OSINT-tiedustelun implementointi osaksi organisaation kyberturvallisuutta

Krista Tiitta

2023 Laurea

Laurea-ammattikorkeakoulu

OSINT-tiedustelun implementointi osaksi organisaation kybertur-vallisuutta

Krista Tiitta
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2023

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittely, kyberturvallisuus

Tradenomi (AMK)

Krista Tiitta

OSINT-tiedustelun implementointi osaksi organisaation kyberturvallisuutta

Vuosi 2023 Sivumäärä 38

Organisaatioiden suurena haasteena nykypäivänä on jatkuvasti kehittyvä kyberturvallisuuden uhkatason ja kohdistettujen hyökkäysten määrän nousu. Muuttuva digitaalinen ympäristö on luonut uuden hyökkäysalustan rikollisille ja organisaatioiden on kehitettävä uusia keinoja kyberrikollisuudelta ja -uhkilta suojautumiseksi.

Tässä opinnäytetyössä esiteltiin avointen lähteiden tiedustelua (OSINT – Open Source Intelligence) ja sen implementointia osaksi organisaation kyberturvallisuutta kehittelemällä organisaatiolle toimintaprosessi OSINT-tiedustelua varten. Kohdeorganisaationa työssä toimi kansainvälinen finanssialan toimija. Kohdeorganisaatio anonymisoitiin työssä, koska organisaatio on huoltovarmuuskriittinen toimija. Työn tavoitteeksi oli asetettu OSINT-tiedustelun implementointi osaksi organisaation kyberturvallisuutta.

Työn teoriaosuudessa käytiin läpi OSINT-tiedustelua yleisesti, sen historiaa ja siihen liittyviä työkaluja. Työn lähdemateriaaleina käytettiin kattavasti OSINT-tiedustelua koskevia tieteellisiä julkaisuja, materiaaleja ja aiheeseen liittyvää kirjallisuutta. Opinnäytetyön työmetodina oli suunnittelutieteellinen tutkimusmenetelmä. Suunnittelutieteellisellä tutkimuksella pyritään luomaan jokin teknologiaorientoitunut ratkaisu relevanttiin ongelmaan.

Tutkimuksen perusteella suunniteltuun toimintaprosessiin sisältyi vaiheet ja ohjeet OSINT-tiedustelun toteuttamiseksi kohdeorganisaatiossa. Tutkimuksen tulos oli hyödyllinen kohdeorganisaatiolle, koska opinnäytetyön tutkimuksen tuloksena syntynyt toimintaprosessi OSINT-tiedustelua varten vastaa kohdeorganisaation tarpeeseen kehittää tiedusteluun liittyviä prosesseja ja se parantaa organisaation valmiustasoa kyberuhkilta suojautumiseen ja uhkien mitigointiin.

Asiasanat: OSINT, tietoturva, kyberturvallisuus, organisaatioturvallisuus, uhkatiedustelu

Laurea University of Applied Sciences **Abstract**

Bachelor's Degree Programme in Business Information Technology, Cybersecurity

Bachelor of Business Administration

Krista Tiitta

Implementation of OSINT to Organization's Cybersecurity

Year 2023 Pages 38

Some of the greatest challenges of modern organizations are the constantly evolving cybersecurity risks and the rising number of cyber-attacks. The transforming digital environment has created a new platform for criminal activity and therefore organizations need to create new methods to protect themselves from these potential threats.

The objective of this thesis project was to highlight the open-source intelligence process (OSINT) and its implementation as a part of organizations' cyber security measures by developing operating process for utilizing OSINT. The study focuses on an international organization operating within the finance sector. The organization's name will not be published due to it being a critical operator within the National Emergency Security Supply. The aim of this thesis was to deploy the OSINT process as a part of the organization's cybersecurity toolkit.

The knowledge base of the thesis report consists of an introduction to open-source intelligence, its history and the available tools relating to it. The sources are drawn from various scientific publications, materials and literature relating to the OSINT method. The thesis project also utilizes the design science research method. This method aims to generate a technology-oriented solution to a relevant research problem.

Based on this study, a process was designed which contains the phases and guidance for how to perform OSINT within the targeted organization. The outcome of this thesis project will be useful to the targeted organization as the resulting OSINT process relates to the organization's constant need to develop intelligence processes and to improve its ability to respond to various cyber threats whilst mitigating risks.

Keywords: OSINT, cybersecurity, information security, organizational security, threat intelligence

Sisällys

1 Johdanto

Nykymaailman jatkuvasti muuttuva digimaailma tuottaa organisaatioille haasteita pysyä mukana kyberuhkien torjunnassa. Hallitukset, yhteiskunnat ja eri organisaatiot luottavat yhä enemmän ja enemmän teknologiaan, esimerkiksi julkisten palveluiden siirtyessä etenevissä määrin sähköisiksi. Samalla, kun yhteiskunta jatkaa digisiirtymäänsä, on digitaalinen ympäristö luonut uuden hyökkäysalustan rikollisille. Digimaailman kehittyessä myös rikolliset ovat kasvattaneet tietämystään ja ottaneet käyttöönsä uusia kehittyneempiä hyökkäystapoja organisaatioita ja yksityishenkilöitä kohtaan, jotka ovat hyvin suunniteltuja ja kohdistettuja. Hyökkäysten ollessa kehittyneempiä ja kohdistetumpia, organisaatioiden on todennäköisempää joutua vakavien kyberhyökkäysten kohteeksi, joilla on suuria taloudellisia vaikutuksia sekä mainehaittaa. (Martins & Medeiros, 2.)

Kyberrikollisuus maksaa organisaatioille ja yksityishenkilöille kymmeniä ja jopa satoja miljoonia vuosittain. Suomalaiset menettävät verkkorikollisuuden vuoksi vuosittain kymmeniä miljoonia euroja, esimerkiksi pankkien mukaan suomalaiset menettivät vuonna 2022 verkkorikollisuuden vuoksi yhteensä 32,4 miljoonaa euroa. Viranomaiset ja pankit onnistuivat estämään 14,5 miljoonan euron päätymisen rikollisille vuonna 2022. (Finanssiala Ry 2023.)

Kyberrikollisuuden haitat eivät ole pelkästään taloudellisia, koska ne voivat osua myös kriittiseen infrastruktuuriin tai vaikuttaa kansalaisten henkiseen hyvinvointiin. Tämän takia organisaatioiden onkin erittäin tärkeää tarkastella kyberturvallisuutensa resilienssiä. Venäjän hyökättyä Ukrainaan kyberrikollisuuden määrä on noussut huomattavasti ympäri maailmaa. (Sayegh 2022.)

Tässä opinnäytetyössä käsitellään avointen lähteiden tiedustelun (OSINT – Open Source Intelligence) implementointia osaksi organisaation kyberturvallisuutta. Kohdeorganisaationa toimii kansainvälinen finanssialan toimija. Työn taustana on kohdeorganisaation tarve avointen lähteiden tiedustelun tehostamiseen ja toimintaprosessien luomiseen. Tavoitteena on luoda kohdeorganisaatiolle vahva toimintaprosessi avointen lähteiden tiedustelua varten esittelemällä avointen lähteiden tiedustelua, siihen liittyviä prosesseja, työvaiheita ja yleisimpiä työkaluja avointen lähteiden tiedustelun toteuttamiseen. Tällä tutkimustiedolla kohdeorganisaatio voi halutessaan tuottaa organisaatiostaan OSINT-tutkimuksen tai muuta haluamaansa tutkimustietoa.

Tämä opinnäytetyö on tehty suunnittelutieteen pohjalta. Opinnäytetyössä kehitetään teoriaan pohjautuen kohdeorganisaatiolle toimintaprosessi avointen lähteiden tiedustelua varten. Työssä pohditaan kehitys- ja tutkimustyön taustaa, tarpeellisuutta, käydään läpi OSINT-tutkimuksen prosessi, työkalut ja tulokset.

Opinnäytetyön tietolähteinä käytettiin avointen lähteiden tiedusteluun liittyvää materiaalia internetistä ja alaan liittyvää kirjallisuutta.

2 OSINT

Open Source Intelligence eli OSINT tarkoittaa avointen lähteiden tiedustelua. Sillä viitataan mihin tahansa laillisesti hankittuun tietoon vapaasti saatavilla olevista ja julkisista lähteistä. Yleisesti tämä tarkoittaa internetistä löytyvää tietoa, mutta kaikki julkisesti saatavilla oleva tieto, esimerkiksi sanomalehdet, aikakausilehdet, televisio ja radio kuuluvat avoimiin tietolähteisiin. Sosiaalisen median käytön lisääntyminen on lisännyt avoimen tiedon määrää huomattavasti. (Akhgar & Bayerl 2015, 62.)

Internetin käytön yleistyminen ja saatavuus on merkittävästi muokannut tapaamme kommunikoida ja jakaa tietoa. Sosiaalisen median alustat ja viestipalvelut antavat yksilöille ja organisaatioille mahdollisuuden viestiä ja ilmaista itseään reaaliajassa. Kaiken tämän sivutuotteena internetissä julkaistaan paljon sensitiivistä tietoa, joka saattaa olla kaikkien käytettävissä maailmanlaajuisesti. Joissain tapauksissa jaettua tietoa saatetaan käyttää laittomasti esimerkiksi vainoamiseen, terrorismiin tai identiteettivarkauksiin. (Azzopardi, Glisson, Maxwell & McKeown 2014, 175–176.)

Avointen lähteiden tiedustelua käytetään hyödyksi rikostutkinnassa, terrorismin vastaisessa taistelussa, APT-toimijoiden tutkinnassa (APT = Advanced Persistent Threat, esimerkiksi organisoitunut hakkeriryhmä, joka saattaa toimia jonkin valtion alaisuudessa) ja kyberrikollisuuden kitkemisessä. OSINT on nykypäivänä organisaatioille ja tiedusteluyhteisöille merkittävä tiedustelutapa. Avointen lähteiden tiedustelu on halvempaa ja vähemmän riskialtista kuin perinteinen vakoilu. (Oikarinen 2020.)

2.1 OSINT-tiedustelun historia

Avointen lähteiden tiedustelulla on takanaan pitkä historia. Vuonna 1883 Upstatessa New Yorkissa syntyi yksi tiedustelun vaikutusvaltaisimmista henkilöistä. Irlantilaisten maahanmuuttajien poika William Donovan varttui työnväenluokkaisessa perheessä ja menestyi erinomaisesti eri kouluasteissa. Donovanin intohimona oli tulla Yhdysvaltain ensimmäiseksi roomalaiskatoliseksi presidentiksi ja hänen haaveensa melkein toteutui. Donovan kävi Columbia Law Schoolin, jossa hänen luokkatoverinaan oli Franklin D. Roosevelt. (Colquhoun 2016.)

Ensimmäisen maailmansodan jälkeen Donovanilla oli menestyksekäs ura kansainvälisenä lakimiehenä. Sotien välisen ajan Donovan matkusteli ympäri maailmaan tehden töitä lakimiehenä

ja samalla hän toimitti raportteja tapaamisistaan vaikutusvaltaisten henkilöiden kanssa Yhdysvaltojen hallitukselle. (Colquhoun 2016.)

Donovanin yhteys Franklin D. Rooseveltiin oli yhdistävä tekijä tiedustelupalvelun syntyyn Yhdysvalloissa. Heinäkuussa 1941 Franklin D. Roosevelt loi Donovanille virallisen roolin nimeltään ”Coordinator of Information”. Japanin iskettyä Pearl Harbouriin toisen maailmansodan aikaan joulukuussa 1941, oli selvää, että tiedustelun tarve oli lisääntynyt. Iskun jälkeen Donovanin osasto uudelleennimettiin Office of Strategic Services (lyhyesti OSS). OSS oli Central Intelligence Agencyn (CIA) edeltäjä. Iso-Britannian tiedustelupalvelu Special Operations Executive (SOE) hyödynsi myös toisen maailmansodan aikana OSINT-tiedustelua. (Colquhoun 2016.)

OSS:llä oli kokonainen osastohaara nimeltään Research and Analysis Branch omistettuna avointen lähteiden tiedustelulle. Se keräsi kymmeniä sanoma- ja aikakausilehtiä, lehdistöleikkeitä, radiolähetyksiä, valokuvia, raportteja ja artikkeleja ympäri maailmaa, joista saataisiin koostettua tärkeitä vihollista koskevia tietoja. (Colquhoun 2016.)

Kylmän sodan aikaan tiedustelu ja vakoilu keskittyi pääasiassa tiedon hankkimiseen sähköisistä signaaleista ja henkilölähteistä. OSINT nousi 1980-luvulla taas esiin lisäkeinona tiedustelutietojen keräämiseen. (Imperva 2022.)

Vuonna 2009 Iranissa alkoi Green Revolution-vallankumous. Miljoonat nuoret iranilaiset protestoijat käyttivät internetiä hyödykseen koordinoidessaan aktiviteetteja ja kampanjoita, joissa he kannustivat muitakin liittymään protestiin. Protestin ensimmäisten viikkojen aikana noin 60 prosenttia Twitteriin julkaistuista blogilinkeistä koski iranilaisia poliitikkoja. Vaikka protestit lopulta epäonnistuivat ja Iranin hallinto sai tiukan hallinnan internetistä Iranissa, voidaan Green Revolutionia pitää OSINT-tiedustelun mullistavana tapahtumana, koska ensimmäistä kertaa koskaan kuka tahansa mistä tahansa maailmaa pystyi keräämään tiedustelutietoa ja jakamaan sitä eteenpäin. (Colquhoun 2016.)

Hieman alle vuosi Iranin Green Revolutionin jälkeen sosiaalisen median ruokkimat protestit ja vallankumoukset levisivät Lähi-Idässä. Älypuhelimien, sosiaalisen median ja vihan yhdistelmä järkytti diktatuureja Lähi-Idässä ja Pohjois-Afrikassa. CIA:n OSINT-keskus ei kyennyt ennakoimaan internet-pohjaisen sosiaalisen aktivismin kehitystä Lähi-Idässä ja Afrikassa. Yksi syy epäonnistumiselle oli se, että Yhdysvaltojen hallituksen tiedusteluosastot olivat kiinnostuneempia keräämään tiedustelutietoja vahvalta eliitiltä sen sijaan, että olisi keskitytty hyödyntämään valtavaa määrää avointa dataa. (Colquhoun 2016.)

Viime vuosina valtiot ovat ottaneet opikseen ja kehittäneet omaa avointen lähteiden tiedusteluaan. Esimerkiksi vuonna 2015 Yhdysvaltojen armeija onnistui tuhoamaan terroristiryhmittymän pommitehtaan 23 tunnin kuluttua siitä, kun yksi terroristiryhmittymän jäsen oli julkaissut sosiaaliseen mediaan kuvan itsestään, jossa näkyi pommitehtaan kattorakenne. (Colquhoun 2016.)

2.2 Mihin OSINT-tiedustelua voidaan käyttää?

Avointen lähteiden tiedustelua voidaan tehdä turvallisuuden ammattilaisten toimesta sekä uhkatoimijoiden toimesta. Kyberturva-ammattilaiset ja penetraatiotestaajat käyttävät OSINT-tiedustelua löytääkseen avoimista lähteistä arkaluontoisia tietoja ja muita tietoja, joita voitaisiin käyttää esimerkiksi kyberhyökkäyksen suunnittelussa kohdeyritystä tai -organisaatiota vastaan. Organisaatioiden ja yritysten vahingossa julkaisemat tiedot voivat sisältää erittäin sensitiivistä dataa ja olla vapaasti saatavilla organisaatioiden tai yritysten tietämättä. Tällaisia tietoja ovat esimerkiksi avoimet portit, IT-laitteiston tiedot ja kokoonpano, IP-osoitteet ja ohjelmistot, joissa on todettu paikkaamattomia haavoittuvuuksia. Myös sosiaalinen media on isossa osassa usean organisaation ja yrityksen arkea. Sosiaalinen media sisältää valtavan määrän olennaista tietoa organisaatioista ja yrityksistä ja myös mahdollisesti niiden työntekijöistä. (Imperva 2022.)

Lainvalvontaviranomaiset käyttävät OSINT-tiedustelua suojellakseen kansalaisia esimerkiksi identiteettivarkauksilta, seksuaaliselta hyväksikäytöltä, väkivallalta ja muilta rikoksilta. Tiedustelutietoa kerätään usein useista sosiaalisen median kanavista. Tällä tavoin esimerkiksi poliisi pystyy luomaan rikollisjärjestöistä ja niihin kuuluvista henkilöistä tarkkoja profiileja. Lisäksi OSINT-tiedustelua käytetään tekijänoikeusrikkomusten jäljittämiseen ja verkkoväärennösten tunnistamiseen. (Hwang 2022.)

Esimerkkinä lainvalvontaviranomaisten suorittamasta OSINT-tiedustelusta on italialaisen Vito Roberto Palazzolon vangitseminen. Hän toimi Italian mafian rahastonhoitajana 30 vuoden ajan. Lainvalvontaviranomaiset seurasivat muun muassa Palazzolon Facebook-sivua, josta oli hyötyä pidätyksen tekemisessä. (Akhgar & Bayerl 2015, 62.)

Organisaatioille ja yrityksille tieto on valtaa ja useat organisaatiot ja yritykset käyttävät OSINT-tiedustelua kilpailijoidensa seuraamiseen, markkinoinnin suunnitteluun ja uusien markkinoiden tutkimiseen. OSINT-tiedustelua tekevät nykyään melkein kaikki yritykset ja organisaatiot niiden koosta riippumatta sen kustannustehokkuuden vuoksi. OSINT-tiedustelua käytetään organisaatioissa myös muihin tarkoituksiin, esimerkiksi kyberhyökkäyksiltä suojautumiseen ja niiden hallintaan, uhkatiedusteluun ja maineriskien minimoimiseen. (Hassan & Hijazi 2018, 12.)

OSINT-tiedustelua voidaan käyttää myös rikolliseen toimintaan ja esimerkiksi terroristijärjestöt voivat käyttää avointen lähteiden tiedustelua terroristihyökkäysten suunnitteluun. Terroristit keräävät avoimista lähteistä tietoja kohteistaan ennen hyökkäystä. He käyttävät muun muassa satelliittikuvia ja Google Mapsia tutkiessaan hyökkäyksen kohdettaan. He voivat hyödyntää sosiaalista mediaa uusien taistelijoiden värväämiseen ja analysoida verkosta löytyvää hallitusten julkaisemaa sotilaalliseen toimintaan liittyvää dataa ja levittää propagandaansa ympäri maailmaa eri sähköisten kanavien kautta. (Hassan & Hijazi 2018, 13.)

Päivittäisessä organisaation ja yrityksen kyber- ja tietoturvassa OSINT-tiedustelulla on kaksi kriittistä käyttötarkoitusta:

2.2.1 Penetraatiotestaus ja Red Teaming

Tietoturva-ammattilaiset käyttävät OSINT-tiedustelua löytääkseen ja tunnistaakseen organisaation IT-infrastruktuurin haavoittuvuuksia. Red Teamilla tarkoitetaan ryhmää, joka toimii simuloidussa tilanteessa organisaatiota vastaan hyökkäävänä tahona, joka antaa hyökkäyksensä jälkeen palautetta kohdeorganisaatiolle löydöksistään. Yksi Red Teamingin ensimmäisistä vaiheista on tiedonkeruu, jota tehdään isoilta osin avoimia lähteitä käyttämällä. (BreachLock 2023.)

OSINT-tiedustelun käyttö penetraatiotestauksessa ja Red Teamingissä auttaa löytämään ja paljastamaan organisaation ulkopuolelle vuotaneita resursseja ja haavoittuvuuksia. Näin tietoturva-asiantuntijat voivat korjata mahdolliset haavoittuvuudet ja mitigoida riskejä ennen kuin hyökkääjät käyttävät niitä hyväkseen. Yleisesti OSINT-tiedustelun avulla löydettyjä haavoittuvuuksia ovat:

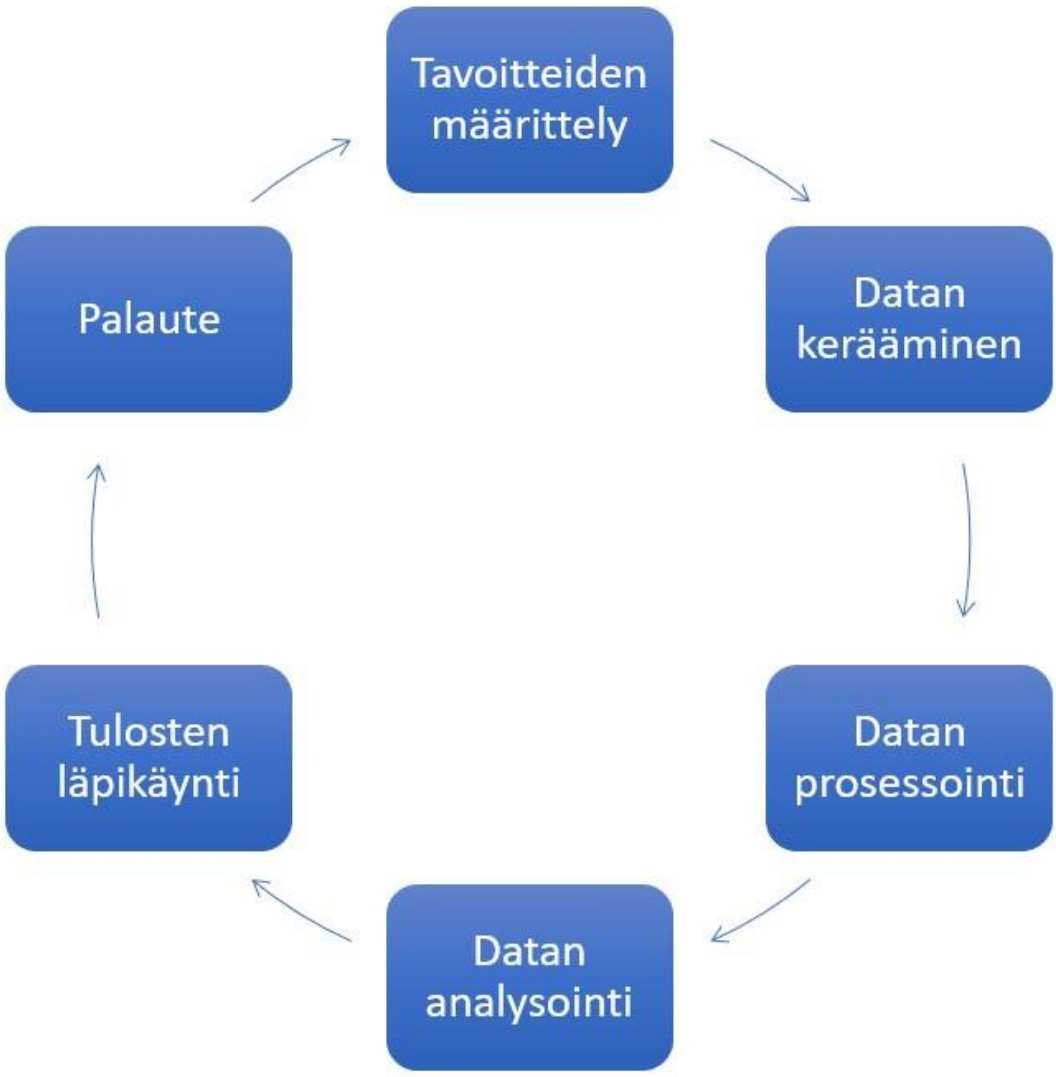
1. Arkaluonteisten ja luottamuksellisten tietojen tahaton vuotaminen julkiseen jakoon.
2. Vanhentuneet ja päivittämättömät ohjelmistot.
3. IT-laitteiden avoimet portit. (BreachLock 2023.)

Tämän tyyppistä avointen lähteiden tiedustelua kutsutaan myös organisaation ”hyökkääjänäkymäksi”, koska samat haavoittuvuudet ja löydökset näkyvät myös kyberrikollisille. Sen jälkeen, kun hyökkääjät ovat löytäneet haavoittuvuuden, ei sen hyödyntäminen ole hyökkääjille erityisen vaikeaa. Tästä syystä monet pienet ja keskisuuret yritykset ja organisaatiot ovat joutuneet kyberhyökkäysten kohteeksi. Hyökkääjällä ei edes pakosti ole erityistä mielenkiintoa organisaatiota kohtaan, mutta koska haavoittuvuuksien löytäminen ei vaadi erityisiä ponnisteluja, voidaan hyökkäyksiä tehdä matalammalla kynnyksellä. Hyökkääjät käyttävät OSINT-tiedustelun lisäksi sosiaalista manipulointia (tutummin Social Engineering) kohdistetuissa tietojenkalastelukampanjoissaan. (BreachLock 2023.)

Kuvio 1: Penetraatiotestauksen vaiheet

2.2.2 Mahdollisten uhkien ja kyberhyökkäysten tunnistaminen / uhkatiedustelu

Uhkatiedustelulla (Threat Intelligence) organisaatio voi tunnistaa ajoissa siihen kohdistuvia uhkia. Kybertapahtumien havaitseminen ja estäminen on uhkatiedustelun yleisin tavoite. Organisaatiot näkevät uhkatiedustelun usein hyvänä keinona vahvistaa toimintaympäristöään ja varautumisessa tunnettuja ja tuntemattomia kyberuhkia vastaan. Organisaation on tärkeää tunnistaa vapaasti saatavilla oleva data, joka kohdistuu organisaatioon ja sen avulla määrittää organisaatiolle mahdolliset uhat. Uhkatiedustelu on organisaatiolle arvokasta silloin, jos sen prosessit ja toimintamallit ovat toimivia. Uhkatiedustelulla on kuusi vaihetta: tavoitteiden määrittely, datan kerääminen, datan prosessointi, datan analysointi, tulosten läpikäynti ja palaute. (Martins & Medeiros 2022, 5.)



Kuvio 2: Threat Intelligence Lifecycle

OSINT voi auttaa turvallisuuden ammattilaisia ymmärtämään paremmin mahdollisia uhkia, joita heidän organisaationsa voi kohdata kyberrikollisten toimesta. Internetistä löytyy erinomaisesti tietoa tämän päivän uhkista, nousevista kybertrendeistä ja kehittyvistä hyökkäysvektoreista. Tietoturva-asiantuntijat ja -tiimit voivat käyttää avoimista lähteistä löytyviä tietoja suojellakseen esimerkiksi IT-infrastruktuuriaan nollapäivähaavoittuvuuksilta tai toteuttaa muita suojaustoimenpiteitä suojatakseen organisaatiotaan. (BreachLock 2023.)

2.3 Avoimet tietolähteet

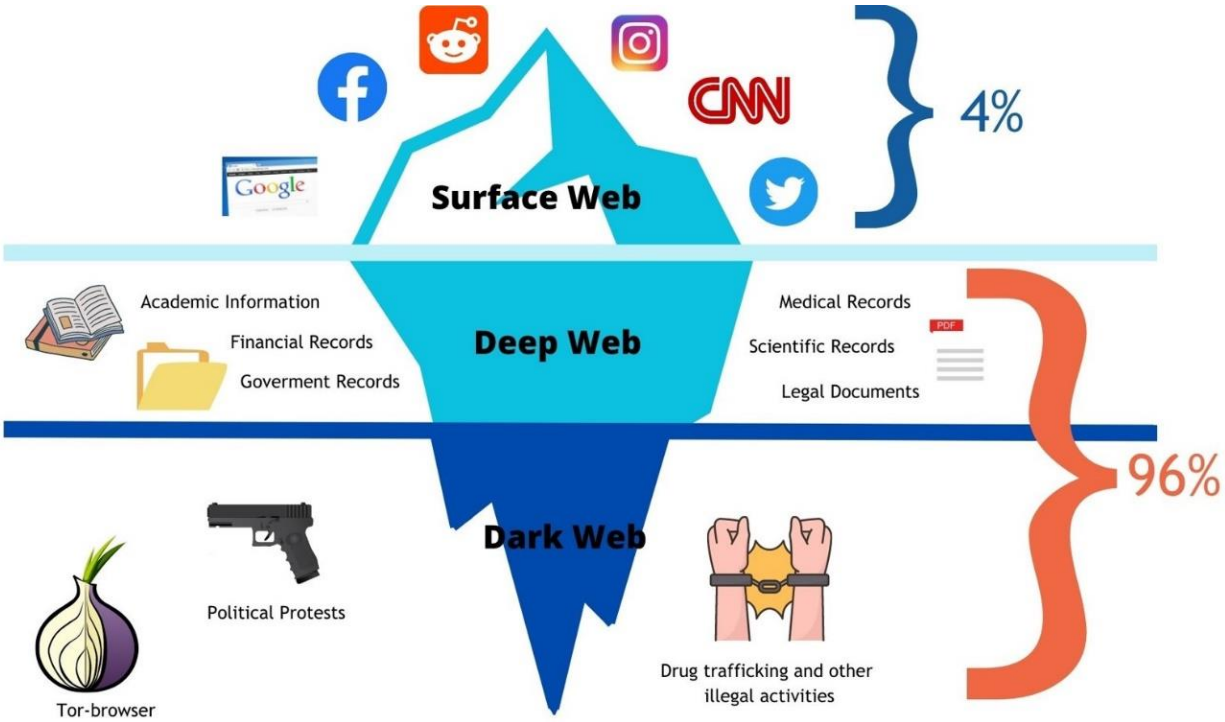
Menneisyydessä avoimet lähteet olivat rajautuneet enimmäkseen painettuihin medioihin, kuten kirjoihin ja artikkeleihin, joiden tutkiminen oli aikaan ja paikkaan sidottua. Nykyään tietoa löytyy valtavasti internetistä ja muista sähköisistä lähteistä. (Blackdot 2021.)

Usein nykyäänkin miellämme tietolähteeksi tekstipohjaiset lähteet, mutta valokuvissa, videoissa ja webinaareissa oleva tieto luokitellaan myös avoimiksi tietolähteiksi. Avoimiksi tietolähteiksi luokitellaan kaikki tieto, joka on saatavilla vapaasti tai joka voidaan asettaa saataville pyynnöstä. Alla on lueteltu esimerkkejä avoimista tietolähteistä. (Crowdstrike 2022.)

1. Uutismediasisältö verkossa, televisiossa ja painetuissa lähteissä on avoin tietolähde. Näitä ovat esimerkiksi aikakausi- ja sanomalehdet, radio ja televisio. (Hassan & Hijazi 2018, 5.)
2. Sosiaalisessa mediassa on saatavilla melkein rajattomasti tietoa. Sosiaalisen median alustoja ovat muun muassa LinkedIn, Reddit, Facebook ja Twitter. Jopa yhdestä sosiaaliseen mediaan jaetusta kuvasta tai videosta voi selvittää paljon tietoja esimerkiksi kuvan metadataa tutkimalla tai kiinnittämällä huomiota kuvatun materiaalin ympäristöön. (Crowdstrike 2022.)
3. Materiaalit ja julkaisut, jotka on julkaistu organisaatioiden tai instituutioiden toimesta. Näitä ovat muun muassa akateemiset julkaisut, väitöskirjat, konferenssijulkaisut, vuosikertomukset, ansioluettelot ja yritysprofiilit. (Hassan & Hijazi 2018, 5.)
4. Geospatiaaliset tiedot, esimerkiksi kartat (Hassan & Hijazi 2018, 5).
5. World Wide Web (WWW), eli verkko sisältää paljon enemmän tietoa, kuin voimme havaita tai ymmärtää. Se sisältää kolme eri kerrosta, jotka ovat pintaverkko, syvä verkko (Deep Web) ja pimeä verkko (Dark Web). Pintaverkko on verkon osa, joka on helposti jokaisen saatavilla. Pintaverkosta löytyvät verkkosivut ovat löydettävissä tavallisilla hakukoneilla kuten Googlella tai Bingillä. (Hassan & Hijazi 2018, 96.)

   Syvästä verkosta löytyy resursseja, joita ei ole indeksoitu näkymään perinteisissä hakukoneissa, mutta syvä verkko on kuitenkin käytettävissä samalla tavalla kuin mikä tahansa HTTP/HTTPS-verkkoprotokollaa käyttävä verkkosivusto ilman erikseen ladattavaa selainta tai ohjelmistoa. Syvästä verkosta löytyvät resurssit ovat usein esimerkiksi tietokantoihin upotettuja tietoja. (Hassan & Hijazi 2018, 98.)

   Pimeässä verkossa (Dark Web, Darknet) on paljon tietoa, jota ei löydy perinteisiä selaimia ja hakukoneita käyttämällä. Pimeän verkon maine on useasti liitetty laittomaan sisältöön ja rikolliseen toimintaan, mutta sitä hyödyntävät myös lailliset tahot. Pimeästä verkosta voi löytää muun muassa dataa varastetuista käyttäjätunnuksista ja henkilötiedoista. Pimeän verkon käyttämiseen liittyy myös paljon riskejä, jotka on hyvä ottaa huomioon vieraillessaan pimeässä verkossa. Pimeän verkon riskejä ovat haittaohjelmat, valtiovallan harjoittama valvonta ja erilaiset huijaukset. (Hassan & Hijazi 2018, 101.)



Kuvio 3: Verkon eri kerrokset (IFF Lab 2023)

2.4 Avointen lähteiden tiedustelun hyödyt ja haitat

Avointen lähteiden tiedustelua on hyödynnetty laajasti kaikkialla jo toisesta maailmansodasta lähtien. Valtiot, armeijat, organisaatiot ja myös yksityishenkilöt hyödyntävät OSINT-tiedustelua. Avointen lähteiden tiedusteluun sisältyy useita eri hyötyjä ja haittoja. (Hwang 2022.)

Avointen lähteiden tiedustelun hyötyjä ovat:

1. Reaaliaikainen ja nopea tiedonkeruu. Tietoa saadaan kerättyä valtavasti avoimista lähteistä ja tietoja pystyy yleensä seuraamaan myös reaaliajassa. Tietoja etsitään yleisesti internetistä. (Hwang 2022.)
2. Tiedonkeruu on vähemmän riskialtista. Avointen lähteiden tiedustelu on turvallisempaa kuin muut tiedustelumuodot, koska tietoa kerätään julkisesti saatavilla olevista lähteistä. (Hassan & Hijazi 2018, 15.)
3. Useita luotettavia lähteitä. Avoimia tietolähteitä käyttämällä voidaan tietoa etsiä luotettavista lähteistä ja tiedon alkuperä voidaan yleensä tarkastaa. (Hwang 2022.)
4. Helppous. Kaikki pääsevät halutessaan käsiksi avointen lähteiden sisältämiin tietoihin, joten tietojen etsiminen on kohtalaisen helppoa ja tietoa pystytään käyttämään käyttäjän käyttötarpeisiin nojautuen. (Hwang 2022.)

5. Lakiasiat. OSINT-tiedustelussa käytetään julkisesti ja vapaasti saatavilla olevaa tietoa, joten tekijänoikeuslisenssien rikkomisesta ei täydy olla huolissaan. (Hassan & Hijazi 2018, 16.)
6. Kustannustehokkuus. OSINT-tiedustelun etuna on se, että siinä on alhaiset kustannukset verrattuna muihin tiedustelulajeihin. Pienet organisaatiot, joiden budjetti ei taivu isoihin investointeihin, voivat hyödyntää OSINT-tiedustelua pienin kustannuksin. (Hassan & Hijazi 2018, 15.)
7. Kansallisen turvallisuuden ja poliittisen vakauden ylläpitäminen. OSINT-tiedustelu auttaa lainvalvontaviranomaisia ja hallituksia pysymään ajan tasalla uhkaympäristön muutoksista. (Hassan & Hijazi 2018, 16.)

Avointen lähteiden tiedustelun haittoja ovat:

1. Saatavilla olevan tiedon määrä on liian suuri. Nykypäivänä tietoa on saatavilla melkeinpä loputtomasti. Tämä johtaa siihen, että tiedustelua tekevillä on yhä vaikeampaa erottaa relevantti tieto epärelevantista tiedosta. Relevantin ja luotettavan tiedon etsimiseen ja valitsemiseen menee aiempaa enemmän aikaa. (Hwang 2022.)
2. Organisaatioiden negatiivinen tiedustelukäsitys. Organisaatioilla saattaa olla negatiivisia ennakkoluuloja tiedustelusta, esimerkiksi OSINT-tiedustelun avulla löydettyä tietoa aliarvioidaan tai tiedustelun tärkeyttä ei oteta huomioon mietittäessä organisaation kokonaisturvallisuutta. (Hwang 2022.)
3. Tekniset rajoitteet. Koska kaikki tieto ei ole saatavilla vapaasti, saattaa tämä aiheuttaa teknisiä haasteita tiedustelutavoitteen kokonaiskuvan luomiseksi. (Hwang 2022.)
4. Verkkorikollisuus ja tiedon väärinkäyttö. Kuka tahansa pääsee käsiksi avoimista tietolähteistä löytyvään tietoon. Haittapuolena on se, että myös rikolliset tekevät aktiivisesti avointen lähteiden tiedustelua ja pystyvät käyttämään löytämiään tietojaan rikollisuuden mahdollistamiseksi. (Hwang 2022.)

Hyödyt	Haitat
Reaaliaikainen ja nopea tiedonkeruu	Saatavilla olevan tiedon määrä on liian suuri
Tiedonkeruu on vähemmän riskialtista	Organisaatioiden negatiivinen tiedustelukäsitys
Useita luotettavia lähteitä	Tekniset rajoitteet
Helppous	Verkkorikollisuus ja tiedon väärinkäyttö
Lakiasiat	
Kustannustehokkuus	
Kansallisen turvallisuuden ja poliittisen vakauden ylläpitäminen	

Taulukko 1: Avointen lähteiden tiedustelun hyödyt ja haitat

2.5 Oman toiminnan suojaaminen

OSINT-tiedustelua tehdessä on tärkeää suojata itsensä ja pysyä anonyymina. Omaa toimintaansa voi suojata käyttämällä virtuaalista erillisverkkoa (VPN ”virtual private network”), jonka avulla pystyy peittämään muun muassa IP-osoitteen ja sijainnin. On varmistettava, että VPN-yhteys on käytössä myös mahdollisessa virtuaalikoneessa. Vaihtoehtoisesti anonyymien verkkojen käyttö on suositeltavaa (esimerkiksi Tor tai I2P). (Hassan & Hijazi 2018, 69.)

Tor-verkko (The Onion Router) on anonyymi verkko, joka salaa tiedonsiirron ja reitittää sen usean verkon solmukohdan läpi ennen saapumistaan halutulle verkkosivustolle. Tiedonsiirto kulkee Tor-verkossa vähintään kolmen solmukohdan kautta. Jotta Tor-verkkoa voi käyttää OSINT-tiedusteluun, tulee laitteelle ladata Tor-selain. Tor-verkkoa käyttäessä on suositeltavaa käyttää myös VPN-yhteyttä. (Hassan & Hijazi 2018, 69–70.)

2.6 OSINT-tiedustelun vaiheet

OSINT-tiedustelussa on viisi vaihetta. Sen tärkein vaihe on tiedon kerääminen avoimista tietolähteistä. Jotta tiedustelua voidaan tehdä tehokkaasti, on löydettävä hyviä tapoja etsiä ja käyttää tietoa, joka on lisääntynyt nykypäivänä räjähdysmäisesti. Jotta haluttu tieto löydetään vaivattomasti, on tarpeellista suunnitella OSINT-tiedusteluun johdonmukaiset vaiheet. (Hwang 2022.)

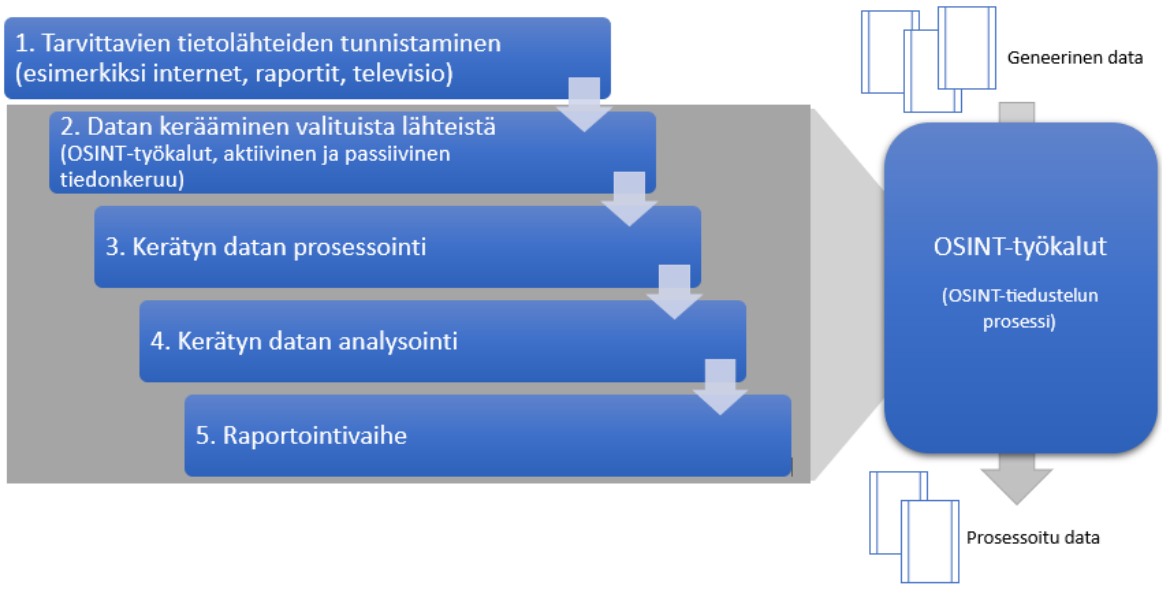
Ensimmäinen vaihe on eri avointen tietolähteiden tunnistaminen. On tärkeää tunnistaa projektilleen kaikista tärkeimmät lähteet, josta tietoa lähdetään etsimään ja keräämään. (Hwang 2022.)

Toinen vaihe on tiedonkeruuvaihe. Tässä vaiheessa kerätään avoimista lähteistä saatu tieto talteen. Tiedonkeruuvaiheessa on kolme tyyppiä; aktiivinen-, puolipassiivinen- ja passiivinen tiedonkeruu. Passiivinen tiedonkeruu on yleisin tiedonkeruutyyppi OSINT-tiedustelussa, koska passiivisessa tiedonkeruussa tietoa kerätään vain julkisesti saatavilla olevien resurssien kautta. Passiivisessa tiedonkeruussa tiedustelun kohde ei saa tietää tiedustelusta, koska tiedustelun kohteeseen ei olla suorassa vuorovaikutuksessa. Passiivista tiedonkeruuta voi tehdä esimerkiksi hyödyntämällä Maltegoa. Aktiivisessa tiedonkeruussa tietoa kerätään suoraan kohteesta. Aktiivinen tiedonkeruu altistaa sille, että kohde tulee tietoiseksi siihen kohdistuvasta tiedustelusta. Tämän tyyppinen tiedustelu jättää jälkiä kohteen IT-infrastruktuuriin ja siitä koituva verkkoliikenne näyttää epäilyttävältä tai haitalliselta. Myös sosiaalista manipulointia pidetään eräänlaisena aktiivisena tiedusteluna. Puolipassiivisessa tiedonkeruussa kohteen palvelimille lähetetään rajoitettua verkkoliikennettä, jotta kohteesta saadaan kerättyä tietoa. (Hassan & Hijazi 2018, 14–15.)

Kolmas vaihe on tiedon prosessointivaihe. Tiedonkeruun aikana kerättyä tietoa on yleensä kerätty valtavasti, joten tieto on suodatettava ja prosessoitava, jotta kerättyä tietoa voidaan hyödyntää tehokkaasti. Tiedosta voidaan koostaa esimerkiksi helppolukuisia kaavioita. (Hwang 2022.)

Neljäs vaihe on tiedon analysointivaihe. Tässä vaiheessa prosessoitu tieto analysoidaan ja tutkitaan, tukeeko tiedustelutieto tiedustelun määriteltyä päämäärää. (Hwang 2022.)

Viides vaihe on raportointivaihe. Tässä vaiheessa luodaan kerätystä tiedosta esimerkiksi raportti tai tilannekuva. Raporttiin lisätään kerätyn tiedon lähteet, jotta tietojen paikkansapitävyys voidaan tarvittaessa tarkastaa. (Hwang 2022.)



Kuvio 4: OSINT-tiedustelun vaiheet (Hwang 2022)

2.7 OSINT-tiedustelun eettisyys

Monet nykyaikaiset organisaatiot ovat dilemman edessä tietojenkäytön suhteen. Koska tietoa on saatavilla valtavasti verkossa saattaa se jättää organisaation alttiiksi riskeille, jotka olisivat voineet olla helposti tunnistettavissa. Avoimesti saatavilla olevan tiedon hyödyntäminen voi johtaa eettisiin huolenaiheisiin ja syytöksiin vastuuttomasta tietojen käytöstä ja esimerkiksi massatiedonkeruun eettisyydestä. (Brown 2023.)

Eettinen tiedonkeruu on mahdollista OSINT-tutkimuksissa, jos tutkimuksissa noudatetaan mahdollisimman eettisiä keinoja tutkimuksien tekemiseen (Brown 2023).

Alla on lueteltu keinoja eettisen OSINT-tutkimuksen suorittamiseen:

1. Tutkimuksessa hyödynnetään julkisesti saatavilla olevaa tietoa aina, kun se on mahdollista. OSINT-tutkimuksissa käytetään avoimista lähteistä saatavia tietoja. Tällä varmistetaan se, että tietoja ei ole saatu laittomista lähteistä, eikä suojattuja tietoja käytetä väärin.
2. Varmistetaan, että tiedonkeruu on mahdollisimman kohdennettua. On tärkeää tunnistaa mitä tietoa kerätään valitusta kohteesta. Suunnittelematon ja summittainen tiedonkeruu voi vaarantaa myös muita organisaatioita tai yksilöitä.
3. Vain ihmisten tulisi tehdä päätöksiä. Tekoälyratkaisut luovat haasteita eettiseen päätöksentekoon, koska tekoälyt eivät osaa arvioida tilanteita ihmislähtöisellä tavalla.

4. Dokumentoidaan kaikki toiminta tutkimuksen aikana. Tällä varmistetaan, että tutkimus pysyy vastuullisena ja eettisenä ja että jokaisesta tutkimuksen työvaiheesta jää jälki. (Brown 2023.)

2.8 OSINT-työkalut

Kuten tässä opinnäytetyössä on todettu jo aiemmin, OSINT-tiedustelua käytetään muun muassa riskienhallintaan, petosten havaitsemiseen ja rikollisuuden torjuntaan. Erilaisia OSINT-työkaluja voidaan hyödyntää avointen lähteiden tiedustelussa. Googlen entisen toimitusjohtaja Eric Schmidtin mukaan noin 99 prosenttia internetissä olevasta tiedosta on piilossa yleisimmiltä hakukoneilta. Erityisesti näiden tietojen keräämiseen käytetään OSINT-työkaluja. (Kadar 2023.)

OSINT-työkalut tukevat yritysten ja organisaatioiden tieto- ja kyberturva-ammattilaisia erilaisten tieto- ja kyberturvariskien tunnistamissa ja niihin vastaamisessa nopeasti. Sosiaalisen median alustat ja verkostot tarjoavat laajasti reaaliaikaista tietoa ja pimeässä verkossa julkaistaan usein varhaisimmat tiedot tietomurroista. (Kadar 2023.)

Organisaatiot, jotka hyödyntävät OSINT-tiedustelua tarvitsevat työkaluja tiedustelunsa tehostamiseen, jotta poikkeamat ja mahdolliset riskit havaittaisiin mahdollisimman nopeasti ja tehokkaasti. OSINT-työkaluilla voidaan helposti indeksoida kerättyä dataa. Tämä auttaa siihen, että data on helposti haettavissa ja suodatettavissa, kun sitä tarvitaan. (Flashpoint 2022.)

Useat OSINT-työkalut toimivat Linux-pohjaisissa järjestelmissä. Kali Linuxissa on vakiona saatavilla monia OSINT-työkaluja, esimerkiksi Maltego. (Hassan & Hijazi 2018, 93.)

Tässä osassa esittelen kymmenen yleisesti käytettyä OSINT-työkalua.

1. Maltego

   Maltego on Java-pohjainen avoimen lähdekoodin ohjelmisto, joka toimii Windows-, Mac- ja Linux-alustoilla. Sitä käytetään avoimen tiedon etsintään henkilöistä, verkkotunnuksista ja yrityksistä. Maltego osaa piirtää hakemistaan tiedoistaan helposti luettavia kaavioita.

   Maltego toimii siten, että se automatisoi haun eri julkisista tietolähteistä. Maltegon mukana on valmiina useita avoimia tietolähteitä (noin 58 kappaletta), kuten DNS-tietueita, whois-tietueita, eri hakukoneita ja sosiaalisia verkostoja. Tietolähteitä voi ladata Maltegoon myös manuaalisesti. Kun tiedot on haettu ja kerätty, Maltego muodostaa tietojen välille yhteyksiä. Nämä yhteydet voivat paljastaa piilotettuja yhteyksiä esimerkiksi nimien, sähköpostiosoitteiden, yritysten verkkosivujen ja dokumenttien välillä. Tiedot voivat olla hyödyllisiä verkkorikollisuuden torjunnassa.

Ohjelmasta on saatavilla ilmainen- ja PRO-versio. Ilmaisessa versiossa on rajoitetut ominaisuudet. (Breeden II, Fruhlinger & Sharma 2021.)

2. Google

Google on läntisen maailman suosituin hakukone ja vierailluin verkkosivusto. Se käyttää algoritmia, joka on suunniteltu hakemaan ja järjestelemään hakutuloksia, jonka perusteella se tarjoaa mahdollisimman osuvia ja luotettavia tietolähteitä. (Rouse 2020.)

3. Google Maps

Google Maps on Googlen tuottama verkkopalvelu, joka tarjoaa yksityiskohtaista maantieteellistä tietoa ympäri maailmaa. Google Maps tarjoaa muun muassa tiekarttoja sekä satelliitti- ja ilmanäkymiä. Joissain paikoissa ja kaupungeissa se tarjoaa myös katunäkymiä kohteista.

Google Maps tarjoaa apua reittisuunnitteluun ja tarjoaa reittiohjeita autoilijoille, pyöräilijöille, jalankulkijoille ja joukkoliikenteen käyttäjille. Lisäpalveluna se tarjoaa kuvia taivaasta, planeetoista, tähdistä ja kuusta. (Zola 2023.)

4. Have I Been Pwned?

Suurin osa internetistä löydetyistä murretuista tiedoista on käyttäjätunnuksia, salasanoja ja sähköpostiosoitteita. Have I Been Pwned on verkkosivusto, joka tarjoaa mahdollisuuden tarkastaa onko tietojasi päässyt vuotamaan mahdollisissa tietomurroissa. Kaikki sivustolla oleva tieto on peräisin tietomurroista, joissa olevien tietojen ei olisi pitänyt olla näkyvissä julkiselle yleisölle. Sivusto kertoo, että missä ja milloin mahdollinen tietomurto on tapahtunut. (Hunt 2023.)

5. Google Hacking (Google Dorking)

Google Hacking (tunnetaan myös nimellä Google Dorking) on keino käyttää Googlen hakutoimintoa esimerkiksi haavoittuvuuksien löytämiseen tai sellaisten tietojen etsimiseen, jotka eivät ole saatavilla julkisissa hakutuloksissa. Google Hackingissä käytetään hauissa eri operaattoreita ja komentoja. Esimerkiksi jos tietoa halutaan etsiä tietyltä verkkosivustolta, voidaan tietoa hakea seuraavalla komennolla Googlen hausta: site: google.fi. (Maltego 2021.)

6. Recon-ng

   Recon-ng on tehokas ilmainen työkalu eri kohteiden tiedusteluun. Se on Python-pohjainen ja hieman teknisempi työkalu kuin muut tässä esitellyt työkalut, koska siinä on pelkästään komentorivikäyttöliittymä. Recon-ng:n avulla voidaan arvioida ja tunnistaa verkkohaavoittuvuuksia. Sen ominaisuuksiin kuuluu DNS-haku, porttiskannaus ja GeoIP-haku. (Kadar 2023.)

7. SpiderFoot

   SpiderFoot on ensisijaisesti suunniteltu kyberturvallisuuden asiantuntijoiden käyttöön. Sitä käytetään muun muassa IP-osoitteiden, verkkotunnuksien, sähköpostiosoitteiden, puhelinnumeroiden, nimien ja osoitteiden keräämiseen ja analysoimiseen. Työkalu käyttää satoja avoimia tietolähteitä ja seuraa tuloksia reaaliajassa. SpiderFootin saa ilmaisversiona tai maksullisena versiona. Maksullisessa versiossa on monia parannuksia ilmaiseen versioon verrattuna, esimerkiksi parempi suorituskyky ja rajapinta hakujen tekemiseen pimeästä verkosta. (Kadar 2023.)

8. Lampyre

   Lampyre on maksullinen työkalu, joka on suunniteltu erityisesti OSINT-tiedustelua varten. Sitä käytetään muun muassa due diligence-tarkastuksissa, kyberuhkien tiedustelussa, rikosten analysoinnissa ja talousanalytiikassa. Siinä on valmiina noin 100 erilaista avointa tietolähdettä. Sen voi asentaa suoraan tietokoneelle tai käyttää verkkoselaimessa. (Kadar 2023.)

9. Shodan

   Shodan on työkalu, jolla pääasiassa etsitään avointa tietoa IoT-laitteista (Internet of Things). Shodania voidaan käyttää myös avoimien porttien ja haavoittuvuuksien etsintään. Shodanin avulla voidaan tunnistaa eri kohteiden sisältämiä haavoittuvuuksia. Perusversio Shodanista maksaa 59 dollaria kuukaudessa. (Breeden II, Fruhlinger & Sharma 2021.)

10. theHarvester

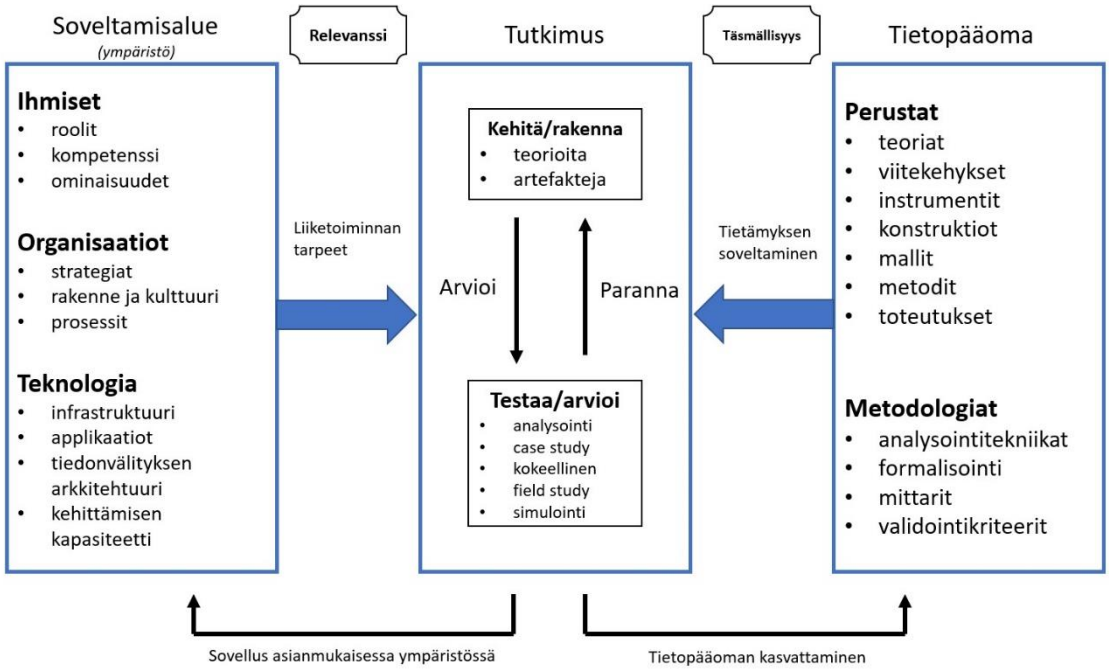
    theHarvester on yksi yksinkertaisimmista OSINT-työkaluista. Se on suunniteltu keräämään tietoa organisaation omistaman verkon ulkopuolelta. Työkalun käyttämiä lähteitä ovat yleisimmät hakukoneet (Google, Bing) sekä esimerkiksi dogpile, DNSdumpster ja Exalead. theHarvesterilla voi kerätä esimerkiksi sähköpostiosoitteita, nimiä,

verkkotunnuksia ja IP-osoitteita. Työkalun voi ladata ilmaiseksi GitHubista. (Breeden II, Fruhlinger & Sharma 2021.)

3 Opinnäytetyön tutkimusmenetelmä

Tässä luvussa käsittelen opinnäytetyöni tutkimusmenetelmää ja sen soveltamista opinnäytetyön tekemiseen.

IT-alalla hyödynnetään yleisesti suunnittelutiedettä tutkimusotteena. Suunnittelutieteellisellä tutkimuksella pyritään parantamaan kohdeympäristöä/soveltamisaluetta suunnittelemalla ja implementoimalla uusia ja innovatiivisia konstruktioita (artefakteja). Soveltamisalue koostuu ihmisistä, organisaatioon liittyvistä rakenteista ja prosesseista sekä teknisistä järjestelmistä, joita hyödyntämällä pyritään ratkaisemaan jokin käytännöllinen ongelma. Hyvä suunnittelutieteellinen tutkimus alkaa sillä, että tunnistetaan relevantti ongelma soveltamisalueella. (Hevner 2007, 88–89.)



Kuvio 5: Suunnittelutieteellinen tutkimuskehys (Hevner, March, Park & Ram 2004, 80.)

Suunnittelutieteen systematiikkaa kuvataan seitsemän periaatteen avulla. Suunnittelutieteellinen tutkimus edellyttää innovatiivisen ja tarkoituksellisen tuotoksen/konstruktion luomista spesifin ongelman ratkaisemiseksi. Konstruktio voi olla esimerkiksi konkreettinen laite tai toimintamalli (periaate 1). (Hevner ym. 2004, 82–83.)

Tutkimuksen tavoitteena on kehittää konstruktio, jonka avulla pyritään ratkaisemaan jokin todellinen ja käytännöllinen ongelma. Lähtökohtaisesti kuvatun kaltainen ongelma voi olla esimerkiksi jokin toistaiseksi ratkaisematon teknologiaa hyödyntävä liiketoimintaan liittyvä ongelma (periaate 2). (Hevner ym. 2004, 84–85.).

Arviointi on olennainen osa tutkimusprosessia. Konstruktion hyödyllisyys, laatu ja tehokkuus on osoitettava testaamalla konstruktio huolellisesti. Toteutetun konstruktion tulisi ratkaista kohdeorganisaation alkuperäinen ongelma. Kohdeorganisaatio, jossa uutta konstruktiota hyödynnetään määrittelee vaatimukset konstruktion arvioinnille ja testaamiselle (periaate 3). (Hevner ym. 2004, 85.)

Tehokas suunnittelutieteellinen tutkimus tarjoaa lisäarvoa myös tieteellisestä näkökulmasta. Konstruktio, joka on tehty soveltamalla suunnittelutiedettä voi antaa huomattavaa tieteellistä lisäarvoa, jos konstruktion suorituskyky on parempi kuin aikaisemmat samaan tarkoitukseen käytetyt ratkaisut tai se soveltaa uutta teknologiaa (periaate 4). (Hevner ym. 2004, 87.)

Suunnittelutieteellinen tutkimus vaatii kurinalaista ja systemaattista toimintatapaa. Systemaattisuudella tarkoitetaan sitä, että tutkimusote ja -menetelmä valitaan huolellisesti ja niihin perehdytään sopivalla laajuudella. Konstruktiosta tulee laatia vaatimusmäärittely ja konstruktion testaamisesta saatuja tuloksia tulee verrata vaatimusmäärittelyyn. Suunnittelutyön ohessa tulee perehtyä täsmällisesti olemassa olevaan tietopääomaan ja lopuksi kuvata suunnittelutyön tuomaa lisäarvoa suhteessa olemassa olevaan tietopääomaan (periaate 5). (Hevner ym. 2004, 87–88.)

Suunnittelutiede on luonnostaan iteratiivista. Parhaan tai optimaalisimman konstruktion tuottaminen ja testaus on usein työlästä. Pohjimmiltaan suunnittelu on erilaisten ratkaisujen ideointia ja testausta parhaimman ja tehokkaimman lopputuloksen saavuttamiseksi. Huolellisesti tehdyssä suunnittelutyössä perehdytään jo olemassa oleviin ratkaisuihin. Olemassa olevia ratkaisuja hyödynnetään ja sovelletaan uudessa ympäristössä tai olosuhteissa (periaate 6). (Hevner ym. 2004, 88.)

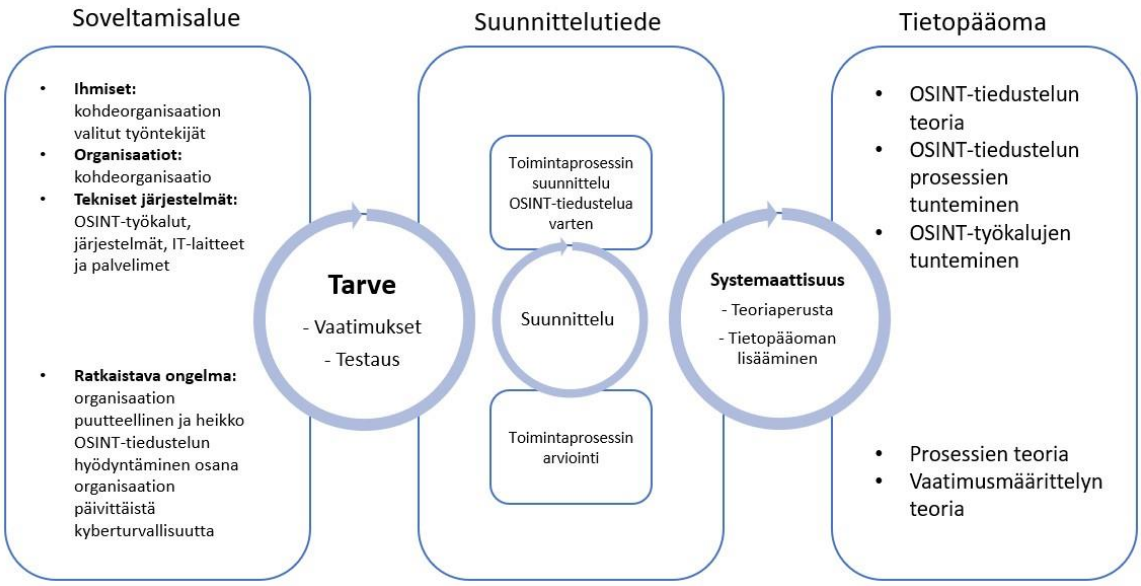
Tieteelliseen tekemiseen liittyvissä töissä työn julkisuus ja tulosten julkaiseminen ovat keskeisiä asioita. Tulokset tulisi julkaista siten, että tulokset ovat luettavissa ja ymmärrettävissä teknologiaorientoituneen yleisön ja päätöksentekijöiden joukossa. Teknologiaorientoitunut yleisö tarvitsee riittävästi yksityiskohtia konstruktiosta, jotta he voivat hyötyä sen tarjoamista

eduista ja tiedoista. Päätöksentekijät tarvitsevat yksityiskohtaista, mutta ei niin teknistä tietoa konstruktiosta, jotta he voivat määritellä sen arvon organisaatiolleen (periaate 7). (Hevner ym. 2004, 90.)

Suunnittelutieteen soveltamisen periaatteet	
Periaate	**Kuvaus**
Periaate 1: Tuotos on konstruktio	Suunnittelutieteen soveltamisen tuotoksena on konkreettinen tuote tai toimintamalli
Periaate 2: Todellinen ongelma	Suunnittelutieteen soveltamisen tavoitteena on ratkaista jokin merkityksellinen ongelma teknologiaa soveltaen
Periaate 3: Tulosten arviointi	Toteutuksen toimivuus, laadukkuus ja suorituskyky tulee osoittaa testaamalla tuotos huolellisesti
Periaate 4: Tieteellinen arviointi	Suunnittelutieteen soveltamisen tulee luoda selkeää ja arvioitavissa olevaa tieteellistä arvoa uutuudellisena tuotoksena, suunnittelutietämyksenä tai -menetelmänä
Periaate 5: Systemaattisuus	Suunnittelutieteen tuotosta luotaessa ja arvioitaessa tulee noudattaa systemaattista suunnittelumetodiikkaa
Periaate 6: Tunnetun tiedon soveltaminen	Toimivan konstruktion toteuttamisessa sovelletaan ja arvioidaan aiemmin tunnettuja menetelmiä ja ratkaisuja uudessa tilanteessa, kunnes tavoiteltu lopputulos saavutetaan
Periaate 7: Tulosten julkaiseminen	Suunnittelutieteen soveltamisen tulokset tulee julkaista siten, että ne ovat sekä teknisesti orientoituneiden ihmisten, että päätöksentekijöiden hyödynnettävissä

Taulukko 2: Suunnittelutieteen soveltamisen periaatteet (Hevner ym. 2004)

Alla olevassa kuviossa kuvaan opinnäytetyöni nojaten suunnittelutieteelliseen viitekehykseen ja avaan viitekehyksen tutkimussyklejä.



Kuvio 6: Suunnittelutieteellisen tutkimuksen viitekehys opinnäytetyössä (Jokinen 2021.)

Suunnittelutieteellisen tutkimuksen viitekehyksessä on kuvattu kolme tutkimussykliä: Relevance Cycle (tarve), Design Cycle (suunnittelu) ja Rigor Cycle (systemaattisuus). Relevance cycle yhdistää tutkimuksen kontekstuaalisen soveltamisalueen suunnittelutieteelliseen tutkimukseen ja siihen liittyviin toimintoihin. Tällä pyritään määrittelemään tutkimuksen vaatimukset (esimerkiksi ongelma, joka pyritään käsittelemään tutkimuksen avulla) ja testaustarpeet (miten suunniteltu konstruktio parantaa soveltamisaluetta/ympäristöä ja miten tehtyä parannusta voidaan mitata). Suunniteltu tuotos implementoidaan soveltamisalueelle sen tutkimista ja arviointia varten. (Hevner 2007, 89.)

Rigor Cycle tarjoaa teoriaperustan tutkimusprojektille. Suunnittelutiede ammentaa laajasta tietopääomasta tieteellisiä teorioita ja teknisiä menetelmiä, jotka luovat systemaattisen perustan suunnittelutieteelliselle tutkimukselle. Suunnittelutieteellistä tutkimusta tehdessä on tärkeää viitata tietopääomaan. Tietopääoma kasvaa vastavuoroisesti tutkimuksen edetessä. (Hevner 2007, 89–90.)

Design Cycle on minkä tahansa suunnittelutieteellisen tutkimuksen sydän. Suunnittelusyklissä tuotosta suunnitellaan ja arvioidaan. Suunnittelusyklin vaatimukset on syötetty Relevance Cy-

clesta ja teoriatieto ja menetelmät on syötetty Rigor Cyclesta. Suunnittelusykli on suunnittelutieteellisen tutkimuksen työläin ja haastavin osa. On tärkeää ymmärtää Design Cyclen riippuvuus Relevance- ja Rigor Cycleihin. (Hevner 2007, 90–91.)

Opinnäytetyössäni viitekehyksen muodostavat soveltamisalueena kohdeorganisaatio, tutkimuksena toimintaprosessin suunnittelu OSINT-tiedustelua varten ja tietopääoma, jota tarvitaan tutkimuksen tekemiseen.

4 OSINT-tiedustelun implementointi osaksi kohdeorganisaation kyberturvallisuutta

Tässä luvussa käsittelen OSINT-tiedustelun implementointia osaksi kohdeorganisaation kyberturvallisuutta suunnittelemalla organisaatiolle toimintaprosessin OSINT-tiedustelua varten.

4.1 Työn tausta, alkutilanne ja tavoite

Työn taustana toimii kohdeorganisaation jatkuva tarve kehittää kyberuhkilta ja vaikuttamiselta suojautumistaan ja jalkauttaa OSINT-tiedustelu osaksi organisaation jokapäiväistä kyberturvallisuutta. Kohdeorganisaationa opinnäytetyössä toimii kansainvälinen finanssialan toimija. Kohdeorganisaatiota koskevat havainnot esitetään yksinkertaistettuna ja anonyymisti, koska kohdeorganisaatio on huoltovarmuuskriittinen toimija.

Opinnäytetyön tutkimuskysymys on miten implementoida OSINT-tiedustelu osaksi organisaation kyberturvallisuutta.

Opinnäytetyön tutkimuksella pyritään luomaan ratkaisu kohdeorganisaation OSINT-tiedustelun jalkauttamiseksi organisaation käyttöön, koska organisaatiossa on tunnistettu OSINT-tiedustelun puutteellinen ja heikko hyödyntäminen. Opinnäytetyössä suunnitellaan toimintaprosessi kohdeorganisaatiolle OSINT-tiedustelua varten. Tutkimuksen hyötyä pyritään arvioimaan tutkimuksen tuloksena syntyvän toimintaprosessin, sekä sen työkalujen ja menetelmien tarkoituksenmukaisuuden ja hyödyllisyyden näkökulmasta kohdeorganisaatiolle. Toimintaprosessin toimivuutta testataan suorittamalla anonymisoitu OSINT-tutkimus henkilöstä, joka on antanut luvan tutkimuksen tekemiseen.

4.2 Prosessit yleisesti

Jokainen organisaatio tekee asioita saavuttaakseen tavoitteensa. Näitä asioita ovat esimerkiksi työntekijöiden rekrytointi, uusien asioiden suunnittelu ja tilausten käsittely. Edellä mainitut asiat sisältävät prosesseja. Prosessi on toisiinsa liittyvien tehtävien ja erilaisten tapahtumien muodostama yhtenäinen kokonaisuus ja sitä voisi kuvata tapahtumien kehityskulkuna. Prosessi sisältää toimintaa: ihmiset ja koneet tekevät asioita saavuttaakseen määriteltyjä tavoitteita. (Ould 2005, 3–6.)

Prosesseja tehdään syystä ja niillä on aina jokin tavoite. Joskus tavoitetta ei saavuteta, tai prosessin lopputuloksena on jokin muu tulos tai epäonnistuminen. Prosessin tavoitteena saattaa olla esimerkiksi tietokoneohjelman suunnittelu, budjetin hallinnointi tai sairaanhoitopalvelujen tarjoaminen. Prosessin mallinnuksesta tulisi näkyä, kuinka prosessilla saavutetaan sille asetetut tavoitteet. Ennen uuden prosessin suunnittelua tulisi miettiä seuraavia asioita: mitä parannuksia prosessilla haetaan, ovatko parannukset pieniä vai suuria, onko prosessin tarkoitus ja mekanismit hyödyllisiä organisaatiolle ja missä kohtaa prosessia sen onnistumista mitataan. (Ould 2005, 32, 271.)

Mitä selkeämmin organisaatio tai yritys määrittelee prosessinsa ja mitä johdonmukaisemmin niitä toteutetaan päivittäisessä toiminnassa, sitä tehokkaampia prosessit ovat. Monen organisaation ja yrityksen kilpailukyky ei nykypäivänä perustu enää pelkkään tarjoamansa tuotteen ainutlaatuisuuteen, vaan tuotteen hankinnan prosessien laatuun. Sujuvat prosessit ovat avain menestykseen. Prosessien mukautus muuttuvaan maailmaan on tärkeää ja niiden tulisi olla tarpeeksi selkeitä ja tarkkoja, jotta organisaation työntekijät voivat hyödyntää prosesseja jokapäiväisessä työssään. (Fleischmann, Oppl, Schmidt & Stary 2020, 1–2.)

Prosessin implementoinnilla viitataan strategiseen lähestymistapaan, jolla organisaatiota autetaan omaksumaan uusia menettelytapoja. Organisaatiot ottavat käyttöönsä uusia prosesseja eri syistä, kuten esimerkiksi päivittäisten tehtävien tehostamiseksi, virheiden minimoimiseksi ja liiketoiminnan kasvun edistämiseksi. Prosessin implementointi sisältää usein ohjeet uusien tehtävien toteuttamiseksi ja loppuun saattamiseksi organisaatiossa. Uusien prosessien implementoinnilla organisaatioon on monia hyötyjä, kuten työn tehokkuuden ja laadun paraneminen, tehtävien ja prosessien läpinäkyvyyden lisääminen ja tehtävien skaalautuvuuden varmistaminen. (Indeed 2023.)

Uuden toimintaprosessin implementoimiseksi organisaatioon tehokkaasti on hyvä miettiä implementointiprosessi huolellisesti. Implementointiprosessi tulisi aloittaa määrittelemällä uusi prosessi ja siihen liittyvät vaatimukset. Suunnittelu on onnistumisen kannalta tärkeää. Halutut tavoitteet, resurssit ja työkalut tulisi tunnistaa. Organisaation henkilöt, joita uusi prosessi koskee tulisi kouluttaa uuden prosessin käyttöön ajoissa, jotta prosessin käyttöönottovaiheessa uusi prosessi olisi jo tuttu. Kun prosessin vaatimukset ja tavoitteet on mietitty huolella, on helpompaa myös tarkastella prosessin käyttöönoton jälkeen uuden prosessin tehokkuutta ja toimintaa. (Indeed 2023.)

4.3 Toimintaprosessin suunnittelu kohdeorganisaatiolle

Toimintaprosessin suunnittelu kohdeorganisaatiolle lähti organisaation tarpeiden tunnistamisesta. Organisaatiossa oli tunnistettu avointen lähteiden tiedustelun hyödyntämisen heikkous ja puutteellisuus, ja siihen ei liittynyt mitään vakiintuneita prosesseja. Tästä syntyi idea suunnitella kohdeorganisaatiolle OSINT-tiedustelua varten toimintaprosessi. Toimintaprosessi on suunniteltu nojautuen tieteelliseen tietoon.

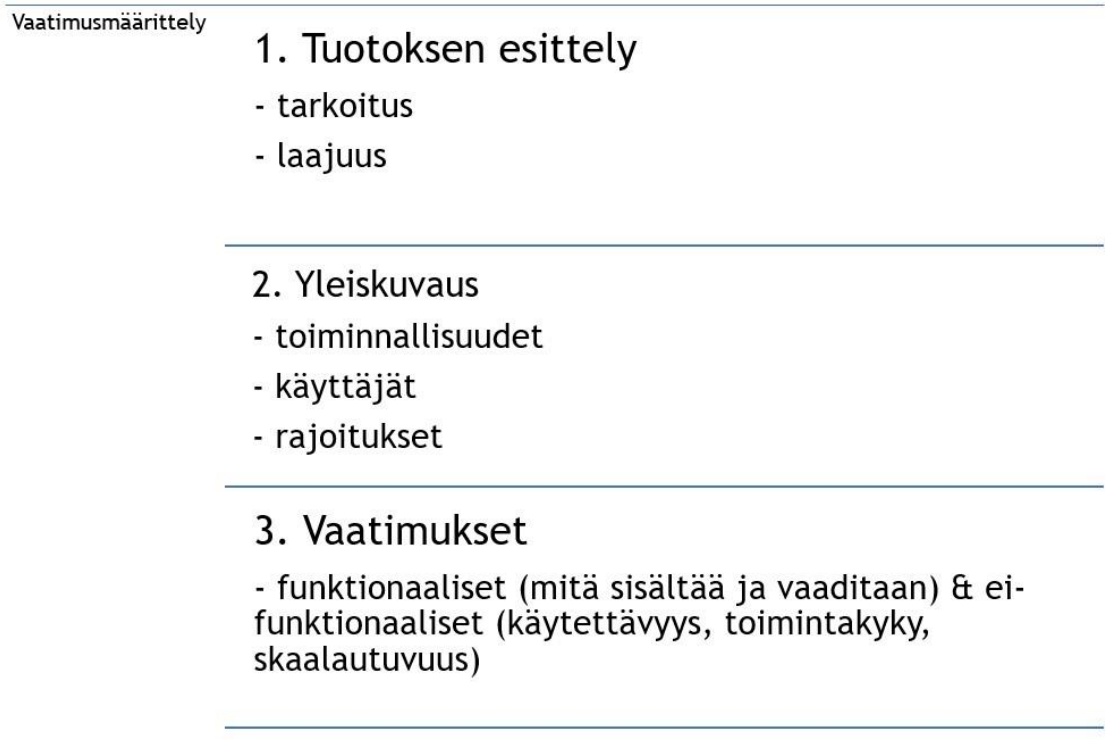
Tieto- ja kyberturvan peruspilareita ovat tiedon luottamuksellisuuden (Confidentiality), eheyden (Integrity) ja saatavuuden (Availability) turvaaminen ja suojaaminen. Nämä yhdessä muodostavat niin kutsutun CIA triadin. Kun arkaluontoista tietoa välitetään ja joku ulkopuolinen pääsee tietoihin käsiksi, on silloin kyseessä tiedon luottamuksellisuuden rikkoutuminen. Jos tietoja muutetaan tai tiedot menevät sekaisin, on silloin kyseessä tiedon eheyden rikkoutuminen. Jos tiedot eivät ole saatavilla tai tiedon saaminen estetään, on silloin kyseessä tiedon saatavuuden rikkoutuminen. Organisaatioiden tehtävänä on turvata näitä tietoja mahdollisimman tehokkaasti. Samalla turvataan muun muassa organisaation IT-laitteita, henkilöstöä ja pyritään pienentämään hyökkäyspinta-alaa. Jos organisaatio ei kykene turvaamaan ja suojaamaan tietoa, voi tällä olla esimerkiksi suuriakin taloudellisia vaikutuksia, lisätyötä henkilöstölle, lakiasioiden läpikäymistä ja mainehaittaa. (Gatlin, Yampolskiy & Yung 2021, 4.) OSINT-tiedustelulla pyritään parantamaan myös tiedon turvaamista ja suojaamista kohdeorganisaatiossa.

Kuvio 7: CIA Triad

Tämän jälkeen prosessin suunnittelulle luotiin vaatimusmäärittely.

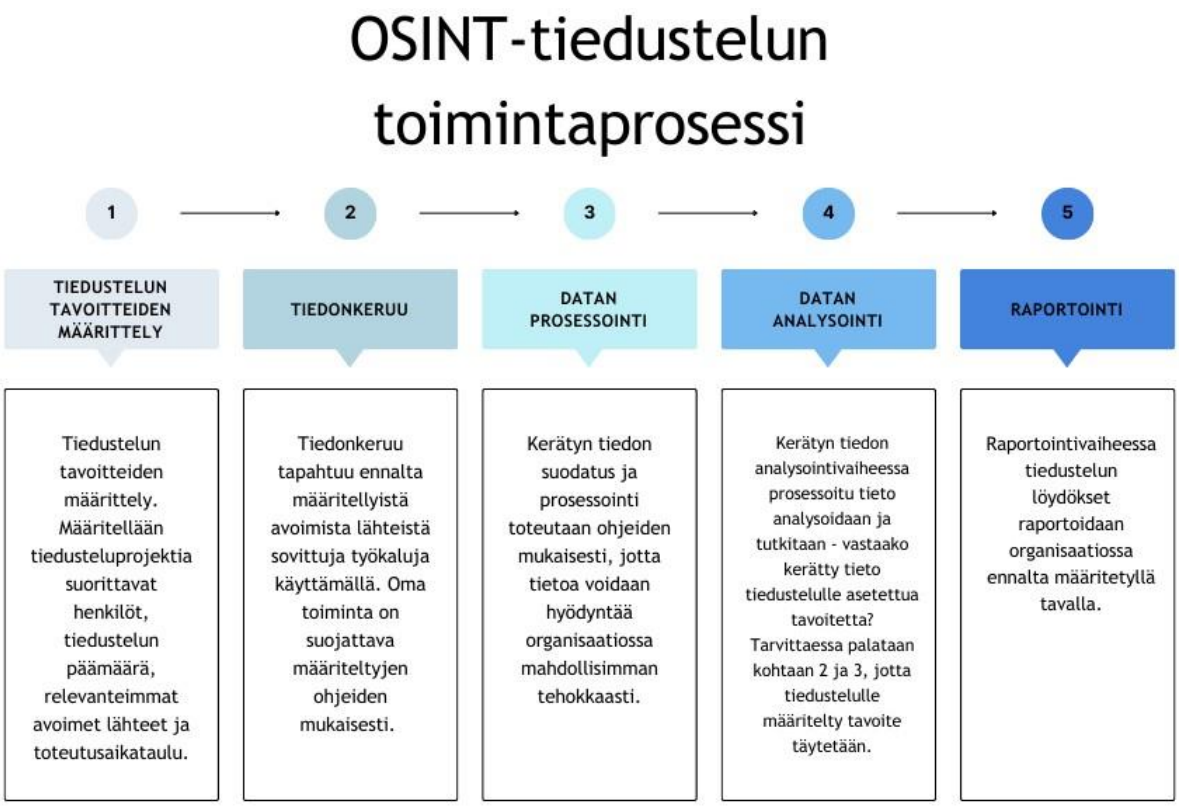
Vaatimusmäärittely on dokumentaatio, johon kirjataan mitä vaatimuksia suunnitellulta tuotokselta vaaditaan. Dokumenttiin kirjataan tuotoksen käyttötarkoitus, eri ominaisuudet ja minkä ongelman ratkaisua tuotoksella haetaan. Vaatimusmäärittelyn luominen on avain menestykseen, kun kehitellään esimerkiksi tietojärjestelmiä. Vaatimusmäärittely on ensimmäinen askel kehitys- ja suunnitteluprojektissa ja sen täsmällisyydellä on merkittävä vaikutus kehitys- ja suunnitteluprojektin tuotoksen tehokkuudessa ja onnistumisessa. (Conger & Vessey 1994, 102.)

Anonymiteetin säilyttämiseksi tässä opinnäytetyössä OSINT-tiedustelun toimintaprosessin vaatimusmäärittely on esitetty yksinkertaistettuna. Vaatimusmäärittelyssä on määritelty prosessin suunnittelun tarpeet ja lähtökohta. Kuten aiemmin on mainittu, tässä opinnäytetyössä prosessin suunnittelun lähtökohta ja tarpeet perustuvat kohdeorganisaation tarpeeseen ja oikeaan ongelmaan. Lähtökohtana oli kehitellä toimiva, selkeä ja tehokas toimintaprosessi avointen lähteiden tiedustelua varten. Vaatimusmäärittelyssä on esitelty myös prosessin suunnittelun yleiskuvaus, joka kattaa toimintaprosessin laajuuden, toiminnallisuudet, käyttäjät, rajoitukset, funktionaaliset vaatimukset (mitä prosessi sisältää ja mitä siltä vaaditaan, että se vastaa haluttua käyttötarkoitusta) ja ei-funktionaaliset vaatimukset (skaalautuvuus, toimintakyky ja käytettävyys, eli laadulliset vaatimukset).



Kuvio 8: Esimerkki vaatimusmäärittelystä

Alla olevassa kuviossa kuvaan suunnittelemaani toimintaprosessia OSINT-tiedustelua varten ja avaan prosessin sisältöä.



Kuvio 9: Yksinkertaistettu OSINT-tiedustelun toimintaprosessi

OSINT-tiedustelun toimintaprosessia tullaan hyödyntämään kohdeorganisaatiossa pääasiassa uhkatiedustelua (Threat Intelligence) varten. Ihanteellisessa skenaariossa uhkatiedustelu on osa jokaisen organisaation kyberturvallisuusstrategiaa. Olemassa olevien ja mahdollisten uusien uhkien monitorointi, johdonmukainen tiedon kerääminen ja analysointi lisää organisaation kykyä suojata itseään kyberrikollisuudelta. Uhkatiedustelun elinkaari (Threat Intelligence Lifecycle) sisältää kuusi vaihetta. Vaiheet ovat tavoitteiden määrittely uhkatiedustelulle, datan kerääminen, datan prosessointi, datan analysointi, tulosten läpikäynti ja palaute. (Snyk 2023.)

Toimintaprosessi alkaa tiedustelun tavoitteiden määrittelyllä. Tässä vaiheessa määritellään tiedustelulle päämäärä ja valitaan tiedustelua suorittavat henkilöt. Pääasiassa tiedustelua suorittavat organisaatiossa ennalta määritellyt työntekijät, jotka ovat tiedusteluorientoituneita. Tähän vaiheeseen kuuluu myös relevanteimpien avointen lähteiden valitseminen, jotta tiedustelusta saadaan mahdollisimman paljon irti. Samalla määritellään tiedusteluprojektin aikataulu.

Prosessin tiedonkeruuvaiheessa tietoa haetaan niistä avoimista lähteistä, jotka määriteltiin toimintaprosessin ensimmäisessä vaiheessa. Tietoa kerätään ennalta määritetyillä työkaluilla, jotka ovat hyväksytetty organisaatiossa tiedustelutarkoituksiin. OSINT-tiedusteluun usein käytettyjä työkaluja ovat esimerkiksi Maltego ja SpiderFoot. Oma toiminta on suojattava organisaatiossa määritellyin tavoin, kun tietoa kerätään avoimista lähteistä varsinkin silloin, jos tehdään aktiivista tiedustelua passiivisen tiedustelun lisäksi tai tietoa kerätään pimeästä verkosta.

Prosessin kolmannessa vaiheessa tiedonkeruuvaiheessa kerätty data suodatetaan ja prosessoidaan. Kerätyn datan suodatus ja prosessointi toteutetaan organisaation ohjeiden mukaisesti. Kerätyn datan tulisi vastata tiedustelulle asetettuja tavoitteita.

Prosessin neljännessä vaiheessa prosessoitu ja suodatettu data analysoidaan ja tutkitaan. Tässä vaiheessa määritellään, vastasiko kerätty data tiedustelutavoitetta. Jos analysoitu data vastaa tiedustelutavoitetta, voidaan siirtyä prosessin viimeiseen vaiheeseen (raportointi). Jos kuitenkin todetaan, että analysoitu data ei vastaa tiedustelutavoitetta, toistetaan prosessin kohdat kaksi ja kolme uudestaan, jotta tiedustelutavoitteeseen päästään ja analysoitu data on tarkkaa ja sen hyödyntäminen tehokasta. Jos kohdat kaksi ja kolme joudutaan toistamaan, voidaan määritellä myös uusia avoimia lähteitä, joista tietoa etsitään.

Toimintaprosessin viimeinen vaihe on raportointivaihe. Tässä vaiheessa analysoitu tieto raportoidaan. Tiedustelun löydökset raportoidaan organisaatiossa ennalta määritetyllä tavalla ja ennalta määritetyille henkilöille ja/tai yksiköille. Tuotetun raportin tulisi olla selkeä ja ytimekäs, jotta myös ei niin teknologiaorientoituneet henkilöt ymmärtävät raportissa esitellyt asiat. Raportin ja tiedustelussa nousseiden tietojen perusteella määritellään mahdolliset jatkotoimenpiteet organisaation suojaamiseksi.

4.4 Toimintaprosessin testaus

Toimintaprosessia testattiin suorittamalla OSINT-tutkimus organisaation työntekijästä. Häneltä kysyttiin lupa tutkimuksen tekemiseen. Tiedustelulle määriteltiin selkeät tavoitteet. Tavoitteena oli löytää henkilöstä mahdollisimman paljon tietoa, jolla voitaisiin suorittaa esimerkiksi kohdistettu tietojenkalasteluhyökkäys henkilöä kohtaan. Opinnäytetyön tekijä suoritti tämän OSINT-tutkimuksen. Aikatauluksi määriteltiin huhtikuu 2023, mutta tiedustelutavoitteeseen päästiin jo huhtikuun alussa. Tietolähteinä käytettiin pääasiassa sosiaalista mediaa. Tähän OSINT-tutkimukseen oli määritelty erikseen käytettävät työkalut. Työkaluina käytettiin muun muassa Maltegoa, SpiderFootia, Googlea ja Google Mapsia. Tiedonkeruu oli nopeaa ja tiedustelutavoitetta vastaavat tiedot löydettiin kohtuullisen vaivattomasti. Kerätty tieto analysointiin ja varmistettiin, että kerätty tieto on relevanttia. Tiedon relevanttius tarkastettiin ristitarkastelemalla useampia lähteitä. Tässä tutkimuksessa ei ollut tarvetta palata toimintaprosessin vaiheisiin kaksi ja kolme. Henkilöstä saatiin kerättyä tiedustelutavoitetta vastaavaa

tietoa riittävä määrä. Tiedon laatu oli sellaista, että sillä olisi voinut kohdistaa henkilöön esimerkiksi kohdistettua tietojenkalastelua tai muuta vaikuttamista ja kiristystä. Tiedon analysoinnin jälkeen tiedustelun löydöksistä luotiin raportti, joka luovutettiin tiedustelun kohteelle. Tämän jälkeen tiedusteluraportti käytiin läpi tiedustelun kohdehenkilön kanssa. Tiedustelun kohdehenkilölle annettiin neuvoja, miten hän pystyy suojautumaan verkossa paremmin. Korjausliikkeet henkilön omassa toiminnassa verkossa eivät vaatineet isoja muutoksia.

4.5 Tutkimuksen ja sen lopputuloksen arviointi

Opinnäytetyön tutkimus suoritettiin suunnittelutieteellisellä metodilla. Tutkimukseen hyödynnettiin Hevnerin ja muiden (2004, 80–90) suunnittelutieteellistä viitekehystä ja suunnittelutieteellisen tutkimuksen seitsemää periaatetta. Viitekehys, seitsemän periaatetta ja suunnittelutiedettä koskeva ohjeistus oli selkeä ja soveltuva tämän tutkimuksen tekemiseen. Tutkimuksen teoriapohjana käytettiin tieteellisiä artikkeleita, kirjallisuutta ja muuta OSINT-tiedusteluun liittyvää materiaalia.

Seuraavaksi avaan suunnittelutieteen seitsemän periaatteen soveltamisen soveltuvuutta opinnäytetyön tutkimukseen (Hevner ym. 2004, 82–90). Tutkimus on pyritty tekemään täsmällisesti soveltaen suunnittelutieteen seitsemää periaatetta ja vastaamaan periaatteissa esitettyjä asioita.

1. Suunnittelutieteellinen tutkimus edellyttää innovatiivisen ja tarkoituksellisen tuotoksen/konstruktion luomista spesifin ongelman ratkaisemiseksi. Konstruktio voi olla esimerkiksi konkreettinen laite tai toimintamalli. (Hevner ym. 2004, 82–83.)

   Tässä tutkimuksessa kohdeorganisaatiolle luotiin toimintaprosessi OSINT-tiedustelua varten, jolla ratkaistiin organisaation tarve kehittää organisaation sisäistä OSINT-tiedustelun puutteellista ja heikkoa toimintatapaa.

2. Tutkimuksen tavoitteena on kehittää konstruktio, jonka avulla pyritään ratkaisemaan jokin todellinen ja käytännöllinen ongelma. Lähtökohtaisesti kuvatun kaltainen ongelma voi olla esimerkiksi jokin toistaiseksi ratkaisematon teknologiaa hyödyntävä liiketoimintaan liittyvä ongelma. (Hevner ym. 2004, 84–85.).

   Tutkimuksen lopputuloksena syntynyt toimintaprosessi ratkaisee kohdeorganisaation ongelman, joka liittyi heikkoon avointen lähteiden tiedustelun hyödyntämiseen organisaatiossa.

3. Arviointi on olennainen osa tutkimusprosessia. Konstruktion hyödyllisyys, laatu ja tehokkuus on osoitettava testaamalla konstruktio huolellisesti. Toteutetun konstruktion tulisi ratkaista kohdeorganisaation alkuperäinen ongelma. Kohdeorganisaatio, jossa

uutta konstruktiota hyödynnetään määrittelee vaatimukset konstruktion arvioinnille ja testaamiselle. (Hevner ym. 2004, 85.)

Toimintaprosessi testattiin huolellisesti ja sen todettiin vastaavan toimintaprosessin toimivuudelle asetettuja tavoitteita.

4. Tehokas suunnittelutieteellinen tutkimus tarjoaa lisäarvoa myös tieteellisestä näkökulmasta. Konstruktio, joka on tehty soveltamalla suunnittelutiedettä voi antaa huomattavaa tieteellistä lisäarvoa, jos konstruktion suorituskyky on parempi kuin aikaisemmat samaan tarkoitukseen käytetyt ratkaisut tai se soveltaa uutta teknologiaa. (Hevner ym. 2004, 87.)

   Tutkimuksen pohjalta syntynyt toimintaprosessi tarjoaa kohdeorganisaatiolle räätälöidyn prosessin OSINT-tiedustelun suorittamiseksi organisaatiossa. Toimintaprosessi perustuu tieteelliseen tietoon.

5. Suunnittelutieteellinen tutkimus vaatii kurinalaista ja systemaattista toimintatapaa. Systemaattisuudella tarkoitetaan sitä, että tutkimusote ja -menetelmä valitaan huolellisesti ja niihin perehdytään sopivalla laajuudella. Konstruktiosta tulee laatia vaatimusmäärittely ja konstruktion testaamisesta saatuja tuloksia tulee verrata vaatimusmäärittelyyn. Suunnittelutyön ohessa tulee perehtyä täsmällisesti olemassa olevaan tietopääomaan ja lopuksi kuvata suunnittelutyön tuomaa lisäarvoa suhteessa olemassa olevaan tietopääomaan. (Hevner ym. 2004, 87–88.)

   Tutkimusta tehdessä tutustuttiin laajasti OSINT-tiedustelua koskevaan tieteelliseen teoriaan, vaatimusmäärittelyn teoriaan sekä prosessien suunnitteluun liittyvään teoriaan.

6. Suunnittelutiede on luonnostaan iteratiivista. Parhaan tai optimaalisimman konstruktion tuottaminen ja testaus on usein työlästä. Pohjimmiltaan suunnittelu on erilaisten ratkaisujen ideointia ja testausta parhaimman ja tehokkaimman lopputuloksen saavuttamiseksi. Huolellisesti tehdyssä suunnittelutyössä perehdytään jo olemassa oleviin ratkaisuihin. Olemassa olevia ratkaisuja hyödynnetään ja sovelletaan uudessa ympäristössä tai olosuhteissa. (Hevner ym. 2004, 88.)

   Tutkimuksella tuotettu toimintaprosessi tuotettiin käyttämällä tieteellisesti validia tietoa ja siihen sovellettiin jo olemassa olevaa ratkaisua tiedusteluprosessin osalta.

7. Tieteelliseen tekemiseen liittyvissä töissä työn julkisuus ja tulosten julkaiseminen ovat keskeisiä asioita. Tulokset tulisi julkaista siten, että tulokset ovat luettavissa ja ymmärrettävissä teknologiaorientoituneen yleisön ja päätöksentekijöiden joukossa. Teknologiaorientoitunut yleisö tarvitsee riittävästi yksityiskohtia konstruktiosta, jotta he voivat hyötyä sen tarjoamista eduista ja tiedoista. Päätöksentekijät tarvitsevat yksityiskohtaista, mutta ei niin teknistä tietoa konstruktiosta, jotta he voivat määritellä sen arvon organisaatiolleen. (Hevner ym. 2004, 90.)

   Tutkimuksen tulokset esitettiin kohdeorganisaation sisällä niille henkilöille, joille tutkimuksen tulos oli relevantti. Tutkimuksen tulokset esiteltiin myös kouluyhteisön sisällä.

5 Johtopäätökset ja pohdintaa

Tässä luvussa käyn läpi tutkimukseen liittyvät johtopäätökset ja pohdin tutkimuksen luotettavuutta.

Tämän opinnäytetyön tutkimuksen tavoitteena oli implementoida OSINT-tiedustelu osaksi kohdeorganisaation kyberturvallisuutta. Implementointi toteutettiin suunnittelemalla kohdeorganisaatiolle toimintaprosessi OSINT-tiedustelua varten, jolla organisaatio voi parantaa omaa kyberturvallisuutensa hallintaa.

Tutkimuksen tuloksena syntynyt toimintaprosessi testattiin ja testauksessa saadut tulokset vastasivat tiedustelulle ja testaukselle annettuja tavoitteita. Kohdeorganisaatio voi hyödyntää toimintaprosessia esimerkiksi uhkatiedusteluun. Näin ollen voidaan todeta, että tutkimuksen tuloksena syntynyt toimintaprosessi tuotti kohdeorganisaatiolle lisäarvoa ja tutkimuksen tavoite onnistuttiin saavuttamaan.

Opinnäytetyössä käytettiin tutkimusmetodina suunnittelutiedettä. Toimintaprosessin suunnittelu nojasi vahvasti suunnittelutieteen seitsemään periaatteeseen ja tutkimus täytti periaatteissa luetellut asiat. Kohdeorganisaatiolle luotiin toimintaprosessi OSINT-tiedustelua varten, jolla ratkaistiin organisaation ongelma, joka liittyi tiedustelun heikkoon hyödyntämiseen ja prosesseihin. Nämä asiat täyttivät periaatteiden kohdat yksi ja kaksi. Kolmannen periaatteen täytti toimintaprosessin huolellinen testaaminen. Neljäs periaate täyttyi sillä, että kohdeorganisaatiolle luotiin räätälöity prosessi, joka vastaa organisaation tarpeeseen ja prosessi on suunniteltu nojaten tieteelliseen tietoon. Tutkimusta tehdessä tutustuttiin laajasti OSINT-tiedustelun, prosessien ja vaatimusmäärittelyn teoriaan, joka täytti periaatteiden kohdan viisi. Periaatteiden kohdan kuusi täytti se, että tutkimuksella tuotettu toimintaprosessi tuotettiin käyttämällä tieteellisesti validia tietoa ja siihen sovellettiin jo olemassa olevaa ratkaisua tie-

dusteluprosessin osalta. Periaatteiden seitsemännen eli viimeisen kohdan täytti se, että tutkimuksen tulokset esiteltiin kouluyhteisön sisällä sekä kohdeorganisaatiossa relevanteille henkilöille.

Opinnäytetyössä tutustuttiin laajasti OSINT-tiedustelun teoriaan. Teoriapohjana käytettiin laajasti eri lähteitä, tieteellisiä julkaisuja ja kirjallisuutta. Lähdemateriaalit sisälsivät paljon toistoa samoista asioista ja tulkinnallisesti tätä voidaan pitää mittarina tutkimuksen luotettavuudesta, koska lähteet olivat johdonmukaisia eivätkä ne olleet ristiriidassa keskenään. Tutkimuksen luotettavuutta voidaan tarkastella myös suunnittelutieteellisen tutkimuksen seitsemän periaatteen täyttymisellä, jolloin suunnittelutieteellinen tutkimus on onnistunut. Tässä työssä suunnittelutieteen periaatteet pystyttiin täyttämään ja tutkimus nojasi vahvasti suunnittelutieteen seitsemään periaatteeseen. Tutkimuksen validius todettiin sillä, että tutkimuksen alussa määriteltyyn tutkimuskysymykseen pystyttiin vastaamaan.

6 Jatkotutkimus

Tutkimusta tehdessäni ja lähdemateriaaleihin tutustuessani törmäsin useasti siihen, että muuttuvan kybermaailman haasteista ja kyberrikollisuuden lisääntymisestä ollaan huolissaan maailmanlaajuisesti. World Economic Forumin Risk Reportin (World Economic Forum 2023, 11) mukaan kahden ja kymmenen vuoden aikavälillä tapahtuvan laajamittaisen kyberrikollisuuden ja kybermaailmaan liittyvän epävarmuuden riskit ovat suuret. Esimerkiksi vuosien 2022–2023 yhdeksi suurimmista riskeistä on nostettu kyberhyökkäykset kriittistä infrastruktuuria kohtaan (World Economic Forum 2023, 14). Kun riskit ovat suuret, lisää se myös erityistä tarvetta uhkien tarkasteluun useasta näkökulmasta.

Jatkotutkimuksena olisi mielenkiintoista tutkia miten eri finanssialan toimijat hyödyntävät OSINT-tiedustelua ja sen prosessia uhkatilannekuvan ylläpitämiseksi, kohdennetun uhkatiedon hankintaan ja miten hyökkäysvektorien alkupäätä voisi mitigoida OSINT-tiedustelulla. Tutkimuksessa voisi erityisesti painottaa tiedustelua pimeässä verkossa, eli mitä tietoa finanssialan toimijoista löytyy pimeästä verkosta ja miten näitä tietoja voidaan käyttää kohdistetusti verkkorikollisuuden mahdollistamiseksi finanssialan toimijoita kohtaan. Tätä voisi tarkastella esimerkiksi Lockeed Martinin suunnitteleman Cyber Kill Chainin kautta. Cyber Kill Chain-viitekehys on osa Intelligence Driven Defense mallia, jolla tunnistetaan ja estetään rikollista kybertoimintaa. (Lockheed Martin 2023.)

Toinen jatkotutkimuskohde voisi olla tekoälyn tuomat haasteet ja mahdollisuudet OSINT-tiedustelussa. Mitä hyötyjä tekoäly tarjoaa OSINT-tiedusteluun ja mitä haasteita voidaan kohdata tekoälyjen kehittyessä?

Lähteet

Sähköiset

Akhgar, B. & Bayerl, P. 2015. Surveillance and Falsification Implications for Open Source Intelligence Investigations. Communications of the ACM, Volume 58, Issue 8, 62. Viitattu 4.4.2023. https://dl-acm-org.nelli.laurea.fi/doi/10.1145/2699410

Azzopardi, L., Glisson, W., Maxwell, D., & McKeown, S. 2014. Investigating people: a qualitative analysis of the search behaviours of open-source intelligence analysts. IIiX '14: Proceedings of the 5th Information Interaction in Context Symposium, 175-176. Viitattu 4.4.2023. https://dl-acm-org.nelli.laurea.fi/doi/10.1145/2637002.2637023

BreachLock 2023. What is Open-source Intelligence, and how is it used? Viitattu 26.3.2023. https://www.breachlock.com/resources/blog/what-is-open-source-intelligence-and-how-is-it-used/

Breeden II, J., Fruhlinger, J. & Sharma, A. 2021. 15 top open-source intelligence tools. Viitattu 26.3.2023. https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html

Brown, C. 2023. How to Conduct an Ethical OSINT Investigation. Viitattu 26.3.2023. https://blackdotsolutions.com/blog/ethics-in-data-collection/

Colquhoun, C. 2016. A Brief History of Open Source Intelligence. Viitattu 4.4.2023. https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/

Conger, S. & Vessey, I. 1994. Requirements specification: learning object, process, and data methodologies. Communications of the ACM, Volume 37, Issue 5, 102. Viitattu 19.4.2023. https://dl-acm-org.nelli.laurea.fi/doi/10.1145/175290.175305

Crowdstrike 2022. Open Source Intelligence (OSINT). Viitattu 27.2.2023. https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/

Finanssiala Ry 2023. Varo, varmista, varoita-kampanja: Digihuijausten määrä kasvoi selvästi vuoden 2022 jälkipuoliskolla. https://www.finanssiala.fi/uutiset/varo-varmista-varoita-kampanja-digihuijausten-maara-kasvoi-selvasti-vuoden-2022-jalkipuoliskolla/

Flashpoint 2022. What Is Open Source Intelligence: The Importance of OSINT in Your Organization's Threat Landscape. Viitattu 27.2.2023. https://flashpoint.io/blog/what-is-osint-open-source-intelligence/

Fleischmann, A., Oppl, S., Schmidt, W. Stary, C. 2020. Contextual Process Digitalization, 1-2. Viitattu 18.4.2023. E-kirja. Springer Nature.

Gatlin, J., Yampolskiy, M. & Yung, M. 2021. Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad. AMSec '21: Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security, 4. Viitattu 26.4.2023. https://dl.acm.org/doi/abs/10.1145/3462223.3485618

Hassan, N. & Hijazi, R. 2018. Open Source Intelligence Methods and Tools – A Practical Guide to Online Intelligence, 5-101. Viitattu 7.4.2023. E-kirja. Apress L. P.

Hevner, A. 2007. A Three Cycle View of Design Science Research. Scandinavian Journal of Information Systems 19, 88-91. Viitattu 17.4.2023. https://www.researchgate.net/publication/254804390_A_Three_Cycle_View_of_Design_Science_Research

Hevner, A., March, S., Park, J., & Ram, S. 2004. Design Science in Information Systems Research. MIS Quarterly Vol. 28 No. 1, 80–90. Viitattu 16.4.2023. https://www.researchgate.net/publication/201168946_Design_Science_in_Information_Systems_Research

Hunt, T. 2023. Who, what and why. The background on the who, the what and the why of Have I Been Pwned. Viitattu 26.3.2023. https://haveibeenpwned.com/About

Hwang, Y-W. 2022. Current Status and Security Trend of OSINT. Viitattu 26.3.2023. https://www.hindawi.com/journals/wcmc/2022/1290129/#copyright

IFF Lab 2023. The Layers of the Web – Surface Web, Deep Web and Dark Web. Viitattu 26.3.2023. https://ifflab.org/the-layers-of-the-web-surface-web-deep-web-and-dark-web/

Imperva 2022. Open-Source Intelligence (OSINT). Viitattu 27.2.2023. https://www.imperva.com/learn/application-security/open-source-intelligence-osint/

Jokinen, T. 2021. Konstruktiivinen tapaustutkimus ja suunnittelutiede – kaksi insinööritieteisiin soveltuvaa tutkimusotetta. Viitattu 16.4.2023. https://blogi.oamk.fi/2021/02/19/konstruktiivinen-tapaustutkimus-ja-suunnittelutiede-kaksi-insinooritieteisiin-soveltuvaa-tutkimusotetta/

Kadar, T. 2023. Top 10 OSINT (Open Source Intelligence) Software Tools 2023. Viitattu 26.3.2023. https://seon.io/resources/comparisons/osint-software-tools/

Lockheed Martin 2023. Putting Intelligence to Work. Viitattu 21.4.2023. https://www.lockheedmartin.com/en-us/capabilities/cyber/intelligence-driven-defense.html

Martins, C. & Medeiros, I. 2022. Generating Quality Threat Intelligence Leveraging OSINT and a Cyber Threat Unified Taxonomy. ACM Transactions on Privacy and Security, Volume 25, Issue 3, Article 19, 2-5. https://dl-acm-org.nelli.laurea.fi/doi/10.1145/3530977

Maltego 2021. Useful Google Dorks for Open Source Intelligence Investigations. Viitattu 4.4.2023. https://www.maltego.com/blog/using-google-dorks-to-support-your-open-source-intelligence-investigations/

Oikarinen, A. 2020. Open-Source Intelligence – It's Incredible what you can find from public sources. Viitattu 26.3.2023. https://www.nixu.com/blog/open-source-intelligence-its-incredible-what-you-can-find-public-sources

Ould, M. 2005. Business Process Management – A Rigorous Approach, 3-6, 32, 271. Viitattu 19.4.2023. E-kirja. British Informatics Society Limited 2005.

Rouse, M. 2020. Google. Viitattu 26.3.2023. https://www.techopedia.com/definition/5359/google

Sayegh, E. 2022. Cybersecurity Megatrends: Signal, Noise, And Existential Threats. Viitattu 27.2.2023. https://www.forbes.com/sites/emilsayegh/2022/07/21/cybersecurity-megatrends-signal-noise-and-existential-threats/?sh=43d344494a1d

Snyk 2023. Threat Intelligence Lifecycle - Phases & Best Practices Explained. Viitattu 19.4.2023. https://snyk.io/learn/threat-intelligence/threat-intelligence-lifecycle/

World Economic Forum 2023. Global Risks Report 2023 18th Edition, 11-14. Viitattu 21.4.2023. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Zola, A. 2023. Google Maps. Viitattu 26.3.2023. https://www.techtarget.com/whatis/definition/Google-Maps

Kuviot

Taulukot