Terveys- ja hyvinvointialojen opintokokonaisuus

Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa

OPETUS- JA KULTTUURIMINISTERIÖ
UNDERVISNINGS- OCH KULTURMINISTERIET

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

07A – Riskienhallinta ja johtaminen

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Riskienhallinta

Päätösten tekeminen

- Lukitsetko aina: Auton, huoneen tai talon poistuessasi?
- Miksi, mikä ohjaa päätöstä?
  - Sääntöihin pohjautuvat päätökset
    - Esim. Seurataan jonkun toisen sääntöjä (puoliso / perheenjäsen)
  - Relatiivisia päätöksiä
    - Esim. Naapurillani on aita ja hän aina lukitsee ovensa, joten mekin lukitaan.
  - Vaatimuspohjaiset päätökset
    - Esim. Tarkastelemme riskejä ja valitsemme turvatoimenpiteet niiden mukaisesti (jokin viitekehys?)

jamk

Riskienhallinta

Päätösten tekemisen elinkaari

- Tunnista käytännön tavoitteesi
  - Mitä "oikeita" asioita haluat saavuttaa?
- Valitse sopiva suojaus
  - Mitä heikkouksia on olemassa?
  - Mitkä turvatoimenpiteet voisivat toimia?
  - Mitkä ovat kompromissit maaleja (suojaustavoitteisiin pääsyä) vastaan?
- Mittaa menestystä
  - Tarkkaile hyökkäyksiä tai muita epäonnistumisia
  - Toivu ongelmista

jamk

Riskienhallinta

Terminologia

- Riskien tunnistaminen
  - Sellaisten riskien määrittäminen ja luokittelu, jotka voivat vaikuttaa resursseihin (esim. palvelimiin).
  - Riskirekisteri (kuvaus, odotettu vaikutus, todennäköisyys (likelihood), lievennyskeinot (mitigaatio), ”ränkkäys” (tai priorisointi))
- Riskianalyysi
  - Laadullinen (laadullinen) riskianalyysi käyttää suhteellista järjestystä riskireaktioiden määrittämiseen (todennäköisyys ja seuraukset).
  - Kvantitatiivinen (määrällinen) riskianalyysi käyttää matemaattisia kaavoja riskin vakavuuden luokitteluun.
- Riski-vastaus
  - Valitse kontrollit, joilla voit vaikuttaa riskeihin
- Riskien seuranta
  - Jatkuva riskien tunnistaminen ja analysointi

jamk

Riskienhallinnan viitekehys - Risk Management Framework (RMF)

jamk

Riskienhallinta

Risk Management Framework (RMF)

- NIST RMF on kattava ja joustava riskienhallintaprosessi, joka integroi tietoturvan, yksityisyyden ja kybertoimitusketjun riskienhallinnan järjestelmän kehityssyklin aikana.
- RMF:n avulla organisaatiot voivat hallita riskejä tehokkaasti ja varmistaa, että tietoturva ja yksityisyys otetaan huomioon kaikissa järjestelmän elinkaaren vaiheissa

- NIST RMF:ää ohjaa useita dokumentteja, joista keskeisimmät ovat:
  1. **NIST SP 800-37 Rev. 2**: Tämä dokumentti kuvaa RMF:n ja tarjoaa ohjeet sen soveltamiseen tietojärjestelmiin ja organisaatioihin
  2. **NIST SP 800-53**: Tämä dokumentti sisältää kontrollit, jotka valitaan ja toteutetaan RMF:n mukaisesti
- Näiden lisäksi RMF:ään liittyy muita NIST-dokumentteja, jotka tukevat eri vaiheita ja tarjoavat lisäresursseja implementoijille

NIST = National institute of standards and technology (Amerikan)

jamk

Riskienhallinta

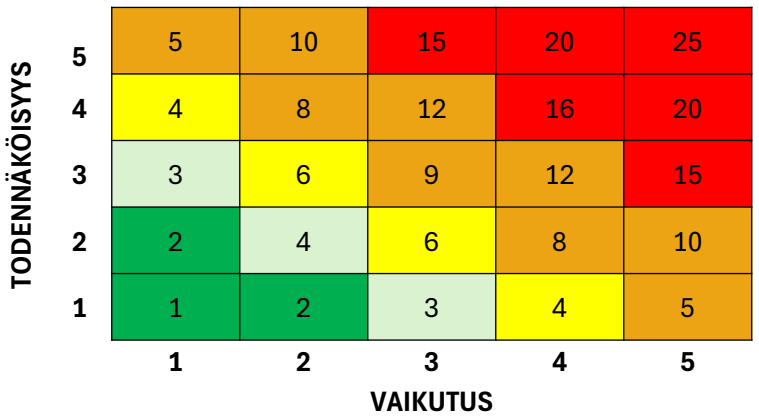
Risk Management Framework (RMF)

Vaihe	Kuvaus
Valmistelu	Organisaation valmistelu riskienhallintaan.
Luokittelu	Järjestelmän ja sen käsittelemän tiedon luokittelu vaikutusanalyysin perusteella.
Valinta	NIST SP 800-53 -kontrollien valinta riskinarvioinnin perusteella.
Toteutus	Kontrollien toteuttaminen ja dokumentointi.
Arviointi	Kontrollien toimivuuden ja tehokkuuden arviointi.
Valtuutus	Johtavan virkamiehen päätös järjestelmän valtuuttamisesta käyttöön.
Seuranta	Kontrollien toteutuksen ja järjestelmän riskien jatkuva seuranta.

jamk

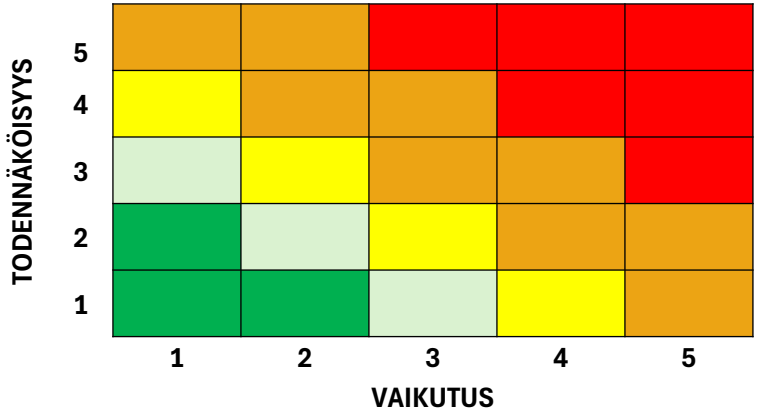
Riskienhallinta

Soveltamiseen esimerkkejä



Sovelletaan: Laita oikean puoleiseen taulukkoon seuraavat esimerkit:

a) Lämmittely kysymys: Lapsi kiipeää puuhun päiväkodissa



1. Haittaohjelmat (Esim. Kiristyshaittaohjelma)
2. Tietojenkalastelu (Phishing)
3. Palvelunestohyökkäykset (DDoS)
4. Tietojärjestelmän haavoittuvuudet
5. Henkilökunnan tietoturvaosaamisen puute

Esimerkki laskentatavasta (myös muita malleja on olemassa)

Todennäköisyys * Vaikutus = Riski

jamk

Muita turvallisuusjohtamisen malleja

NIST SP 800-34 Rev. 1

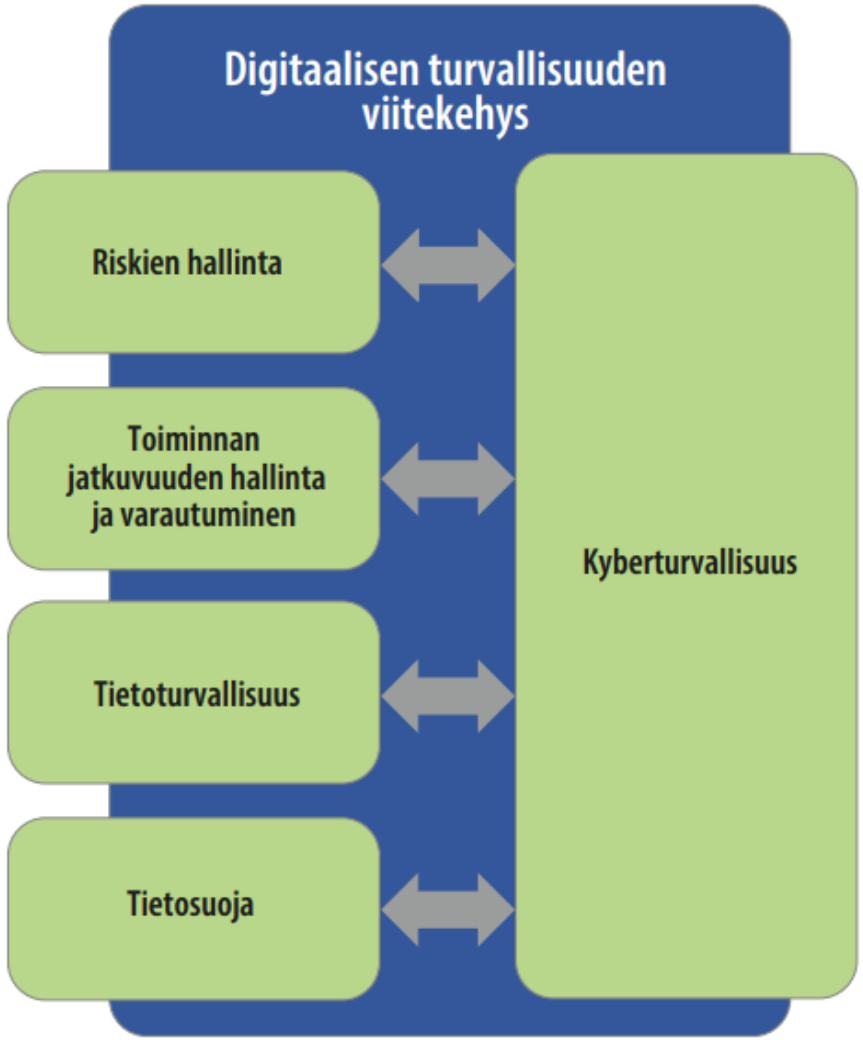
- Varautumissuunnitelma opas dokumentaatio esittää myös muita malleja, joita johtamisessa tulee ottaa huomioon, tässä muutama nosto:
  - Liiketoiminnan jatkuvuuden malli (Business Continuity Plan = BCP)
  - Onnettomuudesta selviytymissuunnitelma (Disaster Recovery Plan = DRP)
  - Tietojärjestelmän varasuunnitelma (Information System Contigency Plan = ISCP)
  - ISCP eroaa DRP:stä ensisijaisesti siinä, että tietojärjestelmän varasuunnitelmamenettelyt on kehitetty järjestelmän palauttamiseksi paikasta tai sijainnista riippumatta.

jamk

Johtaminen

Digitaalisen turvallisuuden viitekehys

- Digitaalisen turvallisuuden viitekehykseen sisältyy niin kyberturvallisuuteen kuin riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita.
- Digitaalisen turvallisuuden tavoitteena on kokonaisturvallisuuden viitekehyksessä suojata kansalaisia, yhteisöjä ja yhteiskuntaa niiltä riskeiltä ja uhkilta, jotka voivat kohdistua henkilötietoihin ja kansalaisten palveluihin sekä yhteiskunnan ja viranomaisten toimintaan, prosesseihin, palveluihin ja tietoaineistoihin digitaalisessa toimintaympäristössä.



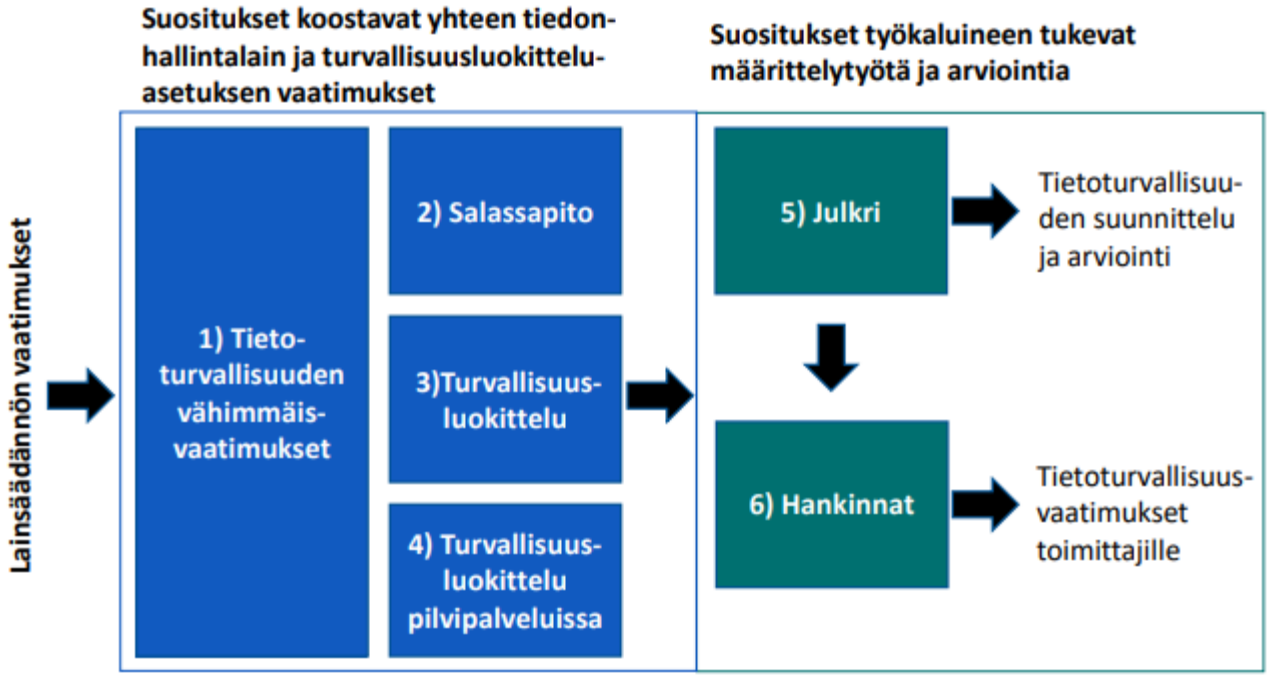
Lähde: Julkisen hallinnon digitaalinen turvallisuus. 2020. Valtiovarainministeriö.

jamk

Johtaminen

Tietoturvallisuutta koskevat tiedonhallintalautakunnan suositukset

- 1) Suositus tietoturvallisuuden vähimmäisvaatimuksista (VM 2024:19)
- 2) Suositus salassa pidettävien asiakirjojen käsittelystä (VM 2023:4)
- 3) Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5)
- 4) Turvallisuusluokiteltavaien asiakirjojen käsittely pilvipalveluissa (VM 2022:4)
- 5) Julkisen hallinnon tietoturvallisuuden arviointikriteeristö, Julkri (VM 2023:46)
- 6) Suositus tietoturvallisuudesta hankinnoissa (VM 2023:57)



Lähde: [Valtiovarainministeriön julkaisu 2024:19 – Suositus tietoturvallisuuden vähimmäisvaatimuksista]

Johtaminen

Vaatimusten vieminen käytäntöön

- Nykypäivänä digitaalinen turvallisuus huomioidaan jatkuvasti johdon päätöksissä.
- Nämä näkyvät työntekijöille ohjeistuksia ja määräyksinä
  - Tavoitteena ei ole vaikeuttaa toimintaa.
  - Suuri osa vaatimuksista perustuu lakiin.
    - Esimerkiksi potilaan tietosuoja
  - Usein ongelmana, että vaatimuksia ei perustella ja työntekijät kokevat, että nämä vaikeuttavat työntekoa.

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

07B – ICT tiimin haasteet

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Ohjaavat säädökset, lait ja auditoinnit

Lähiaikojen isoimpia muutoksia

- Sote-uudistus (Sosiaali- ja terveydenhuollon uudistus)
  - Uudistus on tuonut mukanaan uusia toimintamalleja ja organisaatiorakenteita.
- GDPR (General Data Protection Regulation)
- Digitalisaatio ja eHealth
  - Digitalisaatio on edennyt nopeasti, ja terveysalalla on otettu käyttöön monia uusia digitaalisia ratkaisuja, kuten sähköiset potilastietojärjestelmät, etävastaanotot ja mobiilisovellukset.
- COVID-19-pandemia
  - Pandemia on korostanut tietoturvan ja tietosuojan merkitystä, kun etätyö ja digitaaliset palvelut ovat yleistyneet.

jamk

Ohjaavat säädökset, lait ja auditoinnit

Lähiaikojen isoimpia muutoksia

- Kyberturvallisuusuhkien lisääntyminen.
- Tekoälyn ja koneoppimisen käyttöönotto.
- NIS2-direktiivi (Network and Information Systems Directive) on Euroopan unionin uusi kyberturvallisuusdirektiivi.
  - Direktiivi asettaa velvoitteita riskienhallinnalle ja merkittävien poikkeamien raportoinnille erityisesti kriittisillä sektoreilla.

jamk

Ohjaavat säädökset, lait ja auditoinnit

Auditoinnit esimerkkinä ISO 2700x -auditointi

- ISO 2700x auditointi on yksi tyypillisimmistä IT-auditoinneista.
- ISO 2700x -standardit, erityisesti ISO 27001, keskittyvät tietoturvan hallintajärjestelmän (ISMS) luomiseen ja ylläpitoon.
  - **Tietoturvakoulutus**: Linjatyöntekijöiden on osallistuttava säännöllisiin tietoturvakoulutuksiin, joissa käsitellään tietoturvapolitiikkoja, riskienhallintaa ja tietoturvakäytäntöjä
  - **Tietojen käsittely**: Työntekijöiden on noudatettava tiukkoja tietojen käsittelysääntöjä, kuten salasanakäytäntöjä, tietojen salausmenetelmiä ja pääsynhallintaa
  - **Tietoturvapoikkeamien raportointi**: Työntekijöiden on oltava valmiita raportoimaan tietoturvapoikkeamista välittömästi ja noudattamaan organisaation poikkeamien hallintaprosesseja
  - **Fyysinen turvallisuus**: Työntekijöiden on varmistettava, että fyysiset työtilat ovat turvallisia ja että pääsy tietoihin on rajoitettu vain valtuutetuille henkilöille

jamk

Ohjaavat säädökset, lait ja auditoinnit

Säädökset esimerkkinä NIS2-direktiivi

- NIS2-direktiivi, joka astui voimaan huhtikuussa 2025, pyrkii parantamaan kyberturvallisuuden tasoa EU:n jäsenvaltioissa
  - **Riskienhallinta**: Linjatyöntekijöiden on osallistuttava kyberturvallisuuden riskienhallintaan
  - **Poikkeamien ilmoittaminen**: Direktiivi velvoittaa organisaatiot ilmoittamaan merkittävistä tietoturvapoikkeamista valvovalle viranomaiselle.
  - **Toimitusketjun turvallisuus**: Työntekijöiden on varmistettava, että **kaikki toimittajat** ja **alihankkijat** noudattavat kyberturvallisuusvaatimuksia, mikä voi vaatia lisävalvontaa ja yhteistyötä
  - **Tietoturvan jatkuva parantaminen**: Työntekijöiden on oltava valmiita omaksumaan uusia käytäntöjä ja teknologioita tietoturvan ylläpitämiseksi

jamk

ICT tiimin haasteet

ICT tiimin ja työntekijöiden väliset haasteet

- Työntekijät eivät kerro havainnoistaan.
  - Ongelmatilanteessa työntekijät usein ohittavat hälytysmerkit → ei tiedetä kenelle ilmoittaa.
  - Työntekijä avaa haitallisen sähköpostin → ei uskalleta kertoa, koska näyttäisin tyhmältä.
- Ymmärtämisen puute
  - Tietohallinto käyttää usein teknistä kieltä, joka voi olla vaikeaa työntekijöille ymmärtää. Tämä voi johtaa siihen, että tietoturvaohjeet jäävät epäselviksi.
  - Työntekijät eivät välttämättä ymmärrä, miten heidän päivittäiset toimintansa vaikuttavat organisaation tietoturvaan.
  - Työntekijät voivat kokea tietoturvaohjeet rajoittavina ja hidastavina heidän työtään.

jamk

Yritysten dataliikenteestä

Case example: jamkin ICT kampuksen “labraverkko”

jamk

Näkymättömät kyberturvallisuustoimenpiteet

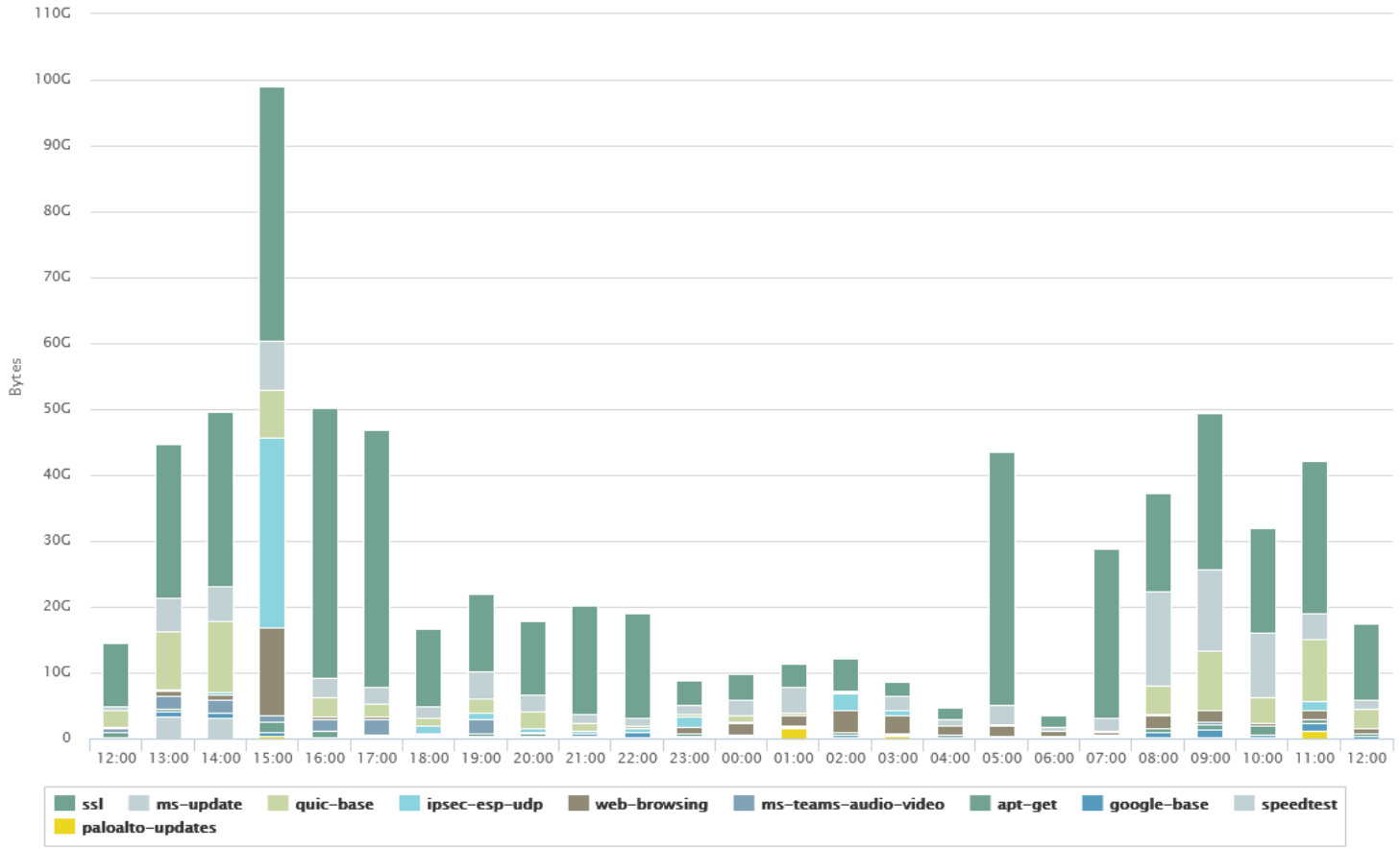
Pohjustus

- Yrityksiin kohdistuu jatkuvasti paljon porttiskannauksia ja erilaisia haavoittuvuuksien testauksia yrityksestä ja palveluista riippuen vähintään päivittäin ja isommissa, jopa tunneittain.
  - Valtaosa näistä ei näy tavalliselle työntekijälle ja moni jää suoraan puolustuskeinoihin, kuten palomuureihin kiinni.
  - Eritasoista palvelunestohyökkäystä tulee jatkuvasti jossain muodossa (DoS / DDoS).
- Roskaposteja suodatetaan (filtteröidään) jatkuvasti ja paljon, erään arvion mukaan kaikesta maailman liikenteestä valtaosa on pelkkiä roskaposteja.
  - Silti osa roskapostista tulee läpi, roskapostitehtailijat oppivat myös väistelemään automaattisia suodatuksia.

jamk

Esimerkkejä

Kampuksen ICT laboratorio verkon tapahtumia 24h ajalta



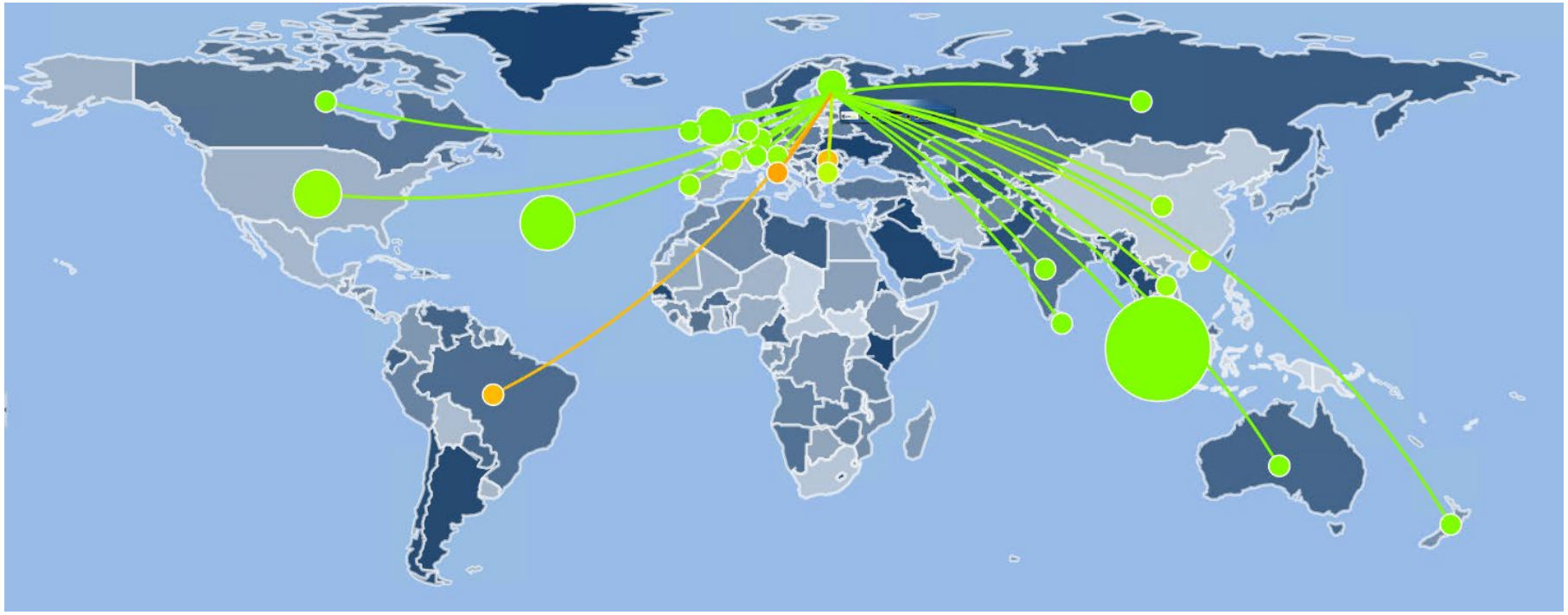
- Tämä sisältää kaiken tietoliikenteen, eli myös tavallisen tietoliikenteen.
- Pystyakselilla näemme liikenteen määrän tavuina
- Vaaka-akselilla näemme kellonajat tunneittain
- (Kaavion palkkien selitteillä ei ole tässä suurta merkitystä)

jamk

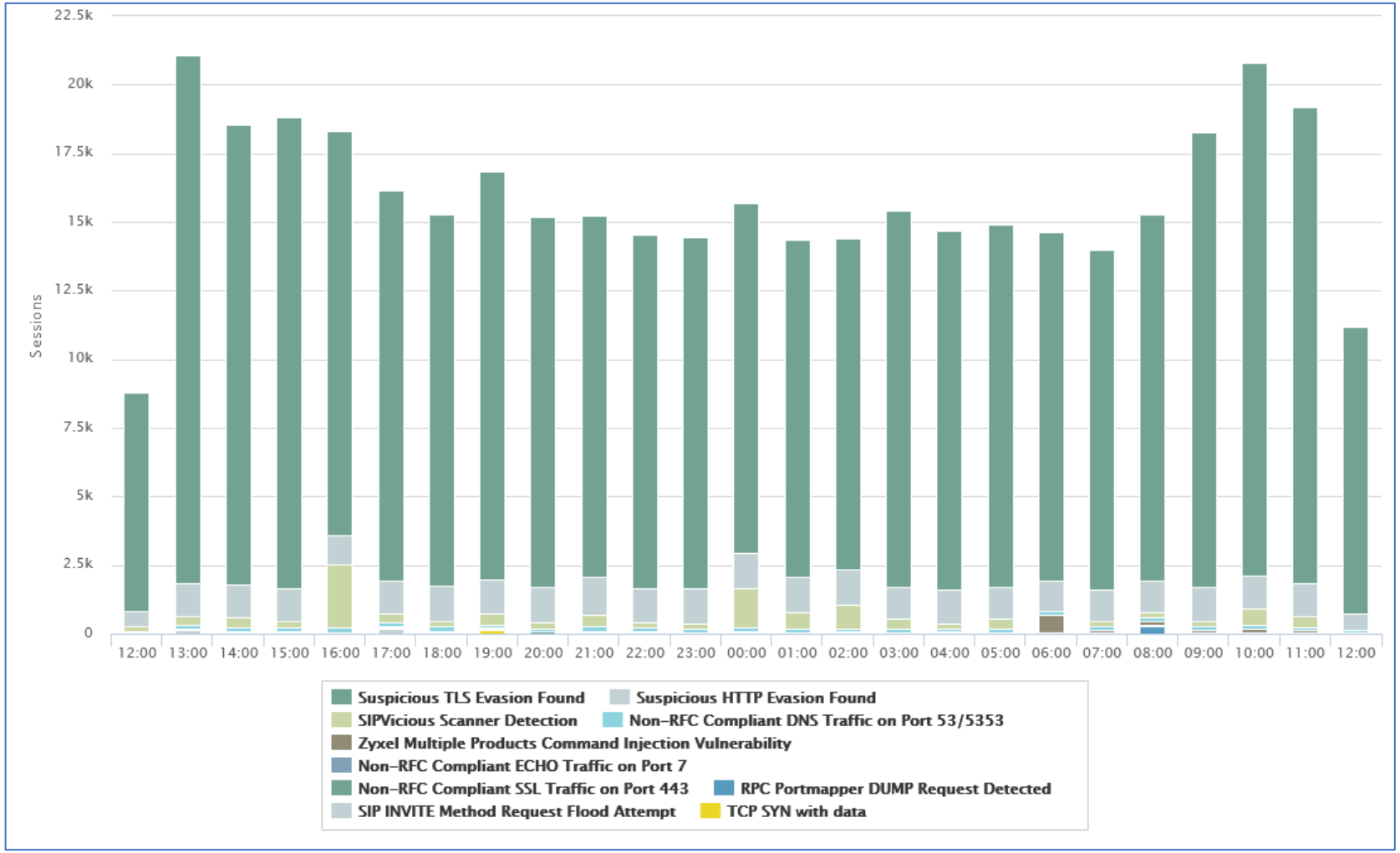
Esimerkkejä

Kampuksen ICT laboratorio verkkoon kohdistuneita hyökkäyksiä 24h ajalta

- Mistä haaviin jääneet paketit ovat saapuneet?



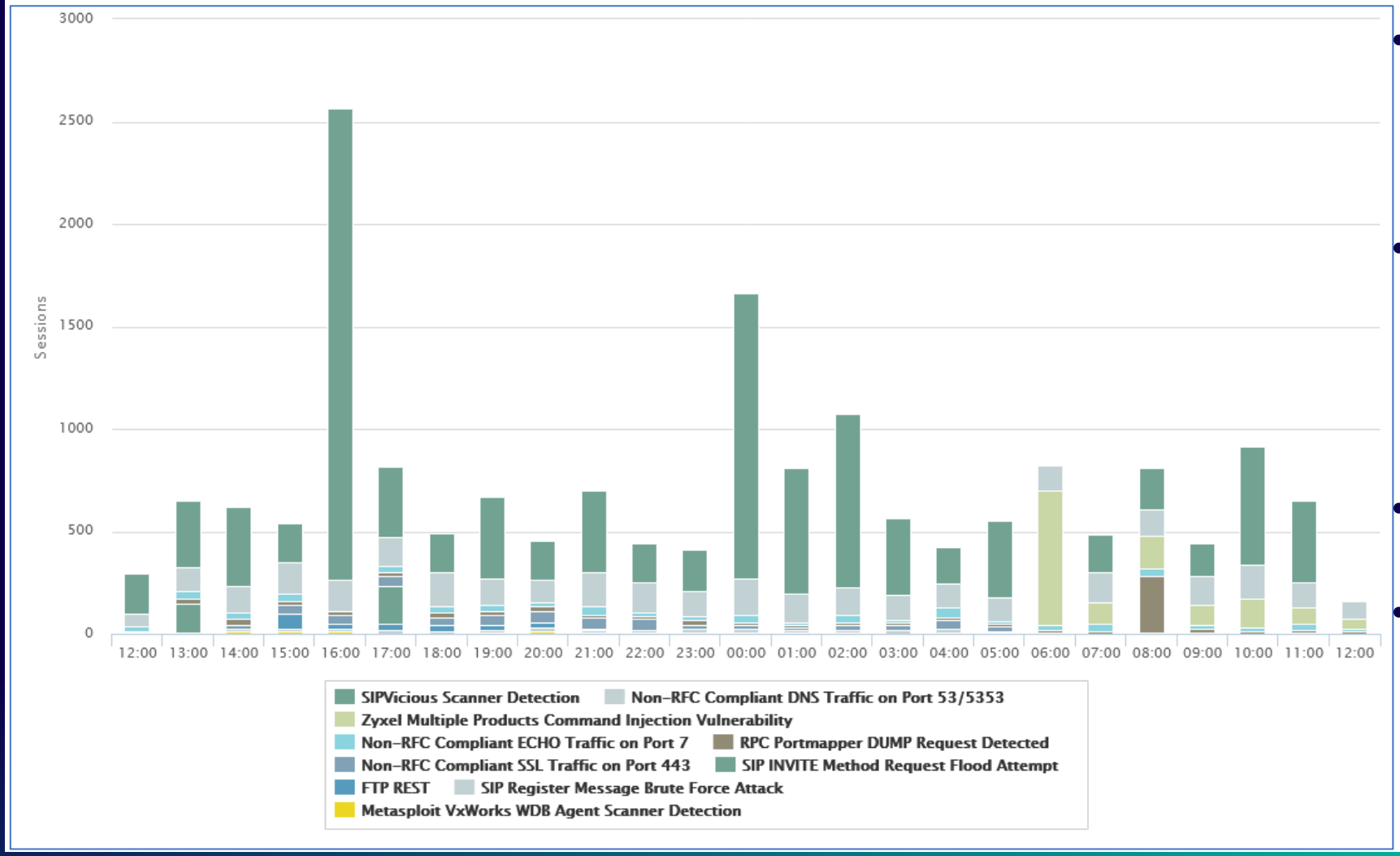
Havaitut saapuvat uhat



- Pystyakselilla näemme havaittujen saapuvien uhkien määrän
- Vaaka-akselilla näemme tilanteen tunneittain
- (Kaavion palkkien selitteillä ei ole tässä suurta merkitystä)

jamk

Havaitut saapuvat haavoittuvuushyökkäykset



- Pystyakselilla näemme havaittujen saapuvien haavoittuvuus hyökkäyksien määrän
- Haavoittuvuushyökkäyksellä tarkoitetaan tapausta, jossa on suoraan yritetty hyödyntää tunnettua haavoittuvuutta
- Vaaka-akselilla näemme tilanteen tunneittain
- (Kaavion palkkien selitteillä ei ole tässä suurta merkitystä)

jamk

Näkymättömät kyberturvallisuustoimenpiteet

Suojauksista

- **Automaattiset ohjelmistopäivitykset**: Ohjelmistojen haavoittuvuudet korjataan automaattisesti päivitysten avulla
- Pakettien suodattaminen on tärkeä tekniikka, joka valvoo verkon liikennettä ja estää luvattoman pääsyn:
  - **Pakettien tarkistus**: Suodattimet tarkistavat lähtevät ja saapuvat paketit
  - **Palomuurit**: Palomuurit käyttävät pakettisuodattimia estääkseen haitallisen liikenteen pääsyn verkkoon

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

07C – Tietoturvavalvomo
Security Operations Center (SOC)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Tietoturvavalvomo

Security Operations Center (SOC) – Mikä?

- **Security Operations Center (SOC)** on organisaation keskus, joka vastaa kyberturvallisuuden parantamisesta ja uhkien torjumisesta. SOC-tiimi valvoo jatkuvasti organisaation tietojärjestelmiä, kuten palvelimia, tietokantoja ja verkkoja, havaitakseen ja estääkseen mahdolliset kyberhyökkäykset.
- **SOC:n päätehtäviin kuuluu**:
  - Uhkatilanteiden havaitseminen ja estäminen
  - Reagointi uhkiin
  - Tietojen suojaaminen

jamk

Tietoturvavalvomo

Security Operations Center (SOC) – Mikä?

- Tietoturvavalvomon toimintaa, jota kuvataan tässä osiossa, voi suorittaa useampi yksikkö yrityksestä riippuen. Voi olla esimerkiksi erillinen talon sisäinen IT-tiimi, joka tekee osan näistä ja lisäksi voi olla erillinen ulkoinen toimija, joka tuottaa vaikka 24/7 valvomopalvelun.
  - Näillä kalvoilla puhutaan näistä yhtenä kokonaisuutena.

jamk

Tietoturvavalvomo

Security Operations Center (SOC) – Mitä?

- **Mitä SOC pystyy tekemään?**
  - **Jatkuva valvonta**: SOC-tiimi valvoo järjestelmiä ympäri vuorokauden, mikä mahdollistaa nopean reagoinnin uhkiin.
  - **Uhkatietojen hyödyntäminen**: SOC käyttää ulkoisia tietolähteitä ja analytiikkaa ymmärtääkseen hyökkääjien toimintatapoja ja motiiveja. Tämä käytännössä kattaa vaikkapa juuri sairaalaympäristöstä kiinnostuneiden uhkatoimijoiden tapojen selvittämisen ja varautumisen.
  - **Hyökkäyspinnan pienentäminen**: SOC-tiimi ylläpitää tietoa kaikista organisaation resursseista ja soveltaa tietoturvapäivityksiä ja korjauksia.

jamk

Tietoturvavalvomo

Security Operations Center (SOC) – Mitä ei?

- **Mitä SOC ei pysty tekemään?**
  - **Täydellinen suojaus**: Vaikka SOC voi vähentää riskejä, se ei voi taata täydellistä suojaa kaikilta mahdollisilta hyökkäyksiltä.
  - **Inhimillisten virheiden estäminen**: SOC ei voi estää kaikkia inhimillisiä virheitä, kuten tietojen tallentamista väärään paikkaan tai heikkojen salasanojen käyttöä.
  - **Kaikkien uhkien ennakointi**: SOC voi käyttää uhkatietoa ja analytiikkaa, mutta se ei voi ennakoida kaikkia mahdollisia uusia uhkia.
- Samaan aikaan kun puolustusvalmistautuminen paranee, niin myös puolustuksen kiertäminen kehittyy.

jamk

Tietoturvavalvomo

Security Operations Center (SOC) – Miten tämä liittyy minuun?

- **Miten SOC liittyy tavallisiin työntekijöihin?**
  - **Tietoturvakoulutus**: SOC voi tarjota koulutusta ja ohjeita työntekijöille tietoturvakäytännöistä.
  - **Uhkatilanteiden raportointi**: Työntekijöiden tulee raportoida epäilyttävästä toiminnasta SOC-tiimille, jotta he voivat tutkia ja reagoida nopeasti.
  - **Tietoturvakäytännöt**: Työntekijöiden tulee noudattaa organisaation tietoturvakäytäntöjä, kuten tallentaa tiedot vain hyväksyttyihin järjestelmiin ja käyttää vahvoja salasanoja.

jamk

Tietoturvavalvomo

Security Operations Center (SOC) – Esimerkkiratkaisuja

- **Virustorjuntaohjelmistot**: Skannaavat ja poistavat haitalliset ohjelmat tietokoneelta
- **Palomuurit**: Estävät ei-toivotut yhteydet ja hyökkäykset
- **VPN-yhteydet**: Salaavat verkkoliikenteen ja suojaavat yksityisyyttä
- **Automaattiset päivitykset**: Korjaavat tunnetut tietoturva-aukot ohjelmistoissa ja laitteissa
- **Tekoälypohjaiset ratkaisut**: Käytetään esimerkiksi roskapostin suodattamiseen ja haittaohjelmien tunnistamiseen

jamk

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences