Antti Tuokko

Oppimispäiväkirja kyberturvallisuuden asiantuntijatyöstä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

25.11.2025

Tiivistelmä

Tekijä:	Antti Tuokko
Otsikko:	Oppimispäiväkirja kyberturvallisuuden asiantuntijatyöstä
Sivumäärä:	25 sivua
Aika:	25.11.2025
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ohjaajat:	Osaamisaluepäällikkö Janne Salonen

Tämä insinöörityö on oppimispäiväkirjamuotoinen kuvaus tekijän ammatillisesta kehittymisestä kyberturvallisuuden asiantuntijatyössä. Työ perustuu päivittäisiin tehtäviin tietoturvapalveluja tarjoavassa asiantuntijaorganisaatiossa, jossa yhdistyvät tekninen analyysi, prosessien kehittäminen ja yhteistyö eri sidosryhmien kanssa. Työn keskiössä on oman osaamisen ja ajattelun reflektointi neljän viikon seurantajakson aikana.

Tavoitteena on jäsentää, miten tekninen asiantuntijuus, analyyttinen päätöksenteko ja prosessilähtöinen toiminta kytkeytyvät moderniin kyberturvallisuusympäristöön. Työ tarkastelee käytännön tehtäviä, jotka liittyvät uhkatiedon hallintaan, hyökkäyspinnan hallintaan, poikkeamien käsittelyyn ja tietoturvaprosessien kehittämiseen. Näiden teemojen kautta hahmotetaan, miten teoria ja käytäntö nivoutuvat yhteen operatiivisessa tietoturvatyössä ja millaista osaamista nykyaikainen asiantuntijarooli tietoturvassa edellyttää.

Oppimispäiväkirja toimii dokumentaationa jatkuvasta ammatillisesta kasvusta ja asiantuntijuuden syventymisestä. Työ tuo esiin, miten tekninen osaaminen, tilannetietoisuus ja kehittämisorientoitunut ajattelutapa tukevat tietoturvapalveluiden laadukasta toteutusta ja organisaation kokonaisturvallisuuden vahvistamista.

Avainsanat: kyberturvallisuus, uhkatiedon hallinta, hyökkäyspinnan hallinta, poikkeamien käsittely, prosessien kehittäminen

---

Abstract

Author:	Antti Tuokko
Title:	Learning Diary on the Work of a Cyber Security Specialist
Number of Pages:	25 pages
Date:	25 November 2025
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Supervisors:	Janne Salonen, Competence Area Manager

This bachelor's thesis is a learning-diary–based description of the author's professional development in a cyber security specialist role. The work is based on daily tasks in a managed service provider organization, where technical analysis, process development, and collaboration with various stakeholders intersect. The four-week observation period centers on reflective examination of the author's skills and thinking.

The objective is to structure how technical expertise, analytical decision-making, and process-oriented practices connect in a modern cyber security environment. The thesis examines practical tasks related to threat intelligence, attack surface management, incident handling, and the development of security processes. Through these themes, it outlines how theory and practice intertwine in operational cybersecurity work and what competencies a contemporary specialist role in cybersecurity requires.

The learning diary serves as documentation of ongoing professional growth and deepening expertise. The work highlights how technical capability, situational awareness, and a development-oriented mindset support the high-quality delivery of cybersecurity services and strengthen an organization's overall security posture.

Keywords: cybersecurity, threat intelligence, attack surface management, incident handling, security process development

Tekoälyn hyödyntäminen opinnäytetyössä

Tässä opinnäytetyössä on käytetty OpenAI:n ChatGPT-ohjelmaa (versiot 5.0 ja 5.1) kirjoitusprosessin tukena. Tekoälyä hyödynnettiin tekstin kielelliseen muotoiluun, rakenteen selkeyttämiseen, ilmaisun parantamiseen sekä lähdeviitteiden esitystavan tarkistamiseen. Opinnäytetyön tekijänä olen vastuussa kaikesta opinnäytteeni sisällöstä.

Sisällys

Lyhenteet

RACI: Responsible, Accountable, Consulted, Informed. Roolien ja vastuiden määrittelyyn käytettävä matriisi, jota hyödynnetään prosessien ja projektien selkeyttämisessä.

POV: Proof of Value. Arviointimenetelmä, jossa teknistä ratkaisua kokeillaan rajatussa ympäristössä sen arvon, toimivuuden ja hyötyjen todentamiseksi ennen laajempaa käyttöönottoa.

DFIR: Digital Forensics and Incident Response. Tietoturvaloukkausten tutkintaan ja käsittelyyn keskittyvä osa-alue, joka yhdistää digitaalisen forensiikan ja poikkeamienhallinnan menetelmät.

SOC: Security Operations Center. Organisaation kyberturvallisuuden valvontakeskus, joka seuraa ympäristöä, analysoi havaintoja ja reagoi tietoturvapoikkeamiin.

DNS: Domain Name System. Järjestelmä, joka muuntaa verkkotunnuksia vastaaviksi verkko-osoitteiksi ja mahdollistaa palveluiden käyttämisen nimipohjaisesti numeroarvojen sijaan.

OSINT: Open Source Intelligence. Avoimista ja julkisesti saatavilla olevista lähteistä kerätty ja analysoitu tieto, joka perustuu esimerkiksi digitaalisiin aineistoihin, rekistereihin, mediasisältöihin ja julkisiin tietokantoihin.

1 Johdanto

Tämä insinöörityö on oppimispäiväkirjamuotoinen kuvaus omasta ammatillisesta kehittymisestäni kyberturvallisuuden asiantuntijatyössä. Työ perustuu neljän viikon seurantajaksoon, jonka aikana dokumentoin päivittäisiä tehtäviäni, havaintojani ja oppimiskokemuksiani. Tarkoituksena on reflektoida, millaista osaamista ja ajattelutapaa nykyaikainen tietoturva-asiantuntijan työ vaatii, sekä jäsentää omaa kehitystäni osana tätä kokonaisuutta.

Työni tapahtuu tietoturvapalveluja tarjoavassa organisaatiossa, jossa toimin asiantuntijaroolissa vastaten uhkatiedon hyödyntämisestä, altistumisen hallinnasta ja poikkeamien käsittelystä osana laajempaa kyberturvallisuuden kokonaisuutta. Päivittäinen työ koostuu teknisen analyysin, viestinnän ja prosessikehityksen yhdistelmästä. Työssä korostuvat järjestelmällinen ongelmanratkaisu, päätöksenteon tukeminen ajantasaisen tiedon avulla sekä kyky sovittaa tekninen tieto ymmärrettävään muotoon eri sidosryhmille.

Oppimispäiväkirjamuoto mahdollistaa oman toiminnan tarkastelun aidossa työympäristössä. Kirjoittamisen tavoitteena ei ole yksityiskohtainen kuvaus yksittäisistä työkaluista tai asiakkuuksista, vaan laajempi ammatillinen pohdinta siitä, miten käytännön tilanteet kehittävät asiantuntijuutta. Päiväkirjassa kuvaan, miten käsittelen havaittuja ilmiöitä, arvioin niiden merkitystä ja pohdin, miten ne liittyvät teoreettisiin viitekehyksiin kuten riskienhallintaan, tilannetietoisuuteen ja jatkuvaan kehitykseen.

Työn tuloksena syntyy kokonaisuus, joka havainnollistaa, miten teoria ja käytäntö yhdistyvät modernissa kyberturvallisuusympäristössä. Samalla se toimii itsereflektion välineenä, joka auttaa tunnistamaan omat vahvuudet, kehityskohteet ja ammatillisen kasvun suuntaviivat tulevaisuutta varten.

2 Oppimispäiväkirja

2.1 Ensimmäinen seurantaviikko

2.1.1 Viikon tavoitteet

Ensimmäisen viikon tavoitteena oli tarkastella omaa roolia osana organisaation kyberturvallisuusprosessia ja hahmottaa, miten päivittäiset tehtävät tukevat havaintojen käsittelyä, riskienhallintaa ja tiedon jakamista. Tavoitteena oli muodostaa kokonaiskuva siitä, miten eri turvallisuuden osa-alueet, kuten tekninen havaitseminen, vastuunjako ja viestintä, muodostavat yhtenäisen ja hallitun toimintamallin.

Viikon aikana oli tarkoitus kiinnittää huomiota erityisesti siihen, miten turvallisuusperiaatteet kuten Defense in Depth, Risk Management Lifecycle ja Incident Response -malli näkyvät käytännön työssä (NIST SP 800-160, 2022; NIST SP 800-37, 2018; NIST SP 800-61, 2012). Näiden avulla pyrin ymmärtämään, miten havaintojen analysointi, poikkeamatilanteiden käsittely ja prosessien kehittäminen kytkeytyvät toisiinsa ja tukevat organisaation kokonaisturvallisuutta.

Tavoitteiden keskiössä oli myös oman toiminnan ja ajattelun kehittäminen. Tarkoituksena oli nähdä yksittäiset tehtävät osana laajempaa turvallisuuskokonaisuutta ja vahvistaa ymmärrystä siitä, miten hyvin määritellyt prosessit, selkeät roolit ja jatkuva oppiminen edistävät järjestelmällistä ja kestävää tietoturvatyötä.

2.1.2 Seurantajakso

Maanantai

Viikko alkoi poikkeamatilanteen käsittelyllä, joka liittyi käyttäjän tekemään verkkoselailuun ja siihen liitettyyn riskihälytykseen. Käyttäjän havaittiin vierailleen sivulla, jonka mainejärjestelmä oli merkinnyt mahdollisesti haitalliseksi. Tarkistin tapahtumalokit ja analysoin sivuston käyttäytymisen, mikä osoitti sen tehneen DNS-kyselyitä tunnetulle haitalliselle osoitteelle. Lokit vahvistivat, että liikenne oli estynyt palomuuritasolla ennen kuin mitään haitallista toimintaa ehti tapahtua.

Tapaus vahvisti Defense in Depth -ajattelun käytännön merkityksen: useampi suojauskerros toimi odotetusti ja esti tapahtumaketjun etenemisen (NIST SP 800-160, 2022). Poikkeamien hallinnassa keskeistä on myös todennus ja dokumentointi, sillä ne muodostavat perustan Incident Response Lifecyclen alkuvaiheille (Tunnistaminen ja arviointi) (NIST SP 800-61, 2012).

Päivän lopuksi osallistuin päätelaiteinventaarion tarkistamiseen toisen tiimin apuna, jossa selvitettiin laitehallinnan ulkopuolisia päätelaitteita ja niiden käyttöjärjestelmäversioita. Työ konkretisoi näkyvyyden merkityksen riskienhallinnan lähtökohtana: riskiä ei voi hallita, jos suojeltavia kohteita ei tunneta.

Tiistai

Päivän aikana keskityttiin vastuiden ja roolien tarkentamiseen. Kävimme läpi valvontateknologian tuotteistusprosessiin liittyvän RACI-matriisin ja varmistimme, että eri osapuolten tehtävät ja päätöksentekovaltuudet ovat selkeitä palvelun hallinnan ja kehittämisen eri vaiheissa (PMI, 2021). Työn aikana nousi esiin kohtia, joissa vastuut olivat osittain päällekkäisiä tai

epäselviä. Näiden täsmentäminen auttoi varmistamaan, että päätöksenteko ja vastuunjako ovat yhdenmukaisia koko prosessin ajan.

Selkeä työn- ja vastuunjako tukee ISO/IEC 27001 -standardin mukaista hallintamallia ja sen painotusta johdonmukaisiin prosesseihin ja jatkuvaan parantamiseen (ISO/IEC 27001, 2022). Ymmärsin, että tehokas turvallisuustoiminta ei perustu pelkästään tekniseen kyvykkyyteen, vaan siihen, että organisaatiossa on selkeät rakenteet ja määritellyt roolit, jotka varmistavat hallitun reagoinnin poikkeamatilanteissa.

Keskiviikko

Aamupäivän aikana käytiin läpi erään teknisen ratkaisun koekäyttöön liittyviä asioita. Tarkoituksena oli arvioida, miten sen tarjoama kyvykkyys voisi tukea havaintojen rikastamista ja priorisointia osana olemassa olevia prosesseja. Keskustelujen myötä muodostui selkeämpi käsitys siitä, miten tiedon laatu ja ajantasaisuus vaikuttavat suoraan päätöksenteon nopeuteen ja havaintojen luotettavuuteen.

Iltapäivällä julkaistiin laajasti vaikuttava haavoittuvuus, joka koski useita eri asiakasympäristöjä. Kävin haavoittuvuusskannerin tulokset läpi vastuualueeseeni kuuluvista kohteista. Tunnistin, kenen vastuulla kukin haavoittunut laite oli ja välitin tiedon eteenpäin oikeille tahoille yhdessä mitigointisuositusten kanssa. Näin varmistettiin, että korjaavat toimenpiteet etenevät nopeasti priorisoituihin ympäristöihin. Tilanne kuvasti hyvin Risk Management Lifecyclen ja Incident Response Lifecyclen vaiheita: tunnistamista, arviointia, toimenpiteiden kohdistamista ja viestintää (NIST SP 800-37, 2018; NIST SP 800-61, 2012). Kokonaisuutena päivä osoitti, että hallittu reagointi perustuu oikea-aikaiseen tiedonkulkuun ja vastuiden selkeyteen.

Torstai

Torstain aikana pidettiin tiimin yhteinen palaveri, jossa käsiteltiin ajankohtaisia asioita, yhteistyön kehittämistä ja tutustuttiin uuteen työntekijään. Keskustelu oli monivivahteinen ja toi esiin, kuinka erilaiset näkökulmat ja tiimien toimintatavat voivat vaikuttaa yhteisen suunnan löytymiseen. Tilanne korosti, että avoin viestintä ja selkeät toimintaperiaatteet ovat olennaisia, jotta yhteistyö pysyy rakentavana myös erilaisten mielipiteiden keskellä.

Myöhemmin osallistuin asiakasesittelyyn, jossa käytiin läpi asiakasympäristön rakenteita ja sen turvallisuusarkkitehtuurin perustoja. Tällaiset katsaukset tukevat kokonaiskuvan muodostamista ja auttavat ymmärtämään, miten eri osa-alueet kytkeytyvät toisiinsa. Päivän kokonaisuus vahvisti käsitystä siitä, että tehokas tietoturva nojaa paitsi teknisiin ratkaisuihin, myös ihmisten väliseen yhteistyöhön ja kykyyn toimia yhtenäisesti yhteisten tavoitteiden eteen.

Perjantai

Päivän aikana sain sidosryhmältä ajankohtaisiin hyökkäyskampanjoihin liittyviä indikaattoreita, jotka kävin läpi ja lisäsin organisaation käytössä olevaan uhkatiedonhallintajärjestelmään. Tarkoituksena oli varmistaa, että uudet tunnisteet integroituvat olemassa olevaan uhkatietoprosessiin ja tukevat havaintojen rikastamista sekä analytiikan ajantasaisuutta.

Iltapäivällä kävin läpi omien vastuuasiakkuuksieni avoimet työpyynnöt ja varmistin, ettei mikään poikkeama jäänyt viikonlopun ajaksi odottamaan toimenpiteitä. Näin varmistettiin, että kaikki keskeneräiset tehtävät olivat hallinnassa ja tarvittavat jatkotoimet ohjattu eteenpäin oikeille tahoille.

2.1.3 Yhteenveto

Ensimmäinen seurantaviikko tarjosi kokonaiskuvan siitä, kuinka monipuolista ja toisiin ihmisiin tukeutuvaa kyberturvallisuuden asiantuntijatyö on. Päivät sisälsivät niin teknistä analysointia, poikkeamatilanteiden käsittelyä, prosessien ja vastuiden tarkastelua kuin myös yhteistyötä eri tiimien ja sidosryhmien kanssa. Viikko osoitti, että teknisen osaamisen rinnalla korostuvat kyky priorisoida, tehdä päätöksiä ja viestiä tehokkaasti muiden toimijoiden kanssa.

Erityisesti havaintojen käsittely ja haavoittuvuuksien arviointi toivat esiin, kuinka tärkeää on hallittu reagointikyky ja tiedonkulun sujuvuus. Roolien ja vastuiden läpikäynti puolestaan vahvisti ymmärrystä siitä, että selkeä työnjako ja yhteiset toimintaperiaatteet tukevat koko organisaation turvallisuuskyvykkyyttä. Myös yhteistyö sidosryhmien kanssa ja ajantasaisen uhkatiedon ylläpito konkretisoivat jatkuvan tiedonvaihdon merkitystä osana ennakoivaa puolustusta.

Viikko antoi hyvän pohjan tuleville seurantajaksoille. Se auttoi tunnistamaan omia vahvuuksia ja kehityskohteita erityisesti siinä, miten tekninen analyysi, prosessien kehittäminen ja yhteistyö nivoutuvat yhteen päivittäisessä työssä. Kokonaisuutena viikko vahvisti käsitystä siitä, että tietoturva on jatkuvaa oppimista, jossa jokainen tilanne tarjoaa mahdollisuuden kehittää sekä omaa asiantuntijuutta että organisaation toimintamalleja.

2.2 Toinen seurantaviikko

2.2.1 Viikon tavoitteet

Toisen viikon tavoitteena oli syventää ymmärrystä uhkatiedon hyödyntämisestä, yhteistyöstä ja ennakoivasta toiminnasta osana organisaation tietoturvatoimintaa. Viikon aikana tarkoituksena oli tarkastella, miten erilaiset

tiedonlähteet, analyysimenetelmät ja sidosryhmien välinen vuorovaikutus tukevat havaintojen käsittelyä ja päätöksentekoa.

Tavoitteena oli myös vahvistaa osaamista uhkienmetsästyksen ja haavoittuvuuksien hallinnan osa-alueilla sekä pohtia, miten ajankohtaiset ilmiöt ja alan trendit vaikuttavat omaan työhön. Lisäksi viikon aikana kiinnitettiin huomiota siihen, miten oman työn suunnitelmallisuus ja valmistautuminen parantavat valmiutta reagoida tehokkaasti muuttuviin tilanteisiin.

2.2.2 Seurantajakso

Maanantai

Viikko alkoi projektien ja palveluiden tilannekatsauksella, jossa käytiin läpi ajankohtaiset asiat eri asiakkuuksien osalta. Samalla tarkastelin oman vastuualueeni tikettejä viikonlopun jäljiltä ja varmistin, että avoimet tehtävät etenivät suunnitellusti.

Päivän aikana tarkastelin eri lähestymistapoja, joilla organisaation tiedonhankintaa ja ennakoivaa kyvykkyyttä voidaan vahvistaa. Tavoitteena oli hahmottaa, miten käytettävissä oleva tieto voidaan hyödyntää aiempaa järjestelmällisemmin osana arjen havaintojen käsittelyä. Lisäksi tarkistin viikonlopun aikana ilmoitetut kriittiset haavoittuvuudet ja varmistin tietokannoista ja haavoittuvuusskannereista, että nämä eivät koskeneet asiakkuuksiamme (CISA, 2016). Päivän kokonaisuus painottui käytännön näkyvyyteen, tiedonhallintaan ja oman työn koordinointiin.

Tiistai

Päivä kului alan tapahtumassa, joka tarjosi mahdollisuuden tavata muita tietoturva-alan asiantuntijoita ja keskustella ajankohtaisista kehityssuunnista. Kävin läpi erityisesti uhkatiedon tuottamiseen ja hyödyntämiseen liittyviä

näkökulmia sekä sitä, miten eri toimijat ratkaisevat tiedon rikastamiseen ja analysointiin liittyviä haasteita.

Keskustelut avasivat hyvin alan tämänhetkisiä painotuksia, kuten datan laadun, kontekstin ja ajantasaisuuden merkitystä. Tapahtuma tarjosi myös tilaisuuden vertailla eri toimittajien ajatusmalleja siitä, miten laadukas uhkatieto tukee päätöksentekoa ja parantaa organisaatioiden reagointikykyä muuttuvaa uhkaympäristöä vastaan.

Päivän aikana seurasin myös useita esityksiä, joissa käsiteltiin muun muassa ajankohtaisia hyökkäystrendejä Euroopassa. Itselleni merkittävimpiä aiheita olivat kiristyshaittaohjelmien kehityssuunnat, identiteettipohjaisten hyökkäysten yleistyminen ja se, miten hyökkääjät hyödyntävät yhä useammin automatisoituja menetelmiä tiedustelussa ja valmistelussa. Nämä näkökulmat auttoivat suhteuttamaan omassa työssä näkyviä havaintoja laajempaan toimintaympäristöön ja vahvistivat kokonaiskuvaa tämänhetkisistä painopisteistä hyökkääjien toiminnassa.

Kokonaisuutena päivä tarjosi hyvän tilaisuuden verkostoitumiseen ja tiedonvaihtoon sekä mahdollisuuden peilata organisaation omia havaintoja siihen, mitä muualla Euroopassa ja kansainvälisesti koetaan. Tapahtuma vahvisti käsitystä siitä, että jatkuva vuorovaikutus alan toimijoiden kanssa on tärkeää, jotta oma osaaminen ja tilannetietoisuus pysyvät ajan tasalla nopeasti kehittyvässä uhkaympäristössä.

Keskiviikko

Keskiviikkona yhtenä aiheena oli uhkienmetsästys ja sen kehittäminen osana organisaation toimintaa. Kävimme läpi menetelmiä ja ideoita siitä, millaisia ilmiöitä ja poikkeamia olisi hyödyllistä tarkastella tulevien viikkojen aikana. Keskustelussa nousi esiin ajankohtaisia trendejä ja havaintoja, joita voisi hyödyntää proaktiivisessa metsästyksessä. Uhkienmetsästys on keskeinen osa

modernin SOC-toiminnan ennakoivaa puolustusta, jossa käyttäytymis- ja indikaattoripohjaisia havaintoja tarkastellaan ilman erillisiä herätteitä (ENISA, 2020).

Päivän aikana tutustuin myös tuoreeseen kansainvälisen tason uhka-analyysiin, joka käsitteli Euroopan muuttuvaa kyberuhkaympäristöä. Analyysi tarjosi laajemman näkymän siihen, millaisia kehityssuuntia eri toimijaryhmissä on viime vuosina nähtävissä, kuten hyökkäystekniikoiden monipuolistuminen, identiteettipohjaisten hyökkäysten yleistyminen ja geopoliittisten jännitteiden vaikutukset kohdevalintoihin.

Tarkastelu auttoi suhteuttamaan omassa työssä havaittuja ilmiöitä laajempaan eurooppalaiseen kokonaisuuteen ja toi lisää ymmärrystä siitä, miten uhkatoimijoiden toimintatavat kehittyvät. Kokonaisuutena raportin läpikäynti vahvisti käsitystä siitä, miksi monikerroksinen puolustus, riittävä näkyvyys ja ennakoiva analyysi ovat keskeisiä elementtejä nykyaikaisessa tietoturvatyössä.

Torstai

Torstaina pidettiin asiakkuuskohtainen tilannekatsaus, jossa käytiin läpi avoimet työpyynnöt ja meneillään olevat projektit sekä niiden eteneminen. Valmistauduin palaveriin tarkistamalla etukäteen asiakkaan haavoittuvuustilanteen ja ajankohtaiset havainnot skannerilta. Katsauksessa keskusteltiin myös ajankohtaisista uhkatrendeistä ja niiden mahdollisista vaikutuksista ympäristöön.

Palaverin jälkeen päivitin asiakkuuden dokumentaatiota ja tarkistin, että tiedot vastasivat ajankohtaista tilannetta. Samalla arvioin, miten eri tiimien käyttämät raportointikäytännöt eroavat toisistaan ja missä määrin niitä voisi yhdenmukaistaa. Tämä nosti esiin useita kehitysideoita, jotka liittyivät tiedonkulun selkeyttämiseen ja raportointiprosessien parantamiseen.

Päivän aikana vahvistui ajatus siitä, että yhtenäinen ja ajantasainen dokumentointi on tärkeä osa tietoturvatoiminnan laatua. Kun tieto on helposti löydettävissä ja esitetty yhdenmukaisesti, se tukee päätöksentekoa ja vähentää väärinymmärrysten riskiä. Hyvin organisoitu tiedonhallinta toimii käytännön vastineena tietoturvan hallintajärjestelmissä korostetulle periaatteelle, jonka mukaan prosessien ja kommunikoinnin johdonmukaisuus on keskeinen osa kokonaisvaltaista turvallisuutta (ISO/IEC 27001, 2022).

Perjantai

Päivän aikana osallistuin asiakkuuden sisäisen harjoituksen tulosten tarkasteluun ja selvitin, miten sen havainnot liittyivät käyttäjien toimintaan ja valvontaan. Lisäksi kävin läpi vastuuasiakkuuksieni avoimet työpyynnöt ja varmistin, että kaikki tarvittavat toimenpiteet oli tehty ennen viikonvaihdetta.

Iltapäivällä päivitin asiakkuuden hälytyssääntöjä edellisenä päivänä pidetyn palaverin pohjalta. Kehitysidean tavoitteena oli parantaa havaintojen kohdentumista ja vähentää turhia ilmoituksia. Päivän tehtävät korostivat käytännön hienosäätöä ja sitä, miten pienillä muutoksilla voidaan parantaa havaintojen tarkkuutta ja vähentää turhaa kuormitusta.

2.2.3 Yhteenveto

Toinen seurantaviikko korosti yhteistyön, ennakoivuuden ja tiedon hyödyntämisen merkitystä. Viikon aikana tehtävät vaihtelivat operatiivisesta työstä ja analytiikan kehittämisestä asiakasyhteistyöhön ja tiedonvaihtoon. Kokonaisuus osoitti, että tehokas tietoturvatyö rakentuu teknisen osaamisen, suunnitelmallisen toiminnan ja jatkuvan vuorovaikutuksen varaan.

Erityisesti uhkienmetsästykseen ja ajankohtaisiin trendeihin perehtyminen syvensi ymmärrystä siitä, miten laajempi uhkaympäristön tuntemus tukee

käytännön havaintotyötä. Samalla asiakkuuksien hallinta ja raportointikäytäntöjen kehittäminen toivat esiin sen, että tietoturvatoiminnan vaikuttavuus riippuu myös siitä, miten tieto esitetään ja jaetaan organisaation sisällä.

Viikko vahvisti käsitystä siitä, että kyberturvallisuus on jatkuvaa kehittämistä, jossa oppiminen tapahtuu sekä päivittäisen työn että yhteistyön kautta. Kokemukset toivat selkeyttä siihen, miten oma työ linkittyy laajempiin prosesseihin ja miten tekninen ja viestinnällinen osaaminen täydentävät toisiaan organisaation turvallisuuden kokonaisuudessa.

2.3 Kolmas seurantaviikko

2.3.1 Viikon tavoitteet

Kolmannen viikon tavoitteena oli syventää ymmärrystä haavoittuvuuksien hallinnasta, prosessien kehittämisestä ja teknisten kokeilujen suunnittelusta. Viikolla keskityttiin erityisesti siihen, miten havaintoja priorisoidaan, miten korjaustoimenpiteitä koordinoidaan ja millä tavoin tekniset kokeilut (kuten POV-kierrokset) voidaan suunnitella niin, että niistä saadaan mahdollisimman luotettavaa ja käyttökelpoista tietoa päätöksenteon tueksi.

Lisäksi tavoitteena oli tarkastella yhteistyön merkitystä sekä sisäisten tiimien että ulkopuolisten toimittajien kanssa. Viikon aikana oli tarkoitus kehittää valmiuksia dokumentoida teknisiä havaintoja selkeästi, arvioida riskien vaikutuksia liiketoimintaan ja tukea asiakkuuksia tilanteissa, joissa tekniset ongelmat tai uudet löydökset vaativat nopeaa reagointia.

2.3.2 Seurantajakso

Maanantai

Maanantai painottui haavoittuvuuksien hallintaan. Kävin läpi toisen tiimin tuottamia haavoittuvuuksien skannausraportteja ja selvitin, mihin järjestelmiin nostetut havainnot liittyivät ja mistä ongelmat mahdollisesti johtuivat. Laadin löydöksistä koontiraportit, joissa hahmoteltiin toimenpidejärjestys ja arvioitiin eri vaihtoehtojen vaikutusta palveluiden käytettävyyteen. Tavoitteena oli löytää ratkaisu, joka minimoisi tuotantoympäristön käyttökatkot ja mahdollisti korjausten suorittamisen hallitusti (CISA, 2016).

Päivän aikana pidettiin myös sisäinen palaveri, jossa käytiin läpi ajankohtaisia asiakasvastuita ja operatiivisen työn tilannetta. Keskustelut auttoivat muodostamaan kokonaiskuvaa käynnissä olevista projekteista ja priorisoimaan tulevia tehtäviä.

Tiistai

Tiistaina osallistuin organisaation laajuiseen kuukausikatsaukseen, jossa käytiin läpi talouden lukuja, toiminnan painopisteitä ja johdolle esitettyjä kysymyksiä. Tilaisuus tarjosi hyvän mahdollisuuden nähdä laajempi näkymä organisaation tilanteesta ja hahmottaa, miten kyberturvallisuustyö liittyy muihin liiketoiminnan osa-alueisiin. Katsaus auttoi ymmärtämään, miten turvallisuuden kehityshankkeet suhteutuvat kokonaisuuteen ja minkälaisia odotuksia eri sidosryhmillä on tulevalle vuodelle.

Kuukausikatsauksen jälkeen pidettiin koko osaston yhteinen palaveri, jossa käsiteltiin ajankohtaisia tiimikohtaisia kuulumisia, resurssitarpeita ja muutoksia toimintaympäristössä. Palaveri auttoi varmistamaan, että osaston sisäinen viestintä ja käsitys meneillään olevista projekteista pysyi yhtenäisenä. Samalla

se selkeytti, miten oman tiimin työ kytkeytyy muihin kyberturvallisuustoimintoihin ja miten kokonaisuutta voidaan koordinoida tehokkaammin.

Päivään sisältyi myös sisäinen suunnittelukokous, jossa tarkasteltiin erästä SOC-toimintaan liittyvää tulevaa muutosta. Keskusteluissa arvioitiin muutoksen yleisiä vaikutuksia valvonnan prosesseihin, tiedonkeruuseen ja operatiiviseen työnkulkuun. Lisäksi pohdittiin, millaisia tarkennuksia palvelukuvaukseen tai tiimirajapintoihin mahdollisesti tarvitaan, jotta muutos voidaan toteuttaa hallitusti osana kokonaisuutta.

Kokous korosti sitä, että teknisiä uudistuksia on tärkeää tarkastella paitsi järjestelmien näkökulmasta myös operatiivisen toiminnan jatkuvuuden ja havaintokyvyn kannalta. Huolellinen ennakkosuunnittelu auttaa varmistamaan, että muutokset voidaan jalkauttaa vaiheittain ja ilman tarpeettomia häiriöitä päivittäisessä työssä.

Myöhemmin päivällä oli valmistautumistilaisuus vastuuasiakkuuden kuukausipalaveria varten. Kävimme läpi kuukauden aikana esiin nousseita havaintoja ja koottavia nostoja sekä arvioimme ajankohtaista tietoturvatilannetta laajemmin. Tarkistin myös haavoittuvuusskannausten raportit varmistaakseni, että palaverissa voitaisiin esittää mahdollisimman ajantasainen kuva ympäristön tilasta. Valmistelun tavoitteena oli varmistaa, että asiakkuuden tilannekuva perustuu luotettavaan tietoon ja että mahdolliset kehityskohteet voidaan perustella selkeästi.

Keskiviikko

Keskiviikkona osallistuin teknologiatoimittajatapaamiseen, jossa määriteltiin seuraavana päivänä alkavan POV-kierroksen tavoitteet, tekniset toteutukset ja arvioinnin rajaukset. Keskusteluissa varmistettiin, että lähtöoletukset, testattavat kokonaisuudet ja odotetut tulokset olivat kaikilla osapuolilla selkeästi

ymmärrettyjä. Tällainen yhteinen suunnitteluvaihe on tärkeä, jotta kokeilu tuottaa käyttökelpoista ja vertailukelpoista tietoa päätöksenteon tueksi.

Aloin samalla laatia kokeilulle arviointikriteeristöä, jonka tarkoituksena on määrittää, millä perusteilla ratkaisun toimivuutta ja tuottamaa arvoa voidaan arvioida. Kriteeristön suunnittelu sisältää sekä teknisiä että prosessipainotteisia näkökulmia, jotta arviointi olisi mahdollisimman kattava. Rakenteen muodostamisessa hyödynsin yleisiä periaatteita, joita käytetään teknologioiden arviointimalleissa, kuten havainnon laadun, relevanssin, käytettävyyden, integraatiovalmiuden ja operatiiviseen työmäärään kohdistuvien vaikutusten tarkastelua. Näiden pohjalta syntyi alustava runko, joka selkeyttää, mitä POV-kierrokselta odotetaan ja millä perusteilla tuloksia voidaan tulkita.

Päivän aikana jatkoin myös haavoittuvuusskannausten läpikäyntiä ja laadin korjaussuosituksia asiakkuudelle. Keskityin tunnistamaan, mitkä havainnot olivat liiketoiminnallisesti kriittisimpiä ja miten korjaustoimet voitaisiin toteuttaa mahdollisimman pienellä vaikutuksella tuotantoon (CISA, 2016). Työ sisälsi riskien arviointia, priorisointia sekä eri vaihtoehtojen vertailua suhteessa käyttökatkoihin ja operatiiviseen jatkuvuuteen. Tilanne vahvisti käsitystä siitä, että onnistunut haavoittuvuuksienhallinta vaatii sekä teknistä tarkkuutta että ymmärrystä liiketoiminnan tarpeista.

Kokonaisuudessaan keskiviikko toi esiin, miten tekninen analyysi, rakenteinen arviointikehikko ja toimittajayhteistyö tukevat toisiaan käytännön työssä. Hyvin suunniteltu POV luo edellytykset sille, että päätökset perustuvat luotettavaan dataan ja että valittavat ratkaisut vastaavat organisaation todellisia tarpeita.

Torstai

Torstaina aloitimme POV-kierroksen ja pidimme aloituspalaverin, jossa käytiin läpi kokeilun tavoitteet, tekniset periaatteet ja toteutustapa. Palaverissa varmistettiin, että ympäristö oli valmis kokeilun käynnistämiseen ja että

seuranta- ja arviointimenetelmät olivat yhtenäiset. Alkuvaiheen tarkennukset loivat pohjan sille, että kokeilu tuottaisi vertailukelpoista ja päätöksenteon kannalta hyödyllistä dataa.

Aamupäivä kului uuden ratkaisun tuottaman kokonaisuuden tarkastelussa. Kiinnitin huomiota siihen, miten ratkaisu jäsentää ja esittää asioita suhteessa muihin käytössä oleviin järjestelmiin, kuinka johdonmukaisesti näkymät rakentuvat ja miten hyvin ne tukevat päivittäistä arviointi- ja seurantatyötä. Tavoitteena oli muodostaa käsitys siitä, miten ratkaisu täydentäisi organisaation nykyistä kokonaiskuvaa ja missä määrin se auttaisi tunnistamaan jatkotoimia vaativat tilanteet aiempaa systemaattisemmin.

Pidin myös kollegani puolesta asiakkuuskohtaisen palaverin, sillä hän oli estynyt osallistumasta. Palaverissa käytiin läpi ympäristön ajankohtaiset havainnot, avoimet kysymykset ja tulevien viikkojen prioriteetit. Keskustelu oli hyödyllinen, sillä se tarjosi mahdollisuuden nähdä asiakkuuden arkea laajemmasta näkökulmasta ja kuulla ajatuksia ongelmista, joita ei välttämättä tule vastaan omissa tavanomaisissa tehtävissä.

Iltapäivällä osallistuin keskusteluun erään toisen teknologiatoimittajan kanssa. Keskustelussa tarkasteltiin, miten heidän ratkaisunsa voisi osaltaan tukea havaintojen käsittelyä ja eri järjestelmistä kertyvän tiedon jäsentelyä sekä täydentää organisaation nykyisiä analyysi- ja seurantakäytänteitä (Dietle, 2016). Vaihdoimme näkemyksiä muun muassa siitä, miten useista taustajärjestelmistä koottu tieto vaikuttaa johtopäätösten luotettavuuteen sekä siitä, miten kokonaisnäkyvyyttä voidaan kehittää johdonmukaisesti.

Päivän kokonaisuus korosti sitä, kuinka tärkeää on tarkastella uusia työvälineitä sekä teknisestä että prosessinäkökulmasta. Pelkkä ominaisuuksien tarkastelu ei riitä, vaan olennaista on myös arvioida datan laatua, sen käytettävyyttä

päätöksenteossa ja sitä, miten ratkaisu soveltuu organisaation nykyisiin toimintamalleihin.

Perjantai

Perjantaina pidimme SOC-tiimin sisäisen kehityskeskustelun, jossa tarkasteltiin meneillään olevia projekteja sekä tulevia kyvykkyyksiä, joita voitaisiin pilotoida tai suunnata osaksi pidemmän aikavälin kehitystyötä. Keskusteluissa painottui erityisesti se, miten havaintojen laatua ja luotettavuutta voidaan parantaa rakenteisilla toimintamalleilla ja yhtenäisillä analyysikäytännöillä. Tarkastelimme myös, miten eri tietolähteistä saatua dataa voidaan hyödyntää johdonmukaisemmin valvonnassa ja miten analyytikoiden välistä toimintatapaa voidaan yhdenmukaistaa osana jatkuvaa kehittämistä.

Keskusteluissa sivuttiin lisäksi erilaisia lokikeräysmenetelmiä ja tiedonvälitystapoja, joiden roolia arvioidaan osana organisaation valvontakyvykkyyden kehittämistä. Näiden vaihtoehtojen tarkastelu auttoi hahmottamaan, miten näkyvyyttä voidaan vahvistaa eri järjestelmäkerroksissa ja millaisia vaikutuksia mahdollisilla muutoksilla olisi operatiiviseen työskentelyyn.

Päivän aikana tarkastelin konsultatiivisesti erään DFIR-tapauksen havaintoja ja niiden mahdollisia vaikutuksia (Luttgens et al., 2014). Arvioin erityisesti tapahtumaketjun riskivaikutuksia, lateraalisen liikkeen mahdollisuutta sekä tunnistettavissa olevia artefakteja. Vaikka en ollut tapauksen päävastuullinen analyytikko, tehtävä tarjosi hyvän mahdollisuuden harjoitella tapahtumaketjujen tulkintaa ja vahvisti käsitystä siitä, millaiset signaalit voivat viitata poikkeavaan toimintaan.

Iltapäivällä osallistuin tiimipalaveriin, jossa valmistauduimme seuraavalla viikolla järjestettävään organisaation sisäiseen kybertapahtumaan. Tilaisuuden tavoitteena on tuoda yhteen eri tiimien asiantuntijoita ja tarkastella

kyberturvallisuuden kehitysmahdollisuuksia organisaation tasolla. Valmistautuminen auttoi jäsentämään niitä teemoja, joita olisi hyödyllistä nostaa esiin, ja vahvisti ymmärrystä omasta roolista osana laajempaa kokonaisuutta.

2.3.3 Yhteenveto

Kolmas seurantaviikko painottui haavoittuvuuksien hallintaan, teknisten kokeilujen suunnitteluun ja yhteistyöhön niin asiakkaiden, sisäisten tiimien kuin toimittajienkin kanssa. Viikko tarjosi monipuolisen näkymän siihen, miten korjaustoimenpiteitä priorisoidaan ja miten teknisiä ratkaisuja arvioidaan osana päivittäistä tietoturvatoimintaa.

POV-kierroksen suunnittelun myötä korostui tarve selkeille tavoitteille ja hyvin määritellyille arviointikriteereille. Samalla yhteistyö eri sidosryhmien kanssa vahvisti käsitystä siitä, että kyberturvallisuuden kehittäminen on jatkuva prosessi, jossa yksittäisetkin havainnot ja ideat voivat johtaa konkreettisiin parannuksiin.

2.4 Neljäs seurantaviikko

2.4.1 Viikon tavoitteet

Neljännen seurantaviikon tavoitteena oli tarkastella asiantuntijatyötä kokonaisuutena ja syventää ymmärrystä siitä, miten erilaiset tehtävät, yhteistyö ja seuranta muodostavat johdonmukaisen osan organisaation kyberturvallisuusprosessia. Viikon aikana tarkoituksena oli kiinnittää huomiota erityisesti siihen, miten havaintoja käsitellään, miten altistumista arvioidaan ja millä tavoin riskejä priorisoidaan osana jatkuvaa toimintaa.

Lisäksi viikon tavoitteena oli osallistua organisaation sisäisiin kehityshankkeisiin sekä suunnittelutyöhön, jossa kartoitetaan tulevaisuuden tarpeita ja arvioidaan

erilaisten toimintamallien hyödyllisyyttä strategisesta näkökulmasta. Tavoitteena oli ymmärtää paremmin, miten laajempi palvelukokonaisuus rakentuu ja millä tavoin asiantuntijan rooli tukee sitä.

2.4.2 Seurantajakso

Maanantai

Maanantaiaamu käynnistyi projektien ja palveluiden tilannepalaverilla, jossa käytiin läpi asiakkuuksien ajankohtaiset tilanteet, edellisellä viikolla tehdyt toimenpiteet sekä tulevan viikon tärkeimmät painopisteet. Palaverin jälkeen kävin läpi oman vastuualueeni työpyynnöt viikonlopun ajalta, priorisoin avoimet tehtävät ja varmistin, että käynnissä olevat toimeksiannot etenivät suunnitellun aikataulun mukaisesti. Muutamat tapauksista olivat viikonlopun aikana nousseet epäiltyinä tietoturvaherätteinä, mutta tarkemman analyysin perusteella ne osoittautuivat konfiguraatiovirheiksi. Tapaukset toimivat hyvänä muistutuksena siitä, että kaikki hälytykset eivät välttämättä liity todellisiin uhkiin, ja että korkealaatuinen analyysi ja systemaattinen juurisyiden selvittäminen ovat keskeisiä virheellisten havaintojen minimoimisessa (NIST SP 800-61, 2012).

Yhdessä tapauksessa havaittu poikkeuksellisen suuri verkkoliikenne osoittautui palveluun kohdistuneeksi automaattiseksi skannaukseksi, jonka seurauksena asiakkaan julkisesta päätepisteestä löytyi oletusasetuksille jäänyt palvelusivu. Ilmiö korosti ulkoisen näkyvyyden ja peruskonfiguraatioiden tason merkitystä sekä sitä, miten pienetkin huolimattomuudet voivat lisätä hyökkäyspintaa. Tilanteen dokumentointi ja suositeltujen toimenpiteiden esittäminen auttoivat selkeyttämään, miten vastaavanlaiset tapaukset voidaan jatkossa estää osana kokonaisvaltaista altistumisenhallintaa.

Päivän aikana selvitin myös uuden haavoittuvuuden mahdollista vaikutusta yhteen vastuuasiakkuuteen. Tarkastelu vaati ympäristön komponenttien

läpikäyntiä ja riippuvuuksien varmistamista. Lopullinen analyysi osoitti, että kyseinen komponentti ei ollut käytössä, eikä haavoittuvuus näin ollen kohdistunut kyseiseen ympäristöön. Tällaiset tapaukset havainnollistavat haavoittuvuuksienhallinnan iteratiivista luonnetta ja sitä, miten tärkeää on tarkistaa ympäristö kunkin uhkatiedotteen osalta ennen toimenpiteiden kiirehtimistä (CISA, 2016).

Iltapäivällä osallistuin palaveriin, jossa tarkasteltiin uhkatiedon hyödyntämiseen liittyviä kokonaisuuksia sekä organisaation yleisiä tarpeita tulevien kehitysaskeleiden näkökulmasta. Keskusteluissa pohdittiin, millaisia osa-alueita olisi tarkoituksenmukaista vahvistaa pitkällä aikavälillä ja miten eri tiimien näkemykset tulisi huomioida mahdollisten uudistusten suunnittelussa. Lisäksi käytiin läpi, millaisia odotuksia sidosryhmillä yleisesti on tiedon saatavuudelle, selkeydelle ja hyödyntämiselle arjen työssä. Palaveri auttoi muodostamaan kokonaiskuvan siitä, missä kohdin nykyisiä toimintamalleja voisi kehittää ja miten uhkatiedon roolia olisi tarkoituksenmukaista vahvistaa osana päätöksenteon tukea.

Tiistai

Tiistaina viimeistelin POV-kierroksen vertailukriteeristön, jonka luonnostelu oli aloitettu edellisellä viikolla. Työ painottui mittareihin ja arviointiperiaatteisiin, joiden avulla kokeilun hyötyjä voidaan tarkastella yhdenmukaisesti ja objektiivisesti myöhemmässä vaiheessa. Kriteeristön kehittäminen auttoi selkeyttämään, mitä osa-alueita kokeilun aikana halutaan mitata ja millä tavoin tuloksia voidaan hyödyntää päätöksenteossa.

Iltapäivällä käsittelin vastuuasiakkuuteni esittämää tiedontarvetta, joka koski palvelinympäristön aplikaatioiden käyttöä. Tarkastelin asiakkuuden toimittamaa dataa ja kokosin yhteenvedon, joka auttoi heitä arvioimaan päivitysten priorisointia ja varmistamaan, että resurssit kohdistetaan

tarkoituksenmukaisesti. Työ tuki asiakkaan omaa päätöksentekoa ja tarjosi paremman näkyvyyden ympäristön nykytilanteeseen.

Keskiviikko

Keskiviikko painottui asiakkuuksien koordinointiin ja kokonaisuuksien hallintaan. Aamupäivällä osallistuin asiakkaan tikettipalaveriin, jossa käytiin läpi kaikki avoinna olevat tehtävät ja niiden tämänhetkinen tilanne. Keskusteluissa tarkasteltiin myös haavoittuvuuksienhallintaa yleisellä tasolla: missä vaiheessa korjaukset etenevät, mihin kohteisiin liittyy eniten kiireellisyyttä ja mitkä tapaukset tulisi viedä eteenpäin seuraaville vastuuhenkilöille. Palaveri auttoi muodostamaan selkeän näkymän asiakkuuden tilanteesta ja priorisoimaan toimenpiteitä niin, että työ etenee johdonmukaisesti.

Myöhemmin päivällä osallistuin sisäiseen valmistelupalaveriin, jossa käytiin läpi toisen asiakkuuden kuukausikatsausta varten koottavat aiheet. Kokouksessa tarkasteltiin meneillään olevia projekteja, ajankohtaista haavoittuvuustilannetta sekä viime aikojen turvallisuushavaintoja. Valmistelutyö mahdollisti sen, että varsinaisessa palaverissa voidaan esittää kattava tilannekuva ja tuoda esiin ne kohdat, jotka edellyttävät erityistä huomiota.

Iltapäivällä tein kollegan pyytämän palautteen sekä arvioin omaa suoriutumistani osana organisaation vuosittaista arviointikäytäntöä. Reflektointi tarjosi hyvän tilaisuuden tarkastella omaa kehitystäni kuluneen vuoden ajalta. Huomasin, että vuoden aikana on kertynyt merkittävästi uusia kyvykkyyksiä ja vastuuta, ja työssä kehittyminen on ollut huomattavasti laaja-alaisempaa kuin olin arjessa tullut miettineeksi. Prosessi vahvisti käsitystä siitä, miten tärkeää on pysähtyä aika ajoin arvioimaan omaa edistymistä ja tunnistamaan osa-alueet, joissa kasvu on ollut merkittävää.

Torstai

Torstain aamupäivä painottui ulkoiseen näkyvyyteen liittyvään selvitystyöhön ja laajemman hyökkäyspinnan arviointiin. Tein OSINT-pohjaista kartoitusta erään asiakasorganisaation julkisista palveluista ja ulkoisesta rajapinnasta. Analyysin perusteella tunnistin muutamia kohteita, jotka poikkesivat tavanomaisesta profiilista ja jotka edellyttivät tarkempaa tutkintaa. Dokumentoin havaitut palvelut ja tiketöin ne eteenpäin lisäselvityksiä varten.

Kartoituksen sivulöydöksenä huomasin myös erään ulkopuolisen yrityksen kehitysympäristön, joka oli jätetty avoimeksi internetiin siten, että hakemistorakenne oli selattavissa ilman autentikointia. Koska kyseessä ei ollut oma asiakkuus, otin tilanteesta yhteyttä yritykseen sekä ilmoitin asiasta kyberturvallisuuskeskukselle. Ilmoituksen tekemisen jälkeen palvelu poistettiin näkyvistä nopeasti, mikä osoitti, että tieto kulki oikeille tahoille ja ympäristön näkyvyys ulospäin pystyttiin rajaamaan havaintojen jälkeen.

Osallistuin myös teknologiatoimittajan kanssa pidettävään määräaikaiseen katsaukseen, jossa käytiin läpi ajankohtaisia kysymyksiä ja kehitysehdotuksia liittyen erääseen valvonnassa hyödynnettävään ratkaisuun. Palaveri tarjosi hyvän mahdollisuuden tarkentaa havaittuja ilmiöitä, esittää parannusideoita ja varmistaa, että teknologian käyttö vastaa arjessa esiin tuleviin tarpeisiin.

Iltapäivällä osallistuin organisaation sisäiseen kyberturvallisuustapahtumaan, jossa eri tiimien asiantuntijat työstivät kehitysehdotuksia pienissä ryhmissä. Tapahtuman tavoitteena oli tunnistaa mahdollisuuksia palveluiden, prosessien ja yhteistyön parantamiseen. Keskustelut toivat esiin uusia näkökulmia siitä, miten eri osa-alueet voidaan sovittaa yhteen entistä tehokkaammin ja miten palveluiden vaikuttavuutta voitaisiin kasvattaa tulevaisuudessa.

Perjantai

Perjantain työ painottui kehityshankkeisiin ja suunnitteluun. Aamupäivällä työstin luonnosta uudesta palvelukokonaisuudesta, jota olen valmistellut organisaation sisäiseksi ehdotukseksi. Rakensin ideasta tiiviin yhden dian esityksen ja jaoin sen palveluiden kehittämisestä vastaaville tahoille jatkokäsittelyä varten. Tavoitteena oli selkeyttää kokonaisuuden päälinjat ja arvioida alustavasti, miten se voisi tukea nykyisiä palveluprosesseja.

Jatkoin myös käynnissä olevan kehitysprojektin tilannekartoitusta tarkastelemalla aiemmin arvioituja ratkaisuja ja niiden soveltuvuutta asetettuihin tavoitteisiin. Koostin aiheesta yhteenvedon, jonka tarkoituksena on tarjota johdolle selkeä näkymä projektin etenemisestä ja vaihtoehdoista, joita arvioidaan osana päätöksentekoa.

Päivän aikana kävin läpi yhden asiakasorganisaation haavoittuvuusskannerin tuloksia ja keskityin erityisesti palvelinten päivitystarpeisiin. Laadin löydöksistä yhteenvedon ja toimitin asiakkaalle suositukset, joiden perusteella he voivat priorisoida päivitykset ja toteuttaa ne hallitusti.

Iltapäivällä osallistuin teknologiatoimittajan kanssa käytyyn alustavaan keskusteluun, jossa tarkasteltiin heidän tuotteidensa mahdollista soveltuvuutta tulevaisuuden tarpeisiin. Tapaaminen tarjosi hyödyllisen näkymän siihen, millaisia vaihtoehtoja markkinoilla on ja mitä osa-alueita voisi olla perusteltua tarkastella osana laajempaa kehitystyötä.

2.4.3 Yhteenveto

Neljäs seurantaviikko kokosi yhteen useita keskeisiä osa-alueita, jotka ovat olennainen osa päivittäistä kyberturvallisuuden asiantuntijatyötä. Viikon aikana korostui erityisesti se, miten tärkeää on erottaa todelliset uhat konfiguraatiovirheistä ja virheellisistä hälytyksistä, sekä se, miten systemaattinen analysointi ja juurisyiden selvittäminen tukevat laadukasta poikkeamienhallintaa. Useampi viikon tapaus vahvisti näkyvyyden ja peruskonfiguraatioiden merkitystä riskien arvioinnissa.

Haavoittuvuuksienhallinta ja asiakkuuksien koordinointi olivat merkittävä osa viikon työskentelyä. Raporttien läpikäynti, päivitystarpeiden arviointi ja tikettien tilannekuva loivat selkeän ymmärryksen siitä, missä vaiheessa korjaukset etenevät ja mihin resursseja kannattaa kohdistaa. Samalla viikko osoitti, kuinka olennaista on esittää havainnot ymmärrettävästi ja priorisoidusti, jotta asiakkailla on realistinen kuva ympäristön riskitasosta.

Kehitysprojektien ja palveluehdotusten eteenpäin vieminen vahvisti kokonaiskuvaa siitä, miten uudet ideat, prosessit ja tekniset kokeilut voidaan liittää osaksi organisaation strategista suunnittelua. Erityisesti vertailukriteeristön viimeistely osoitti, kuinka tärkeää on luoda selkeät mittarit, joiden avulla eri vaihtoehtoja voidaan arvioida tasapuolisesti ja todennettavasti.

Kokonaisuutena neljäs seurantaviikko osoitti, miten monipuolisesti asiantuntijatyö yhdistää teknistä analyysia, koordinointia, riskienhallintaa ja prosessien kehittämistä. Viikko tarjosi selkeän näkymän siihen, miten eri toimintojen rajapinnat liittyvät toisiinsa ja miten oma rooli tukee sekä operatiivista turvallisuutta että organisaation pitkäjänteistä kehitystyötä.

3 Pohdinta

Tämän oppimispäiväkirjan neljän viikon seurantajakso tarjosi kokonaisvaltaisen kuvan siitä, millaista osaamista ja ajattelutapaa kyberturvallisuuden asiantuntijatyö käytännössä edellyttää. Jakso osoitti selkeästi, että tekninen osaaminen muodostaa vain yhden osan laajempaa kokonaisuutta, jossa korostuvat jatkuva oppiminen, yhteistyö eri sidosryhmien kanssa sekä kyky tunnistaa ja priorisoida olennaisia riskejä osana päivittäistä työtä.

Keskeinen havainto liittyi työssä tarvittavaan systemaattisuuteen. Poikkeamienhallinnan ja haavoittuvuuksien käsittelyn aikana korostui, kuinka tärkeää on erottaa todelliset uhat konfiguraatiovirheistä ja virheellisistä hälytyksistä. Tämä edellyttää johdonmukaista analyysia, luotettaviin tietolähteisiin perustuvaa päätöksentekoa sekä ymmärrystä siitä, miten yksittäiset havainnot kytkeytyvät laajempaan kokonaiskuvaan.

Toinen merkittävä oppi liittyi yhteistyöhön ja tiedonvaihtoon. Viikoittaiset palaverit, tikettikoordinointi, toimittajatapaamiset ja asiakkuuksien kanssa käydyt keskustelut osoittivat, että tietoturvatoiminnan laatu riippuu olennaisesti siitä, miten tieto liikkuu eri tiimien ja roolien välillä. Tiedon esittäminen ymmärrettävässä ja priorisoidussa muodossa nousi yhdeksi tärkeimmistä taidoista, sillä se vaikuttaa suoraan siihen, miten nopeasti ja tarkoituksenmukaisesti asiakkaat ja muut sidosryhmät pystyvät tekemään päätöksiä.

Kolmas kokonaisuus liittyi kehittämistyöhön ja sen realiteetteihin. Osallistuminen POV-suunnitteluun, arviointikriteerien rakentamiseen, sisäisiin kehitysprojekteihin ja palveluideoiden konseptointiin osoitti, että kehittämistyö vaatii kykyä yhdistää tekninen ymmärrys organisaation tarpeiden arviointiin ja laajemman kokonaisuuden hahmottamiseen. Samalla se edellyttää valmiutta tarkastella olemassa olevia käytäntöjä kriittisesti ja esittää perusteltuja

parannusehdotuksia. Tämä vahvisti käsitystä siitä, että teknologiset päätökset ja prosessit tulee asemoida osaksi organisaation pidemmän aikavälin tavoitteita.

Seurantajakson aikana opin myös paljon omasta työskentelytavastani. Reflektointi toi esiin vahvuuksia erityisesti analyyttisessä työskentelyssä, priorisoinnissa ja yhteistyössä eri tiimien kanssa. Samalla tunnistin kehityskohteita, kuten tarpeen vahvistaa dokumentointini yhdenmukaisuutta ja tavoitteideni tarkkaa määrittelyä kehitysprojekteissa. Onnistumiset ja pienemmät epävarmuudet muodostivat kokonaisuuden, joka osoitti, että jokainen viikko tarjosi mahdollisuuden oppia uutta ja syventää osaamista.

Kokonaisuutena oppimispäiväkirja vahvisti käsitystä siitä, että kyberturvallisuus on jatkuvasti kehittyvä ja monialainen kokonaisuus. Asiantuntijan rooli ei rajoitu pelkkään tekniseen tekemiseen, vaan edellyttää laaja-alaista ymmärrystä prosesseista, ihmisten välisestä vuorovaikutuksesta ja strategisista valinnoista. Seurantajakso osoitti, että oma työni tukee sekä operatiivista toimintaa että organisaation laajempaa kehitystä ja että kehittyminen tässä roolissa on jatkuva prosessi, joka rakentuu arjen havaintojen ja pitkäjänteisen oppimisen varaan.

Lähteet

CISA. 2016. CRR Supplemental Resource Guide, Volume 4: Vulnerability Management. Carnegie. Mellon University.

Dietle, James. 2016. Effective Threat Intelligence: Building and Running an Intel Team for Your Organization. CreateSpace Independent Publishing Platform.

ENISA. 2020. How to Set Up CSIRT and SOC: Good Practice Guide. Athens: European Union Agency for Cybersecurity.

ISO. 2022. ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva: International Organization for Standardization.

Luttgens, Jason; Pepe, Matthew & Mandia, Kevin. 2014. Incident Response & Computer Forensics, Third Edition. New York: McGraw-Hill Professional.

NIST. 2012. SP 800-61 Revision 2 – Computer Security Incident Handling Guide. Gaithersburg, MD: National Institute of Standards and Technology.

NIST. 2018. SP 800-37 Revision 2 – Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Gaithersburg, MD: National Institute of Standards and Technology.

NIST. 2022. SP 800-160 Volume 1 Revision 1 – Engineering Trustworthy Secure Systems. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-160v1r1.

PMI. 2021. A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Seventh Edition. Newtown Square, PA: Project Management Institute.