cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

O1. Küberturvalisuse õppekava

Küberturbe pädevused erinevatele õppija profiilidele

Projekti on rahaliselt toetanud Euroopa Komisjon. Publikatsiooni sisu peegeldab autori seisukohti ja Euroopa Komisjon ei ole vastutav selles sisalduva informatsiooni kasutamise eest.

SISUKORD

1. Sissejuhatus

Vastavalt Intel Security värskele aruandele "Hacking the Skills Shortage" (https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf), on 2019. aastaks maailmas täitmata umbes 1-2 miljonit küberturbe spetsialisti ametikohta. Aruanne põhineb uuringul, milles osales 775 IT valdkonna küberturbega seotud otsustajat. 82% vastanutest on veendunud, et nende ettevõtetes on puudus küberturbe valdkonna teadmistest ja oskustest.

Samuti näitab ESG´s (Enterprise Strategy Group) 2017. aastal tehtud uuring, et 45% organisatsioonidest on märkinud, et neil on puudu küberturbe oskustest (https://www.esg-global.com/blog/esg-research-suggests-cybersecurity-skills-shortage-is-getting-worse). Antud uuring katab kõiki küberturbe valdkondi, ent ESC uuring näitab, et oskuste puudumine mõjutab otseselt nii küberturbe valdkonna analüütikat kui igapäevast tegevust.

Vaadates tänapäeva ühe suuremate ja laialdasemate küberohtudega maailma ning EL 2013. aasta küberstrateegia põhjal on just küberturve üks kolmest Digital Single Market´ ülevaates toodud väljakutsest. Seetõttu andis Euroopa Komisjon 13. septembril 2017. aastal välja küberturbe paketi.

Pakett toob välja olemasolevad vahendid ja esitab uued initsiatiivid, kuidas parendada EL küberturbe paindlikkust ja võimekust. EL strateegiline huvi on kindlustada, et luuakse tehnoloogilised küberturbe vahendid, mis aitaksid digitaalsel majandusel õitseda ning kaitseksid meie turvalisust, ühiskonda ja demokraatiat. See sisaldab nii kriitilise riist- kui tarkvara kaitset. Et suurendada EL küberturbe võimekust on Euroopa Komisjon ja juhtorganid teinud muude prioriteetide hulgas ka ettepanekuid ja koostanud tegevuskava, kuidas vähendada tühimikku küberkaitse teadmistes. EL on kavandanud luua 2018. aastal küberturbe koolituste ja hariduse platvormi.

Need on vaid mõned andmed ja initsiatiivid, mis näitavad kuivõrd oluline teema on tänases maailmas küberturvalisus. Lähtudes kogu maailma ja Euroopa suunistest, püüab CyVET projekt omalt poolt vähendada tühimikku küberturvalisuse kompetentside ja tegelike vajaduste vahel

(ettevõtete ja kogu ühiskonna vajaduste). Projekti eesmärk on luua intellektuaalsed väljundid, mis aitavad tõsta erinevate profiilidega inimestel tõsta küberturbe alast teadlikkust ja kompetentsust.

Kahest intellektuaalset väljundist esimene „Küberturbe õppekava“, mis on valik küberturbe põhiteadmistest ja kompetentsidest, aluseks projekti meeskonna uurimistöö, mis põhines järgmistel allikatel:

- **SANS Institute (Escal Institute of Advanced Technologies),** USA ettevõte, mis on spetsialiseerunud küberturvalisusele, koolitustele ja sertifitseerimisele.
- **National Institute of Standards and Technology (NIST),** mitte-regulatiivne USA agentuur, mis on välja töötanud NIST 800-53 küberutrbe raamistiku.
- **International Organization for Standardization** (ISO), mis on koostanud küberturbe standardite pere ISO/IEC 27000 .
- DigiComp Framework (**European Digital Competence Framework for Citizens**), mis kirjeldab põhjalikult inimestele vajalikud 5 võtmevaldkonna sh küberturvalisuse teadmised, oskused ja hoiakud.

Uurimistöö käigus leidsime, et küberturbe teadmised, oskused ja kompetentsid on võimalik grupeerida järgnevalt (vastavalt SANS Institute):

- **Rünnakute tuvastamine.** Avastada potentsiaalselt ohtlikke tegevusi, mis võiksid kahjustada konfidentsiaalsust, terviklikkust või informatsiooni kättesaadavust. Rünnakute tuvastamiseks on mõned tavapärased meetodid. Võrguvahendid võrguliikluse jälgimiseks, et tuvastada autoriseerimata tegevusi. Serveripõhised (host-based) püüavad avastada illegaalseid tegevusi spetsiifilistel seadmetel. Füüsiline tuvastamine tegeleb võimalike füüsilise keskkonna ohtude avastamisega.
- **Turvaline tarkvaraarendus.** Sageli on rünnakud edukad, sest tarkvaras on haavatavused või vead, seetõttu tuleks kommertstarkvaras teha regulaarselt tarkvara uuendusi.
- **Riskianalüüs.** Sisaldab riskide määratlemist, uute riskide avastamist ja riskide monitoorimist kogu projekti vältel. Esmalt on vajalik mõista, milliseid andmeid tuleb kaitsta ja miks. Äri valdkond peab määratlema oma väärtuslikumad varad ja ohud ning hindama nendega

seotud riske. Kuidas andmeid hoitakse, kellel on andmetele ligipääs ja kuidas andmeid kaitstakse on optimaalse andmekaitse 3 kriitilist küsimust.

- **Pilveteenuste turvalisus.** Pilveteenustele on omased teatud tüüpi ohud. Kõige suuremad ohud on andmetele ligipääs, süsteemi haavatavuste ära kasutamine, kasutajakontode kaaperdamine, kuritegelik hoolimatus või kuritahtlik tegevus.
- **Võrgu monitoorimine ja juurdepääsu haldamine.** Organisatsionoid vajavad spetsialiste, kes teavad mida ja kust otsida ning suudavad langetada kiirelt otsuseid kui on avastatud kahtlast tegevust.
- **Analüüs.** Innovatiivsete lahenduste loomiseks takistamaks häkkerite rünnakuid suurkorporatsioonide võrkudele ja sensitiivsete andmete varastamist.
- **Andmete kaitse.** Eriti oluline organisatsioonides, mis tegelevad tundlike valdkondadega – tervishoid, finantsteenused jms.

Mida võid leida sellest dokumendist?

Lähtudes eelnevatest valdkondadest oleme defineerinud kompetentsid ja õpiväljundid ja hindamiskriteeriumid. Oleme arvestanud ka profiilide eripäradega.

Järgmises peatükis selgitame, millist metoodikat oleme kasutanud kompetentside ja õpiväljundite kirjeldamisel ning küberturbe õppekava loomisel, kuid alustuseks selgitame, kuidas antud dokumenti kasutada:

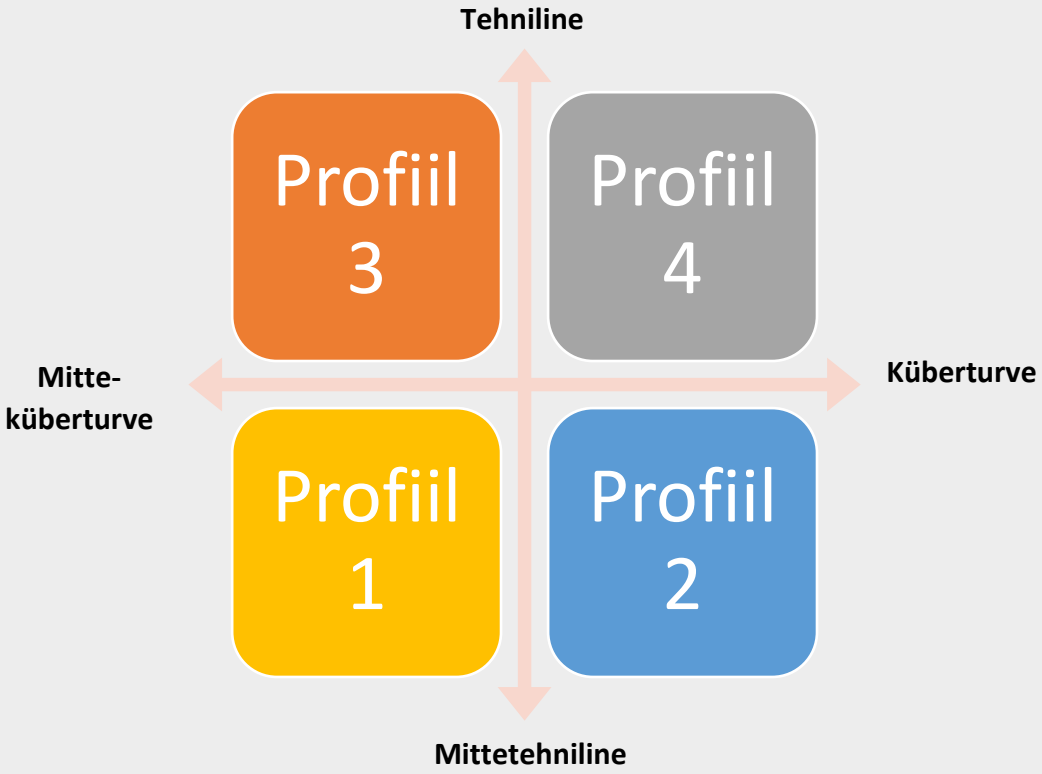
- Kui oled kutseõppe õpetaja, siis on sul võimalik kasutada õppekava tervikuna või selle üksikuid osi, sõltuvalt koolitatavatest ja eesmärkidest. Mooduleid on võimalik kasutada küberturbe valdkonna tutvustamiseks, lülitada neid olemasolevatesse kutseõppe moodulitesse , võid kasutada uue koolituse välja töötamiseks. Mooduleid võib kasutada nii nagu need on algselt loodud või kohendada vastavalt konkreetsetele vajadustele. Õppekavale lisaks oleme koostanud õppematerjale (väljund 2), mis katavad erinevaid kompetentse. Mõlemaid väljundeid võib kasutada nii koos kui eraldi, kuid meeles tuleb pidada, et väljund 2 materjalid põhinevad väljund 1 raames loodud dokumentidel.

- Kui oled organisatsioon või ettevõte, siis on võimalik kasutada mõlemaid väljundeid oma töötajate koolitamiseks või kasutada ainult 1. väljundit, et selgitamaks koolitajale, millist koolitust teie organisatsioon vajab ja millised moodulid on organisatsioonile olulised. Mooduleid võib kasutada tulevaste töötajate profiili kirjeldamisel, täpsustamaks, millised peavad olema nende küberturbe teadmised.
- Kui oled haridusasutus, kes vastutab õppekava arenduse eest, siis võiks vaadata projekti väljundid selle pilguga, et milliseid mooduleid oleks võimalik kasutada kutseõppe õppekavades või isegi spetsiaaletes küberturbe õppekavades Viimases peatükis toodud allikad võivad samuti olla kasuliku.

Õppekava ülesehitus on modulaarne (st mooduleid võib kasutada koos või eraldi) ja seda kirjeldab maatriks, milles ridades on kompetentsid ja veergudes moodulitega seotud õpiväljundid,.

2. Metoodika

Lähtudes eelnevast otsustasime defineerida ja kirjeldada 4 küberturvalisuse profiili.



- **Profiil 1** siia kuuluvad mittetehnilised töötajad, kellel oma ameti tõttu vaid minimaalse küberturbe valdkonna teadmised ja tehnilised oskused (näiteks kokk, automehhaanik, õde ..). Mooduli kompetentsid keskenduvad küberturbe põhiteadmistele (küberhügieen), tegeledes peamiselt tüüpiliste küberohtude ja nende ennetamisega, sotsiaalmeedia kasutamise hea tava ning tõstes arvutikasutajate küberturbealast teadlikkust.

- **Profiil 2** siia kuuluvad mittetehnilised töötajad, kes puutuvad kokku sensitiivse informatsiooniga ning seetõttu vajavad enam teadmisi küberturvalisusest (näiteks pangatöötajad, kindlustustöötajad, haigla registraatorid …). Mooduli kompetentsid keskenduvad peamiselt andmekaitse teemadele ja turvalisele andmeedastusele.

- **Profiil 3** siia kuuluvad tehnilised töötajad, kellel peavad olema nende töö spetsiifikast lähtuvalt küberturbest teatud piiratud teadmised ja oskused (näiteks CNC masinate operaatorid, robootika, internetipõhine tööstus, digitaaltööstus, IoT). Mooduli kompetentsid käsitlevad peamiselt küberturvet tänapäevases IT-l põhineval tootmises.

- **Profiil 4** IT taustaga tehniliste oskustega töötajad, kellel on küberturbe spetsiifilised teadmised ja oskused, et kaitsta/hoida ära rünnakuid, ning kes peavad arvutisüsteemi monitoorima ja koguma tõendeid. Mooduli kompetentsid on seotud haavatavuste analüüsiga, küberkaitse korraldamise, turvalisue tagamise ja tõendite analüüsiga,

Profiilid defineeriti esimesel projekti koosolekul Tallinnas. Tuleb siiski täpsustada, et profiilid pole seotud konkreetse EQF tasemega. Igale profiilile on sõnastatud õpiväljundid koos hindamiskriteeriumitega annab teadmise, kas seda profiili on võimalik sihtgrupi puhul kasutada. Õppekava koostamisel lähtusime:

- Profiil 1 moodulid nii, et neid oleks võimalik kasutada kõikidel kutseõppe õppekavadel. Moodulid annavad õppijale küberturvalisuse põhiteadmised, mida saab kasutada nii töö kui isiklikul tasandil. Fookuses on küberhügieen ja teadlikkuse tõstmine, mida kutseõppes ei õpetata, aga mis on hädavajalik digitaalne pädevus (loe lisaks https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework and http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110624/dc_guide_may18.pdf)
- Profiil 2 moodulid sobivad kasutamiseks EQF tasemetel 3-5. Pidasime silmas selliseid õppekavasid nagu ärikorraldus, majandusarvestus, kaubandus, tervishoid.
- Profiil 3 moodulid sobivad kasutamiseks EQF tasemetel 3-5, keskendudes tootmisega seotud valdkondadele (CNC pingid, robootika, elektrotehnika, automaatika).
- Profiili 4 moodulid sobivad kasutamiseks EQF tasemetel 4-5 IT-valdkonnas, näiteks rakenduste arendamine, tarkvaraarendus või IT-süsteemide haldus.

Õpiväljundite ja hindamiskriteeriumite välja töötamine oli selle dokumendi kõige keerulisem osa. Informatsiooni oli väga palju ja seda oli keeruline jagada meie poolt loodud profiilidesse. Abiks selles töös oli SANS instituudi poolt välja töötatud küberturbe valdkonnad. Suure hulga õpiväljundite lihtsustamine oli samuti suur väljakutse. Alustasime iga moodulis 12-20 õpiväljundiga ja vastavate hindamiskriteeriumitega. Grupeerisime õpiväljundid teemadele vastavalt ja osa väljundeid liitsime või lihtsustasime. Järgnevalt üks näide, millised olid algsed õpiväljundid:

UNITS OF COMPETENCE	LEARNING OUTCOMES
Unit 1. Penetration test **(This unit is based on the work roles described for: "system test and evaluation specialist" and "Information systems security developer" in the NICE**	U1LO1. The learner is able to determine the level of assurance of developed capabilities based on test results.
	U1LO2. The learner is able to test plans to address specifications and requirements.
	U1LO3. The learner is able to install and maintain network infraestructure device operating system software (e.g., IOS, firmware)
	U1LO4. The learner is able to make recommendations based on test results.
	U1LO5. The learner is able to determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated
	U1LO6. The learner is able to validate specifications and requirements for testability.
	U1LO7. The learner is able to analyze the results of software, hardware or interoperability testing.
	U1LO8. The learner is able to perform developmental testing on systems under development.
	U1LO9. The learner is able to perform interoperability testin on systems exchanging eletronic information with other systems.
	U1LO10. The learner is able to perform operational testing.
	U1LO11. The learner is able to test, evaluate and verify hardware and/or software to determine compliance with defined specifications and requirements.
	U1LO12. The learner is able to record and manage test data.
	U1LO13. The learner is able to develop and direct system testing and validation procedures and documentation.
	U1LO14. The learner is able to identify and direct the remediation of technical problems encountered during testing and implementaion of new systems
	U1LO15. The learner is able to identify, assess and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization´s evaluation and validation requirements.
	U1LO16. The learner is able to perform risk analysis (e.g. threat, vulnerability and probability of occurrence) whenevar an application or system undergoes a major change.
	U1LO17. The learner is able to utilize models and simulations to analyze or predict system performance under different operating conditions
	U1LO18. The learner is able to test and evaluate secure interfaces between information systems, physical systems and/or embedded technologies.
	U1LO19. The learner is able to perform an information security risk assessment.
	U1LO20. The learner is able to perform security reviews and identify security gaps in architecture.

Ja milline on tulemus:

Moodul 1. Testimine	U1LO1. Õppija on võimeline ära tundma ja kohaldama auditi protsessi etappe.
	U1LO2. Õppija oskab koguda tõendeid.
	U1LO3. Õppija oskab otsida ja avastada turvaauke.
	U1LO4. Õppija oskab koostada haavatavuste aruannet.

Mõnedel juhtudel lihtsustasime pädevused ja moodulid ise, kuid keerulisematel juhtudel (profiilid 3 ja 4) kasutasime Hispaania ja Hollandi partnerite abi.

Veel tuleks silmas pidada, et profiilide moodulid ei ole üksteist välistavad ja mooduleid on võimalik kasutada erinevates profiilides. Näiteks profiili 3 kuuluv õppija võib soovi korral kasutada ka profiili 2 mooduleid ja vastupidi. Kõik sõltub konkreetsest sihtgrupist ja nende vajadustest. Ülesannete koostamisel lähtusime õppijate eelnevatest teadmistest või taustast või millised võimalikud väljakutsed teda tööl ees ootavad. Soovi korral võib kõikide profiilide mooduleid kasutada ning saavutada eriti võimas multidistsiplinaarsus!

Õppekava peaks olema piisavalt paindlik, et seda oleks võimalik rakendada erinevates kutseõppe õppekavades, erinevatel tasemetel ja erinevatel ametitel. Tuleb lihtsalt uurida ja leida oma eesmärkidele kõige sobivamad moodulid!

3. Õppekava

	Moodul	Õpiväljundid	Hindamiskriteerium
Profiil 1	Moodul 1. Seadme ja digitaalse sisu kaitse	U1LO1. Õppija identifitseerib tehnoloogiaga seotud füüsilisi ja virtuaalseid riske	Õppija grupeerib riskid füüsilisteks ja virtuaalseteks.
		U1LO2. Õppija rakendab meetmeid riskide ennetamiseks, arendab oma teadmisi ja oskusi nimetatud valdkonnas	Õppija kirjeldab strateegiat riskide ennetamiseks.
		U1LO3. Õppija oskab viirusetõrje programme installeerida ja neid uuendada	Õppija installeerib/uuendab seadme viirusetõrje tarkvara.
		U1LO4. Õppija kasutab turvalist parooli, et kaitsta ennast võimalike pettuste eest.	Õppija genereerib turvalise parooli.
		U1LO5. Õppija oskab kaitsta erinevaid haavatavaid seadmeid võimalike digitaalsete ohtude eest (viirused, andmepüük jms).	Õppija määratleb uue seadme haavatavusi ja võimalikke kaitsemeetmeid.
		U1LO6. Õppija oskab identifitseerida andmete sensitiivsust/väärtust ja tunneb ära rünnakud erinevat tüüpi andmetele	Õppija määratleb sensitiivsed andmed ja võimalikke rünnakuid sensitiivsetele andmetele.
	Moodul 2. Isiklike andmete ja identiteedi kaitse	**U2LO1**. Õppija käitub adekvaatselt digitaalses maailmas ja haldab oma digitaalset jälge korrektselt.	Õppija tunneb GDPR Õppija kirjeldab Google Analyticsi tööpõhimõtet. Õppija mõistab ja kirjeldab digitaalse jalajälje kontseptsiooni.
		U2LO2. Õppija on võimeline tuvastama, et tema digitaalne identiteet on teiste poolt varastatud või väärkasutatud.	Õppija kirjeldab stsenaariumit, kus tema andmeid on väärkasutatud. Õppija kirjeldab identiteedivarguse mõistet ja hindab selle esinemise tõenäosust.
		U2LO3. Õppija on võimeline kaitsma teiste inimestega seotud informatsiooni (kolleeg, sõber jne).	Õppija kirjeldab isikliku informatsiooni (PII) kaitsmise tehnikaid,
		U2LO4. Õppija on võimeline otsima, kustutama ja/või muutma tema endaga seotud online infot.	Õppija selgitab, kuidas kustutada/muuta organisatsioonis hoitavat isiklikku informatsiooni. Õppija mõistab, milline on tema digitaalne jalajälg.
		U2LO5. Õppija oskab hallata oma digitaalset jälge.	Õppija haldab oma digitaalselt jalajälge.
		U2LO6. Õppija oskab kriitiliselt käituda jagades internetis enda kohta infot.	Õppija demonstreerib sobivaid auditeerimise tehinkaid isklike andmete internetis jagamisel.
		U2LO7. Õppija oskab luua vastavalt eesmärkidele erinevaid digitaalseid identiteete.	Õppija loob erinevaid sotsiaalmeedia kontosid, diferentseerides neid isiklikeks ja tööalasteks.

Profiil 2	**Moodul 3. Infoturbe haldamine ja regulatsioonid**	**U3LO1**. Õppija on mõistab infoturbe tähtsust ja selle olulisust organisatsioonis.	Õppija selgitab millised on organisatiooni infoturbe juhendid. Õppija oskab teha ettepanekuid juhendite parandamiseks ja täiendamiseks.
		U3LO2. Õppija teab peamisi küberturvalisuse ja infoturbe seaduseid, regulatsioone ja eetilisi põhimõtteid (näiteks GDPR ja ISO 27 000)	Õppija selgitab, mis on info- ja küberturbe põhimõtted, eeskirjad ja protseduurid, Õppija oskab rakendada infoturbe regulatsioone.
		U3LO3. Õppija on planeerib oma tööd vastavalt organisatsiooni infoturbe reeglitele.	Õppija rakendab oma töös infoturbe nõudeid ja reegleid.
		U3LO4. Õppija rakendab oma töös tele-/andmeside turbenõudeid: konfidentsiaalsus, terviklikkus, kättesaadavus.	Õppija selgitab, mis on konfidentsiaalsus, terviklikkus ja kättesaadavus. Õppija selgitab, millised on kofidentsiaalsuse nõude eiramise võimalikud tagajärjed.
		U3LO5. Õppija on rakendab töötajate koolitamisel infoturbe juhendeid, ohjata ja monitoorida.	Õppija koostab infoturbe reeglid oma organisatsioonile või töötajate grupile.
	Moodul 4. Infoturve kui organisatsiooni turvalisuse üks osa	**U4LO1.** Õppija on võimeline jälgima, sekkuma, ennetama ja raporteerima infoturbe riskidest töökohal.	Õppija oskab nimetada igapäevatöös ettetulevaid andmekaitse ohte ja riske Õppija oskab rakendada meetmeid andmete kaitsmiseks.
		U4LO2. Õppija on võimeline kasutama organisatsiooni turvasüsteeme vastavalt infoturbe nõuetele.	Õppija kasutab seoses infoturbega organisatsiooni turbevahendeid.
		U4LO3. Õppija oskab tagada füüsilise keskkonna turvalisust.	Õppija oskab kirjeldada erinevaid organisatsiooni füüsilise keskkonna ohte.
		U4LO4. Õppija oskab töötada turvaliselt nutiseadme ja pilveteenustega.	Õppija rakendab abinõusid, et töötada virtuaalses keskkonnas turvaliselt.
		U4LO5. Õppija on võimaline kaitsma materjale ja andmesalvestusi.	Õppija säilitab ja kaitseb materjale ja andmeid.
		U4LO6. Õppija on oskab rakendada põhimeetmeid tarkvara (operatsioonisüsteemid, rakendused) kaitsmiseks.	Õppija kasutab turvaliselt isiklikke seadmeid ja rakendusi.
	Moodul 5. Sissejuhatus küberturvalisusesse	**U5LO1**. Õppija oskab tuvastada erinevatest meediatest tulevat kriitilist informatsiooni.	Õppija võrdleb ja analüüsib kriitiliselt erinevatest allikatest saadud informatsiooni, et tuvastada kõige olulisemad haavatavused.
		U5LO2. Õppija on võimeline hindama kriitilise infrastruktuuri haavatavusi.	Õppija oskab tuvastada ühiskonna jaoks kriitilise infrastruktuuri haavatavusi.
		U5LO3. Õppija on võimeline tuvastama küberrünnakuid ja -ohte.	Õppija on kursis tüüpiliste küberrünnakute ja -ohtudega, mis võivad tema töös esineda.

Profile 3	**Moodul 6. Põhiteadmised IT ja OT seostest**	**U6LO1.** Õppija eristab IT ja operatsioonitehnoloogia (OT) valdkondi.	Õppija teab mõisteid kättesaadavus, terviklikkus ja konfidentsiaalsus IT ja OT valdkonnas.
		U6LO2. Õppijal on olemas põhiteadmised arvutivõrkudest (cisco,hp)	Õppija selgitab arvutivõrkude tööpõhimõtteid, mida tähendavad mõisted routing/switching või portforwarding.
		U6LO3. Õppija oskab määratleda tootmises tekkivaid küberohte ja küberrünnakute tagajärgi.	Õppija oskab määratleda vähemalt 3 ohtu ja nende võimalikke tagajärgi toomisele.
		U6LO4. Õppija teab IT valdkonna infoturbe standardeid.	Õppija teab ja oskab kirjeldada lühidalt järgnevaid standardeid: ISO 27001, COBIT, NIST and SANS
		U6LO5. Õppija teab OT valdkonna infoturbe standardeid.	Õppija teab ja oskab kirjeldada lühidalt vähemalt 3 järgnevatest standarditest: IEC 62443/ISA99, NIST 800 82, NIST 800 53, NERC CIP, CyberEssentials, NISTIR7228
		U6LO6. Õppija oskab kirjeldada paari tootmisega seotud infoturbe võtet.	Õppija teab, mis on segmenteerimine ja oskab kirjeldada vähemalt 2 tööstuses kasutavat tulemüüri.
		U6LO7. Õppija oskab selgitada, mis on OT põhikomponendid ja tüüpprotokollid.	Õppija oskab identifitseerida ja kirjeldada vähemalt 3 protokolli järgnevatest: PLC, SCADA, HMI, MES, MODBUS, PROFINET
	Moodul 7. Ettevõtte tööprotsessid ja -vahendid	**U7LO1**. Õppija oskab nimetada ja kirjeldada tootmisprotsessi tasemeid.	Õppija oskab nimetada ja kirjeldada tootmisprotsessi tasemeid etteantud stsenaariumi põhjal.
		U7LO2. Õppija oskab järgida ettevõtte tööprotsess, avastada võimalikke probleeme ja teavitada spetsialiste turvaprobleemidest.	Õppija järgib turvarikete avastamisel protseduuri reegleid Õppija suhtleb IT spetsialistidega konkreetselt ja arusaadavalt.
		U7LO3. Õppija on võimeline aru saama riketest ja turvaprobleemidest tööprotsessides või masinates.	Õppija toob 3 näidet võimalikest masinate turvariketest ja selgitab, mida peab sellises olukorras tegema.
		U7LO4. Õppija on võimeline aru saama, millised on ohud juhusliku mälupulga kasutamisel ettevõtte arvutivõrgus, masinates või arvutites.	Õppija selgitab, miks ei tohi kasutada suvalist mälupulka, millised on võimalikud ohud ja kuidas neid ennetada.
		U7LO5. Õppija on võimeline kasutama võrgu monitoorimisvahendeid, et tuvastada ebaharilikku võrguliiklust.	Õppija oskab kasutada monitoorimisvahendeid (näiteks wireshark) võrguliikluse jälgimiseks, et avastada anomaaliaid. , Õppija suhtleb võimalike ohtude teemal turvaspetsialistiga järgides ettevõtte protseduure.
		U7LO6. Õppija teab, mis on võrguprotokollid routing/vpn/PF/jne.	Õppija selgitab arvutivõrgu tööpõhimõtteid mitte IT valdkonna inimestele.
	Moodul 8. GDPR ja andmekaitse	**U8LO1**. Õppija teab, millised on vastav riigi ja Euroopa andmekaitseregulatsioonid.	Õppija teeb lühikokkuvõtte riigis kehtivatest GDPR reeglitest. Õppija oskab otsida oma tööga seotud andmekaitse alast relevantset informatsiooni sobivatest allikatest.
		U8LO2. Õppija oskab turvaliselt käsitleda erinevate masinatega seotud andmeid.	Õppija mõistab, mis on sensitiivne informatsioon, mille puhul peab eeldatavasti lähtuma andmekaitse regulatsioondiest.

Profiil 4	**Moodul 9. Testimine**	U1L01. Õppija on võimeline ära tundma ja kohaldama auditi protsessi etappe.	Auditi etapid on selgelt defineeritud. Testitakse vastavalt auditi etappidele, hinnates ja kontrollides riist- ja/või tarkvara vastavust spetsifikatsioonile / nõuetele.
		U1L02. Õppija oskab koguda tõendeid.	Sobiv skoop, infrastruktuur, ressursid ja piisav testjuhtumite arv, et adekvaatselt demonstreerida süsteemi nõudeid, Testandmed on korrektselt salvestatud ja hallatud.
		U1L03. Õppija oskab otsida ja avastada turvaauke.	Kasutatakse mudeleid ja simulaatoreid süsteemi analüüsimiseks või käitumise ennustamiseks. Riist-, tarkvara ja koostöövõime testimistulemused on põhjalikult analüüsitud. Haavatavuste leidmiseks hinnatakse infosüsteemi liideste, füüsilise keskkonna ja/või kasutavate tehnoloogiate turvalisust.
		U1L04. Õppija oskab koostada haavatavuste aruannet.	Õppija oskab hinnata andmete haavatavust ja süsteemi arhitektuuri kitsaskohti lähtudes andmeturbest. Testide tulemusena saadud soovitused on konkreetsed ja selged.
	Moodul 10.Juhtimine ja haldus	U2L01. Õppija teab ja mõistab standardeid ja küberturbe seadusandlust (ISO, ISACA, NIST)	Õppija oskab selgitada IT juhtimise praktikaid kasutades mõne tuntud raamistikku (näiteks ITL). Rakendab infoturbe standardeid (näiteks ISO/IEC 27001/27002).
		U2L02. Õppija on võimeline rakendama infoturbe juhtimise põhimõtteid (information security governance (ISMS))	Oskab selgitada informatsiooni tähtsust organisatsiooni strateegilises vaates. On määratletud rollid ja huvipooled infotehnoloogia valdkonnas. Äri ja IT strateegia toimivad kooskõlas. Soovitused, kuidas hallata organisatsiooni andmeid vastavalt dokumentatsioonile.
		U2L03. Õppija oskab teostada riskianalüüsi.	Analüüsitakse haavatavuste ja küberohtude võimalikku mõju organisatsiooni põhitegevusele. Monitooringus tulemusena uuendatakse valdkonna dokumentatsiooni.
		U2L04. Õppija oskab oma töös rakendada isikliku informatsiooni kasutamise reegleid (regulations about personal information (RGPD)).	Andmekaitses lähtutakse riiklikest ja rahvusvahelistest regulatsioonidest.
	Moodul 11. Arendus	U3L01. Õppija teab, mis turvalise programmeerimise tehnikad.	Küberturbe kavandamine arvutisüsteemile ja -võrgule on pidev ja integreeritud. On tagatud turvaline konfigureerimise. Programmeerimisel lähtutakse turvalise programmeerimise nõuetest, et minimeerida võimalikke ründeid.
		U3L02. Õppija on võimeline arendama rakendusi, milles andmete edastamiseks kasutatakse turvatud lahendusi (sertifikaadid, protokollid, signatuurid)	Rakendustes kasutatakse signatuuripõhist juurdepääsu. Juurdepääs rakenduste sisuhaldajatele on keelatud. Rakenduste loomisel lähtutakse võrgu Apps are developed adding a network security configuration.
		U3L03. Õppija on võimeline arendama rakendusi, milles ei saa olla andmeleket (autoriseerimine ja juurdepääs)	Rakendusi arendatakse nii, et privaatseid andmeid hoitakse lokaalsetes andmehoidlates. Andmete usaldusväärsus on tagatud.
		U3L04. Õppija on võimeline töötama vastavalt valdkonna regulatsioonidele (ASVS)	Veebirakenduste kavandamine, arendamine ja testimine toimub vastavalt ASVS nõuetele (Application Security Verification Standards)

Moodul 12. Analüüs	U4L01. Õppija on võimeline tuvastama ja järgima tõendite kogumis ja uurimise etappe.	Tõendite kogumise ja uurimise etapid on arusaadavad ja neid järgitakse. Tulemusi dokumenteeritakse ja jagatakse vastavalt organisatsioonis kehtivatele protseduurireeglitele.
	U4L02. Õppija oskab seadmeid kloonida.	Oskab kasutada varukoopiate tegemiseks erinevaid andmekandjaid
	U4L03. Õppija oskab kasutada erinevaid analüüsimetoodikaid.	Analüüsitakse logifaile, sündmusi ja muud informatsiooni, et leida parimaid meetodeid arvutivõrku rünnanud kurjategijate kindlaks tegemiseks. Informatsioon, millele ründe tulemusena ligi pääseti, on tuvastatav. Võrguliiklust jälgitakse ja kahtlased tegevused takistatakse ja analüüsitakse.
	U4L04. Õppija oskab andmeid taastada.	Varukoopiad analüüsitakse, et eha kindlaks kahjude ulatus. Andmed taastatakse vastavalt kirjeldatud protsessidele ja vahenditele (Forensic Tool Kit, Foremost…) Andmed dekrüpteeritakse.
Moodul 13. Perimetral security	U5L01. Õppija oskab tagada ühenduste turvalisust.	E-posti- ja veebiserver on kaitstud. Serverite kaitseks on konfigureeritud tulemüür. On tagatud DNS ja DHCP serverite kaitse. Turbenõudeid on tutvustatud organisatsiooni teistele üksustele.
	U5L02. Õppija oskab kavandada ja ehitada võrku vastavalt turvalise nõuetele vastavalt.	Potentsiaalselt kriitiliste komponentide tõrked on tuvastatud. Tõrgete tagajärgede leevendamiseks on võetud tarvitusele abinõud. Võrguühendused on krüpteeritud. Traadita ühendused on kaitstud krüpteerimise ja paroolidega. Tagavarakoopiate tegemine ja säilitamine on automatiseeritud kohalikus või globaalvõrgus ja kaitstud lubamatute pöördumiste vastu.
	U5L03. Õppija teab, mis on autentimise ja identideedi haldamise süsteemid (authentication and identity management systems (SSO))	On rakendatud AAA mudelit (authentication, authorisation and accounting). VPN kasutamine on hallatud. Individuaalsed juurdepääsusüsteemid on veebi ja mobiilirakendustega integreeritud.
	U5L04. Õppija on võimeline leidma ja tuvastama juhtumite lahendusi juhtumihaldussüsteemis	Peamised teenustepakkujad (SIEM systems) on identifitseeritud. Organisatsioonile on valitud vajadustelt ja hinnalt sobivaim lahendus.

4. Allikad

- International Organization of Standardization. *ISO/IEC 27000:2018*
  https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
- European Digital Competence Framework for Citizens. *DigComp into Action. A user guide to the European Digital Competence Framework.* http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110624/dc_guide_may18.pdf
- National Institute of Standards and Technology. National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
- Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF). *Marco Común de Competencia Digital Docente*. 2017. https://aprende.intef.es/sites/default/files/2018-05/2017_1020_Marco-Com%C3%BAn-de-Competencia-Digital-Docente.pdf