jamk

# Verkkojen eristyksentestausjärjestelmän käyttöönoton pilotointi

Aleksi Antikainen

Opinnäytetyö, AMK
Maaliskuu 2024
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

**Kuvailulehti**

**Antikainen Aleksi**

**Verkkojen eristyksentestausjärjestelmän käyttöönoton pilotointi**

Jyväskylä: Jyväskylän ammattikorkeakoulu. Maaliskuu 2024, 31 sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

**Tiivistelmä**

Maailman digitalisoituessa kyberturvallisuus on noussut kriittisen tärkeäksi osaksi turvallisuutta. Digitalisoitumisen kasvun myötä käytännössä kaikki yhteiskunnan palvelut ja infrastruktuuri, kuten myös esimerkiksi yksityishenkilöiden kodinkoneet (IOT), toimivat tietoverkkojen- ja järjestelmien avulla. Järjestelmiä pystytään ohjaamaan satojen kilometrien päässä etänä, joka nopeuttaa ja tuo joustavuutta teollisuuden kehitykseen, mutta se tuo mukanaan myös uhkatilanteita.

Automatisoitu eristyksentestausjärjestelmä auttaa parantamaan kriittisesti tärkeiden verkkojen turvallisuutta ja varmistamaan ettei tahattomia tietovuotoja pääse niissä tapahtumaan. Opinnäytetyön tavoitteena oli pilotoida automaattisen eristyksentestausjärjestelmän käyttöönottoa puolustusvoimissa. Opinnäytetyön viitekehyksenä oli eristettyjen tietoverkkojen turvallisuuden testaaminen sekä eristyksen ja eheyden varmistaminen.

Automaattinen verkkojen eristyksentestausjärjestelmänä käytettiin kaupallisen yrityksen (SensorFu) järjestelmää, jonka tuotenimi on Beacon. Pilotointi tapahtui toimittajan ylläpitämässä demoympäristössä. Toteutus tehtiin systemaattisesti seuraavin vaihein: 1) järjestelmään perehtyminen, 2) asentaminen ja käyttöönotto, 3) hälytysten ja lokien lähettämisen testaus ja 4) käyttökohteiden kartoittaminen puolustusvoimissa.

Beacon toimii hyvin automaattisena verkkojen eristyksentestausjärjestelmänä. Järjestelmän eristetyn verkon testausmenetelmät auttavat löytämään aukkoja ja haavoittuvuuksia verkoista. Järjestelmän käyttöönotto on helppoa ja valmistajan manuaalit olivat toimivia ja selkeitä. Järjestelmä tuo merkittävää turvallisuutta ja aikasäästöä jatkuvan automaattisen testauksen ansiosta.

**Avainsanat (asiasanat)**

Kyberturvallisuus, verkkojen eristyksentestausjärjestelmä, käyttöönotto, pilotointi.

**Muut tiedot (salassa pidettävät liitteet)**

jamk

**Description**

**Antikainen, Aleksi**

**Pilot work of an automatic network isolation testing system**

Jyväskylä: JAMK University of Applied Sciences, March 2024, 31 pages

Degree Programme in Information and Communications Technology, Bachelor´s thesis

Permission for open access publication: Yes

Language of publication: Finnish

**Abstract**

As the world becomes more digitalized, cybersecurity has become a critically important part of security. With the growth of digitalization, practically all societal services and infrastructure, including private household appliances (IOT), operate through information networks and systems. Systems can be controlled remotely from hundreds of kilometers away, speeding up their usage and adding flexibility to industrial development. However, at the same time, potential threat situations arise.

The automated network isolation testing system helps to improve the security of critically important networks and ensure that unintentional leaks do not occur. The purpose of the thesis was to pilot the implementation of an automatic network isolation testing system in the Defense Forces. The framework of the thesis focused on testing the security of isolated networks and ensuring isolation and integrity.

The automated network isolation testing system utilized a commercial company's (SensorFu) system, named Beacon. The piloting was done in a demo environment maintained by the supplier. The implementation was carried out systematically following steps: 1) getting to know the system, 2) installation and commissioning, 3) testing of sending alerts and logs and 4) mapping of the system's use within the Finnish Defense Forces.

Beacon works well as an automatic network isolation testing system. The testing methods of the system for isolated networks help in finding leaks and vulnerabilities in the networks. The implementation of the system is easy and the manufacturer's manuals are helpful and clear. The system brings significant safety and time savings thanks to continuous automated testing.

**Keywords/tags (subjects)**

Cybersecurity, network isolation testing system, pilot work, introduction.

**Miscellaneous (Confidential information)**

**Sisältö**



**Kuviot**

## Sanasto

API = Application Programming Interface

DNS = Domain Name System

GPO = Group Policy

IAM = Identity and Access Management

IOT = Internet of Things

IP = Internet Protocol

OT = Operational Technology

SIEM = Security information and event management

TCP = Transmission Control Protocol

TLS = Transport Layer Security

UDP = User Datagram Protocol

VLAN= Virtual Local Area Network

# 1 Johdanto

Maailman jatkuvasti digitalisoituessa kyberturvallisuus on noussut kriittisen tärkeäksi osaksi turvallisuutta (Kotipelto, n.d). Digitalisoitumisen kasvun myötä käytännössä kaikki yhteiskunnan palvelut ja infrastruktuuri, kuten myös esimerkiksi yksityishenkilöiden kodinkoneet (IOT), toimivat tietoverkkojen- ja järjestelmien avulla. Järjestelmiä pystytään ohjaamaan satojen kilometrien päässä etänä, joka nopeuttaa ja tuo joustavuutta teollisuuden kehitykseen, mutta se tuo mukanaan myös uhkatilanteita.

Kyberhyökkäysten kohteiksi valikoituu usein kriittinen infrastruktuuri. Tämä käsittää rakenteet ja palvelut, jotka ovat välttämättömiä yhteiskunnan elintärkeille toiminnoille. Tähän sisältyy niin fyysiset laitokset ja rakenteet sekä digitaaliset toiminnot ja palvelut. Näitä ovat esimerkiksi sähköntuotanto-, sairaaloiden- ja puolustusvoimienverkot. Näiden verkkojen kyberturvallisuus on elintärkeää sillä mahdolliset häiriöt tai hyökkäykset voivat aiheuttaa vakavia seurauksia, kuten tuotannon pysähtymistä, laadun heikkenemistä tai jopa vaaratilanteita. (Jurvanen, 2023.)

Opinnäytteen toimeksiantaja oli Ilmavoimien esikunta. Opinnäytetyön tavoitteena oli pilotoida automaattisen eristyksentestausjärjestelmän käyttöönottoa puolustusvoimissa. Automaattinen verkkojen eristyksentestausjärjestelmänä käytettiin kaupallisen yrityksen (SensorFu) järjestelmää, jonka tuotenimi on Beacon. Työskentelin Ilmavoimien esikunnassa määräaikaisena työntekijänä ajanjaksolla 9.1.2023 – 31.12.2023.

## 1.1 Toimeksiantaja

Ilmavoimat vastaa Suomen ilmapuolustuksesta ja ilmaoperaatioista. Ilmavoimat suorittaa Suomen alueellisen koskemattomuuden valvontaa ympäri vuorokauden. Rauhanaikana Ilmavoimien lentokalusto toimii pääasiassa Lapin lennoston, Karjalan lennoston, Satakunnan lennoston sekä Ilmasotakoulun tukikohdissa. Kriisiaikana ilmavoimien päätehtävä on hävittäjätorjunta ja suojata yhteiskunnan kriittisiä kohteita ja toimintoja. Tämän lisäksi ilmavoimat johtavat kaikkien puolustushaarajoen ilmapuolustuksen tulenkäyttöä. (Ilmavoimat vastaa Suomen ilmapuolustuksesta, n.d.)

Tikkakoskella sijaitseva Ilmavoimien esikunta vastaa Suomen ilmapuolustuksen johtamisesta rauhan- sekä kriisiaikana. Esikunnan kokoonpanoon kuuluvat kanslia, operatiivinen osasto, henkilöstö-, suunnittelu-, huolto- ja johtamisjärjestelmäosastot, lentoturvallisuusyksikkö, viestintäkeskus, oikeudellinen sektori ja ilmaoperaatiokeskus. Ilmaoperaatiokeskus toimii Suomen ilmapuolustuksen ylimpänä johtokeskuksena ja vastaa alueellisen koskemattomuuden valvonnasta ja turvaamisesta ilmatilan osalta. (Ilmavoimien johtoesikunta, n.d.)

## 1.2 Tavoite

Automatisoitu eristyksentestausjärjestelmä auttaa parantamaan puolustusvoimien verkkojen turvallisuutta ja varmistamaan ettei tahattomia verkkojen vuotoja pääse tapahtumaan. Opinnäytetyön tavoitteena on pilotoida verkkojen automaattisen eristyksentestausjärjestelmän Beacon käyttöönottoa.

## 1.3 Aineiston haku

Janet Finna verkkokirjaston hakusanalla ”cyber security” löytyi 874 kappaletta, joista 684 oli kirjoja ja 59 artikkelia ja loput opinnäytetöitä. Kyberturvallisuuden kirjallisuuden määrä on kasvanut huimasti 2010 luvun jälkeen.  Vuosina 2000–2009 kyberturvallisuuteen liittyvää kirjallisuutta oli ainoastaan 54 kappaletta kun taas aikavälillä 2010–2020 määrä oli noussut 646 kappaleeseen.

IEEE Xplore tietokannassa kyberturvallisuuteen liittyvää kirjallisuutta vuosina 2000–2009 oli ainoastaan 19 kappaletta. Vuosina 2010–2020 kirjallisuuden määrä oli kasvanut yli 300 ja viimeisten vuosien aikana yli tuplaantunut.

Tutkimusaiheeseen on saatavilla viittaavia ja sivuavia aineistoja. Eristettyjen verkkojen tietoturvallisuuteen liittyvää tietoa löytyy eniten artikkeleista eri verkkosivuilta mm. Kyberturvallisuuskeskuksen ja Katakri – tietoturvallisuuden auditointityökalu.

Tämän työn tietoperustassa on hyödynnetty edellä kuvattuja tietokantoja. Eristyksentestausjärjestelmälle ei suoraan löydy kirjallisuutta, joten tässä työssä on hyödynnetty pääasiallisesti järjestelmän valmistajan SensorFu tuottamaa dokumentaatiota sekä internetlähteitä.

# 2 Tietoperusta

Tietoturvalla tarkoitetaan teknillisiä sekä hallinnollisia toimia, joita organisaatiot käyttävät tietojen suojaamiseen. Tietoturvan tarkoitus on suojata arkaluonteisia tietoja luvattomalta toiminnalta, kuten vakoilulta, muuttamiselta, tallentamiselta sekä häirinnältä tai tuhoamiselta. Tavoitteena on varmistaa kriittisten tietojen, kuten asiakastilitietojen ja taloudellisten tietojen turvallisuus ja yksityisyys. Tietoturva koostuu kolmesta kohdasta, luottamuksellisuus, eheys ja käytettävyys. Nämä kolme kohtaa muodostavat niin sanotun CIA-kolmion. (Tietoturva, 2020.) Luottamuksellisuudella varmistetaan, että tieto on ainoastaan oikeudenhaltioiden käsiteltävissä eli vain henkilöiden, joille se on tarkoitettu. Eheydellä varmistetaan, että luvattomat käyttäjät eivät voi muokata, muuttaa tai muuten häiritä tietoja. Käytettävyys varmistetaan, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen käytettävissä. (What is information security (InfoSec), n.d.)

## 2.1 Eristetyt verkot

Tietoturvan yksi keskeinen ja kriittinen osa on eristetyt verkot. Nämä verkot ovat eristetty fyysisesti tai loogisesti julkisista ja muista ei luotetuista verkoista. Erittäin arkaluonteisten tietojen, kuten armeijoiden ja kriittisen infrastruktuurin käyttämät verkot halutaan eristää kokonaan eli verkko niin sanotusti Air-gapataan muista verkoista. Tuotantoverkot ovat yleensä vahvasti eristettyjä julkisista verkoista sekä yrityksen omista IT-järjestelmistä, ja niitä operoivat erilliset käyttäjät. (Toivonen, 2020; Peterson,2016.) Tuotantoverkkoja voidaan käyttää ohjaamaan yhteiskunnan kriittisiä toimintoja. Näitä ovat esimerkiksi metro-, juna- ja lentoliikenne, elintarviketeollisuuden valmistumista sekä energian- ja sähköntuotantoa. Heikkinen (2021) arvelee, että sairaaloiden ja terveydenhuollon hoitoprosessien ja muiden kriittisteninfrastruktuurin digitalisoitumisen myötä kyberhyökkäysriskien pinta-ala kasvaa merkittävästi. Tämän lisäksi, nykyään tuotantoverkoihin tarvitaan joustavampi pääsy, tai verkon dataa halutaan hyödyntää joustavasti, tarvittaessa jopa reaaliaikaisesti. Etätyöskentelyn yleistyminen ovat asettaneet myös omat haasteensa tuotantoverkkojen tietoturvalle. (Koskinen, 2023.)

Verkkojen eristämisen tarkoitus on toimia suojausmekanismina ja se onkin yksi tietotuvan kulmakivistä. Verkkojen eristäminen, jotta palvelut ja laitteet eivät voi kommunikoida aiottujen verkkojen ulkopuolella, vähentää hyökkäys pintaa huomattavasti. (Network segmentation in OT environments. N.d.) Fyysisesti eristetyt verkot ovat monesti immuuneja yleisille haittaohjelmille ja

kyberhyökkäyksille, jotka ovat riippuvaisia internet-yhteydestä mutta yksin turvallisuutta näiden varaan ei voida laskea. Tuotantoverkkojen eli Operational technology (OT-verkot) eristäminen IT-verkoista ja muista ulkopuolista verkoista auttaa rajoittamaan hyökkäysten leviämistä ja samalla tavalla pienentää riskiä, etteivät OT-järjestelmiin kohdistuvat hyökkäykset vaikuta koko organisaatioon tai edes koko OT-verkkoon. Segmentoinnilla eli verkon jakamisella pienempiin osiin voidaan eriyttää eri laitetyypit ja palvelut omiin OT-verkkoihinsa tai rajoittaa riskejä eri yhteyksien välillä. (Jurvanen,2023.)

Verkkojen eristämisellä on kuitenkin myös haittapuolia. Järjestelmien päivittäminen on hidasta ja työlästä ja tämän seurauksena OT-järjestelmien elinkaari on usein kymmeniä vuosia ja päivityksiä järjestelmien sisällä oleviin useimmiten tarjoaa vain järjestelmätoimittaja (Toivonen, 2020). Tämä johtaa tilanteisin, jossa kriittisen infrastruktuurin järjestelmät ovat tulleet elinkaarensa päähän, eikä niihin ole saatavilla tietoturvapäivityksiä, jonka seurauksena voi syntyä isoja tietoturva-aukkoja. Eristettyjen verkkojen ylläpito ja hallinta voi olla toiminnallisesti monimutkaista, mikä edellyttää huolellista suunnittelua ja koordinointia. Tiedonsiirto verkkojen välillä voi olla haastavaa ja vaatia erillisiä turvallisuusprotokollia ja menettelyjä. (Katakri, 2020, 84.)

Verkkojen eristyksen suurimpana haasteena voi kuitenkin olla, että miten yritykset tietävät varmasti onko eristetyksi tarkoitettu verkko oikeasti eristetty. Tämä korostuu etenkin isoissa ja komplekseissa järjestelmissä, joissa verkkoja on hajautettu ja segmentoitu pieniin osiin. Verkon vuotokohtia saattaa syntyä vahingossa, esimerkiksi konfiguraatio muutoksissa, inhimillisten virheiden takia tai vihamielisen toimijan tekemänä. (Is your network isolation leaking. N.d.) Vuonna 2020 kyberturvallisuuskeskus piti toteutettavuustutkimuksen (TONTTU), jonka tarkoitus oli helpottaa ja parantaa yritysten kyberturvallisuutta ja osaamista. Toteutettavuustutkimukseen osallistui 11 yritystä, joiden kokoluokka vaihteli 1 työntekijästä aina yli 500. Jopa 81 % osallistuvien organisaatioiden eristetyiksi tarkoitetuista verkoista vuotivat odottamattomilla tavoilla. Tutkimuksen perusteella voidaan todeta, ettei yrityksillä ole tarkkaa tietämistä ovatko eristetyt verkot oikeasti eristettyjä. Kyberturvallisuuskeskuksen mukaan yritysten tulisi panostaa tuotantoverkkojen tärkeiden tietoturvakontrollien, kuten verkkojen eristyksen ja toimivuuden valvontaan. (Traficom, 2022.)

## 2.2 Kriittinen infrastruktuuri kyberhyökkäysten kohteena

Digitalisoidussa maailmassa kyberhyökkäykset ja tietoturvavuodot voivat aiheuttaa laajasti vaaraa ihmisten hyvinvoinnille ja terveydelle sekä yleiselle turvallisuudelle. Niiden seurauksena arkaluoteista tietoa voi vuotaa nettiin ja jopa yhteiskunta voi lamaantua, jos hyökkäys kohdistuu erittäin kriittiseen infrastruktuuriin. Tämän lisäksi organisaation tai yrityksen maine voi kärsiä pahasti ja ihminen voi joutua identiteetti varkauden uhriksi. (Heikkinen. 2021.)

Kyberhyökkäysten määrä on ollut kasvussa jo useamman vuoden verran. Kyberhyökkäyksiksi kutsutaan laajaa kirjoa erilaisia tapoja ja menetelmiä, joilla pyritään muun muassa lamauttamaan järjestelmiä, varastamaan tietoja, vahingoittaa tai saada käyttöön tärkeitä tiedostoja ja järjestelmiä yrityksen tai henkilön tietokoneverkossa. Kyberhyökkäykset voivat koostua eri muodoista. Yleisimpiä hyökkäyksen muotoja ovat kiristyshaittaohjelmat, tietojenkalastelu ja troijalaiset. Kiristyshaittaohjelmat eli ransomwaret tavoitteena on lukita uhriensa laiteet tai estää pääsyä hakemistoihin ja tiedostoihin. Hyökkääjät lupaavat avata lukituksen, mikäli lunnaat maksetaan, mutta tämä on usein valhetta. Tietojenkalastelulla pyritään huijaamalla saamaan uhrin käyttäjätunnukset. Yleisimpiä tietojenkalastelu yrityksistä on naamioida sähköpostiviesti, jonkin luotettavan tahon nimiin, kuten pankin. Troijalainen on haittaohjelma, joka on naamioitu harmittomaksi tiedostoksi. Troijalainen voi levitä esimerkiksi sähköpostin liitteenä. (F-secure, n.d; Microsoft, n,d.)

Kyberturvallisuuskeskuksen raportin mukaan (2022) vuonna 2022 kiristyshaittaohjelmien määrä oli kasvanut jopa 30 % ja tietojenkalasteluiden määrä 8 % sekä palvelunestohyökkäysten määrä jatkanut tasaista kasvua. Watefall-securityn toukokuussa 2023 julkaiseman raportin mukaan pandemian jälkeen tuotantolaitoksiin kohdistuneet kybersabotaasihyökkäykset ovat kasvaneet runsaasti. Raportin mukaan hyökkäykset, jotka johtivat fyysisiin seurauksiin prosessivalmistuksessa, erillisessä valmistuksessa ja kriittisissä teollisissa infrastruktuureissa, vaikuttivat yli 150 teolliseen toimintaan vuonna 2022. Lisäksi kyberhyökkäysten kokonaismäärä kasvoi jopa 2,4-kertaiseksi edellisvuoteen nähden. (Ginter, Hale, Machtemes, Molina, Wallhof & Schneider, 2023.)

### 2.2.1 Kyberhyökkäykset sodankäynnissä

Kyberhyökkäyksiä on pitkään käytetty myös sodankäynnissä eri toimijoiden toimesta. Lehto (2022) toteaa, että Ukrainan infrastruktuuri on joutunut useiden vuosien ajan vakavien kyberhyökkäysten

kohteeksi. Joulukuussa 2015 hyökkääjät onnistuivat iskemään ukrainalaiseen energiayhtiöön ja katkaisemaan sähkönjakelun 80 000 asukkaalta. Vuonna 2016 tehty kyberhyökkäys katkaisi 20 % Kiovan sähköntarpeesta. Kesäkuussa 2017 NonPetya-haittaohjelma levisi Ukrainassa käytetyn M.E.Doc -kirjanpito-ohjelmistoon, jonka kautta se levisi nopeasti aiheuttaen jopa yli 10 miljardin dollarin kustannukset.

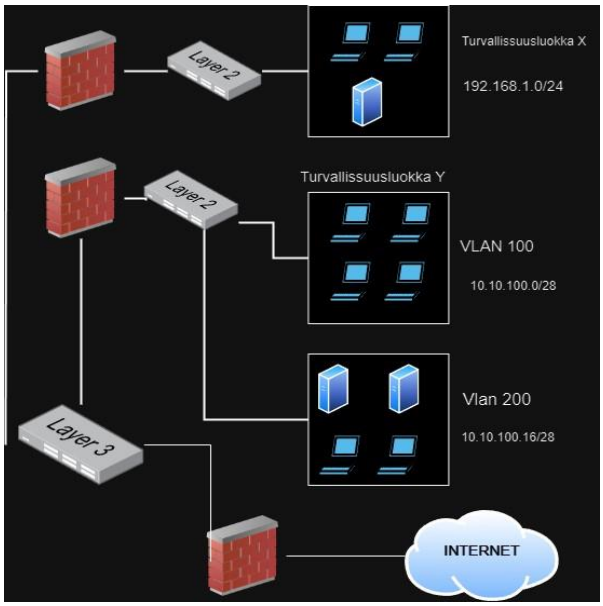
Tammikuussa 2022, kuukautta ennen Venäjän aseellista hyökkäystä Ukrainaan alkoivat laajat palvelunestohyökkäykset Ukrainan hallinon, asevoimien sekä pankkien verkkosivuja vastaan. Helmikuussa 2022 aseellisen hyökkäysten alettua samaan aikana levisi tietoja tuhoava haittaohjelma satoihin järjestelmiin Ukrainassa. Lisäksi hakkerit hyökkäsivät Ukrainan satelliittilaajakaistaan tavoitteenaan lamauttaa Ukrainan asevoimien johtamisjärjestelmä. (Lehto, 2022.)

## 2.3 Verkon eristäminen

Yleisin tapa eriyttää verkkoja on segmentoimalla. Segmentointi tarkoittaa verkon jakamista fyysisiin tai loogisiin vyöhykkeisiin (Petryschuk, n.d). Eli verkko pilkotaan pienempiin hallittavampiin aliverkkoihin, joita kutsutaan segmenteiksi tai vyöhykkeiksi. Fyysisessä segmentoinnissa käytetään laitteistoa kuten reitittimiä, kytkimiä ja palomuureja verkon jakamiseen vyöhykkeisiin. Fyysinen tai virtuaalinen palomuuri toimii aliverkon yhdyskäytävänä, joka hallitsee, mikä liikenne tulee sisään ja lähtee ulos. Loogisessa segmentoinnissa luodaan aliverkkoja käyttämällä virtuaalisia lähiverkkoja eli VLAN tai verkon osoitejärjestelmiä (Network Addressing Scheme). (What Is Network Segmentation, n.d.) Verkossa olevat laitteet ja palvelut ryhmitellään loogisesti siten, että niille voidaan luoda omat aliverkot. Tällöin eri aliverkkojenkin välistä liikennettä voidaan valvoa palomuurien ja mm. IDS (Intrusion Detection System) tai IPS (Intrusion Prevention System) järjestelmien avulla. (Järvinen, 2023.)

Segmentit erotellaan muista yleensä palomuurien, reitittimien ja kytkimien avulla. Segmentit jaetaan osiin, joilla on samanlaiset tietoturvavaatimukset (katso kuvio 1). Tarkoituksena on, että eri turvaluokat eivät keskustele keskenään. Yksi KATAKRI oppaiden (Kansallinen turvallisuusviranomaisen tuottama auditointityökalu) keskeisistä vaatimuksista on erottaa tietojärjestelmät niiden turvallisuusluokittelun mukaan. Tämä tarkoittaa, että ei-luotetut verkot ovat joko rajoitettuja tai korkeamman turvallisuuden verkoissa, joissa kaikki yhteydet muihin verkkoihin on katkaistu koko-

naan. Tarkoituksena on luoda loogiset rajat, jotka rajoittavat luvatonta käyttöä ja rajoittavat mahdollisen tietoturvaloukkauksen vaikutusta. Segmentointi jakaa verkot pienempiin aliverkkoihin. Verkkoliikenteen eristäminen pienentää hyökkäyspinta-alaa ja estää sivuttaisliikkeen (lateral movement). (Katakri, 2020.) Segmentointi myös eristää hyökkäykset ennen niiden leviämistä. Esimerkiksi haittaohjelmatartunta yhdessä aliverkossa ei välttämättä vaikuta toisen aliverkon järjestelmiin, vaan vahingot pystytään rajoittamaan tiettyyn segmenttiin (Jurvanen, 2023).




Kuvio 1 Eri turvallisuusluokan verkot segmentoituna

Verkon segmentoinnin etuna on myös ruuhkautumisen vähentyminen. Kun verkossa on liian monta isäntää (hostia) ja paketteja lähetetään liian monta, jonka seurauksena voi olla ruuhkautuminen. Joissakin tapauksissa suorituskyky voi kärsiä siinä määrin, että pakettia ei toimiteta. Aliverkotus vähentää ruuhkautumista merkittävästi. (Silk, 2022.)

### 2.3.1 Turvallisuus eristetyissä verkoissa

Verkkojen segmentoinnin lisäksi palomuureille tulee asettaa tiukat säännöt, jossa määritellään mitkä verkot saavat keskustella minkäkin verkon kanssa. Kriittisissä ympäristöissä pelkkä verkon segmentointi ei riitä vaan verkko eristetään fyysisesti muista verkoista. Fyysisellä eristämisellä tarkoitetaan OSI-mallin ensimmäisen (fyysisen) kerroksen tasolla tapahtuvaa erottelua. (Katakri, 2020.)

Tuotantoverkkojen tiukka identiteetin- ja pääsynhallinta (IAM) ja käyttöoikeuksien hallinta (acccess control). Tietoliikenneverkon segmentointi ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti. (Katakri, 2020.)

Käyttäjiltä vaaditaan vahvoja tunnistautumismenetelmiä. Vain valtuutetuilla käyttäjillä tulisi olla pääsy arkaluontoisiin järjestelmiin ja toimintoihin ja järjestelmät erotetaan muista siihen ei kuuluvista järjestelmistä. OT-laitteiden ja järjestelmien fyysinen turvallisuus on tärkeää. Tilat tulee olla tiukastivalvottuja esimerkiksi valvontakameroilla, kulunvalvonta- sekä hälytysjärjestelmillä. Fyysisiin laitetiloihin pääsy rajataan ainoastaan valtuutettuihin henkilöihin, jotta estetään luvattomat pääsyt laitteisiin ja järjestelmiin. (Katakri, 2020.) Fyysinen turvallisuus ei rajoitu ainoastaan rakeenteelliseen turvallisuuteen vaan, myös palvelinten ja päätelaitteiden fyysiseen tietoturvaan on otettava huomioon. Laitteiden tietoturvallisuutta voidaan parantaa esimerkiksi käyttämällä laiteautentikointia, kuten Radiuspalvelinta, USB porttien poistamista tai rajoittamista ja langattoman verkonkortin ja Bluetooth komponenttien poistamista. (Jurvanen, 2023.)

Eristetyssä verkossa suoritetaan verkon valvontaa. Tuotantoverkon laitteiden ja järjestelmien tulisi tallentaa lokeja ja parhaassa tapauksessa lähettää niitä valvontaa suorittavalle osapuolelle esim. kybervalvomoon. Valvonnan ja lokien avulla pystytään tunnistamaan ja reagoimaan uhkiin. Lisäksi tämä avustaa jälkeenpäin tehtävää tutkimusta ja vianselvitystä. (Jurvanen,2023.)

Yleinen eristettyjen ympäristön ongelmana on päivittäminen. Haittaohjelmatunnisteiden tulisi olla ajan tasalla. Päivitykset eristettyyn ympäristöön voidaan toteuttaa esimerkiksi käyttämällä hallittua suojattua päivitystenhakupalvelinta, jonka tunnistekanta pidetään ajan tasalla esimerkiksi erillisestä Internetiin kytketystä järjestelmästä, josta tunnisteet voidaan siirtää käsin kohde ympäristöön tai vaihtoehtoisesti tuomalla tunnisteet hyväksytyn yhdyskäytäväratkaisun kautta. Tuodessa internetistä päivityksiä suljettuun ympäristöön, eheyden tarkistaminen (lähde, tarkistussumma, allekirjoitukset) on tärkeää. (Katakri, 2020.)

### 2.3.2 Verkoneristyksen testaaminen

Verkoneristyksen testauksella etsitään mahdollisia aukkoja suljetusta verkosta. Tämä on usein työlästä ja vaatii tuntemusta verkkotekniikoista ja protokollista. Eristyksentestauksen tavoite on kartoittaa koko eristetty verkko eli verkon osoiteavaruudet ja segmentit sekä tunnistaa mitä kaikkia laitteita ja järjestelmiä sinne on kytketty. Yleisimpiä verkkojentestaus ja analysointityökaluja ovat Wireshark ja Nmap.

Wireshark on avoimeen lähdekoodiin perustuva pakettianalysaattori. Wiresharkilla voi kaapata tietoliikennettä ja analysoida siellä liikkuvia paketteja. Wireshark esittää siepatun pakettidatan mahdollisimman yksityiskohtaisesti. (What Is Wireshark and How Is It Used, n.d.)

Nmap on avoimeen lähdekoodiin perustuva Linux komentorivityökalu, jota käytetään verkkojenskannaukseen. Nmap skannaa verkkojen IP-osoitteet ja avoimia portteja ja niiden takana olevia ohjelmia ja sovelluksia. Nmap avulla voidaan helposti selvittää verkossa olevat laitteet ja niiden osoitteet sekä avoimet portit ja tämän myötä löytää haavoittuvuuksia. Nmapia käytetään usein penetraatiotestauksessa. (Shivanandhan, 2020.)

Näiden yleisimmin käytettyjen analysointityökalujen heikkous verkoneristyksen testaamisessa on hitaus ja työläys, joka aiheutuu siitä, että nämä työkalut eivät ole automatisoituja. Suurien ja monimutkaisten verkkojen analysointi vaatii erityisosaamista ja siihen kuluu paljon työtunteja. Tästä huolimatta verkkoon voi jäädä aukkoja, joita ei testauksessa huomattu. Automaattiseen eristyksen testaukseen ei ole kehitetty montaa teknologiaratkaisua. Suomalainen SensorFu Beacon on yksi näistä sekä israelilainen XmCyber tuote.

Xmcyber etsii automaattisesti hyökkäysreittejä ja yrittää paljastaa hyökkäystekniikat, joita voidaan käyttää tunkeuduttaessa kriittiseen verkkoon. (Heikkinen, 2022.) Teknologia replikoi hyökkääjän toimintoja ja tekniikoita etsien haavoittuvuuksia verkosta ja ympäristöstä. Näihin sisältyy esimerkiksi verkon aukkojen etsiminen. (XM Cyber Breach and Attack Simulation,2020.)

# 3 Toteutus ja tulokset

Opinnäytetyön viitekehyksenä oli eristettyjen tietoverkkojen turvallisuuden testaaminen sekä eristyksen ja eheyden varmistaminen. Tässä työssä tavoitteena oli pilotoida verkkojen automaattisen eristyksentestausjärjestelmän Beaconin SensorFu käyttöönottoa. Toteutus tehtiin systemaattisesti seuraavin vaihein: 1) järjestelmään perehtyminen, 2) asentaminen ja käyttöönotto, 3) hälytysten ja lokien lähettämisen testaus ja 4) käyttökohteiden kartoittaminen puolustusvoimissa.

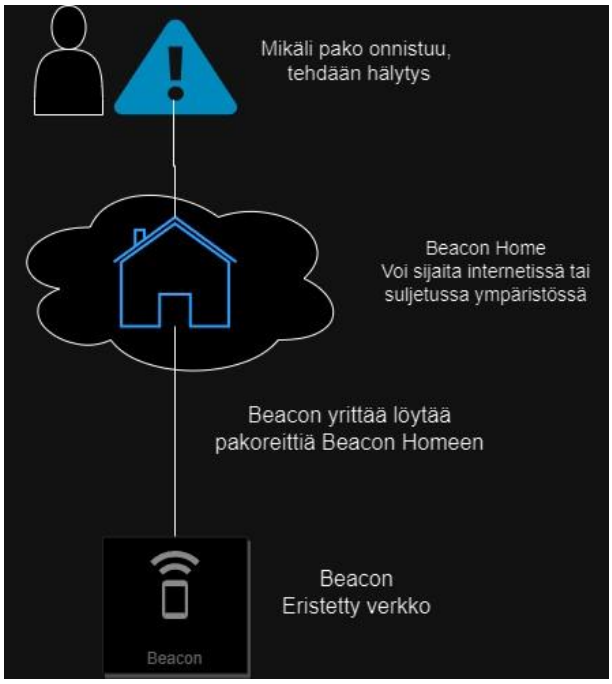
Verkoneristyksentestauksen tarpeeseen Suomen Ilmavoimat tekivät alustavan hankinnan ja tuotekartoituksen SensorFu yritykseltä. SensorFu Oy on vuonna 2017 perustettu oululainen kyberturvallisuusyritys. Yrityksessä työskentelee noin 10 työntekijää. (Lukka P. 2022.) Osa SensorFu perustajista ja työntekijöistä oli vuonna 2014 mukana tutkijaryhmässä, joka löysi vakavan Heartbleed-haavoittuvuuden Yrityksen päätuote, on Beacon eristyksentestausjärjestelmä. SensorFu asiakkaita ovat muun muassa Suomen Ilmavoimat, Kyberturvallisuuskeskus, Erillisverkot, Synopsys ja Seagate. SensorFu asiakasryhmä koostuu yrityksistä ja tahoista, jotka käsittelevät työssään teollisuuden ohjausjärjestelmiä, automaatioverkkoja, turvakamerajärjestelmiä, hallintaverkkoja sekä muita kriittisiä verkkoympäristöjä, jotka tarvitsevat suojausta kellon ympäri. (Sensorfu, n.d) Puumalainen (2021) toteaa, että SensorFu Beacon on helposti käyttöönotettava kriittisten tietojärjestelmien palohälytin, joka pohjautuu yhtiön perustajien vuosien kokemukseen tietoturvan ja tietoverkkojen toimintavarmuuden kehittämiseksi (Nordic Option sijoittaa SensorFun kansainvälistymiseen, 2021).

Vuonna 2021 SensorFu sai päätöksen 610 000 euron rahoituskierokseen nopeuttaakseen laajenemista kansainvälisille markkinoille (Nordic Option sijoittaa SensorFun kansainvälistymiseen, 2021). Vuonna 2022 yrityksen liikevaihto oli reilut 326 000 euroa ja vuonna 2023 reilut 430 000 euroa. (Finder, 2023.)

## 3.1 Beacon-järjestelmään perehtyminen

SensorFu on kehittänyt tietoverkkojen eristyksen toimivuuden automaattisen testauksen ratkaisun Beaconin, helpottaakseen yritysten tietoturvaa. Eristyksentestausjärjestelmän tavoitteena on havaita verkkovuodot ennen niiden hyödyntämistä. Eristyksentestausjärjestelmä luo kyvykkyyden

verkon eristyksen toimivuuden jatkuvalle valvonnalle. (Toteutettavuustutkimus: Yritysten tietoturvaa voi parantaa helposti, 2020.) Verkkojen eristys on yksi tärkeimmistä tietoturvakontrolleista korkean turvallisuuden tietoverkoissa. Beacon automatisoi normaalisti käsin tehtävän eristyksen testauksen ja tuottaa hälytyksiä löytyvistä vuotokohdista. Eristyksentestausjärjestelmän tavoitteena on havaita verkkovuodot ennen niiden hyödyntämistä. Beacon valvoo eritettyjen ja eristettyjen verkkojen tilaa etsimällä pääsyä kiellettyihin verkkoihin. Beacon yrittää soittaa erilliseen määritettyyn Home-verkkoon. Mikäli Beacon löytää reitin Home-verkkoon, käyttäjä saa siitä hälytyksen. (Beacon By SensorFu, n.d.)




Kuvio 2 Beacon toimintaperiaate

### 3.1.1 Beacon komponentit

Beacon on suunniteltu toimimaan Internetistä eristetyissä järjestelmissä mukaan lukien on-premise ja AirGap ympäristöt. Järjestelmä koostuu kahdesta komponentista, Beacon ja Beacon-Home.

Beacon, on agentti, joka asennetaan eristettyyn verkkoon. Agentti pyrkii jatkuvasti eri tekniikoilla ottamaan yhteyttä Beacon Homeen. Agentti voidaan asentaa kohdeverkkoon joko sovelluksena, virtuaalikoneena tai laitteena. Palvelinkomponentti ei vaadi kaksisuuntaista yhteyttä eristettyyn verkkoon asennettuihin komponentteihin. (SensorFu Oy:n Vastaus tietopyyntöön, 2023.)

Beacon Home on palvelin, jota kohti Beacon pyrkii pakenemaan ulos eristetystä verkosta. Home kuuntelee verkkoliikennettä ja pyrkii havaitsemaan eristetystä verkosta tulevat yhteydet. Home toimii vastaanottimena Beacon pakoyrityksille sekä hallintakäyttöliittymänä koko SensorFu Beacon asennukselle. Home Apista voidaan hallita Beaconeja sekä tehdä näiden esikonfigurointi ja seurata hälytyksiä. Home voi olla fyysinen tai virtuaalinen asennus. Home-komponentteja voi olla useita, esimerkiksi paikalliseen konesaliin asennettu Home-komponentti ja julkiseen internetiin asennettu Home-komponentti. Beacon Home -komponentissa on HTTP-rajapinta sekä käyttöliittymää, että ohjelmistorajapintaa (API) varten. Rajapinta on suojattu TLS-protokollalla. Beacon pystytään liittämään erilliseen SIEM-järjestelmään salatusti HTTP API:n tai Webhookien avulla. Loki- ja hälytysdata välitetään salattuna. (SensorFu Oy:n Vastaus tietopyyntöön, 2023.)

### 3.1.2 Beacon verkoneristyksen testausmenetelmät

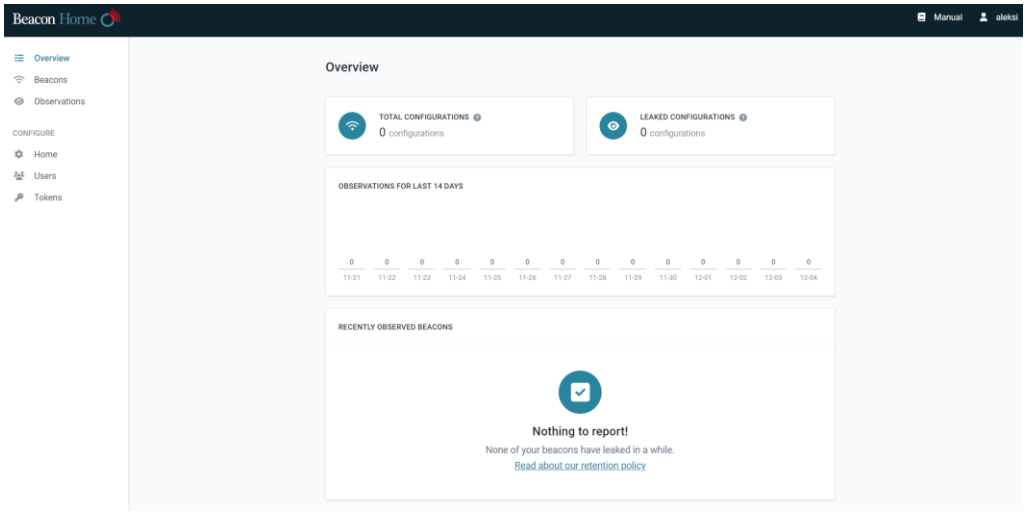
Beacon tukee useita erilaisia teknisiä testausmenetelmiä verkon eristyksen testaukseen. Testausmenetelmissä tuetaan sekä IPv4- että IPv6-prokollia. Rinnakkain suoritetaan kaksi testisykliä, nopea ja hidas. Nopea sykli testaa tärkeitä käsin valittuja näkyvimpiä pakopaikkoja. Tämä sisältää muutamia kymmeniä tärkeimpiä TCP- ja UDP-portteja sekä pakopaikkoja, kuten DNS, ICMP ja Broadcast. Nopea sykli kestää noin 30 minuuttia. Hitaan silmukan tarkoituksena on luetella kaikki TCP- ja UDP-portit (1–65535) aiheuttamatta liikaa kohinaa verkossa. Konfiguraatiosta riippuen yksi hitaan silmukan sykli kestää noin 4–8 päivää. (Escape Methods, n.d.) Kun pako on onnistunut Beacon lähettää välittömästi hälytyksen käyttämällä kodinhallintakäyttöliittymässä määritettyjä asetuksia. Jokainen havainto ja hälytys Homessa vastaa yhtä näistä murtautumismenetelmistä. Tämän lisäksi kyseinen pakotekniikka menee jäähylle noin 1.5 tunniksi. Jos pakotyyppi on jo jäähyllä, hälytystä ei lähetetä ja viilennystä jatketaan uudella jäähdytyksellä. Tällä estetään useiden samanlaisten hälytysten lähettämistä ja ruuhkautumista (Alerts, n.d)

Beacon lähettää pingejä kohti Home komponenttia, yrittäen etsien reittiä ulos eristetystä verkosta. Ping sisältää ainoastaan pakollisen tiedon, jotta Home ymmärtää mistä ping tuli, kuka sen lähetti ja minne se lähetettiin. Jos Home saa pinging, se tarkastaa pingin tiedon ja nostaa hälytyksen, josta loppukäyttäjä saa tiedon. Sensofun tekemä ping ei ole sama kuin perustietotekniikassa käytetty ping-komento tai ICMP echo paketti. Beacon ping paketti sisältää seuraavat tiedot, Beaconin ennalta määritelty nimi, järjestysnumero ja objecti nimeltä ”kind”. Objecti vastaa, minkälainen

ping on kyseessä ja se sisältää käytetyn protokollan, kohde IP-osoitteen ja valinnaisesti kohde portin. Kind objectin avulla voidaan käyttää port forwardaamista ja IP uudelleenohjausta Homeen. Onnistuneesta vuodosta saadaan mm. seuraavia tietoja: vuotaneen beaconin nimi, lähde- ja kohdeosoite, mahdollinen pako-osoite, portti tai protokollanumero, verkkohyppyjen määrä (hop count) sekä tieto onko vuoto yksisuuntainen (eristetystä verkosta ulos) vai kaksisuuntainen (eristetystä verkosta ulos ja takaisin sisään). (Herrala, 2017.)

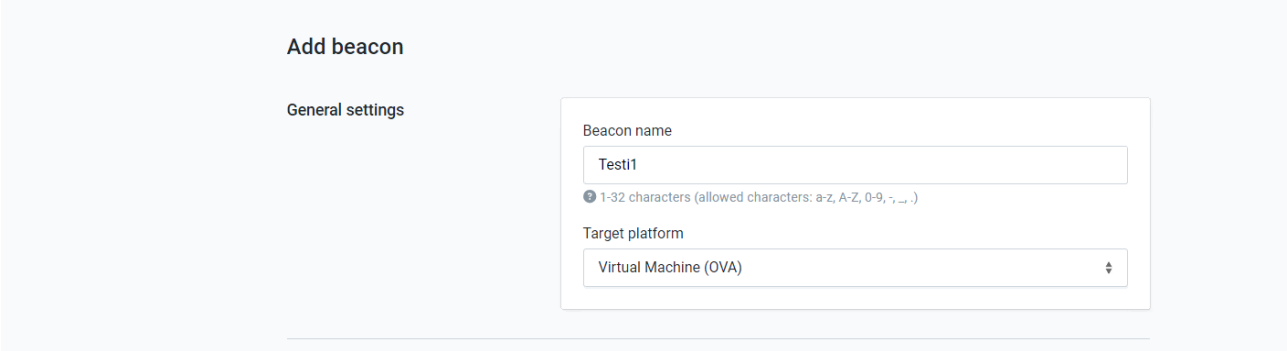
## 3.2 Beacon asennus ja käyttöönotto

Eristyksentestausjärjestelmä Beacon asennetaan ja otetaan käyttöön kirjautumalla Beacon Home -palveluun. Home toimii hallintakäyttöliittymänä, josta voidaan hallita Beaconeja sekä valvoa vuotavia verkkoja. Tämän lisäksi Home toimii myös käyttäjienhallintatyökaluna. Beacon Home voi sijaita julkisessa verkossa kuten pilviympäristössä tai se voidaan asentaa erikseen suljettuun ympäristöön.



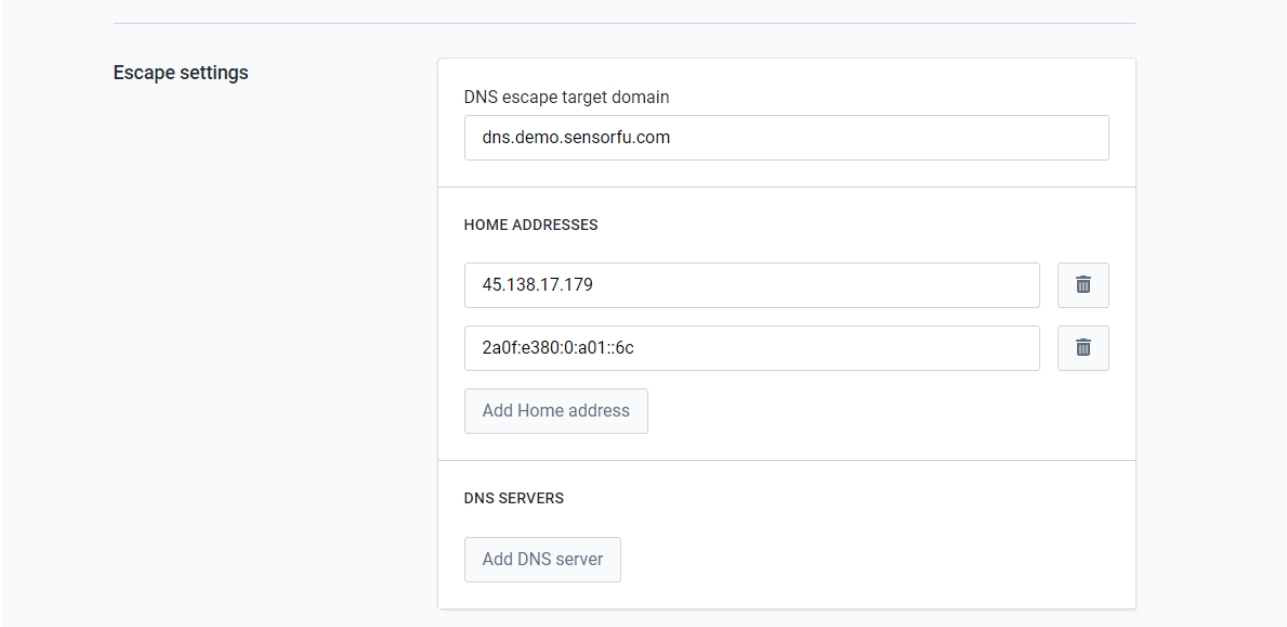

Kuvio 3 Beacon Home

Tässä tapauksessa Beacon asennusta ja toimintaa on testattu tuotteen toimittajan demoympäristössä, jolloin Home-komponentti sijaitsee julkisessa verkossa. Uusi Beacon voidaan lisätä kohdasta Beacon -> Add Beacon. Beaconille annetaan nimi ja valitaan sopiva ympäristö pudotusvalikosta, jolle se asennetaan. Beacon voidaan asentaa Rasperry Pi, Linux sovelluksena, Windows sovelluksena tai VMware ESXi, VMware workstation, KVM tai Virtualbox virtualisointialustalle.



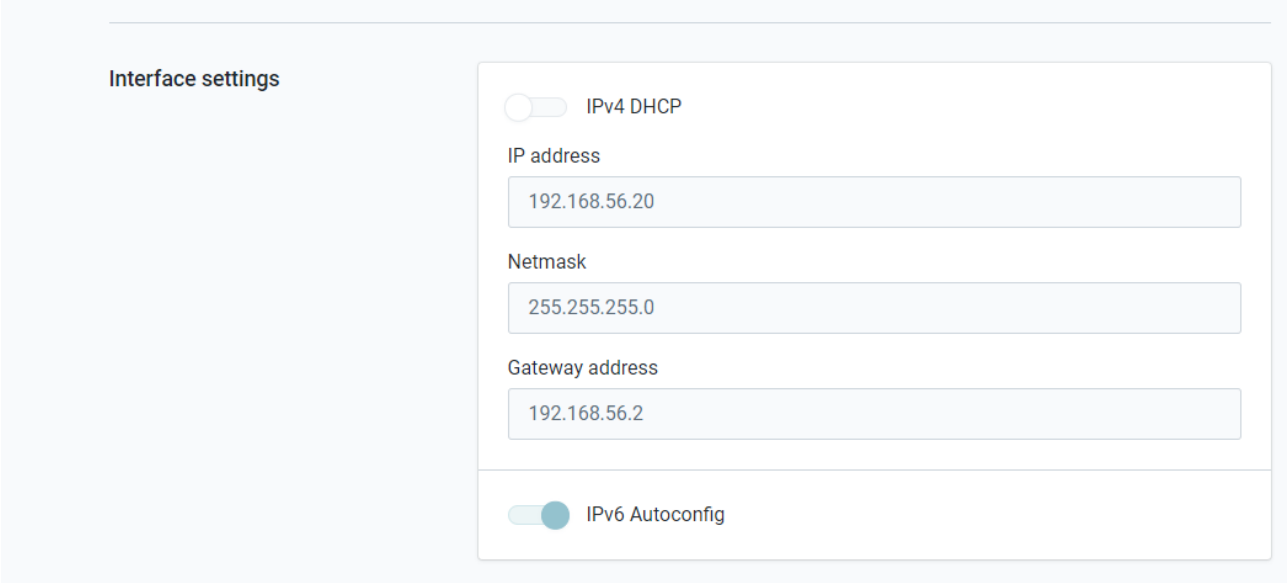

Kuvio 4 Uuden Beacon lisääminen

Tämän jälkeen Beaconille määritellään pakoasetukset. Asetetaan kohde domain-osoite sekä Homen IP-osoite, joita kohti Beacon pyrkii pakenemaan eristetystä verkosta. Tämän lisäksi voidaan lisätä DNS osoitteita. (katso kuvio 5).

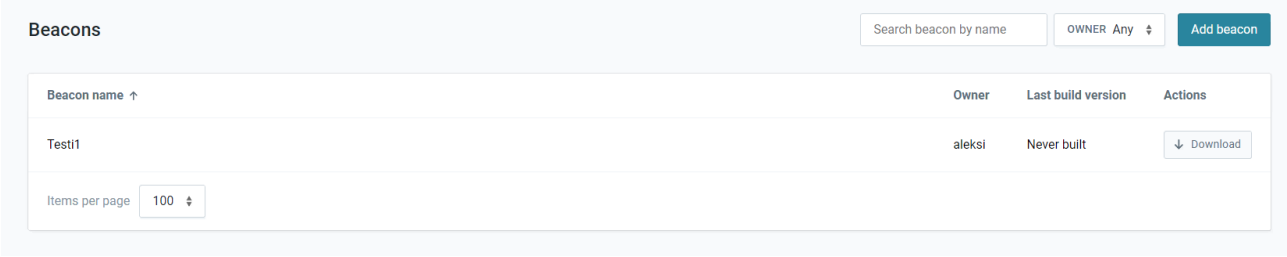



Kuvio 5 Beacon pako asetukset

Viimeiseksi Beaconille määritellään verkkoasetukset. Beaconille voidaan asettaa DHCP päälle tai manuaalisesti lisätä osoite, verkkomaski sekä yhdyskäytävä.

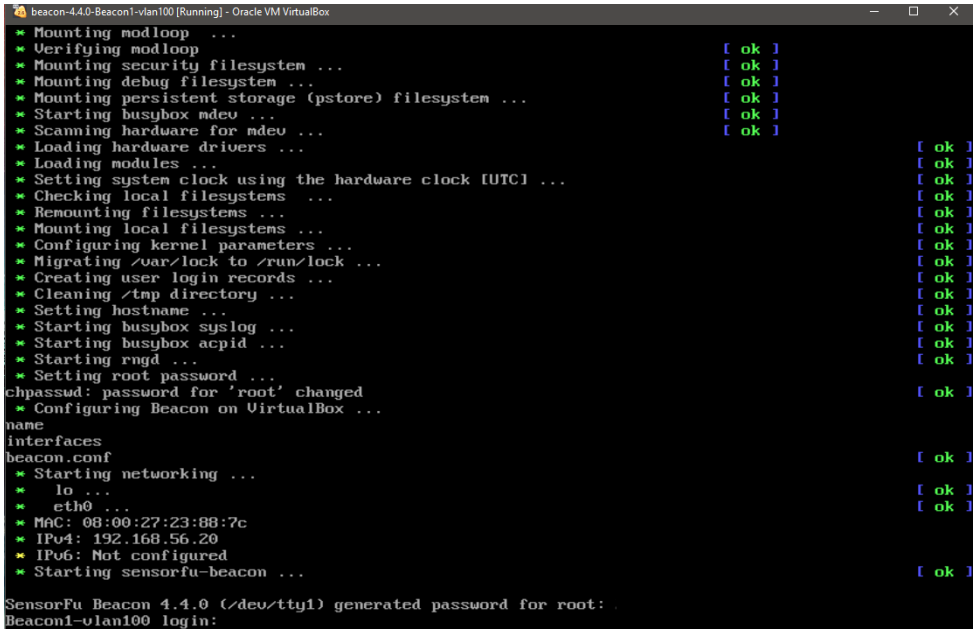



Kuvio 6 Beacon verkkoasetukset

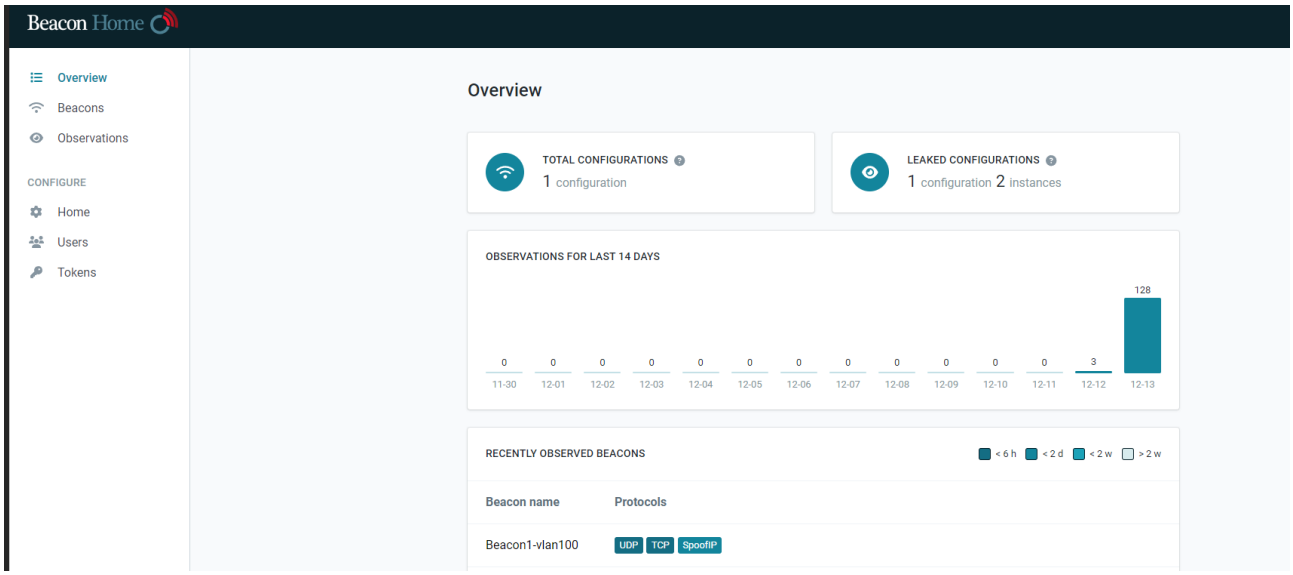



Kuvio 7 Beacon valmis ladattavaksi

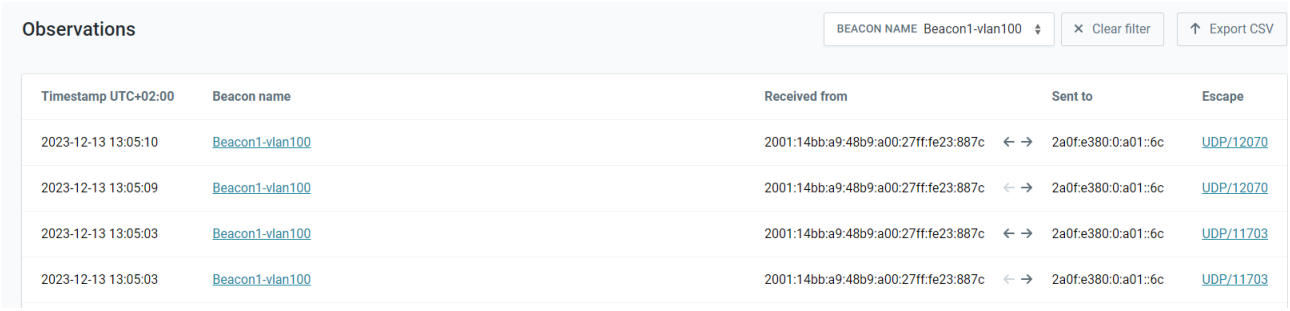
Verkko- ja pakomääritysten jälkeen Beacon voidaan ladata Download kohdasta ja siirtää eristettyyn kohdeympäristöön. Kun Beacon on asennettu kohdeympäristöön se alkaa automaattisesti jatkuvalla testauksella etsimään pakoreittiä kohti Beacon Home komponenttia käyttämällä edellisessä vaiheessa määriteltyjä asetuksia. Jos pako onnistuu, Beacon Home tulee siitä ilmoitus (katso kuvio 9). Observation valikosta voidaan tarkastella hälytyksiä ja vuotoja tarkemmin sekä pakomenetelmää (katso kuvio 10 ja 11). Lisäksi pakomenetelmää kilkkaamalla saadaan tarkempia tietoja siitä ja mahdollisia syitä sekä korjausehdotuksia (katso kuvio 12).



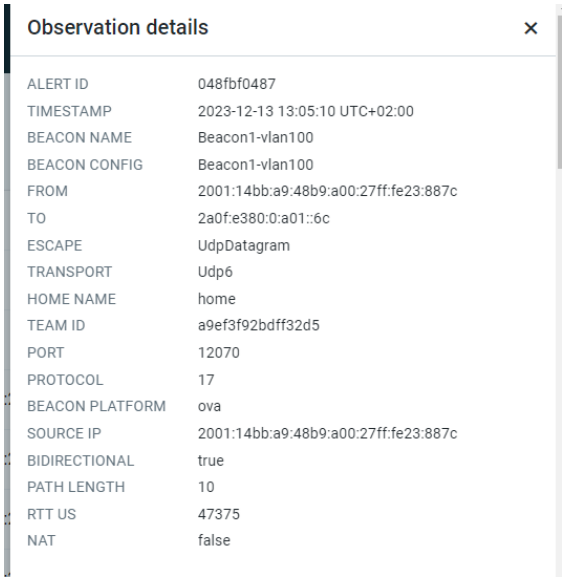

Kuvio 8 Beacon asennettu virtuaalikoneelle



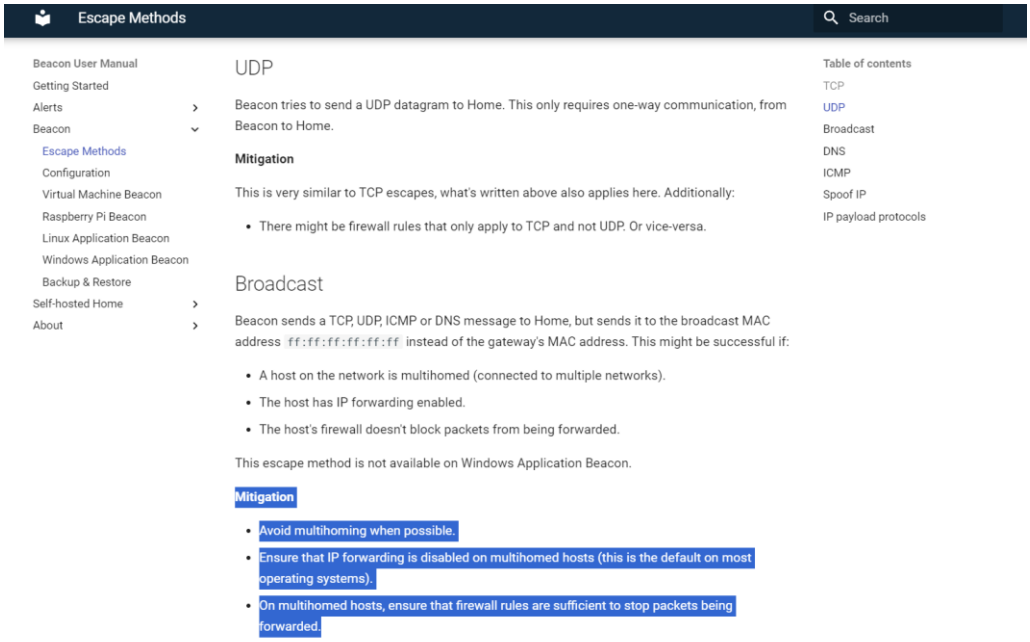

Kuvio 9 Hälytys Beacon Home-komponentissa




Kuvio 10 Beacon Observations




Kuvio 11 Observation details




Kuvio 12 Pakomenetelmän tiedot

### 3.2.1 Asennuksen ja käyttöönoton vaiheeseen liittyvät havainnot

Testiympäristössä käytössä oli ainoastaan demoympäristö, jossa Home-komponentti sijaitsi SensorFu ylläpitämässä pilvipalvelussa. Näiden testien perusteella eristyksentestausjärjestelmän asentamiseen ei tarvitse henkilökunnalta lisäkoulutusta vaan SensorFu tuottama manuaali on tarpeeksi kattava asentamiseen. Beaconin asentaminen eristettyihin ympäristöihin on nopeaa ja yksinkertaista. Beaconin asentaminen ei vaikuta muun päivittäiseen toimintaan eikä palveluita tarvitse keskeyttää asettamisen ja käyttöönoton ajaksi.

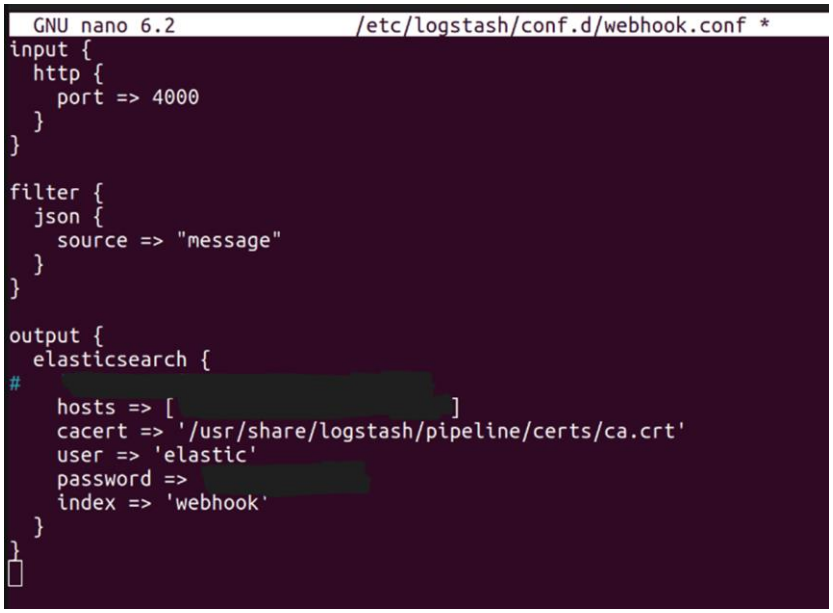
## 3.3 Beacon hälytysten ja lokien lähettämisen testaus

SensorFu Beacon Home tuottaa lokitietoa havaituista eristetyn verkon vuodoista sekä Homen itsensä toimintaa seuraavaa lokitietoa. Beacon Home tallentaa lokitiedot käyttöjärjestelmän lokituspalveluun (Journald ). Vuotoihin liittyvän lokitiedon pystytään siirtäään TLS:llä suojattua HTTP API -rajapintaa hyödyntäen toiseen järjestelmään kuten erilleselle SIEM järjestelmälle tai sähköpostiin. (SensorFu Oy:n Vastaus tietopyyntöön, 2023.)

### 3.3.1 Beacon lokien säilyttäminen ja integroiminen kybervalvomoon

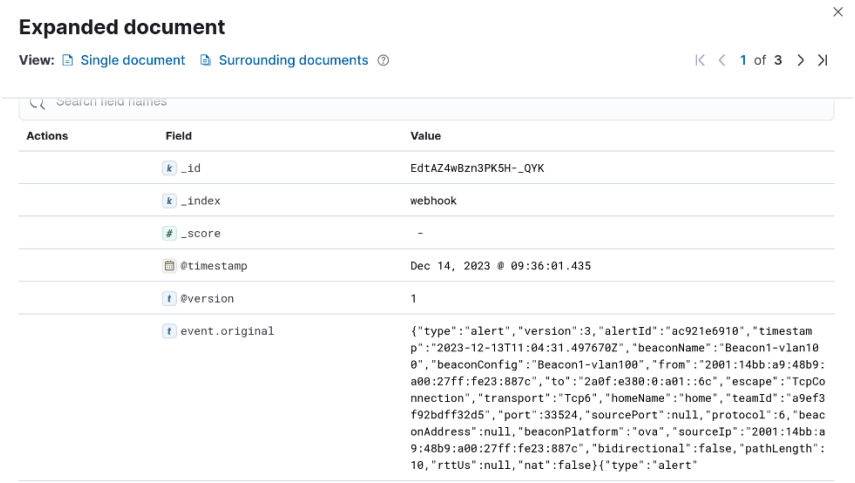
Beacon Home ei ole suunniteltu pitkäaikaiseen lokien säilyttämiseen, vaan tämä tulee delegoida erilliselle SIEM-järjestelmälle hälytysintegroinnin tai Observations Token APIn kautta. Hälytykset voidaan integroida kybervalvomoiden näkymiin. SIEM järjestelmänä voidaan käyttää esimerkiksi ELK Stack (Elastic Logstash Kibana) tai Splunk. Beacon Home havaintojen ja hälytysten säilytysaika on 30 päivää ja enimmäismäärä on 2500000 havaintoa. (Alerts, n.d.)

Jotta hälytykset saadaan integroitua kybervalvomon SIEM järjestelmään, tulee järjestelmään lisätä webhookeille konfiguraatio (Tiwari, 2023). ELK Stackilla webhook lokien vastaanottaminen onnistuu lisäämällä logstashiin uusi konfiguraatio webhookeille, jossa määritetään isännän (host) osoite, portti, sertifikaatit, käyttäjätunnukset ja indeksiksi webhook. Tämän jälkeen webhookit voidaan ottaa käyttöön Kibanassa. Kibanan discovery valikon alta valitaan data viewksi webhook. Beacon Home-komponentin hälytys asetuksiin lisätään Elasticin osoite, jonne hälytykset lähetetään. Nyt hälytykset saadaan suoraan Kibanaan ja voidaan integroida kybervalvomon näkymiin Dashboardien avulla.

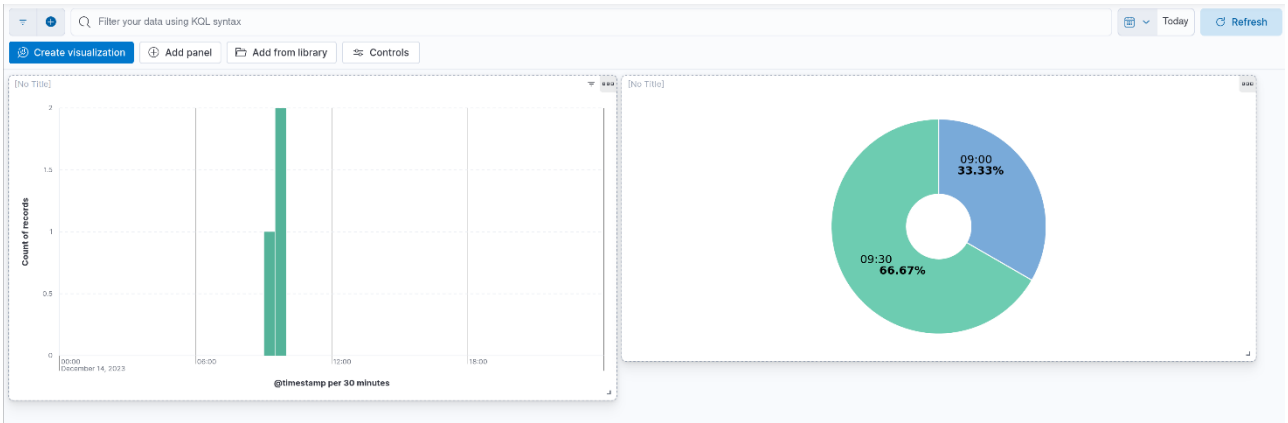



Kuvio 13 Webhook.conf


Kuvio 14 Hälytykset Kibana discovery näkymässä




Kuvio 15 Kibana alert expanded



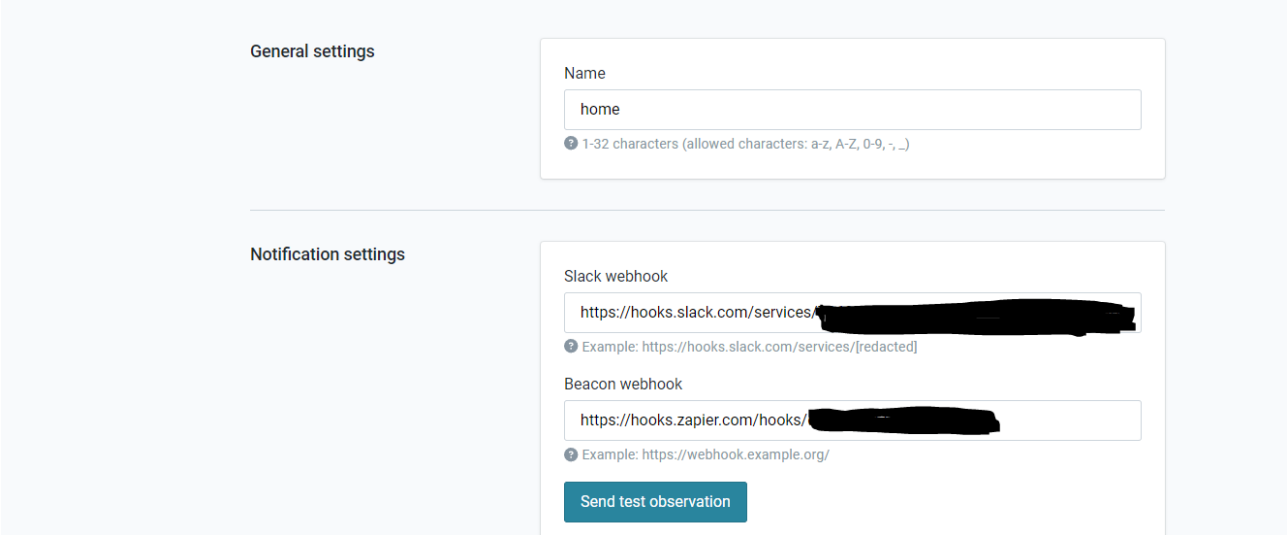

Kuvio 16 Hälytykset Kibana Dashboards näkymässä

### 3.3.2 Hälytysten lähettäminen sähköpostiin

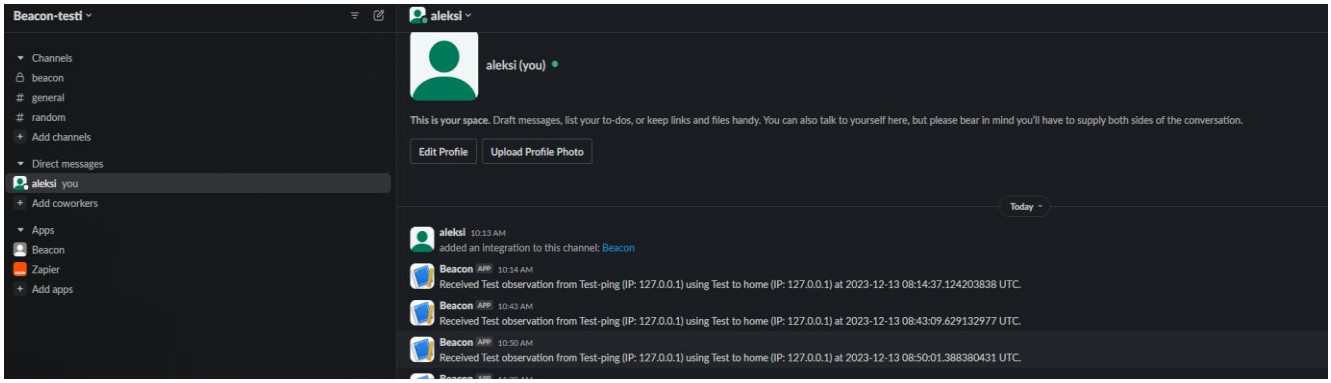
Hälytyksiin nopean reagoinnin takaamiseksi ne voidaan lähettää Beacon Homen lisäksi webhookkejen avulla sähköpostiin, jolloin käyttäjien ei tarvitse valvoa Home näkymää aktiivisesti. (Beacon user manual, n.d). Webhook on HTTP-pohjainen takaisinsoittotoiminto, joka mahdollistaa kevyen, tapahtumapohjaisen viestinnän kahden sovellusohjelmointirajapinnan (API) välillä. Useat verkkosovellukset käyttävät webhookeja pienten tietomäärien vastaanottamiseen muista sovelluksista. (What is a webhook, 2022.)

Beacon Configure Home valikon alta voidaan muokata, minne hälytykset lähetään. Valittavan on kaksi kohtaa, Slack webhook, joka lähettää hälytykset Slack työtilaan ja Beacon webhook, joka lähettää hälytykset mille tahansa HTTP-palvelimelle JSON POST -pyyntönä. Send test observation kohdasta voidaan testata hälytysten lähettävyyden toimivuutta.

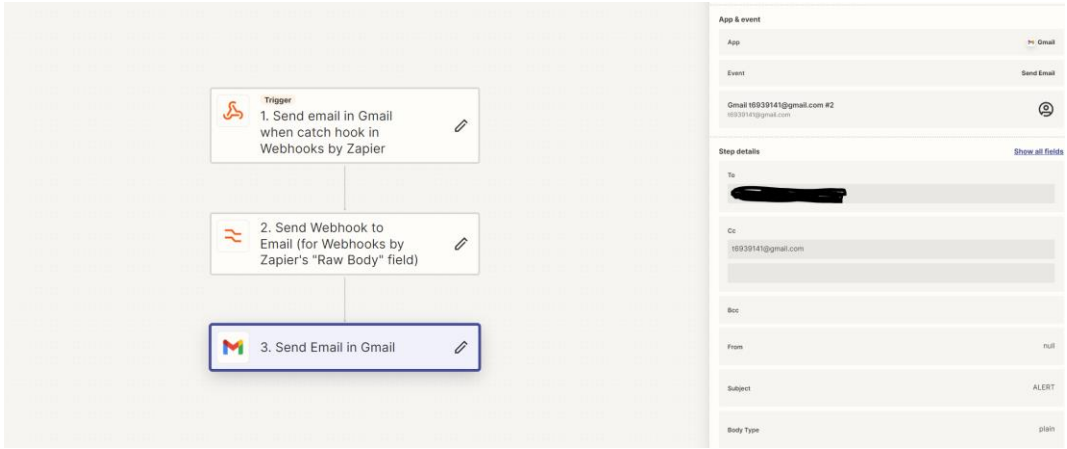
Hälytykset voidaan lähettää esim. Slack ympäristöön, jolloin tieto hälytyksistä saadaan nopeasti halutuille osapuolille. Slackista hälytyksiä voidaan myös lähettää esimerkiksi sähköpostiin tai tekstiviestillä käyttäjälle. Sähköpostiin viestit voidaan automatisoida esimerkiksi Zapier työkalun avulla. Sähköpostiin tulevia hälytyksiä voidaan myös parsia Zapierin avulla.



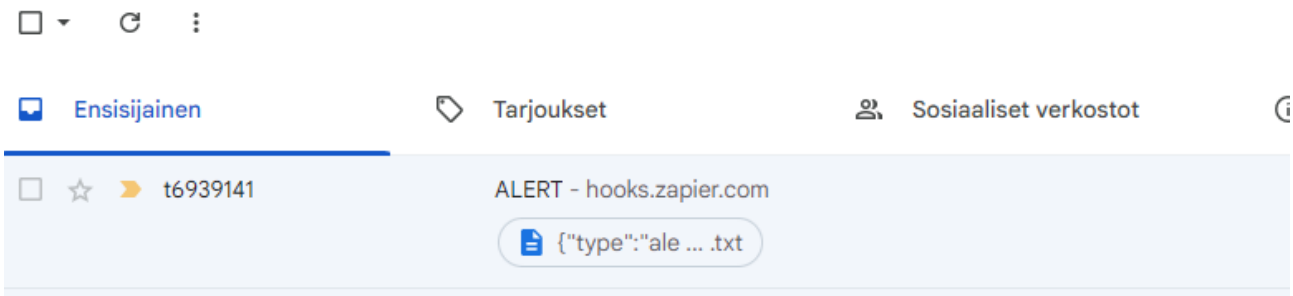

Kuvio 17 Hälytysten lähettäminen webhookeilla




Kuvio 18 Slack työtila




Kuvio 19 Zapier sähköposti asetukset




Kuvio 20 Hälytys sähköpostiin

{"type":"alert","version":3,"alertId":"09057b7ad5","timestamp":"2023-12-13T10:13:46.4446374222","beaconName":"Test-ping","beaconConfig":"Test-ping","from":"127.0.0.1","to":"127.0.0.1","escape":"Test","transport":"Test","homeName":"home","teamId":"a9ef3f92bdff32d5","port":null,"sourcePort":null,"protocol":null,"beaconAddress":null,"beaconPlatform":null,"sourceIp":null,"bidirectional":null,"pathLength":null,"rttUs":null,"nat":null}

Kuvio 21 Hälytys sähköpostiviestin liitteenä

### 3.3.3 Havainnot hälytysten ja lokien lähettämisestä

Beacon hälytyksiä voidaan webhookkien avulla lähettää esimerkiksi sähköpostiin, jolloin niihin reagoiminen on varmempaa. Hälytysten lähettäminen webhookkien avulla on yksinkertaista eikä vaadi ylläpidolta paljoa työtä.

Beacon tuottamien lokien ja hälytysten vieminen erilliselle SIEM järjestelmälle ei tuottanut ongelmia. Hälytykset saatiin onnistuneesti integroitua Kibanan dashboard näkymiin, joita voidaan räätälöidä sopiviksi kybervalvomo käyttöä varten.

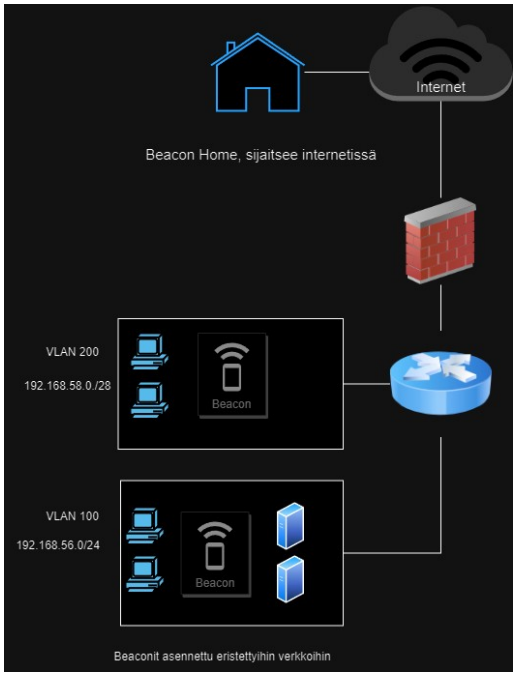
## 3.4 Beacon käyttökohteet puolustusvoimissa

Puolustusvoimissa kriittisiä verkkoja valvotaan tiukasti. Monet verkot ovat vahvasti eristettyjä mutta huomaamattomia konfiguraatio virheitä on voinut syntyä versioiden päivitysten yhteydessä. Automaattinen eristyksentestausjärjestelmä auttaa parantamaan tietoturvaa ja löytämään virheelliset konfiguraatiot, jonka myötä verkoista saadaan entistä turvallisemmat.

Automaattisen eristyksentestausjärjestelmän Beaconin käyttöönotossa tulee tunnistaa kohde ympäristöt, jonne Beacon sekä Home asennetaan. Kohde ympäristöt ovat eristettyjä arkaluontoisia verkkoja, joita halutaan valvoa. Ympäristöistä tulee olla tiedossa, mitkä ovat sallittuja verkkoja ja mitkä eivät sekä mitä laitteita kyseisiin verkkoihin kuuluu.

Tietoverkkojen eristyksen toimivuuden automaattisen testauksen ratkaisulle on puolustusvoimissa tunnistettu käyttökohteiksi muun muassa vuodot internettiin, järjestelmien välinen vuoto, yhdyskäytävien yli menevät vuodot, järjestelmien verkkosegmenttien sisäiset vuodot sekä työasemien oikean käytön varmistaminen.

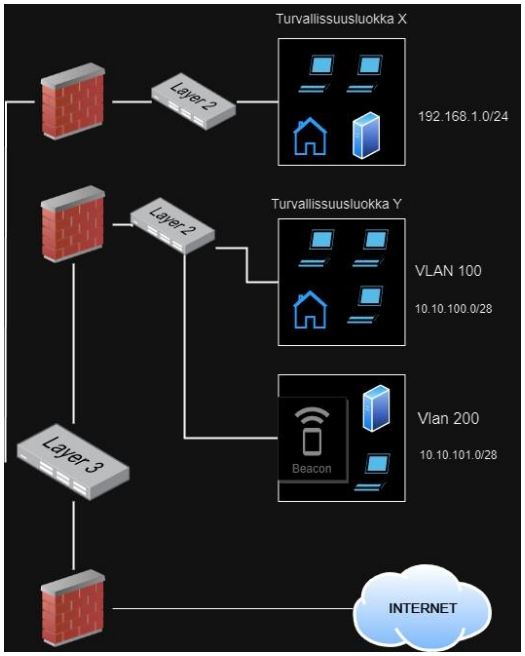
Peruslähtökohta on, että eristetyistä verkoista ei koskaan haluta liikennöidä julkiseen internettiin. Beaconilla voidaan valvoa eristettyjen verkkojen vuotoja internettiin päin, jolloin Beacon Home instanssi sijaitsee pilvessä olevalla palvelimella, jonne Beacon pyrkii pakenemaan. Beacon asennetaan eristettyyn verkkoon, jolle asettaan Home instanssi pako kohteeksi.




Kuvio 22 Verkon vuotojen valvonta julkiseen verkkoon päin

Eristyksentestausjärjestelmällä voidaan valvoa eri järjestelmien välillisiä vuotoja. Toisistaan eristettyjen järjestelmien välisen eristyksen varmistaminen, jotka käyttävät samaa runko- tai liityntäverkkoa. Näiden järjestelmien välillä ei ole tarvetta liikennöidä, Beaconin avulla voidaan varmistaa, että liikenne ei kulje ristiin. Järjestelmien työasemia ei saa käyttää ristiin, jolloin tällä voidaan varmistaa työasemien käyttö vain oikeissa ympäristöissä.

Yksisuuntaisia yhdyskäytäviä eri turvaluokan verkkojen välillä ja halutaan varmistaa, ettei tieto vuoda väärään suuntaan. Lisäksi varmistetaan verkkosegmenttien eheys. Valvotaan, että segmenttien verkkoliikenne kulkee vain sallittujen segmenttien välillä. Tämä tarkoittaa esimerkiksi sitä, että työasemaverkosta ei pääse liikennettä järjestelmän hallintaverkon segmenttiin. Jokaisella segmentillä on erilliset hallintaverkot. Beacon Home voidaan asentaa tässä tapauksessa suljettuun ympäristöön toiseen segmenttiin, jota kohden Beacon pyrkii pakenemaan.




Kuvio 23 Verkon vuotojen valvonta segmenttien välillä

Työasemien käytön varmistamine ainoastaan niille tarkoitetuissa ympäristöissä. Näitä ovat esimerkiksi erillistyöasemat, joita ei saa kytkeä internettiin sekä yhden järjestelmän hallintaan tarkoitetut työasemat. Beaconilla voidaan valvoa, että kyseiset työasemat eivät keskustele halutun verkon ulkopuolelle.

### 3.4.1 Havainnot käyttökohteista

Beaconille tunnistetut käyttökohteet puolustusvoimissa ovat relevantteja. Näillä käyttökohteilla pystytään kattamaan puolustusvoimien tarve kriittisten turvallisuusverkkojen eheyden varmistaminen, vuotojen valvonta sekä työasemien oikea käyttö.

# 4 Pohdinta

Tämän opinnäytetyön tavoitteena oli pilotoida verkkojen automaattisen eristyksentestausjärjestelmän Beacon käyttöönottoa. Opinnäytetyön viitekehyksenä oli eristettyjen tietoverkkojen turvallisuuden testaaminen sekä eristyksen ja eheyden varmistaminen. Työ toteutettiin systemoidusti vaiheiden kautta.

Opinnäytetyön tulokset vahvistavat aikaisemmin tutkittua tietoa, joka osoittaa, että kriittisten eristettyjen infrastruktuurin tietoverkkojen kyberturvallisuus on elintärkeää yhteiskunnan toiminnan kannalta nyt ja tulevaisuudessa. Isoimmat turvallisuusriskit eristetyissä verkoissa ovat vahingossa syntyneet konfiguraatiovirheet, jolloin verkkoon on jäänyt huomaamattomia aukkoja. Aikaisempi tutkimusnäyttö tukee oletusta, että kriittisesti tärkeiden verkkojen tietoturvallisuutta voidaan parantaa automaattisen eristyksentestauksen järjestelmillä. (Yritysten tietoturvaa voi parantaa helposti, 2020.)

Opinnäytteessä käytetty Beacon-järjestelmä ei edellytä henkilökunnalta lisäkoulutusta vaan järjestelmän valmistajan (SensorFu) tuottama käyttöohje on tarpeeksi kattava. Tämä mahdollistaa sen, että verkkojen eristyksentestausjärjestelmä voidaan käyttöönottaa ilman käyttäjäorganisaation laatimaa omaa erillistä ohjetta. Tämä ei kuitenkaan poissulje käyttöönottosuunnitelman vaadetta, joka on aina laajempi kuin käyttöohje ja huomioi käyttäjäorganisaation erityistarpeet ja toimintaympäristön.

Erityisenä vahvuutena nousi esille, että Beaconin asentaminen eristettyihin ympäristöihin on nopeaa ja yksinkertaista. Beaconin asentaminen ei vaikuta muun päivittäiseen toimintaan eikä palveluita tarvitse keskeyttää asettamisen ja käyttöönoton ajaksi. Lyhyellä testaus jaksolla Beaconin toimivuus osoittautui erinomaiseksi ainakin pilotoinnissa käytetyssä demoympäristössä. Beacon onnistui löytämään aukkoja verkoista, jotka vaikuttivat eristetyiltä.

Beacon testaa jatkuvasti eri pakomenetelmillä reittiä ulos eristetystä verkosta. Havaintona pilotissa nousi esille se, että järjestelmä tuottaa tämän vuoksi verkkoon ylimääräistä liikennettä, joka voi näkyä valvomonlokeissa. Beacon kokeilee usealle eri protokolla jokaista porttia läpi, joten se voi myös nostaa tarpeettomia hälytyksiä. Mikäli valvottavaan ympäristöön on asennettu monta Beaconia, verkkoliikenne moninkertaistuu. Liikenteen ja Beacon tuottaman lokien määrä tulee tämän vuoksi testata huolellisesti ennen käyttöönottamista.

## 4.1 Työn aineiston soveltuvuuden ja luotettavuuden arviointi

Työn luotettavuutta tarkastellaan yleensä reliabiliteetti ja validiteetti käsitteiden avulla. Reliabiliteetti kertoo, miten toistettavasti tutkimuksessa käytetty mittari mittaa kohteena olevaa ilmiötä. Validiteetti kertoo puolestaan, miten hyvin käytetty mittausmenetelmä mittaa kohteena olevaa

ilmiötä. (Tilastokeskus, n,d.) Tässä työssä luottavuuden arviointi reliabiliteetti ja validiteetti käsitteiden avulla ei ole relevanttia, koska työssä ei käytetty selkeitä mittareita.

Työn aineiston soveltuvuus ja luotettavuus voidaan arvioida korkeat kriteerit täyttäväksi. Käytetty eristyksentestausjärjestelmä on valikoitunut puolustusvoimien koekäyttöön tiukkojen standardien ja valintaprosessin kautta. Tunnistettavaa kuitenkin on, että eristyksentestausjärjestelmistä ei löydy paljoa tausta-aineistoa ja teoriakirjallisuutta, jota olisi voinut käyttää vertailussa toimittajan tuottamaan materiaaliin. Lisäksi tuotteesta löytyvät vähäiset artikkelit olivat kaupallisia, joten niihin tulee suhtautua lähdekriittisesti. Toisaalta Beacon on uusi tuote, joten siihen liittyvät aineisto on tuoretta, joka puolestaan lisää aineiston soveltuvuutta testauksen ajankohtaan.

Työn luotettavuutta vähentää pilotoinnissa suoritettujen testien vähyys ja ympäristö, jossa ne toteutettiin. Beacon asennusta ja käyttöönottamista testattiin ainoastaan demoympäristössä, joten Home-komponentin toimintaa eristetyssä verkossa jäi kokonaan testaamatta. Tämä johtui työlle varatuista resursseista.

## 4.2 Työn eettisyyden arviointi

Eettisyyttä arvioidessa pohditaan hyödyn ja haitan suhdetta. Tieteellistä tutkimusta ohjaa niin lainsäädäntö kuin kansainvälisesti tunnustetut ohjeistukset. Esimerkiksi ihmistieteissä tutkittavien suojelemiseksi on olemassa kansainvälinen ja kansallinen lainsäädäntö, jota jokaisen tutkijan tulee ehdottomasti noudattaa. Keskeisin tutkimuseettinen periaate on tietoon perustuvan suostumuksen vaade. (Laki lääketieteellisestä tutkimuksesta, 488/1999.) Hyvä tieteellinen käytäntö puolestaan määrittelee periaatteet, joilla huolehditaan hyvän tieteellisen käytännön toteutumisesta tieteellisen toiminnan koko elinkaaren ajan (Tutkimuseettisen neuvottelukunnan julkaisuja 2/2023, 2023).

Tämä työ ei ole tieteellinen tutkimus, mutta se ei poista vaatimusta noudattaa soveltuvia eettisiä ohjeita. Opinnäytetyötä tehdessä on noudatettu Jyväskylän ammattikorkeakoulun eettisiä säännöksiä ja ohjeistusta. Erityistä eettisesti huomioitavaa kohdetta tässä työssä ei ollut. Keskeisimpänä on ollut noudattaa plagiointi ja lähdeviittauksiin liittyviä eettisiä ohjeita.

Yksi eettinen arvioinnin kohde on myös hankintalain noudattaminen silloin kuin kyseessä on julkisin varoin hankittu tuote tai palvelu. Tässä työssä pilotoinnin kohteena ollut eristyksentestausjärjestelmä on valittu puolustusvoimien hankintaprosessin mukaisesti, joka noudattaa hankintalakia. (Laki julkisista hankinnoista ja käyttöoikeussopimuksista, 29.12.2016/1397.)

# 5 Johtopäätökset

Opinnäytetyön perusteella voidaan tehdä seuraavat johtopäätökset:

Käytetty automaattisen verkkojen eristyksentestausjärjestelmän Beacon toimii hyvin automaattisena verkkojen eristyksentestausjärjestelmänä. Järjestelmän eristetyn verkon testausmenetelmät auttavat löytämään aukkoja ja haavoittuvuuksia verkoista.

Beaconin käyttöönotto oli helppoa ja valmistajan manuaalit olivat toimivia ja selkeitä.

Beacon tuo merkittävää turvallisuutta ja aikasäästöä jatkuvan automaattisen testauksen ansiosta.

Opinnäytetyöhön varatut resurssit ja aikajänne olivat rajalliset, joten järjestelmää ei ollut mahdollista testata aidossa toimintaympäristössä. Testaaminen toteutui demoympäristössä. Beaconin testaaminen aidossa ympäristössä on suoritettava ennen tuotantoon asentamista sekä Homen asentamista eristettyyn verkkoon.

# Lähteet

Aikio,E. 2017. Easy|Secure|Reliable: Not Just in the Marketing Materials. Artikkeli Medium sivustolla. Viitattu 11.2023. https://medium.com/sensorfu/easy-secure-reliable-not-just-in-the-marketing-materials-ad8ef7afd086

Alueellisen koskemattomuuden valvonta ja turvaaminen (AKV / AKT). N.d. Ilmavoimien verkkosivuilla julkaistu artikkeli. https://ilmavoimat.fi/akv/akt-toiminta

Beacon by SensorFu. N.d. SensorFu kotisivut. Viitattu 11.2023. https://sensorfu.com/

Beacon User Manual. N.d. Beacon online käyttöohjeet. Viitattu 12.2023. https://portal.sensorfu.com/manual/

Finder. 2023. SensorFu taloustiedot Finder palvelussa. Viitattu 12.2023. https://www.finder.fi/IT-konsultointi+IT-palvelut/SensorFu+Oy/Oulu/yhteystiedot/3159522

Heikkinen, P. 2021. Kriittiset tuotannon ja teollisuuden verkot ovat jatkuvasti hyökkäyksen kohteena. Loihdetrust verkkosivuilla julkaistu blogiteksti. Viitattu 11.2023. https://www.loihdetrust.com/blogi/kriittiset-tuotannon-ja-teollisuuden-verkot-ovat-jatkuvasti-hyokkayksen-kohteena/

Heikkinen, P. 2022. Miten suojata ja valvoa kriittistä infrastruktuuria. Loihdetrust verkkosivuilla julkaistu blogiteksti. Viitattu 11.2023. https://www.loihdetrust.com/blogi/miten-suojata-ja-valvoa-kriittista-infrastruktuuria/

Herrala, O, 2017. The Story about Ping. Artikkeli Medium sivustolla. Viitattu 11.2023. https://medium.com/sensorfu/the-story-about-ping-723dd71ac50b

Ilmavoimat vastaa Suomen ilmapuolustuksesta. N.d. Ilmavoimien verkkosivuilla julkaistu artikkeli. https://ilmavoimat.fi/tietoa-meista

Ilmavoimien johtoesikunta. N.d. Ilmavoimien verkkosivuilla julkaistu artikkeli. https://ilmavoimat.fi/ilmave-tietoa-meista

Is your network isolation leaking. N.d. Adventica verkkosivulla julkaistu artikkeli. Viitattu 12.2023. https://advenica.com/fi/node/970

Järvinen, A. 2023. Turvallisuusjärjestelmien digitaalinen turvallisuus. Julkaisija Sähköinfoja Turva-alan yrittäjät. Kustantaja Huoltovarmuusorganisaation Digipooli. Viitattu 12.2023. https://www.finanssiala.fi/wp-content/uploads/2023/02/turvallisuusjarjestelmien-digitaalinen-turvallisuus_2023.pdf

Juillion, P. 2019. What is an isolated network?. Studybuff sivustolla julkaistu artikkeli. Viitattu 11.2023. https://studybuff.com/what-is-an-isolated-network/

Jurvanen, L. 2023. Mikä on OT-verkko? Opas tuotantoverkkojen maailmaan! Savelan verkkosivuilla julkaistu artikkeli. Viitattu 11.2023. https://www.savelan.fi/mika-on-ot-verkko/

Kenttälä, M. 2019. SensorFu Beacon How To: 3 steps to always know if your isolated Linux leaks. Artikkeli Medium sivustolla. Viitattu 11.2023. https://medium.com/sensorfu/sensorfu-beacon-how-to-3-steps-to-always-know-if-your-isolated-linux-leaks-e2206252782c

Knight,A. 2020. Network isolation and segmentation explained. AT&T Cybersecurity blogit artikkeli Viitattu 11.2023. https://cybersecurity.att.com/blogs/security-essentials/demystifying-network-isolation-and-micro-segmentation

Koskinen, T. 2023. Hyökkäykset tuotantoverkkoihin lisääntyvät – miten huomioit tämän suunnittelussa? Tekniikka & Talous verkkosivuilla julkaistu artikkeli. Viitattu 11.2023. https://kumppanisisallot.fi/tekniikkatalous/afry/miten-hallitset-tuotantoverkon-tietoturvariskeja-teollisuuslaitoksissa/

Kotipelto, H. N.d. Kyberturvallisuus osana kansallista turvallisuutta. Sisäministeriön verkosivuilla julkaisut artikkeli. Viitattu 12.2023. https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus

Laki julkisista hankinnoista ja käyttöoikeussopimuksista. 29.12.2016/1397. Finlex verkkosivulla haettu laki. Viitattu 01.2024. https://www.finlex.fi/fi/laki/ajantasa/2016/20161397

Laki lääketieteellisestä tutkimuksesta, 488/1999. 1999. Finlex verkkosivulta haettu laki. Viitattu 01.2024. https://www.finlex.fi/fi/laki/smur/1999/19990488?search%5Btype%5D=pika&search%5Bpika%5D=tutkimuslaki

Lehto, M. 2022. Ukrainan infrastruktuuri kyberhyökkäysten kohteena. Sotilasaikakauslehti julkaistu upseeriliiton verkkosivuilla. https://upseeriliitto.fi/verkkolehti/ukrainan-infrastruktuuri-kyberhyokkaysten-kohteena/

Lukka P. 2022 Yhdessä verkkovuotoja vastaan. Siemens verkkosivulla julkaistu artikkeli. Viitattu 12.2023. https://www.siemens.com/fi/fi/yhtio/stories/teollisuus/sensorfu-siemens-yhdessa-verkkovuotoja-vastaan.html

Network segmentation in OT environments. N.d. Verve verkkosivuilla julkaistu artikkeli. Viitattu 12.2023. https://verveindustrial.com/resources/whitepaper/network-segmentation-in-ot-environments/

Nordic Option sijoittaa Sensor Fun kansainvälistymiseen. 2021. Arvo sijoitusosuuskunta verkkosivuilla julkaistu artikkeli. Viitattu 12.2023. https://www.arvosijoitus.fi/arvo/ajankohtaista/nordic-option-sijoittaa-sensor-fun-kansainvalistymiseen

Projektiorientoitunut tietoturvakonsultti taitaa OT-verkot. 2022. Loihdetrust verkkosivuilla julkaistu artikkeli. Viitattu 11.2023. https://www.loihdetrust.com/loihtijat/projektiorientoitunut-tietoturvakonsultti-taitaa-ot-verkot/

Reliabiliteetti. N.d. Tilastokeskuksen verkkosivuilla reliabiliteettin validiteetin määritelmä. Viitattu 01.2024. https://www.stat.fi/meta/kas/reliabiliteetti.html

SensorFu Oy:n Vastaus tietopyyntöön, 2023. Viitattu 12.2023.

Shivanandhan. M. 2020. What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time. FreeCodecamp verkkosivuilla julkaistu artikkeli. Viitattu 12.2023.

Tiwari, A. 2023. Receive Webhook Requests Using ELK. Ashish Tiwari verkkosivuilla julkaistu blogiteksti. Viitattu 1.2024. https://ashish.one/blogs/elastic/receive-webhook-requests-using-elk/

Tiwari, A. 2023. Receive Webhook Requests Using ELK. Blogiteksti. Viitattu 12.2023. https://ashish.one/blogs/elastic/receive-webhook-requests-using-elk/

Toivonen, M. 2020. Mikko Toivonen: Kyberturvallisuus Tuotantoverkoissa Ja Järjestelmissä. Elisan yrityksille verkkosivujen blogissa julkaistu. Viitattu 11.2023. https://yrityksille.elisa.fi/ideat/kyberturvallisuus-tuotantoverkoissa-ja-jarjestelmissa/

Toteutettavuustutkimus: Yritysten tietoturvaa voi parantaa helposti! 2020. Kyberturvallisuuskeskuksen julkaisema raportti. Viitattu 29.11.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TONTTU_2.pdf

Tutkimuseettisen neuvottelukunnan julkaisuja 2/2023, 2023. TENK verkkosivuilta haettu julkaisu. Viitattu 01.2024. https://tenk.fi/fi/ohjeet-ja-aineistot

Validiteetti. N.d. Tilastokeskuksen verkkosivuilla validiteetin määritelmä. Viitattu 01.2024. https://www.stat.fi/meta/kas/validiteetti.html

What is a webhook. 2022. RedHat verkkosivulla julkaistu artikkeli. Viitattu 12.2023. https://www.redhat.com/en/topics/automation/what-is-a-webhook

What is Network Segmentation? N.d. Paloalto verkkosivuilla julkaistu artikkeli. Viitattu 11.2023. https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation

What Is Wireshark and How Is It Used. N.d. CompTIa verkkosivulla julkaistu artikkeli. Viitattu 12.2023. https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it

Why Data Diodes Are Essential for Isolated and Classified Networks. 2016. Opswat sivustolla julkaistu blogiteksti. https://www.opswat.com/blog/why-data-diodes-are-essential-isolated-and-classified-networks

XM Cyber Breach and Attack Simulation. N.d. Cybersecurity excellence awards verkkosivulla julkaisut artikkeli. Viitattu 12.2023. https://cybersecurity-excellence-awards.com/candidates/xm-cyber-breach-and-attack-simulation/