Timo Broström

UHKATIETOJEN MAHDOLLISUUDET KORKEAKOULUJEN TIETOTURVASSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Broström, Timo
Uhkatietojen mahdollisuudet korkeakoulujen tietoturvassa
Jyväskylä: Jyväskylän yliopisto, 2023, 49 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Hämäläinen, Timo

Alati muuttuvassa kyberuhkien ympäristössä ennalta varautuminen erilaisiin kyberhyökkäyksiin on yhä tärkeämpää. Jotta hyökkäyksiin voitaisiin ennalta varautua, tarvitaan tietoa. Uhkatieto ja sen jakaminen sidosryhmien kesken voi olla osa ratkaisua ennalta varautumisessa. Kun sidosryhmän jäsenet saavat ajoissa tiedon käynnistymässä olevasta kyberhyökkäyksestä, he voivat ottaa tarvittavat varautumiskeinot käyttöön jo ennen hyökkäyksen alkua. Tämä pro gradu -tutkielma tarkasteli uhkatietojen mahdollisuuksia korkeakoulujen tietoturvan kehittämisessä. Uhkatietojen jakamiseen käytettiin MISP-alustaa, joka on avoimen lähdekoodin sovellus uhkatietojen keräämiseen ja jakamiseen. Tutkielman tutkimusmenetelmiksi valittiin kirjallisuuskatsaus sekä konstruktiivinen tutkimusmenetelmä, joka etsii ratkaisua reaalimaailman ongelmiin. Tutkielman lähteiksi valittiin luotettavia, relevantteja, hyvän tason lähteitä. Lopputuloksena havaittiin, että MISP on varteenotettava työkalu uhkatietojen jakamisessa. Integraatioiden muodostaminen toisiin järjestelmiin, tapahtumien jakaminen toisen organisaation kanssa ja uhkatietojen organisointi oli parhaimmillaan yksinkertaista ja suoraviivaista. Toisaalta havaittiin, että MISP on lopulta vain työkalu, varasto, johon uhkatietoa viedään, eikä se yksin ole vastaus tehokkaaseen tietojen jakamiseen ja hyödyntämiseen, vaan lisäksi tarvitaan selkeitä prosesseja, sääntöjä ja standardeja, selkeää lainsäädäntöä sekä motivoituneita ihmisiä työskentelemään uhkatiedon keräämisen, käsittelemisen ja jalostamisen parissa. Lisäksi MISP:n ylläpitäminen ja ongelmien selvittely olivat pahimmillaan reilusti aikaa vieviä prosesseja. MISP-alustassa on potentiaalia, mutta se tarvitsee käyttäjiä, jotka ymmärtävät sen toimintaa ja jotka ovat sitoutuneet yhteisiin pelisääntöihin uhkatietojen jakamisessa.

Asiasanat: Uhkatieto, MISP, uhkatunniste

ABSTRACT

Broström, Timo
Potential of threat intelligence in information security of universities
Jyväskylä: University of Jyväskylä, 2023, 49 pp.
Cyber Security, Master's Thesis
Supervisor(s): Hämäläinen, Timo

In the ever-changing environment of cyber threats, it is increasingly important to be prepared in advance for various cyber-attacks. In order to prepare for attacks in advance, information is needed. Threat intel and its sharing among stakeholders can be part of the solution in preparing for the cyber threats in advance. When the stakeholders receive timely information about a cyber-attack that is about to start, they can take the necessary precautions before the attack begins. This master's thesis examined the possibilities of threat information in the development of information security in higher education institutions. The MISP platform was used to share threat information, which is an open-source application for collecting and sharing threat intel. The research methods chosen for the dissertation were a literature review and a constructive research method that seeks solutions to real-world problems. Reliable, relevant, high-quality sources were chosen as sources for the thesis. As a result, it was found that MISP is a viable tool for sharing threat information. Creating integrations with other systems, sharing events with another organization, and organizing threat information was simple and straightforward at best. On the other hand, it was found that in the end MISP is only a tool, a storage, to which threat information is saved, and it alone is not the answer to efficient threat intel sharing and utilization, but it also requires clear processes, rules and standards, clear legislation, and motivated people to collect, handle, and process the threat information. In addition, maintaining MISP and solving errors were quite time-consuming processes at worst. The MISP platform has potential, but it needs users who understand how it works and who are committed to follow agreed rules in sharing threat information.

Keywords: threat intel, MISP, indicators of compromise (IoC)

KUVIOT

KUVIO 1 Uhkatietoneliö 12
KUVIO 2 Tunnisteet 16
KUVIO 3 Galaksit 17
KUVIO 4 Tapahtuman attribuutit 18
KUVIO 5 Uusi jakoryhmä 20
KUVIO 6 Konstruktiivinen tutkimusote 24
KUVIO 7 Attribuuttien korrelaatio 27
KUVIO 8 Lokienhallintapalvelun MISP-paneelin alapaneeli 28
KUVIO 9 Sentinelin uhkatietotaulukko 29
KUVIO 10 Lisätietopaneeli 30
KUVIO 11 MISP tapahtuman luominen ServiceNow-palvelussa 31
KUVIO 12 Yhden MISP tapahtuman uhkatunnistetietoja Splunkissa 32
KUVIO 13 Yhteyden testaaminen 34
KUVIO 14 Puuttuvat tunnisteet 35
KUVIO 15 Työnvirtaus 35
KUVIO 16 Muutosehdotus 36
KUVIO 17 Muutosehdotus tapahtumassa 37
KUVIO 18 Havainto 37
KUVIO 19 Korkeakoulujen MISP-järjestelyn ehdotus 38

TAULUKOT

TAULUKKO 1 Konstruktiivisen tutkimuksen vaiheet 23

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT JA TAULUKOT

1 JOHDANTO 6

2 UHKATIETO JA SEN MAHDOLLISUUDET SEKÄ HAASTEET 8
2.1 Uhkatietojen kategoriat 11
2.2 Uhkatiedon elinkaari 12
2.3 Uhkatietojen jakamisen hyödyt sekä esteet 13

3 UHKATIETOJEN JAKOALUSTA MISP 15

4 TUTKIMUSMENETELMÄ 22
4.1 Kirjallisuuskatsaus 22
4.2 Konstruktiivinen tutkimusmenetelmä 23

5 UHKATIEDON JA MISP:N KÄYTTÖ YKSITTÄISESSÄ KORKEAKOULUSSA 26

6 UHKATIEDON JA MISP:N KÄYTTÖ KORKEAKOULUJEN VÄLILLÄ SUOMESSA 34

7 ANALYYSI JA JOHTOPÄÄTÖKSET 40

8 YHTEENVETO 43

LÄHTEET 45

1 JOHDANTO

Kyberrikollisuuden kasvu uhkaa organisaatioiden tietoturvallisuutta, ja käynnissä onkin jatkuva kamppailu erilaisten kyberhyökkäyksien estämiseksi ja oman kyberpuolustuksen parantamiseksi. Kyberrikollisuus on Thomasin ja Loaderin (2000, s. 3) määritelmän mukaan ”tietokonevälitteistä toimintaa, joka on joko laitonta tai mitä jotkut osapuolet voivat pitää laittomana ja joita voidaan toteuttaa maailmanlaajuisten sähköisten verkkojen kautta.”

Yksi keino tehokkaampaan kyberpuolustukseen voisi olla uhkatieto. Uhkatiedon avulla organisaatiot voivat kehittää kyberpuolustustaan paremmaksi. Uhkatiedolla tarkoitetaan lyhyesti kaikkea sitä informaatiota, jota organisaatiot voivat käyttää hyväkseen ymmärtääkseen uhkia, jotka ovat joko joskus uhanneet heitä, tai uhkaavat heitä nyt tai tulevaisuudessa. Uhkatieto on organisoitua ja analysoitua tietoa potentiaalisista tai nykyisistä uhkista, jotka voivat vaarantaa organisaation turvallisuuden. (Cobb, 2021.)

Huolimatta uhkatietopalvelualustojen olemassaolosta sekä kyberturvallisuuden parhaiden käytäntöjen ohjeista, kirjallisuudessa esiintyy todella vähän tutkimustietoa siitä, kuinka organisaatiot voisivat käyttää ja integroida uhkatietoa, tai miten uhkatietojen käyttö toteutuisi käytännössä (Kotsias, Ahmad & Scheepers, 2022).

Tämän tutkimuksen tavoite on selvittää, miten uhkatietojen jakoalusta MISP:iä voitaisiin käyttää hyväksi yksittäisessä yliopistossa sekä korkeakoulujen kesken Suomessa.

Tutkimuskysymykset ovat seuraavat:

- Miten yksittäisessä yliopistossa voitaisiin käyttää hyväksi MISP-alustaa?
- Miten Suomen korkeakoulut voisivat käyttää hyväksi MISP-alustaa uhkatietojen jakamiseen?

Tutkielma on toteutettu kirjallisuuskatsauksena sekä käyttämällä toisena tutkimusmenetelmänä konstruktiivista tutkimusotetta, joka on innovatiivisia konstruktioita tuottava metodologia, jolla pyritään ratkaisemaan reaalimaailman ongelmia ja tällä tavoin tuottamaan kontribuutioita sille tieteenalalle, jossa sitä sovelletaan (Lukka, 2001).

Lähdekirjallisuus koostuu tieteellisistä artikkeleista, kirjoista, sekä kokoelmateoksista. Lisäksi lähteinä käytetään asiaankuuluvia blogeja ja uutisia, sekä MISP:n dokumentaatiota. Lähdekirjallisuus koottiin Google Scholar-, IEEE Xplore-, Scinapse- ja JYKDOK-hakukoneista. Lisäksi Internetistä haettiin uutisia ja blogeja tarpeen mukaan. Hakusanoina olivat ”MISP”, ”cyber threat intelligence”, ”threat intelligence”, ”threat intelligence sharing” ja vastaavat sekä näiden yhdistelmät. Lähdekirjallisuutta haettiin enimmäkseen vain englannin kielellä, sillä suomenkielisiä, hyvän tason lähteitä on vielä vähän. Tavoitteeksi lähteiden valinnalle otetaan se, että ne ovat saaneet vähintään tason 1 Julkaisufoorumilla, ja jotta ne olisivat suhteellisen tuoreita lähteitä. Lisäksi lähteiden arvioinnissa otettiin huomioon lähteiden kirjoittajien tunnettuus ja arvostettuus, lähteen uskottavuus ja kustantajan arvovalta.

Tutkielman tavoitteena on selvittää, miten uhkatietoa voitaisiin hyödyntää yliopistoissa ja niiden kesken käyttämällä uhkatietojen jakamiseen tarkoitettua alustaa, MISP:ä.

Tutkielma jakaantuu kahdeksaan eri lukuun: johdantoon, kuuteen sisältölukuun sekä yhteenvetoon. Ensimmäisessä sisältöluvussa lukija tutustutetaan uhkatietoon, sen piirteisiin ja käyttöön. Toisessa sisältöluvussa käydään yleisesti läpi uhkatietojen jakoalusta MISP:n toimintaa. Sen jälkeen lukijalle avataan tutkielman tutkimusmenetelmää ja sen piirteitä. Neljännessä sisältöluvussa keskitytään uhkatietojen käyttöön yksittäisen yliopiston sisällä, ja viidennessä sisältöluvussa esitetään näiden uhkatietojen käyttöä ja jakamista Suomen korkeakoulujen kesken. Sen jälkeen tuloksia pohditaan ja analysoidaan kuudennessa sisältöluvussa, jonka jälkeen yhteenvetoluvussa kootaan tutkielman keskeiset havainnot yhteen.

2 UHKATIETO JA SEN MAHDOLLISUUDET SEKÄ HAASTEET

Tässä luvussa käydään läpi uhkatiedon määritelmä, sekä mistä se koostuu, mihin se jakautuu, miten uhkatieto elää ja miten sitä käytetään.

Kyberuhkatietojen jakaminen sidosryhmien välillä on luvattu olevan uusi keino tilannetietoisuuden nostamiseksi sidosryhmien kesken (Sigholm & Bang, 2013). Nykyisessä digitaalisessa maailmassa organisaatioiden on pystyttävä vastaamaan uhkiin ennaltaehkäisevästi eikä vain reagoimalla meneillään oleviin hyökkäyksiin (Wagner, Mahbub, Palomar & Abdallah, 2019).

Uuden tyyppiset uhat, joihin organisaatiot joutuvat varautumaan, ovat muun muassa APT-hyökkäykset (Ahmad, Webb, Desouza & Boorman, 2019; Johnson, 2015; Pahi & Skopik, 2017), monimuotoiset (engl. Polymorphic) haittaohjelmat (Christodorescu, Jha, Seshia, Song & Bryant, 2005; Johnson, 2015; Tounsi & Rais, 2018), nollapäivähaavoittuvuudet (Johnson, 2015) ja yhdistelmäuhkat (engl. Composite threat) (Tounsi & Rais, 2018), joita voidaan kutsua myös monivaiheisiksi hyökkäyksiksi (Navarro, Deruyver & Parrend, 2018).

Edellä mainittujen uhkien torjumiseen voidaan hyödyntää uhkatietoa. Uhkatiedot voivat koostua seuraavista asioista (Vázquez, Acosta, Spirito, Brown & Reid, 2012):

- Haavoittuvuustiedot, kuten tiedot palveluiden haavoittuvuusskannauksista ja laadusta
- Tiedot uhkatoimijoista, kuten nimet, kotimaa, hyökkäystyypit ja yleisimmät metodit ja taktiikat
- Esto- ja sallittujen listojen informaatio (IP-osoitteet)
- Sovellukset
- Laitteet
- Haittaohjelmat
- Turvallisuusohjaus
- Turvallisuusasetukset
- Turvallisen koodauksen käytännöt
- Protokollien määrittely

Uhkatietoja jaetaan manuaalisesti sekä automaattisesti. Tällä hetkellä kuitenkin laaja-alainen automaattinen tietojen jakaminen on heikkoa, eivätkä nykyiset uhkatietojen jakoalustat taivu erityisen hyvin automatisoituun tietojen jakamiseen (Dandurand & Serrano, 2013; Sauerwein, Sillaber, Mussmann & Breu 2017). Manuaalinen työ on puolestaan hidasta, ja analyytikot joutuvat käyttämään paljon aikaa datan prosessointiin sekä ongelmien arviointiin (Pawlinski ym., 2014), sekä ratkaisujen implementointiin ja tietojen jakamiseen (Wagner ym., 2019).

Manuaalinen tietojen jako koostuu Wagnerin ym. (2019) mukaan seuraavista keinoista:

- Sähköpostit
- Puhelut
- Datasyötteet
- Internet-portaalit (engl. Web portals)
- Jaetut tietokannat
- Palaverit

Uhkatietojen jaon automatisointi nopeuttaisi ja yksinkertaistaisi merkittävästi tiedon jakamista, dokumentaatiota ja analysointia (Kampanakis, 2014).

Uhkatietoja ei kuitenkaan jaeta erityisen innokkaasti, sillä se saatetaan kokea vaikeaksi organisaatioissa. Organisaatiot saattavat myös kokea, ettei heillä ole mitään jaettavaa muille (Chismon & Ruks, 2015). Lisäksi organisaatiot eivät välttämättä osaa arvioida, mitä heidän on sallittua jakaa (Shin & Lowry, 2020). Vaikka uhkatietoja jaettaisiinkin, niin niitä käytetään edelleen varsin harvoin hyödyksi (Oosthoek & Doerr, 2021).

Uhkatietojen jakamisella on omat hyötynsä ja haittansa. Hyötyjä ovat muun muassa duplikaatti-informaation väheneminen (Zibak & Simpson, 2019), tietomurtojen havaitseminen (Woods, Perl & Lindauer, 2015) ja tietomurtojen aiheuttamien vahinkojen vähentäminen (Woods, Perl & Lindauer, 2015). Uhkatietojen hyödyntämisen avulla kyberhyökkäys voidaan estää jo ennen sen tapahtumista (Feledi, Fenz & Lechner, 2013), ja näin varmistetaan palveluiden häiriötön toiminta sekä jatkuvuus (Wagner ym., 2019). Muita hyötyjä ovat muun muassa jaettu tilannetietoisuuden nosto, jolloin pelkästään yhden organisaation jakama uhkatieto voi parantaa koko yhteisön kyberpuolustusta (Johnson, Badger, Waltermire, Snyder & Skorupka, 2016).

Haittoina nähdään puolestaan se, että jos organisaation jakamat omat uhkatiedot vuotavat kyberrikollisille, kyberrikolliset voivat käyttää näitä tietoja hyväkseen ja kokeilla hyökätä organisaatiota vastaan ennen kuin organisaatio kerkeää korjata mahdolliset haavoittuvuudet (Al-Ibrahim, Mohaisen, Kamhoua, Kwiat & Njilla, 2017; Mohaisen, Al-Ibrahim, Kamhoua, Kwiat & Njilla, 2017). Toisaalta näitä riskejä voidaan lieventää arvioimalla jaettavan tiedon sensitiivisyyttä ja vaikutusta. Tähän on erilaisia malleja, kuten esimerkiksi Kokkosen, Hautamäen, Siltasen ja Hämäläisen (2016) esittelemä malli, joka estää tietojen jaon sidosryhmien kesken, jos riski kasvaa liian suureksi.

Uhkatiedot voivat sisältää myös henkilötietoja, mikä asettaa laillisia rajoitteita uhkatietojen jakamiseen. Euroopan Unionin yleinen tietosuoja-asetus

(GDPR) voi vaikuttaa siihen, mitä tietoja ja milloin on laillista jakaa tiettyjä uhkatietoja. (Albakri, Boiten & Lemos, 2019.) Tietojen jakamisen lailliset rajoitteet saattavatkin pelästyttää, eikä tietoja jaeta lakiin liittyvien seurausten pelossa.

Eräs mahdollinen keino pienentää sensitiivisen tiedon jaon riskiä tahattomasti on käyttää jakamisen yhteydessä tunnisteita, jotka määrittelevät datan sensitiivisyyttä (Albakri, Boiten & Lemos, 2019). Yleisesti käytetty tunniste on muun muassa liikennevaloprotokolla (engl. Traffic Light Protocol, TLP), joka jakautuu neljään rajoitusluokkaan (First, 2022; Traficom, 2022). Rajoitusluokat ovat tiukimmasta alkaen: TLP:RED, TLP:AMBER, TLP:GREEN ja TLP:CLEAR (First, 2022). Kun uhkatiedot on selkeästi merkitty näillä rajoitusluokilla, se voi helpottaa tietojen jakamista muille, kun jaettavista tiedoista poistetaan sensitiiviset tiedot, joita ei ole tarkoitus jakaa ulkopuolisille.

Yksi uhkatietojen jakamisen päämääristä on varoittaa organisaatioita haavoittuvuuksista ja uhkista. Jakamisen kanssa on kuitenkin oltava tarkkana, ettei julkiseen tietoon päädy vahingossa tietoja sellaisista haavoittuvuuksista, joita ei voi vielä paikata, sillä se jättäisi organisaatiot alttiiksi kyberhyökkäyksille, jotka käyttäisivät hyväkseen löytynyttä haavoittuvuutta. (Skopik, Settanni & Fiedler, 2016.)

Muita ongelmia uhkatietojen jakamisessa on muun muassa luottamuksen puute organisaatioiden kesken sekä puutteet uhkatiedon luotettavuudessa ja tarkkuudessa (Riesco, Larriva-Novo & Villagrá, 2020). Uhkatunnisteet, joista tekninen uhkatieto yleensä koostuu, eivät ole valmista prosessoitua uhkatietoa, eikä näitä pitäisi käyttää suoraan uhkatietona (Oosthoek & Doerr, 2021). Lisäksi uhkatunnisteet voivat olla vääriä positiivisia, esimerkiksi jos aikaisemmin haitallinen IP-osoite onkin siirtynyt normaaliin käyttöön (Iklody, Wagener, Dulaunoy, Mokaddem & Wagner, 2018; Mokaddem, Wagener, Dulaunoy & Iklody, 2019; Oosthoek & Doerr, 2021).

Uhkatietojen on oltava luotettavia ja laadukkaita, jotta niitä voitaisiin käyttää tehokkaasti organisaatioissa. Kotsias, Ahmad ja Scheepers (2022) määrittelivätkin yhdeksän eri kriteeriä, joilla uhkatiedon laatua voidaan arvioida:

1. Virheettömyys
2. Olennaisuus
3. Valmis kokonaisuus eli tiedoissa ei voi olla puutteita
4. Täsmällisyys
5. Oikea-aikaisuus
6. Käyttökelpoisuus
7. Luotettavuus
8. Ennustettavuus
9. Räätälöinti eli tyydyttää tiedon pohjalta päättävien henkilöiden tarpeet

2.1 Uhkatietojen kategoriat

Tieteellisissä artikkeleissa uhkatiedot harvemmin jaetaan osa-alueisiin, vaan niitä käsitellään yleensä yhtenä nippuna. Organisaatiot ja instituutiot yleensä kuitenkin jakavat uhkatiedot neljään eri osaan seuraavasti (Chismon & Ruks, 2015):

- Taktinen,
- Strateginen,
- Tekninen ja
- Operatiivinen uhkatieto

Taktinen uhkatieto koostuu hyökkääjien yksityiskohtaisista ominaisuuksista sekä erilaisista uhkatunnisteista, kuten esimerkiksi haittaohjelmatunnisteista (Gschwandtner, Demetz, Gander & Maier, 2018; Shackleford, 2015).

Strateginen uhkatieto on korkeamman tason uhkatietoa, esimerkiksi tietoa, joka on saatu analysoimalla taktista tai teknistä uhkatietoa (Dog, 2016). Tiedot voivat sisältää esimerkiksi mahdollisia hyökkäyskohteita sekä riskejä, joita organisaatiolla on (Gschwandtner ym., 2018).

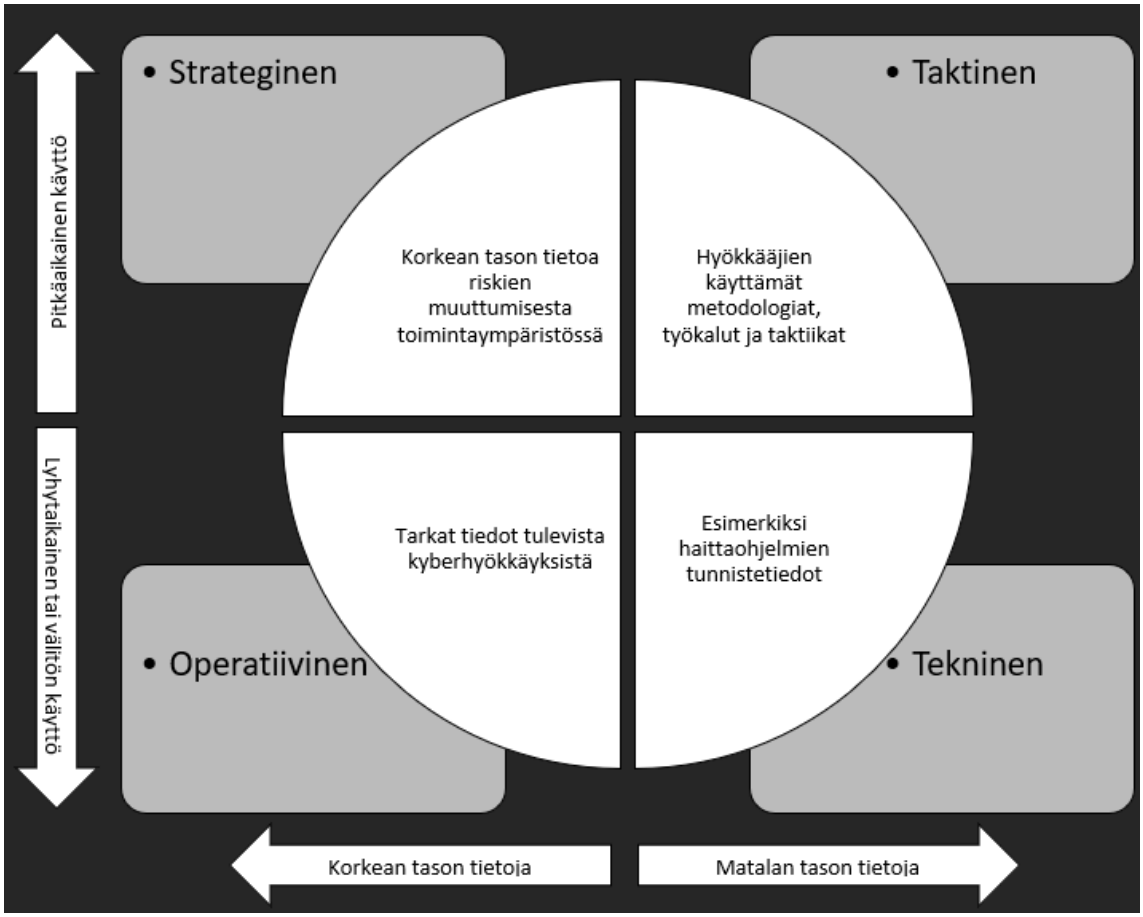
Tekninen uhkatieto on informaatiota tai pikemminkin dataa, jota yleensä käsitellään teknisestä näkökulmasta, esimerkiksi uhkatietojen jakoalustalla (Chismon & Ruks, 2015). Tekninen uhkatieto koostuu yleensä uhkatunnisteista (engl. Indicators of Compromise, IoC), ja näitä tunnisteita ovat esimerkiksi IP-osoitteet, verkkotunnukset ja tiedostojen tiivisteet (Oosthoek & Doerr, 2021; Tounsi & Rais, 2018). Muita yleisiä uhkatunnisteita ovat Tounsin ja Raisin (2018) mukaan muun muassa:

- Haittaohjelmien nimet
- Rekisteriavaimet
- Sähköpostiosoitteet
- Liitteet ja linkit
- IP-osoitteiden lähde- ja kohdeosoitteet

Tekninen uhkatieto voidaan myös liittää taktiseen uhkatietoon (Gschwandtner ym., 2018).

Operatiivinen uhkatieto on puolestaan tietoa, joka auttaa suojattavan tietojärjestelmän turvaamisessa. Operatiivista uhkatietoa voidaan käyttää esimerkiksi jonkin tietyn kyberhyökkäyksen torjuntaan. (Tao ym., 2017.) Lisäksi operatiivista uhkatietoa käyttämällä voidaan muodostaa potentiaalinen kyberhyökkäysmalli ja arvioida kyseisen hyökkäyksen vahinkoja, jos sellainen toteutuisi (Gschwandtner ym., 2018).

Alla oleva kuvio havainnollistaa uhkatietoneliötä. Kuvio on suomennettu Chismonin ja Ruksin (2015) raportista:



KUVIO 1 Uhkatietoneliö

2.2 Uhkatiedon elinkaari

Uhkatiedon elinkaari koostuu yleensä viidestä osasta (Doerr, 2018):

- Suunnittelu ja ohjaus
- Tiedon kerääminen
- Tiedon prosessointi ja hyödyntäminen
- Tiedon analysointi ja valmistelu
- Tiedon levitys ja integraatio

Uhkatiedon elinkaarta voi pilkkoa pienempiinkin osiin, esimerkiksi kahdeksaan eri osaan (Yeboah-Ofori, Islam, & Yeboah-Boateng, 2019), mutta sisällöllisesti viisiportaisella tai kahdeksanportaisella elinkaarella ei ole juurikaan eroa. Ainoana lisänä voidaan pitää tiedon arviointia ja kertausta, joka on tiedon elinkaaren viimeinen osa Yeboah-Oforin, Islamin ja Yeboah-Boatengin (2019) esittämässä mallissa. Lisäksi palaute on mainittu yhtenä mahdollisena

uhkatiedon elinkaaren viimeisenä vaiheena (Cascavilla, Tamburri & Van Den Heuvel, 2021).

Elinkaaren ensimmäisessä osassa tunnistetaan puutteelliset tiedot sekä priorisoidaan tiedon keräämistä (Doerr, 2018). Tässä vaiheessa organisaatio voi esimerkiksi asettaa saavutettavat tavoitteet uhkatiedon hyödyntämiselle, pohtia toimenpiteitä, sekä tunnistaa suojattavat tiedot ja sijoittaa ne arvokkuutensa mukaan järjestykseen (Cascavilla, Tamburri & Van Den Heuvel, 2021).

Elinkaaren toisessa osassa päätetään mistä lähteistä tietoa kerätään ja miten, sekä haetaan kerättävä data (Doerr, 2018). Uhkatietoa voidaan hakea esimerkiksi julkisista tietokannoista tai niitä voidaan jakaa organisaatioiden kesken (Brown, Gommers & Serrano, 2015). Uhkatietoa voidaan hakea myös uutisista, blogeista, Internetin foorumeilta ja jopa pimeästä verkosta (Cascavilla, Tamburri & Van Den Heuvel, 2021).

Kolmannessa vaiheessa tietoa prosessoidaan ja hyödynnetään (Doerr, 2018). Kun tieto on haettu, se on yleensä isona massana, ja tiedot voivat olla eri muodoissa tallennettuina. Tämä tietomassa pitää muotoilla selkeäksi, ja tästä massasta pitää erotella ja linkittää yhteen olennaiset tiedot, ja samalla duplikaattitiedot sekä väärät tiedot tulee poistaa aiheuttamasta hämmennystä (Brown, Gommers & Serrano, 2015; Cascavilla, Tamburri & Van Den Heuvel, 2021).

Neljäs vaihe koostuu tiedon analysoinnista, eli arvioidaan, soveltuuko se puutteellisen tiedon paikkaamiseen (Doerr, 2018). Tässä vaiheessa arvioidaan esimerkiksi tiedon luotettavuutta tai tiedon analysointiin käytettävää aikaa (Brown, Gommers & Serrano, 2015). Analysoinnin perusteella voidaan tehdä päätöksiä esimerkiksi potentiaalisen uhan lisätutkinnasta, ryhtyä ennakoiviin toimenpiteisiin mahdollisen hyökkäyksen pysäyttämiseksi tai parantaa organisaation kyberturvallisuutta (Cascavilla, Tamburri & Van Den Heuvel, 2021).

Viimeinen vaihe on tiedon levitys ja integraatio, joka voi sisältää esimerkiksi tiedon jakamista asiakkaille tai muille organisaatioille (Doerr, 2018). Tässä vaiheessa valmiiksi jalostettua tietoa voidaan käyttää hyväksi esimerkiksi uhkatietoraporteissa ja työkalujen konfiguroinnissa (Cascavilla, Tamburri & Van Den Heuvel, 2021).

2.3 Uhkatietojen jakamisen hyödyt sekä esteet

Kuten jo aiemmin tämän luvun alussa on mainittu, uhkatietojen jakamisella on selkeitä hyötyjä. Näitä tietoja ei kuitenkaan päästä tehokkaasti hyödyntämään, jos tietojen omistajat suhtautuvat epäilevästi tai välinpitämättömästi tietojen jakamiseen.

Uhkatietojen jakamisen hyötyjä ovat muun muassa tilannetietoisuuden lisääntyminen, organisaatioiden verkostoitumisen lisääntyminen, kustannuksien vähentyminen, epätietoisuuden vähentyminen kyberturvallisuuteen liittyvissä investoinneissa, tietomurtojen havaitsemisen paraneminen sekä tietomurtojen haittojen väheneminen (Zibak & Simpson, 2019). Zibak ja Simpson (2019)

tunnistivat yhteensä 19 eri hyötyä uhkatietojen jakamisesta, joista mainitsin edellä olennaisimmat.

Selkeimpänä esteenä puolestaan voidaan nähdä metodiikan puute, eli uhkatietojen jakamiselle ei ole määritelty selkeitä metodeja, käytäntöjä, prosesseja tai sääntöjä. Uhkatieto tulee yleensä järjestelmiin ”raakana”, eli ihminen ei käy suodattamassa uhkatietoa käytännöllisempään muotoon. (Oosthoek & Doerr, 2021.)

Toinen yleinen este on uhkatietojen hyödyntämättä jättäminen. Vaikka organisaatio saisikin ulkoisista lähteistä uhkatietoa, se saattaa jättää ne huomioimatta eikä niitä lisätä omiin järjestelmiin. (Oosthoek & Doerr, 2021.)

Uhkatieto on yleensä myös itsessään huonolaatuista. Uhkatietoa ei voi hyödyntää yksinään, vaan sitä on yleensä verrattava esimerkiksi verkon lokitietoihin, jonka lisäksi uhkatieto voi sisältää vääriä positiivisia. (Oosthoek & Doerr, 2021.)

Uhkatietojen jakajat eivät myöskään yleensä ole tarpeeksi läpinäkyviä sen suhteen, mistä uhkatieto on kerätty. Uhkatiedon lähteeksi voi olla kirjattu ”honeypot” tai muu yksittäinen sana, mikä voi herättää epäilyksiä uhkatiedon laadusta. (Oosthoek & Doerr, 2021.)

Organisaatiot ovat myös haluttomia jakamaan sensitiivistä uhkatietoa esimerkiksi lainsäädäntöön ja yksityisyyteen liittyvien ongelmien takia (de Fuentes, González-Manzano, Tapiador & Peris-Lopez, 2017; Mermoud, Keupp, Huguenin, Palmié & Percia David, 2019; Murdoch & Leaver, 2015; Skopik, Settanni & Fiedler, 2016). Organisaatiot ovat myös yleensä haluttomia jakamaan uhkatietoa, koska heillä ei ole ohjeistusta siihen mitä tietoa se saavat jakaa ilman että he joutuisivat oikeudellisiin ongelmiin (Tounsi & Rais, 2018).

Edellä on käyty läpi yleisimmät syyt mitkä estävät tietojen jakamista. Riesco, Larriva-Novo ja Villagrá (2020) tunnistivat yhteensä 21 eri haastetta tai estettä uhkatietojen jakamiselle.

3 UHKATIETOJEN JAKOALUSTA MISP

Tässä luvussa käydään läpi yleisellä tasolla MISP:n toimintaa ja tarkastellaan sen ominaisuuksia ja käyttöä.

MISP eli Malware Information Sharing Platform eli suomeksi haittaohjelmatietojen jakamisalusta on avoimeen lähdekoodiin perustuva sovellus, jota käytetään uhkatunnisteiden (engl. Indicators of Compromise, IoC) jakamiseen, tallentamiseen ja vertailuun (MISP, 2023).

Organisaatioille MISP on käytännössä säilö, mihin voi tallentaa ja mistä löytyy tiedot kaikista tunnetuista uhkista ja haavoittuvuuksista, joita organisaatio on kohdannut. MISP antaa näille tiedoille selkeän rakenteen, mikä helpottaa informaation etsimistä ja sen vertailua. MISP myös luokittelee samankaltaisen informaation saman luokan alle, ja esimerkiksi tapahtumat, joissa on ollut mukana sama IP-osoite, linkittyvät keskenään (Cosive, 2022; MISP, 2023).

Koska tieto varastoidaan selkeässä muodossa, organisaatiot voivat jakaa tätä tietoa keskenään helposti toistensa kesken (Cosive, 2022; MISP, 2023). MISP:n tarkoituksena on siis helpottaa uhkatietojen ylikuormaa tarjoamalla analyytikoille selkeän ja helpon tavan kerätä, etsiä, analysoida, jakaa ja käyttää tätä tietoa (Cosive, 2022; MISP, 2023).

MISP:n pääasialliset käyttötavat jakautuvat kahteen eri osaan (Cosive, 2022; MISP, 2023):

1. Tiedon etsiminen ja jakaminen: MISP:n avulla voi jäsentää paremmin uhkatunnistetietoja. Voit esimerkiksi etsiä IP-osoitteen avulla tietoja, kuten onko kyseinen IP-osoite merkattu haitalliseksi esimerkiksi muissa organisaatioissa.
2. Automaattiset uhkatunnisteiden työnnöt palomuureihin, päätetoimijoihin (engl. Endpoint agents), ja tunkeilijan havainnointijärjestelmiin, mikä tarkoittaa vähemmän manuaalista työtä.

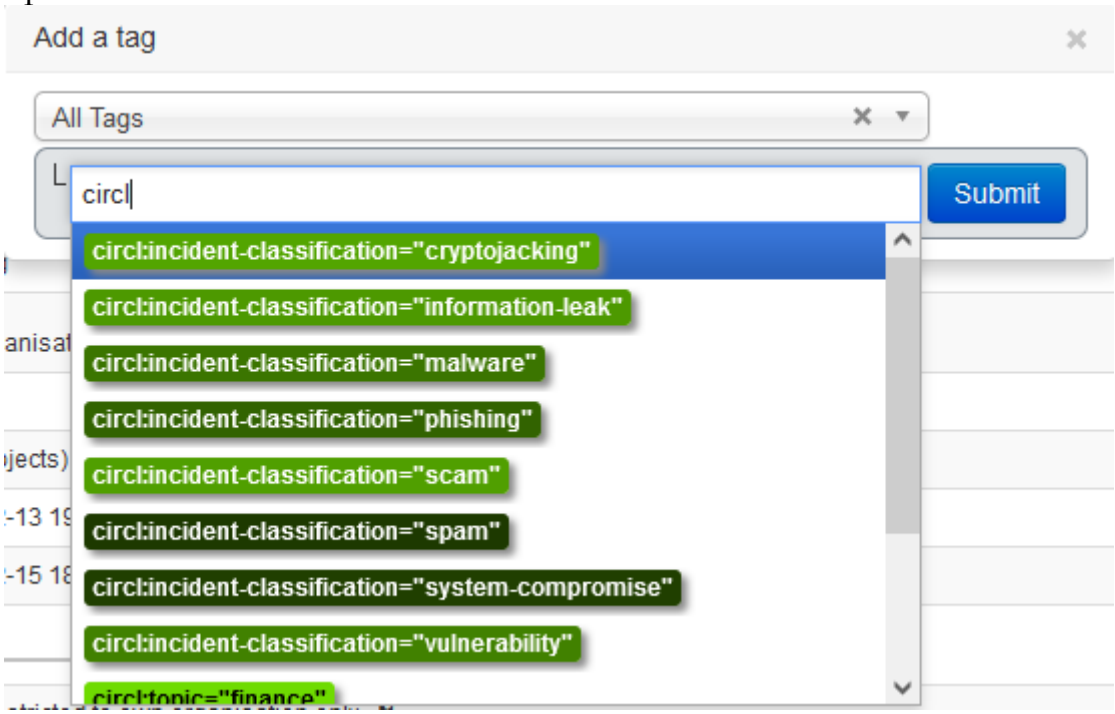
Aiemmissa tutkimuksissa MISP:n potentiaalista käyttöä on esitelty muun muassa pienissä ja keskisuurissa yrityksissä (van Haastrecht ym., 2021).

Kun MISP:ssä jaetaan informaatiota, sitä kutsutaan tapahtumaksi. Tapahtuma koostetaan ominaisuuslistoista, joihin kuuluu esimerkiksi IP-osoitteita ja

tiedostojen tiivisteitä. (Fotiadou, 2020; MISP, 2023.) Jokaisessa tapahtumassa on ainakin seuraavat tiedot, kun sellainen luodaan (MISP, 2023):

- Jakamisen taso (esimerkiksi vain organisaation sisällä)
- Luonnin päivämäärä
- Uhkan taso (matala, keskitaso, korkea)
- Tapahtuman yleistiedot, kuten tapahtuman numero ja luojan tiedot (esimerkiksi sähköposti ja organisaation nimi)
- Onko tapahtuma jonkun toisen tapahtuman osa tai jatke
- Analyysin vaihe (alkanut, vaiheessa, valmis)

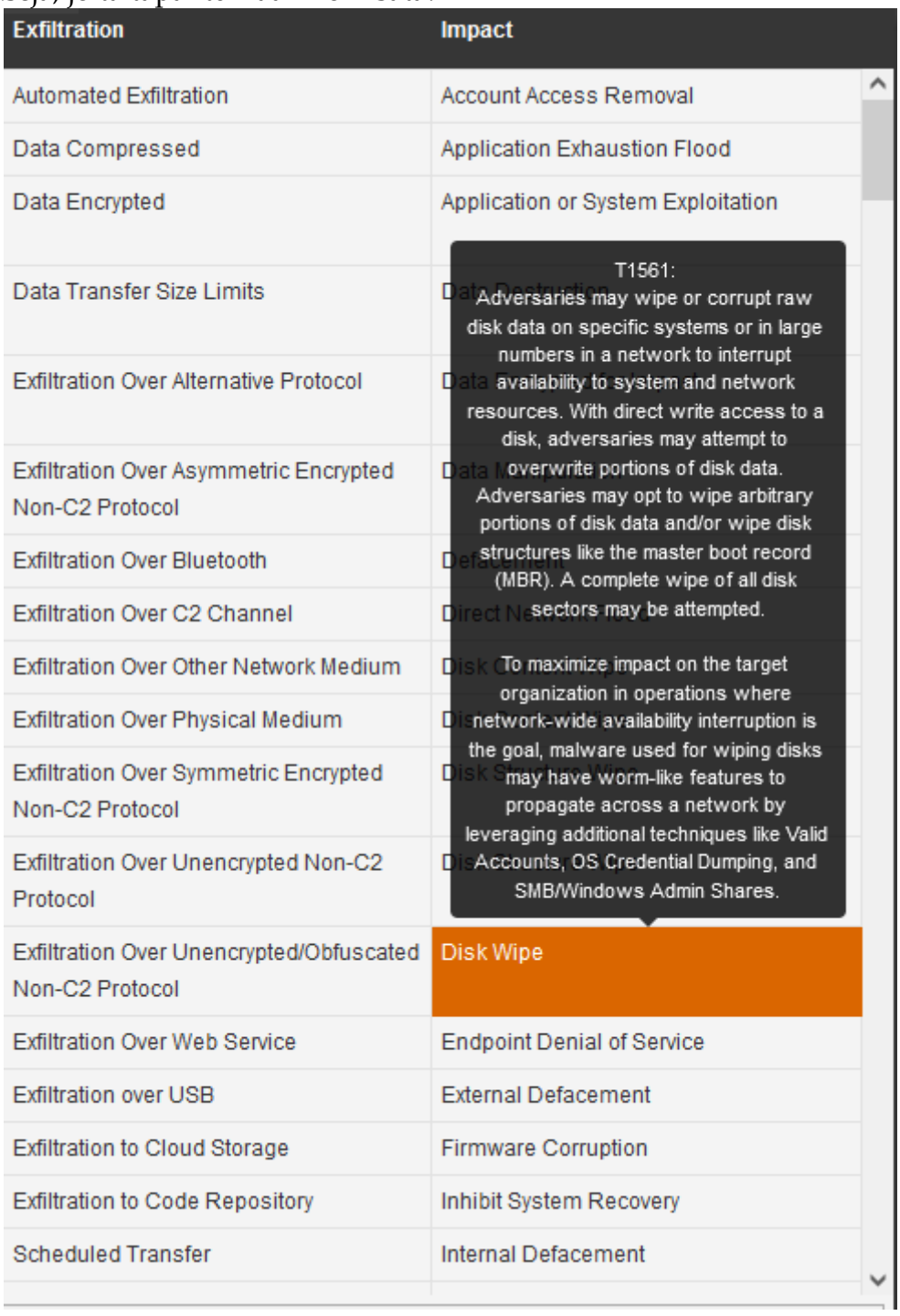
Tapahtumaan yleensä lisätään myös tunnisteita ja galakseja. Tunnisteilla tarkoitetaan kyseiseen tapahtumaan liitettäviä piirteitä. Esimerkiksi haittaohjelmaan liittyvään tapahtumaan voidaan lisätä tunnisteita kuten ”haittaohjelma” ja ”trojalainen.” Käyttäjät voivat lisätä omia tunnisteita MISP:n, mistä voi olla hyötyä esimerkiksi, jos organisaatiolla on jokin oma organisaation sisäinen tunniste tai tunnisteet käytössä. Alla olevasta kuvasta voi nähdä esimerkkejä tunnisteista, joita tapahtumaan voi lisätä:



KUVIO 2 Tunnisteet

Galaksit ovat puolestaan metodi MISP:ssä, jonka avulla laaja objekti, joka sisältää paljon tietoa, voidaan liittää tapahtumaan. Galaksi on kuin tietosanakirja, ja galaksi voikin olla esimerkiksi jonkin kyberhyökkäyksen vaikutus, ja jos kyseinen galaksi liitetään tapahtumaan, voi kyseistä galaksia painamalla lukea lisätietoa kyseisestä vaikutuksesta. Galaksia lisätessään käyttäjä voi viedä hiiren galaksin päälle, ja MISP näyttää tiedot tiivistetysti kyseisestä galaksista. Tästä on hyötyä esimerkiksi silloin, jos termi ei ole käyttäjälle täysin tuttu, ja näin käyttäjän ei

tarvitse avata aina uutta sivua tarkistaakseen kyseisen galaksin tiedot. Käyttäjät voivat myös lisätä omia galakseja MISP:n. Alla olevasta kuvasta näkyy erilaisia galakseja, joita tapahtumaan voi lisätä:



KUVIO 3 Galaksit

Kuviossa 3 näkyy vain pieni määrä kaikista mahdollisista galakseista, joita MISP:ssä on. Jokaista galaksia klikkaamalla avautuu oma sivu, josta käyttäjä voi lukea lisätietoa kyseisestä termistä.

Pohjatietojen lisäksi jokaiseen tapahtumaan olisi hyvä lisätä ainakin seuraavat tiedot, jos mahdollista (MISP, 2023):

- Hyökkääjän alkuperäinen IP-osoite
- Sähköposti, jota käytettiin haittaohjelman jakamiseen
- Tarkistussumma, esimerkiksi MD5 tai SHA256
- Hyökkääjän kokonainen isäntänimi (engl. Host name) tai nimipalvelun (DNS) nimi
- Haittaohjelman käyttämä verkkotunnus (engl. Domain)

Alla olevasta kuvasta näkyy yhdessä tapahtumassa olevia attribuutteja:

☐	2023-02-13	Payload delivery	filename	~WRS{CDE70751-8E1C-4EA8-B63D-0F9FAC4ADB0B}.tmp
☐	2023-02-13	Payload delivery	filename	Invoice-Number-579705.LNK
☐	2023-02-13	Payload delivery	md5	77dc1ba26c6157aef7638e5cc2426b00
☐	2023-02-13	Network activity	ip-dst	162.251.81.235
☐	2023-02-13	Payload delivery	sha256	c6ae8e9e00713ecb94843892fb49abb5234105a363cfdf46412423a244530d1a
☐	2023-02-13	Payload delivery	md5	8ae2bc02f5ed0cf08b844d09d35e13ba
☐	2023-02-13	Payload delivery	sha256	99b1d396c891e74ea83c2de381779da317cd2b807b373e980e65649171796189
☐	2023-02-13	External analysis	link	https://www.virustotal.com/#/file/99b1d396c891e74ea83c2de381779da317cd2b807b373e980e65649171796189/detection
☐	2023-02-13	Payload delivery	filename	HEUR_VBA.O2
☐	2023-02-13	Payload delivery	filename	Trojan.Generic
☐	2023-02-13	Network activity	ip-dst	12.162.84.2
☐	2023-02-13	Network activity	ip-dst	158.69.249.236
☐	2023-02-13	Network activity	ip-dst	192.241.241.94
☐	2023-02-13	Payload delivery	sha256	3aae0a07f4af6eb722b1e1ccbf286b07dd3481291d73ac52789a1edd6e58df47
☐	2023-02-13	Network activity	ip-dst	205.186.133.51
☐	2023-02-13	Network activity	ip-dst	218.213.239.89
☐	2023-02-13	Network activity	ip-dst	220.227.247.35
☐	2023-02-13	Network activity	ip-dst	87.106.37.146
☐	2023-02-13	Network activity	domain	iclub8.hk
☐	2023-02-13	Payload delivery	sha256	3882a3e04d6cf66707b31c8cb14a7c9fe512d10dd355f97a37e8666270f6e17d
☐	2023-02-13	Payload delivery	filename	~$Normal.dotm
☐	2023-02-13	Payload delivery	filename	~$voice-Number-579705.doc
☐	2023-02-13	External analysis	link	https://www.hybrid-analysis.com/sample/99b1d396c891e74ea83c2de381779da317cd2b807b373e980e65649171796189?environmentId=120

KUVIO 4 Tapahtuman attribuutit

Yksittäisiin attribuutteihinkin voidaan tarvittaessa liittää tunnisteita ja galakseja. Lisäksi attribuuttien näkyvyyttä voidaan muokata, jolloin kaikki tapahtuman attribuutit eivät näy muille organisaatioille esimerkiksi tapahtumaa julkaistessa.

Tapahtumatietoja voidaan lisätä tapahtumaan manuaalisesti tai tuomalla niitä ulkoisista lähteistä. Tapahtumatiedot voivat olla esimerkiksi tekstimuodossa, tai niitä voidaan tuoda erilaisista viitekehyksistä (MISP, 2023).

Käyttäjä voi myös lisätä erilaisia liitteitä tapahtumaan, kuten raportteja tai jopa itse haittaohjelmatiedoston. Liitetty haittaohjelmatiedosto pakataan sekä suojataan salasanalla, jotta muut käyttäjät eivät vahingossa aukaise ja aja tiedostoa. (MISP, 2023.)

Kun tapahtumaan on lisätty kaikki tarvittavat tiedot, se voidaan julkaista. Kun tapahtuma julkaistaan, julkaisusta lähtee tieto sähköpostilla kaikille oman organisaation jäsenille. Tapahtuma voidaan julkaista myös ilman sähköposti-ilmoitusta. Lisäksi tapahtuman jakeluasetusten mukaan, tapahtuman julkaisusta lähtee tieto myös esimerkiksi oman jakeluryhmän jäsenille. (MISP, 2023.)

MISP asennetaan yleensä virtuaalikoneille. MISP:n voi asentaa itse käsin tai ladata valmiin virtuaalikoneen Internetistä. Lisäksi Luxemburgin tietokoneonnettomuuksien torjuntakeskus (CIRCL) ylläpitää verkossa MISP:n virtuaalikonetta. (MISP, 2023.)

Käyttäjän toimintaa on helpotettu MISP:ssä siten, että suuret pyynnöt tai tehtävät pyörivät taustalla sen jälkeen, kun pyynnöt tai tehtävät ovat aloitettu, antaen käyttäjälle mahdollisuuden tehdä muita asioita alustalla sen aikaa, kun tehtävää prosessoidaan (MISP, 2023). Esimerkki tällaisesta tehtävästä on uhkatietosyötteiden varastoiminen MISP:n.

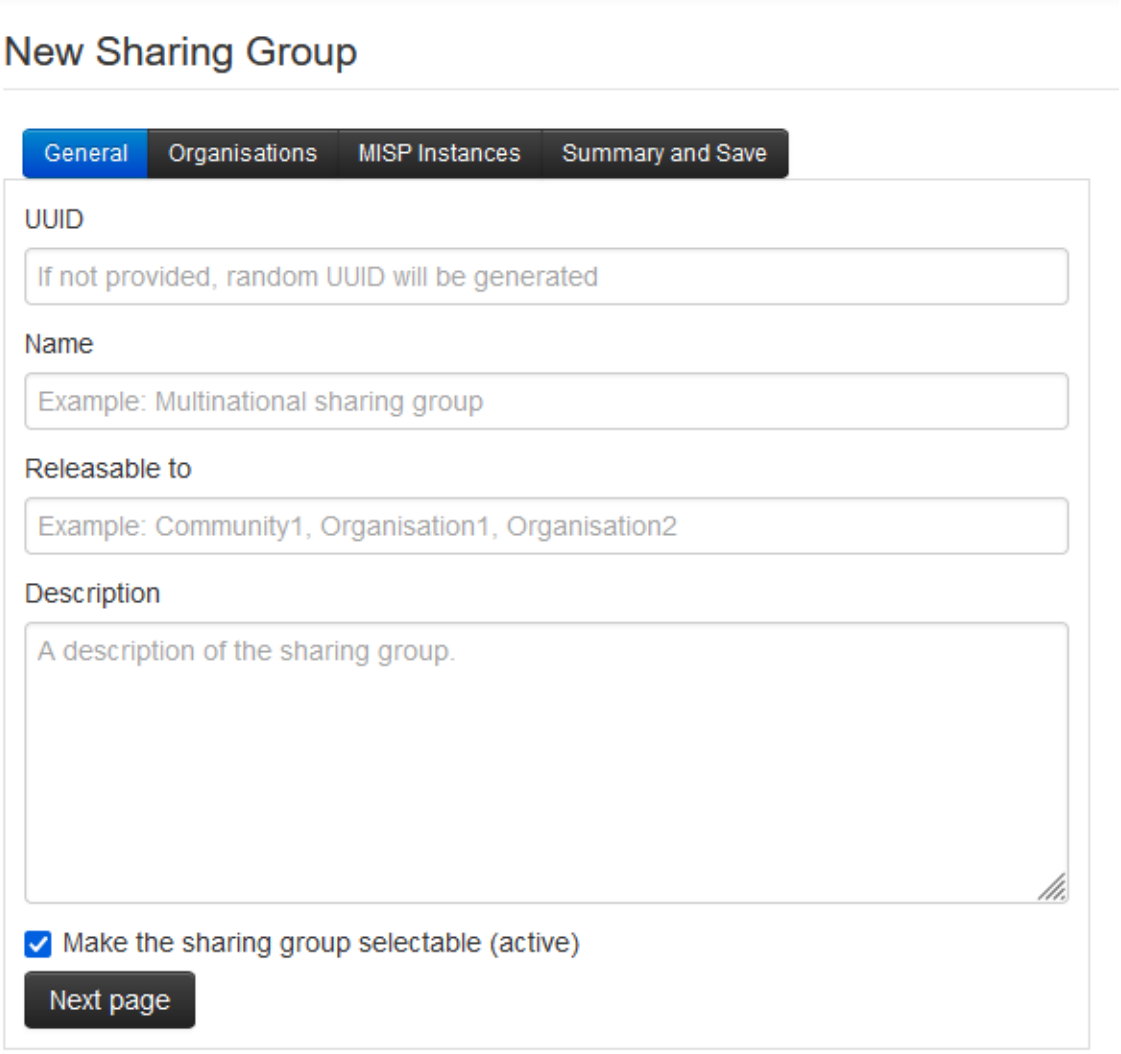
Ylläpitoroolit jakautuvat kahteen osaan: sivuston ylläpitäjiin ja organisaation ylläpitäjiin. Sivuston ylläpitäjät hallitsevat kaikkea ylläpitotoimintaa ja voivat esimerkiksi muokata käyttäjien rooleja. Organisaation ylläpitäjät puolestaan voivat muokata vain oman organisaation käyttäjiä, lokeja ja tapahtumia. (MISP, 2023.)

Uhkatietosyötteet (engl. Feeds) ovat tärkeä osa MISP:n toimintaa. Uhkatietosyötteistä saadaan paljon tietoa vallitsevista uhista. Uhkatietosyötteet ovat kuitenkin laadultaan erilaisia, ja jotkin uhkatietoja toimittavat osapuolet kuvaavat todella ylimalkaisesti uhkatietoja, jolloin loppukäyttäjän vastuulle jää päättää, miten toimia (Li ym., 2019).

MISP:stä löytyy myös varoitus- sekä huomautuslistoja, joiden avulla pyritään välttämään esimerkiksi vääriä positiivisia tunnisteissa. Käyttäjä voi lisätä omia varoitus- sekä huomautuslistoja, ja lisätä niihin esimerkiksi organisaation omia IP-osoitteita tai muita tietoja, jotta vältytään turhilta hämmennyksiltä sekä korrelaatioilta.

MISP:ssä on myös uhkatietojen kulumisen huomioivia malleja. Kun tietty hyökkäystapa vähenee tai kyberhyökkäyksessä käytetty IP-osoite saadaan takaisin oikeaan lailliseen käyttöön tai tietojenkalastelussa käytetty verkkosivu poistetaan, niin kyseiset uhkatiedot eivät ole enää päteviä (Iklody ym., 2018). Nämä kulumismallit toimivat niin, että ajan kuluessa uhkatiedon pisteissä laskettu luotettavuus vähenee, mikäli kyseistä uhkatietoa ei havaita enää. Käyttäjät voivat myös luoda omia kaavoja ja toimintamalleja uhkatiedon luotettavuuden heikkenemiselle (MISP, 2023).

MISP:ssä sisäinen yhteisö voidaan muodostaa seuraavanlaisesti: Luodaan asetuksista uusi jakoryhmä, jonka jälkeen ryhmälle määritellään oma tunniste, nimi, kenelle ryhmä voidaan julkaista sekä ryhmän kuvaus. Alla olevasta kuvasta voi nähdä edellä mainitut määritykset.



KUVIO 5 Uusi jakoryhmä

Sen jälkeen ryhmään lisätään ne organisaatiot, jotka kuuluvat tähän ryhmään. Organisaatiot voidaan lisätä helposti organisaatiot-välilehdessä. Kolmannessa välilehdessä ”Palvelimet” määritellään ne MISP instanssit, joiden kanssa jakoryhmä voi synkronoida tietoja. Lopuksi näytetään yhteenveto, jossa ryhmän luoja voi tarkistaa asetukset ja lopuksi tallentaa jakoryhmän.

Kun MISP:ssä halutaan jakaa tietoja organisaatioiden välillä, voidaan luoda erilaisia jakoryhmiä sekä muokata niiden asetuksia. Jakoryhmien avulla organisaatiot voivat jakaa ja käyttää omia sekä toisten organisaatioiden tapahtumatietoja omissa tapahtumissaan. (MISP, 2023.)

Käytännössä tietojen hakeminen ulkoisista lähteistä tapahtuu kahdella tavalla, joko synkronoinnilla, tai linkkien kautta käyttäen uhkatietosyötteitä. Synkronointi tapahtuu lisäämällä synkronointiserveri toisen organisaation MISP instanssiin. Uhkatietosyötteet voidaan puolestaan hakea MISP:ssä helposti syötteet sivulta. Syötteet ovat paikallisia tai ulkoisia resursseja, jotka sisältävät uhkatunnisteita (MISP, 2023).

Synkronoinnissa on otettava huomioon muutamia asetuksia. Ensinnäkin veto- ja työntöasetukset on syytä huomioida, sillä ne määrittelevät kuinka tietoa jaetaan muille instansseille. Esimerkiksi työnnön valitsemalla tapahtuma synkronoidaan aina kaikkien muiden instanssien kanssa, kun tapahtuma julkaistaan. Työntö- ja vetoasetuksia tarkastellaan tarkemmin luvussa 6.

Synkronoinnin toteuttamisen jälkeen ryhmän jäsenet voivat aloittaa tietojen jakamisen keskenään. Kun yksi ryhmän jäsen julkaisee tapahtuman, kaikki ryhmän organisaatiot saavat tiedon julkaisusta. Jos tapahtumassa on sellaisia attribuutteja, joita organisaatio ei halua muiden ryhmän jäsenten tietoon, voi organisaatio kyseisen attribuutin näkyvyysasetuksia muuttamalla rajata tiedon näkyvyyden vain omaan organisaation. Siten, vaikka tapahtuma on muuten julkaistu kaikille ryhmän jäsenille, kyseinen attribuutti tai attribuutit eivät näy muille.

Ryhmien jäsenet voivat tarkastella muiden jäsenten julkaisemia tapahtumia, ja tarvittaessa ehdottaa muokkauksia niihin. Ehdotuksen tekemisen jälkeen tapahtuman alkuperäinen julkaisija voi hyväksyä ehdotuksen tarvittaessa.

Ryhmän jäsenet voivat myös delegoida tapahtumien julkaisun toisille ryhmän jäsenille. Tästä voi olla hyötyä esimerkiksi silloin, kun organisaatio ei halua tulla yhdistetyksi kyseiseen tapahtumaan. Delegoinnin kohde voi joko hyväksyä tai hylätä tapahtuman julkaisun.

MISP:n käyttäjät ovat yleensä taustaltaan erilaisia. MISP soveltuu monen eri tekijän käyttöön, kuten esimerkiksi organisaation petoksien tutkijalle, tietoturva-analyytikolle sekä riskien analysoijille (MISP, 2023).

4 TUTKIMUSMENETELMÄ

Tässä luvussa käydään läpi tämän tutkielman tutkimusmenetelmät, jotka ovat kirjallisuuskatsaus ja konstruktiivinen tutkimusmenetelmä.

4.1 Kirjallisuuskatsaus

Kirjallisuuskatsauksen tavoitteena on tehdä yhteenveto aiemmasta tutkimuksesta, tarkastella kriittisesti aikaisemman tutkimuksen myötävaikutusta, selittää aikaisempien tutkimuksien tuloksia, sekä selventää vaihtoehtoisia näkemyksiä aikaisempaan tutkimukseen (Rowe, 2014).

Kirjallisuuskatsaus auttaa kirjoittajaa oppimaan aiheesta niin paljon kuin mahdollista, jonka lisäksi kirjoittajalle selvenee, mitä aiheesta on jo kirjoitettu sekä mitä mahdollisesti puuttuu. Lukijalle puolestaan kirjallisuuskatsaus on osoitus siitä, että tutkimuksen kirjoittaja on perehtynyt aiheeseen ja osaa hyvin aihealueen käsitteet. (Denney & Tewksbury, 2013.) Lisäksi kirjallisuuskatsauksen tekeminen on yleensä vaadittu osa esimerkiksi loppututkielmaa, ja sen toteuttaminen auttaa tekijää tarkistamaan, ettei hänen esittämiin tutkimuskysymyksiin ole vielä vastattu. Kirjallisuuskatsauksen teko voi myös antaa tekijälle uusia ideoita, joita hän voi käyttää omassa tutkimuksessaan, sekä se auttaa tutkijaa asettamaan tutkimuksensa isompaan kontekstiin. (Knopf, 2006.) Kirjallisuuskatsaus sisältää lähes aina kattavan yleiskuvan aiheesta, käsitellen lyhyesti aiheeseen liittyvät alakohdat (Denney & Tewksbury, 2013).

Kirjallisuuskatsauksen rakentava pohja ovat lähteet. Lähteitä kerätään yleensä Internetin tietokannoista tai yliopiston kirjastoista. (Denney & Tewksbury, 2013.) Lähteiden valinnassa on syytä ottaa huomioon niiden sopivuus, sillä kaikki lähteet eivät välttämättä sovellu kirjallisuuskatsauksen lähteiksi (Denney & Tewksbury, 2013).

Denneyn ja Tewksburyn (2013) mukaan sopiviksi lähteiksi kelpaavat seuraavat lähteet:

- Tieteelliset empiiriset artikkelit, väitöskirjat ja kirjat

- Tieteelliset ei-empiiriset artikkelit ja esseet
- Oppikirjat, tietosanakirjat ja sanakirjat
- Tietyt kansainvälisesti tunnustetut uutislehdet
- Kauppalehtien artikkelit

Parhaimmat lähteet ovat Denneyn ja Tewksburyn (2013) mukaan akateemiset artikkelit ja akateemiset kirjat. Perinteinen kirjallisuuskatsaus käyttääkin lähteinään yleensä akateemisten aikakausilehtien ja kustantajien julkaisemia kirjoja ja artikkeleita (Knopf, 2006). Lähteiden laadun arviointiin voi käyttää esimerkiksi eri instituutioiden ylläpitämiä verkkosivuja, jotka arvioivat lähteitä arvosanoin (Paul & Criado, 2020). Esimerkiksi tämän tutkielman lähteiden arviointiin olen käyttänyt Julkaisufoorumia, joka arvioi tutkimuksien julkaisukanavien laatua.

4.2 Konstruktiivinen tutkimusmenetelmä

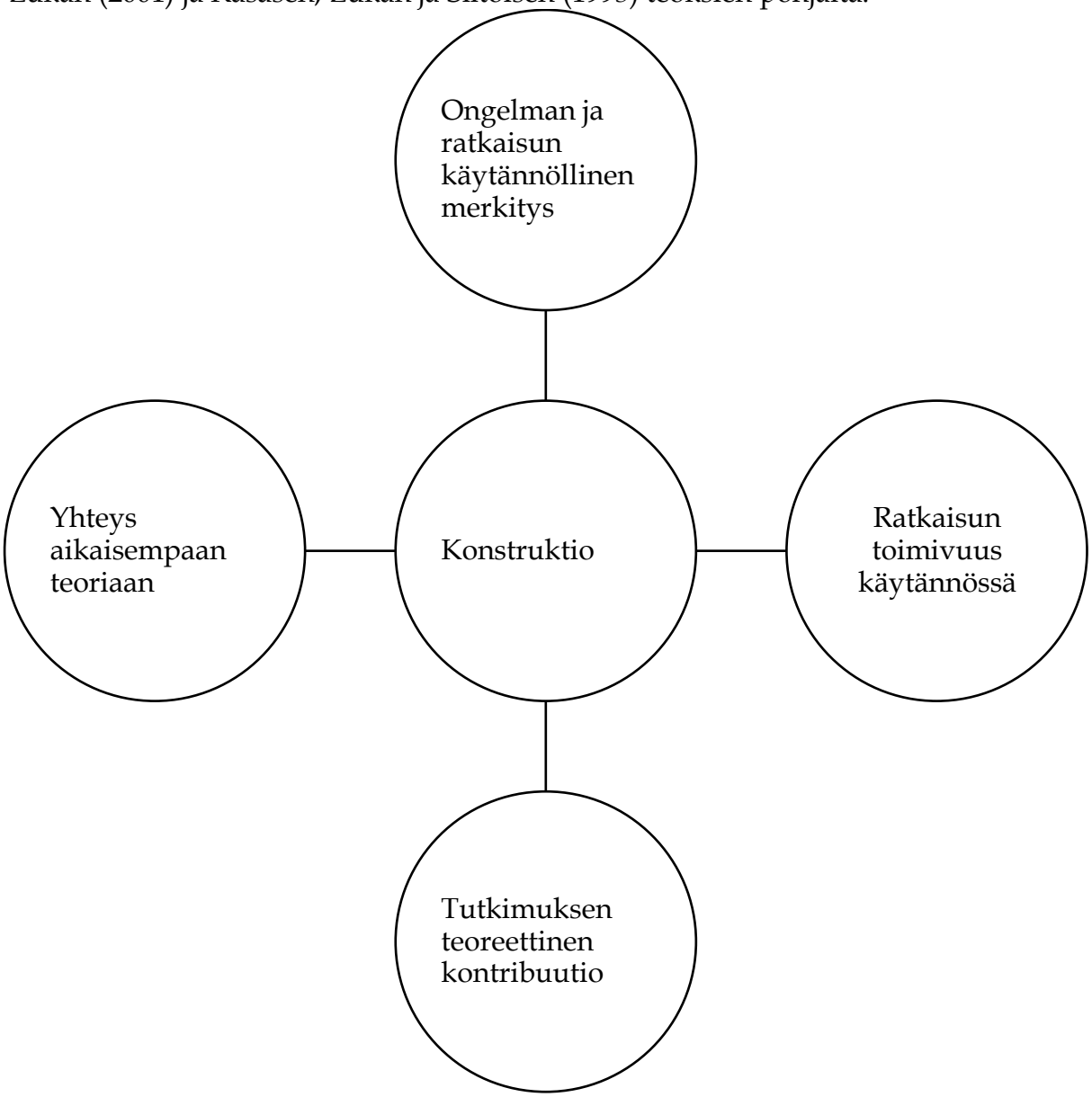
Konstruktiivinen tutkimusmenetelmä pyrkii etsimään ratkaisua reaalimaailman ongelmaan (Kasanen, Lukka & Siitonen, 1993). Konstruktiivinen tutkimusmenetelmä kehitettiin aluksi tukemaan kirjanpidon hallinnan tutkimusta (Jones, Gold & Claxton, 2022) mutta sitä on sen jälkeen käytetty myös tietojärjestelmien hallinnan ja logistiikan tutkimuksissa (Piirainen & Gonzalez, 2014). Konstruktiivinen tutkimusote pyrkii kehittämään konstruktion käyttämällä olemassa olevaa tietoa uusilla tavoilla, ja mahdollisesti yhdistäen puuttuvia linkkejä (Crnkovic, 2010). Konstruktiivinen tutkimusmenetelmä on ollut varsin suosittu Suomessa (Piirainen & Gonzalez, 2014) sekä joissain määrin Skandinaviassakin (Jönsson & Lukka, 2006).

Konstruktiivisen tutkimuksen vaiheet voidaan jakaa kuuteen osaan. Alla oleva taulukko havainnollistaa näitä vaiheita. Taulukko on muodostettu Kasasen, Lukan ja Siitosen, (1993) työstä:

TAULUKKO 1 Konstruktiivisen tutkimuksen vaiheet

Vaihe	Konstruktiivinen tutkimus
1	Löydä käytännön ongelma, jota voidaan myös tutkia.
2	Tutustu aiheeseen perin pohjin.
3	Rakenna (innovoi) ratkaisu ongelmaan.
4	Näytä että ratkaisu toimii.
5	Osoita tutkimuksen tieteellinen kontribuutio.
6	Tutki ratkaisun käyttökelpoisuuden laajuutta ja yleistettävyyttä.

Alla oleva kuvio havainnollistaa konstruktiivista tutkimusmenetelmää. Kuvio on tehty Lukan (2001) ja Kasasen, Lukan ja Siitoisen (1993) teoksien pohjalta:



KUVIO 6 Konstruktiivinen tutkimusote

Konstruktiivisen tutkimuksen luomukset, kuten mallit, diagrammit, suunnitelmat ja algoritmit ovat tyypillisiä konstruktioita, joita syntyy tutkimuksen perusteella (Crnkovic, 2010).

Konstruktiivisen tutkimuksen onnistuminen ja menestys perustuu pitkälti luodun konstruktion käytännön hyötyyn organisaatiossa (Rautiainen, Sippola & Mättö, 2017). Toisaalta ei ole aina selkeää, miten hyödyllisyys määritellään, ja toimiiko konstruktio käytännössä (Labro, & Tuomela, 2003; Piirainen & Gonzalez, 2014). Rautiainen, Sippola ja Mättö (2017) esittivät merkitystestin (engl. Relevance test) sisällyttämistä konstruktiivisen tutkimuksen yhteyteen, jonka avulla voitaisiin arvioida, onko konstruktiosta hyötyä.

Konstruktiivinen tutkimus antaa tuloksia, joilla on sekä teoreettista että käytännöllistä hyötyä. Tutkimus pyrkii yleensä selvittämään tietoon liittyviä ongelmia, liittyen asian uutuuteen, käyttökelpoisuuteen ja parantamiseen. (Crnkovic, 2010; Kasanen, Lukka & Siitonen, 1993.)

5 UHKATIEDON JA MISP:N KÄYTTÖ YKSITTÄISESSÄ KORKEAKOULUSSA

Tässä luvussa tarkastellaan, miten yksittäisessä yliopistossa voitaisiin käyttää hyödyksi uhkatietoja sekä uhkatietojen jakoalusta MISP:ä.

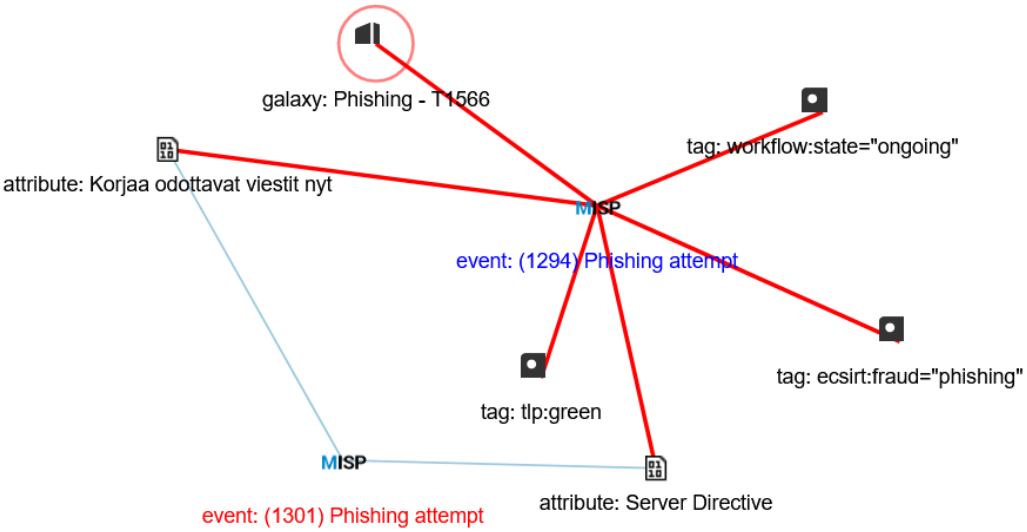
Yksittäisessä yliopistossa MISP:ä voidaan käyttää esimerkiksi poikkeamatapausten selvittelyyn sekä niiden vertailuun. Lisäksi MISP:n voi integroida varsin vaivattomasti esimerkiksi lokienkeräysjärjestelmiin, tunkeilijan havainnointijärjestelmiin sekä muihin yleisesti käytettyihin järjestelmiin kuten Microsoft Azureen/Sentineliin, jotka valvovat loppukäyttäjien laitteiden toimintaa organisaatiossa ja joihin tulee niiden havaitsemat poikkeamat.

Kun MISP:n integroi toisen palvelun kanssa, yleinen toimintapa sovellusten kesken on seuraavanlainen: esimerkiksi lokienhallintapalvelu tarkistaa jokaisen lokin kohdalla, löytyykö jokin lokissa esiintyvä tieto MISP:n puolelta. Jos jokin tieto löytyy, palvelu rikastaa kyseisen lokin lisäämällä MISP:stä haetut tapahtumatiedot. Toisaalta esimerkiksi integraatio asiakaspalveluhallintaan tarkoitetun järjestelmän kanssa voisi auttaa luomaan tapahtumia MISP:n asiakaspalvelujärjestelmästä käsin. Palvelu esitäyttäisi asiakkaan tiketin perusteella MISP:n tapahtuman tietoja, ja käyttäjä voi lisätä tarvittaessa muita tietoja.

Kun yliopistossa havaitaan poikkeama, sen tiedot voidaan kirjata MISP:iin. MISP:iin voidaan kirjata kaikki tarpeelliseksi koetut tiedot. Esimerkiksi kalastelukampanjan tapauksessa voidaan kirjata sähköpostiosoitteet, josta kalasteluviestit on lähetetty, mahdolliset haitalliset liitteet ja linkit, viestin otsikko ja sisältö, lähettäjän IP-osoite sekä muut tarvittavat tiedot.

Yliopisto voikin käyttää MISP:ä esimerkiksi varastona, johon kirjataan esimerkiksi erilaiset poikkeamat tai muut tapahtumat, joita yliopisto haluaa kirjata ylös. Automatisoinnin avulla MISP:n voidaan syöttää paljon tietoa eri lähteistä, mikä helpottaa tietojen yhdistelyä ja vertailua.

Jos yksittäinen attribuutti linkittyy useampaan tapahtumaan, se voidaan näyttää visuaalisesti. Alla ovesta kuvasta näkyy kaksi tapahtumaa (Engl. event), joissa on yksi tai useampi sama attribuutti:



KUVIO 7 Attribuuttien korrelaatio

Tapahtumaan 1294 kuuluvat attribuutit, tunnisteet ja galaksit näkyvät punaisella viivalla, jonka lisäksi tapahtumaan 1301 linkittyvät attribuutit näkyvät sinisellä viivalla. Tämä tarkoittaa sitä, että tapahtumilla 1294 ja 1301 on kaksi yhdistävää attribuuttia.

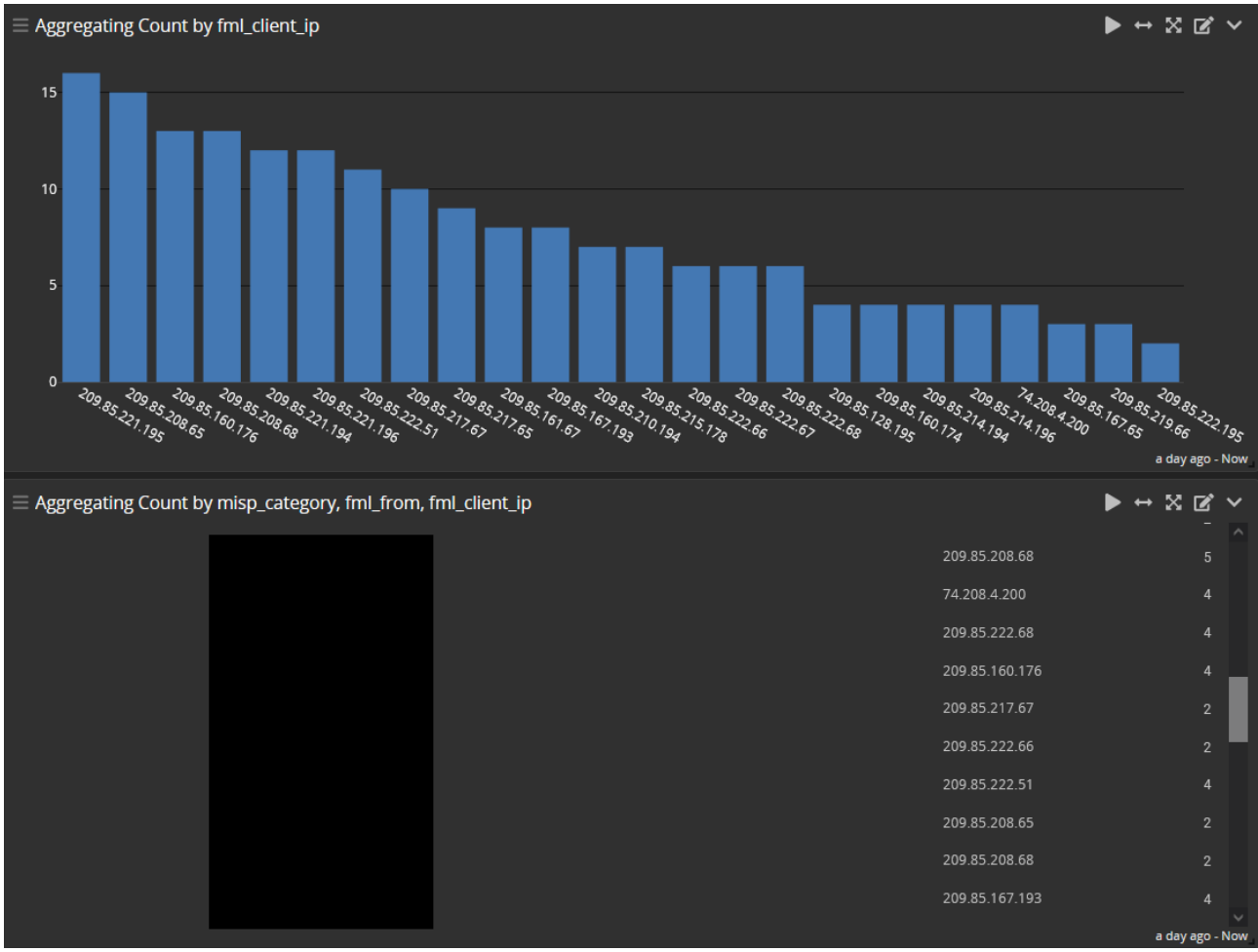
MISP:ssä olevat attribuutit voidaan viedä esimerkiksi tunkeilijan havaitsemisjärjestelmään (Engl. IDS), joka voi auttaa sovellusta havaitsemaan esimerkiksi epäilyttäviä IP-osoitteita tai verkkotunnuksia ja siten estää ne.

Yliopisto voi myös muodostaa isompaa tilannekuvaa, kun se yhdistää tietoja, jotka ovat esimerkiksi MISP:ssä, lokienhallintapalvelussa, tunkeilijan havaitsemisjärjestelmässä sekä muissa järjestelmissä, joita yliopisto käyttää. Tietojen avulla voidaan esimerkiksi luoda tai muokata palomuurien estolistoja.

Toisaalta MISP:n aktiivinen käyttö ja ylläpito vaatii työntekijöiltä tiettyjen asioiden osaamista. Esimerkiksi MISP:n ja siihen liittyvien osien asennus vaatii Python-ohjelmointikielen sekä Linux-käyttöjärjestelmän käytön tuntemista ja osaamista.

Kun MISP:ssä julkaisee tapahtuman, siitä lähtee sähköpostiviesti kyseisen instanssin käyttäjille. Koska tapahtumassa voi olla sensitiivistä tietoa, on salaaminen hyvä ottaa käyttöön. Salaus toteutettiin ottamalla käyttöön GnuPG-salausohjelmisto. Jokaisen käyttäjän tulee syöttää omaan MISP profiiliinsa oma julkinen avain, jotta he voivat vastaanottaa salattuja viestejä. Jos käyttäjällä ei ole julkista avainta profiilissaan, ei sähköposti lähde kyseiselle henkilölle.

MISP:n integrointi lokienhallintapalvelun kanssa tehtiin API-rajapinnan kautta. Integroinnin toteuttamisen jälkeen lokienhallintapalvelu tekee jokaisen lokin kohdalla kyselyn MISP:n, ja jos jokin lokissa olevista tiedoista löytyy MISP:stä, lokienhallintapalvelu lisää kyseisen MISP tapahtuman tiedot omaan lokiinsa. Lisäksi lokienhallintapalveluun pystyi toteuttamaan paneelin, johon kerääntyi esimerkiksi IP ja sähköpostitietoja. Alla oleva kuva havainnollistaa tietojen koontia yhden paneelin alapaneeliin:

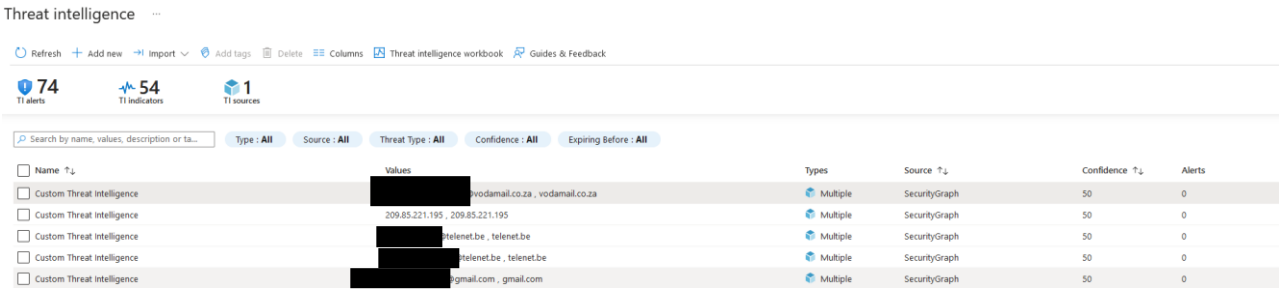


KUVIO 8 Lokienhallintapalvelun MISP-paneelin alapaneeli

Paneeliin voi luoda useita eri alapaneeleita, joihin voi rakentaa mieleisensä tietojenkeruukuviot. Käyttäjä voi esimerkiksi luoda paneelin, josta ilmenee kuinka monesta eri IP-osoitteesta tietty sähköposti lähettää liikennettä. Kuvioita ja tietojen yhdistelemistä on useita erilaisia.

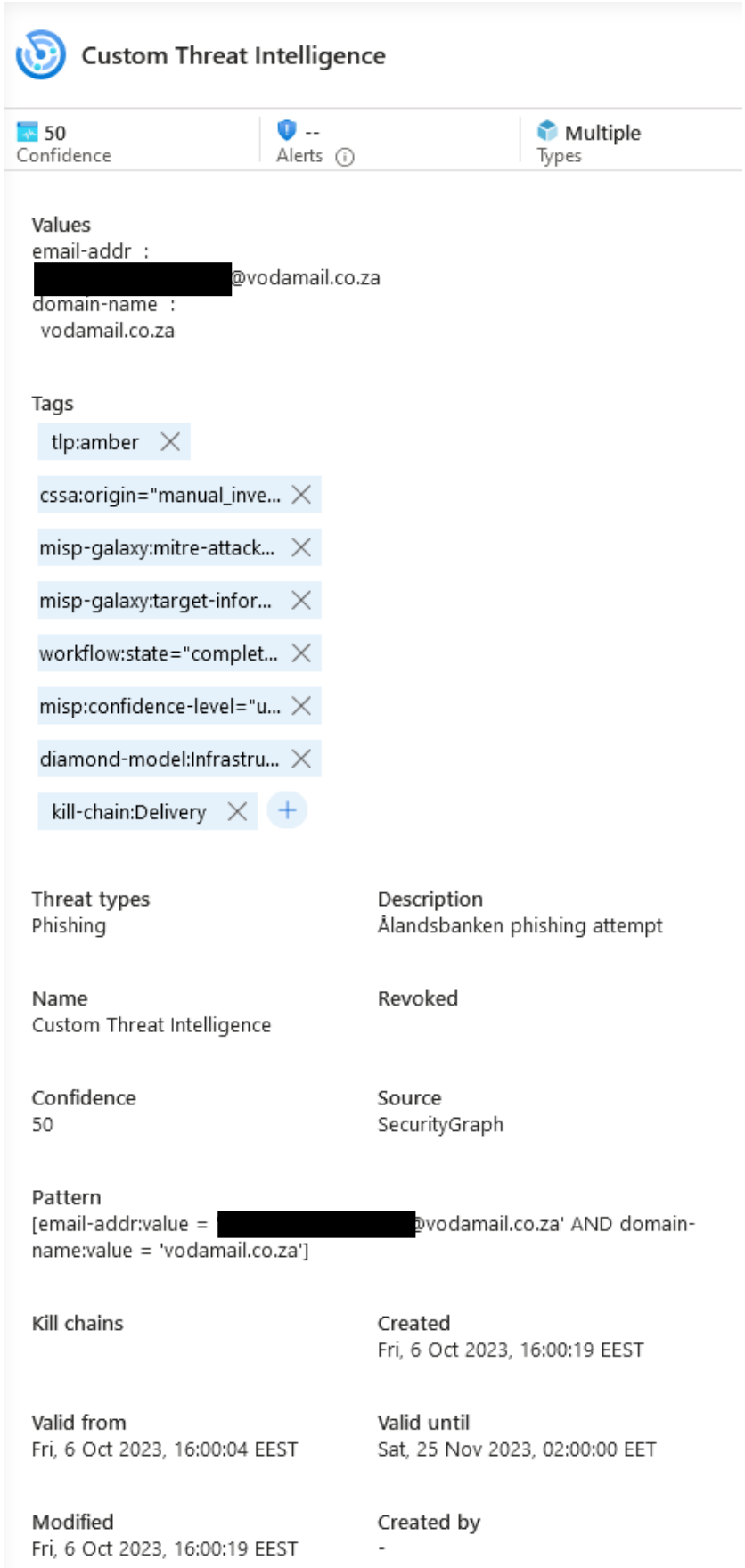
Kyselyt MISP:n päin voivat olla varsin raskaita, sillä kyselyjä voi tulla jopa miljoona päivässä. Tämä kuormittaa MISP:n järjestelmää paljon, mikä saattaa rajoittaa useiden eri integraatioiden toteuttamista. Tämän tutkielman aikana ei kuitenkaan ilmennyt minkäänlaisia ongelmia integraatioiden toteutuksien kanssa, joita tehtiin yhteensä neljä kappaletta.

MISP:n integraatio Microsoft Sentineliin mahdollistaa uhkatietojen viemisen MISP:stä Sentinelin uhkatietotauluun. MISP voidaan asettaa työntämään esimerkiksi julkaistujen tapahtumien uhkatiedot Sentineliin parin viikon välein. Sentinelissä puolestaan otetaan käyttöön tarvittavat uhkatiedon hyödyntämiseen tarvittavat analytiikkasäännöt, jotka käyttävät yhtenä lähteenään MISP:stä saatuja uhkatietoja. Jos jokin tieto korreloi jossain muualla Sentinelissä, niin siitä luodaan uusi poikkeama. Alla olevasta kuvasta näkyy Sentinelin uhkatietotaulukko, johon on haettu uhkatietoja MISP:stä:



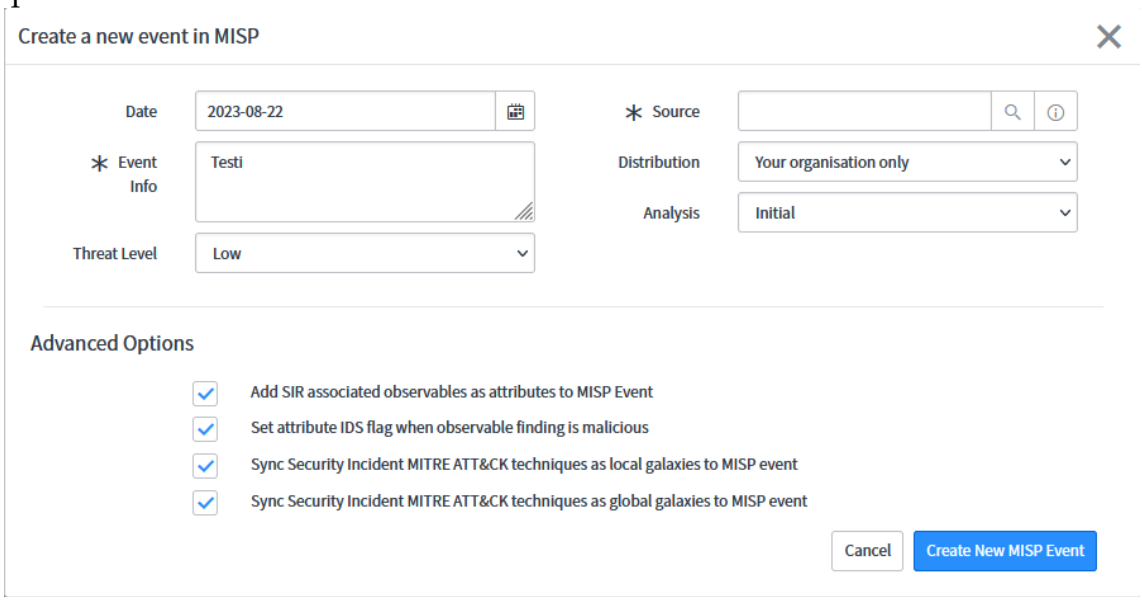
KUVIO 9 Sentinelin uhkatietotaulukko

Yksittäistä uhkatietoa painamalla avautuu lisätietopaneeli, joka kertoo esimerkiksi, onko kyseisen tiedon pohjalta syntynyt hälytyksiä, mitä tunnisteita se sisältää sekä muuta lisätietoa mitä MISP:stä on haettu. Alla oleva kuva näyttää yhden uhkatiedon lisätietopaneelin:



KUVIO 10 Lisätietopaneeli

MISP:n integraatio tikettijärjestelmään voi nopeuttaa tapahtumien viemistä MISP:n. Esimerkiksi ServiceNow-tikettijärjestelmän voi yhdistää MISP:n kanssa, jonka jälkeen tapahtumia voi luoda tikettijärjestelmästä käsin. MISP kuuluu ServiceNow-palvelussa ”Security Operations” -lisäosaan, joka on käytännössä poikkeamanhallintatyökalu. Kun poikkeama on tehty, niin siitä voi luoda tapahtuman MISP:n. Alla olevasta kuvasta näkyy MISP tapahtuman luominen ServiceNow-palvelussa:



KUVIO 11 MISP tapahtuman luominen ServiceNow-palvelussa

Tapahtuman luomisen jälkeen tapahtumaa voi muokata suoraan ServiceNow-palvelussa, ilman että käyttäjän tarvitsee kirjautua erikseen MISP:n. Tämä vähentää järjestelmien välillä hyppelyä, kun tikettijärjestelmän käyttäjän ei tarvitse siirtyä MISP:n puolelle tekemään tapahtumaa.

Splunk on konegeneroidun datan etsimiseen, monitoroimiseen ja analysoimiseen tarkoitettu selaimessa toimiva sovellus. Integrointi Splunk sovellukseen tapahtui lisäämällä Splunkin sovelluskirjastosta MISP-lisäosa, ja yhdistämällä MISP instanssi. Sen jälkeen Splunkissa pystyi hakemaan tapahtumia sekä uhkatunnisteita MISP:stä. Näin tietojen vertailu Splunkin ja MISP:n välillä on nopeampaa ja helpompaa. Alla oleva kuva havainnollistaa haettuja uhkatunnistetietoja, jotka voi myös ladata Splunkista ulos PDF-muodossa:

| mispgetioc misp_instance=mispdev last="30d" (Columns 26-33 of 33)

#	misp_object_relation	misp_sharing_group_id	misp_tag	misp_text	misp_timestamp	misp_to_ids	misp_type	misp_value
1	EMAIL_ADDRESS EMAIL_ADDRESS EMAIL_ADDRESS EMAIL_ADDRESS EMAIL_ADDRESS EMAIL_ADDRESS EMAIL_ADDRESS EMAIL_ADDRESS EMAIL_ADDRESS	0 0 0 0 0 0 0 0 0			1675943040 1675943040 1675943040 1675943040 1675943040 1675943040 1675943040 1675943040 1675943040	True True True True True True True True True	email-src email-src email-src email-src email-src email-src email-src email-src email-src	[redacted]@gmail.com [redacted]@gmail. com [redacted]@gmail.com [redacted]@gmail.com [redacted]gmail.com [redacted]@gmail. com [redacted]@gmail.com [redacted]@gmail.com [redacted]@gmail. com

KUVIO 12 Yhden MISP tapahtuman uhkatunnistetietoja Splunkissa

Splunkissa pystyy myös luomaan tapahtumia MISP:n. Tällekin on oma paneeli, jossa käyttäjä pystyy valitsemaan haluamansa MISP instanssin, sekä syöttämään tapahtuman liittyvät tiedot, kuten nimen, uhkatunnisteet, tunnisteet (engl. Tags), ja valitsemaan julkaistaanko tapahtuma vai ei. Käyttäjä pystyy muokkaamaan mitä kaikkea tapahtuman julkaisemisen yhteydessä MISP:n viedään.

Huolimatta edellä mainituista mahdollisuuksista ja hyödyistä, MISP:n käyttöön liittyy myös ongelmia. MISP:n asentaminen ja varsinkin ylläpitäminen aiheuttivat valitettavan suurta päänvaivaa. Suurin osa ongelmista keskittyi tämän tutkielman kirjoittamisen aikana ylläpito-ongelmiin, johon kuului muun muassa ongelmat MISP:n päivittämisessä, tapahtumien julkaisussa, virhetilanteiden selvittelyssä ja korjaamisessa sekä GnuPG-salausohjelmiston käytössä MISP:n kanssa. Lisäksi ongelmia esiintyi myös tiedostojen oikeuksissa Linux-ympäristössä, johon MISP oli asennettu. MISP:n omat ohjeet voisivat huomioida paremmin alustakohtaiset erot komentojen ajamisessa komentoriviltä. Vaikka suurin osa edellä mainituista ongelmista saatiinkin korjattua, niiden korjaamiseen meni kohtuuttoman paljon aikaa, eikä asiaa auttanut se, että MISP:n omien virhe- ja testilokien sisältämät tiedot olivat yleensä todella vähäisiä ja ylimalkaisia. Lokitiedot jakaantuivat useaan eri paikkaan, ja yleensä lokitiedoissa ei joko ollut mitään tai todella vähän tietoa liittyen virheeseen, joka oli sillä hetkellä olennainen. Virheiden korjaaminen vaati yleensä lukuisten olemassa olevien ongelmatikettien lukemista Githubissa, ja yleensä juuri niihin ongelmiin ei löytynyt vastausta, mitkä olivat kyseessä tutkielmassa käytetyssä MISP-ympäristössä. Lisäksi vaikutti vahvasti siltä, että kun yhden asian korjasi, niin jotain muuta meni rikki. MISP kannustaa käyttäjiään vahvasti käyttämään MISP:ä ainoastaan käyttöliittymästä, mutta jos jotain menee siellä rikki, käyttöliittymän virhelokit eivät myöskään anna juuri mitään tietoa siitä, mikä on mennyt vikaan. Pahimmissa tapauksissa virheilmoitus on ”jotain meni vikaan, ota yhteyttä ylläpitäjään”, eikä mitään muuta. Lisäksi tämän tyylinen virheilmoitus aiheutti välillä sen, että

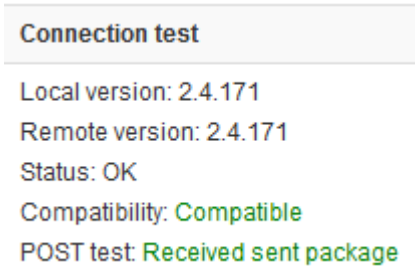
mikään muukaan toiminto järjestelmässä ei toiminut ennen kuin sivun tai koko istunnon päivitti. Tämä käytännössä pakottaa käyttäjän siirtymään käyttämään ja tutkimaan asiaa komentoriviltä. Linuxin lokitiedot eivät välttämättä myöskään kertoneet yhtään mitään, sillä välillä minkäänlaista virheilmoitusta ei rekisteröitynyt koneen lokitietoihin. Lisäosien asentaminen, päivittäminen ja virhetilanteiden korjaaminen olikin välillä suorastaan yritys ja erehdys -tyyppistä kokeilemista, ja jos jokin meni vikaan, niin palattiin aiemmin otettuun pikakuvaan (engl. Snapshot) instanssista.

6 UHKATIEDON JA MISP:N KÄYTTÖ KORKEAKOULUJEN VÄLILLÄ SUOMESSA

Tässä luvussa tarkastellaan, miten uhkatietoja ja MISP:ä voitaisiin hyödyntää Suomen korkeakoulujen kesken.

Suomen korkeakoulut voivat hyödyntää MISP:ä uhkatietojen jakamiseen ja siten parantaa omaa kyberpuolustustaan. MISP:n avulla korkeakoulut voisivat jakaa uhkatietoa tehokkaammin.

Uhkatietojen jakamista varten Jyväskylän yliopiston ja toisen organisaation välille muodostettiin synkronointiryhmä. Ensimmäiseksi toinen organisaatio lisättiin paikalliseksi organisaatioksi Jyväskylän yliopiston MISP instanssissa käyttäen toisen organisaation oman instanssin UUID:tä eli tunnusta. Seuraavaksi Jyväskylän yliopiston instanssissa lisättiin synkronointikäyttäjä ja se lisättiin toisen organisaation paikallisorganisaatioon. Lopuksi toinen organisaatio lisäsi synkronointiserverin omalla instanssillaan käyttäen äskettäin lisätyn synkronointikäyttäjän autentikointiavainta. Lopuksi testattiin yhteyden toimivuutta, joka toimi, kuten alla olevasta kuvasta voidaan havaita:

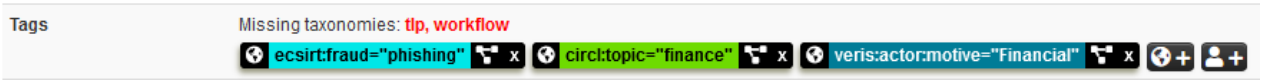


KUVIO 13 Yhteyden testaaminen

Synkronointiserverin lisäämisessä voidaan määritellä muutamia olennaisia asetuksia, kuten veto (engl. Pull) ja työntö (engl. Push). Vedolla voidaan käyttää synkronointikäyttäjää hakemaan toisesta instanssista kaikki mahdollinen data, joka voidaan jakeluasetusten mukaan hakea. Veto toimii vain silloin, jos se on sallittu ja vain jos käyttäjä tekee sen itse. Työnnöllä puolestaan voidaan lähettää julkaistu tapahtuma toiseen instanssiin, toki taas jakeluasetuksien mukaisesti.

Työntö toimii puolestaan automaattisesti, eli joka kerta, kun julkaistaan tapahtuma, se synkronoidaan muiden instanssien kanssa välittömästi. Yhteysongelmat sekä kuolleet työläiset voivat kuitenkin estää työntöä tapahtumasta. Työläisillä tarkoitetaan taustalla tapahtuvia asioita, ja työläiset hoitavat esimerkiksi sähköpostien lähetyksiä, tapahtumien julkaisuja ja MISP:n päivittämistä.

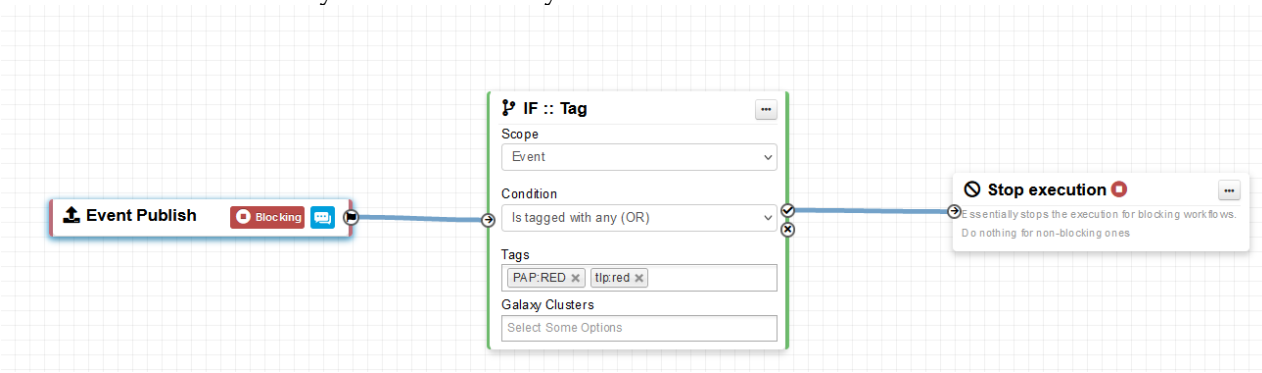
Asetuksista jokaiseen tapahtumaan voidaan määritellä pakolliset luokittelut eli tunnisteet, jotka on merkittävä tapahtumaan, ennen kuin sen voi julkaista. Esimerkiksi asettamalla pakolliseksi liikennevaloprotokollatunnisteiden (TLP) käytön sekä tunnisteet tiedon alkuperästä sekä tiedon luotettavuudesta, voidaan välttää sellaisten tapahtumien vahinkojulkaisut, joissa ei ole tarpeeksi tietoa tai tunnisteita. Alla olevasta kuvasta voidaan nähdä miten MISP ilmoittaa puuttuvista tunnisteista tapahtuman sivulla:



KUVIO 14 Puuttuvat tunnisteet

Huolimatta tunnisteiden käytöstä, korkeakoulujen on huomioitava, että jos synkronointiserveri ja synkronointikäyttäjä on lisätty instanssien välille, myös julkaisemattomat tapahtumat näkyvät toiselle organisaatiolle, jos tietää mistä etsiä, ellei näkyvyysasetusta ole asetettu arvoon ”vain meidän organisaatiomme”. Tämän huomiotta jättäminen saattaa jättää tahattomasti näkyviin sellaisia tapahtumia, joita ei ole vielä tarkoitus jakaa muille. Tämä voidaan estää valitsemalla MISP:n yleisistä asetuksista oletusjakoasetukseksi arvo ”vain meidän organisaatiomme”.

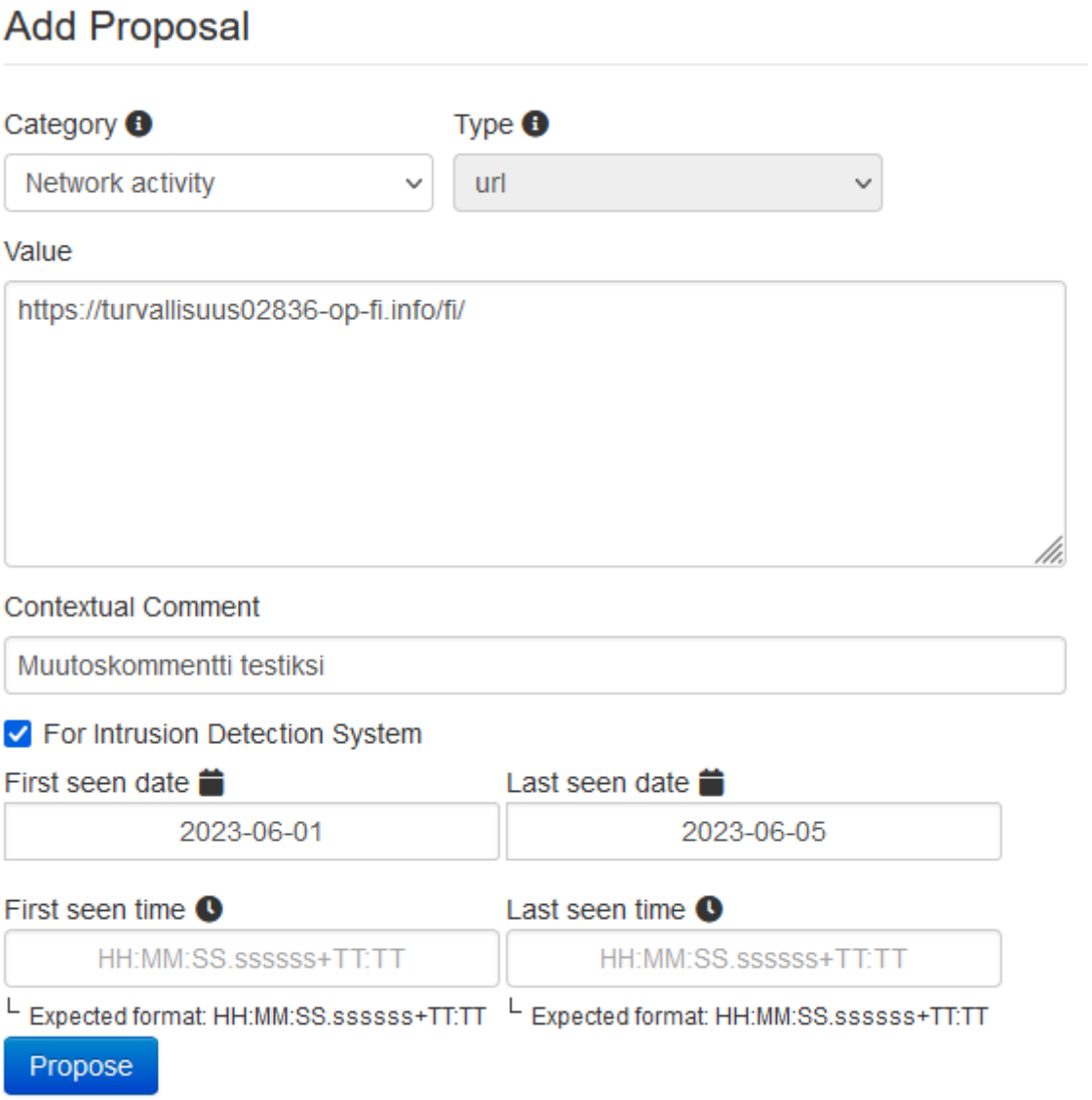
MISP:n on myös hiljattain tullut työnvirtaus (engl. Workflow) ominaisuus, jonka avulla voidaan luoda sääntöjä, jotka tarkistetaan ennen jotakin toimintoa. Esimerkiksi tapahtuman julkaisemisen yhteyteen voitaan luoda sellainen ehto, että jos tapahtuma sisältää tietyn tunnisteen niin tapahtumaa ei julkaista. Alla olevasta kuvasta voi nähdä yksinkertaisen työnvirtauksen:



KUVIO 15 Työnvirtaus

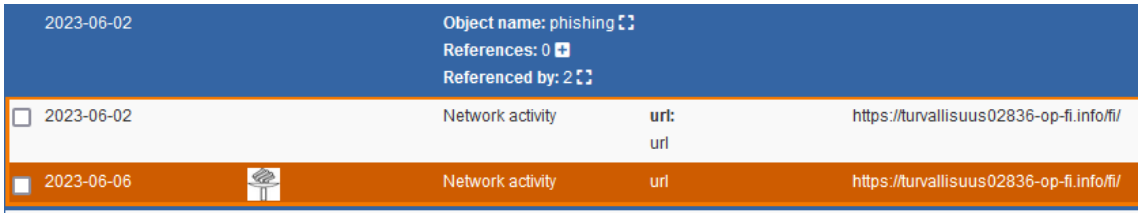
Jokaisen tapahtuman julkaisemisen yhteydessä yllä kuvattu työnvirta aktivoituu, ja se tarkistaa löytyykö tapahtumasta PAP:RED tai TLP:RED tunnisteita. Jos tapahtumasta löytyy sellainen tunniste, työnvirtaus pysäyttää tapahtuman julkaisemisen.

Korkeakoulut voivat ehdottaa toisilleen muutoksia tapahtumiin ehdotuksien kautta, joista olen maininnut luvussa kolme. Muutoksia voi ehdottaa jokaiseen attribuuttiin. Alla olevasta kuvasta voi näkyy ehdotuseditori, jossa käyttäjä voi ehdottaa nykyisen attribuutin tilalle jotain muuta:



KUVIO 16 Muutosehdotus

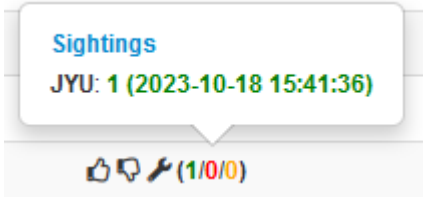
Ehdotuksien avulla muut käyttäjät voivat esimerkiksi huomauttaa potentiaalisista virheistä, jotka esiintyvät toisen organisaation julkaisemassa tapahtumassa. Kun tarvittavat ehdotukset on tehty, käyttäjä tallentaa muutosehdotuksen, ja se menee tapahtuman alkuperäiselle julkaisijalle, joka voi joko hyväksyä tai hylätä muutosehdotuksen. Muutosehdotus näkyy tapahtumassa eri värisenä, jonka lisäksi siinä näkyy ehdottajaorganisaation tiedot, kuten alla olevasta kuvasta voi havaita:



KUVIO 17 Muutosehdotus tapahtumassa

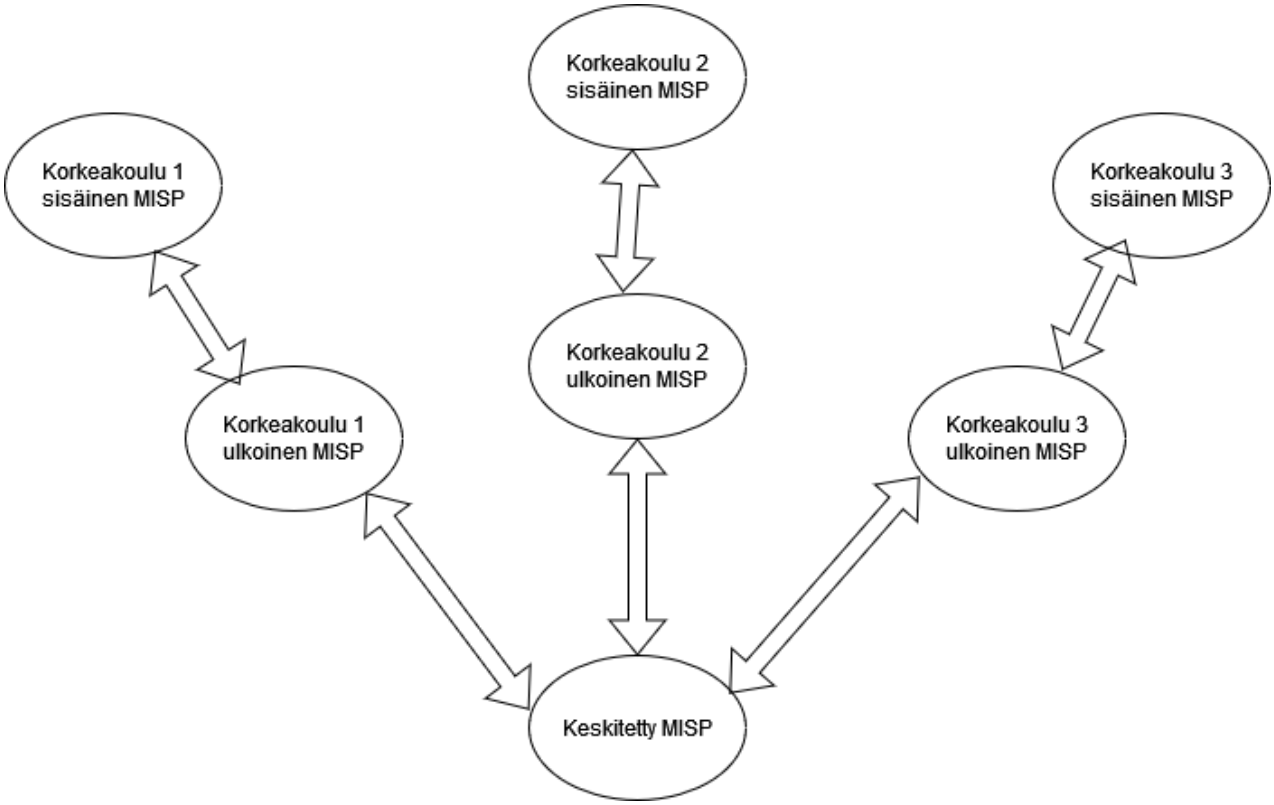
Muutoksia voi ehdottaa kategoriaan, arvoon, onko arvo sopiva vietäväksi tunkeilijanhavaitsemisjärjestelmään sekä milloin attribuutti on havaittu. Tämän ominaisuuden avulla korkeakoulut voivat kätevästi ehdottaa virheiden korjaamista tai attribuuttien muokkaamista selkeämmäksi sekä informatiivisemmaksi.

Muutoksien lisäksi käyttäjät voivat arvioida jokaista attribuuttia peukuttamalla. Tätä kutsutaan attribuutin havaitsemiseksi (engl. Sightings). Peukutuksen avulla käyttäjä voi joko todeta attribuutin todelliseksi eli havaituksi tai vääräksi positiiviseksi. Peukku ylös tarkoittaa, että toinen organisaatio on havainnut kyseisen attribuutin myös omassa ympäristössään, ja peukku alas tarkoittaa väärää positiivista. Havaintojen yhteyteen voi kirjata havainnon lähteen sekä tunnisteita. Alla oleva kuva näyttää yhden havainnon:



KUVIO 18 Havainto

Miltä sitten koko järjestelmä näyttäisi käytännössä korkeakoulujen välillä? Ensiksi on tietenkin sovittava tietojen jakamisen pelisäännöistä. Korkeakoulujen on sovittava esimerkiksi, miten, kuinka usein ja missä muodossa tietoja jaetaan MISP:ssä. Jokaiselta osallistuvalta korkeakoululta on edustaja, joka huolehtii sekä on vastuussa omasta MISP-alustastaan sekä julkaisemistaan tapahtumista. Yhdellä taholla on tärkeämpi tehtävä kuin muilla; yksi taho on vastuussa keskitetystä MISP:stä. Tällä tarkoitetaan sitä yhtä MISP-alustaa, johon kerätään kaikki julkaistut tapahtumat. Alla oleva kuvio havainnollistaa, miltä tämä näyttäisi käytännössä:



KUVIO 19 Korkeakoulujen MISP-järjestelyn ehdotus

Jokaisella korkeakoululla olisi siis vähintään kaksi MISP instanssia. Niitä voidaan kutsua vaikka sisäiseksi ja ulkoiseksi MISP instanssiksi. Sisäinen instanssi ei ole yhteydessä julkiseen verkkoon, ja sisäisen instanssin tarkoitus olisi esimerkiksi yhdistää korkeakoulun omiin toisiin sisäisiin järjestelmiin integraatioiden kautta, sekä sinne voisi kerätä muutakin tietoa, jonka tarkoitus on pysyä vain sisäisessä tiedossa.

Julkisen instanssin tarkoitus olisi puolestaan valmistella tapahtuman julkaisu. Siellä instanssin käyttäjä tarkistaisi julkaistavan tapahtuman ja lopulta julkaisisi tapahtuman. Edellä mainittu visio ei ole kuitenkaan ainoa vaihtoehto, vaan yliopistot voivat käyttää myös vain yhtä MISP instanssia. Tällöin on kuitenkin huomioitava tapahtumien näkyvyysasetukset, jotta vältytään tahattomilta tietojen jakamisilta.

Keskitetyn MISP:n tarkoitus olisi puolestaan olla julkaistun tiedon keskus, johon jokaisen osallistuvan korkeakoulun MISP-edustajalla olisi pääsy. Keskitetyssä MISP:ssä käyttäjät voisivat kommentoida ja ehdottaa muutoksia toisten tapahtumiin, sekä ilmoittaa esimerkiksi vääristä positiivisista havainnoista. Jokaisen käyttäjän olisi pakko ottaa käyttöön monivaiheinen tunnistautuminen, mikä parantaisi käyttäjien turvallisuutta. Keskitetyssä MISP:ssä olisi siis korkeakoulujen havaitsemien tietoturvapoikkeamien uhkatiedot. Keskitetyn MISP:n ylläpitäjät voivat myös seurata esimerkiksi kyberturvallisuuskeskuksen ja muiden vastaavanlaisten tahojen tiedotuksia, ja lisätä heidän julkaisemiaan uhkatietoja omiksi tapahtumiksi keskitettyyn MISP:n, josta ne synkronoituisivat kaikille mukana oleville korkeakouluille. Näin voidaan vähentää tietojen jakamista

sähköpostien ja viestintäsovelluksien kautta, josta jokaisen korkeakoulun pitäisi kopioida ne omiin järjestelmiinsä. Jokaisessa MISP tapahtumassa on mahdollisuus kommentointiin, mikä mahdollistaa tapahtumasta keskustelun. Kommenttiketju jää tapahtumaan, eikä käyttäjien tarvitse etsiä vastaavaa keskusteluketjuja rullaamalla esimerkiksi viestintäsovelluksen keskustelua ylöspäin. Keskusteluketjujen tarpeellisuus ei kuitenkaan poistuisi, mutta nyt sitä ei välttämättä tarvitse käyttää juuri uhkatietojen jakamiseen.

7 ANALYYSI JA JOHTOPÄÄTÖKSET

Tässä luvussa keskitytään aikaisempien lukujen havaintojen analysointiin ja niistä vedetään johtopäätöksiä.

Huolimatta luvussa kuusi mainitusta järjestelystä, jossa yliopisto on osa laajempaa tietojenjakoverkostoa, yksittäinen korkeakoulu voi myös käyttää MISP:ä ilman, että se olisi osa laajaa uhkatietojen jakamiseen tarkoitettua verkostoa. Kuten luvussa viisi on mainittu, MISP:ä voi käyttää omien uhkatietojen varastona, jonka lisäksi MISP:llä on laajat integraatiomahdollisuudet toisiin järjestelmiin, mikä mahdollistaa tietojen jaon nopeasti ja vaivattomasti. Jakamisverkoston puuttuminenkaan ei ole ongelma, sillä kuten mainitsin luvussa kolme, MISP:ssä on monipuoliset uhkatietosyötteet, ja ottamalla syötteet käyttöönsä voi saada hyvinkin osumia omiin uhkatietoihin.

Tietojen jakamisella on omat hyötynsä ja haittansa. Hyödyiksi voidaan laskea parempi varautuminen erilaisiin kyberhyökkäyksiin, jotka kohdistuvat juuri korkeakouluihin. Jos yksi korkeakoulu on tietynlaisen hyökkäyksen, esimerkiksi taitavan tietojenkalastelukampanjan kohteena, tämän tiedon jakaminen uhkatunnisteineen voi nostaa tietoisuutta ja varautumista muissa korkeakouluissa.

Haittoina puolestaan voi nähdä vaikeudet tietojen jakamisessa, jos tietojen jakaja ei tunnista tiedon arkaluontoisuutta sekä tietojen jakamisen lailliset haasteet. Lisäksi huolimattomuus, tunnisteiden käyttämättömyys ja epätietoisuus siitä, mitä ylipäätään voi jakaa toisille organisaatioille haittaavat tehokasta tietojen jakamista.

Suomessa ei ole yleistä tai virallista ohjeistusta siihen, mitä tietoja ja miten organisaatiot voivat jakaa näitä tietoja keskenään. Tämä lisää myös haluttomuutta aloittaa tietojen jakamista yhteisön kesken. Kyberturvallisuuskeskukselta löytyy lyhyehkö ohje liikennevaloprotokollan käytöstä (Kyberturvallisuuskeskus, 2022), mutta tämä ohje painottuu lähinnä kokouksissa ja tiedotustilaisuuksissa jaettuun tietoon.

Uhkatietojen jakaminen perustuu organisaatioiden väliseen luottamukseen. Jos luottamus puuttuu, myös tietojen jakaminen on puutteellista tai olematonta. Tarvitaankin perusteelliset säännöt, kuinka tietoa jaetaan, ja miten mahdollisissa ongelmatilanteissa menetellään.

On myös muistettava, että MISP on loppujen lopuksi vain työkalu tietojen jakamiseen, eikä se korvaa ihmisen kontribuutiota esimerkiksi uhkatietojen validiteetin tarkistamiseen. Automaatiokaan ei ratkaise kaikkea, sillä organisaatioilla voi olla tietoa sellaisissa sovelluksissa tai tietokannoissa, joihin MISP:n integraatio ei taivu. Lisäksi jotkin sovellukset, kuten ServiceNow, mahdollistavat integraation vain maksua vastaan. Organisaatiot keräävät myös uhkatietoa eri tavoin sekä eri muodossa, ja jos kaikki yhteisön organisaatiot alkaisivat jakamaan tietoa suoraan ilman että jaettuja tietoja suodatettaisiin yhteisesti sovittuun muotoon, tietojen tulkitsemisesta tulisi vaikeaa ja aikaa vievää.

Uhkatietojen analysointi, kerääminen, siirtäminen, suodattaminen ja muut siihen liittyvät asiat vievät työaikaa ja vaativat vähintään yhden siihen orientoituneen henkilön työpanosta. Tämä voi vaatia yliopistoilta yhden lisähenkilön palkkaamisen tai jonkun jo työsuhteessa olevan henkilön työtehtävien lisäämistä. Kaupalliset yritykset käyttävät jopa 4–6 asiantuntijan ryhmää, joka on erikoistunut uhkatietojen analysointiin ja keräämiseen (Kotsias, Ahmad & Scheepers, 2022). Yliopistoilla tuskin on varaa kokonaisen ryhmän muodostamiseen, joten alustan ylläpitämisen ja uhkatietojen jakamisen vastuu jäisi jollekin työntekijöistä, mitä luultavammin tietoturvan parissa työskentelevälle. Lisäksi työntekijällä pitäisi olla motivaatiota edellä mainittujen tehtävien tekemiseen. Huomattavaa on, että kun tämän tutkielman kirjoittamisen alussa kysyttiin muiden korkeakoulujen kiinnostusta tai mahdollisuutta osallistua yhteisen uhkatietoalustan testaamiseen, yliopistojen tietoturvasta vastaavilta joko ei tullut vastausta tai vedottiin kiireeseen, minkä takia mukaan ei osallistuttu.

Kotsias, Ahmad ja Scheepers (2022) tunnistivat seitsemän eri avaintekijää, jotka ovat keskeisiä uhkatiedon jakamisessa:

- Tieto on vakaata ja johdonmukaista
- Tieto on keskitettyä ja yhtenäistä
- Tieto on oikea-aikaista ja kohdistettua
- Tieto on analysoitua ja siihen pääsee käsiksi

Jotta yllä olevat neljä kokonaisuutta toteutuisivat, tarvitaan seuraavat kolme tekijää:

- Ihmiset
- Prosessit
- Teknologia

Ihmiset, tai uhkatiedon käsittelijät varmistavat, että tieto on analysoitua ja sitä pääsee käyttämään. Prosessit varmistavat sen, että tieto on vakaata ja johdonmukaista. Teknologia varmistaa sen, että tieto keskitettyä ja yhtenäistä.

Jos ylempiä avaintekijöitä sovelletaan korkeakouluympäristöön, niin jokaisesta korkeakoulusta tarvitaan edustaja, joka vastaa omasta ympäristöstä, eli huolehtii teknologian käyttöönotosta ja osallistuu prosessien kehittämiseen. Prosessien kehittäminen tietojen jakamista varten on tärkeää, jotta korkeakoulujen kesken kehittyy yhtenäinen ja johdonmukainen tietojenjakoprosessi. Lisäksi

tähän voisi kuulua ohjeistus siitä, mitä tietoa jaetaan ja mitä ei. Teknologia puolestaan olisi uhkatietojen jakoalusta, kuten MISP, jonne uhkatieto kerättäisiin.

Alustaan tallennettavien tietojen sensitiivisyys voi aiheuttaa myös päänvaivaa. MISP:n käytössä on muistettava, että jos tapahtuman näkyvyysasetus on jotain muuta kuin ”vain meidän organisaatiollemme”, niin tapahtuma näkyy kaikille organisaatioille, jotka ovat samassa yhteisössä huolimatta siitä, onko tapahtuma julkaistu vai ei. Näitä tapahtumia ei näe suoraan tapahtumalistauksessa, mutta jos käyttäjä osaa suunnistaa MISP-alustalla synkronointiserverin asetuksiin, niin käyttäjä pääsee näkemään kyseisen serverin tapahtumat. Tätä ominaisuutta ei ole nostettu erityisesti esiin MISP:n dokumentaatiossa, jonka lisäksi tapahtumien näkyvyysasetus MISP:n yleisissä asetuksissa on oletuksena ”meidän yhteisöllemme”. Tämä voi johtaa sellaisten tietojen ja tapahtumien tahattomaan näkymiseen muille, joita organisaatio ei ole suunnitellut jakavansa. Toisaalta edeltävässä luvussa mainitsemani malli keskitetystä sekä sen lisäksi yliopistojen sisäisestä ja ulkoisesta MISP:stä vähentäisivät tahattomien julkaisujen riskiä.

Korkeakoulujen onkin tarpeen suunnitella ja sopia yksityiskohtaisesti niistä tiedoista, joita sovellukseen voi syöttää muiden näkyville. Lisäksi automaation kanssa on oltava tarkkana, jos muista palveluista tulee automaattisesti tietoja MISP:n. Jos automaattisesti MISP:n tulevat tiedot julkaistaan suoraan tapahtumana, osa tiedoista voi olla luokiteltu väärin tai niiden näkyvyysasetukset voivat olla väärin.

Aikanaan tulisi myös arvioida sitä, onko alustan käytöstä ollut konkreettista hyötyä. Vähensikö alustan käyttö uhkatietojen jakamiseen käytettävää aikaa, oliko jaetuista uhkatiedoista hyötyä ja saatiinko niillä jotain konkreettista aikaan, esimerkiksi saatiinko estettyä kalastelukampanja tai muu vastaava kyberhyökkäys.

8 YHTEENVETO

Uhkatietojen hyödyntämisellä voidaan parantaa korkeakoulujen varautumista kyberhyökkäyksiä vastaan. Tässä pro gradu -tutkielmassa pyrittiin selvittämään miten Suomen korkeakoulut voivat hyödyntää uhkatietoja jakamalla sitä uhkatiedon jakamiseen tarkoitetun sovelluksen eli MISP:n kautta. Tutkielma toteutettiin käyttäen kahta eri tutkimusmenetelmää, kirjallisuuskatsausta ja konstruktiivista tutkimusmenetelmää.

Tutkielman lähteiksi valittiin soveltuvaa kirjallisuutta, kuten tieteellisiä artikkeleita, kokoomateoksien artikkeleita, dokumentaatiota ja verkkosivuja. Tieteelliset artikkelit ja kokoomateoksien artikkelit otettiin mukaan, jos se oli saanut Julkaisufoorumilla vähintään tason 1. Dokumentaatioita ja verkkosivuja otettiin lähteiksi soveltuvilta osin.

Tutkielmassa haettiin vastauksia seuraaviin tutkimuskysymyksiin:

- Miten yksittäisessä korkeakoulussa voitaisiin käyttää hyväksi MISP-alustaa?
- Miten Suomen korkeakoulut voisivat käyttää hyväksi MISP-alustaa uhkatietojen jakamiseen?

Tutkielma jaettiin kahdeksaan eri lukuun: johdantoon, kuuteen sisältölukuun ja yhteenvetoon. Johdannossa lukijalle avattiin tutkielman taustaa ja tarpeellisuutta, tutkimuskysymykset, tutkimusmenetelmät, lähdekirjallisuuden keräämisen menetelmät, tutkimuksen tavoite ja tutkielman rakenne.

Toisessa luvussa keskityttiin yksinomaan uhkatietoon ja sen mahdollisuuksiin ja rajoitteisiin. Luvussa käytiin muun muassa läpi mistä kaikesta uhkatieto voi koostua, kuten haavoittuvuustiedoista ja IP-osoitteista, uhkatietojen kategorioita, uhkatiedon elinkaari sekä uhkatiedon jakamisen hyödyt ja haitat.

Kolmannessa luvussa käytiin läpi uhkatietojen jakoalusta MISP:n toimintaa ja käyttöä. Luvussa selitettiin auki tärkeimmät ominaisuudet, kuten tapahtuma ja siihen liittyvät ominaisuudet, kuten attribuutit, galaksit ja tunnisteet.

Neljännessä luvussa perehdyttiin siihen, mitä on kirjallisuuskatsaus ja konstruktiivinen tutkimusote. Konstruktiivisesta tutkimusotteesta käytiin läpi kuvioiden avulla esimerkiksi tutkimusotteen vaiheet ja mistä se koostuu.

Viidennessä luvussa aloitettiin uhkatietojen jakoalustan käyttö ja testaus. Luvussa selvitettiin MISP:n käytettävyyttä uhkatietojen tallentamiseen sekä MISP:n integraatiomahdollisuuksia toisiin järjestelmiin.

Kuudennessa luvussa tarkasteltiin MISP:n käyttöä ja uhkatiedon jakamista korkeakoulujen välillä. Luvussa käytiin läpi instanssien synkronointi kahden toimijan välillä sekä tietojen jakamista käytännössä.

Seitsemännessä luvussa pohdittiin lukujen viisi ja kuusi havaintoja, sekä vedettiin johtopäätöksiä. Lopputuloksena oli se, että uhkatietojen jakamisyhteisön muodostaminen Suomen korkeakoulujen kesken tulisi olemaan suhteellisen iso operaatio, joka vaatii paljon aikaa ja vaivaa. Onnistuessaan se kuitenkin voisi parantaa korkeakoulujen resilienssiä kyberhyökkäyksiä vastaan.

Tämän pro gradu -tutkielman tavoitteena on ollut myös herättää mielenkiinto tietojen jakamisen mahdollisuuksiin ei pelkästään Suomen korkeakoulujen kesken, mutta myös muiden toimijoiden, esimerkiksi kuntien kesken Suomessa. Uhkatietojen jakoalusta MISP:ä käyttää uhkatietojen jakamiseen esimerkiksi NATO sekä Tanskan eCrimeLabs yhteistö, joka kannustaa Tanskan organisaatioita yhteistyöhön uhkatietojen jakamiseksi (MISP, 2023).

Tässä pro gradu -tutkielmassa on ollut omat rajoitteensa. Tutkielman laajuus oli todella rajoitettu, ja tietojen jakamista päästiin kokeilemaan vain yhden muun organisaation kanssa. Lisäksi kaikkia MISP:n ominaisuuksia ei voitu testata perusteellisesti osallistujaorganisaatioiden vähäisyyden vuoksi. Näitä ominaisuuksia olivat muun muassa havaintojen ja väärien positiivisten syvällisempi kirjaaminen ja tutkiminen, uutisten käyttö ja keskustelujen käyttö. Näitä ei voitu testata mielekkäästi, sillä mukana alustan kokeilussa oli tutkielman kirjoituksen aikana vain yksi organisaatio.

Tulevaisuudessa olisi hyvä tutkia lisää uhkatiedon jakamisen työkaluja. Tällä hetkellä ilmaisia, avoimen lähdekoodin työkaluja on vain kaksi, MISP ja OpenCTI. Lisäksi uhkatietojen jakamisen laillisuuteen liittyviä ongelmia olisi myös hyvä tutkia lisää. Myös uhkatietojen jakamiseen tarkoitettujen alustojen tehokkuutta ja vaikutusta uhkien torjumiseen ja selvittämiseen olisi hyvä tutkia lisää.

LÄHTEET

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, *86*, 402-418.

Al-Ibrahim, O., Mohaisen, A., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Beyond free riding: quality of indicators for assessing participation in information sharing for threat intelligence. *arXiv preprint arXiv:1702.00552*.

Albakri, A., Boiten, E., & Lemos, R. D. (2019). Sharing cyber threat intelligence under the general data protection regulation. Teoksessa *Annual Privacy Forum* (s. 28-41). Springer, Cham.

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. Teoksessa *Proceedings of the 2nd ACM workshop on information sharing and collaborative security* (s. 43-49).

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258.

Chismon, D., & Ruks, M. (2015). Threat intelligence: Collecting, analysing, evaluating. *MWR InfoSecurity Ltd*, *3*(2), 36-42.

Christodorescu, M., Jha, S., Seshia, S. A., Song, D., & Bryant, R. E. (2005). Semantics-aware malware detection. Teoksessa *2005 IEEE symposium on security and privacy (S&P'05)* (s. 32-46). IEEE.

Cobb, M. (2021, kesäkuu). threat intelligence (cyber threat intelligence). Haettu 22.11.2022 osoitteesta https://www.techtarget.com/whatis/definition/threat-intelligence-cyber-threat-intelligence

Cosive. (2022, 4. lokakuuta). What is MISP? The Ultimate Introduction. Haettu 18.10.2022 osoitteesta https://www.cosive.com/blog/2022/10/4/what-is-misp-the-ultimate-introduction

Crnkovic, G. D. (2010). Constructive research and info-computational knowledge generation. Teoksessa *Model-Based Reasoning in Science and Technology* (s. 359-380). Springer, Berlin, Heidelberg.

Dandurand, L., & Serrano, O. S. (2013). Towards improved cyber security information sharing. Teoksessa *2013 5th International Conference on Cyber Conflict (CYCON 2013)* (s. 1-16). IEEE.

de Fuentes, J. M., González-Manzano, L., Tapiador, J., & Peris-Lopez, P. (2017). PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing. *Computers & Security*, *69*, 127-141.

Denney, A. S., & Tewksbury, R. (2013). How to write a literature review. *Journal of criminal justice education*, *24*(2), 218-234.

Doerr, C. (2018). Cyber Threat Intelligences Standards–A High Level Overview. *TU Delft CTI Labs*.

Dog, S. E., Tweed, A., Rouse, L., Chu, B., Qi, D., Hu, Y., ... & Al-Shaer, E. (2016). Strategic cyber threat intelligence sharing: a case study of ids logs. Teoksessa *2016 25th International Conference on Computer Communication and Networks (ICCCN)* (s. 1-6). IEEE.

Feledi, D., Fenz, S., & Lechner, L. (2013). Toward web-based information security knowledge sharing. *Information security technical report*, *17*(4), 199-209.

First. (2022, elokuu).TRAFFIC LIGHT PROTOCOL (TLP). FIRST Standards Definitions and Usage Guidance — Version 2.0. Haettu 22.11.2022 osoitteesta https://www.first.org/tlp/

Fotiadou, K., Velivassaki, T. H., Voulkidis, A., Railis, K., Trakadas, P., & Zahariadis, T. (2020). Incidents information sharing platform for distributed attack detection. *IEEE Open Journal of the Communications Society*, *1*, 593-605.

Gschwandtner, M., Demetz, L., Gander, M., & Maier, R. (2018). Integrating threat intelligence to enhance an organization's information security management. Teoksessa *Proceedings of the 13th International Conference on Availability, Reliability and Security* (s. 1-8).

Iklody, A., Wagener, G., Dulaunoy, A., Mokaddem, S., & Wagner, C. (2018). Decaying indicators of compromise. *arXiv preprint arXiv:1803.11052*.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. *NIST special publication*, *800*(150).

Johnson, T. A. (2015). Cybersecurity Threat Landscape and Future Trends. Teoksessa Johnson, T. A. (toim.), *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare.* (s. 287–325). CRC Press.

Jones, O., Gold, J., & Claxton, J. (2022). An exposition of the constructive research approach: a tactical treatise for addressing methodological and practical issues in organisational research. *International Journal of Organizational Analysis*.

Jönsson, S., & Lukka, K. (2006). There and back again: doing interventionist research in management accounting. *Handbooks of management accounting research*, *1*, 373-397.

Kampanakis, P. (2014). Security automation and threat information-sharing options. *IEEE Security & Privacy*, *12*(5), 42-51.

Kasanen, E., Lukka, K., & Siitonen, A. (1993). The constructive approach in management accounting research. *Journal of management accounting research*, *5*(1), 243-264.

Knopf, J. W. (2006). Doing a literature review. *PS: Political Science & Politics*, *39*(1), 127-132.

Kokkonen, T., Hautamäki, J., Siltanen, J., & Hämäläinen, T. (2016). Model for sharing the information of cyber security situation awareness between organizations. Teoksessa *2016 23rd International Conference on Telecommunications (ICT)* (s. 1-5). IEEE.

Kotsias, J., Ahmad, A., & Scheepers, R. (2022). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, 1-17.

Kyberturvallisuuskeskus. (2022, 19. syyskuuta). Yhteistyöryhmien tiedonvaihtokäytäntöjä. Haettu 5.6.2023 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/yhteistyoryhmien-tiedonvaihtokaytantoja

Labro, E., & Tuomela, T. S. (2003). On bringing more action into management accounting research: process considerations based on two constructive case studies. *European accounting review*, *12*(3), 409-442.

Li, V. G., Dunn, M., Pearce, P., McCoy, D., Voelker, G. M., & Savage, S. (2019). Reading the tea leaves: A comparative analysis of threat intelligence. Teoksessa *28th USENIX security symposium (USENIX Security 19)* (s. 851-867).

Lukka, K. (2001). Kari Lukka: Konstruktiivinen tutkimusote. Haettu 21.11.2022 osoitteesta https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M., & Percia David, D. (2019). To share or not to share: A behavioral perspective on human participation in security information sharing. *Journal of Cybersecurity*, *5*(1), tyz006.

MISP project. (2023). Haettu 25.05.2023 osoitteesta https://www.misp-project.org/

Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Rethinking information sharing for threat intelligence. Teoksessa *Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies* (s. 1-7).

Mokaddem, S., Wagener, G., Dulaunoy, A., & Iklody, A. (2019). Taxonomy driven indicator scoring in MISP threat intelligence platforms. *arXiv preprint arXiv:1902.03914*.

Murdoch, S., & Leaver, N. (2015). Anonymity vs. trust in cyber-security collaboration. Teoksessa *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security* (s. 27-29).

Navarro, J., Deruyver, A., & Parrend, P. (2018). A systematic survey on multi-step attack detection. *Computers & Security*, *76*, 214-249.

Oosthoek, K., & Doerr, C. (2021). Cyber threat intelligence: A product without a process?. *International Journal of Intelligence and CounterIntelligence*, *34*(2), 300-315.

Pahi, T., & Skopik, F. (2017). A systematic study and comparison of attack scenarios and involved threat actors. Teoksessa Skopik, F. (toim.). *Collaborative cyber threat intelligence: detecting and responding to advanced cyber attacks at the national level*. CRC Press.

Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know?. *International Business Review*, *29*(4), 101717.

Pawlinski, P., Jaroszewski, P., Kijewski, P., Siewierski, L., Jacewicz, P., Zielony, P., & Zuber, R. (2014). Actionable information for security incident response. *European Union Agency for Network and Information Security, Heraklion, Greece*.

Piirainen, K. A., & Gonzalez, R. A. (2014). Constructive synergy in design science research: a comparative analysis of design science research and the constructive research approach. *Liiketaloudellinen Aikakauskirja*, *3*(4), 206-234.

Rautiainen, A., Sippola, K., & Mättö, T. (2017). Perspectives on relevance: The relevance test in the constructive research approach. *Management Accounting Research*, *34*, 19-29.

Riesco, R., Larriva-Novo, X., & Villagrá, V. A. (2020). Cybersecurity threat intelligence knowledge exchange based on blockchain. *Telecommunication Systems*, *73*(2), 259-288.

Rowe, F. (2014). What literature review is not: diversity, boundaries and recommendations. *European Journal of Information Systems*, *23*(3), 241-255.

Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. Teoksessa *Leimeister, J.M.; Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, S*. 837-851.

Shackleford, D. (2015). Who's using cyberthreat intelligence and how. *SANS Institute*.

Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability'that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security*, *92*, 101761.

Sigholm, J., & Bang, M. (2013). Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats. Teoksessa *2013 European Intelligence and Security Informatics Conference* (s. 166-171). IEEE.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154-176.

Tao, Y., Zhang, Y. X., Ma, S. Y., Fan, K., Li, M. Y., Guo, F. M., & Xu, Z. (2017). Combining the big data analysis and the threat intelligence technologies for the classified protection model. *Cluster Computing*, *20*(2), 1035-1046.

Thomas, D., & Loader, B. D. (2000). Introduction. Teoksessa Thomas, D., & Loader, B. D. (toim.), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. (s. 1–14)*. Routledge.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & security*, *72*, 212-233.

Traficom. (2022, 24. elokuuta). Kansainvälinen tiedonvaihtoprotokolla (TLP) päivittyi versioon 2.0. Haettu 22.11.2022 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kansainvalinen-tiedonvaihtoprotokolla-tlp-paivittyi-versioon-20?toggle=M%C3%A4%C3%A4ritykset&toggle=Liikennevalot

van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., ... & Spruit, M. (2021). A shared cyber threat intelligence solution for smes. *Electronics*, *10*(23), 2913.

Vázquez, D. F., Acosta, O. P., Spirito, C., Brown, S., & Reid, E. (2012). Conceptual framework for cyber defense information sharing within trust relationships. Teoksessa *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (s. 1-17). IEEE.

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, *87*, 101589.

Woods, B., Perl, S. J., & Lindauer, B. (2015). Data mining for efficient collaborative information discovery. Teoksessa *Proceedings of the 2Nd ACM Workshop on Information Sharing and Collaborative Security* (s. 3-12).

Yeboah-Ofori, A., Islam, S., & Yeboah-Boateng, E. (2019). Cyber threat intelligence for improving cyber supply chain security. Teoksessa *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)* (s. 28-33). IEEE.

Zibak, A., & Simpson, A. (2019). Cyber threat information sharing: Perceived benefits and barriers. Teoksessa *Proceedings of the 14th international conference on availability, reliability and security* (s. 1-9).