Raamlepingu lisa 1 - Tehniline kirjeldus

Raamlepingu esemeks on Eesti Rahvusvahelise Arengukoostöö Keskuse (***ESTDEV***) poolt teostatavate küberturvalisuse projektide elluviimiseks vajalike asjade ja teenuste ostmine.

1. Taustainfo

1.1. ESTDEV viib ellu rahvusvahelise arengukoostöö raames ellu kutsutud IKT ja küberturvalisuse projekte, kasutades selleks era- ja avaliku sektori kogemusi ja oskusteavet. Sõlmitavate raamlepingutega soovime kaasata ettevõtteid, kes panustavad ESTDEV-i poolt koordineeritud projektidesse, töötades välja ja rakendades innovaatilisi info- ja küberturvalisusega seotud lahendusi mis võivad sisaldada (või osaliselt või täielikult koosneda) vastavat tarkvara, rakendusi, tehnilist infrastruktuuri ja selle komponente ning eelnevatega seotud või mitteseotud paigaldamis-, seadistamis-, koolitus- ja nõustamistegevusi.

2. Üldine

2.1. Riigihanke eesmärk on sõlmida raamlepingud partneritega (edaspidi ühiselt nimetatud kui ***töövõtja***) Eesti arengukoostöö raames küberturvalisuse alaste asjade ja teenuste tellimiseks.

2.2. Hankeleping minikonkursil esitatud tellimuse täitmiseks sõlmitakse ESTDEV-i (edaspidi ka ***tellija või hankija***) ning hanke võitnud **töövõtja** vahel. Hanke projektikohase sisu ja tehnilised nõuded lisab **tellija** igale tellimustööle eraldi.

2.3. Tellija rakendab töövõtjatega lepingute sõlmimise eel rahvusvaheliste sanktsioonide kontrolli. Hankija ei sõlmi hankelepingut ja kõrvaldab hankemenetlusest pakkuja või taotleja kellega hankelepingu sõlmimine rikuks rahvusvahelist või Vabariigi Valitsuse sanktsiooni rahvusvahelise sanktsiooni seaduse tähenduses.

2.4. Raamlepingu raames teostatavate tööde ja teenuste kasusaajad on sageli välisriikides asuvad isikud ja asutused. Seetõttu on vajalik arvestada igakordselt sihtriigi eripäradega. Töövõtja tööde ja teenuste teostamisel sihtriigi normide järgimise eest (elekter, tööohutus, side jm) ja vastutab oma alltöövõtjate ja kohapealse personali töö eest. Sihtriigis tööle saadetavad töötajad peavad vastama nõuetele, mis on kirjeldatud käesoleva riigihanke alusdokumendis “ PEE Lisa 1 – Nõuded pakkuja meeskonnale ja CV vorm ”. Tellijal on õigus minikonkurssides nõuda sihtkoha riikides asuvate partnerite kaasamist, vastavad tingimused esitatakse minikonkursil.

2.5. Kõik töövõtja poolt tarnitavad seadmed ja konfiguratsioonid peavad vastama EL andmekaitse ja infoturbe standarditele.

2.6. Töövõtja peab tagama, et raamlepingu alusel tarnitavate seadmete paigaldus, hooldus- ja garantiiteenused on kättesaadavad paigaldusriigis. Töövõtja tagab, et tal on sihtriigis piisav tehniline võimekus, ressursid ja vajadusel kohalikud partnerid tööde teostamiseks. Kõik kohalikud õigusaktid, standardid ja nõuded (sh tööohutus, elektri- ja side-eeskirjad) tuleb täita töövõtja kulul ja vastutusel.

2.7. Riigihange raamlepingute sõlmimiseks on jaotatud järgmisteks osadeks, millest kõikides võib teha soovi korral pakkumused:

2.7.1. OSA 1 - Info- ja küberturvalisuse alased konsultatsiooniteenused;

2.7.2. OSA 2 - Info- ja küberturvalisuse tarkvaraanalüüs, -arendus ja -rakendused;

2.7.3. OSA 3 – Erinevad IT ja küberturvalisuse infrastruktuuri komponendid, paigaldamine ja seadistamine.

2.8. Juhul, kui minikonkursi raames on teatavaks tehtud, siis on kohustuslik lepingu täitmisel rakendada ka tellija sisekordasid.

3. OSA 1 - Info- ja küberturvalisuse alased konsultatsiooniteenused

3.1. Info- ja küberturbe alaste konsultatsiooniteenuste hulka kuuluvad näiteks järgmised teenused:

3.1.1. erinevad analüüsitööd, sh koolitusvajaduste välja selgitamine ning koolituskavade loomine;

3.1.2. nõustamisteenused küberturvalisusega seotud küsimustes;

3.1.3. küberturvalisusega seotud erinevate seminaride, töötubade jmt ürituste sisuline ja organisatsiooniline läbiviimine;

3.1.4. küberharjutusväljal põhinevate (*cyber range*) tehniliste ja mittetehniliste lauaõppuste (*tabletop exercise)* ning muus vormis küberturvalisusega seotud väljaõppe läbiviimine;

3.1.5. turvaseire korraldamise ja olukordadele reageerimisplaanide koostamine (sh. infoturbe riskianalüüsid, turbekorralduse eeskirjade ja strateegiate loomine ja juurutamine);

3.1.6. küberturvalisust tagavate lahenduste väljatöötamine;

3.1.7. turbeläbistuse testimine, haavatavuse ja riskide hindamine;

3.1.8. Koolitusprogrammide ja -materjalide väljatöötamine;

3.1.9. Sihtgruppide- ja tasemepõhised koolitused erinevatele sihtrühmadele eri viisidel ja keeltes;

3.1.10. muud olemuslikult küberturvalisuse konsultatsiooni valdkonda kuuluvad tööd.

3.2. Nõuded teenuste läbiviimisele:

3.2.1. Toimumisviis – kohapealne, kaug- või hübriidtöö;

3.2.2. Keeled – inglise (kokkuleppel ka muu kohalik keel). Lepingu täitmise keel on sätestatud raamlepingus ja hankelepingus igakordselt minikonkursil, kui see erineb raamlepingu sätestatust;

3.2.3. Tehniliste koolituste puhul eeldatakse, et koolitaja on võimalik kasutada oma praktilisi ja tehnilisi laboreid.

3.3. Näidistena on loetletud ka võimalike tellitavate konsultatsiooniteenuste (sh selle erinevad vormid nagu näiteks koolitused) teemad, kuid nimekiri ei ole lõplik:

3.3.1. Küberhügieen (erinevatele tasemetele);

3.3.2. Erinevate standardite ja raamistike rakendamise koolitused (NIST, ISO, CIS, GDPR, NIS2 jne);

3.3.3. Riskihaldus ja juhtimine;

3.3.4. *Blue team* ja *Red team*, ehk tehnilised kaitsmise ja ründamise koolitused;

3.3.5. *Threat hunting* (ohujahi) töötoad;

3.3.6. CERT / CSIRT / SOC / CSOC vajadustele vastavad operatsioonilased ja tehnilised koolitused;

3.3.7. Võrguseadmete ja muu IT infra kaitsmise (*hardening*) koolitused ja töötoad ;

3.3.8. Lõppseadmed ja identiteet: EDR/XDR *(Entpoint Detection and Response / Extended Detection and Response*), Windows/Linux/macOS karastamine, AD/AAD/Entra (*Active Directory/Azure Active Directory*), PAM (*Privileged access management*);

3.3.9. Pilv ja konteinerid: AWS/Azure/GCP turve, Kubernetes, IaC (Terraform) turve, CI/CD (*Continuous Integration / Continuous Deployment)* & DevSecOps

(SAST/DAST/SCA (*Static Application Security Testing / Dynamic Application Security Testing / Software Composition Analysis*));

3.3.10. Rakendused: OWASP (*Open Web Application Security Project*) Top 10, turvaline programmeerimine (Java/.NET/JS/Python), API-turve;

3.3.11. Luure ja ohumudelid; veebi/rakenduste/API testimine; AD-rünnakud; Wi-Fi; andmepüügikampaaniad;

3.3.12. Telemeetria ja andmevalmidus, meetodikad, päringudisain (SIEM/EDR/XDR, Wasuh, Elastic);

3.3.13. SIEM/SOAR/juhtumihaldus (*Security Information and Event Management / Security Orchestration, Automation, and Response*): Splunk, Microsoft Sentinel, Elastic, TheHive/Cortex, MISP;

3.3.14. Võrk/võrgu ekspertiis: Zeek, Suricata, Wireshark, Arkime, Velociraptor, Autopsy;

3.3.15. AppSec/DevSecOps: OWASP ZAP, Burp Suite, Trivy, Semgrep, GitHub/GitLab Security.

4. OSA 2 - Info- ja küberturvalisuse tarkvaraanalüüs, -arendus ja -rakendused

4.1. Info- ja küberturbe tarkvaraliste lahenduste analüüsi ja hankimise ning rakenduste juurutamise ja seadistamise tööde hulka kuuluvad näiteks:

4.1.1. Eelanalüüs ja nõuete kaardistus – ärivajadused, infoturbe- ja vastavusnõuded (nt GDPR/NIS2/ISO 27001);

4.1.2. Lahenduse arhitektuur – kõrgtaseme (HLD, *High-level Design*) ja detailne (LLD, *Low-level Design*) arhitektuur ning üleminekukava (*as-is → to-be*);

4.1.3. Hankimise tugi – tootjate/edasimüüjate võrdlus, litsentsimudelite ja kogukulude analüüs, pakkumiste küsimine ja võrdlustabelid;

4.1.4. Piloot/PoC (*Proof of Concept*) – kontrollitud keskkonnas sobivuse, jõudluse ja turbe-eelduste valideerimine;

4.1.5. Keskkonna ettevalmistus – võrgu- ja juurdepääsumudelid, serverid/pilvekontod, rollid/õigused, logiallikad;

4.1.6. Paigaldus ja seadistamine – tootja parimad praktikad, kõvendamine (*hardening*) ja turvalised baas-konfiguratsioonid;

4.1.7. Integratsioonid – AD/AAD/Entra, IAM/PAM (*Identity Access Management / Privileged Access Management*), SIEM/SOAR, EDR/XDR, piletisüsteem (*ticketing*), CMDB (*configuration management database*), e-posti ja pilveteenused;

4.1.8. Tarkvara arendus – klientide soovidele vastavalt tarkvara arendus kas nullist, olemasoleva tarkvara muutmine või täiendamine;

4.1.9. Andmete migreerimine – reeglite, sätete, logide, identiteetide ja integratsioonide ületoomine; tagasipööramise (*rollback*) plaan;

4.1.10. Automatiseerimine ja IaC (*Infrastructure as Code*) – skaleeritav *deploy* (nt Terraform/Ansible), CI/CD (*Continuous Integration / Continuous Deployment)* integratsioon, versioonihaldus;

4.1.11. Testimine ja vastuvõtukriteeriumid – funktsionaal-, turbe-, jõudlus- ja koormustestid; UAT/SAT (*User Acceptance Test / System Acceptance Test)* kriteeriumid;

4.1.12. Dokumentatsioon – HLD/LLD, konfiguratsioonipõhjad, *runbook*'id ja SOP-id *(Standard Operating Procedures)*, varahalduse/CMDB uuendused;

4.1.13. Koolitus ja üleandmine – admin-, kasutaja- ja ops-koolitus, üleandmisseminar ja teadmiste siire;

4.1.14. Teenuste, andmete ja infosüsteemide kättesaadavus ja töökindlus – RTO/RPO (*Recovery Time Objective/Recovery Point Objective*), varundus ja taastamine, DR-protseduurid, hoolduse aknad;
4.1.15. Infosüsteemide ja IT lahenduste jõudlus ja skaleeritavus – mõõdikud/KPI-d (läbilaske, latentsus, agentide arv), skaleerimis- ja arhiveerimisstrateegia;
4.1.16. Turbe- ja kvaliteedikontroll – CIS benchmark'id, haavatavuse skanneeringud.
4.1.17. IT süsteemide ja tarkvaralahenduste hooldus ja tugi (SLA (*Service Level Agreement*)) – *patch*-imine ja versiooniuuendused;
4.1.18. Litsentsid ja IP – litsentsi haldus (CAPEX/OPEX (*Operational Expenditure / Capital Expenditure*)), sõltuvuste/*vendor lock-in* riski maandamine;
4.1.19. Avatud lähtekood – *community vs enterprise* -tugi, turvapaikade poliitika, konfigureerimine tootmisvalmidusse;
4.1.20. Muud olemuslikult küberturbe tarkvara analüüsi, arenduse ja rakendamisega seotud tegevused.

4.2. Muud tingimused:
4.2.1. Toimumisviis – kohapeal, kaug- või hübriitöö;
4.2.2. Keeled – inglise (kokkuleppel ka muu kohalik keel). Lepingu täitmist puudutav dokumentatsioon eesti keeles. Lepingu täitmise keel on sätestatud raamlepingus ja hankelepingus igakordselt minikonkursil, kui see erineb raamlepingu sätestatust;
4.2.3. Tarne- ja muude tööde dokumendid – väljastatakse ühtse paketina (arhitektuur, testiplaanid, konfiguratsioonid, üleandmisakt).

4.3. Näidislahenduste kategooriad (teemade lõikes):
4.3.1. SIEM/SOAR ja juhtumihaldus – logide kogumine, kasutusjuhtude inseneeria, automaatika ja eskalatsioon; nt MS Sentinel, Elastic, Splunk; TheHive/Cortex, SOAR-tööriistad;
4.3.2. EDR/XDR/AV – lõpp- ja serverikaitse, telemeetria, reageerimine; nt Defender for Endpoint, CrowdStrike, Wazuh, Elastic Agent;
4.3.3. IAM/SSO/MFA/PAM – identiteet, ligipääs ja privileegide haldus; nt Entra ID/AD, Okta/Keycloak, CyberArk/Teleport;
4.3.4. NDR/IDS/IPS/NTA – võrgukäitumise ja sissetungide tuvastus; nt Zeek, Suricata, Security Onion/Corelight;
4.3.5. Perimeeter ja kaug-ligipääs – tulemüürid, WAF, DDoS, ZTNA/SASE/SSE; segmenteerimine ja VPN;
4.3.6. E-posti ja veebi turve – SEG, liivakastid, DMARC/DKIM/SPF, andmepüügikaitse;
4.3.7. Pilveturve – CSPM/CNAPP/CWPP, pilve-KMS/HSM, pilve-native kontrollid (AWS/Azure/GCP);
4.3.8. Konteiner ja Kubernetes – pildi skannimine (nt Trivy), runtime kaitse (Falco), poliitikad (OPA/Gatekeeper), registri turve;
4.3.9. AppSec/DevSecOps – SAST/DAST/SCA, secrets-haldus (nt Vault), CI/CD integreerimine, koodiskaneerimine;
4.3.10. Haavatavuste ja paigalduse haldus – skannerid (nt Nessus/OpenVAS), paigahaldus (WSUS/SCCM, repo'd), parandus-töövood;
4.3.11. Varundus, arhiveerimine ja DR – immuutsed varukoopiad, testitud taastamine, säilitustähtajad;
4.3.12. Krüptograafia, PKI ja võtmehaldused – sertide elutsükkel (ACME), PKI/CA, Vault/KMS/HSM;
4.3.13. Ohuluure (TIP/TI, (*Threat Intelligence Platform / Threat Intelligence*)) – MISP, OpenCTI, feed'id ja rikastamine; integratsioon SOC-i töövoogu;

4.3.14. DFIR ja andmeanalüütika – tööriistad forensikaks ja logi-/andmeladudeks (nt Velociraptor, Autopsy, Elastic);
4.3.15. OT/ICS/IoT turve – avastus, protokollid, segmentimine, monitooring;
4.3.16. MDM/UEM ja mobiiliturve – seadmete haldus, rakenduste ja andmete kaitse;
4.3.17. API turve – API lüüs, mTLS, ründekaitse ja avastus.

5. OSA 3 - Erinevad IT ja küberturvalisuse infrastruktuuri komponendid, paigaldamine ja seadistamine

5.1. IT infrastruktuuri komponentide soetamise, paigaldamise, seadistamise ja koolitamise teenuse hulka kuuluvad näiteks:
5.1.1. Arhitektuur ja projekteerimine – HLD/LLD, võrgu- ja süsteemiarhitektuur, IP-plaanid, aadressiruumid, nimetamistavad, „as-is → to-be" üleminekukava;
5.1.2. Hankimise tugi – tootjate/edasimüüjate võrdlus, pakkumiste küsimine ja võrdlustabelid, litsentsi- ja hooldusmudelid, tarneplaan;
5.1.3. Piloot/PoC – sobivuse, jõudluse ja turvaeelduste valideerimine kontrollitud keskkonnas;
5.1.4. Tarne ja logistika – tarnete planeerimine, toll/formaliseeringud (vajadusel);
5.1.5. Ruumide ja taristu ettevalmistus – riiulid/*rack*-id, *patch*-paneelid, kaabeldus (võrk/FO), tähistus ja märgistus, toide/UPS/PDU, jahutus, maandus; dokumenteerimine (rack elevations);
5.1.6. Paigaldus – füüsiline paigaldus, kaabeldus ja optika, algkonfiguratsioonid, ligipääs, turvaline esmane juurdepääs;
5.1.7. Seadistamine ja kõvendamine (hardening) – tootja best practice, paroolipoliitikad, RBAC, krüptograafia, logi- ja auditisätted, ajasünkroon (NTP/PTP), haldusvõrgud;
5.1.8. Integratsioonid ja vastavad tarkvaralised lahendused – AD/AAD/Entra, DNS/DHCP/NTP, SIEM/SOAR, EDR/XDR, varuhaldus, CMDB, piletisüsteem, jälgimine/valve (monitoring);
5.1.9. Virtualiseerimine ja platvormid – hüperviisori klastrite seadistamine (nt VMware/Hyper-V/Proxmox), HCI, konteiner-sõlmede loomine, ressursiplaanide teostus (CPU/RAM/IO);
5.1.10. Andmesalvestus ja varundus – SAN/NAS/objektsalvestus, replikatsioon, snapshot'id, NFS/SMB/iSCSI/FC, varundus- ja taastamisprotseduurid, RPO/RTO;
5.1.11. Kaugligipääs ja haldus – VPN/ZTNA appliance'id, bastion-host'id, PAM, turvaline kaugjuhtimine ja auditijälg;
5.1.12. Võrgukaitse ja tuvastus – tulemüürid, IDS/IPS/NDR sensorid, WAF/Load Balancer, segmenteerimine/ACL-id, QoS;
5.1.13. Testimine ja vastuvõtukriteeriumid – FAT/SAT/UAT; läbilaske- ja latentsustestid, IOPS/latentsus salvestil, failover/HA test, varutaaste test; vastuvõtuaktid;
5.1.14. Dokumentatsioon – HLD/LLD, „as-built", IP- ja VLAN-plaanid, kaabelduse skeemid, konfiguratsioonifailid, runbook'id/SOP-id, hooldus- ja DR-juhendid;
5.1.15. Koolitus ja üleandmine – admin-/operaatori koolitus, hooldusprotseduurid, teadmiste siire, üleandmisseminar;
5.1.16. Turbe- ja vastavusnõuded – ligipääsu tasemed, logimine/auditeerimine, krüpteerimine, seadmete ja piltide allkirjad/SBOM (kui kohaldub), tarneahela turvalisus;
5.1.17. Hooldus ja tugi (SLA) – tootjagarantii ja laiendused, püsivara/patch'i protsess, eskalatsioon tootjale, reservosad;
5.1.18. Jõudlus ja skaleeritavus – KPI-d (läbilaske, CPU/RAM utilisation, IOPS/latentsus), skaleerimis- ja arhiveerimisstrateegia, capacity planning;

5.1.19. Elutsükli haldus – EOL/EOS jälgimine, uuendus-/asendusplaanid, varade haldus (*asset id/serial*), CMDB uuendused;
5.1.20. Migreerimine ja üleminek – teenuste/VM-ide/andmete üleviimine, pilveteenuste kasutuselevõtt, hooldusaknad, tagasipööramise (rollback) plaan;
5.1.21. Väljatõstmine ja utiliseerimine – turvaline andmete hävitus (nt NIST 800-88), keskkonnanõuded, utiliseerimise tõendid;
5.1.22. Muud olemuslikult raamlepingu esemega seotud asjad ja teenused.

5.2. Muud tingimused:
5.2.1. Toimumisviis – kohapeal, kaug- või hübriidtöö (turvaline kaugjuhtimine);
5.2.2. Keeled – inglise (kokkuleppel muu kohalik keel). Lepingu täitmise keel on sätestatud raamlepingus ja hankelepingus igakordselt minikonkursil, kui see erineb raamlepingu sätestatust;
5.2.3. Tarne- ja vastuvõtu- komplektne üleandmine (kogu dokumentatsioon inglise (ja kokkuleppel muus kohalikus) keeles, sh arhitektuur, testid, konfiguratsioonid, kasutusjuhendid, vastuvõtuakt ja seadmed) kasusaajale tema asukohas vastavalt minikonkurssi tingimustele.
5.2.4. töövõtja on kohustatud tagama tarnitavatele asjadele vähemalt 24-kuulise garantii alates asjadele üleandmisest ja vastuvõtmisest, sh väljaspool Euroopa Liitu. Pakutav garantii peab kehtima kõigile toodetele.

5.3. Näidiskategooriad (teemade lõikes):
5.3.1. Lülitid ja ruuterid – Core/Distribution/Access-switching (L2/L3), QoS, EVPN/VXLAN (kui kohaldub), SD-WAN;
5.3.2. Tulemüürid ja perimeeter – NGFW, WAF, DDoS kaitse, segmenteerimine, VPN/SSL;
5.3.3. Traadita võrk (Wi-Fi) – kontrollerid, AP-d, külalisvõrk, 802.1X/NAC, RF-planeerimine;
5.3.4. Serverid – rack-/blade-platvormid, RAID, draiverid ja püsivara;
5.3.5. HCI ja klastrid – compute+storage klastrid, HA, quorum, replikatsioon;
5.3.6. Salvestus – SAN/NAS/objekt; FC/iSCSI; tiering; deduplikatsioon ja kompressioon;
5.3.7. Varundus ja taastamine – varundusaparaadid ja tarkvara, kataloogiseerimine, DR-proovid;
5.3.8. Virtualiseerimine – VMware/Hyper-V/Proxmox; ressursihaldus, vMotion/Live Migration, DRS/HA;
5.3.9. Konteineriplatvormi sõlmed – Kubernetes *worker*'id/registrid, pildi skannimine ja runtime kaitse (koostöös turbelahendustega);
5.3.10. Kaugligipääs/PAM/bastion – privaatne ligipääsu haldus, sessioonide salvestus ja audit;
5.3.11. IDS/IPS/NDR – sensorid, TAP/SPAN, reeglistikud ja signatuurid, integratsioon SIEM-iga;
5.3.12. Laadijad/Load Balancer'id – L4/L7 koormusejaotus, tervisekontrollid, SSL-offload;
5.3.13. Ajastus ja nimiteenused – NTP/PTP, DNS/DHCP, logi- ja sünkrooniteenused;
5.3.14. Haldus ja monitooring – NMS/APM, logi- ja mõõdikuarmatuurlauad, hoiatused, CMDB sidumine;
5.3.15. Riiulid ja toide– rack-id, UPS/PDU, kaabeldus/optika, märgistus, füüsiline turve ja ligipääs;
5.3.16. Optika ja meedia – SFP/SFP+/QSFP, DAC/AOC, FO terminaatorid ja patch'id.