

RIIGIPILVES TEENUSE OSUTAMISE LEPING 5-3/25-0068-1

Tallinnas,

kuupäev digiallkirjas

Riigi Info- ja Kommunikatsioonitehnoloogia Keskus, registrikood 77001613, aadressiga Lõõtsa 8a, 10122 Tallinn, keda esindab seaduse ja põhimääruse alusel direktor Ergo Tars, edaspidi nimetatud **RIT**,

ja

ByteLife Solutions OÜ, registrikood 11179901, aadressiga Toompuiestee 35, 10149 Tallinn, keda esindab põhikirja alusel Janek Gridin, edaspidi nimetatud **teenusepakkuja**,

edaspidi eraldi nimetatud ka pool ning koos pooled, sõlmisid käesoleva Riigipilve lisateenuse osutamise lepingu (edaspidi nimetatud leping) alljärgnevas:

1. LEPINGU ALUS JA ESE

- 1.1. Leping sõlmitakse riigihangete seaduse § 49 lg 1 punkti 2 ja § 72 alusel, lähtudes läbiviidud väljakuulutamisetähtaajaga läbirääkimistega hankemenetlusega riigihanke „Riigipilve lisateenuse Zabbixi monitooring, lisateenused koos IT haldusteenusteenuse ning küberohtude avastamise ja reageerimise lahendusega“ (viitenumber 289841) III osa alusdokumentidest ja nimetatud riigihankele täitja poolt 10.03.2025 esitatud pakkumusest nr 547473.
- 1.2. Tellija sõlmib lepingu täitjaga, tuginedes täitja pakkumusele, lepingus fikseeritud täitja avaldustele ja kinnitustele ning eeldades heas usus täitja professionaalsust ja võimekust lepingut nõuetekohaselt täita. Alltöövõtjate kasutamise korral jääb lepingu nõuetekohase täitmise eest tellija ees vastutavaks täitja.
- 1.3. Lepingu esemeks on Riigipilve teenuste kataloogis oleva lisateenuse Vectra AI küberohtude avastamise ja reageerimise lahendus logihaldusega (edaspidi teenus) Riigipilve tellijatele vastavalt lepingus ja selle lisas 1 sätestatud tingimustele ja korrale.
- 1.4. RIT sõlmib lepingu teenusepakkujaga, eeldades heas usus teenusepakkuja professionaalsust ja võimekust lepingut nõuetekohaselt täita.
- 1.5. Lepingu lahutamatuks osadeks on riigihanke „Riigipilve lisateenuse Zabbixi monitooring, lisateenused koos IT haldusteenusteenuse ning küberohtude avastamise ja reageerimise lahendusega“ (viitenumber 289841) III osa alusdokumendid, täitja pakkumus, pooltevahelised kirjalikud teated ning lepingu muudatused ja lisad.
- 1.6. Kõik lepingu muudatused sõlmitakse lepingu lisadena, mis jõustuvad nende allkirjastamise hetkel või poolte määratud tähtajal.

2. LEPINGU TÄHTAEG, EELDATAV MAKSUMUS JA TASUMISE KORD

- 2.1. Leping jõustub allkirjastamisest ja kehtib 3 aastat või 280 000 euro täitumiseni, millele lisandub Eesti Vabariigis kehtiv käibemaks. Nimetatud maksumus on eeldatav ning RIT ei ole kohustatud teenusepakkujalt tellima teenust lepingu kogumaksumuse summas.

2.1.1. Teenuse näidispalett:

Pakett	Teenuse 3 aasta maksumus kokku käibemaksuta (EUR)
--------	---

TEENUSE OSUTAMISE LEPING

Näidispakett: 500 IP NDR (RUX), 250 AzureAD/M365 kasutajat, STREAM meta data to LogStack 30GB/päevas Vectra X3 Brain 3a toega.	136 000,00
--	------------

2.1.2. Teenuse komponendid, millest tellija komplekteerib talle vajaliku paketi, on järgmised:

Teenuse komponendid	Arveldus
500-999 IP (RUX)	aasta
1000-2000 IP (RUX)	aasta
500-999 IP (QUX)	aasta
1000-2000 IP (QUX)	aasta
250-499 AzureAD/M365 kasutajat	aasta
500-1000 AzureAD/M365 kasutajat	aasta
Lisa 3 kuni 14-päevane metaandmete säilitamine	aasta
Vectra Match	aasta
Vectra Cognito Stream	aasta
Vectra Recall	aasta
Virtuaalne Sensor	aasta, tasuta
Vistuaalne Brain	aasta, tasuta
Vectra X29 Brain / Sensor / Mixed Mode Appliance	ühekordne
Vectra S11 Sensor	ühekordne
S1 Sensor	ühekordne

- 2.2. Pooltel on õigus lepingu ja selle lisade muutmises kokku leppida kirjalikku taasesitamist võimaldavas vormis.
- 2.3. Lepingu võib lõpetada lepingu ülesütlemisega seaduses või lepingus sätestatud alusel.
- 2.4. Lepingu lõppemisel jääb kehtima teenusepakkuja kohustus hoida salajasena konfidentsiaalset informatsiooni ning RIT õigus rakendada selle kohustuse rikkumisest tulenevaid õiguskaitsevahendeid.
- 2.5. RIT tasub teenusepakkujale teenuse eest arve alusel vastavalt tellijate tellimuste täitmisele.
- 2.6. RIT kohustub tasuma arve 21 (kahekümne ühe) kalendripäeva jooksul. Teenusepakkuja esitab arve e-arvete operaatori või riigi poolt loodud e-arveldaja infosüsteemi <https://www.rik.ee/et/e-arveldaja> kaudu. Teenusepakkuja poolt esitatavad arved peab selgelt ja üheselt viitama lepingu viitenumbrile 289841 001 000 003 ja sisaldama makse teostamiseks vajalikke andmeid, RIT kontaktisiku nime ning vastama käibemaksuseaduse nõuetele.

3. POOLTE VASTUTUS

- 3.1. Pooled vastutavad oma lepingust tulenevate kohustuste rikkumise eest. Pool on kohustatud hüvitama lepinguga võetud kohustuste täitmata jätmise või mittekohase täitmisega teisele poolele tekitatud kahju.

TEENUSE OSUTAMISE LEPING

- 3.2. Teenusepakkuja vastutab teenuse osutamise eest vastavalt kokkulepitud tingimustele ja kehtivatele nõuetele, tähtaegadele ja kohase kvaliteediga.
- 3.3. Teenusepakkuja ei vastuta vigade eest, mis tulenevad RIT või Riigipilve tellija esitatud valedest või mittetäielikest lähtematerjalidest.
- 3.4. Teenusepakkuja vastutab oma lepingulise kohustuse rikkumise eest, mis tuleneb lepingu täitmisse kaasatud isikute tegevusest.
- 3.5. Kohustuse rikkumisel on teisel poolel õigus kasutada kõiki seadusest või lepingust tulenevaid õiguskaitsevahendeid vastavalt võlaõigusseadusele.
- 3.6. Poolte rahaline koguvastutus on piiratud konkreetse(te) RIT tellija(te) poolt tehtud tellimus(t)e maksumus(t)ega, kuid nimetatud piirang ei kehti süülise rikkumise, intellektuaalomandiõiguse, konfidentsiaalsuskohustuse või andmekaitsealaste kohustuste rikkumisel.
- 3.7. Tasu maksmisega viivitamisel on teenusepakkujal õigus nõuda viivist võlaõigusseaduses sätestatud määras maksmisele kuuluvast tasust iga tasumisega viivitatud kalendripäeva eest. Viivise maksimaalne määr on kuni 10% tasumisele kuuluva jooksva kuu summast. Teenusepakkuja esitab viivise nõude RIT'le allkirjastatult vähemalt kirjalikku taasesitamist võimaldavas vormis.
- 3.8. Teenusepakkuja lepinguliste kohustuste rikkumisena käsitletakse eeskätt olukorda, kus Riigipilve tellijale üle antud teenus ei vasta osaliselt või täielikult lepingu ja teenuse tingimustele või esineb muid teenusepakkuja poolseid lepingu rikkumisi.
- 3.9. Kui teenusepakkuja rikub lepingulist kohustust, on RIT'l õigus nõuda leppetrahvi tasumist, mille suuruseks on kuni 50% eelmise kalendrikuu konkreetse(te) teenuse maksumusest.

4. AVALIKUD SUHTED

- 4.1. Teenusepakkuja ei tegele seoses lepinguga avalike suhetega ega anna teateid pressile, elektroonilisele meediale, üldsusele või teistele auditooriumidele, välja arvatud RIT eelneval kirjalikul nõusolekul.
- 4.2. Kõik eelnimetatud kohustused kehtestab teenusepakkuja ka kõigile kolmandatele isikutele, keda ta kasutab oma lepingujärgsete kohustuste täitmisel.

5. INTELLEKTUAALSE OMANDI ÕIGUSED JA NENDE KASUTAMINE

- 5.1. Lepingu allkirjastamisega kinnitab kumbki pool, et talle kuuluvad lepingu täitmiseks vajalikud varalised autoriõigused, litsentsid ja muud intellektuaalse omandi õigused, mis on tarvilikud lepingujärgse teenuse täielikuks teostamiseks lepingus toodud ulatuses ning, et nende suhtes ei ole kolmandatel isikutel nõudeid. Pooled kinnitavad, et on võtnud tarvitusele kõik meetmed autori isiklike õiguste realiseerimiseks viisil, mis ei takista ega raskenda teose kasutamist ja autori varaliste õiguste teostamist.
- 5.2. Pool kohustub lahendama kõikvõimalikud lepinguga seotud intellektuaalse omandi õigustest tekkivad vaidlused kolmandate isikute või oma töötajate või koostööpartneritega. Juhul, kui eeltoodust tekib RIT'le rahaline või muu kohustus või juhul, kui RIT on kohustatud lõpetama lepingu alusel teostatud ja vastuvõetud teenuse kasutamise, on teenusepakkuja kohustatud RIT nõudmisel täitma selle rahalise või muu kohustuse ja/või looma samaväärse tulemi tasuta ning võimalikult lühikese aja jooksul, hoidudes mistahes viivitustest tulemi arendamises, kasutuselevõtmises ja kasutamises RIT poolt.
- 5.3. Lepingu täitmisel kolmandatele isikutele kuuluvate komponentide (tarkvara) kasutamise osas juhinduvad pooled nende kasutamise litsentsitingimustest. Teenusepakkuja kinnitab, et kasutab teenuse osutamisel selliseid kolmandatele isikutele kuuluvaid komponente, mis ei too RIT'le kaasa täiendavaid litsentsitasusid või piiranguid tarkvara kasutamisel (v.a juhul, kui nimetatud komponentide kasutamine on ette nähtud teenusepakkuja pakkumuses).
- 5.4. Teenusepakkuja võib kasutada töö teostamiseks kolmandatele isikutele kuuluvaid komponente vaid RIT eelneval kirjalikul nõusolekul. Kirjaliku nõusoleku taotlemisel on teenusepakkuja kohustatud esitama RIT'le litsentsi hinna ja litsentsitingimused.

TEENUSE OSUTAMISE LEPING

- 5.5. Lepinguga reguleerimata autoriõiguse küsimustes lähtutakse Eesti Vabariigis kehtivatest autoriõigusealastest õigusaktidest.

6. KONFIDENTSIAALSUS JA ISIKUANDMETE TÖÖTLEMINE

- 6.1. Teenusepakkuja kinnitab, et ei avalda ühelgi viisil konfidentsiaalset informatsiooni kolmandatele isikutele ilma RIT kirjaliku nõusolekuta, välja arvatud seadusega ettenähtud juhtudel.
- 6.2. Konfidentsiaalse informatsiooni all mõistavad pooled igasugust informatsiooni (sh RIT partnerite, tellijate/klientide ja töötajate, hindade, tegevuse meetodite ja taktika kohta, turvasüsteemide ja seadmete asukohta, omadusi, pakkumise kirjeldusi, spetsifikatsioone, manuaale, äriplaane, turvanõudeid; tehnilist, ärialast või muud teavet), mis on teenusepakkujale teatavaks saanud lepingu täitmise raames ja mis ei ole kolmandatele isikutele üldises korras kättesaadav.
- 6.3. Kui avaldatud konfidentsiaalne teave sisaldab isikuandmeid, peab teabesaaja järgima isikuandmete kaitse üldmäärust (Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta) ja vastutab määruse rikkumise eest.
- 6.4. Teenusepakkuja ei edasta lepingu täitmise käigus saadud isikuandmeid väljapoole Euroopa Liidu liikmesriikide ja Euroopa Majandusühendusse kuuluvate riikide territooriumit ilma RIT sellekohase selgesõnalise kirjaliku nõusolekuta.
- 6.5. Teenusepakkuja kasutab ja töötleb lepingu täitmise käigus saadud isikuandmeid üksnes lepingu täitmiseks ja RIT juhiste alusel, välja arvatud juhul, kui teenusepakkuja on kohustatud isikuandmeid töötleva tema suhtes kohalduva õiguse alusel. Viimati nimetatud juhul teavitab teenusepakkuja RITi vastava kohustuse olemasolust enne isikuandmete töötlemist, kui selline teavitamine ei ole olulise avaliku huvi tõttu teenusepakkuja suhtes kohalduva õigusega keelatud.
- 6.6. Teenusepakkuja võimaldab juurdepääsu lepingu täitmise käigus saadud isikuandmetele ainult nendele isikutele, kellel on selleks oma tööülesannete täitmiseks vajadus ning tagab, et need isikud on teadlikud ning järgivad isikuandmete töötlemise alaseid nõudeid ja õigusakte, nad on saanud asjakohase koolituse eelmainitud nõuete kohta, on võtnud endale konfidentsiaalsuskohustuse või neile kehtib asjakohane seadusest tulenev konfidentsiaalsuskohustus. Vastav konfidentsiaalsuskohustus jääb kehtima pärast lepingu lõppemist.
- 6.7. Teenusepakkuja rakendab kõiki talle kättesaadavaid mõistlikke ja õigusaktide kohaselt nõutavaid organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid lepingu täitmise käigus saadud isikuandmete kaitseks juhusliku või tahtliku volitamata muutmise, juhusliku hävimise ja tahtliku hävitamise eest ning andmete kättesaadavuse takistamise eest õigustatud isikule, samuti igasuguse muu volitamata töötlemise s.h. avalikustamise eest.
- 6.8. Teenusepakkuja kustutab lepingu lõppemisel kõik lepingu täitmise käigus saadud isikuandmed ja nende koopiad 30 päeva jooksul lepingu lõppemisest, v.a juhul, kui lepingust või õigusaktidest tuleneb teisiti.
- 6.9. Konfidentsiaalsuskohustus on tähtajatu. Teenusepakkuja tagab, et konfidentsiaalsuskohustus kehtib ka nende töötajate ning muude lepingu täitmisse kaasatud isikute suhtes.

7. VÄÄRAMATU JÕUD

- 7.1. Lepingust tulenevate kohustuste mittetäitmist või mittenõuetekohast täitmist ei loeta lepingu rikkumiseks, kui selle põhjuseks olid asjaolud, mille saabumist pooled lepingu sõlmimisel ei näinud ega võinud ette näha (vääramatu jõud).
- 7.2. Pool, kes soovib vabaneda lepingu täitmise kohustusest vääramatu jõu tõttu, peab esitama teisele poolele sellekohase kirjaliku taotluse, selgitades lepingu täitmise raskusi ning näidates ära nende põhjused.

TEENUSE OSUTAMISE LEPING

7.3. Kui vääramatu jõu asjaolud kestavad üle kuuekümne (60) päeva, loetakse, et käesolev leping on lõppenud täitmise võimatusega, v.a. juhul, kui pooled ei ole selleks ajaks kokku leppinud teisiti. Lepingu lõppemisel vääramatu jõu asjaolude tõttu ei ole kummalgi poolel õigus nõuda teiselt poolelt lepingu mittetäitmise või mittenõuetekohase täitmisega tekitatud kahju hüvitamist.

8. POOLTE KONTAKTISIKUD

8.1. Koostöö korraldamise eest vastutavad ja teenuse üleandmisel-vastuvõtmisel esindavad pooli järgmised kontaktisikud:

8.1.1. RIT Riigipilve talituse kontaktisikud: talituse juhataja Rain Nõmmik (e-post rain.nommmik@rit.ee), iseteeninduse peakasutaja Ave Aun (tel: 5666 1091, e-post ave.aun@rit.ee) või projektijuht Gennet Jaadla (tel: 508 8295, e-post: gennet.jaadla@rit.ee).

8.1.2. Teenusepakkuja kontaktisik: projektijuht Kalmer Päts (tel: 5455 6600, e-post: kalmer.pats@bytelife.com).

8.2. Kontaktpunktid:

8.2.1. RIT Riigipilve kliendihaldus: tel 699 1140, e-post: [klient@riigipilv.ee](mailto: klient@riigipilv.ee).

8.2.2. Teenusepakkuja: tel 5333 0112, e-post: support@bytelife.com.

9. LÕPPSÄTTED

9.1. Lepingule kohaldatakse Eesti Vabariigi õigusakte.

9.2. Lepingu täitmisel tekkivad vaidlused ja lahkarvamused lahendavad pooled läbirääkimiste teel.

9.3. Kokkuleppe mittesaavutamisel lahendatakse vaidlus Harju Maakohtus.

10. Lepingu lisa

10.1. Lisa 1 Teenuse teenustingimused

11. POOLTE ESINDAJATE ALLKIRJAD

11.1. Lepingule allakirjutamisega kinnitavad pooled, et on sellega tutvunud ja on nõus lepingus toodud tingimustega ning mõistavad täielikult enesele võetavate kohustuste sisu ning tagajärgi.

11.2. Leping omab digitaalselt allkirjastatuna juriidilist jõudu ning edastatakse pooltele elektrooniliselt.

**Riigi Info- ja Kommunikatsioonitehnoloogia
Keskus:**

(allkirjastatud digitaalselt)

Ergo Tars
direktor

Teenusepakkuja:

(allkirjastatud digitaalselt)

Janek Gridin
juhatuse liige

TEENUSE OSUTAMISE LEPING

Lisa 1 Teenuse teenustingimused

Vectra AI küberohtude avastamise ja reageerimise lahendus logihaldusega teenustingimused

Käesolevad teenustingimused reguleerivad Riigi Info- ja Kommunikatsioonitehnoloogia Keskuse (edaspidi RIT), (edaspidi teenusepakkuja) ja tellija suhteid seoses teenuse kasutamisega ning kehtestavad sellekohaste õiguste teostamise ja kohustuste täitmise tingimused. Teenustingimusi rakendatakse alates tellija poolt Riigipilve iseteeninduses teenuse tellimisest.

1. Mõisted

RIT: Riigi Info- ja Kommunikatsioonitehnoloogia Keskus;

Lahenduse pakkuja:

Lahendus: Vectra AI küberohtude avastamise ja reageerimise lahendus logihaldusega;

Riigipilve kasutajatugi: RIT 24/7 töötav seirekeskus, mille kaudu toimub probleemide registreerimine ja suunamine vastava valdkonna spetsialistidele, e-post: kasutajatugi@riigipilv.ee, tel 699 1140;

Riigipilve kliendihaldus: RIT Riigipilve tööajal töötav üksus, mille kaudu toimub kasutajate juhendamine, probleemide väljaselgitamine ja lahendamine ning vajadusel nende edasi suunamine vastava valdkonna spetsialistidele, e-post: klient@riigipilv.ee, tel 699 1140;

Lepe: RIT ja tellija vahel sõlmitud koostöökokkulepe;

Tellija: RIT lepinguline partner, kes tellib või kasutab Riigipilve teenust;

Tööpäev: kalendripäev, mis ei ole laupäev või pühapäev või rahvuspüha või riigipüha pühade ja tähtpäevade seaduse tähenduses;

Tööaeg: tööpäev kella 9.00-st kuni 17.00-ni;

Tööväline aeg: aeg, mis ei ole tööaeg;

Teenuse rike (intsident): olukord, kus tellijal ei ole võimalik teenust vastavalt lepingus kokkulepitule kasutada, sh nt teenuse, IT süsteemi, vahendi või rakenduse töö planeerimata seiskumine või häire. Teenuse rikke vormideks on teenuse seisak ja teenuse häire;

Teenuse seisak: olukord, kus lepingus kirjeldatud teenuse, IT süsteemide või vahendite või rakenduse töö ei saa jätkuda (on seiskunud);

Teenuse häire: olukord, kus lepingus kirjeldatud teenuse, IT süsteemide või vahendite või rakenduse töö on piiratud (on häiritud);

Teenuse rikke mõju ulatuse määrang:

puudub - mõju teenusele puudub;

madal - teenus on häiritud ühel kasutajal või teenuse raames kasutatava komponendi töö on häiritud, kuid teenus on kasutatav;

keskmise - teenus on seiskunud ühel või on häiritud paljudel kasutajatel või on häiritud mitu teenuses kasutatavat komponenti, kuid Teenus on kasutatav;

kõrge - teenus on seiskunud mitmel kasutajal või pole kasutatav;

Reageerimisaeg: ajavahemik teenuse rikke kohta teate saamisest kuni teenusepakkuja spetsialisti töö alustamine intsidendi lahendamiseks;

Kordategemisaeg: ajavahemik teenuse rikke kohta teate saamisest kuni teenuse, IT süsteemi või vahendi või rakenduse töövõime taastamiseni.

Muudatus: igasugune lisamine, modifitseerimine või eemaldamine, mis mõjutab olemasolevat ja töötavat teenust, funktsiooni või IT vahendit või selle konfiguratsiooni;

TEENUSE OSUTAMISE LEPING

Tellimus: tellija soov saada abi teenuse osas või tellida standardset muudatust või ligipääsu;

Riigipilve iseteenindus: veebiaadressil <https://minu.riigipilv.ee> asuv veebipõhine keskkond, mille kaudu on tellijal võimalik jälgida teenusega seonduvate pöördumiste hetkestaatusid ja lahenduskäike;

Süsteem: tellija poolt defineeritud süsteemiskeem.

2. Lahenduse kirjeldus

2.1 Tuvastamise ja analüüsi automatiseerimine

- 2.1.1 Lahendus kasutab masinõppe baasil Network Detection and Response (NDR) tehnoloogiat.
- 2.1.2 Lahendus tuvastab ja liigitab automaatselt kõik ohud, sealhulgas ründefaasi ja riski, ilma manuaalse sekkumise vajaduseta.
- 2.1.3 Lahendus kogub ja prioriseerib aja jooksul ohte füüsiliste hostide kaupa, isegi IP- ja kasutajatunnuse muutuste korral.
- 2.1.4 Lahendus eristab võtmetähtsusega varasid teistest hostidest riski prioriseerimiseks.
- 2.1.5 Lahendusel on mehhanism, mis automaatselt näitab avastamise kindlust, kui ohud tuvastatakse anomaaliate põhjal.
- 2.1.6 Lahendus suudab kategoriseerida järgmised ohud:
 - 2.1.6.1 botivõrgu käitumine, sealhulgas rämpspost, DDoS, välise haavatavuse skaneerimine, bitcoinide kaevandamine jne;
 - 2.1.6.2 varjatud tunnelid (HTTP, HTTPS ja DNS), mida kasutatakse käsu- ja juhtimiseks ning andmete väljaviimiseks;
 - 2.1.6.3 algoritmiliselt loodud domeenide või DGA-de kasutamine;
 - 2.1.6.4 kohandatud RAT-id (Remote Access Trojan) tavalisest kasutajaliiklusest;
 - 2.1.6.5 andmete väljaviimine sõltumata kasutaja identiteedist või IP-aadressist;
 - 2.1.6.6 ründaja siseluure;
 - 2.1.6.7 luure, kasutades aeglaseid või "paranoilisi" võrguskaneeringuid;
 - 2.1.6.8 haldus- ja haldusprotokollide (sh RDP, SSH ja IPMI) väärkasutamine.

2.2 Ohu prioriteet ja uurimine

- 2.2.1 Lahendus automaatselt hindab ja prioriseerib iga tuvastatud ründaja käitumise.
- 2.2.2 Lahendus automaatselt hindab ja seab igale seadmele prioriteedi, lähtudes selle käitumisest aja jooksul.
- 2.2.3 Lahendus pakub suuremat nähtavust võtmetähtsusega varadele, millel on tuvastatud ründaja käitumine.
- 2.2.4 Lahendusel on võimalus teavitada tellija töötajaid ohuskoori alusel.
- 2.2.5 Lahendus pakub individuaalseid skoori nii ohu kui ka kindluse/usaldusväärsuse jaoks.
- 2.2.6 Lahendus võimaldab nähtavust hostide omavahelise liikluse kohta.
- 2.2.7 Lahendus pakub analüüsimiseks tuvastatud ründaja käitumise pakethõivet (packet capture).
- 2.2.8 Uurimise hõlbustamiseks on lahenduse igas metaandmete kirjes seadme hostinimi.

2.3 Tuvastamise metoodika

- 2.3.1 Lahendus tuvastab ohud võrguliikluse pakettide analüüsi põhjal.
- 2.3.2 Lahendusel on võimalus tuvastada võrgupõhiseid ohte krüpteeritud liikluses.
- 2.3.3 Lahendus tuvastab kohandatud või tundmatud ohud, kus puudub signatuur või IP/domeeni maine ajalugu.

TEENUSE OSUTAMISE LEPING

- 2.3.4 Lahendus on rakendatav kõikides kasutaja- ja infrastruktuuriseadmetes (Windows, Mac, mobiilseadmed, asjade internet, ruuterid, tulemüürid jne).
- 2.3.5 Lahendusel on triiaži võimalus valepositiivsete tulemuste minimeerimiseks.
- 2.3.6 Lahendus esitab iga tuvastuse kohta Mitre ATT&CK kaardistuse, et optimeerida tuvastuse hindamist.
- 2.4 **Ohtude kohalik modelleerimine**
 - 2.4.1 Lahendus tuvastab potentsiaalselt kahjulikke anomaaliaid, mis põhinevad kõrvalekaldumisel õpitud kohalikest normidest võrgus.
 - 2.4.2 Lahendus õpib pidevalt võrgu ja selle kasutuse muutudes.
 - 2.4.3 Lahendusel on võime tuvastada ohte uutes seadmetes või seadmetes, mis olid juba ohustatud, kui baastase oli moodustatud.
- 2.5 **Analüüs ja integreerimine**
 - 2.5.1 Lahendus säilitab võrgu paketi salvestusi tuvastatud ründaja käitumisest.
 - 2.5.2 Lahendus pakub API põhist juurdepääsu kõikidele sündmustele, hostidele ja hindamisteabele, et integreerida teiste turvalahenduste ja operatsioonisüsteemidega.
 - 2.5.3 Uurimise tõhususe suurendamiseks võimaldab lahendus integratsiooni EDR lahendustega ja liidab EDR andmed otse enda kasutajaliidesesse. Toetatud on vähemalt järgmised EDR lahendused:
 - 2.5.3.1 CrowdStrike
 - 2.5.3.2 Microsoft Defender
 - 2.5.3.3 SentinelOne
 - 2.5.3.4 Cybereason
 - 2.5.3.5 FireEye.
 - 2.5.4 Lahendus võimaldab ohtude tuvastamist pilveteenustest
 - 2.5.4.1 Azure AD
 - 2.5.4.2 Microsoft 365
 - 2.5.4.3 AWS.
 - 2.5.5 Lahendus võimaldab ohtudele reageerimiseks integratsiooni kohaliku tulemüüriga
 - 2.5.5.1 Fortinet
 - 2.5.5.2 Palo Alto
 - 2.5.5.3 Juniper
 - 2.5.5.4 Check Point.
- 2.6 **Tuvastavate ohtude tüübid**
 - 2.6.1 Lahendus tuvastab vähemalt järgmist tüüpi ohud:
 - 2.6.1.1 ründajate poolt kasutatavad kaugjuhtimistunnelid kompromiteeritud süsteemide kontrollimiseks;
 - 2.6.1.2 peidetud tunnelid HTTP, HTTPS või DNS kaudu suhtlemiseks C&C-ga (Command and Control) või andmete väljaveoks;
 - 2.6.1.3 veebipõhine C&C (IP maine või ohtude loeteludele mitte tuginev);
 - 2.6.1.4 pahavara, mis kasutab võltsbrauserit;
 - 2.6.1.5 pahavara värskendamine;
 - 2.6.1.6 pahavara, mis kopeerib pakke (Payload) teistele hostidele/kasutab turvaauke teiste hostide vastu;
 - 2.6.1.7 TOR liiklus;
 - 2.6.1.8 P2P (Peer-to-Peer) liiklus;

TEENUSE OSUTAMISE LEPING

- 2.6.1.9 Botneti rahastamise käitumine: klikipettus, bitcoinide kaevandamine, väljaminev DoS, väljaminev SPAM;
 - 2.6.1.10 lunavara tegevus: failide jagamine;
 - 2.6.1.11 võrgu luure skaneerib: pordiskaneerimised, pordiulatuse skaneerimine, kasutamata IP-de skaneerimine;
 - 2.6.1.12 varastatud kasutajatunnuste kasutamine hostilt, kus seda varem pole kasutatud;
 - 2.6.1.13 varastatud kasutajatunnuste kasutamine tavapärasest süsteemist, kuid ebatavaliste teenuste või liigse mahuga päringute jaoks;
 - 2.6.1.14 host, kes proovib mitmeid volitusi serveri juurdepääsu saamiseks;
 - 2.6.1.15 Kerberos teenuse skaneerimine;
 - 2.6.1.16 Brute Force rünnakud;
 - 2.6.1.17 haldusprotokollide (sh RDP, SSH ja IPMI) kasutamine, mille kaudu lähtehost sihtkosti tavaliselt ei halda;
 - 2.6.1.18 host, mis viib andmeid ebatavalisse sihtkohta;
 - 2.6.1.19 host, mis kogub ebatavaliselt suuri andmeid ja saadab seejärel välisele IP-le;
 - 2.6.1.20 host, mida kasutatakse releena andmete viimiseks välisesse süsteemi.
- 2.7 **Värskendused**
- 2.7.1 Lahendus võimaldab tootjapoolset tarkvara värskendamist ilma lõppkasutaja sekkumiseta.
 - 2.7.2 Lahendus toimib täielikult „õhukindlas režiimis“ ehk välisvõrgust eraldatuna; sel juhul võimaldab Pakkuja Hankijale värskenduspakettide kättesaadavuse.
3. **Teenuse osutamise tingimused**
- 3.1 Teenust osutatakse tööajal.
- 3.2 Teenusepakkuja kohustub:
- 3.2.1 osutama teenust vastavalt tellijaga kirjalikku taasesitamist võimaldavas vormis sõlmitud kokkuleppele;
 - 3.2.2 esitama tellija nõudmisel raporteid teostatud tegevustest;
 - 3.2.3 sõlmima tellija nõudmisel NDA lepingu.
- 3.3 Tellija kohustub:
- 3.3.1 sõlmima teenusepakkujaga nõudmisel NDA lepingu;
 - 3.3.2 esitama teenusepakkujale jooksvalt teenuse osutamiseks vajalikud lähteandmed ja –dokumendid;
 - 3.3.3 teavitama teenusepakkujat, kui teenuse raames töödeldakse isikuandmeid;
 - 3.3.4 andma teenusepakkujale mõistliku ja piisava aja oma kohustuste täitmiseks;
 - 3.3.5 andma teenusepakkujale vajalikke juhiseid, sh teenusepakkuja nõudmisel kirjalikult.
4. **Teated**
- 4.1 Tellija edastab teenusega seotud pöördumised (tellimused, infopäringud, intsidendid) Riigipilve iseteenindusest.
 - 4.2 Tellija teavitab viivitamatult Riigipilve iseteeninduse vahendusel teenuse kasutamisel tekkinud probleemidest vastavalt Riigipilve eeskirjale.
 - 4.3 Juhul, kui iseteenindus ei toimi, kontakteerub tellija Riigipilve kasutajatoega (24/7) e-post teel kasutajatugi@riigipilv.ee või telefonil 699 1140 ja teatab oma nime, ettevõtte nime, projekti nimetuse, probleemi kirjelduse ning muud olulised asjaolud.
 - 4.4 Tellija kontaktisik peab pärast veast teatamist olema Riigipilve kliendihalduse nõudmisel kättesaadav.
5. **Teenuse tasu**

TEENUSE OSUTAMISE LEPING

- 5.1 Teenuse maksumus arvestatakse vastavalt valitud paketi kuutasu ja vajadusel juurde tellitud seadistus- või lisatöödele.
- 5.2 Teenuste eest arveldamist alustatakse hetkest, millal tellijal on võimalus teenust kasutada.
- 5.3 Tellija kohustub tasuma RIT'le teenusega seonduvad tasud vastavalt teenuse kataloogist tellitud teenuse maksumusele ja teenustingimustele ning RIT poolt esitatud arvele.
- 5.4 Tellija on kohustatud tasuma tellija ja teenusepakkuja vahel kokku lepitud tasu tasuliste teenuste eest.

6. Teenuse lõpetamine ja täiendavad tingimused

- 6.1 Tellija edastab teenuse lõpetamise pöördumise Riigipilve iseteenindusest või teavitab teenuse lõpetamise soovist Riigipilve kliendihaldust vähemalt kaks kuud ette enne 12 kuu täitumist ja Riigipilve kliendihaldus edastab teenuse lõpetamise soovi teenusepakkujale.
- 6.2 Teenusepakkuja teavitab Riigipilve kliendihaldust ja Riigipilve kliendihaldus tellijat Riigipilve iseteeninduse vahendusel teenuse osutamise lõpetamisest vähemalt kaks kuud ette enne 12 kuu täitumist.
- 6.3 Teenuse lõpetamisel on tellija kohustatud tasuma esitatud arve(te) alusel teenuse lõpetamise momendiks faktiliselt tehtud teenuse eest ja kolmeaastase litsentsi tasu puudujääva osa hüvitamine.
- 6.4 Teenusepakkuja ja RIT juhinduvad lisaks teenustingimustele Riigipilve eeskirjast ja käesolevast leppest.
- 6.5 Tellija ja RIT juhinduvad lisaks teenustingimustele Riigipilve eeskirjast ja koostöökokkuleppest.