Päiväkirjamuotoinen opinnäytetyö tietoturva-asiantuntijan kehittymisestä

Markus Björklund

2019 Laurea

Laurea-ammattikorkeakoulu

Päiväkirjamuotoinen opinnäytetyö tietoturva-asiantuntijan kehittymisestä

Markus Björklund
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Joulukuu, 2019

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutusohjelma
Tradenomi (AMK)

Markus Björklund

Päiväkirjamuotoinen opinnäytetyö tietoturva-asiantuntijan kehittymisestä

Vuosi 2019 Sivumäärä 75

Päiväkirjamuotoisessa opinnäytetyössä seurataan tietoturva-asiantuntijan työtä tietoturvaan erikoistuneen ICT-alan asiantuntijayrityksessä kymmenen viikon ajan. Opinnäytetyössä kuvataan työtehtävässään uuden asiantuntijan ammatillisen osaamisen kehittymistä ja kasvua vastuualueensa työroolissa. Työviikkojen työpäivistä kirjoitettiin päiväkirjaa, ja työviikot kokonaisuudessaan analysoitiin viikkoyhteenvedoissa.

Opinnäytetyön aikana yhtenä työtehtävistä oli tietoturvapalvelimien ylläpito- ja kehitystyö, ja opinnäytetyössä käsitellään palvelimien ylläpitotyössä havaittuja haasteita. Opinnäytetyössä myös tutustuttiin yrityksen perehdytysprosessiin uuden työntekijän näkökulmasta, ja tehtiin havaintoja perehdytyksen laajuudesta ja laadusta.

Työviikkojen jälkeisissä viikkoanalyyseissä käsiteltiin työviikkoja ja viikkojen aikana kohdattuja asioita ammatillisen osaamisen kehittymisen kannalta. Opinnäytetyön tietoperustaa rakennettiin täydentämällä viikkoanalyysien sisältöä teoreettisella sisällöllä tietojärjestelmien pääkäyttäjämateriaaleista, sekä muista sähköisistä lähteistä ja nettisivustojen sisällöistä kerätyllä materiaalilla.

Opinnäytetyön aikana havaittiin merkittävää ammatillisen osaamisen kehittymistä ja kasvua. Opinnäytetyön alkutilanteeseen verrattuna, ammatillinen osaaminen kasvoi kymmenessä viikossa tasolle, missä omalla vastuualueella kyettiin suoriutumaan asiantuntijaroolissa. Yrityksen tavassa hoitaa tietoturvapalvelimien ylläpito- ja kehitystyötä havaittiin haasteita, ja vielä opinnäytetyön aikana ylläpitovastuu järjestettiin uudelleen yhdelle nimetylle vastuuhenkilölle. Yrityksen tavassa perehdyttää uusi työntekijä havaittiin opinnäytetyötä tehtäessä selkeitä kipukohtia, ja näiden kohtien parannusehdotuksia on käsitelty tässä opinnäytetyössä.

Asiasanat: tietoturva, perehdytys, kehittyminen

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's degree

Markus Björklund

A Diary Thesis on Professional Development as a Cyber Security Specialist

Year 2019 Pages 75

This diary thesis follows the work of a Cyber Security Specialist in an ICT company for a period of ten weeks. The thesis describes the professional growth and development of a specialist in a new role. Working days were described in the diary, with weekly summaries analyzing the week.

During the thesis, one task was to maintain and develop Information Security servers, and the thesis covers the challenges discovered in maintaining the servers. The thesis also examines the familiarization process of the company from the point of view of a new employee. Observations were made of the extent and quality of the familiarization provided.

Topics encountered during the working days were analyzed in the weekly summaries from the point of view of professional development. The theoretical framework of the thesis was created by supplementing weekly summaries with content and material from technical documents, electronic publications and web pages.

Significant professional growth and development was identified during the thesis project. After ten weeks professional competence had improved to the required level for a Cyber Security Specialist. Challenges were discovered in the company's processes in maintaining Information Security servers. During the thesis the responsibility for maintenance of the servers was appointed to a new person. Issues were found in the familiarization process of the company and improvements were suggested in the thesis.

Keywords: Information Security, familiarization, development

Sisällys

1 Johdanto

Tämän opinnäytetyön tavoitteena on seurata työtäni, työssä oppimista ja osaamisen kehittymistä tietoturva-asiantuntijana tietoturva-alan yrityksessä. Opinnäytetyö toteutetaan päiväkirjamuotoisena, ja se sisältää 10 viikon ajalta kuvauksia päivittäisistä työtehtävistä ja viikoittaisia analyysejä linkitettynä osaamisen kehittämisessä tarvittuun ammattikirjallisuuteen ja dokumentaatioon.

Opinnäytetyö toteutetaan vuoden 2019 syksyllä, 10 viikon aikana, välillä 12.9.-13.11.2019.

Opinnäytetyö suoritetaan työn ohessa, tietoturva-asiantuntijan työpaikalla. OptimeSys on tietoturvaan erikoistunut n. 60 työntekijän ICT-alan asiantuntijayritys, joka pitää huolta asiakkaidensa IT-ympäristöjen toimivuudesta ja tietoturvasta.

2 Nykytilanne

2.1 Nykyinen työ ja osaaminen

Työni koostuu yrityksen asiakasyritysten tietoturvatuotteiden ylläpidosta ja kehitystyöstä. Työtehtäviäni ovat yrityksemme ja asiakkaidemme käytössä olevan tikettijärjestelmän kautta saapuneiden työ- ja muutospyyntöjen hoitaminen, sekä tietoturvatuotteiden asennus-, ylläpito- ja kehitystyöt.

Työtehtävässäni tarvitsen yleistä osaamista tietoturvatuotteiden ja haittaohjelmien toiminnasta. Syvällisempää osaamista tarvitaan yrityksemme tuotteistamista Trend Micro OfficeScan- ja Apex One –tietoturvatuotteista. Asiakkaiden tietoturvaratkaisuiden kehitystyössä tarvitsen tarkempaa tietoa asiakasyritysten prosesseista ja toimintaympäristöstä. Työtehtävissäni tarvitsen taitoina mm. kykyä selvittää asiakkaiden tarpeet, ja osaamista tarjota näihin tarpeisiin sopivia ratkaisuja.

Oman osaamisen arviointi

Aloitin työpaikassani muutama kuukausi sitten, ja tästä syystä minulle on kertynyt Trend Micro -tietoturvatuotteista vasta vähäinen kokemus. Yleisemmin tietoturvatuotteiden ylläpidosta minulla kuitenkin on yli 15 vuoden kokemus, ja suoriudun tyypillisistä työtehtävistäni itsenäisesti. Ongelmanselvitys- ja kehitystyöt vaativat toistaiseksi minua ohjaavan kollegan tukea.

Olen kehittänyt nykyisessä työtehtävässäni osaamistani tutustumalla Trend Micron tietoturvatuotteisiin, sekä kokeneemman työntekijän opastuksella suorittanut yhä vaativampia, osaamistani kartuttavia tehtäviä.

2.2 Sidosryhmät

Sisäisiin sidosryhmiini kuuluvat yrityksen myynti- ja asiakastukiorganisaatio. Ulkoisiin sidosryhmiin kuuluvat asiakkaat, ja tietoturvatuotteiden päämiehet asiantuntija, tuki- ja myyntiorganisaatioineen.

2.3 Vuorovaikutustaidot

Uutena työntekijänä kohtaan tilanteita, missä tarvitsen kokeneemman työkaverin apua ja ohjausta työssäni. Työkaverini tarvittaessa opastaa minua työtehtävässäni, tai ohjaa minut itsenäisesti etsimään tarvitsemaani tietoa.

Asiakaspalvelutilanteessa on tärkeää selvittää ongelman tai kehitystarpeen kokonaiskuva. Kehitystyössä on osattava tarkoin selvittää asiakkaan tarve ja tarjottavan ratkaisun sopivuus asiakkaalle.

2.4 Kehittäminen

Yritys on elänyt voimakkaan kasvun aikaa, ja kiireessä osa kehitystyöstä on siirretty odottamaan rauhallisempaa hetkeä. Aloitettuani, minulle on kohdistettu aiemmin odottamaan jääneitä kehitysprojekteja. Päiväkirjassani tulen kuvaamaan mm. tietoturvatuotteille tekemääni versiopäivitystyötä, sekä asiakasympäristössä tapahtuvia tietoturvatuotteiden versiopäivityksiä, että asiakkaiden tietoturvapolitiikoiden kehitystyötä.

2.5 Opinnäytetyön tavoitteet

Opinnäytetyössä tulen kuvaamaan Trend Micro OfficeScan- ja Apex One –tietoturvatuotteisiin tutustumisen ja osaamisen kehittämisen, sekä tietoturvapalvelimen ylläpito- ja päivitystyön. Opinnäytetyössä kuvataan myös sekä asiakkaille suoritettavia tietoturvatuotteiden versiopäivitystöitä, että tietoturvapolitiikoiden kehittämistöitä.

Opinnäytetyön aikana dokumentoin tietoturvapalvelimen päivitystyön, mistä yritys saa opinnäytetyöni seurauksena valmiin ohjeistuksen em. palvelimen päivitystyöhön.

3 Päiväkirjaraportointi

3.1 Viikko 1

Maanantai

Maanantaina tavoitteeni on aloittaa tutustuminen Trend Micron OfficeScan ja Apex One –tietoturvatuotteisiin. Olen työurani ajan ylläpitänyt tietoturvatuotteita, mutta nämä työasemaympäristöjen haittaohjelmilta suojaamiseen tarkoitetut tuotteet ja niiden ominaisuudet ovat minulle tuntemattomia. Työtehtäviini minua perehdyttävä kollega opastaa minut hakemaan tietoa Trend Micron internet-sivustolta. Tämän lisäksi saan tietokoneeni selaimeen hänen keräämänsä tärkeiksi tai hyödyllisiksi muodostuneet selainlinkit mm. tietoturvatuotteiden dokumentaatioon ja yrityksemme tietoturvapalvelimille.

Esimieheni kanssa käydyn keskustelun perusteella olen saanut näkemyksen, että yrityksessämme on käytössä oppimistapa, missä työtekijät itse oppivat työtä tehdessään. Ongelmien ja uusien asioiden selvittelyssä tärkeänä pidetään itseohjautumista, sekä tiedon itsenäistä etsimistä ja uuden omaksumista.

Kollegani opastuksella löydän Trend Micron internet-sivustolta OfficeScan- ja Apex One –tietoturvatuotteiden dokumentaatiota, mitä alan läpikäydä. Pyrin ensin muodostamaan yleiskatsauksen tuotteista ja niiden ominaisuuksista, ja aloitan tutustumiseni sivuilta löytyvistä markkinointimateriaaleista ja esitteistä. Opin päivän aikana, että OfficeScan on tuotteena vielä käytössä, mutta sen rinnalle on julkaistu uudempi ja ominaisuuksiltaan kehittyneempi Apex One -tietoturvatuote. Yrityksemme tuottaa tietoturvapalveluita asiakkaille molemmilla näillä tuotteilla, mutta tulevaisuudessa asiakkaamme tullaan siirtämään käyttämään Apex One –tuotetta.

Tiistai

Jatkan tiistaina tuotteisiin ja niiden ominaisuuksiin tutustumista. Kollegani tekee tänään minulle käyttöoikeudet tietoturvapalvelimien hallintaympäristöihin. Tarkistamme yhdessä, että käyttöoikeudet toimivat, ja kirjautumiseni palvelimille onnistuu.

Jatkan dokumentaation läpikäymistä aamupäivän ajan. Huomaan, että helposti omaksuttavaa materiaalia ei juurikaan ole, vaan joudun käyttämään oppimateriaalinani pääkäyttäjille tarkoitettua monisataasivuista dokumentaatiota. Kollega opastaa minut yrityksemme verkkolevyllä olevaan materiaaliin, missä on listattuna asiakkaamme ja tietoturvapalvelimemme. Opin samalla, että pienemmät asiakkaamme on koottu muutamalle, näiden asiakkaiden kesken jaetulle tietoturvapalvelimelle, isoimpien asiakkaiden käyttäessä asiakaskohtaisia tietoturvapalvelimia.

Kollega ohjaa minut tutustumaan Trend Micron dokumenttiin, missä esitellään kovennetun tietoturvapolitiikan suositusasetuksia. Asiakaskohtainen tietoturvapolitiikka määrittää asiakkaan tietoturvatuotteen asetukset, kuten esimerkiksi mihin vuorokauden aikaan ajastettu haittaohjelmatarkistus suoritetaan tietokoneella. Huomaan tämän dokumentin olevan hyvin tiivistetyssä ja helposti omaksuttavassa muodossa.

Keskiviikko

Keskiviikon aamupäivän jatkan tietoturvatuotteisiin tutustumisella. Pääkäyttäjille suunniteltu dokumentaatio sisältää kaiken tuotteen asennuksesta ylläpitoon ja päivittämiseen, mutta yksittäisen tiedon etsiminen ja löytäminen ei dokumentin valtavan koon takia ole helppoa. Käytän hetken aikaa Trend Micron sivuilla, etsien muita mahdollisia tuotedokumentteja.

Juttelemme kollegani kanssa käytössä olevien tuotteiden toimintavarmuudesta, sekä aiemmista ohjelmisto-ongelmista ja ratkaisuista niihin. Saan kuulla, että työtehtävässäni tarvitsen kumppanitunnukset Trend Micron portaaliin, mutta näitä tunnuksia ei ole vielä minulle tehty. Tunnuksillani pääsisin käsiksi ohjelmistotoimittajan tuki- ja koulutusmateriaalipankkiin. Kysyn tietoturvaosaston esimieheltä, mitä kautta saisin tilattua itselleni em. tunnukset.

Iltapäivällä kollegani opastaa minua OfficeScan- ja Apex One –ohjelmistojen asentamisessa tietokoneille. Opin tärkeänä tietona sen, että jokaisella tietokoneelle on asennettu tietoturvaohjelmiston hallinta-agentti, ja tämä agentti ylläpitää tietokoneen tietoturvaohjelmiston yhteyttä tietoturvapalvelimeen. Agentin vikaantuessa, tietokone menettää yhteyden tietoturvapalvelimeen, missä tapauksessa tyypillinen ja toimiva ratkaisukeino on uudelleenasentaa tietokoneen hallinta-agentti.

Läpikäymme kollegan kanssa Trend Micron ohjelmistotyökalua, millä tietokoneen tietoturvaohjelmisto voidaan poistaa tietokoneelta. Iltapäivällä suoritan kokeiluja testitietokoneella, testaten tietoturva-asennuksen poistoa ja eri asennuspakettiversioiden käyttöä ohjelmistoa asennettaessa.

Iltapäivän lopuksi läpikäymme kollegani kanssa asiakas A:n tietoturvapolitiikkaa, ja suoritan asiakkaan yritykseltämme tilaaman tietoturvapolitiikan asetusmuutoksen.

Torstai

Aamulla avustan toista kollegaani selvittääksemme asiakas B:n toimialueelta löytyviä tietokonetilejä. Tämä työtehtävä on minulle työhistoriastani tuttu, ja saan tuotettua kollegani tarvitseman tiedon.

Aamupäivällä läpikäyn asiakkaiden käytössä olevia jaettuja tietoturvapalvelimia. Palvelimemme ovat kolmea eri tuoteversiota, ja selvitän Trend Micron sivustolta kuhunkin palvelimeen tarvittavat päivityspaketit, ja tutustun samalla näiden asennuspakettien asennusohjeisiin. Totean uusimpiin saatavilla oleviin päivityspaketteihin vertaamalla palvelimiltamme puuttuvan versiopäivityksiä.

Opin tänään, että palvelimelle tehtävä päivitys päivittää myös kyseiseen palvelimeen yhteydessä olevat tietokoneiden hallinta-agentit. Opin myös, että ennen palvelimen päivittämistä, palvelimelta kytketään päälle agenttien päivitysjakeluiden esto. Ilman tätä asetusta agentit, huomattuaan palvelimella olevan uuden agenttiversion, aloittavat lataamaan uutta agenttiversiota, ja päivittävät itsensä uuteen versioon. Jos palvelimelle yhteydessä olevat sadat tai tuhannet agentit kaikki lataavat uutta versiota samaan aikaan, kuormittuu sekä asiakkaiden että palvelimiemme resurssit tarpeettomasti.

Iltapäivällä opiskelen asiakkaille tarjottavia päivitystapoja siirryttäessä OfficeScan-tuotteesta Apex One -tuotteeseen. Selvitän, mitkä OfficeScan-agenttiversiot ovat yhteensopivia ja kykenevät kommunikoimaan Apex One –palvelimen kanssa.

Perjantai

Perjantaiaamu alkaa tietoturvaosaston kokouksella, missä läpikäydään asiakkaiden projektien tilannetta, minkä jälkeen käsitellään osaston muita asioita. Jatkan kokouksen jälkeen torstaina aloittamaani OfficeScan-agenttiversioiden päivityspolkujen ja agenttien yhteensopivuuden selvitystyötä.

Iltapäivällä jatkan agenttiversioiden ja Microsoft Windows 10 –ominaisuuspäivitysten yhteensopivuuden selvitystä. Ominaisuuspäivitys on Windows 10 –käyttöjärjestelmän versiopäivitys, mikä tyypillisesti sisältää uusia ominaisuuksia, mutta myös käyttäjälle näkymättömäksi jäävää käyttöjärjestelmän kehitystyötä. Ominaisuuspäivitykset vaativat tietokoneelta ajantasaisia laiteajureita, mutta myös asennettujen ohjelmistojen pitää olla yhteensopivia uuden Windows-version kanssa. Myös Trend Micron hallinta-agentista julkaistaan uuden Windows 10 –ominaisuuspäivityksen kanssa yhteensopiva versio, mutta Trend Micro kykenee tuotetestaamaan ja julkaisemaan uuden version tyypillisesti vasta muutaman viikon kuluttua Windows 10 -ominaisuuspäivityksen julkaisun jälkeen.

Loppuiltapäivästä selvitän asiakas C:n hallinta-agenttien sijaintia eri tietoturvapalvelimilla. Käynnissä on projekti, missä asiakkaan OfficeScan-asennukset päivitetään Apex One –asennuksiksi, ja tätä varten selvitän eri palvelimilla olevien agenttien kappalemäärät.

Viikkoanalyysi 1

Viikon aikana jouduin oppimaan paljon uutta, mutta kykenin hyödyntämään myös aiemmin työurallani omaksumaani osaamista. Sain muodostettua itselleni yleissilmäyksen Trend Micron tietoturvapalvelintuotteista, ja pääsin suorittamaan ensimmäistä asiakkaalle tehtävää tietoturvan asetusmuutostyötä. Yrityksellläni ei ole tietoturvapalvelimista omaa perehdytysmateriaalia, eli jouduin oppimisessa hyödyntämään ohjelmistovalmistajan tuottamaa materiaalia. Työurani aiempi kokemukseni toisen ohjelmistotuottajan tietoturvatuotteista auttoi minua uuden oppimisessa.

Perehdyttämisellä tarkoitetaan niitä toimenpiteitä, joiden avulla uusi työntekijä oppii tuntemaan työpaikkansa, sen tavat, ihmiset, sekä omaan työhön liittyvät odotukset. Työnopastukseen kuuluvat ne asiat, jotka liittyvät itse työhön ja sen tekemiseen. Näitä ovat esimerkiksi mistä osista ja vaiheista työ koostuu, ja mitä osaamista ja tietoa työ edellyttää (Työturvallisuuskeskus, 2019). Työsuojelulainsäädännöissä on työnantajaa velvoittavia määräyksiä perehdyttämisen järjestämiseksi. Käytännössä yrityksessä lähin esimies vastaa perehdyttämisestä ja opastamisesta, joko itse tehden tai delegoiden tehtävät toisille henkilöille.

Perehdytyksessä oppimista tukeva dokumentaatio auttaisi itseoppimisessa. Yrityksellä on olemassa dokumenttipankki esimerkiksi yrityksen henkilöstöasioita varten, mutta tietoturvapalvelimien perusylläpitoon ei ole olemassa dokumentaatiota. Ainoat saatavilla olevat dokumentit ovat ohjelmistotoimittajan pääkäyttäjille tarkoitettuja, ja näiden omaksumisessa on työssään aloittelevalle henkilölle korkea oppimiskynnys.

Viikon aikana olen huomannut, että yrityksemme tapa perehdyttää uusi työntekijä riippuu vahvasti perehdyttävästä henkilöstä. Minun tapauksessani perehdytystä tekevä henkilö on asiaosaamisessa taitava, ja osaa kouluttaessaan jakaa uuden tiedon sopivan kokoisiin osiin oppimisen varmistamiseksi. Yrityksessä perehdytystä ei ole tuotteistettu, eli perehdyttävä henkilö itse muodostaa läpikäytävät aihekokonaisuudet, ja näin on mahdollista, että osa perehdytettävälle tärkeästä aiheesta jää käsittelemättä.

Perehdytyksen ja opastuksen tueksi tulisi yrityksen tehdä kirjallinen suunnitelma, millä voidaan seurata työntekijän perehdytyksen etenemistä. Etukäteen tehty suunnitelma säästää aikaa, ja toimii tärkeiden asiakohteiden muistilistana (Työturvallisuuskeskus, 2019). Lisäksi esimerkiksi uusien henkilöiden kohdalla kaikkia tarvittavien käyttöoikeuksien tilauksia ei ole etukäteen tehty, vaan tiettyjä käyttöoikeuksia joudutaan odottamaan. Kuten perehdytyksen aihelista, myös tarvittavien käyttöoikeuksien lista pitäisi luoda uusia käyttäjiä varten. Näin tunnukset tulisi tilattua, olisivat nopeasti käyttövalmiina, ja käyttöoikeuksia edellyttävä työ voisi alkaa aiemmin.

3.2 Viikko 2

Maanantai

Asetan viikon tavoitteeksi jatkaa tutustumista Trend Micro OfficeScan- ja Apex One –tietoturvapalvelimiin. Tämän lisäksi tulen osallistumaan asiakkaiden tietoturvan kehitysprojekteihin. Aloitan maanantain tutustumalla yhteen asiakkaille jaetuista tietoturvapalvelimista. Palvelimen Windows-palvelinkäyttöjärjestelmän tuki on muutaman kuukauden kuluttua päättymässä, ja tätä ennakoiden kyseinen palvelin on jo poistettu tuotantokäytöstä. Palvelimella olleet asiakkaiden tietoturva-agentit on myös jo siirretty toisille palvelimille.

Tietoturvapalvelimen versiotietoja Trend Micron internet-sivuston päivitystietokantaan vertaamalla totean palvelimelta puuttuvan uusimman korjauspäivityksen. Koska palvelin on jo poistettu tuotantokäytöstä, voin suorittaa palvelimen päivityksen uusimpaan versioon ennen tuotantopalvelimien kuukausittaista huoltokatkoa. Tutustun päivitystietokannasta löytyviin asennusohjeisiin, ja totean ne läpikäyden päivityksen helpoksi tehdä.

Saan kollegaltani tarvitsemani tiedot kyetäkseni kirjautumaan VMware-virtualisointiympäristöön. Teen virtualisointiympäristön hallinnassa palvelimelle varmistuksen ennen päivityksen aloittamista. Päivityksen epäonnistuessa, palvelin voidaan palauttaa varmistuksen aikaiseen tilaan. Päivityksen suoritan etätyöpöytäyhteyden yli, minkä jälkeen tarkistan tietoturvapalvelimen toiminnan mahdollisten ongelmien varalta.

Iltapäivällä tutustun toisten tietoturvapalvelimien päivitystilanteeseen. Kuten aamupäivällä, vertaan jälleen palvelimien versiotietoja internet-sivustolta löytyviin versioihin. Totean muutaman palvelimen tarvitsevan päivityksiä, ja läpikäyn tilannetta kollegani ja tietoturvaosaston esimiehen kanssa. Opin, että useammalla tietoturva-asiantuntijalla on vastuu ylläpitää palvelimia, mutta palvelimille ei ole nimetty yhtä vastuullista henkilöä, kenen tehtävänä ja vastuulla olisi varmistaa palvelimien ajantasaisuus.

Tiistai

Jatkan aamusta tietoturvapalvelimien päivitysten selvitystyötä, ja esimieheni pyynnöstä kirjoitan samalla dokumentaatiota palvelimien päivitysten tilasta. Valmistelen alustavasti tulevia päivitystöitä lataamalla päivitystiedostot ja asennuksiin liittyvät ohjedokumentaatiot saataville verkkolevyasemalle.

Keskipäivällä, Jatkuvien tietoturvapalveluiden kokouksessa, läpikäymme asiakasprojektien tilannetta. Huomaan että kokous tarjoaa minulle hyvän tilaisuuden oppia sekä asiakkaistamme että projektien etenemisestä.

Iltapäivällä saan kollegaltani pyynnön tarkistaa, miksi Windows-käyttöliittymästä näyttää puuttuvan loppukäyttäjän mahdollisuus suorittaa haittaohjelmatarkistus kansiolle tai tiedostolle. Totean, että myös omalta tietokoneeltani puuttuu tämä kyseinen ominaisuus. Aloitan asian selvittämisen tietoa etsimällä Trend Micron internet-sivuston tukiosiosta. Ratkaisun löytymistä pitkittää sivuston oman hakutoiminnallisuuden rajoittuneisuus, sillä vasta tarkan hakutermin selvitettyäni löydän sivustolta etsimäni tiedon.

Totean, että käyttäjäkohtainen asetus on kytkettävissä päälle, mutta sitä ei jostain syystä ole otettu käyttöön asiakkaiden tietoturvapolitiikoissa. Kohdistan tietoturvapalvelimelta kyseisen asetuksen testimielessä ensin omalle tietokoneelleni, ja agenttini vastaanotettua palvelimelta nämä uudet asetukset, toteamme kollegani kanssa, että asetus on oikein kytkeytynyt käyttöön, ja se voidaan levittää kaikille asiakkaillemme.

Tiistaipäivän lopuksi listaan tietoturvapalvelimelta asiakas D:n agenttien määrän. Tietoa tarvitaan myöhemmin viikolla käynnistyvässä asiakkaan agenttien siirtoprojektissa.

Keskiviikko

Aamu alkaa tarkistamalla asiakas D:n tietoturva-agenttien määrät ja tilatiedot sekä nykyiseltä että uudelta tietoturvapalvelimelta. Listaan molemmilta palvelimilta löytyvät agentit, ja vertailemalla näitä keskenään, löydän usean agentin kaksoiskappaleen: Nämä ovat nykyiseltä palvelimelta uudelle siirrettyjä agentteja, mitkä ovat olemassa molemmilla palvelimella. Tarkistamalla agenttien uusimmat yhteydenottopäivämäärät, voin todeta uudella palvelimella olevat agentit aktiivisiksi, ja poistan nykyiseltä palvelimelta tarpeettomiksi käyneet agentit.

Aamupäivän aikana osallistun asiakas A:n ongelmanselvitystyöhön: Asiakkaan ympäristössä monitoimilaitteen sähköpostitse lähettämiä dokumenttiskannauksia on huomattu kadonneen, ja tehtäväni on tarkistaa, johtuuko katoaminen asiakkaalle tuottamamme tietoturvapalvelun luokitellessa sähköposteja virheellisesti roskaposteiksi.

Ongelmanselvitystyö jatkuu iltapäivälle. Kysyn kollegaltani ongelmanselvitystyössä tarvitsemaani lisätietoa, ja läpikäyn tietoturvapalvelimen keräämiä lokitietoja. En selvitystyössäni löydä jälkiä siitä, että asiakkaan sisäisesti lähetettyjä sähköposteja olisi luokiteltu ja estetty roskapostina. Totean asiakkaalle, ettei syy sisäiseen sähköpostien katoamiseen ole tässä tapauksessa ole tietoturvapalvelussamme.

Valmistelen jaettujen tietoturvapalvelimien tulevaa päivitystyötä kytkemällä palvelimilta tietoturva-agenttien päivitysjakelun pois päältä. Päivityksen jälkeen agentit havaitsisivat päivityksen jälkeen palvelimella odottavan uuden version, ja päivittäisivät itsensä. Koska palvelimilla voi olla jopa tuhansia agentteja, hallitsematon päivitysten jakelu kuormittaisi sekä palvelinta, tietoliikenneyhteyksiä, että asiakkaiden omia tietojärjestelmiä.

Teen edellisen ohessa muutostyöpyynnön palvelimien päivityksestä yrityksemme infra-ryhmälle. Pyynnössä käsitellään tulevan muutostyön sisältö ja aikataulu, muutostyön arvioidut riskit, palautumissuunnitelma, muutostyöhön tarvittavat resurssit yms. Muutostyö voidaan suorittaa vasta muutostyöpyynnön hyväksymisen jälkeen.

Torstai

Aloitan torstain jatkamalla tutustumista jaettuihin tietoturvapalvelimiin. Läpikäyn asiakkaille rakennettuja tietoturvasääntöjä, ja vertailen käytössä olevia sääntöjä Trend Micron omaan, kovennettujen tietoturva-asetusten dokumenttiin. Totean että yritysten käytössä olevat säännöt poikkeavat toisistaan jonkin verran, ja asiakaskohtaisia määrityksiä esimerkiksi tiettyjen tiedostokansioiden haittaohjelmatarkistusten ohittamiseen on rakennettu muutamia kappaleita. Tehtyjä muutoksia ei kuitenkaan ole dokumentoitu helposti löydettävästi, eikä tietoturvasäännöissä ole esimerkiksi tekstikenttiä, minne tehtyjen muutosten syitä tai luontipäivämääriä voisi kirjata.

Iltapäivällä listaan tietoturvapalvelimilta agentteja, joiden yhteydenotosta palvelimelle on kulunut yli kaksi kuukautta. Vertaan tätä listaa uudelle palvelimelle siirrettyihin agentteihin, ja totean että osa käytöstä poistuneista agenteista selittyy niiden siirrolla uudelle palvelimelle. Tarkistan listallani olevat kaksoiskappaleet, ja poistan tarpeettomat agentit vanhoilta palvelimilta.

Iltapäivällä dokumentoin asiakas E:n tietoturva-agentit listaksi. Asiakkaan agenttien siirto uudelle tietoturvapalvelimelle on alkamassa, ja tuotan listan kollegalleni tiedoksi. Hän suorittaa perjantaiaamuna hallintapalvelimen kautta yrityksen tietoturva-agenttien siirron nykyiseltä palvelimelta uudelle.

Perjantai

Perjantaiaamuna tarkistan asiakas E:n tietoturva-agenttien tilan. Totean uudelle palvelimelle ilmestyneiden agenttien olevan onnistuneesti siirretyt, ja siivoan kyseiset agentit pois vanhalta palvelimelta. Tuotan ja tiedotan kollegaani asiakkaan siirtyneistä agenteista.

Aamupäivällä osallistun viikoittaiseen tietoturvaosaston kokoukseen, missä läpikäymme asiakkaiden projektien tilannetta.

Kokouksen jälkeen aloitan kollegani kanssa rakentamaan Apex One –agentin asennuspakettia. Paketti poistaa tietokoneelta aiemmin asennetun OfficeScan-agentin, minkä jälkeen tietokoneella asennetaan Apex One –agentti. Asennuksen yhteydessä Trend Micron ohjelmalla määritetään agentin uudet asetukset ja uuden tietoturvapalvelimen yhteysosoite.

Asennuspaketti saadaan valmiiksi keskipäivään mennessä, ja käytän iltapäivän paketin testaamiseen testitietokoneessa. Lähtötilanteessa tietokoneella on OfficeScan-agentti yhdistyneenä OfficeScan-palvelimeen, ja asennuspaketin ajon jälkeen testitietokoneella on Apex One –agentti yhdistyneenä Apex One –palvelimeen.

Asennustestauksen yhteydessä havaitsemme kollegani kanssa virheen asennuspaketin toiminnassa: Asennuksen jälkeen tarvitaan tietokoneen uudelleenkäynnistys, mikä oikein suoritetaankin, mutta tietokoneen käynnistyttyä asennuspaketti suorittaa uudelleen asennuksen poiston ja asennuksen, sekä uudelleenkäynnistyksen. Vianselvitykseen ja ongelman korjaamiseen kuluu loppu perjantai-iltapäivä, mutta asennuspaketin virhe löydetään, ja korjauksen ja testauksen jälkeen asennuspaketti todetaan valmiiksi käyttöönottoon.

Viikkoanalyysi 2

Toisen viikon tavoitteena oli syventää ensimmäisellä viikolla muodostamaani näkemystä ja osaamista Trend Micron OfficeScan- ja Apex One –tietoturvapalvelimissa. Tämän viikon aikana opin tietoturvapalvelimien päivitysten perusteita, kuten esimerkiksi mistä tarkistan palvelimille asennettujen päivitysten versiotiedot. Näitä tietoja vertaamalla Trend Micron tukisivustoon, kykenin selvittämään, mitkä päivitykset palvelimille on saatavilla ja tarpeellista asentaa.

Päivitysten asentamista tuotantoympäristön tietoturvapalvelimille ei yrityksessäni ole dokumentoitu. Ainoa asiasta saatavilla oleva materiaali oli kollegoille kertynyt suullisessa muodossa jaettava tieto. Tietoturvapalvelimien päivittämisen prosessi on tarpeellista dokumentoida, ja pohjana tähän käyttäisin saatavilla olevaa Trend Micron ylläpitodokumentaatiota.

Trend Micron Product Patch –päivitysten mukana on saatavilla ReadMe-dokumentti, mikä sisältää tarkemmat tiedot kyseisestä päivityksestä, luettelee päivityksen sisältämät korjaukset ja aiemman päivitystiedostohistorian, ilmoittaa päivityksen kanssa yhteensopivan palvelinversion, sekä ohjeistaa päivityksen suoritustavan (Trend Micro, 2019).

Product Patch –dokumentti ei kuvaa ennen päivitystä suoritettavia tehtäviä, eivätkä tehtäviä mitkä tapahtuvat päivitystyön suorittamisen jälkeen. Yrityksessäni näitä tehtäviä ovat:

- Käytössä olevan version tarkistaminen palvelimelta
- Jos päivitys todetaan tarpeelliseksi, muutostyöpyynnön tekeminen infra-osastolle
- Päivitysluvan valmistuttua, agenttien automaattipäivittymisen poistaminen käytöstä
- Palvelimen varmistus ennen päivityksen suorittamista
- Päivitystiedoston ja oheisdokumentaation lataaminen Trend Micro –lataussivustolta

Päivityksen suorittaminen on ohjeistettu päivityksen mukana seuraavassa oheisdokumentaatiossa. Päivitys suoritetaan siirtämällä päivitystiedosto palvelimelle, ja suorittamalla päivitystiedosto paikallisesti palvelimella.

Päivitystiedosto muodostaa tietoturvapalvelimen sisällöstä varmuuskopion, ja jos päivitys epäonnistuu, päivitys palauttaa ennen päivitystä olleen tietoturvapalvelimen sisällön.

- Päivityksen jälkeen palvelimen yleinen toiminta tarkistetaan
- Päivitetyltä tietoturvapalvelimelta kohdistetaan agenttipäivitys testausympäristössä olevalle testitietokoneelle, ja tarkistetaan että palvelimen uusi agenttiversio asentuu testitietokoneeseen.
- Testauksen päätyttyä, muutostyöpyynnön tila vaihdetaan valmiiksi suoritetuksi
- Testauksen päätyttyä, uusi agenttiversio hallitusti vapautetaan jakeluun asiakasympäristöissä.

3.3 Viikko 3

Maanantai

Aamulla läpikäyn työkalenteriani, ja asetan viikon tavoitteekseni hyödyntää aiemmilla viikoilla keräämääni osaamista tulevien päivien asiakasprojekteissa: Asiakkaiden tietoturva-agentteja tullaan siirtämään poistuvalta OfficeScan-tietoturvapalvelimelta uudelle Apex One –palvelimelle. Toiseksi tavoitteekseni asetan asiakkaiden työasemien tietoturvatuotteita määrittäviin tietoturvapolitiikkoihin tutustumisen.

Aloitan aamun jatkamalla edellisellä viikolla valmistuneen asennuspaketin parissa. Kollegani kanssa kohdistamme asennuspaketin testitietokoneelle, ja seuraamme asennuksen etenemistä sekä tietokoneella että asennuksen valmistuttua tietoturvapalvelimella. Tavoitteemme on automatisoida agentin siirtyminen siten, että tietoturva-agentti saadaan kohdistettua uudella

tietoturvapalvelimella asiakkaan organisaation alle, ilman tarvetta käsin suoritettaviin viimeistelytoimenpiteisiin.

Iltapäivällä tarkistan asiakas D:n siirtoprojektin tilan. Agentteja on siirtynyt vanhalta tietoturvapalvelimelta uudelle, ja todettuani agentit uudella palvelimella toimintakuntoisiksi, poistan vanhalle palvelimelle jääneet agenttikopiot. Listaan siirtyneet agentit sähköpostitse asiakkaalle, tiedottaen samalla kollegaani siirtoprojektin etenemisestä. Lopun iltapäivän käytän tiketöintijärjestelmän kautta saapuneen ongelman selvittämiseen.

Ongelman kuvauksessa palvelintietoturvatuotteen hallintapalvelimen todetaan kuluttavan asiakkaan F palvelimella liiallisen määrän muistia, aloitan ongelmanselvityksen ensin tutustumalla tuotteen tyypilliseen muistinkäyttöön. Läpikäyn tuotedokumentaatiota selvittääkseni myös, onko muistinkäyttö korjattavissa esimerkiksi tuotteen korjauspäivityksellä. Kysyn asiassa apua kollegalta, joka jatkaa ongelmanselvitystyötä puolestani.

Tiistai

Aamulla tarkistan asiakas D:n projektin etenemisen. Eilisen jälkeen uusia agentteja on siirtynyt uudelle tietoturvapalvelimelle, ja teen eilisen tavoin poistuneiden agenttien siivoamisen vanhalta palvelimelta. Tiedotan jälleen sekä asiakasta että kollegaani projektin etenemisestä.

Aamupäivällä etenen asiakkaille jaettujen tietoturvapalvelimien parissa, selvittäen palvelimien tietoturvapolitiikkojen sisältöä. Teen vertailua asiakkaille rakennettujen politiikkojen välillä, ja tutustun tarkemmin käytössä oleviin poikkeussääntöihin. Kiinnitän politiikoissa huomioita kiristyshaittaohjelmiin liittyviin sääntöihin. Kiristyshaittaohjelmat salaavat tietokoneen tiedostoja, minkä jälkeen käyttäjä ei enää saa avattua kyseisiä tiedostoja ilman kiristyshaittaohjelman kehittäjältä, maksua vastaan, saatavaa salauksen purkuavainta.

Ennen keskipäivää poimin työn alle asiakas D:ltä tulleen pyynnön tarkistaa yhden siirron alle otetun tietokoneen tilan. Tietokone oli maanantaina siirrettävien tietokoneiden listalla, mutta asiakkaan käyttäjältä tulleen tiedon mukaan siirtoa ei ollut tapahtunut. Otan yhteyttä kollegaan, joka uudelleen kohdistaa kyseiselle tietokoneelle siirron suorittavan työn. Saan tietää, että hallintapalvelin yrittää tiettyyn rajaan asti käskyttää siirtoa, mutta jos tietokone on ollut tavoittamatta, asennustyö vanhentuu muutaman yrityksen jälkeen tietokoneen osalta.

Iltapäivän aluksi kirjaudun yrityksemme omia tietokoneita hallinnoivalle tietoturvapalvelimelle, ja poistan kollegani pyynnöstä päivitysten jakelun käytöstä. Palvelimelle tullaan lähiaikoina suorittamaan päivitysasennus, ja Trend Micron ohjeistuksen mukaisesti ennen palvelimen päivitystä agenttipäivitykset kytketään pois päältä.

Iltapäivällä jatkan tietoturvapalvelimiin tutustumista. Keskityn tällä kertaa palvelimien tuottamiin raportteihin, kuten torjuttujen haittaohjelmien ja estettyjen haitallisten sivujen tilastotietoihin. Jatkan myös tutustumista kiristyshaittaohjelmien torjuntaan tietoturvapolitiikan asetusten keinoin.

Iltapäivän lopuksi käymme osastollamme läpi eräältä asiakkaalta tullutta kysymystä heidän tietoturvatuotteensa yhteensopivuudesta uusimman Windows 10 –ominaisuuspäivityksen kanssa.

Keskiviikko

Kirjaudun yrityksemme omia tietokoneita hallinnoivalle tietoturvapalvelimelle, ja tarkistan agenttien tilatiedot. Totean että usea agentti on jo siirretty kyseiseltä palvelimelta yrityksemme Apex One –tietoturvapalvelimelle, ja voin siivota nämä agentit pois vanhalta palvelimelta.

Saan aamupäivällä lyhyellä varoitusajalla kutsun Trend Micron kokoukseen, mikä alkujaan oli tarkoitettu myyntiorganisaatiollemme. Nyt mukaan toivotaan myös teknisiä asiantuntijoita, sillä sisältö sivuaa tulevien tuotteiden teknisiä ominaisuuksia. Kokouksessa saan hyvän näkemyksen Trend Micron tuotteiden lähitulevaisuuden kehityskulkuun.

Soitan tiistai-iltapäivänä meihin yhteyttä ottaneelle asiakkaalle. Totean että heidän käytössään olevassa tietoturvatuotteessa on yhteensopivuusongelma uusimman Windows 10 –ominaisuuspäivityksen kanssa, mutta asiakkaan sopimus mahdollistaa siirtymisen uusimpaan tietoturvatuotteeseen. Ehdotan asiakkaalle siirtymisprojektia, minkä aikana agentit siirretään ja päivitetään Apex One –versioon. Asiakas haluaa siirron tehtäväksi, ja aloitan siirtoon liittyvät valmistelutyöt.

Rakennan iltapäivän aikana asiakkaalle tietoturvapolitiikkaa Apex One –palvelimelle. Käytän mallina käytössä olevaa OfficeScan-palvelimen vastaavaa politiikkaa, mutta teen sääntöihin muutaman, tietoturvaa parantavan muokkauksen.

Iltapäivän lopuksi kytken kollegan pyynnöstä pois yhden tietoturvapalvelimen agenttipäivitykset. Kyseiselle palvelimelle tullaan suorittamaan versiopäivitys, mitä ennakoiden agenttipäivitykset kytketään pois päältä.

Torstai

Jatkan keskiviikkona aloittamaani asiakkaan tietoturvapolitiikan rakentamista. Käytän työhön pari tuntia, minkä aikana saan sekä politiikan että palomuuria ohjaavat palomuurisäännöt rakennettua.

Avaan aamupäivän aikana muutospyynnöt kahden tietoturvapalvelimen tulevista päivitystöistä. Päivityksissä palvelimille tullaan asentamaan uusimmat korjauspäivitykset, sisältäen sekä virhekorjauksia että tietoturva-aukkojen korjauksia. Toisen palvelimen päivityksen tulen suorittamaan itse, toisen kollegani.

Ennen keskipäivää, tarkistan asiakas D:n siirtoprojektin tilanteen. Agentteja on siirtynyt uudelle tietoturvapalvelimelle, minkä seurauksena poistan vanhalta palvelimelta tarpeettomia agentteja. Tiedotan projektin etenemisestä asiakasta ja kollegaani.

Iltapäivällä aloitan asiakas G:n siirtoprojektiin liittyvän testauksen. Asennan testiympäristöömme asiakkaan nykyisen tietoturva-agentin, ja avustan kollegaani, rakentaessamme asiakkaan agenttien siirtoon käytettävän asennuspaketin.

Iltapäivän lopuksi selvitän asiakas E:n tietoturva-agentin poistossa tarvittavaa salasanaa. Tietoturva-agentti on suojattu kahdella salasanalla, joista toisella agentti voidaan sammuttaa, ja toisella asennus poistaa tietokoneelta. Salasanaa tullaa tarvitsemaan myöhemmin tehtävässä asiakkaan agenttien siirrossa uudelle tietoturvapalvelimelle.

Perjantai

Jatkan perjantaina asiakas G:n asennuspaketin testausta kollegani kanssa. Asennuspakettiin on tehty muutama asetusmuutos, ja testaamme paketin toimivuutta testiympäristössä, verraten tilannetta ennen muutosta olevaan asennuspaketin versioon.

Aamupäivällä osallistun tietoturvaosaston viikkokokoukseen, missä läpikäymme asiakasprojektien etenemistä. Kokouksesta valtaosa käytetään asiakkaiden projektien tilatietoihin, ja kokouksen loppu tietoturvatuotteiden ongelmista päämiehelle avattujen tukitikettien tilanteeseen. Kokouksessa havaitaan, että muutamassa tukitiketissä kuvattu ongelma on toistunut useamman teknisen asiantuntijan kesken.

Iltapäivällä selvitän torstaina havaittua asiakas E:n ongelmaa tietoturvatuotteen unload-salasanan toimimattomuuden kanssa. Selvitän tilannetta testiympäristössä, ja tutustun tarkemmin tuotteen dokumentaatiossa kuvattuihin aiempien versioiden ongelmiin ja niiden korjauksiin. Totean, että kyseinen ongelma on kuvattu päivityskorjauksen dokumentaatiossa, eli ongelmaan on saatavilla korjaus. Kerron asiasta kollegalle, kenen kanssa teemme päätöksen, että kyseisen tietoturvatuotteen hallintapalvelin pitää päivittää kyseisellä korjauspäivityksellä.

Viikkoanalyysi 3

Kolmannen viikon ensimmäisenä tavoitteena minulla oli hyödyntää muutaman viikon aikana työasemien tietoturvatuotteista kerryttämääni kokemusta. Viikon aikana osallistuin asiakkaille tehtäviin tietoturvatuotteiden käyttöönottoprojekteihin, joissa suoritin asennuspakettien testausta ennen asennuspakettien käyttöä asiakkaiden tuotantoympäristöissä. Viikolla tehtäviini kuului myös projektien etenemisen viestintä asiakkaille ja projektin sisäisille jäsenillemme. Selvitin muutamaa tiketöintijärjestelmämme kautta saapunutta vianselvityspyyntöä, sekä tietoturvapalvelimella havaittua ongelmaa.

Viikon aikana toisena tavoitteenani oli tutustua tietoturvatuotteiden toimintaa määrittäviin tietoturvapolitiikkoihin ja asiakkailla käytettävien politiikkojen asetuksiin. Viikkoanalyysissäni tulen tarkemmin käsittelemään tietoturvapolitiikkojen asetuksia kiristyshaittaohjelmien torjunnan kannalta.

Trend Micro määrittää kiristyshaittaohjelmat ryhmäksi haittaohjelmia, mitkä salakirjoittavat tietokoneen tiedostoja tai suoraan estävät tietokoneen käytön, kunnes haittaohjelman kehittäjän vaatima lunnassumma on maksettu tiedostojen tai tietokoneen vapauttamiseksi (Trend Micro 2019). Tyypillisesti maksu vaaditaan kryptovaluuttana, sen maksutapahtuman käytännössä mahdottomana pidettävän jäljitettävyyden vuoksi. Tunnettuja kiristyshaittaohjelmia ovat mm:

- Trojan:Win32/Crilock.A
- Trojan-Ransom.Win32.Blocker.cgmz
- TROJ_RANSOM
- TROJ_CRILOCK
- Cryptolocker
- Trojan-Ransom.Win32.Foreign.acc
- Trojan.Ransom.FH
- Trojan:Win32/Ransom.GT

Kiristyshaittaohjelman hyökkäys työasemalle on mahdollista estää, ja OfficeScan-tietoturvatuotteen tärkeimmät asetukset haittaohjelmia vastaan ovat (Trend Micro 2019):

- Käyttää paikallisen tietokoneen ja Trend Micron käyttäjäpilven havaintotunnisteita yhdistävää Smart Scan –tarkistusta
- Kytkeä päälle haitallisille Internet-sivustoille pääsyn estävä Web Reputation Service –suojaus sekä yritysten sisäisissä, että ulkoisissa verkoissa
- Kytkeä päälle käyttäytymisen tunnistamiseen perustuva Behavior Monitoring, mikä kykenee tunnistamaan haittaohjelmat epäilyttävät käytöksen perusteella.
- Käyttää tietoturvatuotteiden keräämän tiedon jakamista Trend Micron palvelimille kytkemällä päälle Smart Feedback.

Viikon aikana asiakkaiden käytössä olevia tietoturvapolitiikkoja verrattiin Trend Micron suosittelemiin asetuksiin. Todettiin, että kaikilla asiakkaille ei vielä ollut käytössä kehittynyttä Smart Scan –tarkistusta, vaan käytössä oli perinteisiä haittaohjelmatunnisteita käyttävä Conventional Scan. Haitallisilta sivustoilta suojaava Web Reputation Service todettiin olevan myös vain osittain käytössä. Behavior Monitoring ja Smart Feedback todettiin olevan asiakkaiden tietoturvapolitiikoissa käytössä.

Havaintojen perusteella asiakkaiden tietoturvapolitiikkojen määrityksiä todettiin tarpeelliseksi muuttaa tietoturvan tason kehittämiseksi.

3.4 Viikko 4

Maanantai

Viikon tavoitteekseni asetan tietoturvapalvelimelle tehtävän päivitystyön, minkä yhteydessä aloitetaan tietoturva-agentin päivittyneen version jakelu asiakkaille. Toiseksi tavoitteekseni asetan kertyneeni osaamiseni hyödyntämisen asiakasprojekteissa.

Viikko alkaa tietoturvapalvelimelle suoritettavalla päivitystyöllä. Päivityksessä Trend Micro OfficeScan –palvelinohjelmisto päivitetään uusimmalla korjauspäivityksellä. Päivitys tulee päivittämään myös tietoturvapalvelimeen yhteydessä olevat tietoturva-agentit uuteen versioon, minkä olin edellisellä viikolla huomioinut kytkemällä palvelimelta jaettavat agenttipäivitykset pois päältä.

Lataan Trend Micron lataussivustolta päivitystiedoston, minkä siirrän palvelimelle. Ennen päivitystyötä, suoritan palvelimen varmuuskopioinnin palautumistilannetta varten. Varmuuskopioinnin valmistuttua, suoritan tietoturvapalvelimen päivityksen, minkä jälkeen tarkistan uuteen versioon päivittyneen palvelimen toiminnan.

Asiakas H tulee toimimaan pilottikumppanina uuden agenttiversion käyttöönotossa. Ennen agenttipäivityksen jakelua asiakkaalle, testaan uuden agenttiversion toimivuuden testiympäristössämme. Testin valmistuttua, kohdistan etukäteen sovitun mukaisesti uuden agentin päivityksen asiakkaan muutamalle pilottitietokoneelle.

Iltapäivällä vastaan asiakas I:ltä saapuneeseen kysymykseen tietoturvatuotteen ja uusimman Windows 10 –ominaisuuspäivityksen yhteensopivuudesta. Tarkistan asiakkaan ympäristöstä heidän tietoturva-agenttien versiot, mitkä totean olevan vielä epäyhteensopivassa versiossa Windows-ominaisuuspäivityksen kanssa. Selvitän asiakkaalle heidän tilanteensa agenttien yhteensopivuuden suhteen, ja sovimme ensimmäisten agenttien hallitusta päivityksestä yhteensopivaan versioon. Kohdistan muutamalle asiakkaan agentille päivityksen jakelun, ja tarkistan myöhemmin iltapäivällä agenttien päivittyneen uusimpaan versioon.

Iltapäivällä avaan muutospyynnön käytöstä poistuneen tietoturvapalvelimen alasajosta infra-ryhmämme tehtäväksi. Palvelinta ei enää tarvita, minkä lisäksi palvelimen käyttöjärjestelmäalustan tuki on pian päättymässä. Palvelin on todettu sekä tarpeettomaksi, että tekniikaltaan vanhentuneeksi. Infra-ryhmä tulee käytöstä poistamaan palvelimemme käsiteltyään työpyynnön.

Maanantaipäivän päätteeksi tarkistan kollegani pyynnöstä, että ajastetut haittaohjelmatarkistukset ovat kytkettynä päällä yrityksemme omilla työasemillamme.

Tiistai

Edellisenä päivänä päivitetty tietoturvapalvelin on nyt uudemmassa versiossa kuin siihen yhteydessä olevat asiakkaiden tietoturva-agentit. Versioerosta huolimatta agentit kykenevät kommunikoimaan palvelimen kanssa. Päivityksen jälkeen tietoturva-agentit kuitenkin aina päivitetään samaan versioon palvelimen kanssa.

Tietoturvapalvelimelle on yhdistetty useita satoja agentteja, mistä johtuen agenttien päivitykset tullaan suorittamaan hallitusti tietty määrä kerrallaan. Aloitan tiistaiaamulla kohdistamaan agenttipäivityksiä pienen määrän per asiakasympäristö. Havaittuaan palvelimella olevan uuden agenttiversion, agentti lataa ja päivittää itsensä uuteen versioon.

Aamupäivällä testaan edellisellä viikolla havaittua ongelmaa agentin unload-salasanan kanssa. Testin perusteella totean, että uusi agenttiversio on korjannut aiemmin havaitun ongelman, ja kun uusi agenttiversio saadaan levitetyksi, ei ongelmaa tulla enää kohtaamaan.

Iltapäivän aluksi osallistun jatkuvien palveluiden säännölliseen kokoukseen, missä tärkeäksi luokiteltuna asiana käsittelemme asiakkaille suoritettavien työpyyntöjen kommentoinnin sisältöä.

Kollega ohjaa selviteltäväkseni asiakas J:ltä saapuneen pyynnön tarkistaa mahdollinen palvelimen päivitysten ongelma. Asiakkaan epäily on, että palvelin ei enää tarjoa agenteille uusimpia haittaohjelmatunnisteita. Selvitän asiaa vertailemalla kahden eri palvelimen hakemien tunnisteiden versioita, ja totean että toinen palvelin ei ole saanut noudettua uusia tunnisteita. Ajan kyseiselle palvelimelle manuaalisen tunnisteiden haun, ja tarkistan myöhemmin, onko palvelimen tunnisteet päivittyneet haun jälkeen.

Maanantainen asiakas I ottaa iltapäivällä yhteyttä, toivoen tarkempia tietoja Windows 10 – ominaisuuspäivityksen yhteensopivuusongelmasta heidän käyttämänsä agenttiversion kanssa. Ohjeistan asiakasta heidän tilanteestaan, ja annan toimintaohjeita siitä, kuinka vain harvoin käynnissä ja palvelimeen yhteydessä olevat tietokoneet saadaan päivitettyä uusimpaan agenttiversioon.

Iltapäivän lopuksi tarkistan manuaalisen tunnisteiden haun tulokset, ja totean että kyseisellä palvelimella on selvä ja toistettavissa oleva ongelma saada noudettua uusimpia tunnisteita Trend Micron internetissä sijaitsevalta palvelimelta. Avaan asiasta ongelmanselvitystyöpyynnön Trend Micron tukeen.

Keskiviikko

Jatkan keskiviikkoaamuna agenttipäivitysten kanssa. Selvitän ensin, kuinka moni tiistain jakelussa ollut agentti on päivittänyt itsensä, ja laajennan jakelua useammalle agentille. Valikoin jakeluryhmää muodostaessani aktiivisimpia agentteja, joiden ominaisuuksia ovat mm.:

- Agentti on päivittäin käynnissä ja yhteydessä tietoturvapalvelimeen
- Agentti on päivittäin käynnistetty uudelleen, mikä helpottaa agenttipäivityksen suorittamista

Aktiivisten agenttien tapauksessa kesto päivityksen kohdistamisesta asennuksen valmistumiseen on hyvin lyhyt, minkä seurauksena voin aamupäivän aikana lisätä valmistuneiden agenttien rinnalle uusia agentteja päivitettävien agenttien listalle.

Aamupäivällä tarkistan myös yrityksemme omien tietoturva-agenttien tilanteen sekä käytöstä pian poistuvalta, että uudelta tietoturvapalvelimeltamme. Käynnissä on projekti, missä omat

agenttimme siirretään vanhalta palvelimelta uudelle, ja tehtävänäni on tarkistaa, onko uudelle siirrettyjen agenttien kopioita jäänyt vanhalle palvelimelle. Löydän muutaman agentin vanhalta palvelimelta, mitkä siivoan pois.

Ennen keskipäivää saan sisäisen työpyynnön selvittää asiakas K:n tietoturva-agenttien kappalemäärän asiakaslaskutusta varten. Asiakkaalla on käynnissä agenttien siirto käytöstä poistuvalta tietoturvapalvelimelta uudelle, ja siirron ollessa kesken, agentteja on kahdella palvelimella. Tuotan molemmilta palvelimilta agenttien listaukset, ja näitä keskenään vertailemalla poistan ensin kaksoiskappaleet, minkä jälkeen raportoin agenttien määrän eteenpäin.

Keskipäivän jälkeen läpikäyn tietoturvaosaston esimiehen kanssa tietoturvapalvelinten versio- ja päivitystilannetta kokoukseen valmistelemani taulukon avulla. Aiemmin palvelimilla ei ole ollut nimettyä vastuuhenkilöä, ja palvelinten ylläpitoa on suorittanut useampi henkilö ilman tarkempaa koordinaatiota näiden henkilöiden kesken. Kokouksessa päätetään, että jatkossa asiakkaiden työasematuotteita hallinnoivien tietoturvapalvelimien vastuu keskitetään minulle, ja tulen säännöllisesti seuraamaan palvelimien päivitysten tilaa.

Kokouksen jälkeen muokkaan asiakas G:n tietoturvapolitiikassa määritettyjä unload- ja uninstall-salasanoja. Politiikan muutoksen tarve tulee kollegaltani, ja liittyy käynnissä olevaan agenttien siirtoon vanhalta tietoturvapalvelimelta uudelle.

Iltapäivän aikana kohdistan agenttipäivityksiä kahdelle asiakkaalle. Molempien kanssa olemme sopineet pilottitietokoneryhmiin kuuluvat jäsenet, joihin agenttipäivitykset tullaan ensin kohdistamaan. Päivitysten kohdistamisen jälkeen viestin asiakkaille asiasta sähköpostitse, ja seuraan päivitysten etenemistä iltapäivän ajan.

Torstai

Jatkan aamulla tietoturvapalvelimen agenttipäivitysten kohdistamista asiakkaiden tietokoneille. Aloitan tarkistamalla edellisten päivien päivitysten onnistumisen vertailemalla listoilta agenttien versionumerotietoja ennen ja jälkeen päivitysten kohdistamista. Totean versionumeron vaihtumisen perusteella valtaosan agenteista päivittyneen, ja lisään seuraavan erän per asiakas päivittymään uuteen versioon.

Aamupäivän aikana selvitän asiakas D:ltä saapunutta pyyntöä suorittaa kahden agentin siirto vanhalta palvelimelta uudelle. Teemme asiassa yhteistyötä kollegan kanssa: Selvitän asiakkaalta siirrettävien tietokoneiden verkkonimet ja siirtoon sopivat aikaikkunat. Välitän tiedon kollegalleni, joka kohdistaa kyseisiin tietokoneisiin hallintaohjelmiston kautta asennuspaketit

asiakkaan haluamana aikana. Tiedotan lopuksi asiakasta, että päivitys tullaan suorittamaan sovitusti tietokoneille.

Ennen keskipäivää läpikäyn asiakas H:n agenttipäivitysten tilannetta, ja sovimme sähköpostitse päivitysten kohdistamisesta seuraavalle agenttiryhmälle.
Iltapäivällä selvitän asiakas G:ltä saapunutta viestiä: Asiakkaan mielestä vanhalta palvelimelta uudelle siirretty agentti ei ole saanut oikeaa tietoturvapolitiikkaa. Selvitän agentin tilannetta kollegani kanssa, ja toteamme ettei kyseinen agentti ole siirron jälkeen saanut käyttöönsä oikeaa tietoturvapolitiikkaa.

Tarkistamme tietoturvapalvelimelta agentin sijaintia asiakkaan organisaatiorakenteessa, ja huomaamme että agentti on väärässä hakemistopuussa, minkä seurauksena agentti on saanut käyttöönsä väärän sijainnin mukaiset asetukset. Siirrän agentin organisaatiorakenteessa oikeaan sijaintiin, minkä jälkeen odotamme agentin uuden sijainnin mukaisten asetusten pienen viiveen jälkeen päivittyvän.

Edellisen ongelman ratkettua, otan asiakas C:hen yhteyttä agenttien siirtoprojektin seuraavan osan aikatauluttamisesta. Kyseisellä yrityksellä valtaosa tietokoneista on pääkaupunkiseudulla, ja näiden tietokoneiden agentit ovat jo siirretty uudelle palvelimelle. Loput agentit ovat yrityksen etätoimipisteissä usealla eri paikkakunnalla. Sovimme asiakkaan kanssa, että Pääkaupunkiseudun ulkopuoliset tietoturva-agentit tullaan päivittämään lähitukihenkilön toimesta etukäteen sovittuna päivänä, kun etätoimipisteiden käyttäjät ovat paikalla päätoimipisteessä.

Perjantai

Aamupäivällä suoritamme asiakas G:n muutaman agentin ajastetun asennuksen kollegan kanssa. Asiakkaan käyttäjät ovat sovitusti tuoneet tietokoneensa asiakkaan toimipisteeseen, missä paikalla on myös asiakkaan lähitukipalvelun asiantuntija. Kyseisille agenteille kohdistetaan hallintapalvelimen kautta asennuspaketti, mikä ensin poistaa tietokoneelta nykyisen version agentista, sen jälkeen asentaa uuden agenttiversion, ajaa agentin kohdistamisen asiakkaan organisaatiorakenteeseen, sekä lopuksi suorittaa tietokoneelle uudelleenkäynnistyksen. Seuraamme kollegan kanssa asennusten etenemistä, ja toteamme asennusten onnistuvan, mistä tiedotamme asiakasta.

Aamupäivällä osallistun tietoturvapalveluiden kokoukseen, missä läpikäymme asiakkaiden projektien tilannetta. Tämän lisäksi sivuamme avoinna olevien ja jo valmistuneiden vianselvitys-

pyyntöjen tilaa. Huomaan tämä hyödylliseksi, sillä kokouksen aikana useammalla asiantuntijalla on ollut selvitettävänään keskenään identtisiä ongelmatapauksia. Tämä kokous tarjoaakin hyvän mahdollisuuden näiden tapausten läpikäyntiin.

Seuraavalla viikolla olen suunnitellut suorittavani kahden tietoturvapalvelimen päivityksen, ja valmistelen ennen keskipäivää nämä palvelimet päivityksiä varten, siirtämällä päivitystiedostot kyseisille palvelimille, ja vielä varmistamalla agenttipäivitysten olevan kytkettynä palvelimilta pois päältä.

Keskipäivän jälkeen otan yhteyttä asiakas L:ään, kenen kanssa sovimme tietoturva-agenteille tehtävistä päivityksistä. Asiakkaan useampi agentti on vanhassa versiossa, ja teemme asiakkaan kanssa suunnitelman agenttien päivittämisestä uusimpaan versioon. Kohdistan sovitun mukaisesti agenttipäivitykset ensimmäisille kahdelle agentille, ja seuraan päivittymisen onnistumista iltapäivän aikana. Totean päivitysten onnistuneen, mistä tiedotan sähköpostitse asiakasta.

Keskiviikkona sovitun mukaisesti aloitan perjantai-iltapäivänä dokumentoimaan työasemaympäristön tietoturvaa hallinnoivien tietoturvapalvelimien tilannetta. Rakennan taulukon, mihin koostan tiedot käytössä olevista Trend Micro –tuotteista ja niiden versioista. Lisään rinnalle uusimmat saatavilla olevat versiotiedot, mistä voidaan nähdä palvelinten päivitystarve. Lisäksi lisään taulukkoon palvelinten käyttöjärjestelmäversiot, huomioiden myös käyttöjärjestelmien tuen päättymispäivät.

Taulukosta on todettavissa, että esimerkiksi yhden palvelimen käyttöjärjestelmän tuki on päättymässä tulevan vuoden alussa, samoin kyseisen palvelimen tietoturvapalvelimen tuki myös on päättymässä loppuvuodesta.

Iltapäivän lopuksi tarkistan asiakkaiden päivän aikana siirrettyjen agenttien tilan uudella palvelimella, ja siivoan siirtyneiden agenttien kopiot pois vanhalta palvelimelta.

Viikkoanalyysi 4

Viikolle asettamani tavoite oli suorittaa tietoturvapalvelimelle versiopäivitys. Olin edeltävinä viikkoina tutustunut kyseiseen tuotteeseen, ja läpikäynyt päivitykseen liittyvää dokumentaatiota, keskittyen päivityksen suorittamiseen liittyviin työvaiheisiin. Viikon aikana suoritin kyseisen päivitystyön, mikä eteni ennalta tehdyn suunnitelman mukaisesti, enkä kohdannut päivitystyön aikana ongelmia.

Kokonaisuudessaan olin kerännyt riittävän osaamisen tämän työtehtävän suorittamiseen, ja tätä osaamistani hyödyntäen suoritin työn onnistuneesti, sovitussa aikataulussa, saavuttaen oikean lopputuloksen.

Toisena tavoitteenani oli osallistua asiakasprojekteihin. Viikkoa tarkastellessani huomaan viestineeni tehokkaasti asiakkaille, sekä kyenneeni hyödyntämään osaamistani projektieni työvaiheissa. Huomaan myös, että työtäni projektien eri työvaiheissa olisi auttanut parempi osaaminen yrityksemme käyttämästä hallintatyökalusta. Kyseisellä työkalulla rakennetaan ja kohdistetaan ohjelmistoasennuksia hallinnan piirissä oleville työasemille. Ilman omaa osaamistani tuotteesta, jouduin tukeutumaan kollegan apuun asennuksia kohdistettaessa työasemiin. Koen tärkeäksi omaksua kyseisen työkalun osaamisen, ja tulen jatkossa panostamaan osaamisen kasvattamiseen tässä asiassa.

Viikkoanalyysissä käsitellään Windows 10 -käyttöjärjestelmän Ominaisuuspäivityksiin rakennettua päivitysten estotekniikkaa, mikä estää päivityksen tietokoneella, jos asennuksen aikana havaitaan epäyhteensopiva ohjelmisto tai laiteajuri. Analyysissä tarkemmin selvitetään päivitysten estotekniikkaa Trend Micro OfficeScan –agenttiversioiden yhteensopivuuden kannalta.

Uusien Windows-käyttöjärjestelmien sijaan Microsoft päivittää käyttöjärjestelmään ominaisuuksia julkaisemalla Microsoft Windows 10 -Ominaisuuspäivityksiä kahdesti vuodessa, tyypillisesti keväällä ja syksyllä (Microsoft 2019). Julkaistavat päivitykset ovat kumulatiivisia: Ne ovat päivityksiä, mitkä perustuvat kyseistä päivitystä edeltävään päivitykseen. Ominaisuuspäivitysten välillä Microsoft julkaisee käyttöjärjestelmään myös kuukausittaisia päivityksiä, mitkä sisältävät käyttöjärjestelmän käyttöä parantavia ja ongelmia korjaavia päivityksiä, mutta eivät sisällä uusia käyttöjärjestelmän ominaisuuksia.

Windows-tuotteilla on Microsoftin määrittämä elinkaari, mikä alkaa tuotteen julkaisusta ja päättyy ylläpidon päättyessä (Microsoft 2019). Windows 10 -Ominaisuuspäivitys on Microsoftin ylläpitämä 18 kuukauden ajan julkaisupäivämäärästä, ja esimerkiksi Windows 10, versio 1903 (myös nimellä Windows 10 toukokuun päivitys 2019) on tuettu julkaisupäivästään (21.5.2019) 18 kuukauden ajan.

Ominaisuuspäivitykset sisältävät muutoksia käyttöjärjestelmään, mistä johtuen Trend Micro joutuu julkaisemaan omiin tuotteisiinsa Ominaisuuspäivitysten yhteensopivuuspäivityksiä. Trend Micro tyypillisesti julkaisee yhteensopivuuspäivityksensä yhden kalenterikuukauden kuluttua Microsoft Windows 10 Ominaisuuspäivityksen julkaisun jälkeen (Trend Micro 2019). Trend Micro suosittelee siirtämään Ominaisuuspäivityksen suorittamista, kunnes tietokoneen

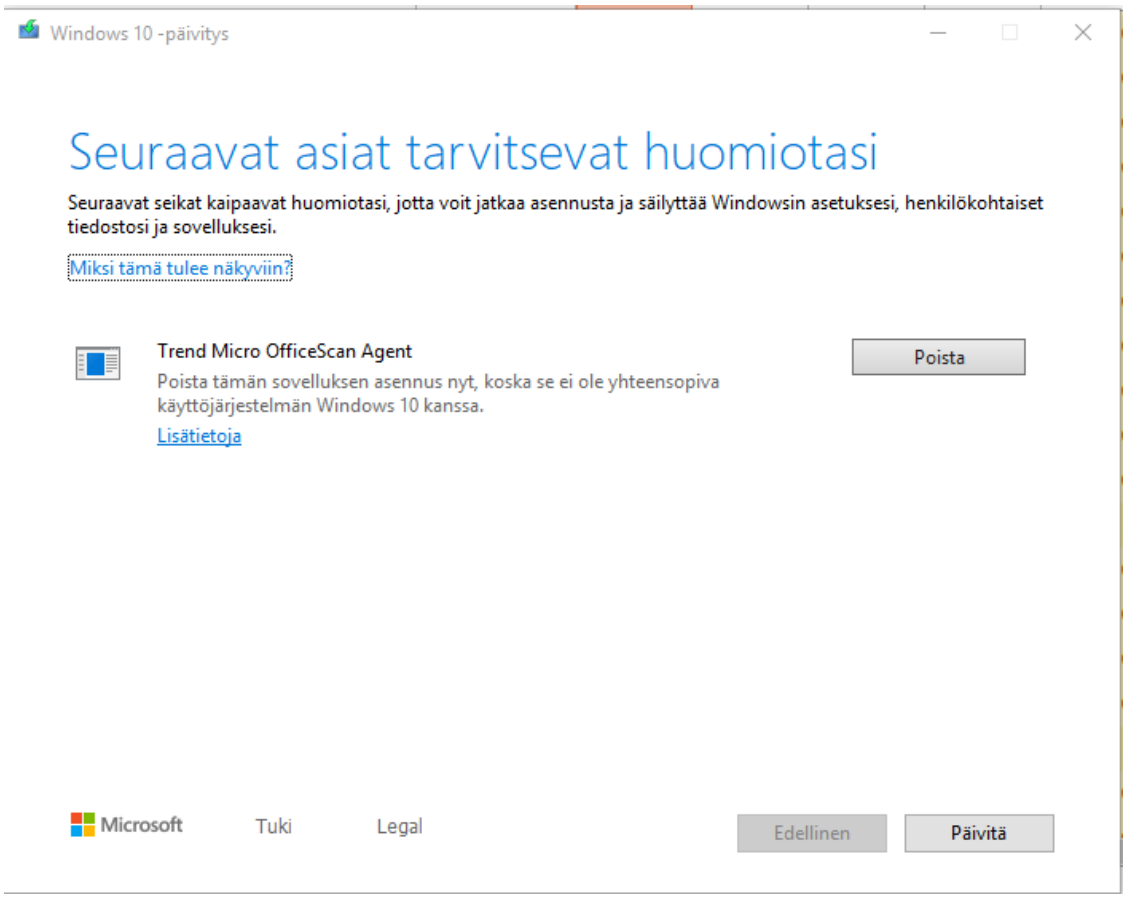
tietoturva-agentti on päivitetty Ominaisuuspäivityksen kanssa yhteensopivaan versioon. Epäyhteensopiva versio voi aiheuttaa suorituskykyongelmia, ohjelmien kaatumisia tai käyttöjärjestelmän virhetilanteen.

Estääkseen Ominaisuuspäivityksen asentamisen epäyhteensopivalla agenttiversiolla varustettuun tietokoneeseen, Trend Micro on pyytänyt Microsoftilta Ominaisuuspäivityksen asentamisen estävien toiminnallisuuksien kytkemisen päälle. Näitä ovat:

- Offer Block
- Setup Block

Käyttäjä voi tarkistaa tietokoneelleen tarjolla olevat Microsoft-päivitykset Windows Update –toiminnallisuuden kautta. Offer Block estää Ominaisuuspäivityksen näkymisen käyttäjälle, jos Windows Update havaitsee tietokoneelta epäyhteensopivan OfficeScan-agenttiversion. Offer Block toimii 60 vuorokauden ajan, eikä tietokoneen käyttäjä sinä aikana näe ilmoitusta Ominaisuuspäivityksen estämisestä.

Käyttäjän itse ladatessa Windows 10 –Ominaisuuspäivityksen asennustiedoston, Setup Block havaitsee tietokoneella olevan epäyhteensopivan agenttiversion, ja estää Ominaisuuspäivityksen suorittamisen, ilmoittaen ongelmasta virheviestillä käyttäjälle.



Kuvio 1: Käyttöjärjestelmän Setup Block -ilmoitus (Markus Björklund 2019)

Käyttäjälle tarjotaan mahdollisuus poistaa epäyhteensopiva Trend Micro OfficeScan-agentti, mutta tietoturvasyistä käyttäjällä ei ole asennuksen poistamiseen tarvittavaa poistosalasanaa, eikä käyttäjä voi suorittaa Ominaisuuspäivityksen asentamista.

Microsoft julkaisi Windows 10 -Ominaisuuspäivitys 1903:n toukokuussa 2019, ja Trend Micro julkaisi yhteensopivan agenttiversion lähes neljä viikkoa myöhemmin kesäkuussa 2019 (Trend Micro 2019). Agenttiversio päivitetään tietokoneelle päivittämällä ensin tietoturvapalvelin uuteen päivitysversioon, minkä jälkeen palvelimelta jaetaan uusi agenttiversio tietokoneille.

Trend Micron ohjeistuksen mukaisesti, ennen palvelimen päivitystä agenttien, päivitysjakelut kytketään pois päältä noin viikkoa ennen päivitystä, palvelimen ja asiakkaiden tietojärjestelmien kuormituksen minimoimiseksi. Jos agenttipäivitykset olisivat kytketty päälle, palvelimen päivityksen jälkeen agentit alkaisivat välittömästi päivittämään itsensä uuteen versioon, mahdollisesti liiallisesti kuormittaen sekä tietoturvapalvelimen että asiakkaiden tietojärjestelmiä.

Asiakkaiden joukossa tyypillisesti on käyttäjiä, ketkä ovat kiinnostuneita hyvin nopealla aikataululla käyttöönottamaan Microsoftin julkaisemia Ominaisuuspäivityksiä. Johtuen Trend Micron päivitysten julkaisuaikataulusta, sekä tietoturvapalvelimien päivitysten suoritustavasta, Windows 10 -Ominaisuuspäivitysten kanssa yhteensopivien agenttipäivitysten asentamisessa asiakkaiden tietokoneille voi kulua aikaa lähes kaksi kuukautta. Tämä viive on pitkä, mutta Trend Micro OfficeScan –tuotteen osalta aikaa vaikeaa saada pienennettyä, edellä mainituista syistä.

Microsoftin käyttämät Ominaisuuspäivitysten yhteensopivuusongelmia minimoivat asennusestot toimivat mielestäni hyvin, estäen Ominaisuuspäivitysten asentumisen tietokoneille, joilla on havaittu epäyhteensopivia ohjelmia tai laiteajureita.

3.5 Viikko 5

Maanantai

Viikon tavoitteekseni asetan kahden tietoturvapalvelimen versiopäivitysten suorittamisen, sekä päivitysten jälkeisen agenttipäivitysten hallitun jakelun asiakasympäristöihin.

Aloitan viikon valmistelemalla kaksi tietoturvapalvelinta tiistaina tehtävään päivitykseen. Siirrän molemmille palvelimille päivityksessä tarvittavat päivitystiedostot ja päivityksiin liittyvät ohjedokumentit. Tarkistan samalla, että molemmista palvelimista on poiskytketty tietoturva-agenttien päivitysjakelut. Palvelimet ovat eri versiosukupolvea, minkä takia palvelimet tullaan päivittämään eri päivitystiedostoilla. Läpikäyn molempien päivitysversioiden asennusohjeet, mutta versioeroista huolimatta totean päivitysten tapahtuvan molemmille palvelimille samalla tavalla.

Aamupäivän lopuksi läpikäyn palvelutilauksensa päättäneen asiakas M:n yhä aktiivisina olevia agentteja, joista muodostan listauksen. Saan kuulla kollegaltani, että ei ole tavatonta, että poistuneiden asiakkaiden yksittäisiä agentteja jää aktiivisiksi yhä ottamaan yhteyttä tietoturvapalvelimille. Näissä tapauksissa yrityksemme ottaa poistuneisiin asiakkaisiin yhteyttä, ja pyytää asiakkaita itse poistamaan yhä aktiiviset agenttiasennukset.

Keskipäivän jälkeen jatkan edellisellä viikolla aloittamaani asiakkaiden tietoturva-agenttien päivitysjakelua. Tarkistan tietoturvapalvelimelta päivitettäväksi kohdistettujen agenttien tilanteen, ja totean valtaosan päivittyneen uusimpaan versioon. Kohdistan tietyn määrän agenttipäivityksiä asiakasympäristöihin, ja merkitsen muistiin päivitysten tilanteen.

Kahden asiakkaan siirtymä OfficeScan-tietoturvatuotteesta Apex One –tuotteeseen eteni edellisellä viikolla. Työn ovat suorittaneet asiakkaiden omat it-organisaatiot, yrityksemme asiantuntijoiden ohjeistuksen ja teknisen tuen perusteella. Vertailen uudella ja vanhalla palvelimella olevia agentteja, ja siivoan vanhalta palvelimelta pois tarpeettomia agenttien kaksoiskappaleita.

Iltapäivällä keskustelen kollegani kanssa yhden tietoturvapalvelimemme tilanteesta. Palvelimella on aiemmin havaittu ongelma, mitä on korjattu ohjelmistotoimittajalta saadulla korjauspäivityksellä. Kyseinen korjauspäivitys on saatu ohjelmistotoimittajalta vain tämän ongelman korjaamiseksi. Päivityksen suorituksen jälkeen on havaittu alkuperäiseen ongelmaan liittyvä uusi ongelma, mitä kollegani on jo selvittänyt. Ohjelmistotoimittajan kanssa järjestetään myöhemmin iltapäivällä aiheesta kokouspuhelu.

Ennen iltapäivän loppua, jatkan asiakasympäristöjen agenttipäivitysten jakelua. Tarkistan jälleen päivittyneiden agenttien lukumääriä, ja merkitsen ylös agenttien eri versioiden lukumäärät päivitysten etenemisen seuraamiseksi.

Iltapäivän lopuksi osallistun kollegan vetämään kokouspuheluun, missä ohjelmistotoimittajan kanssa selvitämme tietoturvapalvelimella olevan ongelman kokonaiskuvaa. Ongelmaa analysoitaessa selviää, että ongelma mahdollisesti johtuu tietoturvapalvelimilla olevista varmenteista. Tehtäväksemme jää selvittää, hallitaanko palvelimen varmenteita yrityksemme omien ryhmäkäytäntöjen avulla, ja voiko näiden takia johtuen tietoturvapalvelimen tarvitsemia varmenteita jäädä päivittymättä.

Tiistai

Aloitan tiistain jatkamalla asiakasympäristöjen tietoturva-agenttien päivityksiä. Vertailemalla maanantaina keräämiäni päivittyneiden agenttien määriä tiistaiaamun tilanteeseen, totean päivitysten etenevän hyvin: Valtaosa päivityksen kohteena olevista agenteista on päivittynyt uuteen versioon. Lähes kaikki päivittymättömät agenttitietokoneet ovat olleet poissa käytöstä maanantain aikana, mikä selittää päivittymättömät agentit.

Listaan seuraavaksi asiakas D:lle uudelle tietoturvapalvelimelle siirrettyjen agenttien määrän. Lisäksi, asiakkaan pyynnöstä, kohdistamme kollegan kanssa hallintapalvelimelta siirron suorittavan asennuspaketin asiakkaan pyytämälle yhdelle tietokoneelle.

Edellisellä viikolla olin suorittanut asiakas L:lle pilottipäivitystyön. Tarkistan asiakkaalta, oliko suoritettu päivitys aiheuttanut ongelmia. Päivitykseen liittyviä ongelmia ei ole havaittu,

eli jatkamme kahden seuraavan tietokoneen päivityksellä, joihin molempiin kohdistan sovitusti päivitykset.

Iltapäivällä suoritan maanantaina valmistelemani päivitykset kahdelle tietoturvapalvelimelle. Aloitan työn ottamalla molemmista palvelimista virtuaaliympäristön hallinnassa varmistukset. Varmistusten valmistuttua suoritan päivityksen ensin toiselle palvelimelle, ja päivityksen jälkeen tarkistan palvelimen toiminnan sekä palvelimella että testiympäristön agentilla. Tarkistan lisäksi, että testiympäristön agenttipäivitys palvelimen uuteen versioon onnistuu, ja että agentti toimii ja kommunikoi päivityksen jälkeen.

Todettuani ensimmäisen palvelimen päivitystyön valmiiksi, suoritan päivityksen vastaavalla tavalla myös toiselle palvelimelle. Molemmat palvelimien päivitystyöt ovat valmistuneet aikataulussa, ja tiedotan tietoturvaosastoa päivitysten valmistumisesta.

Tarkistan iltapäivällä asiakas I:n ympäristön agenttien versiotilanteen. Totean, että useampi kymmenen agenttia on päivittänyt itsensä uuteen versioon. Luon kokonaistilanteesta listan asiakkaalle, ja ohjeistan asiakkaan yhteyshenkilöä tiedottamaan yrityksen käyttäjiä pitämään tietokoneensa säännöllisesti käynnissä, mikä nopeuttaa agenttien päivittymistä.

Iltapäivän lopuksi läpikäyn asiakas L:n tietoturvapolitiikan asetuksia, ja suoritan sääntöihin muutamia asiakkaan toivomia muutoksia.

Keskiviikko

Keskiviikkoaamulla tarkistan asiakas D:n siirrettyjen agenttien tilanteen. Tiistaina yhdelle tietokoneelle oli kohdistettu siirto, ja totean kyseisen agentin siirtyneeksi uudelle tietoturvapalvelimelle. Tiedotan asiakasta asiasta, ja toimitan samalla päivittämäni listauksen siirron tilanteesta.

Tiistaina asiakas L:n kahdelle agentille oli kohdistettu päivitys uuteen versioon, ja tarkistan nyt näiden tilan. Totean agenttien päivittyneen ilman ongelmia, ja asiakkaalta saadun luvan jälkeen kohdistan agenttipäivityksen asiakkaan muille tietokoneille. Tiedotan asiakasta agenttipäivitysten tilanteesta.

Ennen keskipäivää, ehdin tarkistamaan yrityksemme omien agenttien tilan sekä poistuvalla että uudella tietoturvapalvelimella. Käynnissä on omien agenttiemme siirto uudelle palvelimelle, ja valtaosa agenteista on jo siirretty. Totean vanhalta palvelimelta muutaman agentin

olevan yhä aktiivisessa käytössä, ja luon näistä listan kollegalleni agenteille kohdistuvaa siirtoa varten. Vertailen samalla vanhan ja uuden palvelimen agentteja, ja poistan muutaman jo siirretyn agentin pois vanhalta palvelimelta.

Iltapäivän aluksi rakennan asiakas L:lle tietoturva-agentin asennuspaketin uusien koneiden asennusta varten. Asennuspaketti on tarkoitettu tilanteeseen, missä kyseisen asiakkaan uudella tai uudelleenasennetulla tietokoneella ei vielä ole tietoturvaohjelma-asennusta. Asennuspaketti asentaa sekä tietoturva-agentin, että kohdistaa agentin tietoturvapalvelimella oikeaan asiakasorganisaatioon.

Iltapäivällä aloitan alkuviikosta päivitettyjen tietoturvapalvelimien päivittyneiden agenttien levittämisen asiakasympäristöihin. Kohdistan palvelimilla uuden agenttiversion päivittymään muutamalle valikoidulle agentille. Merkitsen ylös päivityksen kohteena olevien agenttien nimet pystyäkseni tarkistamaan kuinka päivitysten asennukset onnistuvat.

Lopun iltapäivästä käytän selvittääkseni löytämääni ongelmaa tietoturvapalvelimeen integroidun internet-sivujen ja tiedostojen mainetarkistuksia suorittavassa palvelimessa. Lokeja aiemmin läpikäymällä havaitsin, että kyseinen palvelin ei ole kyennyt muodostamaan yhteyttä pilvipalvelussa sijaitseviin, mainepäivityksiä tarjoaviin palvelimiin. Paikannan ongelman palvelimelle määritettyihin asetuksiin, mitkä ovat jostain syystä jääneet päivittämättä käytöstä poistuneista uusiin. Päivitetyillä asetuksilla palvelin kykenee noutamaan tuoreet päivitystiedot, ja totean ongelman selvitetyksi.

Torstai

Aloitan aamupäivän tekemällä asiakas L:n tilaamat muutokset tietoturvapolitiikkaan. Muutosten jälleen vielä läpikäyn kyseisen politiikan kokonaisuudessaan, ja totean sisällön olevan hyvien käytäntöjen mukaan tehty. Tiedotan asiakasta, että halutut muutokset on saatettu tietoturvapolitiikkaan, ja että uudet asetukset tulevat tietoturva-agenteilla voimaan, kun agentit havaitsevat ja lataavat uuden politiikan palvelimelta.

Aamupäivällä jatkan keskiviikkona suorittamaani asiakkaiden tietoturva-agenttien päivittämistä. Tarkistan jälleen päivittyneiden agenttien tilan, ja kohdistan tällä kertaa päivityksen suuremmalle määrälle asiakasympäristöjen agentteja.

Edellisenä päivänä olin selvittänyt yhdessä tietoturvapalvelimessa havaittua ongelmaa, mikä esti internet-sivujen ja tiedostojen mainetarkistuspäivitysten noutamisen pilvipalvelusta. Oli mahdollista, että kyseinen ongelma oli myös toisissa palvelimissa, mistä syystä toisten palvelimien vastaavat asetukset oli tarkistettava saman ongelman varalta. Totesin, että toisessakin

palvelimessa oli käytössä samat, virheelliset asetukset. Korjasin asetukset oikeiksi, ja tarkistin, että palvelin kykeni korjauksen jälkeen hakemaan päivitykset.

Iltapäivällä läpikävin myös kolmannen palvelimen vastaavat asetukset. Oletukseni oli, että myös tällä palvelimella olisi väärin määritetyt asetukset, mutta tarkistettuani palvelimen, totesin että tässä tapauksessa asetukset olivat oikein määritetyt, eikä palvelin tarvinnut asetusmuutoksia.

Iltapäivän lopuksi sain kollegaltani pyynnön läpikäydä asiakas K:n agenttimäärät laskutusta varten. Kyseisellä asiakkaalla on kesken agenttien siirto vanhalta tietoturvapalvelimelta uudelle, ja tästä syystä agentteja on kahdella eri ohjelmistoversion palvelimella. Listasin agentit näiltä kahdelta palvelimelta, ja kaksoiskappaleen listalta poistamalla, kokosin kollegalle agenttien määrät kummallakin palvelimella.

Perjantai

Perjantaiaamulla tarkistin yhden tietoturvapalvelimen agenttien versiotietoja, ja totesin agenttipäivitysten jakelun olevan tarpeellista useammalle agentille. Palvelimelta oli kytketty agenttipäivitykset pois päältä, minkä takia päivityksiä ei ollut automaattisesti tehty. Kohdistin jokaisen asiakkaan muutamalle agentille päivitykset, ja merkitsin itselleni iltapäiväksi muistutuksen tarkistaa päivitysten etenemisen.

Aamupäivällä jatkoin torstai-iltapäivällä suorittamaani asiakas K:n agenttimäärien tarkistamista. Kollegani lisäksi asiaa käsittelevässä kokouksessa mukana oli asiakkaan laskutusta läpikäyvä myyjä, kenen kanssa ratkoimme löytynyttä eroa agenttimäärien ja hallintapalvelimella olevien asiakkaan tietokoneiden välillä.

Aamupäivän lopuksi tarkistin asiakas I:n agenttien siirtoprojektin tilanteen. Totesin agenttien onnistuneesti siirtyneen, ja tiedotin asiakasta siirtoprojektin tilasta.

Iltapäivällä jatkoin asiakas D:n siirtoprojektin edistämistä. Asiakkaalta olimme saaneet toiveen kolmen agentin siirrosta, ja välitin näiden agenttien tietokonenimet kollegalleni asennuspakettien kohdistusta varten.

Suoritin iltapäivällä kahden muun asiakkaan siirrettyjen agenttien siivoamista vanhalta palvelimelta. Siirrettäessä agenttia vanhalta palvelimelta uudelle, siirron sijaan agentti kopioituu uudelle palvelimelle, ja lopputuloksena agentti on löydettävissä sekä vanhalta että uudelta palvelimelta. Verrattaessa eroja agentin kommunikointipäivämäärässä ja –kellonajassa, voidaan todeta, kumpi agentti on poistunut käytöstä, ja näistä tarpeeton voidaan poistaa.

Iltapäivän lopuksi tarkistin aamulla päälle kytkemäni agenttipäivitysten jakelun. Agenttien versiotietoja aamun tilanteeseen verrattuani totesin päivitysten onnistuneen.

Viikkoanalyysi 5

Viikon tavoitteeksi olin asettanut kahden tietoturvapalvelimen versiopäivitykset, sekä päivitysten jälkeiset agenttipäivitysjakelut asiakasympäristöissä.

Päivitysten aikana huomasin hyödyntäväni muutaman viikon aikana keräämääni kokemusta tietoturvapalvelinten ylläpidosta, ja kykenin itsenäisesti suoriutumaan työstäni ilman tarvetta tukeutua toisten apuun työni suorittamisessa. Totesin, että mahdollisten ongelmatapausten kohdalla olisin kyennyt käyttämään ohjelmistotoimittajan teknistä tukikanavaa, eli omasin riittävän osaamistason ja keinot työtehtävän valmiiksi saattamiseen.

Päivitysten jakelu asiakasympäristöihin tapahtui mielestäni hyvin aikataulutettuina, ja järkeviin osiin jaettuina paloina. Asiakasympäristöissä ei kohdattu päivitysten aiheuttamia ongelmia, eivätkä suoritetut päivitystyöt häirinneet asiakasyritysten käyttäjiä.

Viikon analyysin kohteeksi on otettu viikon aikana työtehtävässäni kohtaamani internet-sivujen mainepalvelut. Sivujen mainepalvelut on tarkoitettu internet-sivuja käyttävien käyttäjien suojaamiseen, etukäteen tarkistamalla sivujen sisältö haitallisen sisällön varalta (Trend Micro, 2019). Mainepalvelut myös luokittelevat sivut sisällön perusteella esimerkiksi uutis-, aikuis-, ja vedonlyöntisisällöiksi (Cisco Talos Intelligence 2019).

Moderni päätelaitteen tietoturvaohjelma tarkistaa pilvestä löytyvästä tietokannasta käyttäjän käyntikohteena olevan internet-sivun, ja jos sivu on aiemmin todettu turvalliseksi, sallitaan käyttäjän pääsy sivulle. Jos aiemmassa tarkistuksessa sivun sisältö on todettu haitalliseksi, voidaan tietoturvaohjelman asetuksilla käyttäjää varoittaa sivulta löytyvästä haitallisesta sisällöstä, tai käyttäjän pääsy sivulle kokonaan estää.

Jos sivulla ei aiemmin ole vierailtu, suoritetaan sivun sisällön tarkistaminen haittaohjelmien varalta, ja sivun sisältö luokitellaan. Sivun sisällön tarkistaminen ensimmäisen käynnin jälkeen kuitenkin mahdollistaa sen, että ensimmäisellä käynnillä käyttäjä kohtaa sivulla olevaa haitallista sisältöä. Tietoturvaohjelmissa on mahdollista estää tarkistamattomalle ja luokittelemattomalle sivulle pääsy (Trend Micro 2019), mutta tämä asetus estäisi kaikille tarkastamattomille mutta turvallisille sivuille pääsyn.

Tietoturvaohjelman internet-selaimeen asennettava selainlaajennus suojaa käyttäjää etsittäessä sivuja hakukoneella. Turvalliset hakutulokset merkitään hakutuloksiin käyttäjälle, samoin haitallisiksi todetut ja vielä tarkistamattomat sivut, joista käyttäjää kyetään näin ennalta varoittamaan.

Trend Micron työasematuotteet sisältävät suojausasetuksia, mitkä asetusten tasosta riippuen estävät pääsyn varmasti tai mahdollisesti haitalliselle sivulle. Lisäksi asetuksilla voi estää käyttäjää pääsemästä vielä tarkistamattomalle sivulle. Asetuksissa voidaan myös aina estää tai aina sallia tietty sivuosoite (Trend Micro 2019).

Oikein toimiessaan mainepalvelu on käyttäjiä haitalliselta sivusisällöltä suojaava palvelu. On kuitenkin todettava, että turvalliseksi merkitty sivu on tarkistettu vain tunnetuilta haittaohjelmilta, ja sivu voi olla saastunut toistaiseksi tuntemattomalla haittaohjelmalla. Lisäksi turvalliseksi todettu sivu voi suoritetun tarkistuksen jälkeen olla saastunut haittaohjelmalla, minkä takia mainepalvelu ei mahdollista täydellistä suojaa haitallisia sivuja vastaan.

3.6 Viikko 6

Syyslomalla

3.7 Viikko 7

Maanantai

Syyslomaviikon jälleen aloitan maanantain käsittelemällä edellisellä viikolla saapuneita sähköposteja, sekä läpikäymällä tämän viikon kalenteria. Osaamiseni kehittämisen tavoitteeksi asetan Apple macOS -tietokoneiden tietoturvaan tutustumisen Trend Micro –tietoturvaohjelmiston näkökannasta. Viikolla tulen myös tutustumaan Trend Micro OfficeScan –palvelimen ohjelmistoversion päivittämiseen uudempaan versioon.

Sähköpostien läpikäynnin jälkeen, muokkaan aamulla yrityksemme oman työasemaympäristömme tietoturvapalvelimemme tietoturvapolitiikkoja. Työasemissa on havaittu käynnistyksen jälkeistä hitautta, minkä oletetaan johtuvan muutamasta käytössä olevasta tietoturva-asetuksesta. Muokkaan asetuksia uuden määrityksen mukaiseksi, ja merkitsen itselleni myöhemmälle viikolle muistutuksen tarkistaa, onko muutetuilla asetuksilla ollut toivottuja vaikutuksia.

Aamupäivällä läpikäyn kollegani kanssa samaiselle tietoturvapalvelimelle myöhemmin iltapäivällä tehtävää päivitystyötä. Kollegani on selvittänyt palvelimen ja tietoturva-agenttien vä-

listä ongelmaa, mikä tultaisiin korjaamaan ohjelmistotoimittajan tuottamalla korjauspäivityksellä. Valmistelen iltapäivän päivitystyötä kytkemällä palvelimelta agenttien versiopäivitykset pois päältä.

Ennen keskipäivää läpikäyn aamulla tekemiäni asetusmuutoksia, ja tarkistan Trend Micron internet-sivuston tukidokumentteja mahdollisten lisäasetusmuutosten varalta.
Keskipäivällä jatkan viime viikolla suorittamiani jaettujen tietoturvapalvelimien asiakkaiden agenttipäivitysten jakelua. Aloitan tarkistamalla ensin ensimmäisen palvelimen päivitysten tilanteen, listaan päivittyneiden ja vielä päivittämättömien agenttien määrät, ja kohdistan uudelle ryhmälle päivitysjakelun. Teen saman työn myös kahdelle muulle tietoturvapalvelimelle, ja dokumentoin tekemäni työn.

Iltapäivällä osallistun kollegani kanssa yrityksemme oman tietoturvapalvelimen päivitystyöhön, minkä suoritamme yhdessä kokoukseen etäyhteydellä osallistuvan Trend Micron teknisen asiantuntijan kanssa. Palvelimelle asennetaan ohjelmistotoimittajan korjauspäivitys, minkä jälkeen kohdistamme korjauspäivityksen mukana tulleen tietoturva-agentin päivityksen muutamalle testiryhmään kuuluvalle agentille.

Tarkistamme, että agentit päivittyvät uuteen versioon, ja testaamme, toimiko korjauspäivitys odotetusti. Selviää, että vaikka korjauspäivitys on asentunut sekä palvelimelle että agenteille, ei päivitys ole korjannut palvelimen ja agenttien välistä ongelmaa.
Läpikäymme palvelimen määrityksiä yhdessä teknisen asiantuntijan kanssa, ja löydämme ongelman aiheuttajan, minkä korjaamme kuntoon. Toteamme ongelman ratkenneen, ja korjauksen onnistuneen.

Edellisen kokouksen päätyttyä, selvitän asiakas N:n tietoturvapalvelimen ilmoitusasetuksia. Kyseisiä asetuksia käytetään, jos palvelimelle yhteydessä olevilla agenteilla havaitaan haittaohjelmia. Tieto haittaohjelma-havainnoista lähtee tietoturvapalvelimelta raportointipalvelimelle, mistä tieto edelleen välitetään haittaohjelmien torjuntaa hoitavalle ryhmälle.

Tiistai

Aamulla alan läpikäydä Trend Micron dokumentaatiota koskien OfficeScan-palvelimen 11-version päivitystä versioon XG. Aiemman 11-ohjelmistoversion ylläpito päättyy vuoden lopulla, ja yksi tässä versiossa oleva tietoturvapalvelin on päivitettävä XG-ohjelmistoversioon.
Lyhyen etsimisen jälkeen löydän Trend Micron sivustolta ohjedokumentin, missä esitellään versiopäivitys, vertaillaan 11- ja XG-versioiden tärkeimpiä eroja, sekä läpikäydään päivityksen suorittaminen.

Dokumentissa esitellään selkeä päivityspolku versionumeroineen, ja koen kykeneväni suorittamaan päivityksen ohjetta noudattamalla. Läpikäyn kollegani kanssa päivityksen suorittamisen ja ohjedokumentin, ja kollegani ehdottaa tarkistamaan Trend Micron tukipalvelusta, liittyykö päivitykseen mahdollisesti muita työvaihteita tai huomioitavaa kuin ohjeessa mainitut. Avaan Trend Micron tukipalveluun työpyynnön, missä esittelen palvelimen nykytilan ja päivityksen tavoitteen, ja pyydän mahdollisia lisätietoja päivityksen suorittamisesta.

Aamupäivällä osallistun kokoukseen, missä käsittelemme tietoturvapalvelimia. Läpikäymme palvelimien tilaa asennettujen päivitysten ja päivitystarpeen kannalta. Omalta osaltani esittelen asiakkaiden jaettujen tietoturvapalvelimien tilannetta jakamalla valmistelemani taulukon palvelimista ja niihin asennetuista palvelimista kokoukseen osallistujille.

Keskipäivän jälkeen jatkan maanantaina suorittamaani jaettujen tietoturvapalvelimien agenttiversiojakelua. Aloitan työn keräämällä ensin palvelimelta listauksen päivitysten tilanteesta. Vertaan päivittyneiden agenttien määrää maanantain tilanteeseen, ja totean, että lähes kaikki päivityksen kohteena olleet agentit ovat päivittyneet. Kohdistan palvelimella seuraavan erän agentteja agenttipäivityksen kohteeksi. Suoritan vastaavan työn myös kahdelle muulle tietoturvapalvelimelle, ja merkitsen itselleni kalenterimuistutuksen tarkistaakseni myöhemmin päivitysten tilanteen.

Keskiviikko

Aloitan keskiviikkoaamun tutustumalla tarkemmin tiistaiaamupäivällä lukemaani tietoturvapalvelimen versiopäivitysohjeeseen. Vaikka ohjeessa kuvataankin päivityksen läpikäynti, päätän kirjoittaa lyhyen palvelimen versiopäivitysohjeen, käyttämällä pohjana Trend Micron ohjetta. Kuvaan dokumentissa oman palvelimemme lähtötilanteen, päivityksessä suoritettavat työvaiheet, sekä selvitän ja dokumentoin päivityksessä tarvittavat kolme päivitystiedostoa. Valmistuva dokumentti tulee jatkossa toimimaan yrityksemme sisäisenä ohjeena ohjelmistoversiopäivitystä suoritettaessa.

Aamupäivällä tarkistan yhden tietoturvapalvelimen käyttöjärjestelmäpäivitysten tilan. Kyseessä on vanha, käytöstä lähiaikoina poistuva palvelin. Kyseinen palvelin tarjoaa minulle hyvän mahdollisuuden tutustua tuotantokäytössä pitkän ajan olleen palvelimen päivityshistoriaan. Totean, että palvelimelta puuttuvat uusimmat Windows-korjauspäivitykset. Tietoturvapalvelimien käyttöjärjestelmäpäivitykset hoidetaan keskitetysti, eli kyseinen palvelin pitäisi olla päivitysten suhteen ajan tasalla.

Alan selvittämään, mistä syystä palvelimen päivitykset ovat jääneet asentumatta. Tarkemman ongelmanselvitystyön jälkeen palvelimelta löytyykin virhetila, mistä syystä palvelimelle kohdistetut käyttöjärjestelmäpäivitykset ovat epäonnistuneet. Koska kyseessä on käytöstä poistuva palvelin, eikä palvelimella enää ole asiakkaiden tietoturva-agentteja, totean että laajempi ongelmanselvitystyö ei ole tässä tapauksessa tarpeellista, sillä palvelin tullaan poistamaan käytöstä.

Aamupäivän lopuksi edistän asiakas D:n tietoturva-agenttien siirto- ja päivitysprojektia. Asiakkaan muutamalle tietokoneelle on kohdistuttu asennuspaketti, millä ensin poistetaan asennettu tietoturva-agentti, minkä jälkeen tietokoneelle asennetaan uusi agenttiversio, ja määritystiedostolla agentti kohdistetaan asiakkaan organisaatiorakenteen alle.

Asennuspaketti on kohdistettu muutamalle tietoturva-agentille, mutta tietoturvapalvelimelta näen, että agentit eivät ole siirtynyt uudelle palvelimelle. Otan yhteyttä asiakkaaseen, ja yhdessä yhteyshenkilön kanssa tarkistamme kyseisten tietokoneiden tilan. Sovimme asiakkaan kanssa, että kyseisille tietokoneille kohdistetaan uudelleen siirron suorittava asennuspaketti, ja tulen tarkistamaan siirron onnistumisen myöhemmin viikolla.

Keskipäivän jälkeen suoritan testiympäristössä vanhan tietoturva-agentin testausta. Asiakkaiden vanhoja agentteja päivitettäessä on havaittu ongelma saada vanha agenttiversio päivittymään uuteen versioon. Vaikka agentti on yhteydessä tietoturvapalvelimeen ja kykenee raportoimaan tilansa palvelimelle, ei agentti kykene päivittämään itseänsä palvelimelta saatavalla uudella agenttiversiolla.

Selvitän kyseistä ongelmaa asentamalla testitietokoneelle ensin vanhan agenttiversion, minkä jälkeen kohdistan kyseiselle agentille palvelimelta agentin versiopäivityksen. Totean, että testiympäristössä vanha agentti kykenee päivittämään itsensä uuteen versioon. Ongelma todennäköisesti aiheutuu asiakkaiden agenteista, mitkä eivät enää kykene päivittämään itseään uuteen versioon. Keskustelen asiasta kollegani kanssa, ja hänen tiedossaan on aiempia vastaavia tapauksia, missä pitkään käytössä olleet tietoturva-agentit ovat toiminnaltaan korruptoituneita, eivätkä enää kykene päivittymään uuteen versioon. Ongelman toistaiseksi ainoaksi toimivaksi todettu korjaustapa on ollut poistaa kyseinen agenttiasennus ja asentaa tilalle uusi.

Iltapäivän lopuksi edistän asiakas G:n agenttien päivitysprojektia. Päivitän yhteenvedon jo siirretyistä ja vielä siirtoa odottavista agenteista, ja kommunikoin tilannetiedon asiakkaalle sähköpostitse. Samaan viestiin lisään tiedon myöhemmin viikolla siirrettävistä agenteista.

Torstai

Aloitan aamun selvittämällä kollegani pyynnöstä asiakas O:n tietoturva-agenttien tilannetta ja päivitysten jakelua tietoturvapalvelimelta. Kokoan palvelimelta listauksen asiakkaan agenteista versionumeroineen, ja lisään listaukseen tiedon agenttien uusimmasta yhteydenottohetkestä. Listauksen valmistuttua toimitan tiedot kollegalleni.

Aamupäivällä tarkistan tietoturvapalvelimilta omien tietoturva-agenttiemme tilan ja versiotiedot. Käynnissä on agenttien siirtoprojekti vanhalta tietoturvapalvelimelta uudelle, ja tehtäväni on selvittää, mitkä agentit ovat vielä siirtämättä uudelle palvelimelle. Siivoan samalla uudelle palvelimelle siirrettyjen agenttien kopiot pois vanhalta palvelimelta. Toimitan listauksen asiasta tiedustelleelle kollegalleni.

Tämän jälkeen aloitan tutustumisen Trend Micro OfficeScan -palvelimen Apple macOS –tietoturvatuotteeseen. Tuote on tarkoitettu työpöytäympäristön macOS-tietokoneiden suojaamiseen. Käytän aamupäivän lopun tutustumisella Trend Micron sivuilta löytyvään tuotteen esittelymateriaaliin.

Keskipäivän jälleen jatkan etsimällä ja läpikäymällä tarkempaa teknistä tietoa Trend Micro Apex One for Mac –tuotteesta. Tuote vaikuttaa dokumenttien perusteella sisältävän Windows-versiota vähemmän määritettäviä ominaisuuksia. Oletan eron johtuvat macOS-käyttöjärjestelmän teknisistä rajoituksista, mitkä estävät osaa Windows-tuotteen ominaisuuksista toimimasta.

Luen iltapäivällä pääkäyttäjille suunnattua materiaalia Apex One for Mac –tuotteesta. Dokumenttien perusteella opin, että Trend Micro Apex One for Mac –palvelin asennetaan OfficeScan-palvelimen lisäosaksi, eli kyseessä ei ole itsenäinen tuote vaan vaatii aiemmin asennetun OfficeScan-palvelimen alustakseen. Tutustun lisäksi Apex One for Mac –palvelimen asentamiseen ja ylläpitämiseen, sekä macOS-agentin asennus- ja ylläpitotapoihin.

Tarkistan OfficeScan-palvelimiltamme Apex One for Mac –palvelimien versiotiedot, ja totean palvelimien tarvitsevan uusimmat päivitykset asennettaviksi. Varaan itselleni perjantaille aikaa läpikäydä ja päivittää palvelimet uusimpaan versioon.

Iltapäivän lopuksi hoidan asiakas P:ltä saapuneen työpyynnön, missä tiedustellaan asiakkaan ympäristössä käytettävän tietoturva-agentin versioyhteensopivuutta uusimman Windows 10 –Ominaisuuspäivityksen kanssa. Tuotan asiakkaalle sähköpostilla listauksen, mihin kokoan asiakkaan agentit versionumeroineen, sekä lisään tiedon jokaisen agentin yhteensopivuudesta Windows 10 –Ominaisuuspäivityksen kanssa.

Perjantai

Osallistun aamulla tietoturvapalveluiden viikoittaiseen kokoukseen, missä läpikäymme asiakkaiden projektien tilaa, ja tärkeimmiksi luokiteltuja asiakasympäristöjen työpyyntöjä. Kokouksessa keskitymme muutamaan suurimpaan asiakkaaseen, ja vaikka itse en ole osallistunut näiden asiakkuuksien ympäristöjen ylläpitoon, tarjoaa kokous hyvän esittelyn näiden nykytilasta ja asiakkailla esiintyvistä ongelmista.

Olin eilen torstaina tutustunut Apex One for Mac –tuotteeseen, ja nyt aamupäivällä suoritan tuotteen versiopäivityksen yhdelle OfficeScan-palvelimista. Apex One for Mac on OfficeScan-palvelimen laajennusosa, ja versiopäivitys suoritetaan päivittämällä OfficeScan-palvelimen kyseinen laajennus.

Päivitys on helppo suorittaa: Laajennusosa ladataan palvelimelle, ja suoritetaan latauksen jälkeen. Päivitys päivittää Apex One for Mac –palvelimen, minkä jälkeen päivitetty palvelin on käyttövalmis, ja päivittynyt tietoturva-agentti jaettavissa agenteille.

Päivityksen jälkeen läpikäyn palvelimen tietoturva-asetukset, ja lisään uuden agentin päivityksen jaeltavaksi Mac-agenteille.

Iltapäivällä suoritan vastaavan Apex One for Mac –päivitystyön kahdelle muulle tietoturvapalvelimelle. Tarkistan näidenkin palvelimien tietoturva-asetukset, ja käynnistän päivittyneen tietoturva-agentin jakelun Mac-agenteille.

Iltapäivällä avaan Trend Micron tekniseen tukeen työpyynnön CUT Tool –poistotyökalun uuden version tilaamisesta. Kyseinen työkalu on tarkoitettu tietoturva-agentin poistamiseen tietokoneelta, ja työkalu kykenee suorittamaan poiston, vaikka agentti on suojattu poistoa vastaan suojaussalasanalla. Työkalu on tarkoitettu tilanteisiin, missä agenttia ei käytännössä muilla keinoilla saada poistettua tietokoneelta.

Koska työkalu ohittaa agentin oman salasanasuojauksen, on Trend Micro tietoturvasyystä rajannut työkalun käyttöiän 90 päivään. Tämän käyttöiän jälkeen työkalu lakkaa toimimasta, eli asiattomaan käyttöön levinneen työkalun käyttö on tällä keinolla estetty. Työpyynnössäni pyydän yritykselleme työkalusta uuden version, millä on käyttöikää uudet 90 päivää.

Iltapäivän päätteeksi saan kollegaltani työpyynnön tarkistaa asiakas F:n tietoturva-agenttien yhteensopivuuden uusimman Windows 10 –Ominaisuuspäivityksen kanssa. Tarkistan palvelimelta, että asiakkaan lähes kaikki agentit ovat ominaisuuspäivityksen suhteen uudessa, yhteensopivassa versiossa, mutta muutama agentti vielä vaatii päivityksen uuteen versioon.

Viikkoanalyysi 7

Viikon tavoitteeksi asetin Apple macOS –käyttöjärjestelmän tietoturvaan tutustumisen Trend Micro –tietoturvatuotteiden kannalta. Viikolla keräsin tietoa Trend Micro Apex One for Mac –palvelintuotteesta, millä hallinnoidaan macOS-tietoturva-agenttien asetuksia työasemissa. Tuotteesta minulla ei ollut aiempia kokemuksia, mutta viikon loppuun mennessä kykenin ylläpitämään Apex One for Mac –palvelimia, ja sekä päivitin palvelimet uusimpaan päivitysversioon, että jakelin uudet tietoturva-agentit Mac-käyttäjille.

Tässä viikkoanalyysissä käsittelen Apple macOS-käyttöjärjestelmän tietoturvaa, sekä analysoin mitä lisäominaisuuksia erillinen tietoturvaohjelma tuo macOS-käyttöjärjestelmään. macOS-käyttöjärjestelmän ydin perustuu avoimeen lähdekoodiin, valtaosin BSD Unixiin. Mikroydin puolestaan perustuu Mach-mikroytimeen. Apple on pyrkinyt suunnittelemaan käyttöjärjestelmänsä turvalliseksi, mutta samaan aikaan helpoksi käyttäjien sitä käyttää, määrittää ja hallita (Apple 2019).

Sovellusten turvallisuus pyritään takaamaan sallimalla vain luotettujen sovellusten asennus. Käyttöjärjestelmän Gatekeeper-ominaisuus voidaan määrittää sallimaan vain allekirjoitettujen sovellusten asennus Applen App Storesta. Oletuksena Developer ID –allekirjoitettujen sovellusten asennus on myös hyväksytty. Havaittuaan haittaohjelman, Apple voi hylätä kehittäjän Developer ID:n, minkä seurauksena haitalliseksi todettua sovellusta ei enää voida levittää. Tietokoneen käyttäjällä on kuitenkin mahdollista asentaa kyseinen sovellus, näin ohittaen Gatekeeper-suojauksen.

XProtect on Applen haittaohjelmia tunnistava teknologia, mikä havaitsee tunnettuja haittaohjelmia säännöllisesti päivittyvien tunnisteiden avulla. Teknologia ei kuitenkaan kykene havaitsemaan haittaohjelmia, mitä vastaan ei vielä ole ehditty tunnisteita rakentamaan. Apple julkaisee päivityksiä myös macOS-käyttöjärjestelmään, millä mahdollistetaan saastuneen käyttöjärjestelmän itse puhdistavan itsensä. Haittaohjelma kyetään kuitenkin poistamaan tietokoneelta vasta kun se osataan tunnistaa ja löytää.

Trend Micro Apex One for Mac mahdollistaa macOS-tietoturvan kasvattamisen seuraavin keinoin (Trend Micro 2019):

- Predictive Machive Learning
- Device Control
- Enhanced Smart Scan
- Web Reputation

Koneoppimiseen perustuva Predictive Machine Learning kykenee suojaamaan tietokoneen aiemmin tunnistamattomilta tai tuntemattomilta uhilta arvioimalla millä todennäköisyydellä tiedoston sisällössä voi olla haittaohjelma, sekä mahdollisen uhan tyypin. Tekniikka kykenee suojaamaan vielä toistaiseksi tuntemattomilta haittaohjelmilta.

Device Control mahdollistaa ulkoisten laitteiden ja verkkoresurssien käytön estämisen. Teknologialla voidaan rajoittaa tiedon katoamista tai sen päätymisen vääriin käsiin. Device Controlia käyttäen voidaan myös rakentaa lisäsuojaus tietoturvariskejä vastaan.

Enhanced Smart Scan on kehittyneempi, pilvitunnisteisiin perustuva haittaohjelmien havaintoteknologia. Pilviteknologialla mahdollinen haittaohjelmahavainto voidaan välittää pilveen analysoitavaksi, ja haittaohjelmaksi varmistunutta ohjelmaa vastaan voidaan tuottaa ja levittää tunniste kaikille tätä pilvisuojauspalvelua käyttäville.

Web Reputation –teknologia suojaa tietokonetta haitallisilta tai mahdollisesti vaarallisilta internet-sivustoilta varoittamalla tai estämällä käyttäjän pääsy sivulle.

3.8 Viikko 8

Maanantai

Kalenterin perusteella viikosta on tulossa monipuolinen, sisältäen asiakasprojektien edistämistä ja tietoturvapalvelimien ylläpitotyötä. Asetan viikon tavoitteekseni edelleen vahvistaa edellisellä viikolla keräämääni osaamista macOS-tietoturvasta.

Työviikko alkaa maanantaiaamun toimitusjohtajan tilannekatsauksella. Tässä säännöllisesti järjestettävässä kokouksessa läpikäydään yrityksen loppukesän ja syksyn asioita, sekä luodaan näkemys vuoden loppukuukausiin ja seuraavaan alkuvuoteen.

Kokouksen jälkeen aloitan listaamalla asiakas E:n OfficeScan-tietoturvapalvelimella olevat tietoturva-agentit. Asiakkaan agentteja on siirretty Apex One –tietoturvapalvelimelle, ja tarkistan, kuinka monta siirtämätöntä agenttia vielä on jäljellä.

Yrityksemme omia agentteja on siirretty OfficeScan-palvelimeltamme uudelle Apex One –palvelimellemme, ja aamupäivällä läpikäyn sekä vanhalla että uudella palvelimella olevia agentteja. Palvelimien agentteja vertailemalla totean, että valtaosa agenteistamme on jo siirretty, ja listaan ylös vielä siirtämättömät agentit. Samalla poistan vanhalta palvelimelta jo siirretyt agenttien kaksoiskappaleet.

Aamupäivällä käsittelen saapuneen työpyynnön tarkistaa, miksi asiakkaan agenttien tietoturvapäivitykset eivät ole ajan tasalla. Tutkin tietoturvapalvelimelta noudettujen päivitysten lokia, ja vertaan virustunnistepäivitysten versionumeroita toisen palvelimen vastaaviin päivityksiin. Totean, että tietoturvapalvelin ei ole kyennyt noutamaan uusimpia päivityksiä, ja myös palvelimen päivitysten lokissa on merkintä noudon epäonnistumisesta. Ajan päivitysten haun manuaalisesti, ja merkitsen itselleni muistutuksen tarkistaa palvelimen tilanteen myöhemmin maanantaina.

Aamupäivän lopuksi tarkistan yhden tietoturvapalvelimen laajennusten päivitystilanteen, ja päivitän palvelimelle muutaman julkaistun laajennuspäivityksen.

Keskipäivän jälkeen läpikäyn asiakkaiden omien tietoturvapalvelimien versiotilanteen. Kyseessä olevat palvelimet ovat niiden asiakkaiden käytössä, joiden omien tietoturvavaatimusten tai agenttimääränsä takia tarvitsevat oman palvelimen. Aloitan selvittämällä palvelinten verkko-osoitteet ja tarvittavat käyttäjätunnukset ja salasanat. Lisäksi tarvitsen tehtävään tiedon uusimmista päivitysversioista, minkä tiedon etsin Trend Micron sivustolta. Tarkistaessani palvelinten versioita, dokumentoin samalla löydökseni palvelindokumenttiin, mistä nykyiset versiot ovat jatkossa helposti saatavilla. Merkitsen taulukkoon ajan tasalla ja päivityksiä tarvitsevat palvelimet eri väreillä.

Iltapäivällä suoritan yhdelle tietoturvapalvelimelle versiopäivityksen asennuksen. Palvelimella ei tällä hetkellä ole tietoturva-agentteja, eli tyypillisesti tehtävää agenttipäivitysten poiskytkemistä ei tässä tapauksessa tarvitse palvelimelle tehdä. Ennen päivitystä suoritan palvelimelle varmuuskopioinnin, ja päivityksen jälkeen tarkistan palvelimen toiminnan, minkä jälkeen totean päivityksen valmiiksi suoritetuksi.

Saatuani palvelimen päivityksen valmiiksi, läpikäyn asiakkaiden käytössä olevien Trend Micro for Mac –tietoturvapalvelimien agenttipolitiikkojen asetuksia tietoturvan kannalta. Vertailen asiakkaille rakennettuja sääntöjä, ja suoritan muutaman säännön muutoksen koventaakseni asiakkaiden tietoturvan tasoa.

Maanantai-iltapäivän lopuksi tarkistan manuaalisesti päivittämäni tietoturvapalvelimen tilanteen, ja totean palvelimen nyt päivittäneen uusimmat virustunnisteversiot.

Tiistai

Maanantaina läpikävin asiakkaiden omat tietoturvapalvelimet, tarkistaen palvelimilta versiotilanteet ja päivitystarpeet. Tänään tarkistan samoilta palvelimilta käyttöjärjestelmäpäivitys-

ten tilanteen. Maanantaina suoritin versiotarkistuksen kirjautumalla selaimella tietoturvapalvelimien hallintakonsoliin, mistä versiotiedot ovat luettavissa. Käyttöjärjestelmäpäivityksien tilanteen näen kirjautumalla etäyhteydellä palvelimien työpöydälle, mitä kautta voin tarkistaa asennetut käyttöjärjestelmäpäivitykset.

Työtä varten selvitän palvelimien paikalliset kirjautumiskäyttäjätunnukset, ja kirjaudun palvelimille etätyöpöytäyhteydellä. Vertaan palvelimelta näkyvää tilannetta palvelinten hallintaympäristön raporttiin. Lisään palvelinten päivitystilanteen maanantaina aloittamaani palvelindokumenttiin.

Keskipäivän jälleen selvitän asiakas L:n macOS-agenttien määrän ja tilan tietoturvapalvelimelta, ja pidän asiakkaan kanssa puhelinkokouksen asiasta. Läpikäyn puhelimessa palvelimelta löytyvät macOS-agentit, ja toteamme että yksi palvelimelle yhä yhteydessä olevista macOS-agenteista on asiakkaalta jo poistunut tietokone, mistä ei ole poistettu tietoturva-agenttia. Opastan asiakasta keinoista poistaa kyseinen agentti. Puhelun jälkeen toimitan asiakkaalle nykyisen version agentin asennuspaketista, minkä oheen liitän puhelimessa asiakkaalle esittelemäni agentin poisto-ohjelman.

Iltapäivällä listaan asiakas Q:n tietoturva-agenttien määrät sekä OfficeScan- että Apex One –tietoturvapalvelimilla. Agenttimääriä tullaan tarvitsemaan käynnistyvässä agenttien siirtoprojektissa vanhalta palvelimelta uudelle.

Lopun iltapäivää käytän selvittääkseni, miksi Tietoturvan raportointipalvelimella havaitaan eri määrä macOS-agentteja kuin yhdellä Apex One for Mac –tietoturvapalvelimella. Toimiessaan oikein, tietoturvapalvelin raportoi agenttimääränsä raportointipalvelimelle, ja agenttimäärät ovat samat näillä molemmilla. Nyt havaitussa ongelmassa tietoturvapalvelimen macOS-agentit eivät näy raportointipalvelimella, mutta samaisen tietoturvapalvelimen Windows-käyttöjärjestelmän agentit raportoituvat oikein. Avaan ongelmasta vianselvityspyynnön Trend Micron tekniseen tukeen.

Keskiviikko

Jatkan tiistaina aloittamaani macOS-tietoturva-agenttien vianselvitystyötä. Tiistai-iltapäivän jälkeen olen saanut Trend Micron tuesta pyynnön vianselvityksessä tarvittavista lisätiedoista. Listaan palvelimella olevat macOS-agentit, ja poimin palvelimelta tiedot agentin raportoimasta IP-osoitteesta ja uusimmasta yhteyspäivämäärästä ja –ajasta. Näitä tietoja käyttäen etsin raportointipalvelimelta puuttuvia macOS-agentteja sekä nimellä että agentin IP-osoitteella, mutta joudun toteamaan, että näilläkään tiedoilla etsittäessä toisella palvelimella näkyviä agentteja ei löydy toiselta.

Aamupäivän lopuksi tarkistan asiakas G:n agenttien tilan sekä nykyisellä että uudella tietoturvapalvelimella. Kokoan agenttien siirron tilanteesta raportin, minkä lähetän asiakkaalle sähköpostiviestinä.

Keskipäivän jälkeen käsittelen asiakas R:ltä saapuneen työpyynnön poistaa tietokoneelta tietoturva-agentti. Kyseinen asiakas on korvaamassa käyttämänsä Trend Micro –tietoturvatuotteen toisella ohjelmistolla, ja työpyynnössä mainitulta tietokoneelta pyydetään poistamaan tietoturva-agentti. Sovin asiakkaan kanssa hänelle sopivan ajan agentin poistoa varten etäyhteyden yli.

Työpyynnön jälkeen valmistelen asiakas S:n tietoturvapalvelimen tulevaa päivitystyötä varten. Poistan agenttien päivitysjakelun pois päältä, ja tiedotan asiakasta palvelimelle myöhemmin tehtävästä päivityksestä.

Käynnistymässä on projekti siirtää tiettyjen asiakkaiden tietoturva-agentit nykyisiltä OfficeScan-palvelimilta Apex One –palvelimelle. Tietoturvapalveluiden esimiehen lähettämän asiakaslistauksen pohjalta läpikäyn OfficeScan-palvelimia ja palvelimilla olevia agenttimääriä. Rakennan dokumentin, missä palvelimet, asiakkaat ja agenttimäärät on listattu.

Iltapäivän lopuksi jatkan vielä raportointipalvelimelta puuttuvien macOS-agenttien vianselvitystyötä. Läpikäyn Trend Micron internet-sivuston tukiosiota, ja etsin ongelmaa koskevia tukiartikkeleita. Löydän muutaman ongelmaa sivuavan artikkelin, joissa mainittuja ohjeita seuraamalla yritän löytää vikaan mahdollista korjausta, tässä kuitenkaan onnistumatta.

Torstai

Jatkan torstaiaamulla eilistä vianselvitystyötä. Kokeilen poistaa ongelmasta kärsivän Apex One for Mac –tietoturvapalvelimen yhteyden raportointipalvelimelta, minkä jälkeen rakennan palvelimen yhteyden raportointipalvelimelle uudelleen. Merkitsen itselleni iltapäivälle muistutuksen tarkistaa, onko tämän korjauskeinon jälkeen macOS-agentit ilmestyneet raportointipalvelimelle.

Aamupäivällä vertailen OfficeScan-palvelimien raportointipalvelimella olevia agentteja Apex One –raportointipalvelimen agentteihin. Käynnissä on useampi projekti, missä agentteja siirretään OfficeScan-palvelimilta Apex Oneen, ja siirron yhteydessä agentti voi kahdentua, ollen siirron jälkeen sekä uudella että vanhalla palvelimella. Rakennan agenttilistaukset molemmista palvelimista, ja vertailemalla näitä kahta listaa keskenään, löydän kahdentuneet agentit. Tarkistan kahdentuneiden agenttien uusimmat yhteydenottopäivämäärät ja –kellonajat,

minkä perusteella totean kaikkien kahdentuneiden agenttien olevan aktiivisia Apex One –palvelimella. Tämän tiedon perusteella voin siivota kahdentuneet agentit pois OfficeScan-palvelimelta.

Suunnittelen asiakas R:n tietoturvapalvelimen päivityksen jälkeen tehtäviä agenttien päivityksiä. Asiakkaalta on saapunut lista pilottiagenttiasennuksista, ja tarkistan listalla olevien agenttien tilan palvelimelta.

Keskipäivän jälkeen suoritan yhden tietoturvapalvelimen versiopäivityksen. Aloitan päivityksen tekemällä tietoturvapalvelimen käyttöjärjestelmälle varmuuskopioinnin. Otan palvelimen työpöydälle etäyhteyden, siirrän palvelimelle päivitystiedoston, ja suoritan palvelimen päivityksen. Päivitystyön valmistuttua, tarkistan vielä palvelimen toiminnan testiympäristöön asennetulla agentilla.

Iltapäivällä suoritan OfficeScan-asennuspaketointia asiakkaan tulevaa asennusprojektia varten. Tietoturva-agentin poistamista varten Trend Micro on tuottanut CUT Tool –poisto- ja asennuspaketin. Asennuspaketointia tehdessäni huomaan, että testiympäristössä käyttämäni CUT Tool –työkalu ei toimi: Työkalu tuottaa virheen. Ongelmanselvitystyön jälkeen vian aiheuttajaksi selviää korruptoitunut työkaluversio, ja korvaamalla ohjelma verkkolevyltä löytyvällä versiolla, saan ongelman korjattua.

Perjantai

Olin aiemmin viikolla ollut yhteydessä asiakas L:ään, selvittääkseni heillä käytössä olevien macOS-agenttien määrää. Asiakkaalta nyt saadun tiedon perusteella siivoan käytöstä poistuneita agentteja pois tietoturvapalvelimelta. Tarkistan asiakkaalta, millä asennuspaketilla asiakkaan it-organisaatio suorittaa uusien tietokoneiden asennustyön. Totean käytettävän asennuspaketin olevan versioltaan vanhentuneen, ja sovin toimittavani asiakkaalle ajan tasalla olevan asennuspaketin.

Ennen keskipäivää, tarkistan OfficeScan-palvelimien raportointipalvelimen version ja päivitystarpeen. Selvitän, onko kyseiselle palvelimelle asennettavissa palvelimelta puuttuvia päivityksiä, mitkä mahdollisesti korjaisivat raportointipalvelimelta puuttuvien macOS-agenttien ongelman korjaamisessa. Asentamattomia päivityksiä raportointipalvelimelle ei kuitenkaan löydy Trend Micron päivitysten lataussivustolta.

Keskipäivän jälkeen jatkan macOS-agenttien vianselvitystyötä suorittamalla raportointipalvelimelle sisäisen tietokannan puhdistustyön. Työ suoritetaan raportointipalvelimen sisäisellä ylläpitotyökalulla, mikä suoritetaan kyseisellä palvelimella työpöytäetäyhteyden yli. Työkalu

läpikäy, siivoaa ja korjaa palvelimen tietokannan. Ajan työkalulla kannan puhdistustyön, mutta totean lyhyen testauksen jälkeen, ettei ongelma ole korjaantunut.

Iltapäivällä aloitan rakentamaan asennuspakettia aamulla yhteyttä ottaneelle asiakkaalle. macOS-käyttöjärjestelmän tietoturva-agenttien asennus- ja poistopaketti koostuu kahdesta tiedostosta, joista toisella agentti asentuu tietokoneelle, ja toiselle tarvittaessa suoritetaan asennuksen poisto. Yhteyttä palvelimella ottaessaan, vanha agenttiversio kykenee päivittämään itsensä uusimpaan versioon. Asiakkaalla on käytössään hyvin vanha asennuspaketti, minkä tilalle rakennan ja lähetän asiakkaalle uuden version.

Perjantai-iltapäivän lopuksi rakennan kollegani kanssa asiakas T:n tietoturvapalvelimelle monivaiheisen tunnistautumisen eli MFA:n (Multi-Factor Authentication). Perinteisellä kirjautumistavalla tietoturvapalvelimen hallintasivustolle kirjaudutaan selaimella, käyttäen käyttäjätunnuksena palvelimelle määritettyä käyttäjätunnus-salasana -paria. Käyttäjätunnuksen tuottama tietoturva voidaan ylläpitää vain salasanan ollessa turvassa, eikä vääriin käsiin joutunut käyttäjätunnus-salasana tarjoa muuta suojauskerrosta asiatonta käyttöä vastaan. MFA tarjoaa käyttäjän tunnistautumiseen lisäkerroksen, esimerkiksi vaatimalla kirjautuvalta henkilöltä sekä oikean kirjautumissalasanan että oikean käyttäjän hallussa olevaan matkapuhelimeen saapuvan tekstiviestikoodin syöttämisen kirjautumisen yhteydessä järjestelmään.

Viikkoanalyysi 8

Työviikon sisältöä jälkikäteen tarkastellessani koin viikon sisällöltään monipuoliseksi. Työni koostui kestoltaan lyhyistä, keskenään vuorottelevista työtehtävistä, missä kykenin käyttämään minulle kertynyttä teknistä osaamista. Viikon tavoitteeksi olin asettanut macOS-käyttöjärjestelmän Trend Micro –tuotteiden asiantuntemuksen kehittämisen, missä mielestäni onnistuin, pystyen hyödyntämään osaamistani suorittamissani työtehtävissä.

Viikon analyysiaiheessani käsittelen monivaiheista tunnistautumista eli MFA:a (Multi-Factor Authentication). Perinteinen käyttäjätunnus-salasana -yhdistelmä on turvallinen vain salasanan ollessa yksin haltijansa tiedossa. Salasanaa vastaan voidaan hyökätä esimerkiksi tietojenkalasteluviestillä, millä salasanan haltija erehdytetään paljastamaan salasanansa kalasteluviestin lähettäjälle. Salasana voi paljastua myös salaisuuden huolimattoman säilytyksen takia. Esimerkkinä tästä tavasta on salasanan säilyttäminen selkokielisessä muodossa, mikä mahdollistaa salasanan paljastumisen tietomurron yhteydessä (Helsingin Sanomat 2019).

Perinteistä käyttäjätunnus-salasana -paria turvallisempi tapa tunnistaa käyttäjä, on käyttää monivaiheista tunnistautumista (Microsoft 2019). Yksi esimerkki monivaiheisesta tunnistautu-

misesta on pankkien seteliautomaattien käyttö. Käyttäjä tunnistautuu automaattiin hallussaan olevalla yksilöidyllä maksukortilla, ja suorittaa toisen tunnistautumisen tiedossaan olevalla maksukortin PIN-koodilla. Ilman molempia näitä tunnisteita, käyttäjän tunnistautuminen hylätään.

Suositut ja yleisessä käytössä olevat palvelut, kuten Microsoft Office 365, ovat houkuttelevia kohteita tietojenkalasteluhyökkäyksille (Kyberturvallisuuskeskus 2019). O365-tilin käyttäjätunnus on helposti arvattavissa, palvelun käyttäjätunnuksen tyypillisesti ollessa käyttäjän sähköpostiosoite. Yrityksen henkilökunta saattaa olla esitelty yrityksen internet-sivuilla, samoin yrityksen käyttämä sähköpostiosoitteen muoto. Näillä tiedoilla käyttäjien käyttäjätunnukset ovat arvattavissa, ja käyttäjille voi lähettää heidän salasanojaan kalastelevia viestejä (Cisco 2019).

Tyypillinen kalasteluviesti on rakennettu erehdyttämään vastaanottajansa luulemaan viestin saapuneen yrityksen omasta it-organisaatiosta. Viestissä väitetään käyttäjän tunnuksessa olevan ongelman, minkä korjaamiseen tarvitaan käyttäjän tekemää kirjautumista viestissä olevaan osoitteeseen. Osoite johtaa palvelun kirjautumissivustolta näyttävälle sivulle, minne käyttäjä erehdytetään syöttämään käyttäjätunnuksensa salasana. Kirjauduttuaan sivustolle, saatetaan käyttäjä johtaa palvelun oikealle kirjautumissivustolle, missä tapauksessa käyttäjä ei välttämättä edes huomaa joutuneensa tietomurron kohteeksi. O365-palvelun tapauksessa käyttäjän käyttäjätunnuksella ja salasanalla on pääsy käyttäjän ja yrityksen tietoihin kaikkialta internetistä.

Monivaiheinen tunnistautuminen tuo suojauskerroksen käyttäjän tunnistautumiseen. O365-tunnus voidaan suojata esimerkiksi kirjautumisen yhteydessä käyttäjän matkapuhelimeen lähetettävällä koodin sisältävällä tekstiviestillä. Salasanan lisäksi myös tämä koodi on syötettävä palvelun kirjautumisen sitä pyytäessä, eikä palveluun pääse ilman salasanaa ja koodia. Käyttäjän tunnuksen murtaminen vaatisi hyökkääjältä tässä tapauksessa sekä käyttäjän salasanan selvittämisen että pääsyn käyttäjän matkapuhelimelle, tai hyökkääjän tulisi kyetä ohjaamaan käyttäjä tilapäisesti toiselle sivustolle, ja käyttäjän sinne syöttämillä salasanalla ja tekstiviestin koodilla itse kirjautua oikealle palvelun kirjautumissivulle.

3.9 Viikko 9

Maanantai

Kalenteria läpikäymällä totean viikosta tulevan monipuolisen. Työpäivät tulevat sisältämään useamman asiakasprojektin edistämistä, sekä teknistä kehitystyötä Trend Micro –tuotteiden

parissa. Asetan viikon tavoitteekseni asiakkaan tietoturvapalvelimen päivitystyön, ja erityisesti tulen huomioimaan työssä asiakkaan suuntaan tapahtuvan viestinnän päivitykseen liittyvissä asioissa.

Aloitan työviikon käsittelemällä asiakas R:ltä saapuneen kysymyksen koskien Windows 10 kahta uutta tietoturva-asetusta. Tamper Protection estää haittaohjelmia tekemästä muutoksia Windows Defender –haittaohjelmatorjunnan asetuksiin, ja Controlled folder access suojaa tietokoneella olevaa arvokasta dataa haittaohjelmilta.

Kyseessä ovat Windows 10 –käyttöjärjestelmän sisäiset suojausasetukset, ja ne ovat tarkoitettu käytettäviksi yhdessä käyttöjärjestelmän oman Microsoft Windows Defender –haittaohjelmantorjunnan kanssa. Työasemaympäristöissään asiakkaamme käyttävät tyypillisesti Trend Micron tuotteita haittaohjelmien torjunnassa, eikä em. suojausasetukset ole käytössä esimerkiksi Trend Micro –tuotteen kanssa.

Asiakas on kysymyksessään tiedustellut, pitäisikö kyseiset kaksi suojausasetusta olla kytkettynä päälle. Tutustun ensin tarkemmin näihin kahteen asetukseen, ja tarkistan asetusten yhteensopivuuden asiakkaan tietojärjestelmiin. En löydä ongelmia suojausten käyttöön ottamisen suhteen, ja vastauksessani asiakkaalle suosittelen kyseisten suojausasetusten päälle kytkemistä.

Aamupäivällä selvitän yrityksessämme omissa tietokoneissa havaittua hitautta käynnistyksen yhteydessä. Tyypillinen käyttäjien raportoima oire on kirjautumisen jälkeen esiintyvä ohjelmien hidas käynnistyminen ja suorituskyky muutaman minuutin ajan. Windows-käyttöjärjestelmän Tehtävienhallinnasta tilannetta tarkastellessa tietokoneen suoritin on käyttäjän kirjautumisen jälkeen täysin kuormitettuna Trend Micron haittaohjelmatuotteen toimesta usean minuutin ajan.

Aloitan ongelman selvitystyön ensin tarkastelemalla yrityksemme tietoturvaohjelmiston tietoturvapolitiikkaa. Totean, että käytettävät asetukset on tietokoneillamme määritetty toteuttamaan hyvin tarkkaa haittaohjelmien havainnointia, minkä kääntöpuolena on käyttäjiemme havaitsema tietokoneen käytön hidastuminen kirjautumisen yhteydessä.

Läpikäyn Trend Micron sivuilta dokumentteja, joissa toisaalta esitellään korkean tietoturvan mahdollistavat asetukset, mutta myös läpikäydään suositukset Windows-käyttöjärjestelmän kansioille ja tiedostoille, mitkä olisi tietokoneen sujuvan käytön vuoksi syytä ohittaa haittaohjelmatarkistuksissa.

Keskipäivän jälkeen jatkan tietoturvaohjelmiston aiheuttaman hitauden selvittämistä. Aamupäivällä läpikäymieni dokumenttien perusteella olen muodostanut listan asetuksista, joilla mielestäni ylläpidetään tietoturvan hyvä taso, samalla parantaen käyttäjien havaitsemia hitausongelmia. Keskustelen asiasta kollegani kanssa, ja päätämme testata ehdottamiani asetuksia ensin kohdistamalla asetukset testitietokoneelle.

Alkuiltapäivän aikana rakennan asetusten perusteella tietoturvapalvelimellemme uuden tietoturvapolitiikan, minkä testivaiheessa kohdistan vain testitietokoneelle. Tietokoneella tullaan suorittamaan suorituskykytestejä selvittääksemme uusien asetusten vaikutuksen havaittuihin suorituskykyongelmiin.

Maanantain loppuiltapäivän käytän kollegani kutsumana Windows-palvelimien tietoturvapolitiikan kehityskokouksessa. Trend Micro Apex One –tietoturvatuote on ensisijaisesti Windows-työasemakäyttöjärjestelmiin tarkoitettu, mutta Apex One –tuotteella voidaan suojata myös Windows-palvelinkäyttöjärjestelmiä. Tässä käytössä on huomioitava työpöytä- ja palvelintietokoneiden tyypillisen käyttötavan eroavaisuudet, ja myös tietoturvapolitiikat on syytä rakentaa erikseen työasema- ja palvelintietokoneille.

Kokouksessa läpikäymme tietoturvapolitiikan asetuksia ja niiden vaikutuksia palvelinkäyttöjärjestelmän suorituskykyyn. Iltapäivän aikana saamme rakennettua mallin säännöistä, mitä tulemme jatkossa käyttämään pohjana asennettaessa Apex One –tietoturvaohjelmisto palvelimille.

Tiistai

Tiistaina aamulla käsittelen sisäisen työpyynnön poistaa tarpeettomat VMware-virtualisointiympäristöön kertyneet palvelinvarmistukset. Toisin kuin päivittäiset varmuuskopiot, esimerkiksi ennen suoritettavaa asennustyötä tehtävä varmistus sisältää palvelimen tietyltä tarkasti määritetyltä hetkeltä. Suoritettaessa esimerkiksi ohjelmistoasennusta, virtuaalitietokoneelta otetulla varmistuksella voidaan tietokone palauttaa varmistuksen ottohetkeen, käytännössä palata aikaan ennen tietokoneella tehtyä asennustyötä.

Tarpeettomat varmistukset vievät tarpeetonta levytilaa, ja kertyneitä varmistuksia siivotaankin säännöllisesti tallennustilan vapauttamiseksi. Läpikäyn työpyynnössä listatut varmistukset, ja poistan itse tekemäni, nyt jo tarpeettomiksi jääneet varmistustiedostot virtualisointiympäristöstä.

Ennen aamupäivää, ehdin vielä suorittamaan testiympäristössä vanhan tietoturva-agentin päivittymistä koskevan testin. Asiakasympäristössä on havaittu, että tietty versio tietoturva-

agentista ei päivity uuteen agenttiversioon. Testaan asiaa asentamalla ensin vastaavan version tietoturva-agentista, ja kohdistamalla agentille palvelimelta agenttipäivityksen. Totean, että testiympäristössä kyseinen agentti kykenee päivittymään uuteen agenttiversioon ilman ongelmia. Keskustelen kollegani kanssa asiasta, ja kollega esittää aiemman kokemuksensa perusteella arvion, että asiakkaan agenttiohjelma on käytön aikana korruptoitunut, eikä vikaantumisen jälkeen enää kykene päivittymään uuteen versioon.

Keskipäivän jälkeen valmistelen lähitulevaisuudessa alkavaa asiakas U:n agenttien siirtoprojektia, listaamalla asiakkaan nykyiset tietoturva-agentit OfficeScan-palvelimilta. Kyseisessä projektissa asiakkaan tietokoneisiin tullaan asentamaan nykyisen OfficeScan-tuotteen tilalle Apex One –tuote.

Olen huomenna keskiviikkona suorittamassa asiakas S:n tietoturvapalvelimen versiopäivityksen, ja suoritan tänään iltapäivällä valmistelevia toimenpiteitä palvelimella. Tarkistan että aiemmin poiskytketyt päivitysjakelut ovat edelleen poissa käytöstä, ja siirrän huomenna tarvittavat päivitystiedostot valmiiksi palvelimelle. Läpikäyn samalla päivitykseen liittyvän dokumentaation, ja totean että päivityksen suoritustapa on minulle tuttu aiemmista päivitystöistä, enkä ennakoi päivityksessä ongelmia.

Edellisellä viikolla olin tuottanut asiakas L:lle macOS-käyttäjiä varten tietoturva-agentin asennuspaketin, ja asiakkaan nyt iltapäivällä otettua asiasta yhteyttä, tarkistin tietoturvapalvelimelle yhteyttä ottaneiden uusien agenttien tilan. Agentit olivat asentuneet oikein ja kohdistuneet asiakkaan organisaatiorakenteen alle.

Keskiviikko

Ensimmäiseksi aamulla tarkistan asiakas G:n tietoturva-agenttien siirron tilanteen. Asiakkaan etätoimipisteen yksi tietoturva-agentti oli ollut siirtoasennuksen kohteena, ja uudelta palvelimelta tarkistettuna agentti oli siirtynyt ja päivittynyt oikeaan versioon. Siivosin siirron aikana kahdentuneen agentin pois vanhalta palvelimelta, ja tiedotin asiakasta siirron onnistumisesta.

Aamupäivän käytin asiakas S:n tietoturvapalvelimen päivitykseen. Aloitin työn tekemällä virtuaalipalvelimesta varmuuskopion. Varmistuksen valmistuttua, kirjauduin palvelimelle työpöytäetäyhteydellä, ja suoritin tietoturvapalvelimen versiopäivityksen. Päivityksen suorittamisen jälkeen testasin testiympäristössä uuden agenttiversion asentuvan ilman ongelmia. Testauksen jälkeen totesin palvelimen päivityksen valmiiksi, ja kohdistin agenttipäivityksen suoritettavaksi asiakkaan pilottitietokoneille.

Keskipäivällä suoritin tietoturva-agentin versiopäivitystestausta, rakentamalla uuden version asennuspaketista ja suorittamalla asennuksen käsin testiympäristössä. Dokumentaation mukaan, käytettäessä asennuspaketin päivitystilaa, kykenisi agentti päivittämään vanhan version päälle asennuspaketissa olevan uuden version. Testatessa asennuspaketin toimivuutta, totesin asennuksen olevan kykenemätön suorittamaan suoraa päivitystä uuteen versioon. Kysyessäni kollegaltani asiasta, hän vahvisti, että dokumentaation vastaisesti agentin suora päivitys asennuspaketista ei toimi, ja toimivana tapana on poistaa ensin olemassa oleva vanha agentti, ja asentaa tilalle uusi agenttiversio.

Iltapäivällä suoritan asiakas K:n tietoturva-agenttien määrän tarkistuksen tuottamalla listaukset agenteista sekä vanhalta että uudelta tietoturvapalvelimelta. Näitä listoja vertailemalla poistan ensin kahdentuneet agentit. Tämän jälkeen rakennan jäljelle jääneistä kolmannen listauksen, minkä välitän myyntiorganisaatiomme jäsenelle. Läpikäymme hänen ja kollegani kanssa asiakkaan tietoturva-agenttien määrää, ja vertailemme lukua hallintapalvelimelta tuotettuun vastaavaan listaan. Päädymme agenttimäärässä lukumäärään, mikä vastaa etukäteen ennakoitua agenttimäärää, ja toteamme agenttien lukumäärän olevan selvitetty.

Torstai

Olin keskiviikkona suorittanut asiakas S:n tietoturvapalvelimen versiopäivityksen, sekä kohdistanut agenttipäivitykset asiakkaan määrittelemälle pilottiryhmälle. Tarkistan nyt torstaiaamuna pilottiagenttien tilanteen, ja totean valtaosan agenteista päivittyneen uuteen agenttiversioon. Palvelimelta on myös nähtävissä, että päivittymättömät agentit ovat kaikki olleet ei-aktiivisia eivätkä siten ole voineet päivittää itseänsä uuteen versioon. Koostan pilottiryhmän tilanteesta listauksen, minkä lähetän asiakkaalle. Samalla kysyn, onko agenttipäivitysten jälkeen kyseisillä tietokoneilla havaittu mitään tavallisuudesta poikkeavaa.

Aamulla käytän hetken aikaa tutustuakseni tarkemmin tietoturva-agentin Device Control –asetuksiin. Kyseisillä asetuksilla voidaan tietokoneella rajata pääsyä ulkoisiin tallennus- ja verkkoresursseihin, sekä esimerkiksi estää optisessa asemassa olevan tallennusmedian sisällön automaattinen käynnistys.

Aamupäivällä suoritan kollegaltani tulleen pyynnön tarkistaa asiakkaiden tietoturvapalvelimen automaattisten päivitysten tilan. On huomattu, että palvelimella olevat haittaohjelmatunnisteet eivät ole päivittyneet uusiin. Totean tilanteen palvelimella olevankin näin: Tunnisteet Trend Micron internet-sivustolla ovat uudempaa versiota kuin mitä palvelimella tällä hetkellä on. Käynnistän palvelimella päivitysten manuaalisen noudon, minkä aikana palvelimelle pitäisi latautua uusimmat tunnisteet.

Todettuani tunnisteiden päivittymisen, suoritan palvelimelle tietokannan huoltoajon Trend Micron työkalulla. Tämä työkalu on tarkoitettu tilanteeseen, missä palvelin ei kykene päivittämään tunnisteita sisäisen tietokannan ongelmien takia.

Keskipäivän jälkeen tarkistan tietokantapalvelimen tilanteen manuaalisen päivitysten noudon ja tietokannan huoltoajon jälkeen. Totean, että palvelimen tunnisteet ovat nyt samassa versiossa Trend Micron sivustolta löytyvien versioiden kanssa, ja havaittu ongelma on siten korjattu.

Iltapäivällä otan yhteyttä asiakas V:hen heidän haittaohjelmatuotteensa päivittämisestä OfficeScan-tuotteesta Apex One –tuotteeseen. Ehdottamani agenttien alustava siirtoaikataulu sopii asiakkaalle, ja sovimme pilottiagentin siirron tekemisestä seuraavalla viikolla.

Iltapäivän aikana rakennan kyseistä asiakasta varten siirrossa käytettävän siirtotyökalun asetuksineen, ja testaan testikoneella seuraavalla viikolla tehtävän siirron. Testiympäristössä siirto onnistuu suunnitellusti, ja siirron jälkeen agentti päivittää itsensä OfficeScan-versiosta Apex One –versioon.

Iltapäivän lopuksi jatkan vielä aamuista asiakkaan agenttien päivitysprojektia. Saan luvan kohdistaa ensimmäiselle tuotantokäytössä olevalle agenttiryhmälle päivitykset, ja merkitsen itselleni perjantaiaamulle muistutuksen tarkistaa päivittyneiden agenttien tilan.

Perjantai

Aamulla tarkistan ensimmäiseksi asiakas S:n päivittyneiden agenttien tilanteen. Totean lähes kaikkien päivityksen kohteena olleiden agenttien päivittyneen uuteen versioon. Koostan listan päivitystilanteesta asiakkaalle, ja samalla kohdistan seuraavan agenttiryhmän päivitysten kohteeksi.

Osallistun aamupäivällä säännölliseen tietoturvaosaston kokoukseen, missä läpikäymme yhdessä viikon aikana asiakkaiden avaamia työpyyntöjä ja niiden tilaa. Kokouksessa ehditään käsittelemään vain muutaman suuren asiakkaamme työpyynnöt, mutta muiden asiakkaiden työpyynnöt joudutaan jättämään ajanpuutteen takia pois kokouksesta. Pohdin, että kokous palvelee hyvin muutaman suuren asiakkaamme työpyyntöjen läpikäyntiä, mutta muut jäävät vaille koko osaston yhteistä läpikäyntiä.

Yrityksessämme on havaittu tärkeäksi yhdessä läpikäydä asiakkaiden työpyyntöjä, riippumatta työpyynnön lähettävän yrityksen koosta. Niinpä kokouksessa ehdimme myös pohtia, kuinka

löytäisimme aikaa myös muiden kuin muutaman suurimman asiakkaamme työpyyntöjen läpikäyntiin.

Iltapäivällä käyn käytäväkeskustelua kollegani kanssa yrityksessämme olevasta macOS-kannettavan tietoturvapolitiikasta. Toistaiseksi kyseisessä tietokoneessa ei ole käytetty keskitetysti hallittua tietoturva-agentin hallintapolitiikkaa, ja tähän halutaan nyt muutos. Otan tämän tehtävän itselleni, ja rakennan iltapäivän aikana yrityksemme sisäisen macOS-tietokoneiden tietoturva-agenttipolitiikan. Mallina tälle käytän Windows-tietokoneidemme vastaavaa politiikkaa.

Totean, että teknisistä syistä macOS-politiikka on hyvin pelkistetty verrattuna Windows-tietokoneiden vastaavaan. Syynä tähän on macOS-käyttöjärjestelmän rajoitteet, eli agentin ei ole mahdollista hallita kaikkia samoja tietoturvan osa-alueita.

Rakennettuani politiikan, koostan agentin asennus- ja poistopaketit yrityksemme sisäiseen käyttöön. Lähetän kollegalleni latauslinkin agentin asennuspakettiin, ja pyydän häntä asentamaan linkistä löytyvän paketin koneellensa.

Viikkoanalyysi 9

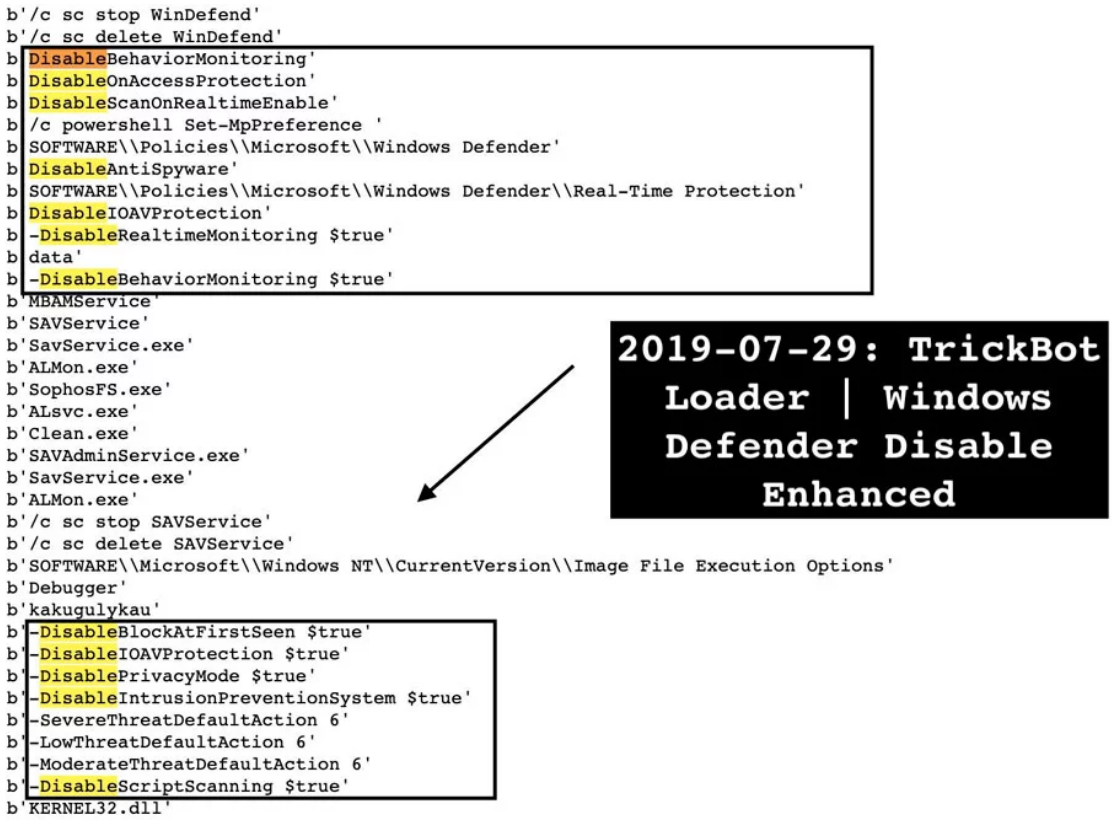
Viikon tavoitteenani oli suorittaa asiakkaalleni tietoturvapalvelimen päivitystyö, ja hoitaa päivitykseen liittyvä viestintä tehokkaasti asiakkaan suuntaan.

Päivitystyö sujui ilman ongelmia, eikä aamupäivällä suoritettu työ aiheuttanut asiakkaan ympäristöön häiriötä. Päivityksen jälkeen asiakkaan kanssa sovitun aikataulun mukaisesti kohdistin tietoturva-agenttipäivitykset ensin pilottiryhmälle, minkä jälkeen päivitykset kohdistettiin ensimmäiselle ryhmälle. Mielestäni hoidin päivitystyöhön kuuluvan asiakkaalle suunnatun viestinnän oikea-aikaisesti, tehokkaasti ja sisällöltään ymmärrettävästi.

Lisäksi huomasin kehittyneeni macOS-käyttöjärjestelmän tietoturvatuotteen osaamisessa tasolle, millä kykenin rakentamaan yrityksemme sisäisen tietoturvapolitiikan, tuottamaan asennuspaketin, ja asennuttamaan tietoturvatuotteen yrityksessämme sisäiseen käyttöön.

Viikoittaisen analyysin aiheeksi olen tällä viikolla valinnut Microsoft Windows 10 –käyttöjärjestelmään rakennetun Windows Defender Antivirus -virustorjuntaohjelman Tamper Protection -tietoturvaominaisuuden. Kyseinen suojaustekniikka lisättiin käyttöjärjestelmän sisäiseen virustorjuntaohjelmaan 1903 ominaisuuspäivityksen mukana, ja se oletuksena kytketään päälle, jos käyttöjärjestelmässä ei havaita muuta haittaohjelmantorjunta-ohjelmistoa (Microsoft 2019).

Microsoft on kehittänyt Windows Defender -tuotteensa suojausominaisuuksia samalle tasolle muiden vastaavien haittaohjelmantorjunta-tuotteiden kanssa (AV-TEST 2019), minkä takia haittaohjelmat pyrkivät ohittamaan tai estämään Windows Defender -tuotteen suojauksen PowerShell-käskyillä, Group Policy –määrityksin ja käyttöjärjestelmän rekisteriä muokkaamalla (Bleeping Computer 2019).



Kuvio 2: TrickBot-haittaohjelman hyökkäys Microsoft Windows Defender -suojausta vastaan

Tamper Protection estää haittaohjelmia suorittamasta seuraavia toimenpiteitä:

- Poistaa käytöstä haittaohjelmantorjunta
- Poistaa käytöstä tosiaikainen haittaohjelmantorjunta
- Sammuttaa ohjelmien suorittamista seuraava käyttäytymisentunnistus
- Poistaa käytöstä virustorjunta
- Poistaa käytöstä pilvipohjainen haittaohjelmantorjunta
- Estää haittaohjelmantorjunnan päivitykset

Tamper Protection -suojausominaisuus estää haittaohjelman aiheuttamat muutokset Windows Defender -tuotteen asetuksissa (Microsoft 2019). Estokeinoihin kuuluvat:

- Windows-käyttöjärjestelmän rekisterimuutokset
- PowerShell-komentojen kautta tehtävät muutokset
- Suojausasetusten muuttaminen Group Policy -määrityksin

Microsoft Windows Defender -haittaohjelmantorjunnan Tamper Protection -ominaisuus suojaa tietokonetta haittaohjelmien tekemiltä muutoksilta, ja siten kyseisen ominaisuuden käyttäminen on tärkeää rakennettaessa Windows 10 -käyttöjärjestelmän hyvää suojaustasoa.

3.10 Viikko 10

Maanantai

Tarkistelen maanantaiaamulla alkavan viikon kalenteria: Viikolla tulen tekemään töitä useamman asiakkaan projekteissa, minkä lisäksi työviikkooni tulee kuulumaan myös kehitystyötä mm. tietoturvapalvelimien hallintapalvelimen kanssa. Viikon tavoitteekseni asetan tutustua tarkemmin Trend Micron työasema-tietoturvatuotteen palomuurin tunkeilijan havaitsemisjärjestelmään eli Intrusion Detection Systemiin (IDS).

Aloitan maanantain jatkamalla asiakas S:n tietoturva-agenttien päivitysprojektia. Edellisellä viikolla asiakkaan tietoturvapalvelimelle oli asennettu uusin korjauspäivitys, minkä yhteydessä myös työasemien tietoturva-agentin versio oli palvelimella päivittynyt uuteen versioon. Jatkan agentin versiojakelua kohdistamalla päivityksen seuraavalla 50 tietokoneen ryhmälle, minkä jälkeen koostan asiakkaalle raportin aiempien päivitysten etenemisestä.

Ennen keskipäivää läpikäyn ja muokkaan saman asiakkaan tietoturvapolitiikka. Politiikassa on käytössä muutama asetus, mitkä muuttaen asiakkaan työasemaympäristössä saavutetaan korkeampi tietoturvan taso.

Keskipäivän jälkeen, tarkistan yrityksemme omalta tietoturvapalvelimelta sinne yhteyttä ottaneiden macOS-tietokoneidemme tilan. Havaitsen palvelimelta puuttuvat tietokoneita, ja yhdessä kollegani kanssa aloitamme ongelmanselvitystyön.

Palomuurilta tietoturvapalvelimen ja työaseman välistä yhteyttä tutkiessamme selviää, että yksi macOS-agentin tarvitsemista tietoliikenneporteista on estetty yrityksemme palomuurissa. Kyseisen portin avauksen jälkeen tietoturva-agentin tietoliikenneyhteys onnistuu, ja agentti kykenee liikennöimään tietoturvapalvelimen kanssa.

Tietoliikenneyhteysongelman korjaustyön jälkeen, läpikäyn kyseisen palvelimen tietoturvapolitiikkaa. Teen muutaman havainnon säännöistä, mitä muuttamalla macOS-tietokoneidemme tietoturvaa saadaan kovennettua vastaaviksi Windows-työasemiemme kanssa. Suoritan havaitsemani muutokset, ja tiedotan käyttäjiämme tietoturvapolitiikan muutosten astumisesta voimaan.

Keskipäivän ongelmanselvitystyön valmistuttua, alan läpikäydä Trend Micro Control Manager -palvelimen teknisiä vaatimuksia ja tuotteen asennusohjeita. Trend Micro Control Manager on hallinnointipalvelin, mihin tietoturvapalvelimet ottavat yhteyttä ja raportoivat toiminnastaan. Control Manager -palvelimelta voidaan keskitetysti seurata ja raportoida esimerkiksi tapahtuneita haittaohjelmahavaintoja haittaohjelmia vastaan suoritettuja operaatioita.

Kyseisen palvelimen käyttöjärjestelmän ylläpitotuki on pian päättymässä, ja palvelin tullaan korvaamaan uudella. Tehtäväni on selvittää palvelimen tekniset vaatimukset uutta virtuaalipalvelimen tilausta varten.

Tarvitsemani tiedon saan Trend Micron tekniseltä tukisivustolta, ja selvittämäni tiedon perusteella teen infra-tiimillemme työpyynnön uuden virtuaalipalvelimen rakentamisesta. Virtuaalipalvelimen valmistumisen jälkeen, tulen asentamaan uuden Control Manager- palvelimen kyseiselle palvelimelle.

Maanantai-iltapäivän lopuksi kehitän yhden asiakkaamme tietoturva- ja palomuuripolitiikkaa, läpikäymällä nykyisen politiikan sisältöä ja muokaten politiikkaa korkeamman tietoturvatason saavuttamiseksi.

Tiistai

Tiistaiaamulla tarkistan asiakas S:n agenttien päivitystilanteen. Totean että lähes kaikki päivityksen kohteena olleet agentit ovat päivittyneet uuteen agenttiversioon, ja agenttien tilan tarkistamalla syy muutaman agentin päivittymättömyyteen on ollut poissa käytöstä oleva tietokone.

Lisään seuraavan päivitysryhmän vastaanottamaan tietoturva-agentin päivityksen, ja rakennan asiakkaalle ajantasaisen raportin agenttipäivitysten etenemisestä.

Aamupäivällä selvitän kollegaltani minulle saapunutta työpyyntöä asiakas W:n agentin poistoongelmasta. Kyseinen tietoturva-agentti on suojattu ohjelma-asennuksen poistoa vastaan salasanasuojauksella, ja asiakkaalla on ollut epätietoisuutta oikeasta poistosalasanasta, poistoyrityksen epäonnistuttua ilmeisen väärän salasanan takia.

Tarkistan asiakkaan tietoturvapolitiikan dokumentaatiosta oikean poistosalasanan, mutta koska kyseessä on yhden tietyn tietokoneen agentin poisto, muutan tämän yksittäisen agentin asetuksista poistamisen sallituksi ilman salasanasuojausta. Tiedotan tämän muutoksen asiakkaalle, ja jätän työpyynnön odottamaan asiakkaan kuittausta.

Keskipäivän jälkeen otan yhteyttä asiakas V:hen, kenen kanssa aloitan tietoturva-agenttien siirtoa OfficeScan-tuotteesta Apex One -tuotteeseen. Siirtymisen yhteydessä uudet tietoturva-agentit tulevat ottamaan yhteyttä eri palvelimelle, ja viestissäni kerron uuden palvelimen nimen ja yhteyteen tarvittavat tietoliikenneportit. Saan vielä saman päivän aikana asiakkaalta varmistuksen, että uusi palvelin ja sen tietoliikenneportit ovat yhteensopivat asiakkaan tietoliikenneyhteyden kanssa.

Saatuani tietoliikenneyhteyksien toimivuudesta varmistuksen, rakennan tiistai-iltapäivällä samaiselle asiakkaalle tietoturva- ja palomuuripolitiikan Apex One -palvelimelle. Politiikkojen perustana käytän asiakkaan OfficeScan-palvelimen politiikkoja, mutta läpikäydessäni nykyisiä sääntöjä, teen muutaman tietoturvaa kehittävän muutoksen asiakkaan politiikkaan.

Iltapäivällä selvitän macOS-tietoturva-agenttien yhteensopivuutta uuden macOS-käyttöjärjestelmäversion kanssa. Kyseinen versio vaatii yhteensopivan Trend Micro Apex One for Mac -agenttiversion, mutta nykyinen tietoturvapalvelimella oleva versio ei sitä vielä ole. Tarkistan agentin päivityksen saatavuuden, mutta uutta versiota ei vielä ole saatavissa palvelimelle. Tyypillisesti käyttöjärjestelmäversion julkaisun jälkeen päivittynyt agenttiversio on julkaistu pienen viiveen jälkeen, ja merkitsen itselleni muistutuksen lähitulevaisuuteen tarkistaa uudelleen päivitetyn agentin saatavuus.

Keskiviikko

Aloitan aamun jatkamalla asiakas S:n agenttipäivitysten parissa. Tarkistan ensin edellisen päivän tilanteen, ja totean taas lähes kaikkien agenttien päivittyneen uuteen agenttiversioon. Koska agenttipäivitykset ovat onnistuneet ilman ongelmia, suurennan tämän päivän päivitysryhmän kooksi kaksinkertaisen määrän agentteja. Päivitysjakelun kohdistamisen jälkeen rakennan jälleen asiakkaalle raportin agenttien päivitystilanteesta.

Sain eilen tiistaina valmiiksi asiakas V:n Apex One -politiikan, ja tänään valmistelen tulevaa pilottiasennusta rakentamalla asennusta varten agentin siirto-ohjelman.

Tietoturva-agenttia voidaan käskyttää ottamaan nykyisen tietoturvapalvelimen sijaan yhteyttä uuteen tietoturvapalvelimeen ajamalla kyseisellä työasemalla Trend Micron IPXFER-

siirtotyökalu. IPXFER on työkalu, millä tietoturva-agentille kerrotaan uuden tietoturvapalvelimen yhteysosoite ja käytettävät tietoliikenneportit. Tämän lisäksi työkalun kautta agentille kerrotaan agentin sijainti uuden palvelimen organisaatiopuussa.

Rakennan siirtotyökalua ohjaavan asennuspaketin, ja testaan asiakkaan agentin siirtoa testiympäristössämme. Testissä tietokoneella olevaa agenttia käskytetään ottamaan yhteyttä uuteen palvelimeen, antamalla siirtotyökalulle uuden palvelimen yhteysosoite ja tietoliikenneportit. Testissä agentti ottaa yhteyttä uuteen palvelimeen, ja kohdistuu oikein asiakkaan organisaation alle. Tämän jälkeen agentti tarkistaa palvelimelta saatavilla olevan agenttiversion, ja päivittää itsensä uuteen versioon. Totean testin onnistuneen, ja siirtotyökalua ohjaavan asennuspaketin olevan valmis.

Eilen tiistaina olin tarkistanut, oliko uudelle macOS-käyttöjärjestelmäpäivitykselle yhteensopivaa tietoturva-agenttia, ja tänään keskiviikkona agenttipäivitys oli julkaistu. Kirjauduin yrityksemme omalle tietoturvapalvelimelle, suoritin sieltä Apex One for Mac -palvelimen päivityksen, ja tarkistin että palvelimen macOS-agentti päivittyi uuteen versioon.

Päivitystyön jälkeen suoritin testiympäristössämme asennustestauksen, todetakseni että uusi agenttiversio toimii ilman havaittavia ongelmia. Totesin testin perusteella päivityksen olevan valmiin jakeluun, ja kohdistin uuden agenttiversion jaeltavaksi yrityksemme macOS-tietokoneille.

Keskipäivän jälkeen aloin kollegani pyynnöstä selvittämään, miksei asiakas X:n agenteista osa enää ole ollut yhteydessä tietoturvapalvelimeen. Palvelimen suunnasta ongelmaa tarkastellen ongelman aiheuttajaa ei löytynyt, minkä takia otin yhteyttä kollegaani, joka voisi käydä paikan päällä asiakkaalla tarkistamassa asiakkaan tietokoneilta tietoturva-agentin tilan.

Myöhemmin iltapäivällä samainen kollega otti yhteyttä, ja kertoi kyseisen ongelman johtuvan asiakkaan useamman tietoturva-agentin vääristä yhteysasetuksista. Agentit yrittivät ottaa yhteyttä toiseen tietoturvapalvelimeen, minkä takia agentit eivät enää olleet yhteydessä oikean palvelimen kanssa. Merkitsin itselle seuraavalle viikolle aikavarauksen rakentaa asiakasta varten uuden agenttiversion asennuspaketti.

Iltapäivän lopuksi selvitin kollegan pyynnöstä asiakas Y:n palomuuripolitiikassa havaittua ongelmaa. Tietoturvapalvelimelta oli havaittavissa, että muutamalla asiakkaan agentilla oli politiikan vastaisesti palomuuri kytkettynä pois päältä. Selvitin ongelmaa rakentamalla asiakkaalle muutaman koneen testiryhmän, mille uuden palomuurisäännön kohdistamalla tarkistin,

johtuiko ongelma palvelimen palomuuripolitiikasta vai useammalla agentilla olevasta ongelmasta. Merkitsin itselleni seuraavalle päivällä muistutuksen tarkistaa asiakkaan testiryhmän tilan.

Torstai

Torstaiaamulla toimitin asiakas W:lle uusimman version Trend Micro CUT Tool -poistotyökalusta. Kyseinen työkalu on tarkoitettu toiminnaltaan korruptoituneen tietoturva-agentin poistamiseksi tietokoneelta. Tietoturvasyystä agentti on suojattu asiattoman poiston estämiseksi salasanalla, mutta CUT Tool -poistotyökalu kykenee poistamaan myös salasanasuojatun agentin. Tästä syystä työkalu on saatavilla Trend Micro -tuesta vain erillisellä pyynnöllä, ja työkalun käyttöikä on rajattu kolmeen kuukauteen. Näillä keinoilla Trend Micro pyrkii estämään työkalun karkaamisen asiattomaan käyttöön.

Asiakkaan käytössä oleva poistotyökalu oli vanhentunut ja siten ei enää käytettävissä. Asiakkaan pyynnöstä toimitin asiakkaalle uuden version poistotyökalusta.

Aamupäivällä jatkon asiakas S:n tietoturva-agenttien päivitysjakelua. Tarkistin ensin edellisenä päivänä jakelemani päivitysten tilanteen, ja kohdistin päivitysjakelun seuraavalle päivitysryhmälle. Raportoin jälleen asiakkaalle päivittyneiden agenttien määrät.

Aamupäivällä suoritin etätyöpöytäyhteyttä käyttäen IPXFER-työkalulla asiakas V:n pilottitietokoneen siirron OfficeScan-ympäristöstä Apex One -ympäristöön. Tarkistin siirron jälkeen, että agentti oli ottanut uudelle palvelimelle yhteyttä ja saanut sieltä tietoturvapolitiikan ladattua itselleen. Merkitsin itselleni seuraavalle päivälle muistutuksen tarkistaa, oliko agentti kyennyt päivittämään itsensä palvelimella olevaan uuteen agenttiversioon.

Saman etäyhteyden aikana läpikävin siirtotyökalun toimintaa asiakaan kanssa. Esittelin työkalun ja sen toiminnan, sekä neuvoin asiakasta työkalun käytössä. Tämän lisäksi kirjoitin asiakkaalle lyhyen siirtotyökalun käyttöohjeen, ja pyysin asiakasta olemaan yhteydessä, jos siirtotyökalun käytössä on ongelmia.

Ennen keskipäivää tarkistin asiakas Y:n testiryhmän palomuurin tilan. Totesin tietoturvapalvelimelta, että testiryhmän tietokoneilla palomuuri oli nyt päällä, eli testiryhmälle kohdistettu palomuuripolitiikka korjasi havaitun virheen. Tiedotin kollegaani havainnoistani, ja hän otti vastuun ongelman jatkoselvitystyöstä.

Keskipäivän jälkeen selvitin kollegan pyynnöstä asiakas K:n tietoturva-agenttien määrän sekä OfficeScan- että Apex One -tietoturvapalvelimilla. Koostin molemmilta palvelimilta keräämäni

agenttilistausten perusteella yhden taulukon, mistä poimin molemmilta palvelimilta löytyvät kahdentuneet agentit. Läpikävimme lopullista taulukkoa kollegani kanssa, vertailemalla tietoturvapalvelimien agenttimääriä hallintapalvelimen agenttimääriin. Näiden perusteella päädyimme lopulliseen agenttimäärään, minkä esitimme myyntiorganisaation kollegallemme.

Iltapäivällä osallistuin yrityksemme palveluita ja projekteja käsittelevään kokoukseen. Yrityksessämme on huomattu tarpeelliseksi kehittää projektityön laatua, ja tässä kokouksessa läpikävimme projektityössämme tehtyjä havaintoja, haasteita ja kipupisteitä. Kokouksen jälkeen asian käsittelyä tultaisiin jatkamaan seuraavissa projektityötä käsittelevissä kokouksissa, ja yrityksen projektityössä käytettäviä työkaluja tultaisiin kehittämään helppokäyttöisemmiksi. Torstaipäivän päätteeksi läpikävin vielä kahden asiakkaan tietoturva- ja palomuuripolitiikkaa, tehden molempiin tietoturvaa kehittäviä muutoksia.

Perjantai

Perjantaiaamulla tarkistin asiakas S:n agenttien päivitystilanteen. Totesin jälleen lähes kaikki päivityksen kohteena olevat agentit päivittyneen uuteen versioon, ja kohdistin päivityksen seuraavalle, laajemmalle päivitysryhmälle. Listasin päivittyneiden agenttien tilanteen raportiksi asiakkaalle.

Aamupäivällä osallistuin joka-perjantaiseen tietoturvapalveluiden kokoukseen, missä läpikävimme sekä asiakkaiden projekteja, että asiakkaiden avaamia tukipyyntöjä. Kokouksessa ehdimme käytännössä läpikäymään vain pari-kolme suurinta asiakasta, ja koska en itse ole suoraan ollut mukana näiden asiakkuuksien teknisessä työssä, tarjoaa kokous minulle mahdollisuuden tutustua näiden yritysten projektien tilaan.

Kokouksen päätyttyä otin yhteyttä asiakas G:hen, ja raportoin agenttien siirtoprojektin tilanteen. Listasin vielä siirtämättömät agentit, ja ehdotin seuraavaksi tehtäviä agenttiasennuksia. Keskipäivän molemmin puolin rakensin asiakas Z:lle uuden tietoturva- ja palomuuripolitiikan, käyttäen mallina toisen asiakkaan politiikkaa. Huomasin, että yritykseltämme puuttuu tietoturvapolitiikan valmis malli, mitä voisimme hyödyntää pohjana uusien asiakkaiden politiikan rakentamisessa. Käytin tässä tapauksessa politiikan rakentamisen perustana Trend Micron suosituksia hyvän tietoturvapolitiikan asetuksista, ja saatuani asiakkaan politiikan valmiiksi, lähetin tiedon asetusten sisällöstä kollegalleni politiikan läpikäymiseksi.

Iltapäivällä läpikävin aiemmin kokoamani taulukon tietoturvapalvelimille asennetuista ohjelmistoversioista. Vertasin tätä listaa ensin Trend Micron uusimpiin saatavilla oleviin päivitysversioihin, ja merkitsin ylös palvelimet, mitkä mahdollisesti tarvitsevat päivityksiä uudempiin versioihin. Tämän jälkeen läpikävin kaikki tietoturvapalvelimet, ja päivitin taulukkoon tiedon

palvelimille tarvittavista päivityksistä. Nyt päivittämääni taulukkoa tultaisiin läpikäymään seuraavan viikon kokouksessa, missä esittelisin palvelinten tilan ja päivitystarpeet.

Perjantaipäivän lopuksi läpikävin vielä tietoturvapalvelimilta löytyvät tietoturva-agenttien asennuspaketit. Palvelimien päivittyessä uudempaan versioon, jäävät vanhat asennuspaketit tarpeettomiksi, ja ne korvataan uusilla versioilla. Vanhoja asennuspaketteja ei kuitenkaan siivota automaattisesti pois, vaan ne jäävät palvelimille.

Vertailin verkkoasemilta löytyviä agenttien asennuspaketteja, ja siivosin nyt tarpeettomiksi osoittautuneet asennuspaketit pois. Vanhentuneiden asennuspakettien poistaminen estää niiden käyttämisen vahingossa asiakasympäristöissä.

Viikkoanalyysi 10

Viikkoanalyysin kohteeksi olen tällä viikolla ottanut Trend Micro -palomuuriin liitetyn Tunkeilijan havaitsemisjärjestelmän eli Intrusion Detection Systemin (IDS).

IDS on verkkoon kohdistuneita hyökkäysyrityksiä tunnistava järjestelmä, mikä havaitsee verkkoliikenteestä hyökkäysyrityksiin yhdistettäviä paketteja. Havainto hyökkäysyrityksestä ei vielä itsessään torju hyökkäystä, mutta havaitessaan hyökkäysyrityksen, IDS aiheuttaa hälytyksen, ja käynnistää torjunnan muita keinoja käyttäen (Imperva 2019). Trend Micron työasematietoturvatuotteessa IDS:n havaitsema hyökkäysyritys torjutaan palomuurissa, estämällä hyökkäysyritykseen liittyvä verkkoliikenne (Trend Micro 2019).

Yleisimmistä hyökkäysyrityksistä Trend Micro -tietoturvatuotteen palomuurin IDS kykenee havaitsemaan mm. seuraavat:

- Too Big Fragment
- Ping of Death
- Conflicted ARP
- SYN Flood
- Overlapping Fragment
- Teardrop
- Tiny Fragment Attack
- Fragmented IGMP
- LAND Attack

Edellämainituista esimerkiksi Ping of Death on palvelunestohyökkäys, mikä toteutetaan lähettämällä vastaanottajan tietojärjestelmään liian suuri tietoliikennepaketti, mikä aiheuttaa kohdejärjestelmän kuormittumisen tai kaatumisen (Cloudflare 2019).

Palvelunestohyökkäyksen tarkoituksena on estää hyökkäyksen kohteena olevan palvelun toiminta esimerkiksi ruuhkauttamalla palvelun käyttämä tietoliikenneyhteyden kaista tai kuormittamalla palveluun liittyvä laite ylimääräisellä prosessointikuormalla (Kyberturvallisuuskeskus 2016). IDS kykenee tunnistamaan kyseisen hyökkäyksen, ja hyökkäys torjutaan palomuurissa estämällä kyseinen liikenne.

Työasemaympäristön tietoturvaohjelma tyypillisesti sisältää sekä haittaohjelmatorjunnan että palomuurin. Trend Micro -tuotteessa IDS ja palomuuri tekevät yhteistyötä, toisen havaitessa ja toisen torjuessa uhan. Tietoturvatuote kykenee myös viestimään sekä havaitsemastaan uhasta että sen torjunnasta raportointipalvelimelle.

Jos työasemaympäristössä IDS ja palomuuri eivät tee yhteistyötä, esimerkiksi jos käytössä on Microsoft Windows -käyttöjärjestelmän oma palomuuri, ei hyökkäyksen havainnointia välitetä Trend Micron IDS:ltä Windows-palomuurille, vaan on luotettava palomuurin kykyyn hyökkäyksen havainnointiin ja torjuntaan.

Windows-palomuurin toiminnasta ei välity tietoa takaisin Trend Micro -tietoturvatuotteelle, vaan palomuurin toiminnasta on kerättävä tietoa muilla tavoin.

3.11 Viikko 11

Tarkistelen viikon alussa työkalenteria: Viikolla tulen jälleen tekemään töitä useamman asiakkaan projekteissa. Pohdin, että työviikosta saattaa tulla sisällöltään samankaltainen edellisen viikon kanssa. Edistän tälläkin viikolla asiakasprojekteja, sekä suoritan tietoturvapalvelimien kehitystyötä. Tämä työviikko tulee olemaan päiväkirjamuotoisen opinnäytetyöni viimeinen viikko.

Maanantai

Aloitan maanantain tarkistamalla asiakas S:n tietoturva-agenttien päivittymisen tilan. Totean, että päivitysten kohteina olleet agentit ovat lähes kaikki päivittyneet uuteen versioon. Kokoan asiakkaalle raportin päivityksen tilanteesta, minkä jälkeen kohdistan päivityksen seuraavalle ryhmälle agentteja.

Edellisellä viikolla läpikävin tietoturvapalvelimilta löytyviä tietoturva-agenttien vanhoja asennuspaketteja. Jatkan maanantain aamupäivän samaa työtä: Siivoan pois käytöstä poistuneita asennuspaketteja sekä palvelimilta että jaetuista verkkokansioista.

Asiakas AA:lla on alkamassa projekti siirtää tietoturva-agentit tietoturvapalvelimelta toiselle. Tarkistan sekä nykyisen agenttiversion että uudella palvelimella tarvittavan agenttiversion, ja kokoan hallintapalvelimelta tapahtuvaa asennustyötä varten kollegalleni oikean agenttiversion asennuspaketin. Asennuspaketin määritysten perusteella asennettava tietoturva-agentti kohdistuu tietoturvapalvelimella oikean yrityksen organisaatiorakenteeseen. Kollegani tulee asennuspaketin perusteella rakentamaan hallintapalvelimelle asennustehtävän, mikä myöhemmin kohdistetaan asiakkaan tietokoneille.

Aamupäivän lopuksi korjaan yhdeltä tietoturvapalvelimelta löytyneen tietoturvapolitiikan määritysvirheen. Virheellisen määrityksen perusteella muutama tiedosto oli väärin merkitty kuuluvaksi tarkistettavien tiedostojen joukkoon, ja tehtävä muutos poistaa kyseiset tiedostot tarkistusten piiristä.

Keskipäivän jälkeen jatkan asiakkaan asennuspaketin rakentamista. Kollega on saanut koottua hallintapalvelimen asennuspaketin, ja testaamme kollegan kanssa asennuspaketin toimivuuden testiympäristössämme.

Oikein toimiessaan asennuspaketti havaitsee tietokoneella olevan vanhan version tietoturva-agentista, poistaa sen, ja asentaa tilalle uuden version tietoturva-agentista. Tämän jälkeen tietokoneelle kirjautunut käyttäjä saa ilmoituksen, että asennuksen loppuun saattamiseksi tietokone pitää vielä käynnistää uudelleen. Tämän jälkeen asennustehtävä on suoritettu kokonaisuudessaan valmiiksi. Käytämme kollegani kanssa aikaa erityisesti vanhan agenttiversion luotettavaan tunnistamiseen, sillä uutta agenttiversiota ei turhaan haluta poistaa tietokoneesta.

Iltapäivällä vielä läpikäyn kollegoideni kanssa kokouksessa yhden asiakkaamme tietoturva-agenttien määriä. Olen edellisellä viikolla selvittänyt tietoturvapalvelimilta kyseisen asiakkaan agenttien määriä, ja vertailemalla tätä lukua hallintapalvelimen agenttien määrään, saamme muodostettua asiakkaan käytössä olevien tietokoneiden määrän laskutusta varten.

Tiistai

Tiistaiaamulla jatkan asiakas S:n tietoturva-agenttien päivitysprojektia. Aloitan ensin tarkistamalla päivityksen kohteena olleiden agenttien tilan, minkä perusteella laadin projektin etenemisestä asiakkaalle raportin. Tämän jälkeen kohdistan agenttipäivityksen seuraavalle päivitysryhmälle.

Rakentaessani asiakkaalle raporttia, havaitsen omassa tietokoneessani ongelman. Tyypillinen it-alan yrityksen haaste on tuottaa yrityksen omille työntekijöille it-tukea. Käyttäjät ovat teknisesti osaavia, ja pienet ongelmat ratkeavat käyttäjän itse suorittaman vianselvitystyön aikana. Samoin tässäkin tapauksessa: Selvitän ja korjaan tietokoneessani ilmenneen ongelman. Ongelman ratkaisemisen jälkeen otan yhteyttä asiakas AA:han. Olemme kollegan kanssa saaneet maanantaina valmiiksi tietoturva-agentin asennuspaketin, ja sovin pilottiasennuksen tehtäväksi tänään iltapäivällä. Merkitsen itselleni huomiselle keskiviikolle muistutuksen tarkistaa asennuksen tilan.

Aamupäivän päätteeksi osallistun kokoukseen, missä läpikäymme tietoturvapalvelimiemme versiotilannetta. Olen valmistellut kokoukseen raportin palvelimien versiotiedoista, mitä vertailen uusimpiin saatavilla oleviin korjaus- ja päivityspaketteihin. Palvelimien päivitysten tilanne on kehittynyt myönteisesti, ja vain muutama päivitys tarvitsee suorittaa tietoturvapalvelimille.

Keskipäivän jälkeen, osallistun joka toinen viikko järjestettävään jatkuvien palveluiden kokoukseen, missä läpikäydään asiakasprojektien etenemistä, sekä tikettityöjonojen tilannetta ja käsittelyaikoja.

Kokouksen jälkeen läpikäyn asiakkaidemme eri tietoturvapalvelimilla olevien agenttien määriä. Käynnissä on projekti, missä osa asiakkaistamme keskitetään useammalta palvelimelta yhdelle uudelle tietoturvapalvelimelle, ja tätä varten kokoan listan, mihin asiakkaiden agenttien määrät ja agenttien sijainnit eri palvelimilla on luetteloitu.

Iltapäivällä kohdistan kollegani kanssa tietoturva-agentin pilottiasennuksen asiakas AA:n tietokoneelle. Kyseessä on maanantaina rakentamamme asennuspaketti, ja asiakkaan kanssa sovitusti asennus suoritetaan tänään tiistaina, ja asennuksen tila tarkistetaan aamulla keskiviikkona.

Lopun iltapäivästä käytän yhden tietoturvapalvelimen tietoturvapolitiikkojen läpikäynnissä. Vertailen palvelimella olevien asiakkaiden politiikkoja toisiinsa, ja havaitsen että politiikat

ovat rakennettu vaihtelevin tietoturva-asetuksin. Pienin muutoksin on mahdollista tiukentaa käytössä olevia asetuksia, ja siten kehittää asiakkaiden tietoturvan tasoa.

Keskustelen asiasta kollegani kanssa, ja hän ohjeistaa minua, että mahdollisuuksien mukaan asiakkaiden tietoturva-asetuksia voidaan tiukentaa. Osa asiakkaista kuitenkin edellyttää etukäteen tiedottamaan ja sopimaan tehtävistä muutoksista, ja tässä yhteydessä en tee muutoksia näille asiakkaille.

Keskiviikko

Jatkan aamulla asiakas S:n agenttien päivitysprojektia. Tarkistan ensin edellisten päivien asennusten tilan, ja kokoan asiakkaalle raportin tilanteesta. Tämän jälkeen kohdistan seuraavalle asennusryhmälle agenttiversiopäivityksen.

Eilen tiistaina asiakas AA:n pilottitietokoneelle oli kohdistettu agenttipäivityspaketti. Tarkistan tietoturvapalvelimelta, onko kyseisen tietokoneen agentti päivittynyt, ja palvelimen tietojen mukaan kyseinen agentti on nyt oikeassa versiossa. Asiakkaalta kysyessäni, saan kuitenkin kuulla, että asennuksen kohteena oleva tietokone käynnistyy yhä uudelleen ja uudelleen. Pyydän kollegaani tarkistamaan hallintapalvelimelta kyseisen tietokoneen asennustyön tilan, ja saan kuulla, ettei hallintapalvelin ole merkinnyt asennusta valmiiksi, ja asennus on suoritettu käynnistyksen jälkeen yhä uudelleen. Varaan itselleni iltapäivälle aikaa asian jatkoselvitystä varten.

Aamupäivällä saan kollegaltani pyynnön rakentaa tietoturva-agentin poistoon ja uuden version asennukseen tarvittavan paketin. Agentin poistamiseen käytetään Trend Micron CUT Tool – työkalua, mikä poistaa tietokoneesta tietoturva-agentin. Agentin poistettuaan, työkalu voidaan määrittää käynnistämään uuden agentin asennustyö, ja tätä varten valmistelen uuden agentin asennuspaketin. Testaan testiympäristössämme kokoamallani asennuspaketilla sekä poiston että asennuksen, ja toimitan valmiin paketin kollegalleni.

Aamupäivän lopuksi valmistelen yhden tietoturvapalvelimemme myöhemmin tapahtuvaa versiopäivitystä varten. Versiopäivitys päivittää sekä palvelimen että palvelimeen yhteydessä olevien agenttien versiot, ja ennen tehtävää päivitystä agenttien versiopäivitys on kytkettävä palvelimelta pois päältä. Läpikäyn palvelimella olevat asiakkaat, ja poistan agenttien päivittymisen käytöstä. Samalla siirrän palvelimelle päivityksessä tarvittavat päivitys- ja ohjetiedostot.

Iltapäivällä jatkan aamupäivällä havaitun asiakkaan pilottiasennuksen ongelmanselvitystä kollegani kanssa. Havaitsemme ongelman johtuvan siitä, että asennustehtävä ei tunnista uuden,

oikean version asennusta tietokoneelta, vaan asennus suoritetaan tietokoneella uudelleen heti edellisen asennuksen päätyttyä. Kollegani löytää asennuspaketissa olevan virheen: Uutta versiota tietoturva-agentista ei tunnisteta oikein. Vika on helppo korjata kuntoon, ja iltapäivällä asennuspaketti on valmis seuraaviin asennuksiin.

Tiistaina läpikävin yhden tietoturvapalvelimen asiakkaiden tietoturvasääntöjä, ja nyt keskiviikkoiltapäivänä suoritan saman työ toiselle palvelimelle. Läpikäydessäni asiakkaiden sääntöjä, havaitsen vastaavia kehityskohteita, joissa pienillä muutoksilla asiakkaiden tietoturvan tasoa saadaan parannettua tietoturvapolitiikkaa muuttamalla.

Torstai

macOS-käyttöjärjestelmään oli vähän aikaa sitten julkaistu uusi versio, ja Trend Micro on pienellä viiveellä julkaissut uuden käyttöjärjestelmäversion kanssa yhteensopivan tietoturva-agentin. Saadakseni uuden version päivitettyä agenteille, kirjaudun tietoturvapalvelimelle, ja lataan päivityspaketin palvelimen hallinnassa jakeluvalmiiksi. Tarkistan, että agenttien päivitysasetukset sallivat agenttipäivitykset, ja merkitsen itselleni muistutuksen seuraavalle viikolle tarkistaakseni, että macOS-agentit ovat saaneet päivityksen ladattua.

Olin eilen kollegani kanssa saanut agenttien päivityspaketin korjattua levitysvalmiiksi, ja tänään aamupäivällä sovin asiakas AA:n kanssa asennusten kohdistamisesta muutamalle ensimmäiselle käyttäjälle. Asennusten kohdistamisen jälkeen merkitsen huomiselle perjantaille muistutuksen tarkistaa asennusten tilan.

Aamupäivän lopuksi selvitän asiakas AB:ltä saapuneen vianselvityspyynnön koskien tietokonetta missä etätyöpöytäohjelma ei Trend Micro –tietoturvaohjelman vuoksi enää toimi. Läpikäyn asiakaan tietoturvapolitiikkaa, mutta sen perusteella etäyhteysohjelmaa tai sen tarvitsemia tietoliikenneyhteyksiä ei ole estetty. Pyydän asiakkaalta lisätietoa ongelmasta sekä mahdollisista virheilmoituksista ongelman ratkaisemiseksi. Keskipäivän jälkeen saan samalta asiakkaalta vastuksen, että kyseinen ongelma on ratkaistu asiakkaalla, ja vianselvityspyynnön voi sulkea ratkenneena. Asiakas oli uudelleenasentanut työaseman tietoturvatuotteen, ja tämä toimenpide oli korjannut asian.

Iltapäivällä jatkan projektia, missä osa asiakkaistamme tullaan siirtämään usealta nykyiseltä tietoturvapalvelimelta uudelle. Listaan yhdeltä palvelimelta kaikki projektiin kuuluvat asiakkaat, ja kirjaan luetteloon asiakkaiden agenttien määrät samoin kuin agenttien uusimmat yhteydenottoajat. Jälkimmäisestä tiedosta selviää, onko kyseinen agentti eli tietokone yhä käytössä vai jo poistunut käytöstä.

Iltapäivällä edistän projektia, missä asiakas U:n nykyiset agentit siirretään toiselle tietoturvapalvelimelle. Läpikäyn nykyiset agentit, sekä niiden aktiivisuuden tilan. Lisäksi läpikäyn asiakkaan nykyisen tietoturva- ja palomuuripolitiikat. Tiedot kerättyäni, otan asiakkaaseen yhteyttä, esitellen projektin ja alustavan aikataulun.

Torstai-iltapäivän päätteeksi teen vielä muutamia muutoksia asiakas K:n tietoturvapolitiikkaan.

Perjantai

Aloitan aamun edistämällä asiakas S:n agenttien päivitysprojektia. Tarkistan edellisten päivitysten tilanteen vertailemalla palvelimella agenttiversioiden määriä tämän aamun lukemiin. Rakennan päivittyneistä tiedoista asiakkaalle uuden raportin, ja kohdistan jälleen uudelle agenttiryhmälle versiopäivityksen.

Aamupäivällä osallistun viikoittaiseen tietoturvapalveluiden kokoukseen, missä läpikäymme suurimpien asiakkaiden projektien etenemistä, sekä katsomme näiden asiakkaiden ja yleisen tukijonomme työpyyntöjen tilannetta.

Kokouksen jälkeen otan yhteyttä asiakas AA:han, ja läpikäyn asiakkaan kanssa agenttien siirtoprojektin etenemistä sekä vielä jäljellä olevien agenttien siirron aikataulutusta.

Ennen keskipäivää selvitän kollegani kanssa yrityksemme omilla tietokoneillamme käynnistyksen yhteydessä ajettavaa työtä. Kyseinen työ on käynyt tarpeettomaksi, mutta dokumentaatiostamme ei löydy tietoa mistä kyseistä työtä ajetaan. Keskipäivään mennessä toteamme, että ajankäytön puolesta on tehokkaampaa osoittaa kyseisen asian selvitystyö infra-ryhmällemme.

Keskipäivän jälkeen osallistun kokoukseen, missä suunnittelemme ohjeistusta Trend Micro Apex One –tuotteen käyttöönottoon. Dokumentaatiossamme ei tällä hetkellä ole kuvausta kyseisen projektin tyypillisestä rakenteesta, ja rakennamme tässä kokouksessa alustavan rungon projektin läpivientiä ajatellen. Lopputuloksena saamme rakennettua luettelon tarpeellisista tehtävistä Apex One –tuotteen käyttöönotossa.

Iltapäivän aikana jatkan torstaina aloittamaani tietoturvapalvelimien asiakkaiden läpikäyntiä. Aiemman yhden palvelimen asiakasagenttien lisäksi listaan myös muiden palvelimien asiakkaat ja näiden agenttimäärät. Saan valmiiksi listauksen, missä ovat kaikki siirrettävät asiakkaat ja näiden päivittyneet agenttimäärät. Merkitsen itselleni kalenteriin säännöllisen muistutuksen ylläpitää tätä listaa projektin edetessä, ja agenttien siirtyessä palvelimilta toisille.

Perjantai-iltapäivän päätteeksi läpikäyn ja päivitän työasematuotteiden tietoturvaa ylläpitävien palvelinten luetteloa. Tähän on lueteltu palvelimet, versiot, asennetut tietoturvapäivitykset, sekä palvelimelta mahdollisesti puuttuvat päivitykset.

Vertailen luettelossa olevia versiota palvelimilla oleviin versioihin, ja havaitsen muutamalle palvelimelle tehdyn päivityksen, mitä listallani ei vielä ole. Päivitän luetteloon uusimmat palvelimille asennetut versiot.

4 Yhteenveto

Päiväkirjamuotoisessa opinnäytetyössäni kuvasin työtäni tietoturva-asiantuntijana 11 viikon ajan. Opinnäytetyöni tavoitteena oli seurata työssä oppimista ja osaamisen karttumista, sekä kehittymistä asiantuntijaroolissani.

Alkaessani kirjoittaa opinnäytetyötäni, olin työskennellyt työpaikassa vasta lyhyen aikaa, ja uutena työntekijänä kykenin näkemään ja kokemaan työni kuin ulkopuolisen silmin tarkasteltuna. Opinnäytetyötä aloittaessani kuvasin itseni osaamistasoltani kykeneväksi suorittamaan tyypillisiä työtehtäviä itsenäisesti, mutta ongelmanselvitys- ja kehitystyössä tarvitsin kokeneemman kollegan tukea ja ohjausta. Opinnäytetyön aikana osaamiseni on kehittynyt tasolle, millä koen suoriutuvani työtehtävissäni samalla tasolla kollegoideni kanssa. Kykenen myös puolestani neuvomaan ja ohjaamaan toisia asiantuntijoita oman vastuualueeni työtehtävissä. Toki, yksittäisissä vaativissa työtehtävissä tukeudun edelleen kollegoideni apuun.

Kymmenen viikon päättyessä vedin itsenäisesti asiakkaiden tietoturvatuotteiden käyttöönottoprojekteja, selvitin asiakkailta saapuneita ongelmanselvitys- ja kehitystyöpyyntöjä, sekä ylläpidin ja päivitin tietoturvapalvelimia.

Olen kehittänyt osaamistani ja tietoperustaani tutustuen tietoturvaohjelmistojen toimintaan, sekä läpikäyden näiden pääkäyttäjille suunnattua koulutusmateriaalia ja dokumentaatiota. Osaamisaluettani olen kehittänyt tutustumalla tässä päiväkirjamuotoisessa opinnäytetyössäni kuvaamiin aiheisiin. Aihealueiksi olen valinnut työviikoilla kohtaamani, tarkempaa selvitystyötä vaatineet aiheet.

Koin päiväkirjamuotoisen opinnäytetyön kirjoittamisen sopivan työelämässä jo olevalle henkilölle, sillä sain mielestäni yhdistettyä työn ja opinnäytetyön kirjoittamisen toisiinsa. Huomasin kuitenkin jo muutaman viikon jälkeen, että päiväkirjamuotoinen opinnäytetyö sitoo joustamattoman aikataulunsa ja säännöllisten aikarajojensa vuoksi vapaa-aikaa, ja tämä asia on opinnäytetyötä harkitsevan tärkeä tiedostaa pohtiessaan päiväkirjamuotoisen opinnäytetyön laadintaa. Perinteinen opinnäytetyö antaa aikataulunsa puolesta vapauksia, mutta itse koin säännölliset aikarajat opinnäytetyötäni edistävänä ja ennalta sovittuun aikatauluun sitovana.

Opinnäytetyöni aikana huomasin työpaikkani uusien työntekijöiden perehdytyksessä kehittämisen varaa mm. työntekijän käyttöoikeuksien ja ensimmäisten työpäivien sisällön suhteen. Räätälöimällä perehdytyksen sisällön valmiiksi perehdytettävällä henkilölle, tehostetaan perehdytyksen tulosta. Samoin, valmistelemalla aloittavan käyttäjän käyttäjätunnukset ja käyttöoikeudet, nopeutetaan aloittavan työntekijän työn alkua. Olen kuvannut omassa perehdytyksessä kohtaamiani haasteita tässä opinnäytetyössä, ja havaintoni ovat tämän työni kautta työnantajani käytettävissä, perehdytystä kehitettäessä.

Tein myös havaintoja tietoturvapalvelinten ylläpitovastuun jakautumisesta useammalle henkilölle. Vastuun jakautuminen oli johtanut tilanteeseen, missä kenelläkään ei ollut kokonaiskuvaa palvelinten tilasta, jokaisen ylläpitoa tehneen henkilön nähdessä tilanteen vain omalta kantiltaan. Palvelimet olivat yhden vastuuhenkilön puuttuessa jääneet ilman ylläpidon koordinointia. Yrityksessä ei tiedetty palvelimien ylläpidon. kokonaistilaa. Opinnäytetyöni aikana toin nämä havainnot ilmi työnantajalle, ja palvelinten tilaa seurataan nyt säännöllisissä kokouksissa, ja minut on nimetty vastaamaan tietoturvapalvelinten ylläpidon seurannasta.

Lähteet

Sähköiset

Cisco Systems Incorporated. 2019. Office 365 phishing. Viitattu 1.11.2019. https://blogs.cisco.com/security/office-365-phishing-threat-of-the-month

Microsoft Corporation. 2019. Windows 10 release information. Viitattu 6.10.2019. https://docs.microsoft.com/en-us/windows/release-information/

Microsoft Corporation. 2019. Enable controlled folder access. Viitattu 10.11.2019. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-controlled-folders

Microsoft Corporation. 2019. Protect security settings with Tamper Protection. Viitattu 10.11.2019. https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/prevent-changes-to-security-settings-with-tamper-protection

Microsoft Corporation. 2019. Top 10 tapoja suojata Office 365 ja Microsoft 365 liiketoiminta suunnitelmat. Viitattu 1.11.2019. https://docs.microsoft.com/fi-fi/office365/admin/security-and-compliance/secure-your-business-data?view=o365-worldwide#setup

Trend Micro Incorporated. 2019. Intrusion Detection System. Viitattu 15.11.2019. http://docs.trendmicro.com/all/ent/apex-one/2019/en-us/apexOne_2019_agent_olh/Intrusion-Detection-.html

Trend Micro Incorporated. 2019. Trend Micro Apex One (Mac) Administrators's Guide. Viitattu 26.10.2019. http://docs.trendmicro.com/all/ent/apex-mac/2019/en-us/apexMac_2019_ag.pdf

Trend Micro Incorporated. 2019. Configuring a Web Reputation Policy. Viitattu 11.10.2019. http://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-widget-and-policy-management-guide/officescan-agent-pol/web-reputation-polic/wrs_policy_config_tm.aspx

Trend Micro Incorporated. 2019. Trend Micro OfficeScan XG Service Pack 1. Viitattu 21.9.2019. https://files.trendmicro.com/products/officescan/XG/SP1/osce_xg_sp1_win_en_criticalpatch_b5383.html

Trend Micro Incorporated. 2019. Web Reputation Services (WRS) Lookup process in Officescan. Viitattu 11.10.2019. https://success.trendmicro.com/solution/1056324-web-reputation-services-wrs-lookup-process-in-officescan-osce

Trend Micro Incorporated. 2016. Information about Trend Micro Web Reputation Services (WRS). Viitattu 11.10.2019. https://success.trendmicro.com/solution/1058991-information-about-trend-micro-web-reputation-services-wrs

Trend Micro Incorporated. 2019. Best practices in preventing Ransomware infection using OfficeScan (OSCE) and Worry-Free Business Security/Services (WFBS/WFBS-SVC). Viitattu 29.9.2019. https://success.trendmicro.com/solution/1099423-best-practices-in-preventing-ransomware-infection-using-officescan-osce-and-worry-free-business-security-services-wfbs-wfbs-svc#collapseOne

Trend Micro Incorporated. 2019. Compatibility between Windows 10 and OfficeScan/Apex One. Viitattu 6.10.2019. https://success.trendmicro.com/solution/1112083-compatibility-between-windows-10-and-officescan-apex-one

Microsoft Corporation. 2019. Windows-elinkaaren tietosivu. Viitattu 6.10.2019. https://support.microsoft.com/fi-fi/help/13853/windows-lifecycle-fact-sheet

Microsoft Corporation. 2019. Estä tietoturva-asetusten muutokset peukaloinnin torjunnalla. Viitattu 10.11.2019. https://support.microsoft.com/fi-fi/help/4490103/windows-10-prevent-changes-to-security-settings-with-tamper-protection

Cisco Systems Incorporated. 2019. Intelligence Categories. Viitattu 11.10.2019. https://talosintelligence.com/categories#contentcats

Ahokas, L. & Mäkeläinen, J. 2013. Perehdyttäminen ja työnopastus - Ennakoivaa työsuojelua. Viitattu 13.9.2019. https://ttk.fi/koulutus_ja_kehittaminen/julkaisut/digijulkaisut/perehdyttaminen_ja_tyonopastus_-_ennakoivaa_tyosuojelua

Apple Incorporated. 2018. macOS:n tietoturva – Yleiskatsaus IT:lle. Viitattu 26.10.2019. https://www.apple.com/business/docs/resources/macOS_Security_Overview.pdf

AV-TEST GmbH. 2019. The best Windows antivirus software for home users. Viitattu 10.11.2019. https://www.av-test.org/en/antivirus/home-windows/

Bleeping Computer LLC. 2019. Microsoft Now Enables Windows 10 Tamper Protection By Default. Viitattu 10.11.2019. https://www.bleepingcomputer.com/news/microsoft/microsoft-now-enables-windows-10-tamper-protection-by-default/

Cloudflare Incorporated. 2019. Ping of Death DDoS attack. Viitattu 15.11.2019. https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/

Helsingin Sanomat. 2019. Facebook säilytti miljoonia salasanoja salaamattomassa muodossa sisäisillä palvelimilla. Viitattu 1.11.2019. https://www.hs.fi/teknologia/art-2000006043756.html

Imperva. 2019. Intrusion detection and intrusion prevention. Viitattu 15.11.2019. https://www.imperva.com/learn/application-security/intrusion-detection-prevention/

Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus. 2018. Office 365 -sähköpostin tietojenkalastelu ja tietomurrot erittäin yleisiä – havaitse, suojaudu, tiedota! Viitattu 1.11.2019. https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota

Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus. 2016. Ohje 3/2016 Palvelunestohyökkäysten ehkäisy ja torjunta. Viitattu 1.11.2019. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta.pdf

Kuviot