

KyberSoTe – Kyberturvallisuutta sote-arkeen

Sote-alan ammattilaisten kyberosaamista ja eri ammattiryhmien välistä yhteistyötä vahvistamassa

Projektin päätavoitteena on sosiaali- ja terveydenhuollon organisaatioiden varautumisen, palveluiden jatkuvuuden ja potilasturvallisuuden edistäminen.

Tähän tähdätään kahdesta näkökulmasta:

1. Lisäämällä sote-alan ammattilaisten kyberturvallisuusosaamista ja kyberturvallisten toimintamallien hyödyntämistä.
2. Vahvistamalla soten ja tietohallinnon ammattilaisten välistä yhteistyötä/vuorovaikutusta kyberturvallisuuden osalta.

Toteutusaika:

12.2.2024 – 31.12.2026

Rahoitusohjelma:

Digitaalinen turvallisuus 2030
(Huoltovarmuuskeskus)

Toteuttajat:

Jamk, LAUREA, Turku amk, TAMK

Yhteistyökumppanit:

Keski-Suomen hyvinvointialue
Pirkanmaan hyvinvointialue
Päijät-Hämeen hyvinvointialue
Vantaan ja Keravan hyvinvointialue
Varsinais-Suomen hyvinvointialue

Ota projekti seurantaan!
www.jamk.fi/kybersote



Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency



AMMATTIKORKEAKOULU
University of Applied Sciences

TURKU AMK 

 Tampereen
ammattikorkeakoulu

jamk

Janine Klauenbösch,
kyberturvallisuusinsinööri,
KyberSoTe-projektin asiantuntija



Johanna Niskakangas, lehtori,
KyberSoTe-projektin
projektipäällikkö

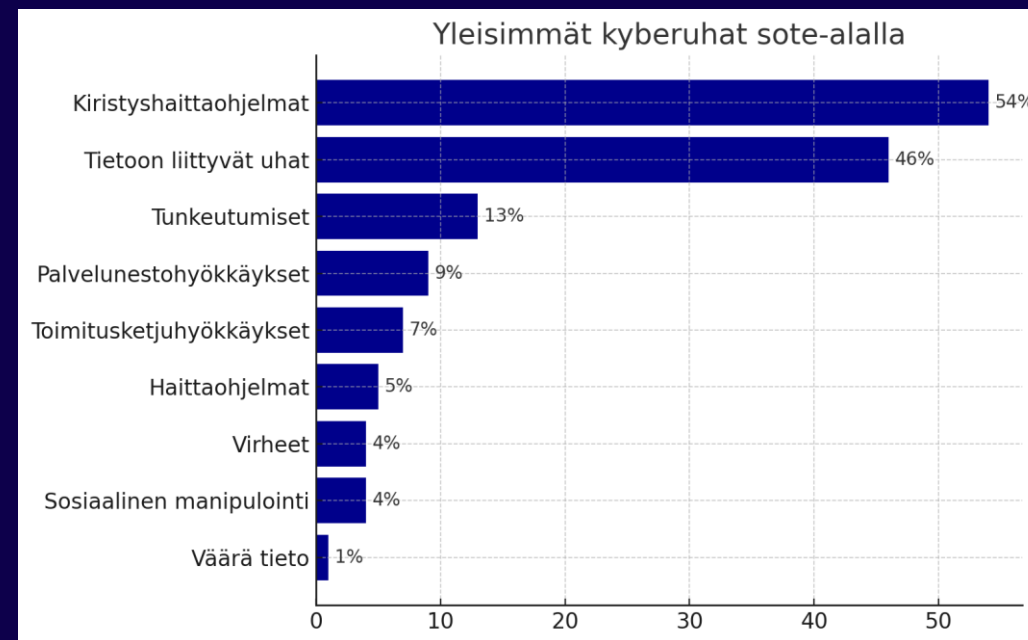


Uutisotsikoista...

- **”Kyberhyökkäys horjuttaa yhä Lahden terveystalouksia – Krp: ”Kaikki voitava tehdään, että pahuuden levittäjä saadaan kiinni” (Yle 13.6.2019)**
Vielä ei tiedetä, oliko hyökkäyksen takana hakkerijoukko vai yksittäinen tekijä.”
- **”Nainen kuoli ambulanssiin, kun kyberhyökkäys jumitti saksalaisen sairaalan tietojärjestelmän – syyttäjä avasi harvinaisen henkirikostutkimuksen (Yle 19.9.2020)**
Jos tutkimukset johtavat syytteeseen, on kyseessä Reutersin mukaan ensimmäinen kerta, kun ihmisen kuolema on suoraan yhdistetty kyberhyökkäykseen. Rikosnimikkeenä olisi kuolemantuottamus.”
- **”Terveystalo on tietojenkalastelijoille mieluisa kohde, ja siksi kyberuhkia opetellaan torjumaan yhä tanakammin (Yle 30.10.2024)**
Tietojenkalastelua ja huijausviestejä ropisee sähköposteihin myös sosiaali- ja terveystalolla. Huijauksiin varaudutaan yhä paremmin ja tilanteita myös harjoitellaan.”

Tilannekatsaus

- Kiristyshaittaohjelmat sekä tietolähteisiin kohdenetut hyökkäykset ovat yleisimpiä (ENISA 2023)
- Todennäköisesti hyökkäyksiä ja niiden yrityksiä tapahtuu huomattavasti enemmän, kuin mitä viranomaisten tilastoihin päätyy
- Yhdysvaltalaisen tutkimuksen mukaan 88 % sote-organisaatioista ilmoitti joutuneensa vähintään yhden kyberhyökkäyksen kohteeksi viimeksi kuluneen vuoden aikana. Keskimäärin kyseisiin organisaatioihin kohdistui vuoden aikana 40 kyberhyökkäystä (Ponemon Institute, 2023)
- Hyökkäyksen seurauksena arkaluontoiset asiakas- ja potilastiedot sekä potilasturvallisuus voivat vaarantua.
- Asiakas- ja potilastiedot arvokkaita, jopa 10-kertainen arvo luottokorttitietoihin verrattuna



Kuva mukaillen: *Enisa Threat Landscape: Health Sector, 2023*

Tilannekatsaus

- Suuri osa kyberhyökkäyksistä vaatii onnistuakseen inhimillisen osan tai tekijän, kuten haitallisen linkin klikkaamisen > Meidän on tärkeä tunnistaa uhat ja toimia valppaasti
- Tutkimus osoittaa, että 45% kaikista havaituista tietomurroista terveydenhuollossa olisi ollut estettävissä pienillä teoilla (Goud 2026)
- Tutkimusten perusteella sote-alan työntekijöiden kyberturvallisuusosaaminen ja -käyttäytyminen vaihtelevat paljon. Taso vaihtelee hyvän ja heikon välillä, eli mukana on sekä vahvuuksia että merkittäviä puutteita (Bhaskar 2025)
- Sosiaali- ja terveysalan henkilöstön keskuudessa vielä tiedon vajausta (mm. Rajamäki ym. 2023)
 - Kyberturvallisuusuhat ja -riskit
 - Oman toiminnan vaikutukset organisaation kyberturvallisuuteen
- **Valtaosalla sote-henkilöstöstä (84 %) on kiinnostusta lisäkoulutukseen tietoturvasta, tietosuojasta ja kyberturvallisuudesta** (Blek ym. 2023)



Sote-ammattilaisten osaamistarpeita uudistetaan

Esimerkkinä oikealla
sairaanhoidajan ydinosaamisen
(180 op)uudet
osaamisvaatimukset ja niiden
sisällöt

Informaatioteknologia ja dokumentointi

- 1) Osaa noudattaa tietojen tuottamisessa, käytössä, säilyttämisessä ja hävittämisessä sosiaali- ja terveydenhuollon tietosuojaja- ja kyberturvallisuusvaatimuksia sekä säädöksiä.
 - Tietosuojaja- ja -turva sekä lainsäädäntö ja muu ohjeistus eri toimintaympäristöissä
 - Asiakkaan tuottaman terveystiedon ja hyvinvointitiedon tunnistaminen ja käyttö
 - Vastuullinen ja turvallinen tietojärjestelmien ja sosiaalisen median käyttö
- 2) Osaa dokumentoida asiakkaan/potilaan hoitotyön prosessin tarvelähtöisesti.
 - Hoitotyön rakenteinen dokumentointi
 - Reaaliaikaisen tiedon tuottaminen, tiedon arviointi ja hyödyntäminen
- 3) Ymmärtää tekoälyn toimintaperiaatteet ja osaa hyödyntää tekoälyä vastuullisesti hoitotyössä.
 - Tiedonlukutaito tekoälyn käytössä
 - Tekoälyn hyödyntäminen hoitotyössä
 - Tekoälyn eettiset ja ammatilliset näkökulmat

Sote-ammattilaiset keskiössä

Teknisillä keinoilla voidaan suojautua kyberrikoksia vastaan, mutta valistuneen henkilöstön ja vahvan tietoturvakulttuurin puuttuminen jättävät organisaation suojauksen vajaaksi (Kamerer & McDermott 2020) → Ihmispalomuuuri!



Oma kyberturvallinen tapa toimia



Laitteisiin ja välineisiin liittyvien kyberturvallisuusuhkien tunnistaminen



Kyberhäiriöiden vaikutusten tunnistaminen



Kyberhäiriötilanteessa toimiminen

Kyberhygienia

Kyberhygienialla viitataan yksinkertaisiin käytäntöihin ja toimenpiteisiin, joita me kaikki voimme toteuttaa suojellaksemme tietoja, laitteita ja järjestelmiä kyberuhkilta.

Tavoitteena on estää “tartunnat”, kuten virukset, madot, troijalaiset...

Kyberhygieniasta huolehtiminen on kuin huolehtisit käsihygieniasta. Ethän jätä käsidesiäkään käyttämättä.



10 KyberSoTe-projektissa tunnistettua uhkacasea

1. Tietojenkalastelu- ja huijausviestien tunnistaminen

2. Turvallinen tekoälyn käyttö

3. Valppaus etätyössä

4. Tietojen turvaaminen ulkopuolisilta, esim. shoulder surfing

5. Laitteiden lukitseminen ja kulkulupien tarkastaminen

6. Turvallinen tunnusten ja salasanojen hallinta

7. Turvalliset salasanaikäytännöt

8. Verkkoon kytkettyihin laitteisiin liittyvien riskien tunnistaminen (IoT/IoMT)

9. Ulkoisiin laitteisiin liittyvien riskien tunnistaminen (esim. USB-tikku, puhelin)

10. Turvalliset tiedon tallentamisen ja jakamisen käytännöt



Muistetaan kyberhygienia arjessa!

Näin voi oikeasti käydä! Ei pidetä asioita itsestään selvinä vaan muistetaan kyberhygienia arjessa!



Iltalehden otsikossa 29.1.2026

”Tietokone jätettiin valvomatta sairaalan käytävälle: Arkaluontoiset potilastiedot kaikkien nähtävillä Kuka tahansa olisi voinut päästä käsiksi potilaan henkilö- ja hoitotietoihin Husin Meilahden kolmiosairaan käytävällä olevalla tietokoneella keskiviikkona.”



Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency



AMMATTIKORKEAKOULU
University of Applied Sciences

TURKU AMK 

 **Tampereen
ammattikorkeakoulu**

jamk

VERKKOKOULUTUS

Sote-alalle räätälöity ja käyttäjälähtöisesti kehitetty kyberturvallisuuskoulutus (~2 h) vaatii osallistujalta enemmän kuin klikkaamista.

Koulutus sisältää:

- 10 Case -esimerkkiä sotekentän arjesta (tosielämän esimerkeistä uutisoitiin tammikuussa 2026).
- Pelillisyyden avulla syvennetään opittua.

Hyödyt:

- Osaavat ja koulutetut sote-ammattilaiset luovat pohjan varautuneelle organisaatiolle.
- Valmiiksi käyttöön otettava, maksuton koulutusratkaisu kyber- ja tietoturvaosaamiseen kehittämiseen.
- Siirrettävissä organisaation omaan Moodle-ympäristöön.

KYBERAGENTTI TOIMINTAMALLI - sillanrakentajana eri ammattiryhmien välillä

Kyberagentin rooli:

- Jakaa HVAn vinkkejä, ohjeita ja toimivia käytäntöjä sote-yksikön sekä tekee tieto- ja kyberturvallisuuden jatkuvasti näkyväksi.

Kyberagentin työkalut:

- Käsikirja
- Verkosto
- Tsekkilistat, kyberkortit, kyberkävelyt, kyberständit
- Suusta suuhun kulkeva tieto on yksi tehokkaimmista tapoista levittää tietoa.

Hyödyt:

- Vahvistaa kyberturvallista arkea ja toimintakulttuuria sote-yksikössä.
- Tehostaa kyberhygieniakäytäntöjä ja hoksauttaa vaaranpaikoista.
- Pitää kyberturvan aktiivisesti esillä ja toimii yhteyshenkilönä tietoturvapäälikölle.
- Tukee kollegoita tietoturvaohjeissa ja antaa rakentavaa palautetta.

KyberSoTen työkalut

VUOROVAIKUTUKSEN KEHITTÄMISMALLI

Sote- ja ICT-ammattilaisten vuorovaikutuksen ja yhteistyön kehittämiseksi.

Kehittämismallin työkalut:

- Mallipohja ja ohjeet työpajojen fasilitoijalle.
- Havainnekuvat keskustelun herättämiseksi (viisi case-esimerkkiä haastavista tilanteista).
- Ohjeistus kehityskohteiden jalkauttamiseen.

Hyödyt:

- Varautunut organisaatio yhteiseen hiileen puhaltamalla.
- Lisääntynyt yhteinen ymmärrys ja luottamus eri ammattiryhmien välillä.
- Ohjeita noudatetaan ja niihin sitoudutaan paremmin, kun ymmärretään toista.
- Tehokas ja henkilöstöä osallistava päätöksenteko.

OSAAMISKARTOITUSKYSELY

Kyselyllä kartoitetaan henkilöstön tieto- ja kyberturvallisuusosaamista tietojen, taitojen ja asenteiden näkökulmasta. Kysely integroidaan organisaation omiin kyselytyökaluihin.

Tuloksia hyödyntää:

- HVA:n johto
- Tietoturvapäälikkö
- Yksikön johto
- Cyberagentti

Hyödyt:

- Osaamistason tuntemisesta tukea kehittämistoimenpiteiden tarkoituksenmukaiseen suuntaamiseen.
- koulutusten suunnittelu
- tietoturvakäytäntöjen kehittäminen
- toimintatapojen arviointi
- riskienhallinta
- seuranta ja jatkuva parantaminen.

Kokemuksia piloteista

KyberSoTen verkkokoulutus:

- Lähes 100 ammattilaista tehnyt jo loppuun
- Videoista ja konkreettisista case-esimerkeistä paljon positiivista palautetta
- Useissa palautteissa korostui aiheen tärkeys
- Selkeimpinä kehittämis ehdotuksina koulutuksen pituus ja navigointi oppimisalustalla > pyritty tiivistämään, koulutuksen kesto arviolta 2 h

Suosittelisin tätä verkkokurssia myös muille

**83 % suosittelisi
(n = 36)
(täysin samaa tai
jokseenkin samaa
mieltä)**

Tervetuloa opiskelemaan sosiaali- ja terveysalan kyberturvallisuuteen liittyviä teemoja!

Käytyäsi tämän koulutuksen:

- *Ymmärrät kyberturvallisuuteen liittyvät keskeiset käsitteet ja ilmiöt sosiaali- ja terveysalalla*
- *Tiedät, millaisia vaikutuksia kyberhyökkäyksillä saattaa olla sosiaali- ja terveysalalla*
- *Ymmärrät oman ammattiryhmäsi kyberturvallisen toiminnan merkityksen käytännössä*
- *Tunnistat oman roolisi organisaation kyberturvallisuuden varmistamisessa*



Huoltovarmuuskentus
Försörjningsberedskapscentralen
National Emergency Supply Agency



AMMATTIKORKEAKOULU
University of Applied Sciences

TURKU AMK 

 Tampereen
ammattikorkeakoulu

jamk

Oppilaitokset tulevien sote-ammattilaisten kouluttajina

Tavoitteena kyberturvallisuusteemojen sisällyttäminen tulevien sote-ammattilaisten koulutukseen läpileikkaavana teemana

- Pilotoidaan myös sote-alan ammattikorkeakouluopettajille suunnattua koulutusta
- Tuodaan työkaluja ja pedagogisia malleja sote-alan opettajien saataville
- KyberSoTe-projektissa tunnistettua:
 - Miten kyberosaamisen kehittyminen huomioidaan jo koulutuksen aikana? > tarvitaan osaavat ammattilaiset töihin
 - Opettajien kautta opiskelijoille (tulevat sote-ammattilaiset) kerrytetty ja jaettu osaaminen mahdollista pysyä pitkään ”aktiivisena”



Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency



AMMATTIKORKEAKOULU
University of Applied Sciences

TURKU AMK 



Tampereen
ammattikorkeakoulu

jamk

Taklataanko teillä inhimillisistä virheistä johtuvia kyberhaasteita?

Nyt on oikea hetki toimia.

KyberSoTen ratkaisut muodostuvat havainnollistavista, toiminnallisista ja audiovisuaalista koulutusmateriaaleista sekä käyttövalmiista kyberturvallisuuden työkaluista, jotka on kehitetty ja räätälöity yhteistyössä viiden hyvinvointialueen kanssa.

Huoltovarmuuskeskuksen rahoittamassa projektissa kyber- ja sotealan todellisuudet kohtaavat.
Tue henkilöstön osaamista ja vahvista organisaatiosi varautumista nopeasti ja käytännönlähteisesti.

Milloin ja mistä?

Heti saatavilla: Osaamiskartoituskysely saatavilla KyberSoTen verkkosivuilta, Forms-pohja pyydettäessä

04/2026: Verkkokoulutus avoimna DigiCampuksen Moodlessa (päivitykset 31.12.2026 asti),
Moodle-tiedostopaketti

04/2026: Yhteistyön ja vuorovaikutuksen kehittämismalli (+työpohjat) ladattavissa KyberSoTen verkkosivuilta.

08/2026: Kyberagentin roolikuvaus, käsikirja ja työkalut löydettävissä KyberSoTen verkkosivuilta.

Syksy 2026: Opettajille suunnattu verkkokoulutus avoimeksi DigiCampukseen



KYY-hankkeessa tuotetut oppimateriaalit

- ”Kyberturvallisuuden opintojakso työntekijänäkökulmasta. Opintojakso on kohdennettu alan työntekijälle ja jaksoa tarkastellaan työntekijän ja yksityishenkilön näkökulmasta. Toteutettu OKM rahoitteessa hankkeessa: Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa Työpaketissa 1.4.”
 - Ovaska, Joonatan (Jamk) & Kallio, Annika (Laurea)
- <https://aoe.fi/#/materiaali/5058>

Kiitos!



Johanna Niskakangas, johanna.niskakangas@jamk.fi
Janine Klauenbösch, janine.klauenbosch@jamk.fi



Jyväskylän ammattikorkeakoulu, Piippukatu 2, 40100 Jyväskylä

KyberSoTe-projektissa julkaistavat työkalut tulevat projektin verkkosivuille vuonna 2026: www.jamk.fi/kybersote