ISO/IEC 27001

CERTIFIED BY

huld | Certification

# Tietoturva sote-alalla

Digivointi

Opsec Oy

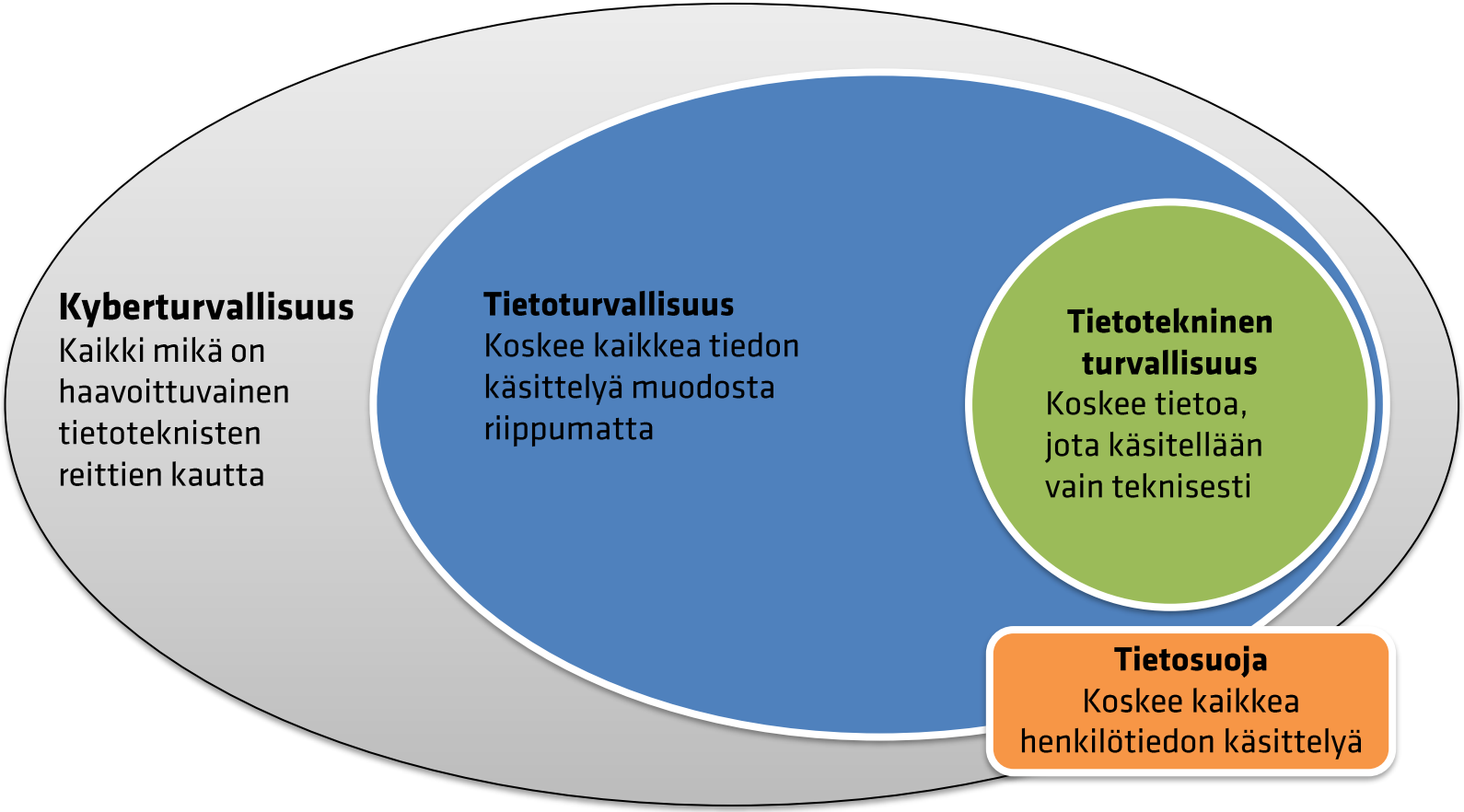
opsec

ISO/IEC 27001

CERTIFIED BY

huld | Certification

# KYBERTURVALLISUUS




Kyberturvallisuus tänä päivänä melko usein viittaa laajasti tietoturvallisuuteen.

## Ransomware attack forces French hospital to transfer patients

By Sergiu Gatlan

December 5, 2022 03:41 PM 0

## Brooklyn hospital network reverts to paper charts for weeks after cyberattack

By Sean Lyngaas, CNN
Published 7:53 AM EST, Tue December 20, 2022


Kunnat

## Suun terveydenhuollon aikoja joudutaan yhä siirtämään Säkylässä – taustalla joulukuun kyberhyökkäys

Suun terveydenhuollon asiakkaita pyydetään ottamaan yhteyttä aikojen siirtämiseksi.

Etusivu / Etusivu

## Tietoverkkoon tehty kyberhyökkäys lamaannutti terveysasemien toiminnan Lahdessa - Nastola häiriön ulkopuolella

# Toimijat kybermaailmassa

**Rikolliset**


**Aktivistit ja muut toimijat**

**Valtiolliset toimijat**

Hacker Photo by Sora Shimazaki: https://www.pexels.com/photo/crop-cyber-spy-hacking-system-while-typing-on-laptop-5935794/
Activist photo by Nick Youngson CC BY-SA 3.0 Pix4free

# Kyberuhkien tyyppejä

**Onnettomuudet, vahingot, virheet, laiterikot**

- Laiterikot
  - Palvelimien ja verkkolaitteiden vikaantumisten aiheuttamat katkokset
- Sähkönsyötön häiriöt, muut kiinteistöön sekä infrastruktuurin kohdistuvat häiriöt
  - Tulipalot, alueelliset laajemmat viat
- Prosessien kypsymättömyys ja virheet
  - Prosessien puuttuminen tai niiden kypsymättömyys - muutoshallinta
- Toimittajariskit
  - Toimittajan tai alihankkijan toiminnasta johtuvat katkot ja muut häiriöt
- Luonnonkatastrofit, sodat, pandemiat

**Rikollisuus ja väärinkäytökset**

- Sisäinen uhka, toimittajariski
  - Merkittävässä roolissa etenkin tietovuotojen kohdalla.
- Palvelunestohyökkäykset
  - Pyritään estämään palveluiden käyttö ja organisaation toiminta.
- Haittaohjelmien levitys ja tunkeutuminen verkkoon
  - Linkit viesteissä minkä avulla levitetään viruksia ja etähallintasovelluksia.
  - Tietojenkalastelu (phishing)
- Kiristyshaittaohjelmat – ransomware

# Kyberuhkien luonne

**Onnettomuudet, vahingot, virheet, laiterikot**

- **Odottamattomia tilanteita**
  - Varautumisesta huolimatta onnettomuusriskit aina olemassa
- **Vaikutusmahdollisuuksien ulkopuolella**
  - Osaan tilanteista, kuten pandemiat ja sodat, ei yksittäisellä toimijalla mahdollista vaikuttaa
- **Varautuminen vaatii panostuksia henkilöstöön ja tiloihin sekä laitteisiin**
  - Varautumisen keinoina usein varalaitteistot, väistötilat, varahenkilöt ja prosessit

*Kenen papereissa oli pandemia todellisena riskinä ennen koronaa? – Tuntematon pohtija 2021 syksyllä*

*Kuka oikeasti varautui täysimittaiseen sotaan Euroopassa 2022? – Tuntematon pohtija 2022 kesällä*

**Rikollisuus ja väärinkäytökset**

- **Hyvin pitkälle automatisoitua**
  - Kaikki internettiin auki olevat palvelut ovat jatkuvasti erilaisten hyökkäyskokeilujen kohteena.
- **Luonteeltaan opportunistista**
  - Kohdetta tutkitaan, kun sisään on päästy.
  - Kohdetta pyritään hyödyntämään mahdollisimman paljon.
- **Kansainvälistä**
  - Verkossa ei fyysisiä rajoitteita, joten kaikki olemme yhtä lähellä ja kaukana rikollisuuden näkökulmasta.

*Järjestäytyneet rikollisjengit, jotka ovat rahan perässä. Se on maantieteellisesti riippumatonta. Se on myös demokraattista, koska se kohdistuu kaikkiin tasapuolisesti, Hyppönen sanoi. Ilta-Sanomat 1.6.2022*

# Kyberuhkien seurauksia

- Suorat rahalliset menetykset
  - Toimitusten (palvelut ja tavarat) häiriöt
  - Saamatta jääneet tilaukset
- Välilliset menetykset ja haitat
  - Imagolliset haitat toiminnan häiriöistä
- Toipumisen ja palautumisen kustannukset
- Uhka yksityisyydensuojalle ja terveydelle
  - Henkilötietojen paljastuminen
  - Kriittisen infrastruktuurin ja terveydenhuollon järjestelmät
- Sakot ja vahingonkorvaukset
  - Sopimussakot syynä esimerkiksi toimitusten viivästyminen tai palvelukatkot
  - Sakot ja vahingonkorvaukset– tietosuoja-asetus 32 artiklan 1.kohta
    - *b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;*
    - *c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;*

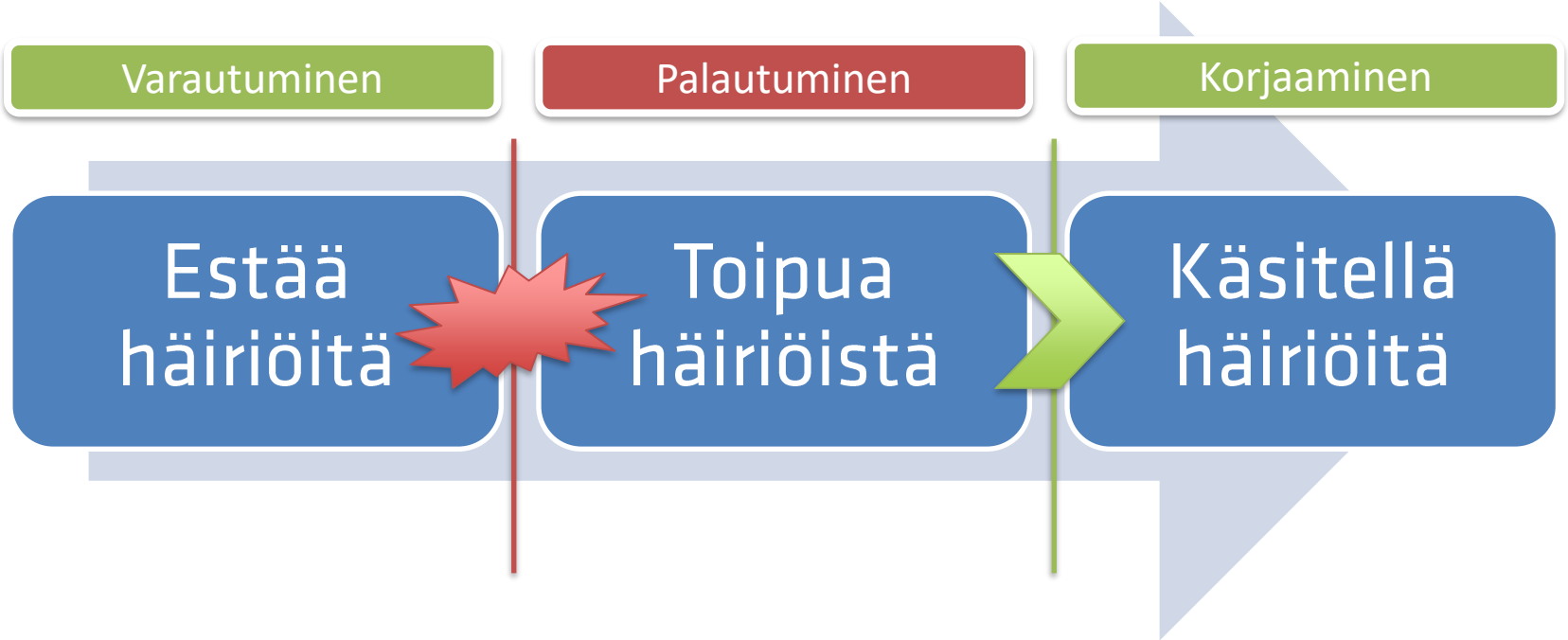
opsec

ISO/IEC 27001
CERTIFIED BY
huld | Certification

# KYBERTURVALLISUUSTOIMET

# Kyberturvallisuustoimet

- Varautuminen
  - Tunnista vaatimukset ja riskit
  - Tee varautumistoimet
- Havainnoi
  - Hanki tilannetietoa
  - Tunnista uhkaavat tilanteet
- Vastatoimet
  - Palauta toimintakyky
  - Palaudu normaalitilaan


Varautuminen
Palautuminen
Korjaaminen
Estää häiriöitä
Toipua häiriöistä
Käsitellä häiriöitä

# Ennakoinnin ensimmäiset askeleet

- Aloita perusteista ja tärkeimmistä asioista
  - Älä yritä ensimmäisellä kierroksella kattaa kaikkea.

- Tunnista ja arvioi
  - Vaatimukset – sopimukset ja lait
    - THL:n määräys 3/2021 Tietoturvasuunnitelma
    - Tietosuoja-asetus
  - Riskit – todennäköisyys ja vaikutus

    **-> Toimenpiteiden oikea kohdennus**

- Teknisten keinojen lisäksi toimintaohjeet, koulutus ja sopimukset
  - Henkilöstön tietoisuus ja motivaatio tärkeä tekijä turvallisuuden ylläpitämisessä

# Työkalu (ja osalle vaatimus)

## Tietoturvasuunnitelma

Tietoturvasuunnitelman laatimisvelvoite koskee kaikkia sosiaali- ja terveydenhuollon palvelunantajia, apteekkeja sekä Kanta-välityspalveluiden tuottajia ja Kelaa.

Sosiaali- ja terveydenhuollon palvelunantajat sekä apteekit huolehtivat omavalvonnan kautta siitä, että heillä on asianmukaiset tietoturva- ja tietosuojakäytännöt arkaluonteisten asiakastietojen suojaamiseksi ja niitä noudatetaan käsitellessä asiakas- ja potilastietoja.

Lähde https://www.kanta.fi/ammattilaiset/tietoturvasuunnitelma

# Tietoturvasuunnitelma – soveltaen organisaatioon

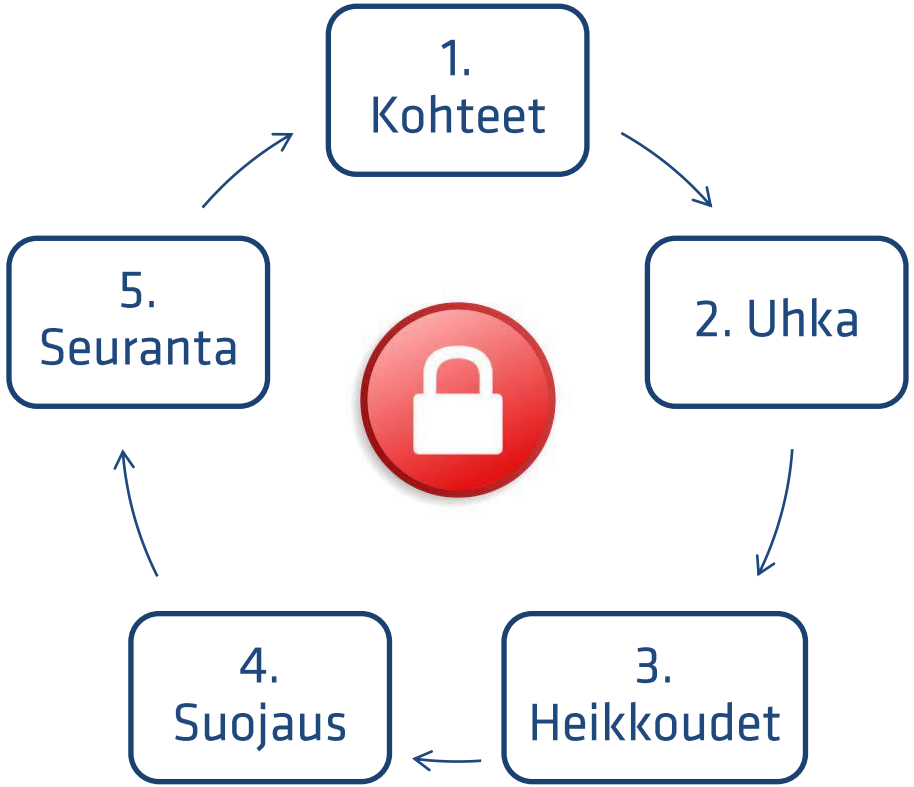
Tietoturvasuunnitelman laatiminen ohjaa ennakointityötä.

Mallipohja
https://thl.fi/documents/9204422816495/THL_Maarays_3_2021_liite_1_Tietoturvasuunnitelman_mallipohja.docx/f37d6a8c-1fe9-cfba-ccc6-f448ba2bc506?t=1640009534893



Lähde https://www.kanta.fi/documents/20143/1740138/Tietoturvasuunnitelman-esittely.pdf/7c890222-f375-62f7-8dc7-db5144adc67e?t=1644997872277

1. Mikä meillä on tärkeää? Mitä ilman ei toiminta jatku?
   - Tieto, työvälineet, tietojärjestelmät, henkilöt, tilat…
2. Mikä (kohteita) uhkaa?
   - Onnettomuusriskit, ulkoinen mielenkiinto, kilpailija, aktivistiryhmä…?
3. Mitä heikkouksia kohteiden suojaamiseen uhkiin nähden liittyy?
   - Yhtä lailla varahenkilöt, lukitukset kuin tietojärjestelmätestaus
4. Miten kohteet pitää suojata heikkoudet ja uhat huomioiden?
   - Hyvin suunniteltu on jo puoliksi tehty – toisaalta liian täydellistä suunnitelmaa ei kukaan ehdi koskaan toteuttaa
5. Seuranta
   - Seuraa toimintaa ja paranna sen perusteella



# Havainnointi

**Inhimilliset sensorit**
Henkilöstö
Kumppanit ja asiakkaat
Verkostot
Tiedotteet
KOULUTA

**Tunnusmerkit**

*Hiljaiset signaalit*

Poikkeama normaalista

HÄLYTYS

**Tekniset sensorit**
Tietoturvasovellus
Valvontajärjestelmät
Manuaalinen tarkastus

VAATII SEURANTAA

# Vastatoimet

**Varautuminen**
Tietojen salaus
Tietojen varmistus
Varmistuksen valvonta
Palautumisen testaus
Päivitykset

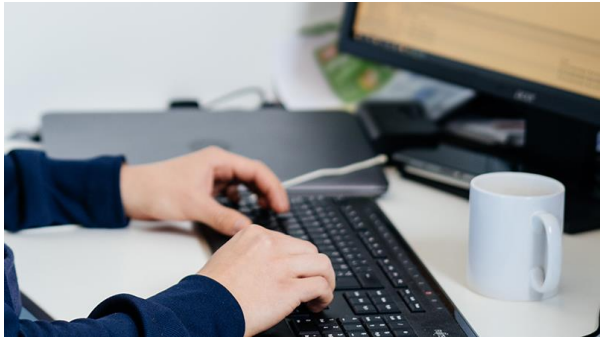
Backup by Nick Youngson CC BY-SA 3.0 Pix4free

**Henkilöstö ja ohjeet**
Toimintaohjeet
Koulutus
Sovitut menettelyt johtamiseen

Staff training by Nick Youngson CC BY-SA 3.0 Pix4free

**Muista ENNAKOINTI – kohta 1**

**Asiantuntija avustaa**
Ennakoinnissa
Palautumisessa
Tutkinnassa
Viranomaisilmoituksissa
- tietosuoja 72 tuntia



# Tarkistuslista

**Hallinnolliset toimet**

Onko meillä tietoturvasuunnitelma?
- Tietoturvakäytännöt
- Häiriötilanteissa toiminta
- Koulutus
- Käyttövaltuushallinta

Koskee meitä muut lainsäädännölliset tai sopimukselliset velvoitteet (tietoturvassa)?

Olemmeko arvioineet riskit ja tehneet toimia niiden hallitsemiseksi?

Muutosten hallinta ja hankinnat –tietoturvan huomiointi

**Tekniset toimet**

Tietoturvasovellus – virustorjunta ja sen valvonta

Ohjelmistojen ja päätelaitteiden päivitykset

Päätelaitteiden salaus

Varmistukset ja niiden valvonta sekä testaus
- Myös pilvipalveluiden varmistus selvitettävä

Käyttäjien hallinta ja salasana käytännöt

**KUMPPANIT JA TOIMITTAJAT - VARMISTA TIETOTURVATASO**

opsec

ISO/IEC 27001

CERTIFIED BY

huld | Certification

# OPSEC OY

# Opsec Oy

Opsec Oy on kotimainen ja yksityisessä omistuksessa oleva IT-alan asiantuntijayritys, joka on perustettu vuonna 2009. Yrityksen toimitilat sijaitsevat Framilla, joka Seinäjoen merkittävin yritysten ja tutkimus- ja koulutustoimijoiden keskittymä. Toinen toimipiste sijaitsee Tampereella.

Opsec Oy:n palvelut koostuvat tietohallinnon, tietoturvan ja tietosuojan asiantuntija- ja kehityspalveluista sekä IT-ympäristön valvonta-, ylläpito- ja tukipalveluista.

Opsec Oy:n toiminta koostuu Suomessa ja Suomesta käsin toimivien yritysten liiketoiminnan kehittämisestä ja tukemisesta tietohallinnon, tietoturvan ja tietosuojan osalta. Yrityksen kansainvälinen toiminta koostuu asiakkaiden kansainvälisen liiketoiminnan kehittämisestä.

Opsec Oy:llä on turvallisuusalan elinkeinolupa rikoksen paljastamiseen johtavaan IT-tutkintaan.

Opsec Oy:lle on myönnetty tietoturvallisuuden hallintajärjestelmän sertifikaatti standardin ISO/IEC 27001:2013 mukaisesti.

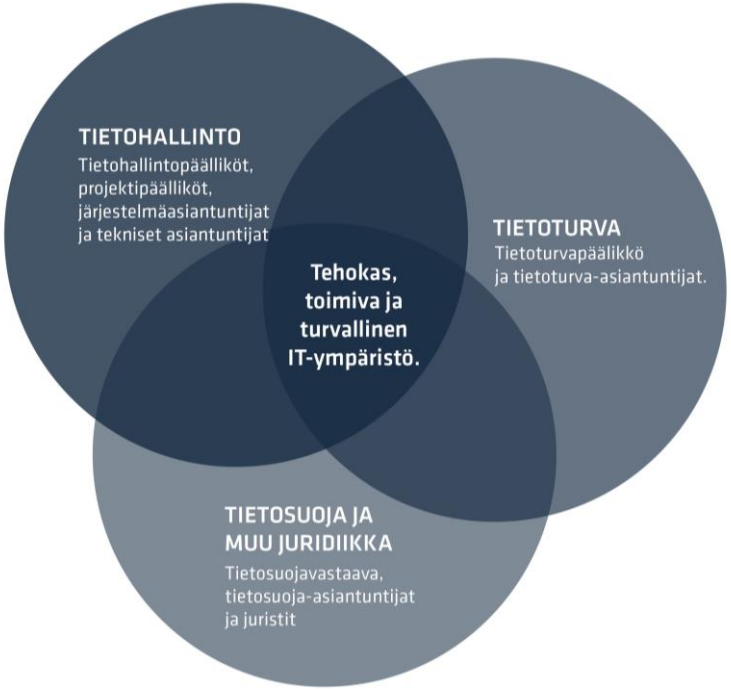
# Opsec Oy

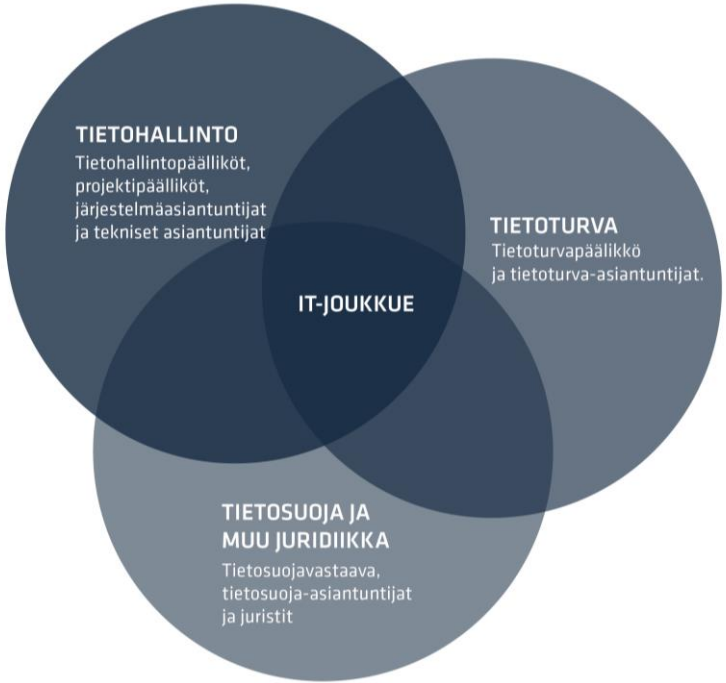
Opsec Oy:n asiantuntijat auttavat ja tukevat asiakkaita menestymään omassa ydinliiketoiminnassaan tuottamalla laadukkaita ja asiakkaan liiketoimintaa tukevia IT-ympäristön kokonaispalveluja.

Opsec Oy:n vahvuus IT-palveluiden kokonaistuottajana on sekä hallinnollisen että teknisen IT-ympäristön asiantuntija- ja projektiosaaminen, kehityssuunnitelmien ja –vaiheiden toteuttaminen, päivittäinen IT-ympäristön valvonta ja ylläpito sekä laadukas tekninen asiakaspalvelu. Lisäksi Opsec Oy:n asiantuntijat toimivat kouluttajina sekä asiakasympäristöissä että omissa ja yhteistyökumppaneiden koulutustilaisuuksissa.

Asiakas saa Opsec Oy:n palveluita hankkiessaan käyttöönsä aina joukkueellisen asiantuntijoita, jotka käyvät yhdessä läpi asiakkaiden digitaaliseen ympäristöön liittyviä ratkaisuja ja jotka jakavat osaamista keskenään. Näin asiakas saa aina laaja-alaista IT-ympäristön syväosaamista liiketoimintansa tueksi.

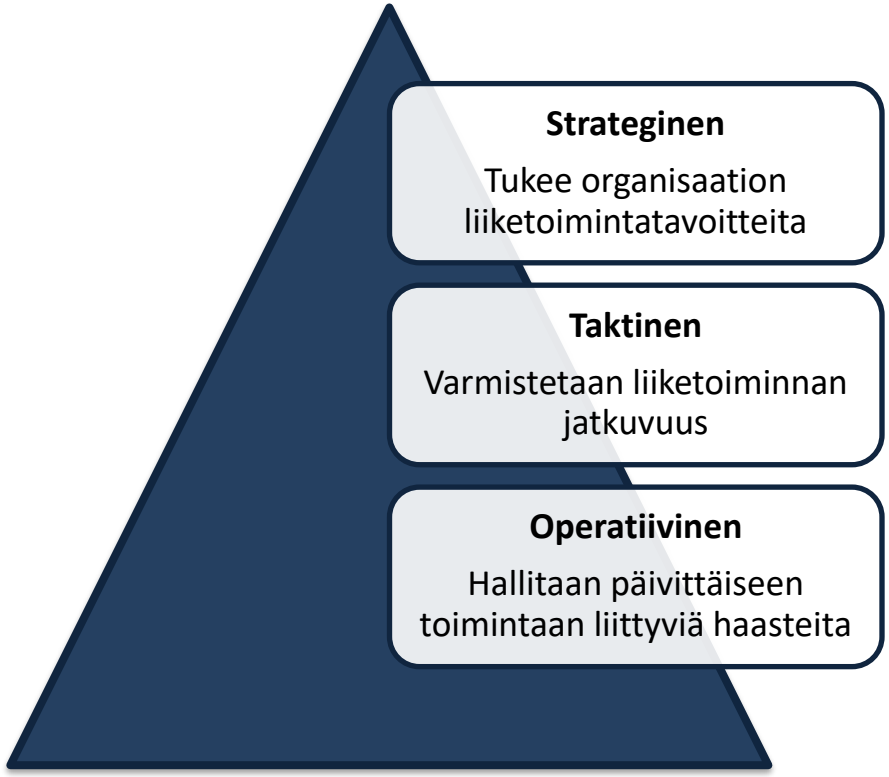
# Opsec Oy:n toiminta-ajatus



# Miksi Opsec Oy?

Opsec Oy on teknologiariippumaton ja asiakkaan kanssa samalla puolella pöytää istuva asiantuntija organisaation digiympäristön riskilähtöiseen johtamiseen sekä arjen, että strategian tasolla.



# Opsec Oy:n palveluiden kokonaisuus

**Tietohallinto - tietoteknisen ympäristön tehokkuus ja toimivuus**

- Tietotekniikka, järjestelmät, tietoverkot ja muut teknologiaan liittyvät ratkaisut
- Kehitys- ja hankintaprojektit, IT-strategiat ja -budjetit, laiterekisterit ja laite- ja lisenssihankinnat
- Valvonta-, ylläpito- ja IT-tukipalvelut; mm. verkon valvonta, ohjelmistopäivitykset ja tekninen asiakaspalvelu

**Tietoturva - tietojen suojaaminen**

- Tietojen, tietojärjestelmien, palveluiden, verkkoliikenteen ja ihmisten suojaaminen
- Hallinnollinen tietoturva; kehitys- ja hankintaprojektit, riskienhallinta, tietoturvapolitiikka, tietoturva-auditoinnit, tietoturvapoikkeamien hallinta, jatkuvuus- ja toipumissuunnitelmat, tietoturvakulttuuri, tietoturvatestaukset, tietoturvakoulutukset ja -ohjeistukset
- Tekninen tietoturva; päätelaitteiden, tietoverkkojen, järjestelmien ja pilvipalveluiden tekninen suojaus

**Tietosuoja, sopimukset ja muu lainsäädäntö - henkilötietojen suojaaminen ja lainmukainen toiminta**

- Tietosuojaan ja tietosuojalainsäädäntöön liittyvät tehtävät; henkilötietojen suojaamiseen liittyvät kehitys- ja hankintaprojektit ja -tehtävät, konsultoinnit, tietosuojavastaava- ja tietosuojakoordinaattoripalvelut ja tietosuojakoulutukset ja -ohjeistukset
- Sopimuksiin, teknologiajuridiikkaan, tiedonhallintalakiin ja digipalvelulakiin liittyvät tehtävät

# Opsec Oy:n asiakkaita

Opsec Oy:n asiakkaina on sekä julkisen että yksityisen puolen toimijoita. Asiakkaita löytyy mm. terveydenhuollon, koulutusorganisaatioiden, sähkö-, vesi-, jäte- ja kiinteistöhuollon, teollisuuden, logistiikan, vähittäiskaupan, mainostoiminnan ja muiden erilaisten palveluiden alalta. Esimerkkejä:

**Mika Lindberg**
toimitusjohtaja, CISSP, CISA, CISM
p. 020 198 6698
mika.lindberg@opsec.fi

**OPSEC OY**
Tiedekatu 2, 60320 Seinäjoki
p. 020 198 6690,
info@opsec.fi
www.opsec.fi

ISO/IEC 27001
CERTIFIED BY
huld | Certification


# Avoin työpaja 5.

# Tietoturva sote-alalla

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

sedu

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan sosiaalirahasto

Hanke rahoitetaan REACT-EU-välineen määrärahoista osana Euroopan unionin COVID-19-pandemian johdosta toteuttamia toimia.

# Tietoturvavaatimusten soveltaminen käytäntöön

Huoltovarmuuskeskuksen KYBER-Terveyshankkeen materiaaleja mukaillen

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Toteutuneita uhkakuvia

- **Case Lahden kaupunki 2019**
  - Kaupungin verkkoon hyökättiin tahallisesti saastuttaen yli 1000 tietokoneetta.
  - Tietojärjestelmiin tunkeuduttiin **jo toista kertaa** puolentoista vuoden sisällä. Edellinen helmikuussa 2018 (WannaMine)
- Terveydenhuollon osalta katkos aiheutti mm.
  - Sähköisten reseptien uusimispyyntöjä ei saatu hoidettua ja potilastietojen kirjaaminen ei toiminut normaalisti.
- Seuraukset:
  - Organisaation Internet-yhteys kiinni lähes kaksi viikkoa, jonka jälkeen rajoitettuja palveluja käytössä pitkään
  - Suorat kustannukset **kuukautta myöhemmin jo 700 000€**
    - it-palvelutuottajan tekemä työ, asiantuntijapalvelut, erityisohjelmistojen lisenssit ym.
  - Välillisiä kustannuksia mm. kaupungin it-tuen oma työ
- Vakuutus ei tässä tapauksessa korvaa kaupungille mahdollisesti aiheutuvia kustannuksia.

Lahden tietohallintojohtaja Marko Monni kertoo, mitä tapahtui sen jälkeen, kun kaupungin verkossa havaittiin haittaohjelma kesällä 2019: https://www.youtube.com/watch?v=K8mqA94RVQ4

# Toteutuneita uhkakuvia

- **Arkaluontoisia tietoja Turun kaupunki**
  - Potilaiden henkilö- ja terveystietoja sisältäneitä asiakirjoja päätyi kahdella eri kerralla 2018 huhtikuussa Turussa tavalliseen paperinkeräyslaatikkoon.
    - Tapahtuma-aikaan laitoksella oli käynnissä muutto
    - Henkilö ei ollut kertomuksensa mukaan saanut ohjetta salassapidettävistä paperiroskista. Hän sai vasta tapahtuneen jälkeen tietää, että rakennuksessa oli erillinen tietoturvaroskien tyhjennyspaikka.
    - Henkilö sai syytteen virkavelvollisuuden rikkomisesta, joka kuitenkin hylättiin näytön puuttumisen vuoksi
- **Arkaluontoisia tietoja Kristiinan kaupunki/Vaasan sairaanhoitopiiri**
  - Kristiinankaupungin terveysasiakkaiden sosiaaliturvatunnuksia, hoitosuunnitelmia ja terveystietoja sisältäneitä rikkinäisiä tietokoneita löytyi kaksi kappaletta kirpputorilta Porista vuonna 2019
  - Koneista löytyi myös tunnukset sairaanhoitopiirin järjestelmään, jossa olisi voinut määrätä lääkkeitä ja nähdä terveystietoja.
    - Löytäjä havaitsi tiedot korjatessaan koneitta ja toimitti tietokoneet poliisille
    - Vastuuorganisaatio ei osannut sanoa miten tiedot ovat päätyneet kirpputorille, koska ”Meillä vanhat koneet menevät ICT-palvelun kautta tyhjennettäväksi ja hävitettäväksi.”

https://www.iltalehti.fi/kotimaa/a/cc7fed80-2d7e-4803-81a7-8427c2d83451

https://yle.fi/a/3-10991831

# Toteutuneita uhkakuvia

- **Iso-Britannia, WannaCry 2017**
  - WannaCry-kiristyshaittaohjelma vaikutti 80 sairaanhoidosta vastaavan organisaatioon
    - 34 organisaation tietoverkko saastui
    - 46 joutui sulkemaan järjestelmiään estääkseen haittaohjelman leviämisen heidän toimintaansa
    - 685 muuta hoito-organisaatiota oli saastunut
    - 19494 hoitoaikaa peruttiin ja sisältäen hoito-operaatiot
    - 1220 lääketieteellistä laitteitta oli saastunut tai irrotettu toimintaympäristöstä saastumisen estämiseksi
  - Kustannusarvio
    - Hyökkäyksen aikana 22,5m€
    - Hyökkäyksen jälkeen 80,7m€

https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

# Mitä organisaation tietoturvan kannalta kannattaa miettiä?

- Tietoturvavaatimukset ovat riskienhallintatyökalu, joka on sovitettava käsiteltävään tietoon
  - Substanssi

- **Mitä tietoa suojataan?**
  - Mieti mitä tietoa kerätään ja miten se kulkeutuu organisaatiossasi
  - Mieti tiedon kulun polku tiedon lähteestä tiedon kohteeseen
- **Mihin tietoa käytetään?**
  - Henkilötietojen käsittelyyn tulee aina olla käyttötarkoitus!
- **Mihin tietoa tallennetaan?**
  - Erityisesti henkilötietojen käsittely vaikuttaa tallentamisen suojausmekanismeihin ja siihen liittyviin sopimuksiin

# Mitä organisaation tietoturvan kannalta kannattaa miettiä?

- Järkevät tietoturvavaatimukset edellyttävät organisaatiolta tukevia rakenteita
  - Selkeä käsitys **toimijoista** sekä näiden **rooleista** ja **vastuista**

- **Mikä on tiedon elinkaari?**
  - Mieti mitä tietoa kerätään ja miten se kulkeutuu organisaatiossasi
  - Mieti tiedon kulkua tiedon lähteestä tiedon kohteeseen
- **Ketkä tietoa käsittelevät?**
  - Ketkä kaikki ja missä tilanteissa pääsevät pääsevät tietoon käsiksi? Huomio myös huolto/ylläpito!
- **Kuka vastaa mistäkin osasta tiedonkäsittelyä?**
  - Huomioi etenkin myös ulkoistettujen palveluiden osalta.

# Seuraavat tapahtumat

## Teemoitellut työpajat:

# Hankkeen verkkosivut

# www.digivointi.fi

Seuraa meitä somessa!

@DigiVointihanke

@DigiVointihanke

@DigiVointihanke