CyberAgent

Co-funded by the European Union

EQF-TASO 4 KOULUTUSOHJELMA

TIMTALIN LAATIMA LUONNOSVERSIO

KYBERAGENTTI 01.2025

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Työpaketti 3: Kyberturvallisuuden muutosagenttien oppimateriaalien kehittäminen

Tuloksena 3.2: Koulutusmoduulit ammatillisen koulutuksen opiskelijoille
3.2:n johtaja – TIMTAL (TR)

SISÄLTÖ

TAULUKOIDEN LUETTELO

JOHDANTO

Nopeat muutokset tieteessä ja teknologiassa, yksilöiden ja yhteiskunnan muuttuvat tarpeet sekä oppimisen ja opetuksen teorioiden ja lähestymistapojen innovaatiot ja kehitys ovat vaikuttaneet suoraan yksilöiltä odotettuihin rooleihin. Tämä muutos määrittelee yksilön, joka tuottaa tietoa, osaa käyttää sitä toiminnallisesti elämässä, osaa ratkaista ongelmia, ajattelee kriittisesti, on yritteliäs, päättäväinen, omaa viestintätaitoja, osaa empatiaa, edistää yhteiskuntaa ja kulttuuria jne.

Tietoyhteiskunnan huimaava vauhti tuo mukanaan yksilöiden ja yhteiskuntien alati muuttuvat tarpeet. Oppimisen ja opetuksen teorioiden innovaatiot muuttavat radikaalisti yksilöiltä odotettuja rooleja. Nykyään ei riitä, että ihminen vain omistaa tietoa, vaan esiin nousevat myös taidot, kuten kyky käyttää tietoa toiminnallisesti elämässä, kyky tuottaa ratkaisuja monimutkaisiin ongelmiin, kyky ajatella kriittisesti, kyky toimia yrittäjähenkisesti, kyky kommunikoida tehokkaasti, kyky osoittaa empatiaa ja kyky tuottaa lisäarvoa yhteiskunnalle. Tämä muutos kannustaa yksilöitä oppimaan, sopeutumaan ja parantamaan itseään jatkuvasti.

Tässä yhteydessä myös ammatillinen koulutus on käymässä läpi suurta muutosta. Perinteiset ammatit ovat korvautumassa uusilla, teknologiapainotteisilla ja jatkuvasti kehittyvillä ammateilla. Kyberturvallisuus on tässä muutoksessa ratkaisevan tärkeää. Digitaalistuvassa maailmassa kyberturvallisuusriskit ovat kasvussa kaikilla aloilla ja kaikissa ammateissa. Kyberturvallisuus on tärkeässä roolissa monilla aloilla, henkilötietojen suojauksesta yrityssalaisuuksien suojaamiseen, kriittisten infrastruktuurien turvallisuudesta rahoitustapahtumien turvallisuuteen.

Kyberturvallisuuskoulutuksen merkitys ammatillisessa koulutuksessa ei rajoitu teknisiin taitoihin. Se sisältää myös sellaisten yksilöiden kasvattamisen, joilla on eettiset arvot, korkea vastuuntunto, jotka tuntevat lainsäädännön ja ovat avoimia jatkuvalle oppimiselle. Kyberturvallisuus ei ole vain tekninen ongelma, vaan myös sosiaalinen vastuu. Siksi kyberturvallisuuskoulutuksen merkityksen korostaminen ammatillisessa koulutuksessa on kriittinen askel sekä yksilöiden että yhteiskunnan tulevaisuuden kannalta.

Ammatillinen koulutus sisältää kaikkien ammatillisten ja teknisten koulutuspalvelujen suunnittelun, tutkimuksen, kehittämisen, organisoinnin ja koordinoidun hallinnoinnin, valvonnan ja opetustoiminnan yhdessä maatalouden, teollisuuden ja palvelualojen kanssa koulutusjärjestelmän yhtenäisyyden puitteissa. Näiden koulutustoimintojen tavoitteena on kouluttaa asiantuntijoita, jotka varmistavat yhteiskunnan jatkuvuuden ja tuotannon kaikissa vaiheissa tarvittavan pätevän henkilöstön, sekä korostaa ammatillista koulutusta.

Cyber Agent -ammatillinen koulutusohjelma (EQF4) on suunniteltu valmistamaan yksilöitä kyberturvallisuuden pariin ja se perustuu työmarkkinoiden tarpeisiin ja työanalyysiin. Tässä lähestymistavassa analysoidaan kyberturvallisuusosaamista, määritellään ammatillinen profiili ja määritetään kyberturvallisuushenkilöstön tehtävät ja menettelytavat. Cyber Agent -opetussuunnitelman tavoitteena on tarjota oppituntien ja saavutusten kautta tiedot, taidot, asenteet ja käyttäytymismallit, jotka ovat välttämättömiä kyseisen työn ja tehtävien suorittamiseksi, ja toisaalta koulutustoiminta suunnitellaan siten, että se valmistaa henkilöitä työelämään tämän kehyksen mukaisesti.

1. CYBERAGENT EQF TASO 4 -OHJELMAN TAVOITTEET

Kyberturvallisuuden tarve on tullut varsin tärkeäksi erityisesti EU-maissa, mutta myös muualla maailmassa, ja se on kasvanut nopeasti viime vuosina. Teknologian kehityksen myötä myös kyberriskit ja -uhat ovat muuttuneet samaa vauhtia ja monimutkaistuneet. Kyberriskit ja -uhat ovat saavuttaneet potentiaalin, joka aiheuttaa paljon kattavampia ja negatiivisempia tuloksia kuin fyysiset hyökkäykset. Kun esimerkiksi rahoitus-, sähköisen viestinnän, energia-, liikenne- ja ilmailualat tarjoavat palveluita turvallisessa digitaalisessa ympäristössä, kansallisen kyberturvallisuuden varmistaminen on tullut yksi maamme tärkeimmistä prioriteeteista. Tässä yhteydessä tavoitteena on levittää kyberturvallisuuskoulutusta virallisessa ja epävirallisessa koulutuksessa sekä kehittää ja rikastuttaa koulutussisältöä.

2. EUROOPPALAINEN TUTKINTOJEN VIITEKEHYS

EU on kehittänyt eurooppalaisen tutkintojen viitekehyksen (EQF) käännöstyökaluksi, jonka avulla kansallisia tutkintoja on helpompi ymmärtää ja verrata toisiinsa. EQF:n tavoitteena on tukea oppijoiden ja työntekijöiden rajat ylittävää liikkuvuutta sekä edistää elinikäistä oppimista ja ammatillista kehitystä kaikkialla Euroopassa.

EQF on kahdeksan tasoinen, oppimistuloksiin perustuva viitekehys kaikille tutkinnoille, joka toimii käännöstyökaluna eri kansallisten tutkintojen viitekehysten välillä. Tämä viitekehys auttaa parantamaan ihmisten tutkintojen läpinäkyvyyttä, vertailukelpoisuutta ja siirrettävyyttä ja mahdollistaa eri maiden ja oppilaitosten tutkintojen vertailun.

EQF kattaa kaikki tutkintotyypit ja -tasot, ja oppimistulosten käyttö tekee selväksi, mitä henkilö tietää, ymmärtää ja osaa tehdä. Taso nousee osaamisen tason mukaan, taso 1 on alin ja 8 korkein taso. Tärkeintä on, että EQF on tiiviisti yhteydessä kansallisiin tutkintojen viitekehyksiin, jolloin se voi tarjota kattavan kartan kaikista tutkintotyypeistä ja -tasoista Euroopassa, jotka ovat yhä helpommin saatavilla tutkinto-tietokantojen kautta.

EQF perustettiin vuonna 2008 ja tarkistettiin myöhemmin vuonna 2017. Tarkistuksessa on säilytetty ydintavoitteet, jotka ovat läpinäkyvyyden ja keskinäisen luottamuksen luominen Euroopan tutkintojen kentällä. Jäsenvaltiot ovat sitoutuneet kehittämään EQF:ää edelleen ja tehostamaan sen toimintaa, jotta työnantajat, työntekijät ja oppijat ymmärtäisivät paremmin kansallisia, kansainvälisiä ja kolmansien maiden tutkintoja.

Kukin EQF:n kahdeksasta tasosta määritellään joukko kuvaajia, jotka osoittavat kyseisen tason tutkintoihin liittyvät oppimistulokset missä tahansa tutkintojärjestelmässä. Oppimistulokset määritellään seuraavasti:

- Tieto: EQF:n yhteydessä tieto kuvataan teoreettisena ja/tai faktatietona.
- Taidot: EQF:n yhteydessä taidot kuvataan kognitiivisiksi (loogisen, intuitiivisen ja luovan ajattelun käyttö) ja käytännöllisiksi (käsien taitojen ja menetelmien, materiaalien, työkalujen ja välineiden käyttö).
- Vastuullisuus ja itsenäisyys: EQF:n yhteydessä vastuullisuus ja itsenäisyys kuvataan oppijan kykynä soveltaa tietoja ja taitoja itsenäisesti ja vastuullisesti.

Taulukko1 – EQF-taso 4: oppimistulokset

Tieto	*Kyky*	*Vastuullisuus ja itsenäisyys*
Tosiasioihin ja teoriaan perustuva laaja-alainen tieto tietyn alan opinnoissa tai oppimisessa	Kognitiivisten ja käytännön taitojen kokonaisuus, jota tarvitaan ratkaisujen tuottamiseen tiettyihin ongelmiin työ- tai koulutusalan kontekstissa	Sovelletaan itsensä johtamista työ- tai oppimistilanteissa, jotka ovat yleensä ennustettavia mutta voivat muuttua; valvotaan muiden rutiinityötä, otetaan vastuuta työn tai oppimisen arvioinnista ja parantamisesta

3. KYBERTURVALLISUUDEN AMMATILLISEN KOULUTUKSEN OPISKELIJAT (EQF-TASO 4)

Kyberturvallisuusasiantuntija (taso 4) on pätevä ammattilainen, joka työskentelee työpaikan tietojärjestelmien parissa, osallistuu kyberturvallisuuden ennaltaehkäiseviin tutkimuksiin haavoittuvuuksien seurannan ja kyberturvallisuustietoisuuden lisäämisen prosessien puitteissa, seuraa toimia, valvoo kyberturvallisuusanalyyseissä käytettävien järjestelmien toimintaa ja kestävyyttä, määrittää yksinkertaisten verkkojen vaatimukset, perustaa fyysiset verkot, suorittaa yksinkertaisia verkko-laitteistoon liittyviä konfigurointeja, varmistaa verkon turvallisuuden, ylläpidon ja parannukset, tarjoaa teknistä tukea käyttäjille ja suorittaa ammatillista kehitystä koskevia tutkimuksia työpaikan IT-infrastruktuurien suojaamiseksi kyberuhkilta laatuvaatimusten puitteissa toteuttamalla työterveys- ja turvallisuus- sekä ympäristönsuojelutoimenpiteitä.

3.1. CYBERAGENT LEARNING -OHJELMA EQF-4

Ammatillisen koulutuksen opetussuunnitelma (EQF 4-5) on kehitetty mukauttamalla strategisesti kattavaa korkeakouluopetussuunnitelmaa (EQF 5-6). Mukautusprosessissa materiaalia tiivistettiin vastaamaan 1 ECTS-laajuutta ja keskityttiin ammatillisen koulutuksen kohderyhmälle ja pk-yritysten välittömille tarpeille merkityksellisimpiin oppimistuloksiin. Etusijalle asetettiin aiheet, joissa korostetaan käytännön sovelluksia ja perustason kyberturvallisuusosaamista, kun taas syvällisemmät teoreettiset käsitteet yksinkertaistettiin ammatillisen koulutuksen oppimispolkua vastaaviksi.

Taulukko2 -Moduuli: 1

Yksiköt	**Aiheet**
Projektinhallinta	Projektin suunnittelu Projektin tavoitteiden määrittely

	Nykyiset kyberturvallisuusuhkat (DDoS, kiristysohjelmat, haittaohjelmat, tietojenkalastelu, nollapäivähyökkäykset, IoT-hyökkäykset jne.) Uhkamallinnus ja haavoittuvuusanalyysi Kyberturvallisuusuhkien ja -tapahtumien raportointi
Oppimistulokset • Oppijat osaavat määritellä projektinhallinnan vaiheet ja luoda perustason projektisuunnitelman. (Soveltaminen) • Oppijat osaavat muotoilla selkeät, mitattavat ja saavutettavissa olevat projektitavoitteet. (Analyysi) • Oppijat tunnistavat, luokittelevat ja arvioivat erilaisia kyberturvallisuusuhkia. (Analyysi) • Oppijat kehittävät uhkamalleja ja suorittavat haavoittuvuusanalyyseja tietyille skenaarioille. (Soveltaminen) • Oppijat laativat tapahtumaraportit vakiintuneiden protokollien mukaisesti. (Soveltaminen)	
Resurssien hallinta	Turvallisuustyökalut ja -ohjelmistot Teknologisten resurssien tehokas käyttö
Oppimistulokset • Oppijat osoittavat kykenevänsä käyttämään tehokkaasti kyberturvallisuustyökaluja ja -ohjelmistoja uhkien havaitsemiseen ja niihin reagoimiseen. (Soveltaminen) • Oppijat optimoivat teknologiset resurssit turvallisuuden ja tehokkuuden parantamiseksi. (Sovellus)	
Turvallisuusmittarit	Turvallisuusmittarit ja mittaustekniikat Tietojen kerääminen SIEM-järjestelmällä Turvallisuusmittareiden analysointi Projektin seuranta ja suorituskyvyn arviointi Turvallisuusmittareiden raportointi
Oppimistulokset: • Oppijat tunnistavat ja soveltavat asiaankuuluvia turvallisuusmittareita ja mittaustekniikoita. (Sovellus) • Oppijat konfiguroivat ja käyttävät SIEM-työkaluja tietojen keräämiseen ja turvallisuuden seurantaan. (Sovellus) • Oppijat tulkitsevat ja analysoivat turvallisuusmittareita turvallisuustilanteen arvioimiseksi. (Analyysi) • Oppijat seuraavat ja arvioivat projektin suorituskykyä turvallisuusmittareiden avulla. (Arviointi) • Oppijat laativat ja esittävät raportteja turvallisuusmittareiden analyysin perusteella. (Soveltaminen)	
Laadunvarmistus ja laadunvalvonta	Laadunhallinta Kyberturvallisuuden laatustandardit Testaus- ja validointitekniikat
Oppimistulokset: • Oppijat toteuttavat laadunhallintakäytäntöjä kyberturvallisuusprojekteissa. (Soveltaminen)	

• Oppijat tunnistavat ja soveltavat asiaankuuluvia kyberturvallisuuden laatustandardeja. (Soveltaminen) • Oppijat kehittävät ja toteuttavat kyberturvallisuusratkaisujen testaus- ja validointimenettelyjä. (Sovellus)

Taulukko3 -Moduuli: 2

Yksiköt	**Aihe**
Käyttöjärjestelmän hallinta	Käyttöjärjestelmät Laitteiston ja ohjelmiston välinen suhde Binaarit, heksadesimaalilaskenta Bitit ja tavut Käyttöjärjestelmän komentorivi Windows- ja Linux-komennot Windows-asiakas ja -palvelin Sovellukset, prosessit ja palvelut Windowsissa Tiedostotunnisteet ja -tyypit Rekisteriavaimet ja -arvot Ohjauspaneelin asetukset Käyttäjät ja ryhmät Verkkotunnuksen rakenne ja palvelimen hallinta AD ja GPO Linux-rajapinnat ja ytimen Prosessit Linuxissa Tiedostojen ja hakemistojen nimeämiskäytännöt Linux-komentotulkki ja komentosyntaksi Tiedostojen ja kansioiden käsittely Putkien ja järjestelmänvalvontakomentojen käyttö Prosessien hallinta ja tehtävien ohjaus Palvelunhallinta
Oppimistulokset: • Oppijat vertailevat ja kontrastoivat erilaisia käyttöjärjestelmiä ja niiden arkkitehtuureja. • Oppijat selittävät laitteiston ja ohjelmiston välisen vuorovaikutuksen käyttöjärjestelmäympäristössä. • Oppijat suorittavat binaari- ja heksadesimaalimuunnoksia ja ymmärtävät datan esittämisen. • Oppijat suorittavat peruskomentoja Windows- ja Linux-ympäristöissä. • Oppijat hallinnoivat sovelluksia, palveluita ja prosesseja järjestelmätyökalujen avulla. • Oppijat konfiguroivat ja hallinnoivat Active Directoryä ja GPO:ita. • Oppijat käyttävät Linux-käyttöliittymiä ja suorittavat ytimen tason toimintoja. • Oppijat hallinnoivat palveluita ja järjestelmäprosesseja Linux-komentojen avulla.	

Tietokantajärjestelmien hallinta	Tallennustilat ja lähdeluettelot Verkkopalvelimen hallinta Järjestelmälokit ja lokien seuranta Tehtävien ajoittaminen Linuxissa Palvelimen ja verkon vianmääritys Varmuuskopiointi ja palautus GRUB:n suojaaminen Palomuurit Active Directory -objektien ja GPO:n hallinta DNS ja DHCP PowerShellin perusteet Microsoft BitLocker, AppLocker ja palomuuri LDAP ja Kerberos NTLM Salasana- ja lukituskäytännöt Todennus ja pääsyn hallinta Internet Control Message Protocol (ICMP) TCP vs. UDP NetBIOS ja SMB SSL ja TLS Sertifikaatit Telnet- ja Secure Shell (SSH) -protokollat HTTP ja HTTPS Sähköpostijärjestelmien protokollat Verkkotunnusjärjestelmäprotokolla (DNS) FTP ja RDP Kapselointi vs. dekapsulointi Verkkosnifferit ja Wireshark TCP/UDP DHCP, DNS
Oppimistulokset: • Oppijat konfiguroivat arkistot ja hallinnoivat lähdeluetteloita. • Oppijat analysoivat ja valvovat lokitiedostoja vianmäärityksen ja tietoturvan varmistamiseksi. • Oppijat suorittavat varmuuskopiointi- ja palautustoimenpiteitä tietojen eheyden varmistamiseksi. • Oppijat ottavat käyttöön tietoturvatoimenpiteitä, kuten palomuurit, BitLocker ja AppLocker.	
Verkon hallinta	Verkkotyypit ja langattomat verkot Verkot ja topologiat Laitteet Tunnistautuminen ja pääsy Laitteet Infrastruktuuri ja turvalaitteet Erikoistuneet laitteet ja verkkoarkkitehtuuri Virtuaaliset verkot Fyysiset ja loogiset osoitteet OSI- ja verkkomallit Tietojen kapselointi ja dekapsulointi Verkkoprotokollat ja porttinumerot

	Verkkovälineet ja kaapelit Langattomat teknologiat Verkonhallintatyökalut Cisco Packet Tracer Verkkoluokat ja aliverkot Osoitteenratkaisuprotokolla (ARP) Staattinen vs. dynaaminen IP-osoitteistus Verkkosoitteen muunnos (NAT) Kytkimet ja Cisco IOS Kytkinporttien suojaus ja reitittimen rajapinnat VLAN-verkkojen ja DTP:n konfigurointi VLAN-verkkojen välinen reititys Johdanto ACL:iin Verkon vianmääritys
Oppimistulokset: • Opiskelijat suunnittelevat ja hallinnoivat verkkoja sekä ymmärtävät protokollia ja topologioita. • Oppijat konfiguroivat VLAN-verkot ja ACL-luettelot sekä hallinnoivat IP-osoitteistojärjestelmiä. • Oppijat käyttävät Wireshark- ja Cisco Packet Tracer -työkaluja seurantaan ja vianmääritykseen.	
Pilvipalveluiden hallinta	Hypervisorit ja virtuaalikoneet Kontit Virtuaaliympäristöjen suojaaminen Varmuuskopiointi ja palautus Pilvilaskenta ja CSP:t Mitä ovat pilvipalvelumallit Pilvipalvelujen käyttöönottotyypit Virtuaaliset verkot AWS-laskentapalvelut Amazon Elastic Compute Cloud (EC2) Pilvipalvelujen valvontatyökalut Automaatio- ja orkestrointityökalut Pilvipalvelujen tietoturvauhat ja haavoittuvuudet Identiteetin ja pääsyn hallinta (IAM) Roolipohjainen pääsynhallinta (RBAC) Monivaiheinen todennus (MFA) Pilvipalvelun tietojen salaus Virtuaalinen yksityinen pilvi (VPC) Docker ja Kubernetes
Oppimistulokset: • Oppijat hallitsevat virtuaaliympäristöjä AWS:n, Docker:n ja Kubernetes:n avulla. • Oppijat ottavat käyttöön pilvipalvelun tietoturvakontrollit ja identiteetin hallinnan.	
Kyberfysikaalisten järjestelmien hallinta	Turvallisuus ja pääsyn hallinta Todentamistyypit TACACS+ ja RADIUS AAA-konfiguraatio Riskienhallinnan tavoitteet

	Salaus ja salauksen purku Hash-funktiot ja sateenkaaritaulukot MAC-spoofing ja ARP-myrkytys VLAN-hyppely ja rogue DHCP ICMP-tulva TCP- ja UDP-tulva Istunnon kaappaus DNS-spoofing Syväpuolustus (DID) ja nollaluottamus Demilitarisoidut vyöhykkeet (DMZ) Honeypotit ja verkon vahvistaminen Parhaat käytännöt turvallisen verkon luomiseksi VPN SSH ja VNC Tilannekohtaiset ja tilattomat palomuurit Isäntäpohjaiset vs. verkkopohjaiset Laitteistopohjaiset vs. ohjelmistopohjaiset palomuurit Verkkosovellusten palomuuri (WAF) Tekoäly palomuureissa IDS ja IPS NIDS ja HIDS Snort tcpdump
Oppimistulokset: • Oppijat osaavat suojata verkkoja palomuurien, IDS/IPS-järjestelmien ja uhkien havaitsemistyökalujen avulla. • Oppijat soveltavat salaustekniikoita ja hallinnoivat turvallisuusprotokollia.	
Järjestelmän vahvistaminen	GenAI-tekniikat Koodin luominen Käyttäjätilien hallinta ja pääsynvalvonta Poikkeavuuksien havaitseminen ja vianmääritys Apache2-palvelun virheiden ratkaiseminen Päivitysten ja korjaustiedostojen hallinta Automatisoitu varmuuskopiointi ja palautus Poistettujen tiedostojen palauttaminen GenAI:n avulla Kyberturvallisuusmenettelyt Uhkien havaitseminen ja analysointi Uhkiin reagointi ja korjaaminen Tekoälyn hyödyntäminen reaaliaikaisessa uhkien havaitsemisessa GenAI-mallien validointi ja testaus DNS-määritykset ja -turvallisuus DHCP-määritykset ja -turvallisuus PowerShellin perusteet Kytkimen portin turvallisuus Verkon perus-I/O-järjestelmä (NetBIOS) Palvelinviestiprotokolla (SMB) SSL (Secure Sockets Layer) ja TLS (Transport Layer Security)

	Turvallisuussertifikaatit Sähköpostijärjestelmien protokollat Verkkotunnusjärjestelmäprotokolla (DNS) Tiedostonsiirtoprotokolla (FTP) Etätyöpöytäprotokolla (RDP) Tehtävien ajoittaminen Linuxissa Palvelimen vianmääritys Verkon vianmääritys Varmuuskopiointi ja palautus GRUB:n suojaaminen Palomuurien määrittäminen ja suojaaminen
Oppimistulokset: • Oppijat soveltavat vahvistamistekniikoita järjestelmän turvallisuuden parantamiseksi. • Oppijat hyödyntävät tekoälyä uhkien havaitsemisessa ja järjestelmän valvonnassa.	
Järjestelmän vahvistaminen	IR vs. SOC Tapahtumat ja vaaratilanteet Hälytysten havaitseminen ja luokittelu Dokumentointi ja raportointi Mitä ovat verkkohyökkäykset? DoS ja DDoS SQL-injektio ja XSS Komentoinjektio ja paikallisen tiedoston sisällyttäminen (LFI) Sivustojen välinen pyynnön väärentäminen (CSRF) Brute-Force ja Credential Stuffing Hashin ja lipun välittäminen Rikkoutunut pääsynvalvonta Lunnasohjelmat Tietokonevirus ja mato Troijalainen ja mainosohjelma Keylogger ja kryptokaappaus Tiedostoton haittaohjelma Haittaohjelmien leviämisen ymmärtäminen IOC-tunnisteiden ja salasanakäytäntöjen hallinta Hyväksyttävän käytön periaatteet (AUP) Oman laitteen käyttö (BYOD) -käytännöt Etäkäyttökäytännöt
Oppimistulokset: • Erota R:n ja SOC:n keskeiset roolit ja yhteistyö. • Määritellä ero turvallisuuspoikkeamien ja tietoturvaloukkausten välillä. • Selitä tietoturvahälytysten lähteet ja luokitteluprosessit. • Laadi tehokas dokumentaatio ja raportointi tietoturvaloukkauksista. • Kuvata yleisiä verkkohyökkäystyyppejä (DoS/DDoS, SQL-injektio, XSS, komentoinjektio, LFI, CSRF). • Selitä brute force- ja credential stuffing -hyökkäykset ja kuvaile niiden torjuntakeinoja. • Ymmärrä "pass the hash" ja "pass the ticket" -hyökkäysten perusperiaatteet. • Selitä, miten rikkinäisiä pääsynvalvonnan haavoittuvuuksia voidaan hyödyntää. • Selitä erilaiset haittaohjelmat (ransomware, virus, mato, troijalainen, adware, keylogger, cryptojacking, tiedostoton haittaohjelma) ja niiden leviämistavat.	

• Selitä uhkatietojen indikaattoreiden (IOC) hallinnan merkitys. • Esitä vahvojen salasanakäytäntöjen ja hyväksyttävän käytön käytäntöjen (AUP) keskeiset elementit. • Arvioi BYOD- ja etäkäytön käytäntöjen vaikutukset tietoturvaan.

Taulukko4 -Moduuli: 3

Yksiköt	**Aihe**
Suorituskyvyn mittaaminen (mittarit)	Suorituskykymittarit Järjestelmän ja verkon valvonta Suorituskykymittareiden valvonta Verkon kartoitus Haavoittuvuuksien skannaus Verkkoliikenteen analysointi
Oppimistulokset: • Oppijat määrittelevät suorituskykymittarit ja selittävät niiden merkityksen järjestelmän ja verkon suorituskyvyn arvioinnissa. • Oppijat esittelevät seurantatyökalujen asennuksen ja käytön järjestelmän ja verkon suorituskyvyn jatkuvaan arviointiin. • Oppijat analysoivat ja tulkitsevat suorituskykymittareita järjestelmän kunnon arvioimiseksi ja optimointimahdollisuuksien tunnistamiseksi. • Oppijat luovat verkkokarttoja verkkojen rakenteiden visualisointia, seurantaa ja optimointia varten. • Oppijat suorittavat haavoittuvuustarkistuksia, tunnistavat tietoturvariskejä ja suosittelevat korjaustoimenpiteitä. • Oppijat suorittavat verkkoliikenteen analyysin havaitaakseen ja vastatakseen mahdollisiin uhkiin.	
Tietojen analysointi	Tietojen kerääminen Datan puhdistus ja esikäsittely Tietojen analysointi Tietojen visualisointi Analyyttiset työkalut Tietoturvassa käytettävät data-analyysit
Oppimistulokset • Oppijat keräävät analysoitavaksi relevanttia dataa järjestelmistä, verkoista ja tietoturvalokeista. • Oppijat puhdistavat ja esikäsittelevät raakadataa tarkkuuden ja johdonmukaisuuden varmistamiseksi. • Oppijat soveltavat tilastollisia ja analyyttisiä tekniikoita merkityksellisten johtopäätösten tekemiseksi tiedoista. • Oppijat luovat datavisualisointeja analyysitulosten tehokkaaksi viestittämiseksi. • Oppijat käyttävät työkaluja, kuten Python, R ja Power BI, kattavaan tietojen analysointiin.	

• Oppijat soveltavat data-analyysitekniikoita kyberturvallisuusuhkien havaitsemiseen, analysointiin ja lieventämiseen.	
Turvallisuustiedustelu	Turvallisuustiedustelun ymmärtäminen Turvallisuustiedustelun lähteet Uhkatiedustelun keräämisen menetelmät Tietoturvatietojen sovellusten tapaustutkimukset
Oppimistulokset • Opiskelijat osaavat selittää turvallisuustiedustelun merkityksen ennakoivassa uhkien hallinnassa. • Oppijat arvioivat turvallisuustiedon lähteitä, mukaan lukien uhkatiedot, raportit ja avoimen lähdekoodin työkalut. • Oppijat kuvaavat menetelmiä uhkatietojen keräämiseksi ja analysoimiseksi. • Oppijat tutkivat todellisia tapauksia ymmärtääkseen turvallisuustiedustelun soveltamisen kyberuhkien ehkäisemisessä.	

Taulukko5 -Moduuli: 4

Yksiköt	**Aihe**
Turvallisuusoperaatioiden perusteet	Turvallisuusoperaatioiden ja SOC:n (turvallisuusoperaatiokeskus) ymmärtäminen Turvallisuusoperaatioiden roolit ja vastuut Yleiskatsaus turvallisuusoperaatioiden työkaluihin ja tekniikoihin Käytännön esimerkkejä ja tapaustutkimuksia
Oppimistulokset • Oppijat osaavat selittää turvallisuusoperaatiokeskuksen tarkoituksen ja rakenteen sekä sen roolin kyberturvallisuudessa. • Oppijat kuvaavat turvallisuusoperaatioiden henkilöstön roolit ja vastuut, mukaan lukien tapahtumien reagointi, uhkien etsiminen ja seuranta. • Oppijat tunnistavat ja osoittavat yleisten turvallisuusoperaatiotyökalujen ja -teknologioiden käytön. • Oppijat analysoivat todellisia esimerkkejä ja tapaustutkimuksia ymmärtääkseen turvallisuusoperaatioita käytännössä.	
Turvallisuuden konvergenssi	Turvallisuuden konvergenssin ymmärtäminen Fyysisen turvallisuuden perusteet (fyysisen turvallisuuden periaatteet, fyysisten omaisuuserien suojaus, toimintaperiaatteet) Pk-yritysten yleiset uhat Yhteenliittymäkysymyksiä korostavat tapaustutkimukset
Oppimistulokset • Oppijat määrittelevät turvallisuuden konvergenssin ja selittävät sen merkityksen fyysisen ja kyberturvallisuuden toimenpiteiden integroinnissa. • Oppijat soveltavat fyysisen turvallisuuden periaatteita omaisuuden, tilojen ja henkilöstön suojaamiseen. • Oppijat tunnistavat ja arvioivat pienille ja keskisuurille yrityksille (pk-yrityksille) yleisesti tyypillisiä turvallisuusuhkia.	

• Oppijat tutkivat tapausesimerkkejä ymmärtääkseen konvergenssin haasteiden vaikutuksia. • Oppijat tarkastelevat turvallisuustietojen ja tapahtumien hallintaprosesseja.	
Turvallisuustietojen ja tapahtumien hallinta	Turvallisuuden seurannan periaatteiden tarkastelu (perustuu muiden kumppaneiden moduuliin) SIEM-ratkaisujen käyttöönotto Lokien ja hälytysten määrittäminen Uhkatiedon ja havaitsemismenetelmien tarkastelu (perustuu muiden kumppaneiden moduuliin)
Oppimistulokset: • Oppijat osaavat selittää turvallisuuden valvonnan periaatteet ja niiden soveltamisen SIEM-ratkaisuissa. • Oppijat konfiguroivat ja käyttävät SIEM-ratkaisuja tehokkaaseen uhkien havaitsemiseen ja niihin reagoimiseen. • Oppijat määrittävät loki- ja hälytysmekanismit SIEM-työkaluissa turvallisuustapahtumien seurantaa varten. • Oppijat arvioivat uhkatietojen ja havaitsemismenetelmien tehokkuutta turvallisuustoiminnoissa.	
Turvallisuusoperaatioiden käytännöt	Vaatimustenmukaisuus ja sääntely Turvallisuusoperaatioiden jatkuvan parantamisen strategiat Automaatio ja koordinointi Mittarit ja raportointi
Oppimistulokset: • Oppijat selittävät vaatimustenmukaisuuden ja sääntelyn merkityksen turvallisuusoperaatioissa. • Oppijat suunnittelevat ja toteuttavat jatkuvan parantamisen strategioita turvallisuusoperaatioissa. • Oppijat hyödyntävät automaatiota ja koordinointia turvallisuusoperaatioiden tehokkuuden parantamiseksi. • Oppijat kehittävät ja käyttävät turvallisuusmittareita ja raportointitekniikoita turvallisuustilanteen viestittämiseen.	

Taulukko6 -Moduuli: 5

Yksiköt	**Aihe**
Organisaation konteksti	Kyberturvallisuuden kehitys pk-yrityksissä Nykyiset suurimmat uhat ja haavoittuvuudet Kyberturvallisuuden vaikutus liiketoimintastrategiaan Pk-yritysten kyberturvallisuuden erityishaasteet verrattuna suuryrityksiin Kyberturvallisuuskäytäntöjen sääntelyvaikutusten ymmärtäminen ja niiden yhdenmukaistaminen hallintorakenteiden kanssa.

	Pk-yrityksille tyypilliset kyberturvallisuuden haasteet, kuten rajalliset budjetit, erikoistuneen turvallisuushenkilöstön puute ja käytännön menetelmät kyberturvallisuusinvestointien priorisoimiseksi.
Oppimistulokset: • Opiskelijat seuraavat kyberturvallisuuskäytäntöjen kehitystä pienissä ja keskisuurissa yrityksissä. • Oppijat tunnistavat ja arvioivat pk-yrityksiin vaikuttavat kriittisimmät nykyiset uhat ja haavoittuvuudet. • Oppijat analysoivat, miten kyberturvallisuus vaikuttaa liiketoimintastrategiaan ja operatiiviseen päätöksentekoon. • Oppijat vertaavat pk-yritysten kyberturvallisuushaasteita suurempien organisaatioiden haasteisiin. • Oppijat tulkitsevat kyberturvallisuutta koskevia sääntelyvaatimuksia ja arvioivat, miten ne integroituvat organisaation hallintoon. • Opiskelijat kuvaavat käytännön ratkaisuja pk-yritysten yleisiin kyberturvallisuushaasteisiin, kuten budjettirajoitteisiin ja rajalliseen henkilöstöön.	
Tietosuoja	Tietoturvan yksityisyyden periaatteet Henkilötietojen suojaus ja GDPR Tietosuojan vaikutus pk-yritysten toimintaan Työkalut ja tekniikat yksityisyyden suojaamiseksi
Oppimistulokset • Opiskelijat osaavat selittää tietoturvan ydinkäsitteet tietoturvan kontekstissa. • Oppijat soveltavat GDPR-vaatimuksia ja arvioivat niiden vaikutusta henkilötietojen suojaan. • Oppijat arvioivat, miten tietosuojasäännökset vaikuttavat pk-yritysten päivittäiseen toimintaan ja liiketoimintamalleihin. • Oppijat käyttävät työkaluja ja tekniikoita yksityisyyden suojaamiseen ja arkaluonteisten tietojen suojaamiseen.	
Lait, etiikka ja säännösten noudattaminen	Kyberturvallisuusorganisaatiot, -politiikat ja -standardit Asiaankuuluvat kansalliset ja kansainväliset lait Säännösten noudattaminen pk-yrityksissä Kyberturvallisuuden etiikka Kyberturvallisuuden vaatimusten noudattamatta jättämisen oikeudelliset seuraukset Analyysi siitä, miten tekoälypohjaisia työkaluja voidaan hyödyntää kyberturvallisuuden hallinnan vahvistamiseksi ja vaatimustenmukaisuuden varmistamiseksi jatkuvan seurannan ja automatisoidun uhkien torjunnan avulla.
Oppimistulokset • Opiskelijat tunnistavat keskeiset kyberturvallisuusorganisaatiot ja arvioivat asiaankuuluvia politiikkoja ja standardikehyksiä. • Oppijat tekevät yhteenvedon keskeisistä kyberturvallisuutta koskevista laeista kansallisella ja kansainvälisellä tasolla. • Oppijat suunnittelevat strategioita sääntöjen noudattamisen saavuttamiseksi ja ylläpitämiseksi pk-yritysten kontekstissa.	

<table>
<tr><td colspan="2">

Oppijat tarkastelevat kyberturvallisuuden päätöksenteon ja käyttäytymisen eettisiä näkökohtia.
Oppijat arvioivat kyberturvallisuuslakien noudattamatta jättämisen oikeudellisia seurauksia.
Oppijat tutkivat, miten tekoälytyökalut voivat parantaa hallintoa, automatisoida seurantaa ja tehostaa säännösten noudattamista.

</td></tr>
<tr><td>Turvallisuuden hallinto</td><td>Kyberturvallisuuden hallintorakenne
Turvallisuuden hallinnan roolit ja vastuut
Kyberturvallisuuden kypsyysmallit
Parantaa kykyä suorittaa riskinarviointeja ja laatia strategisia vastasuunnitelmia simuloiduissa kriisitilanteissa (kiristyshakkerointi, tietojenkalastelu jne.)
Johto- ja hallitustason viestintä
Kyberturvallisuuden viestintästrategiat
Turvallisuusraportointi ylimmälle johdolle
Kyberturvallisuuden kriisinhallinta ja viestintä
Hallitse kriisinhallinta- ja päätöksentekotaidot stressaavissa tilanteissa, joissa on kyse tekoälypohjaisista hyökkäyksistä ja kiristysohjelmista.</td></tr>
<tr><td colspan="2">Oppimistulokset

Opiskelijat suunnittelevat ja arvioivat hallintorakenteita, jotka tukevat tehokasta kyberturvallisuuden hallintaa.
Oppijat määrittelevät ja selkeyttävät vastuut organisaation turvallisuuskehyksissä.
Oppijat arvioivat kyberturvallisuuden kypsyystasoa vakiintuneiden mallien avulla.
Oppijat suorittavat riskinarviointeja ja kehittävät vastastrategioita tilanteisiin, kuten kiristysohjelmistoihin tai tietojenkalasteluun.
Oppijat laativat viestintäsuunnitelmia kyberturvallisuutta koskevien tietojen välittämiseksi ylimmälle johdolle ja hallituksen jäsenille.
Opiskelijat laativat tehokkaita viestintästrategioita sisäisille ja ulkoisille kyberturvallisuuden sidosryhmille.
Oppijat laativat raportteja, joissa kerrotaan ylimmälle johdolle kyberturvallisuuden suorituskyvystä ja riskeistä.
Oppijat harjoittelevat johtamista ja viestintää kyberturvallisuuskriisien aikana, mukaan lukien tekoälypohjaiset hyökkäykset.

</td></tr>
<tr><td>Johtamispolitiikka</td><td>Politiikan täytäntöönpano ja seuranta</td></tr>
<tr><td colspan="2">Oppimistulokset

Oppijat toteuttavat kyberturvallisuuspolitiikkaa ja laativat menettelyt sen jatkuvaa seurantaa ja täytäntöönpanoa varten.

</td></tr>
</table>

Taulukko7 -Moduuli: 6

Yksiköt	Aihe
Johdanto kyberturvallisuuden suunnitteluun: Tietojen, ihmisten ja yhteiskunnan turvallisuus	Tietoturva – tietojen tallennuksen turvallisuus, tutkintaprosessi Tietoturva – Salasanahyökkäystekniikat Ihmisten turvallisuus – tietoisuus ja ymmärrys Yhteiskunnan turvallisuus – mitä ovat kyberrikollisuus ja kyberetiikka Yhteiskunnan turvallisuus – kyberlaki – digitaaliset todisteet, digitaaliset sopimukset, monikansalliset yleissopimukset (sopimukset)
Oppimistulokset • Oppijat toteuttavat strategioita tallennettujen tietojen suojaamiseksi ja tutkintaprosessien tukemiseksi. • Oppijat tunnistavat ja analysoivat yleisiä salasanahyökkäystekniikoita ja kehittävät niihin sopivia vastatoimia. • Oppijat edistävät tietoturvatietoisuutta ja lisäävät ymmärrystä työntekijöiden ja sidosryhmien keskuudessa. • Oppijat selittävät kyberrikollisuuden yhteiskunnalliset vaikutukset ja arvioivat eettisiä näkökohtia digitaalisissa ympäristöissä. • Oppijat tulkitsevat keskeisiä kyberlakien käsitteitä, kuten digitaaliset todisteet, sopimukset ja kansainväliset sopimukset.	
Operatiivinen ja taktinen johtaminen	Pääsynvalvonnan toteuttaminen Päivitysten hallinta ja ohjelmistopäivitykset Järjestelmän jatkuva valvonta Työntekijöiden tietoturvatietoisuuden koulutus
Oppimistulokset: • Oppijat suunnittelevat ja toteuttavat tehokkaita pääsynvalvontamekanismeja järjestelmien ja tietojen suojaamiseksi. • Oppijat laativat menettelytavat ajantasaiselle korjaustiedostojen hallinnalle ja ohjelmistopäivityksille haavoittuvuuksien vähentämiseksi. • Oppijat seuraavat jatkuvasti järjestelmiä turvallisuustapahtumien havaitsemiseksi ja niihin reagoimiseksi. • Oppijat kehittävät ja toteuttavat tietoturvatietoisuuskoulutusohjelmia työntekijöiden sitoutumisen parantamiseksi ja inhimillisten riskien vähentämiseksi.	

Taulukko8 -Moduuli: 7

Yksiköt	**Aihe**
Riskien arviointi	Yleinen riskienhallinnan kehys ja prosessi Riskienhallinnan periaatteet Riskienhallinnan standardit Käytännön esimerkkejä ja tapaustutkimuksia
Oppimistulokset: • Oppijat kuvaavat ja soveltavat kyberturvallisuuden riskienhallinnan yleistä kehystä ja prosessia. • Oppijat selittävät tehokkaan kyberturvallisuuden riskienhallinnan perusperiaatteet. • Oppijat tunnistavat ja tulkitsevat yleisesti hyväksyttyjä riskienhallinnan standardeja. • Oppijat arvioivat riskiskenaarioita todellisten esimerkkien ja tapaustutkimusten avulla.	
Riskien tunnistaminen	Konkreettiset ja aineettomat riskilähteet Syyt ja tapahtumat Uhat ja mahdollisuudet Haavoittuvuudet ja kyvykkyydet Ulkoisen ja sisäisen kontekstin muutokset Uusien riskien indikaattorit Omaisuuden ja resurssien luonne ja arvo Seuraukset ja niiden vaikutus tavoitteisiin Tiedon rajoitukset ja luotettavuus Osallistujien ennakkoluulot, oletukset ja uskomukset. Käytännön esimerkkejä ja tapaustutkimuksia.
Oppimistulokset: • Oppijat oppivat erottamaan konkreettiset ja abstraktit riskilähteet kyberturvallisuusympäristöissä. • Oppijat tunnistavat riskien syyt ja laukaisevat tapahtumat. • Oppijat analysoivat kyberturvallisuusuhkia ja arvioivat mahdollisia parannuskohteita. • Oppijat arvioivat haavoittuvuuksia ja organisaation kykyjä riskien hallinnassa. • Oppijat arvioivat, miten kontekstuaaliset muutokset vaikuttavat kyberturvallisuusriskeihin. • Oppijat tunnistavat indikaattorit, jotka viittaavat uusien kyberturvallisuusuhkien syntymiseen. • Oppijat arvioivat omaisuuden arvon ja resurssien kriittisyyden suhteessa riskiin. • Oppijat arvioivat mahdollisia seurauksia ja niiden vaikutusta strategisiin tavoitteisiin. • Oppijat tunnistavat tiedon ja osaamisen rajoitukset riskien tunnistamisprosessissa. • Oppijat pohtivat, miten inhimilliset tekijät vaikuttavat riskien havaitsemiseen ja tunnistamiseen. • Oppijat soveltavat tunnistamistekniikoita todellisissa tilanteissa.	
Sisäiset uhat	Sisäisten uhkien määritelmä ja tyypit Sisäisten uhkien havaitseminen ja tunnistaminen Käytännön esimerkkejä ja tapaustutkimuksia
Oppimistulokset • Oppijat määrittelevät sisäiset uhat ja luokittelevat niiden eri tyypit.	

• Oppijat kehittävät taitoja sisäisten uhkien merkkien havaitsemiseksi ja niihin reagoimiseksi. • Oppijat analysoivat todellisia sisäisiä uhkia koskevia tapaustutkimuksia.	
Riskien mittaamisen ja arvioinnin mallit ja menetelmät	Kvantitatiiviset ja kvalitatiiviset riskien arviointimallit ja -menetelmät Tapahtumien todennäköisyys ja seuraukset Seurausten luonne ja laajuus Herkkyys- ja luotettavuustasot. Käytännön esimerkit ja tapaustutkimukset
Oppimistulokset: • Oppijat vertaavat ja soveltavat sekä kvantitatiivisia että kvalitatiivisia malleja kyberturvallisuusriskien arvioinnissa. • Oppijat arvioivat tunnistettujen riskien todennäköisyyttä ja mahdollisia seurauksia. • Oppijat arvioivat kyberturvallisuusriskeihin liittyvien seurausten vakavuuden ja laajuuden. • Oppijat määrittävät riskien arvioinnin epävarmuus- ja luotettavuustasot. • Oppijat toteuttavat riskien arviointimallit käytännön tilanteissa.	
Riskien hallinta	Seuranta ja tarkastelu Kirjaaminen ja raportointi Käytännön esimerkit ja tapaustutkimukset
Oppimistulokset • Oppijat suorittavat säännöllisiä riskien seuranta- ja arviointiprosesseja. • Oppijat dokumentoivat ja raportoivat riskienhallintatoimenpiteistä tehokkaasti. • Oppijat tutkivat todellisia esimerkkejä ymmärtääkseen tehokkaan riskienhallinnan toteutuksen.	

Taulukko9 -Moduuli: 8

Yksiköt	**Aihe**
Tapahtumien reagointi	Tapahtumien hallinnan määritelmä ja merkitys Tehokkaan tapahtumien reagointisuunnitelman keskeiset osat Yleiset kyberturvallisuusuhkat
Oppimistulokset • Oppijat määrittelevät tapahtumien hallinnan ja selittävät sen merkityksen kyberturvallisuuden hallinnassa. • Oppijat tunnistavat ja toteuttavat jäsennellyn tapahtumien hallinnan palautumissuunnitelman keskeiset osat. • Oppijat tunnistavat ja reagoivat yleisiin kyberturvallisuusuhkiin, joita kohtaavat tapahtumien käsittelyssä.	
Katastrofien jälkeinen palautuminen	Katastrofien jälkeisen palautumisen ymmärtäminen Roolit ja vastuut katastrofien jälkeisessä palautumisessa Palautumisen vaiheet katastrofin jälkeen
Oppimistulokset	

• Oppijat selittävät katastrofien jälkeisen palautumisen periaatteet ja tavoitteet kyberturvallisuuden kontekstissa. • Oppijat kuvaavat katastrofien jälkeiseen palautumiseen osallistuvien tiimin jäsenten roolit ja vastuut. • Oppijat laativat vaiheittaisen suunnitelman järjestelmien ja toimintojen palauttamiseksi kyberkatastrofin jälkeen.	
Liiketoiminnan jatkuvuus	Liiketoiminnan jatkuvuuden ymmärtäminen Liiketoiminnan jatkuvuuden roolit ja vastuut Liiketoiminnan vaikutusten analysointi
Oppimistulokset: • Oppijat selittävät liiketoiminnan jatkuvuuden suunnittelun käsitteen ja merkityksen. • Oppijat tunnistavat liiketoiminnan jatkuvuuden varmistamiseen liittyvät roolit ja vastuut. • Oppijat suorittavat liiketoiminnan vaikutusanalyysin arvioidakseen kriittisiä toimintoja ja riippuvuuksia.	
Turvallisuustietoisuus, koulutus ja valistus	Turvallisuustietoisuuden ymmärtäminen Työntekijöiden vastuut kyberturvallisuudessa
Oppimistulokset • Oppijat selittävät tietoturvatietoisuuden roolin ihmisiin liittyvien kyberturvallisuusriskien vähentämisessä. • Oppijat tunnistavat työntekijöiden vastuut kyberturvallisuusprotokollien ja parhaiden käytäntöjen noudattamisessa.	
Turvallisuuteen liittyvät rekrytointikäytännöt	Turvallisuusroolien vaatimusten määrittely Taustatarkistusten suorittaminen
Oppimistulokset: • Oppijat määrittelevät kyberturvallisuuden työroolit ja laativat niille sopivat vaatimukset. • Oppijat soveltavat parhaita käytäntöjä turvallisuuskriittisten roolien taustatarkistusten suorittamisessa.	
Turvallisuuden irtisanomiskäytännöt	Pääsyn välitön peruuttaminen Ilmoittaminen asiaankuuluville tiimeille Oikeudelliset ja säännösten noudattamista koskevat näkökohdat
Oppimistulokset • Oppijat ottavat käyttöön menettelyt, joilla käyttöoikeudet peruutetaan välittömästi työntekijän työsuhteen päättyessä. • Oppijat koordinoivat viestintää asiaankuuluvien osastojen kanssa irtisanomisprosessin aikana. • Oppijat tutkivat kyberturvallisuuden alalla työsuhteen päättymiseen liittyviä oikeudellisia ja säännösten noudattamista koskevia vaatimuksia.	
Kolmannen osapuolen turvallisuus	Kolmannen osapuolen riskien arviointi Kontrastien ja turvallisuusvaatimusten toteuttaminen Jatkuva seuranta ja auditointi Tapahtumien reagointi ja viestintä
Oppimistulokset: • Oppijat arvioivat kolmansien osapuolten toimittajiin ja kumppaneihin liittyviä turvallisuusriskejä.	

• Oppijat suunnittelevat ja soveltavat sopimuslausekkeita kolmansien osapuolten turvallisuusvaatimusten noudattamisen varmistamiseksi. • Oppijat ottavat käyttöön jatkuvan seurannan ja auditoinnin käytännöt kolmansien osapuolten turvallisuuden varmistamiseksi. • Oppijat koordinoivat kolmansien osapuolten kanssa tapahtumien reagointitoimien aikana.	
Turvallisuus tarkastusprosesseissa	Turvallisuuden sisällyttäminen tarkastuksiin Haavoittuvuuksien arviointi ja tunkeutumistestaus Tapahtuman jälkeiset tarkastukset
Oppimistulokset: • Oppijat integroivat turvallisuusnäkökohdat organisaation arviointiprosesseihin. • Oppijat suorittavat haavoittuvuuden arviointeja ja tunkeutumistestejä osana arviointitoimintaa. • Oppijat suorittavat tapahtuman jälkeisiä arviointeja tehokkuuden arvioimiseksi ja tulevien reagointien parantamiseksi.	
Erityiskysymys työntekijöiden henkilötietojen yksityisyydestä	Tietojen keräämisen rajoitukset Tallennus ja pääsyn hallinta Tietosuojamääräysten noudattaminen Tietojen jakaminen ja kolmannet osapuolet Työntekijöiden suostumus ja oikeudet
Oppimistulokset • Oppijat tunnistavat asianmukaiset rajat työntekijöiden henkilötietojen keräämiselle. • Oppijat soveltavat turvallisia tallennus- ja pääsynvalvontatoimenpiteitä työntekijöiden arkaluonteisiin tietoihin. • Oppijat varmistavat asiaankuuluvien tietosuojasäännösten, kuten GDPR:n, noudattamisen. • Oppijat arvioivat työntekijöiden tietojen jakamiseen kolmansille osapuolille liittyviä riskejä ja sääntöjä. • Oppijat ymmärtävät työntekijöiden oikeudet ja tietoon perustuvan suostumuksen saamisen tärkeyden.	

JOHTOPÄÄTÖS

Tässä raportissa esitetään ammatillisen koulutuksen tasolle sopiva opetussuunnitelma, joka on otettava huomioon CyberAgent-koulutuksen onnistuneessa toteuttamisessa. Projektin alusta lähtien tehdyn koulutustarpeiden kartoittamisen perusteella tässä asiakirjassa kuvataan ammatillisen koulutuksen opiskelijoiden tarpeet osallistumiseen.

Ohjelman valmistelussa on käytetty viitteenä CyberAgent-projektin EQF-tasolle 6 laadittua opetussuunnitelmaa. Tästä tasosta on valittu EQF-tasolle 4 sopivat aiheet ja poistettu sopimattomat aiheet.

Lopuksi, jotta koulutus olisi sisällöltään, järjestelyiltään ja taitojen kehittämisen kannalta mahdollisimman korkealaatuista, EQF-tasolta 6 siirrettäviä aiheita koskevia kysymyksiä ei sisällytetä arviointi- ja arviointivaiheeseen.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau