Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa -hanke

Pilotti kevät 2025

Työpaja: Kyberturvallisuus lääkinnällisissä laitteissa (1 op)

Mikael Soini
Metropolia Ammattikorkeakoulu Oy
10.04.2025

Sisältö

1. Yleistä opintojaksosta

Tavoitteet: Opintojakson tavoitteena on tutustua lääkinnällisten laitteiden kyberturvallisuuteen terveydenhuollon ympäristössä, omaksua kyberturvallisuuteen liittyviä tärkeitä termejä ja käsitteitä, oppia tekemään uhkamallinnusta ja integroimaan kyberturvallisuusnäkökulmia ISO 14971 -perusteiseen riskinhallintaan.

Sisältö: Opintojakso koostuu työpajaan valmistavasta ennakkotehtäväpaketista ja yhden työpäivän mittaisesta työpajasta. Opintojakson laajuus on 1 op (26,7 h). Ennakkotehtävät suoritetaan ennen työpajaa. Työpajassa analysoidaan Case-esimerkin avulla lääkinnällisen laitteen kyberturvallisuutta ja liitetään se ISO 14971 -perusteiseen riskinhallintaan. Työpaja toteutetaan kampuksella.

Arviointi: Opintojakso arvioidaan asteikolla Hyväksytty/Hylätty. Hyväksytty suoritus tarkoittaa, että opiskelija on tehnyt ennakkotehtäväpaketin kokonaan ja osallistunut aktiivisesti työpajaan.

Esitietovaatimukset: Perustiedot ja -taidot lääkinnällisistä laitteista ja niiden riskinhallinnasta.

2. Johdanto

Kyberturvallisuus on tärkeää terveydenhuollossa, koska se suojaa potilastietoja ja varmistaa hoidon jatkuvuuden. Terveydenhuollon organisaatiot käsittelevät suuria määriä arkaluonteista tietoa, kuten potilastietoja, jotka ovat houkutteleva kohde kyberrikollisille. Viime vuosina kyberhyökkäykset ovat lisääntyneet merkittävästi, ja ne ovat aiheuttaneet vakavia häiriöitä terveydenhuollon palveluissa. Kyberhyökkäykset, kuten kiristyshaittaohjelmat ja tietomurrot, voivat johtaa potilastietojen varastamiseen ja väärinkäyttöön. Lisäksi hyökkäykset voivat häiritä sairaaloiden toimintaa, mikä voi johtaa hoidon viivästymiseen ja potilasturvallisuuden vaarantumiseen. Terveydenhuollon organisaatioiden on investoitava kyberturvallisuuteen. Tämä sisältää tehokkaiden tietoturvakäytäntöjen ja -teknologioiden käyttöönoton sekä henkilöstön kouluttamisen kyberturvallisuusuhkien tunnistamiseksi ja torjumiseksi. Kyberturvallisuuden parantaminen ei ainoastaan suojaa potilastietoja, vaan myös vähentää taloudellisia menetyksiä ja parantaa potilasturvallisuutta.

Kyberturvallisuus on myös kriittinen tekijä lääkinnällisten laitteiden valmistajille, koska se suojaa sekä potilastietoja, että laitteen toimivuutta. Lääkinnälliset laitteet ovat yhä useammin yhteydessä internetiin ja sairaalaverkkoihin, mikä lisää niiden alttiutta kyberhyökkäyksille. Kyberhyökkäykset voivat vaarantaa potilasturvallisuuden, aiheuttaa laitteiden toimintahäiriöitä ja johtaa merkittäviin tietovuotoihin. Lääkinnällisten laitteiden valmistajien on otettava kyberturvallisuus huomioon koko laitteen elinkaaren ajan, suunnittelusta aina markkinoille saattamiseen ja ylläpitoon asti. Tämä sisältää uhkien jatkuvan seurannan ja haavoittuvuuksien nopean korjaamisen. Kyberturvallisuuden laiminlyönti voi johtaa laajoihin laitepalautuksiin, maineen menetykseen ja sääntelyviranomaisten antamiin sanktioihin. Lisäksi potilaiden luottamus lääkinnällisiin laitteisiin ja niiden valmistajiin voi heikentyä, jos laitteiden turvallisuutta ei pystytä takaamaan. Lääkinnällisten laitteiden valmistajien on investoitava kyberturvallisuuteen suojatakseen potilaita ja varmistaakseen laitteiden turvallisen ja tehokkaan käytön. Tämä edellyttää mm. kattavaa kyberturvallisuusuhkien mallintamista, riskienhallintaa ja tiivistä yhteistyötä terveydenhuollon organisaatioiden kanssa.

3. Ennakkotehtävä: Valmistautuminen työpajaan

Tutustu seuraaviin osiin 1–8. Jokaiseen osaan liittyy materiaalia ja tehtäviä. Tee tehtävät yhteen dokumenttiin.

Osa 1: Kyberturvallisuuden lukuja

HIPAA Journalin verkkosivulla (https://www.hipaajournal.com/healthcare-cybersecurity/) esitetään 50+ faktaa ja tilastoa Yhdysvaltojen terveydenhuoltoalan kyberturvallisuuden tilasta. Tutustu lukuihin.

***Tehtävä**: listaa viisi (5) sinun mielestäsi mielenkiintoisinta lukua. Perustele lyhyesti.*

Osa 2: Kyberturvallisuuden näkökulmia

Seuraavissa FDA:n (U*.S. The Food and Drug Administration*) videoissa käsitellään eri osapuolien näkökulmia kyberturvallisuuteen liittyen.

- Terveydenhuollon organisaatiot (videon kesto 3:12): https://www.youtube.com/watch?v=YLyPo4vUytQ
- Lääkäri (videon kesto 3:12): https://www.youtube.com/watch?v=oxLbTPdtsLI
- Potilas (videon kesto 4:29): https://www.youtube.com/watch?v=TU1w6fQ-yf8

***Tehtävä**: Tiivistä lyhyesti videoiden keskeinen sisältö 1) terveydenhuollon organisaation, 2) lääkärin ja 3) potilaan näkökulmasta.*

Osa 3: Tieto-omaisuus

Tänä päivänä terveydenhuollon ympäristössä on valtavasti tietoon liittyvää omaisuutta (*asset*), jotka ovat välttämättömiä niiden toiminnalle ja siksi ne on suojattava. Näihin kuuluvat esimerkiksi mobiililaitteet, tunnistusjärjestelmät ja kliiniset tietojärjestelmät.

***Tehtävä**: ENISA on EU:n virasto, jonka tehtävänä on saavuttaa korkeatasoinen ja yhteinen kyberturvallisuuden taso kaikkialla Euroopassa. Tutustu ENISA:n raportin (https://www.enisa.europa.eu/sites/default/files/publications/Smart%20Hospitals.pdf) lukuun 2.2 (s. 13–17) ja listaa mielestäsi viisi (5) oleellisinta tieto-omaisuutta terveydenhuollossa.*

Osa 4: Haavoittuvuudet

Kyberturvallisuuden sanasto (https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf) määrittelee haavoittuvuuden alttiudelle tietoturvaan kohdistuville uhkille. Kyseisen sanaston mukaan haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuus voi liittyä teknisiin järjestelmiin, erilaisiin toimintaprosesseihin tai ihmisten toimintaan. Erityisesti IoT:n käyttö terveydenhuollossa tuo mukanaan vakavia haavoittuvuuksia.

***Tehtävä**: Tutustu ENISA:n raportin (https://www.enisa.europa.eu/sites/default/files/publications/Smart%20Hospitals.pdf) lukuun 3.1 (s. 18–20) ja listaa mielestäsi viisi (5) oleellista haavoittuvuutta IoT-laitteisiin liittyen.*

Osa 5: Uhkat ja uhka-analyysi

Kyberturvallisuuden sanasto (https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf) määrittelee kyberuhkan mahdollisesti toteutuvaksi haitalliseksi kybertoimintaympäristöön kohdistuvaksi

tapahtumaksi, joka toteutuessaan vaarantaa siitä riippuvaisen toiminnon. Kybertoimintaympäristöllä tarkoitetaan yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvaa toimintaympäristöä.

Terveydenhuollon ympäristössä uhkien perimmäisiä syitä ovat pahantahtoiset toimet (*malicious actions*), inhimilliset virheet (*human errors*), järjestelmäviat (*system failures*), luonnonilmiöt (*natural phenomena*) ja toimitusketjussa tapahtuvat virheet (*supply chain failure*).

***Tehtävä**: Tutustu ENISA:n raportin (https://www.enisa.europa.eu/sites/default/files/publications/Smart%20Hospitals.pdf) lukuun 3.2 (s. 20–29) ja selitä lyhyesti, mitä seuraavilla termeillä tässä yhteydessä tarkoitetaan:*

- *Pahantahtoiset toimet (malicious actions)*
- *Inhimilliset virheet (human errors)*
- *Järjestelmäviat (system failures)*
- *Luonnonilmiöt (natural phenomena)*
- *Toimitusketjussa tapahtuvat virheet (supply chain failure)*
- *Uhkatoimijat (threat actors)*
- *Hyökkäysvektorit (attack vectors)*
- *Hyökkäysrajapinnat (attack surfaces)*

Osa 6: Hyökkäysskenaariot

Hyökkäysskenaariot kuvaavat erilaisia tapoja, joilla hyökkääjä voi yrittää tunkeutua järjestelmään tai verkkoon. Ne sisältävät hyökkääjän tavoitteet, kuten tietojen varastamisen tai järjestelmän lamauttamisen, sekä käytetyt menetelmät, kuten haittaohjelmat tai tietojenkalastelun. Hyökkäysskenaariot tunnistavat järjestelmän haavoittuvuudet, joita hyökkääjä voi hyödyntää.

Tutustu *ENISA:n* raportin (https://www.enisa.europa.eu/sites/default/files/publications/Smart%20Hospitals.pdf) lukuun 4 (s. 30–44), missä kerrotaan viisi esimerkkiä hyökkäysskenaarioista (attack scenarios) terveydenhuoltoon. Skenaariot:

1. Sairaalan henkilökuntaan kohdistunut Social engineering -hyökkäys
2. Lääkinnällisten laitteiden peukalointi
3. Sairaalalaitteiden varastaminen
4. Ransomware-hyökkäys sairaalan tietojärjestelmiin
5. Hajautettu palvelunestohyökkäys sairaalan palvelimelle.

***Tehtävä**: Tiivistä skenaarioista lyhyt kuvaus mallipohjassa annettuun taulukkoon.*

Tämän jälkeen tutustu USA:n Department of Health & Human Services raportin (https://405d.hhs.gov/Documents/HICP-Main-508.pdf) lukuun 4 (s. 16–31), missä kerrotaan viisi hieman samanlaista esimerkkiä liittyen kyberturvallisuusuhkiin. Raportti:

1. Social engineering -hyökkäys
2. Ransomware-hyökkäys
3. Laitteiden tai tietojen katoaminen tai varastaminen
4. Sisäpiirin tahaton tai tahallinen tietojen menetys.
5. Hyökkäykset verkkoon liitettyjä lääkinnällisiä laitteita vastaan, jotka voivat vaikuttaa potilasturvallisuuteen.

***Tehtävä**: Tiivistä kyberturvallisuusuhat lyhyesti mallipohjassa annettuun taulukkoon.*

Osa 7: Lainsäädännön näkökulmia

NIS2- eli kyberturvallisuusdirektiivin (https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi) tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa valittujen kriittisten sektoreiden osalta.

Suomessa hallituksen esitys NIS2-direktiivin täytäntöön panevasta kansallisesta kyberturvallisuuslaista on paraikaa eduskunnan käsittelyssä.

Tutustu Fimea kyberturvallisuussivuihin: https://fimea.fi/valvonta/kyberturvallisuuden-ja-hairionsietokyvyn-valvonta/kyberturvallisuus

***Tehtävä**: Vastaa seuraaviin väittämiin (Totta vai tarua):*

1. *Kansallinen kyberturvallisuuslaki koskee suuria lääkinnällisten laitteiden valmistajia*
2. *Kyberturvallisuuslaki tuo ilmoittautumisvelvoitteen Fimean toimijaluetteloon*
3. *Kyberturvallisuuslaki tuo kyberturvallisuuden riskienhallintavelvoitteet toimijoille*
4. *Kyberturvallisuuslaki tuo kyberturvallisuuden raportointivelvoitteet*
5. *Riskienhallintavelvoitteet liittyvät viestintäverkkojen ja tietojärjestelmien turvallisuuteen*
6. *Ilmoitus merkittävästä poikkeamasta tehdään Fimealle*
7. *Merkittävällä poikkeamalla tarkoitetaan esimerkiksi poikkeamaa, joka on aiheuttanut vakavan palvelujen toimintahäiriön tai huomattavia taloudellisia tappioita asianomaiselle toimijalle*
8. *Ensi-ilmoitus on tehtävä 48 tunnin kuluessa poikkeaman havaitsemisesta*

Osa 8: Standardit ja menetelmät

Team-NB pyrkii aktiivisesti lisäämään ilmoitettujen laitosten avoimuutta Euroopassa. Tässä heidän kannanottonsa kyberturvallisuuteen liittyen: https://www.team-nb.org/wp-content/uploads/2022/10/Team-NB-PositionPaper-CyberSecurity-V1-20221005.pdf

***Tehtävä**: Tutustu STRIDE-malliin (*https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf*, luku 2.4.1). Suomenna taulukon 2 1. sarake (jätä englanninkielinen termi mukaan), suomenna 2. sarake ja tee suomenkielinen esimerkki sarakkeeseen 3 (voi olla sama esimerkki kuin lähteessä tai oma esimerkki).*

4. Työpaja

Johdanto

Työpajan tavoitteena on Case-esimerkin kautta tutustua lääkinnällisten laitteiden kyberturvallisuuteen ja liittää se lääkinnällisten laitteiden ISO 14971-perusteiseen riskinhallintaan. Tämän työpajan rakenteen suunnittelussa on hyödynnetty Cleion ”*Enhancing Medical Device Cybersecurity with the STRIDE Threat Model*” -artikkelia (https://cleio.com/insights/blog/stride-threat-model-medical-device-cybersecurity/).

Työpaja tehdään pienryhmässä. Työpajaan on varattu aikaa klo 9–16. Aikatauluttakaa päivän kulku siten, että työt ovat valmiina ja dokumentoituna viimeistään klo 16, tauot ja lounas sopiviin kohtiin. Opettaja ohjaa työskentelyä. Dokumentoikaa eri osien tuotokset yhteen dokumenttiin.

Työpajassa ***tulee*** käyttää apuna tekoälyä.

Osa 1: Tuotteen määrittely

ICD (Implantable Cardioverter-Defibrillator) on lääkinnällinen laite, joka asennetaan potilaan rintaan. Se seuraa jatkuvasti potilaan sydämen rytmiä ja antaa sähköiskun, jos se havaitsee hengenvaarallisen rytmihäiriön, kuten kammiovärinän tai nopean kammiotakykardian. ICD-laitteet ovat erityisen hyödyllisiä henkilöille, joilla on suuri riski hengenvaarallisiin rytmihäiriöihin, kuten kammiotakykardiaan tai kammiovärinään. ICD-laitteet voivat myös tallentaa tietoja sydämen toiminnasta ja lähettää nämä tiedot etäseurantajärjestelmään, mikä mahdollistaa reaaliaikaisen seurannan ja laitteen ohjelmoinnin.

Tehtävä: Tutustu case-esimerkkiin Medtronic: Azure MRI SureScan ja tee käyttötarkoituksen määrittely.

Tietolähteitä:

- Medtronic, Verkkosivu: https://www.medtronic.com/en-us/healthcare-professionals/products/cardiac-rhythm/pacing-systems/pacemakers/azure-mri-surescan-pacemaker.html
- Medtronic, Verkkosivu: https://europe.medtronic.com/content/dam/medtronic-com/01_crhf/brady/pdfs/product-azure-brochure.pdf
- Medtronic, Verkkosivu: kts. Manuaalit Medtronic, Contact and support -osiosta

Osa 2: Kyberturvallisuusongelmat

ICD-laitteiden kyberturvallisuus on erityisen tärkeää, koska mahdolliset ongelmat kyberturvallisuudessa vaikuttavat mm. potilasturvallisuuteen, tietosuojaan ja tiedon luotettavuuteen.

Tehtävä: Tutustutaan yleisesti ICD-laitteiden kyberturvallisuusongelmiin. Tutustu raportoituihin tahdistimiin liittyviin kyberturvallisuusongelmiin. Merkitse lähteet.

Tietolähteitä:

- Pubmed: https://pubmed.ncbi.nlm.nih.gov/
- AHA Journal, Implantable Cardioverter-Defibrillator–Cybersecurity: https://www.ahajournals.org/doi/10.1161/CIRCEP.119.008261
- Journal of the American College of Cardiology, Cybersecurity for Cardiac Implantable Electronic Devices–What Should You Know?: https://pmc.ncbi.nlm.nih.gov/articles/PMC8418792/

Osa 3: Käyttötapaukset

Ymmärtämällä, miten tuotetta käytetään, ketkä tuotetta käyttävät ja missä tilanteissa, voidaan tunnistaa mahdolliset tuotteen käyttöön liittyvät haavoittuvuudet ja uhat. Käyttötapaukset auttavat hahmottamaan, millä tavoin hyökkääjät voivat yrittää käyttää tuotetta hyväkseen.

Tehtävä: Määritellään valitulle tuotteelle realistisia käyttötapauksia.

Osa 4: Tieto-omaisuus

Tieto-omaisuus on organisaation infrastruktuurin resurssi, jota on suojeltava sen arvon vuoksi. Tällaisia ovat mm. digitaalinen data, fyysiset asiakirjat sekä työntekijöiden tiedot ja taidot. Niiden arvo altistaa ne erilaisille uhkille ja riskeille, kuten luvattomalle käytölle, tietomurroille, haittaohjelmahyökkäyksille, järjestelmähäiriöille ja muille kyberuhkille.

Tehtävä: Tunnista ja dokumentoi ICD-laitteeseen liittyvä tieto-omaisuus.

Tietolähteitä: kts. Osa 1

Osa 5: Tietovirtakaavio

Tietovirtakaavio (DFD, Data Flow Diagram) tarjoaa visuaalisen esityksen siitä, miten data liikkuu järjestelmässä. Tämä auttaa ymmärtämään, missä ja miten dataa käsitellään, tallennetaan ja siirretään. Kun tiedetään, miten data virtaa järjestelmässä, voidaan helpommin tunnistaa mahdolliset haavoittuvuudet ja uhat. Tietovirtakaavio helpottaa kommunikaatiota sidosryhmien välillä, kuten kehittäjien, tietoturva-asiantuntijoiden ja liiketoimintajohdon.

Tehtävä: Piirrä järjestelmän tietovirtakaavio. Jaa järjestelmä pienempiin osiin, kuten moduuleihin tai palveluihin.

Vinkkejä tietovirtakaavion piirtämiseen:

1. Määritä järjestelmän rajat: Aloita määrittämällä, mitä järjestelmä kattaa ja mitkä ovat sen rajat. Tämä auttaa keskittymään olennaisiin osiin ja välttämään tarpeettoman monimutkaisuuden.
2. Tunnista pääkomponentit: Määritä järjestelmän pääkomponentit, kuten tietovarastot, prosessit ja ulkoiset toimijat (esim. käyttäjät tai muut järjestelmät).
3. Käytä selkeitä symboleja: Käytä standardoituja symboleja, kuten ympyröitä prosesseille, suorakulmioita tietovarastoille ja nuolia tietovirroille. Tämä tekee kaaviosta helposti luettavan ja ymmärrettävän.
4. Määritä tietovirrat: Piirrä nuolia kuvaamaan, miten data liikkuu järjestelmän eri osien välillä. Merkitse nuoliin, mitä tietoa siirretään ja mihin suuntaan.
5. Pidä kaavio yksinkertaisena: Vältä liiallista monimutkaisuutta. Kaavion on tarkoitus olla selkeä ja helposti ymmärrettävä. Jos kaavio alkaa näyttää liian monimutkaiselta, harkitse sen jakamista useampaan osaan.
6. Käytä selkeitä nimiä: Anna prosesseille, tietovarastoille ja tietovirroille selkeät ja kuvaavat nimet. Tämä auttaa ymmärtämään kaavion sisältöä ilman lisäselvityksiä.
7. Käytä työkaluja: Hyödynnä kaavion piirtämiseen tarkoitettuja työkaluja, kuten Microsoft Visio, Lucidchart tai muita kaavioiden piirtämiseen tarkoitettuja ohjelmistoja.

Tietolähteitä:

- Osat 1 ja 4
- Cleio, Verkkosivu: https://cleio.com/insights/blog/stride-threat-model-medical-device-cybersecurity/

Osa 6: Hyökkäyspinnat

Hyökkäyspinnalla tarkoitetaan kaikkia mahdollisia kohtia, joissa hyökkääjä voi yrittää päästä käsiksi järjestelmään tai laitteeseen ja aiheuttaakseen vahinkoa. Tämä voi sisältää esimerkiksi ohjelmistojen haavoittuvuudet, verkkoportit, käyttäjätilit ja fyysiset pääsypisteet.

Tehtävä: Määritä hyökkäyspinnat (attack surfaces).

Tietolähteitä:

- Cleio, Verkkosivu: https://cleio.com/insights/blog/stride-threat-model-medical-device-cybersecurity/

Osa 7: Kyberturvallisuusanalyysi

Kyberturvallisuusanalyysissa arvioidaan potentiaaliset kyberturvallisuusriskit kaikkien järjestelmän kautta kulkevien tietojen osalta.

Tehtävä: Tunnista mahdolliset uhat. Käytä STRIDE-mallia mahdollisten uhkien ja haavoittuvuuksien tunnistamiseen.

Termejä:

- Hyökkäysskenaario on uhkatyyppiin (STRIDE) sovellettava hyökkäystyyppi. Samalle uhkatyypille voi olla useita mahdollisia hyökkäysskenaarioita, joilla kullakin on erilaiset vaikutukset. Tällöin kullekin skenaariolle olisi oltava oma rivinsä matriisissa.
- Tapahtumien kulku -sarakkeessa esitetään korkean tason kuvaus hyökkäyksen kulusta.
- Vaikutus (Impact): Mikä on vaikutus toiminnallisuuteen, järjestelmän suorituskykyyn, käyttäjätietoihin, potilaaseen tai järjestelmän käytettävyyteen?

Tietolähteitä:

- Cleio, Verkkosivu: https://cleio.com/insights/blog/stride-threat-model-medical-device-cybersecurity/

STRIDE-malli:

STRIDE-elementit	**Selitys**	**Hyökkäysskenaario***
Väärennys	Järjestelmän huijaaminen uskomaan, että väärennetty asia on todellinen.	Hyökkääjä voi varastaa käyttäjän salasanan ja kirjautua hänen tililleen.
Peukalointi	Järjestelmän tarkoituksellinen muuttaminen luvattomalla tavalla	Hyökkääjä voi siepata ja muokata verkossa kulkevia tietoja
Kieltäminen	Toteutetun toimen aitouden kiistäminen	Hyökkääjä voi muokata järjestelmän lokitietoja peittääkseen toimintansa.
Tietojen luovutus	Tietojen paljastuminen, joihin on tarkoitus soveltaa rajoitettua käyttöoikeustasoa	Hyökkääjä antaa luvattomalle käyttäjälle pääsyn arkaluontoisiin tietoihin
Palvelunesto	Järjestelmän laillisen käytön tai toiminnallisuuden estäminen haitallisten prosessien toimesta.	Hyökkääjä tulvii järjestelmän liiallisilla pyynnöillä, mikä tekee sen saavuttamattomaksi.
Etuoikeudennosto	Pääsy toimintoihin, joihin hyökkääjällä ei normaalisti saisi olla pääsyä tuotteen turvallisuuspolitiikan mukaan.	Hyökkääjä varastaa kirjautumistiedot ja käyttää niitä järjestelmän pääsyyn korkeammilla oikeuksilla

Osa 8: Riskianalyysi

Riskianalyysi on kriittinen osa lääkinnällisten laitteiden turvallisuutta. Riskianalyysi auttaa tunnistamaan ja arvioimaan mahdollisia vaaroja, jotka voivat vaikuttaa potilaan turvallisuuteen. Riskianalyysi auttaa myös varmistamaan, että laitteet täyttävät lääkinnällisiä laitteita koskevat vaatimukset. Käytännössä tuotteita Euroopan markkinoille tekevät yritykset hyödyntävät riskinhallintaan (riskianalyysiin) ISO 14971 -standardia.

Tehtävä: Tehdään kyberturvallisuusanalyysin perusteella riskianalyysi kyberturvallisuusongelmille. Pohditaan lisäksi riskien hyväksyttävyyttä. Kts. ISO 14971: luku 5–6.

Osa 9: Riskinvalvonta

Riskianalyysissä löydetyt riskit tulee poistaa tai niitä tulee vähentää. Kehitä riskeille riskinvalvontatoimenpiteet. Tämä voi sisältää esimerkiksi pääsynvalvonnan parantamista tai tietojen salaamista.

Tehtävä: Tehdään riskianalyysin ja riskien hyväksyttävyyden perusteella ratkaisut riskien vähentämiseen tai poistamiseen. Kts. ISO 14971: luku 7.

Osa 10: Yhteenveto ja palaute

Kiitos osallistumisestasi kurssille! 😊

Arvostamme palautettasi.