cyVETsecurity

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

01. Paikallisesti tarjottava ammatillinen tutkinnon osa kyberturvallisuudesta

Työkalu kyberturvallisuusosaamisen tunnistamiseen eri oppimisprofiileille

Hanke on rahoitettu Euroopan komission tuella. Tästä julkaisusta (tiedotteesta) vastaa ainoastaan sen laatija, eikä komissio ole vastuussa siihen sisältyvien tietojen mahdollisesta käytöstä.

Sisällysluettelo

1. Johdanto

Lähiaikoina julkaistun Intel Security raportin "Hacking the Skills Shortage" (https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf) mukaan maailmanlaajuisesti on yhdestä kahteen miljoonaa kyberturvallisuustoimea täyttämättä vuonna 2019. Raportti sisältää 775:ltä IT-turvallisuusalan päätöksentekijältä saadun kyselyn tulokset. Vastanneista 82 % raportoi kyberturvallisuustaitojen puutteista liiketoiminnassaan.

Samansuuntaisesti ESG:n (Enterprise Strategy Group) tutkimus osoittaa, että 45 %:ia organisaatioista on raportoinut ongelmallisen puutteen kyberturvallisuustaidossa vuonna 2017 (https://www.esg-global.com/blog/esg-research-suggests-cybersecurity-skills-shortage-is-getting-worse). Tämä soveltuu tietenkin kaikille kyberturvallisuuden aloille, mutta viimeaikaiset ESG-tutkimukset osoittavat, että osaamispulalla on suora yhteys turvallisuusanalytiikkaan ja operaatioihin.

Dynaamisesti kehittyvän uhkanäkymän ja EU:n 2013 kyberturvallisuuskatsauksen valossa, kyberturvallisuusvaarojen estäminen yhdessä, oli yksi kolmesta haasteesta, joka oli tunnistettu Digital Single Marketin väliraportissa. Tästä johtuen 13.9.2019 Komissio otti käyttöön kyberturvallisuuspaketin.

Paketti perustuu olemassa oleviin instrumentteihin ja esittää uusia aloitteita EU:n kybervastustuskyvyn ja -vastauksien parantamiseksi entisestään. EU:n strategisena intressinä on varmistaa, että kyberturvallisuuden teknologisia työkaluja on kehitetty sellaisilla tavoilla, että digitaalinen talous kukoistaa, mutta samalla suojelee turvallisuuttamme, yhteiskuntaamme ja demokratiaamme. Tämä sisältää kriittisen hardwaren ja softwaren suojauksen. EU:n kyberturvallisuuskapasiteetin vahvistamiseksi, Komissio ja korkea edustaja ehdottavat, muiden prioriteettien ja toimintojen ohella, kyberpuolustuksen osaamispulaan vastaamista. Tällä tavoitteella EU loi kyberpuolustukseen valmennus- ja koulutusalustan vuonna 2018.

Nämä ovat vain joitakin tietoja ja aloitteita, jotka kuvaavat IT-maailman todellisuutta kyberturvallisuuden osalta. CyVETsecurity-projekti kasvaa tässä tilanteessa, jossa kyberturvallisuus on eurooppalaisella ja globaalilla agendalla, ja tuottaa kaksi tuotosta, joilla yritetään pienentää olemassa olevan kyberturvallisuusosaamisen (ja tietoisuuden) ja todellisen tarpeen välistä rakoa (ei pelkästään yrityksissä mutta yhteiskunnassa itsessään).

Ensimmäinen näistä kahdesta tuotoksesta on "paikallisesti tarjottava tutkinnon osa kyberturvallisuudesta", joka on valikoima kyberturvallisuuteen liittyviä perustietoja, taitoja ja osaamista. Se on tehty laajalla tutkimuksella, jonka on toteuttanut projektitiimi, joka on sisällyttänyt seuraavat lähteet:

- SANS Instituutti (Escal Institute of Advanced Technologies), yhdysvaltalainen yritys, joka on erikoistunut turvallisuuteen ja kyberturvallisuuskoulutukseen ja sertifikaatteihin.
- National Institute of Standards and Technology (NIST), sääntelemätön toimija USA:sta, joka on kehittänyt NIST 800-53 sertifikaation kyberturvallisuuden viitekehyksessä.
- International Organization for Standardization (ISO), joka tarjoaa standardiperheen koskien tietoturvaa ISO/IEC 27000.
- DigiComp-viitekehys (European Digital Competence Framework for **Citizens**), joka tarjoaa laajan kuvauksen tiedoista, taidoista ja asenteista, joita ihmiset tarvitsevat viidellä avainalueella, joista yksi on turvallisuus.

Tutkimuksen aikana löysimme, että kyberturvallisuuteen liittyvät tiedot, taidot ja osaaminen voidaan ryhmitellä seuraavasti (SANS Instituutin mukaan) näihin osa-alueisiin:

- **Tunkeutumisen havaitseminen.** Se sisältää potentiaalisesti haitallisen toiminnan löytämisen, joka voisi vaarantaa informaation luottamuksellisuutta, eheyttä ja saatavuutta. On olemassa muutamia yleisiä tunkeutumisen havaitsemistyyppejä. Verkkopohjainen havaitseminen pyrkii havaitsemaan autorisoimattoman käytöksen verkkoliikenteeseen perustuen. Host-perusteinen havaitseminen pyrkii löytämään luvattoman toiminnan tietyllä laitteella. Fyysinen havaitseminen sisältää uhkien löytämisen fyysisillä järjestelmillä.
- **Turvallinen ohjelmistokehitys.** Useimmat datamurrot ovat onnistuneita, koska ohjelmistokoodissa on haavoittuvuuksia tai virheitä ja kaupallisia ohjelmistoja pitää korjata säännöllisesti.
- **Riskien lieventäminen.** Sisältää tunnistettujen riskien seuraamisen, uusien riskien löytämisen ja riskien seuraamisen koko projektin aikana. Ensiksi on välttämätöntä ymmärtää, että datan pitää olla suojattuna ja miksi. Yritysten tulee tunnistaa arvokkaimmat etunsa ja uhat, jotka asettavat ne riskiasemaan. Optimaalisen datan suojauksen osalta kolme kriittistä kysymystä ovat: miten informaatio on varastoitu, kenellä on sinne pääsy ja miten data on suojattu.
- **Pilviturvallisuus.** Pilviturvallisuuteen liittyy useita erityisiä uhkia. Joitakin päävaaroja ovat datamurrot, järjestelmien heikkouksien hyödyntäminen, tilien kaappaaminen, riittämätön tarkkuus ja pahansuovat sisäpiiriläiset.
- **Verkkomonitorointi ja sisäänpääsyyn hallinta.** Organisaatiot tarvitsevat myös asiantuntijoita, jotka tietävät mitä he etsivät ja jotka voivat tehdä nopeita päätöksiä, kun epäilyttävää käytöstä on havaittu.
- **Turvallisuusanalyysi**. Innovatiivisten ratkaisujen rakentaminen, jotta ehkäistään hakkereiden sisäänpääsy korporaatioiden verkkoihin ja arkaluontoisen datan varastaminen.
- **Dataturvallisuus.** Erityisen tärkeää haavoittuvilla aloilla oleville organisaatioille, kuten terveydenhuolto ja talouspalvelut.

Mitä löydät tästä dokumentista?

Ottaen kyseiset asiantuntemusaiheet pohjaksi, olemme määritelleet erilaiset osaamisalueet, oppimistulokset ja niihin liittyvät arviointikriteerit. Olemme tehneet sen ottaen huomioon erilaiset ammatilliset profiilit.

Seuraavassa kappaleessa selitämme mitä metodologiaa käytimme sen ja kyberturvallisuus-tutkinnon osan tekemiseen. Ensiksi haluamme, että ymmärrät miten voit käyttää tätä dokumenttia:

- Jos olet ammatillinen opettaja, voit käyttää tätä koko tutkinnon osaa tai vain osan siitä. Riippuen siitä kenelle ja mitkä ovat tavoitteesi, huomaat, että tarvitset vain joitakin osia, suurimman osan niistä tai jopa ne kaikki! Osien lukumäärästä riippumatta, voit käyttää niitä johdantona kyberturvallisuuteen ja tietoturvaratkaisuihin ja -käytöntöihin olemassa olevissa ammatillisissa koulutuksissa ja / tai voit suunnitella uuden koulutusohjelman ottamalla tutkinnon osamme (osittain tai kokonaan) sellaisenaan tai soveltamalla tai täydentämällä sitä millä tahansa muulla sisällöllä, jonka koet relevanttina. Tutkinnon osan jakamista varten, olemme tuottaneet myös koulutusmateriaalia, jotka kattavat erilaiset osaamisalat, joka on meidän toinen tuotos “kyberturvallisuushaasteet”. Voit käyttää molempia dokumentteja yhdessä tai erikseen, mutta pidä mielessä, että O2 (toinen tuotos) on rakennettua O1 (ensimmäinen tuotos) päälle.
- Jos olet yrityksen edustaja, voit käyttää molempia tuotoksia työntekijöiden sisäiseen koulutukseen tai pelkästään O1:stä, josta voit kysyä koulutuksen järjestäjää suunnittelemaan valmennuksen tiettyjen organisaatiosi näkökulmasta tärkeiden alueiden kattamiseen. Voit jopa käyttää tuotoksia tulevaisuuden työntekijäprofiilin määrittelyyn rekrytointiprosessia varten.

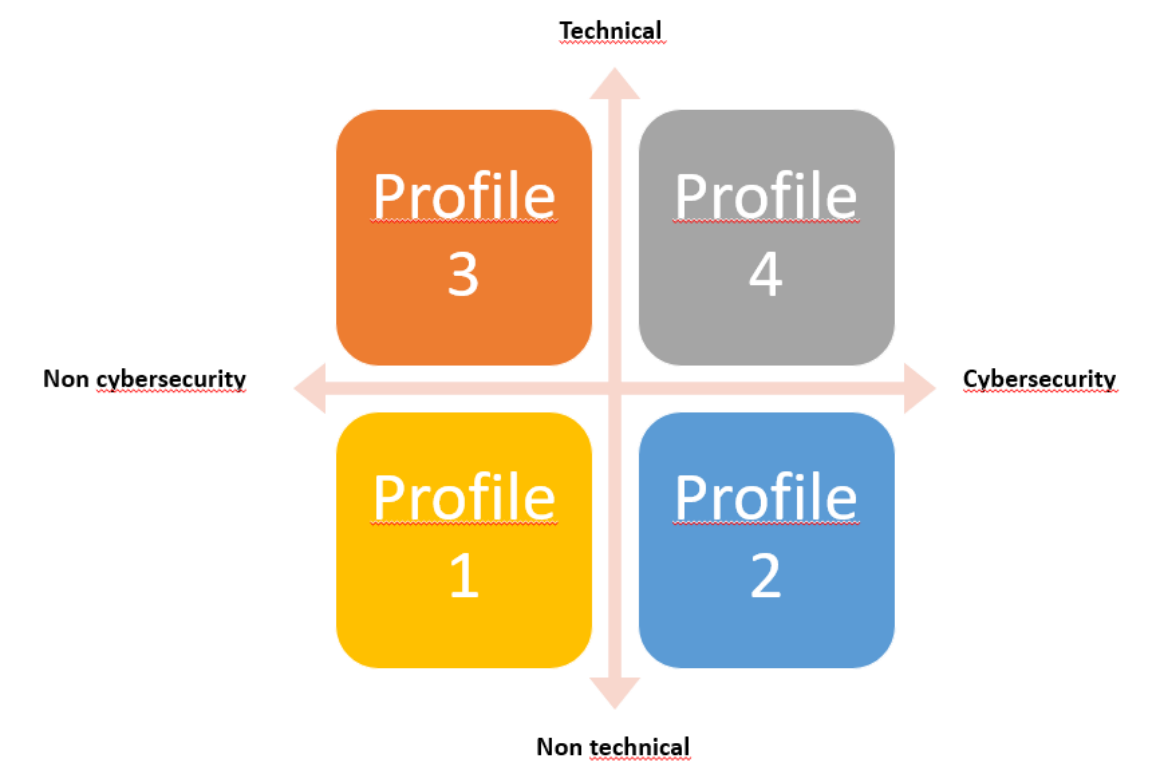
- Jos olet koulutusviranomaisen edustaja, joka on vastuussa opetussuunnitelmatyöstä, voit löytää tästä tuotoksesta mielenkiintoisia näkökulmia ja näet mitä mahdollisia osia voisi toteuttaa erilaisissa ammatillisissa tutkinnoissa tai jopa kyberturvallisuuteen erikoistuneissa koulutusohjelmissa. Viimeiseen kappaleeseen koottu sisällysluettelo voi olla myös hyödyllinen.

Modulaarista rakennetta noudattaen rakennettu (oppimistulokset ryhmiteltynä osiin, joita voi kouluttaa yhdessä tai erikseen), matriisin muodossa, jossa osaamisalat ovat riveillä ja oppimistulokset sarakkeilla, jokaiseen osaan liittyen.

2. Metodologia

Edellisessä kappaleessa kuvatut osaamisalat on otettu pohjaksi seuraavalla askeleella, jonka otimme erilaisten ammatillisten profiilien määrittelyssä ja niiden suhteesta kyberturvallisuuteen.

Määrittelimme neljä erilaista profiilityyppiä:



- **Profiili 1** Ammattilaiset, jotka eivät kuulu teknisiin profiileihin ja jotka eivät tarvitse paljon kyberturvallisuustietoja ja -taitoja ammatissaan, mutta tarvitsevat yleisiä jokaisen ihmisen tarvitsemia tietoja (esimerkiksi kokki, automekaanikko, putkimies, hoitaja…). Moduulit / osaamisalat keskittyvät tietoisuuteen (kyberturvallisuushygieniaan) ja käsittelevät uhkatyyppejä, hyviä käytäntöjä sosiaalisessa mediassa, uhkien lieventämistä ja peruskyberturvallisuustietoisuutta.

- **Profiili 2** Ammattilaiset, jotka eivät kuulu teknisiin profiileihin, mutta jotka tarvitsevat korkean tason asiantuntemusta kyberturvallisuudesta työn luonteen takia pääosin, koska he hallitsevat arkaluontoista informaatiota (esimerkiksi pankkityöntekijä, kirjanpitäjä, vakuutustyöntekijä, hallinnoija sairaalassa…) Moduulit / osaamisalat keskittyvät pääosin datan suojaukseen (säädökset…) ja turvalliseen datan vaihtoon.

- **Profiili 3** Ammattilaiset, jotka kuuluvat teknisiin profiileihin, mutta jotka tarvitsevat vain rajattuja tietoja ja taitoja kyberturvallisuuteen liittyen, pääosin liittyen heidän työtehtäviinsä (CNC-koneistaja, robotiikkatyöntekijä… jotka ovat yhteenliitetyn teollisuuden, digitaalisen teollisuuden, IoT:n kontekstissa). Tähän profiiliin kuuluvat osaamisalat keskittyvät kyberturvallisuuteen, joka liittyy OT ja IT yhteyteen.

- **Profiili 4** Ammattilaiset, joilla on tekninen profiili (IT-tausta) ja joilla on erikoistuneet tiedot ja taidot kyberturvallisuudesta suojauksen / ehkäisyn, monitoroinnin ja rikosteknisen analyysin näkökulmista. Osaamisalat käsittelevät haavoittuvuuksien analyysiä, turvallisuushallintaa, perimetraalista turvallisuutta ja rikosteknistä analyysiä.

Nämä neljä profiilia määriteltiin ja kuvattiin ensimmäisessä projektikokouksessa Tallinnassa. Selvennyksenä tulee mainita: nämä profiilit eivät viittaa mihinkään tiettyyn EQF-tasoon. Oppimistuloksien määrittely yhdessä arviointikriteerien kanssa tarjoaa käyttäjälle ohjeen, jotta hän voi päättää ovatko ne käyttökelpoisia tietylle kohderyhmälle. Tästä huolimatta, tutkinnon osan suunnittelussa otimme huomioon seuraavat asiat:

- Osat, jotka liittyvät profiiliin 1, ovat määritelty kuuluvaksi kaikille tasoilla ja kaikille ammatillisille tutkinnoille, sillä ne kattavat todella perusnäkökulmat kyberturvallisuuteen, joita voi soveltaa ammatillisella ja henkilökohtaisella tasolla. Ne keskittyvät kyberhygieniaan ja tietoisuuteen, joita ei opeteta ammatillisissa tutkinnoissa ja jotka kattavat perusdigitaaliset taidot, joita useimmilla ihmisillä ei kuitenkaan

ole. (katso https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework ja http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110624/dc_guide_may18.pdf)

- Osat, jotka liittyvät profiiliin 2, ovat määritelty pitäen mielessä EQF-tasot 3-5. Ajattelimme ammatillisia tutkintoja, kuten liiketoiminnanhallinto, talous, terveydenhuolto tai e-liiketoiminta ja vähittäiskauppa.
- Osat, jotka liittyivät profiiliin 3, ovat määritelty pitäen mielessä EQF-tasot 3-5, tavoitellen erityisesti teollisuusaloja, kuten CNC-koneistus, robotiikka, sähköala, elektroniikka tai automaatio.
- Osat, jotka liittyivät profiiliin 4, ovat määritelty pitäen mielessä EQF tasot 4-5 IT-taustalla, kuten sovelluskehitys, ohjelmointi tai IT-verkon hallinto.

Tämän dokumentin yksi haastavimmista osista oli jokaiseen osaan oppimistulosten määrittely ja arviointikriteerien tunnistaminen. Saatavilla oleva informaatio oli todella laaja, ja tiettyjen osien määrittely oli myös vaikeaa, mutta pitäen mielessä profiilit, jotka olimme määritelleet ja asiantuntemusalueet kyberturvallisuudesta, jotka SANS Instituutti oli määritellyt, tehtävä tuli helpommaksi. Informaation määrän yksinkertaistaminen suhteessa tiettyihin oppimistuloksiin oli monimutkaisempi prosessi, joka meni erilaisten askelten läpi. Aloitimme 12-20 oppimistuloksella osaa kohti (ja jopa vielä enemmän arviointikriteerejä!) ja ryhmittelimme oppimistuloksia niin, että se olisi hallittavampi, yhdistäen ja yksinkertaistaen joitakin niistä. Tässä on esimerkki alkutilanteesta:

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 tässä lopputilanteesta:

UNITS OF COMPETENCE	LEARNING OUTCOMES
Unit 1. Penetration test	U1LO1. The learner is able to identify and apply the phases of the Audit Process
	U1LO2. The learner is able to collect evidences
	U1LO3. The learner is able to search and exploit vulnerability
	U1LO4. The learner is able to do a vulnerability report

Joissakin tapauksissa teimme tätä yksinkertaistamisprosessia itse, mutta profiilien 3 ja 4 (sisällön osalta monimutkaisimpien) osalta saimme apua kumppaneilta Espanjasta ja Hollannista.

Viimeinen kysymys, joka tulee pitää mielessä on, että profiilit eivät ole välttämättä toisiaan poissulkevia. Esimerkiksi vaikka olemme määritelleet tietyt osat tietyille profiileille, voit vaihtaa osia oman mielesi mukaan ja antaa jollekin profiilissa 3 aktiviteetin profiilista 2 tai toisin pain. Se riippuu kohderyhmästäsi ja tavoitteistasi. Haasteiden suunnittelussa olemme ottaneet tämän huomioon ja määrittelemme mitkä edeltävät tiedot tai tausta henkilöllä tulee olla, jotta hän voi suorittaa tietyn haasteen. Tai voit jopa hullutella ja sekoittaa profiileja saavuttaaksesi monialaisen lähestymistavan!

Kuten voit nähdä, tutkinnon osan suunnittelu on tarpeeksi joustavaa, jotta sitä voi soveltaa erilaisiin ammatillisiin tutkintoihin ja tasoihin tai erilaisiin ammattilaisryhmiin. Katso mitkä osat ovat sopivimmat sinun tavoitteisiisi!

3. CyVETsecurity tutkinnon osa

	OSA	OPPIMISTULOKSET	ARVIOINTIKRITEERIT
Profiili 1	OSA 1. Laitteiden ja digitaalisen sisällön suojaus	U1LO1. Oppija osaa tunnistaa fyysisiä ja virtuaalia riskejä, jotka liittyvät teknologiaan	Oppija ryhmittelee monipuolisia riskejä 3 fyysisiin ja 3 virtuaalisiin riskeihin
		U1LO2. Oppija osaa soveltaa riskien ehkäisyn strategioita ja pitää tietonsa ajan tasalla	Oppija kuvaa strategian, jolla hän ehkäisee riskejä
		U1LO3. Oppija osaa ladata ja päivittää virus/haittaohjelmatorjuntaohjelmiston	Oppija asentaa / päivittää virus/haittaohjelmaohjelmiston annetulle laitteelle
		U1LO4. Oppija osaa suojata itsensä väärinkäytöksiltä käyttämällä turvallisia salasanoja	Oppija luo ja testaa turvallisen salasanan
		U1LO5. Oppija osaa suojata erilaisia haavoittuvia laitteita digitaalisilta uhilta (haittaohjelmat, kalastelu jne.)	Oppija tunnistaa potentiaalisia, haavoittuvia laitteita ja mahdollisia mekanismeja niiden suojeluun
		U1LO6. Oppija osaa tunnistaa arkaluontoisen / arvokkaan informaation ja hyökkäykset erityyppisessä datassa	Oppija tunnistaa arkaluontoisen datan ja mahdolliset hyökkäykset datan luonteesta riippuen
	OSA 2. Henkilökohtaisen datan ja digitaalisen identiteetin suojaus	U2LO1. Oppija osaa säädellä käytöstään digitaalisessa maailmassa ja hallita digitaalista jälkeään oikein	Oppija tietää GDPR-laista Oppija kuvaa miten Google Analytics toimii Oppija ymmärtää ja selittää digitaalisen jalanjäljen käsitteen
		U2LO2. Oppija osaa tunnistaa hänen digitaalisen identiteetin varkauden tai väärinkäytöksen riskit	Oppija tunnistaa skenaariot, jossa hänen data voisi olla väärinkäytetty Oppija kuvaa identiteettivarkaus käsitteen ja arvioi sen tapahtumisen riskit
		U2LO3. Oppija osaa suojella toisiin ihmisiin liittyvää tietoa ympäristössään (työntekijänä, ystävänä…)	Oppija tunnistaa tekniikat, joita käytetään henkilökohtaisten tietojen suojaamiseen
		U2LO4. Oppija osaa löytää, poistaa ja / tai muuttaa omia tietojaan online-järjestelmissä	Oppija selittää kuinka poistaa/ muuttaa henkilökohtaisia tietoja, jota pidetään organisaatiossa Oppija kokoaa hänen digitaalisen jalanjäljen
		U2LO5. Oppija osaa hallita omaa digitaalista jälkeään	Oppija hallitsee digitaalisen jalanjäljen
		U2LO6. Oppija osaa toimia kriittisesti jakaessaan omia tietojaan online-järjestelmissä	Oppija osoittaa kunnollisen teknisen tarkistuksen, kun hän jakaa henkilökohtaisia tietojaan online-järjestelmissä
		U2LO7. Oppija osaa käyttää useita digitaalisia identiteettejä, jotka on osoitettu erilaisiin tavoitteisiin	Oppija luo useita sosiaalisen median tilejä ja erottaa työ- ja henkilökohtaiset tilit toisistaan

Profiili 2	OSA 3. Tietoturvan hallinta ja säädökset	**U3L01**. Oppija ymmärtää tietoturvan tärkeyden ja sen merkityksen organisaatiolle	Oppija selittää selvästi mitkä ovat organisaation tietoturvaohjeistukset Oppija ehdottaa parannuksia olemassa oleviin ohjeistuksiin
		U3L02. Oppija osaa tunnistaa tietoturvan ja kyberturvallisuuden ohjeistuksen peruslait, säädökset ja eettiset periaatteet (esimerkiksi GDPR ja ISO 27 000)	Oppija tunnistaa tietoturvan ja kyberturvallisuuden peruskäsitteet, säädökset ja proseduurit Oppija soveltaa säädöksiä suhteessa tietoturvaan
		U3L03. Oppija osaa suunnitella työtään perustuen tietoturvaohjeistuksiin	Oppija soveltaa tietoturvaohjeita työhönsä
		U3L04. Oppija osaa työskennellessään soveltaa tele / datakommunikaatioturvallisuutta: luottamuksellisuus, eheys ja saatavuus	Oppija selittää luottamuksellisuuden, eheyden ja saatavuuden merkityksen Oppija selittää mahdolliset seuraukset luottamuksellisuuden rikkomisesta
		U3L05. Oppija osaa soveltaa henkilöstön turvallisuuskoulutusta: turvallisuusohjeistukset, kontrolli ja monitorointi	Oppija valmistelee lyhyen ohjeistusosion tietoturvasta organisaatiolle tai organisaation osalle henkilöstölle
	OSA 4. Tietoturva osana organisaation turvallisuuskäytäntöjä	**U4L01.** Oppija osaa havainnoida, arvioida, ehkäistä ja raportoida tietoturvariskeistä työpaikalla	Oppija nimeää tietoturvauhkia ja -riskejä, joita hän kohtaa arkipäiväisessä työssään Oppija soveltaa toimintatapoja, jotka varmistavat datan suojauksen
		U4L02. Oppija osaa käyttää organisaation turvallisuusjärjestelmiä suhteessa tietoturvaan	Oppija käyttää organisaation turvallisuusjärjestelmiä suhteessa tietoturva-asioihin
		U4L03. Oppija osaa hallinnoida fyysistä turvallisuutta alueella	Oppija tunnistaa erilaisia fyysisiä turvallisuustilanteita organisaatiossa
		U4L04. Oppija osaa työskennellä turvallisesti mobiili- ja pilvipalveluissa	Oppija käyttää toimintatapoja, joilla hän voi työskennellä turvallisesti virtuaalisessa ympäristössä
		U4L05. Oppija osaa varmistaa materiaalin ja datan säilytyksen ja suojauksen	Oppija säilyttää ja suojelee materiaalia ja dataa
		U4L06. Oppija osaa käyttää perustasolla software turvallisuutta: käyttöjärjestelmä ja ohjelmat	Oppija käyttää turvallisesti henkilökohtaisia laitteita ja ohjelmia
	OSA 5. Kyberturvallisuuden ja torjunnan perusteet	**U5L01**. Oppija osaa tunnistaa kriittisen tiedon eri medioista	Oppija vertailee ja analysoi tietoa kriittisesti, jota hän on saanut erilaisista medioista ja tunnistaa haavoittuvimmat tiedot
		U5L02. Oppija osaa arvioida yhteiskunnan kriittisen infrastruktuurin haavoittuvuutta	Oppija tunnistaa yhteiskunnan kriittisen infrastruktuurin haavoittuvuuden
		U5L03. Oppija osaa tunnistaa kyberhyökkäykset ja uhat	Oppija listaa yleisiä kyberturvallisuushyökkäyksiä ja uhkia, jotka voisivat mahdollisesti tapahtua ottaen huomioon informaation, jota hän hallitsee työssään

Profiili 3	Unit 6. Perustiedot IT & OT:n välisestä suhteesta	**U6LO1.** Oppija osaa erottaa IT:n ja OT:n toisistaan	Oppija erottaa IT:n ja OT:n luottamuksellisuuden, eheyden ja saatavuuden kannalta
		U6LO2. Oppija kykenee ymmärtämään verkkojen perustiedot (cisco,hp)	Oppija määrittelee perusverkot ja ymmärtää, mitä on reititys / kytkentä tai siirtäminen
		U6LO3. Oppija osaa tunnistaa pääuhat ja kyberhyökkäysten vaikutukset teollisuuden ympäristössä	Oppija tunnistaa vähintään kolme uhkaa ja niiden mahdolliset vaikutukset and seuraukset teollisuuden ympäristössä
		U6LO4. Oppija osaa kuvailla IT:n päätietoturvastandardit	Oppija tunnistaa ja kuvaa lyhyesti ainakin nämä standardit: ISO 27001, COBIT, NIST ja SANS
		U6LO5. Oppija osaa tunnistaa pääturvallisuusstandardit liittyen OT:hen	Oppija tunnistaa ja lyhyesti kuvailee vähintään kolme näistä standardeista: IEC 62443/ISA99, NIST 800 82, NIST 800 53, NERC CIP, CyberEssentials, NISTIR7228
		U6LO6. Oppija osaa tunnistaa joitakin turvallisuusarvioita teollisissa prosesseissa	Oppija kuvaa mitä segmentaatio on ja tunnistaa vähintäänkin kaksi teollista palomuuria
		U6LO7. Oppija osaa tunnistaa mitkä ovat OT:n pääkomponentit ja yleiset protokollat	Oppija tunnistaa ja kuvailee vähintäänkin kolme näistä protokollista: PLC, SCADA, HMI, MES, MODBUS, PROFINET
	Unit 7. Yrityksen proseduurit ja laitteet	**U7LO1**. Oppija osaa tunnistaa ja kuvata teollisen prosessin tasot	Oppija nimeää ja kuvailee tietyssä skenaariossa teollisen prosessin tasot
		U7LO2. Oppija osaa soveltaa yrityksen proseduureja, havaita mahdollisia ongelmia ja tiedottaa asiantuntijalle turvallisuusaiheista	Oppija soveltaa proseduuria, kun turvallisuusrikkomus on havaittu. Oppija tiedottaa IT spesialistia selkeästi ja ymmärrettävästi
		U7LO3. Oppija osaa havaita laitteen toimintahäiriön tai laitteen turvallisuusrikkomuksen	Oppija selittää kolme esimerkkiä mahdollisista laitteen turvallisuusrikkomuksista ja miten toimia niissä tilanteissa
		U7LO4. Oppija osaa tunnistaa riskit liittyen satunnaisen USB-tikun liittämiseen yrityksen verkkoon, laitteeseen tai tietokoneeseen	Oppija selittää miksi ei pidä liittää satunnaista USB-tikkua, USB-tikkujen liittämisen riskit ja miten estää ne
		U7LO5. Oppija osaa lukea verkon hallintatyökalua havaitakseen epätavallista verkkoliikennettä	Oppija käyttää hallintatyökalua (kuten wireshark) verkkoliikennelistan lukemiseen, arvioiden onko listassa mitään epätavallista. Oppija tiedottaa mahdollisista uhista turvallisuusspesialistille selkeällä tavalla ja noudattaen yrityksen protokollaa
		U7LO6. Oppija kykenee ymmärtämään verkkoprotokollaa, reititystä/ VPN/ PF jne.	Oppija selittää verkkojen perustiedot, ei ICT:n tasolla, mutta alemmalla tasolla
	Unit 8. GDPR ja datan suojaus	**U8LO1**. Oppija osaa tunnistaa mitkä ovat datan suojauksen säädökset hänen maassaan ja Euroopassa	Oppija antaa pienen yhteenvedon GDPR:stä hänen maassaan. Oppija katsoo relevanttia informaatiota koskien datan suojausta hänen toiminnassaan käyttäen oikeita lähteitä
		U8LO2. Oppija osaa työskennellä turvallisella tavalla, kun data on yhdistettynä erilaisiin laitteisiin töissä	Oppija tunnistaa haavoittuvan informaation, joka voi olla herkästi vahingoittuvaa datan suojaus säädösten kannalta

Profiili 4	OSA 9. Penetraatiotesti	U1L01. Oppija osaa tunnistaa ja soveltaa tarkastusprosessin vaiheet	Tarkastusprosessin vaiheet ovat selvästi tunnistettu Testi suoritetaan tarkastusprosessin vaiheiden mukaisesti, arvioiden ja varmistaen hardware ja / software, jotta varmistetaan määriteltyjen ohjeiden tai vaatimusten noudattamainen
		U1L02. Oppija osaa kerätä todistusaineistoa	Järjestelmän vaatimuksien mukainen laajuus, infrastruktuuri, resurssit ja datan otoskoko on riittävästi todennettu Testidata on kunnollisesti tallennettu ja hallittu
		U1L03. Oppija osaa etsiä ja hyödyntää haavoittuvuutta	Järjestelmän toiminnan analysoinnin tai ennustamisen malleja ja simulaatioita on käytetty Softwaren, hardwaren tai yhteistoimijuuden testitulokset ovat kunnollisesti analysoitu Informaatiojärjestelmien, fyysisten järjestelmien ja / tai upotettujen teknologioiden turvallisten rajapintojen arviointi on tehty haavoittuvuuksien etsimiseksi
		U1L04. Oppija osaa tehdä haavoittuvuusraportin	Informaation haavoittuvuudet ja turvallisuusaukot arkkitehtuurissa ova tunnistettu oikein Testitulosten perusteella on annettu suosituksia konkreettisella ja selvällä tavalla
	OSA 10. Turvallisuuden hallinto ja hallinta	U2L01. Oppija tietää ja ymmärtää standardit ja turvallisuussäädökset (ISO, ISACA, NIST)	IT-hallinnon hyvät käytännöt on selitetty käyttäen joitakin tunnettuja viitekehyksiä (esimerkiksi ITIL) Tietoturvahallinnon standardit (e.g. ISO/IEC 27001/27002) on sovellettu käyttöön
		U2L02. Oppija osaa soveltaa tietoturvahallintoa (ISMS)	Informaation rooli strategisesta näkökulmasta on selitetty Roolit & sidosryhmät informaatioteknologiassa on tunnistettu Liiketoiminta- ja ICT strategiat ovat yhdensuuntaisia Organisaation turvallisuusdokumentaation datan hallintaan liittyvät suositukset on annettu
		U2L03. Oppija osaa tehdä riskianalyysin	Haavoittuvuus ja uhka-arviointi on tehty osana liiketoiminnan vaikuttavuusanalyysia Turvallisuusdokumentaatio on päivitetty monitorointituloksien perusteella
		U2L04. Oppija osaa työskennellä soveltaen henkilötietoihin liittyviä säädöksiä (RGPD)	Kansalliset ja kansainväliset säädökset datan suojaukseen liittyen on otettu huomioon
	OSA 11. Turvallisuuden kehittäminen	U3L01. Oppija osaa tunnistaa turvallisia ohjelmointitekniikoita	Järjestelmien ja verkkojen kyberturvallisuussuunnitelma on kehitetty ta integroitu Turvalliset konfiguraatiohallintoprosessit ovat käytössä Ohjelmointi suoritetaan suojaus huomioon ottaen tunkeutumisen minimoimiseksi
		U3L02. Oppija osaa kehittää sovelluksia, joissa on informaationjakelu (sertifikaatit, protokollat ja allekirjoitukset)	Sovellukset on kehitetty käyttäen allekirjoitusperusteisia suostumuksia Sovelluksien sisällöntuotantoon sisäänpääsy on estetty Sovellukset on kehitetty verkon turvallisuuskonfiguraatioita lisäten
		U3L03. Oppija osaa kehittää sovelluksia ilman datavuotoa (autorisaatio & sisäänpääsy)	Sovelluksia on kehitetty yksityistä dataa varastoiden sisäiseen varastoon Datan oikeellisuus on tarkistettu
		U3L04. Oppija osaa työskennelle huomioiden säädökset (ASVS)	Web-sovellusten design, kehitys ja testaus on tehty huomioiden ASVS (Application Security Verification Standards)

OSA 12. Rikostekninen analyysi	U4LO1. Oppija osaa tunnistaa ja soveltaa rikosteknisen analyysin vaiheita	Rikosteknistä analyysiä tehdessä vaiheet ovat määriteltyjä ja niiden mukaan toimitaan Löydökset esitetään käyttäen vakiintuneita raporttiproseduureja
	U4LO2. Oppija osaa kloonata laitteita	Luotettavat kopiot kovalevyistä, levykkeistä, mobiililaitteiden CD:stä tai GPS on luotu
	U4LO3. Oppija osaa tehdä monipuolisen analyysin	Lokitiedostojen, todisteiden ja muiden tietojen analyysi on suoritettu parhaan metodin päättämiseksi, jotta voidaan tunnistaa verkkotunkeutumisen aiheuttaneet rikoksentekijät Tunkeutumisen jälkeen saavutettu informaatiota on tunnistettu Verkkoliikenne liittyen haitallisiin aktiviteetteihin on saatu kiinni ja analysoitu
	U4LO4. Oppija osaa palauttaa informaatiota	Palautettu data on tutkittu tunkeutumisen merkittävyyden määrittämiseksi Data on louhittu käyttäen kaiverrustekniikoita (Forensic Tool Kit, Foremost…) Kaapattu data on salattu
OSA 13. Perimetraalinen turvallisuus	U5LO1. Oppija osaa soveltaa kommunikaatioturvallisuustekniikoita	Sähköposti ja web-serverit ovat turvattuja Serveriturvallisuutta varten oleva palomuuri on konfiguroitu DNS ja DHCP serverisuojaus on varmistettu Turvallisuusvaatimuksista on tiedotettu toisille organisaation yksiköille
	U5LO2. Oppija osaa suunnitella ja soveltaa verkkoa turvallisuusmallin mukaisesti	Potentiaaliset kriittisten osien häiriöt on tunnistettu Häiriöiden vaikutusten lieventämiseksi on suoritettu toimenpiteitä Verkkoyhteydet ovat salattuja Lankattomat verkot ovat salauksella ja salasanajärjestelmällä suojattuja Backup-tiedostojen säilytys on automatisoitu paikalliseen tai globaaliin verkkoon ja suojattu luvattomalta käytöltä
	U5LO3. Oppija osaa tunnistaa todennus- ja identiteetinhallintajärjestelmiä (SSO)	AAA mallia (tunnistus, valtuutus ja kirjanpito) on sovellettu VPN menetellytapa on hallittu Kertakirjautumisjärjestelmät ovat integroituja verkko- ja mobiilisovelluksiin
	U5LO4. Oppija osaa tunnistaa tapahtumanhallintaratkaisuja	SIEM-järjestelmien päätarjoajat on tunnistettu Paras ratkaisu organisaation tarpeiden ja budjettitehokkuuden yhteensovittamiseksi on valittu

4. Lähdeluettelo

- 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