CyberCare Kymi

Kyberharjoitusten simulaatioympäristö

Janine Klauenbösch

XAMK Kaakkois-Suomen ammattikorkeakoulu
KYMEN LAAKSON LIITTO
Euroopan unionin osarahoittama
CyberCare Kymi

Sisällysluettelo

Konsepti on tuotettu CyberCare Kymi -hankkeessa, jota rahoitti Kymenlaakson liitto Euroopan unionin Oikeudenmukaisen siirtymän rahastosta (JTF).

Termien ja lyhenteiden sanasto

Lyhenne	Selite
HTV	Henkilötyövuosi (HTV) / työpanos
KPI	Keskeinen suorituskykymittari (Key Performance Indicator)
ICT	Tieto- ja viestintäteknologia (Information and Communication Technology)
NIS2	EU:n verkko- ja tietojärjestelmien turvallisuusdirektiivi (NIS2)
SOC	Turvavalvomo / tietoturvavalvomo (Security Operations Center)
DoS / DDoS	Palvelunestohyökkäys ((Distributed) Denial of Service)
EHR / EMR	Sähköinen potilas-/terveystietojärjestelmä (Electronic Health / Medical Record)
ELY	Elinkeino-, liikenne- ja ympäristökeskus
ESR+	Euroopan sosiaalirahasto +
EAKR	Euroopan aluekehitysrahasto
H2020 / Horizon Europe	Horisontti 2020 / Horisontti Eurooppa
HVA	Hyvinvointialue
STM	Sosiaali- ja terveysministeriö
THL	Terveyden ja hyvinvoinnin laitos

Yhteenveto

Tässä konseptissa ehdotetaan kattavaa kyberturvallisuuden harjoitusekosysteemiä Suomen sosiaali- ja terveydenhuoltosektorille. Se yhdistää kolme toisiaan täydentävää koulutuspolkua:

- Polku A: VirtualLab-kybersimulaatiot (tekniset harjoitukset)
- Polku B: Työpöytäharjoitukset (ei-tekninen päätöksenteko)
- Polku C: Mini-Sairaala-kybersimulaatio (monialainen, todentuntuinen harjoittelu)

Alkuperäinen tarkoitus oli ankkuroida ohjelma Mini-Sairaala-ympäristöön. Kehitystyön aikana kuitenkin VirtualLab- ja työpöytäharjoitusalustat nousivat esiin skaalautuvina, kustannustehokkaina vaihtoehtoina, jotka tarjoavat korkean pedagogisen arvon ilman kampusrakenteiden muutostarpeita.

Mini-Sairaala-polku on innovatiivinen, mutta siihen liittyy merkittäviä fyysisen infrastruktuurin investointeja — verkkokaapelointeja, simulaatiotilojen integrointia ja erikoislaitteistoa. Pitkän aikavälin kannattavuus edellyttäisi 30–40 organisaation vuotuista osallistumista, mikä on epätodennäköistä ottaen huomioon olennaisten yritysten alueellisen tiheyden. Ilman tätä volyymia investointi ei välttämättä olisi kestävä.

Sen sijaan VirtualLab- ja työpöytäharjoituskokonaisuudet voivat tarjota tehokasta koulutusta kannettavien tietokoneiden, siirrettävien laitepakkausten ja etäohjauksen avulla. Ne mahdollistavat kansallisen skaalauksen, vaativat pienemmät jatkuvat kustannukset ja mukautuvat ketterämmin kehittyviin uhkiin ja sääntelyyn. Jotta ratkaisu olisi kuitenkin täysin toimiva, alustojen luotettavuuteen, skenaariokehitykseen ja fasilitointikyvykkyyteen tarvitaan alkuinvestointeja.

Kolmen polun malli on teknisesti toteuttamiskelpoinen ja pedagogisesti vahva. Käytännöllisyyden ja taloudellisuuden näkökulmasta suositellaan kuitenkin VirtualLab- ja työpöytäharjoitusalustojen kehittämisen priorisointia, ja Mini-Sairaala-harjoitusten laajentamista myöhemmässä vaiheessa, mikäli tarve ja resurssit sen mahdollistavat. Tällainen vaiheittainen eteneminen varmistaa varhaisen vaikuttavuuden, pitkän aikavälin joustavuuden ja kestävän toiminnan kansallisen varautumisen tavoitteiden mukaisesti.

Osa 1: Konsepti ja arvolupaus

Tavoite ja perusteet

Konseptin tavoitteena on kaventaa merkittävää harjoitteluvajetta Suomen sosiaali- ja terveydenhuoltosektorilla tarjoamalla saavutettavaa, skaalautuvaa ja realistista kyberharjoittelua kaiken kokoisille organisaatioille – yksinyrittäjistä keskisuuriin yrityksiin.

Miksi tämä on tärkeää

Kyberuhat tällä sektorilla kasvavat nopeasti Enisan uhkakuvaston mukaan (Abad ym. 2023, 3–4). Noin puolet kaikista alan kyberhyökkäyksistä on kiristyshaittaohjelmahyökkäyksiä. Silti useimmilta palveluntuottajilta – erityisesti pieniltä ja mikroyrityksiltä – puuttuvat resurssit tai mahdollisuudet harjoitella kyberhäiriötilanteita. Nykyiset vaihtoehdot, kuten Jyväskylässä sijaitseva kansallinen kyberharjoitusalusta (Jyvsectec), ovat usein kalliita, ylikuormitettuja ja suunnattu suuremmille organisaatioille.

Tavoitteemme

Vahvistaa sosiaali- ja terveydenhuollon organisaatioiden kyvykkyyttä ja itsevarmuutta kyberhäiriötilanteisiin vastaamisessa:

- Tarjoamalla edullisia, selaimessa toimivia harjoituksia, jotka on räätälöity eri kokoisille organisaatioille
- Mahdollistamalla käytännönläheisen, skenaarioihin perustuvan harjoittelun, joka tukee NIS2-vaatimustenmukaisuutta
- Hyödyntämällä olemassa olevia alustoja ja kumppanuuksia kustannusten minimoinniksi ja päällekkäisyyksien vähentämiseksi

Vahvalle pohjalle rakennettu

Ratkaisu perustuu kahteen EU-rahoitteiseen hankkeeseen – CyberCare Kymi ja Kyberturvan tulevaisuus Kymenlaaksossa – joissa harjoituksia pilotoitiin menestyksekkäästi laajan joukon palveluntuottajia, mukaan lukien sosiaali- ja terveydenhuollon toimijat, kanssa. Lisäksi konsepti integroi Mini-Sairaala-simulaatioympäristön, jota käytetään nykyisin hoitotyön koulutuksessa, tuomalla siihen kyberhäiriöskenaarioita.

Tämä kokonaisuus mahdollistaa joustavan ja modulaarisen käyttöönoton:

- Aloita työpöytä- ja virtuaaliharjoituksilla mikro- ja pienyrityksille
- Laajenna tarvittaessa reaaliaikaiseen, monialaiseen simulaatioon
- Tue opiskelijoiden harjoittelua ammattilaisten rinnalla

Tämä konsepti varmistaa, että jopa pienimmät sosiaali- ja terveydenhuollon palveluntuottajat Suomessa saavat työkalut ja harjoittelumahdollisuuksia suojatakseen potilaitaan, järjestelmiään ja dataansa – ja luo mallin, joka voidaan skaalata valtakunnalliseen käyttöön.

Kohderyhmä ja sektorin relevanssi

Tämä koulutusjärjestelmä on suunniteltu modulaariseksi ja tasomaiseksi kokonaisuudeksi, jotta yritykset voivat osallistua niiden kokoon, toiminnan monimutkaisuuteen ja sääntelyvelvoitteisiin sopivaan harjoitteluun. Harjoitukset on tarkoitettu 1–50 työntekijän yrityksille.

Sosiaali- ja terveydenhuollon palveluntuottajat

- Yksinyrittäjät
  Terapeutit, sairaanhoitajat ja muut itsenäiset ammatinharjoittajat käsittelevät arkaluonteista tietoa, mutta heillä ei usein ole resursseja kyberturvallisuusharjoitteluun. Työpöytä- ja VirtualLab-harjoitukset tarjoavat edullisen ja helposti saavutettavan tavan harjoitella ilman kehittynyttä teknistä infrastruktuuria.
- Mikro- ja pienyritykset (1–10 työntekijää)
  Mukana ovat esimerkiksi yksityiset lääkäriasemat, kotihoidon palveluntarjoajat ja terapiaklinikat. Näillä yrityksillä ei yleensä ole omia IT-asiantuntijoita, mutta ne kohtaavat kuitenkin merkittäviä operatiivisia riskejä sekä samankaltaisia lakisääteisiä velvoitteita kuin suuret yritykset.
- Pienet–keskisuuret yritykset (11–50 työntekijää)
  Digitalisaation kasvaessa näihin organisaatioihin kohdistuu yhä kehittyneempiä kyberuhkia, vaikka niiden budjetit ovat edelleen rajalliset. Ne hyötyvät edistyneemmistä, skenaarioihin perustuvista simulaatioista, jotka on sovitettu niiden kokoluokkaan ja palvelumalliin.

Suomessa on noin 18 300 yksityistä sosiaali- ja terveysalan yritystä, joista 95 % on mikroyrityksiä, joissa on alle 10 työntekijää. (Rantakoski, 2023)

Julkinen sektori

- Hyvinvointialueet
  Hyvinvointialueet vastaavat sosiaali- ja terveyspalvelujen järjestämisestä, rahoituksesta ja tuotannosta. Harjoittelu tukee toiminnan jatkuvuutta, viranomaisyhteistyötä ja NIS2-vaatimusten täyttämistä.
- Kansalliset viranomaiset ja valvontatahot
  Poliittiset ja valvovat organisaatiot varmistavat, että harjoitukset tukevat

kansallisia strategioita ja edistävät kybervalmiuden yhdenmukaistamista valtakunnallisesti.

NIS2-direktiivin mukaan monet sosiaali- ja terveysalan organisaatiot luokitellaan ”keskeisiksi” tai ”tärkeiksi” toimijoiksi. Niiltä vaaditaan riskienarviointeja, toimintasuunnitelmia ja säännöllistä henkilöstökoulutusta. (Directive (EU) 2022/2555, 85 artikla)

Jopa organisaatiot, joihin NIS2 ei suoraan sovellu, voivat silti kohdata velvoitteita hyvinvointialueiden kautta. Vuoden 2024 tietohallintolainsäädännön päivitykset toivat NIS2-pohjaisia vaatimuksia palveluntuottajille. Näitä ovat esimerkiksi varautuminen palvelunestohyökkäyksiin ja joissain tapauksissa säännölliset kyberturvallisuusauditoinnit, joita alueet edellyttävät kumppaneiltaan. (Kyberturvallisuuslaki, NIS2)

Koulutusorganisaatiot ja opiskelijat

- Sosiaali- ja terveysalan opiskelijat
  Harjoituksiin osallistuminen valmistaa opiskelijoita todellisiin tilanteisiin, joissa digitaalinen häiriö vaikuttaa asiakastyöhön. Varhainen altistuminen vahvistaa valmiutta ja tukee koko sektorin resilienssiä.
  Huolimatta sosiaali- ja terveydenhuollon nopeasta digitalisaatiosta, kyberturvallisuus ja digitaalisten järjestelmien turvallinen käyttö eivät juuri näy alan koulutusohjelmissa. Monet ammattilaiset aloittavat työuransa ilman perustietämystä tietoturvasta, vaikka heidän odotetaan käyttävän järjestelmiä turvallisesti ja vastuullisesti. Tämä lähtötasovaje vaikeuttaa turvallisten käytäntöjen omaksumista työelämässä.
- Kyberturvallisuuden ja ICT-alan opiskelijat
  Nämä opiskelijat osallistuvat harjoitusten suunnitteluun, toteuttamiseen ja fasilitointiin sekä teknisestä että prosessien näkökulmasta. Heidän roolinsa

vahvistaa teknistä ja pedagogista osaamista sekä tarjoaa käytännön kokemusta, joka yhdistää teoriaa ja työelämän tarpeita. Opiskelijoiden integrointi tukee osaajapolkuja ja pitkäaikaista kestävyyttä.

Teknologiatoimittajat ja palveluntarjoajat

- IT-yritykset ja lääkinnällisten laitteiden toimittajat
  Nämä toimijat hyötyvät, kun ne voivat testata ratkaisujaan realistisissa toimintaympäristöissä. Yhteistyö parantaa turvallisuutta, käyttökokemusta ja teknistä resilienssiä käytännössä.

Tämä laaja kohderyhmä varmistaa, että koulutusekosysteemi tukee yhteistä kybervarautumisen kulttuuria sosiaali- ja terveydenhuollon sisällä — yhdistäen julkisen ja yksityisen sektorin, ammattilaiset, opiskelijat, johtoportaan ja teknologiatoimittajat.

Keskeiset ominaisuudet

Tämä koulutusympäristö yhdistää teknisiä, strategisia ja eläytymiseen perustuvia koulutusmenetelmiä modulaariseksi kokonaisuudeksi, joka on räätälöity Suomen sosiaali- ja terveydenhuoltosektorille. Painopisteinä ovat saavutettavuus, skaalautuvuus ja todellisen maailman tilanteiden huomioiminen.

Kolmen polun harjoittelumalli

Konsepti rakentuu kolmen toisiaan täydentävän harjoittelupolun varaan, jolloin organisaatiot voivat valita juuri niiden kokoon, tekniseen kypsyyteen ja käytettävissä oleviin resursseihin sopivan tason:

- Polku A – VirtualLab: Teknisiä kyberhäiriösimulaatioita selainpohjaisella alustalla. Harjoitukset ovat realistisia, automatisoituja ja skaalautuvia – yksinyrittäjistä keskisuuriin yrityksiin.
- Polku B – Työpöytäharjoitukset: Strategisia, matalan kynnyksen pöytäharjoituksia, jotka ohjaavat osallistujia päätöksenteko- ja viestintäprosessien läpi käyttäen heidän nykyisiä valmiussuunnitelmiaan.
- Polku C – Mini-Sairaala: Paikan päällä toteutettavia, monialaisia simulaatioita kliinisistä ja IT-kriiseistä kontrolloidussa sairaalaympäristössä. Suunnattu erityisesti keskisuurille toimijoille.

Jokainen polku tukee tiettyjä rooleja (esim. hoitotyö, IT, johto) ja noudattaa voimassa olevia säädöksiä ja lakeja.

Skenaariopohjainen oppiminen

Kaikki harjoitukset perustuvat todellisiin kyberhäiriötapauksiin ja etenevät dynaamisesti:

- Sisäpiiriuhat
- Kalastelu ja kiristyshaittaohjelmat
- Lääkinnällisten laitteiden viat
- Potilastietojärjestelmien häiriöt ja tietovuodot
- Toimitusketjun vaarantuminen
- Palvelunestohyökkäykset

Jokaisessa skenaariossa on haarautuvia tapahtumapolkuja, ajastettuja syötteitä ja roolikohtaisia tehtäviä, jotka haastavat osallistujat toimimaan paineen alla ja mukauttamaan suunnitelmiaan.

Roolikohtainen osallistuminen

Harjoitukset on suunniteltu simuloimaan realistista, moniammatillista yhteistyötä:

- Hoitohenkilöstö keskittyy potilashoidon jatkuvuuteen
- IT- ja kyberturvallisuushenkilöstö hallitsee tilanteen rajaamisen ja palautumisen
- Johto vastaa julkisesta viestinnästä ja strategisesta koordinoinnista

Tämä kerroksellinen rakenne varmistaa, että organisaatiot voivat harjoitella kokonaisuuksina, eivät erillisinä osastoina.

Integroitu palaute ja kehittäminen

Harjoituksen jälkeiseen arviointiin sisältyy:

- Rakenteiset jälkipuinnit
- Suorituspalautteet
- Kehitysehdotukset
- Toimintakorttien ja valmiussuunnitelmien tarkennukset

Työkalut ovat sisäänrakennettuina sekä VirtualLab- että työpöytäharjoitusalustoihin mitattavan edistymisen tukemiseksi.

Modulaarinen, skaalautuva rakenne

- Konsepti on täysin modulaarinen – Polut A ja B toimivat itsenäisesti, mikä mahdollistaa vaiheittaisen käyttöönoton.
- Olemassa oleva infrastruktuuri ja henkilöstö pienentävät käyttöönoton kustannuksia (esim. Mini-Sairaala on jo käytössä hoitotyön opetuksessa; VirtualLab tekniikan opetuksessa).

- Sisällön jakaminen polkujen välillä takaa kustannustehokkuuden ja nopeamman skaalautuvuuden.
- Tulevaisuusvalmis: rakenne mahdollistaa laajentamisen myös muihin kriittisiin sektoreihin sosiaali- ja terveydenhuollon ulkopuolella.

Harjoittelutasot ja simulaatiokatalogi (Tasot 1–3)

Suomen sosiaali- ja terveydenhuollon toimijoiden laajan kirjon tukemiseksi harjoitusympäristö on jaettu kolmeen tasoon. Jokainen taso vastaa organisaation kokoa, toiminnan monimutkaisuutta ja kyberturvallisuuskyvykkyyttä, jotta harjoittelu olisi oikean tasoista ja skaalautuvaa.

Taso 1 – Yksinyrittäjät ja mikroyritykset

Kohderyhmä: Yksinyrittäjät ja 1–5 työntekijän yritykset

Koulutusmuoto: Täysin automatisoidut, etänä käytettävät simulaatiot VirtualLab- ja työpöytäharjoitusalustoilla

Keskeiset ominaisuudet:

- Pääsy edullisiin harjoituksiin molemmilla alustoilla
- Ei teknistä asennusta; selainpohjainen toteutus
- Ei-teknisiä skenaarioita, kuten:
    - Miten jatkan asiakkaideni hoitoa, kun potilastietoni on lukittu?
    - Kuinka tiedotan asiakkaita ja mediaa tietomurron sattuessa?
- Sisäänrakennettu ohjaus ja palaute
- Harjoitukset saatavilla 24/7
- Suunniteltu tukemaan lakisääteisiä velvoitteita ja perustietoisuuden vahvistamista

Tämä taso varmistaa saavutettavuuden ja poistaa teknisiä sekä taloudellisia esteitä pienimmiltä toimijoilta.

Taso 2 – Pienyritykset

Kohderyhmä: 6–10 työntekijän toimijat (esim. pienet klinikat, kotihoitoyksiköt)

Koulutusmuoto: Katalogipohjaiset harjoitukset, mahdollisuus lähiopetukseen

Keskeiset ominaisuudet:

- Pääsy edullisiin harjoituksiin molemmilla alustoilla
- Ei teknistä asennusta; selainpohjainen toteutus
- Skenaariot, joissa yhdistyvät ei-tekninen työpöytäharjoitus ja tekninen VirtualLab-harjoitus
- Mahdollisuus kampuksella järjestettävään VirtualLab-harjoitukseen tuen kanssa
- Ennen ja jälkeen harjoitusta tapahtuva fasilitointi sekä strukturoitu palaute ja tilanteen jälkipuinti
- Painotus monirooliseen harjoitteluun (johto, kliininen työ)
- Korostaa kyberhäiriötilanteiden toimintakyvyn kehittämistä

Tämä taso yhdistää ei-tekniset ja tekniset harjoitukset ja rakentaa valmiutta tiimitason koordinointiin.

Taso 3 – Keskisuuret yritykset

Kohderyhmä: 11–50 työntekijän yritykset (esim. keskisuuret klinikat ja kuntoutuskeskukset)

Koulutusmuoto: Hybridimalli (etänä ja paikan päällä kampuksella)

Keskeiset ominaisuudet:

- Täysi pääsy molempien alustojen katalogiin
- Mahdollisuus räätälöityihin VirtualLab- ja työpöytäharjoituksiin organisaation rakenteen mukaan
- Mahdollisuus kampuksella toteutettaviin harjoituksiin (Mini-Sairaala, VirtualLab)
- Suunnittelupalaverit, raportointi ja jälkipuinti
- Painotus eri toimintojen yhteisharjoitteluun: johto, IT ja hoitotiimit

Tämä taso tarjoaa vaikuttavampaa harjoittelua organisaatioille, joilla on monimutkaisempia järjestelmiä ja sääntelystä nousevia velvoitteita, pysyen silti kustannustehokkaana ja joustavana.

Simulaatiokatalogin kehityspolku

Taso	Alusta	Julkaisuskenaariot (V0–3)
1	VirtualLab + työpöytäharjoitus	2–3 skenaariota: ei-tekninen + kevyt tekninen
2	VirtualLab + työpöytäharjoitus	2–3 skenaariota: ei-tekninen + operatiivinen/tekninen
3	Kaikki alustat	2 skenaariota: ei-tekninen + edistynyt tekninen, + valinnainen Mini-Sairaalaskenaario

Hyödyt ja odotettu vaikuttavuus

Tämä monipolkuinen koulutusympäristö – joka perustuu VirtualLab-kybersimulaatioon ja työpöytäharjoitusalustaan sekä valinnaiseen Mini-Sairaala-simulaatioon – tuottaa mitattavaa vaikutusta kyberturvallisuusvalmiuteen, henkilöstön osaamiseen ja koko sektorin resilienssiin. Se tarjoaa inklusiivisen,

tasomallisen pääsyn realistiseen koulutukseen samalla kun se noudattaa kansallista lainsäädäntöä ja pitkän aikavälin kestävyyden tavoitteita.

Parantaa kyberresilienssiä sosiaali- ja terveydenhuollon sektorilla

- Realistiset ja turvalliset koulutusympäristöt valmistavat henkilöstöä digitaalisiin kriiseihin.
- Organisaatiot voivat testata ja kehittää jatkuvuussuunnitelmia, viestintää ja häiriötilanteiden toimintaa simuloidussa paineessa.
- Harjoitukset noudattavat voimassa olevaa lainsäädäntöä ja tarjoavat todisteen vaatimustenmukaisuudesta.
- Rakenteiset jälkipuinnit ja palaute mahdollistavat jatkuvan kehityksen ja vaiheittaisen oppimisen.

Mitattavat tulokset: keskeiset suorituskykymittarit

Koulutusympäristö on suunniteltu tuottamaan selkeitä ja seurattavia tuloksia, kuten:

Koulutetut organisaatiot / vuosi

- Vuosi 1: ~50
- Vuosi 2: ~180
- Vuosi 3: ~540
- Pitkän aikavälin tavoitetaso: tuhansia vuosittaisia käyttäjiä.

Kehitetyt harjoitukset / vuosi

- Hankkeen alussa 4 yhteiskäyttöistä harjoitusta (VirtualLab ja työpöytä)
- Vuosittain 4–6 uutta harjoitusta, mukaan lukien toimialakohtaiset ja räätälöitävät vaihtoehdot

Häiriötilannekyvykkyyden osoitettu kehittyminen

- Osallistujat tekevät ennen- ja jälkeen -arvioinnit sekä palautepisteytyksen
- Organisaatiot saavat konkreettiset raportit, jotka tukevat kyberturvallisuusvalmiuden ja riskienhallinnan kehittämistä

Tekee kyberharjoittelusta edullista ja saavutettavaa

- Hinnoittelu suhteutetaan organisaation kokoon: yksinyrittäjä voi saada 2 harjoituksen paketin 80 eurolla.
- Ei teknistä asennusta: työpöytäharjoitusalusta ja VirtualLab toimivat selaimessa.
- Etäkäyttö mahdollistaa osallistumisen kaikkialta Suomesta.
- PK-yritykset saavat käyttöönsä harjoitteluvaihtoehtoja, joita niillä ei aiemmin ole ollut – paikkaa merkittävän kansallisen kapasiteettivajeen.

Vahvistaa monialaista osaamista ja työvoimakapasiteettia

- Roolikohtainen koulutus (IT, kliininen työ, johto, hallinto) parantaa kriisiajan vuorovaikutusta ja yhteistyötä.
- Hoitotyön, kyberturvallisuuden, logistiikan ja IT-alan opiskelijat osallistuvat skenaarioiden suunnitteluun, fasilitointiin ja testaukseen.
- Tukee kansallista osaajakehitystä sisällyttämällä työelämärelevantin oppimisen koulutukseen.

Mahdollistaa valtakunnallisen mallinnuksen ja sektorilaajennukset

- Modulaarinen rakenne mahdollistaa mallin käytön myös Kymenlaakson ulkopuolella ja tukee muiden alueiden sosiaali- ja terveydenhuollon resilienssin vahvistamista.
- Kaksikäyttöskenaariot ja jaettu infrastruktuuri pienentävät kehityskustannuksia.
- Laajennettavissa helposti muihin kriittisen infrastruktuurin sektoreihin (energia, logistiikka, koulutus, ruokahuolto).

Tukee Suomen digitaalisia ja strategisia tavoitteita

- Noudattaa Suomen lainsäädäntöä ja EU-laajuisia aloitteita digitaalisen resilienssin ja julkisten palvelujen jatkuvuuden vahvistamiseksi.
- Vahvistaa julkisen ja yksityisen sektorin yhteistyötä: harjoitukset kokoavat yhteen palveluntuottajat, toimittajat, viranomaiset ja kouluttajat.
- Tukee suoraan NIS2-vaatimusten kansallista toimeenpanoa tarjoamalla konkreettisen koulutusratkaisun.

Tämä koulutusympäristö antaa jopa pienimmille organisaatioille valmiudet täyttää kyberturvallisuusvelvoitteensa – ja samalla tarjoaa laajat, skaalautuvat työkalut kypsimmille toimijoille. Modulaarisen rakenteensa, kansallisen merkityksensä ja mitattavien tulostensa ansiosta se vastaa käytännöllisesti ja kestävästi Suomen kasvaviin kyberharjoittelutarpeisiin tällä sektorilla.

Osa 2: Toteutuksen operatiivinen kokonaisuus

Tässä osassa kuvataan käytännön vaiheet, joiden avulla edetään konseptista valtakunnalliseen palvelutuotantoon. Se sisältää vaiheittaisen käyttöönoton suunnitelman, skenaariokehityksen aikataulut, infrastruktuurin rakentamisen, resursoinnin, pilotoinnit sekä arviointikriteerit. Lähestymistapa painottaa pienille toimijoille suunnatun matalan kynnyksen harjoitusten varhaista käyttöönottoa, samalla kun rakennetaan kohti Mini-Sairaala-ympäristön vaativampia, todentuntuisia simulaatioita.

Toteutusstrategia

Toteutus noudattaa vaiheittaista mallia, joka tasapainottaa nopean alkuvaikuttavuuden ja pitkäjänteisen kapasiteetin rakentamisen.

Polut A ja B voidaan käynnistää jo ensimmäisen projektivuoden aikana, tarjoten välittömiä hyötyjä yksinyrittäjille sekä mikro- ja pienyrityksille. Polku C on usean vuoden ja usean projektin kokonaisuus, joka vaatii vaiheittaisia investointeja, hankintoja ja integraatiota.

Ohjaavat periaatteet

- Nopeat onnistumiset: Matalan kynnyksen, kysytyt harjoitukset käyntiin nopeasti selainpohjaisilla alustoilla.
- Skaalautuva kasvu: Sisältöjen, ominaisuuksien ja tasojen lisääminen vaiheittain ilman käyttökatkoja.
- Jaetut resurssit: Skenaariot kehitetään siten, että niitä voidaan hyödyntää sekä työpöytäharjoitus- että VirtualLab-alustoilla kustannusten ja aikataulujen optimoimiseksi.
- Kytkentä koulutukseen: Opiskelijaprojektit ja harjoittelut osallistuvat skenaarioiden suunnitteluun, testaukseen ja fasilitointiin.

Vaihe 1 – Valmistelu ja ydinkehitys (Kuukaudet 0–6)

- Määritellään VirtualLab- ja työpöytäharjoitusalustojen päivitystarpeet (käyttöoikeudet, palaute, raportointi, maksutavat).
- Kehitetään neljä ensimmäistä jaettua harjoitusta (2 yksinyrittäjille/mikroyrityksille ja 2 pienille yrityksille).
- Aloitetaan Mini-Sairaala -järjestelmävaatimusten ja infrastruktuurin suunnittelu.
- Laaditaan viestintä- ja markkinointimateriaalit sekä hinnoittelumallit tasoille 1 ja 2.
- Käynnistetään asiakaspolut, harjoituskalenteri ja varhainen markkinointi.

Lopputulos: Selainpohjaisten harjoitusten rungon ensikäynnistys valmis; fyysisen simulaation perusta luotu.

Vaihe 2 – Alkuvaiheen käyttöönotto (Kuukaudet 6–12)

- Julkaistaan VirtualLab ja työpöytäharjoitusalusta ulkoisille asiakkaille.
- Jatketaan harjoitusten kehitystä tasoille 1 ja 2.
- Aloitetaan Mini-Sairaala -hankintaprosessi (laitteisto, ohjelmisto, integraatiopalvelut).
- Jatketaan markkinointia.

Lopputulos: Pienten toimijoiden valtakunnallisesti saavutettava kyberharjoittelu; Mini-Sairaala siirtyy rakennusvaiheeseen.

Vaihe 3 – Palvelun laajennus (Kuukaudet 12–24)

- Laajennetaan polkujen A ja B katalogia roolipohjaisilla ja toimialakohtaisilla harjoituksilla.
- Tarjotaan paikan päällä toteutettavia simulaatioita keskisuurille toimijoille.

- Asennetaan ja konfiguroidaan Mini-Sairaala -infrastruktuuri.
- Kehitetään Mini-Sairaala -harjoitus.
- Otetaan käyttöön analytiikkatyökaluja ja automaattisia arviointijärjestelmiä.

Lopputulos: Kasvava asiakaskunta; fyysisen simulaation infrastruktuuri lähes valmis, Mini-Sairaala-harjoitus suunniteltu.

Vaihe 4 – Viimeistely ja Mini-Sairaala-harjoituksen valmistuminen (Kuukaudet 24–30)

- Kerätään tekninen, pedagoginen ja osallistujapalaute poluille A ja B.
- Mukautetaan skenaarioiden vaativuutta, aikatauluja ja resursointia.
- Toteutetaan Mini-Sairaala -harjoitus; suoritetaan sisäinen opiskelijapilotti.
- Valmistaudutaan täyteen operatiiviseen käyttöönottoon.

Lopputulos: VirtualLab- ja työpöytäharjoitus -mallin toimivuus vahvistettu.

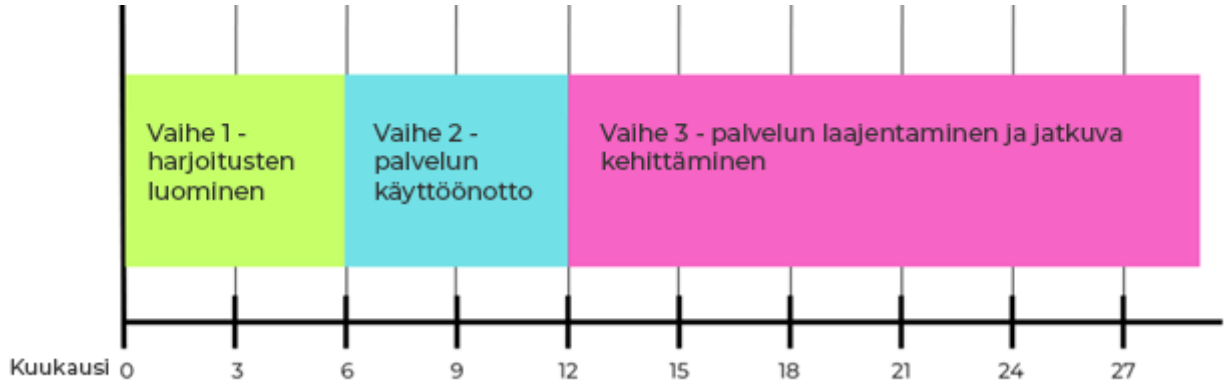
Vaihe 5 – Täysi operatiivinen kapasiteetti (Kuukaudet 30–42)

- Toteutetaan 1–2 Mini-Sairaala-pilottia ulkoisille organisaatioille.
- Mini-Sairaala integroidaan täysimääräisesti palveluvalikoimaan.
- Räätälöitävät skenaariot saatavilla kaikilla poluilla.
- Varaukset, maksut ja raportointi toimivat automaattisesti.

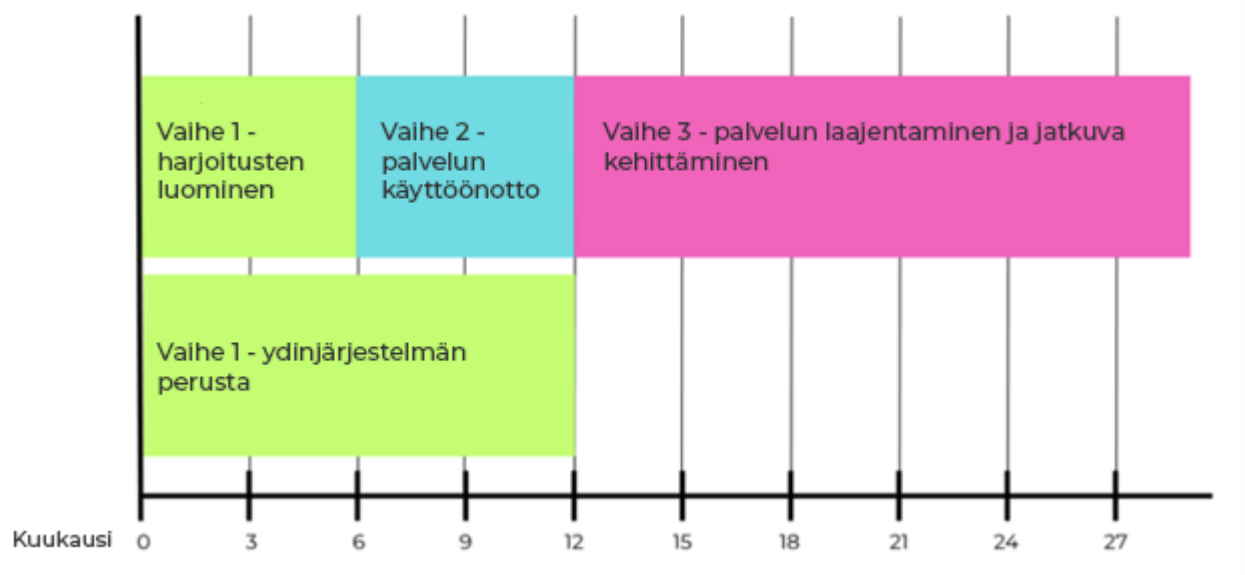
Lopputulos: Itseohjautuva, valtakunnallisesti monistettava sosiaali- ja terveydenhuollon kyberharjoitteluympäristö.

Rinnakkaiset toiminnot kaikilla alustoilla

- Jatkuva skenaariokehitys ja kaksikäyttöön sovittaminen polkujen välillä.
- Markkinointi ja uusien sektorien tavoittaminen.
- Opiskelijoiden osallistuminen kehittämiseen, fasilitointiin ja TKI-toimintaan.
- Kumppanuuksien rakentaminen viranomaisten, toimittajien ja alueellisten toimijoiden kanssa.



Kuva 1: Aikajana työpöytäharjoitusalustalle.



Kuva 2: Aikajana VirtualLab-simulaatioille.

Kuva 3: Aikajana Mini-sairaalalle.

Polku A: VirtualLab-kybersimulaatio

VirtualLab-kybersimulaatio tarjoaa realistisia kyberhäiriöharjoituksia turvallisen, selainpohjaisen alustan kautta. Se hyödyntää aiempien EU-hankkeiden (CyberCare Kymi, Kyberturvan tulevaisuus Kymenlaaksossa) kokemusta vastatakseen sosiaali- ja terveysalan mikro-, pien- ja keskisuurten yritysten välittömiin koulutustarpeisiin – yksinyrittäjistä keskisuuriin toimijoihin.

Keskeiset vahvuudet:

- Saavutettava: Ei erityislaitteita, toimii selaimessa
- Skaalautuva: Sopii yksin- ja ryhmäharjoitteluun
- Todennettu: Testattua sisältöä todellisista kyberhäiriöistä

Vaiheittainen käyttöönotto ja välitavoitteet

Vaihe & kuvaus	Välitavoitteet
Vaihe 1 – Ydinjärjestelmän perusta (kuukaudet 0–6)	• Käyttäjätodennus ja roolipohjainen käyttöoikeuksien hallinta varmistettu • Helpdesk ja UKK integroituna • Kaksi Taso 1 ja 2-harjoitusta kehitetty • Sisäinen turvallisuuskatselmus tehty

	• Yhteydenotot yksityisiin ja julkisiin sosiaali- ja terveydenhuollon toimijoihin
Vaihe 2 – Palvelun käyttöönotto (kuukaudet 6–12)	• Ensimmäiset 4 harjoitusta julkaistu automatisoidulla palautteella • Selkokieliset perehdytysmateriaalit valmiina • Ensimmäiset 10+ organisaatiota koulutettu
Vaihe 3 – Laajentuminen ja jatkuva kehittäminen (kuukaudet 12+)	• Taso 3:n kehittyneet skenaariot lisätty • Kampuksella tapahtuvan harjoittelun vaihtoehto käytössä • Analytiikan hallintapaneeli toiminnassa • 4–6 uutta harjoitusta lisätään vuosittain • Ensimmäiset räätälöidyt skenaariot toimitettu

Vaikutukset kolmannen vuoden loppuun mennessä

- Katalogi: 15–20 harjoitusta yhteensä eri tasoilla
- Koulutettuja organisaatioita vuosittain: 200+
- Uusintaosallistumisaste: ≥50 %
- Resilienssin paraneminen: ≥30 % lähtötasoon verrattuna

Polku B: Työpöytäharjoitusalusta

Työpöytäharjoitusalusta on nopeimmin käyttöönotettava kokonaisuus. Harjoitukset tarjoavat strategisia, päätöksentekoon keskittyviä kyberhäiriösimulaatioita sosiaali- ja terveydenhuollon toimijoille. Ne on suunniteltu vahvistamaan organisaatioiden valmiutta simuloimalla häiriön eskalaatiota – sisäisestä häiriöstä mediahuomioon ja palvelun jatkuvuuden haasteisiin.

Harjoitukset eivät vaadi mitään teknistä asennusta ja toimivat suoraan selaimessa, mikä tekee niistä ihanteellisen ratkaisun yksinyrittäjille ja pk-yrityksille.

Keskeiset vahvuudet:

- Ei teknisiä esteitä: Verkkopohjainen ja käyttövalmis ilman asennuksia
- Skenaariovetoinen: Päätöksenteko realistisen paineen alla
- Sääntely-yhteensopiva: Tukee pk-yritysten vaatimustenmukaisuutta
- Kaksikäyttöinen sisältö: Skenaarioita voidaan muokata VirtualLab-käyttöön, mikä pienentää kehityskustannuksia

Vaiheittainen käyttöönotto ja välitavoitteet

Vaihe & kuvaus	Välitavoitteet
Vaihe 1 – Ydinskenaarioiden kehitys (Kuukaudet 0–6)	• 2 olemassa olevaa mikroyritysten skenaariota viimeistelty • 2 uutta skenaariota pienyrityksille kehitetty • Häiriön eskalaatiomalli suunniteltu • Automaattinen raportointiformaatti luotu
Vaihe 2 – Palvelun käyttöönotto (mikro ja pienet) (Kuukaudet 6–12)	• Julkaisu yksinyrittäjille, mikro- ja pienyrityksille valtakunnallisesti • 4 skenaariota käytössä (2 olemassa olevaa, 2 uutta) • Aloitusmateriaalit ja fasilitointiohjeet valmiina • Ensimmäiset asiakasharjoitukset toteutettu
Vaihe 3 – Laajennus pk-yrityksiin (Kuukaudet 12–24)	• 4–6 uutta pk-yrityksille suunnattua skenaariota

	• Toimialakohtaiset erikoistumiset (esim. apteekit, yksityisklinikat) • Mahdollisuus yhdistettyihin työpöytä- + VirtualLab -harjoituksiin
Vaihe 4 – Katalogin jatkuva kasvu (Kuukaudet 24+)	• 4 uutta skenaariota vuosittain • Laajennus toimialakohtaisiin teemoihin (esim. vanhuspalvelut, fysioterapia) • Osallistujien tyytyväisyys ≥80 % osallistujapalautteessa

Vaikutukset kolmannen vuoden loppuun mennessä

- Katalogi: 15–20 skenaariota, jotka kattavat yksinyrittäjät, mikroyritykset ja pk-toimijat
- Koulutettuja organisaatioita vuosittain: 200+
- Uusintaosallistumisaste: ≥50 %
- Resilienssin paraneminen: ≥30 % lähtötasoon verrattuna

Polku C: Mini-Sairaala-kybersimulaatio

Mini-Sairaala-kybersimulaatio tarjoaa todentuntuista, paikan päällä toteutettavaa harjoittelua sosiaali- ja terveydenhuollon toimijoille simuloimalla realistisia kyberhäiriöitä kontrolloidussa kliinisessä ympäristössä.

Tämä koulutuspolku etenee konseptista täyteen operatiiviseen valmiuteen noin 36–42 kuukaudessa hankintaprosessien, infrastruktuurin vaativuuden ja räätälöityjen järjestelmien tarpeen vuoksi.

Keskeiset vahvuudet

- Realistinen: Todentuntuiset simulaatiot jäljittelevät todellisia kyberhäiriöitä kliinisessä ympäristössä
- Räätälöitävä: Skenaariot ja järjestelmät voidaan muokata eri organisaatioiden ja uhkatasojen mukaan
- Yhteistoiminnallinen: Mahdollistaa kliinisten, teknisten ja hallinnollisten tiimien yhteisharjoittelun

Vaiheittainen käyttöönotto ja välitavoitteet

Vaihe & kuvaus	Välitavoitteet
Vaihe 1 – Suunnittelu (Kuukaudet 0–6)	• Järjestelmävaatimukset määritelty (räätälöity potilastietojärjestelmä, tarkkailuhuoneet, automaatiotriggerit jne.) • Tilakierrokset toteutettu sidosryhmien kanssa • Riskienhallintasuunnitelma ja kustannusmalli viimeistelty
Vaihe 2 – Hankinnat (Kuukaudet 6–12)	• Laitteet, kaapelointi, verkon segmentointi ja simulaatio-ohjelmisto määritelty • Virallinen hankintaprosessi käynnistetty
Vaihe 3 – Infrastruktuurin rakentaminen (Kuukaudet 12–24)	• Fyysinen infrastruktuuri asennettu • Tarkkailuhuoneet toimintavalmiina • Simuloitu potilastietojärjestelmä ja potilasmonitorointi integroitu • Harjoituskäsikirjoitus ja walkthrough laadittu
Vaihe 4 – Pilotti (Kuukaudet 24–30)	• Mini-Sairaala -harjoituksen toteutus • Sisäinen testiskenaario opiskelijoilla

	• Valmistautuminen operatiiviseen julkaisuun • Teknisen ja pedagogisen palautteen sisäänrakentaminen • Vaikeustason kalibrointi (tekninen vikatilanne, automaatiotriggerit) • Henkilöstön koulutus
Vaihe 5 – Täysi operatiivinen käyttö (Kuukaudet 30–42)	• Teknisen, pedagogisen ja osallistujapalautteen keruu • Pilotointi oikeiden yritysten kanssa • Skenaarioiden vaativuuden, aikataulujen ja resursoinnin hienosäätö • Varaus-, perehdytys- ja analytiikkajärjestelmät aktiivisina • Räätälöidyt simulaatiot tason 3 asiakkaille käytettävissä

Rinnakkaiset jatkuvat toiminnot

- Yhteisten harjoitus- ja jälkipuintipohjien kehittäminen Mini-Sairaalalle, VirtualLabile ja työpöytäharjoitusalustalle
- Opiskelijaprojektien osallistaminen skenaariokehitykseen
- Mini-Sairaala -skenaarioiden VirtualLab-yhteensopivien versioiden rakentaminen hybridiharjoitteluun
- Yhteistyön ylläpitäminen sairaaloiden, hyvinvointialueiden ja viranomaisten kanssa

Valmiustavoite

Täysi operatiivinen valmius: noin 3–4 vuotta projektin käynnistymisestä, edellyttäen vakaata rahoitusta ja ilman merkittäviä viivästyksiä.

Valmistuessaan Mini-Sairaala toimii valtakunnallisesti monistettavana mallina immersiiviselle terveydenhuollon kyberharjoittelulle.

Pilotointi- ja arviointisuunnitelma

Tässä luvussa esitellään jokaiselle kolmelle koulutuspolulle suunniteltu pilotointi- ja arviointiprosessi. Sen sijaan, että käytettäisiin yhtä yhtenäistä mallia, pilotoinnit on sovitettu kunkin koulutuspolun kypsyystasoon ja käyttöönoton aikatauluun. Tavoitteena on varmistaa, että jokainen kokonaisuus toimii suunnitellusti, vastaa kohderyhmän tarpeisiin ja tuottaa mitattavia parannuksia sosiaali- ja terveydenhuollon kyberturvallisuusvalmiudessa.

Polkukohtaiset pilotit ja tavoitteet

Jokainen koulutuspolku käy läpi räätälöidyn pilotointivaiheen, jonka tarkoituksena on testata ydintoimintoja, tunnistaa käytettävyyshaasteita ja kerätä palautetta todellisilta käyttäjiltä kentältä.

Työpöytäharjoitusten pilotti käynnistyy projektin kuukausien 6–9 aikana. Sen tavoitteena on testata sekä fasilitointimallia että osallistujien sitoutumista harjoitusten aikana. Nämä pöytäharjoitukset korostavat päätöksentekoa paineen alla ja soveltuvat erityisen hyvin yksinyrittäjille sekä mikro- ja pienyrityksille. Pilottiryhmään kuuluu kaksi mikro- ja kaksi pientä sosiaali- ja terveydenhuollon toimijaa.

VirtualLab-kybersimulaation pilotti toteutuu pian tämän jälkeen, projektin kuukausien 9–12 aikana. Sen pääpaino on selainpohjaisen alustan teknisen vakauden varmentamisessa, käyttäjien kirjautumis- ja tunnistautumisprosessien sujuvuuden varmistamisessa sekä siinä, että skenaariot etenevät suunnitellusti automatisoidun palautteen ja raportoinnin kanssa. Pieni joukko sosiaali- ja

terveysalan pk-yrityksiä (2–3 organisaatiota tasoilta 1 ja 2) suorittaa kukin yhden tai kaksi harjoitusta, mikä tarjoaa realistisen mutta hallittavan testialustan.

Mini-Sairaala-kybersimulaation pilotti toteutetaan myöhemmin projektin aikana, kuukausien 30–36 välillä, johtuen sen monimutkaisuudesta ja fyysisen infrastruktuurin vaatimuksista. Pilotin päätavoitteena on arvioida simulaatioympäristön realismia ja käytettävyyttä, mukaan lukien tekniset järjestelmät, kuten potilasmonitorointi ja automaatiotriggerit. Pilotissa arvioidaan myös moniammatillisen tiimityön toimivuutta simuloidun kyberhäiriön aikana. Osallistujina on yksi keskisuuri sosiaali- ja terveydenhuollon organisaatio tai hyvinvointialue.

Osallistujien rekrytointi ja valinta

Pilotointivaiheen osallistujat rekrytoidaan suoralla yhteydenotolla organisaatioihin, jotka ovat jo aktiivisia Kymenlaakson verkostossa, sekä valtakunnallisten kumppanuuksien kautta esimerkiksi Suomen Yrittäjien tai alueellisten kauppakamarien kanssa.

Myös koulutusorganisaatiot osallistuvat erityisesti opiskelijoiden roolin osalta skenaarioiden testauksessa ja palautteen keruussa. Valinnassa pyritään monipuoliseen osallistujajoukkoon, joka kattaa erikokoisia ja erityyppisiä organisaatioita — yksinyrittäjistä suurempiin pk-yrityksiin — jotta pilotin tulokset ovat mahdollisimman edustavia.

Valintakriteereihin kuuluu osoitettu halukkuus sitoutua koko pilotointisykliin, mukaan lukien ennen- ja jälkeen -arvioinnit, sekä suostumus jakaa anonymisoituja toiminnallisia havaintoja, jotka voivat tukea tulevaa kehitystyötä. Lisäksi pyritään siihen, että mukana olisi osallistujia eri alueilta, jotta voidaan arvioida, kuinka hyvin etä- ja hybridimalli toimivat käytännössä.

Arviointikriteerit ja onnistumisen mittarit

Kunkin pilotin vaikuttavuutta arvioidaan teknisten, pedagogisten ja kokemuksellisten mittareiden yhdistelmällä.

Teknistä luotettavuutta mitataan järjestelmän käytettävyysasteella (tavoitteena vähintään 99 % harjoitusten aikana), kriittisten virheiden puuttumisella sekä skenaariot automatisoivan ja palautetyökaluja hyödyntävän kokonaisuuden saumattomalla toiminnalla.

Oppimistuloksia arvioidaan ennen ja jälkeen harjoitusten täytettävillä kyselyillä, ja tavoitteena on, että vähintään 75 % osallistujista kokee itseluottamuksensa kyberhäiriöihin vastaamisessa parantuneen. Lisäksi arvioijat tarkastelevat päätöksenteon kehittymistä paineen alla sekä roolien välisen yhteistyön vahvistumista simulaatioharjoituksissa.

Kumppaniorganisaatioiden palaute on keskeinen onnistumisen osoitin. Tavoitteena on vähintään 80 %:n tyytyväisyys sekä vähintään 70 %:n osallistumisaikeet tuleviin harjoituksiin. Laadullista palautetta hyödynnetään erityisesti skenaariosuunnittelun ja toteutuksen parantamisessa.

Raportointi ja iterointi

Jokaisen pilotointivaiheen jälkeen toteutetaan sisäiset tekniset ja pedagogiset arvioinnit, joiden perusteella skenaarioita tarkennetaan, käytettävyysongelmia korjataan ja kokonaiskulkuun tehdään parannuksia. Prosessi sisältää yksityiskohtaiset jälkipuinnit insinöörien, pedagogien ja simulaatiofasilitaattoreiden kesken.

Ulkoinen raportointi sisältää kvartaalittaiset raportit rahoittajille ja keskeisille sidosryhmille, joissa kuvataan edistyminen, pilotoinnin tulokset ja keskeiset havainnot. Kunkin kehitysvuoden päätteeksi julkaistaan koontiraportti, joka

sisältää datavisualisointeja, anonymisoituja osallistujakommentteja ja kehityssuunnitelman. Lisäksi julkaistaan julkinen yhteenveto kansallisia havaintoja ja sektorille tuotettua arvoa varten.

Aikataulu ja skaalausstrategia

Pilotointien käyttöönotto etenee laajemman toteutusaikataulun mukaisesti. Ensimmäisen vuoden aikana (kuukaudet 6–12) pilotoidaan polut A ja B, joita kehitetään edelleen ja hyödynnetään perehdytysmateriaalien ja hinnoittelumallin viimeistelyyn. Tämä luo perustan varhaiselle käyttöönotolle ja palautteeseen perustuvalle kehittämiselle.

Toisen projektivuoden aikana (kuukaudet 12–24) VirtualLab- ja työpöytäharjoituspilotit laajennetaan uusille alueille ja käyttäjäryhmille, tavoitteena 10–15 osallistuvaa organisaatiota. Tänä aikana kerätty data tukee myös analytiikkatyökalujen ja arviointinäkymien käyttöönottoa.

Mini-Sairaala siirtyy pilottivaiheeseen kolmantena vuonna (kuukaudet 24–30). Tulosten perusteella viimeistellään tekniset järjestelmät, skenaarioiden etenemistahti ja moniammatillisen fasilitoinnin mallit. Neljännen vuoden loppuun mennessä koko harjoitusekosysteemin odotetaan olevan valmiina laajentamiseen.

Kuukausien 36–42 aikana kaikki koulutuspolut skaalataan, ja tavoitteena on vähintään 30 aktiivisesti osallistuvaa organisaatiota. Tänä aikana otetaan käyttöön myös hybridiharjoitusvaihtoehtoja – kuten Mini-Sairaala-skenaarioiden VirtualLab-versiot – mikä laajentaa koulutusten saavutettavuutta entisestään.

Kuva 4: Pilotointi-, skaalaus- ja laajentumisaikajana kaikille toteutuspoluille.

Osa 3: Henkilöstö ja hallintomalli

Usean koulutuspolun ja teknisesti vaativan koulutusekosysteemin toteuttaminen edellyttää selkeää henkilöstösuunnitelmaa sekä hallintorakennetta, joka varmistaa laadun, jatkuvuuden ja vastuunjaon.

Tässä osassa kuvataan kunkin kehitys- ja operatiivisen vaiheen henkilöstötarpeet, mukaan lukien ne roolit, joita tarvitaan VirtualLab-, työpöytäharjoitus- ja Mini-Sairaala-kokonaisuuksien tukemiseen. Lisäksi selitetään, miten opiskelijat voidaan integroida skenaarioiden suunnitteluun ja testaukseen ilman, että heidän panoksensa korvaa ydinhenkilöstöä.

Samanaikaisesti hallintomalli määrittelee selkeät päätöksentekovastuut operatiivisella, teknisellä ja strategisella tasolla. Sisäisen johtamisen, sektorikumppanuuksien ja asiantuntijaneuvonnan yhdistelmä varmistaa, että projekti pysyy linjassa kansallisen sääntelyn ja toimialakohtaisten tarpeiden kanssa.

Henkilöstötarpeet

Polut A ja B – VirtualLab ja työpöytäharjoitusalusta

Toiminto	Rooli	Arvioitu HTV	Vaihe
Projektipäällikkö	Johtaminen, markkinointi	1.0	1-4
Tekninen insinööri	VirtualLab, integraatio ja tekninen ylläpito	1.0	1-3
Tekninen insinööri	Työpöytäharjoitusalusta, integraatio, tekninen ylläpito	1.0	1-3

Tekninen insinööri	VirtualLab- ja työpöytäharjoitusalustojen tekninen ylläpito	1.0	1-2
Kyberturvallisuusinsinööri (SOTE)	Skenaariokehitys, markkinointi	1.0	1-4
Simulaatiopedagogi	Skenaarioiden kulku	0.3	1-4
Admin / tuki	Aikataulutus, perehdytys, markkinointi	0.5	1-3
Yhteensä		**5.8**	

Polku C – Mini-Sairaala-kybersimulaatio

Tekninen infrastruktuuri ja järjestelmäkehitys

Toiminto	Rooli	Arvioitu HTV	Vaihe
Projektipäällikkö	Johtaminen	1.0	1-5
Tekninen lead	Infrastruktuurin määrittely ja integraatio	1.0	1-4
Sisällöntuottaja	Skenaarioiden kirjoittaminen	1.0	3-5
Automaation asiantuntija	Ohjausjärjestelmien suunnittelu ja toteutus	1.0	1-4
Ohjelmoija	Potilastietojärjestelmä, potilasmonitorointi, simulaatiotriggerien kehitys ja integraatio	2.0	1-4
Admin / Tuki	Aikataulutus, perehdytys, logistiikka, tukirooli	0.5	1-5

Markkinointi	Markkinointi	1.0	3-5
Yhteensä		**7.5**	

Opiskelijoiden osallistuminen

Polku	Mahdolliset tehtävät
Harjoittelu	Harjoituskehitys, skenaariologiikan testaus, virtuaaliympäristöjen käyttöönotto, ohjelmointi
Opinnäytetyö	Koulutusmallien suunnittelu, automaattisten palautetyökalujen kehittäminen, käyttäjäkokemuksen arviointi
Projektikurssi	Skenaariokehitys (Polut A + B), uhkasimulaatio, UX/UI-elementtien suunnittelu

Opiskelijoiden osallistuminen on aina tukiroolissa, ei henkilöstön korvaamista.

Projektin hallintomalli

Tehokas hallintomalli on välttämätön, jotta teknisesti monimutkainen ja useasta koulutuspolusta koostuva kokonaisuus voidaan toteuttaa aikataulussa, budjetissa ja vaaditulla laatutasolla. Hallintomalli yhdistää selkeän johtamisen, teknisen vastuun ja ulkoisen asiantuntijavalvonnan, jotta projekti pysyy linjassa toimialan tarpeiden ja kansallisten standardien kanssa.

Hallintorakenne

Projektia johdetaan kolmitasoisella mallilla, jossa on selkeät roolit ja vastuualueet:

1. Ydinhallintotiimi – vastaa päivittäisestä johtamisesta, operatiivisesta päätöksenteosta ja resurssien kohdentamisesta.
2. Ohjausryhmä – tarjoaa strategista ohjausta, varmistaa rahoituksen ja tavoitteiden yhteensopivuuden sekä hoitaa riskienhallintaa.
3. Ulkoinen asiantuntijaryhmä – tuo asiantuntijanäkökulmaa sosiaali- ja terveydenhuollosta, kyberturvallisuudesta ja koulutussektorilta.

Ydinhallintotiimi

Ydinhallintotiimi vastaa kaikkien harjoituspolkujen suunnittelusta, toteutuksesta ja laadunvarmistuksesta.

Rooli	Vastuut
Projektipäälliköt	Kokonaisvastuu projektin toteutuksesta, budjettiseurannasta, sisällön ja julkaisujen lopullisesta hyväksynnästä, raportointi ohjausryhmälle
Kyberpedagogiikan ja oppimismuotoilun vetäjä	Vastaa skenaarioiden laadusta, oppimistavoitteista ja pedagogisesta integraatiosta
Tekniset leadit	Hyväksyvät teknisen arkkitehtuurin, ohjaavat insinööritiimiä ja validoivat skenaarioiden käyttöönoton
Markkinointi	Ylläpitää suhteita sosiaali- ja terveydenhuollon toimijoihin, vastaa perehdytyksestä ja kumppaniviestinnästä

Projektikoordinaattori	Hallinnollinen tuki, aikataulutus ja dokumentinhallinta

Ohjausryhmä

Ohjausryhmä tarjoaa strategisen suunnan, varmistaa rahoitusehtojen ja organisaation strategian yhteensopivuuden sekä valvoo riskejä.

Kokoonpano:

- Xamkin senioritason johdon edustaja (puheenjohtaja)
- Projektipäällikkö (raportointi)
- Hyvinvointialueen edustaja
- Traficomin Kyberturvallisuuskeskuksen edustaja
- Yksityisen sektorin edustaja (sosiaali- ja terveysalan pk-yritys)

Keskeiset tehtävät:

- Hyväksyy projektin päävaiheet ja budjetit
- Valvoo riskirekisteriä ja riskienhallintatoimenpiteitä
- Mahdollistaa organisaatioiden välisen yhteistyön

Ulkoinen asiantuntijaryhmä

Ulkoinen asiantuntijaryhmä neuvoo toimialan tarpeiden, skenaarioiden realismin ja kyberuhkien kehityksen näkökulmista.

Ehdotetut jäsenet:

- Sairaalan IT- tai kyberturvallisuuspäällikkö
- Hyvinvointialueen kliinisen toiminnan edustaja
- Pk-yritysedustaja (yksityinen sektori)

- Kyberturvallisuuden akateeminen asiantuntija
- Lääkinnällisten laitteiden asiantuntija

Keskeiset tehtävät:

- Arvioi vuosittaisen skenaariokatalogin realismin ja toimialasopivuuden
- Tarjoaa näkemyksiä kehittyvästä uhkakentästä
- Neuvoo uusien teknologioiden ja parhaiden käytäntöjen integroinnissa
- Vahvistaa yhteyksiä kansallisiin ja kansainvälisiin kyberresilienssitavoitteisiin

Päätöksentekoprosessi

1. Operatiiviset päätökset
    a. Tehdään ydintiimin toimesta
    b. Eskaloidaan ohjausryhmälle, jos kyse on budjetti-, laajuus- tai riskiasioista, jotka ylittävät sovitut rajat
2. Tekniset päätökset
    a. Tekevät tekniset leadit yhteistyössä insinöörien ja pedagogien kanssa
    b. Merkittävät arkkitehtuurimuutokset edellyttävät ohjausryhmän hyväksyntää
3. Strategiset ja rahoitukseen liittyvät päätökset
    a. Vain ohjausryhmän päätettävissä
    b. Perustuvat ulkoisen asiantuntijaryhmän ja ydintiimin suosituksiin

Osa 4: Talous ja kestävyys

Tämän kokonaisuuden pitkäaikainen onnistuminen riippuu taloudellisesti kestävästä mallista, joka mahdollistaa valtakunnallisen saavutettavuuden, jatkuvan skenaariokehityksen ja edulliset hinnat kaiken kokoisille organisaatioille.

Tässä osassa kuvataan kunkin harjoituspolun kehitys- ja operatiiviset kustannukset sekä realistinen tulomalli, joka perustuu tasohinnoitteluun ja käyttöaste-ennusteisiin. Vaikka ulkoinen rahoitus on välttämätöntä rakentamis- ja pilotointivaiheissa, konsepti on suunniteltu saavuttamaan omavaraisuuden neljänteen toimintavuoteen mennessä.

Hyödyntämällä olemassa olevia alustoja, opiskelijayhteistyötä ja modulaarisesti uudelleenkäytettäviä skenaarioita projekti pystyy minimoimaan yleiskustannukset ja maksimoimaan toimialakohtaisen arvon – samalla kun se rakentaa skaalautuvan palvelumallin, joka mukautuu tuleviin harjoitustarpeisiin, sääntelymuutoksiin ja toimialalaajennuksiin.

Yksityiskohtainen budjetti ja kustannusarvio

Budjetti jakautuu kahteen pääkomponenttiin harjoituspolkujen mukaan:

a. Polut A & B: VirtualLab-kybersimulaatio ja työpöytäharjoitusalusta

b. Polku C: Mini-Sairaala-kybersimulaatio (valinnainen + kertaluonteinen infrastruktuuri-investointi)

Jokainen polku jaetaan henkilöstö- ja ei-henkilöstökustannuksiin, ja kustannukset kohdistetaan hankkeen vaiheisiin (esim. kehitys, käyttöönotto, testaus, operointi). Henkilöstökulut lasketaan arvioitujen FTE-määrien ja vastaavien palkkatasojen perusteella. Budjettiin sisältyy myös varmuuspuskurit epävarmuuksien varalta.

Tulomalli ja kestävyyssuunnitelma

Konseptin taloudellinen kestävyys perustuu realistiseen hinnoittelumalliin, vaiheittaiseen markkinakehitykseen ja pakettikokonaisuuteen, joka sisältää sekä VirtualLab-kybersimulaation että työpöytäharjoitukset.

Tässä osiossa käsitellään tasot, markkinapotentiaalin oletukset, tulonkehitysarvio sekä kannattavuusanalyysi projektin neljän ensimmäisen vuoden ajalle.

1. Hinnoittelurakenne (per organisaatio / per vuosi)

Palvelu myydään pakettina: VirtualLab- ja työpöytäharjoitukset perustuvat yhteiseen tarinalliseen skenaarioon. Tämä malli parantaa oppimistuloksia ja samanaikaisesti vähentää kehitystyötä.

Organisaatio	Paketin hinta (€)
Yksinyrittäjät	80
1-5 työntekijää	100
6-10 työntekijää	180
11-20 työntekijää	250
21-50 työntekijää	400

Paketin hinnoittelu on 20–25 % edullisempi kuin harjoituspolkujen ostaminen erikseen, mutta maksimoi silti tulot.

1. Markkinan koko ja omaksumisoletus

Kohderyhmä: Sosiaali- ja terveysalan organisaatiot Suomessa

Kokonaisosoitettavissa olevat organisaatiot: n. 15 000

Oletettu vuosittainen käyttö per organisaatio: 1 VirtualLab + 1 työpöytäharjoitus

Omaksuminen (vuodet 1–4)

Vuosi	Yksinyrittäjä/Mikro -omaksuminen	PK-omaksuminen
1	1 %	0.5 %
2	3 %	1 %
3	5 %	2 %
4	7 %	3 %

2. Liikevaihtoennusteet, polut A & B

Vuosi	Yksinyrittäjä/ Mikro	Keskihinta (€)	Liikevaihto (€)	PK	Keskihinta (€)	Liikevaihto (€)
1	50	120	3 780	15	325	4 875
2	200	120	24 000	30	325	9 750
3	600	120	72 000	60	325	19 500
4	840	120	100 800	90	325	29 250

Painotetut keskihinnat heijastavat organisaatiojakaumaa ja porrastettua hinnoittelua.

3. Kustannus- ja kannattavuusanalyysi

Arvioidut toiminta- ja kehityskustannukset (sisältö, tekniikka, tuki) vuoden 4 jälkeen: ~130 000 € / vuosi

Vuosi	Kumulatiivinen liikevaihto (€)
1	19 275
2	52 950
3	91 500
4	130 050

Kannattavuusskenaariot

- Ulkopuolisella rahoituksella vuosille 1–2: Toiminta on omavarainen vuoden 4 jälkeen.
- Ilman rahoitusta: Break-even saavutetaan noin 6 vuodessa olettaen tasainen omaksuminen

Yhteenveto: Mallin kestävyys

- Hinnoittelu on saavutettavaa yksinyrittäjille ja pienille toimijoille, mutta skaalautuu oikein pk-yrityksille.
- Omaksumistaso on realistinen, pohjaten toimialan digitaaliseen kypsyystasoon.
- Paketoitu tarjoama maksimoi kustannustehokkuuden sekä sisällön kehityksessä, että toimituksessa.
- Malli muuttuu kestäväksi neljässä vuodessa konservatiivisilla oletuksilla – ja nopeammin, jos käyttöönotto ylittää ennusteet.

Rahoitusmahdollisuudet ja -strategiat

Harjoitusekosysteemin pitkäaikaisen onnistumisen ja valtakunnallisen vaikuttavuuden varmistaminen edellyttää monilähteistä rahoitusmallia, joka tukee sekä alkuvaiheen kehitystä että jatkuvaa toimintaa. Tässä osiossa esitellään kohdennetut rahoitusmahdollisuudet, jotka ovat linjassa kansallisten ja EU:n painopisteiden kanssa, sekä kuvataan, miten eri rahoituslähteet voivat tukea hankkeen eri vaiheita — infrastruktuurin ja sisällön kehittämisestä aina skaalaukseen, mallinnukseen ja kansainvälistämiseen.

Markkinointi- ja viestintästrategia

Tehokas viestintä on ratkaisevan tärkeää, jotta harjoitusekosysteemi tavoittaa kohderyhmänsä — erityisesti sosiaali- ja terveydenhuollon pk-yritykset sekä hyvinvointialueet (HVA). Strategian tavoitteena on rakentaa tunnettuutta, luottamusta ja sitoutumista kohdennettujen kanavien ja kumppanuuksien kautta, painottaen varhaisen vaiheen viestintää kehitys- ja pilotointijaksoina.

Pk-yritysten tavoittamiseksi projektissa hyödynnetään toimialakohtaisia viestintäkanavia, kuten uutiskirjeitä, webinaareja ja kohdennettuja sosiaalisen median kampanjoita yhteistyössä terveysalan toimijoiden ja kyberturvallisuusverkostojen kanssa. Kumppanuudet keskeisten alueellisten toimijoiden — kuten kehitysyhtiöiden, korkeakouluverkostojen ja kauppakamarien — kanssa toimivat vahvistimina, laajentaen näkyvyyttä ja auttaen tunnistamaan pilottiasiakkaita eri puolilta Suomea.

Näkyvyyttä lisätään myös osallistumalla aktiivisesti valtakunnallisiin tapahtumiin, jotka kokoavat yhteen sekä kyberturvallisuuden että sosiaali- ja terveysalan sidosryhmiä. Näitä voivat olla konferenssit, messut ja valtionhallinnon järjestämät innovaatiotilaisuudet. Projektitiimi osallistuu paneeleihin, järjestää työpajoja ja esittelee pilotointien tuloksia kiinnostuksen herättämiseksi ja uskottavuuden vahvistamiseksi.

Varhaisen vaiheen viestinnän painopiste on ennakoivien organisaatioiden tunnistamisessa — erityisesti pk-yritysten ja hyvinvointialueiden joukosta — jotka ovat valmiita kokeilemaan uusia harjoitusmenetelmiä ja osallistumaan ensimmäisten skenaarioiden yhteiskehittämiseen. Nämä edelläkävijät eivät ainoastaan validoi harjoitustyökaluja, vaan toimivat myös lähettiläinä edistäen mallin käyttöönottoa omissa verkostoissaan, mikä tukee orgaanista kasvua ja koko sektorin laajuista vaikutusta.

Rahoitustavoite

Haettavalla rahoituksella tuetaan suoraan valtakunnallisesti skaalautuvan ja toimialakohtaisen kyberharjoitusekosysteemin rakentamista. Rahoituksen painopisteet kohdistuvat hankkeen alkuvaiheen resursseiltaan raskaimpiin ja strategisesti kriittisiin osiin.

Ensisijainen rahoitustarve liittyy Mini-Sairaala-simulaatioympäristön laitteistoinfrastruktuuriin. Tämä sisältää oman simulaatiokerroksen realistisine kliinisine tiloineen, segmentoidut verkot hallittuja kyberhäiriöitä varten sekä erikoisvalmisteiset palvelimet, jotka tukevat monimutkaisia automaatiopohjaisia harjoitusskenaarioita.

Samanaikaisesti tarvitaan räätälöityä ohjelmistokehitystä, jolla rakennetaan immersiivisiä terveydenhuollon kyberskenaarioita Mini-Sairaalaan. Tähän sisältyvät simuloitu potilastietojärjestelmä, integraatiot potilasmonitorointilaitteisiin sekä incident-automaatiojärjestelmät todentuntuisen, moniammatillisen harjoittelun mahdollistamiseksi.

Rahoituksella tuetaan myös avainhenkilöstön rekrytointia ja sitouttamista intensiivisen 30 kuukauden kehitysvaiheen aikana. Näitä ovat skenaariokehittäjät, tekniset insinöörit, kyberturvallisuusasiantuntijat ja pedagogiset asiantuntijat — kaikki keskeisiä realistisen, toimivan ja toimialan tarpeisiin sopivan harjoitussisällön luomisessa.

Lopuksi projektin tavoitteena on merkittävästi laajentaa VirtualLab-skenaariokatalogia, jotta mikro- ja pienet sosiaali- ja terveysalan organisaatiot eri puolilla Suomea voivat hyötyä matalan kynnyksen selainpohjaisista harjoituksista. Näiden modaalien saatavuus ja laadun varmistaminen ovat ratkaisevia projektin skaalautuvuuden ja pitkän aikavälin kestävyyden kannalta.

Mahdolliset rahoituslähteet

Rahoittaja	Perustelu
Maakuntaliitto / ELY-keskus	Tukee pk-yritysten digitalisaatiota, alueellista innovaatiota ja NIS2-valmiutta; linjassa alueellisen kyberturvakapasiteetin vahvistamisen kanssa
Business Finland	Innovaatio terveydenhuollon infrastruktuurissa ja kyberturvallisuuspalveluissa
Sosiaali- ja terveysministeriö (STM)	Strateginen yhteensopivuus kansallisen SOTE-resilienssin, NIS2:n toimeenpanon ja varautumisen vahvistamisen kanssa
EU:n Resilienssirahastot / Digital Europe / Horizon Europe	Rahoittaa simulaatioinfrastruktuuria, kriittisen sektorin digitaalista turvallisuutta ja rajat ylittäviä koulutusympäristöjä; mahdollistaa mallin skaalattavan monistamisen
ESR+ (Euroopan sosiaalirahasto Plus)	Keskittyy työvoiman kehittämiseen, jatkuvaan oppimiseen ja koulutuksen ja työelämän rajapinnan vahvistamiseen kriittisillä toimialoilla

Osa 5: Riskit ja vaatimustenmukaisuus

Tämä konsepti yhdistää useita eri osa-alueita — terveydenhuollon simulaation, kyberturvallisuuden, IT-infrastruktuurin ja julkisen sektorin koulutuksen — yhdeksi valtakunnalliseksi palveluksi. Hyödyt ovat merkittävät, mutta niin ovat riskitkin. Teknologiset viivästykset, hankintaprosessit, monialainen koordinointi sekä rahoituksen epävarmuus on kaikki hallittava aktiivisesti, jotta varmistetaan hankkeen ajantasainen toteutus ja pitkäaikainen toiminnallinen kestävyys.

Tässä osiossa esitetään hankkeen riskit ja vaatimustenmukaisuustoimenpiteet selkeästi ja läpinäkyvästi. Haasteet kuvataan rakenteisessa riskimatriisissa, jossa arvioidaan todennäköisyys ja vaikutus, ja jokaiselle riskille on määritelty ennaltaehkäisevät toimet sekä vastuuhenkilöt. Mukana on myös taloudellisia ja operatiivisia varasuunnitelmia, jotka osoittavat kokonaisuuden resilienssin.

Riskimatriisin yleiskuva

Monimutkaisen, useasta polusta koostuvan kokonaisuuden hallintaan sovelletaan systemaattista riskienarviointimallia, jota kutsutaan Riskimatriisiksi. Matriisi tarjoaa läpinäkyvän kokonaiskuvan keskeisistä riskeistä, jotka voivat vaikuttaa harjoitusmallin kehittämiseen, käyttöönottoon ja pitkäaikaiseen kestävyyteen.

Jokainen tunnistettu riski arvioidaan kahdella akselilla:

- Todennäköisyys – Arvio siitä, miten todennäköisesti riski toteutuu projektin aikana.
- Vaikutus – Seurauksien vakavuus, jos riski toteutuu.

Molemmat arvioidaan kolmiportaisella asteikolla:

Taso	Kuvaus
Matala	Epätodennäköinen tai vaikutuksiltaan vähäinen.
Keskitaso	Voi toteutua tietyissä olosuhteissa; vaikutukset hallittavissa, mutta aiheuttaa häiriötä.
Korkea	Todennäköinen; merkittävä vaikutus projektin aikatauluun, laatuun tai laajuuteen.

Jokaiselle riskille määritellään myös lieventämisstrategia, joka pyrkii vähentämään sen todennäköisyyttä tai vaikutusta.

Riskimatriisia päivitetään säännöllisesti projektin aikana — erityisesti suurten päätöspisteiden yhteydessä.

Haasteet ja riskit

Riski	Todennäköisyys	Vaikutus	Lieventämisstrategia
Rekrytointihaasteet ydinhenkilöstölle – Projekti vaatii korkeasti koulutettua henkilöstöä, jolla on kokemusta kyberturvallisuudesta, simulaatiosta ja terveydenhuollosta. Tämänkaltaisten asiantuntijoiden rajallinen saatavuus	Korkea	Korkea	Aloita rekrytointi varhain; osallista opiskelijat aikaisessa vaiheessa; luo kumppanuuksia yliopistojen ja sairaaloiden IT-yksiköiden kanssa; pidä rekrytointirakenne joustavana osaajien houkuttelemiseksi.

Suomessa saattaa viivästyttää rekrytointeja ja lisätä nykyisen henkilöstön työkuormaa.			
Terveydenhuollon kokemusta omaavien skenaariokehittäjien puute – Henkilöstön saatavuus, jolla on sekä kliininen tausta että kyberturvallisuusosaamista, on rajallinen. Ilman aitoa ymmärrystä sairaalaprosesseista harjoitukset voivat jäädä heijastamatta todellisia olosuhteita.	Korkea	Korkea	Kehittäkää harjoituksia yhdessä HVA:n kliinisen henkilöstön kanssa; perustakaa asiantuntijaryhmä skenaarioiden validointiin; hyödyntäkää yhteisiä opiskelijaprojekteja sisäisen osaamisen vahvistamiseksi.
Toiminnallinen ylikuormitus intensiivisissä vaiheissa – Kehityksen huippukuukausina sama henkilöstö saattaa vastata teknisistä, pedagogisista ja koordinaatiotehtävistä, mikä voi johtaa uupumiseen tai laadun heikkenemiseen.	Keskitaso	Korkea	Toteuttakaa työkuormakartoitus; varmistakaa tilapäinen tekninen tuki; jakakaa vastuut eri kokonaisuuksien kesken; priorisoikaa tehtävät ja välttäkää päällekkäisiä välitavoitteita.

Keskeisen henkilöstön menettäminen kehitysvaiheen aikana – Kriittisen henkilöstön (tekninen johtaja, pedagogi tai sisällöntuottaja) lähteminen tai poissaolo voi aiheuttaa osaamisvajeita tai tarvetta tehdä työtä uudelleen.	Keskitaso	Korkea	Laaditaan yksityiskohtainen dokumentaatio; otetaan käyttöön luovutus- ja sijaisuusprosessit; koulutetaan varahenkilöstöä; tarjotaan sitouttamiskannustimia avainhenkilöille.
Teknisen järjestelmäintegraation epäonnistumiset – Potilastietojärjestelmien, valvontalaitteiden ja automaatiotyökalujen yhdistämisen monimutkaisuus voi aiheuttaa toimintahäiriöitä tai tietokonflikteja simulaation aikana.	Keskitaso	Korkea	Toteuttakaa vaiheistetut testaukset ja integraatiokatselmukset; hyödyntäkää ulkopuolisia asiantuntijoita kriittisissä liitännöissä; käyttäkää eristettyjä testiympäristöjä ennen tuotantokäyttöä.
Rahoituksen katkeaminen tai vähentyminen – Ulkoisen rahoituksen viivästykset tai muutokset voivat	Keskitaso	Korkea	Monipuolistakaa rahoituslähteitä (EU, STM, Sitra, alueelliset tahot); ylläpitäkää projektivarantoja; priorisoikaa

keskeyttää käynnissä olevan kehitystyön tai rajoittaa Mini-Sairaala-kokonaisuuden rakentamista.			VirtualLab-tuotokset edistymisen osoittamiseksi ja rahoittajien luottamuksen säilyttämiseksi.
Kohdeorganisaatioiden vähäinen sitoutuminen – PK-yritykset tai HVA:t eivät välttämättä varaa aikaa tai budjettia osallistuakseen pilottikoulutuksiin, mikä voi hidastaa kansallista käyttöönottoa.	Keskitaso	Korkea	Hyödyntäkää vahvoja markkinointikampanjoita alueellisten verkostojen kautta; tarjotkaa tuettuja pilottisessioita; julkaiskaa vaikuttavuustuloksia luottamuksen rakentamiseksi; sovittakaa skenaariot NIS2-velvoitteisiin.
Laitteisto- ja ohjelmistokustannuksista johtuvat budjettiylitykset – Inflaatio, toimittajien hintamuutokset tai aliarvioidut integraatiotarpeet voivat ylittää alkuperäiset kustannusarviot.	Keskitaso	Keskitaso	Ylläpitäkää 10–15 %:n vararahasto; tehkää toimittajaneuvottelut varhaisessa vaiheessa; vaiheistakaa hankinnat kokonaisuuksittain; priorisoikaa ensin kriittiset komponentit.
Sääntely- tai politiikkamuutokset vaikuttavat projektin vaatimuksiin –	Matala	Keskitaso	Seuratkaa sääntelypäivityksiä STM:n ja Kyberturvallisuuskeskuks

Muutokset NIS2-direktiivissä, terveydenhuollon IT-standardeissa tai julkisia hankintoja koskevassa lainsäädännössä voivat edellyttää teknisiä tai menettelytapojen muutoksia.			en kautta; ylläpitäkää mukautuvaa infrastruktuuria; varmistakaa järjestelmädokumentaation joustavuus.
Teknisten valmiuksien ja koulutustarpeiden yhteensopimattomuus – Jos simulaatioympäristöstä puuttuu oikeat laukaisimet, laitekäyttäytyminen tai automaatio-ominaisuudet, harjoitukset eivät välttämättä riittävästi heijasta terveydenhuollon todellisia työnkulkuja tai kyberturvallisuuden kriittisiä painopisteitä.	Keskitaso	Korkea	Osallistakaa loppukäyttäjät (kliininen henkilöstö ja IT) skenaarioiden suunnitteluun varhaisessa vaiheessa; tehkää tekniset läpikäynnit ennen pilotteja; iterokaa palautteen perusteella; rakentakaa simulaation joustavuus osaksi infrastruktuuriratkaisuja.

Harjoitus

Skenaariopohjainen kyberturvallisuusharjoitus suunniteltiin simuloimaan kyberkriisiä sairaalaympäristössä, jossa moniammatilliset tiimit osallistuvat realistiseen ja ajallisesti kriittiseen päätöksentekoon. Harjoitus kehitettiin osana CyberCare Kymi -hanketta, ja se heijastaa modernien terveydenhuoltoympäristöjen monimutkaisuutta ja keskinäistä riippuvuutta — tilanteissa, joissa digitaaliset häiriöt voivat suoraan vaikuttaa potilasturvallisuuteen ja hoidon jatkuvuuteen.

Harjoitus toimii koulutusalustana, jonka tavoitteena on vahvistaa operatiivista valmiutta, tietoturvatietoisuutta sekä kliinisten, teknisten ja johtotason roolien välistä koordinointia. Osallistujat upotetaan skenaarioon, jossa kriittiset järjestelmät vikaantuvat ja heidän on hallittava häiriötilannetta, sovellettava voimassa olevia tietoturvaprotokollia ja varmistettava hoidon turvallinen toteutus vaihtoehtoisin toimintatavoin.

Vastaamalla todellisia uhkia ja toimialakohtaisia vaatimuksia heijastaviin tilanteisiin, harjoitus tukee organisaation oppimista, tunnistaa keskeisiä haavoittuvuuksia ja edistää ennakoivaa turvallisuuskulttuuria terveydenhuoltosektorilla.

Harjoituksen suunnitteli ja toteutti Sitowise.

Sairaalan kybermyrsky - kyberturvallisuusharjoitus

Teknistoiminnallinen harjoitus sairaalaympäristöön

Tässä luvussa kuvataan CyberCare Kymi -hankkeelle luotu sairaalan toimintaympäristöön tarkoitettu kyberturvallisuusharjoitus ja sen sisältämät skenaariot. Työssä luotiin useamman pelaajan ryhmäharjoitus. Turvavalvonnasta (Security Operation Center, SOC) käytetään tästä eteenpäin lyhennettä SOC.

Tausta ja tavoitteet

CyberCare Kymi -hanke tukee Kymenlaakson sosiaali- ja terveysalan toimijoita kyber- ja tietoturvan osaamistason parantamisessa, toiminnan jatkuvuuteen varautumisessa ja palautumisen harjoittelussa. Harjoituksen tavoitteena on vahvistaa kyberkriisivalmiuksia ja lisätä ymmärrystä osallistujien omassa tutussa sairaalan toimintaympäristössä.

Työ on toteutettu lisätyönä aiemmalle ”CyberCare Kymi – teknistoiminnalliset kyberharjoitukset 2024” työlle ja se noudattaa kyseisessä työn loppuraportissa asetettuja lähtökohtia.

Tarinallistaminen ja tarinan kulku skenaarion kautta

Organisaation tausta ja alkuasetelma

Kymen hyvinvointialueeseen kuuluva tavanomainen sairaalaorganisaatio, joka on varautunut nykyisen kyberturvallisuusympäristön uhkiin mm. laatimalla tietoturvasuunnitelman ja varautuen potilasturvallisuuden varmistamiseen.

Tarinan alku ja käänne

”Organisaatio on kokenut muutoksia viime aikoina ja nyt koko porukka on ensimmäistä kertaa uusissa tiloissa. Tietojärjestelmät ovat myös jonkin verran vaihtuneet, mutta niiden käyttöön oppii. Onneksi on tuttuja kasvoja ympärillä.”

Johto ja IT ovat kokoontuneet käymään läpi tietoturvasuunnitelmaa ja sen kehittämistä. Hoitajat ja vastaanottotyöntekijät suorittavat tavanomaisia työpäivän tehtäviään omissa työpisteissään/osastolla.

Johto ja IT ovat päässeet alkuun tietoturvasuunnitelman läpikäynnissä, kun ensimmäiset häiriömerkit ilmenevät. Sairaalan tietojärjestelmiin kohdistuu kyberhyökkäys, joka häiritsee kriittistä potilastietojärjestelmää (Skenaario 1). Juuri kun tilanne näyttää rauhoittuvan, sähköpostipalvelua koskeva häiriö iskee puun takaa (Skenaario 2). Tilanne eskaloituu, kun järjestelmät eivät hyökkäyksen jälkeen toimi odotetusti, ja henkilöstö joutuu siirtymään manuaalisiin toimintamalleihin potilasturvallisuuden varmistamiseksi.

Skenaario 2 on ajateltu optioksi harjoitukseen riippuen siitä, miten paljon skenaario 1:een on mennyt aikaa. Kokonaisuudessaan harjoitukseen käytettävä aika on arvioitu 4 tunniksi, jonka jälkeiselle jälkipuinnille on varattava myös aikaa.

Harjoituksen tavoite, pelin päätös ja arviointi

Harjoituksen tavoitteena on kehittää osallistujien kykyä toimia poikkeustilanteessa, jossa tietojärjestelmään kohdistuu kyberhyökkäys. Osallistujat toimivat omissa rooleissaan, tunnistavat kehityskohteita omaan varautumiseensa ja vahvistavat osaamistaan johtamisen, päätöksenteon, viestinnän ja käytännön hoitotyön toimintamalleista häiriötilanteessa. Priorisointina on sairaalan toiminnan jatkuvuuden ja potilasturvallisuuden varmistaminen sekä tietojärjestelmän palauttaminen.

Onnistuminen mitataan sillä, kuinka hyvin johtaminen, kriisiviestintä, tekninen reagointi ja käytännön hoitotoiminnan jatkuvuuden toimintamallit toimivat yhdessä, ja kuinka organisaatio palauttaa kriittiset toiminnot hallitusti.

Mittarit, jolla harjoituksen onnistumista voidaan arvioida:

- Oman tietoturvasuunnitelman noudattaminen (ja puutteiden tunnistaminen)
- Kriisiviestinnän selkeys ja toiminta
- Potilasturvallisuus (manuaalisen toimintamallin toteutus ja reagointiaika)
- Palautuminen

Päätapahtumat (MITRE MSEL)

Orientaatio

Pelaajien orientaatio ja poikkeaman läpivientisuunnitelman anto. Samassa yhteydessä Pelaajille esitellään tarinan alkuasetelma. Tarinan alun kertoo WHITE, joka esiintyy orientaatiossa IT-konsultin roolissa ja kuvaa pelaajien toimintaympäristön sekä kertoo huolestuneena kybertoimintaympäristön muutoksesta, josta hän on lukenut lehdistä ja nähnyt TV-uutisista juttuja.

Oletukset orientaatioon: WHITE tuottaa mediapeliin kybertoimintaympäristöä kuvaavaa mediamateriaalia. Mediamateriaalissa on myös sote-alan yrityksen toimialaa koskevia uutisia kyberhyökkäyksistä ja niiden seurauksista.

Oletukset harjoitukseen

1. Osallistuvalla organisaatiolla on oma tietoturvasuunnitelma, jota noudattavat harjoituksen aikana.
2. Koska harjoituksen tekninen ympäristö poikkeaa jonkin verran organisaation omasta ympäristöstä, toimitetaan harjoituksen osallistujille harjoituksen järjestäjän toimesta liite, jossa on kuvattu seuraavanlaiset asiat
    a. Liitteessä kuvattu tahot, joihin IT voi tukeutua: SOC ja järjestelmätoimittaja. Järjestelmätoimittaja vastaa potilastietojärjestelmästä sekä sähköpostijärjestelmästä.
    b. Organisaation sisällä häiriötilanteissa ensisijainen ilmoittamiskeino sähköposti, seuraavaksi SMS.

   c. Kanta-palveluihin liittyvässä poikkeustilanteessa Kelaan ilmoitus häiriöilmoituslomakkeella (Simternet). Toinen vaihtoehto puhelimitse Kelan tukeen WHITE
   d. Hätäkeskukseen (HäKe) ilmoitus tehdään puhelinsoitolla.
3. Hoitajille lisäksi tulostettu versio yhteystiedoista:
   a. IT:n puhelinnumero ja sähköpostiosoite
   b. HäKe puhelinnumero
   c. Kelataksi puhelinnumero
4. Hoitotapausten määrät osastoilla skaalautuvat sen mukaan, kuinka harjoitukseen osallistuvan organisaation puolelta harjoitukseen osallistuu hoitajia. Esim. suuri osallistujamäärä mahdollistaa jatkuvan uusien potilaiden saapumisen vastaanottoon
5. Harjoituksessa tulee tarvetta paperisille lomakkeille järjestelmähäiriöiden vuoksi.
6. Järjestelmähäiriön tulisi olla riittävän pitkä, jotta harjoituksen eri rooleissa olevat henkilöt ehtivät toimimaan odotetusti.
7. Harjoitukseen tulee valmistautua.

Skenaario 1	Kohde: Sairaalan potilas-/ asiakastietojärjestelmä			
Aika (suhteellinen	Syöte	Kuvaus	Roolit	Odotettu toiminta
T-00:00	Tietoturva-suunnitelma Hoitotilanne: Nilkan nyrjähdys Hoitotilanne: Teho-osaston potilas	Johto BLUE ja IT BLUE saavat tietoturvasuunnitelman ja harjoitusspesifisen liitteen	Johto BLUE IT BLUE Potilas (teho-osasto) WHITE Potilas (nilkan nyrjähdys) WHITE	Johto BLUE ja IT BLUE käyvät läpi tietoturvasuunnitelmaa ja liitettä. Hoitajat BLUE aloittavat hoitotoimenpiteet TODO
T+00:10	Hyökkäys potilastietojärjestelmää vastaan	Hyökkääjä RED toteuttaa hyökkäyksen potilastietojärjestelmään, poistaa	Hyökkääjä RED	Potilastietojärjestelmä menee häiriötilaan käyttäjien näkökulmasta

		palvelimelta järjestelmän loki- ja konfiguraatiot iedostoja ja kaataa järjestelmän.		
T+00:10	Päivystykseen saapuu potilas, joka valittaa kovasta päänsärystä.	WHITE esittää potilasta, joka saapuu hoitoon vastaanottotiskille.	Uusi potilas WHITE Vastaanottohoitaja BLUE	Vastaanottohoitaja kyselee potilaan syytä vastaanotolle saapumiseen. Hoitaja yrittää avata Potilastieto-järjestelmän.
T+00:15	Asiakastietojärjestelmän päänäkymä ei käynnisty.	Vastaanottotiskillä oleva hoitaja ei pääse asiakastieto-järjestelmään tarkistamaan saapuneen potilaan tietoja.	Hoitaja BLUE Vastaava hoitaja BLUE	Vastaanottotiskin hoitaja toteaa asiakasjärjestelmän olevan häiriötilassa. Hoitaja BLUE tekee häiriöilmoituksen tietoturvasuunnitelman mukaisesti IT:lle BLUE.
T+00:25	Häiriöilmoitus asiakastietojärjestelmästä IT:lle	IT BLUE saa häiriöilmoituksen asiakastietojärjestelmästä sähköpostilla	IT BLUE Johto BLUE Kelan tuki WHITE	IT BLUE aloittaa selvittämään häriötilannetta tietoturvasuunnitelman incident-prosessin mukaisesti. IT BLUE tiedottaa Johtoa BLUE häiriötilanteesta. IT BLUE tutkii, onko asiakastietojärjestelmän häiriö paikallinen vai ulkoinen. Ongelma on paikallinen.

				IT BLUE tekee häiriöilmoituksen Kelaan käyttäen häiriölomaketta tai soittamalla Kelan tukeen WHITE IT BLUE pyytää SOC:lta GREEN lokeja liittyen asiakastietojärjestelmään (verkkoliikenne, palvelin ja sovellus).
T+00:55	Johto saa häiriöilmoituksen asiakastietojärjestelmään liittyen	Johto saa häiriöilmoituksen asiakastietojärjestelmään liittyen IT:ltä joko suullisesti tai sähköpostilla.	Johto BLUE	Johto BLUE on mukana incident-prosessin mukaisesti selvittämässä tilannetta, erityisesti viestinnän näkökulmasta ja sen osalta mitä pitää ottaa huomioon sairaalan näkökulmasta. Toimenpiteitä: kriisiryhmän kokoontuminen Tiedottaa Hätäkeskukseen (puhelinsoitto), että sairaala ei voi ottaa potilaita vastaan.
T+01:15	Johto tiedottaa vastaanottoa ja osastoja kiireellisten	Vastaanotto ei voi ottaa potilaita vastaan. Kiireellisiä potilaita	Johto BLUE	Johto tiedottaa, että potilasturvallisuus varmistettava ja siirrytään käsin paperille tehtävään potilas- ja

	potilaiden siirroista.	aletaan siirtämään osastoilta muualle hoitoon.		hoitotietojen dokumentointiin osastoilla. Johto ohjeistaa, että osastoilla olevia potilaita joudutaan siirtämään toiseen paikkaan hoitoon (teho-osaston potilas).
T+01:25	Vastaanotto saa Johdolta tiedotteen. Hoito-osasto saa Johdolta tiedotteen. Teho-osasto saa Johdolta tiedotteen.	Päivystys suljetaan, koska potilastietojärjestelmä ei toimi. Hoito-osastolla arvioidaan siirtoa tarvitsevat potilaat ja jatketaan hoitoa, jos ei siirtotarvetta. Teho-osastolla aloitetaan potilaan siirron suunnittelu.	Vastaanotto hoitaja BLUE Vastaava hoitaja BLUE	Vastaanotolle tullut potilas joudutaan käännyttämään toiseen paikkaan. Hoitaja tilaa Kelataksin toimittaakseen potilaan terveyskeskukseen (nilkan nyrjähdys). Päänsärkypotilas ambulanssilla toiseen sairaalaan. Hoitaja organisoi siirron toiseen paikkaan. Teho-osastolta siirretään potilaita. Hoitaja organisoi potilassiirron sekä tiedonsiirron uuteen hoitopaikkaan. Hoitoon ja siirtoihin liittyvät asiat dokumentoidaan paperille.
T+01:30	SOC toimittaa	SOC GREEN toimittaa IT:lle	SOC GREEN IT BLUE	IT BLUE tutkii lokit ja löytää reitin mitä

	lokit IT:lle sähköpostilla	BLUE lokit sähköpostitse.		pitkin hyökkääjä päässyt sisälle (palvelutoimittajan compromised credentials).
T+02:15	IT ohjeistaa järjestelmätoimittajalle asiakastietojärjestelmän palautuksen ja hyökkäysreitin sulkemisen	IT BLUE ohjeistaa järjestelmätoimittajalle GREEN asiakastietojärjestelmän palautuksen ja hyökkäysreitin sulkemisen.	IT BLUE Järjestelmätoimittaja GREEN	Järjestelmätoimittaja GREEN sulkee hyökkäysreitin ja tekee potilastietojärjestelmän palautuksen. Järjestelmätoimittaja GREEN tiedottaa IT:tä BLUE, että järjestelmä on palautettu.
T+02:45	Järjestelmätoimittaja tiedottaa IT:tä, että järjestelmä on palautettu.	Järjestelmätoimittaja GREEN tiedottaa IT:tä BLUE, että järjestelmä on palautettu.	IT BLUE Järjestelmätoimittaja GREEN	IT BLUE tiedottaa Johtoa BLUE, että järjestelmä on palautunut toimintaan. IT BLUE tiedottaa hoitohenkilöstöä BLUE, että potilastieto-järjestelmän häiriötilanne on ohi. IT BLUE ilmoittaa Kelan tukeen GREEN, että häiriötilanne ohi (Kelan lomake, Simternet)
T+02:50	IT tiedottaa Johtoa, että järjestelmä on palautunut	IT BLUE tiedottaa Johtoa BLUE, että järjestelmä on palautunut toimintaan.	IT BLUE Johto BLUE Vastaava hoitaja BLUE	Johto miettii tiedottamista häiriötilanteesta: kenelle kaikille? Henkilökunta, HVA, media, asiakkaat, CERT-FI.

	toimintaan. IT tiedottaa hoitohenkilöstöä, että järjestelmä on palautunut ennalleen.	IT BLUE tiedottaa hoitohenkilökuntaa BLUE, että järjestelmä on palautunut toimintaan.		Pohdittava onko henkilötietoja vaarantunut (tällöin tietosuojavaltuutetulle ilmoitus). Valvira. Johto suunnittelee tekevänsä rikosilmoituksen poliisille. Osastoilla paperille kirjatut potilaiden hoitotoimenpiteet täydennetään potilastietojärjestelmään takautuvasti.
Skenaario 2 (optio/ lisäskenaario)	Kohde: Sairaalan sähköpostijärjestelmän (häiriötilanne)			
Aika (suhteellinen)	Syöte	Kuvaus	Roolit	Odotettu toiminta
T+03:15	SMS-viesti vastaavalle hoitajalle: ”Työvuorolistoja ei ole saapunut.”	Vastaavalle hoitajalle BLUE tulee SMS-viesti vapaalta olevalta hoitajalta WHITE. Viestissä kerrotaan, ettei työvuorolistat ole saapuneet sähköpostitse.	Vastaava hoitaja BLUE Ulkopuolinen hoitaja WHITE	Vastaava hoitaja BLUE yrittää päästä sähköpostijärjestelmään varmistaakseen ongelmaa. Webbipohjainen sähköpostijärjestelmä ei lataudu. Vastaava hoitaja BLUE viestii IT:lle BLUE SMS:llä, että onko sähköpostijärjestelmässä jotain ongelmaa.

T+03:20	SMS-viesti vastaavalta hoitajalta IT:lle	Vastaaja hoitaja BLUE viestii IT:lle BLUE, että sähköpostijärjestelmässä jotain ongelmaa, koska vapaalla oleva hoitaja viesti, ettei ole saanut sähköpostiin työvuorolistoja.	IT BLUE Vastaaja hoitaja BLUE	IT BLUE varmistaa, onko ongelmaa sähköpostijärjestelmässä ja kun ongelma varmistuu tiedottaa Johtoa BLUE suullisesti ongelmasta.
T+03:25	IT:n suullinen tiedotus sähköposti järjestelmän häiriötilanteesta Johdolle	IT BLUE tiedottaa Johtoa BLUE suullisesti ongelmasta sähköpostijärjestelmän suhteen. Ongelma on varmistettu.	IT BLUE Johto BLUE	Johto BLUE suunnittelee viestinnän liittyen sähköpostijärjestelmän häiriötilanteeseen: kelle viestitään sisäisesti ja ulkoisesti ja mitä viestitään.
T+03:30	IT ottaa yhteyttä puhelinsoitolla järjestelmätoimittajaan selvittääkseen ongelmaa	IT ottaa yhteyttä puhelinsoitolla järjestelmätoimittajaan selvittääkseen ongelmaa sähköpostijärjestelmän suhteen. Järjestelmätoimittaja kertoo, että heillä on järjestelmässä tilapäinen häiriö, jonka ratkaisuun menee 30 min.	IT BLUE Järjestelmätoimittaja GREEN	IT BLUE ryhtyy Johdon BLUE kanssa miettimään mihin kaikkialle järjestelmähäiriö vaikuttaa.

T+04:00	Järjestelmätoimittajan tekstiviesti saapuu IT:n puhelimeen: häiriötilanne ohi	Järjestelmätoimittaja GREEN on palauttanut sähköpostijärjestelmän toimintaan ja tiedottaa IT:tä BLUE	Järjestelmätoimittaja GREEN IT BLUE	IT BLUE tiedottaa johtoa suullisesti ja henkilöstöä tekstiviestein, että häiriötilanne on ohi.

Harjoituksen etenemisen seuranta

Harjoituksessa Valkoinen tiimi tarvitsee pelin etenemisen seurantaan tilannekuvan, jotta se voi arvioida harjoituksen etenemistä ja pelaajien tuntemusten ja taitojen kehittymistä harjoituksen aikana. Pelaajien kyky edetä harjoituksessa vaikuttaa paljon siihen miten ennalta suunnitellut tarina ja skenaariot saadaan vietyä läpi.

Harjoitusta seurataan seuraavaan taulukkoon listatuilla asseteilla:

Järjestelmä	Konfiguraatio
Valkoisen tiimin sähköpostijärjestelmä	Hälytys, kun tietty Pelaaja tai Pelaajatiimi lähettää sähköpostin Valkoiselle tiimille
Sinisen tiimin sähköpostijärjestelmä	Operatiivinen järjestelmä, johon kohdistuu hyökkäys. Järjestelmän tilaa on voitava seurata valkoisen tiimin taholta
Mobiilipuhelimia n kpl: IT / Johto BLUE Vastaava hoitaja BLUE Kyberopiskelijat RED / GREEN / WHITE	Ei erityistä. Huomioitava, ettei viestien lähetystä ei ole mahdollista seurata ilman erityistä sovellusta, jota käytettäisiin laitteilla SMS-viestisovellusten tyyliin.
Pelaajan tai Pelaajatiimin ympäristön käyttövaltuushallintaratkaisu	Käyttövaltuushallintaratkaisun lokitus tai vastaava tapahtumien kirjaus ja luku Vihreän tiimin hallitsemalle alueelle sekä tapahtumien lukemisen mahdollistaminen Valkoiselle tiimille. Valkoinen tiimi pystyy varmistamaan,

	että Pelaaja on päässyt peliympäristöön ja on valmis pelaamaan tai on voinut varmistua järjestelmän palautuneen käyttökuntoon hyökkäyksen / häiriötilanteen päättyessä.
Pelaajan tai Pelaajatiimin ympäristön verkkoliikenteen valvonta HTTP – yhteyksien palvelin – työasema - välillä havaitsemiseksi.	Verkkoliikenteen valvonta, lokitus ja tapahtumien kirjaus ja luku Vihreän tiimin hallitsemalle alueelle sekä tapahtumien lukemisen mahdollistaminen Valkoiselle tiimille. Valkoinen tiimi pystyy varmistamaan, että Pelaaja on edennyt syötteiden viitoittamaan suuntaan ja tehnyt peliskenaarion edellyttämiä käytännön tehtäviä.
Kelan ilmoitus häiriöilmoituslomake Kelan häiriötiedotussivusto (Simternet) WHITE	Häiriöilmoitusten tekeminen, valvonta ja hallinta. Järjestelmällä Kela ilmoittaa myös omista häiriöistään.
Pelaajan tai Pelaajatiimin ympäristön Potilastietojärjestelmä sekä liiketoimintadata ja käyttäjät	Potilastietojärjestelmän ja Asiakastietojärjestelmän ja niiden tietokantojen tapahtumalokin tapahtumien kirjaus ja luku Vihreän tiimin hallitsemalle alueelle sekä tapahtumien lukemisen mahdollistaminen Valkoiselle tiimille. Valkoinen tiimi pystyy varmistamaan, että Pelaajat ovat edenneet syötteiden viitoittamaan suuntaan ja tehnyt peliskenaarion edellyttämiä käytännön tehtäviä.
Punaisen tiimin jalansijaohjelman (RAT) tai käänteinen komentotulkki Pelaajan tai Pelaajatiimin ympäristössä.	Punainen tiimi kerää jalansijaohjelman kautta esimerkiksi skripteillä tietoa, joka osoittaa jalansijan kohdejärjestelmässä syntyneen. Tieto kootaan Vihreän tiimin hallitsemalle alueelle ja tiedon lukeminen mahdollistetaan Punaiselle ja Valkoiselle tiimille

Konseptin päätelmä

Tämä konsepti alkoi keskittymisellä fyysisen Mini-Sairaala Kybersimulaatio -ympäristön luomiseen—elämykselliseen harjoitustilaan, joka on suunniteltu simuloimaan teknisiä häiriöitä kliinisissä ympäristöissä. Projektin edetessä kaksi muuta ratkaisua osoittautui kuitenkin joustavammiksi, skaalautuvammiksi ja kustannustehokkaammiksi: VirtualLab ja työpöytäharjoitusalusta.

Vaikka Mini-Sairaala-konsepti tarjoaa pedagogista syvyyttä ja realismia, sen pitkäaikainen toteutettavuus on rajattu korkeiden infrastruktuurikulujen, henkilöstötarpeiden sekä rajallisen lähialueen terveydenhuollon toimijoiden määrän vuoksi, jotka voisivat säännöllisesti hyötyä paikan päällä toteutettavasta koulutuksesta. Arviolta 30–40 osallistuvaan organisaatioon vuodessa perustuva kestävyyden alaraja tarkoittaa, että tällaisen tilan ylläpitoa ei voida perustella ilman merkittäviä jatkuvia tukia tai valtakunnallisen tason institutionaalista tukea.

Kehitysprosessin aikana kävi ilmi, että VirtualLab ja työpöytäharjoitusalusta tuottavat suurimmalle osalle kohderyhmistä samankaltaisia harjoitustuloksia huomattavasti pienemmillä kustannuksilla ja laajemmalla saavutettavuudella. Rakentamalla Mini-Sairaala-skenaario uudelleen VirtualLab-pohjaiseksi harjoitukseksi—toteutettuna kannettavilla tietokoneilla olemassa olevissa tiloissa—konsepti säilyttää pedagogisen vahvuutensa, mutta poistaa tarpeen fyysisille muutostöille, tarkkailutilojen integroinnille ja räätälöidylle infrastruktuurille.

Jotta tämä muutos onnistuisi, VirtualLabin on oltava vakaa, intuitiivinen ja hyvin tuettu, ja sen on kyettävä käsittelemään monipuolisia skenaariopohjaisia harjoituksia niin teknisillä kuin ei-teknisilläkin osa-alueilla. Tämä edellyttää kohdennettua panostusta alustan kehittämiseen, automaatioon ja jatkuvaan tekniseen ylläpitoon.

Suositus

Suunnataan kehityksen painopisteet ja rahoitus VirtualLab- ja työpöytäharjoituskokonaisuuksiin, jotka ovat nousseet harjoitusmallin vahvemmiksi ja muuntautumiskykyisemmiksi tukipilareiksi. Ne mahdollistavat laajemman käyttöönoton, pienemmän operatiivisen riskin sekä joustavuuden kasvaa osaksi kansallisia ja kansainvälisiä koulutusekosysteemejä—säilyttäen samalla alkuperäisen vision sosiaali- ja terveydenhuollon valmistamisesta tulevaisuuden kyberuhkiin.

Viitteet ja lähteet

Abad, A. H., Corbiaux, S., Ifigeneia, L., Theocharidou, M. 2023. Enisa Threat Landscape: Health Sector. European Union Agency for Cybersecurity. PDF-dokumentti. Saatavissa: https://www.enisa.europa.eu/publications/health-threat-landscape [viitattu 8.2.2025]

Directive (EU) 2022/2555 of the European Parliament and of the Council

Advanced and unique cyber range. Jyvsectec by jamk. WWW-dokumentti. Saatavissa: https://jyvsectec.fi/en/realistic-global-cyber-environment/ [viitattu 3.11.2025]

Rantakoski, T. 2023. Sote-yritykset tehostaisivat hyvinvointialueiden palveluja – Ministeri: Erikokoisia toimijoita tarvitaan. Yrittäjät. Artikkeli. Saatavissa: https://www.yrittajat.fi/uutiset/sote-yritykset-tehostaisivat-hyvinvointialueiden-palveluja-ministeri-erikokoisia-toimijoita-tarvitaan/ [viitattu 2.6.2025]

Cybersecurity Act (NIS2). Valvira. WWW-dokumentti. Saatavissa: https://valvira.fi/en/healthcare-and-social-welfare/cybersecurity-act [viitattu 3.11.2025]