės dėl nenugalimos jėgos (Force majeure) aplinkybėmis", taisyklėmis.

9. SUTARTIES GALIOJIMAS IR NUTRAUKIMAS

9.1. Sutartis įsigalioja šalims ją pasirašius ir galioja iki visiško šalių įsipareigojimų pagal šią sutartį įvykdymo, bet ne ilgiau kaip 36 (trisdešimt šešis) mėnesius.

9.2. Pirkėjas turi teisę vienašališkai nutraukti Sutartį, jeigu Pardavėjas ją iš esmės pažeidė:

9.2.1. parduota prekė yra netinkamos kokybės ir jos trūkumų neįmanoma pašalinti per protingą ir Pirkėjui priimtiną terminą;

9.2.2. Pardavėjas nurodytu terminu prekių nepristatė.

9.3. Pardavėjas turi teisę vienašališkai nutraukti Sutartį, jeigu Pirkėjas ją iš esmės pažeidė:

9.3.1. Pirkėjas laiku nesumokėjo už Prekes, kai jos buvo perduotos nustatytais terminais;

9.3.2. Pirkėjas nepriėmė tinkamoms kokybės Prekių, kai jos buvo perduotos nustatytais terminais.

9.4. Sutartis taip pat gali būti nutraukta Šalių raštišku susitarimu.

9.5. Pirkėjas turi teisę nutraukti Sutartį prieš 15 (penkiolika) kalendorinių dienų apie tai raštu įspėjęs Pardavėją.

10. KITOS SĄLYGOS

10.1. Pardavėjas įsipareigoja išrašomoje PVM sąskaitoje faktūroje vartoti tuos pačius prekių pavadinimus ir mato vnt., kokie yra pridedamoje specifikacijoje. Taip pat ant sąskaitos faktūros privalo užrašyti sutarties numerį ir datą, pagal kurią parduodamos prekės.

10.2. Sutarties vykdymo metu Pardavėjo gauta informacija ir dokumentai yra konfidencialūs. Be išankstinio raštiško Pirkėjo leidimo Pardavėjas neskelbia ir neatskleidžia jokių sutarties nuostatų, išskyrus atvejus, kai tai būtina vykdant sutartį.

10.3. Ginčai, kylantys tarp šalių, sprendžiami šalių derybomis, o nepavykus jų išspręsti – teismine tvarka Lietuvos Respublikos teismuose.

10.4. Sutartis sudaryta dviem egzemplioriais, po vieną šalims, lietuvių kalba. Abu egzemplioriai turi vienodą juridinę galią.

10.5. Pardavėjas patvirtina, kad į parduodamas prekes tretieji asmenys neturi jokių teisių.

10.6. Pridedama: Sutarties 1 priedas „Techninė specifikacija"; Sutarties 2 priedas „Tiekėjo pasiūlymas".

11. ŠALIŲ ADRESAI IR REKVIZITAI

PIRKĖJAS
VĮ „Infostruktūra"
Pilies g. 23/15, Vilnius
Juridinio asmens kodas 121738687
PVM mokėtojo kodas: LT217386811
Tel.: +370 52 391708 / faks.: +370 52 791331
Banko rekvizitai:
AB SEB bankas
A/s LT78 7044 0600 0090 8457

Laikinai einantis direktoriaus pareigas
Algimantas Inčius

.....
A.V.

PARDAVĖJAS
UAB „NT Service"
Ateities pl. 34, LT-52165 Kaunas
Juridinio asmens kodas 135188876
PVM mokėtojo kodas: LT351888716
Tel.: +370 37 320222 / faks.: +370 37 320122
Banko rekvizitai:
AB SEB bankas, Kauno filialas
A/s LT26 7044 0600 0320 8002

Generalinis direktorius
Egidijus Šilanskas

.....
A.V.

Deimantas Jonikas
Vyresnysis saugos ekspertas

Darius Skritas
Tinklo technologijų departamento vadovas

Marius Gurskas
Pirkimų projektų vadovas

Jolita Eidukonienė
Vyriausioji buhalterė

Andrius Papinigis
IT skyriaus vadovas

TECHNINĖ SPECIFIKACIJA

Eil. Nr.	Reikalavimas
1	2
INTERNETO SVETAINIŲ APSAUGOS UGNIASIENIŲ SISTEMA (1 komplektas.)	
1.	**IDENTIFIKAVIMO DUOMENYS**
1.1.	Sistemos pavadinimas.
1.2.	Sistemos gamintojas.
1.3.	Visos žemiau išvardytos sistemos ir paslaugų savybės turi būti taikomos kiekvienai licencijuojamai interneto svetainių apsaugos ugniasienių sistemos virtualiai ugniasienei, o visos reikiamos licencijos reikalaujamam funkcionalumui pasiekti turi būti įtrauktos į pateikiamą komplektaciją.
1.4.	Sistemą sudaro trys ugniasienės, kurių kiekviena turi dirbti kaip virtuali mašina (įrenginys) VĮ „Infostruktūra“ dedikuotoje virtualioje infrastruktūroje.
1.5.	**Reikalavimai aukštam patikimumui:**
1.5.1.	Kiekviena sistemos ugniasienė turi funkcionuoti su kitomis ugniasienėmis ir tai sudarytų viena kitą dubliuojančią aukšto patikimumo klasterizuotą sistemą.
1.5.2	Sistema gali būti plečiama naudojant klasterius iš ne mažiau kaip dviejų ugniasienių. Sistema privalo leisti atlikti saugumo nustatymų pakeitimus visose klasterio ugniasienėse vienu metu.
1.5.3.	Sistema privalo palaikyti tris darbo režimus: • Apėjimo – sistema veikia, bet neaptinka ir nesaugo nuo įsibrovimų; • Pasyvus – sistema aptinka įsibrovimus; • Aktyvus – sistema aptinka ir apsaugo nuo įsibrovimų.
2.	**FUNKCINIAI REIKALAVIMAI**
2.1.	Sistemos kiekvieno nario pralaidumas ne mažesnis kaip 200 Mbps.
2.2.	Turi būti galimybė išplėsti kiekvieno klasterio nario pralaidumą iki 1 Gbps (įsigyjant papildomas licencijas).
2.3.	**Apsaugos nuo atakų metodai:**
2.4.	Sistema privalo saugoti taikomąsias programas (interneto svetaines) nuo dešimties dažniausiai pasitaikančių taikomųjų programų (interneto svetainių) atakų, kurias išskyrė OWASP (*The Open Web Security Project*) organizacija.
2.5.	Sistema privalo saugoti nuo WASC (*Web Application Security Consortium*) klasifikuojamų saugos atakų.
2.6.	Sistema privalo saugoti nuo žemiau nurodytų pažeidžiamumų: • SQL injekcija; • Įterptinių komandų atakos (XSS); • CSRF atakos; • Nustatymų klastojimas; • Paslėptų laukelių klastojimas (Hidden field manipulation); • Sesijų klastojimas; • Slapukų užnuodijimas; • Valdymas paslapčia (Stealth commanding); • Nesankcionuoto priėjimo atakos; • Taikomųjų programų buferio perpildymo atakos; • Grubios jėgos atakos; • Duomenų kodavimas atakos; • Nesankcionuotos navigacijos atakos; • SOAP ir Web procesų klastojimas; • Duomenų rinkimo iš tinklapių HTML išeities kodų atakos (Web Scraping).
2.7.	Sistema privalo palaikyti saugumo politiką nepriklausomai nuo simbolių koduotės, siekiant apsaugoti nuo žemiau nurodytų pažeidžiamumų: • URL iššifravimas (pvz.: %XX); • Savaiminis maršrutų nukreipimas (pvz.: that is,. use of /./ and encoded equivalents)); • Maršrutų atgalinis nukreipimas (pvz.: that is,. use of /./ and encoded equivalents); • Mišrus maršrutų nukreipimas; • Pernelyg didelis tarpų ir naujų eilučių (whitespace) naudojimas;

Eil. Nr.	Reikalavimas
1	2
	• Komentarų šalinimas (pvz.: convert DELETE/**/FROM to DELETE FROM); • „Backslash“ simbolio keitimas „forwardslash“ simboliu; • IIS apibrėžtų unikodo ženklo šifruočių keitimas (%uXXYY) • IIS išplėstinių unikodo ženklų; • Virtualių katalogų (directory) maršrutai (positive folder enforcement); • Base64 kodavimas.
2.8.	Sistema privalo naudoti teigiamo saugumo mokymosi modelį arba mokėti nustatyti taisyklių rinkinį, numatantį aplikacijos ar paslaugos elgesį, bei mokėti blokuoti visus srautus, kurie neatitinka šių taisyklių.
2.9.	Sistema neturi reikalauti kriterijų/parašų (signature) atnaujinimų, kurie saugoja nuo naujų grėsmių.
2.10.	**Srauto blokavimo metodai:**
2.10.1.	Sistema turi veikti kaip atvirkštinė tarpinė stotis ir atremti atakas, pagal galimybę sukuriant naujas tinkamai suformuotas užklausas arba ignoruoti užklausas, jei neįmanoma sukurti naujų.
2.10.2.	Sistema turi būti suderinama su šiuo metu VĮ “Infostruktūra” eksploatuojama kibernetinių atakų bei įsilaužimo prevencijos sistema DefensePro bei privalo dirbti DefenseMessaging protokolu, siekiant automatiškai atiduoti informaciją apie aptiktas atakas, kad DefensePro sistema galėtų jas blokuoti prieš atakoms patenkant į tinklą.
2.10.3.	Sistema privalo gebėti aptikti ir blokuoti nesankcionuotas užklausas, įvertindama užklausos siuntėjo įrangos parametrus (pvz. operacinė sistema, naršyklė, ekrano raiška, įskiepiai ir kt.), bet nevertindama IP adreso.
2.10.4.	Sistema privalo leisti pateikti vartotojui personalizuotą aplikacijos klaidos pranešimą, kai Web aplikacijos užklausa yra blokuojama.
2.10.5.	Sistema privalo tikrinti ir blokuoti nepageidaujamas / blogas / netinkamas HTTP / SOAP / XML / JSON užklausas.
2.10.6.	Sistema privalo palaikyti “brute force” saugos taisyklių filtrą.
2.10.7.	Sistema privalo palaikyti duomenų bazių saugos taisyklių filtrą.
2.10.8.	Sistema privalo palaikyti bylų išsiuntimo saugos taisyklių filtrą.
2.10.9.	Sistema privalo palaikyti visuotinių nustatymų saugos taisyklių filtrą.
2.10.10.	Sistema privalo palaikyti HTTP saugos taisyklių filtrą.
2.10.11.	Sistema privalo palaikyti įvykių žurnalo saugos taisyklių filtrą.
2.10.12.	Sistema privalo palaikyti nustatymų saugos taisyklių filtrą.
2.10.13.	Sistema privalo palaikyti maršrutų blokavimo saugos taisyklių filtrą.
2.10.14.	Sistema privalo palaikyti saugaus atsakymo saugos taisyklių filtrą.
2.10.15.	Sistema privalo palaikyti sesijų saugos taisyklių filtrą.
2.10.16.	Sistema privalo palaikyti pažeidžiamumų saugos taisyklių filtrą.
2.10.17.	Sistema privalo palaikyti WEB servisų saugos taisyklių filtrą.
2.10.18.	Sistema privalo palaikyti XML saugos taisyklių filtrą.
2.11.	**Saugos taisyklių valdymas:**
2.11.1.	Sistema privalo mokėti atpažinti patikimus kompiuterinio tinklo įrenginius, stebėdama įprastą tinklo srautą.
2.11.2.	Sistema privalo pati gebėti išmokti aplikacijų elgsenas tinkle, nenaudojant žmogiškųjų išteklių.
2.11.3.	Sistema privalo mokėti pritaikyti automatinį apsaugos lygį, atsižvelgiant į aptiktą ataką.
2.11.4.	Sistema privalo sekti sistemos nustatymų pakeitimus.
2.11.5.	Sistema privalo mokėti automatiškai pritaikyti saugos taisyklių patobulinimus, remiantis srauto ir statistiniais duomenimis.
2.11.6.	Sistema privalo leisti pasirinktinai pertvarkyti automatiškai sukurtas taisyklės, siekiant sumažinti arba panaikinti klaidingą atakų aptikimo reitingą.
2.11.7.	Sistema privalo atlikti apsaugą nuo taikomosios programinės įrangos lygio DoS atakų.
2.11.8.	Sistema privalo leisti koreguoti saugos politikoje nustatytą patikimos įrangos sąrašą (testavimo ir problemų sprendimo tikslais).
2.11.9.	Sistema privalo palaikyti skirtingus autentifikavimo būdus: tokius kaip SSL, SSL Client Certificates ir proxy klientų autentifikavimas.
2.12.	**Stebėsena, valdymas, ataskaitų generavimas:**
2.12.1.	Sistema privalo palaikyti įrangos pajėgumo ir veiksmingumo stebėseną. Pranešimai ir įvykių žurnalai turėtų būti siunčiami SYSLOG ir SMTP protokolu.
2.12.2.	Sistema privalo siųsti pranešimus apie įtartinus įvykius elektroniniu paštu arba SNMP Trap.
2.12.3.	Sistema turi pateikti sistemos ir jos našumo statistikos ataskaitas.

Eil. Nr.	Reikalavimas
1	2
2.12.4.	Sistema turi pateikti aplikacijos įvykių ataskaitas.
2.12.5.	Sistema turi pateikti saugos filtrų įvykių ataskaitas.
2.12.6	Sistema turi leisti automatiškai ir/arba rankiniu būdu formuoti ataskaitas.
2.12.7.	Sistema privalo automatiškai išsiųsti ataskaitas elektroniniu paštu arba kitais metodais.
2.13.	**Sistemos valdymas:**
2.13.1.	Sistema turi palaikyti neigiamą saugumo modelį – sistema turi mokėti atpažinti ir blokuoti neteisėtą srautą, pagal gamintojo iš anksto aprašytas saugumo taisykles.
2.13.2.	Sistema turi palaikyti teigiamą saugumo modelį – sistema turi mokėti atpažinti teisėtus prisijungimus, o visa kita blokuoti.
2.13.3.	Sistema turi palaikyti saugų nuotolinį įrenginio valdymą su prieigos kontrole.
2.13.4.	Sistema privalo turėti galimybę eksportuoti ir importuoti ugniasienės nustatymus bei saugumo taisykles į naują įrenginį.
2.13.5.	Sistema privalo būti suderinama su Radware APSolute Vision (versija 3.9x) centralizuotu valdymo sprendimu.
2.14.	**Reikalavimai garantiniam aptarnavimui:**
2.14.1.	garantinio aptarnavimo trukmė 3 metai nuo sistemos priėmimo-perdavimo akto pasirašymo dienos
2.14.2.	garantinį aptarnavimą sudaro: - konsultacijos ar pagalba el. paštu, telefonu ir/ar internetiniame techninio aptarnavimo centre nustatant gedimą ar įrangos sutrikimo priežastį turi būti teikiamos visą parą (24x7x365); - naujų programinės įrangos versijų pateikimas; - programinės įrangos pataisymų "patch" pateikimas; - prieiga prie gamintojo publikuojamų informacijos šaltinių, susijusių su šios įrangos eksploatacija.

Pirkėjas
Laikinai einantis direktoriaus pareigas
Algimantas Inčius

.....
A.V.

Pardavėjas
Generalinis direktorius
Egidijus Šilanskas

.....
A.V.

TIEKĖJO PASIŪLYMAS

NTSERVICE
UŽDAROJI AKCINĖ BENDROVĖ

Valstybės įmonei „Infostruktūra“

PASIŪLYMAS
DĖL INTERNETO SVETAINIŲ APSAUGOS UGNIASIENIŲ SISTEMOS

2017-11-20 Nr. V-NTS1-11.20
Vilnius

Tiekėjo pavadinimas	UAB „NT Service“,
Tiekėjo adresas	Ateities pl. 34, LT-52165 Kaunas
Už pasiūlymą atsakingo asmens vardas, pavardė	Ramutė Budrevičienė
Telefono numeris	+370 5 268 5222
Fakso numeris	+370 37 320122
El. pašto adresas	ntservice@ntservice.eu

1. Šiuo pasiūlymu pažymime, kad sutinkame su visomis pirkimo sąlygomis, nustatytomis:
1.1. skelbime apie pirkimą;
1.2. kituose pirkimo dokumentuose (jų paaiškinimuose, papildymuose). Teikdamas pasiūlymą, tiekėjas deklaruoja, jog išsamiai susipažino su visomis konkurso sąlygomis, joms neprieštarauja, pateikė visus reikiamus dokumentus, būtinus tam tikroms aplinkybėms pagrįsti arba paneigti.

Siūlome interneto svetainių apsaugos ugniasienių sistemą, kuri atitinka žemiau nurodytus reikalavimus:

Eil. Nr.	Reikalavimas	Tiekėjo siūlomi parametrai
	INTERNETO SVETAINIŲ APSAUGOS UGNIASIENIŲ SISTEMA (1 komplektas)	
1.	**IDENTIFIKAVIMO DUOMENYS**	
1.1.	Sistemos pavadinimas.	AppWall VA
1.2.	Sistemos gamintojas.	Radware Ltd.
1.3.	Visos žemiau išvardytos sistemos ir paslaugų savybės turi būti taikomos kiekvienai licencijuojamai interneto svetainių apsaugos ugniasienių sistemos virtualiai ugniasienei, o visos reikiamos licencijos reikalaujamam funkcionalumui pasiekti turi būti įtrauktos į pateikiamą komplektaciją.	Visos žemiau išvardytos sistemos ir paslaugų savybės taikomos kiekvienai licencijuojamai interneto svetainių apsaugos ugniasienių sistemos virtualiai ugniasienei, o visos reikiamos licencijos reikalaujamam funkcionalumui pasiekti įtrauktos į pateikiamą komplektaciją.
1.4.	Sistemą sudaro trys ugniasienės, kurių kiekviena turi dirbti kaip virtuali mašina (įrenginys) VĮ „Infostruktūra“ dedikuotoje virtualioje infrastruktūroje.	Siūlomą sistemą sudaro trys ugniasienės, kurių kiekviena dirbs kaip virtuali mašina (įrenginys) VĮ „Infostruktūra“ dedikuotoje virtualioje infrastruktūroje.
1.5.	**Reikalavimai aukštam patikimumui:**	
1.5.1.	Kiekviena sistemos ugniasienė turi funkcionuoti su kitomis ugniasienėmis ir tai sudarytų viena kitą dubliuojančią aukšto patikimumo klasterizuotą sistemą.	Kiekviena siūlomos sistemos ugniasienė funkcionuos su kitomis ugniasienėmis ir tai sudarys viena kitą dubliuojančią aukšto patikimumo klasterizuotą sistemą.
1.5.2	Sistema gali būti plečiama naudojant klasterius iš ne mažiau kaip dviejų ugniasienių. Sistema privalo leisti atlikti saugumo nustatymų pakeitimus visose klasterio ugniasienėse vienu metu.	Siūloma sistema gali būti plečiama naudojant klasterius iš ne mažiau kaip dviejų ugniasienių. Sistema leidžia atlikti saugumo nustatymų pakeitimus visose klasterio ugniasienėse vienu metu.
1.5.3.	Sistema privalo palaikyti tris darbo režimus: • Apėjimo – sistema veikia, bet neaptinka ir nesaugo nuo įsibrovimų; • Pasyvus – sistema aptinka įsibrovimus; • Aktyvus – sistema aptinka ir apsaugo nuo įsibrovimų.	Siūloma sistema palaiko tris darbo režimus: • Apėjimo – sistema veikia, bet neaptinka ir nesaugo nuo įsibrovimų; • Pasyvus – sistema aptinka įsibrovimus; • Aktyvus – sistema aptinka ir apsaugo nuo įsibrovimų.
2.	**FUNKCINIAI REIKALAVIMAI**	

Eil. Nr.	Reikalavimas	Tiekėjo siūlomi parametrai
2.1.	Sistemos kiekvieno nario pralaidumas ne mažesnis kaip 200 Mbps.	Siūlomos sistemos kiekvieno nario pralaidumas 200 Mbps.
2.2.	Turi būti galimybė išplėsti kiekvieno klasterio nario pralaidumą iki 1 Gbps (įsigyjant papildomas licencijas).	Siūlomos sistemos kiekvieno klasterio nario pralaidumą pagal poreikį galima plėsti nuo 1 Mbps iki 2 Gbps, įsigyjant papildomas licencijas.
2.3.	**Apsaugos nuo atakų metodai:**	
2.4.	Sistema privalo saugoti taikomąsias programas (interneto svetaines) nuo dešimties dažniausiai pasitaikančių taikomųjų programų (interneto svetainių) atakų, kurias išskyrė OWASP (*The Open Web Security Project*) organizacija.	Siūloma sistema geba saugoti taikomąsias programas (interneto svetaines) nuo dešimties dažniausiai pasitaikančių taikomųjų programų (interneto svetainių) atakų, kurias išskyrė OWASP (*The Open Web Security Project*) organizacija.
2.5.	Sistema privalo saugoti nuo WASC (*Web Application Security Consortium*) klasifikuojamų saugos atakų.	Siūloma sistema saugoja nuo WASC (*Web Application Security Consortium*) klasifikuojamų saugos atakų.
2.6.	Sistema privalo saugoti nuo žemiau nurodytų pažeidžiamumų: • SQL injekcija; • Įterptinių komandų atakos (XSS); • CSRF atakos; • Nustatymų klastojimas; • Paslėptų laukelių klastojimas (Hidden field manipulation); • Sesijų klastojimas; • Slapukų užnuodijimas; • Valdymas paslapčia (Stealth commanding); • Nesankcionuoto priėjimo atakos; • Taikomųjų programų buferio perpildymo atakos; • Grubios jėgos atakos; • Duomenų kodavimas atakos; • Nesankcionuotos navigacijos atakos; • SOAP ir Web procesų klastojimas; • Duomenų rinkimo iš tinklapių HTML išeities kodų atakos (Web Scraping).	Siūloma sistema saugo nuo žemiau nurodytų pažeidžiamumų: • SQL injekcija; • Įterptinių komandų atakos (XSS); • CSRF atakos; • Nustatymų klastojimas; • Paslėptų laukelių klastojimas (Hidden field manipulation); • Sesijų klastojimas; • Slapukų užnuodijimas; • Valdymas paslapčia (Stealth commanding); • Nesankcionuoto priėjimo atakos; • Taikomųjų programų buferio perpildymo atakos; • Grubios jėgos atakos; • Duomenų kodavimas atakos; • Nesankcionuotos navigacijos atakos; • SOAP ir Web procesų klastojimas; • Duomenų rinkimo iš tinklapių HTML išeities kodų atakos (Web Scraping).
2.7.	Sistema privalo palaikyti saugumo politiką nepriklausomai nuo simbolių koduotės, siekiant apsaugoti nuo žemiau nurodytų pažeidžiamumų: • URL iššifravimas (pvz.: %XX); • Savaiminis maršrutų nukreipimas (pvz.: that is,. use of /./ and encoded equivalents)); • Maršrutų atgalinis nukreipimas (pvz.: that is,. use of /./ and encoded equivalents); • Mišrus maršrutų nukreipimas; • Pernelyg didelis tarpų ir naujų eilučių (whitespace) naudojimas; • Komentarų šalinimas (pvz.: convert DELETE/**/FROM to DELETE FROM); • „Backslash" simbolio keitimas „forwardslash" simboliu; • IIS apibrėžtų unikodo ženklo šifruočių keitimas (%uXXYY) • IIS išplėstinių unikodo ženklų; • Virtualių katalogų (directory) maršrutai	Siūloma sistema palaiko saugumo politiką nepriklausomai nuo simbolių koduotės, siekiant apsaugoti nuo žemiau nurodytų pažeidžiamumų: • URL iššifravimas (pvz.: %XX); • Savaiminis maršrutų nukreipimas (pvz.: that is,. use of /./ and encoded equivalents)); • Maršrutų atgalinis nukreipimas (pvz.: that is,. use of /./ and encoded equivalents); • Mišrus maršrutų nukreipimas; • Pernelyg didelis tarpų ir naujų eilučių (whitespace) naudojimas; • Komentarų šalinimas (pvz.: convert DELETE/**/FROM to DELETE FROM); • „Backslash" simbolio keitimas „forwardslash" simboliu; • IIS apibrėžtų unikodo ženklo šifruočių keitimas (%uXXYY) • IIS išplėstinių unikodo ženklų; • Virtualių katalogų (directory) maršrutai

Eil. Nr.	Reikalavimas	Tiekėjo siūlomi parametrai
	(positive folder enforcement); • Base64 kodavimas.	(positive folder enforcement); • Base64 kodavimas.
2.8.	Sistema privalo naudoti teigiamo saugumo mokymosi modelį arba mokėti nustatyti taisyklių rinkinį, numatantį aplikacijos ar paslaugos elgesį, bei mokėti blokuoti visus srautus, kurie neatitinka šių taisyklių.	Siūloma sistema geba naudoti tiek teigiamo tiek ir neigiamo saugumo mokymosi modelius. Sistema leidžia nustatyti saugos taisyklių rinkinį, numatantį aplikacijos ar paslaugos elgesį bei geba blokuoti visus srautus, kurie neatitinka šių taisyklių.
2.9.	Sistema neturi reikalauti kriterijų/parašų (signature) atnaujinimų, kurie saugoja nuo naujų grėsmių.	Siūloma sistema naudoja patentuotą kriterijų/parašų mechanizmą, kuriam nereikia kriterijų/parašų atnaujinimų.
2.10.	**Srauto blokavimo metodai:**	
2.10.1.	Sistema turi veikti kaip atvirkštinė tarpinė stotis ir atremti atakas, pagal galimybę sukuriant naujas tinkamai suformuotas užklausas arba ignoruoti užklausas, jei neįmanoma sukurti naujų.	Siūloma sistema geba veikti kaip atvirkštinė tarpinė stotis ir atremti atakas, pagal galimybę sukuriant naujas tinkamai suformuotas užklausas arba ignoruoja užklausas, jei neįmanoma sukurti naujų. Pvz. kiekvienam užklausos parametrui gali būti sukurta (automatiškai) saugos taisyklė nustatanti jo dydį, tipą ir reikšmę.
2.10.2.	Sistema turi būti suderinama su šiuo metu VĮ "Infostruktūra" eksploatuojama kibernetinių atakų bei įsilaužimo prevencijos sistema DefensePro bei privalo dirbti DefenseMessaging protokolu, siekiant automatiškai atiduoti informaciją apie aptiktas atakas, kad DefensePro sistema galėtų jas blokuoti prieš atakoms patenkant į tinklą.	Siūloma sistema suderinama su šiuo metu VĮ "Infostruktūra" eksploatuojama kibernetinių atakų bei įsilaužimo prevencijos sistema DefensePro bei geba dirbti DefenseMessaging protokolu, kuomet siekiama automatiškai atiduoti informaciją apie aptiktas atakas DefensePro sistemai, kad ji galėtų jas blokuoti prieš atakoms patenkant į tinklą.
2.10.3.	Sistema privalo gebėti aptikti ir blokuoti nesankcionuotas užklausas, įvertindama užklausos siuntėjo įrangos parametrus (pvz. operacinė sistema, naršyklė, ekrano raiška, įskiepiai ir kt.), bet nevertindama IP adreso.	Siūloma sistema geba aptikti ir blokuoti nesankcionuotas užklausas, įvertindama užklausos siuntėjo įrangos parametrus (pvz. operacinė sistema, naršyklė, ekrano raiška, įskiepiai ir kt.), bet nevertindama IP adreso.
2.10.4.	Sistema privalo leisti pateikti vartotojui personalizuotą aplikacijos klaidos pranešimą, kai Web aplikacijos užklausa yra blokuojama.	Siūloma sistema leidžia pateikti vartotojui personalizuotą aplikacijos klaidos pranešimą, kai Web aplikacijos užklausa yra blokuojama.
2.10.5.	Sistema privalo tikrinti ir blokuoti nepageidaujamas / blogas / netinkamas HTTP / SOAP / XML / JSON užklausas.	Siūloma sistema tikrina ir blokuoja nepageidaujamas / blogas / netinkamas HTTP / SOAP / XML / JSON užklausas.
2.10.6.	Sistema privalo palaikyti "brute force" saugos taisyklių filtrą.	Siūloma sistema turi "brute force" saugos taisyklių filtrą (sukuriama saugos taisyklė ir blokuojamas galimo įsilaužėlio IP adresas).
2.10.7.	Sistema privalo palaikyti duomenų bazių saugos taisyklių filtrą.	Siūloma sistema turi duomenų bazių saugos taisyklių filtrą (tikrinamos užklausos siekiant aptikti kenksmingus SQL injekcijos komandas).
2.10.8.	Sistema privalo palaikyti bylų išsiuntimo saugos taisyklių filtrą.	Siūloma sistema turi bylų išsiuntimo saugos taisyklių filtrą.
2.10.9.	Sistema privalo palaikyti visuotinių nustatymų saugos taisyklių filtrą.	Siūloma sistema turi visuotinių nustatymų saugos taisyklių filtrą (tikrina ar užklausos parametrų reikšmės atitinka bendrus/visuotinius saugos nustatymus).
2.10.10.	Sistema privalo palaikyti HTTP saugos taisyklių filtrą.	Siūloma sistema turi HTTP saugos taisyklių filtrą (tikrina HTTP užklausos metodą).
2.10.11.	Sistema privalo palaikyti įvykių žurnalo saugos taisyklių filtrą.	Siūloma sistema turi įvykių žurnalo saugos taisyklių filtrą.
2.10.12.	Sistema privalo palaikyti nustatymų saugos	Siūloma sistema turi nustatymų saugos taisyklių

Eil. Nr.	Reikalavimas	Tiekėjo siūlomi parametrai
	taisyklių filtrą.	filtrą.
2.10.13.	Sistema privalo palaikyti maršrutų blokavimo saugos taisyklių filtrą.	Siūloma sistema turi maršrutų blokavimo saugos taisyklių filtrą (blokuojama nesankcionuota prieiga prie bendro pobūdžio bylų ir aplankų).
2.10.14.	Sistema privalo palaikyti saugaus atsakymo saugos taisyklių filtrą.	Siūloma sistema turi saugaus atsakymo saugos taisyklių filtrą (išsiunčiamos žinutės turinyje aptinka nutekinamą arba neteisėtą turinį).
2.10.15.	Sistema privalo palaikyti sesijų saugos taisyklių filtrą.	Siūloma sistema turi sesijų saugos taisyklių filtrą (nutolusiems naudotojams neleidžiama keisti sesijos būsenos informacijos ir patvirtinti).
2.10.16.	Sistema privalo palaikyti pažeidžiamumų saugos taisyklių filtrą.	Siūloma sistema turi pažeidžiamumų saugos taisyklių filtrą.
2.10.17.	Sistema privalo palaikyti WEB servisų saugos taisyklių filtrą.	Siūloma sistema turi WEB servisų saugos taisyklių filtrą.
2.10.18.	Sistema privalo palaikyti XML saugos taisyklių filtrą.	Siūloma sistema turi XML saugos taisyklių filtrą (tikrinamas post užklausos XML turinys ir struktūrizuojamos XML inkapsuliuotos reikšmės, joms priskiriant parametrus, kurie tikrinami pritaikant tolimesnius saugos filtrus).
2.11.	**Saugos taisyklių valdymas:**	
2.11.1.	Sistema privalo mokėti atpažinti patikimus kompiuterinio tinklo įrenginius, stebėdama įprastą tinklo srautą.	Siūloma sistema moka atpažinti patikimus kompiuterinio tinklo įrenginius, stebėdama įprastą tinklo srautą.
2.11.2.	Sistema privalo pati gebėti išmokti aplikacijų elgsenas tinkle, nenaudojant žmogiškųjų išteklių.	Siūloma sistema pati geba išmokti aplikacijų elgsenas tinkle, nenaudojant žmogiškųjų išteklių.
2.11.3.	Sistema privalo mokėti pritaikyti automatinį apsaugos lygį, atsižvelgiant į aptiktą ataką.	Siūloma sistema moka pritaikyti automatinį apsaugos lygį, atsižvelgiant į aptiktą ataką.
2.11.4.	Sistema privalo sekti sistemos nustatymų pakeitimus.	Siūloma sistema geba sekti sistemos nustatymų pakeitimus.
2.11.5.	Sistema privalo mokėti automatiškai pritaikyti saugos taisyklių patobulinimus, remiantis srauto ir statistiniais duomenimis.	Siūloma sistema moka automatiškai pritaikyti saugos taisyklių patobulinimus, remiantis srauto ir statistiniais duomenimis.
2.11.6.	Sistema privalo leisti pasirinktinai pertvarkyti automatiškai sukurtas taisyklės, siekiant sumažinti arba panaikinti klaidingą atakų aptikimo reitingą.	Siūloma sistema leidžia pasirinktinai pertvarkyti automatiškai sukurtas taisyklės, siekiant sumažinti arba panaikinti klaidingą atakų aptikimo reitingą.
2.11.7.	Sistema privalo atlikti apsaugą nuo taikomosios programinės įrangos lygio DoS atakų.	Siūloma sistema atlieka apsaugą nuo taikomosios programinės įrangos lygio DoS atakų.
2.11.8.	Sistema privalo leisti koreguoti saugos politikoje nustatytą patikimos įrangos sąrašą (testavimo ir problemų sprendimo tikslais).	Siūloma sistema leidžia koreguoti saugos politikoje nustatytą patikimos įrangos sąrašą (testavimo ir problemų sprendimo tikslais).
2.11.9.	Sistema privalo palaikyti skirtingus autentifikavimo būdus: tokius kaip SSL, SSL Client Certificates ir proxy klientų autentifikavimas.	Siūloma sistema palaiko skirtingus autentifikavimo būdus: SSL, SSL Client Certificates ir proxy klientų autentifikavimas.
2.12.	**Stebėsena, valdymas, ataskaitų generavimas:**	
2.12.1.	Sistema privalo palaikyti įrangos pajėgumo ir veiksmingumo stebėseną. Pranešimai ir įvykių žurnalai turėtų būti siunčiami SYSLOG ir SMTP protokolu.	Siūloma sistema atlieka įrangos pajėgumo ir veiksmingumo stebėseną. Pranešimai ir įvykių žurnalai siunčiami SYSLOG ir SMTP protokolu.
2.12.2.	Sistema privalo siųsti pranešimus apie įtartinus įvykius elektroniniu paštu arba SNMP Trap.	Siūloma sistema geba siųsti pranešimus apie įtartinus įvykius elektroniniu paštu arba SNMP Trap.
2.12.3.	Sistema turi pateikti sistemos ir jos našumo	Siūloma sistema geba teikti sistemos ir jos našumo

Eil. Nr.	Reikalavimas	Tiekėjo siūlomi parametrai
	statistikos ataskaitas.	statistikos ataskaitas.
2.12.4.	Sistema turi pateikti aplikacijos įvykių ataskaitas.	Siūloma sistema geba teikti aplikacijos įvykių ataskaitas.
2.12.5.	Sistema turi pateikti saugos filtrų įvykių ataskaitas.	Siūloma sistema geba teikti saugos filtrų įvykių ataskaitas.
2.12.6	Sistema turi leisti automatiškai ir/arba rankiniu būdu formuoti ataskaitas.	Siūloma sistema leidžia automatiškai ir/arba rankiniu būdu formuoti ataskaitas.
2.12.7.	Sistema privalo automatiškai išsiųsti ataskaitas elektroniniu paštu arba kitais metodais.	Siūloma sistema geba automatiškai išsiųsti ataskaitas elektroniniu paštu arba kitais metodais (SNMP, Syslog, OPSEC ELA, ODBC.).
2.13.	**Sistemos valdymas:**	
2.13.1.	Sistema turi palaikyti neigiamą saugumo modelį – sistema turi mokėti atpažinti ir blokuoti neteisėtą srautą, pagal gamintojo iš anksto aprašytas saugumo taisykles.	Siūloma sistema naudoja neigiamą saugumo modelį – sistema moka atpažinti ir blokuoti neteisėtą srautą, pagal gamintojo iš anksto aprašytas saugumo taisykles.
2.13.2.	Sistema turi palaikyti teigiamą saugumo modelį – sistema turi mokėti atpažinti teisėtus prisijungimus, o visa kita blokuoti.	Siūloma sistema naudoja teigiamą saugumo modelį – sistema moka atpažinti teisėtus prisijungimus, o visa kita blokuoja.
2.13.3.	Sistema turi palaikyti saugų nuotolinį įrenginio valdymą su prieigos kontrole.	Siūloma sistema užtikrina saugų nuotolinį įrenginio valdymą su prieigos kontrole.
2.13.4.	Sistema privalo turėti galimybę eksportuoti ir importuoti ugniasienės nustatymus bei saugumo taisykles į naują įrenginį.	Siūloma sistema leidžia eksportuoti ir importuoti ugniasienės nustatymus bei saugumo taisykles į naują įrenginį.
2.13.5.	Sistema privalo būti suderinama su Radware APSolute Vision (versija 3.9x) centralizuotu valdymo sprendimu.	Siūloma sistema suderinama su Radware APSolute Vision (versija 3.9x) centralizuotu valdymo sprendimu.
2.14.	**Reikalavimai garantiniam aptarnavimui:**	
2.14.1.	garantinio aptarnavimo trukmė 3 metai nuo sistemos priėmimo-perdavimo akto pasirašymo dienos	Siūlomos sistemos garantinio aptarnavimo trukmė 3 metai nuo sistemos priėmimo-perdavimo akto pasirašymo dienos
2.14.2.	garantinį aptarnavimą sudaro: - konsultacijos ar pagalba el. paštu, telefonu ir/ar internetiniame techninio aptarnavimo centre nustatant gedimą ar įrangos sutrikimo priežastį turi būti teikiamos visą parą (24x7x365); - naujų programinės įrangos versijų pateikimas; - programinės įrangos pataisymų "patch" pateikimas; - prieiga prie gamintojo publikuojamų informacijos šaltinių, susijusių su šios įrangos eksploatacija.	Siūlomos sistemos garantinį aptarnavimą sudaro: - konsultacijos ar pagalba el. paštu, telefonu ir/ar internetiniame techninio aptarnavimo centre nustatant gedimą ar sistemos sutrikimo priežastį turi būti teikiamos visą parą (24x7x365); - naujų programinės įrangos versijų pateikimas; - programinės įrangos pataisymų "patch" pateikimas; - prieiga prie gamintojo publikuojamų informacijos šaltinių, susijusių su siūlomos sistemos eksploatacija.

Bendra pasiūlymo kaina (skaičiais ir žodžiais): **31.830,00 Eur (trisdešimt vienas tūkstantis aštuoni šimtai trisdešimt eurų) (be PVM).**

PVM, kuris sudaro (skaičiais ir žodžiais) **6.684,30 Eur (šeši tūkstančiai šeši šimtai aštuoniasdešimt keturi eurai ir 30 centų).**

Bendra pasiūlymo kaina (skaičiais ir žodžiais): **38.514,30 Eur(trisdešimt aštuoni tūkstančiai penki šimtai keturiolika eurų ir 30 centų) (su PVM).**

Mūsų pasiūlymas visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus.

Generalinis direktorius Egidijus Šilanskas

Ateities pl. 34, Kaunas LT-52165, Lietuva, Tel.: 8-37-320222, faks.: 8-37-320122, el. paštas: ntservice@ntservice.eu
Įmonės kodas 135188876, PVM mokėtojo kodas LT351888716, registruota VĮ Registrų centras

Pirkėjas
Laikinai einantis direktoriaus pareigas
Algimantas Inčiūra

.....
A.V.

Pardavėjas
Generalinis direktorius
Egidijus Šilanskas

.....
A.V.