

# **Tehisaru turvalisuse intensiivprogramm / AI Security Bootcamp**

## **Õppekava**

### **Täienduskoolitusasutuse nimetus**

Koiv Invest OÜ, reg. nr. 11517964

Kontakt: info@areng.ee

### **Õppekava nimi**

Tehisaru turvalisuse intensiivprogramm / AI Security Bootcamp

### **Õppekavarühm**

Arvutikasutus, ettevõtlus, juhtimine

### **Arenguprogrammi läbiviimise aeg**

9. novembrist 3. detsembrini 2026

esmaspäevast neljapäevani kell 10.00–

12.00.

43 ak/h veebipõhist õpet;

### **Õppekeel**

inglise keel

### **Õppe maksumus**

1500€ (lisandub km 24%)

### **Sihtgrupp**

Turvajuhid, küberturbe spetsialistid, arendajad ja IT-juhid, kes soovivad õppida AI-süsteemide toimimist, kaitset ja ründeid ning AI kasutamist organisatsiooni küberturbes ja juhtimises.

### **Õppe alustamise tingimused**

Nõutav on varasem arvuti kasutamine. Varasem tehisaru kasutamise kogemus ei ole vajalik.

### **Õppe eesmärk**

Anda osalejatele teadmised, praktilised oskused ja tööriistad, et kasutada tehisaru oma töös turvaliselt ning kaitsta, hinnata ja juhtida AI-süsteeme organisatsioonis.

## Õppesisu

Õppesisu jaguneb neljaks nädalaks. Igal nädalal toimub neli kahetunnist veebikohtumist koos praktiliste laboritöödega:

- 1. nädal (9.–12. november): AI alused – keelemudelid ja multimodaalsed mudelid, AI-agendid, viipade ja konteksti koostamine, turvaline ja privaatne kasutamine, kohalikud mudelid (Ollama), LLM-ruuterid ja AI-lüüsid, koodiagentide isoleerimine, MCP, RAG, Claude Code ja Codex.
- 2. nädal (16.–19. november): AI ja kaitse – AI-süsteemide pääsuhood, logimine, seire ja muud turvakontrollid; AI rakendamine turbeoperatsioonides (SOC), rakenduste turbes ja haavatavuste halduses.
- 3. nädal (23.–26. november): AI ja rünne – viibasüstid, jailbreak'id, andmete mürgitamine, mudeli petmine ja vargus ning andmete väljaviimine; AI kasutamine ründaja tööriistana, sh analüüs, automatiseerimine, sotsiaalne manipuleerimine ja exploit'ide arendamine; praktilised laborid.
- 4. nädal (30. november – 3. detsember): AI juhtimine – Euroopa ja USA reguleerimiskäsitlused, standardid, riskijuhtimise raamistikud, OWASP LLM Top 10 ja MITRE ATLAS, agentide kaardistamine ja haldamine, kaitsepiirded (guardrails), vari-AI ohjamine ning AI-poliitika.

## Õpiväljundid

Kursuse (programmi) läbinu:

- Selgitab keelemudelite ja AI-agentide toimimist ning kasutab neid igapäevatoos.
- Kasutab AI-d privaatset ja turvaliselt, arvestades andmekaitse ja tundliku teabe käsitlemise põhimõtteid.
- Rakendab AI-süsteemide kaitseks pääsuhoode, logimist ja seiret.
- Kasutab AI-tööriistu turbeoperatsioonides, rakenduste turvamiselt ja haavatavuste haldamisel.
- Tunneb ära peamised AI-süsteemide vastased ründed ning on neid praktiseerinud laborikeskkonnas.
- Hindab organisatsiooni AI-ga seotud ründepinda ja riske.
- Tunneb AI regulatsioone, standardeid ja riskijuhtimise raamistikke ning oskab panustada organisatsiooni AI-poliitika koostamisse.

## Õppemeetodid

Veebiloengud, juhendatud praktilised laboritööd virtuaalses laborikeskkonnas, demonstratsioonid, arutelud ning osalejate küsimustele vastamine. Teoreetilise ja praktilise õppe osakaal on ligikaudu võrdne.

## Iseseisev töö

Programmi käigus etteantud praktiliste laboriülesannete lahendamine ja õpitu iseseisev rakendamine.

## Õppematerjalide loend

Osalejad saavad elektroonilised õppematerjalid. Koolitused salvestatakse ning pärast programmi säilib õppuritel juurdepääs materjalidele ja laborikeskkonnale. Lõpetajad on oodatud Guild Security kogukonda.

## Nõuded õpingute lõpetamiseks

Programmi lõpetamise tingimused on osalemine vähemalt 75% koolitusest ning nõutud laboritööde sooritamine.

## **Hindamismeetodid ja hindamiskriteeriumid**

- Hindamismeetodiks on praktiliste laboriülesannete sooritamise kontroll.

## **Koolituse läbimisel väljastatav dokument (tunnistus või tõend)**

- Tunnistus väljastatakse õppijale, kes on osalenud vähemalt 75% koolitusest ning sooritanud laboritööd.
- Kui tunnistuse saamise tingimused ei ole täidetud, võib osalemise kohta väljastada tõendi, milles kajastub tegelik osalemine.

## **Koolitajate kompetentsust tagava kvalifikatsiooni või õpi- ja töökogemuse kirjeldus**

### **Patrik Maldre, Guild Security kaasasutaja**

Patrikul on üle 12 aasta kogemust küberturbes nii Eestis kui ka USA-s. Viimati töötas ta infoturbejuhina (CISO) CR14-s, kus vastutas turbeoperatsioonide, riskide ja juhtimise, turvateadlikkuse ning füüsilise turvalisuse eest. Varem juhtis ta ründava turvalisuse meeskonda ettevõttes Early Warning ning küberohuluure ja haavatavuste halduse programme ettevõttes Corteva Agriscience. Ta on töötanud ka ründava turvalisuse inseneri, FireEye ja CyberCube'i ohuluureanalüütiku ning Eesti Välisministeeriumi küberjulgeolekupoliitika referendina.

Alates 2018. aastast on Patrik Chicagos tegutseva Evolve Security Academy küberohuluure peainstruktor. Guild Securitys viib ta läbi AI Security Bootcampi, CybHER Bootcampi ja ettevõtete tellimuskoolitusi.

### **Sigrid Ojavee, infoturbejuht (CISO), Eesti Loto**

Sigridil on üle kümne aasta kogemust küberturbes ja sellega seotud rollides. Ta on praktikas kaitsnud olulist taristut, hoidnud ettevõtte äri turvaliselt käimas ja teinud turvalisuse kõigile asjaosalistele mõistetavaks ja atraktiivseks.

### **Martin Ojala, Kordoni kaasasutaja**

Martin on infoturbe juhtimise, riskihalduse ja vastavuse (GRC) ekspert. Alates 2020. aastast on ta infoturbe juhtimissüsteemide ja vastavuse platvormi Kordon kaasasutaja. Varem töötas ta Zendesk QA-s (endine Klaus) infoturbe- ja vastavusjuhina ning Pipedrive'is andmekaitse spetsialistina. Pipedrive'is kuulus ta infoturbemeeskonda, kes viis ettevõtte juhtimise, riskihalduse ja vastavuse uuele tasemele. Ta juhtis andmekaitsealgatusi ning osales SOC 2 Type II ja ISO 27001 auditites ja intsidendihalduses.

## **Õppemaksu tasumine ja tagastamine**

Õppemaks tuleb tasuda esitatud arve alusel, arvel kirjeldatud maksetähtjaks.

## **Tasumine maksegraafikuga**

- Võimalik on tasuda kahes osas. Esimene osamakse peab olema tasutud enne koolituse algust ja teine osamakse enne viimase koolituspäeva toimumise algust.
- Kui koolitusprogrammi viimase päeva alguseks pole kogu summa tasutud, siis on Koiv Invest OÜ-l õigus osalejale Tunnistus või Tõend mitte väljastada.
- Koolitusest loobumise korral palume sellest teada anda [info@areng.ee](mailto:info@areng.ee).
- Koolitusest loobumisel peale registreerumisperioodi lõppu tagastatakse 80% koolitusprogrammi maksumusest.
- Koiv Invest OÜ jätab endale õiguse teha õppeplaanis ja teemades ajakohaseid muudatusi. Väheste registreerujate tõttu on meil õigus kursus ära jätta või edasi lükata. Programmi registreerunud teavitatakse konkreetse koolituspäeva ära jäämisest või edasi lükkumisest

viivitamatult. Ärajäänud koolituspäeva eest tasutud summa makstakse tagasi või kantakse soovi korral üle mõne järgneva koolituse osavõtutasuks.

### **Vaidluste lahendamise kord**

Vaidlused lahendatakse kokkuleppe teel. Kui kokkulepet ei saavutata, lahendatakse vaidlused Harju Maakohtus.

### **Õppekeskkonna kirjeldus**

- Programm toimub veebikeskkonnas ning selles saab osaleda asukohast sõltumata. Praktilised ülesanded lahendatakse virtuaalses laborikeskkonnas.
- Iga õppeteema jaoks on ette valmistatud elektroonilised õppematerjalid.
- Õpe toimub veebis; kohapealset toitlustamist ega koolitusruumi ei kasutata.
- Osalejal peab olema stabiilne internetiühendus.
- Õppetöös osalemiseks on vaja arvutit, kaamerat ja mikrofoni.
- Veebipõhise õppe ja virtuaalsete laborite ligipääsuinfo edastatakse osalejatele enne kursust.
- Õppetöö toimub veebis juhendatud kohtumiste ja virtuaalsete laborite vormis

### **Koolitusprogrammi ja koolituspäevade kvaliteedi tagamise eeldus**

- Koiv Invest OÜ on Eesti üks juhtivaid avatud koolituste korraldajaid.
- Koiv Invest OÜ korraldab Eesti ettevõtete ja asutuste juhtidele ning spetsialistidele suunatud tööalast täienduskoolitust aastast 2008.
- Koiv Invest OÜ korraldab Eesti ettevõtete ja asutuste juhtidele ning spetsialistidele suunatud tehisaru koolitusi aastast 2023.
- Koiv Invest OÜ juhatuse liige on tegelenud avatud koolituste ja konverentside valdkonnas aastast 1997.
- Koiv Invest OÜ poolne kvaliteedi tagamise eeldus on Koiv Invest OÜ poolt väljatöötatud õppekorralduse ja kvaliteedi tagamise alused, mis kuvatakse koolituste veebilehel.
- Igal koolitusel võimaldatakse koolitusel osalejatel anda koolitajale ja koolituse korraldusele tagasisidet

### **Koolitajate kvaliteedi tagamine**

- Koolitajad omavad pikaajalist koolitaja töö kogemust, tuntust ja aktsepteeringut klientide-sihtrühmade hulgas.
- Koolitajate töö tulemust hinnatakse koolituse järgselt osalejate kirjaliku tagasiside põhjal. Vajadusel tehakse koolitajatele parandus- ja täiendustepanekuid.

### **Õppekeskkonna kvaliteedi tagamine**

- Koolitusprogrammi info tehakse osalejatele kättesaadavaks Areng.ee veebilehel enne kursuse algust.
- Koolitusprogramm võib olla kuvatud ka eraldi dokumendina, mille Koiv Invest OÜ osalejatele kirjalikus vormis väljastab.
- Kõik koolitusprogrammidele registreerunud saavad vähemalt 5 päeva enne programmi algust detailse info korraldusliku poole kohta.
- Koolituse jooksul luuakse õppimist toetav keskkond.
- Veebipõhised loengud ja virtuaalsed laborid toetavad teooria rakendamist praktilistes ülesannetes.

- Osalejal peab olema arvuti, kaamera ja mikrofoni ning stabiilne internetiühendus.
- Kõigi õppeteemade jaoks on koostatud elektroonilised õppematerjalid.
- Koolitus toimub veebis; kohapealset toitlustust ei pakuta.
- Veebikohtumisteks ja laboritöödeks on vajalik toimiv internetiühendus.
- Laboriülesanded toimuvad virtuaalses laborikeskkonnas.
- Veebikoolitusel osaledes tagab õppija oma internetiühenduse ja vajaliku arvutivarustuse.

#### **Koolituse kohta tagasiside kogumine**

- Koolitusprogrammi lõpul täidavad osalejad tagasisidelehe, kus annavad hinnangu programmi sisule ja lektori(te)le ning võimalus on teha ettepanekuid koolituse sisu ja formaadi paremaks muutmiseks.
- Koiv Invest OÜ juhtkond koos koolitaja(te)ga analüüsivad saadud tagasisidet ning vajadusel muudavad kursuse sisu või korraldust.
- Juhul kui tagasiside koolitajale on halb mitmel koolitusel järjest, kaalutakse koolitajaga koostöö lõpetamist ja kvaliteetsema koolitajaga koostöö alustamist.

Õppekava kinnitamise aeg: 12.10.2026

Urmas Kõiv

Koiv Invest OÜ juhatuse liige