Leping nr 2/13-25

Lisa nr 1

Registrite ja Infosüsteemide Keskus

Turu-uuring „Logide haldus- ja analüüsitarkvara“

Tallinn 2025

Sisukord

Turu-uuring

1. Turu-uuringu põhimõtted
   1.1. Turu-uuringu eesmärk on tutvuda hankija tehnilises kirjelduses väljatoodud nõuetele vastava logide haldus- ja analüüsitarkvaraga, paigaldades tarkvara hankija serverisse ning testides tarkvara võimekust hankija enda logidega. Turu-uuring annab hankijale sisendi tema enda tehniliste nõuete sobivuse kohta hankija süsteemide logide haldamiseks ning üldise info samalaadsete tarkvarade võimekuse kohta.
   1.2. Turu-uuring viiakse läbi kahe pakkujaga - Telia ja Elasticuga. Hankijale teadaolevalt osutavad nimetatud pakkujad hankija nõuetele vastavat teenust ning võimalike erisuste kaardistamiseks on valitud nii Eesti kui välismaa pakkuja. Kuna tarkvara sobivuse testimine võib võtta aega maksimaalselt 6 kuud, ei ole ajaliselt otstarbekas turu-uuringu valimisse rohkem pakkujaid võtta.
   1.3. Turu-uuringus pakkumusi ei esitata. Turu-uuringu käigus viiakse läbi demo valitud pakkujate lahendustele ning edastatakse vastused hankija küsimustele eraldi failina.
   1.4. Turu-uuringu käigus tutvutud lahenduste ja saadud vastuste põhjal otsustab hankija tulevikus samalaadsele lahendusele riigihanke korraldamise. Hankija kasutab vajadusel turu-uuringu käigus saadud sisendit riigihanke korraldamisel, tagades kõigile pakkujatele sisendi turu-uuringute tulemustest ja piisava ajalise ettevalmistuse.
   1.5. Hankija dokumenteerib kogu turu-uuringu käigus pakkujatele edastatud ja saadud teabe ning nimetatu kajastatakse hankedokumentides.
   1.6. Hankija tagab turu-uuringu tegemisel ja selle käigus saadud nõuannete kasutamisel mittediskrimineerimise ja läbipaistvuse põhimõtete järgimise. Konkreetsetele turu-uuringus osalejatele riigihanke avaldamisel ei viidata.
   1.7. Turu-uuring viiakse läbi maksimaalselt 6 kuu jooksul. Pakkuja on kohustatud jagama hankijaga tehnilist dokumentatsiooni. Turu-uuringu käigus on pakkuja valmis pakkuma hankijale konsultatsiooniteenust. Vajadusel seadistab ja paigaldab pakkuja tarkvara hankija poolt valitud asukohta, mille eest tasutakse konsultatsioonteenuse tunnihinna alusel.
   1.8. Pakkujal on õigus turu-uuringu raames küsida teenuse osutamise eest kulupõhist tasu (nii tarkvara kasutustasu kui konsultatsiooniteenuse tunnihinda).
   1.9. Turu-uuringu läbiviimiseks sõlmitakse hankija ja pakkuja vahel leping, mis reguleerib turu-uuringu läbiviimist, tasumise kohustust ja pooltevahelist konfidentsiaalsuskohustust.

2. Turu-uuringu küsimused

Palume pakkujatel hinnata tehnilises kirjelduses toodud nõudeid ning pakkuja võimekust nõuete täitmiseks.

1. Kas tehnilises kirjelduses kirjeldatud nõudeid on pakkuja võimeline täitma?
2. Palume pakkujatel anda orienteeruv hinnang pakkumuse maksumusele ühe logiallika kohta. Millised võiksid olla tingimused, mis pakkumuse hinda võiksid tõsta.
3. Millised oleks pakkujate ettepanekud teenuse hinnastamise osas?
4. Palume pakkujatel lisada ettepanekuid tehnilise kirjelduse täiendamiseks, mis aitaks hankijal saada heal tasemel ja turvalist teenust.
5. Kui pikk on pakkuja poolt pakutava lahenduse paigalduse ning seadistuse aeg?
6. Muud ettepanekud hankijale.

Tehniline kirjeldus (kavand)

1. Mõisted
   1.1 Haldus – logide kogumine ja töötlemine, mis tagab nende kõrge käideldavuse, muutumatuse, tõrgete parandamise jms.
   1.2 Analüüs – kogutud logide analüüs, mis annab ülevaate logisündmuste kohta ning edastab teavitusi anomaaliate ning kriitiliste turvasündmuste puhuks.
   1.3 Välisvõrk – võrk, mis ei ole osa hankija võrgust.
   1.4 Sisevõrk – võrk, mis on osa hankija võrgust.
   1.5 Analüütika – logide haldus- ja analüüsitarkvara poolt kogutud logide põhjal reaalajaline detailne ülevaade serverite, tööjaamade, arvutite jms kohta.
   1.6 Konsultatsioon – tehniline konsultatsioon, mille raames lahendatakse hankija poolt esitatud pöördumisi (nt. küsimused tarkvara kohta, abistamine lisaseadistamisel jms) kokkulepitud tunnihinna alusel.
   1.7 Paigaldus – pakkuja ja hankija koostöös pakkuja poolt pakutava lahenduse installeerimine ja juurutamine hankija keskkonnas ning esmaste logiallikate liidestamine haldus- ja analüüsitarkvaraga, millega tagatakse tehniline valmidus funktsionaalses osas.
   1.8 Kaugtöölaud – üle VPN-i ühendumine logide haldus- ja analüüsitarkvaraga.
   1.9 Agent – tarkvara poolt pakutav lahendus, mis kogub ja edastab logisid serveritest keskhalduses olevasse logide haldus- ja analüüsitarkvarasse.
   1.10 Logiallikas – masin/server/tööjaam, mis genereerib logisid.
   1.11 Hosti/rakenduse vaade – detailsem vaade iga hosti ja/või rakenduse kohta, mis toob esile ülevaatliku pildi rakenduse hetkeseisust kui ka olulisemad sündmused.
   1.12 Elutsükkel – logidele määratud tähtaeg, mille möödumisel logid kustutakse või tõstetakse uude kohta.
   1.13 Lõppkasutaja – hankija töötaja, kes tarkvara kasutab.
   1.14 Ajatelg – graafiline vaade logidega seotud sündmustest konkreetsel ajahetkel, mis näitab intsidentide võimalikku teket ja mõju.
   1.15 Raport – logide põhjal koostatud aruanne, mida on võimalik jagada kolmanda osapooltega, nt. kokkuvõtvad logid intsidendist.

2. Teenuse üldised tingimused ja nõuded
   2.1 Teenus hõlmab logide haldus- ja analüüsitarkvara kasutamisõigust, vajadusel pakkuja poolset paigaldust ja konsultatsiooniteenust.
   2.2 Pakutav lahendus ei tohi otse suhelda välisvõrguga, v.a erandjuhtudel (nt. päringu asukoha määramine ehk geoIP).
   2.3 Pakutav lahendus peab olema isoleeritud välisvõrgust.
   2.4 Pakutava lahenduse puhul ei ole lubatud edastada kogutud analüütikat lahenduse pakkujale või kolmandatele osapooltele.
   2.5 Pakkujal ei ole lubatud paigaldatud lahendusele ühenduda üle kaugtöölaua. Kui tekib olukord, kus hankija vajab tarkvara kasutamise käigus konsultatsiooni, kasutatakse muid võimalusi.
   2.6 Lahenduse dokumentatsioon ja juhendid peavad olema ajakohased ning ligipääs dokumentatsioonile peab olema hankijale tagatud.
   2.7 Pakkuja jagab hankijaga lahenduse tehnilist arhitektuuri, sh kas logid on transpordi ajal krüpteeritud; kuidas toimub andmete liikumine; keskmine agendi ressursi kasutus; millist logide põhist meetrikat (ing. k. Log-based metrics) oskavad agendid korjata.
   2.8 Tarkvara esmase paigalduse järgselt peab hankijal olema võimalus kogu tarkvara haldust/uuendamist ise administreerida.

3. Lahenduse funktsionaalsed nõuded:
   3.1. Lõppkasutajale peab olema võimalik määrata rollipõhiseid ligipääse. Lõppkasutaja peab saama vaadata ainult tema rolliga seotud logisid ja vaateid (ing. k. dashboard).
   3.2. Intsidendi uurimisel peab olema võimalus luua tarkvara siseselt logidest ajatelg, mis näitab intsidendi võimalikku teket, tegevusi ja mõju.

3.3. Lahendus peab võimaldama eelseadistatud reeglite järgi teavituste genereerimist logidest ehk anomaaliate tuvastamist.
3.4. Logidele peab olema võimalik määrata elutsükkel, mille põhjal logid teatud aja tagant kas tõstetakse uude kohta või kustutatakse.
3.5. Logidele peab olema võimalik lisada integratsioone (nt. CVE scanner, teavituste saatmine erinevatesse suhtluskanalitesse jms).
3.6. Logi kirje järgi peab olema võimalik tuvastada, mis serverist, tööjaamast ja/või domeenist logid saadeti.
3.7. Lahendus peab võimaldama logide põhjal raportite genereerimist ning nii manuaalset kui ka automaatset raportite edastamist.
3.8. Logikirjed peavad sisaldama tõestust, mille kaudu on võimalik kinnitada andmete terviklust.

4. Nõuded turvalisusele
4.1. Süsteem peab olema kaitstud rünnakute vastu parima OWASP (https://owasp.org/ sealhulgas: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology; OWASP ASVS https://owasp.org/www-project-application-security-verification-standard/) praktika kohaselt.
4.2. Teenuse pakkujal peab olema läbitud Eesti Infoturbestandardi audit või olemas ISO 27001 sertifikaat või nendega samaväärne tunnistus/sertifikaat.
4.3. Infoallika ja serveri vaheline liiklus peab olema krüpteeritud.
4.4. Kõik paroolid ja salasõnad peab rakendus alati salvestama soolatud ja krüpteeritud kujul. Krüpteerimise korral tuleb kasutada tugevaid algoritme.
4.5. Teenus peab logima turvalisuse seisukohalt kriitilised sündmused, sh sessiooni algamine ja lõppemine, rolli muutumine jms. Logi peab sisaldama kõigi failidega tehtavate toimingute kohta kasutaja ID-d, mis tegevused andmetega tehti (loomine, muutmine, kustutamine, vaatamine) ja kas tegevus õnnestus. Logi peab olema lihtsalt inim- ja masinloetav.