

LĪGUMS Nr. 05-03/57
par informācijas sistēmu automātiskās drošības testēšanas rīka
nodrošināšanu un integrāciju esošajās sistēmās

Rīgā

2014. gada 26. februārī

Valsts akciju sabiedrība „Tiesu namu aģentūra”, reģistrācijas numurs 40003334410, juridiskā adrese Baldones iela 1B, Rīga, LV-1007, tās valdes locekles Santas Sausiņas personā, kura rīkojas saskaņā ar sabiedrības statūtiem, turpmāk tekstā – Pasūtītājs, no vienas puses, un

sabiedrība ar ierobežotu atbildību „Analytica”, reģistrācijas numurs 40003823267, juridiskā adrese Tērbatas iela 32, Rīga, LV 1011, tās prokūrista Jura Pūces personā, kurš rīkojas saskaņā ar 2012. gada 2. aprīlī izdotu prokūru, turpmāk tekstā – Izpildītājs, no otras puses,

Pasūtītājs un Izpildītājs kopā/atsevišķi turpmāk tekstā – Puses/Puse, pamatojoties uz iepirkuma „Informācijas sistēmu automātiskās drošības testēšanas rīka nodrošināšana un integrācija esošajās sistēmās”, identifikācijas Nr. TNA 2014/4, rezultātiem, noslēdz šādu līgumu, turpmāk tekstā – Līgums.

1. LĪGUMA PRIEKŠMETS

- 1.1. Pasūtītājs uzdod, bet Izpildītājs apņemas saskaņā ar Līguma noteikumiem un Pasūtītāja dotajiem norādījumiem, savlaicīgi un atbilstošā kvalitātē veikt informācijas sistēmu automātiskās drošības testēšanas rīka nodrošināšanu un integrāciju esošajās sistēmās šajā Līgumā noteiktajā kārtībā saskaņā ar tehnisko specifikāciju (Līguma 1. pielikums), turpmāk tekstā - Pakalpojumi.
- 1.2. Izpildītājs sniedz Līguma 1.1. punktā minētos pakalpojumus sākot ar 2014. gada 1. martu un turpina sniegt līdz 2016. gada 29. februārim.

2. LĪGUMA SUMMA UN APMAKSAS KĀRTĪBA

- 2.1. Cena par Līguma 1.1. punktā minēto Pakalpojumu sniegšanu ir EUR 20811,52 (divdesmit tūkstoši astoņi simti vienpadsmit *euro* un 52 centi), ietverot pievienotās vērtības nodokli 21%.
- 2.2. Līguma summā ietilpst visas ar Tehniskajā specifikācijā (Līguma pielikums Nr. 1) noteikto prasību izpildi saistītās izmaksas, visi piemērojamie nodokļi, personāla izmaksas, kā arī visas ar to netieši saistītās izmaksas (dokumentācijas drukāšana, transporta pakalpojumi u.c.).
- 2.3. Samaksa par Līguma 1.1. punktā noteikto Pakalpojumu izpildi tiek veikta 10 (desmit) darba dienu laikā pēc rēķina un nodošanas pieņemšanas akta iesniegšanas uzsākot Pakalpojuma lietošanu, pārskaitot attiecīgo summu uz Izpildītāja norādīto bankas kontu.

3. PUŠU TIESĪBAS UN PIENĀKUMI

- 3.1. Izpildītāja personālam ir tiesības izmantot Pasūtītāja tehnisko un sistēmu nodrošinājumu, ja tas ir nepieciešams Izpildītāja saistību veikšanai. Izpildītājs apņemas ievērot Pasūtītāja noteiktos ekspluatācijas noteikumus.
- 3.2. Pasūtītājam ir pienākums nodrošināt Izpildītāju ar nepieciešamo pieeju Pasūtītāja dokumentācijai, kā arī nodrošināt savu darbinieku atbalstu Izpildītājam Pakalpojuma veikšanai.
- 3.3. Pasūtītājs sniedz visu Pasūtītāja rīcībā esošo informāciju, kas nepieciešama šī Līguma izpildei.
- 3.4. Bez otras Puses iepriekšējas rakstiskas piekrišanas Puses apņemas neizpaust informāciju par otru Pusi, ko Puses ieguvušas šī Līguma izpildes gaitā.
- 3.5. Ja vienas Puses saistību izpildes nokavējums (tikai tāds nokavējums, kas ietekmē otras Puses spējas izpildīt savas saistības) liedz otrai Pusei veikt savlaicīgu saistību izpildi, tad otras Puses saistību izpildes termiņš tiek pagarināts par pirmās Puses nokavēto laika posmu. Pusei, kura

prasa, lai minēto apstākļu dēļ tiktu pagarināts saistību izpildes termiņš, ir pienākums iesniegt pierādījumus, kuri apliecina otras Puses saistību izpildes nokavējuma faktu.

- 3.6. Ja tas ir nepieciešams, Izpildītājam ir tiesības pieaicināt Līguma izpildē trešās personas, par to iepriekš informējot Pasūtītāju. Izpildītājs uzņemas pilnu atbildību par trešo personu sniegtajiem pakalpojumiem. Ja Pasūtītājs iebilst pret konkrētās trešās personas piesaisti, Izpildītājam ir pienākums ievērot šo iebildumu un nepiesaistīt attiecīgo personu.
- 3.7. Izpildītājs nav atbildīgs par jebkādiem Pasūtītāja sistēmas darbības traucējumiem, ja vien tie nav radušies Izpildītāja darbības (pakalpojuma sniegšanas) rezultātā. Izpildītāja vainas dēļ radušās nepilnības tiek novērstas uz Izpildītāja rēķina iespējami īsā laikā pēc to atklāšanas.
- 3.8. Pušu tiesības un pienākumus, kas nav atrunāti šajā Līgumā, nosaka Latvijas Republikā spēkā esošie normatīvie akti.

4. PAKALPOJUMU SNIEGŠANAS KĀRTĪBA

- 4.1. Katra no Pusēm nozīmē atbildīgo personu šī Līguma izpildei. Pasūtītājs no savas puses nozīmē Infrastruktūras attīstības daļas vadītāju Sandi Vuli (tālrunis 67804744, e-pasts: sandis.vulis@tna.lv), Izpildītājs no savas puses nozīmē Juri Pūci (tālrunis 67471283, e-pasts: juris.puce@analytica.lv).
Atbildīgo personu maiņas gadījuma, Puses nekavējoties par to rakstiski informē otru Pusi.
- 4.2. Parakstot nodošanas-pieņemšanas aktu, Pasūtītājs atsakās no pretenzijām par veiktajiem Pakalpojumiem, izņemot slēptos trūkumus, kurus Pasūtītājs nevar noteikt nodošanas brīdī. Pakalpojumu nepilnības, kas radušās Izpildītāja vainas dēļ un tikušas atklātas pēc Pakalpojumu nodošanas – pieņemšanas akta abpusējas parakstīšanas, jānovērš iespējami īsā laikā uz Izpildītāja rēķina.

5. LĪGUMA TERMIŅŠ

- 5.1. Līgums stājas spēkā ar 2014. gada 1. martu un ir noslēgts uz Līguma 1.2. punktā noteikto termiņu, un spēkā līdz šajā Līgumā noteikto Pušu saistību pilnīgai izpildei.

6. LĪGUMA LAUŠANA

- 6.1. Pusēm savstarpēji vienojoties ir tiesības pārtraukt šo Līgumu jebkurā brīdī.
- 6.2. Pasūtītājam ir tiesības atkāpties no Līguma bez jebkādu zaudējumu atlīdzības pienākuma, rakstveidā informējot par to Izpildītāju vismaz 30 (trīsdesmit) dienas pirms Līguma pārtraukšanas.
- 6.3. Izpildītājam ir tiesības atkāpties no Līguma, ja Pasūtītājs nepamatoti kavē Līgumā noteiktos maksājuma termiņus vairāk par 30 (trīsdesmit) dienām un minētais trūkums nav novērsts 10 (desmit) darba dienu laikā pēc Izpildītāja rakstveida brīdinājuma, par iepriekš minētā termiņa iestāšanos, saņemšanas.

7. NEPĀRVARAMA VARA

- 7.1. Puses tiek atbrīvotas no atbildības par Līguma nepildīšanu, ja tā rodas pēc Līguma noslēgšanas nepārvaramas varas vai ārkārtēju apstākļu ietekmes rezultātā, kurus attiecīgā Puse nevarēja paredzēt, novērst, ietekmēt, t.i. stihiskas nelaiimes, kara darbība, blokāde, civiliedzīvotāju nemieri, streiki.
- 7.2. Pusei, kura pamatojas uz nepārvaramas varas apstākļiem kā saistību vai pienākumu neizpildes iemeslu, 10 (desmit) kalendāro dienu laikā no šādu apstākļu konstatēšanas par to ir rakstveidā jāinformē otra Puse, turklāt, šādu nepārvaramas varas apstākļu iestāšanās jābūt pamatotai ar attiecīgiem pierādījumiem.

8. CITI NOSACĪJUMI

- 8.1. Jebkuri Līguma grozījumi vai papildinājumi ir noformējami rakstveidā, apstiprināmi ar Pušu pārstāvju parakstiem, pievienojami šim Līgumam un kļūst par tā neatņemamu sastāvdaļu.

- 8.2. Visi strīdi un domstarpības starp Pusēm, kas var rasties Līguma izpildes gaitā, tiek risinātas sarunu ceļā. Ja Pusēm neizdodas vienoties sarunu ceļā, strīdi tiek izskatīti Latvijas Republikas tiesā, Latvijas Republikas normatīvajos aktos noteiktajā kārtībā;
- 8.3. Šis Līgums sagatavots uz 7 (septiņām) lapām 2 (divos) eksemplāros, pa vienam eksemplāram katrai Pusei.

9. PUŠU REKVIZĪTI UN PARAKSTI

IZPILDĪTĀJS

SIA „Analytica”

Reģ. Nr. 40003823267

Juridiskā adrese Tērbatas iela 32,

Rīga, LV 1011

Banka: AS "Swedbank"

Kods HABALV22

Konta Nr. LV18HABA0551013143775

PASŪTĪTĀJS

VAS „Tiesu namu aģentūra”

Reģ. Nr. LV40003334410

Juridiskā adrese Baldones iela 1B,

Rīga, LV-1007

Banka: AS „SEB banka”

Kods UNLALV2X

Konta Nr. LV64UNLA0002021469371

/J. Pūce/



/S. Sausiņa/

TEHNISKĀ SPECIFIKĀCIJA

Piedāvātajam pakalpojumam jāietver automatizētas drošības pārbaudes sistēmas pieejamības nodrošināšana uz 2 (divu) gadu periodā un jānodrošina šāda funkcionalitāte:

1. Vispārējā funkcionalitāte	Risinājums automatizē ievainojamību pārvaldības procesu organizācijas iekšienē, noteiktajām IP adresēm, kas sevī iekļauj – tīkla resursu noteikšana un attēlošana teksta un grafiskā formā, tīkla iekārtu pārbaude, nosakot to ievainojamības un veidojot atskaites par tām, ievainojamību novēršanas procesa kontrole.
2. Vispārējās drošības pārbaudes	<p>Risinājumam jābūt iepriekš izveidotiem pārbaudītu un resursu noteikšanas parametru kopumiem kā arī iespējai šādus kopumus veidot lietotājam, ļaujot izvēlēties sekojošas darbības:</p> <ul style="list-style-type: none">- definēt pārbaudē iekļaujamos TCP portus;- definēt pārbaudē iekļaujamos UDP portus;- definēt ievainojamību noteikšanā iekļaujamās ievainojamības (pilna pārbaude, SANS20sarakstā iekļautās, OVAL iekļautās, u.t.t.);- autentificēšanās iespējas izmantošana;- izmantot paroļu minēšanas mēģinājumus ar iespēju izvēlēties iepriekš noteiktu paroļu sarakstu vai arī tās pašam pievienojot;- definēt vienlaicīgu HTTP procesu skaitu un pakešu sūtījumu intensitāti, atkarībā no pieejamo pārbaudītu ierīču skaita. <p>Risinājumam jānodrošina automātiska ievainojamību datu bāzu atjaunināšana no vismaz NIST un CVS datu bāzēm visā darbības periodā.</p> <p>Tīkla resursu pārbaudes (tīkla diski (CIFS, WebDav un cita veida tīkla diski) ar autentificētu lietotāju un anonīmi.</p> <p>Microsoft Active Directory domēna drošības pārbaudes (pārbaudot pieslēgto serveru/datoru ievainojamības un konfigurācijas parametrus) gan anonīmi, gan ar autorizētu domēna lietotāju.</p>
3. Web aplikāciju pārbaudes	Veicot web aplikāciju pārbaudes risinājumam jānodrošina vismaz šādas pārbaudes: <ul style="list-style-type: none">- OWASP Top 10 metodoloģijai atbilstošās pārbaudes;- OSSTMM metodoloģijai atbilstošās pārbaudes;- Web aplikāciju automātiska funkcionalitātes identificēšana (HTML linki);- autorizācijas iespējas (GET un POST formu bāzēta autentifikācija).
4. Interfeisi un resursi	Risinājumam ir jānodrošina automātisko pārbaudītu veikšana šādiem resursiem: <ol style="list-style-type: none">1. Vispārējās drošības pārbaudes (skat. iepriekš):<ol style="list-style-type: none">A. pārbaudītu veikšanai no ārpusē (no Piegādātāja nodrošinātiem datu centriem) – vismaz 100 IP adreses;B. pārbaudītu veikšana no Pasūtītāja tīkla iekšējā segmenta (uzstādot atbilstošu iekārtu iekšējā tīklā) vismaz 100 IP adresēm.

	<p>2. Web aplikāciju pārbaudes (skat. iepriekš):</p> <p>A. vismaz 6 web aplikācijas (pārbaude iespējama gan no iekšpuses, gan no ārpuses).</p>
5. Autentificēšanās iespēja	Risinājumam jābūt iespējamam veikt padziļinātu pārbaudi, autorizējoties vismaz šādās sistēmās: Windows, Unix, Oracle, Oracle Listener and SNMP.
6. Integrācija ar CA Unicenter ServiceDesk	<p>Risinājumam jānodrošina iespēja automātiski atvērt atbilstošu drošības ievainojamību/incidentu CA Unicenter ServiceDesk sistēmā un automātiski pareizi maršrutizēt to atbilstošajai, par drošību atbildīgajai personai.</p> <p>Risinājumam jānodrošina eskalācijas procedūras CA Unicenter ServiceDesk sistēmā.</p> <p>Risinājumam jānodrošina automātiska incidenta slēgšana CA Unicenter ServiceDesk sistēmā, ja drošības incidents tiek atzīts par <i>false positive</i> vai arī tiek veiktas atbilstošās korekcijas informācijas sistēmā, kas novērš drošības ievainojamību.</p>
7. Risinājuma komponentes	<p>Risinājumam jāsaturs vismaz sekojošas komponentes:</p> <ul style="list-style-type: none"> - atskaišu kopsavilkums; - gala iekārtu noteikšanas rīki; - gala iekārtu pārbaudes rīki; - darbību ieplānošana (<i>scheduling</i>); - atskaišu sagatavošana; - ievainojamību novēršanas kontrole; - Web lapu pārbaudīšanas komponente (SQL Injection un citām ievainojamībām); - meklēšana; - lietotāju pārvaldības rīks.
8. Komponente: Atskaišu kopsavilkums	<p>Risinājumā jābūt atskaišu kopsavilkuma komponente, kurā atspoguļojama vismaz sekojoša informācija:</p> <ul style="list-style-type: none"> - ievainojamību skaits pēc bīstamības pakāpes (pakāpes iepriekš definētas); - ievainojamību skaits, šķiroti pēc statusa (atvērts, atrisināts vai apstiprināts); - izveidoto ievainojamību novēršanas uzdevumu skaits, šķiroti pēc bīstamības pakāpes, vidējais novēršanas laiks; - Top 10 Izveidoto ievainojamības novēršanas uzdevumi; - Top 10 Ievainojamības; - visievainojamākās atrastās gala iekārtas infrastruktūrā; - risinājumam jānodrošina lietotājam iespēja mainīt atskaišu kopsavilkuma iestatījumus, mainot norādāmo informāciju.
9. Komponente: Gala iekārtu noteikšanas rīki	<p>Risinājumam jānodrošina iespēja atrast gala iekārtas un attēlot rezultātus teksta vai grafiskā veidā, sastādot tīkla karti, kas izveidota pamatojoties uz meklēšanas sākumā ievadīto informāciju:</p> <ul style="list-style-type: none"> - iepriekš definētām gala iekārtu grupām; - iepriekš definētām domēnu adresēm; - definētām IP adresēm vai to diapazonu; - izvēlētajai iekārtai, kura paredzēta gala iekārtu noteikšanai.

<p>10. Komponente: Gala iekārtu pārbaudīšanas rīki</p>	<p>Risinājumam jānodrošina iespēja pārbaudīt gala iekārtu ievainojamību, pamatojoties uz lietotāja ievadītu informāciju:</p> <ul style="list-style-type: none"> - iepriekš definētām gala iekārtu grupām; - iepriekš definētām domēnu adresēm; - definētām IP adresēm vai to diapazonu; - iepriekš definētām ievainojamību meklēšanas iestatījumu kopumam; - izvēlētajai iekārtai, kura paredzēta gala iekārtu pārbaudei.
<p>11. Komponente: Darbību ieviešana</p>	<p>Risinājumam jānodrošina iespējāmība ieplānot automātiskas gala iekārtu noteikšanas un gala iekārtu pārbaudes, pamatojoties uz lietotāja ievadītu informāciju:</p> <ul style="list-style-type: none"> - iepriekš definētu gala iekārtu; - iepriekš definētām domēnu adresēm; - definētām IP adresēm vai to diapazonu; - izvēlēto iekārtu pārbaudes vai meklēšanas veikšanai; - datumu un laiku; - darbību biežumu.
<p>12. Komponente: Atskaišu sagatavošana</p>	<p>Risinājumam jānodrošina iespēja izveidot atskaites pēc iepriekš definētiem paraugiem:</p> <ul style="list-style-type: none"> - atskaites vadībai par ievainojamības novēršanas gaitu; - apkopotā atskaite vadībai; - SANS20 Atskaite; - atskaite tehniskajiem darbiniekiem; - atskaite par iepriekš norādītu gala iekārtu kopumu; - atskaite par ievainojamību novēršanas uzdevumu skaitu norādītajam risinājuma lietotājam; - atskaite par ievainojamību novēršanas uzdevumu skaitu, kādai konkrētai ievainojamībai; - atklāto, nezināmo gala iekārtu saraksts. <p>Risinājumam jānodrošina iespēja definēt atskaišu izveidošanas šablonus pēc sekojošiem parametriem:</p> <ul style="list-style-type: none"> - ievainojamību pārbaudes rezultāti; - ievainojamību novēršanas uzdevuma statusi; - iepriekš definētas gala iekārtu grupas; - iepriekš definētas domēnu adreses; - definētas IP adreses vai to diapazoni. <p>Risinājumam jāspēj šķirot atskaites pēc sekojošiem parametriem:</p> <ul style="list-style-type: none"> - gala iekārtas; - ievainojamības; - operētājsistēmas; - gala iekārtu grupas; - servisi; - porti. <p>Visām veidotajām atskaitēm jābūt eksportējamām vismaz sekojošos formātos HTML, PDF, CSV un XML.</p>
<p>13. Komponente: Ievainojamību</p>	<p>Risinājumā jābūt iespējai izveidot ievainojamības novēršanas uzdevumu un to norīkot izpildei lietotājam, kurš veicis pārbaudi, kurš ir atbildīgs par</p>

novēšanas kontrole	<p>konkrēto gala iekārtu vai kādam citam lietotājam kā arī noteikt izpildes termiņus, pamatojoties uz sekojošiem datiem:</p> <ul style="list-style-type: none"> - iepriekš definētas gala iekārtas vai to grupas; - iepriekš definētas domēna adreses; - definētas IP adreses vai to diapazoni; - noteikto ievainojamību bīstamības pakāpes; - konkrētas ievainojamības.
14. Komponente: meklēšana	<p>Risinājumam jānodrošina plaša gala iekārtu meklēšanas funkcionalitāte, balstoties uz:</p> <ul style="list-style-type: none"> - DNS hostname; - NETBIOS hostname; - IP adrese; - pperētājsistēma; - atvērtie porti; - darbojošies servisi; - ievainojamības; - pēdējās pārbaudes veikšanas datums.
15. Komponente: Lietotāju pārvaldības rīks	<p>Piekļuve risinājumam nodrošināma ar dažādām piekļuves tiesībām, iepriekš definētiem lietotāju tipiem:</p> <ul style="list-style-type: none"> - risinājuma galvenais lietotājs / Administrators; - gala iekārtu grupas galvenais lietotājs / Administrators; - pārbaudītājs; - rezultātu skatītājs.
16. Ievainojamību datu bāze	<p>Risinājuma pārbaudēs iekļauto ievainojamību informācijai jāsaturs:</p> <ul style="list-style-type: none"> - ievainojamības pamatinformācija (kategorija, ID, atsauce uz ražotāju u.t.t.); - ietekme uz infrastruktūru, ja tiek pielietota ļaunprātīgi; - rekomendācijas novēršanai.
17. Atbalsts	<p>Risinājuma darbībai nepieciešamajiem jauninājumiem, jābūt automātiski uzstādītiem visā līguma darbības laikā. Risinājuma cenā jāiekļauj telefonisks ražotāja un Piegādātāja atbalsts un automātiska jauninājumu uzstādīšana.</p>
18. Lietotāja saskarne	<p>Risinājuma lietotāju saskarnei jābūt nodrošinātai caur interneta pārlūkprogrammu. Risinājuma lietošanai nedrīkst tikt uzstādītas papildus programmas.</p>