VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Pihla Alatyppö

VERKKOSENSORIN HYÖDYNTÄMINEN PALVELULIIKETOIMINNASSA

Tekniikka

2025

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Pihla Alatyppö
Opinnäytetyön nimi	Verkkosensorin hyödyntäminen palveluliiketoiminnassa
Vuosi	2025
Kieli	suomi
Sivumäärä	69 + 13 liitettä
Ohjaaja	Jani Ahvonen

Tässä tutkimuksessa tarkastellaan SensorFun Beacon -tuotteen käyttöä ja sen yhteensopivuutta Hitachin järjestelmien kanssa. Tutkimuksen tavoitteena on varmistaa, että Beacon toimii luotettavasti järjestelmien kanssa ja tuottaa käyttökelpoisia havaintoja. Tutkimuksessa tutustutaan Beaconin teknisiin ominaisuuksiin sekä sen integroimiseen Hitachin järjestelmiin.

Tutkimuksessa hyödynnettiin toiminnallisia testausmenetelmiä, joissa laitetta testattiin Hitachin järjestelmien kanssa. Testauksessa arvioitiin laitteiden suorituskykyä lyhyellä ja pitkällä aikavälillä. Aineisto kerättiin testausprosessin aikana. Lokitiedostoja analysoitiin ja erityisesti laitteiden välisiin tietovuotoihin ja virheisiin kiinnitettiin huomiota.

Tutkimuksessa todettiin, että Beacon tuo merkittävää lisäarvoa palveluliiketoiminnassa. Sen helppo käyttöönotto, kyky tunnistaa verkon haavoittuvuuksia ja tietoturvariskejä parantavat kyberturvallisuutta, erityisesti NIS2-direktiivin vaatimusten täyttämisessä. Beaconin proaktiivinen lähestymistapa estää kyberhyökkäyksiä ja toimintahäiriöitä, mikä vähentää ylläpitokustannuksia ja parantaa asiakastyytyväisyyttä

Avainsanat eristyksentestaus, tietoturvallisuus, palveluliiketoiminta

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

ABSTRACT

Author	Pihla Alatyppö
Title	The utilisation of Network Sensors in Service Business
Year	2025
Language	Finnish
Pages	69 + 13 Appendices
Name of Supervisor	Jani Ahvonen

This study focuses on the use of the SensorFu Beacon device and its compatibility with the Hitachi systems. The goal of the study is to ensure that the Beacon device operates reliably with the systems and provides useful insights. The study explores the technical features of the Beacon device and its integration into the Hitachi systems.

The research utilized functional testing methods, where the device was tested together with the Hitachi systems. The performance of the devices was evaluated both in the short and long term. Data was collected during the testing process and analysed using log files with particular attention paid to device-to-device data leaks and errors.

The study found that the Beacon device provides significant added value in service business operations. Its easy deployment, ability to detect network vulnerabilities and identify information security risks enhances cybersecurity, particularly in meeting the requirements of the NIS2 directive. Beacon’s proactive approach helps prevent cyberattacks and operational disruptions, reducing maintenance costs and improving customer satisfaction.

Keywords isolation testing, information security, service business

SISÄLLYS

KUVAT

KUVIOT

TAULUKOT

LYHENTEET

API	Application Programing Interface
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
HTTP	Hypertext Transfer Protocol
IOT	Internet of Things
IP	Internet Protocol
OT	Operational technology
SIEM	Security Information and event management
TCP	Transmission Control Protocol
TSL	Trasport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

1 JOHDANTO

Kyberturvallisuus on noussut keskeiseksi teemaksi digitaalisessa maailmassa, jossa tietoverkkojen ja -järjestelmien suojaaminen on elintärkeää organisaatioiden toiminnan turvaamiseksi. Digitaalisten uhkien ja kyberhyökkäysten määrän kasvaessa verkkojen turvallisuuden testauksen merkitys korostuu. Haavoittuvuuksia voi jäädä huomaamatta ilman asianmukaisia testausmenetelmiä ja pienetkin heikkoudet voivat johtaa vakaviin tietoturvaongelmiin. Tässä opinnäytetyössä tarkastellaan SensorFun Beacon-tuotteen roolia verkkojen haavoittuvuuksien tunnistamisessa ja sen käyttöä kyberturvallisuuden hallinnan tukena.

Opinnäytetyön toimeksiantajana on Hitachi energy ja päätavoitteena on tutustua Beaconin toimintaan, integroida se Hitachi Energyn järjestelmiin ja arvioida sen toimivuutta kyberturvallisuuden parantamisessa. Lisäksi pyritään ymmärtämään Beaconin toimintaperiaatteet sekä sen tarjoamat mahdollisuudet palveluliiketoiminnassa. Työssä tutkitaan, miten Beacon integroituu olemassa olevaan infrastruktuuriin ja millaisia hyötyjä sen käyttö voi tuoda erityisesti verkkojen valvonnassa ja uhkien ennaltaehkäisyssä.

Työn rakenne alkaa teoreettisella tarkastelulla tieto- ja kyberturvallisuudesta sekä tuotantoverkkojen eristämisestä. Tämän jälkeen siirrytään Beaconin teknisten ominaisuuksien ja sen toiminnan tarkasteluun. Työn lopuksi arvioidaan tulokset ja pohditaan jatkokehitysmahdollisuuksia.

2 HITACHI ENERGY

Hitachi on globaali teknologiayritys, joka edistää kestävää energiatulevaisuutta tarjoamalla innovatiivisia ratkaisuja ja palveluita. Yrityksen pääkonttori sijaitsee Zürichissä, Sveitsissä ja sillä on noin 45 000 työntekijää 60 maassa. Hitachi Energy palvelee asiakkaita eri toimialoilla, kuten sähkötuotannossa, teollisuudessa, liikenteessä ja infrastruktuurissa. (Hitachi Energy, n.d.)

Suomessa Hitachilla on useita toimipisteitä, joista keskeisimmät sijaitsevat Vaasassa, Helsingissä, Lappeenrannassa ja Tampereella. Yrityksen pääkonttori sijaitsee Vaasassa. Vuonna 2024 Hitachi työllisti Suomessa 582 henkilöä. (Finder, n.d.-a.)

Hitachi Energy on vakiinnuttanut asemansa merkittävänä toimijana Suomen energiasektorissa. Yhtiö tarjoaa Suomessa laajan valikoiman tuotteita ja ratkaisuja, jotka parantavat sähköverkon tehokkuutta ja luotettavuutta. Suomessa Hitachi toimittaa muun muassa muuntajia ja reaktoreita, jotka ovat olennaisia sähköverkon vakauden ja toiminnan kannalta.

Näiden lisäksi yritys kehittää ja toimittaa sähköverkon hallintaan liittyviä ohjaus-, automaatio- ja valvontajärjestelmiä. Nämä teknologiat mahdollistavat verkon paremman optimoinnin ja reagoinnin muuttuviin olosuhteisiin. Ratkaisut tukevat näin Suomen sähköverkon modernisointia ja varmistavat sen toimintavarmuuden. (Hitachi Energy, n.d.)

3 PALVELULIIKETOIMINTA

Palveluliiketoiminta on liiketoimintamalli, joka voi toimia tuoteliiketoiminnan täydentävänä osa-alueena ja rakentua vahvasti tuotteiden myynnin ympärille (Hänninen, 2021). Tähän liiketoimintamalliin on panostettu merkittävästi viimeisen kymmenen vuoden aikana, ja siitä on tullut tärkeä osa teollisuuden liiketoimintastrategioita. Palveluliiketoiminnassa tuotteeseen yhdistetään lisäarvoa tuottava palvelu, mikä teollisuudessa tarkoittaa usein varaosia, asennuspalveluita, koulutusta sekä huoltoa ja ylläpitoa. Näillä palveluilla tuetaan tuotteen elinkaarta ja pyritään solmimaan pitkäaikaisia sopimuksia ja laajentamaan asiakassuhteita, mikä parantaa liiketoiminnan kannattavuutta ja lisää tuottoja. (Rantanen, n.d.)

Palveluiden merkitys korostuu erityisesti, kun asiakkaat hakevat niillä lisäarvoa, jota ei ole mahdollista toteuttaa pelkästään oman organisaation sisäisistä resursseista. Asiakaskokemus ja asiakaslähtöisyys ovat keskeisiä tekijöitä palveluliiketoiminnan onnistumisessa. Ymmärrys asiakkaan tarpeista ja näkemyksistä on palveluliiketoiminnan kulmakivi, sillä asiakas haluaa yhteistyöltä kustomoitua, tuotteeseen sisällettäviä palveluja, jotka vastaavat hänen liiketoimintatarpeitaan. (Rantanen, n.d.)

Tuotosajattelussa palvelu ja ratkaisu eivät ole erillisiä tuotteita, vaan ne yhdistetään kokonaisuudeksi. Ratkaisu voi olla esimerkiksi prosessien parantaminen, tehokkuuden lisääminen ja asiakaskohtaiset optimoinnit, jotka tukevat asiakkaan liiketoimintaa ja auttavat saavuttamaan parempia tuloksia. (Rantanen, n.d.)

4 TIETOTURVALLISUUS

Riippuvuus sähköisistä palveluista ja järjestelmistä yhteiskunnassa kasvaa nopeasti. Samalla, kun digitaalinen kasvu etenee, kyberturvallisuusriskien määrä lisääntyy ja hyökkäyksien määrä kasvaa. (Traficom, 2020, s. 3.) Tämän vuoksi yritysten on jatkuvasti kehitettävä uusia keinoja suojautua kyberhyökkäyksiltä.

Tietoturvallisuus viittaa toimenpiteisiin ja menetelmiin, jotka on suunniteltu suojaamaan tärkeää tietoa niin hallinnollisesti kuin teknisesti. Tämä on monivaiheinen prosessi, jossa suojaamista tarvitseva tieto voi olla fyysinen dokumentti tai digitaalinen tallenne. Tietoturvallisuus tarkoittaa siis kaiken turvattavan tiedon suojaamista. (Jyväskylän yliopisto, n.d.)

Digitalisoituvassa yhteiskunnassa tietoturvaongelmat ovat laajentuneet ja kohdistuvat enemmän sekä järjestelmäympäristöihin että tietoliikennetekniikoihin. Tietojärjestelmien määrä kasvaa jatkuvasti ja niiden liittäminen tietoliikenneverkkoihin lisää verkkoon tunkeutumisen riskiä. Tämä asettaa uusia haasteita tietojärjestelmien suojaamiselle ja vaatii jatkuvaa kehitystä kyberturvallisuuden alueella. (Suomen Automaatioseura, 2010, s. 14.)

4.1 CIA-malli

CIA-malli on tietoturvan perusperiaatteiden malli, joka koostuu kolmesta osa-alueesta (Kuva 1): luottamuksellisuus, eheys ja saatavuus (Confidentiality, Integrity, Cvailabitlity). Nämä kolme periaatetta muodostavat perustan, jonka avulla organisaatiot voivat havaita haavoittuvuuksia ja keinoina suojata tietojärjestelmiä. CIA-malli toimii ohjenuorana yrityksissä valitettaessa sopivia teknologioita ja käytäntöjä tietojärjestelmien suojaamiseksi. (Holdsworth & Kosinski, 2024.) Mallia käytetään kansainvälisessä ISO 27001 -standardissa, joka koskee sitä, miten käsitellään tietoturvallisuutta (Irwin, 2023).

4.1.1 Luottamuksellisuus

Luottamuksellisuus tarkoittaa, että tietoja voi käsitellä vain ne henkilöt, joilla on siihen valtuus. Tämä periaate kattaa sekä yksityishenkilöiden, että organisaatioiden tietojen suojauksen. Organisaatiossa luottamuksellisuus tarkoittaa, että työntekijöille myönnetään pääsy vain niihin tietoihin, jotka ovat heidän työtehtäviensä kannalta tarpeellisia ja estetään pääsyn arkaluonteisiin tietoihin, jotka eivät kuulu heidän vastuulleen. (Safestate, n.d.)

Luottamuksellisuuden turvaaminen suojaa organisaatioita sisäisiltä ja ulkoisilta uhkilta kuten kyberhyökkäyksiltä, tietomurroilta tai muilta vahingoilta, jotka voisivat johtua epäasianmukaisesta pääsystä. Luottamuksellisuuden turvaaminen on olennainen osa tietosuojakäytäntöä ja se vaatii selkeiden pääsynhallintakäytäntöjen ja valvonnan käyttöä, jotta varmistetaan, että tiedot pysyvät turvassa ja niitä lain ja eettisen periaatteen mukaisesti (Fortinet, n.d.).

4.1.2 Eheys

Eheys eli tietojen oikeellisuus puolestaan varmistaa, että tiedot pysyvät oikeina ja luotettavina niiden koko elinkaaren ajan. Tämä tarkoittaa, että tietoihin ei voida tehdä luvattomia muutoksia tai manipulointia, eikä niitä voida tahallisesti tai vahingossa väärentää. (Safestate, n.d.)

CIA-mallissa eheys keskittyy enemmän tietojen suojaamisesta väärentämiseltä tai vahingolliselta muokkaamiselta. Tähän pyritään käyttämällä salausmenetelmiä ja erilaisia tarkistus menetelmiä kuten digitaalista allekirjoitusta, joilla voidaan varmistaa, että tieto on alkuperäisestä eikä siihen ole puututtu tai ole muokattu ilman valtuuksia. Tämä suojaa organisaatioita uhkilta, kuten hakkerointiyrityksiltä, tietojen manipuloinnilta ja vahingollisilta virheiltä. Tietojen eheys varmistetaan myös valvomalla, kuka käsittelee tietoja ja millä tavalla. (Fortinet, n.d.)

4.1.3 Saatavuus

Saatavuudella pyritään varmistamaan, että tiedot ovat saatavilla, kun niille on tarvetta. Tavoitteena on varmistaa, että oikeutetut käyttäjät pääsevät käsiksi tietoihin ilman viiveitä tai esteitä. Saatavuuden turvaaminen kattaa useita osa-alueita, kuten järjestelmien, palvelimien ja verkkojen toimivuuden sekä tiedonsiirtonopeuden. Tämä tarkoittaa, että tekniset infrastruktuurit ovat suunniteltu, että ne pystyvät käsittelemään tarvitun määrän käyttäjiä sekä liikennettä ilman häiriöitä (Safestate, n.d.)

Saatavuus voidaan varmistaa varmuuskopiointimenetelmillä, redundanssilla ja katastrofipalautusjärjestelmillä, jotka mahdollistavat tietojen palauttamisen ja järjestelmien käynnistämisen, vaikka ilmenee teknisiä ongelmia, luonnonkatastrofeja tai muita poikkeustilanteita. Näin pyritään estämään tilanne, jossa oikeutetut käyttäjät joutuisivat turvautumaan epäluotettaviin tai vähemmän turvallisiin keinoihin, kuten kolmannen osapuolen palveluihin, saadakseen tarvitsemansa tiedot. (Fortinet, n.d.)

Kuva 1. CIA-malli (Ekqvist ja muut, 2024).

4.1.4 AAA-malli

CIA-kolmiota voidaan laajentaa CIA-AAA-mallilla, joka tuo lisäulottuvuuden tietoturvakehykseen ottamalla huomioon käyttäjän roolin ja toiminnan. Tämä malli keskittyy erityisesti pääsynhallintaan, käytäntöjen ylläpitoon ja käyttäjätoiminnan valvontaan. Mallin kolme A-kirjainta tulevat englanninkielisistä termeistä: authentication (varmennus), authorisation (valtuutus) ja accounting (kirjanpito), jotka yhdessä muodostavat tärkeän osan verkon hallintaa ja kyberturvallisuutta. (Fortinet, n.d.)

CIA-AAA-malli täydentää perinteistä CIA-mallia erityisesti verkkopalveluiden pääsynhallinnan osalta. Varmennus tarkoittaa käyttäjän tunnistamista ja sen varmistamista, että hänellä on oikeus käyttää järjestelmää. Esimerkiksi käyttäjätunnus ja salasana ovat yleisiä tunnistautumismenetelmiä, joiden avulla varmistetaan käyttäjän henkilöllisyys ja verrataan tietoja tietokannan tallennettuihin tietoihin. (Fortinet, n.d.)

Valtuuttaminen puolestaan määrittelee, millä oikeuksilla käyttäjä pääsee käsiksi järjestelmän resursseihin. Valtuuttaminen antaa oikeudet pääsyyn tietyille alueille tai järjestelmän osiin ja määrittelee, mitä käyttäjä saa tehdä järjestelmässä. Järjestelmänvalvoja voi muokata käyttäjän oikeuksia, sallien pääsyn aikaisemmin kielletyille alueille tai estäen pääsyn tarvittaessa. (Fortinet, n.d.)

Kirjanpito pitää sisällään käyttäjän toiminnan ja resurssien käytön valvonnan ja kirjaamisen. Tämä tarkoittaa käyttäjän kirjautumisajan, lähetettyjen ja vastaanotettujen tietojen sekä IP-osoitteiden keräämistä ja tallentamista. Kirjanpitoa hyödynnetään myös käyttäjätoiminnan testaamiseen ja mahdollisten poikkeamien seurantaan. (Fortinet, n.d.)

CIA-AAA-malli luo kattavan tietoturvakehyksen, joka hallitsee pääsyä tietokoneresursseihin, ylläpitää käyttöpolitiikkoja ja valvoo käyttäjätoimintaa verkossa. Se on keskeinen osa verkkopalveluiden hallintaa ja

kyberturvallisuutta, koska se auttaa varmistamaan käyttäjien henkilöllisyyksiä ja seuraamaan heidän toimintaansa tehokkaasti. (Fortinet, n.d.)

4.2 Kyberturvallisuus

Kyberturvallisuus on tietoturvallisuuden osa-alue, mutta se keskittyy erityisesti verkko- ja tietojärjestelmien, niiden käyttäjien sekä muiden asianosaisten henkilöiden suojaamiseen kyberuhkilta. Se liittyy tiedon, tietojärjestelmien ja laitteiden turvallisuuden varmistamiseen verkkoympäristöissä (Ekqvist ja muut, 2024). Tämä vaatii teknisempää osaamista, sillä kyberturvallisuuden toimenpiteet ja suojaratkaisut ovat usein monimutkaisempia kuin perinteinen tietoturva.

Kyberturvallisuus, eli digitaalinen turvallisuus, kattaa käytännöt ja teknologiat, joiden avulla suojataan digitaalista tietoa, laitteita, resursseja verkkohyökkäyksiltä (Microsoft, n.d.). Traficomin (2020) mukaan kyberturvallisuus liittyy erityisesti organisaatioiden ja yhteiskunnan digitalisoitumisen myötä ilmeneviin turvallisuusuhkiin. Kyberuhat voivat vaikuttaa merkittävästi yrityksen toimintaan, talouteen, hallussa olevaan tietoon ja liiketoiminnan loppumiseen pahimmassa tapauksessa (Traficom, 2020, s. 4).

Kyberturvallisuus on keskeinen osa kansallista turvallisuutta ja sen merkitys kasvaa digitalisoituvassa maailmassa, jossa lähes kaikki yhteiskunnan toiminnot ovat kytkeytyneet tietoverkkoihin. Kyberturvallisuuden tavoitteena on suojata yhteiskunnan kriittistä infrastruktuuria ja elintärkeitä toimintoja vihamieliseltä kybervaikuttamiselta ja kyberrikollisuudelta. (Kotipelto, n.d.)

4.3 Kyberhyökkäys

Viime vuosina kyberhyökkäykset ovat lisääntynet merkittävästi ja digitalisaation myötä verkkorikollisten toiminta on saanut uusia ulottuvuuksia. Yhä useammat palvelut ja toiminnot siirtyvät verkkoon, mikä luo rikollisille uusia kohteita ja keinoja aiheuttaa vahinkoa. (Heikkinen, 2021.) Tämä kehitys tuo mukanaan entistä suuremman riskin, sillä vihamielinen taho voi iskeä verkon kautta kriittiseen infrastruktuuriin ja aiheuttaa merkittäviä vaurioita (Järvinen, 2023, s. 15).

Kyberhyökkäysten motiivit voi vaihdella rikollisesta toiminnasta poliittisiin tai eettisiin syihin. Yksi ylisimmistä motiiveista on taloudellinen hyöty, joka saadaan esimerkiksi kiristyksellä tai lunnailla. Poliittisella tai eettisellä motiivilla hyökkäyksellä pyritään vahingoittamaan esimerkiksi kilpailijaa tai vaikuttamaan yhteiskunnalliseen tilanteeseen. (Heikkinen, 2021.)

Kyberhyökkäykset voivat ilmetä monilla tavoilla ja niiden yleisimmät muodot ovat kiristysohjelmat, haittaohjelmat, tietojenkalastelu ja troijalaiset. Kiristysohjelmissa hyökkääjät lukitsevat laitteen tiedostot ja vaativat lunnaita järjestelmän palauttamiseksi, mutta maksaminen ei takaa palautusta. Haittaohjelmat voivat vahingoittaa järjestelmiä tai varastaa tietoja ja troijalaiset naamioituvat harmittomiksi tiedostoiksi, kuten laskuiksi varastaen henkilökohtaisia tietoja. Tietojenkalastelussa hyökkääjät huijaavat uhria antamaan tietonsa, esiintyen luotettavana tahona, kuten pankkina. (F-Secure, 2022.)

4.4 NIS2 direktiivi

NIS2 eli Network and Information security -direktiivi on Euroopan Unionin päivitetty kyberturvallisuusdirektiivi, joka korvasi aikaisemman NIS1-direktiivin. Direktiivi asettaa tietoturvavelvoitteita ja raportointivaatimuksia useilla keskeisillä sektoreilla (Luoma, 2024). NIS2 on yksi

Euroopan Unionin keskeisimpiä toimenpiteitä kyberturvallisuuden kehittämiseksi ja sillä pyritään vastaamaan muuttuviin kyberuhkiin. Direktiivin on tarkoitus astua voimaan osaksi kansallista lainsäädäntöä (Valtioneuvosto, 2022).

NIS2-direktiivi kattaa laajan joukon yrityksiä, jotka ovat yhteiskunnan näkökulmasta kriittisiä ja riippuvaisia tieto- ja viestintätekniikasta. Näihin toimialoihin kuuluvat energia, liikenne, vesihuolto, terveydenhuolto ja tärkeät palvelut, kuten pankkitoiminta. Direktiivin tavoitteena on saavuttaa yhtenäinen ja korkea kyberturvallisuustaso koko Euroopan Unionin alueella. (Traficom, 2025.)

Taulukko 1. Kriittiset toimialat (Kyberturvallisuuskeskus, n.d.).

Toimiala	Toimialan osa tai toimijatyyppi
Energia	Sähkö, kaukolämmitys ja -jäähdytys, kaasu, vety, öljy, latauspalvelujen tarjoajat loppukäyttäjille
Liikenne	Ilmaliikenne, raideliikenne, vesiliikenne, tieliikenne
Pankkitoiminta	Luottolaitokset
Finanssimarkkinoiden infrastruktuurit	Kauppapaikkojen ylläpitäjät ja keskusvastapuolet
Terveys	Terveydenhuoltopalvelujen tarjoajat, EU:n vertailulaboratoriot, lääkkeiden tutkimus ja kehitys, lääkeaineiden ja lääkkeiden valmistus, kansanterveyden kriittisten lääkinnällisten laitteiden valmistus hätätilanteessa
Juomavesi	
Jätevesi	
Digitaalinen infrastruktuuri	Hyväksytyt luottamuspalveluntarjoajat
	Ei-hyväksytyt luottamuspalveluntarjoajat
	DNS-palveluntarjoajat (lukuun ottamatta juurinimipalvelimia)
	Aluetunnusrekisterit
	Yleisten sähköisten viestintäverkkojen tarjoajat
	Yleisesti saatavilla olevat sähköisten viestintäpalveluiden tarjoajat
	Internetin yhdysliikennepisteiden tarjoajat
	Pilvipalveluntarjoajat
	Datakeskuspalveluntarjoajat
	Sisällönjakeluverkkojen tarjoajat
Yritysten välinen TVT-palvelujenhallinta	Hallintapalveluntarjoajat, tietoturvapalveluntarjoajat
Avaruus	Maanpäällisen infrastruktuurin ylläpitäjät
Julkishallinto	Keskeiset toimijat: tiedonhallintalakiehdotuksessa* määritellyt toimijat
	Tärkeät toimijat: hyvinvointialueet ja -yhtymät sekä Helsingin kaupunki*

Direktiivi asettaa vaatimuksia kyberturvallisuuden hallintaan eri tasoilla ja sen myötä organisaatioiden on toteutettava käytännön toimenpiteitä suojaamiseksi. Toimijoilla on oltava käytössään ajan tasalla oleva kyberturvallisuuden riskienhallintamalli, jonka avulla voidaan hallita ja suojata verkkoja ja tietojärjestelmiä mahdollisilta uhkilta ja häiriöiltä. (Euroopan komissio, 2025.)

Riskienhallinta ja suojaus:

Organisaatioiden on toteutettava tehokkaita teknisiä ja hallinnollisia toimenpiteitä verkkojen ja järjestelmien suojaamiseksi. Tämä sisältää muun muassa haavoittuvuuksien hallinnan, salauksen ja pääsynvalvonnan sekä muiden tietoturvatoimenpiteiden käyttöönoton. (Traficom, 2025.)

Häiriöiden torjunta ja reagointi:

Organisaatioiden on kyettävä torjumaan kyberuhkia ja tunnistamaan häiriöitä nopeasti. Lisäksi niiden on oltava valmiita reagoimaan tehokkaasti ja ennakoivasti kaikkiin kyberuhkiin ja -hyökkäyksiin. Tämä edellyttää, että organisaatioilla on valmiit suunnitelmat ja prosessit häiriötilanteiden hallintaan. (Traficom, 2025.)

Tietoturvapoikkeamat:

Mikäli kyberhyökkäyksiä tai järjestelmähäiriöitä tapahtuu, organisaatioiden on ilmoitettava viranomaisille ja asiakkailleen tietoturvapoikkeamista tietyssä aikarajassa. Direktiivi määrittää tarkat aikarajat, joiden puitteissa poikkeamista on raportoitu. Tämä varmistaa, että mahdollisiin uhkiin voidaan reagoida nopeasti ja oikea-aikaisesti. (Traficom, 2025.)

Toimintavarmuus ja jatkuvuus:

Organisaatioiden on otettava käyttöön varautumissuunnitelmat ja palautusstrategiat, jotka varmistavat liiketoiminnan jatkuvuuden häiriötilanteissa. Toimintavarmuus edellyttää, että organisaatiot ovat valmiita palautumaan nopeasti mahdollisista kyberhyökkäyksistä tai muista häiriöistä, jotka voivat vaikuttaa niiden toimintaan. (Traficom, 2025.)

NIS2-direktiivi tuo merkittäviä muutoksia erityisesti kriittisten toimialojen kyberturvallisuuden hallintaan ja vaatii organisaatioilta aiempaa suurempaa vastuullisuutta. Direktiivin noudattaminen edellyttää sekä teknisiä, että organisatorisia toimenpiteitä, ja sen täytäntöönpano on olennainen osa EU:n laajuisen kyberturvallisuuden kehittämistä. (Traficom, 2025.)

5 KRIITTISET INFRASTRUKTUURIT

Kriittiset infrastruktuurit koostuvat yhteiskunnan kannalta elintärkeitä järjestelmiä, joiden toimintahäiriöillä voi olla vakavia seuraamuksia. Näihin järjestelmiin kuuluu lämmitysenergia, sähkö, kuljetus, puhtaan veden ja jäteveden käsittely sekä viestintä. (Raivio, 2024.) Näiden järjestelmien luotettava toiminta on välttämätöntä yhteiskunnan turvallisuuden ja hyvinvoinnin kannalta.

5.1 Tuotantoverkot

Teollisuuden tuotantoverkot eli OT-verkot (Operational Technology), ovat perinteisesti olleet eristettyjä julkisesta internetistä ja yrityksen omista IT-järjestelmistä, mikä tarjosi niille suojan kyberuhkia vastaan. Ne oli suunniteltu toimimaan itsenäisesti ilman suoraa yhteyttä muihin järjestelmiin, mikä teki niistä vähemmän alttiita hyökkäyksille. (Jurvanen, 2025.)

Digitalisaation edetessä ja liiketoiminnan siirtyessä enemmän verkkoon on OT-verkkojen valvontatarve kasvanut merkittävästi. Tämä on johtanut siihen, että aiemmin tiukat eristykset ovat muuttuneet joustavimmiksi ja verkkojen yhteyksien laajentaminen on tullut tarpeelliseksi tehokkaan toiminnan ja hallinnan mahdollistamiseksi. Tämän seurauksena OT-verkot ovat alttiimpia kyberhyökkäyksille, sillä verkkojen avoimuus on kasvanut ja hyökkääjät voivat löytää uusia reittejä päästäkseen kyseisiin järjestelmiin. (Toivonen, 2020.)

OT-verkot ovat järjestelmiä, jotka ohjaavat ja valvovat teollisuuden tuotantoverkkojen kriittisiä toimintoja, kuten sähköverkkojen hallintaa. Ne koostuvat erilaisten laitteiden, ohjelmistojen ja verkkojen yhdistelmästä, jotka mahdollistavat tiedonsiirron ja kommunikoinnin laitteiden välillä, varmistaen näin tuotantoprosessin sujuvuuden ja tehokkuuden. OT-verkot on suunniteltu korkeaan reaaliaikaiseen tiedonsiirtoon ja verkkoon kuuluu järjestelmiä, kuten SCADA, sekä antureita, pumppuja

ja katkaisijoita, jotka valvovat ja keräävät tietoa tuotantoprosessien tilasta (Kuva 2). (Jurvanen, 2025.)

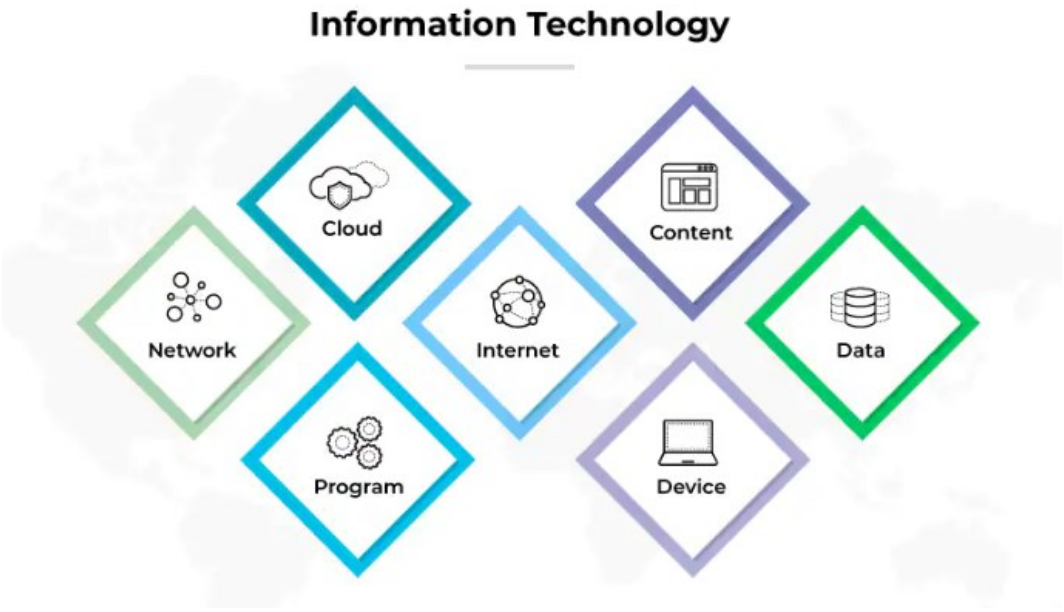
Kuva 2. OT-verkkojen osa-alueet (Paloalto, n.d).

5.2 OT- ja IT-verkkojen keskeiset erot

IT (Information Technology) ja OT (Operational Technology) ovat kaksi erilaista verkkoteknologioiden ja järjestelmien luokkaa, jotka eroavat toisistaan useilla merkittävillä tavoilla. IT-verkot keskittyvät tietojen käsittelyyn, siirtoon ja tallentamiseen digitaalisten laitteiden avulla. Ne tukevat liiketoimintaa ja organisaation toimintaa, kuten tietokoneiden käyttöä, ohjelmistojen kehittämisen, tietohallintoa ja verkkoteknologioita. IT kattaa myös verkkosivustojen ja sovellusten kehittämisen, tiedonsiirtoprotokollat ja verkkoturvallisuuden. IT on keskeinen osa yritys toimintaa ja sen teknologioita, joita käytetään internetin ja sen palveluiden hyödyntämiseen (Kuva 3). Toisin kuin IT, OT-verkot ovat erikoistuneita teollisuuden ja palvelualojen järjestelmiin, jotka keskittyvät fyysisten laitteiden ja prosessien valvontaan ja ohjaukseen. (Jurvanen, 2025.)

Verkot eroavat myös laitteiden elinkaaren suhteen. IT-verkot käyttävät yleensä laitteita, joiden keski-ikä on noin 3–6 vuotta, kun taas OT-verkot on suunniteltu pitkäaikaiseen käyttöön. IT-verkot yhdistyvät yleensä toisiinsa ja käyttävät yleisesti käytettyjä käyttöjärjestelmiä, kuten Windows tai IOS:ää. Sen sijaan OT-verkot voivat sisältää erikoistuneempia järjestelmiä, jotka eivät ole yhtä helposti yhdistettävissä toisiinsa. (Jurvanen, 2025.)

Turvallisuusvaatimukset ovat myös erilaisia IT- ja OT-verkkojen välillä. Vaikka molemmissa pyritään suojaamaan järjestelmiä ja dataa, niiden prioriteetit poikkeavat. IT-verkkojen turvallisuudessa keskeistä on usein tietojen luottamuksellisuus, eheys ja saatavuus (CIA-malli), kun taas OT-verkkojen turvallisuus keskittyy enemmän järjestelmien saatavuuteen ja toimintakykyyn, sillä ne ovat suoraan yhteydessä teollisiin prosesseihin ja laitteisiin, joiden häiriöt voivat aiheuttaa vakavia seurauksia. (Peltola, 2023.)



Kuva 3. IT-verkkojen osa-alueet (Paloalto, n.d.).

5.3 Tuotantoverkkojen haasteet

Teollisuuden infrastruktuurit ovat jatkuvasti kyberuhkien kohteena, ja kyberhyökkäykset voivat aiheuttaa merkittäviä haittoja, kuten tuotannon keskeytyksiä, laadun heikkenemistä ja vaaratilanteita (Jurvanen, 2025). Aiemmin tuotantoverkot on pidetty erillään IT-verkoista, mutta nykyään niitä yhdistetään, jotta voidaan saavuttaa joustavampi pääsy verkon resursseihin ja hyödyntää dataa joustavasti, jopa reaaliajassa (Toivonen, 2020). Tämän yhdistäminen tuo mukanaan uusia haasteita, sillä tuotantoverkot altistuvat nyt enemmän ulkopuolisille hyökkäyksille joko suoraan tai muiden IT-infrastruktuurien kautta. Erityisesti koska tuotantoverkkoja ei ole suojattu samalla tasolla kuin IT-verkkoja, niiden haavoittuvuudet voivat avata mahdollisuuksia hyökkäyksille (Toivonen, 2020).

OT-verkkojen suojaaminen vaatii erikoistuneita käytäntöjä, sillä ne eivät ole yhtä joustavia tai helposti päivitettävissä kuin perinteiset IT-verkot. Päivitysten tekeminen OT-verkoissa on usein haastavaa, minkä vuoksi

niitä päivitetään epäsäännöllisesti tai ei lainkaan. Lisäksi monet laitteistot ovat suunniteltu kestämään pitkään, mikä tarkoittaa, että monet järjestelmät ovat nykyään jo elinkaarensa lopussa (Jurvanen, 2025). Vanhentuneiden ja suojaamattomien järjestelmien liittäminen IT-verkkoon paljastaa uusia haavoittuvuuksia, koska monet vanhat järjestelmät eivät tarjoa tarvittavaa suojaa nykyaikaisia kyberuhkia vastaan.

Yksi OT-verkkojen erityispiirteistä on se, että niissä ei ole yleisesti otettu käyttöön hyökkäyksenestojärjestelmiä (IPS, Intrusion Protection System). Nämä järjestelmät, jotka normaalisti suojaavat IT-verkoissa haitallisilta hyökkäyksiltä, voivat erehtyä tunnistamaan tuotannon verkon toiminnat väärin. Tämä voi johtaa väärien hälytyksien tai jopa tuotannon keskeytymiseen, mikä tekee niiden käytöstä OT-verkkojen kaltaisissa ympäristöissä haasteellista. (Jurvanen, 2025.)

Tämä yhdistäminen ja vanhojen järjestelmien käyttö asettaa entistä suurempia paineita OT-verkkojen kyberturvallisuudelle ja korostaa tarvetta kehittää entistä parempia suojaratkaisuja ja käytäntöjä, jotka huomioivat verkkojen erityispiirteet ja haavoittuvuudet.

5.4 SCADA-järjestelmä kyberhyökkäyksen kohteena

SCADA (Supervisory Control and Data Acquisition) on yksi Hitachin tarjoamista ratkaisuista, joka mahdollistaa reaaliaikaisen valvonnan ja ohjauksen muun muassa voiman tuotannossa, jakelussa, liikenteessä ja vesihuollossa (Network manager SCADA, n.d.). Se on olennainen osa monien elintärkeiden palvelujen hallintaa, mutta sen suojaaminen on haasteellista kyberuhkien vuoksi, erityisesti etäyhteyksien lisääntymisen myötä. Alun perin SCADA-järjestelmät olivat fyysisesti eristettyjä, mutta nykyään niiden liittäminen verkkoihin tuo etuja, mutta myös lisää haavoittuvuuksia. (Alanazi ja muut, 2023.)

SCADA-järjestelmien ja IT-järjestelmien turvallisuusvaatimukset eroavat toisistaan. IT-järjestelmät painottavat tietojen luottamuksellisuutta,

eheyttä ja saatavuutta, kun taas SCADA-järjestelmässä saatavuus on korkeimmalla prioriteetilla. Tärkein tavoite on järjestelmän jatkuva ja häiriötön toiminta reaaliaikaisissa prosesseissa. SCADA-järjestelmät ovat usein resurssirajoitteisia, eivätkä ne sisällä samoja turvatoimia kuin perinteiset IT-järjestelmät. Näiden rajoitusten vuoksi järjestelmien päivitykset voivat jäädä huomiotta, mikä altistaa ne kyberhyökkäyksille. (Alanazi ja muut, 2023.) Palomuurit ovat olennainen osa SCADA-järjestelmien suojaamista. Ne toimivat ensilinjaisena puolustuksena valvomalla ja rajoittamalla verkkoliikennettä, suojaten kriittisiä teollisuusprosesseja ja infrastruktuuria luvattomilta pääsyiltä ja potentiaalisilta uhkilta. (Jurvanen, 2023.) Koska SCADA-järjestelmät ovat kriittisen infrastruktuurin selkäranka, on tärkeää varmistaa verkkojen suojaus, jotta odottamattomia haavoittuvuuksia ei löydy, joita kyberrikolliset voisivat hyödyntää.

Esimerkkinä SCADA-järjestelmän haavoittuvuuksista voidaan mainita Ukrainan kyberhyökkäys vuonna 2015, jolloin hakkeroijat tunkeutuivat Ukrainan sähköverkon SCADA-järjestelmään ja saivat aikaan laajoja sähkökatkoksia. Hyökkäys kohdistui erityisesti sähköverkon infrastruktuuriin ja se vaikutti satoihin tuhansiin ihmisiin. (McElfresh, 2016.) Hyökkäys osoitti, kuinka kyberhyökkäykset voivat vaarantaa kriittisen infrastruktuurin toiminnan ja aiheuttaa vakavia seurauksia.

SCADA-järjestelmät ovat nykyään alttiimpia kyberuhkille, koska ne käyttävät kaupallisia verkkoprotokollia ja sovellusarkkitehtuureja, jotka voivat sisältää haavoittuvuuksia. Näiden haavoittuvuuksien vuoksi SCADA-järjestelmien suojaamiseen on kiinnitettävä erityistä huomiota, ja tarvitaan kehittämistä ja uusia turvatoimia, jotta ne pysyvät suojattuina ja toimintakykyisinä kriittisissä ympäristöissä. (Alanazi ja muut, 2023.)

6 ERISTETYT VERKOT

Eristäminen on olennainen osa tietoturva toimia ja sen avulla voidaan merkittävästi vahvistaa järjestelmien luottamuksellisuutta. Verkon eristäminen tarkoittaa käytännössä sitä, että tietyt järjestelmät tai verkot pidetään erillään muista järjestelmistä estäen näin mahdollisten uhkien leviämistä. Eristämällä kriittisiä järjestelmiä ja verkkoja, kuten tuotanto- ja ohjausverkkoja, voidaan minimoida vaikutukset mahdollisissa kyberhyökkäyksissä (VPN Unlimited, n.d.-b).

Verkkojen eristäminen on erityisen tärkeää silloin kun ne hallitsevat yhteiskunnan kriittisiä toimintoja kuten energiantuotantoa, liikenteen ohjausta tai terveydenhuollon järjestelmiä. Tällöin jopa pienetkin häiriöt voivat johtaa vakaviin seurauksiin ja jopa liiketoiminnan keskeytyksiin. (Heikkinen, 2021.)

6.1 Tietoverkon eristäminen

Verkkojen eristäminen mahdollistaa verkon jakamisen pienempiin osiin, kuten segmentteihin tai vyöhykkeisiin, joilla on omat turvallisuusparametrinsä ja pääsyvalvontansa (Jurvanen, 2024). Näitä eristettyjä osia kutsutaan aliverkoiksi, mikä tekee koko verkon hallinnasta helpompaa ja joustavampaa. Tämän lähestymistavan etuna on, että kunkin verkko-osan hallinta ja suojaaminen voidaan toteuttaa erikseen, mikä parantaa verkon kokonaisvaltaista turvallisuutta. (Nile, n.d.)

Kun verkon osat eristetään toisistaan, mahdollisen hyökkäyksen sattuessa koko verkko ei ole alttiina vaaralle, koska hyökkääjä ei pääse automaattisesti siirtymään muihin verkon osiin (Jurvanen, 2024). Tämä rajoittaa uhkien leviämistä, mikä puolestaan pienentää kokonaisriskiä ja parantaa verkon kykyä kestää hyökkäyksiä.

6.2 Verkon suojaaminen eristämisen avulla

Eristämisellä on useita eri toteutustapoja ja näiden valinta riippuu monista tekijöistä, kuten organisaation tarpeista, verkon rakenteesta, käytettävissä olevista resursseista ja turvallisuusvaatimuksista. Eristämisen päätavoitteena on jakaa verkko erillisiin osiin, joita voidaan hallita ja suojata erikseen, mikä parantaa verkon turvallisuutta ja estää uhkien leviämistä koko järjestelmään (Traficom, 2020, s. 11). Eristämisen toteutustavat voidaan jakaa useisiin eri kategorioihin, kuten fyysinen, looginen ja sovellustason eristäminen. Jokaisella lähestymistavalla on omat etunsa ja haasteensa.

6.2.1 Fyysinen segmentointi

Fyysinen eristäminen tarkoittaa verkon jakamista erillisiksi osiksi käyttämällä laitteistoja, kuten reitittimiä, kytkimiä ja palomuureja. Tämä lähestymistapa luo fyysisiä rajoja verkon eri osien välille, jolloin verkko voidaan jakaa pienempiin aliverkkoihin. Fyysisen eristyksen avulla voidaan tehokkaasti suojata verkon osia toisistaan ja estää liikenteen kulkeminen näiden osien välillä ilman erillisiä pääsyvalvontakäytäntöjä. (Kothari, 2024.)

Vaikka fyysinen eristäminen tarjoaa usein parhaan turvallisuustason, se vaatii myös huomattavasti enemmän laitteistoresursseja ja infrastruktuuria. Tämä lisää kustannuksia ja voi tehdä verkon hallinnasta monimutkaisempaa ja vähemmän joustavaa. Fyysinen eristys on erityisen hyödyllinen ympäristöissä, joissa turvallisuus on ensisijainen prioriteetti ja joissa verkon eri osien välinen liikenne on tarpeen estää kokonaan. (Kothari, 2024.)

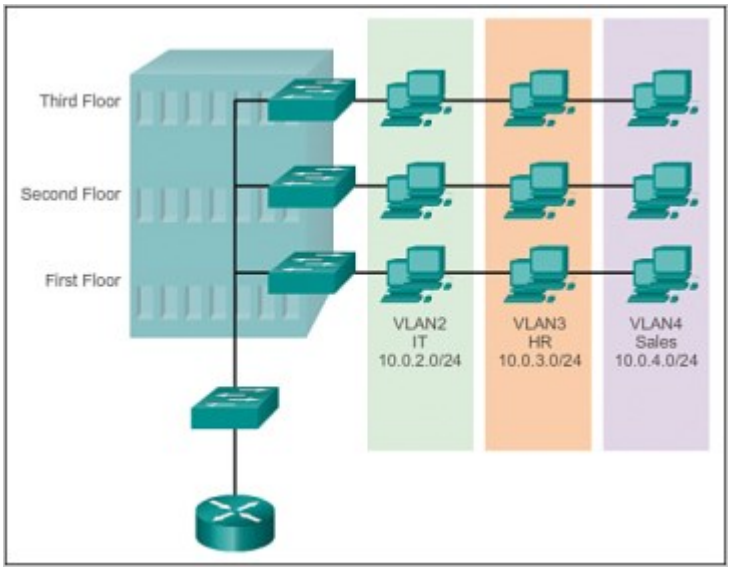
6.2.2 Looginen segmentointi

Looginen eli virtuaalinen eristäminen on joustavampi vaihtoehto, jossa hyödynnetään virtuaalilähiverkkoa (VLAN). VLAN integroidaan fyysiseen verkkoympäristöön, mutta se mahdollistaa verkon jakamisen loogisiin

osiin. Lähiverkon avulla laitteet voidaan ryhmitellä esimerkiksi niiden toiminnan, osaston tai turvallisuustason mukaan. (Kothari, 2024.)

VLANn avulla suuri tietoverkko voidaan jakaa useampiin *broadcast* -alueisiin, mikä parantaa verkon hallittavuutta. VLANn sisällä laitteet toimivat ikään kuin omassa erillisessä verkossaan. Jokainen VLAN luokitellaan erilliseksi loogiseksi verkoksi. (Cisco press, 2014.)

Kuvassa 4 esitetään, kuinka verkko voidaan jakaa ja ryhmitellä fyysisten kytkinten sijasta loogisesti esimerkiksi organisaation tiimien tai laitteiden toiminnan perusteella (Cisco press, 2014). Tämä lähestymistapa on helpompi hallita verrattuna fyysiseen eristämiseen, mutta se ei tarjoa yhtä vahvaa suojaa. VLAN-verkoissa voi olla riski tietovuodoille, koska verkossa kulkee sisäistä liikennettä. Tämä riski korostuu erityisesti, jos verkon segmentointi ei ole riittävän tarkkaa. (Kothari, 2024.)



Kuva 4. VLAN-segmentointi (Cisco Press, 2014).

6.2.3 Sovellustason eristäminen

Sovellustason eristäminen menee pidemmälle kuin perinteinen virtuaalinen eristäminen, koska se keskittyy yksittäisten sovellusten tai prosessien eristämiseen. Tämä toteutetaan käyttämällä tekniikoita, kuten säiliöittämistä ja mikrosegmentointia. (Kothari, 2024.)

Säiliöittäminen rajoittaa säiliöiden välistä vuorovaikutusta ympäristöissä kuten Docker ja Kubernetes. Sovellukset ja niiden riippuvuudet pakataan säiliöihin, jolloin ne voidaan suorittaa itsenäisesti eri ympäristöissä, mikä tekee niistä siirrettäviä ja johdonmukaisia. Säiliökuvat sisältävät sovelluksen, kirjastot, binääritiedostot ja asetustiedostot, jolloin ympäristön erityisvaatimuksia ei tarvitse huolehtia. (VPN unlimited, n.d.-a.)

Mikrosegmentointi puolestaan jakaa verkkoliikenteen pienempiin, eristettyihin osiin, parantaen verkon tietoturvaa. Se mahdollistaa tarkemman pääsynvalvonnan ja turvallisuuspolitiikkojen räätälöinnin, vähentäen hyökkäysalueita ja estäen sivuttaisliikkeen. Segmentit voivat perustua esimerkiksi tietojen herkkyyteen tai käyttäjärooleihin, ja ne estävät mahdollisen tietomurron leviämisen. (VPN unlimited, n.d.-d)

Sovellustason eristäminen antaa tarkempaa kontrollia turvallisuuteen, mutta sen toteutus voi olla monimutkainen, vaativan erikoistyökaluja ja asiantuntemusta. Tämä lähestymistapa on erityisen hyödyllinen ympäristöissä, kuten pilvipalveluissa, joissa sovellusten eristäminen on tärkeää.

6.3 Eristyksen testaaminen ja sen haasteet

Eristetyn verkon suurin haasteen, että yritykset eivät voi olla täysin varmoja, kuinka hyvin suojaus toimii. Vuotokohtia voi syntyä tahattomasti

konfiguraatiomuutosten, inhimillisten virheiden tai vihamielisten toimijoiden vuoksi (Traficom, 2020, s. 9). Tällaiset vuotokohdat voivat jäädä huomaamatta ja paljastaa arkaluontoista tietoa (Advenica, n.d). On kuitenkin ensiarvoisen tärkeää havaita vuotokohtia mahdollisimman nopeasti, jotta ne voidaan korjata ennen kuin niitä pystytään hyödyntämään.

Traficom teki tutkimuksen eristyksien turvallisuudesta eri yrityksillä ja tulokset olivat huolestuttavia: 81 % yritysten järjestelmistä sisälsi odottamattomia vuotokohtia, vaikka niiden piti olla täysin eristettyjä. Tämä korostaa tarvetta tehokkaalle testausratkaisulle, jotka voivat havaita haavoittuvuudet nopeasti. (Traficom, 2020.)

Verkkojen testauksen tarkoituksena on löytää mahdollisia tietoturvahyökkäyksille alttiita aukkoja eristetyistä verkoista. Testausprosessi vaatii osaamista verkkotekniikoista ja protokollista. Tavoitteena on käydä läpi koko eristetty verkko, mukaan lukien osoiteavaruudet, segmentit ja tunnistaa kytketyt laitteet ja järjestelmät. Verkkojen testauksessa yleisimmin käytetyt työkalut ovat Wireshark ja Nmap. (Varghese, 2024.)

Wireshark on avoimen lähdekoodin pakettianalysaattori, jolla voidaan seurata verkon liikennettä. Sen avulla voidaan analysoida verkon protokolleja ja tarkastella, mitä verkossa tapahtuu. Wireshark nappaa paketteja verkon yhteyksistä, kuuntelee reaaliaikaisesti verkon liikennettä ja voi napata koko liikenteen virtauksen. Lisäksi se mahdollistaa pakettien suodattamisen, jolloin käyttäjä voi kohdistaa tutkimuksen haluamaansa liikenteeseen. (Hedge, 2020.) Wireshark visualisoi verkon paketteja, mikä antaa käyttäjälle selkeän kuvan verkon toiminnasta ja tapahtuneista yhteyksistä.

Nmap on avoimen lähdekoodin verkkoskanneri, joka skannaa IP-osoitteita ja niiden takana olevia avoimia portteja sekä sovelluksia. Nmapilla voidaan helposti selvittää verkossa olevat laitteet, niiden IP-osoitteet ja avoimet portit, mikä auttaa tunnistamaan mahdollisia haavoittuvuuksia.

Nmapia käytetään erityisesti penetraatiotestauksessa ja verkkoturvallisuuden arvioinnissa. (Nmap, n.d.)

Perinteisesti verkon testaus on ollut manuaalinen prosessi, joka on aikaa vievä ja työläs. Testausmenetelmät eivät ole olleet täysin automatisoituja, mikä tekee niiden suorittamisesta haasteellista. Eristyksen testaukseen käytettävien automaattiseen työkalujen määrä markkinoilla on ollut rajallinen, mutta kaksi merkittävää ratkaisua ovat SensorFun kehittämä Beacon sekä israelilaisen XMCyberin tuote.

7 SENSORFU JA BEACON

7.1 SensorFu

SensorFu on vuonna 2017 Oulussa perustettu osakeyhtiö, joka erikoistuu IT-konsultointiin ja -palveluihin (Finder, n.d.-b). Yritys kehittää ratkaisuja erityisesti verkko- ja tietoturvan vahvistamiseksi ja sen tuotteet on suunniteltu suojaamaan organisaatioiden kriittistä infrastruktuuria luvattomalta pääsyltä. Yksi yrityksen päätuotteista on Beacon-eristyksentestausjärjestelmä.

Asiakaskunta koostuu yrityksistä ja tahoista, jotka käsittelevät teollisuuden ohjausjärjestelmiä, automaatioverkkoja, turvakamerajärjestelmiä, hallintaverkkoja sekä muita kriittisiä verkkoympäristöjä, jotka vaativat jatkuvaa suojausta. Yrityksiä, jotka kuuluvat asiakaskuntaan ovat muuan muassa Suomen ilmavoimat, Kyberturvallisuuskeskus, Erillisverkot, Synopsys, Seagate, Fingrid, Traficom ja monia muita teollisuuden yrityksiä. (SensorFu, n.d.-b.)

7.2 Eristyksen testausjärjestelmä Beacon

SensorFu Beacon on ohjelmisto, joka on suunniteltu valvomaan eristettyjen verkkojen eheyttä havaitsemalla mahdollisia vuotokohtia (SersorFu, n.d, s. 1). Beacon luo mahdollisuuden verkon eristyksen jatkuvan ja automatisoidun valvonnan, joka parantaa organisaatioiden kykyä havaita mahdollisia vuotoja ja heikkouksia tietoturvassa.

Perinteisesti eristyksen testaus on ollut manuaalinen prosessi, mutta Beaconin avulla kyseinen prosessi voidaan automatisoida. Beaconit seuraavat ja mittaavat jatkuvasti verkon eristyksen tilaa ja havaitsevat mahdolliset vuodot reaaliaikaisesti. (Traficom, 2020, s. 8–9.)

7.3 Toimintaperiaate

Ohjelmisto koostuu kahdesta pääkomponentista: Beacons ja Home. Beacon-komponentti etsii jatkuvasti uusia verkko vuotoreittejä aktiivisen verkon toiminnan avulla, kun taas Home-komponentti kuuntelee onnistuneita pakoja ja luo niistä havainnot sekä käyttäjälle hälytyksen (Kuva 5).

Verkkojen eristys on yksi keskeisimmistä tietoturvakäytännöistä korkean turvallisuuden verkoissa, ja Beacon valvoo, että eristys on toteutettu asianmukaisesti. Beacon automatisoi normaalisti manuaalisesti suoritettavan testauksen ja tuottaa havaintoja sekä hälytyksiä löydetyistä vuotokohdista. (SersorFu, n.d.)

Kuva 5. Beaconin toimintaperiaate (SensorFu, n.d.-b).

7.3.1 Beacon

Beacon toimii eristetyissä verkoissa ja tunnistaa mahdollisia tietoturvapoikkeamia, kuten odottamattomia yhteyksiä ulkoverkkoon. Se toimii

agenttina, joka etsii ja tunnistaa poikkeamia, kuten mahdollisia pakoreittejä, joiden ilmentymisen avulla voidaan parantaa verkon turvallisuutta, kun haavoittuvuudet tulevat tietoon Beaconin avulla. (SensorFu, n.d.-c.)

Beacon asennetaan eristettyyn järjestelmään, jossa se pyrkii löytämään pakoreittejä kohti Home-osoitetta kokeilemalla useita erilaisia pakokeinoja. Beacon voidaan asentaa eristetyille verkkoalueille joustavasti virtuaalikoneena, sovelluksena tai laitteena, riippuen ympäristön ja käyttökohteen tarpeista. Se voidaan luoda virtuaalikoneena sekä sovelluksena Windows- tai Linux-ympäristöissä, tai vaihtoehtoisesti laitteena Raspberry Pillä. (SensorFu, n.d.-a.)

Tämä monipuolinen asennusmahdollisuus mahdollistaa Beaconin käyttöönoton erilaisten ympäristöjen ja verkko-olosuhteiden mukaan. Beaconin ympäristö valitaan aina sen perusteella, mikä parhaiten tukee järjestelmän tarpeita ja käyttötarkoitusta, tarjoten tehokkaan ja joustavan tavan skannata eristettyjä verkkoja.

7.3.2 Home

Home on keskeinen osa Beaconin toimintaa, sillä se mahdollistaa eristetyistä ympäristöistä tulevien onnistuneiden pakoyritysten tarkkailun. Beacon pyrkii pakenemaan kohti Home-palvelinta, joka kuuntelee verkkoliikennettä ja yrittää havaita eristetyistä verkoista tulevat yhteydet. Home toimii vastaanottimena Beaconin pakoyrityksille sekä käyttöliittymänä SensorFun Beaconin asetuksille. (SersorFu, n.d.))

Home-palvelimella hallitaan Beaconeita, luodaan niille konfiguraatioita ja seurataan hälytyksiä. Home voi olla joko fyysinen tai virtuaalinen asennus ja Home-komponentteja voi olla useita eri ympäristöissä, kuten paikallisesti asennettuna ja julkiseen internettiin asennettu Home. Home- komponentissa on HTTP-rajapinta sekä ohjelmistorajapinta (API) ja rajapinta on suojattu TSL-protokollalla. (SensorFu, n.d.-a.)

7.3.3 Hälytys

Beaconin paon onnistuessa Home tuottaa paosta havainnon ja lähettää käyttäjälle hälytyksen, joka sisältää analyysin paosta ja sen tiedoista. Hälytyksillä on "jäähdytys" ajanjakso, joka kestää kolme viikkoa. Tämän jakson aikana, jos pakotapa tekee jatkuvasti onnistuneita läpilyöntejä, käyttäjälle ei lähetetä jatkuvia hälytyksiä. (Alerts, n.d.-a.)

Hälytyksen asetukset määritellään Home-hallintaympäristössä ja hälytysviestit toimitetaan JSON-objekteina. Hälytyksiä voidaan lähettää käyttäjälle Slackin tai Webhookin kautta sähköpostiin. Home ympäristössä hälytyksiä voidaan säilyttää enintään 30 päivän ajan ja enimmillään 2,5 miljoonaa kappaletta. Koska Homea ei ole suunniteltu pitkäaikaiseen hälytysten säilyttämiseen, hälytykset tulee siirtää SIEM-järjestelmään, jos niitä halutaan säilyttää pidempään. Tämä voidaan tehdä käyttäen hälytysintegrointia tai havaintojen Token API-ominaisuutta. (Alerts, n.d.-a.)

7.4 Testausmenetelmät

Beacon on suunniteltu tarjoamaan kattavaa ja monipuolista verkon testausta eristetyissä järjestelmissä. Se tukee useita testausmenetelmiä, jotka auttavat havaitsemaan verkon haavoittuvuuksia ja heikkouksia eri näkökulmista. Laitteessa on tuki sekä IPv4 ja IPV6-protokollille, mikä mahdollistaa verkon testaamisen eri protokollaversioiden mukaan. (SensorFu, n.d.-a.)

Testausprosessi koostuu kahdesta rinnakkain toimivasta syklistä: nopeasta ja hitaasta syklistä (Escape methods, n.d.-a). Näiden syklien avulla laite voi tarkastella verkon turvallisuutta eri aikarajoissa ja intensiteetillä, tarjoten joustavuutta sekä kattavuutta haavoittuvuuksien kartoittamisessa.

Nopea sykli kestää noin puoli tuntia ja keskittyy verkon näkyvimpiin ja helposti hyödynnettävissä oleviin haavoittuvuuksiin. Tässä syklissä laite etsii erityisesti tunnettuja pakopaikkoja, kuten tärkeitä TCP- ja UDP-portteja sekä verkon yleisesti käytettyjä protokollia, kuten DNS, ICMP ja broadcast. (Escape methods, n.d.-a.) Nopea sykli tunnistaa kiireelliset uhkat, joita voidaan hyödyntää mahdollisissa verkkohyökkäyksissä.

Hidas sykli kestää 4–14 päivää ja sen tarkoituksena on tehdä kattavampi tarkastus verkosta. Hidas sykli käy läpi kaikki TCP- ja UDP-portit sekä verkon muut osat, mutta se tapahtuu huomattavasti hitaammin ja aiheuttaen vähemmän kohinaa verkossa verrattuna nopeaan sykliin. Tämä varmistaa, ettei testaus aiheuta liiallista häiriötä verkon normaalille toiminnalle, mutta samalla voidaan havaita haavoittuvuuksia, joita nopeassa testauksessa ei välttämättä löydettäisi. (Escape methods, n.d.-a.)

Beaconin tehtävänä on lähettää ping-viestejä kohti Home-palvelinta etsiäkseen reitin eristetystä verkosta ulospäin. Tämä ping-viesti sisältää vain perustiedot, jotta Home-palvelin ymmärtää viestin lähteen, lähettäjän ja kohteen. Kun Home-palvelin vastaanottaa ping-viestin, se tarkistaa sen tiedot ja antaa tarvittaessa hälytyksen, jonka kautta käyttäjä saa tiedon pingin saapumisesta. (Herrala, 2017.)

SensorFun luoma ping-viesti poikkeaa perinteisestä ping-komennosta tai ICMP echo -paketista. Beaconin ping-viestiin on lisätty erityisesti kolme tärkeää tietoa: Beaconin nimen, järjestysnumeron sekä "kind"-niminen objektin. Kind-objekti määrittelee ping-viestin tyypin ja sisältää tietoa käytetystä protokollasta, kohde-IP-osoitteesta sekä kohdeportista. "Kind"-objektin avulla voidaan myös hyödyntää portinohjausta ja IP:n uudelleenohjausta kohti Home-palvelinta. (Herrala, 2017.)

Ping-viestin onnistuneen läpimenon jälkeen saadaan tarkempia tietoja, kuten Beaconin nimi, joka onnistui paossa, lähde- ja kohdeosoite, mahdollinen pako-osoite, portti tai protokollanumero, verkkohyppyjen määrä (hop count) sekä tieto siitä, onko vuoto ollut yksisuuntainen vai

kaksisuuntainen. Yksisuuntaisessa vuodossa vuoto tapahtuu vain eristetyistä verkoista ulospäin, kun taas kaksisuuntainen vuoto tarkoittaa vuotoa, joka tapahtuu sekä eristetyistä verkoista ulos että takaisin sisään. (Herrala, 2017.) Tämä tekniikka mahdollistaa tehokkaan reitityksen ja verkon suojaamisen, samalla kun voidaan tarkasti monitoroida ja hallita verkon liikennettä eristettyjen verkkojen ja Home-palvelimen välillä.

8 TYÖN TOTEUTUS

Työn tavoitteena on toteuttaa Beaconin käyttöönoton demonstrointi ja sen toiminnan testaamisen kahdessa eri Hitachin järjestelmässä. Tässä työssä hyödynnetään sekä virtuaalista että Windows-sovellusversiota laitteesta ja tavoitteena on tutkia, millaisia hälytyksiä Beaconin avulla saadaan järjestelmistä. Työ etenee seuraavassa järjestyksessä: ensin suoritetaan käyttöönotto, jonka jälkeen tarkastellaan järjestelmän tuottamia tietoja ja analysoidaan saatuja tuloksia.

Raportin tavoitteena on tarjota selkeä ja helposti ymmärrettävä katsaus verkon haavoittuvuuksiin ja turvallisuustilanteeseen. Tavoitteena on luoda kuva verkon heikkouksista ja tarjota käytännön ratkaisuja, jotka tukevat verkon turvallisuutta ja ylläpitoa. Raportti on suunnattu sekä yrityksen sisäiseen käyttöön että asiakkaille, jotka voivat hyödyntää sitä verkon turvallisuustilanteen arvioinnissa ilman teknistä asiantuntemusta.

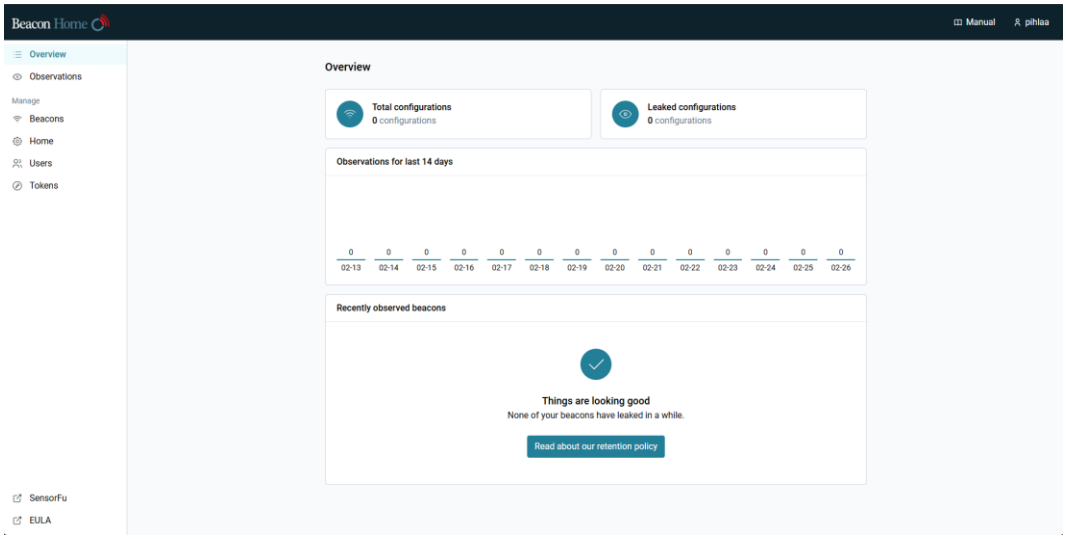
Työn lopputuloksena saadaan kokonaiskuva Beaconin toiminnasta Hitachin ympäristöissä ja pystytään arvioimaan sen tuottaman tiedon merkitystä järjestelmien turvallisuuden parantamisessa. Raportti tarjoaa konkreettista tietoa verkon tilasta ja auttaa tunnistamaan, milloin verkko tarvitsee huomiota ja milloin tilanne on turvallinen. Tämä tukee päätöksentekoa ja mahdollistaa palveluiden laajentamisen, kuten jatkuvan verkonvalvonnan ja räätälöityjen ratkaisujen tarjoamisen.

Raportin toteutus perustuu Beaconin tuottamien havaintojen analysointiin ja visualisointiin Excelin sekä Power BI -työkalujen avulla. Näin saadaan luotua helposti luettava ja ymmärrettävä raportti, joka selkeyttää verkon turvallisuustilannetta. Tämä parantaa raportin saavutettavuutta ja käyttökelpoisuutta eri sidosryhmille, sillä Power BIn avulla voidaan yhdistää eri datalähteet ja luoda visuaalisia esityksiä, jotka selkeyttävät verkon tilan kokonaiskuvaa.

8.1 Beaconin käyttöönotto ja konfigurointi

Beacon konfiguroidaan ja otetaan käyttöön kirjautumalla Beacon Home -palvelimelle, joka toimii keskitettynä hallintaympäristönä. Tässä ympäristössä luodaan ja hallitaan Beacon-laitteita ja seurataan eristetyssä järjestelmässä havaittuja hälytyksiä, joita Beacon tuottaa.

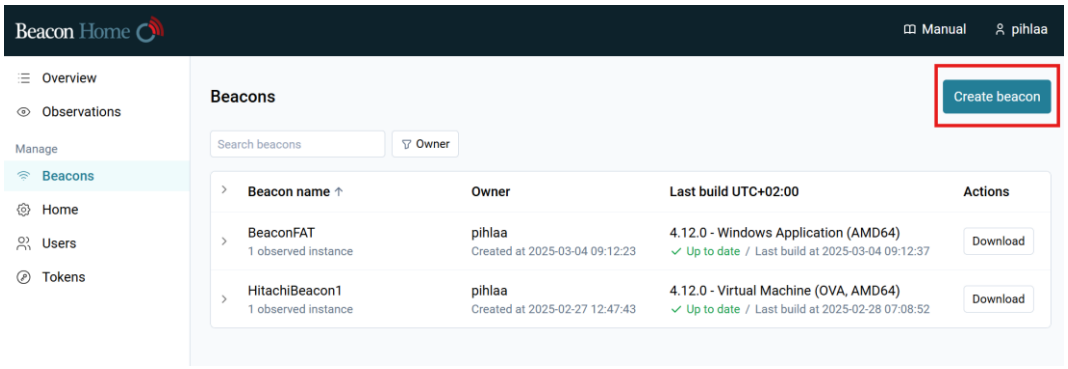
Kuvassa 6 on Beacon Home, joka voidaan sijoittaa joko julkiseen verkkoon tai erilliseen suljettuun ympäristöön organisaation turvallisuus- ja hallintatarpeiden mukaan.



Kuva 6. Beacon Home -palvelin.

8.1.1 Beaconin luonti

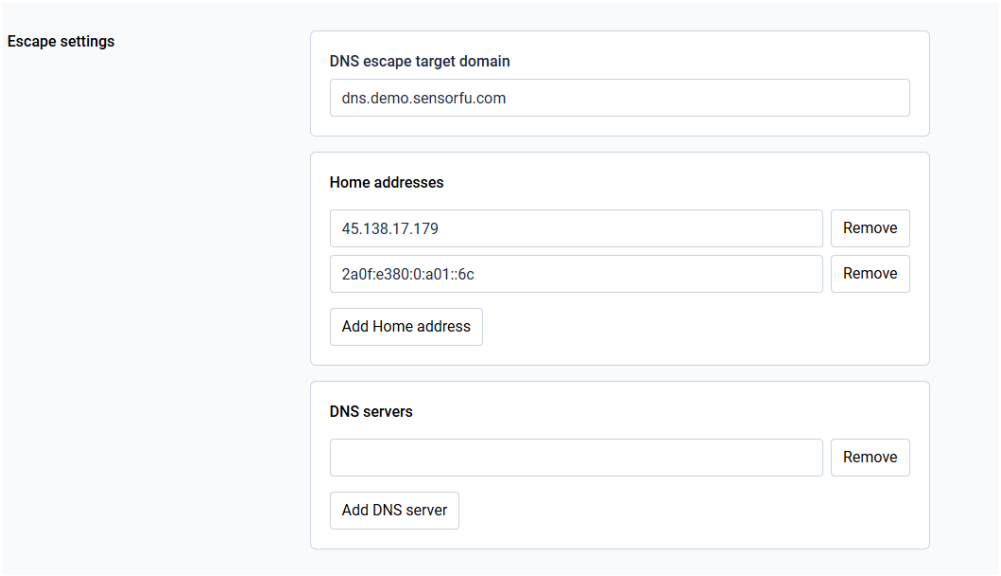
Työssä Beaconin asennusta ja toimintaa on testattu SensorFun demo-ympäristössä, jossa Home-palvelin sijaitsee julkisessa verkossa. Uusi Beacon luodaan avaamalla Beacon-välilehti ja valitsemalla sieltä "Create Beacon" -kohta (Kuva 7). Beaconille annetaan selkeä nimi, jotta se on helposti tunnistettavissa ja sen jälkeen valitaan sopiva ympäristö pudotusvalikosta, johon laite asennetaan (Kuva 8).



Kuva 7. Uuden Beaconin lisääminen.

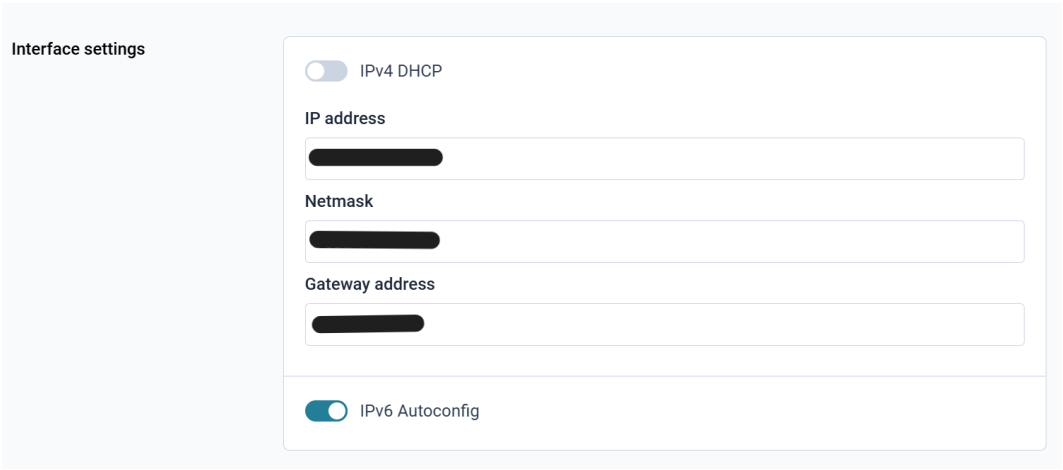
Kuva 8. Beaconin nimeäminen ja version valitseminen.

Beaconille asetetaan kohdeverkkotunnus, jota kohti se pyrkii tekemään pakoyrityksiä eristetystä ympäristöstä. Pakoasetuksissa Home-osoite on oletuksena määritetty, joten sitä ei tarvitse lisätä tai muuttaa (Kuva 9).



Kuva 9. Beaconin pakoasetukset.

Beaconille määriteltävät verkkoasetukset riippuvat valitusta ympäristöstä. Työssä loimme sekä virtuaali- että sovellusversion Beaconista, joten verkkoasetukset poikkeavat toisistaan. Virtuaalikoneversiossa voidaan käyttää DHCP:tä tai määritellä verkkoasetukset manuaalisesti, jolloin lisätään IP-osoite, aliverkon maski (Netmask), yhdyskäytävän tiedot (Kuva 10). Sovellusversiossa Beaconille riittää vain DNS-osoitteiden lisääminen, mutta niitä ei ole pakollista määrittää. DHCP-asetuksia voi käyttää ainoastaan virtuaalikoneversiossa.

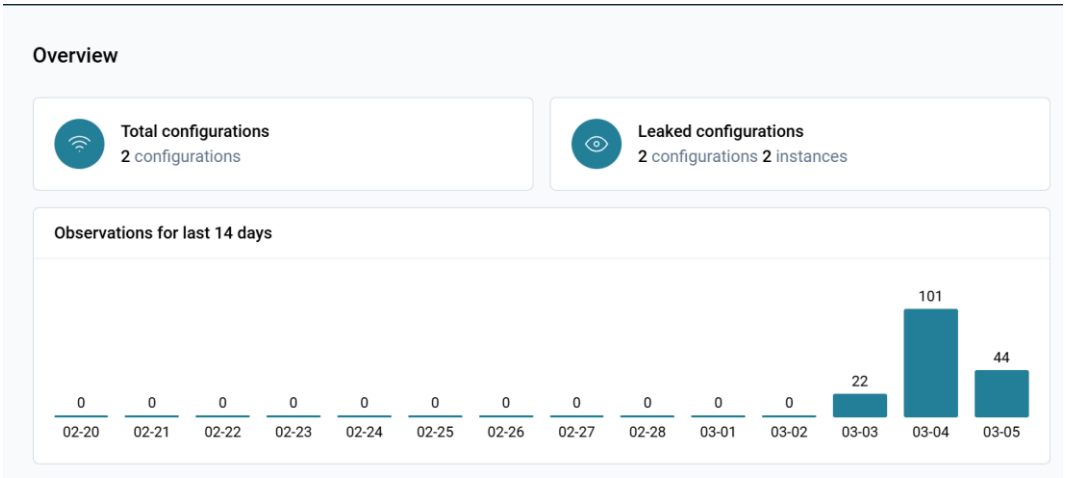


Kuva 10. Beaconin verkkoasetukset.

Asetusten määrittämisen jälkeen Beacon on valmis ladattavaksi ja se ladataan "Downloads"-kohdasta ja siirretään haluttuun eristettyyn ympäristöön. Beaconin asennettua kohdeympäristöön se alkaa automaattisesti etsiä pakoreittiä jatkuvasti kohti Home-komponenttia hyödyntäen asennusvaiheessa määriteltyjä asetuksia.

8.1.2 Hälytysten tarkastelu

Onnistuneiden pakojen määrää ja kokonaisuus esitetään Home-palvelimen etusivulla (Kuva 11). Kun Beacon löytää pakoreitin, se ilmestyy "Observation"-välilehdelle Home-palvelimelle (Kuva 12). Tässä voidaan tarkastella hälytyksiä, löytyneitä vuotokohtia sekä pakomenetelmän tietoja tarkemmin (Kuva 13). Pakomenetelmistä saa lisää tietoa, kuten mahdollisia syitä verkon heikkoudelle ja korjausehdotuksia, klikkaamalla kyseistä pakomenetelmää (Kuva 14).



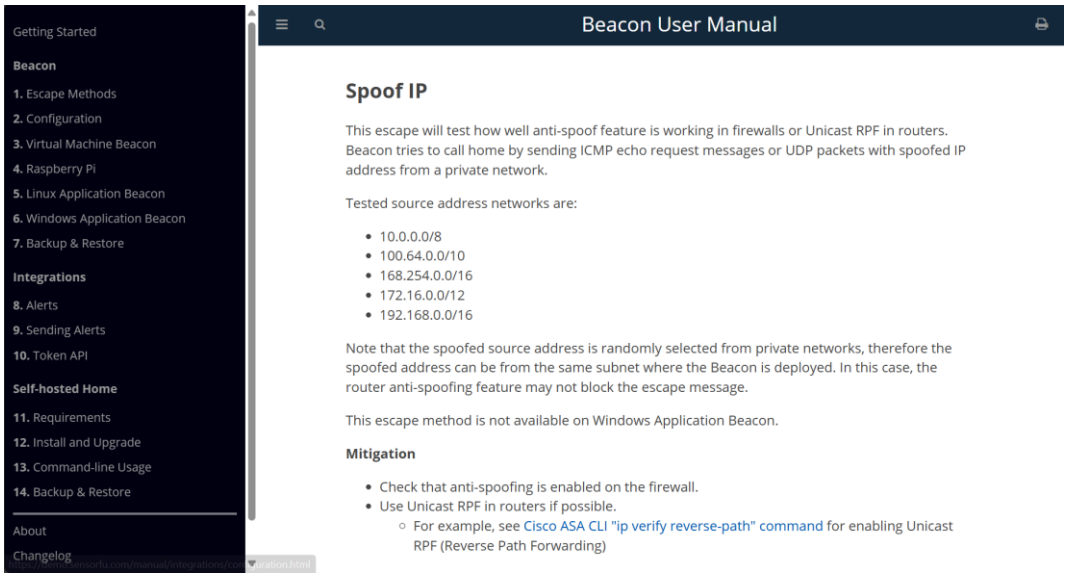
Kuva 11. Hälytykset Home palvelimessa.

Kuva 12. Beacon observations.

Observation details

TIMESTAMP	2025-03-07 10:13:13 UTC+02:00
BEACON NAME	HitachiBeacon1
FROM	
TO	45.138.17.179
ESCAPE	SpoofIp
TRANSPORT	Icmp4
PORT	-
ALERT ID	9af819b09189870a
BEACON ADDRESS	[redacted]
BEACON PLATFORM	Virtual Machine (OVA, AMD64)
BIDIRECTIONAL	-
DUPLICATES	0
HOME NAME	home
NAT	-

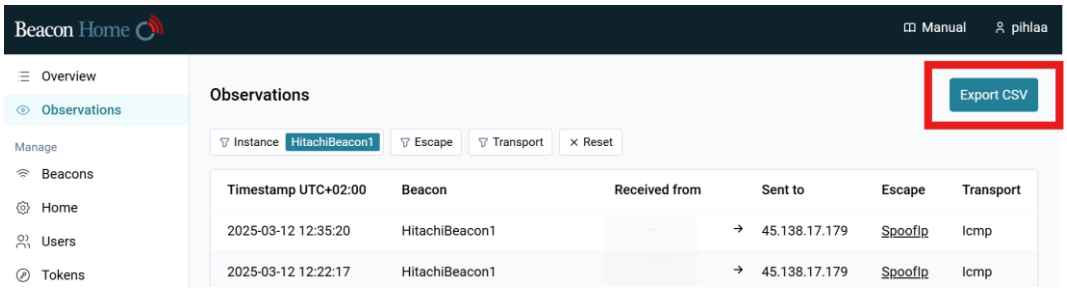
Kuva 13. Observations details.



Kuva 14. Tiedot pakomenetelmistä.

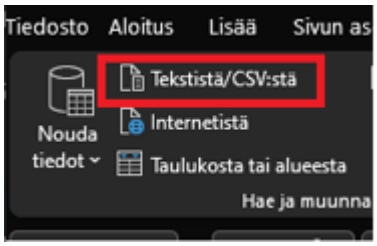
8.2 Havaintojen siirtäminen analysointityökaluun

Beaconin Home-palvelimelta saadut havainnot voidaan ladata CSV-tiedostona (Kuva 15). Tiedot tulee ensin siirtää ja muokata Excelissä, jotta ne ovat yhteensopivia ja helposti käsiteltäviä. Tämän jälkeen tiedot voidaan siirtää Power BI -työkaluun analysointia varten.



Kuva 15. Havaintojen lataaminen CSV-tiedostoksi.

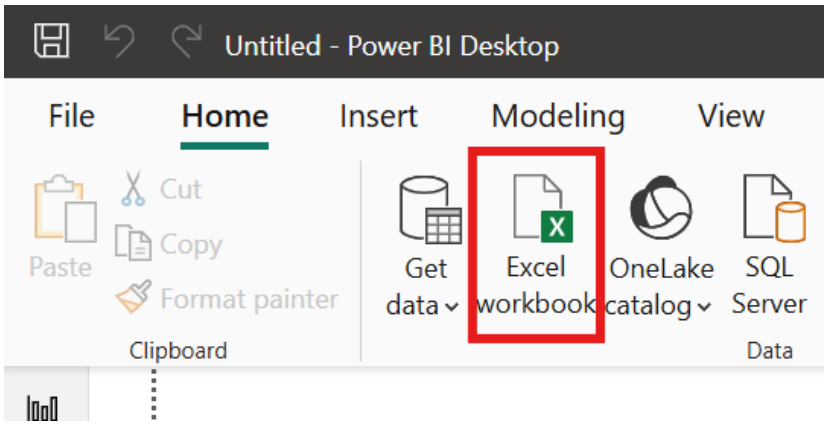
Kuvassa 16 näkyy, kuinka Excel-työkalussa CSV tiedosto voidaan ladata Data-välilehdeltä ja valita sieltä ”Tekstistä/CSV:stä” vaihtoehto. Tämä muokkaa ladatun CSV-tiedoston Excelin tukemaan muotoon.



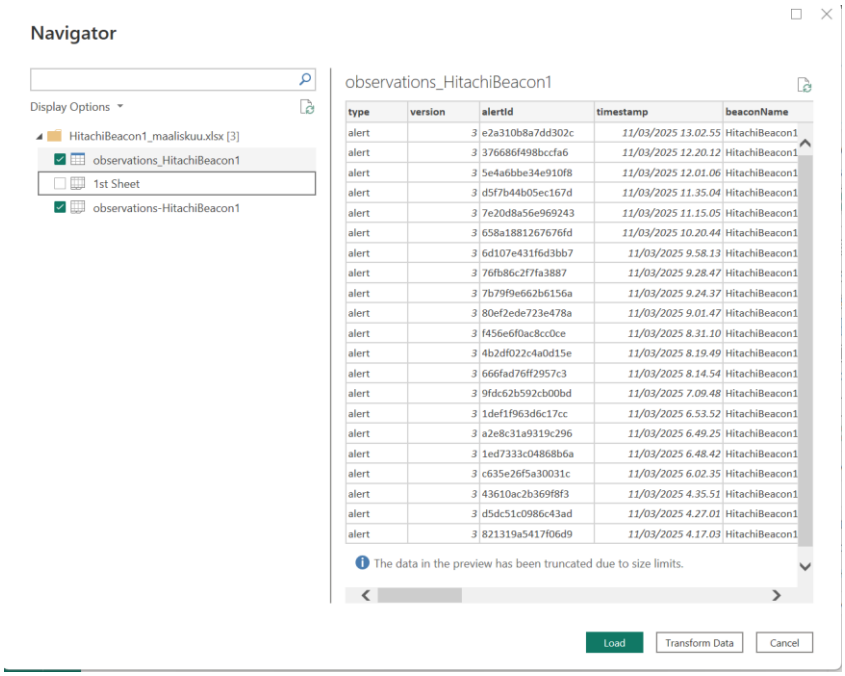
Kuva 16. CSV-tietojen lataaminen Excel työkaluun.

Power BI -työkalussa aiemmin luotu Excel-tiedosto voidaan ladata valitsemalla ”Excel workbook” (kuva 17). Tämän jälkeen voidaan valita,

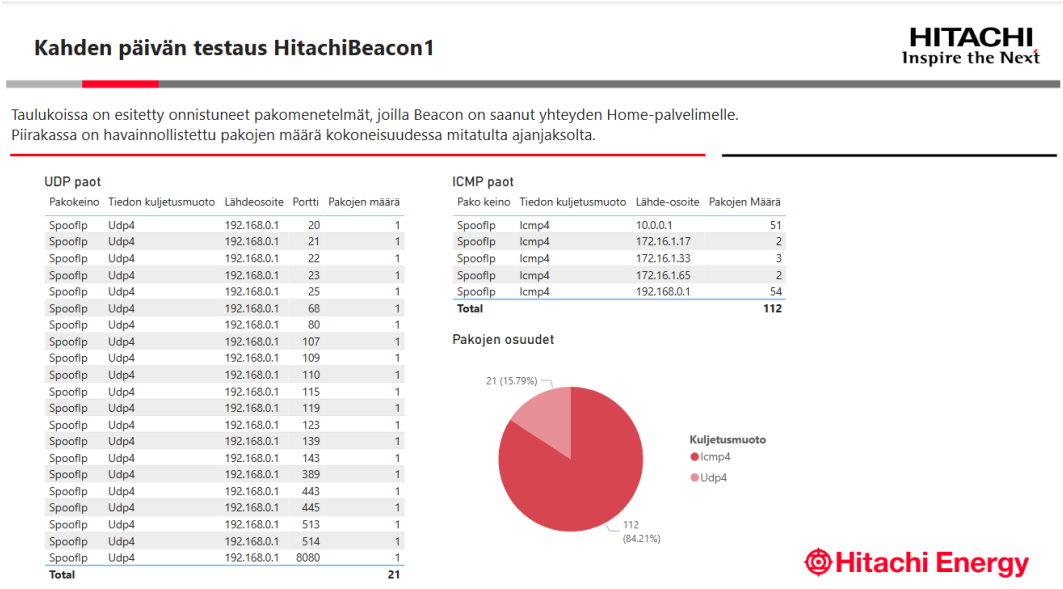
mitkä havainnot halutaan tuoda Power BI -työkaluun (kuva 18). Ladatuista havainnoista voidaan alkaa visualisoimaan tietoa halutulla tavalla. Kuvassa 19 näkyy testausjakson havainnoista luotu raportti Power BIn avulla.



Kuva 17. Excel tiedoston lisääminen Power BI -työkaluun.



Kuva 18. Ladattavat havainnot.



Kuva 19. Power BIllä luotu visualisointi havainnoista.

9 TESTAUS

9.1 Tavoitteet ja menetelmät

Testaus toteutetaan useilla aikaväleillä, jotta voidaan vertailla Beacon -laitteen antamia tuloksia eri vaiheissa testausta. Tuloksia kerätään kolme kertaa testauksen aikana: ensimmäinen tulosten keräys toteutetaan kahden päivän kuluttua testauksen käynnistämisestä, toinen mittaus tehdään noin viikon kuluttua ja kolmas tulos kerätään kahden viikon jälkeen, jolloin laite on ollut käynnissä koko testijakson ajan.

Testauksessa käydään läpi onnistuneita pakokeinoja, joita Beacon on onnistunut tekemään verkoista, joihin se on asennettu. Testauksessa käydään myös läpi, miten ne vaikuttavat verkon turvallisuuteen ja kuinka hyökkääjät pystyvät hyödyntämään kyseistä tapaa sekä kuinka tavalta voidaan suojautua. Havainnot siirretään sekä Excel- että Power BI-työkaluun, jotta niitä olisi helpompi hallita ja niistä voisi tehdä visuaalisempia havaintoja.

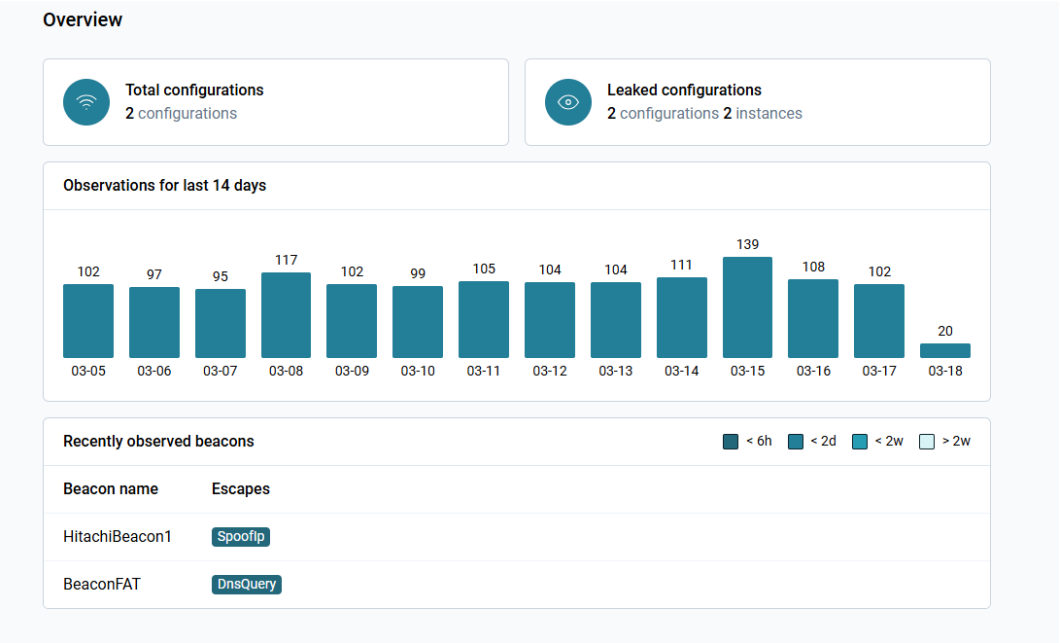
Testattaviksi Beaconeiksi luotiin virtuaalikone sekä Windows-sovellus, jotka asennettiin eri järjestelmiin. Testauksessa tutkimme näiden Beaconien antamia tietoja järjestelmistä kahden viikon ajan. Molemmat Beaconit pyrkivät tekemään pakoja samaa Home-osoitetta kohti.

9.2 Analyysi testauksista

Järjestelmien, joihin Beaconit yhdistettiin, olisi pitänyt olla täysin eristettyjä, mutta kuten Traficomin (2020) tuottamassa tutkimuksessa oli tullut esille, vaikka järjestelmä vaikuttaisi olevan täysin suojattu eikä tietovuodoille näyttäisi olevan mahdollisuuksia, yllättäviä haavoittuvuuksia voi silti esiintyä. Beaconien avulla pystyttiin tunnistamaan järjestelmistä heikkoja kohtia, jotka olisivat muuten jääneet huomaamatta. Näiden haavoittuvuuksien paljastuminen mahdollistaa järjestelmien suojaustason parantamisen ja auttaa ehkäisemään mahdollisia tietoturvauhkia.

Kuvasta 20 käy ilmi pakojen jakautuminen testausjakson aikana ja voidaan havaita, että pakojen määrä on ollut suhteellisen tasainen kahden viikon ajan. Kuitenkin on päiviä, jolloin pakoja on ilmennyt merkittävästi enemmän kuin muina päivinä.

Testauksissa saadut tulokset on koottu taulukoihin, jotka on esitetty työn liitteissä. Virtuaalikone Beaconin tulokset löytyvät liitteistä 1, 2, 5, 6, 9, 10 ja 11. Windows Beaconin tulokset on esitetty liitteissä 3, 4, 7, 8, 12 ja 13.



Kuva 20. Observations testauksen lopussa.

9.3 Virtuaalikone Beaconin havainnot

9.3.1 SpoofIP

Beaconilla onnistui pakokeinona SpoofIP eli IP-osoitteiden väärentäminen. Tämä on hyökkäystekniikka, jossa hyökkääjä manipuloi verkkoviestien lähde-IP-osoitetta niin, että se näyttää tulevan luotettavasta lähteestä (Kirvan, 2023). Beacon testaa pakokeinossa, kuinka tehokkaasti antispoofing-ominaisuudet toimivat palomuureissa ja reitittimissä sekä kuinka hyvin ne pystyivät havaitsemaan ja estämään väärennetyt paketit, jotka näyttivät tulevan luotettavasta lähteestä. Testissä Beacon pyrki saada yhteyden Home-osoitteeseen lähettämällä ICMP Echo -viestejä ja UDP-paketteja, joissa lähde-IP-osoite oli väärennetty yksityisestä verkosta. (Escape methods, n.d.-a.)

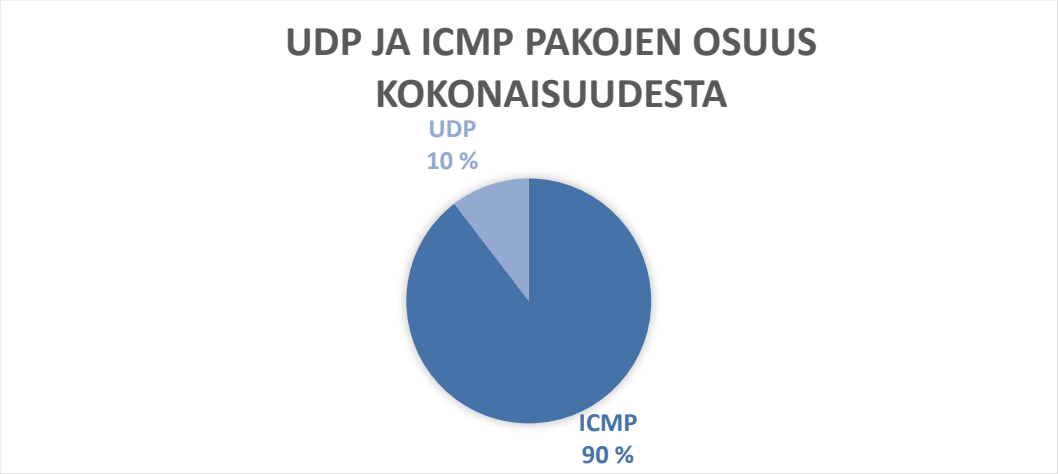
IP-osoitteiden väärentämisen avulla hyökkääjä voi päästä verkkoihin, jotka luottavat tietyistä IP-osoitteista saapuvaan liikenteeseen, ohittaen näin suojausmekanismeja. IP-spoofingia käytetään erityisesti hajautetuissa palvelunestohyökkäyksissä (DDoS), joissa hyökkääjä lähettää

suuren määrän väärennettyjä paketteja eri lähteistä, mikä kuormittaa kohdejärjestelmän resursseja ja estää sen normaalin toiminnan. Vaikka IP-spoofing ei aina suoraan aiheuta haittaa, se luo vakavia turvallisuusriskejä, sillä sitä voidaan käyttää muiden haitallisten toimintojen, kuten tietomurtojen tai palvelunestohyökkäysten mahdollistamiseksi. (Kirvan, 2023.)

IP-spoofing-hyökkäysten torjumiseksi on tärkeää ottaa käyttöön tehokkaita antispoofing-toimenpiteitä. Näitä toimenpiteitä voivat olla esimerkiksi verkkopaketin aitouden tarkistaminen, IP-osoitteiden validointi ja asianmukaiset säännöt verkkoyhdyskäytävissä, kuten palomuureissa ja reitittimissä. (Escape methods, n.d.-a.) Yksi keskeinen torjuntakeino on ingress-suodatus, joka estää paketteja, joiden lähde-IP-osoite ei vastaa odotettuja sääntöjä (VPN unlimited, n.d.-c). IP-spoofing-hyökkäysten estämiseksi verkon suojausmekanismien, kuten palomuurien ja IP-osoitteiden validoinnin, on oltava kunnolla määriteltyjä ja ajan tasalla. Näiden mekanismien avulla voidaan estää epäluotettavien lähteiden liikenne, mikä parantaa verkon turvallisuutta ja suojaa organisaatioita sekä käyttäjiä mahdollisilta kyberhyökkäyksiltä. Tämänkaltaisten toimenpiteiden avulla voidaan minimoida IP-spoofingin aiheuttamat riskit ja varmistaa verkon luotettavuus ja eheys. (Kirvan, 2023.)

9.3.2 Analyysi testausjakson tuloksista

Beaconin virtuaalikoneen testauksen aikana havaittiin yhteensä 808 pakoa, joista 90 % oli ICMP echo -paketeilla onnistuneita (Kuvio 1). Pakoja tapahtui jatkuvasti eri lähdeosoitteista, mutta niiden määrissä oli huomattavia eroja. Taulukosta 2 käy ilmi, että tietyistä lähdeosoitteista tapahtui merkittävästi enemmän pakoja kuin muista. Erityisesti osoitteet 192.168.0.1 ja 10.0.0.1 erottuivat selvästi korkeilla pakojen määrillä, mikä voi johtua niiden kuuluvuudesta nopeaan testausjaksoon. Nopean syklin aikana testaus keskittyy tyypillisesti näkyvämpiin haavoittuvuuksiin ja tunnettuihin pakopaikkoihin, jolloin tietyt osoitteet saavat enemmän huomiota ja kokevat enemmän pakoja kuin muut.



Kuvio 1. UDP- ja ICMP-pakojen osuus testauksesta.

Taulukko 2. Pakojen määrä testausten aikana, virtuaalikone Beacon.

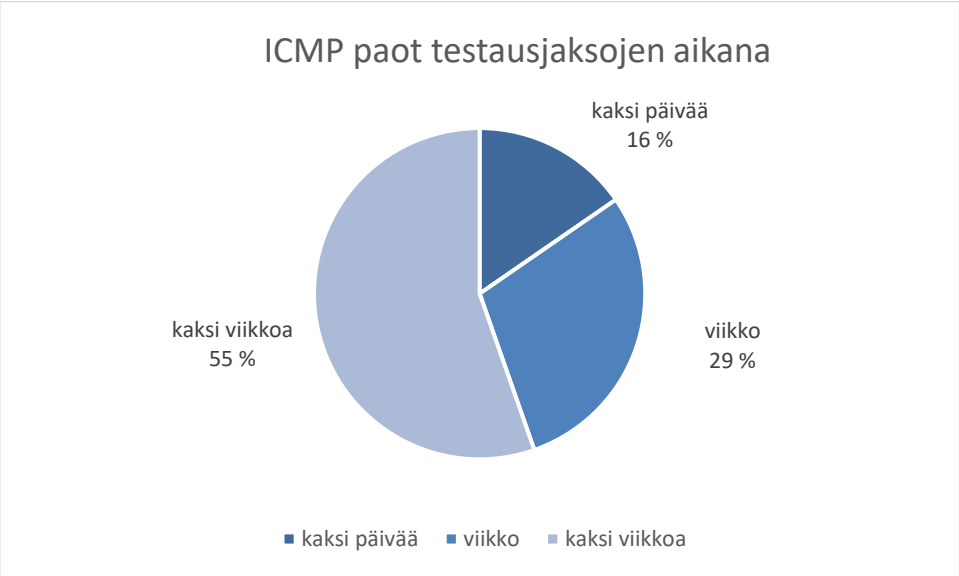
Lähdeosoite	ICMP	UDP	Yhteensä
10.0.0.1	336	21	357
172.16.1.17	18	0	18
172.16.1.33	12	0	12
172.16.1.65	11	0	11
192.168.0.1	347	63	410

Taulukossa 2 käy ilmi, kuinka ICMP-pakoja onnistui erityisesti 10.0.0.1 ja 192.168.0.1-osoitteista, kun taas UDP-pakoja päästettiin läpi ainoastaan näistä kahdesta osoitteesta. Tämä viittaa siihen, että testauksen alussa UDP-portit olivat enemmän rajoitettuja, mutta myöhemmin testausjaksojen edetessä myös muut lähdeosoitteet alkoivat onnistua UDP-paoissa. Erityisesti kolmannen testausjakson aikana molempien pakokeinojen osuudet kasvoivat merkittävästi. Taulukossa 3 näkyy, kuinka testausjakojen aikana pakojen määrät kokonaisuudessa nousevat huomattavasti.

Taulukko 3. Pakojen määrät testausten aikana, virtuaalikone Beacon.

Testaus ajanjakso	Pakojen määrä
Ensimmäinen	133
Toinen	257
Kolmas	418

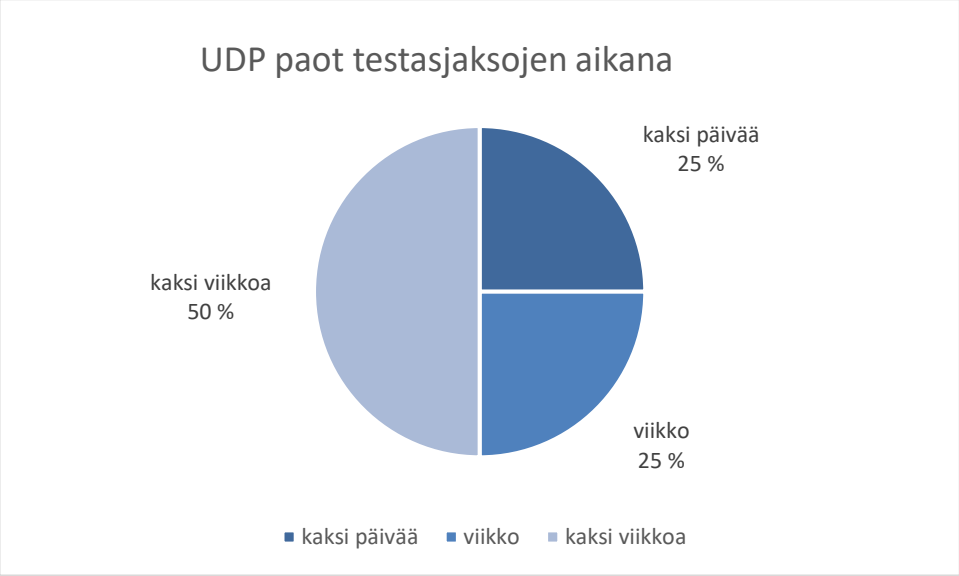
Kuviossa 3 esitetään ICMP-pakojen määrän kasvu erityisesti kolmannella testausjaksolla, jolloin suurin osa ICMP-pakoista tapahtui. Tämä saattaa viitata siihen, että kolmannen testausjakson aikana testattiin laajemmin verkon haavoittuvuuksia, mikä mahdollisti enemmän ICMP-pakettien läpipääsyn.



Kuvio 2. ICMP-paot.

Kuviossa 3 näkyy UDP-pakojen kasvu erityisesti kolmannella testausjaksolla. Aluksi vain tietyt lähdeosoitteet pääsivät läpi UDP-porttien kautta, mutta myöhemmin muista osoitteista tulevat pakot alkoivat myös onnistua. Tämä voi johtua siitä, että kolmannella testausjaksolla

testauksen tarkkuus kasvoi, jolloin havaittiin myös aiemmin piilossa olleita haavoittuvuuksia UDP-porttien osalta.



Kuvio 3. UDP-paot.

Beaconin testauksen aikana pakojen määrä kasvoi merkittävästi testauksen edetessä, erityisesti kolmannella testausjaksolla, joka oli laajin ja kattavin. Testauksen alkuvaiheessa ICMP-pakojen määrä oli huomattavasti suurempi, mutta myöhemmissä vaiheissa myös UDP-pakojen onnistumisprosentti kasvoi. Tietyt lähdeosoitteet, kuten 192.168.0.1 ja 10.0.0.1, olivat erityisen alttiita paon onnistumiselle, mikä saattaa johtua testauksen keskittymisestä nopean syklin aikana näihin osoitteisiin. Viimeinen testausjakso erottuu myös sillä, että molempia pakokeinoja, sekä ICMP että UDP, esiintyi eniten, mikä viittaa siihen, että hidas syklin tarkastelu mahdollisti syvempien haavoittuvuuksien havaitsemisen.

9.3.3 Porttien turvallisuus

Portit ovat tärkeitä verkkopalvelujen tunnistamiseen, ja niitä käytetään erottamaan erilaisia protokollia, sovelluksia ja palveluja toisistaan. Porttinumeroiden avulla verkko- ja sovellusprotokollat, kuten TCP ja UDP, ohjaavat liikennettä ja määrittelevät, mihin palveluun tietovirrat ohjautuvat. Avoimet portit voivat kuitenkin muodostaa vakavan riskin, jos niitä ei suojata riittävästi, sillä ne tarjoavat mahdollisuuden hakkerointiin ja kyberhyökkäyksiin. (Murphy, 2024.)

Vaikka avoimet portit eivät ole itsessään vaarallisia, mutta niitä voi hyödyntää uhkatoimijat, jotka voivat käynnistää erilaisia hyökkäyksiä, kuten spoofing-hyökkäyksiä, DDoS-hyökkäyksiä tai sovelluskerroksen hyökkäyksiä, kuten SQL-injektioita. Näillä hyökkäyksillä voidaan saada luvaton pääsy järjestelmiin, häiritä palvelun toimintaa tai varastaa arkaluontoisia tietoja. Portteja, jotka eivät ole riittävästi suojattuja, voidaan käyttää myös man-in-the-middle-hyökkäyksissä, joissa hyökkääjä voi kaapata yhteyksiä ja manipuloida tietoja. (Murphy, 2024.)

Tietyt portit ovat alttiimpia kyberhyökkäyksille, erityisesti ne, jotka liittyvät heikkoihin sovelluksiin tai joissa ei ole asianmukaisia suojausmekanismeja, kuten kaksivaiheista tunnistautumista. Taulukossa 4 esitetään portit, jotka ovat erityisen haavoittuvia ja joiden riski altistumiselle johtuu puutteista, kuten sovellushaavoittuvuuksista tai heikoista tunnistetiedoista. (Murphy, 2024.)

Taulukko 4. Haavoittumiselle altteimmat UDP-portit (Murphy, 2024).

Portti	Protokolla	Haavoittuvuus
20 ja 21	FTP	Epävarma, altis brute-force-hyökkäyksille, anonyymille autentikoinnille, cross-site scriptingille ja hakemistojen läpikäynnille.
53	DNS	Altis DDoS-hyökkäyksille.
22	SSH	Altis brute-force-hyökkäyksille ja vuotaneille SSH-avaimille.
80, 443, 8080 ja 8443	HTTP JA HTTPS	Altis cross-site scriptingille, SQL-injektioille, cross-site pyyntöväärentäminen ja DDoS-hyökkäyksille.
23	Telnet	Vanhentunut, altis brute-forcingille, spoofingille ja sniffingille.
25	SMTP	Altis spoofingille ja roskapostille.
3389	Etätyöpöytä	Altis etätyöpöytäprotokollien haavoittuvuuksille ja heikolle käyttäjäautentikoinnille.
137, 139 ja 445	NetBIOS TCP:n päällä ja SMB	Altis NTLM-hashien kaappaukselle ja SMB-kirjautumistietojen brute-forcingille.
1433, 1434 ja 3306	Tietokannat	Altis haittaohjelmien levittämiselle ja DDoS-hyökkäyksille.

9.4 Windows Beacon-havainnot

9.4.1 DNSQuery

Beaconin Windows-sovelluksessa DNSQuery-menetelmä toimi onnistuneena pakokeinona. Beacon käytti DNS-peitekanavaa tiedonsalakuljetukseen, jotta se pystyi muodostamaan yhteyden Home-osoitteeseen verkon turvatoimien ohitse. Tämä tapahtuu lähettämällä kyselyitä DNS-palvelimelle, joka yrittää ratkaista ne internetistä ja lopulta Home-osoitteen DNS-palvelimesta. DNS-pakotekniikka hyödyntää sekä DHCP:n tarjoamia DNS-palvelimia, että käyttöjärjestelmän määrityksistä saatuja DNS-palvelimia. Lisäksi Beacon yrittää käyttää avoimia julkisia DNS-palvelimia, kuten Google, Quad9, Cisco Umbrella ja Cloudflare. Se voi myös hyödyntää pilvipalveluntarjoajien metatieto palvelimia, kuten IP-osoitteita 169.254.169.253 ja 169.254.169.254, jotka löytyvät monilta pilvialustoilta. (Escape methods, n.d.-a.)

DNS (Domain Name System) on internetin standardiprotokollan osa, joka mahdollistaa verkkotunnusten kääntämisen IP-osoitteiksi (China & Goodwin, 2024). Kuitenkin tämä järjestelmä voi olla myös houkutteleva väline kyberhyökkäyksille, koska sen liikenne on usein valvomatta ja on välttämätön verkon toiminnan kannalta.

DNS:tä voidaan hyödyntää peitekanavana, jonka avulla hyökkääjät voivat salakuljettaa tietoa verkon turvamekanismien ohi. Peitekanava on tekniikka, jossa tiedonsiirto tapahtuu huomaamatta, usein estäen sen havaitsemisen palomuureilla tai muilla turvatoimilla. DNS-peitekanavassa hyökkääjät manipuloivat DNS-pyyntöjä ja -vastauksia niin, että ne näyttävät tavallisilta verkkotunnuksen ratkaisupyynnöiltä, vaikka todellisuudessa ne voivat sisältää salaista tietoa, komentoja tai jopa haitallista koodia. (Piscitello, 2016.)

Yksi esimerkki tästä on DNS-kyselyiden käyttö, joissa voidaan hyödyntää erityisiä aliverkkotunnuksia tai tekstipohjaisia tietueita (TXT-tietueet). Näiden avulla voidaan kuljettaa tiedostoja, komentoja tai muuta

salaista tietoa, mikä tekee DNS:stä erityisen vaarallisen välineen hyökkääjille. (Piscitello, 2016.)

Verkon turvatoimien parantaminen edellyttää muun muassa eristettävien DNS-palvelimien käyttöä, lähtevän DNS-liikenteen rajoittamista sekä jatkuvaa valvontaa epäilyttävän liikenteen havaitsemiseksi (Escape methods, n.d.-a.). Näin voidaan estää DNS:n väärinkäyttö peitekanavaa hyödyntäen ja parantaa verkon turvallisuutta.

9.4.2 Analyysi testausjaksojen paoista

Testauksen aikana havaittiin, että pakoja tapahtui yhteensä 585 kappaletta eri osoitteita hyödyntäen. Pakoja tehtiin sekä IPv4- että IPv6-osoitteilla, ja molemmilla protokollilla Beacon onnistui saamaan yhteyden Home-palvelimelle. Taulukossa 5 on esitetty pakojen määrä kussakin testausjaksossa.

Taulukko 5. Pakojen määrät testausten aikana, Windows Beacon.

Testaus ajanjakso	Pakojen määrä
Ensimmäinen	133
Toinen	254
Kolmas	357

Taulukossa 5 näkyy pakojen määrän kasvu testausjaksojen aikana. Ensimmäisellä testausjaksolla pakoja tapahtui 133 kappaletta, toisella testausjaksolla määrä nousi huomattavasti 254:ään, ja kolmannella testausjaksolla pakojen määrä oli 357. Tämä kertoo siitä, että testausjaksojen aikana pakojen määrä on jatkuvasti lisääntynyt. Kuviossa 4 esitetään pakojen jakautuminen prosenttiosuuksina testausjaksoille.

Kuvio 4. Pakojen osuudet testausjaksojen aikana.

Kuvio 4 havainnollistaa, kuinka suurin osa paoista tapahtui kolmannella testausjaksolla. Tässä vaiheessa lähes 50 % kaikista testauksen aikana tapahtuneista paoista keskittyi juuri tähän jaksoon. Tämä trendi on merkittävä, sillä se osoittaa, että pakojen määrä kasvoi huomattavasti testauksen edetessä.

Erityisesti viimeinen testausjakso erottuu selkeästi. Kolmannella jaksolla, jossa pakojen määrä oli 357, tapahtui lähes puolet kaikista pakoista testauksen aikana. Tämä viittaa siihen, että joko hyökkäyspaine oli suurimmillaan juuri tässä vaiheessa tai että testauksen olosuhteet muuttuivat jollain tavalla suotuisiksi pakojen tapahtumiselle.

Koko testauksen aikana pakojen määrä kasvoi merkittävästi, ja erityisesti kolmas testausjakso erottui selkeästi suurella prosenttiosuudella. Tämä voidaan nähdä sekä taulukosta nro että kuviossa nro, jotka tukevat toisiaan. Kolmannessa jaksossa tapahtui lähes puolet kaikista paoista, mikä viittaa siihen, että testauksen olosuhteet muuttuivat suotuisammiksi pakojen tapahtumiselle.

10 JOHTOPÄÄTÖKSET

Tämän työn tarkoituksena oli tutustua SensorFun kehittämään Beacon-tuotteeseen ja arvioida sen käyttöä Hitachin järjestelmissä, erityisesti palveluliiketoiminnan näkökulmasta. Beaconin käyttöönoton helppous, toiminnallisuus ja hyödyllisyys osoittautuivat tärkeiksi tekijöiksi laitteiden ylläpidon ja verkon turvallisuuden hallinnan parantamisessa.

Beacon on suunniteltu yksinkertaiseksi ja vaivattomaksi integroida osaksi asiakasympäristöä. Sen nopea käyttöönotto ja helppokäyttöisyys ilman lisäkoulutustarvetta tekevät siitä kustannustehokkaan ratkaisun organisaatioille, jotka haluavat varmistaa verkkojensa turvallisuuden. Sen jatkuva verkon tarkkailu ja kyky havaita vuotoja eristetyissä verkoissa ovat tärkeitä ominaisuuksia, jotka parantavat kyberturvallisuutta erityisesti kasvavassa digitaalisten ratkaisujen maailmassa. Kyberhyökkäysten lisääntyessä Beaconin tarjoama ennakoiva lähestymistapa verkon eheydelle tulee olemaan yhä keskeisempi.

Erityisesti NIS2-direktiivi, joka asettaa tiukempia kyberturvallisuusvaatimuksia kriittisille infrastruktuureille ja digitaalisille palveluille, tuo esiin entistä suuremman tarpeen varmistaa verkkojen turvallisuuden. Direktiivi edellyttää, että organisaatiot tekevät tarvittavia toimenpiteitä kyberturvallisuuden varmistamiseksi, mukaan lukien jatkuva riskienhallinta ja haavoittuvuuksien hallinta. Beaconin avulla organisaatiot voivat vastata näihin vaatimuksiin tehokkaasti. Laitteen kyky havaita verkon haavoittuvuuksia sekä mahdollisia tietoturvariskejä tukee NIS2-direktiivin asettamia vaatimuksia verkkojen ja tietojärjestelmien suojaamiseksi.

Erityisesti palveluliiketoiminnan näkökulmasta Beaconin tarjoamat hyödyt ovat merkittäviä. Laitteen kyky tunnistaa ja raportoida haavoittuvuuksia ennen kuin ne voivat aiheuttaa laajempia ongelmia tai kyberhyökkäyksiä, säästää aikaa ja resursseja. Tämä proaktiivinen lähes-

tymistapa auttaa estämään mahdollisia toimintahäiriöitä ja alentaa ylläpitokustannuksia. Tällöin asiakastyytyväisyys paranee, kun asiakkaat voivat luottaa laitteidensa luotettavuuteen ja kestävyyteen.

Laitteen tuottamat havainnot voidaan helposti visualisoida Power BI -työkalun avulla, mikä parantaa palveluprosessien seurantaa ja mahdollistaa nopeasti reagoimisen verkon haavoittuvuuksiin. Tämä raportointi- ja seurantakyky tekee Beaconista arvokkaan työkalun organisaatioille, jotka haluavat parantaa verkkojensa turvallisuutta ja optimoida laitteidensa elinkaarta.

Yhteenvetona voidaan todeta, että Beacon tarjoaa merkittävää lisäarvoa palveluliiketoiminnan kontekstissa. Sen kyky tunnistaa verkon haavoittuvuuksia, helppo käyttöönotto sekä yhdistäminen raportointi- ja seurantatyökaluihin tekevät siitä erinomaisen ratkaisun verkon turvallisuuden parantamiseen ja laitteiden huoltokustannusten optimointiin. NIS2-direktiivin myötä Beaconin avulla organisaatiot voivat täyttää tiukentuneet kyberturvallisuusvaatimukset ja varmistaa, että niiden verkot ja järjestelmät pysyvät suojattuina kasvavien uhkien maailmassa.

11 POHDINTA

Opinnäytetyön prosessi ja tulokset ovat antaneet syvällistä ymmärrystä verkkojen haavoittuvuuksien tunnistamisesta ja kyberturvallisuuden hallinnasta. Beacon Home -järjestelmän havainnoista saadut tiedot olivat luotettavia ja auttoivat selkeästi havainnollistamaan verkojen heikkouksia. Raporttiin sisällytettävien numeeristen havaintojen avulla tuloksia oli helpompi tulkita sekä visualisoida ja tämä teki raportista sekä lukijaystävällisemmän että informatiivisemman.

Tulokset tukevat teoriaa siitä, että verkkojen haavoittuvuuksien tunnistaminen on keskeinen osa kyberturvallisuuden hallintaa. Tämä korostaa sitä, kuinka tärkeää on jatkuvasti valvoa ja testata verkkojen eheyttä, sillä jopa pienet heikkoudet voivat johtaa vakaviin tietoturvaongelmiin. Testauksen aikana saatu tieto vahvisti sen, että proaktiivinen lähestymistapa verkkojen suojaamisessa on välttämätön, jotta haavoittuvuudet voidaan havaita ennen kuin ne voivat aiheuttaa laajempia ongelmia. Tämän työn avulla on tullut entistä selkeämmäksi, kuinka kyberturvallisuuden hallinta on dynaaminen prosessi, joka vaatii jatkuvaa seurantaa ja päivitystä.

Jatkotutkimusehdotukset avaavat mielenkiintoisia mahdollisuuksia Beaconin kehittämiseen ja sen käytön laajentamiseen. Hälytysten lähettäminen sähköpostiin ja niiden siirtäminen SIEM-järjestelmään ovat loogisia seuraavia askelia, sillä ne mahdollistaisivat paremman reagointikyvyn verkon turvallisuushäiriöihin. Näiden vaiheiden puuttuminen tässä vaiheessa ei vähennä Beaconin hyödyllisyyttä, mutta ne voisivat edelleen parantaa järjestelmän käytettävyyttä ja tehostaa sen tarjoamia ominaisuuksia.

Toinen kiinnostava ehdotus on tehdä Beaconista Raspberry Pi -laiteversio, joka tarjoaisi siirrettävän ja joustavan ratkaisun verkkojen testaamiseen. Tämä voisi laajentaa Beaconin käyttöä ja mahdollistaa sen käytön eri ympäristöissä, mikä puolestaan parantaisi sen joustavuutta ja

monipuolisuutta verkon turvallisuuden testaamisessa. Raspberry Pi -laitteen käyttö toisi myös kustannustehokkuutta ja helpottaisi laitteen laajempaa käyttöönottoa pienemmissä tai liikkuvissa ympäristöissä.

Opinnäytetyö on ollut itselleni erittäin opettavainen kokemus. Työ on antanut arvokasta tietoa siitä, kuinka tärkeää on valvoa ja testata verkkojen turvallisuutta jatkuvasti. Vaikka järjestelmä saattaa ulkoisesti vaikuttaa toimivalta, voi sen sisällä piillä haavoittuvuuksia, jotka voivat johtaa vakaviin tietoturvauhkiin. Tämä havainto korostaa kyberturvallisuuden jatkuvan kehittämisen merkitystä ja se on lisännyt tietoisuuttani siitä, kuinka suojauksia voidaan parantaa entisestään.

Testaaminen on tärkeä osa kyberturvallisuuden kehittämistä, ja opinnäytetyö on auttanut ymmärtämään paremmin, kuinka testausprosessi voi paljastaa piileviä heikkouksia, jotka muuten jäävät huomaamatta. Tämä kokemus on ollut arvokas, ja se on avannut silmiäni kyberturvallisuuden kehittämiselle käytännön tasolla. Työ on myös vahvistanut ymmärrystäni siitä, kuinka tärkeää on kehittää ja ottaa käyttöön uusia teknologioita, kuten Beaconin kaltaisia laitteita, kyberturvallisuuden parantamiseksi ja verkkojen suojaamiseksi entistä tehokkaammin.

Tässä opinnäytetyössä on hyödynnetty tekoälyntyökaluja ChatGPT:tä ja Microsoftin Copilotia erityisesti ideointivaiheessa sekä kielenasun ja selkeyttämisen tukena. Tekoälyä on käytetty apuna tekstin muokkaamisessa, jotta sisällöstä saatiin mahdollisimman ymmärrettävää ja helppolukuista. Kaikki tekoälyn avulla tuotettu tai muokattu sisältö on tarkastettu huolellisesti ja lopullinen vastuu sisällöstä on säilynyt tekijällä.

LÄHTEET

Advenica. (n.d.). Is your network isolation leaking? Noudettu 8.2.2025 osoitteesta https://advenica.com/learning-centre/blog/is-your-network-isolation-leaking/

Alanazi, Mahmood & Chowdhuty. (2023). Computers and security volume 125: SCADA vulnerabilities and attacks: a review of the state of the art and open issues. Noudettu 2.4.2025.

China ja Goodwin. (2024). What is DNS? Noudettu 5.4.2025 osoitteesta https://www.ibm.com/think/topics/dns

Cisco Press. (2014). Cisco networking academy's introduction to VLANs. Noudettu 14.3.2025 osoitteesta https://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=4

Ekqvist, Kiuru, Satopää & Vanharanta. (2024). Kyberturvallisuus. Noudettu 24.2.2025 osoitteesta https://finna.fi/L1Record/aoe.4419?sid=4940381333

Euroopan Komissio. (2025). NIS 2-direktiivi: verkko- ja tietojärjestelmien kyberturvallisuutta koskevat uudet säännöt. Noudettu 16.3.2025 osoitteesta https://digital-strategy.ec.europa.eu/fi/policies/nis2-directive

F-secure. (2022). Mikä on kyberhyökkäys. Noudettu 24.2.2025 osoitteesta https://www.f-secure.com/fi/articles/what-is-a-cyber-attack

Finder. (n.d.-a). Hitachi Energy yritystiedot. Noudettu 5.2.2025 osoitteesta https://www.finder.fi/S%C3%A4hk%C3%B6automaatio/Hitachi+Energy+Finland+Oy/Vaasa/yhteystiedot/3292326

Finder. (n.d.-b). SensorFu yritystiedot. Noudettu 6.2.2025 osoitteesta https://www.finder.fi/IT-konsultointi+IT-palvelut/SensorFu+Oy/Oulu/yhteystiedot/3159522

Hitachi Energy. (n.d.). Company profile. Noudettu 5.2.2025 osoitteesta https://www.hitachienergy.com/us/en/about-us/company-profile

Hitachi Energy. (n.d.). Perustietoja yhtiöstä Suomessa. Noudettu 5.2.2025 osoitteesta https://www.hitachienergy.com/about-us/company-profile/country-and-regional-information/finland/yhtiotietoja

Hedge. (2020). An introduction to Wireshark. Noudettu 21.3.2025 osoitteesta https://www.redhat.com/en/blog/introduction-wireshark

Heikkinen. (2021). Kriittiset tuotannon verkot usein hyökkäyksen kohteina. Noudettu 9.2.2025 osoitteesta https://www.loihde.com/ajankohtaista/blogi/kriittiset-tuotannon-ja-teollisuuden-verkot-ovat-jatkuvasti-hyokkayksen-kohteena

Herrala. (2017). The story about ping. Noudettu 9.3.2025 osoitteesta https://medium.com/sensorfu/the-story-about-ping-723dd71ac50b

Hänninen. (2021). Palveluliiketoiminnan disruptio. Noudettu 5.2.2025 osoitteesta https://www.vere.fi/blogi/palveluliiketoiminnan-disruptio

Irwin. (2023). Demystifying the CIA Triad: Why it's crucial for cyber security. Noudettu 24.2.2025 osoitteesta https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important

Jyväskylän yliopisto. (n.d.). Mitä on tietoturva? Noudettu 24.3.2025 osoitteesta https://www.jyu.fi/fi/yliopistopalvelut/digipalvelut/palvelut/tietoturva/mita-on-tietoturva

Jurvanen. (2025). Mikä on OT-verkko? Noudettu 9.2.2025 osoitteesta https://www.savelan.fi/mika-on-ot-verkko/

Jurvanen. (2023). Mikä on SCADA? Noudettu 9.4.2025 osoiteesta https://www.savelan.fi/mika-on-scada/

Järvinen. (2023). Turvallisuusjärjestelmien digitaalinen turvallisuus. noudettu 9.2.2025 osoitteesta https://www.finanssiala.fi/wp-content/uploads/2023/02/turvallisuusjarjestelmien-digitaalinen-turvallisuus_2023.pdf

Kirvan. (2023). Antispoofing. Noudettu 2.4.2025 osoitteesta https://www.techtarget.com/searchsecurity/definition/antispoofing

Kotipelto. (n.d.). Kyberturvallisuus osana kansallista turvallisuutta. noudettu 9.2.2025 osoitteesta https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus

Kothadi. (2025). What is network isolation & how does it work. Noudettu 19.2.2025 osoitteesta https://www.meter.com/resources/what-is-network-isolation

Luoma. (2014). NIS2- ja CER-direktiivit asettavat uusia vaatimuksia kyberturvallisuudelle ja kriittisten toimijoiden toimintavarmuudelle. Noudettu 2.3.2025 osoitteesta https://www.cgi.com/fi/fi/blogi/tietoturva-ja-kyberturvallisuus/nis2-ja-cer-direktiivit-asettavat-uusia-vaatimuksia?

McElfresh. (2016). Cyberattack on Ukraine grid: Here's how it worked and perhaps why it was done. Noudettu 6.4.2025 osoitteesta https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802

Microsoft. (n.d.). Mitä on kyberturvallisuus? Noudettu 10.2.2025 osoitteesta https://support.microsoft.com/fi-fi/topic/mit%C3%A4-kyberturvallisuus-on-8b6efd59-41ff-4743-87c8-0850a352a390

Nile. (n.d.). Network isolation: What it is & how it works for security. Noudettu 15.2.2025 osoitteesta https://nilesecure.com/network-security/network-isolation-what-it-is-how-it-works-for-security

Nmap. (n.d.). Chapter 15. Nmap reference guide. Noudettu 21.3.2025 osoitteesta https://nmap.org/book/man.html#man-description

Paloalto Networks. (n.d.). What Is the Difference Between IT and OT? Noudettu 9.3.2025 osoitteesta https://www.paloaltonetworks.com/cyberpedia/it-vs-ot

Peltola. (2023). OT on osa IT:tä. Noudettu 23.2.2025 osoitteesta https://www.loihde.com/ajankohtaista/blogi/ot-on-myos-itta

Piscitello. (2016). What is DNS covert channel? Noudettu 2.4.2025 osoitteesta https://www.icann.org/en/blogs/details/what-is-a-dns-covert-channel

Raivio. (2024). Infrastruktuurin kriittisyys in huomioitava jo suunnittelussa. Noudetu 7.4.2025 osoitteesta https://www.sweco.fi/blog/infrastruktuurin-kriittisyys-on-huomioitava-jo-suunnittelussa/

Rantanen. (n.d.). Palveluliiketoiminta - mitä se on. Noudettu 19.2.2025 osoitteesta https://asiakas.kotisivukone.com/files/ukipolis.palvelee.fi/Vipina/amitec.pdf

Safestate. (n.d.). Mitä tietoturvalla tarkoitetaan. Noudettu 17.2.2025 osoitteesta https://www.safestate.com/fi/artikkelit/mita-tietoturvalla-tarkoitetaan/

SensorFu. (n.d.-a). Beacon manual. Noudettu 5.2.2025 osoitteesta https://portal.sensorfu.com/manual/

SensorFu. (n.d.-b). Kotisivut. Noudettu 6.2.2025 osoitteesta https://sensorfu.com/

SensorFu. (n.d.-c). Whitepaper experience with Beacon deployments. Noudettu 5.2.2025 osoitteesta https://sensorfu.com/whitepapers/SensorFu-whitepaper-Experiences-with-Beacon-deployments.pdf

Suomen Automaatioseura. (2010). Teollisuusautomaation tietoturva Verkottumisen riskit ja niiden hallinta. Noudettu 23.2.2025 osoitteesta https://www.automaatioseura.fi/site/assets/files/2157/sas29_teollisuusautomaation_tietoturva.pdf

Toivonen. (2020). Kyberturvallisuus tuotantoverkoissa ja järjestelmissä. Noudettu 15.2.2025 osoitteesta https://yrityksille.elisa.fi/ideat/kyberturvallisuus-tuotantoverkoissa-ja-jarjestelmissa/

Traficom. (2020). Toteutettavuustutkimus: yritysten tietoturvaa voi parantaa helposti! Noudettu 9.2.2025 osoitteesta osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TONTTU_2.pdf

Traficom. (2025). Tärkeää tietoa Euroopan Unionin kyberturvallisuusdirektiivistä (NIS2). Noudettu 2.3.2025 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi/tarkeaa-tietoa

Valtioneuvosto. (2022). Kyberturvallisuus (NIS2-Direktiivi) kansallista toimeenpanoa tukeva työryhmä. Noudettu 13.3.2025 osoitteesta Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallista toimeenpanoa tukeva työryhmä - Valtioneuvosto

Varghese. (2024). A comprehensive guide to network vulnerability scanning. Noudettu 7.4.2025 osoitteesta http://getastra.com/blog/security-audit/network-vulnerability-scanning/

VPN unlimited. (n.d.-a). Containerization. Noudettu 14.3.2025 osoitteesta https://www.vpnunlimited.com/help/cybersecurity/containerization?_gl=1%2aa2rzea%2a_up%2aMQ..%2a_ga%2aMTQ3MTkwMTc0Ny4xNz-QzODQ2Nzc3%2a_ga_DE85JZ9NSX%2aMTc0Mzg0Njc3Ny4xLjAuMTc0Mzg0Njc3Ny4wLjAuMA

VPN unlimited. (n.d.-b). Eristäytyminen. Noudettu 14.3.2025 osoitteesta https://www.vpnunlimited.com/fi/help/cybersecurity/isolation

VPN unlimited. (n.d.-c). Ingress-suodatus. Noudettu 6.4.2025 osoitteesta https://www.vpnunlimited.com/fi/help/cybersecurity/ingress-filtering?srsltid=AfmBOorMRPb9E_f3VH105_2a2j1DP198Oa9uve4VLTEpEm8FP2FNX-Co

VPN unlimited. (n.d.-d). Mikrosegmentointi. Noudettu 14.3.2025 osoitteesta https://www.vpnunlimited.com/fi/help/cybersecurity/microsegmentation?srsltid=AfmBOoqkDNKhBQtG6KTmy-qkD0Ps8XGm6a6mP8ZzmZNoDlE4OF9lzoWPv

LIITTEET

LIITE 1. Virtuaalikone Beacon, testaus 1. UDP-paot taulukko.

Pakokeino	Tiedonkuljetus-muoto	Portti	Lähdeosoite
SpoofIp	Udp4	513	192.168.0.1
SpoofIp	Udp4	22	192.168.0.1
SpoofIp	Udp4	143	192.168.0.1
SpoofIp	Udp4	443	192.168.0.1
SpoofIp	Udp4	389	192.168.0.1
SpoofIp	Udp4	68	192.168.0.1
SpoofIp	Udp4	139	192.168.0.1
SpoofIp	Udp4	445	192.168.0.1
SpoofIp	Udp4	20	192.168.0.1
SpoofIp	Udp4	119	192.168.0.1
SpoofIp	Udp4	25	192.168.0.1
SpoofIp	Udp4	514	192.168.0.1
SpoofIp	Udp4	107	192.168.0.1
SpoofIp	Udp4	110	192.168.0.1
SpoofIp	Udp4	123	192.168.0.1
SpoofIp	Udp4	109	192.168.0.1
SpoofIp	Udp4	8080	192.168.0.1
SpoofIp	Udp4	115	192.168.0.1
SpoofIp	Udp4	23	192.168.0.1
SpoofIp	Udp4	21	192.168.0.1
SpoofIp	Udp4	80	192.168.0.1

LIITE 2. Virtuaalikone Beacon, testaus 1. ICMP-paot taulukko.

Pakokeino	Tiedonkuljetusmuoto	Lähdeosoite	Pakojen määrä
SpoofIp	Icmp4	10.0.0.1	51
SpoofIp	Icmp4	172.16.1.17	2
SpoofIp	Icmp4	172.16.1.33	3
SpoofIp	Icmp4	172.16.1.65	2
SpoofIp	Icmp4	192.168.0.1	54

LIITE 3. Windows Beacon, testaus 1. IPv4 paot taulukko.

Pakokeino	Tiedonkuljetusmuoto	Lähdeosoite IPv4	Pakojen määrä
DNSQuery	DNS	Osoite 1	1
DNSQuery	DNS	Osoite 2	6
DNSQuery	DNS	Osoite 3	2
DNSQuery	DNS	Osoite 4	4
DNSQuery	DNS	Osoite 5	4
DNSQuery	DNS	Osoite 6	1
DNSQuery	DNS	Osoite 7	1
DNSQuery	DNS	Osoite 8	4
DNSQuery	DNS	Osoite 9	2
DNSQuery	DNS	Osoite 10	2
DNSQuery	DNS	Osoite 11	5
DNSQuery	DNS	Osoite 12	5
DNSQuery	DNS	Osoite 14	3
DNSQuery	DNS	Osoite 15	2
DNSQuery	DNS	Osoite 16	1
DNSQuery	DNS	Osoite 17	4
DNSQuery	DNS	Osoite 18	2
DNSQuery	DNS	Osoite 19	2
DNSQuery	DNS	Osoite 20	4
DNSQuery	DNS	Osoite 21	2
DNSQuery	DNS	Osoite 22	3
DNSQuery	DNS	Osoite 23	3
DNSQuery	DNS	Osoite 24	1

LIITE 4. Windows Beacon, testaus 1. IPv6 paot taulukko.

Pakokeino	Tiedonkuljetusmuoto	Lähdeosoite IPv6	Pakojen määrä
DNSQuery	DNS	Osoite 1	3
DNSQuery	DNS	Osoite 2	2
DNSQuery	DNS	Osoite 3	2
DNSQuery	DNS	Osoite 4	1
DNSQuery	DNS	Osoite 5	1
DNSQuery	DNS	Osoite 6	6
DNSQuery	DNS	Osoite 7	3
DNSQuery	DNS	Osoite 8	2
DNSQuery	DNS	Osoite 9	5
DNSQuery	DNS	Osoite 10	2
DNSQuery	DNS	Osoite 12	6
DNSQuery	DNS	Osoite 13	2
DNSQuery	DNS	Osoite 14	5
DNSQuery	DNS	Osoite 17	2
DNSQuery	DNS	Osoite 18	6
DNSQuery	DNS	Osoite 19	1
DNSQuery	DNS	Osoite 20	2
DNSQuery	DNS	Osoite 21	7
DNSQuery	DNS	Osoite 22	3
DNSQuery	DNS	Osoite 23	2
DNSQuery	DNS	Osoite 24	6

LIITE 5. Virtuaalikone Beacon, testaus 2. UDP-paot taulukko.

Pakokeino	Tiedonkuljetusmuoto	Portti	Lähdeosoite
SpoofIp	Udp4	389	192.168.0.1
SpoofIp	Udp4	107	192.168.0.1
SpoofIp	Udp4	123	192.168.0.1
SpoofIp	Udp4	20	192.168.0.1
SpoofIp	Udp4	23	192.168.0.1
SpoofIp	Udp4	119	192.168.0.1
SpoofIp	Udp4	445	192.168.0.1
SpoofIp	Udp4	110	192.168.0.1
SpoofIp	Udp4	22	192.168.0.1
SpoofIp	Udp4	443	192.168.0.1
SpoofIp	Udp4	80	192.168.0.1
SpoofIp	Udp4	8080	192.168.0.1
SpoofIp	Udp4	25	192.168.0.1
SpoofIp	Udp4	514	192.168.0.1
SpoofIp	Udp4	139	192.168.0.1
SpoofIp	Udp4	513	192.168.0.1
SpoofIp	Udp4	115	192.168.0.1
SpoofIp	Udp4	21	192.168.0.1
SpoofIp	Udp4	68	192.168.0.1
SpoofIp	Udp4	143	192.168.0.1
SpoofIp	Udp4	109	192.168.0.1

LIITE 6. Virtuaalikone Beacon, testaus 2. ICMP-paot taulukko.

Pako-keino	Tiedonkuljetus-muoto	Lähde-osoite	Pakojen määrä
SpoofIp	Icmp4	10.0.0.1	78
SpoofIp	Icmp4	172.16.1.17	7
SpoofIp	Icmp4	172.16.1.33	3
SpoofIp	Icmp4	172.16.1.65	6
SpoofIp	Icmp4	192.168.0.1	119

LIITE 7. Windows Beacon, testaus 2. IPv4 paot taulukko.

Pakokeino	Tiedonkuljetusmuoto	Lähdeosoite IPv4	Pakojen määrä
DNSQuery	DNS	Osoite 1	2
DNSQuery	DNS	Osoite 2	15
DNSQuery	DNS	Osoite 3	1
DNSQuery	DNS	Osoite 4	5
DNSQuery	DNS	Osoite 5	10
DNSQuery	DNS	Osoite 6	3
DNSQuery	DNS	Osoite 7	5
DNSQuery	DNS	Osoite 8	2
DNSQuery	DNS	Osoite 9	2
DNSQuery	DNS	Osoite 10	4
DNSQuery	DNS	Osoite 11	10
DNSQuery	DNS	Osoite 12	4
DNSQuery	DNS	Osoite 13	5
DNSQuery	DNS	Osoite 14	6
DNSQuery	DNS	Osoite 15	4
DNSQuery	DNS	Osoite 16	4
DNSQuery	DNS	Osoite 17	11
DNSQuery	DNS	Osoite 18	7
DNSQuery	DNS	Osoite 19	3
DNSQuery	DNS	Osoite 20	7
DNSQuery	DNS	Osoite 21	5
DNSQuery	DNS	Osoite 22	4
DNSQuery	DNS	Osoite 23	6
DNSQuery	DNS	Osoite 24	1

LIITE 8. Windows Beacon, testaus 2. IPv6 paot taulukko.

Pakokeino	Tiedonkuljetusmuoto	Lähdeosoite IPv6	Pakojen määrä
DNSQuery	DNS	Osoite 1	2
DNSQuery	DNS	Osoite 2	1
DNSQuery	DNS	Osoite 3	11
DNSQuery	DNS	Osoite 4	1
DNSQuery	DNS	Osoite 5	2
DNSQuery	DNS	Osoite 6	10
DNSQuery	DNS	Osoite 7	3
DNSQuery	DNS	Osoite 8	2
DNSQuery	DNS	Osoite 9	6
DNSQuery	DNS	Osoite 10	4
DNSQuery	DNS	Osoite 11	7
DNSQuery	DNS	Osoite 12	6
DNSQuery	DNS	Osoite 13	3
DNSQuery	DNS	Osoite 14	3
DNSQuery	DNS	Osoite 15	15
DNSQuery	DNS	Osoite 16	1
DNSQuery	DNS	Osoite 17	9
DNSQuery	DNS	Osoite 18	9
DNSQuery	DNS	Osoite 19	3
DNSQuery	DNS	Osoite 20	2
DNSQuery	DNS	Osoite 21	9
DNSQuery	DNS	Osoite 22	8
DNSQuery	DNS	Osoite 23	3
DNSQuery	DNS	Osoite 24	8

LIITE 9. Virtuaalikone Beacon, testaus 3. UDP-paot taulukko 1.

Pakokeino	Tiedonkuljetus-muoto	Portti	Lähdeosoite
SpoofIp	Udp4	139	10.0.0.1
SpoofIp	Udp4	110	10.0.0.1
SpoofIp	Udp4	513	10.0.0.1
SpoofIp	Udp4	68	10.0.0.1
SpoofIp	Udp4	119	10.0.0.1
SpoofIp	Udp4	514	10.0.0.1
SpoofIp	Udp4	443	10.0.0.1
SpoofIp	Udp4	109	10.0.0.1
SpoofIp	Udp4	8080	10.0.0.1
SpoofIp	Udp4	389	10.0.0.1
SpoofIp	Udp4	23	10.0.0.1
SpoofIp	Udp4	107	10.0.0.1
SpoofIp	Udp4	22	10.0.0.1
SpoofIp	Udp4	143	10.0.0.1
SpoofIp	Udp4	21	10.0.0.1
SpoofIp	Udp4	123	10.0.0.1
SpoofIp	Udp4	80	10.0.0.1
SpoofIp	Udp4	20	10.0.0.1
SpoofIp	Udp4	115	10.0.0.1
SpoofIp	Udp4	445	10.0.0.1
SpoofIp	Udp4	25	10.0.0.1

LIITE 10. Virtuaalikone Beacon, testaus 3. UDP-paot taulukko 2.

Pakokeino	Tiedonkuljetus-muoto	Portti	Lähdeosoite
SpoofIp	Udp4	445	192.168.0.1
SpoofIp	Udp4	443	192.168.0.1
SpoofIp	Udp4	80	192.168.0.1
SpoofIp	Udp4	107	192.168.0.1
SpoofIp	Udp4	23	192.168.0.1
SpoofIp	Udp4	119	192.168.0.1
SpoofIp	Udp4	22	192.168.0.1
SpoofIp	Udp4	143	192.168.0.1
SpoofIp	Udp4	139	192.168.0.1
SpoofIp	Udp4	21	192.168.0.1
SpoofIp	Udp4	20	192.168.0.1
SpoofIp	Udp4	109	192.168.0.1
SpoofIp	Udp4	8080	192.168.0.1
SpoofIp	Udp4	68	192.168.0.1
SpoofIp	Udp4	389	192.168.0.1
SpoofIp	Udp4	25	192.168.0.1
SpoofIp	Udp4	123	192.168.0.1
SpoofIp	Udp4	514	192.168.0.1
SpoofIp	Udp4	110	192.168.0.1
SpoofIp	Udp4	115	192.168.0.1
SpoofIp	Udp4	513	192.168.0.1

LIITE 11. Virtuaalikone Beacon, testaus 3. ICMP-paot taulukko.

Pako-keino	Tiedonkuljetus-muoto	Lähde-osoite	Pakojen määrä
SpoofIp	Icmp4	10.0.0.1	184
SpoofIp	Icmp4	172.16.1.17	9
SpoofIp	Icmp4	172.16.1.33	6
SpoofIp	Icmp4	172.16.1.65	30
SpoofIp	Icmp4	192.168.0.1	174

LIITE 12. Windows Beacon, testaus 3. IPv4 paot taulukko.

Pakokeino	Tiedonkuljetusmuoto	Lähdeosoite IPv4	Pakojen määrä
DNSQuery	DNS	Osoite 1	7
DNSQuery	DNS	Osoite 2	14
DNSQuery	DNS	Osoite 3	3
DNSQuery	DNS	Osoite 4	4
DNSQuery	DNS	Osoite 5	13
DNSQuery	DNS	Osoite 6	3
DNSQuery	DNS	Osoite 7	5
DNSQuery	DNS	Osoite 8	9
DNSQuery	DNS	Osoite 9	3
DNSQuery	DNS	Osoite 10	5
DNSQuery	DNS	Osoite 11	15
DNSQuery	DNS	Osoite 12	8
DNSQuery	DNS	Osoite 13	3
DNSQuery	DNS	Osoite 14	9
DNSQuery	DNS	Osoite 15	4
DNSQuery	DNS	Osoite 16	7
DNSQuery	DNS	Osoite 17	18
DNSQuery	DNS	Osoite 18	5
DNSQuery	DNS	Osoite 19	3
DNSQuery	DNS	Osoite 20	18
DNSQuery	DNS	Osoite 21	2
DNSQuery	DNS	Osoite 22	3
DNSQuery	DNS	Osoite 23	8
DNSQuery	DNS	Osoite 24	2

LIITE 13. Windows Beacon, testaus 3. IPv6 paot taulukko.

Pakokeino	Tiedonkuljetusmuoto	Lähdeosoite IPv6	Pakojen määrä
DNSQuery	DNS	Osoite 1	7
DNSQuery	DNS	Osoite 2	3
DNSQuery	DNS	Osoite 3	8
DNSQuery	DNS	Osoite 4	2
DNSQuery	DNS	Osoite 5	6
DNSQuery	DNS	Osoite 6	11
DNSQuery	DNS	Osoite 7	6
DNSQuery	DNS	Osoite 8	8
DNSQuery	DNS	Osoite 9	14
DNSQuery	DNS	Osoite 10	6
DNSQuery	DNS	Osoite 11	4
DNSQuery	DNS	Osoite 12	11
DNSQuery	DNS	Osoite 13	1
DNSQuery	DNS	Osoite 14	7
DNSQuery	DNS	Osoite 15	14
DNSQuery	DNS	Osoite 16	2
DNSQuery	DNS	Osoite 17	5
DNSQuery	DNS	Osoite 18	20
DNSQuery	DNS	Osoite 19	9
DNSQuery	DNS	Osoite 20	4
DNSQuery	DNS	Osoite 21	15
DNSQuery	DNS	Osoite 22	9
DNSQuery	DNS	Osoite 23	5
DNSQuery	DNS	Osoite 24	8