Haaga-Helia
ammattikorkeakoulu Oy

Kyberturva-analyytikon työtehtävät

Tommi Timonen

Opinnäytetyö
Tietojenkäsittely koulutusohjelma
2020

Haaga-Helia ammattikorkeakoulu Oy

Tiivistelmä

02.12.2020

Tekijä(t)
Tommi Timonen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Kyberturva-analyytikon työtehtävät

Sivu- ja liite-sivumäärä
51 + 0

Opinnäytetyön otsikko englanniksi
Cyber Security Analyst's Work Tasks

Kyberturva on alana nopeasti kehittyvä ja monimuotoinen. Se vaatii jatkuvaa tutustumista erilaisiin uhkiin, haavoittuvuuksiin sekä erilaisiin hyökkäysmetodeihin. Uusia haavoittuvuuksia ja hyökkäysmetodeja erilaisiin järjestelmiin löytyy jatkuvasti ja näiden uhkien tunnistaminen ympäristöissä on ajoittain haastavaa. Uusiin uhkiin tutustumisen lisäksi uhkien torjunta- ja havainnointijärjestelmät ja tekniikat kehittyvät jatkuvasti, joten kyseisiin järjestelmiin tutustuminen on varsin suotavaa, jos haluaa pitää ympäristön turvattuna.

Tässä opinnäytetyössä esittelen kyberturva-analyytikon päivittäistä toimintaa päiväkirjatyyppisellä seurannalla ja lisäksi analysoin viikolla kohdattuja tehtäviä tai ongelmia syvemmin. Tarkoituksena on tuottaa opinnäytetyö, jonka avulla kuka tahansa voi nähdä minkälaista on työskennellä kyberturva-analyytikkona, sekä minkälaisia tehtäviä ja ongelmia työnkuvaan liittyy.

Opinnäytetyössä tutkittavat ympäristöt ovat sekä tekijän oman työpaikan ympäristö että työpaikan asiakkaiden ympäristöt. Kohdatuissa ongelmissa ei välttämättä mainita asiakkaita ollenkaan, koska ongelmat käsitellään prioriteettien mukaan tapauskohtaisesti, riippumatta siitä onko kyseessä työpaikan sisäinen tapaus vai asiakuudessa havaittu tapaus.

Asiasanat
Kyberturvallisuus, tietotekniikka, uhat, kehitys

Sisällys

1 Johdanto

Opinnäytetyön päiväkirjan pito suoritetaan aikavälillä 07.09.2020 - 13.11.2020. Opinnäytetyössä seurataan päivittäistä työelämääni ja käydään läpi kyberturva-analyytikon työssä kohdattuja ongelmia ja tehtäviä.

Kyberturva-analyytikon tehtävissä vaaditaan tietämystä useista eri tietotekniikan osa-alueista kuten palvelimista, käyttöjärjestelmistä, verkkolaitteista, verkkoprotokollista, kryptografiasta ja haittaohjelmista. Lisäksi analyytikon tulee ymmärtää tietoturvapoikkeamien hallintaa. Tietoturvapoikkeamien hallinnasta kerrotaan kattavasti NISTin tuottamassa teoksessa Computer Security Incident Handling Guide (2012). NISTin teos on erittäin kattava ja siinä käydään läpi tietoturvapoikkeaminen hallinnan eri vaiheita kuten ennakointia, valmistautumista, havainnointia, tutkimista, poikkeaman hallintaa, poikkeamasta palautumista sekä poikkeamasta palautumisen jälkeisiä toimenpiteitä. Kokonaisuudessaan teos antaa hyvän kuvan siitä, miten toimia kyberturva-analyytikkona ennen poikkeamaa, poikkeaman aikana ja poikkeaman jälkeen. Toinen kyberturva-analyytikolta vaadittava osaaminen on kyberturvaan liittyvän sanaston osaaminen, sillä kyberturvassa on paljon termejä ja sanoja, jotka eivät ilman selitystä kerro asiasta tietämättömälle ihmiselle mitään. Sanastokeskus TSK ry:n tuottama teos Kyberturvallisuuden sanasto (2018) on kattava kokoelma kyberturvassa käytettävästä sanastosta ja selittää hyvin kunkin sanan tarkoituksen niin, että kuka tahansa pystyy ymmärtämään sanan tarkoituksen. Vaikka analyytikon tulee tuntea tietotekniikan osa-alueita laajasti, niin kaikkia osa-alueita ei kuitenkaan tarvitse osata perusteellisesti. Analyytikko voi erikoistua tiettyihin osa-alueisiin ja osata perusteet useista muista osa-alueista. Koska kyberuhkien hyökkäyspinta-ala on käytännössä loputon ja uusia tapoja hyökätä keksitään jatkuvasti, niin yksi analyytikon tarpeellisimmista taidoista on tiedon etsiminen ja kyky uuden tiedon nopeaan sisäistämiseen ja soveltamiseen.

Työskentelen Fujitsu Finland Oy:lle. Se on osa Fujitsun globaalia organisaatiota, mutta toimii samalla itsenäisenä organisaationaan. Vallitsevasta poikkeustilasta johtuen työskentelen kotoa käsin etätöissä. Työskentely tapahtuu VPN-yhteydellä, jonka kautta pääsen yrityksen sisäisiin järjestelmiin. Lisäksi käytössäni on useita virtuaalisia ympäristöjä erilaisiin käyttötarkoituksiin, kuten haittaohjelmien tutkimiseen, uusien järjestelmien kehitykseen sekä haitallisten tiedostojen tutkimiseen ja analysointiin.

1.1 Keskeiset ammattikäsitteet

Bash

Komentotulkki, jolla voidaan ohjata käyttöjärjestelmää. Voidaan käyttää myös ohjelmointikielenä.

Command and control / C&C / C2

Palvelin, jonka kautta hyökkääjä antaa käskyjä haittaohjelmalleen.

CMDB

Configuration management database. Tietokanta, jossa säilytetään tietoa organisaation laitteista ja ohjelmistoista.

CTI

Cyber threat intelligence. Tietokokoelma uhkista ja uhkien aiheuttajista.

Hash

Tiedosta luotu tiivistelmä, jolla voidaan tarkistaa tiedon eheys.

IOC

Indicator of compromise. Mikä tahansa tunniste, jolla voidaan havaita uhkia ja haitallisiatiedostoja ympäristöissä.

IPv4 ja IPv6

Verkkolaitteiden yksilöimiseen käytettävä osoite.

Jira

Projektien hallintaan ja etenemisen seuraamiseen käytettävä ohjelmisto.

MISP

Malware Information Sharing Platform. Uhkiin liittyvien tietojen keräämiseen ja hallintaan käytettävä järjestelmä.

Python

Ohjelmointikieli.

Regex

Regular expression. Kaava, jolla voidaan havaita kaavaa vastaavia toistuvuuksia tekstistä.

Service desk

Tiimi, joka toimii teknisenä tukena käyttäjille, sekä asiantuntijatiimien ja käyttäjien välisenä kontaktina.

SIEM

Security information and event management. Järjestelmä, joka kerää keskitetysti tapahtumia ja tietoja erilaisilta laitteilta. Käytetään kerätyn tiedon tarkasteluun.

Sinkhole

Osoite, johon voidaan ohjata yhteyksiä, joiden ei haluta pääsevän alkuperäiseen kohteeseensa.

SLA

Service-level agreement. Asiakkaan kanssa tehty sopimus, jossa määritellään palvelun vaatimustasot, kuten vasteajat.

SOAR

Security orchestration automation and response. Kokoelma ratkaisuja, joilla kerätään tietoa, sekä automatisoidaan yksinkertaisia tai pieniä tehtäviä.

SOC

Security operations center. Tiimi, joka hallitsee ja tutkii turvallisuuteen liittyviä hallinnollisia ja teknisiä tehtäviä.

SPOC

Single point of contact. Toimintamalli, jossa yksittäinen osasto tai tiimi toimii kaiken tiedon keskitettynä vastaanottajana ja koordinoijana.

Teams

Pikaviestintäohjelmisto.

Threat intelligence

Uhkiin liittyvä tieto ja tiedon kerääminen, prosessointi ja analysointi.

TLS/SSL

Verkkoliikenteen salaukseen käytettävä protokolla.

Työpyyntö

Työpyyntöjärjestelmässä oleva tunnisteella varustettu objekti, jolle kirjataan työpyyntöön liittyvät tiedot, toimenpiteet ja käytetty aika.

VPN

Virtual private network. Virtuaalinen verkko, jonka kautta voidaan yhdistää laitteita yksityiseen verkkoon salatun yhteyden avulla julkisen verkon yli.

Väsytyshyökkäys

Hyökkäys, jossa yritetään kirjautua järjestelmään väkisin kokeilemalla useita käyttäjätunnuksia ja/tai salasanoja.

2 Lähtötilanteen kuvaus

2.1 Oman nykyisen työn analyysi

Työtehtäviini kuuluu työpyyntöjärjestelmien kautta tulevien tutkintapyyntöjen, ongelmien, havaintojen ja muiden järjestelmien generoimien hälytysten tutkiminen sekä tutkinnan jälkeen työpyynnön lähettäminen eteenpäin toimintaohjeineen. Lisäksi työtehtäviini kuuluu kuukausiraporttien läpikäynti ja esittely asiakkaalle. Työpyyntöjen ja raporttien käsittelyn ohella työhöni kuuluu käytössä olevien järjestelmien kehittäminen ja uusien järjestelmien tutkiminen ja kehittäminen. Esimerkiksi SIEM-järjestelmän hälytysten hienosäätö tai täysin uusien järjestelmien käyttöönotto ja testaaminen. Iso osa analyytikon työtä on myös pysyä perillä ajankohtaisista uhkista ja uusimmista haavoittuvuuksista, joita käytetään aktiivisesti tai joita todennäköisesti tullaan käyttämään lähitulevaisuudessa aktiivisesti.
Konkreettisesti työpyyntöjen käsittely vaihtelee paljon, riippuen mistä työpyynnöissä on kysymys. Suurin osa työpyynnöistä on automaattisesti valvontajärjestelmistä generoituvia hälytyksiä, kuten SIEM-järjestelmän havaitsemia väsytyshyökkäyksiä, joissa joku tai jokin yrittää käyttää väärää salasanaa käyttäjätunnukselle suurissa määrissä tai palomuurilla on havaittu hyökkäys, jossa koitetaan käyttää haavoittuvuutta palvelimelle. Tehtävänäni näissä tapauksissa on tutkia, mitä muita tapahtumia hälytysten ympärillä on, mikä aiheuttaa kyseiset poikkeamat ja selvityksen jälkeen antaa ohjeet, miten toimitaan uhkan estämiseksi, torjumiseksi tai korjaamiseksi.
Joillekin asiakkaille toimitetaan kuukausittain raportti ympäristössä havaituista poikkeamista tai yleinen otanta esimerkiksi palomuurilla liikkuvasta liikenteestä. Näistä raporteista pidetään yleensä palaveri asiakkaiden kanssa. Palaverissa kyberturva-analyytikko, joka on kyseisestä asiakuudesta vastuullinen, käy raportit läpi asiakkaan kanssa ja selittää asiakkaalle mitä mikäkin kohta raportissa tarkoittaa ja mitä raportilla havaittavat poikkeamat kertovat.
Kyberturva-analyytikon työssä tarvitaan laajaa tuntemusta erilaisista järjestelmistä, hyökkäysmetodeista ja verkkoteknologioista. Koska kukaan ei voi tietää kaikesta kaikkea, on välttämätöntä, että analyytikko osaa etsiä ja sisäistää tietoa nopeasti. Näin hän voi suunnitella parhaan mahdollisen tavan toimia kohdatessaan haastavia tilanteita ja ongelmia. Jos tietoa ei löydy verkosta voi nojautua kollegoihin tai kysyä ongelmaan liittyvältä asiantuntijatiimiltä lisätietoja.
Olen toistaiseksi vielä aloitteleva toimija ja tarvitsen kollegoiden apua haastavimmissa, monimutkaisemmissa ja prosesseihin liittyvissä ongelmissa. Yksinkertaisempia ja itselleni tuttuja ongelmia pystyn kuitenkin selvittämään ja ratkomaan itsenäisesti. Pääsin Fujitsulle graduate programmin kautta, jonka tarkoituksena on palkata potentiaalisia, mutta vielä kokemattomampia opiskelijoita tai vastavalmistuneita työntekijöitä ja kouluttaa heitä työn ohessa ammattilaisen tasolle. Graduate program kestää kaksi vuotta ja opinnäytetyön alussa olen suorittanut siitä noin ensimmäisen vuoden.

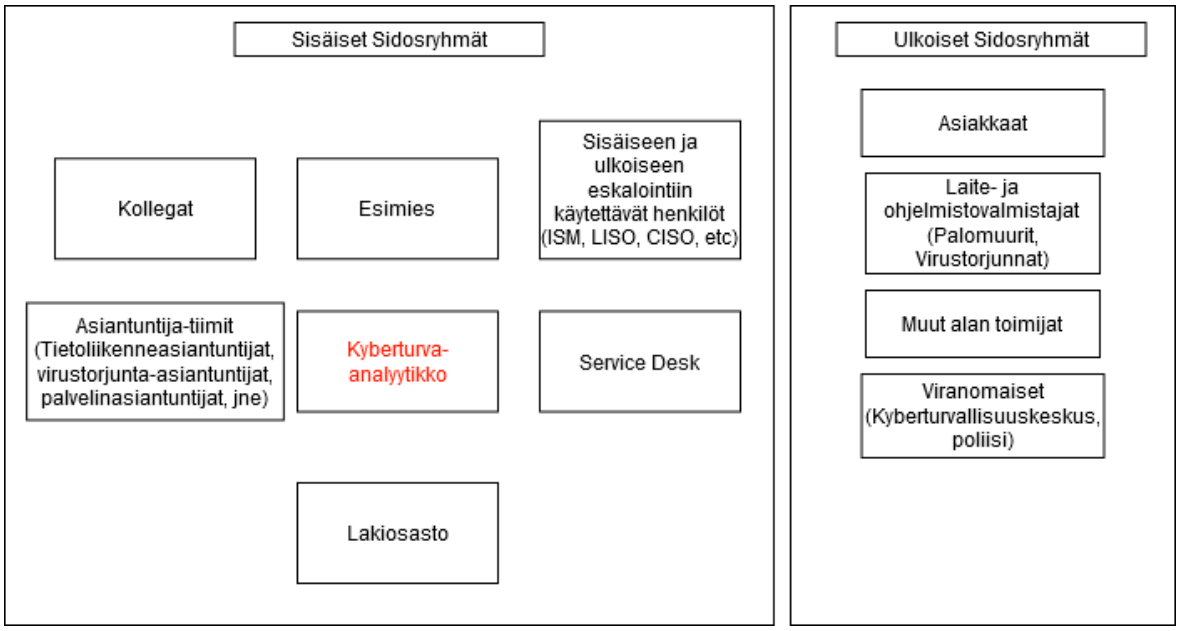
Ammatillinen kehitykseni on vielä alkuvaiheessa ja varaa kehittyä on vielä runsaasti. Olen kuitenkin ehtinyt tutustumaan yleisimpiin uhkiin ja ongelmatilanteisiin, joita kyberturva-analyytikon työssä kohdataan ja oppinut niiden selvitykseen kuuluvia vaiheita sekä luomaan ohjeita tilanteiden hallintaan. Lisäksi olen oppinut käyttämään useita itselleni uusia tietolähteitä, joista voin hakea tietoa uhkiin liittyen ja siten parantaa selvitystyöni tehokkuutta. Vaikka olen oppinut jo paljon työssä ollessani, niin tarvitsen vielä tukea monimutkaisemmissa ongelmanratkaisutilanteissa, joissa tietämykseni järjestelmistä tai prosesseista ei ole riittävä ongelman selvittämiseen tai jatkotoimenpiteistä päättämiseen. Monimutkaisissa tai uusissa tilanteissa joudunkin nojaamaan kollegoideni apuun ja pyrin sisäistämään heiltä avun saannin yhteydessä uusia menetelmiä ja prosesseja.

Pyrin jatkamaan kollegoiden jakaman tiedon sisäistämistä, jotta tulevaisuudessa pystyn toimimaan itsenäisemmin useammissa tilanteissa. Toistaiseksi en ole nähnyt sellaisia ongelmatilanteita, joissa vaaditaan useampaa analyytikkoa sekä useita eskalointikanavia. Isojen uhkatilanteiden ja niistä palautumisen oppiminen sekä palautumisen jälkeinen selvitys on asia, joka minun tulee oppia. Onneksi kyseisiä isoja tilanteita ei kohdata erityisen usein, joten oppiminen on tapahtunut teoriatasolla.

Minun pitää lisäksi päättää mihin osa-alueisiin haluan erikoistua. Toistaiseksi olen mieltynyt linuxiin ja lokeista tiedon ja tapahtumien selvitykseen. Samalla olen kehittänyt työn ohessa testiympäristössä uusia automatisointiin käytettäviä työkaluja, joiden käyttöön ja ylläpitoon minun tulee tutustua paremmin ja pyrin mahdollisesti tulevaisuudessa jopa erikoistumaan uusien työkalujen käyttöönottoon ja kehitykseen.

2.2 Sidosryhmät työpaikalla

Alla olevassa kuviossa 1 esitetään työtäni ja rooliani koskevat sidosryhmät jaoteltuna ulkoisiin ja sisäisiin sidosryhmiin.



Kuvio 1. Työssäni käytettävät sidosryhmät

Sisäisistä sidosryhmistä eniten työskentelen kollegoiden, Service Deskin ja eri asiantuntijatiimien kanssa. Kollegoiden kanssa jaamme tietoa ajankohtaisista kyberturva-asioista ja asiakaskohtaista tietoa, sekä autamme toisiamme haastavammissa tehtävissä. Yhteisenä intressinä tiimilläni on SLA-tavoitteiden pitäminen ja ratkaisujen tuottaminen. Service Desk toimii SPOC-mallin mukaisesti keskitettynä kontaktina tiimien ja asiakkaiden välillä. Service Desk jakaa tiimilleni turvallisuuteen liittyviä työpyyntöjä ja tiimini puolestaan tuottaa ohjeita Service Deskille, jotta se pystyy toimimaan yleisimmissä tilanteissa ilman tiimini apua. Eri asiantuntijatiimit jakavat yhteisenä intressinä SLA-tavoitteista kiinni pitämisen ja tiimini pyrkii antamaan ohjeita turvallisuuden näkökulmasta. Muut asiantuntijatiimit toimivat ohjeiden perusteella soveltaen omaa asiantuntijaosaamistaan. Tiimini työskentely ja yhteistyö muiden tiimien kanssa on kokonaisuudessaan melko itseohjautuvaa, mutta isommissa tapauksissa, joissa vaaditaan eskalointia, tiimini on yhteydessä esimieheemme, eskalointiin käytettäviin henkilöihin, sekä mahdollisesti lakitiimiin, joiden intresseissä on saada tilanne haltuun.

Ulkoisista sidosryhmistä tärkein on asiakkaat, joiden ympäristöjä ja käyttäjiä tiimini monitoroi ja pitää turvattuna. Asiakkaiden intressinä on pitää ympäristönsä turvattuna ja olla tietoisia ympäristössään havaituista poikkeamista, sekä heihin kohdistuvista uhkista.

Laite- ja ohjelmistovalmistajat tuottavat ja kehittävät käyttämiämme työkaluja ja laitteita. Heidän intresseissään on tuottaa laitteita tai palveluita, jotka käyvät kaupaksi ja helpottavat asiakkaiden työskentelyä. Samalla asiakkaat antavat palautetta tuotteista, joka auttaa valmistajia tuottamaan entistä parempia palveluita tai tuotteita.
Muiden alan toimijoiden ja viranomaisten intresseissä on turvata omia ympäristöjään ja jakaa tietoa kaksisuuntaisesti, jolloin kaikki osapuolet hyötyvät.

2.3 Vuorovaikutustaidot työpaikalla

Kollegoiden kanssa kommunikointi tapahtuu etätöissä ollessa pikaviestintäohjelmistoja kuten Skypeä tai Teamsiä käyttäen. Kollegoiden kanssa jaamme keskenämme ajankohtaisia tietoturvaan liittyviä uutisia, artikkeleita ja tietoa mahdollisista erilaisten työkalujen kehittäjien järjestämistä konferensseista ja webinaareista. Lisäksi pyydämme usein apua toisiltamme, jos selvitämme poikkeamaa, jossa vaaditaan tietämystä alueesta tai asiakkaasta, jonka joku kollegoista tuntee paremmin. Tiimin sisäinen viestintä on varsin vapaamuotoista, mikä auttaa rennon ja ystävällisen ilmapiirin ylläpitämistä.

Asiakkaiden kanssa kommunikointi tapahtuu yleensä Service Deskin kautta ja toimii SPOC-periaatteella eli keskitettynä yhteydenpitokontaktina. Tiimini kirjaa työpyyntöihin oman selvityksensä, vaadittavat toimenpiteet ja toimintaohjeet. Sen jälkeen työpyyntö siirretään Service Deskin käsittelyjonoon, jossa Service Desk toimii annettujen ohjeiden mukaisesti ja on tarvittaessa yhteydessä asiakkaaseen tai vaadittavaan asiantuntijatiimiin.

Samalla periaatteella Service Desk välittää asiakkaiden luomat työpyynnöt tiimini käsittelyjonoon tarpeen mukaan. Joissakin tapauksissa, kuten isoissa poikkeamissa tai muutoksissa, kommunikointi asiakkaan kanssa tapahtuu sähköpostitse.

Kommunikointi Service Deskiä välikätenä käyttäen tuottaa ajoittain haasteita, jos työpyynnöllä on käytetty vaativampaa tai kyberturvaspesifiä sanastoa. Tällöin Service Desk ei välttämättä ymmärrä tai osaa selittää asiakkaalle mitä olemme tarkoittaneet. Toinen haaste on työpyynnön käsittelyn viivästyminen, jos ratkaisu vaatii useita muutoksia tai tarkastuksia, joita ei voi tehdä kerralla ja työpyyntöä joudutaan kierrättämään useita kertoja Service Deskin kautta.

Kolmantena haasteena on asiakkaat, joilla on kansainvälistä toimintaa ja asiantuntijatiimit on jaoteltu maakohtaisesti. Tällöin oikean asiantuntijatiimin löytäminen voi osoittautua haastavaksi.

3 Päiväkirjaraportointi

3.1 Seurantaviikko 1

Maanantai 07.09.2020

Asetin itselleni päivän tavoitteeksi ratkaista työpyyntöjonoon tulevia työpyyntöjä ja kehittää sisäistä projektia, jossa tutkin MISP-järjestelmän toimintaa, sekä testaan sen toimivuutta erilaisilla tavoilla. Päivä alkoi sähköpostien ja työpyyntöjonon läpikäynnillä. Työpyyntöjonosta valitsin itselleni työpyynnön, joka oli SIEM-järjestelmän tuottama hälytys suuresta määrästä http-vastausten epäonnistumisia. Aloitinkin päiväni työpyynnön tutkimisella ja avasin SIEM-järjestelmän, josta näen hälytykseen liittyvät tapahtumat. Tapahtumia tutkiessani totesin hälytyksen johtuvan http 404 virheistä. Tämä tarkoittaa, ettei palvelin löytänyt siltä pyydettyä sivua. Tarkistin, että lähde, joka puuttuvaa sivua oli hakenut, on samassa verkossa oleva sisäinen työasema ja jokaisessa virhetapahtumassa oli yritetty hakea samaa polkua.
Tämä viittaa siihen, ettei kyseessä ole ulkoinen hyökkäys ja lisäksi, koska kaikki epäonnistumiset hakevat samaa polkua, kyseessä ei ole tiedostopolkuihin kohdistuva väsytyshyökkäys, jolla pyritään kartoittamaan palvelimella olevat tiedostopolut tiedonkeruuta tai mahdollista jatkohyökkäystä varten. Seuraavaksi siirryin tutkimaan CMDB-järjestelmästä, mitä hälytyksen generoineella palvelimella tehdään, ja mitä järjestelmiä siinä on. Selvisi, että kyseessä on kehityspalvelin, jossa asiakas kehittää uutta järjestelmää käyttöönsä. Olen tutkinut aikaisemmin samaisen järjestelmän kehityksestä johtuvia http virheitä toisella työpyynnöllä ja tiesin, että palvelimelle ajetaan automaattisia testejä, jotka tuottavat ajoittain virheitä ja virheet taas tuottavat hälytyksiä. Keräsin tutkimukseni tuottamat tiedot ja johtopäätökset yhteen ja siirsin työpyynnön Service Deskille jatkoselvitykseen, jotta saisin vahvistuksen, että kyseessä on varmasti testien tuottama virhe.

Seuraavaksi vuorossa olikin joka maanantainen palaveri, jossa tiimini kokoontuu jakamaan tietoa yhteisten projektien ja tehtävien kulusta, työpyyntöjen palvelutason toteutumisesta, sekä jakamaan tietoa mahdollisista viikolla odotettavista poikkeustilanteista ja onnistumisista.

Palaverissa selvisi, että otamme käyttöön Jira-ohjelmiston, jolla voimme seurata ja vastuutta eri projektien vaiheita paremmin. Samalla sovimme toisen palaverin, jossa kävimme läpi Jiran toimintaa ja mitä kaikkea sinne pitää lisätä.

Päivän kolmas palaveri oli kahdenkeskinen tiiminvetäjäni kanssa, jossa lisäsimme minulle vastuullistetun MISP-järjestelmäprojektin eri vaiheita Jiraan parempaa seurantaa varten.
Loppupäivän tutkin miten MISPiin voidaan lisätä omaa dataa ja minkälaisessa formaatissa datan pitää olla.

Päivän tavoitteet tulivat mielestäni täyteen, sillä tutkin onnistuneesti yhtä työpyyntöä ja lisäksi sain tutkittua minulle annettua projektia.

Tiistai 08.09.2020
Tiistain tavoitteeksi asetin, että pyrin tutkimaan ja kehittämään mahdollisimman paljon MISP-projektia.

Aloitin päivän tutustumalla erilaisiin tapoihin eritellä IOC-dataa erilaisista lähteistä, jotta sitä voitaisiin lähettää MISP-järjestelmään. Yksi tekniikoista, jolla esimerkiksi normaalilta nettisivulta voidaan kerätä kaikki IP-osoitteet olisi käyttää CyberChef-nimistä ohjelmaa. Se on täysin selaimessa toimiva erilaisen datan käsittelyyn ja tutkimiseen soveltuva ohjelma. Ohjelma osasikin hienosti kerätä IP-osoitteet esimerkiksi Cryptolaemus.com -osoitteesta, johon kerätään Emotet-haittaohjelmaan liittyviä IP-osoitteita, verkkosivuja ja hash-tunnisteita. Koska kyseinen ohjelma kuitenkin toimii selaimessa, niin päädyin etsimään jotain muuta ohjelmaa, johon voisin itse ohjelmoida tai lisätä toimintoja. Löysinkin ohjelman nimeltään Iocextract, joka osaa kerätä IP-osoitteet, URL-osoitteet, sekä hash-tunnisteet. Kaiken lisäksi Iocextract on Pythonilla kirjoitettu ohjelma, joten sitä on helppo ajaa esimerkiksi bash-skriptien kautta ja siten voin automatisoida tai lisätä toiminnallisuutta tarpeideni mukaan.
Suurin osa päivästä meni Iocextractin kokeilemiseen testidatalla. Ehdin lisäksi käsittelemään kahta työpyyntöä, jotka olivat kuitenkin nopeita käsiteltäviä. Toinen työpyynnöistä ei vaatinut tiimini toimenpiteitä, vaan piti vain ohjata toiselle tiimille käsiteltäväksi ja toinen työpyynnöistä laitettiin suspended -tilaan odottamaan käsittelyä myöhemmin.

Keskiviikko 09.09.2020
Keskiviikon tavoitteena on jatkaa Iocextract työkalun tutkimista ja testaamista sekä ratkaista työpyyntöjä.
Keskiviikko alkoi jokaviikkoisella palaverilla, jossa on oman tiimini lisäksi myös 24h-valvomo mukana. Palaverin tarkoituksena on käydä yhteisesti läpi päivätiimin ja 24h-tiimin tehtäviä ja tavoitteita, sekä havaittuja ongelmia. Koska päivätiimi ja 24h-tiimi tekevät paljon yhteistyötä, niin on tärkeää, että kummatkin tiimit ovat ajan tasalla toistensa toiminnasta. Palaverin jälkeen on vielä toinen palaveri, jossa käydään vapaamuotoisemmin läpi kohdattuja ongelmia tai tulevia uudistuksia ja muutoksia.
Palaverien jälkeen siirryin taas tutkimaan Iocextractin toimintaa ja testaamaan, miten se onnistuu käsittelemään suoraan Cryptolaemus.com -sivulta otettua dataa. Siinä on mukana sekalaista tekstiä IOC-datan joukossa. Locextract onnistui tehtävässään hyvin, mutta kävin vielä dataa käsin läpi siltä varalta, ettei datan sekaan ole joutunut mitään ylimääräistä. Huomasinkin, että Iocextractin tuottamassa IOC-listassa oli ylimääräistä dataa. Esimerkiksi kellonaika oli jostain syystä päässyt IP-osoitteiden joukkoon ja osa IP- ja URL-osoitteista oli datan joukossa useampaan kertaan. Tähän ratkaisuksi tein bash-skriptin, joka ajaa aluksi Iocextractin valitsemaani lähteeseen ja sen jälkeen käyttää sort-komentoa duplikaattien poistoon.

Palaverien ja MISP-projektin lisäksi käsittelin työpyyntöä, jossa tutkin palomuurilla havaittua tunkeutumisyritystä. Hyökkääjä oli yrittänyt käyttää erästä tunnettua ja vakavuudeltaan kriittistä haavoittuvuutta palvelimelle. Selvitin miten hyökkäys käytännössä toimii ja missä järjestelmissä haavoittuvuus on. Tutkiessani kohdepalvelimen versiota totesin, ettei palvelin ole haavoittuvainen kyseiselle haavoittuvuudelle.

Torstai 10.09.2020

Torstain tavoitteena on pitää asiakaspalaveri, ratkaista työpyyntöjä ja jatkaa Iocextract ohjelman testaamista.

Torstai alkoi palaverilla, jossa kävimme läpi uusien järjestelmien kehitystä ja esittelin kehitysprojektissa mukana oleville jäsenille, miten MISP-projekti ja IOC-datan kerääminen ovat kehittyneet. Palaverin jälkeen jatkoin Iocextractin tutkimista ja tutkin miksi Iocextract jättää kellonaikoja dataan, vaikka sen pitäisi kerätä vain IP-osoitteita, URL-osoitteita ja hasheja. Testaamalla Iocextractin eri parametrejä totesin, etteivät kellonajat jää dataan, jos haen Iocextractilla vain IPv4 osoitteita. Locextract siis luuli kellonaikoja todennäköisesti IPv6 osoitteiksi. Kun kellonajat oli saatu selvitettyä, kävin vielä dataa käsin läpi siltä varalta, että siellä on vielä jotain ylimääräistä dataa, jota ei haluta päätyvän MISPiin ja sitä kautta muihin järjestelmiin. Huomasinkin, että datan joukossa oli oikeita, ei haitallisia osoitteita, kuten github.com ja twitter.com. Jouduin tekemään bash-skriptiini vaiheen, jossa se poistaa lopullisista listoista tunnetut osoitteet, jotka tunnetaan turvallisina. Näin ne eivät aiheuta turhia hälytyksiä tai niille pääsyä ei estetä, jos lista päätyy lopulta tuotantokäyttöön.
Loppupäivästä oli asiakaspalaverin aika. Asiakaspalaverissa esittelimme palomuurilta otetun kuukausiraportin kollegani kanssa ja kävimme läpi siinä olevaa liikennettä. Esittelimme myös raporteilla poikkeaman, jonka haivaitsimme kollegan kanssa ja josta olimme jo aikaisemmin tehneet selvityksen asiakkaalle. Lisäksi keskustelimme asiakkaan kanssa siitä, miten poikkeama voitaisiin jatkossa estää tai havaita paremmin. Kokonaisuudessaan palaveri sujui erittäin hyvin. Päivän lopuksi käsittelin vielä yhden työpyynnön.

Perjantai 11.09.2020

Perjantaina ohjelmassa on kuusituntinen webinaari Azure Sentinelistä. Koska webinaari vie lähes koko päivän, niin en aseta sen lisäksi muita tavoitteita. Tietenkin, jos työpyyntöjä ilmaantuu jonoon, niin priorisoin ne ja teen niitä webinaarin ohessa.
Suurin osa päivästä kuluikin webinaaria seuratessa, mutta ohessa ja välitauoilla jatkoin Iocextractin testailua ja kehitin samalla bash-skriptiäni hiukan pidemmälle. Nyt bash-skriptini osaa tarkastaa automaattisesti onko verkkosivu muuttunut ja samalla hakea uusimmat IOC-tiedot sekä automaattisesti ajaa uudet tiedot Iocextractin läpi, poistaa duplikaatit ja jaotella IP-osoitteet, URL-osoitteet ja hashit omiin listoihinsa. Datan seassa ei myöskään näytä enää olevan ylimääräistä dataa.

Päivän lopuksi tutkin kahta työpyyntöä, joissa toisesta selvitin, miten O365 käsittelee haitallisia sähköposteja.

Viikkoanalyysi

Viikko kului suurimmaksi osaksi IOC-datan keräämisen ja käsittelyn tutkimisessa, joten se osoittautui tämän viikon teemaksi.

En ollut pitkään aikaan kirjoittanut skriptejä, joten taitoni olivat hiukan ruosteessa ja tuottamani ratkaisut eivät mahdollisesti ole kaikista optimaalisimpia tuotantokäyttöön. Joka tapauksessa luomani skripti toimii hyvänä pohjana ja samalla näyttää logiikan, jolla tiedot voidaan myöhemmin kerätä optimaalisempia tekniikoita käyttäen. Skriptaustaitoni ja yleisesti IOC datan tutkimistaitoni kehittyivät huomattavasti viikon aikana.

Maanantaina selvittämäni hälytys, joka koski suurta määrää http-virheitä, oli myös varsin mielenkiintoinen. Vaikka kyseessä todennäköisesti ei ollutkaan oikea uhka, niin avaan hiukan, minkälainen on mainitsemani tiedostopolkuihin kohdistuva väsytyshyökkäys. Siinä hyökkääjä pyrkii löytämään palvelimelta kansiopolkuja tai tiedostoja, joita ei ole tarkoitettu julkiseksi. Esimerkiksi yleinen sijainti verkkosivujen hallintaan on /admin -osoitteessa. Kyseiseen hallintasivuun ei välttämättä ole linkkejä tai viittauksia julkiseksi tarkoitetulla sivulla, mutta hyökkääjä voi tehdä valistuneen arvauksen hallintasivun sijainnista ja kokeilla kirjoittaa verkkosivun osoitteen loppuun tuon kyseisen /admin polun ja nähdä minkälainen kirjautumissivu on. Hallintasivulla vaaditaan todennäköisesti käyttäjätunnus ja salasana, joten mahdollinen hyökkääjä ei pääse muuttamaan asetuksia noin vain. Sivu saattaa kuitenkin sisältää tietoa, kuten palvelimen versionumeron tai muuta hyödyllistä tietoa, jota voidaan käyttää hyödyksi toisessa hyökkäyksessä. Kansioiden ja tiedostojen etsiminen palvelimelta voi versiotiedon lisäksi paljastaa jopa käyttäjätunnuksia ja salasanoja, jos palvelimella olevia tiedostoja ei ole suojattu oikein. Esimerkiksi erittäin suosittu blogialusta WordPress säilyttää tietokannan tunnuksia wp-config.php -tiedostossa. Jos wp-config.php -tiedoston oikeudet on asetettu väärin, saattaa se näkyä ulkoverkkoon ja kuka tahansa, joka tietää kyseisen tiedoston polun, voi käydä keräämässä sieltä käyttäjätunnuksen ja salasanan. Kyseinen tiedosto ei tietenkään ole näkyvissä verkkosivuilla ja siihen ei ole linkkejä itse sivulla, mutta jälleen hyökkääjä saattaa tehdä valistuneen arvauksen ja kokeilla onneaan hakemalla kyseistä tiedostoa verkkosivulta. Toki tiedostopolkujen etsiminen käsin pelkällä selaimella on erittäin työlästä ja hidasta. Tämän takia on kehitetty työkaluja, jotka osaavat automaattisesti kokeilla erilaisia polkuja sivustolle, joko perustuen annettuun sanalistaan tai kokeilemalla kaikki mahdolliset kirjainyhdistelmät läpi. (BackwardLogic 2018)

Yksi suosituimmista tiedostopolkuihin käytettävistä väsytyshyökkäystyökaluista on Dirbuster, joka on java-pohjainen ohjelma graafisella käyttöliittymällä varustettuna. Dirbusterille voidaan asettaa haluttu nopeus, kuinka nopeasti se käy eri polkuja läpi. Nopeampi polkujen etsiminen kuitenkin on erittäin äänekästä ja on selvästi havaittavissa palomuureilla, jolloin se todennäköisesti laukaisee hälytyksen suuresta määrästä epäonnistuneita http-pyyntöjä. Kuten maanantaina mainitsinkin, niin työpyynnöllä

nähdyssä hälytyksessä oli kokeiltu vain yhtä polkua, joten kyseessä tuskin oli väsytyshyökkäys, jossa näkyisi useita eri polkuja, jotka ovat aiheuttaneet http virheitä. (Raj Chandel's Blog 2018)
Käytin viikolla paljon aikaa IOC-datan tutkimiseen ja käsittelyyn. IOC on lyhenne sanasta Indicator of compromise eli karkeasti suomeksi käännettynä altistumisen indikaattori. Käytännössä IOC siis tarkoittaa mitä tahansa dataa, joka on havaittavissa hyökkäyksissä tai haittaohjelmalle altistumisessa. Esimerkiksi tällä viikolla käsittelin IP-osoitteita, URL-osoitteita ja hasheja, jotka on yhdistetty Emotet-haittaohjelman toimintaan. Hash-tunnisteet ovat lyhyitä numero- ja kirjainyhdistelmiä, jotka on laskettu tiedostosta algoritmien avulla. Kyseiset tunnisteet ovat uniikkeja jokaiselle tiedostolle ja pienikin muutos tiedostossa muuttaa lopullista hashia. Näin ollen hasheja voidaan käyttää esimerkiksi haittaohjelmien tunnistamiseen ilman, että kokonaista haittaohjelmaa tarvitsee jakaa kaikille virustorjuntaohjelmille. Virustorjunta voi laskea tiedostoille hash-tunnisteen ja verrata sitä sen tiedossa oleviin haitallisiin hash-tunnisteisiin. IP- ja URL-osoitteet toimivat myös hyvänä indikaattorina haittaohjelmille. Useita haittaohjelmia levitetään verkkosivuilta, jolloin osoitteet, joista haittaohjelma ladataan, toimivat IOC:na. Palomuurille voidaan tehdä lista sivuista, jotka ovat tunnettuja haittaohjelmien levittäjiä, jolloin palomuuri osaa automaattisesti estää pääsyn sivulle. (Trend Micro. Indicators of compromise)

Samalla periaatteella toimii myös IP-osoitteiden käyttö IOC:na. Palomuuri havaitsee ja estää yhteyden IP-osoitteeseen, joka jakaa haittaohjelmia tai toimii vaikkapa haittaohjelman hallintaosoitteena, jonne haittaohjelma lähettää varastamaansa dataa tai saa komentoja toimimiseen uhrin koneella. Haittaohjelmien hallintapalvelimia kutsutaan nimellä command and control, C2 tai C&C. Jos palvelimella tai työasemalla havaitaan C&C -yhteyksiä, voidaan olettaa, että kyseiselle kohteelle on päässyt haittaohjelma ja se kaipaa välitöntä virusskannauksen ajoa ja kohteella käytettyjen salasanojen vaihtoa.
(PaloAlto Networks. Command and Control Explained.)

3.2 Seurantaviikko 2

Maanantai 14.09.2020
Maanantain tavoitteena jatkaa tunnisteita keräävän skriptin kehitystä, käydä läpi sisäisen SIEM-järjestelmän tapahtumat ja etsiä sieltä poikkeamia sekä tehdä työpyyntöjä, kun niitä tulee.
Aloitin päivän lukemalla The Hacker News ja Tivi -sivustojen uusimmat uutiset läpi, jotta pysyn ajan tasalla tämänhetkisistä tapahtumista ja uusimmista haavoittuvuuksista. Uutisten lukemisen jälkeen aloin käymään läpi sisäisessä SIEM-järjestelmässä olevia tapahtumia ja tutkimaan onko kerätyissä tiedoissa mahdollisesti poikkeamia, jotka vaativat selvitystä tai viittaisivat mahdolliseen uhkaan ympäristössä. Ehdin aloittaa SIEMin läpikäynnin, mutta jouduin pitämään tauon, sillä vuorossa oli SOC-päivätiimin palaveri. Siinä kävimme läpi projektien etenemisiä ja yleisesti viikolla odotettavia tapahtumia. Heti päivätiimin palaverin jälkeen oli vuorossa toinen palaveri. Siinä kävimme läpi tyytyväisyyskyselyn

tulokset, jolla kartoitettiin koko yrityksen laajuudella kuinka hyväksi työntekijät kokevat uran edistymismahdollisuudet, yrityksen tulevaisuuden, yhteistyön sekä monia muita aspekteja organisaation toiminnassa. Palaverien jälkeen pääsin jatkamaan SIEM-tapahtumien läpikäyntiä, mutta en löytänyt mitään uutta poikkeamaa, joka ei olisi jo selvityksessä.

Koska työpyyntöjono oli tyhjä ja minulla ei ollut muuta agendaa päivälle, niin jatkoin IOC-skriptini kehitystä ja sainkin sen jo melko hyvälle mallille. Skriptailun ohessa sain puhelun kollegaltani, joka kertoi, että edellisellä viikolla työstämäni työpyyntö oli sellainen, ettei se olisi kuulunut palvelusopimukseen. Isosta virheestä ei ollut kyse, mutta kollega suositteli jatkossa katsomaan tarkemmin mistä järjestelmästä on kyse ja tarkistamaan kuuluuko se palvelusopimuksen piiriin.

Tiistai 15.09.2020
Tiistaille ei ole kokouksia varattuna, joten tavoitteenani on jatkaa IOC-skriptin kehittämistä ja selvittää mahdollisia päivän mittaan tulevia työpyyntöjä.

Päivä osoittautuikin kohtuullisen hiljaiseksi ja sain kehitettyä IOC-skriptini käytännössä valmiiksi. Skripti osaa nyt hakea Cryptolaemus Pastedumpista Emotet-haittaohjelman IPv4, URL ja hash IOC tunnisteet ja verrata niitä aikaisemmin kerättyihin tunnisteisiin. Lisäksi skripti osaa ylläpitää listaa minkä päivän tunnisteet on jo haettu, poistaa tuplana tulleet tunnisteet, päivittää uudet tunnisteet yhteenvetolistaan jossa on kaikki kerätyt tunnisteet ja lähettää aina uusimmat kerätyt tunnisteet MISP-järjestelmään Emotet tapahtuman alle. Koska skripti on suurelta osin suunniteltu nimenomaan Cryptolaemus-sivulta tiedon keräämistä varten, tein vielä lyhyen skriptin, joka osaa yhden kerran hakea miltä tahansa sivustolta tunnisteita ja tehdä listat niistä. Kyseinen skripti vähentää manuaalista työskentelyä huomattavasti ja sitä voidaan jatkossa käyttää myös muihin käyttötarkoituksiin.

Päivän lopuksi oli työpyyntöjonoon tullut muutamia vanhoja työpyyntöjä, jotka olivat saaneet selvityksen oudoista käyttäjätunnuksista. Käyttäjätunnukset ja niiden käyttö olivat toisen tiimin selvityksen mukaan normaalia, mutta tarkistin vielä varmuuden vuoksi lokeista, ettei kyseisiltä käyttäjätunnuksilta näkynyt outoa liikennettä.

Keskiviikko 16.09.2020
Päivä tulee olemaan kokous- ja koulutuspainotteinen, joten päivän tavoitteeksi asetan niistä selviämisen ja IOC-skriptin esittelyn kollegalle.

Päivä alkoi viikoittaisella tiimipalaverilla, jossa käytiin yhdessä päivä- ja 24/7-tiimin kanssa kohdattuja ongelmia, yhteisten projektien etenemisiä ja tiedotettavia asioita. Kokouksessa ilmoitin erään asiakkaan ympäristössä tapahtuvasta muutoksesta, joka saattaa vaikuttaa monitorointiin. Tiimipalaverien

jälkeen oli vuorossa M365-käyttöönottokoulutus, jossa käytiin läpi M365-ympäristön käyttöä. Koulutuksessa käytiin läpi myös ympäristön käyttöön liittyviä rajoituksia, kuten arkaluontaisen tiedon ja asiakaskohtaisten tietojen jakamista järjestelmän kautta.

Koulutuksen jälkeen hioin vielä hiukan IOC-skriptejäni ja otin puhelun tiiminjohtajana toimivalle kollegalleni, jolle esittelin tuotokseni ja miten se toimii. Kollega oli tyytyväinen tuotokseen. Keskustelimme seuraavista askelista projektissa, kuten dokumentaation tekemisestä skriptille sekä seuraavasta MISP-projektin vaiheesta, joka on tiedon siirtäminen MISP-järjestelmästä SIEM-järjestelmään, jossa MISPistä kerättyä tietoa voidaan käyttää ympäristön tarkkailuun ja hälytysten luontiin.

Seuraavaksi vuorossa oli jatkokokous maanantain tyytyväisyyskyselyn läpikäynnille, sillä emme ehtineet käydä kaikkia tuloksia läpi maanantaina.

Päivän lopuksi ratkaisin yhden työpyynnön, jossa käyttäjä oli saanut teknisenä tukena esiintyneeltä henkilöltä puhelun. Käyttäjä oli onneksi ymmärtänyt kyseessä olevan huijaus ja sulkenut puhelimen. Huijari oli uhkaillut internetyhteyden sammuttamisella, joten kävin lokeista läpi, ettei käyttäjän työasemalla näkynyt epäilyttäviä yhteyksiä ja ajoimme täyden virusskannauksen.

Torstai 17.09.2020
Tämän päivän tavoitteena on tehdä mahdollisimman tehokkaasti työpyyntöjä, tutkia MISP -datan siirtämistä SIEM-järjestelmään ja mahdollisesti kehittää itseäni katsomalla jokin koulutusvideo.

Aloitin päivän käymällä kyberturvaan ja tietotekniikkaan liittyvät uutiset läpi. Uutisten jälkeen aloin tutkia ja testailla tiedon siirtämistä MISP-järjestelmästä SIEM-järjestelmään. Tiedot siirtyvätkin kauniisti MISPin API-rajapintaa käyttäen yhdellä komennolla. Sain koottua SIEMiin listan haluamistani IPv4-osoitteista ja ne menivät suoraan SIEMin uhkalistoille, joista sen pitäisi kerätä tunnisteet ja korreloida niitä havaittuihin yhteyksiin.
Dashboard-näkymässä kuitenkin näkyi, että vain pieni osa lisätyistä IPv4 osoitteista oli mennyt uhkalistalle. Katsoin SIEM-järjestelmän lokeja läpi enkä havainnut siellä virheviestiä, joka kertoisi miksei kaikki tunnisteet olleet siirtynyt uhkalistalle. Lista, jolle siirsin MISPistä datan näytti, että siellä on kaikki IPv4 osoitteet, mutta SIEM-järjestelmä ei jostain syystä siirtänyt kuin osan osoitteista uhkalistalle. Koitin selvittää lähes koko päivän tätä ongelmaa.
Iltapäivällä olin kokouksessa, jossa käytiin koko yrityksen kanssa läpi yrityksen talouskasvu ja liikevaihto, sekä kuinka nämä jakautuvat eri osa-alueisiin yrityksessä. Lopun päivästä käytin lukemalla SIEM-järjestelmän toiminnasta ja sen dokumentaatioista, jotta tuntisin järjestelmän paremmin.

Perjantai 18.09.2020

Perjantain tavoitteena on jatkaa SIEM-järjestelmän uhkalistan eli threatlistin ongelman tutkimista, tehdä työpyyntöjä mahdollisimman tehokkaasti ja mahdollisesti kouluttaa itseäni.

Aloitin päivän lukemalla tietotekniikka-aiheisia uutisia ja keskustelin niistä kollegoiden kanssa. Yksi kollegoista vinkkasi hyvän whitepaperin liittyen vastikään julkaistuun Zerologoniksi nimettyyn haavoittuvuuteen, jossa käytiin läpi sitä, miten hyökkäys toimii ja sen eri vaiheita läpi. Vaikka kyseisessä kirjoituksessa käytiin erittäin matalalla tasolla läpi miten hyökkäys toimii ja osa siinä esitetyistä tiedoista ylitti oman osaamiseni, niin se oli erittäin avartava ja mielenkiintoinen selvitys hyökkäyksen toiminnasta. Opiskelun lisäksi jatkoin SIEM-järjestelmässä olevan ongelman tutkimista, mutta en saanut vikaa vieläkään selvitettyä. Iltapäivällä olin palaverissa, jossa käytiin ajankohtaisia tapahtumia läpi koko yritykselle. Ratkaisin myös yhden työpyynnön ja ohjasin toisen oikealle tiimille.

Viikkoanalyysi

Viikon aikana opin, että aina pitää tarkastaa kuuluuko jokin työ palvelusopimukseen. Vaikka työpyyntö on muuten aiheellinen ja se vaikuttaa helpolta tai mielenkiintoiselta selvitettävältä, niin on hyvä tarkistaa, kuuluuko kyseinen palvelu tai selvityksen kohde meidän vastuualueellemme. Työaika, jota käytetään sellaisten asioiden selvittämiseen, jotka eivät kuulu meille on aina pois joltain muulta työltä, kuten kehitystyöltä. Lisäksi, jos palvelusopimukseen kuulumattomia töitä tehdään kyseenalaistamatta, voi asiakas luulla palvelun kuuluvan meidän vastuullemme ja asiakas saattaa teettää meillä useamminkin vastaavia töitä.

Toinen asia jonka epäsuorasti opin on asiakaskohtaisen tiedon jakamisen rajoitukset ja siinä huomioon otettavat seikat. Esimerkiksi, jos asiakkaan kanssa on sovittu, ettei heidän tietojaan saa käsitellä Suomen tai EU:n ulkopuolella, niin se tulee ottaa huomioon myös viestintävälineissä. Sähköpostit ja pikaviestit säilytetään lähes aina palvelimilla, joten pitää tietää missä maassa kyseiset palvelimet ovat. Jos asiakkaalla on ehtona, että kaikki heidän järjestelmiään koskevat tiedot täytyy pitää Suomen sisällä, niin tulee tarkistaa missä esimerkiksi työssä käytettävät sähköpostipalvelimet sijaitsevat ja missä sijaitsee palvelimet, joita käytetään pikaviestien välittämiseen ja säilyttämiseen. Vaikka itse olen töissä Suomessa ja lähetän sähköpostin kollegalleni, joka on myös töissä Suomessa, niin saattaa minun tai kollegan sähköpostipalvelin sijaita vaikkapa Saksassa. Sähköpostit, joita lähetämme keskenämme, olisivatkin siis tallennettuina Saksassa, jolloin asiakuuden vaatima Suomessa datan pitäminen ei toteudukaan ja pitää harkita sellaista tiedonvälittämisen tapaa, jolla asiakuuden vaatimat ehdot täyttyvät. (Dblackhurst 2016)

Lisäksi opin paljon asioita käytössä olevan SIEM-järjestelmän toiminnasta ja tapoja etsiä virhekoodeja tai vikaviestejä, joilla selvittää järjestelmässä olevia ongelmia. Vaikka kyseinen oppiminen ei ratkaissutkaan viikolla kohtaamaani ongelmaa, jossa uhkalistaan ei päivittynyt kaikki tiedot, niin tämä auttaa varmasti paljon jatkossa tulevia ongelmatilanteita.

Tutkiessani Zerologonin toimintaa opin hiukan paremmin, miten Microsoft Active Directoryn Domain Controllerit käsittelevät autentikoitumisia ja minkälaista suojausta ne käyttävät.

Kokonaisuudessaan viikko oli varsin opettavainen ja osaamiseni sekä tietämykseni kehittyi huomattavasti hallinnollisen ja teknisen alueen osalta. (Tom Tervoort 2020)
Kyberturva on alana jatkuvasti kehittyvä, joten uutta tietoa ja uusia taitoja pitää sisäistää jatkuvasti. Alalla pitää ottaa huomioon sekä korkean skaalan, että pienen skaalan seikat, jotta turvallisuus pysyy hyvänä. Hyvänä esimerkkinä on juurikin tuo palvelinten sijainti. Kovin moni ei varmaankaan tiedä tai edes ajattele, missä maassa heidän datansa sijaitsee. Joissakin tapauksissa tuo datan sijainti voi olla hyvinkin kriittinen tieto.

3.3 Seurantaviikko 3

Maanantai 21.09.2020
Päivän tavoitteena on tutkia ja kokeilla käyttöön tullutta M365 ympäristöä sekä tehdä työpyyntöjä mahdollisimman tehokkaasti.

Aloitin päivän käymällä läpi ajankohtaisia kyberturvauutisia ja osallistumalla viikoittaiseen maanantain palaveriin, jossa kävimme SOC-päivätiimin kanssa läpi ajankohtaisia asioita, kohdattuja ongelmia ja projektien etenemisiä.
Aamupalaverin jälkeen tutustuin kollegan lähettämään linkkiin, jossa hän kysyi ketkä tiimistämme olisivat kiinnostuneita osallistumaan Splunk Boss of the SOC -kilpailuun, jossa maksimissaan neljän hengen tiimeissä pyritään ratkomaan Splunkin SIEM-järjestelmästä erilaisia tehtäviä ja tietoja vihjeiden avulla. Olen kokeillut jälkikäteen julkaistuja Boss of the SOC -tehtäviä ja ne vaikuttivat varsin mielenkiintoisilta. En kuitenkaan ole mielestäni niin taitava, että voisin vielä osallistua kilpailutasolla.

Työpyyntöjono oli tänä aamuna varsin tyhjä, joten päätin alkaa tutkia juuri käyttöön tullutta M365-ympäristöä. Teams ja sen kautta toimivat pikaviestit ja keskustelukanavat vaikuttivat huomattavasti paremmilta ja kehittyneemmiltä, kuin vanha käytössä ollut Skype. Erilaiset kanavat antavat mahdollisuuden tehdä tiimeille keskustelualustoja, joissa voidaan jakaa hauskoja kuvia ja tarinoita, joilla voidaan ylläpitää työmoraalia ja positiivista työilmapiiriä. Teamsin tukema tiedostojen jakaminen ja Wiki-sivut vaikuttivat myös erittäin hyviltä ominaisuuksilta, joita varmasti tullaan jatkossa hyödyntämään.

Suuri osa päivästä kuluikin Teamsiä tutkien ja testaillen, sekä M365-sovellusten asentamiseen puhelimeen. Puhelimeen kyseisten sovellusten asentaminen veikin odotettua enemmän aikaa erilaisten virheiden takia, mutta lopulta onnistuin siinäkin.

Koska työpyyntöjen osalta päivä oli erittäin hiljainen, kului lähes koko päivä M365-ympäristöön tutustumiseen. Onnistuin kuitenkin tutkimaan ja edistämään yhtä työpyyntöä, jossa tarkastin tietojen luovutuslomakkeen, ilmoitin siinä olevista virheistä ja lähetin sen eteenpäin lakiosaston tarkistettavaksi.

Tiistai 22.09.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi sähköpostin tarkastuksella ja olinkin saanut jo vastauksen lakiosastolta edellisenä päivänä lähettämääni tietojen luovutuspyyntöön. Välitin lakiosaston päätöksen Service Deskille jatkotoimenpiteitä varten. Seuraavaksi valitsin työpyyntöjonosta työpyynnön, jossa oli ilmoitus havaitusta yhteydestä sinkhole -osoitteeseen. Aloitin tutkimalla kuinka usein ja kauan yhteys oli ollut, sekä lähde- ja kohdeosoitteiden omistajat. Yhteys vaikutti olevan toistuva ja alkaneen jo edellisenä päivänä. Selvitin lähdetyöaseman ja aseman käyttäjän tiedot ja lähetin työpyynnön Service Deskille ohjeiden kera tutkittavaksi ja skannattavaksi.

Seuraavassa työpyynnössä oli havaittu runsas määrä SOCKS5 -protokollaa käyttäviä yhteyksiä. Luettuna työpyynnön läpi ja tarkastettuani mitä kohde osoitteen takana on, huomasin, että kyseessä oli yhteys, jonka syy oli jo tiedossa ja jota selvitettiin toisella työpyynnöllä. Kirjoitin kuitenkin yhteenvedon tarkistuksessa tutkimistani tiedoista, sekä lisäsin tiedot kyseisestä selvityksestä asiakuuden dokumentaatioon, jolloin 24/7 -valvonta tietää, että kyseinen ongelma on jo tutkinnan alla.

Loppupäivän jatkoin SIEM-järjestelmässä olevan threatlist-ongelman tutkimista. Tutkinnassa huomasin listoissa olevan jonkin verran roskadataa, jotka sain karsittua yksinkertaisella regular expression -säännöllä pois. Toivoin, että roskadata olisi aiheuttanut datan siirtymisongelman, mutta ongelma ei korjautunut. Aivan päivän lopuksi keskustelin kollegoiden kanssa aikaisemmin käsitellyistä työpyynnöistä ja niissä käytetyistä prosesseista.
Aamulla asettamani tavoitteet toteutuivat mielestäni hyvin tänään.

Keskiviikko 23.09.2020
Keskiviikon tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti.

Päivä alkoi viikoittaisella tiimipalaverilla, jossa kävimme läpi projektien etenemisiä ja kohdattuja ongelmia. Palaverin jälkeen siirryin tekemään työpyyntöjä. Otin käsiteltäväkseni työpyynnön, joka oli jo käynyt Service Deskin käsittelyssä. Työpyyntö oli muodostunut hälytyksestä, jossa oli havaittu suuri määrä epäonnistuneita kirjautumisyrityksiä, eikä yhtään onnistunutta yritystä. Tutkiessani tapahtumia SIEM-järjestelmästä havaitsin, ettei kirjautumisyrityksiä enää tapahtunut ja kaikki aikaisemmat yritykset olivat tulleet samasta sijainnista. Havaitsin myös, että käyttäjä oli poistettu käytöstä eli siirretty disabled-tilaan samoihin aikoihin, kun epäonnistuneet kirjautumisyritykset loppuivat. Työpyynnöllä ei

mainittu käyttäjän käytöstä poistoa, joten päätin hakea työpyyntöjärjestelmästä tapahtumia hälytyksen aiheuttaneella käyttäjätunnuksella. Löysinkin toisen aktiivisen työpyynnön, jossa oli poistettu käytöstä useita käyttäjätunnuksia, joiden epäiltiin olevan poistunut käytöstä. Työpyynnöllä oli lista käyttäjätunnuksista, jotka oli poistettu ja työpyynnössäni ollut käyttäjä oli yksi näistä. Kyseisten käyttäjätunnusten tarkoitusta ja tarvetta kartoitetaan jo tuolla löytämälläni työpyynnöllä, joten kirjasin omaan hälytystyöpyyntööni selvityksen jatkuvan tuolla uudemmalla työpyynnöllä. Käyttäjätunnus oli kuitenkin poistettu käytöstä, joten varsinaista uhkaa se ei pysty enää muodostamaan.

Tänään minulla oli vuorossa myös päivittäinen SIEM-järjestelmän tapahtumien läpikäynti. Tapahtumien seasta havaitsin sallimatonta proxy-liikennettä, jota olin aikaisemminkin havainnut tarkistuksen yhteydessä. Tarkistin käyttäjän identiteetin ja totesin sen olevan sama kuin mistä aikaisemmin oli tietääkseni tehty jo selvityspyyntö. Koska yhteys oli edelleen havaittavissa ja aikaisempi selvityspyyntö oli tehty melko kauan sitten, päätin tehdä uuden selvityspyynnön, jossa pyysin Service Deskiä tarkistamaan käyttäjän asentamat ohjelmat ja selaimen lisäosat ulkopuolisten VPN sovellusten varalta.

Päivän lopuksi ratkaisin vielä työpyynnön, jossa asiakas pyysi roskapostifiltterin poistoa yhdeltä yhteiskäyttö-sähköpostilaatikolta, koska siihen tarttui myös sallittuja sähköposteja. Roskapostifiltterin poistamisen sijaan suosittelin säilyttämään roskapostifiltterin ja sen sijaan suosittelin säätämään filtteriä niin, etteivät sallitut sähköpostit jäisi siihen kiinni. Siirsin työpyynnön jatkokäsittelyyn ja säätöjen tekoa varten sähköpostitiimille.

Torstai 24.09.2020
Päivän tavoitteena on tehdä työpyyntöjä mahdollisimman tehokkaasti.

Päivä alkoi palaverilla, jossa kävimme läpi CTI-ympäristön kehitystä. Esittelin muille kehitykseen osallistuville kehittelemäni skriptit, sekä esitin kysymyksiä liittyen ympäristöihin ja niissä kohtaamiini ongelmiin. Lisäksi muut osalliset esittelivät omia tuotoksiaan ja ongelmiaan. Palaverin päätteeksi kävimme läpi, miten jatkamme omia osuuksiamme projektissa.
Palaverin jälkeen valitsin selvitettäväksi työpyynnön, jossa asiakkaalta oli tullut kyselyä havaitusta hyökkäyksestä. Selvityksen yhteydessä totesin kyseessä olevan meidän oma haavoittuvuusskanneri. Tiedustelin varmuuden vuoksi haavoittuvuuksien hallintatiimiltä, olivatko he ajaneet kyseisen skannauksen ja myöntävän vastauksen saatuani lähetin asiakkaalle selvityksen ja selityksen miksi kyseinen skannaus oli ajettu.
Seuraavassa työpyynnössä tutkin palomuurilla havaittua tunkeutumisyritystä, jossa oli käytetty eräästä ohjelmistosta vastikään löytynyttä haavoittuvuutta. Selvitin yhteyden lähteen ja tarkastin sen AbuseIPDB -nimisestä palvelusta. Palvelussa kyseinen lähde oli saanut useita raportointeja ja se oli saanut sataprosenttisen varmuuden väärinkäytöksestä. Tutkin myös kohteena olleiden palvelimien

tietoja selvittääkseni, onko kyseiset palvelimet haavoittuvaisia käytetylle hyökkäykselle. Valitettavasti näkyvyyteni palvelimiin ei ollut riittävä, joten lähetin työpyynnön aluksi palomuuritiimille tarkistettavaksi, jotta havaittu tunniste on varmasti estetty. Neuvoin myös ohjaamaan työpyynnön Service Deskille, jotta he voivat tarkistaa onko palvelimilla kyseistä haavoittuvaa ohjelmistoa.
Seuraavassa työpyynnössä tutkin hälytystä, jossa oli havaittu suuri määrä epäonnistuneita kirjautumisia. Katsoin SIEM-järjestelmästä lokitietoja ja huomasin, että käyttäjän salasana oli vaihdettu juuri samaan aikaan, kun epäonnistuneet kirjautumiset olivat alkaneet. Käyttäjällä oli kuitenkin myös onnistuneita kirjautumisia samaan aikaan. Lähetin työpyynnön Service Deskille, jotta he voivat olla yhteydessä käyttäjään ja selvittää onko hän tehnyt salasanan vaihdon ja onko käyttäjän koneella esimerkiksi credential manageriin jäänyt vanha salasana, jota työasema koittaa sitten käyttää aiheuttaen epäonnistuneet kirjautumisyritykset. Päivän lopuksi osallistuin vielä nuorisolle tarkoitettuun kahvitauko kokoukseen, jossa esiteltiin ja tutustutettiin organisaatioon juuri tulleet uudet työntekijät.

Perjantai 25.09.2020
Perjantain tavoitteena on opiskella ja kouluttautua, sekä ratkaista työpyyntöjä mahdollisimman tehokkaasti.

Aloitin päivän tutkimalla erästä havaittua tunkeutumisyritystä, jossa oli yritetty tunkeutua palvelimelle käyttäen haavoittuvuutta. Kyseinen tapaus oli jo kollegani tutkittavana eikä työpyyntöjonossa ollut muita työpyyntöjä ratkottavaksi, joten päätin tutustua haavoittuvuuteen hiukan paremmin. Löysin mielenkiintoisen blogin, jossa käsiteltiin kyseistä haavoittuvuutta ja käytiin läpi havaintoja, joissa haavoittuvuutta on onnistuneesti hyödynnetty. Hyökkäys kohdistuu haavoittuvaan php-tiedostoon, jonka kautta hyökkääjä pääsee asentamaan oman php webshell -takaovensa kohdepalvelimelle. Blogin kirjoittajan havaintojen mukaan hyökkääjät ”paikkaavat” haavoittuvuuden salaamalla haavoittuvan php -tiedoston omalla salasanallaan, jolla estetään muiden tunkeutujien yritykset päästä palvelimelle. Hyökkääjät itse pääsevät kuitenkin palvelimelle käsiksi joko omalla webshell -takaovellaan tai antamalla haavoittuvalle tiedostolle salasanan, jolla se on salattu.
Päivä jatkui hiljaisena työpyyntöjen osalta ja pääsin ratkaisemaan vain yhden yksinkertaisen työpyynnön, joten käytin loppupäivän katsomalla Azure Sentinel Ninja -webinaaria, jossa käydään läpi Azure Sentinelin toimintaa.

Viikkoanalyysi
Viikolla tuli opittua paljon. M365 -tutkimisen parissa opin siinä olevia ominaisuuksia ja samalla keksin, miten niitä voidaan käyttää tehokkaaseen keskusteluun ja informaation välittämiseen tiimin sisällä. Samalla voidaan olla yhteydessä muihin tiimeihin ja seurata muiden tiimien tapahtumia. Näiden ominaisuuksien avulla kommunikointi tiimin sisällä sekä tiimien välillä on tehokasta ja auttaa rakentamaan suhteita sellaisten uusien henkilöiden kanssa, joiden kanssa voi jatkossa tehdä tiiviimmin yhteistyötä ongelmien ratkaisemiseksi.

Yksi viikolla opituista asioista oli sinkholejen toiminta. Tiesin sinkholen perusidean, mutta tutkiessani tarkemmin, miten sinkholeja käytetään, opin, että niitä voidaan käyttää erittäin monimuotoisiin tarkoituksiin. Sen lisäksi, että sinkholea käytettäisiin vain yhteyden torjumiseen voivat sinkholen ylläpitäjät seurata miten aktiivisesti erilaiset haittaohjelmat leviävät ja missä päin maailmaa. Seuraamalla sinkholeen otettuja yhteyksiä voidaan kartoittaa trendejä haittaohjelmien keskuudessa. Jotkin sinkholejen ylläpitäjät ovat jaotelleet sinkhole IP-osoitteet eri kategorioihin, jolloin organisaatiot voivat selvittää pelkän sinkhole IP-osoitteen avulla oliko estetty yhteys haittaohjelman, bottiverkon tai vaikkapa vain mainoksen aiheuttama yhteys.
(Lily Hay Newman 2018)
Toinen mielenkiintoinen oppimani asia oli webshellien toiminta. Opin minkälaisia obfuskointimenetelmiä hyökkääjät käyttävät sekä miten hyökkääjät estävät kilpailevien hyökkääjien pääsyn haavoittuvuuksiin. Webshellien avulla hyökkääjät pääsevät palvelimelle käsiksi käyttäen itseluotua takaovea. Webshell toimii kuin mikä tahansa php-tiedosto, mutta siihen on rakennettu toiminnallisuus, jolla hyökkääjät voivat syöttää omia komentojaan palvelimelle. Komentojen antaminen rajoittuu php:ta pyörittävän sovelluksen oikeuksiin, mutta jos palvelimella on jokin toinen haavoittuvuus joka mahdollistaa oikeuksien kohotuksen, voivat hyökkääjät tehdä palvelimella lähes mitä tahansa. Koska hyökkääjät voivat käyttää jotakin palvelimen sisällä olevaa haavoittuvuutta, joka ei ole näkyvissä ulospäin, on tärkeää pitää myös palvelimen sisäiset ohjelmistot päivitettynä.
(Forcepoint 2013)
Kolmantena mielenkiintoisena asiana opin paljon Azure Sentinelistä. Azure Sentinel on Microsoftin kehittämä SIEM ja SOAR -järjestelmä. Sentinel toimii natiivisti Microsoftin Azure pilvipalvelussa. Sitä ei kuitenkaan ole rajattu toimimaan vain Azuressa olevilla virtuaalikoneilla vaan siihen voidaan myös yhdistää omia fyysisiä palvelimia ja laitteita. Sentinel pystyy käsittelemään suuria määriä dataa ja erottelemaan datasta mahdollisia uhkia. Se tunnistaa tunnetut uhkat, sekä sen avulla voidaan harjoittaa threat huntingia, jossa etsitään mahdollisia uhkia aktiivisesti ympäristöstä ennen kuin hälytystä kyseisetä uhkasta on edes luotu. Sentinelin drilldown ja tutkimistyökalut vaikuttavat helppokäyttöisiltä ja vaikuttavat antavan erittäin korkea tasoista tietoa, joka nopeuttaa uhkien selvittämistä. Lisäksi Sentinelissä on SOAR mahdollisuus, jonka avulla voidaan automatisoida toimintoja tietynlaisten uhkien havaitsemisen yhteyteen. Esimerkiksi, jos havaitaan, että käyttäjän tunnuksella on paljon kirjautumisyrityksiä, mutta lähde on sama kuin mistä aikaisemmin on ollut onnistuneita yrityksiä, sekä käyttäjätunnuksen salasana on vaihdettu samaan aikaan kuin epäonnistuneet yritykset ovat alkaneet, niin voidaan automatisoida tämän kaltainen hälytys lähettämään suoraan Service Deskille työpyyntö, jossa pyydetään tarkistamaan käyttäjän credential manager vanhentuneiden salasanojen varalta. Tämä vähentää analytiikkojen yksinkertaisiin työpyyntöihin käyttämää aikaa, jolloin analyytikot voivat keskittyä monimutkaisempiin tehtäviin.
(Microsoft Documentation 2020)

3.4 Seurantaviikko 4

Maanantai 28.09.2020
Päivän tavoitteena on tehdä työpyyntöjä mahdollisimman tehokkaasti.

Maanantai alkoi viikoittaisella SOC-päivätiimin palaverilla. Palaverissa käytiin tuttuun tapaan läpi projektien ja tehtävien edistymistä sekä esiteltiin hiukan Jiran käyttöä. Palaverissa kollegani mainitsi löytäneensä SIEM-järjestelmässä ongelman, jonka takia osa hälytyksistä ei toiminut oikein. Syyksi oli paljastunut liian pitkät kuvauskentät, mistä johtuen SIEM-järjestelmä ei osannut käsitellä tietoja oikein, Kun kuvaukset pakotettiin lyhyemmiksi, niin ongelma poistui. Koska ongelma vaikutti vastaavalta, kuin mitä olin itse tutkinut, päätin kokeilla toimisiko sama ratkaisu minun threatlist ongelmaani. Muutosten teon ja kokeilun jälkeen jouduin toteamaan, ettei ongelmani johtunutkaan liian pitkistä kuvauskentistä.
Päivä jatkui työpyyntöjen ratkomisella. Päivän ensimmäisessä työpyynnössä oli saatu ratkaisu epäonnistuneisiin kirjautumisyrityksiin. Työpyynnössä kuitenkin ilmeni toinen ongelma, jossa käyttäjä oli asettanut verkkolevynsä admin-tunnuksen alle. Tämä ei ole hyvän käytännön mukaista, joten työpyyntö lähti vielä takaisin Service Deskille ohjeiden kera, että käyttäjän verkkolevyt pitää laittaa normaalia pienemmillä oikeuksilla varustetun tunnuksen alle.
Seuraavassa työpyynnössä ratkoin asiakkaalle tullutta kahta epäilyttävää sähköpostia. Tutkin sähköpostien sisällöt, joista toinen osoittautui perinteiseksi CEO scam -viestiksi ja toinen yritti levittää haittaohjelmaa. Sähköpostit osoittautuivat erikoisiksi, sillä ne oli lähetetty edelleen asiakkaan sisäisestä jaetusta sähköpostilaatikosta. Sähköposteissa oli asiakkaan työntekijän allekirjoitus, joten lähetin työpyynnön takaisin Service Deskille, jotta he voivat kysyä kyseiseltä työntekijältä onko hän todella lähettänyt sähköpostit ja jos ei ole, niin työpyyntö tulisi lähettää sähköpostiasiantuntija -tiimille tutkittavaksi.

Tiistai 29.09.2020
Päivän tavoitteena on tehdä työpyyntöjä mahdollisimman tehokkaasti.

Tiistai alkoi työpyyntöjonon läpikäynnillä. Jonosta otin edellisenä päivänä lähettämäni työpyynnön, jossa pyysin muuttamaan verkkolevyt admin tunnuksesta normaalin käyttäjän tunnukseen. Käyttäjä kertoi kuitenkin tarvitsevansa admin-tason tunnusta tiettyjen tiedostojen ja kansioiden muuttamiseen. Annoin Service Deskille ohjeet, että muutoksia tuskin tehdään niin usein, että levyjen pitäisi olla admin tunnuksilla koko ajan. Ehdotin, että käyttäjä voisi avata yhteyden levyille aina erikseen silloin, kun tarvitsee admin-tason oikeuksia. Muussa tapauksessa admin -tunnusten pitäminen levyissä ensisijaisena tunnuksena on turha riski, joka saattaa esimerkiksi haittaohjelmalle altistuttaessa aiheuttaa suuria ongelmia.
Seuraavassa työpyynnössä pääsin tutkimaan epäilyttäväksi ilmoitettua sähköpostia. Sähköpostissa ehdotettiin kokeilua, jossa asiakas pääsisi testaamaan ohjelmoijiensa pätevyyttä heidän myymällään

palvelulla. Kävin sähköpostissa olleet linkit läpi ja viesti osoittautui aggressiiviseksi markkinoinniksi, jota voitaisiin jopa kutsua roskapostiksi. Siirsin työpyynnön sähköpostitiimin tutkittavaksi ja käsiteltäväksi.

Seuraavassa työpyynnössä tutkin palomuurilla havaittua tunkeutumisyritystä haavoittuvuuden avulla. Haavoittuvuus oli kohtuullisen uusi ja vakava, joten tutkimusten jälkeen lähetin työpyynnön palomuuritiimille, jotta haavoittuvuus estetään. Neuvoin sen jälkeen lähettämään Service Deskille työpyynnön, jossa pitää selvittää kohdepalvelimien hallinnoijilta onko palvelimissa kyseistä haavoittuvuutta.

Seuraavaksi vuorossa oli lyhyellä varoitusajalla tullut kutsu sisäiseen tärkeään tiedotustilaisuuteen. Tilaisuudessa kerrottiin alkavista YT-neuvotteluista ja neuvotteluiden piiriin kuuluvista tiimeistä. Tiedotustilaisuuden jälkeen päivä jatkui työpyynnöillä, joista yksi oli muun muassa palomuurilla havaittu tunkeutumisyritys haavoittuvuutta hyväksi käyttäen.

Keskiviikko 30.09.2020
Päivän tavoitteena on tehdä työpyyntöjä mahdollisimman tehokkaasti.

Keskiviikko alkoi viikoittaisella palaverilla, jossa käytiin läpi 24/7 -tiimin ja päivätiimin yhteisiä projekteja ja tehtäviä sekä niiden edistymistä. Palaverissa käytiin myös läpi asiakasvastuullisten kanssa onko asiakkailla jotain erikoista tiedossa, kuten muutoksia tai havaittuja ongelmia.
Palaverien jälkeen pääsin taas työpyyntöjen pariin. Ensimmäiseksi työpyynnöksi otin käsittelyyn takaisin tulleen työpyynnön, jossa olin pyytänyt Service Deskiä tiedustelemaan, oliko käyttäjä lähettänyt epäilyttävät sähköpostit jaetusta sähköpostilaatikosta. Käyttäjä oli myöntänyt lähettäneensä ne, koska ne olivat toisen maan kielellä kirjoitettuja. Hän oli luullut niiden olevan tarkoitettu toisen maan yksikölle. Pyysin Service Deskiä huomauttamaan käyttäjälle, että olisi jatkossa valppaampi haitallisten sähköpostien varalta.
Siirryin korjaamaan aikaisemmin kehittämäni IOC -skriptin koodia hiukan, sillä olin havainnut siinä olevan bugin, joka saattoi rikkoa uusien tunnisteiden hakemisen. Korjattuani kyseisen bugin tein skriptistä uudestaan varmuuskopiot ja aloitin pienen dokumentaation kirjoittamista skriptin käyttöä varten.
Päivän lopuksi tutkin työpyyntöä, jossa oli havaittu Eicar-virustestitiedosto työasemalla Microsoft Defender ATP:n toimesta. Tarkemmin tutkittaessa kyseinen työasema oli lisätty juuri samana päivänä Defender ATP:hen. Kyseessä oli todennäköisesti siis testi, jossa juuri lisätyn ATP:n toimintaa oli testattu ja se näyttikin toimivan. Mielenkiintoiseksi työpyynnön teki se, että kyseisestä työasemasta ei kuitenkaan näkynyt paljonkaan tietoa Defender ATP:n hallintakonsolin kautta. Muun muassa käyttöjärjestelmä luokiteltiin tuntemattomaksi. Koska työasema vaikutti poikkeuksellisesta, niin lähetin työpyynnön asiantuntijatiimille selvitettäväksi, jotta saisin tietooni, mikä käyttöjärjestelmä kyseessä on ja oliko kyseessä tosiaan testi.

Torstai 01.10.2020
Päivän tavoitteena on ratkaista työpyyntöjä ja jatkaa MISP-projektia.

Päivä alkoi lyhyellä palaverilla, jossa tiimin esimies kertoi hiukan lisää YT-neuvotteluista ja että se koskee meidän tiimiämme. Jatkoin päivää skriptin ja MISP-järjestelmän dokumentaatiota kirjoittaen. Päivän edetessä keskustelin kollegan kanssa sinkhole -työpyynnöstä, jota olin käsitellyt aikaisemmin. Kollegani oli ottanut sen työn alle ja se tarvitsi ilmeisesti lisää tutkimista. Kerroin tiedot, jotka olin itse löytänyt ja selvittänyt sekä vertailimme niitä kollegan kanssa keskenään.
Päivä jatkui MISP-projektia dokumentoimalla sekä tutkimalla tiq-test eli Threat Intelligence Quotient Test -nimistä ohjelmaa, jolla voidaan testata threat intelligence syötteiden tietotasoa. Testillä voidaan siis tarkistaa mitkä syötteet antavat hyvää ja informatiivista tietoa ja mikä taas eivät, jolloin tunnisteista saatua tietoa voidaan hyödyntää paremmin, kun havaintoja tulee.
Seuraavaksi vuorossa oli pohjoismaiden kyberturvatiimien yhteispalaveri, jossa käytiin läpi kaikkia koskevia asioita. Palaverin jälkeen huomasin taas yhden aikaisemman työpyyntöni tulleen takaisin. Työpyynnössä olin pyytänyt lisätietoja työasemasta, josta ei näkynyt tietoja Defender ATP:ssä. Tiimi jolle olin työpyynnön aikaisemmin lähettänyt ei nähnyt lisätietoja laitteesta, joten lähetin työpyynnön vielä edelleen toiselle tiimille selvitettäväksi.

Perjantai 02.10.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti.

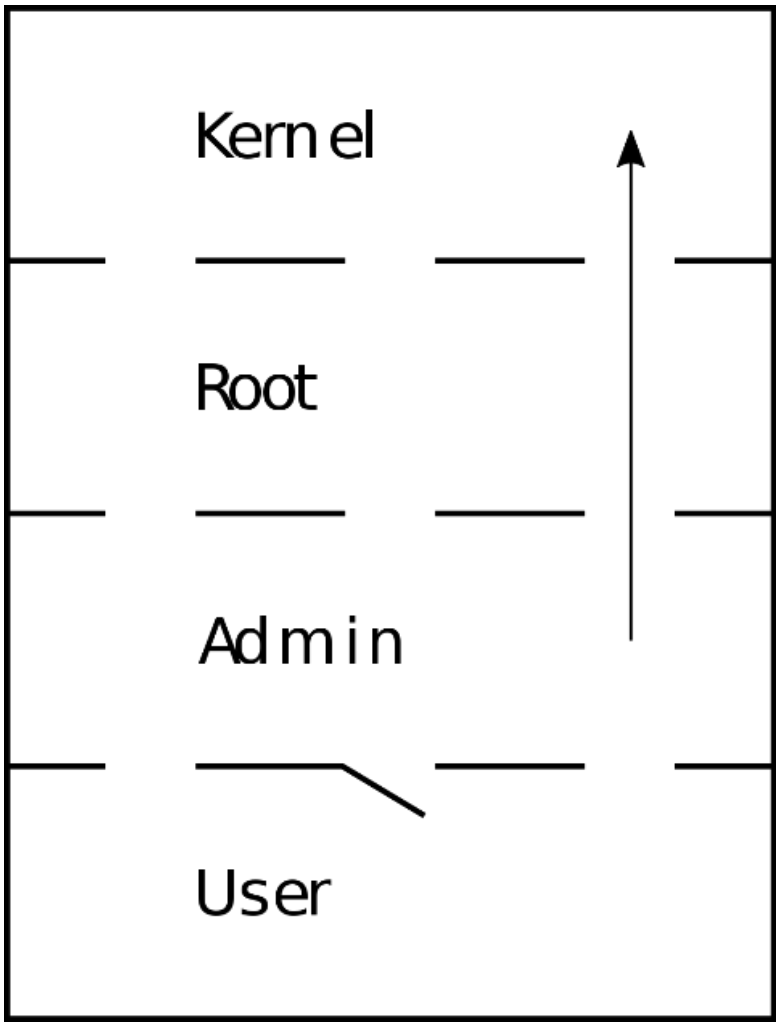
Päivä alkoi työpyyntöjonon läpikäynnillä. Jonosta otin käsittelyyn Service Deskiltä tulleen työpyynnön, jossa oli korjattu eräältä käyttäjältä tulleita epäonnistuneita kirjautumisia. Tarkistin SIEM-lokeista, olivatko epäonnistuneet kirjautumiset loppuneet. Totesin ongelman olevan korjattu, joten suljin työpyynnön. Seuraavassa työpyynnössä oli asiakkaalta tullut tiedustelua epäilyttävästä puhelusta ja voimmeko me estää kyseisen puhelinnumeron. Emme kuitenkaan valvo tai hallinnoi kyseisen asiakkaan puheluita, joten jouduin toteamaan, ettemme voi estää kyseistä numeroa. Neuvoin kuitenkin käyttäjää olemaan soittamatta takaisin kyseiseen numeroon ja mahdollisesti estämään numero itse käyttäjän omasta puhelimesta.

Seuraavassa työpyynnössä Service Desk oli tutkinut virustorjunnan luomaa hälytystä haitallisesta tiedostosta. Kyseessä oli asennusohjelma, jonka mukana tulee adware -lisäosia mukana. Service Desk oli poistanut kyseisen asennustiedoston, mutta he eivät olleet ajaneet täyttä virusskannausta läpi, joten lähetin työpyynnön vielä takaisin ja pyysin ajamaan täyden virusskannauksen vielä läpi.

Kollega pyysi apuani linux lokien seulomisessa SIEM-järjestelmässä, koska olen käyttänyt unix -järjestelmiä häntä enemmän. Tutkimme lokeja yhdessä ja totesimme tietojen jäsentyvän oikein automaattisesti. Ongelmana oli kuitenkin vielä luoda kyseisiin lokeihin uusi sääntö, jolla saadaan luotua hälytys linux lokeissa näkyvistä tapahtumista. Onnistuimme kuitenkin yhdessä luomaan säännön ja saimme uuden hälytyksen toimimaan. Seuraavana vuorossa oli tiedotustilaisuus, jossa saimme ajankohtaista tietoa tämänhetkisistä koronarajoituksista. Loppupäivästä ratkaisin vielä yhden työpyynnön.

Viikkoanalyysi

Viikko ei tuonut hirveästi uutta osaamista tai kehittänyt minua, mutta viikolla tutustuin oikeuksien kohottamiseen. Oikeuksien kohotuksesta eli englanniksi privilege escalation käytetään lyhyempää ilmaisua priv-esc. Maanantain työpyynnöissä, jossa pyysin käyttäjää olemaan käyttämättä admin-tason tunnuksia oletusarvoisesti verkkolevyjen yhdistämiseen, oli kyse nimenomaan priv-esc pinta-alan pienentämisestä. Priv-escillä tarkoitetaan tilannetta, jossa hyökkääjällä on jo pääsy kohteen työasemalle, mutta koska käyttäjän yleisesti käyttämä tunnus on yleensä rajattu pienille oikeuksille, eikä sillä pysty esimerkiksi asentamaan ohjelmia jotka vaativat korkeampia oikeuksia, niin hyökkääjä pyrkii nostamaan oikeudet kohde koneella admin-tasolle. Oikeuksien nostamiseen on useita tapoja. Hyökkääjä voi yrittää arvata käyttäjän admin tunnuksen salasanan eli käyttää väsytyshyökkäystä, etsiä olisiko admin tunnuksen salasanat tallennettu selkokielisenä käyttäjän koneelle tai etsiä admin tai korkeammilla oikeuksilla varustetun ohjelman tai ajurin, jossa on haavoittuvuus ja jonka kautta hyökkääjä pääse suorittamaan komentoja korkeammalla tasolla. Oikeuksien nostoon kuuluu eri tasoja, joista kernel tasoa eli käyttöjärjestelmän ydintä, pidetään korkeimpana tasona, sillä se hallitsee käytännössä kaikkea tietokoneella. (Marcin Teodorczyk, Understanding Privilege Escalation.)
Alla havainnollistava kuva oikeuksien eri tasoista.



Kuvio 2. Privilege Escalation Diagram (Wikimedia Commons 2017)

Kuviossa 2 User ja Admin oikeuksien välissä oleva portti kuvastaa normaalin käyttäjätunnuksen oikeuksien nostamista admin-tasolle käyttämällä admin tunnuksen salasanaa.
Maanantain työpyynnöllä olleessa tapauksessa hyökkääjä pystyisi mahdollisesti käyttämään verkkolevyjä oikeuksien nosto pinta-alana, sillä ne olisivat koko ajan yhdistettynä admin-oikeuksilla varustettuina. Tästä syystä admin -tunnuksia tulisi käyttää vain tarpeen mukaan, ei oletusarvoisesti.
Toinen viikolla oppimani asia oli IOC -datan oikeellisuuden ja tiedollisuuden tarkistamisen tärkeys. Vaikka saatavilla olisi suuri määrä haitallisia tunnisteita ja ne olisivat käytössä aktiivisesti, niin ne ovat lähes turhia, jos eivät kerro mistä uhkasta on kyse. Uhkien tunnistamiseen johtavan tiedon tulisi aina olla kattavaa, jotta tiedon pohjalta voidaan tehdä suoria havaintoja ja johtopäätöksiä mistä uhkasta on kyse. Jos uhkan havaitsemisen jälkeen täytyy alkaa etsimään erikseen tietoa siitä, mistä uhkassa tai hyökkäyksessä on kyse, vie se aikaa uhkan minimointi työltä. Tämä saattaa tapauskohtaisesti olla erittäinkin kriittistä. Ongelmia tulee myös, jos tieto ei olekaan luotettavaa ja käytetyt IOC:t luovat turhia hälytyksiä, jolloin analyytikon aika menee turhanpäiväiseen tutkimiseen ja se olisi voitu käyttää jonkin toisen uhkan tutkimiseen ja torjumiseen.

3.5 Seurantaviikko 5

Maanantai 05.10.2020
Maanantain tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti, sekä käydä sisäisen SIEM-järjestelmän tapahtumat läpi.

Päivä alkoi viikoittaisella SOC -päivätiimin palaverilla, jossa kävimme läpi projektien etenemisiä, SLA -toteutuvuudet ja ilmoitusluontaiset asiat. Palaverin jälkeen aloin käydä läpi sisäistä SIEM-järjestelmää ja siellä olevia tapahtumia. Järjestelmästä havaitsinkin yhden poikkeaman, jossa työasemalta oli ollut toistuvia yhteyksiä edellisestä päivästä asti haitalliseksi merkattuun osoitteeseen. Yhteydet oli estetty palomuurin toimesta. Selvitin työaseman käyttäjän nimen ja tein selvityspyynnön Service Deskille, jotta he voivat ajaa täyden virusskannauksen käyttäjän työasemalla sekä selvittää johtuvatko yhteydet mahdollisesti haitallisesta selaimen lisäosasta. Muita erikoisuuksia tapahtumista ei löytynyt. Loppupäivän käytin työpyyntöjen selvittämiseen ja MISP-projektin dokumentaation parantamiseen.

Tiistai 06.10.2020
Tiistain tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti, sekä jatkaa MISP -dokumentaation kirjoittamista.
Päivän aluksi otin selvitettäväksi työpyyntöjonosta työpyynnön, jossa oli havaittu palomuurilla OpenSSL:ään kohdistuva hyökkäys. Hyökkäys onnistuessaan saattaisi paljastaa tietoa kohdejärjestelmästä. Selvittäessäni lähdettä ja kohdetta huomasin lähteen olevan Qualysin kehittämä SSL Labs -niminen palvelu, jonka kautta kuka tahansa voi tarkistaa verkkosivujensa TLS/SSL salauksen tiedot ja samalla sivu ajaa pienen TLS/SSL kohdistuvan skannauksen, joka oli aiheuttanut palomuurilla havaitun tapahtuman. Katsoin SSL Labsin tuottamaa raporttia kohteesta ja raportilla näkyi, ettei kohde ollut haavoittuvainen kyseiselle haavoittuvuudelle. Samalla huomasin raportilta, että kohde sallii vielä TLS -protokollat 1.0 ja 1.1, jotka eivät ole enää suositeltavia ja niistä pyritään pääsemään eroon. Lähetin työpyynnön jatkokäsittelyyn Service Deskille ja pyysin heitä kertomaan järjestelmän vastaavalle, että suosittelen vanhojen ja haavoittuvien TLS -protokollien pois käytöstä ottamista, koska palvelin käyttää jo myös haavoittumatonta versiota.

Työpyynnön käsittelyn jälkeen lähetin kuukausikokouskutsut asiakkaalle, jonka asiakasvastaavana olen. Kokouskutsun lähettämisen jälkeen kollegani oli käynyt kyseisen asiakkaan kuukausiraportteja pikaisesti läpi ja huomasi siellä olevan poikkeaman. Poikkeamassa näkyi TOR-verkkoliikennettä asiakkaan verkossa. Aloin selvittää yhteyden lähdettä ja kohdetta. Selvityksen päätteeksi tulin lopputulokseen, että yhteys oli normaaliyhteys asiakkaan käyttämään pilvipalveluun, mutta palomuuri oli tunnistanut yhteyden väärin TOR-verkkoliikenteeksi. Aloin tutkimaan palomuurin toimintaa selvittääkseni miksi se tunnistaa yhteyden väärin ja löysin palomuurivalmistajan omilta sivuilta dokumentaatiosta

kohdan, jossa mainitaan vastaavanlaisesta ongelmasta. Ongelma johtuu ilmeisesti siitä, että palomuurin sovellustunnistukseen on jäänyt vanhoja IP-osoitteita jotka tunnistuvat väärin, kun jokin muu palvelu ottaa IP-osoitteen käyttöön.
Loppupäivän käytin MISPin tutkimiseen ja dokumentointiin, sekä muutaman työpyynnön selvittämiseen.

Keskiviikko 07.10.2020
Keskiviikon tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti.

Päivä alkoi viikoittaisella SOC 24/7 -tiimin ja päivätiimin yhteisellä palaverilla, jossa käytiin läpi SLA -toteutumiset ja yhteisten projektien etenemisets sekä käytiin läpi, onko asiakkailla ollut tai onko tulossa muutoksia joista kaikkien olisi hyvä olla tietoisia.
Palaverien jälkeen tutkin työpyyntöä, jossa asiakkaan käyttäjä oli ilmoittanut epäilyttävästä sähköpostista. Työpyyntö oli käynyt jo sähköpostitiimillä, jossa header-tietojen oli todettu olevan oikeita ja työpyyntö oli sieltä siirretty tiimilleni jatkoselvitykseen. Tutkin sähköpostin sisältöä ja kyseessä oli pankilta tullut sähköposti, jossa toimitettiin käyttäjälle jonkinlaiseen järjestelmään käyttäjätunnus ja salasana. Epäilyttäväksi viestin teki se, että viestissä oli salasanasuojattu PDF tiedosto, jossa käyttäjätunnus ilmeisesti olisi. Salasanasuojattu PDF-tiedosto on kohtuullisen harvinainen haittaohjelman levitystapa. Tässä tapauksessa ei kuitenkaan vaikuttanut olevan kyseessä haittaohjelman levitys, koska itse salasanaa tiedostolle ei annettu vaan pyydettiin olemaan yhteydessä pankkiin josta salasanan saisi. Viestissä ei ollut annettu yhteystietoja vaan käyttäjän pitäisi itse olla yhteydessä pankkiin pankin omien sivujen kautta. Kaikki linkit viestissä vaikuttivat myös aidoilta ja header-tiedot oli jo tutkittu oikeiksi, joten kyseessä oli oikea viesti pankilta. Lähetin työpyynnön tietojen kanssa Service Deskille, jotta he voivat kertoa käyttäjälle viestin vaikuttavan oikealta viestiltä pankista.
Työpyynnön jälkeen kollega pyysi apuani tapahtumien tutkimisessa SIEM-järjestelmässä. Kollegan auttamisen jälkeen oli aika osallistua Fujitsu Graduate tapaamiseen, jossa tavattiin pienessä ryhmässä muiden Fujitsu Graduate Programmiin kuuluvien työntekijöiden kanssa ja käytiin läpi työssä kohdattuja ongelmia sekä pyrittiin ryhmänä ratkaisemaan niitä.
Tapaamisen jälkeen toinen kollega pyysi apuani uusien SIEM-lokien keräysohjeiden läpikäymiseen ja korjaamiseen. Kävimme kerättävät kohteet läpi niin, että kollega kertoi miksi haluaa SIEM-järjestelmään minkäkin tiedon ja minä pyysin tarkemman perustelun tai kyseenalaistin tiedon tarpeellisuuden. Tällä toiminnalla saimme tehokkaasti seulottua läpi osan uudistuksista.

Torstai 08.10.2020
Torstain tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti.

Päivä alkoi CTI-ympäristönkehitys -palaverilla, jossa ympäristön kehitykseen kuuluvat jäsenet kertoivat edistymisistään. Kerroin korjauksesta jonka tein IOC -skriptiini ja tehneeni dokumentaatiota skriptin käytöstä sekä MISPistä. Palaverin jälkeen sain tehtäväksi siirtää palaverin vanhasta Skype-kokouksesta uuteen Teams-kokoukseen ja lisäämään uusia kehitykseen osallistuvia henkilöitä siihen. Tein uuden kokouksen Teamsin puolelle ja jouduin sovittamaan kokouksen aikaa hiukan, että sain kaikille sopivan ajan kokoukselle.

Päivä jatkui työpyyntöjen ratkomisella, jossa tutkin muun muassa haitalliseksi merkittyä yhteyttä. Työpyynnöltä selvisi, että käyttäjän työasemalla oli jo ajettu täysi virusskannaus ja sieltä ei löytynyt mitään haitallista. Tutkin yhteyttä palomuurilta tarkemmin ja totesin yhteyden olevan hyvin lyhyt ja tapahtuneen vain yhtenä päivänä. Kyseessä oli siis todennäköisesti jokin verkkosivuilla ollut banneri tai linkki, joka oli aiheuttanut havainnon palomuurilla. Koska yhteys oli estetty ja uusia yrityksiä ei ollut, niin ei työpyyntö mielestäni vaatinut jatkokäsittelyä.
Seuraavana vuorossa oli koulutus, jossa esiteltiin työpyyntöjärjestelmän käyttöä kuten tuntien merkitsemistä, päivitysten tekemistä työpyyntöihin ja käytiin läpi laskutusten toimintaa työpyynnöillä.
Päivä jatkui MISP-projektin kehittämisellä ja kokouksella, jossa meille kerrottiin YT-neuvotteluiden etenemisestä.

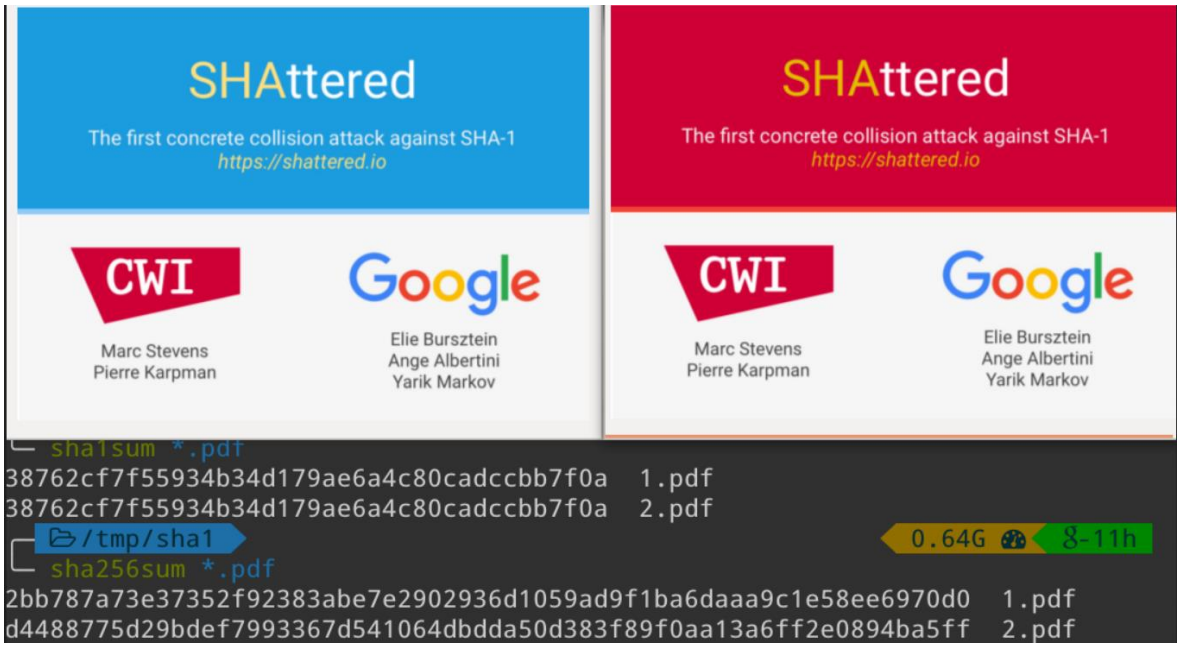
Perjantai 09.10.2020
Perjantain tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti, sekä opiskella kyberturva-asioita.
Päivä alkoi työpyynnöllä, jossa oli havaittu haitalliseksi luokiteltuja yhteyksiä kahdesta lähteestä asiakkaan verkossa. Työpyyntö oli tullut Service Deskiltä takaisin tiimilleni selvitettäväksi, koska Service Desk ei ollut löytänyt tietoja lähdelaitteista. Ryhdyin selvittämään laitteiden tietoja, mutta niitä ei löytynyt mistään lokituksesta tai laitetietokannasta. Pyysin apua kollegalta. Hän osasi heti kertoa toisen lähdeosoitteista olevan vierasverkossa, joten lähdelaitteen selvittäminen olisi erittäin haastavaa. Vierasverkko on kuitenkin eristetty muusta verkosta, joten se ei itsessään aiheuta uhkaa. Toisesta osoitteesta ei kollega ei osannut sanoa mitään, joten siirsin työpyynnön jatkoselvitykseen verkkotiimille.
Työpyyntöjono oli tyhjä, joten päätin jatkaa Microsoftin Azure Sentinel Ninja -koulutusten läpikäyntiä.
Loppupäivä kului kyseisen koulutuksen webinaarivideoita katsoessa.

Viikkoanalyysi
Viikko oli kokonaisuudessaan kohtuullisen hiljainen, joten uutta opittavaa ei erityisesti tullut vastaan. Sen sijaan viikon aikana tuli kerrattua TLS/SSL -suojauksen toimintaa.
Maanantaina SIEM-järjestelmässä havaitsemani toistuva haitallinen yhteys on hyvä esimerkki siitä, minkä takia lokien läpikäynti manuaalisesti on tärkeää. Haitalliseksi merkittyihin osoitteisiin saattaa näkyä yhteyksiä päivittäin eri käyttäjiltä ja osa näistä havainnoista johtuu verkkosivuista, joilla on mai-

noksia tai bannereita, jotka hakevat esitettävän datan tai johtavat haitallisille sivuille. Myös hakukoneet saattavat antaa ensimmäisten hakutulosten joukossa haitalliseksi merkittyjä linkkejä, jos haitallinen tekijä on käyttänyt niin sanottua hakukonemyrkytystä eli search engine poisoningia. Käyttäjä voi helposti hakutuloksien lyhyen kuvauksen perusteella luulla sivua oikeaksi, mutta sivu itsessään onkin täynnä spämmiä. Tällaiset yksittäiset tapahtumat eivät yleensä aiheuta syytä huoleen varsinkaan silloin, kun palomuuri on konfiguroitu estämään haitalliset osoitteet. Yhteyksiä kannattaa kuitenkin seurata myös manuaalisti SIEM:stä jolloin voidaan tarkastaa, onko jollakin lähteellä erityisen paljon yhteyksiä haitallisiin osoitteisiin ja onko yhteydet mahdollisesti olleet pidemmän aikaa aktiivisena. Useat ja pidempikestoiset yhteysyritykset voivat kertoa lähdelaitteella olevasta haittaohjelmasta, joka yrittää olla yhteydessä hallintapalvelimeensa. Usein kyseessä on adware -haittaohjelma, joka pyrkii esittämään adware -ohjelman tekijän asettamia mainoksia uhrille. Mainokset, joita halutaan näytettävän, haetaan adware -ohjelman kehittäjän hallintapalvelimelta ja yhteyden epäonnistuessa adware -ohjelma yrittää yhteyden ottamista useita kertoja päivässä.
(Evan Porter 2019)

TLS -protokollaa käytetään verkkosivujen salaukseen. Kyseinen protokolla on käytössä esimerkiksi HTTPS -protokollassa, jolla salataan yhteys käyttäjän työasemalta palvelimelle asti. TLS -protokollan versio 1.0 on ollut olemassa jo yli 20-vuotta. Version 1.0 jälkeen on kehitetty uudempia versioita kuten 1.1, 1.2 ja 1.3. TLS versio 1.2 julkaistiin yli kymmenen vuotta sitten ja se onkin tällä hetkellä laajimmin käytössä oleva versio TLS:stä. Versiolla 1.2 pyrittiin korjaamaan aikaisemmista versioista löydettyjä heikkouksia, joiden takia niitä ei pidetty enää nykystandardin mukaisesti turvallisina protokollina. Vanhojen TLS -versioiden heikkouden takia on vanhoista protokollista pyritty pääsemään eroon viime vuosina. Esimerkiksi Google, Apple, Microsoft ja Mozilla ovat ilmoittaneet poistavansa vanhentuneet protokollat pois käytöstä uusissa selaimissa ja palveluissaan. Protokollat tulevat kuitenkin edelleen selaimen mukana, mutta ne eivät vain ole päällä tai tuettuna oletuksena, vaan käyttäjän pitää itse ottaa ne käyttöön. Kyseisiä protokollia ei voida poistaa kokonaan, sillä jotkin vanhat järjestelmät joita ei voi korvata saattavat vielä käyttää kyseisiä protokollia. Niiden kokonaan poistaminen aiheuttaisi mittavia ongelmia murto-osalle käyttäjistä. Koska protokollat ovat nykystandardin mukaisesti heikkoja ja niistä pyritään aktiivisesti eroon, niin suosittelinkin maanantaisessa työpyynnössä kyseisten protokollien käytöstä poistamista. Perusteeksi annoin työpyynnölle vielä mukaan Microsoftin ja Googlen artikkelit, joissa kerrotaan protokollien käytöstä poistamisesta. (David Benjamin 2018)

TLS 1.0 heikkous johtuu sen käyttämistä heikoista kryptograafisista tiivistealgoritmeista, kuten SHA-1. SHA-1 heikkous on tiivisteisiin kohdistuvat hash collision hyökkäykset. Tiivistettä käytetään esimerkiksi tiedoston aitouden tarkistamiseen, mutta hyökkäyksessä voidaan luoda väärää dataa tai lisätä ylimääräistä dataa sen verran, että alkuperäisestä ja muunnellusta tiedostosta laskettu tiiviste onkin sama. Tällöin tiedoston aitouden tarkistus luuleekin muunneltua tiedostoa alkuperäiseksi tiedostoksi. Alla on kuvakaappaus Shattered.io verkkosivulta, jolla havainnollistetaan SHA-1 tiivisteen heikkous.



Kuvio 3. Kuvakaappaus (shattered.io 2020)

Kumpikin tiedosto tuottaa saman SHA-1 tiivisteen, vaikka kuvasta näkee selvästi toisessa tiedostossa olevan sininen tausta ja toisessa punainen. Kyseessä on lievä esimerkki, miten tiedostoa on voitu muuttaa ja todellisuudessa tiedoston sisältö voi olla lähes mitä tahansa. Samalla kuvasta näkee SHA256 tiivisteen, joka on paljon pidempi ja turvallisempi. SHA256 tiivisteiden yhteentörmäystä ei toistaiseksi ole vielä onnistuttu tuottamaan.

3.6 Seurantaviikko 6

Maanantai 12.10.2020

Maanantain tavoitteena on tehdä työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Maanantai alkoi viikoittaisella tiimipalaverilla, jossa käytiin läpi päivätiimin suoritusmittareita sekä projektien etenemisiä. Kerroin palaverissa oman projektini edistymisestä.
Aamupalaverin jälkeen kävin läpi työpyyntöjonot, jotka olivat tyhjänä. Koska työpyyntöjä ei ollut tehtäväksi, sovin kollegan kanssa iltapäiväksi palaverin, jossa meidän on tarkoitus käydä asiakkaan palomuurien tapahtumat läpi ennen kuukausittaista palaveria. Jatkoin päivää testiympäristön SIEM-järjestelmää tutkimalla ja yritin selvittää mistä threatlist -ongelma johtuu. Aloin samalla tutkimaan, miten voin tehdä SIEM-järjestelmään omia tapahtumia, jotta voisin testata toimivatko tekemäni tunnistelistat oikein.
Iltapäivällä kävin kollegan kanssa läpi asiakkaan palomuuritapahtumat ja asioita, joita meidän pitää käsitellä asiakkaan kanssa. Loppupäivästä otin työpyyntöjonosta käsittelyyn työpyynnön, jossa tutkin asiakkaalle tullutta epäilyttävää sähköpostia.

Tiistai 13.10.2020

Tiistain tavoitteena on tehdä työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Tiistainakin työpyyntöjono oli aamulla tyhjä, joten päätin siirtyä jatkamaan MISP-projektin edistämistä. Jatkoin SIEM-järjestelmän tapahtumien luomisen tutkimista. Kun sain hyvän kuvan, miten tapahtumat voi luoda, käytin pohjana vanhoja tapahtumia, joiden tietoihin muutin esimerkiksi kohdeosoitteen tilalle osoitteen, joka on varmasti luomallani threatlistillä. Tapahtuman ajankohdaksi muutin hiukan tulevaisuudessa olevan ajan. Tein tapahtumille oman indexin ja merkitsin tapahtumat tulleeksi testihostilta. Koska uhkien korrelaatiohaku hakee uudet tapahtumat vain kerran tunnissa, käytin ajan hyödyksi ja luin ajankohtaisia tietoturva- ja tietotekniikkasivustoja. Korrelaatiohaun pyörähdettyä tarkastin näkyvätkö luomani tapahtumat uhkatapahtumina. Luomani tapahtumat eivät kuitenkaan näkyneet uhkana. Seuraavaksi vuorossa oli asiakkaan kuukausipalaverin aika, joten päätin tutkia syytä sen jälkeen.

Asiakaspalaverissa esittelimme kuukauden aikana havaittuja tapahtumia ja totesimme verkon yleistilanteen olevan hyvä. Palaverin jälkeen jatkoin tapahtumien tutkimista. Pienen tutkiskelun jälkeen totesin luomieni tapahtumien hälyttämättömyyden johtuvan siitä, ettei luomani uusi indexi ole lisättynä korrelaatiohakuun. Lisäsin tapahtumat uudestaan järjestelmään, mutta tällä kertaa asetin indexin yhteen vanhoista indexeistä, jonka tiesin olevan käytössä korrelaatiohaussa ja kyseistä indexiä ei käytetä muissa testeissä tai projekteissa. Kun tiedot oli lisätty uuteen indeksiin, alkoivat ne näkyä uhkina.

Keskiviikko 14.10.2020

Keskiviikon tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi viikoittaisella päivätiimin ja 24/7 tiimin yhteisellä palaverilla. Palaverissa käytiin läpi tiimien yhteisten projektien etenemisiä, sekä asiakaskohtaisia tiedotuksia. Kerroin edellisellä viikolla käsitellystä työpyynnöstä, jossa oli havaittua uhkaavaa liikennettä. Yhteys oli todettu normaaliksi ja asiakas pyrkii eristämään kyseisen liikenteen niin, ettei se enää näy meidän hälytyksissä. Palaverin yhteydessä kollega pyysi minua varaamaan lyhyen kahdenkeskisen palaverin, jossa hän jakaa minulle tietoa ja uusia tehtäviä MISP-projektiini liittyen. Palaverin jälkeen varasin lyhyen palaverin meille puolen päivän aikoihin.

Päivä jatkui SIEM -tapahtumien luonnin tutkimisella ja testaamisella. Eilen olin todennut threatlistissä olevien uhkien toimivan oikein, mutta ongelmana olikin se, ettei kaikki tiedot vaikuttaneet siirtyvän IOC -listoistani tuonne threatlistin puolelle. Päätin kokeilla, onko kyseessä vain visuaalinen ongelma tapahtumien laskemisessa vai eivätkö tiedot oikeasti siirry. Olin testannut, että ainakin threatlistillä ole-

vat tapahtumat toimivat oikein, joten tein uusia tapahtumia, joiden tiedot loin IOC listani pohjalta ja valitsin sellaisia tunnisteita, jotka eivät ainakaan näytä olevan threatlistillä. Tapahtumat lisättyäni olikin aika pitää kollegan kanssa sovittu lyhyt tietojenjakopalaveri.

Palaverissa kollega kertoi uudesta järjestelmästä nimeltä IntelMQ, jonka hän haluaa mukaan MISP-projektiin. IntelMQ ilmeisesti osaa kerätä ja ylläpitää tunnisteita erilaisista lähteistä ja luoda pieniä automatisointeja. Kollega antoi myös paljon hyviä linkkejä, joista saisin lisätietoa ja samalla antoi uuden threat feedin, joka minun tulisi lisätä MISP-järjestelmään. Palaverin jälkeen aloin tutkia IntelMQ:ta ja uutta threat feediä tarkemmin. Järjestelmä vaikutti erittäin järkevältä ja hyödylliseltä sekä se vaikutti tuovan hyvää lisäarvoa MISPille. Loppupäivästä ratkaisin yhden työpyynnön.

Torstai 15.10.2020
Torstain tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja tutustua IntelMQ järjestelmään.

Päivä alkoi aikaisemmin käsittelemäni työpyynnön ratkaisemisella, jonka jälkeen muistin, että on minun vuoroni tarkastaa sisäisen SIEM-järjestelmän tapahtumat. Aloitin SIEM-järjestelmän tapahtumien läpikäynnin. Tapahtumista ei löytynyt mitään erikoista, mutta huomasin yhden toistuvan ei-sallitun VPN –yhteyden. Se oli käyttäjältä, jolle on ilmoitettu jo muutaman kerran aikaisemminkin, ettei kyseinen VPN ole sallittu yrityksen työasemilla. Ilmoitin asiasta kollegalleni, joka on käsitellyt kyseistä asiaa ja hän eskaloi tapahtuman suoraan käyttäjän esimiehelle. Loppupäivästä asentelin IntelMQ:n ja osallistuin muutamaan sisäiseen palaveriin.

Perjantai 16.10.2020
Torstain tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja tutustua IntelMQ järjestelmään.

Aloitin päivän tutkimalla IntelMQ:ta, jonka asensin edellisenä päivänä. Asensin siihen lisäksi IntelMQ Dashboardin, jonka avulla voin helposti selaimen kautta säätää asetuksia ja tutustua käyttöliittymään. Dashboardin asentamisen jälkeen totesin kuitenkin, että IntelMQ korvasi nyt localhost osoitteen, jossa MISP näkyi ennen. Näin ollen esimerkiksi testi SIEM-järjestelmä ei päässyt enää hakemaan tietoja MISPistä. Aloin tutkia, miten saisin järjestelmät eroteltua. Onnistuin asettamaan Apache2 konfiguraatiosta niin, että vain MISP -sivu näytetään localhost osoitteesta. Näin voin käyttää ja tutkia MISPiä samalla, kun tutkin miten saan IntelMQ näkymään toisen osoitteen tai portin kautta. En ehtinyt kuitenkaan pitkälle tutkimaan IntelMQ erityttämistä, kun kollega kysyi olinko ehtinyt lisätä uuden threat feedin MISPiin. Kerroin pienestä virheestäni ja aloin lisätä uutta threat feed lähdettä. Feedille piti tehdä yksinkertainen regex sääntö, jolla sain estettyä väärän datan joutumista MIS:iin. Säännön luonnin jälkeen uusi threat feed näytti toimivan ja sain sen kautta lisättyä uusia indikaattoreita MISPiin.

Viikkoanalyysi

Viikon aikana osaamiseni kehittyi huomattavasti. SIEM-järjestelmän tutkiminen, kehittäminen ja testailu on selvästi parantanut ymmärrystäni järjestelmän toiminnasta sekä kehittänyt ongelmien selvitystaitojani. Vaikka en ongelmaa itsessään saanutkaan vielä ratkaistua, niin huomaan selvää kehitystä selvitysprosesseissa, joita käytän. Lisäksi Apache2 konfiguraatioiden tutkiminen ja säätäminen palautti mieleen koulussa opittuja asioita. Jouduin kuitenkin virkistämään jo opittua tietoa uudella tiedolla eri lähteiden avulla. Kokonaisuudessaan opin Apache2 toiminnasta kohtuullisen paljon ja ymmärrän sen toimintaa paljon paremmin.

Selvitystyötä tuli tehtyä paljon tällä viikolla. Pääsin tutkimaan uutta sekä virkistämään vanhaa osaamista. Muun muassa IntelMQ tuli uutena ratkaisuna, johon pääsin tutustumaan. IntelMQ on ENISA:n eli European Union Agency For Cybersecurity:n aloittama yhteisöprojekti, jonka tarkoituksena on automatisoida ja parantaa kyberturvatapahtumien hallintaa luomalla helposti asennettava ja tuotettava ratkaisu kyberturva toiminta prosesseja varten. Erityisesti IntelMQ pyrkii ratkaisemaan kyberturva tietolähteiden hallinnan ongelmia luomalla yksinkertaisen käyttöliittymän ja ohjelmointikielen, jolla voidaan kerätä ja prosessoida tietolähteistä saatua dataa. IntelMQ:n pystyy itse säätämään mistä tiedot kerätään ja mitkä tai miten tiedot kerätään. Lisäksi tiedot voidaan niin sanotusti rikastaa eli hakea lisätietoa kerättyihin uhkien tunnistetietoihin kuten esimerkiksi IP-osoitteiden tiedot ja missä uhkissa tai hyökkäyksissä kyseistä IP-osoitetta käytetään. Yksinkertaistetulla ja kattavalla keräys- ja rikastusprosessilla saadaan helposti kattavaa tietoa eri uhkatilanteisiin ja tunnistettuihin uhkiin voidaan vastata tarpeellisilla toimenpiteillä, kun tilannetta hoitava analyytikko tietää mistä uhkasta on kyse. Pelkkä havainto IP-osoitteesta, joka on uhkalistalla, ilman lisätietoa mistä uhkasta on kyse, tuottaa lisätöitä analyytikolle, jonka pitää selvittää mikä uhka on kyseessä, mihin se liittyy sekä miten uhkan kanssa tulee toimia. Kun tästä analyytikon prosessista poistetaan vaihe, jossa analyytikon pitää käsin selvittää uhkan syy ja luonne, niin uhkien torjumisvasteajan pitäisi lyhentyä huomattavasti.
(ENISA. Incident Handling Automation)

3.7 Seurantaviikko 7

Maanantai 19.10.2020

Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi viikoittaisella tiimipalaverilla, jossa käytiin läpi projektien etenemisiä. Palaverin jälkeen aloin selvittämään työpyyntöä, jossa käyttäjä kyseli varoitustekstistä, jonka hän sai ohjelman asennuksen yhteydessä. Virheilmoitus osoittautui kuvakaappausten perusteella olevan Windows SmartScreenin luoma varoitus, koska asennuspakettia ei ollut allekirjoitettu ohjelman luojan toimesta. Käyttäjä kertoi kyseessä olevan päivitys jo olemassa olevaan ohjelmaan ja antoi linkin lähteeseen, josta asennuspaketti oli ladattu. Sivusto itsessään näytti aidolta ja oli ollut olemassa jo pitkään, mutta

allekirjoittamaton paketti vaikutti erittäin erikoiselta käytännöltä. Pyysin Service Deskiä selvittämään käyttäjältä, mikä ohjelma tarkalleen oli kyseessä sekä sen käyttötarkoitusta. Toisena työpyyntönä käsittelin lyhyen aikaa olemassa ollutta käyttäjää eli sellaista, joka oli luotu ja poistettu lyhyessä ajassa. Pyysin työpyynnöllä Service Deskiä selvittämään järjestelmän vastuulliselta henkilöltä käyttäjän luonnin ja poiston syytä.

Loppupäivän vietin IntelMQ:hun tutustuessa ja selvittäessä miten Apache2:ssa saadaan eriytettyä MISP- ja IntelMQ -järjestelmät eri porttien taakse. Onnistuinkin eriyttämään IntelMQ -toiminnan toisen portin taakse, jolloin MISP ja IntelMQ voivat olla käynnissä ja saatavilla samaan aikaan samalla palvelimella.

Tiistai 20.10.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi työpyyntöjonon tarkastamisella, josta otin aikaisemmin käsittelemäni takaisin tulleen työpyynnön tutkittavaksi. Työpyynnöllä oli kyse lyhyen aikaa olemassa olleesta käyttäjästä. Järjestelmävastaava kertoi tehneensä testejä ympäristössä, mutta ei tunnistanut hälytyksen aiheuttanutta tapahtumaa. Lisäsin työpyynnölle enemmän tietoa tarkoilla aikaleimoilla varustettuna ja lähetin työpyynnön takaisin järjestelmävastaavan tutkittavaksi. Työpyynnön jälkeen jatkoin MISP -dokumentointia ja dokumentoin uutta IntelMQ -järjestelmää.

Loppupäivästä käsittelin työpyyntöä, jossa asiakas oli saanut epäilyttävän sähköpostin. Tutkiessani työpyyntöä olin samalla kollegoiden kanssa vapaamuotoisessa kahvittelupuhelussa. Sähköposti osoittautui Emotet-haittaohjelmaa levittäväksi sähköpostiksi ja haittaohjelma haettiin suomalaiselta verkkosivulta. Mainitsin asiasta kahvipuhelussa ja tutkimme lähes koko tiimin kanssa sähköpostia. Teimme pikaisesti tehtävien jaottelun, jossa yksi kollegoista ilmoitti käytetystä suomalaisesta verkkosivusta kyberturvakeskukselle ja toinen kollega tutki onko haittaohjelmaa tai sähköpostia havaittu muilla käyttäjillä. Minä tutkin alkuperäistä sähköpostia ja annoin kollegoille tunnistetietoja, joita sain sähköpostista tutkittua. Lopulta alkuperäinen työpyyntö siirrettiin vielä Service Deskille, jolle annettiin ohjeeksi olla yhteydessä kaikkiin käyttäjiin, jotka olivat saaneet vastaavan sähköpostin ja poistamaan viestin, sekä ajamaan täyden virusskannauksen.

Keskiviikko 21.10.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi viikoittaisella tiimipalaverilla, jossa käytiin läpi projektien etenemisiä, sekä asiakaskohtaisia muutoksia. Palaverissa kollega kertoi tulevasta Splunkin järjestämästä konferenssista, joka saattaisi olla mielenkiintoinen. Palaverin jälkeen otin työpyyntöjonosta selvitettäväksi työpyynnön, jota olin

käsitellyt aikaisemmin, liittyen Windows SmartScreen varoitukseen. Käyttäjä kertoi allekirjoittamattoman paketin olevan päivitys aikaisemmin käytettyyn ohjelmaan ja kertoi sen toimineen aikaisemmalla Windows versiolla. Pyysin Service Deskiä siirtämään työpyynnön pakettienhallinta -tiimille, joka voi tutkia ohjelman tarkemmin ja tarvittaessa lisätä sen keskitettyyn pakettien hallintaan turvallisempaa päivittämistä varten.
Päivän toisessa työpyynnössä ratkoin isoa määrää epäonnistuneita kirjautumisyrityksiä, jonka syyksi paljastui SIEMissä näkyvän virhekoodin perusteella vanhentunut salasana. Kirjautumisyritykset loppuivat, kun käyttäjä oli vaihtanut salasanansa uuteen. Loppupäivän luin ajankohtaisia uutisia.

Torstai 22.10.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.
Päivä alkoi CTI-ympäristön kehittäjien palaverilla. Koska tiiminvetäjämme ilmoitti, ettei pääse paikalle, palaverin johtaminen jäi minun vastuulleni. Palaverissa esittelimme projektiemme etenemisiä. Esittelin oman edistykseni ja uuden IntelMQ -järjestelmän, jota todennäköisesti tulemme käyttämään jatkossa. Lisäksi sovin palaverissa olevan SIEM-asiantuntijan kanssa, että sovin toisen lyhyen palaverin hänen kanssaan. Siinä käymme testi SIEM-ympäristössä havaitun ongelman läpi ja yritämme selvittää sen. Palaverin jälkeen otin työpyyntöjonosta käsittelyyn työpyynnön, jossa käyttäjällä oli ongelmia käyttää langatonta kuvanlähetintä. Ongelma ilmeni olevan lähettimen sovelluksessa, jonka pitäisi tulla laitteen sisäisestä muistista. Koska työasemille on pakotettu USB-muistien salakirjoitus, Windows kysyi, halutaanko muistilaite salata. Laitteessa on valmistajan sivujen mukaan vain luettavissa oleva muisti, joten salausta ei voida tehdä. Salauksella pyritään pitämään massamuisteille siirrettävät tiedot turvassa, mutta koska laitteelle ei voi siirtää tiedostoja, niin salausta ei voi tehdä eikä sitä tarvita. Kerroin työpyynnölle, että salauksen voi ohittaa, jolloin Windows pitää laitetta vain luettavassa tilassa ja sen pitäisi toimia. Loppupäivästä pidin puhelun tiiminvetäjän kanssa, jossa kerroin hänelle aamun palaverissa käydyt edistymiset ja tiiminvetäjä vuorostaan esitteli minulle oman kehitystyönsä tuloksia.

Perjantai 23.10.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi työpyyntöjonon läpikäynnillä, josta ensimmäisessä työpyynnössä tutkin käyttäjän raportoimaa epäilyttävää sähköpostia. Sähköposti osoittautui tutkinnassa sisäiseksi sähköpostiksi, jossa oleva linkki johti myös sisäiseen palvelimeen. Sähköpostissa ei vaikuttanut olevan mitään uhkaavaa. Palautin työpyynnön kertoen, että viesti on turvallinen. Tein lisäksi vielä kaksi työpyyntöä, joista toisessa pyysin suorittamaan työasemalla täyden virusskannauksen ja toisessa pyysin ohjaamaan työpyynnön oikealle tiimille.
Loppupäivän vietin tutkien ja testaten MISP- ja IntelMQ-toimintaa.

Viikkoanalyysi

Viikolla ymmärrykseni Windowsin turvatoimintojen, kuten SmartScreenin ja Bitlockerin, osalta kehittyi kohtuullisesti. SmartScreen lisää turvallisuutta tutkimalla suoritettavien tiedostojen allekirjoituksia. SmartScreen estää tiedostojen suorittamisen, jos se havaitsee poikkeaman allekirjoituksessa, kuten puuttuva allekirjoitus tai allekirjoituksen tekijä ei ole tunnettu. SmartScreen vertaa tiedostojen allekirjoituksia ja tunnisteita Microsoftin tietokantaan, jonka perusteella se osaa sallia tunnetut tiedostot tai estää haitalliset tiedostot. Kolmantena vaihtoehtona SmartScreen varoittaa käyttäjää ennen tiedoston suorittamista, mikäli tiedoston allekirjoitus puuttuu tai tiedoston allekirjoittajaa ei tunneta turvalliseksi tai haitalliseksi. SmartScreen tulee oletuksena Windows 8 ja sen jälkeen julkaistuissa Windows käyttöjärjestelmissä. (Chris Hoffman 2017)
Bitlockerilla voidaan suojata työaseman kovalevyt sekä ulkoiset muistit salasanan taakse. Hyvän käytännön mukaista onkin asettaa ympäristön Group Policyn kautta kaikille työasemille pakotettu USB-muistien salakirjoitus. USB-muistien pakotetulla salakirjoituksella varmistetaan, ettei luottamuksellinen tieto joudu vääriin käsiin esimerkiksi USB-muistin katoamistilanteessa. Salakirjoituksen ollessa pakotettuna Bitlocker kysyy käyttäjältä halutaanko muisti salata. Jos käyttäjä kuitenkin vastaa, ettei muistia salata, niin muisti jää vain luettavissa olevaan tilaan. Käyttäjä voi siis edelleen siirtää tiedostoja USB-muistilta tietokoneelle tai suorittaa sovelluksia siltä, mutta hän ei voi lisätä tiedostoja tietokoneelta USB-muistille.
Viikolla havaittu Emotet-haittaohjelmaa levittävä sähköposti ja levitykseen käytetty suomalainen sivu olivat mielenkiintoisia selvitettäviä. Opin tapauksen yhteydessä myös enemmän kyberturvallisuuskeskuksen tärkeydestä. Koska suomalainen sivusto, josta haittaohjelman lataus tapahtui, ei ollut asiakkaamme verkossa eikä kuulu palvelumme piiriin, niin kyberturvakeskus toimii välikätenä, joka osaa ilmoittaa vastuulliselle osapuolelle heidän palvelimellaan havaitusta poikkeamasta. Lisäksi kyberturvallisuuskeskukselle on hyvä ilmoittaa kotimaassa havaituista poikkeamista, koska silloin kyberturvallisuuskeskus osaa pitää tilastoa ja varoittaa kotimaisia yrityksiä heihin mahdollisesti kohdistuvista uhkista ja niiden trendeistä.

3.8 Seurantaviikko 8

Maanantai 26.10.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi viikoittaisella tiimipalaverilla, jossa kävimme läpi projektien etenemisiä sekä ajankohtaisia asioita. Palaverissa virisi keskustelua ajankohtaisesta ja paljon uutisissa näkyneestä terveyspalveluyrityksen tietomurrosta. Spekuloimme mahdollista hyökkäystapaa sekä tapoja, miten havaita ja torjua vastaavia hyökkäyksiä, jos ne kohdistuisivat meidän asiakkaisiimme. Emme kuitenkaan voineet tehdä merkittäviä johtopäätöksiä, koska tapauksen tekniset tiedot eivät ole julkisia eikä meidän saatavillamme.

Palaverin jälkeen huomasin sisäisen SIEM-järjestelmän tarkastuksen vuoron olevan itselläni ja aloin käymään sen tapahtumia läpi. En löytänyt tapahtumista mitään uutta tai poikkeavaa, joka ei olisi jo selvitettävänä. SIEM tarkastuksen jälkeen aloin käymään läpi työpyyntöjonoa ja otin käsittelyyn työpyynnön, jossa asiakas oli pyytänyt sähköpostiosoitteen estämistä. Tarkastin esimerkkinä annetun sähköpostin ja viesti vaikutti aidolta asiakkaan lähettämältä viestiltä ja sisälsi paljon viestittelyä. Pidemmän tutkinnan ja päättelyn jälkeen tulin tulokseen, että kyseessä oli vihainen asiakas, joka lähetti paljon viestejä kiirehtiäkseen asiaansa, mutta viestit eivät sisältäneet kalastelua tai haitallisia liitteitä. Pyysin työpyynnöllä vastaanottajalta varmistusta onko kyseessä todellinen asiakkaan asiakas ja jos on, niin estoa ei voida tehdä palvelintasolla.

Päivän päätteeksi selvitin vielä yhden työpyynnön, jossa oli havaittu useita epäonnistuneita kirjautumisyrityksiä, sekä tutkin IntelMQ:n toimintaa.

Tiistai 27.10.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja esitellä MISP-järjestelmän toimintaa päivälle varatussa demopalaverissa.

Päivä alkoi heti demopalaverilla, jossa kollegat esittelivät projektejaan ja suunnitelmia projektien jatkamiseksi. Esittelin omalla vuorollani MISP-järjestelmän toimintaa ja miten IntelMQ osaa kerätä ja siistiä dataa sekä lähettää siistityn datan MISP-järjestelmään. Kerroin myös vielä olemassa olevista ongelmista ja jatkokehityssuunnitelmista. Kollegat vaikuttivat vakuuttuneilta ja palaverissa heräsi kysymys voitaisiinko tähän asti toimiva osuus MISPistä luoda jo tuotantoympäristöön. Totesin sen olevan mahdollista ja lupasin selvittää asiaa. Palaverin jälkeen aloin käydä työpyyntöjonoa läpi ja sieltä sain selvitettyä muutaman hälytyksen epäonnistuneista kirjautumisista sekä ohjasin yhden työpyynnön oikealle tiimille.

Keskiviikko 28.10.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi viikoittaisella päivätiimin ja 24/7-tiimin palaverilla, jossa käytiin läpi yhteisten projektien edistymistä sekä asiakaskohtaisia muutoksia ja havaintoja. Palaverin jälkeen aloin tutkia MISP-dataa SIEM-järjestelmässä ja tein listan kokeilemistani vianselvitystavoista. Puolen päivän aikaan pidin lyhyen palaverin SIEM-asiantuntijoiden kanssa, jossa kerroin ongelmasta ja kerroin tähän asti tehdystä selvityksestä. Ongelmaa emme palaverissa saaneet ratkaistua ja se vaatii asiantuntijoiden mukaan paljon selvitystä.

Palaverin jälkeen aloin käydä työpyyntöjonoa läpi ja otin sieltä selvitettäväksi työpyynnön, jossa oli havaittu tuntematon vastaus sähköpostipalvelimelta. Palvelimesta joka yritti ottaa yhteyttä SMTP-porttiin ei kuitenkaan ollut tarkkoja tietoja saatavilla, joten siirsin työpyynnön järjestelmävastaavan selvitettäväksi ja tiedustelin, kuuluuko kyseisen palvelimen ylipäätänsä käyttää SMTP-porttia. Päivän lopuksi täytin vielä työntekijöiden puolivuosittaisen itsearvioinnin ja lähetin sen esimiehelle tarkastettavaksi.

Torstai 29.10.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Aloitin päivän työpyyntöjonon läpi käynnillä ja selvitin kaksi työpyyntöä, jotka kummatkin olivat hälytyksiä epäonnistuneista kirjautumisyrityksistä. Työpyyntöjen selvityksen jälkeen siirryin jälleen MISPin ja IntelMQ:n pariin tutkimaan testaamaan ominaisuuksia, mutta en saanut suurempaa edistystä kummankaan järjestelmän suhteen. Loppupäivästä osallistuin koko osastolle tarkoitettuun kokoukseen, jossa esiteltiin osastomme tilastoja ja tulevaa toimintaa. Heti edellisen palaverin perään osallistuin toiseen palaveriin, jossa kävimme läpi turvallisuuskoulutuksen uusiin remontoituihin toimistotiloihin sekä kävimme läpi yleisesti minkälaiset ovat uudet tilat, johon tiimini sijoittuu.

Perjantai 30.10.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti, sekä opiskella uusia asioita.

Aloitin päivän ratkaisemalla yhden työpyynnön liittyen epäonnistuneisiin kirjautumisiin. Työpyynnön jälkeen kävin läpi saamani sähköpostin, jossa kerrottiin tulevasta graduate programiin kuuluville henkilöille tarkoitetusta kahden päivän konferenssista. Konferenssiin oli luotu agenda, josta sai valita itselleen mielenkiintoisia esityksiä. Esityksiä oli useita ja ne vaihtelivat hakukoneoptimoinnista motivaation ylläpitämiseen. Vaihtoehtona oli myös osallistua esityksen sijaan verkostoitumispuheluun, jossa pääsee keskustelemaan globaalisti eri ihmisten kanssa. Kävin kaikkien esitysten kuvaukset läpi ja valitsin mielestäni itselleni sopivimmat esitykset. Loppupäivän tutkin IntelMQ toimintaa ja luin ajankohtaisia uutisia ja artikkeleita kyberturvaan liittyen.

Viikkoanalyysi
Viikko osoittautui kohtuullisen yksinkertaiseksi ja projektin osalta suurta edistystä ei tullut. Oman projektin esittely muille ja positiivisen palautteen saaminen osoitti kuitenkin, että projekti on menossa oikeaan suuntaan ja olisi jo osittain valmis tuotantoon siirrettäväksi.
Maanantaina käsitelty työpyyntö, jossa asiakas oli pyytänyt sähköpostiosoitetta estettäväksi, oli hyvä esimerkki siitä, minkä takia sähköpostit pitää tutkia ennen niiden estämistä. Vaikka sähköposti sisälsi liitteitä ja osoitteesta tuli paljon sähköposteja, niin viestit kuitenkin vaikuttivat olevan oikealta asiakkaan asiakkaalta eivätkä sisältäneet mitään haitallista, jonka takia viestit pitäisi suodattaa pois. Sähköpostien suodatusta tulee käyttää vain todistetusti haitallisiin sähköposteihin, kuten haittaohjelman

levitykseen, kalasteluviesteihin tai oikeaan roskapostiin. Mikäli sähköpostiosoite olisi estetty ilman sen haitallisuuden tarkistamista, olisi asiakkaan ja heidän asiakkaansa välinen viestittely keskeytynyt kokonaan ja mahdollisesti keskeneräisiä tai loppuun käsittelemättömiä asioita ei olisi enää voitu hoitaa sähköpostitse. Lisäksi mahdolliset tulevat yhteydenottotarpeet olisivat keskeytyneet.

Toinen viikolla oppimani asia oli se, että joskus täytyy nojautua asiantuntijatiimeihin. Vaikka haluaisin useasti tehdä kaiken itse ja oppia samalla, niin joskus se voi olla väärä valinta. Esimerkiksi MISP- ja SIEM-välinen datansiirto ja siinä oleva ongelma, jota olen tutkinut jo pidempään. Olen käyttänyt kohtuullisen paljon aikaa ongelman tutkimiseen tuloksettomasti. Kun pidin palaverin SIEM-asiantuntijoiden kanssa, eivät hekään osanneet heti kertoa ratkaisua, mutta osasivat arvioida missä komponenteissa vika mahdollisesti on ja tiesivät miten he voivat ruveta asiaa selvittämään. Toinen tapaus tällä viikolla oli havaittu SMTP-yhteys. En nähnyt lähdepalvelimesta tietoa ja yhteyden kohdekaan ei kertonut minulle yhteyden tarkoitusta, vaikka yritin asiaa selvittää. Näissä tapauksissa tehtävä pitää siirtää sellaisen tiimin käsiteltäväksi, joka tuntee järjestelmät ja joilla on mahdollisuus päästä tutkimaan ongelman juurisyytä syvemmin.

3.9 Seurantaviikko 9

Maanantai 02.11.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi viikoittaisella tiimipalaverilla, jossa käytiin läpi projektien etenemisiä ja SLA-vasteaikojen täyttymisiä. Lisäksi tiimin johtaja kertoi varaavansa kaikille kahdenkeskisen palaverin, jossa käydään jokaisen projekteihin liittyvät tehtävät ja vaiheet läpi sekä suunnitellaan uusia tehtäviä ja vaiheita. Palaverin jälkeen jatkoin IntelMQ:n tutkimista ja onnistuin ratkaisemaan siinä olleen ongelman, joka aiheutti virheitä, jos oletuksena olleesta konfiguraatiosta yritti poistaa joitakin osia. Nyt pystyin tekemään täysin tyhjältä alustalta omia automatisointijonoja ilman, että alkuperäistä konfiguraatiota pitäisi säilyttää.
Iltapäivästä osallistuin kahdenkeskiseen palaveriin tiimin johtajan kanssa. Kävimme Jira-tehtäviäni läpi sekä lisäsimme uusia tehtäviä MISP-projektiin liittyen. Lisäksi keskustelimme MISP-projektin tähän asti toimivan osan siirtämisestä tuotantoon ja siihen valmistautumisesta. Palaverin jälkeen tutkin uusia tehtäviä ja tutustuin niiden vaatimuksiin pintapuolisesti, kunnes tiimin johtaja kutsui minut toiseen lyhyeen palaveriin. Palaverissa todettiin, että on aika aloittaa MISP-projektin tuotantoon siirtämisen suunnittelu ja sain tehtäväksi tutkia ja suunnitella MISPin tuotantovalmiuteen saamisen vaatimuksia ja miten haluan toteuttaa tuotantoympäristön. Sain myös tehtäväksi varata palaverin piakkoin, jossa suunnittelisimme verkkoasiantuntijan kanssa, minne ja miten MISP-palvelin tuotettaisiin tuotantoverkkoon. Päivän lopuksi varasin torstaille suunnittelupalaverin.

Tiistai 03.11.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi työpyyntöjonon läpikäynnillä ja sieltä otin selvitettäväksi työpyynnön, jossa käyttäjä oli poistanut admin-oikeudet toiselta käyttäjältä. Työpyynnöllä oli tapahtunut sekaannus, josta johtuen oikeudet poistaneelta käyttäjältä oli kysytty, oliko häneltä lähtenyt oikeudet. Tarkistin tapahtumat SIEM-lokeista ja huomasin käyttäjän suorittaneen SQL-hallintaohjelmistoa saman aikaisesti. Selvensin työpyynnölle tapahtuneen sekaannuksen ja lisäsin tietona, että käyttäjä oli suorittanut samaan aikaan SQL-hallintaohjelmistoa. Lisäksi pyysin selvitystä oikeuksien poistosta ja kysyin, liittyikö muutos SQL-hallintaan. Toisessa työpyynnössä selvitin GPO-muutoksia tehneen käyttäjän identiteetin ja pyysin selvitystä tehdyistä muutoksista.
Loppupäivän käytin MISP-projektin kehittämiseen. Onnistuinkin ajoittamaan threat feedien noutamisen sekä itse tekemäni IOC-skriptin. Lisäsin skriptiini vielä lisäksi toiminnallisuuden, jonka avulla sen keräämät ja MISPiin lisäämät tunnisteet julkistuvat automaattisesti. Tunnisteiden julkistaminen piti lisätä, koska olin aikaisemmin todennut, ettei julkaisemattomat tunnisteet päivity testi SIEM-järjestelmään, vaikka ne olisivatkin näkyvissä ja haettavissa.

Keskiviikko 04.11.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi viikoittaisella päivätiimin ja 24/7-tiimin palaverilla, jossa käytiin läpi yhteisten projektien edistymisiä, sekä asiakaskohtaisia muutoksia ja havaintoja. Heti palaverin jälkeen oli tiedotustilaisuus, jossa meille kerrottiin käytännön asioita lomautuksista, kuten minne tulee ilmoittaa, jos tulee lomautetuksi ja miten voi laskea paljonko saa rahaa lomautettuna. Tiedotustilaisuuden jälkeen ryhdyin käymään läpi sisäistä SIEM-järjestelmää ja sen tapahtumia. Tapahtumista ei löytynyt mitään erikoista, mutta siellä näkyi sallimattomia VPN-yhteyksiä. Niistä oli juuri viikko sitten annettu tiedote, ettei niitä saa olla työpaikan verkossa eikä työkoneilla asennettuna. Kerroin asiasta kollegalle, joka on hoitanut VPN-ohjelmista tiedottamista ja hän kiitti tiedosta. Loppupäivän käytin MISP-projektin tutkimiseen ja testaamiseen.

Torstai 05.11.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi CTI-ympäristön kehitystiimin palaverilla, jossa kävimme läpi projektiemme edistymisiä ja tarpeita. Lisäksi esittelin pohjustavan arvioni MISPin tuotantovaatimuksista, jotka kollegan mielestä olivat toteutettavissa. Palaverin jälkeen osallistuin MISPin tuotantoon siirtämisen pohjustavaan aloituskokoukseen, jossa suunnittelimme verkkokaavion, joka toimii pohjustavana suunnitelmana toteutukselle. MISPin lisäksi suunnitelmaan lisättiin uusia tulevia tuotteita ja mahdollisia integraatioita, joita

tulevaisuudessa tullaan mahdollisesti käyttämään. Palaverien jälkeen ryhdyin jälleen tutkimaan testaamaan MISPiä. Iltapäiväksi tein pikaisen kahden keskisen palaverivarauksen itselleni ja kollegalle, jossa kävimme läpi asiakkaan kuukausiraportin ja tutkimme siitä löydettyjä havaintoja. Loppupäivän jatkoin MISP-projektin edistämistä.

Perjantai 06.11.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä oli työpyyntöjen osalta hiljainen, joten aloitin käymällä läpi ajankohtaisia kyberturvauutisia ja artikkeleita. Ajankohtaisuuksien lukemisen jälkeen siirryin tutkimaan MISPiä ja sen toiminnallisuutta. Päivän tavoitteena oli selvittää MISPissä olevien IOC-tunnisteiden rikastamista ulkopuolisista lähteistä. Aloitin tutkimalla erilaisia tiedon rikastamiseen käytettäviä moduuleja, joista päädyin kokeilemaan VirusTotal integraatiota ja DNS lookuppia. VirusTotal tuntui toimivan kohtuullisen hyvin ja löysi osassa testejä hyödyllistä tietoa ja lisäsi sen MISPissä oleviin tapahtumiin. Joissakin tapauksissa se tosin tuotti ylimääräisiä viittauksia erilaisiin lähteisiin, joita en kokenut tarpeelliseksi. DNS lookup -moduuli puolestaan ei jostain syystä saanut haettua lainkaan tietoja. Vietin käytännössä koko päivän moduulien toimintaa testaillessa.

Viikkoanalyysi
Viikolla ymmärrykseni ja osaamiseni MISP-projektissa kehittyi huomattavasti. Ymmärrän nyt paremmin järjestelmän toimintaa, osaan automatisoida työvaiheita, opin enemmän PyMISP-integraation käyttöä, sekä tunnisteiden rikastamista. Lisäksi opin torstain MISPin tuotantoon siirtämisen suunnittelupalaverissa paljon alustavasta suunnitteluvaiheesta ja pääsin näkemään, kuinka helposti ja nopeasti kokenut verkkoasiantuntija pystyy luomaan pohjustavan verkkokaavion tuotantoa varten.

Viikolla havaittiin jälleen ei-sallittuja VPN-yhteyksiä, joita on alettu kovemmalla kädellä valvomaan ja huomauttamaan käyttäjiä sekä raportoimaan korkeammille tahoille havainnoista. Ei-sallitut VPN-yhteydet luovan uhkan peittäessään näkyvyyden työasemilla tapahtuvaan liikenteeseen. Mikäli työasemilla olisi haittaohjelmia, joita virustorjunta ei näkisi, mutta esimerkiksi palomuuri pystyisi havaitsemaan yhteyden haitalliseen C&C palvelimeen, niin ei-sallittu VPN-yhteys piilottaisi havainnon ohjaamalla yhteyden salattuna VPN-palvelun palvelimen kautta. Tällöin haittaohjelma saattaisi jäädä havaitsematta ja aiheuttaa tuhoa tai varastaa tietoa.

Lisäksi ongelmaksi muodostuu VPN-palveluntarjoajan luotettavuus. VPN-palveluntarjoaja saattaa vakoilla yhteyden kautta kulkevaa dataa, jolloin ulkopuolinen VPN-palvelu saattaisi saada käsiinsä luot-

tamuksellista tietoa. VPN-yhteys on kaksisuuntainen, joten VPN-palveluntarjoaja saattaa myös lähettää VPN-palvelua käyttävän käyttäjän työasemalle yhteyksiä, jotka kulkevat käyttäjän verkon kautta internettiin. Hyvä esimerkki tästä on vuonna 2015 suosiossa ollut Hola VPN-palvelu. Hola tarjosi ilmaista VPN-lisäosaa selaimiin, jonka kautta sen käyttäjät pääsivät käyttämään Holan VPN-palvelua ja katsomaan esimerkiksi suoratoistopalveluita toisen maan kautta, jossa suoratoistopalvelun valikoima saattoi olla parempi. Moni Holan käyttäjistä ei kuitenkaan tiennyt Holan toimintamallista, jossa Holan toinen brändi, nimeltään Luminati, myi Hola käyttäjien verkkoyhteyksiä. Tällöin kuka tahansa maksava Luminatin asiakas saattoi käyttää Holan käyttäjien verkkoyhteyttä esimerkiksi palvelunestohyökkäyksiin. Palvelunestohyökkäykset näyttäisivät siis tulevan Hola käyttäjien IP-osoitteista. Jos yhteyttä käytettäisiin rikollisiin tarkoituksiin, epäilyt kohdistuisivat ensimmäiseksi Holan käyttäjään, joka saattaa olla täysin tietämätön Holan toiminnasta ja rikollisesta toiminnasta, joka hänen yhteytensä kautta on tapahtunut. (Wayne Rash 2019) (Lorenzo Franceschi-Bicchierai 2015)

3.10 Seurantaviikko 10

Maanantai 09.11.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja osallistua koko päivän kestävään tietoturvapäivä-webinaariin.

Päivä alkoi työpyyntöjonojen läpikäynnillä ja otin selvitettäväkseni työpyynnön, jossa oli havaittu TOR-verkkoliikennettä asiakkaan verkossa. Tarkemmin tutkittaessa totesin yhteyksien olevan käyntejä verkkosivulla, jonka kautta pääsee vierailemaan TOR-verkossa olevilla sivuilla ilman varsinaisen TOR-ohjelmiston asentamista. Verkkosivun kautta oli vierailtu kotimaisella keskustelupalstalla, joka oli ollut viime aikoina otsikoissa, koska sivuston perustaja oli päättänyt lopettaa toimintansa ja oli antanut lopettamiseen liittyen myös haastatteluita uutispalveluille. Totesin ettei kyseessä ollut uhkaa, mutta pyysin Service Deskiä kuitenkin välittämään käyttäjille huomautuksen, ettei TOR-verkossa olevilla sivuilla vierailua sallita asiakkaan verkossa. Mikäli olivat vierailleet sivustolla vahingossa, niin pyysin heitä olemaan tarkkaavaisempia sivustojen kanssa, joissa vierailevat.

Päivä jatkui viikoittaisella tiimipalaverilla, jossa kävimme läpi yhteisten projektien etenemisiä. Lisäksi meitä muistutettiin päivän tietoturvapäivä-webinaarista. Tietoturvapäivä-webinaari alkoikin heti viikkopalaverin jälkeen ja kesti koko päivän ajan. Webinaarin ohessa selvitin kaksi työpyyntöä, joissa oli havaittu epäonnistuneita kirjautumisyrityksiä sekä selvitin kollegan pyynnöstä sinkholeen ohjautunutta liikennettä ja tein siitä selvityspyynnön.

Tiistai 10.11.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi työpyyntöjonojen läpikäynnillä, mutta suurin osa työpyynnöistä oli jo kollegoitteni selvitettävänä ja jäljelle jääneet työpyynnöt eivät kuuluneet tiimini töihin, joten siirsin ne oikeiden tiimien selvitettäväksi. Työpyyntöjen läpikäynnin jälkeen siirryin MISPin kehityksen pariin. Lisäsin MISPiin uuden moduulin, joka osaa rikastaa tapahtumien dataa URLhaus nimisen palvelun kautta. Käytin koko päivän luoden testitapahtumia MISPiin ja kokeilemalla moduulien toiminnallisuutta erilaisilla tunnetuilla haitallisilla osoitteilla. Tutkin myös voisiko MISPin omaa CSVparser-moduulia muokata niin, että sillä voitaisiin käsitellä CSV-tiedostoja hieman monimuotoisemmin.

Keskiviikko 11.11.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi viikoittaisella tiimipalaverilla, jossa kävimme läpi päivän kiireelliset työpyynnöt, yhteisten projektien etenemiset sekä asiakaskohtaisia muutoksia. Palaverin jälkeen kävin läpi työpyyntöjonot, joista otin käsittelyyn kaksi työpyyntöä, joissa selvitin epäonnistuneita kirjautumisyrityksiä. Työpyyntöjen jälkeen siirryin jälleen MISP-projektin pariin. Vietin jälleen koko päivän etsien, tutkien ja testaten MISPin rikastusmoduuleja. Otin testiin muun muassa RiskIQ-nimisen maksullisen threat intelligence -palvelun, joka tarjosi kuukauden mittaista ilmaista kokeilujaksoa. RiskIQ:n tuottama lisätieto vaikutti ensimmäisillä kokeiluilla varsin kattavalta ja hyvältä. RiskIQ:n lisäksi pyysin RecordedFuturelta demoa sähköpostitse, jotta voisin vertailla palveluiden toimintaa.

Torstai 12.11.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti, edistää MISP-projektia ja osallistua kuukausipalaveriin asiakkaan kanssa.

Päivä alkoi työpyyntöjonojen läpikäynnillä. Otin käsittelyyn työpyynnön, jossa asiakkaan käyttäjän työasemalla oli havaittu ohjelma, jonka virustorjunta oli luokitellut hakkerointityökaluksi. Ohjelma on kuitenkin tunnettu myös yleisenä vianselvitystyökaluna, joten pyysin Service Deskiä selvittämään käyttäjältä, oliko ohjelman käyttö hallittua ja mihin tarkoitukseen sitä on käytetty. Annoin myös lisäohjeeksi poistaa työkalu ja ajamaan täyden virusskannauksen, mikäli käyttäjällä ei ollut tietoa ohjelmasta.

Sain aamulla myös kokouskutsun RecordedFuturelta. Kokouksessa oli tarkoitus keskustella palvelun käyttötarkoituksista ja tarpeista. Kokouksen oli määrä tapahtua vielä saman päivän aikana illalla ja minulla oli vapaata illalla, joten hyväksyin kutsun.

Puolen päivän aikaan osallistuin asiakaspalaveriin, jossa kävimme kollegan ja asiakkaan kanssa kuukausittaiset raportit läpi. Asiakaspalaverin jälkeen osallistuin Fujitsun talouskatsauksen läpikäyntiin, sekä osastoni tiedotustilaisuuteen.

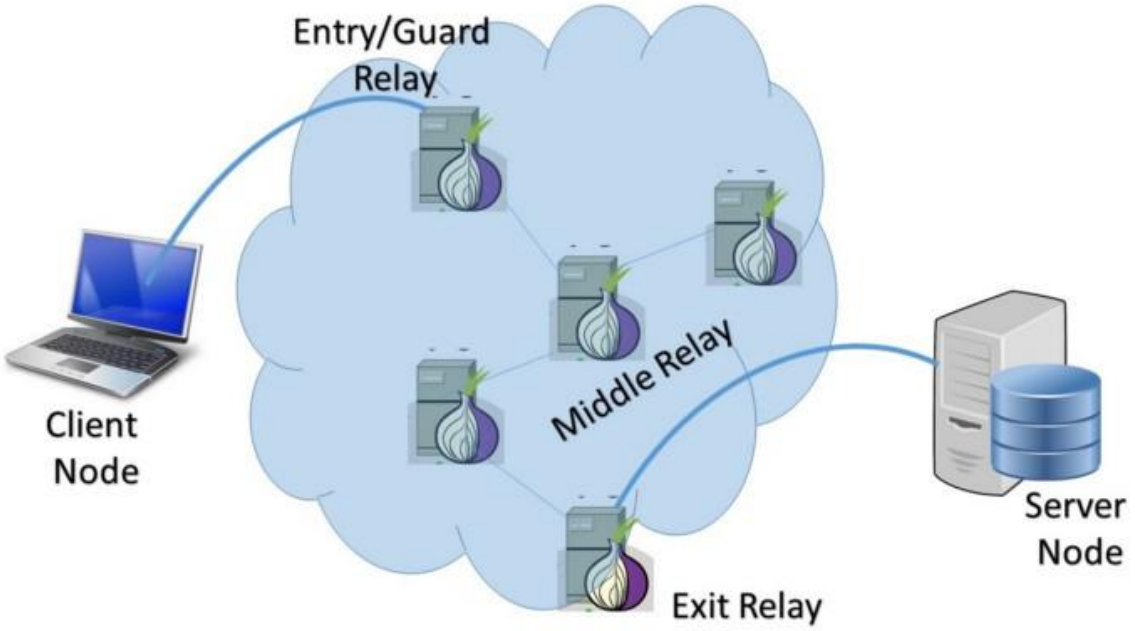
Palaverien jälkeen aloin selvittää työpyyntöä, jossa virustorjunta oli tunnistanut asiakkaan itsekehittämän sovelluksen mahdollisesti haitalliseksi. Koska vastaavia työpyyntöjä on ollut useita aikaisemminkin, ehdotin ratkaisuksi itsekehitettyjen sovellusten digitaalista allekirjoittamista, jolloin ne voitaisiin jatkossa tunnistaa turvalliseksi eivät aiheuttaisi aina hälytystä esimerkiksi sovelluksen päivittyessä. Lähetin ehdotukseni vielä virustorjuntatiimin kautta, jos heillä olisi parempaa ehdotusta ratkaisuksi.

Päivän lopuksi osallistuin vielä RecordedFuturen kokoukseen, jossa kävin heidän työntekijänsä kanssa pikaisen kartoituksen, minkälaista dataa haluaisin heiltä saada. Yritin saada testikäyttäjää, jotta voisin itse arvioida datan käytännöllisyyttä, mutta se ei ollut mahdollista. Työntekijä kuitenkin lupasi yrittää järjestää demotilaisuuden, jossa he esittelevät tuotteen toimintaa.

Perjantai 13.11.2020
Päivän tavoitteena on ratkoa työpyyntöjä mahdollisimman tehokkaasti ja edistää MISP-projektia.

Päivä alkoi puhelulla, jossa kollega pyysi apuani SIEM-järjestelmän toiminnan selvittämisessä. Kollega kertoi ongelmansa ja pyrin auttamaan ja selvittämään ongelman syytä parhaani mukaan. Valitettavasti tietämykseni ja tekemämme tutkinta ei riittänyt ongelman ratkaisuun. Kollega kiitti ajastani ja päätti pyytää SIEMin asiantuntijatiimiltä apua ongelmaansa. Puhelun jälkeen huomasin olevan minun vuoroni käydä SIEM-järjestelmän tapahtumia läpi, joten siirryin niiden läpikäyntiin. Tapahtumista ei löytynyt mitään uutta, joka vaatisi selvitystä. Loppupäivän käytin ajankohtaisten kyberturvaan liittyvien uutisten lukemiseen ja MISPin tutkimiseen.

Viikkoanalyysi
Viikolla tuli selvitettyä jonkin verran uutta asiaa ja olen selvästi kehittynyt itsenäisen työskentelyn ja päätösten teon suhteen. Lisäksi kollegoiden auttaminen ja erityisesti se, että he pyysivät suoraan apuani, nosti itseluottamustani ja käsitystäni tarpeellisuudestani.
Viikolla kohdatuista selvitystöistä voisi nostaa esille maanantaina selvitetyn TOR-liikenne työpyynnön. Vaikka kyseessä oli tällä kertaa selaimen kautta tehty vierailu eikä kohdesivustokaan ole tiedettävästi haitallinen, niin TOR-liikenne voi usein viitata haittaohjelman olemassaoloon. Jotkin haittaohjelmat käyttävät TOR-verkkoa kommunikointiin C2-palvelimien kanssa. TOR-verkko mahdollistaa palvelimen ylläpitämisen verkossa niin, että palvelimen sijaintia tai ylläpitäjää on lähes mahdoton selvittää. TOR-verkon toiminta on mielenkiintoinen konsepti, vaikka tekniikka, jolla lähes jäljittämätön yhteys luodaan, on kuitenkin kohtuullisen yksinkertainen.



Kuvio 4. Yksinkertainen yhteys TOR-verkossa. (medium.com 2018)

Kuten kuvio 4 havainnollistaa niin TOR-verkkoon yhdistävä laite yhdistää aluksi sisääntulopalvelimeen, joka ohjaa yhteyden TOR-verkossa olevien välityspalvelinten kautta ulostulopalvelimelle, joka lopulta yhdistää kohdepalvelimelle. Yhteys siis kiertää monen palvelimen kautta salattuna, joka auttaa yhteyden jäljitettävyyden peittämisessä. TOR-verkon mahdollistama lähes jäljittämätön yhteys on houkutteleva erityisesti haittaohjelmien yhteyksien salaamiseen ja komentopalvelinten piilossa pitämiseen. TOR-verkkoyhteyksien havainnointi on kuitenkin kohtuullisen helppoa, koska yhteyksien pitää poistua TOR-verkosta aina ulostulopalvelimien kautta ja verkosta löytyy useita palveluita, jotka pitävät kirjaa kaikista julkisista TOR-verkon ulostulopalvelimista. Näin ollen yhteydet on helppo estää lisäämällä lista tiedossa olevista ulostulopalvelimista palomuurin estettävien yhteyksien listalle.
(Raja Srivathsav 2018)

Toinen mielenkiintoinen viikolla käsittelemäni työpyyntö oli asiakkaalla havaittu epäilyttävä ohjelma, joka oli kuitenkin asiakkaan itsensä kehittämä sovellus. Ohjelma oli havaittu epäilyttäväksi, koska virustorjuntaohjelmisto ei ollut aiemmin havainnut kyseisellä tunnisteella olevaa ohjelmaa, eikä sovellusta oltu digitaalisesti allekirjoitettu, jotta sen kehittäjä voitaisiin tunnistaa. Koska asiakas kehittää useita omia sovelluksia ja kyseiset sovellukset myös aiheuttavat usein turhia hälytyksiä juurikin edellä mainituista syistä, niin aloin miettimään, miten näitä turhia hälytyksiä voitaisiin vähentää. Mielestäni parhaaksi ratkaisuksi osoittautui nimenomaan ohjelmien digitaalinen allekirjoittaminen. Käytännössä kaikki viralliset ja laajasti käytössä olevat sovellukset käyttävät digitaalista allekirjoitusta, jolla sovelluksen kehittäjä voidaan tunnista turvalliseksi. Koska digitaalista allekirjoitusta on lähes mahdoton väärentää, niin on se siis paras vaihtoehto tässä tilanteessa. Päätin kuitenkin kyseisessä tapauksessa

pyytää vielä virustorjunnan asiantuntijatiimiltä varmistuksen asiasta, koska he tuntevat virustorjunnan ja sen toiminnan paremmin.

4 Pohdinta ja päätelmät

Arvioitaessa kehitystäni opinnäytetyön aikana, voidaan havaita selvää kehitystä itsenäisessä työskentelyssä ja itsenäisten ratkaisujen teossa. Lisäksi erilaisten työkalujen käyttö on muuttunut sulavammaksi ja ratkaisujen löytäminen työpyyntöihin on nopeutunut. Tämän ansiosta työskentelytehokkuuteni on kasvanut merkittävästi. Työpyyntöjen nopeutunut ja itsenäinen selvittäminen on merkki syventyneestä ymmärryksestäni erilaisista tilanteista, joita työssä kohdataan ja kyvystäni soveltaa aikaisempaa oppimaani uusissa ongelmissa.

Myös kollegat ovat pyytäneet apuani useammin opinnäytetyön seuranta-ajanjakson loppupuolella, mikä kertoo myös kollegoiden kasvaneesta luottamuksesta osaamiseeni. Lisäksi seurantajakson loppupuolella on havaittavissa aikaisempaa enemmän painotusta projektien kehittämiseen, kun seurantajakson alkupuolella painotus oli enemmän työpyyntöjen ratkaisemissa ja projektityöskentely oli enemmän sivutoimista työskentelyä. Projektini tuotantoon siirtämisen alustava keskustelu viestii myös kollegoiden luotosta projektini edistymiseen ja kykyihini kehittää projektia. Projektityöskentely todennäköisesti jatkaa kasvuaan ja projektien edetessä ja siirtyessä tuotantoon saatan siirtyä itsekin enemmän kehittämieni projektien ylläpitoon liittyviin tehtäviin.

Päiväkirjamuotoinen opinnäytetyö on auttanut tutkimaan tekemiäni ratkaisuja ja syventämään ymmärrystäni erilaisista tekniikoista ja asioista, joita olen kohdannut työssäni. Erityisesti viikkoanalyyseissä käymäni tekniset ja teoreettiset tarkastelut ovat tuottaneet minulle syvempää ymmärrystä ja auttaneet sisäistämään kyseisten teknologioiden toimintaa. Lisäksi käydessäni läpi aikaisempia päivittäisiä merkintöjä, huomasin työstämieni työpyyntöjen olevan usein kohtuullisen yksinkertaisia ja tuttuja tapauksia, vaikka tarjolla olisi saattanut olla monimutkaisempia ja haastavampia työpyyntöjä. Opinnäytetyön loppupuolella pyrin ottamaan enemmän haastavampia työpyyntöjä, koska tutuissa ja turvallisissa selvityksissä oma osaamiseni ei tule kehittymään.

Aion myös opinnäytetyön jälkeen jatkaa haastavampien ja minulle mahdollisesti tuntemattomampien ongelmien selvittämistä ja pyytää kollegoilta tarpeen tullen apua, jotta pystyn laajentamaan omaa osaamistani. Harkitsen myös jatkavani päiväkirjatyyppisten muistiinpanojen kirjoittamista, mutta vähemmän yksityiskohtaisesti, jotta voin myöhemmin aina arvioida omaa toimintaani ja läpikäymiäni asioita. Jatkuva oman toiminnan arvioiminen saattaa auttaa sisäistämään käsittelemiäni asioita myös jatkossa ja voi auttaa löytämään epäkohtia omassa toiminnassani tai jopa ongelmia työpaikalla käytetyissä prosesseissa. Jos löydän oman toiminnan arvioinnilla ongelmia työskentelytavoissani tai ratkaisuissani, niin pystyn miettimään parempia toimintatapoja ja parantamaan itseäni työntekijänä. Samoin jos löydän ongelmia työpaikalla olevista prosesseista, voin tuoda ongelmat esiin esimiehelleni tai asiaankuuluville sidosryhmille. Lisäksi voin tuoda esiin omia ratkaisuehdotuksiani ja näin ollen mahdollisesti helpottaa kaikkien työskentelyä työpaikallani.

Opinnäytetyön aikana olen oppinut kommunikoimaan paremmin kollegoiden ja sidosryhmien kanssa sekä hyödyntämään erilaisten sidosryhmien asiantuntevuutta erilaisista järjestelmistä ja tietoteknisistä osa-alueista. Opinnäytetyön aikana olen oppinut esittelemään projektiani muille ja pyytämään mielipiteitä edistymisestä. Tämän johdosta kollegani ovat kyselleet ja ehdotelleet parannuksia tai muutoksia projektiini. Kohtasin myös haasteita projektin integroinnissa muihin järjestelmiin ja pyrin ratkaisemaan ongelmia itse, vaikka oma osaamiseni integroitavista järjestelmistä oli kohtuullisen rajoittunut. Opin opinnäytetyön aikana kuitenkin hyödyntämään integroinnin kohteen tuntevaa asiantuntijatiimiä ja pyytämään heiltä apua ongelman selvittämisessä. Yhteistyö sidosryhmien kanssa on auttanut jakamaan työtaakkaa ja samalla lieventämään stressiä, kun tiedän ettei projekti kokonaisuudessaan ole vain minun vastuullani.

Yhteenvetona voisin tiivistää oppineeni opinnäytetyön aikana runsaasti erilaisia asioita ja kasvaneeni kyberturva-asiantuntijana ja yleisesti työntekijänä. Lisäksi opinnäytetyö on tuonut esiin projektiin suuntautuvuutta työssäni ja auttanut minua analysoimaan viikolla käsittelemiäni asioita ja syventämään ymmärrystäni niistä. Hyödyntämällä opinnäytetyössä käytettyjä tekniikoita ja tapoja pystyn jatkossakin analysoimaan omaa toimintaani ja kohtaamiani ongelmia, sekä kehittämään itseäni työntekijänä näiden ongelmien pohjalta. Uskon kaikesta opinnäytetyön aikana oppimastani olevan hyötyä tulevaisuudessa, vaikka vaihtaisin joskus rooliani tai työpaikkaa.

Lähteet

NIST 2012. Computer Security Incident Handling Guide
Luettavissa: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Sanastokeskus TSK ry 2018. Kyberturvallisuuden sanasto.
Luettavissa: https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

BackwardLogic 2018. Directory Brute Force Attacks Are Not Dead!
Luettavissa: http://www.backwardlogic.com/directory-brute-force-attacks/
Luettu: 13.9.2020

Raj Chandel's Blog 2018. Comprehensive Guide on Dirbuster Tool.
Luettavissa: https://www.hackingarticles.in/comprehensive-guide-on-dirbuster-tool/
Luettu: 13.9.2020

Trend Micro. Indicators of compromise.
Luettavissa: https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise
Luettu: 13.09.2020

PaloAlto Networks. Command and Control Explained.
Luettavissa: https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained
Luettu: 13.9.2020

Tom Tervoort 2020. Zerologon: Unauthenticated domain controller compromise by subverting Netlogon cryptography (CVE-2020-1472)
Luettavissa: https://www.secura.com/pathtoimg.php?id=2055
Luettu: 18.09.2020

Dblackhgurst 2016. Do you know where your data's being held?
Luettavissa: https://www.ukbusinessforums.co.uk/articles/do-you-know-where-your-datas-being-held.339/
Luettu: 20.09.2020

Lily Hay Newman 2018. Hacker Lexicon: What Is Sinkholing?
Luettavissa: https://www.wired.com/story/what-is-sinkholing/
Luettu: 27.09.2020

Forcepoint 2013. WebShells WebShells on the Web Server.
Luettavissa: https://www.forcepoint.com/blog/x-labs/webshells-webshells-web-server
Luettu: 27.09.2020

Microsoft Documentation 2020. What is Azure Sentinel?
Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/overview
Luettu: 27.09.2020

Marcin Teodorczyk. Understanding Privilege Escalation.
Luettavissa: https://www.admin-magazine.com/Articles/Understanding-Privilege-Escalation
Luettu: 04.10.2020

Evan Porter 2019. What is Adware? And How to Remove It in 2020
Luettavissa: https://www.safetydetectives.com/blog/what-is-adware-and-how-to-remove-it-in/
Luettu: 11.10.2020

David Benjamin 2018. Modernizing Transport Security
Luettavissa: https://security.googleblog.com/2018/10/modernizing-transport-security.html
Luettu: 11.10.2020

ENISA. Incident Handling Automation
Luettavissa: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
Luettu: 18.10.2020

Chris Hoffman 2017. What Is “SmartScreen” and Why Is It Running on My PC?
Luettavissa: https://www.howtogeek.com/320711/what-is-smartscreen-and-why-is-it-running-on-my-pc/
Luettu: 25.10.2020

Wayne Rash 2019. How to Block Unauthorized VPNs.
Luettavissa: https://uk.pcmag.com/feature/120077/how-to-block-unauthorized-vpns
Luettu: 09.11.2020

Lorenzo Franceschi-Bicchierai 2015. Your Tool to Access Netflix Content Abroad Is Hijacking Your Internet Connection.

Luettavissa: https://www.vice.com/en/article/pga9yk/your-tool-to-access-netflix-content-abroad-is-hi-jacking-your-internet-connection
Luettu: 09.11.2020

Raja Srivathsav 2018. TOR Nodes Explained!
Luettavissa: https://medium.com/coinmonks/tor-nodes-explained-580808c29e2d
Luettu: 16.11.2020