CyberAgent

Co-funded by the European Union

D3.1 KOULUTUSMODUULIT KORKEAKOULUOPISKELIJOILLE

KYBERAGENTTI 09.2025

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

www.cyberagents.eu

Työpaketti 3: Kyberagentti Oppimateriaalien kehittäminen

Tulostavoite 3.1: Koulutusmoduulit korkeakouluopiskelijoille

WP3:n johtaja – TIMTAL. D3.1:n johtaja – VU.

SISÄLTÖ

JOHDANTO

D2.2-raportin mukaan pk-yrityksillä on merkittävä pula pätevistä kyberturvallisuusasiantuntijoista, ja nykyisillä työntekijöillä ei usein ole tarvittavaa systeemistä osaamista, jotta he voisivat vastata asianmukaisesti yhä monimutkaisempiin kyberuhkiin. Siksi on erityisen tärkeää, että korkeakoulutuksessa valmistetaan asiantuntijoita, jotka voivat soveltaa tietojaan pk-yritysten ympäristössä – sekä teknisillä että johtamisen aloilla. Tämän vuoksi D2.3-asiakirjassa luotiin osaamisperusteinen oppimispolku, joka on jaettu eri aihealueisiin ja keskittyy käytännön taitojen kehittämiseen.

Tässä asiakirjassa esitellään yksi projektin tärkeimmistä tuloksista – korkeakouluopiskelijoille tarkoitetut koulutusmoduulit (D3.1). Tämän toiminnan tavoitteena on luoda korkeakouluille koulutusohjelmat, jotka kattavat pienille ja keskisuurille yrityksille (pk-yrityksille) tärkeät kyberturvallisuuden osa-alueet, taidot ja osaamiset.

Nämä moduulit ovat tulosta johdonmukaisesta työstä, joka perustuu yksityiskohtaiseen tarveanalyysiin (D2.2), jonka aikana haastateltiin pk-yritysten, ammatillisen koulutuksen ja korkeakoulujen edustajia, sekä selkeästi määriteltyyn oppimispolun rakenteeseen (D2.3).

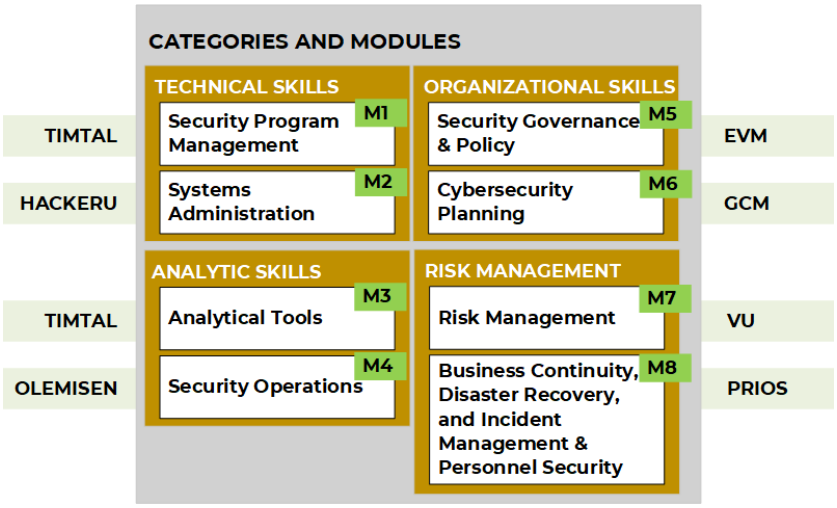
Koulutusohjelma, joka vastaa Euroopan tutkintojen viitekehyksen (EQF) tasoja 5–6, on suunniteltu korkeakouluopiskelijoille ja edistyneille pk-yritysten työntekijöille. Se koostuu kahdeksasta ydinmoduulista ja yhdestä inspiroivasta moduulista, jotka kattavat neljä keskeistä osaamisaluetta:

- **Tekniset taidot** (turvallisuusohjelmien hallinta, järjestelmien hallinta).
- **Analyyttiset taidot** (analyyttiset työkalut, tietoturvaoperaatiot).
- **Organisaatiotaidot** (turvallisuuden hallinto ja politiikka, kyberturvallisuuden suunnittelu).
- **Riskienhallinta** (riskienhallinta ja -lieventäminen, liiketoiminnan jatkuvuus, katastrofien jälkeinen palautuminen sekä tapahtumien hallinta ja henkilöstön turvallisuus).

Jokainen moduuli on arvoltaan 3 ECTS-opintopistettä (vastaa 75 tunnin opiskelijatyömäärää), on korkeakoulutusalueen periaatteiden mukainen ja noudattaa D2.3:ssa määriteltyjä metodologisia suosituksia: koulutus perustuu aktiivisiin oppimismenetelmiin (esim. tapaustutkimukset, projektipohjainen oppiminen) ja itseohjautuvaan oppimiseen, ja oppimistulokset on selkeästi erotettu toisistaan tietojen, taitojen ja osaamisen tasoilla.

Jokainen 3 ECTS-opintopisteen moduuli on kehitetty eri konsortiokumppaneiden toimesta, jotka ovat hyödyntäneet omaa erityisalaansa ja ammatillista kokemustaan.

Kehitettyjen moduulien aiheet ovat seuraavat, jotka on tunnistettu D2.2-raportissa kriittisen tärkeiksi:



1. M1: TURVALLISUUSOHJELMAN HALLINTA

Moduulin nimi	Moduulin koodi
TURVALLISUUSOHJELMAN HALLINTA	

Luennoitsija(t)	Laitos tai osasto, jossa moduuli opetetaan

Opetustapa	Kieli
Lähde:	*Englanti, suomi, turkki, norja, liettua, romania, ranska, puola, espanja*

Edellytykset
Ei mitään

Myönnettyjen ECTS-opintopisteiden määrä	Opiskelijan työmäärä	Yhteistyötyöskentely	Itsenäinen opiskelu
3	75 tuntia	50 tuntia	25 tuntia

Moduulin tarkoitus ja tulokset

Kurssin suoritettuaan opiskelijat hallitsevat taidot, joita tarvitaan tietoturvaohjelmien tehokkaaseen hallintaan kyberturvallisuusuhkien varalta. He kehittävät puolustusstrategioita nykyisiä uhkia, kuten tietojenkalastelua, kiristysohjelmia ja DDoS-hyökkäyksiä vastaan, projektin- ja resurssienhallinnan puitteissa. Lisäksi opiskelijat oppivat soveltamaan turvallisuusmittareita ja laadunvarmistusmenetelmiä, jolloin he saavat kyvyn optimoida turvallisuusohjelmia, hallita resursseja tehokkaasti ja parantaa organisaation turvallisuutta hyödyntämällä sopivia työkaluja kehittyviä uhkia vastaan. Kurssi kehittää myös opiskelijoiden osaamista uhkien arvioinnissa, raportoinnissa ja viestinnässä, jolloin he voivat toteuttaa kyberturvallisuusstrategioita tehokkaasti omissa organisaatioissaan.

Moduulin oppimistulokset	Opetus- ja oppimismenetelmät	Arviointimenetelmät
Tieto: Opiskelijat saavat käytännön tietoa uusimmista kyberturvallisuusuhkista, kuten tietojenkalastelusta, kiristysohjelmista ja DDoS-hyökkäyksistä, sekä siitä, miten näitä hallitaan tehokkaalla projekti- ja resurssienhallinnalla sekä laadunvarmistus- ja valvontatoimenpiteiden toteuttamisella.	Valitaan luennoitsijan toimesta osasta 1.3. [Opetusmenetelmät, esim. teoreettiset luennot, vierailevat luennoitsijat, tietokilpailut, pelit, käytännön tehtävät/laboratoriot, vertaisopetus ja -oppiminen, itseohjattu oppiminen jne.	Itsearviointikokeet Tietotesti

Taidot: Oppijat osaavat käyttää työkaluja ja ohjelmistoja suojautuakseen kehittyviä kyberuhkia vastaan ja soveltaa vankkoja turvallisuuskäytäntöjä projektien ja resurssien hallinnassa parantaakseen organisaatioidensa yleisiä turvallisuusmittareita ja laadunvalvontaa.	Valitaan luennoitsijan toimesta osasta 1.3. [Opetusmenetelmät, esim. käytännön tehtävät/laboratoriot, käytännön harjoitukset, simuloituja ympäristöjä, tietokilpailut, pelit, tapaustutkimukset jne.	Käytännön arvioinnit
Osaaminen: Oppijat osaavat arvioida ja lieventää potentiaalisia turvallisuusuhkia, kommunikoida tehokkaasti kyberturvallisuusasioista ja raportoida tarkasti uhkista ja rikkomuksista organisaationsa asianmukaisten kanavien kautta.	Valitsee opettaja osasta 1.3. [Opetusmenetelmät, esim. simuloituja ympäristöjä, Capture the Flag -kilpailut, 5E, CBL, CL, POGIL, PBL jne.] D2.3:sta ”Pk-yritysten kyberturvallisuuden muutosagenttien oppimispolun rakenne”	Simulaatiot Kilpailut

Moduulin sisältö: aiheiden jaottelu	**Yhteistyötyöskentely**					**Yksilölliset työajat ja tehtävät**	
	Luennot	Konsultaatiot	Harjoitukset	Kokeet	**Kaikki**	**Yksilöllinen työ**	**Tehtävät**
Projektinhallinta • Projektisuunnittelu • Projektin tavoitteiden määrittely • Projektin laajuuden ja vaatimusten määrittäminen • Projektiaikataulun laatiminen • Projektinhallintatyökalut • Nykyiset kyberturvallisuusuhkat (DDoS, kiristysohjelmat, haittaohjelmat, tieto-jenkalastelu, nollapäivähyökkäykset, IoT-hyökkäykset jne.) • Uhkamallinnus ja haavoittuvuusanalyysi • Hätä- ja tapahtumien vaste-suunnitelmat • Kyberturvallisuusuhkien ja -tapahtumien raportointi	8	0,5	3	0,5	**12**	**6**	• Suunnittele kyberturvallisuustietoisuutta edistävä projekti pk-yritysten työntekijöille. • Määritä selkeät tavoitteet kyberturvallisuustietoisuuden lisäämishankkeelle, jotta pk-yritysten työntekijät ymmärtävät paremmin mahdollisia turvallisuusuhkia. • Määritä pk-yritysten työntekijöille suunnatun kyberturvallisuustietoisuuden lisäämiseen tähtäävän hankkeen laajuus ja vaatimukset, mukaan

							lukien koulutuksen aiheet ja tarvittavat resurssit. • Laadi aikataulu pk-yritysten työntekijöille suunnatulle kyberturvallisuustietoisuuden lisäämishankkeelle. • Käytä projektinhallintatyökaluja seurata pk-yritysten työntekijöille suunnatun kyberturvallisuustietoisuuden lisäämiseen tähtäävän projektin etenemistä ja resurssien käyttö • Tutki nykyisiä kyberturvallisuusuhkia ja koosta tulokset raportiksi. • Luo yksinkertaistettu uhkamalli, jonka avulla pk-yritysten työntekijät voivat tunnistaa mahdolliset tietoturvahaavoittuvuudet päivittäisessä toiminnassaan. • Etsi ja tarkastele esimerkkejä hätä- ja tapahtumien vasteohjelmista. • Mitä vaiheita tulisi ottaa huomioon, kun laaditaan raportti kyberturvallisuusuhkien ja -tapauksien raportoinnista? Tutki ja tee yhteenveto.
Resurssien hallinta • Henkilöstöhallinto (projektitiimit) • Tietoturvatietoisuus ja tiimikoulutus • Laitteisto- ja ohjelmistojen inventoinnin hallinta • Turvallisuustyökalut ja -ohjelmistot • Teknologisten resurssien tehokas käyttö • Budjetin ja resurssien kohdentaminen	8	0,5	3	0,5	**12**	**6**	• Suunnittele resurssienhallintastrategia, jolla varmistetaan resurssien tehokas käyttö kuvitteelliselle pk-yritykselle. • Laadi esimerkkiaihepiirros kyberturvallisuustietoisuuden koulutusta varten. • Laadi laitteisto- ja ohjelmistoluettelo kuvitteelliselle pk-yritykselle.

							• Tutki yleisesti käytettyjä tietoturvatyökaluja ja -ohjelmistoja. • Laadi mallibudjetti ja resurssien kohdentamissuunnitelma kuvitteelliselle pk-yritykselle.
Turvallisuusmittarit • Turvallisuusmittarit ja mittaustekniikat • Tietojen kerääminen SIEM-järjestelmällä • Turvallisuusmittareiden analysointi • Projektin seuranta ja suorituskyvyn arviointi • Toimenpiteiden tarkastelu ja projektin mukauttaminen • Turvallisuusmittareiden raportointi	8	0,5	4	0,5	**13**	**6**	• Tutki turvallisuusmittareita, joita käytetään pk-yritysten kyberturvallisuuden arviointiin. • Tutki lähteitä, joista SIEM-ohjelmisto kerää lokitietoja. • Asenna ja tutki avoimen lähdekoodin SIEM-ohjelmisto. • Analysoi turvallisuusmittareita keräämällä lokit SIEM-ohjelmistolla. • Raportoi turvallisuusmittareiden analyysitulokset kaavioiden ja kuvien avulla.
Laadunvarmistus ja laadunvalvonta • Laadunhallinta • Tietoturvan laatustandardit • Vaatimustenmukaisuus ja laatuauditoinnit • Testaus- ja validointitekniikat • Arviointi ja parannusehdotukset	8	0,5	4	0,5	**13**	**7**	• Miten laadunvarmistus- ja laadunvalvontaprosessit tulisi suunnitella, jotta pk-yritysten kyberturvallisuussovellusten tehokkuutta voitaisiin parantaa? Tutki ja tee yhteenveto. • Tutki ISO/IEC 27001:2022 -standardin liitteen A valvontakohdat. • Tutki ja raportoi, mitä testaus- ja validointitekniikat ovat. • Mitä etuja jatkuva laadunprosessien tarkastelu ja parantaminen tarjoaa pk-yrityksille?
Yhteensä	**32**	**2**	**14**	**2**	**50**	**25**	

Arviointistrategia	**Vertaileva painoprosentti**	**Arviointikriteerit**
Itsearviointitesti I	10	10 pistettä – 96–100 % oikeita vastauksia.

Itsearviointitesti II	10	9 pistettä – 91–95 % oikeita vastauksia. 8 pistettä – 86–90 % oikeita vastauksia. 7 pistettä – 80–85 % oikeita vastauksia. 6 pistettä – 70–79 % oikeita vastauksia. 5 pistettä – 60–69 % oikeita vastauksia. 4 pistettä – 50–59 % oikeita vastauksia. 3 pistettä – 40–49 % oikeita vastauksia. 2 pistettä – 30–39 % oikeita vastauksia. 1 piste – 0–29 % oikeita vastauksia.
Itsearviointitesti III	10	
Itsearviointitesti IV	10	
Tietotesti	60	

Opiskelumateriaali *(Sukunimi, etunimen alkukirjain. (Vuosi, kuukausi, päivä). Artikkelin nimi. Lehden/aikakauslehden/sanomalehden nimi, vuosikerta (numero), koko artikkelin sivunumerot, kustantaja, URL)*
Pakollinen kirjallisuus
Suositeltava kirjallisuus
https://sansorg.egnyte.com/dl/RFrVIbX2oc https://edwps.com/wp-content/uploads/2018/04/Cyber-PMO-U.S.-Cyber-Magazine.pdf https://healthybyte.net/cybersecurity/what-is-a-security-program-management

2. M2: JÄRJESTELMÄNHALLINTA

Moduulin nimi	Moduulin koodi
JÄRJESTELMIEN YLLÄPITO	

Luennoitsija(t)	Laitos tai osasto, jossa moduuli opetetaan

Opetustapa	Kieli
Lähdeopetus, verkko-opetus, yhdistetty opetus	*Englanti, suomi, turkki, norja, liettua, romania, ranska, puola, espanja*

Edellytykset
Ei mitään

Myönnettyjen ECTS-opintopisteiden määrä	Opiskelijan työmäärä	Yhteistyötyöskentely	Itsenäinen opiskelu
3	75	50	25

Moduulin tarkoitus ja tulokset

Kurssin suoritettuaan opiskelijat osaavat hallita (tunnistaa, analysoida, arvioida, arvioida, lieventää) jatkuvasti ICT-infrastruktuurien, järjestelmien ja palveluiden kyberturvallisuuteen liittyviä riskejä suunnittelemalla, soveltamalla, raportoimalla ja viestimällä riskianalyysejä, arviointeja ja käsittelyjä. Opiskelijat oppivat verkkojen perusteet, jotta he voivat hallita verkkolaitteita asianmukaisesti ja käyttää sekä Linux- että Windows-palvelimia hallinnoiden ja suojaten niitä. Myös tietoturvan kontekstissa tarvittava tieto pilvipalveluista ja tekoälystä on heille erittäin hyödyllistä, jotta he voivat nopeuttaa tehtäviä ja suorittaa automaatioita ja skaalausta asianmukaisesti. Opiskelijat oppivat myös vahvistamaan järjestelmiä, etsimään uhkia ja varmistamaan palvelimien saatavuuden (lyhenne CIA-kolmiosta).

Moduulin oppimistulokset	Opetus- ja oppimismenetelmät	Arviointimenetelmät
Tieto: Opiskelijat saavat tietoa verkkojen hallinnasta, käyttöjärjestelmistä, verkkojen perusteista, verkkojen hallintatyökaluista, verkkolaitteiden turvallisuudesta, Linux-järjestelmien hallinnasta, Windows-järjestelmien hallinnasta, virtualisoinnista, pilvipalveluista, tekoälyn käytöstä verkko- ja kyberturvallisuusmenettelyissä, kyberturvallisuusmenettelyistä, uhkien havaitsemisesta, uhkien analysoinnista, uhkien torjunnasta, uhkien korjaamisesta, kyberturvallisuuden perusteista, organisaation puolustamisesta hyökkäyksiä vastaan, infrastruktuurin ja verkon turvallisuudesta, verkon seurannasta ja analysoinnista sekä poikkeustilanteiden käsittelystä. He osaavat luoda ja kuvata tehokkaita järjestelmänhallintamenettelyjä ja toimintarutiineja, jotka on räätälöity pk-yritysten työpaikkojen erityistarpeisiin ja vaatimustenmukaisuusstandardeihin.	Luennoitsijan valitsemat menetelmät: live-luennot, videotallenteet, esitykset, virtuaaliset laitteet (tarvittaessa), kirjallisuuden analysointi, vierailevat luennoitsijat, vertaisopetus ja -oppiminen, mentorointi.	Itsearviointitestit ja tietojen arviointitestit
Taidot: Opiskelijat osaavat käyttää menetelmiä ja työkaluja turvallisten järjestelmäarkkitehtuurien suunnitteluun ja toteuttamiseen, mukaan lukien käyttöjärjestelmät, tietokannat, verkot ja pilvi-infrastruktuurit pk-yritysten työpaikoille.	Luennoitsijan valitsemat menetelmät: live-luennot, videotallenteet, esitykset, virtuaaliset laitteet (tarvittaessa), kirjallisuuden analysointi, vierailevat luennoitsijat, vertaisopetus ja -oppiminen, mentorointi.	Itsearviointitestit ja tietojen arviointitestit

Osaaminen: Opiskelijat osaavat kehittää ja toteuttaa strategisia kyberturvallisuuskehyksiä järjestelmänhallintaan, johtaa projekteja ja tiimejä järjestelmien vahvistamiseksi ja käytettävyyden parantamiseksi sekä tehdä eettisiä päätöksiä vahvojen kyberturvallisuuskäytäntöjen ylläpitämiseksi eri hallinnollisilla aloilla pk-yritysten työpaikoilla.	Luennoitsijan valitsemat menetelmät: lähiopetus, videotallenteet, esitykset, virtuaaliset laitteet (tarvittaessa), kirjallisuuden analysointi, vierailevat luennoitsijat, vertaisopetus ja -oppiminen, mentorointi.	Itsearviointitestit ja tietojen arviointitestit

Moduulin sisältö: aiheiden jakautuminen	**Yhteistyötyöskentelyt unnit**					**Yksilölliset työajat ja tehtävät**	
	Luennot	Konsultaatiot	Harjoitukset	Kokeet	**Kaikki**	**Yksilöllinen työ**	**Tehtävät**
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 komento-syntaksi	4	0,5	2	0,5	**7**	**3,5**	Heksadesimaalilaskenta Windows-komentojen harjoittelu Linux-komentojen harjoittelu Tehtävienhallinnan harjoittelu Tiedostojen luominen ja hallinta Rekisteriavaimien ja -arvojen muokkaaminen ja tarkastelu Ohjauspaneelin asetusten muokkaaminen Käyttäjien ja ryhmien hallinta Verkkotunnuksen rakenteen hallinta Active Directory -objektien luominen ja poistaminen Prosessien hallinta Linuxissa Tiedostojen ja kansioiden käsittely

• Tiedostojen ja kansioiden käsittely • Putkien ja järjestelmänvalvon-takomentojen käyttö • Prosessien hallinta ja tehtävien ohjaus • Palvelujen hallinta							Pipe-komennon käyttö Järjestelmän valvontakomennot Linux-palveluiden hallinta
Tietokantajärjestelmän hallinta • Tallennustilat ja lähdeluettelot • Verkkopalvelimen hallinta • Järjestelmälokit ja lokien valvonta • 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 proto-kollat • Verkkotunnusjärjestelmäproto-kolla (DNS) • FTP ja RDP • Kapselointi vs. dekapsulointi • Verkkosnifferit ja Wireshark • TCP/UDP • DHCP, DNS	4	0,5	2	0,5	**7**	**3,5**	Tietovarastojen ja lähdeluetteloiden hallinta Verkkopalvelimen hallinta Järjestelmälokien tarkistaminen ja hallinta sekä lokien seuranta Tehtävien ajoittaminen Linuxissa Palvelimen vianmääritys Varmuuskopioiden palauttaminen GRUB:n suojaaminen Tietokantapalvelujen hallinta Salasanakäytäntöjen määrittäminen Tilin lukituskäytäntöjen määrittäminen Todennuksen ja pääsyn hallinnan määrittäminen
Verkon hallinta • Verkkotyypit ja langattomat verkot • Verkot ja topologiat • Laitteet Tunnistautuminen ja pääsy Laitteet • Infrastruktuuri ja turvalaitteet • Erikoistuneet laitteet ja verkkoark-kitehtuuri • Virtuaaliset verkot	4	0,5	2	0,5	**7**	**3,5**	Verkkotopologioiden luominen Verkkolaitteiden hallinta Verkon rakentaminen Verkkolaitteiden suojaaminen Virtuaalisten verkkojen luominen

• 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 käännös (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							Verkkoprotokollien ja porttinumeroiden määrittäminen Cisco Packet Tracerin käyttö Address Resolution Protocol (ARP) -protokollan käyttö Verkon suunnittelu Staattisen ja dynaamisen IP-osoitteistuksen määrittäminen DHCP:n ja NAT:n määrittäminen Cisco IOS:n käyttö VLAN-verkkojen määrittäminen Verkon vianmääritys
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 • Tunnistuksen ja pääsyn hallinta (IAM) • Roolipohjainen pääsynhallinta (RBAC) • Monivaiheinen todennus (MFA) • Pilvipalvelujen tietojen salaus • Virtuaalinen yksityinen pilvi (VPC) • Docker ja Kubernetes	4	0,5	2	0,5	**7**	**3,5**	Virtuaalikoneiden luominen Konttien määrittäminen Virtuaaliympäristöjen suojaaminen Varmuuskopioiden käsittely Pilvipohjaisen verkon hallinta Virtuaalisten verkkojen määrittäminen Pilvipohjaisten valvontatyökalujen käyttö Automaation ja orkestroinnin toteuttaminen Pilvipalvelujen tietoturvauhkien ja haavoittuvuuksien havaitseminen Identiteetin ja pääsyn hallinnan (IAM) määrittäminen Pilvipalvelujen tietojen salauksen käyttöönotto Työskentely Docker- ja Kubernetes-ohjelmistojen kanssa
Kyberfysikaalisten järjestelmien hallinta • Turvallisuus ja pääsyn hallinta	4	0,5	2	0,5	**7**	**3,5**	Infrastruktuurin pääkomponenttien määrittäminen

• Todentamistyypit • TACACS+ ja RADIUS • AAA-määritykset • 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							Turvallisuusvalvonnan toteuttaminen TACACS+:n ja RADIUS:n käyttö AAA-määritykset Salauksen ja salauksen purkamisen kokeilu Yleisten hyökkäysten ja puolustustekniikoiden analysointi Demilitarisoitujen vyöhykkeiden (DMZ) määrittäminen Honeypot-tutkimus Turvallisen verkon vahvistaminen parhaiden käytäntöjen avulla VPN:n asentaminen Työskentely Secure Shellin (SSH) kanssa Virtual Network Computing (VNC) -ohjelmiston käyttö Palomuurin toimintatekniikat Tekoälyn käyttöönotto palomuureissa Snortin ja tcpdumpin käyttö suojaukseen ja havaitsemiseen
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 • IT-omaisuuden hallinta ja inventointi • Poistettujen tiedostojen palauttaminen GenAI:n avulla • Kyberturvallisuusmenettelyt	4	0,5	2	0,5	**7**	**3,5**	GenAI-tekniikoiden käyttö Käyttäjätilien hallinta ja pääsynvalvonta Poikkeavuuksien havaitseminen ja vianmääritys Apache2-palvelun virheiden ratkaiseminen GenAI:n avulla Päivitysten ja korjaustiedostojen hallinnan määrittäminen Automaattisen varmuuskopioinnin ja palautuksen määrittäminen IT-resurssien hallinta

• Uhkien havaitseminen ja analysointi • Uhkiin reagointi ja korjaaminen • Tekoälyn hyödyntäminen reaaliaikaisessa uhkien havaitsemisessa • GenAI-mallien validointi ja testaus • Hallinto- ja sääntelykehykset • 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							Poistettujen tiedostojen palauttaminen GenAI:n avulla DNS- ja DHCP-turvallisuuden käyttöönotto Microsoft BitLocker- ja Microsoft AppLocker -ohjelmien käyttö Microsoftin palomuurin määrittäminen Switch-portin suojauksen määrittäminen Tiedostonsiirtoprotokollan (FTP) suojaaminen Etätyöpöytäprotokollan (RDP) suojaaminen Turvatehtävien ajoittaminen Linuxissa GRUB:n suojaaminen Palomuurien (iptables) määrittäminen ja suojaaminen
Saatavuus • 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 • LDAP-tiedustelu • Rikkoutunut pääsynvalvonta • Lunnasohjelmat • Tietokonevirus ja mato • Troijalainen ja mainosohjelma • Keyloggerit ja kryptokaappaus • Tiedostoton haittaohjelma	4	0,5	3	0,5	**8**	4	Tapahtumien ja häiriöiden havaitseminen Hälytysten luokittelu Dokumentointi ja asianmukainen raportointi Tapahtuman jälkeisten toimien toteuttaminen DoS- ja DDoS-hyökkäysten suorittaminen ja niiltä suojautuminen Verkkohyökkäysten ja haittaohjelmien leviämisen havaitseminen Turvallisen staattisen ja dynaamisen haittaohjelman analysoinnin suorittaminen IOC:iden hallinta Salasanakäytäntöjen määrittäminen

• Haittaohjelmien leviämisen ymmärtäminen • Staattinen ja dynaaminen haittaohjelmien analysointi • Turvallinen haittaohjelmien analysointi • Hybridianalyysi Haittaohjelmien tutkinta • Staattisen ja dynaamisen haittaohjelman analysoinnin suorittaminen • IOC- ja salasanakäytäntöjen hallinta • Hyväksyttävän käytön käytännöt (AUP) • Oman laitteen käyttö (BYOD) -käytännöt • Etäkäyttökäytännöt							Oman laitteen käyttöä (BYOD) koskevien käytäntöjen määrittäminen Etäkäyttökäytäntöjen määrittäminen
Yhteensä	**28**	**3,5**	**15**	**3,5**	**50**	**25**	

Arviointistrategia	**Vertaileva painoprosentti**	**Arviointikriteerit**
Itsearviointitesti (1)	5 %	10 pistettä – 90–100 % oikeita vastauksia. 9 pistettä – 80–90 % oikeita vastauksia. 8 pistettä – 70–80 % oikeita vastauksia. 7 pistettä – 60–70 % oikeita vastauksia. 6 pistettä – 50–60 % oikeita vastauksia. 5 pistettä – 50–60 % oikeita vastauksia. 4 pistettä – 40–50 % oikeita vastauksia. 3 pistettä – 30–40 % oikeita vastauksia. 2 pistettä – 20–30 % oikeita vastauksia. 1 piste – 10–20 % oikeita vastauksia.
Itsearviointitesti (2)	5 %	
Itsearviointitesti (3)	5 %	
Itsearviointitesti (4)	5	
Itsearviointitesti (5)	5	
Itsearviointitesti (6)	5	
Itsearviointitesti (7)	5	
Tietojen arviointitesti	65 %	

3. M3: ANALYYTTISET TYÖKALUT

Moduulin nimi	**Moduulin koodi**
ANALYYTTISET TYÖKALUT	

Luennoitsija(t)	**Laitos tai osasto, jossa moduuli järjestetään**

Opetustapa	**Kieli**

Lähdeopetus, verkko-opetus, hybridi	*Englanti, suomi, turkki, norja, liettua, romania, ranska, puola, espanja*

Edellytykset
Ei mitään

Myönnettyjen ECTS-opintopisteiden määrä	**Opiskelijan työmäärä**	**Yhteistyötyöskentely**	**Itsenäinen opiskelu**
3	75	50	25

Moduulin tarkoitus ja tulokset		
Kurssin suoritettuaan opiskelijat hallitsevat taidot, joiden avulla he voivat suojata organisaation omaisuutta suorituskykymittareiden, data-analytiikan ja tietoturvatiedustelun avulla. He oppivat soveltamaan analyyttisiä työkaluja tehokkaasti potentiaalisten kyberturvallisuusriskien ja haavoittuvuuksien tunnistamiseen, hyödyntämään datapohjaisia oivalluksia turvallisuustoimenpiteiden parantamiseen sekä käyttämään salasanoihin, selaimen käyttöön, sähköpostiin ja tietojenkäsittelysovelluksiin liittyviä suorituskykymittareita. Moduulin lopussa osallistujat osaavat arvioida ja lieventää mahdollisia tietoturvauhkia käyttämällä sopivia työkaluja ja ilmoittaa uhista tai häiriöistä oikeille sääntelyviranomaisille.		
Moduulin oppimistulokset	**Opetus- ja oppimismenetelmät**	**Arviointimenetelmät**
Tieto: Opiskelijat saavat käytännön tietoa suorituskykymittareiden, data-analytiikan ja tietoturvatietojen soveltamisesta organisaation omaisuuden suojaamiseen.	Valitaan luennoitsijan toimesta osasta 1.3. [Opetusmenetelmät, esim. teoreettiset luennot, vierailevat luennoitsijat, tietokilpailut, pelit, käytännön tehtävät/laboratoriot, vertaisopetus ja -oppiminen, itseohjattu oppiminen jne.	Itsearviointikokeet Tietojen arviointitesti
Taidot: Oppijat osaavat käyttää analyyttisiä työkaluja potentiaalisten kyberturvallisuusriskien ja haavoittuvuuksien tunnistamiseen, soveltaa datapohjaisia oivalluksia kyberturvallisuuskäytäntöjen vahvistamiseen ja hyödyntää suorituskykymittareita salasanojen, selaamisen, sähköpostin ja tietojen käsittelyn turvallisuuden arvioimiseen ja parantamiseen.	Valitaan luennoitsijan toimesta osasta 1.3. [Opetusmenetelmät, esim. käytännön tehtävät/laboratoriot, käytännön harjoitukset, simuloituja ympäristöjä, tietokilpailut, pelit, tapaustutkimukset jne.	Käytännön arvioinnit
Osaaminen: Oppijat osaavat arvioida ja lieventää potentiaalisia turvallisuusuhkia analyyttisten työkalujen avulla sekä raportoida uhat ja	Luennoitsijan valitsemat, osasta 1.3. [Opetusmenetelmät, esim. simuloituja ympäristöjä, Capture the Flag -kilpailut, 5E, CBL, CL, POGIL, PBL jne.	Simulaatiot Kilpailut

rikkomukset tarkasti organisaationsa asianmukaisille tahoille.		

Moduulin sisältö: aiheiden jaottelu	**Yhteistyötyöskentely**					**Yksilölliset työajat ja tehtävät**	
	Luennot (korkeakoulu)	Konsultaatiot	Harjoitukset (korkeakoulu)	Kokeet	**Kaikki kontaktiopetu**	**Yksilöllinen työ**	**Tehtävät**
Suorituskyvyn mittaaminen (mittarit) • Suorituskykymittarit • Järjestelmän ja verkon valvonta • Suorituskykymittareiden valvonta • Verkon kartoitus • Haavoittuvuuksien skannaus • Verkkoliikenteen analysointi	10	0,5	5	0,5	**16**	**8,5**	• Tutki suorituskykymittareita ja -työkaluja. Vertaa suorituskyvyn seurantatyökaluja ja tunnista niiden erot. • Suorita Zabbix-asennus ja tee perusasetukset. • Luo sovellus suorituskykymittareiden seurantaan Zabbixilla. • Tunnista kohdejärjestelmän haavoittuvuudet verkkokartoitusohjelmiston (kuten nmap, rustscan jne.) avulla. • Suorita haavoittuvuustarkistus kohdejärjestelmässä Nessus-ohjelmiston avulla. Laadi haavoittuvuustestausraportti. Suorita verkkoliikenteen analyysi Wireshark-ohjelmiston avulla. • Suorita verkkoliikenteen analyysi Wireshark-ohjelmistolla.
Tietojen analysointi • Tietojen kerääminen • Tietojen puhdistus ja esikäsittely • Tietojen analysointi • Tietojen visualisointi • Analyyttiset työkalut • Tietoturvassa käytettävät data-analyysit	10	0,5	5	0,5	**16**	**8,5**	• Suorita tietojen puhdistus ja esikäsittely vaiheet tietoturvaongelmiin liittyvässä tietojoukossa, joka on valmistettu hypoteettiselle pk-yritykselle. • Analysoi puhdistettu ja esikäsitelty tietojoukko hypoteettisesta pk-yrityksestä ja visualisoi tulokset.

							• Mitä esimerkkejä tietoturva-alan data-analyysisovelluksista on? Tutki asiaa.
Turvallisuustiedustelu • Turvallisuustiedustelun ymmärtäminen • Turvallisuustiedustelun lähteet • Uhkatiedustelun keräämisen menetelmät • Uhkatiedustelun viitekehykset • Tekoälypohjaiset turvallisuustiedustelualustat • Turvallisuustiedustelun sovellusten tapaustutkimukset	10	0,5	7	0,5	**18**	**8**	• Tutki, miten turvallisuustiedustelu edistää pk-yritysten ennakoivia turvallisuusstrategioita. • Mitkä ovat yleisimmät turvallisuustiedon hankintalähteet? Miten arvioit näiden lähteiden luotettavuutta? • Määritä kunkin uhkatietojen keräämisen menetelmän edut ja rajoitukset. • Selitä uhkatietojen keräämisen viitekehysten, kuten MITRE ATT&CK ja Cyber Kill Chain, keskeiset piirteet. • Tutki todellinen tapaustutkimus, jossa turvallisuustietoja on hyödynnetty. Kuvaile kyseisessä tapaustutkimuksessa käytettyjä tietojenkerumenetelmiä.
Yhteensä	**30**	**1,5**	**17**	**1,5**	**50**	**25**	

Arviointistrategia	Vertaileva painoprosentti	Arviointikriteerit
Itsearviointitesti I	15	10 pistettä – 96–100 % oikeita vastauksia. 9 pistettä – 91–95 % oikeita vastauksia. 8 pistettä – 86–90 % oikeita vastauksia. 7 pistettä – 80–85 % oikeita vastauksia. 6 pistettä – 70–79 % oikeita vastauksia. 5 pistettä – 60–69 % oikeita vastauksia. 4 pistettä – 50–59 % oikeita vastauksia. 3 pistettä – 40–49 % oikeita vastauksia. 2 pistettä – 30–39 % oikeita vastauksia. 1 piste – 0–29 % oikeita vastauksia.
Itsearviointitesti II	15	
Itsearviointitesti III	15	
Tietotesti	55	

Tutkimusmateriaali *(Sukunimi, etunimen alkukirjain. (Vuosi, kuukausi, päivä). Artikkelin nimi. Lehden/aikakauslehden/sanomalehden nimi, vuosikerta (numero), koko artikkelin sivunumerot, kustantaja, URL)*
Pakollinen kirjallisuus
…
Suositeltava kirjallisuus
https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use **https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it** **https://medium.com/@jcm3/wireshark-traffic-analysis-part-1-tryhackme-walkthrough-a9bec11d94d9** **https://www.kali.org/tools/nmap/** **https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/** **https://www.varonis.com/blog/cyber-kill-chain** **https://www.youtube.com/watch?v=kVnvIBNiC58**

4. M4: TURVALLISUUSTOIMINNOT

Moduulin nimi	Moduulin koodi
TURVALLISUUSTOIMINNOT	

Luennoitsija(t)	Laitos tai osasto, jossa moduuli opetetaan

Opetustapa	Kieli
Lähdeopetus, verkko-opetus, yhdistetty opetus, konsultaatiot	*Englanti, suomi, turkki, norja, liettua, romania, ranska, puola, espanja*

Edellytykset
Ei mitään

Myönnettyjen ECTS-opintopisteiden määrä	Opiskelijan työmäärä ( )	Yhteistyötyöskentely	Itsenäinen opiskelu
3	75	50	25

Moduulin tarkoitus ja tulokset		
Kurssin suoritettuaan opiskelijat osaavat hallita tehokkaasti tietotekniikan infrastruktuurien, järjestelmien ja palveluiden tietoturvaoperaatioita. He oppivat seuraamaan, havaitsemaan, reagoimaan ja palautumaan kyberturvallisuusuhkiin soveltamalla tietoturvaoperaatioihin liittyviä parhaita käytäntöjä, työkaluja ja viitekehyksiä.		
Moduulin oppimistulokset	**Opetus- ja oppimismenetelmät**	**Arviointimenetelmät**
Tieto: Opiskelijat saavat syvällistä tietoa turvallisuustoiminnoista, mukaan lukien seuranta, havaitseminen, tapahtumiin reagointi ja palautuminen. He osaavat luoda ja kuvata tehokkaita kyberturvallisuuden toimintarutiineja, jotka on räätälöity pk-yritysten työpaikkojen erityistarpeisiin kyberturvallisuusstandardien mukaisesti.	Valitaan luennoitsijan toimesta osasta 1.3. [Opetusmenetelmät, esim. teoreettiset luennot, kirjallisuusanalyysi, vierailevat luennoitsijat, vertaisopetus ja -oppiminen, mentorointi jne.	Itsearviointitestit Tietojen arviointitesti

Taidot: Opiskelijat osaavat soveltaa edistyneitä menetelmiä ja työkaluja tietoturvatehtävien suorittamiseen, suunnitella ja toteuttaa tehokkaita seurantastrategioita, vastata tietoturvaloukkauksiin ja kehittää vakaita toimintarutiineja, jotka on räätälöity erityisesti pk-yritysten työpaikoille.	Valitaan luennoitsijan toimesta osasta 1.3. [*Opetusmenetelmät, esim. teoreettiset luennot, kirjallisuusanalyysi, vierailevat luennoitsijat, vertaisopetus ja -oppiminen, mentorointi jne.]* D2.3:sta *"Pk-yritysten kyberturvallisuuden muutosagenttien oppimispolun* rakenne"	Itsearviointitestit Tietojen arviointitesti
Osaaminen: Opiskelijat osaavat kehittää ja toteuttaa strategisia tietoturvatoimia ja -menettelyjä pk-yritysten työpaikoille.	Valitaan luennoitsijan toimesta osasta 1.3. [*Opetusmenetelmät, esim. teoreettiset luennot, kirjallisuusanalyysi, vierailevat luennoitsijat, vertaisopetus ja -oppiminen, mentorointi jne.]* kohdasta D2.3 *"Pk-yritysten kyberturvallisuuden muutosagenttien oppimispolun rakenne*".	Itsearviointitestit Tietojen arviointitesti

Moduulin sisältö: aiheiden jaottelu	**Yhteistyötyöskentelytunnit**					**Yksilölliset työajat ja tehtävät**	
	Luennot	Konsultaatiot	Harjoitukset (työpaja/koulu)	Kokeet	Kaikki	Yksilöllinen työ	Tehtävät
Turvallisuusoperaatioiden perusteet - Turvallisuusoperaatioiden ja SOC:n (turvallisuusoperaatiokeskus) ymmärtäminen - Turvallisuusoperaatioiden roolit ja vastuut - Yleiskatsaus turvallisuusoperaatioiden työkaluihin ja tekniikoihin	6	0,5	2	0,5	**9**	6	Tunnistaa ja ymmärtää SOC:n rakenteen ja toiminnan, analysoida erilaisia rooleja tietoturvatoiminnassa, tutkia tietoturvatoiminnassa käytettyjä työkaluja ja analysoida tapaustutkimus.

Turvallisuuden konvergenssi - Turvallisuuden konvergenssin ymmärtäminen - Fyysisen turvallisuuden perusteet (fyysisen turvallisuuden periaatteet, fyysisten omaisuuserien suojelu, toimintaperiaatteet) - Tapausesimerkki, jossa korostetaan turvallisuuden konvergenssin periaatteita	8	0,5	4	0,5	**13**	6	Tarkastele turvallisuuden lähentymisen määritelmää ja periaatteita, tunnusta fyysisen ja digitaalisen turvallisuuden toimintojen integroinnin merkitys, tunnista ja arvioi riskejä kyber- ja fyysisillä alueilla.
Turvallisuustietojen ja tapahtumien hallinta - Turvallisuuden seurannan periaatteiden tarkastelu - SIEM-ratkaisujen käyttöönotto	8	0,5	4	0,5	**13**	6	Johdanto turvallisuuden seurantaan ja SIEM-toteutukseen. Perusperiaatteet, kuten lokityypit, havaitsemismenetelmät ja seurannan elinkaari. SIEM-järjestelmän käyttöönoton käytännön näkökohdat, mukaan lukien arkkitehtuuri, tiedonkeruu, sääntöjen luominen ja hälytysten hallinta.

Turvallisuusoperaatioiden käytännöt - Tunnista tietolähteet ja optimoi lokien kerääminen - Hälytysten keskittäminen SIEM:n avulla - SIEM-järjestelmän testaaminen	4	0,5	10	0,5	**15**	7	Kattava ja käytännönläheinen koulutusohjelma, joka tarjoaa olennaista tietoa ja käytännön taitoja lokien hallinnasta, SIEM-konfiguroinnista ja uhkien havaitsemisesta erilaisissa IT-ympäristöissä.
Yhteensä	**26**	**2**	**20**	**2**	**50**	**25**	

Arviointistrategia	**Vertaileva painoprosentti**	**Arviointikriteerit**
Itsearviointitesti (1)	10 %	10 pistettä – 96–100 % oikeita vastauksia. 9 pistettä – 91–95 % oikeita vastauksia. 8 pistettä – 86–90 % oikeita vastauksia. 7 pistettä – 80–85 % oikeita vastauksia. 6 pistettä – 70–79 % oikeita vastauksia. 5 pistettä – 60–69 % oikeita vastauksia. 4 pistettä – 50–59 % oikeita vastauksia. 3 pistettä – 40–49 % oikeita vastauksia. 2 pistettä – 30–39 % oikeita vastauksia. 1 piste – 0–29 % oikeita vastauksia.
Itsearviointitesti (2)	10 %	
Itsearviointitesti (3)	10 %	
Itsearviointitesti (4)	10	
Tietojen arviointitesti	60 %	
HEI/VET-sertifiointi -> Itsearviointitesti I + ...+ Itsearviointitesti n + Tietojen arviointitesti		
Pk-yritykset/itseopiskelu -> Itsearviointi I + ...+ Itsearviointi n + Tietojen arviointitesti		
Mikromoduulit, mikro-osio -> Itsearviointi I (valinnainen), Itsearviointi n (valinnainen)		

Opiskelumateriaali *(Sukunimi, etunimen alkukirjain. (Vuosi, kuukausi, päivä). Artikkelin nimi. Lehden/aikakauslehden/sanomalehden nimi, volyyminumero (numeronumero), koko artikkelin sivunumerot, kustantaja, URL)*

Pakollinen kirjallisuus

Cybellium (2024). *Opas turvallisuusoperaatiokeskuksiin (SOC): Kattava opas turvallisuusoperaatiokeskusten (SOC) oppimiseen*
Muniz, J. (2021). *Moderni turvallisuusoperaatiokeskus*. Pearson Education.
ENISA (2017). *Strategiat tietoturvaloukkausten torjumiseksi ja kyberkriisien yhteistyöhön*. **Strategiat tietoturvaloukkausten torjumiseksi ja kyberkriisien yhteistyöhön — ENISA (europa.eu)**

Suositeltavaa luettavaa

Basta, A., Basta, N., Anwar, W., Essar, M. I. (2024). Avoimen lähdekoodin tietoturvakeskus (SOC): Kattava opas modernin SOC:n perustamiseen, hallintaan ja ylläpitoon.
Cybellium (2023). Turvallisuusoperaatiokeskuksen (SOC) hallinta.

5. M5: TURVALLISUUDEN HALLINTO JA POLITIIKKA

Moduulin nimi	Moduulin koodi
TURVALLISUUDEN HALLINTO JA POLITIIKKA	

Luennoitsija(t)	Laitos tai osasto, jossa moduuli opetetaan

Opetustapa	Kieli
Lähdeopetus / Verkko-opetus / Hybridi	*Englanti, suomi, turkki, norja, liettua, romania, ranska, puola, espanja*

Edellytykset
Ei mitään

Myönnettyjen ECTS-opintopisteiden määrä	Opiskelijan työmäärä	Yhteistyötyöskentely	Itsenäinen opiskelu
3	75	50	25

Moduulin tarkoitus ja tulokset
Aihe "Turvallisuuden hallinta ja politiikka" tähtää valmistamaan opiskelijat kohtaamaan pk-yritysten kyberturvallisuuden haasteet, integroimaan turvallisuuden hallinnan liiketoimintastrategiaan ja varmistamaan lakisääteisten vaatimusten, kuten GDPR:n, noudattamisen. Moduuli kattaa muun muassa uhkien ja haavoittuvuuksien tunnistamisen, vankkojen ja mukautuvien turvallisuuspolitiikkojen suunnittelun sekä tehokkaan tapahtumien hallinnan. Lisäksi se keskittyy kehittämään hallintorakenteita, jotka määrittelevät selkeät roolit organisaatiossa ja sovittavat kyberturvallisuuden strategisiin tavoitteisiin. Opiskelijat hankkivat teknisiä taitoja kyberriskien arvioinnissa ja vähentämisessä sekä kehittävät analysointitaitoja, joiden avulla he voivat ehdottaa parannuksia turvallisuuden kypsyystasoon. He oppivat myös kommunikoimaan tehokkaasti kyberturvallisuuden tarpeista johdolle, tukemaan tietoon perustuvaa päätöksentekoa ja varmistamaan säännösten noudattamisen ja eettisyyden kyberturvallisuudessa. Moduuli ”Turvallisuuden hallinto ja politiikka” sisältää myös tarkemman tarkastelun phishing-hyökkäysten ehkäisystä, tekoälypohjaisista kyberhyökkäyksistä ja ransomware-hallinnasta sekä analyysin siitä, miten nämä erityiset uhat edellyttävät integroitua lähestymistapaa hallintoon ja säännösten noudattamiseen. Turvallisuuspolitiikan tehokkuutta mitataan paitsi sen kyvyn perusteella estää tapahtumia myös sen mukautuvuus uusien uhkien suhteen ja nykyisten lakisääteisten vaatimusten noudattaminen.

Moduulin oppimistulokset	Opetus- ja oppimismenetelmät	Arviointimenetelmät
Tieto: Opiskelijat saavat edistyneitä tietoja siitä, miten uusia kyberturvallisuusrutiineja ja -työnkulkuja voidaan toteuttaa pk-yritysten työpaikoilla, ottaen huomioon nykyiset kyberturvallisuusperiaatteet, trendit ja alan kansallisten ja kansainvälisten lakien noudattamisen. Hankkia edistyneitä tietoja siitä, miten integroida phishing-hyökkäysten ehkäisy, hallita tekoälypohjaisia uhkia ja vastata ransomware-haittaohjelmiin pk-yritysten ympäristöissä.	**Luennot (ohjattu lukeminen):** Luennot tarjoavat vankan käsitteellisen perustan kyberturvallisuudesta, hallinnosta, tietosuojasta ja säännösten noudattamisesta ja kannustavat opiskelijoita aktiiviseen osallistumiseen. Sisältää interaktiivisia luentoja, joihin kuuluu säännöllisiä kysymys- ja vastausosioita, kyselyitä ja live-ongelmanratkaisuharjoituksia. Käytetään työkaluja, kuten Mentimeter ja Poll Everywhere. **Osallistuminen keskusteluihin ja foorumeihin:** Osallistumalla keskusteluihin ja foorumeihin opiskelijat voivat keskustella ja analysoida kriittisesti kyberturvallisuuskysymyksiä, mikä kehittää heidän argumentaatiotaitojaan. Tätä sovelletaan kyberturvallisuuden etiikkaan, politiikkaan ja päätöksentekoon liittyviin kysymyksiin. **Tapaustutkimukset:** Tapaustutkimusten avulla opiskelijat voivat analysoida kyberturvallisuustilanteita pk-yrityksissä ja soveltaa teoreettista tietoa todellisten ongelmien ratkaisemiseen. Niissä keskitytään aiheisiin, kuten tietoturvaloukkausten hallintaan, kiristysohjelmiin, tietojenkalasteluun, tekoälypohjaisiin hyökkäyksiin, tietoturvapolitiikan toteuttamiseen ja hallintoon.	**Itsearviointitestit:** Itsearviointitestien avulla opiskelijat voivat arvioida ymmärrystään kustakin ala-aiheesta erilaisilla kysymyksillä, jotka antavat jatkuvaa palautetta parannettavien alueiden tunnistamiseksi. Ne eivät vaikuta lopulliseen arvosanaan, mutta ovat avainasemassa itseohjautuvassa oppimisessa. **Loppukoe (valinnainen):** Loppukoe on valinnainen, ja sen avulla opiskelijat voivat saada kurssin suorittamisesta todistuksen, jossa arvioidaan heidän yleistä ymmärrystään kurssista kehityskysymysten, tapaustutkimusten ja monivalintakysymysten avulla. Loppukokeen läpäiseminen on edellytys kurssin suorittamisesta todistuksen saamiseksi, kun taas ne, jotka eivät osallistu kokeeseen, saavat osallistumistodistuksen.
Taidot: Oppijat oppivat käyttämään edistyneitä menetelmiä riskien arviointiin, uusien kyberturvallisuusrutiinien suunnitteluun ja toteuttamiseen sekä vastastrategioiden valmisteluun, mikä varmistaa tehokkaan hallinnon ja säännösten noudattamisen pk-yritysten työpaikoilla. Kehitä taitoja suunnitella ja toteuttaa kattavia kyberturvallisuusrutiineja, jotka vastaavat edistyneisiin uhkiin ja varmistavat organisaation säännösten noudattamisen	**Käytännön työpajat:** Käytännön työpajoissa opiskelijat voivat soveltaa kyberturvallisuuden käsitteitä esimerkiksi politiikan kehittämisen ja tapahtumasimulaatioiden kaltaisten harjoitusten avulla, ja he saavat reaaliaikaista palautetta ohjaajalta. Työpajat on suunniteltu vahvistamaan käytännön taitoja ja valmistamaan opiskelijat soveltamaan oppimaansa todellisissa tilanteissa. **Käytännön työ ja yksilölliset projektit:** Käytännön työ ja yksilölliset projektit antavat opiskelijoille mahdollisuuden soveltaa kyberturvallisuuden käsitteitä esimerkiksi politiikan laatimisen ja riskianalyysin tehtävissä, kehittää itsenäisiä työtaitoja ja soveltaa teoreettista tietoa käytännössä.	**Käytännön arvioinnit:** Kurssin aikana tehtävät käytännön arvioinnit antavat opiskelijoille mahdollisuuden soveltaa teoreettista tietoa simuloiduissa tilanteissa, kuten kyberturvallisuuspolitiikan kehittämisessä ja tapahtumasimuloinneissa, tavoitteena arvioida heidän kykyään ratkaista todellisia ongelmia pk-yritysten kontekstissa.

	Yhteistyöprojektit: Yhteistyöprojektit antavat opiskelijoille mahdollisuuden työskennellä tiimeissä kehittääkseen kyberturvallisuusratkaisuja pk-yrityksille, mukaan lukien turvallisuuspolitiikat ja hallintomallit. Ne edistävät tiimityöskentelyä, projektinhallintaa ja hankitun tiedon käytännön soveltamista opettajien ja opiskelijatovereiden antaman palautteen avulla.	**Ryhmäprojektit:** Ryhmäprojekteissa opiskelijat voivat kehittää kattavan kyberturvallisuusprojektin riskien tunnistamisesta hallintomallien ja tapahtumien vastaussuunnitelmien ehdotuksiin, arvioiden sekä sisällön laatua että yhteistyökykyä. Tämä projekti on keskeinen osa lopullista arviointia ja yhdistää kaikki kurssin oppimistulokset.
Osaaminen: Opiskelijat osaavat kehittää ja toteuttaa strategisia kyberturvallisuuspolitiikkoja, johtaa aloitteita uusien rutiinien ja työnkulkujen luomiseksi pk-yritysten työpaikoilla sekä tehdä eettisiä päätöksiä, jotka ovat yhdenmukaisia organisaation tavoitteiden ja vaatimustenmukaisuusvaatimusten kanssa. Opiskelijat oppivat laatimaan ja toteuttamaan kyberturvallisuuspolitiikkoja, jotka estävät kehittyneitä kyberuhkia ja varmistavat kansainvälisten kyberturvallisuusmääräysten noudattamisen.	**Skenaariosimulaatiot:** Skenaariosimulaatioiden avulla opiskelijat voivat hallita kyberturvallisuusuhkia virtuaaliympäristöissä, jotka jäljittelevät todellisia hyökkäyksiä, ja tehdä strategisia päätöksiä paineen alla. Tämä menetelmä parantaa kriisinhallinta- ja uhkatilanteiden hallintataitoja ja on keskeinen osa turvallisuuspolitiikan arvioinnin ja kriittisissä tilanteissa tehtävän päätöksenteon opetusta. Opiskelijoiden on osoitettava, miten he soveltaisivat hallintopolitiikkaa estääkseen tai reagoidakseen tiettyihin tapahtumiin, kuten phishing-hyökkäyksiin, kiristysohjelmiin ja tekoälypohjaisiin hyökkäyksiin, ja arvioitava ymmärrystään asiaankuuluvasta sääntelykehyksestä.	**Simulaatiot ja tapahtumien hallinta:** Opiskelijoita arvioidaan heidän kykynsä hallita kyberturvallisuustapahtumia simulaatioissa, jotka jäljittelevät todellisia kriisejä pk-yrityksissä. Tavoitteena on mitata heidän kykyään käsitellä paineita, tehdä strategisia päätöksiä ja toteuttaa reagointisuunnitelmia reaaliajassa sekä arvioida heidän käytännön soveltamistaan dynaamisissa tilanteissa.

Moduulin sisältö: aiheiden jaottelu	Yhteistyötyötunnit					Yksilölliset työajat ja tehtävät	
	Luennot	Konsultaatiot	Harjoittelu (korkeakoulu)	Kokeet	**Kaikki**	**Yksilöllinen työ**	**Tehtävät**
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 yleiset kyberturvallisuushaasteet, kuten rajalliset budjetit, erikoistuneen turvallisuushenkilöstön puute ja käytännön menetelmät kyberturvallisuusinvestointien priorisoimiseksi.	5	0,5	3	0,5	**9**	**4**	Lukeminen, tutkimus, tapaustutkimuksen valmistelu
Tietosuoja -Tietosuojaperiaatteet kyberturvallisuudessa -Henkilötietojen suojaus ja GDPR -Tietosuojan vaikutus pk-yritysten toimintaan -Työkalut ja tekniikat tietosuojan varmistamiseksi	4	0,5	3	0,5	**8**	**4**	Politiikan analyysi, yksilöllinen tehtävä
Lait, etiikka ja säännösten noudattaminen -Kyberturvallisuusorganisaatiot, politiikat ja standardit -Asiaankuuluva kansallinen ja kansainvälinen lainsäädäntö -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.	5	0,5	3	0,5	**9**	**5**	Tapaustutkimus, lainsäädännön analyysi

Turvallisuuden hallinta -Kyberturvallisuuden hallintorakenne -Turvallisuuden hallinnan roolit ja vastuut -Kyberturvallisuuden kypsyysmallit -Kyberturvallisuuden integrointi yrityshallintoon - Paranna kykyäsi suorittaa riskinarviointeja ja laatia strategisia vastasuunnitelmia simuloiduissa kriisitilanteissa (kiristyshakkerointi, tietojenkalastelu jne.)	4	0,5	3	0,5	**8**	**4**	Riskienhallinnan skenaarioanalyysi
Johto- ja hallitustason viestintä -Kyberturvallisuuden viestintästrategiat -Turvallisuusraportointi ylimmälle johdolle -Turvallisuustietoihin perustuva päätöksenteko -Kyberturvallisuuden kriisinhallinta ja viestintä - Kriisinhallinnan ja päätöksenteon taitojen hallitseminen stressaavissa tilanteissa, joissa on kyse tekoälypohjaisista hyökkäyksistä ja kiristysohjelmista.	4	0,5	3	0,5	**8**	**4**	Esityksen valmistelu, sidosryhmien kanssa viestintä
Johtamispolitiikka -Turvallisuuspolitiikan kehittäminen -Politiikan täytäntöönpano ja seuranta -Politiikan arviointi ja jatkuva parantaminen -Turvallisuuspolitiikan mukauttaminen teknologisiin ja sääntelymuutoksiin -Tutkimus siitä, kuinka tehokkaat koulutus- ja tietoisuuspoliittiset toimet voivat olla keskeinen osa sääntelyn noudattamista ja riskien vähentämistä.	4	0,5	3	0,5	**8**	**4**	Politiikka-asiakirjan laatiminen ja tarkistaminen
Yhteensä	**26**	**3**	**18**	**3**	**50**	**25**	

Arviointistrategia	**Vertaileva painoprosentti**	**Arviointikriteerit**
Itsearviointi I	10	Organisaation kontekstin peruskäsitteiden arviointi.
Itsearviointi II	10	Yksityisyyden peruskäsitteiden arviointi.
Itsearviointi III	10	Lakien, eettisten periaatteiden ja vaatimustenmukaisuuspolitiikkojen arviointi.
Itsearviointi IV	10	Kyberturvallisuuspolitiikkojen arviointi.
Itsearviointi V	10	Johtotason viestinnän arviointi.
Itsearviointi VI	10	Turvallisuuspolitiikan ja politiikan luomisen arviointi.
Tietotesti	40	Loppukoe, joka kattaa integroivia kysymyksiä kaikista kurssin aiheista.
10 pistettä – 96 %–100		

Opiskelumateriaali *(Sukunimi, etunimen alkukirjain. (Vuosi, kuukausi, päivä). Artikkelin nimi. Lehden/aikakauslehden/sanomalehden nimi, volyyminumero (numeronumero), koko artikkelin sivunumerot, kustantaja, URL)*

Pakollinen kirjallisuus

...

"EU:n kyberturvallisuuslaki: resilienssin ja johdonmukaisuuden hallinta digitaalisella aikakaudella" Luisa Marin

- Tämä kirja tarjoaa syvällisen analyysin EU:n kyberturvallisuuslaeista ja -politiikoista, jotka ovat keskeisiä kyberturvallisuuden hallinnon rakenteen ja toteutuksen ymmärtämiseksi EU:n kontekstissa.

"Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy" (Kyberturvallisuus Euroopan unionissa: hallintopolitiikan resilienssi ja sopeutumiskyky), George Christou

- Tämä kirja tarkastelee EU:n kyberturvallisuuden hallintokehystä ja päätöksentekoprosesseja ja auttaa opiskelijoita ymmärtämään eri hallintotasojen välistä dynaamista vuorovaikutusta.

"**Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft"** (Phishing ja vastatoimet: Ymmärtää **kasvava ongelma sähköisen identiteettivarkauden)** Markus Jakobsson ja Steven Myers

- Vaikka tämä kirja ei koske nimenomaisesti EU:ta, sen yksityiskohtainen tarkastelu phishing-tekniikoista ja vastatoimista voidaan sovittaa EU:n kontekstiin keskittymällä GDPR-vaatimustenmukaisuuteen ja tietosuojaperiaatteisiin.

"European Cybersecurity Law and Regulation" (Eurooppalainen kyberturvallisuuslainsäädäntö ja -sääntely), toim. Nadya Purtova ja Bert-Jaap Koops

- Tämä toimitettu teos käsittelee Euroopan unionin kyberturvallisuuteen liittyviä oikeudellisia ja sääntelytoimenpiteitä, mukaan lukien vaatimustenmukaisuuden haasteet ja puitteet, kuten NIS-direktiivi ja GDPR.

"Ransomware: Understanding Digital Extortion and its Threat to Your Organization" (Lunnasohjelmat: digitaalisen kiristyksen ja sen organisaatiollesi aiheuttaman uhan ymmärtäminen), Allan Liska ja Timothy Gallo

- Tämä teksti, jota täydentävät EU:n erityiset tapaustutkimukset ja esimerkit, auttaa opiskelijoita ymmärtämään ransomware-hyökkäysten vaikutuksia EU:n sääntelyn puitteissa.

Suositeltavaa luettavaa

"EU:n yleinen tietosuoja-asetus (GDPR): kommentaari", Lukas Feiler ja Nikolaus Forgó

- Tämä kommentaari tarjoaa yksityiskohtaista tietoa GDPR:stä, joka on välttämätöntä EU:n sääntely-ympäristön ja sen vaikutusten ymmärtämiseksi kyberturvallisuuskäytäntöihin.

"Tietosuoja ja kyberturvallisuus Euroopassa: Oikeudelliset puitteet ja käytännön näkökohdat", Paul Lambert

- Tämä kirja tarjoaa käytännönläheisiä näkemyksiä tietosuoja- ja kyberturvallisuusstrategioiden yhdenmukaistamisesta EU:ssa, mukaan lukien säännösten noudattaminen ja turvallisuustoimenpiteiden parhaat käytännöt.

"Verkko- ja tietoturva: eurooppalaiset ja kansainväliset näkökulmat", toim. Jeanne Pia Mifsud Bonnici ja Joe Cannataci

- Tämä kokoelma tarkastelee verkko- ja tietoturvan tilannetta sekä eurooppalaisesta että kansainvälisestä näkökulmasta ja tarjoaa laajemman kontekstin EU:n kyberturvallisuustoimille.

"Tekoäly kyberturvallisuudessa: käytännöt, haasteet ja etiikka", Elena Fersman ja Martin Fredriksson

- Kattava katsaus tekoälyteknologioiden integroimiseen kyberturvallisuuteen, jossa käsitellään eettisiä, toiminnallisia ja sääntelyyn liittyviä haasteita, jotka ovat erityisen merkityksellisiä EU:n kontekstissa.

"Kyberturvallisuus digitaalisella aikakaudella: työkalut, tekniikat ja sovellukset", Gregory B. White, Eric A. Fisher ja James L. Antonakos

- Vaikka tämä kirja ei keskity yksinomaan EU:hun, se kattaa laajan valikoiman nykyaikaisia kyberturvallisuusaiheita.

Opiskelumateriaali *(HackerU:n ja Cybintin alkuperäismateriaali)*
Pakollinen kirjallisuus
• TCP/IP-verkon hallinta: Apua Unix-järjestelmänvalvojille, 3. painos, Craig Hunt (O'Reilly) • Essential System Administration Pocket Reference: Commands and File Formats (Pocket Administrator), kirjoittanut Eleen Frisch (O'Reilly) • Computer Networking: The Beginner's guide for Mastering Computer Networking, the Internet and the OSI Model, Ramon Nastase
Suositeltava kirjallisuus
• CompTIA A+ -sertifiointi All-in-One For Dummies (tietokoneet/tekniikka), 5. painos, Glen E. Clarke, Edward Tetz, Timothy L. Warner • Coding All-in-One For Dummies 1. painos, Nikhil Abraham • Information Technology Essentials Volume 1: Johdanto tietojärjestelmiin, Eric Frick • IT-arkkitehtuuri aloittelijoille, 1. painos, Kalani Kirk Hausman, Susan L. Cook • Cybersecurity For Dummies (Tietokoneet/tekniikka) 1. painos, Steinberg • Linux For Dummies, 10. painos, Richard Blum • Windows 10 For Dummies, 3. painos (tietokoneet/tekniikka), 3. painos, Rathbone • Verkot aloittelijoille, 12. painos, Doug Lowe

6. M6: KYBERTURVALLISUUDEN SUUNNITTELU

Moduulin nimi	Moduulin koodi
KYBERTURVALLISUUDEN SUUNNITTELU	

Luennoitsija(t)	Laitos tai osasto, jossa moduuli opetetaan

Opetustapa	Kieli
Lähdeopetus, verkko-opetus, yhdistetty opetus, konsultaatiot	*Englanti, suomi, turkki, norja, liettua, romania, ranska, puola, espanja*

Edellytykset
-

Myönnettyjen ECTS-opintopisteiden määrä	Opiskelijan työmäärä	Yhteistyö	Yksilölliset työtunnit
3	75	50	25

Moduulin tarkoitus ja tulokset		
Kurssin suoritettuaan opiskelijat osaavat ymmärtää ja soveltaa kyberturvallisuuden suunnittelun ja hallinnan perusperiaatteita. He oppivat toteuttamaan kansainvälisiä standardeja ja viitekehyksiä, kehittämään pitkän aikavälin turvallisuusstrategioita, hallinnoimaan operatiivisia ja taktisia kyberturvallisuustoimenpiteitä sekä suunnittelemaan turvallisia verkkoarkkitehtuureja, kuten pilvi- ja nollaluottamusarkkitehtuureja. Lisäksi opiskelijat osaavat suunnitella tehokkaita tapahtumien vasteohjelmia ja toteuttaa liiketoiminnan jatkuvuusstrategioita, joilla varmistetaan organisaation sietokyky ja tehokkaat kyberturvallisuustoimenpiteet muuttuvien uhkien edessä.		
Moduulin oppimistulokset	**Opetus- ja oppimismenetelmät**	**Arviointimenetelmät**
Tieto: Opiskelijat saavat syvällistä tietoa siitä, miten edistyneitä kyberturvallisuusperiaatteita ja nykyisiä trendejä voidaan integroida strategiseen suunnitteluun ja operatiiviseen johtamiseen.	Luennot, tapaustutkimukset, ryhmäkeskustelut, itseohjattu oppiminen	Itsearviointitestit, tietotestit
Taidot: Opiskelijat oppivat strategisen suunnittelun ja operatiivisen johtamisen taitoja, joiden avulla he voivat suunnitella ja toteuttaa tehokkaasti kyberturvallisuusstrategioita, joilla vastataan uusiin riskeihin ja varmistetaan vankat taktiset vastatoimet.	Käytännön harjoitukset, työpajat, tapaustutkimukset	Projektipohjaiset arvioinnit, käytännön arvioinnit

Pätevyys: Opiskelijat osaavat kehittää ja toteuttaa strategisia kyberturvallisuuskehyksiä sekä johtaa ja hallinnoida kyberturvallisuusaloitteita	Työpajat, seminaarit, roolipelit	Jatkuva arviointi, skenaariopohjaiset testit

Moduulin sisältö: aiheiden jaottelu	**Yhteistyötyöskentely**					**Yksilölliset työajat ja tehtävät**	
	Luennot	Konsultaatiot	Harjoitukset	Kokeet	**Kaikki kontaktiopetus**	**Yksilöllinen työ**	**Tehtävät**
1. 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)	8	0,5	6	0,5	**15**	**8**	Määritellä tietoturvan, ihmisten ja yhteiskunnan turvallisuuden oikeudelliset näkökohdat sekä pk-yritysten tietoja koskevat lait ja politiikat. Luokittele pk-yrityksille merkitykselliset kyberhyökkäystyypit. Tunnista hyödyllisiä työkaluja kyberhyökkäysten ehkäisemiseksi
2. Strateginen suunnittelu -Kyberturvallisuuden tavoitteiden määrittely -SWOT-analyysi (vahvuudet, heikkoudet, mahdollisuudet, uhat) -Kehitä pitkän aikavälin turvallisuusstrategioita -Keskeisten suorituskykyindikaattoreiden (KPI) asettaminen -Turvallisuusstrategian tarkistaminen ja päivittäminen	8	2	6	2	**18**	**8**	Määritä pk-yrityksille merkitykselliset kyberturvallisuustavoitteet SWOT-analyysin avulla, kehitä pitkän aikavälin strategiat riskien hallitsemiseksi, jaa resurssit ja budjetti vastaavasti, aseta KPI-mittarit edistymisen mittaamiseksi ja päivitä strategia säännöllisesti uusien uhkien perusteella.

3. Operatiivinen ja taktinen johtaminen -Pääsynvalvonnan toteuttaminen -Päivitysten hallinta ja ohjelmis-topäivitykset -Järjestelmän jatkuva valvonta - Työntekijöiden tietoturvatietoisuuden koulutus	8	1	6	2	**17**	**9**	Toteuta pääsynvalvontatoimenpiteitä luvattoman pääsyn estämiseksi, ylläpidä järjestelmiä päivitysten hallinnan avulla, asenna epätavallisten toimintojen seuranta ja tarjoa työntekijöille tietoturvatietoisuuskoulutusta.
Yhteensä	**24**	**3,5**	**18**	**4,5**	**50**	**25**	

Arviointistrategia	**Vertaileva painoprosentti**	**Arviointikriteerit**
Itsearviointitesti (1)	10	10 pistettä – 96–100 % oikeita vastauksia. 9 pistettä – 91–95 % oikeita vastauksia. 8 pistettä – 86–90 % oikeita vastauksia. 7 pistettä – 80–85 % oikeita vastauksia. 6 pistettä – 70–79 % oikeita vastauksia. 5 pistettä – 60–69 % oikeita vastauksia. 4 pistettä – 50–59 % oikeita vastauksia. 3 pistettä – 40–49 % oikeita vastauksia. 2 pistettä – 30–39 % oikeita vastauksia. 1 piste – 0–29 % oikeita vastauksia.
Itsearviointitesti (2)	10	
Itsearviointitesti (3)	10	
Tietojen arviointitesti	70 %	

Tutkimusmateriaali *(Sukunimi, etunimen alkukirjain. (Vuosi, kuukausi, päivä). Artikkelin nimi. Lehden/aikakauslehden/sanomalehden nimi, volyyminumero (numeronumero), koko artikkelin sivunumerot, kustantaja, URL)*

Pakollinen kirjallisuus

1. Nair, A., & Greeshma, M. R. (2023). Mastering Information Security Compliance Management: A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing Limited.
2. Falco, G. J., & Rosenbach, E. (2021). Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press.
3. NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology, 26. helmikuuta 2024

Suositeltavaa luettavaa

1. Mehta, S. (2023). *ISACA Certified in Risk and Information Systems Control (CRISC®) Exam Guide*. Packt Publishing Limited.
2. Gregory, P. H. (2021). *CISM-sertifioitu tietoturvapäällikkö All-in-One -kokeen opas*. McGraw-Hill.
3. ISACA. (2021). *CRISC Review Manual, 7. painos*. ISACA.
4. Euroopan parlamentti ja neuvosto. (14.12.2022). *Asetus (EU) 2022/2554 finanssialan digitaalisesta toimintakestävyydestä*.
5. Opas yleiseen tietosuoja-asetukseen (GDPR), tietosuojavaltuutetun toimisto

7. M7: RISKIENHALLINTA JA RISKIEN VÄHENTÄMINEN

Moduulin nimi	Moduulin koodi
RISKIEN HALLINTA JA VÄHENTÄMINEN	

Luennoitsija(t)	Laitos tai osasto, jossa moduuli järjestetään

Opetustapa	Kieli
Lähdeopetus, verkko-opetus, yhdistetty opetus, konsultaatiot	*Englanti, suomi, turkki, norja, liettua, romania, ranska, puola, espanja*

Edellytykset			
Ei mitään			
Myönnetyt ECTS-opintopisteet	**Opiskelijan työmäärä**	**Yhteistyötyöskentely**	**Itsenäinen opiskelu**
3	75	50	25

Moduulin tarkoitus ja tulokset		
Kurssin suoritettuaan opiskelijat osaavat hallita (tunnistaa, analysoida, arvioida, arvioida, lieventää) jatkuvasti ICT-infrastruktuurien, järjestelmien ja palveluiden kyberturvallisuuteen liittyviä riskejä suunnittelemalla, soveltamalla, raportoimalla ja viestimällä riskianalyysejä, arviointeja ja käsittelyjä.		
Moduulin oppimistulokset	**Opetus- ja oppimismenetelmät**	**Arviointimenetelmät**
Tieto: Opiskelijat saavat edistyneitä tietoja riskienhallintaprosesseista, mukaan lukien riskien tunnistaminen, arviointi ja hallinta, minkä ansiosta he pystyvät luomaan ja kuvaamaan tehokkaita kyberturvallisuusrutiineja, jotka on räätälöity pk-yritysten työpaikkojen erityistarpeisiin kansallisten ja kansainvälisten standardien mukaisesti.	Valitaan luennoitsijan toimesta osasta 1.3. [*Opetusmenetelmät, esim. teoreettiset luennot, kirjallisuusanalyysi, vierailevat luennoitsijat, vertaisopetus ja -oppiminen, mentorointi jne.*	Itsearviointitestit Tietojen arviointitesti
Taidot: Oppijat osaavat soveltaa edistyneitä menetelmiä ja työkaluja kattavien riskinarviointien tekemiseen, tehokkaiden riskinhallintastrategioiden suunnitteluun ja toteuttamiseen sekä pk-yritysten työpaikoille räätälöityjen vankkojen kyberturvallisuusrutiinien kehittämiseen.	Luennoitsija valitsee osan 1.3. [*Opetusmenetelmät, esim. käytännön tehtävät/laboratoriot, tietokilpailut, pelit, tekninen videon analysointi, tapaustutkimukset, käytännön harjoitukset jne.*	Itsearviointitestit Tietojen arviointitesti

Osaaminen: Oppijat osaavat kehittää ja toteuttaa strategisia kyberturvallisuuspolitiikkoja pk-yritysten työpaikoille	Valitaan luennoitsijan toimesta osasta 1.3. [*Opetusmenetelmät, esim. kilpailut, CTF, simuloituja ympäristöjä, 5E, CBL, CL, PBL jne.]* D2.3:sta *"Pk-yritysten kyberturvallisuuden muutosagenttien oppimispolun* rakenne"	Itsearviointitestit Tietojen arviointitesti

Moduulin sisältö: aiheiden jakautuminen	Yhteistyötyötunnit					Yksilölliset työajat ja tehtävät	
	Luennot (korkeakoulu)	Konsultaatiot	Harjoitukset (korkeakoulu)	Kokeet	Kaikki kontaktiopetus	Yksilöllinen työ	Tehtävät
Riskien arviointi - Yleinen riskienhallintaprosessi - Yleinen riskienhallinnan kehys - Riskienhallinnan periaatteet - Riskienhallinnan standardit - Käytännön esimerkkejä	2	0	2	0	**4**	5	- Kuvaile lyhyesti riskienhallintaprosessin keskeiset vaiheet, mukaan lukien riskien tunnistaminen, arviointi ja hallinta. - Määritä riskienhallinnan sisäiset ja ulkoiset kontekstit pk-yritykselle. Määritä riskien arvioinnin laajuus ja tunnista keskeiset riskitekijät. - Kehitä valitulle pk-yritykselle ominaiset riskikriteerit.
Riskien tunnistaminen - johtaminen ja sitoutuminen riskienhallintaan - riskienhallintatoimien laajuuden määrittely - riskienhallinnan ulkoinen ja sisäinen konteksti - konkreettiset ja aineettomat riskilähteet - syyt ja tapahtumat - uhat ja mahdollisuudet - haavoittuvuudet ja valmiudet - ulkoisen ja sisäisen kontekstin muutokset - uusia riskejä osoittavat indikaattorit; - omaisuuden ja resurssien luonne ja arvo; - seuraukset ja niiden vaikutus tavoitteisiin; - tietämyksen ja tiedon luotettavuuden rajoitukset; - osapuolten ennakkoluulot, oletukset ja uskomukset. - Käytännön esimerkkejä ja tapaustutkimuksia.	4	0	4	0	**8**	5	- Tunnista pk-yrityksen konkreettiset ja aineettomat riskilähteet. Luokittele riskit syiden, tapahtumien, uhkien ja mahdollisuuksien perusteella. - Analysoi pk-yrityksen sisäiset haavoittuvuudet ja kyvyt ja arvioi, miten ulkoisten ja sisäisten olosuhteiden muutokset voivat vaikuttaa liiketoimintaan. - Tunnista pk-yrityksen mahdolliset uudet riskit ja ehdota indikaattoreita niiden seurantaan. Mieti, miten omaisuuden ja resurssien luonne ja arvo vaikuttavat tähän analyysiin.
Sisäiset uhat - Sisäisten uhkien määritelmä ja tyypit - Sisäisten uhkien kustannukset - Sisäisten uhkien torjuntaohjelman laatiminen - Sisäisten uhkien havaitseminen ja tunnistaminen - Sisäisten uhkien arviointi	6	0	6	0	**12**	5	- Määritä ja luokittele erilaiset sisäiset uhat, jotka ovat merkityksellisiä pk-yrityksille. Keskustele näiden uhkien mahdollisista kustannuksista yritykselle.

- Sisäisten uhkien hallinta - Käytännön esimerkkejä ja tapaustutkimuksia							- Kehitä perusohjelma sisäisten uhkien torjumiseksi pk-yrityksissä. Korosta keskeisiä osatekijöitä, kuten havaitsemis-, tunnistamis- ja hallintastrategioita. - Ehdota menetelmä sisäisten uhkien arvioimiseksi ja esitä vaiheet näiden uhkien tehokkaaksi hallitsemiseksi pk-yrityksissä.
Riskien mittaus- ja arviointimallit ja -menetelmät - Kvantitatiiviset ja kvalitatiiviset riskien arviointimallit ja -menetelmät - tapahtumien ja seurausten todennäköisyys - seurausten luonne ja laajuus - monimutkaisuus ja yhteydet - aikaan liittyvät tekijät ja volatiliteetti; - nykyisten valvontamenetelmien tehokkuuden arviointi; - herkkyys- ja luotettavuustasot. - Käytännön esimerkkejä ja tapaustutkimuksia	6	0	6	0	**12**	5	- Vertaa ja vertaile yhtä kvantitatiivista ja yhtä kvalitatiivista riskinarviointimallia. - Arvioi riskitapahtuman todennäköisyys sekä sen seurausten luonne ja laajuus pk-yritykselle. Mieti, miten monimutkaisuus, aika- ja volatiliteettitekijät vaikuttavat tähän arviointiin. - Arvioi nykyisten valvontamenetelmien tehokkuutta tunnistettujen riskien hallinnassa. Sisällytä analyysi valvontatoimenpiteiden herkkyys- ja luotettavuustasoista.
Riskien hallinta - riskien käsittelyvaihtoehtojen muotoilua ja valintaa - riskien käsittelyn suunnittelu ja toteutus - riskien hallinnan tehokkuuden arviointi - jäljelle jäävän riskin hyväksyttävyyden arviointi - seuranta ja arviointi - kirjaaminen ja raportointi - Käytännön esimerkkejä ja tapaustutkimuksia	6	0	6	0	**12**	5	- Tunnista ja valitse sopivat riskienhallintavaihtoehdot pk-yrityksille. Perustele valintasi riskien luonteen perusteella. - Laadi lyhyt riskienhallintasuunnitelma, jossa kuvataan, miten valitut riskienhallintavaihtoehdot toteutetaan pk-yrityksessä. - Ehdota menetelmä riskienhallinnan tehokkuuden arvioimiseksi ja jäljellä olevan riskin hyväksyttävyyden määrittämiseksi.
Yhteensä	**24**	**2**	**24**	**0**	**50**	**25**	

Arviointistrategia	**Vertaileva painoprosentti**	**Arviointikriteerit**

Itsearviointitesti (1)	5	10 pistettä – 96–100 % oikeita vastauksia. 9 pistettä – 91–95 % oikeita vastauksia. 8 pistettä – 86–90 % oikeita vastauksia. 7 pistettä – 80–85 % oikeita vastauksia. 6 pistettä – 70–79 % oikeita vastauksia. 5 pistettä – 60–69 % oikeita vastauksia. 4 pistettä – 50–59 % oikeita vastauksia. 3 pistettä – 40–49 % oikeita vastauksia. 2 pistettä – 30–39 % oikeita vastauksia. 1 piste – 0–29 % oikeita vastauksia.
Itsearviointitesti (2)	5	
Itsearviointitesti (3)	5	
Itsearviointitesti (4)	5	
Itsearviointitesti (5)	5	
Tietojen arviointitesti	75	

Opiskelumateriaali *(Sukunimi, etunimen alkukirjain. (Vuosi, kuukausi, päivä). Artikkelin nimi. Lehden/aikakauslehden/sanomalehden nimi, vuosikerta (numero), artikkelin sivunumerot, kustantaja, URL)*

Pakollinen kirjallisuus

1. Adarsh Nair ja Greeshma M. R. (2023) Mastering Information Security Compliance Management : A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&**query=risk%20management
2. Gregory J. Falco, Eric Rosenbach (2021) Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press, eBook
3. Kristina Narvaez, Betty Simkins, John Fraser (2014) Yrityksen riskienhallinnan toteuttaminen: tapaustutkimuksia ja parhaita käytäntöjä. John Wiley & Sons
4. ENISA (2022) Riskienhallintastandardit
5. Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä korkean yhteisen kyberturvallisuustason saavuttamiseksi unionissa, asetuksen (EU) N:o 910/2014 ja direktiiviä (EU) 2018/1972 sekä direktiivin (EU) 2016/1148 (NIS 2 -direktiivi) kumoamisesta
6. ISO 31000 Riskienhallinta – Ohjeet

Suositeltavaa luettavaa

1. Shobhit Mehta (2023) ISACA Certified in Risk and Information Systems Control (CRISC®) Exam Guide. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management**
2. Peter H. Gregory (2021) CISM-sertifioitu tietoturvapäällikkö All-in-One-kokeen opas. McGraw-Hill
3. ISACA (2021) CRISC Review Manual 7. painos. ISACA
4. Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta toimintavarmuudesta ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011

8. M8: LIIKETOIMINNAN JATKUVUUS, KATASTROFISTA TOIPUMINEN, TAPAHTUMIEN HALLINTA JA HENKILÖSTÖN TURVALLISUUS

Moduulin nimi	Moduulin koodi
LIIKETOIMINNAN JATKUVUUS, KATASTROFISTA TOIPUMINEN, TAPAHTUMIEN HALLINTA JA HENKILÖSTÖN TURVALLISUUS	

Luennoitsija(t)	Laitos tai osasto, jossa moduuli opetetaan

Opetustapa	Kieli
Lähdeopetus, verkko-opetus, yhdistetty opetus, konsultaatiot	*Englanti, suomi, turkki, norja, liettua, romania, ranska, puola, espanja*

Edellytykset
Ei mitään

Myönnettyjen ECTS-opintopisteiden määrä	Opiskelijan työmäärä	Yhteistyötyöskentely	Itsenäinen opiskelu
3	75	50	25

Moduulin tarkoitus ja tulokset

Kurssin suoritettuaan opiskelijat osaavat laatia ja hallinnoida kattavia liiketoiminnan jatkuvuus- ja katastrofipalautumissuunnitelmia (BC/DR), kehittää toimivan tapahtumienhallintaohjelman ja luoda vahvan ja tehokkaan henkilöstön turvallisuuspolitiikan. Opiskelijat oppivat suojaamaan omaisuutta, varmistamaan liiallisten tappioiden välttämisen, ehkäisemään seisokkeja, välttämään tai rajoittamaan kriisitilanteita ja kriisinhallintaympäristöjä.
Kurssin suoritettuaan opiskelijat osaavat laatia ja valvoa kattavan kyberturvallisuuskäsikirjan jatkuvaa käyttöönottoa pk-yrityksissä käyttäen edistyneitä kyberturvallisuusperiaatteita ja -tekniikoita, jotka on integroitu kaikkien kansallisten ja kansainvälisten lakien mukaisesti. Opiskelijat seuraavat myös täytäntöönpanoa.

Moduulin oppimistulokset	Opetus- ja oppimismenetelmät	Arviointimenetelmät
Tieto: Opiskelijat saavat edistyneitä tietoja siitä, miten luodaan ja toteutetaan kattava pk-yritysten työpaikan kyberturvallisuuskäsikirja, joka sisältää edistyneitä kyberturvallisuusperiaatteita, uusimmat puolustusmekanismit ja kansallisten ja kansainvälisten lakien ja standardien noudattamisen tapahtumien hallinnassa, liiketoiminnan jatkuvuudessa ja henkilöstön turvallisuudessa.	Valitaan luennoitsijan toimesta osasta 1.3. [Opetusmenetelmät] D2.3:sta ”Pk-yritysten kyberturvallisuuden muutosagenttien oppimispolun rakenne”.	Itsearviointitestit, tietojen arviointitesti

Taidot: Oppijat oppivat luomaan ja ylläpitämään pk-yritysten työpaikan kyberturvallisuuskäsikirjan käyttämällä edistyneitä menetelmiä riskien arviointiin, tehokkaiden riskienhallinta- ja tapahtumien hallintastrategioiden suunnitteluun sekä organisaation tarpeisiin räätälöityjen kattavien liiketoiminnan jatkuvuussuunnitelmien kehittämiseen.	Valitaan luennoitsijan toimesta osasta 1.3. [Opetusmenetelmät] D2.3 ”Pk-yritysten kyberturvallisuuden muutosagenttien oppimispolun rakenne”	Itsearviointitestit, tietotesti
Pätevyys: Oppijat osaavat kehittää ja toteuttaa pk-yritysten kyberturvallisuuskäsikirjan, johtaa turvallisuusprojekteja ja -tiimejä tehokkaasti sekä varmistaa organisaation tavoitteiden ja vaatimustenmukaisuusvelvoitteiden noudattamisen.	Valitaan luennoitsijan toimesta osasta 1.3. [Opetusmenetelmät] D2.3 ”Pk-yritysten kyberturvallisuuden muutosagenttien oppimispolun rakenne”	Itsearviointitestit, tietotesti

Moduulin sisältö: aiheiden jaottelu	**Yhteistyötyöskentely**					**Yksilölliset työajat ja tehtävät**	
	Luennot (korkeakoulu)	Konsultaatiot	Harjoitukset (korkeakoulu)	Kokeet	**Kaikki kontaktiopetus**	**Yksilöllinen työ**	**Tehtävät**
Tapahtumien reagointi - Tapahtumien reagointitoimenpiteiden määritelmä ja merkitys kyberturvallisuudessa - Tehokkaan tapahtumien reagointiprosessin keskeiset osat - Yleisten kyberturvallisuusuhkien yleiskatsaus (tietojenkalastelu, sisäiset uhat) - Tapahtumien hallintasuunnitelman (IRP) laatiminen - Tapahtumien reagointiryhmän roolit ja vastuut - Tapahtuman simulointi: harjoitussuunnitelman toteuttaminen.	5	0,5	3	0,5	**9**	**5**	Laadi yksityiskohtainen tapahtumien vasteen suunnitelma pk-yrityksellesi, mukaan lukien roolit, vastuut ja toimenpiteet, jotka on toteutettava kyberturvallisuustapahtuman sattuessa. Simuloi tapahtuma ja järjestä harjoitus, jossa testataan suunnitelman tehokkuutta.

Katastrofien jälkeinen palautuminen - Katastrofien jälkeisen palautumisen ymmärtäminen - Katastrofien jälkeisen palautumisen suunnitelman laatiminen - Roolit ja vastuut katastrofien jälkeisessä palautumisessa - Palautumisen vaiheet katastrofin jälkeen	5	0,5	3	0,5	**9**	**5**	Laadi katastrofien varalle palautumissuunnitelma, jossa kuvataan menettelytavat IT-infrastruktuurin ja tietojen palauttamiseksi katastrofitilanteen jälkeen. Sisällytä suunnitelmaan palautumisen aikataulu ja jaa vastuut tiimin jäsenille prosessin jokaisessa vaiheessa.
Liiketoiminnan jatkuvuus - Liiketoiminnan jatkuvuuden ymmärtäminen - Liiketoiminnan jatkuvuussuunnitelman (BCP) kehittäminen - Roolit ja vastuut liiketoiminnan jatkuvuudessa - Liiketoiminnan vaikutusten analysointi - BCP:n testaaminen ja parantaminen	5	0,5	3	0,5	**9**	**5**	Laadi liiketoiminnan jatkuvuussuunnitelma, joka varmistaa kriittisten liiketoimintojen jatkumisen häiriön aikana ja sen jälkeen. Määritä olennaiset palvelut ja resurssit ja laadi varautumisstrategiat niiden ylläpitämiseksi erilaisissa tilanteissa.
Turvallisuustietoisuus, koulutus ja valistus - Turvallisuustietoisuuden ymmärtäminen - Turvallisuuskoulutusohjelman kehittäminen - Työntekijöiden vastuut kyberturvallisuudessa - Turvallisuustietoisuuden tehokkuuden mittaaminen -	1	0,5	2	0,5	**4**	**1**	Kehitä pk-yrityksellesi tietoturvatietoisuuden koulutusohjelma, jossa keskitytään keskeisiin kyberturvallisuuspolitiikkoihin ja parhaisiin käytäntöihin. Järjestä koulutustilaisuus työntekijöille ja arvioi heidän ymmärrystään kyselyjen tai interaktiivisten aktiviteettien avulla.

Turvallisuutta koskevat rekrytointikäytännöt - Turvallisuusroolien vaatimusten määrittely - Taustajärjestelmien läpivieminen - Haastattelut turvallisuuskomponenttien osalta - Jatkuva arviointi ja kehittäminen	1	0,5	2	0,5	**4**	**1**	Luo turvallisuuteen keskittyvät rekrytointikäytännöt, mukaan lukien taustatarkistukset ja haastattelukysymykset, joiden tarkoituksena on arvioida ehdokkaiden tietoturvatietoisuutta. Luo tarkistuslista tulevien työntekijöiden välttämättömistä turvallisuuspätevyyksistä ja ominaisuuksista.
Turvallisuuteen liittyvät irtisanomiskäytännöt - Pääsyn välitön peruuttaminen - Tietojen ja laitteiden palauttaminen - Lähtöhaastattelu turvallisuustietojen saamiseksi - Ilmoittaminen asiaankuuluville tiimeille - Oikeudelliset ja säännösten noudattamista koskevat seikat	1	0,5	2	0,5	**4**	**2**	Laadi turvallinen irtisanomismenettely, joka sisältää vaiheet käyttöoikeuksien peruuttamiseksi, yrityksen omaisuuden takaisin saamiseksi ja lähtöhaastattelujen toteuttamiseksi. Toteuta simuloidut irtisanomistilanteet menettelyn tehokkuuden arvioimiseksi.
Kolmannen osapuolen turvallisuus - Kolmannen osapuolen riskien arviointi - Huolellinen toimittajien valinta - Kontrastien ja turvallisuusvaatimusten toteuttaminen - Jatkuva seuranta ja auditointi - Tapahtumien reagointi ja viestintä	2	0,5	2	0,5	**5**	**2**	Tunnista kolmansien osapuolten toimittajiin liittyvät potentiaaliset riskit ja luo turvallisuuden arviointilista, jonka avulla voit arvioida, noudattavatko ne pk-yrityksesi kyberturvallisuusstandardeja. Laadi sopimusmalli, joka sisältää turvallisuusvaatimukset ja seuraamukset vaatimusten noudattamatta jättämisestä.

Turvallisuus arviointiprosesseissa - Turvallisuuden sisällyttäminen arviointeihin - Säännöllisten turvallisuusauditointien suorittaminen - Haavoittuvuuksien arviointi ja tunkeutumistestaus - Tapahtuman jälkeiset tarkastukset	1	0,5	1,5	0,5	**3,5**	**2**	Kehitä prosessi, jolla voit säännöllisesti tarkistaa ja päivittää pk-yrityksesi kyberturvallisuuspolitiikat ja -menettelyt. Suunnittele ja toteuta simuloidut auditoinnit varmistaaksesi, että kaikki turvatoimet ovat ajan tasalla ja noudattavat asiaankuuluvia standardeja.
Erityiskysymys työntekijöiden henkilötietojen yksityisyydestä - Tietojen keräämisen rajoitukset - Tallennus ja pääsyn hallinta - Tietosuojamääräysten noudattaminen - Tietojen jakaminen ja kolmannet osapuolet - Työntekijöiden suostumus ja oikeudet	2	0,5	2	0,5	**5**	**2**	Laadi tietosuojakäytäntö työntekijöiden henkilötietojen käsittelyä varten ja varmista, että tietosuojalakeja ja parhaita käytäntöjä noudatetaan. Suorita riskinarviointi, jotta voit tunnistaa mahdolliset haavoittuvuudet työntekijöiden tietojen tallennuksessa ja käsittelyssä.
Yhteensä	**23**	**2**	**20,5**	**4,5**	**50**	**25**	

Arviointistrategia	**Vertaileva painoprosentti**	**Arviointikriteerit**
Itsearviointitesti (1)	5	**10 pistettä** – 96–100 % oikeita vastauksia. **9 pistettä** – 91–95 % oikeita vastauksia. **8 pistettä** – 86–90 % oikeita vastauksia. **7 pistettä** – 80–85 % oikeita vastauksia. **6 pistettä** – 70–79 % oikeita vastauksia. **5 pistettä** – 60–69 % oikeita vastauksia. **4 pistettä** – 50–59 % oikeita vastauksia. **3 pistettä** – 40–49 % oikeita vastauksia. **2 pistettä** – 30–39 % oikeita vastauksia. **1 piste** – 0–29 % oikeita vastauksia.
Itsearviointitesti (2)	5	
Itsearviointitesti (3)	5	
Itsearviointitesti (4)	5	
Itsearviointitesti (5)	5	
Tietojen arviointitesti	75	

Opiskelumateriaali *(Sukunimi, etunimen alkukirjain. (Vuosi, kuukausi, päivä). Artikkelin nimi. Lehden/aikakauslehden/sanomalehden nimi, volyyminumero (numeronumero), koko artikkelin sivunumerot, kustantaja, URL)*
Pakollinen kirjallisuus

- Gregory J. Falco, Eric Rosenbach (2021). *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. Oxford University Press, eBook.
- Michael Wallace, Lawrence Webber (2017). *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets.* AMACOM.
- Kansallinen standardi- ja teknologiainstituutti (NIST). *Contingency Planning Guide for Information Technology Systems*. NIST SP 800-34 Rev. 1.
- Cochran, K.A. (2024). Incident Response, Business Continuity, and Disaster Recovery. Teoksessa: Cybersecurity Essentials. Apress, Berkeley, CA. **https://doi.org/10.1007/979-8-8688-0432-8_14**

Suositeltavaa luettavaa

- ISACA (2023). *CISM Review Manual 15th Edition*. ISACA.
- Peter H. Gregory (2021). *CISM Certified Information Security Manager All-in-One Exam Guide*. McGraw-Hill.
- IT Governance (2022). *ISO 22301:2019 – Liiketoiminnan jatkuvuuden hallintajärjestelmät. Vaatimukset.*
- M. Souppaya, L. Feldman, G. Witte [2024], Guide for Cybersecurity Incident Recovery, Tietoturvaosasto, Tietotekniikan laboratorio, Kansallinen standardi- ja teknologiainstituutti, Yhdysvaltain kauppaministeriö
- Ihab Hanna Sawalha [2021]. Näkemyksiä liiketoiminnan jatkuvuudesta ja katastrofien jälkeisestä palautumisesta. International Journal of Emergency Services

LIITTEET

SYLLABUSMALLI

MODUULIN KUVAUS

Moduulin nimi	Moduulin koodi
...	

Luennoitsija(t)	Laitos tai osasto, jossa moduuli järjestetään
...	...

Opetustapa	Kieli
Kasvokkain, verkossa, yhdistelmä, konsultaatiot	*Englanti, ...*

Edellytykset
...

Myönnettyjen ECTS-opintopisteiden määrä	Opiskelijan työmäärä	Yhteistyötyöskentely	Itsenäinen opiskelu
3	...	...	...

Moduulin tarkoitus ja tulokset		
...		
Moduulin oppimistulokset	**Opetus- ja oppimismenetelmät**	**Arviointimenetelmät**

Resurssien (laitteet, ohjelmistot, teknologia) hankkiminen
...

Moduulin sisältö: aiheiden jakautuminen	Yhteydenpitotyötunnit					Yksilölliset työajat ja tehtävät	
	Luennot (korkeakoulu)	Konsultaatiot	Harjoitukset (korkeakoulu)	Kokeet	**Kaikki kontaktiopetu**	**Yksilöllinen työ**	**Tehtävät**
1							
...							
n							
Yhteensä							

Arviointistrategia	Vertaileva painoprosentti	Arviointikriteerit
Itsearviointi I		...
...		...
Itsearviointi n		...
Tietojen arviointitesti		...

Tutkimusmateriaali *(Sukunimi, etunimen alkukirjain. (Vuosi, kuukausi, päivä). Artikkelin nimi. Lehden/aikakauslehden/sanomalehden nimi, volyyminumero (numeronumero), koko artikkelin sivunumerot, kustantaja, URL)*
Pakollinen kirjallisuus
...
Suositeltava kirjallisuus
...

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