Opinnäytetyö AMK

Tieto- ja viestintätekniikka

2020

Osku Lund

PÄIVÄKIRJAOPINNÄYTETYÖ

– verkonvalvojana IT Operations Centerissä

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

OPINNÄYTETYÖ (AMK)

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2020 | 41 sivua

Osku Lund

PÄIVÄKIRJAOPINNÄYTETYÖ

- verkonvalvojana IT Operations Centerissä

Tämän päiväkirjatyyppisen opinnäytetyön tavoitteena oli seurata henkilökohtaista kehittymistä verkonvalvojana. Työn tekijä työskentelee IT Operations Centerissä, joka valvoo yrityksen tarjoamia verkko- ja konesaliympäristöjä. Työ tehtiin reilu 400 hengen ICT-alan yrityksessä, joka on osa pohjoismaista telekommunikaatiokonsernia. Seurantaa tehtiin päivittäisillä raporteilla ja viikottaisilla viikkoanalyyseillä 1.6.2020–8.8.2020.

Päiväkirjaopinnäytetyössä seurataan verkonvalvojan työtehtäviä ja ongelmia, joita verkonvalvoja työssään päivittäin joutuu kohtaamaan ja ratkaisemaan. Työtehtävät olivat palvelinpainotteisia, sillä työntekijä työskentelee tiimissä, joka keskittyy palvelinasiakkaiden tiketteihin ja palvelupyyntöihin.

Päiväkirjaopinnäytetyössä havainnoidaan, kuinka verkonvalvoja kehittyi työssään ja kasvatti ammattitaitoaan.

ASIASANAT:

palvelin, verkkovalvonta, tietoverkko, service desk, päiväkirja

BACHELOR´S THESIS

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and communication technologies

2020 | 41 pages

Osku Lund

DIARY-BASED THESIS

- ICT Specialist in an IT Operations Center

The goal of this diary-based thesis was to follow personal growth as an ICT specialist. Writer of the thesis works in an IT Operations Center which monitors all the networks and data center environments the company provides to its customers.The thesis was made in an over 400 employee ICT service company that is part of a Nordic telecommunication concern. Work monitoring was done by daily raports and weekly analysis 1.6.2020–8.8.2020.

This diary-based thesis follows tasks and problems that an ICT specialist investigates and solves on daily basis. Problems that the ICT specialist solves are server oriented as the employee is part of a team that works with and focuses on CDC customers.

This diary-based thesis observes how the ICT Specialist grew his professional skills and got better at his job.

KEYWORDS:

server, ict specialist, network, service desk, diary

SISÄLTÖ

KÄYTETYT LYHENTEET JA SANASTO

AD	Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu (Active Directory)
CDC	Pilvi- ja konesalipalvelut (Cloud and datacenter)
CDP	Protokolla, jolla pystytään tarkastelemaan lähiverkossa olevia laitteita (Cisco Discovery Protocol)
Checkpoint	Israelilainen palomuurivalmistaja
Citrix	Yritys, joka toimittaa palvelin- ja työasemavirtualisointiratkaisuja
CLI	Komentorivin käyttöliittymä (Command Line Interface)
CNAME	Ohjaa verkkotunnuksen alidomainin liikenteen johonkin toiseen verkkotunnukseen tai sen alidoimainiin
Cortex XDR	Palo Alton päätelaitteiden tietoturvavalvontajärjestelmä
Datastore	Virtuaalisessa palvelinympäristössä oleva jaettu datasäiliö
DDoS	Palvelunestohyökkäys, jolla pyritään häiritsemään palvelimen tai palvelun toimintaa (Distributed Denial of Service)
Deadlock	Oracle-palvelimella oleva lukkotila, jonka aiheuttaa jumiin jäänyt prosessi tai resurssi
Failover	Vikasietoisuus, varmistetussa ympäristössä aktiivisuuden vaihtuminen laitteiden välillä
GlobalProtect	Palo Alton VPN -palvelusta käytettävä nimitys
GPM	Keskitetty käyttäjäoikeuksien hallintajärjestelmä (Group Policy Management)
GPO	Hallitsee toimialueen työasemia ja palvelimia. Määrittää toimialueen käyttäjä- ja tietokoneryhmille asetukset (Group Policy Object)
Host	Palvelin, jolla virtuaalikoneet pyörivät ja jonka resursseja virtuaalikoneet käyttävät.
Hälymies	Vuorossa oleva henkilö, joka seuraa hälytaulua ja luo sitä kautta tikettejä
Hälytaulu	Valvontaohjelma, jonne valvotuilta laitteilta generoituvat hälytykset tulevat näkyviin
Händeri	Edelliseltä vuorolta saatu tiketti, jonka tutkintaa täytyy jatkaa
I/O-virhe	Tietokonelaitteen ja toisen tietokonelaitteen tai ulkoisen maailman välillä tapahtuva kommunikaatiovirhe

IAP-klusteri	Tukiasemat, jotka muodostavat WLAN-verkon
iDRAC	Fyysisten Dell-palvelinten hallintajärjestelmä
IPAM	Järjestelmä jolla hallitaan tietoverkkojen osoiteavaruutta (IP Address Management)
WLAN-kontrolleri	Laite, jonka kautta WLAN-verkon tukiasemia voidaan keskitetysti hallita
Kanta	Tietokanta, jonne dataa tallennetaan
LDAP-palvelin	Palvelin, jolla LDAP-hakemistopalvelu pyörii
MPLS	Runkoverkon solmujen kautta kulkeva yhteys, jota ei reititetä erikseen (Multiprotocol Label Switching)
Osio	Linuxissa levy jaetaan osioihin
Palo Alto	Amerikkalainen palomuurivalmistaja
Palveluntarjoaja	Yritys, joka tarjoaa toimipisteelle verkkoyhteyden
Panorama	Palo Alton keskitetty palomuurihallintaohjelma
RDP	Windows-palvelimille kirjautumisessa käytettävä protokolla (Remote Desktop Protocol)
RMA	Laitevalmistajan laitepalautuksissa käytetty numero, jolla laitevalmistaja valtuuttaa palautuksen (Return Merchandise Authorization)
Robot Watcher	Palvelimilla oleva ohjelma, joka valvoo palvelimen toimintaa ja generoi hälytyksiä palvelimesta
SAP	Toiminnanohjausjärjestelmä
SD	Käyttäjätukipalvelu (Service Desk)
SD WAN	Ohjelmisto-ohjattu tapa hallita ja toteuttaa yritysverkkoja (Software-Defined Networking)
Skripti	Pieni ohjelma, joka on lyhyt ja helposti ymmärrettävä
SmartConsole	Checkpointin keskitetty palomuurihallintaohjelma
Snapshot	Virtuaalikoneen sen hetkisestä tilasta otettava kopio, joka tallentaa koneen tilan ja datan
Stream	Suoratoisto. Tiedonsiirtotapa, jolla palveluntarjoaja esittää loppukäyttäjälle tiedoston multimediasisältöä reaaliajassa
Taulutila	Tietokannassa taulujen tallennukseen määritelty fyysinen tietoalue
Tukiasema	Laite, joka kaiuttaa WLAN-verkkoa

vCenter	ESXi-palvelimen keskitetty hallintaohjelma
VLAN	Virtuaalilähiverkko, osiin jaetun fyysisen verkon virtuaalinen verkko (Virtaul LAN)
VPN	Virtuaalinen erillisverkko (Virtual Private Network)

1 JOHDANTO

Päiväkirjatyylisessä opinnäytetyössä kuvataan, millaisia työtehtäviä verkonvalvojana IT Operations Centerissä (ITOC) työskennellessäni suoritan. Raportointia tehtiin kymmenen viikon ajanjaksolla 1.6. – 8.8.2020. Joka viikon päätteeksi kirjoitan viikkoanalyysin, jossa pohdin, onko itselle asetetut viikkotavoitteet täyttyneet ja mitä uutta olen oppinut.

Työskentelen reilun 400 ihmisen ICT-alan yrityksessä, joka on osa pohjoismaista telekommunikaatiokonsernia. Yritykseni on arvostettu asiantuntijaorganisaatio, joka tarjoaa asiakkailleen laadukkaita ICT-palveluratkaisuja. Asiakkaisiin kuuluu julkishallinnon yrityksiä, pörssiyrityksiä ynnä muita keskisuuria ja suuria yrityksiä. Asiakasyritysten yksityisyyden suojaamiseksi raportti ei sisällä yritysten nimiä tai sijainteja.

ITOC:ssa valvomme kaikkien asiakkaiden ympäristöistä ja laitteista tulevia häiriöilmoituksia ja ratkaisemme häiriöistä syntyviä tikettejä. Kirjoitan raportissa erilaisista työtehtävistä, joita kohtaan päivittäin. Työtehtäviini kuuluvat verkonvalvonta, verkkojen ja palvelimien vianhallinta sekä palvelu- ja muutospyyntöjen toteutus. Tehtäviini kuuluu myös asiakasrajapinnassa asiakasyritysten IT-ammattilaisten kanssa edellä mainittuihin työtehtäviin liittyvä kommunikointi ja asiakaspalvelu

2 NYKYTILANTEEN KUVAUS

Kaikki työtehtäväni ovat tikettejä. N. 80 % tiketeistä luodaan hälytaulun kautta ja lopput 20 % tulevat asiakkaalta sähköposteina tai puheluina. Ratkon päivisin pääasiassa häiriötikettejä, mutta välillä teen myös palvelupyyntö- tai muutostikettejä.

2.1 Oman nykyisen työn analyysi

ITOC:ssa on neljä eri tiimiä, joiden välillä asiakkaat on jaettu. Kuuluun tiimiin, joka keskittyy konesali- ja pilvipalveluasiakkaisiin. Työssäni vaaditaan hyvää ymmärrystä tietotekniikasta, ymmärrystä verkko- tai palvelinasioista ja asiakaspalvelutaitoja. Palvelukielinä ovat suomi ja englanti. Käytän monia eri järjestelmiä ja teknologioita päivittäisessä työssäni.

ITOC:ssa käsittelemme ja vastaanotamme asiakkaiden tukipyyntöjä. Päätyövälineeni on tikettijärjestelmä, jossa kaikki häiriö-, palvelupyyntö- ja muutostiketit sijaitsevat. Teen päivisin pääasiassa häiriötikettejä (IM). Palvelupyyntö- (SR) ja muutostikettejä (CM) suorittavat entiset ITOClaiset, jotka ovat siirtyneet vuorokierrosta päivävuoroon. Teen päivisin myös SR:ä tai CM:ä, jos asiakkaan pyynnöllä on kiire tai jos vastaanotan puhelun tällaiseen tikettiin liittyen.

Häiriötiketillä käsitellään asioita, jotka ovat ennen toimineet, mutta eivät toimi enää, esim. toimipistellä yksi kytkin lakkaa vastaamasta valvonnassa. Palvelupyynnöt ovat nopeita ja helppoja muutoksia, joilla asiakas pyytää pientä lisäystä tai muutosta, esim. kytkinportin konfiguraatiomuutosta. Muutospyynnöt ovat pitempikestoisia ja haastavampia tikettejä, joilla tehdään suurempia muutoksia asiakkaiden ympäristöön, esim. uuden VPN-tunnelin luonti.

Olen koko vuoron ajan kirjautuneena puhelinsovellukseemme, jota kautta asiakkaiden puhelut tulevat. Päivävuorossa puhelin soi normaalisti 5–15 kertaa päivässä. Asiakkaat soittavat ilmoittaakseen aktiivisesta häiriöstä tai jos heillä on asiaa tiettyyn tikettiin liittyen. Päivävuorossa tiketit, joita ratkon, tulevat pääosin päivän aikana tulleista puheluista. Yövuorossa, kun puheluita tulee muutamia, kerkeän tutkimaan syvällisesti häiriötilanteita ja tekemään palvelupyyntötikettejä.

Keskeisessä asemassa ovat myös kollegat, joilta saa apua tarvittaessa. Koska valvomme asiakkaiden ympäristöjä ja laitteita, tarvitsemme työssämme monia erilaisia järjestelmiä, joista valtaosa oli minulle uusia, kun aloitin verkonvalvojan työt. Minulla ja kollegoilla on koko ajan mahdollisuus kysyä ja saada apua ongelmien ratkaisemiseksi. Jos kollegoilta ei saa apua, voi kysyä päivävuorolaisilta ja viimeiseksi asiantuntijoilta.

Tarvitsen työssäni asiakaspalvelutaitoja, sillä olen päivittäin asiakkaisiin yhteydessä. Asiakaskommunikointi tapahtuu pääosin sähköpostin välityksellä. Lähetän päivittäin kymmeniä sähköposteja asiakkaiden IT-asiantuntijoille. Puhelintyöskentely vaatii myös hyvät asiakaspalvelutaidot.

Hyvä verkonvalvoja kykenee toimimaan itsenäisesti, ymmärtää ja osaa käyttää erilaisia järjestelmiä ja teknologioita, osaa etsiä ratkaisuja, pystyy selvittämään ongelmia ja omaa hyvät asiakaspalvelutaidot.

Aloitin ITOC:ssa vuoden 2019 toukokuussa kesätyöntekijänä ja työskentelin yrityksessä viisi kuukautta, ennen kuin menin takaisin opiskelemaan. Tämän vuoden maaliskuussa kirjoitin vakituisen työsopimuksen verkonvalvojan työhön. Kun aloitin, en ymmärtänyt oikeastaan mistään mitään. Aluksi termejä ja alan jargonia tuli paljon opittavaksi ja ne olivat vieraita. Ensimmäiset viikot menivät kollegoita konsultoidessa, sillä en osannut ratkaista kuin helpoimpia tikettejä. Kesän loppuun mennessä kykenin työskentelemään itsenäisesti ilman, että minun tarvitsi koko ajan kysellä apua. Ammatilliset taitoni ovat kehittyneet valtavasti kuluneen vuoden aikana. Haluaisin kehittää asiakaspalvelutaitojani, sillä tunnen, että se on tällä hetkellä heikoin osa-alueeni.

2.2 Sidosryhmät työpaikalla

Sidosryhmiä on useita. Jaoittelen sidosryhmät ulkoisiin ja sisäisiin.

Sisäisistä sidosryhmistä kaikista läheisin on kollegat. Nyt etätyöaikana olemme koko ajan samassa Teams-palaverissa, jossa voi kysyä neuvoja ja apuja koko vuoron ajan. Yleensä vastauksen saa kysymykseen kollegoilta tai päivävuorolaisilta. Jos kenelläkään ei ole antaa vastausta, kysyn asiantuntijoilta. Asiantuntijat työskentelevät asiakasprojekteissa ja keskittyvät muutamiin järjestelmiin tai teknologioihin, joista heillä on syvä ymmärrys. Olen kymmeniä kertoja saanut asiantuntijoilta loistavia vinkkejä ja neuvoja.

Asiakkaat ovat läheisin ulkoinen sidosryhmä, jonka kanssa kommunikoin päivittäin. Usein ongelmien ratkaisu vaatii lisää tietoja, joita tiedustelen asiakkailta niin sähköpostin kuin puhelun välityksellä. Laajempia tai pitkäkestoisempia ongelmia tutkiessa asiakkaan kanssa voidaan olla päivittäin yhteydessä jos ongelman ratkaisu vaatii jatkuvaa kommunikointia.

Alihankkijoiden kanssa olen myös lähes päivittäin tekemisissä. Alihankkijat ovat kolmannen osapuolen yrityksiä, jotka hoitavat lähitukea eli pääasiassa asentavat ja huoltavat laitteita. Alihankkijoiden yleisimmät työnkuvat ovat uusien laitteiden asennus ja rikkinäisten laitteiden tarkastus ja vaihto.

Palveluntarjoajien kanssa työskentely on päivittäistä. Jos toimipisteen verkko ei toimi, olemme herkästi palveluntarjoajaan yhteydessä. Kun toimipisteellä on verkko-ongelmaa ja olemme tarkastaneet, että ongelma ei ole sisäverkossa, delegoimme häiriöntutkinnan palveluntarjoajille.

Laitevalmistajien kanssa työskentelemme myös tiiviisti. Laitteella ilmenneen ongelmatilanteen jälkeen avaamme tiketin laitevalmistajalle ja mahdollisesti aloitamme RMA prosessin. Haastavimmissa ongelmatilanteissa, mitä emme pysty ratkaisemaan talon sisällä, olemme laitevalmistajaan yhteydessä ja avaamme TAC tiketin heille. Laitevalmistajat ovat keskeisessä asemassa ongelmanratkaisua monissa haastavissa ongelmissa.

2.3 Vuorovaikutustaidot työpaikalla

Hyvät vuorovaikutustaidot ovat keskeisessä asemassa työssäni. Työskentelen päivittäin läheisesti vuorossa olevien kollegoiden kanssa. Toimistolla pystyn koko ajan kysymään vieressä istuvalta kollegalta neuvoja tai ohjeita, jos en pysty ongelmaa itsenäisesti ratkaisemaan. Etänä töitä tehdessä viestintä tapahtuu Teamsin, Skypen ja sähköpostin välityksellä, mikä tuo omat haasteensa.

Asiakkaiden kanssa viestintä vaatii hyvät asiakaspalvelutaidot. Puhelimitse tapahtuva kommunikointi on vaativampaa, sillä vastaukset täytyy tietää lähes välittömästi. Kommunikoinnin täytyy olla selkeää ja asiantuntevaa. Asiakkaan kanssa järjestettävissä tapaamisissa, joissa aktiivista häiriötä tutkitaan, on hiukan rennompaa, kuin yleensä. Tapaamisissa saattaa olla useampia eri tahoja, jotka kaikki tarkastavat, että niiden ylläpitämänsä järjestelmä tai laite toimii. Reipas asiakaspalveluasenne ja selkeä kommunikointi on tärkeää, sillä tällaisissa tilanteissa häiriö saattaa olla laaja ja asiakas on suuren

paineen alla. Sähköpostin välityksellä tapahtuva kommunikointi vaatii hyvät oikeinkirjoitustaidot. Esitetty asia täytyy osata muotoilla sellaiseen muotoon, joka on selkeä ja hyvien asiakaspalvelutapojen mukainen.

Minulla on hyvät vuorovaikutustaidot, joista on hyötyä työssäni. Aikaisemmasta asiakaspalvelukokemuksestani oli hyötyä tässä työssä aloittaessani. Sähköpostin välityksellä käytävässä kommunikaatioissa osaan muotoilla esitettämäni asian selkeään ja kohteliaaseen muotoon.

3 PÄIVÄKIRJARAPORTOINTI

3.1 Seurantaviikko 1

Viikon tavoitteet

Ensimmäisen viikon olin yövuorossa eli tavoitteena luonnollisesti oli pysyä hereillä ja virkeänä. Uusien palomuurisääntöjen tekeminen oli jäänyt vähemmälle, joten tavoitteena on tehdä yksi palvelupyyntö, jossa pyydetään uutta palomuurisääntöä. Tavoitteenani oli myös kartuttaa tietoa palomuureista.

Maanantai 1.6.2020

Päivän tavoitteena oli tehdä tiketti, mitä en ennen osannut ratkaista.

Päivä alkoi ilmoituksella, että käyttäjätunnukseni salasana on vanhenemassa. Vaihdoin sen ja jatkoin työskentelyä muutaman minuutin, kunnes tarvitsin uutta salasanaa. Tajusin, että en muistanut uutta, juuri vaihtamaa salasanaani, ja jouduin vaihtamaan sen uudestaan.

Löysin tikettijonosta palvelupyyntötiketin, jossa asiakas haluaa yhteen palomuurisääntöön uuden lähdeosoitteen. Kysyin kollegalta, mihin muutos täytyi tehdä. Osoitteen lisääminen osoittautui vaivattomaksi toimenpiteeksi, jonka osasin suorittaa kollegan neuvojen ansiosta onnistuneesti.

Erään toimipisteen kahden palomuurin klusterin molemmat laitteet piti käynnistää uudelleen ja sitä ennen suorittaa failover aktiiviselta palomuurilta passiiviselle palomuurille. Toimenpiteelle löytyi valmiit ohjeet ja niitä seuraamalla sain suoritettua failoverin ja käynnistettyä ensimmäisen palomuurin onnistuneesti. Suoritin failoverin uudestaan ja käynnistin toisen palomuurin onnistuneesti uudestaan. Lopuksi lähetin asiakkaalle sähköpostin, jossa ilmoitin, että toimenpiteet on suoritettu.

Sain puhelun, jossa asiakas ilmoitti, että hänen kriittinen palvelin ei toimi. Tarkistin pikaisesti palvelimen tilan ja huomasin, että palvelin oli epäresponsiivisessa tilassa, joten käynnistin palvelimen uudestaan. Soitin hetken päästä asiakkaalle varmistaakseni, että palvelin toimii. Asiakas varmisti, että palvelin toimii nyt halutulla tavalla.

Tiistai 2.6.2020

Päivän tavoitteena oli oppia jotain uutta.

Vuoron aluksi suljin rutiininomaisia tikettejä, jotka eivät vaatineet erityisempiä toimenpiteitä. Löysin muutaman tiketin, joita pystyin edistämään tämän yön aikana.

Asiakas oli pyytänyt virtuaalipalvelimen kovalevyllä lisää tilaa. Suoritin lisäyksen ja informoin asiakasta levyn onnistuneesta laajennuksesta.

Asiakas oli tehnyt töitä palvelimella, minkä seurauksena palvelimen etäyhteys oli mennyt rikki. Kirjauduin palvelimelle konsoliyhteydellä. Huomasin verkkokorttiasetuksista, että palvelimen molemmista verkkokorteista oli IP-osoitteet kadonneet. Pienen ihmettelyn jälkeen lisäsin oikeat IP-osoitteet molemmille verkkokorteille, jonka jälkeen pystyin taas kirjautumaan RDP:llä palvelimelle. Ilmoitin asiakkaalle tehdyistä tutkinnoista ja toimenpiteistä ja suljin tiketin.

Meidän keskitetty palvelintenvalvontasivu ei toiminut. Kävin kuormantasaajalta tarkastamassa, että valvontasivun pool oli alhaalla. Käynnistin kuormantasaajien robot watcherit ja yhden valvonta-anturin uudestaan, jonka jälkeen sivusto alkoi taas toimimaan.

Toimipisteen IAP klusteri piti päivittää, koska toimipisteen nykyinen versio ei tue toimipisteelle tulleita uusia tukiasemia. Tarkistin toimipisteen kytkimeltä, minkä porttien takana uudet tukiasemat ovat ja kytkin niiden porttien virransyötön pois päältä. Päivitys ei onnistu, jos uudet tukiasemat ovat päällä. Ajoin päivityksen klusterille WLAN kontrollerin graafisen käyttöliittymän kautta. Klusterin versiopäivityksen jälkeen kytkin kytkimeltä uusien tukiasemien virransyötön takaisin päälle. Hetken odottelun jälkeen uudet tukiasemat tulivat kontrollerille näkyviin, eli päivitys onnistui.

Edellisöinen kriittinen palvelin oli taas lakannut toimimasta. Olin käynnistämässä palvelinta uudestaan, kun kollega ilmoitti, että palvelin toimii taas. Huomasin, että tästä palvelimesta oli tullut aiemmin tänään tiketti palvelimen muistin loppumisesta. Palvelimella toimiva sovellus tai prosessi käytti kaiken muistin, jonka takia palvelin jumiutui.

Keskiviikko 3.6.2020

Päivän tavoitteena oli oppia jostain uudesta järjestelmästä tai teknologiasta.

Edellisyön palvelin, jonka verkkokortit kävin konfiguroimassa, oli taas mennyt rikki, eikä asiakas saanut enää siihen yhteyttä. Toinen verkkokortti, jolla yhteys ulkoverkkoon toimii, oli disabloitu. Laitoin verkkokortin päälle ja yhteys alkoi toimimaan. Samalla tiketillä

asiakas pyysi, voisimmeko tarkastaa asetuksista, miksi nettiyhteys palvelimella ei toimi. Tutkintojen jälkeen tulin siihen tulokseen, että liikennettä ei ole sallittu palomuurilla, sillä samassa verkossa olevia palvelimia pystyi pingaamaan, mutta ulkoverkkoon asti paketit eivät menneet.

Asiakkaan uuden virtuaalisen SQL palvelimen levyä piti laajentaa 2 Tt:a. Laajennusta suorittaessani huomasin, että datastore, jolla palvelimen levyt ovat, on sen verran täynnä, että levyä ei pysty kasvattamaan. Koska tämä datastore on täynnä, siitä pitäisi tulla hälytys ja sitä kautta tiketti. Löysinkin datastoren korkeasta täyttöasteesta tiketin ja otin sen heti työn alle. Migrasin 2.8 Tt:n edestä virtuaalikoneita toiselle datastorelle. Sen jälkeen levyn laajennus onnistui ja datastore ei enää hälyttänyt korkeasta täyttöasteesta.

Palvelupyyntötiketti, jolla asiakas pyysi uutta palomuurisääntöä. Tiketillä oli uutta sääntöä varten toimitettu kaikki vaadittavat tiedot. Pyysin kollegalta apua muurisäännön luomiseen. Muurisäännön luomisen jälkeen informoin asiakasta suoritetusta työstä ja laitoin tiketin kiinni.

Pidin huolta hälytaulusta sen aikaa kun kollega avusti toista kollegaa erään haastavan tiketin tutkinnan kanssa.

Torstai 4.6.2020

Päivän tavoitteena oli oppia jotain uutta.

Eräältä Oracle-palvelimelta oli tullut tiketti, jossa yhden instanssin yksi taulutila on täyttymässä. Käytin palvelimella olevaa hallintaskriptiä, jolla taulutilojen tiedot saa näkyviin. Taulutilasta oli tila loppumassa, joten sitä pitää laajentaa. Tarkastin, että osiolla, jolta datablokit tulevat, on vielä vapaata tilaa. Menin instanssiin kiinni ja lisäsin 3 Gt:n datafileä tauluun, jonka jälkeen hälytys kuittaantui.

Puhelin oli soinut yövuoroksi melko paljon. Tavallisena yönä vastaan kahteen kolmeen puheluun keskimäärin, tänä yönä muutaman ensimmäisen tunnin aikana olin vastaanottanut neljä puhelua. Asiakas oli tehnyt muutoksia kahdelle Exchange-palvelimella, jonka takia Exchange oli lakannut toimimasta. Ongelman korjatakseni minun olisi pitänyt tehdä palvelimilla rekisteriin muutoksia, mutta koska minulla, tai kenelläkään vuorossa olleilla ei ollut tietoa, mitä olisi pitänyt tehdä, päätin antaa asian päivävuorolle hoidettavaksi. Asiakas soitti hetken päästä uudestaan ja kertoi, että hän tekee rollbackin ja muutokset tehdään tulevaisuudessa.

Toinen asiakas ihmetteli, miksi eräs hänen palvelimellaan toimiva ohjelma toimii huonosti. Asiakas ei ollut ilmoittanut mitään olennaisia lähtötietoja ongelmasta. Kysyin asiakkaalta tarkentavia kysymyksiä, jotta ongelmaa voitaisiin tutkia. Lisätietojen kyseleminen on melko yleistä, sillä turhan usein tiketeillä vain lukee, että joku ei toimi, voisitteko tutkia.

Kollega sai puhelun, jossa asiakas ilmoitti, että palvelin ei toimi. Kollega oli menossa käynnistämään palvelinta uudestaan, mutta ei pystynyt kirjautumaan vCenteriin. Hän pyysi minulta apua ja kävin käynnistämässä palvelimen uudestaan. Asiakas tiedusteli samalla palvelimen muistin ja prosessorien määrää ja pohti, pitäisikö palvelimen tehoja lisätä. Asiakkaan mielestä tehoja oli riittävästi, joten lisäyksiä ei suoritettu.

Viikkoanalyysi

Yövuorot ovat parasta aikaa oppia uutta, sillä puhelin ei juurikaan soi ja päivän mittaan tulleet palvelupyynnöt odottavat tikettijonossa. Yövuoroissa pystyy rauhassa tutkimaan syvällisempää tutkintaa vaativia häiriöitä ja ongelmia. Ylitin viikkotavoitteet reilusti, sillä sain paljon enemmän aikaan kuin kuvittelin. Tartuin ennalta tuntemattomiin ongelmiin kiinni ja opettelin ratkaisemaan niitä.

3.2 Seurantaviikko 2

Torstai 11.6.2020

Päivän tavoitteena oli vastata puhelimeen paljon.

Sain puhelun asiakkaalta, jossa hän ilmoitti erään toimipisteen tukiasemasta, joka ei toiminut kunnolla. Tein tiketin tästä häiriöstä. Saman puhelun aikana asiakas pyysi erään kytkimen portille porttiautentikoinnin päälle. Tein porttimuutosta varten palvelupyyntötiketin ja konfiguroin porttiin autentikoinnin päälle ja liitin portin oikeaan VLAN:in.

Sain toisen puhelun. Asiakas oli tukiasemia siirtäessään huomannut, että tukiasema ei kaiuta yhtä WLAN verkkoa. Tein tiketin tästä. Puhelun aikana asiakas mainitsi, että toimipisteen palomuurista oli myös tiketti auki. Palomuuri oli lopettanut vastaamasta valvonnassa. Toimipisteellä oli tehty sähkötöitä sinä ajankohtana, kun muuri oli lakannut vastaamasta valvonnassa. Ehdotin asiakkaalle, että hän kävisi käynnistämässä palomuurin uudestaan. Asiakas huomasi, että muurin management-portin valo ei ole päällä. Palomuuri alkoikin puhelun aikana vastaamaan pingiin, joten muuria ei tarvinnut

käynnistää uudestaan. Asiakas oli tarkastanut, että liitännät ovat kunnolla kiinni. Muurin liitännät olivat kärsineet sähkötöiden takia ja palvelin oli sen takia lakannut vastaamasta valvonnassa.

Sain puhelun palvelupyyntötiketistä, jolla asiakas halusi kytkimen portin konfiguroitua. Tarkastelin kytkimen konfiguraatioita ja ne vaikuttivat olevan jo niin kuin asiakas pyysi. Huomasinkin, että kollegalla oli tiketti työn alla. Kerroin kollegalle puhelusta ja hän teki tiketin loppuun.

Asiakas soitti tiedustellakseen erään tiketin tilaa. Tiketti oli delegoitu kolmannen osapuolen toimijalle, joka kertoi, että he eivät voi edistää tutkintaa, koska heillä ei ole pääsyä tarvittaviin järjestelmiin. Kysyin apuja tämän asiakkuuden asiantuntijalta, joka kertoi minulle, että työasema, josta tiketti on luotu, vaihdetaan pian uuteen. Ilmoitin asiakkaalle, että työasema vaihdetaan lähitulevaisuudessa, joten vanhan työaseman korjaaminen ei ole enää kannattavaa.

Uudelle kesätyöläiskollegalle oli tullut puhelu, jossa asiakas tiedusteli palvelimen tilaa, koska asiakas ei pystynyt kirjautumaan palvelimelle. Autoin kollegaa hädässä ja tarkistin, että palvelimella on kaikki hyvin. Ilmoitin kollegalle nopean tutkinnan jälkeen, että palvelin näyttää toimivan normaalisti. Kollega sanoi, että asiakas oli nyt päässyt kirjautumaan palvelimelle.

Asentaja soitti eräältä toimipisteeltä, jossa hän oli asentamassa kytkintä corekytkimeen kiinni, mutta uusi kytkin ei saanut verkkoa. Tarkastin corekytkimen lokeista, että corekytkimen portti uuteen kytkimeen oli BPDU error-tilassa. Kytkimen konfiguraatiosta huomasin, että portissa oli BPDU-suoja päällä. Otin BPDU suojan pois päältä ja uusi kytkin pääsi heti verkkoon.

Perjantai 12.6.2020

Päivän tavoitteena oli vastata puhelimeen paljon ja tehdä jotain uutta.

Sain puhelun asiakkaalta, joka halusi palauttaa palvelimen toissapäiväiseen versioon. Palvelin oli SQL-palvelin, joten delegoin palautuksen backup asiantuntijoille. Palautukset eivät menneet toivotulla tavalla, jolloin asiantuntija ehdotti, että palautus voidaan suorittaa tavalla, joka ajallisesti kestää paljon kauemmin. Soitin asiakkaalle varmistaakseni, että palvelin voidaan palauttaa tällä aikaa vievämmällä tavalla.

Tiketti, jossa palvelimella oli yksi palvelu sammunut. Kirjauduin palvelimelle ja käynnistin palvelun uudestaan. Odotin, että hälytys kuittaantui hälytysjärjestelmästä ja laitoin tiketin kiinni.

Asiakas soitti, että hän ei pääse kirjautumaan eräälle palomuurille, ja pyysi luomaan tilapäiset admin-tason tunnukset. Varmistin heti, että soittajalla on oikeudet pyytää muutoksia. Kysyin apua kollegalta tunnusten luomiseen, sillä en ollut niitä aiemmin tehnyt. Kirjauduin palomuurille ja loin tilapäistunnuksen. Testatakseni uusia tunnuksia, kirjauduin palomuurille niillä. Samaan aikaan kollega kysyi, olenko luonut tunnukset jo. Ilmoitin, että tunnukset on luotu ja toimivat. Sama asiakas oli soittanut kollegalle ja tiedusteli tunnusten tilaa. Kollega lähetti tunnuksen tiedot asiakkaalle ja puhelun aikana varmistivat, että tunnukset toimivat. Pyysin asiakasta ilmoittamaan sähköpostilla, kun tilapäistunnukset voidaan poistamaan. Kävin tunnin päästä poistamassa tunnukset, kun asiakas oli ilmoittanut, että ne voidaan poistaa.

Otin työn alle tiketin, jossa OSPF-naapuruudet ovat menneet alas. Tarkastin edellisistä samanlaisista tiketeistä, miten ongelmaa on ratkottu. Kirjauduin palomuureille tarkastellakseni lokeja, joista huomasin, että OSPF-yhteys oli katkennut kahdesti. Ensimmäinen katkos oli 18 s ja toinen 19 s. Juurisyytä katkolle en tiedä. Kirjoitin tiketille tutkinnat ja suljin tiketin.

Välillä laskutus huomaa, että joidenkin palvelinten tiedot (esim. levyjen määrä, levykapasiteetti, muisti) eivät ole ajan tasalla. Nyt laskutuksesta oli tullut pyyntö kahdesta palvelimesta, joiden tiedot eivät ole ajan tasalla. Kävin vCenteristä tarkastamassa palvelimien tiedot ja ilmoitin laskutukselle.

Viikkoanalyysi

Tämän viikon aikana tuli paljon puheluita häiriöistä, joiden parissa viikko vierähti. Mitään syvempiä tutkimisia en pystynyt suorittamaan, sillä puheluita tulee arkena sitä tahtia, että kun olen aikaisemman puhelun jälkeiset työtehtävät saanut suoritettua soikin puhelin jo uudestaan. Opin paljon langattoman verkon ongelmien ratkaisemisesta ja palomuureista.

3.3 Seurantaviikko 3

Tiistai 16.6.2020

Päivän tavoitteena oli oppia jotain uutta.

Tiketti, jossa asiakas kertoi, että eräs stream ei toimi. Olen kerran aiemmin käynyt resetoimassa vastaavanlaisen streamin, mutta en muistanut, miten se tehdään. Etsin ohjeistuksesta pitkän aikaa, mistä streamin pääsee resetoimaan. Pitkän etsinnän jälkeen löysin ohjeet streamin resetoimiseksi. Ohjeiden avulla päädyin oikealle palvelimelle, josta sain streamin resetoitua. Ilmoitin asiakkaalle, että stream on resetoitu ja laitoin tiketin kiinni.

Kahdesta palvelimesta oli tullut hälytys, että palvelimien E: levy ei vastaa. Lähetin sähköpostin asiakkaan asiantuntijoille, jotka myöhemmin vastasivat, että palvelimilla ei ole E: levyä. Ihmettelin tilannetta hetken, kunnes kysyin valvonnoista vastaavalta asiantuntijalta neuvoja. Asiantuntija kertoi, että E: levy on todellisuudessa ollut USB-tikku, joka on ollut kiinni palvelimessa. Kun USB-tikku otetaan irti palvelimesta, tästä generoituu tiketti. Asiantuntija poisti E: levyn valvonnasta ja minä suljin tiketin.

Palvelimelta tullut database error -hälytys, josta minulla ei ole mitään käsitystä. Kyselin kollegalta, onko hän nähnyt vastaavaa hälytystä aiemmin, mutta ei kuulemma ollut. Laitoin asiakkaalle viestiä, että palvelimesta on tullut tämänlainen hälytys ja kyselin, onko kyseessä vakava hälytys, ja jos palvelimella on häiriötilanne aktiivinen, tutkisivat häiriötä.

Opin käyttämään paremmin uutta tikettijärjestelmää.

Keskiviikko 17.6.2020

Päivän tavoitteena oli oppia uutta palvelimista.

Päivä alkoi CDC-asiakkaiden jonon siivouksella. Poistin turhia tikettejä ja suljin rutiininomaisia tikettejä.

Asiakas oli avannut korkeimman tason eli prioriteetin 1 tiketin. Otin tiketin itselleni ja aloin tutkimaan ongelmaa. Tiketillä asiakas kertoo, että yksi käyttäjä ei pysty yhdistämään GlobalProtectiin. Laskin tiketin prioriteettia, sillä yhden käyttäjän ongelmat eivät ole korkeimman prioriteetin häiriöitä. Asiakas oli liittänyt tiketille kuvan virheviestistä, jonka käyttäjä sai yritettyään kirjautua GlobalProtectiin. Tarkastin palomuurilta, että käyttäjä pääsee kirjautumaan GlobalProtectiin, mutta sen jälkeen tulee ongelma. Googlasin ongelmasta ja vaikutti siltä, että käyttäjällä ei ole asetettu tarvittavia AD-ryhmiä. Viestitin asiakkaalle, että tarkastavat käyttäjän AD-ryhmät ja jos ongelma ei sillä korjaannu, ovat uudestaan meihin yhteydessä.

Uudet kesätyöntekijät esittävät päivän aikana paljon kysymyksiä, joihin vastailin päivän mittaan useita kertoja.

Erään asiakkaan monen toimipisteen verkkoyhteydet lakkasivat toimimasta, jonka takia hälytaululle tuli paljon häylytyksiä näistä toimipisteistä. Otin hälytaulun auki ja autoin hälymiestä, sillä taululla oli satoja hälytyksiä. Vastasin kymmenen minuutin sisällä moneen puheluun, joissa asiakas ilmoitti näiden toimipisteiden verkkoyhteyden katkenneen.

Asentaja soitti ja kertoi, että oli asentanut toimipisteelle kaksi uutta tukiasemaa. Tarkastin, että kytkimellä on tarvittavat konfiguraatiot, jotta uudet tukiasemat toimivat. Uudet tukiasemat näkyivät jo toimipisteen WLAN kontrollerilla. Tehtäväkseni jäi nimetä tukiasemat kontrollerilla, lisätä ne kantaan ja päivittää toimipisteen verkkokuva vastaamaan nykytilannetta.

Torstai 18.6.2020

Päivän tavoitteena oli opettaa kollegalle, miten uutta tikettijärjestelmää käytetään.

Töihin tultuani huomasin vuorolistasta, että minulle oli laitettu perehdytysvuoro. Tarkoitukseni oli perehdyttää kollegalle uutta tikettijärjestelmää ja kertoa, miten siellä tikettejä käsitellään ja ratkotaan.

Linux-palvelimesta tullut tiketti erään prosessin sammumisesta. Kirjauduin palvelimelle ja tarkastin, että prosessi on sammunut. Löysin ongelmasta vanhan tiketin, jossa kollega oli huomannut, että prosessin konfiguraatiotiedosto oli tyhjentynyt jostain syystä. Huomasimme kollegan kanssa, että prosessin konfiguraatiotiedosto oli tyhjä. Samassa kansiossa, missä konfiguraatiotiedosto sijaitsi, oli myös konfiguraatio_template -tiedosto. Kopioin templaatin tyhjään konfiguraatiotiedostoon. Prosessi käynnistyi itsestään 30 minuutin välein. Odottelun jälkeen varmistimme, että prosessi lähti käyntiin ja pysyy käynnissä. Merkitsimme tutkinnat tiketille ja laitoimme tiketin kiinni.

Esimieheni delegoi meille kaksi tikettiä, joissa toimipisteiden 4G yhteys ei toimi kunnolla. Toimipisteiden 4G-liittymistä täytyi avata tiketti palvelutoimittajalle tiketti-integraation kautta. Löysin ohjeet, miten tiketti-integraatio toimii. Ohjeita seuraten saimme avattua palvelutoimittajalle tiketit molemmista toimipisteistä.

Kävin kollegan kanssa läpi, miten tikettejä ratkotaan ja miten järjestelmiin pääsee käsiksi. Muutaman esimerkkitiketin jälkeen annoin kollegan ratkaista itse tikettejä ja vastailin hänen kysymyksiinsä.

Viikkoanalyysi

Kulunut viikko oli mielestäni hyvä, sillä pääsin asettamiini tavoitteisiin. Sain ratkaistua paljon sellaisia ongelmia, mitä en ennen osannut ratkaista. Opin myös paljon uutta uudesta tikettijärjestelmästä. En ole ennen ratkaissut Linux palvelinten ongelmia, mutta nyt niitä muutaman tehneenä, voin sanoa mielenkiinon kasvaneen tätä käyttöjärjestelmää kohtaan.

3.4 Seurantaviikko 4

Maanantai 22.6.2020

Päivän tavoitteena oli oppia jotain uutta.

Tänään keskityin tekemään yhden asiakkaan tikettejä uudessa tikettijärjestelmässä. Tältä asiakkaalta tulee paljon sellaisia tikettejä, joita vanhassa tikettijärjestelmässä ei ole. Päivä kului suurelta osin ohjeistusta lukiessa, sillä tikettien otsikot, missä häiriö aina lukee, ovat täysin uudenlaisia.

Ilmoittauduin vapaaehtoiseksi huomiseen palaveriin asiakkaan kanssa, jossa pitäisi palomuurilla luoda uusi VPN-tunneli. Kyselin kollegoilta apuja, sillä en ole aiemmin tällaista tehnyt. Minulle kerrottiin, mitä pitäisi tehdä ja mistä ja minulle kirjoitettiin ohjeet, miten saan tunnelin luotua.

Tiistai 23.6.2020

Päivän tavoitteena oli oppia jotain uutta.

Yhdellä käyttäjällä oli VPN hidastellut. Koska kyse on yhden käyttäjän ongelmasta, on ongelma hyvin luultavasti muualla kuin VPN-yhteydessä. Ilmoitin asiakkaalle, että tarkastaisivat asiakkaan asetukset ja selitin esimerkkien avulla, mistä VPN-yhteyden hidastelu voi johtua.

Asiakas pyysi, että muutama palvelin pitäisi ottaa tietyksi ajaksi pois valvonnasta palvelimilla tehtävien muutostöiden takia. Tällä vältetään palvelimista mahdollisesti generoituvat turhat tiketit. Hiljensin palvelimien valvonnat pyydetyksi ajankohdaksi.

Erään palvelimen tuuletin pitää kovaa ääntä ja asiakas oli siitä huolissaan. Kysyin palvelimesta vastaavalta asiantuntijalta ja hän kertoi, että oli menossa palvelinhuoneeseen tänään ja tarkastaa siellä tuulettimen kunnon.

Liityin palaveriin, mihin eilen ilmoittauduin vapaaehtoiseksi. Kävi ilmi, että olin merkinnyt palaverin alkamiskellonajan itselleni väärin ja olin tunnin myöhässä. Asiakkaalle ei sopinut pitää palaveria enää, joten kysyin uutta aikaa. Asiakas ehdotti perjantaita ja kerroin, että se sopii hyvin. En ole perjantaina vuorossa, joten jouduin etsimään uuden henkilön tekemään muutoksen.

Päivän mittaa vastailin moniin kesätyöntekijöiden kysymyksiin. Opin myös, että Windowsissa MBR-tyyppistä levyä ei voi laajentaa yli 2 Tt:n, kuten GPT-tyyppisen levyn voi [1].

Keskiviikko 24.6.2020

Päivän tavoitteena oli oppia jotain uutta.

Yövuoron kollega antoi minulle tutkittavaksi tiketin, jossa eräs palomuuri ei vastaa valvonnassa, mutta palomuuri on muuten täysin toiminnassa. Ihmettelin ongelmaa aikani ja päätin kysyä apua kollegoilta. Selitin tutkimani ongelman ja kävi ilmi, että kollegat olivat jo tutkimassa tätä ongelmaa. Palomuurilla oli eilen tehty joku muutos, joka oli rikkonut reitityksen. Hetken päästä kollegat saivat korjattua reitityksen ja palomuuri alkoi taas vastaamaan valvonnassa.

Sain puhelun, jossa soittaja ilmoitti, että hänen toimipisteellään ei verkko toimi. Toimipisteen laitteista oli tullut hälytys hälytaululle ja epäilin, että ongelma on palveluntarjoajan päässä. Tein tiketin tästä ja kerroin soittajalle, että alan tutkimaan häiriötä välittömästi. Olin ottamassa palveluntarjoajaan yhteyttä, kun toimipisteen laitteet alkoivat vastaamaan valvonnassa. Monitoroin tilannetta hetken varmistaakseni, että ongelma ei uusiutunut.

Heti perään tuli samanlainen puhelu, että toimipisteellä ei verkko toimi. Laitteet vastasivat valvonnassa, joten soitin palveluntarjoajalle kysyäkseni lisätietoja toimipisteen yhteydestä. Toimipisteen verkkoliittymiä oli yhdistetty ja nyt uuden liittymän käyttöönottopäivä oli merkitty 30.6. Pyysin, jos liittymä voitaisiin ottaa käyttöön pikimmiten. Päivitin tiedot tiketille ja lähetin päivityksen asiakkaalle.

Yhdellä käyttäjällä oli ongelmia avata sovellus Citrixin kautta. Kirjauduin asiakkaan Citrix hallintapalvelimelle ja etsin kansion, jossa käyttäjien Citrix-profiilit sijaitsevat. Epäilen,

että ongelma oli käyttäjän Citrix-profiilissa. Citrix luo sisäänkirjautumisen yhteydessä uuden profiilin käyttäjälle, joten vanha profiili voidaan ottaa pois käytöstä lisäämällä nykyisen profiilikansion nimen perään ”_old”. Tällöin vanha profiili pystytään säilyttämään.

Palvelimen valvontarobotti oli sammunut. Kirjauduin palvelimelle ja käynnistin robotin uudestaan. Robotti kuitenkin sammui hetken päästä, kun olin sen käynnistänyt. Tarkastelin Windowsin lokeja, mutta en löytänyt sieltä syytä, miksi robotti ei pysynyt päällä. Kirjoitin tutkinnat tiketille ja delegoin tiketin valvontaroboteista vastaavalle tiimille.

Sain puhelun kolmannen osapuolen yhteistyökumppanilta, joka kertoi, että eräällä toimipisteellä tietyt päätelaitteet kadottavat verkon hetkellisesti epäsäännöllisin väliajoin. Hän pyysi tarkastamaan, jos toimipisteen tukiasemilla näkyisi häiriöitä, joka aiheuttaisi yhteyskatkoja. Suurin osa tämän laitevalmistajan tukiasemahäiriöistä johtuu tukiasemien muistivuodosta. Tutkimme muistivuotohäiriötä laitevalmistajan kanssa. En löytänyt virheitä WLAN-kontrollerilta ja aloin kyselemään lisää tietoja ongelmallisista laitteista esim. MAC-osoitteen. Soittajalla ei ollut antaa yhtään enempää tietoa ja hän kertoi, että jos ongelma jatkuu, olisivat he yhteydessä meihin uudestaan.

Asiakas soitti ja kertoi, että kahdessa hänen laitteessaan oli vikaa. Tämän asiakkuuden laitteista generoituu runsaasti tikettejä ja meninkin ensitöikseni tarkastamaan, onko näistä laitteista jo olemassa olevaa tikettiä. Löysin tiketin molemmista laitteista. Molempien laitteiden korjaustoimenpiteet oli jo aloitettu. Ilmoitin soittajalle tikettinumerot ja että laitteille on tilattu korjaus.

Viikkoanalyysi

Viikko oli opettavainen ja tavoitteisiin päästiin. Täysin uuden asiakkuuden tikettin tekeminen on alkuun hankalaa, sillä en tiedä heidän ympäristöstään mitään. Perehdyin tämän viikon aikana kahden suuremman asiakkaan verkkoympäristöihin, jotta osaisin ratkaista paremmin heidän häiriötilanteita. Ensimmäistä kertaa korjasin Citrix-ongelmia ja perehdyin syvemmin VPN-ongelmiin.

3.5 Seurantaviikko 5

Maanantai 29.6.2020

Päivän tavoitteena oli pysyä virkeänä ja tehdä paljon tikettejä.

Yöviikko alkoi sulkemalla runsaasti rutiininomaisia tikettejä.

Monet valvontarobotit olivat lakanneet vastaamasta valvonnassa. Käynnistin robottipalvelun uudestaan palvelimilla, mutta ne sammuivat aina uudestaan. Tarkastin, että palvelimien sopimus ei ollut loppunut. Kollegan kanssa tutkimme palomuurilta lokeja, mutta lokeissa ei näkynyt mitään yhteysvikaan viittaavaa. Delegoin häiriön roboteista vastaavalle tiimille.

Tiketti, jossa eräs Citrix-palvelin oli sammunut. Kirjauduin Citrixin hallintapalvelimelle, josta Citrix-palvelimien tilaa pystyy tarkastelemaan. Palvelimella avasin Citrix Studio -ohjelman, josta näin, että hälyttävä palvelin oli käynnissä.

Asiakas soitti ilmoittaakseen, että hän ei saa yhteyttä erääseen palvelimeen. En löytänyt palvelinta kannasta, ja kävikin ilmi, että palvelin ei ole meillä valvonnassa. Palvelimesta oli tehty tiketti, jossa kollega oli käynyt korjaamassa palvelimen ongelman. Ilmoitin tämän soittajalle ja toivotin hyvät päivänjatkot.

Tiistai 30.6.2020

Päivän tavoitteena oli oppia jotain uutta.

Asiakas tiedusteli, voisiko hänen palvelimensa tehoja lisätä. Kyseessä on Dellin fyysinen palvelin, joten tehojen lisääminen ei onnistu niin helposti, kuin virtuaalikoneella. Kirjauduin palvelimen iDRACiin ja huomasin, että palvelimella ei ole vapaita paikkoja muistille, kovalevyille tai prosessorille. Löysin vanhemman tiketin tästä samasta palvelimesta, jossa asiakkaalle oli ehdotettu, että palvelimesta tehtäisiin virtuaalipalvelin. Ilmoitin asiakkaalle, että vapaita paikkoja ei ole ja olisi järkevämpää, jos palvelin virtualisoitaisiin.

Otin työkseni tiketin, jossa seurataan neljän toimipisteen Checkpoint-palomuuriklusterien muistin käyttö. Seurantaa tehdään, sillä Checkpointin palomuureilla oli ollut muistivuotoongelmaa, joka oli aiheuttanut häiriötilanteita. Yhden toimipisteen aktiivisen palomuurin muistinkäyttö ylitti ennalta määritellyn rajan 80 %, jolloin palomuuri täytyi käynnistää uudelleen ja kerätä talteen muistinkäyttötiedot. Ennen palomuurin uudelleenkäynnistystä käänsin liikenteen palomuuriklusterin passiiviselle palomuurille. Kun palomuuri oli käynnistynyt uudestaan, käänsin liikenteen takaisin sille.

Asiakkaan tietokantapalvelimella oli eräs jobi epäonnistunut. Kysyin kollegalta, mistä jobien tilaa pystyy tarkastelemaan ja sainkin ohjeet. Kirjauduin palvelimelle ja käynnistin SQL Server Management Studio -ohjelman, jolla pystyy hallitsemaan SQL-

infrastruktuuria. Pienen etsimisen jälkeen löysin oikean jobin. Jobin historiatiedoista huomasin, että se oli epäonnistunut kerran ja sen jälkeen onnistunut. Jos jobi epäonnistuu kerran, ei ole syytä huolestua, mutta jos jobi ei seuraavalla kerralla onnistu, häiriötä tulisi tutkia.

Asiakas oli avannut tiketin, jossa hän pyysi avaamaan yhden kytkimen RMA-prosessin uudestaan. Tiketille oli lueteltu neljä eri asiakkaan auki olevaa tikettiä, joista yksi oli se, josta asiakas haluaa RMA:n uusia. Ilmeisesti vaihtolaite ei ollut vielä saapunut ja asiakas huolestui, että RMA-prosessia ei ole vielä käynnistetty. Kävin nämä neljä tikettiä läpi ja yritin ymmärtää, mitä tikettiä asiakas tarkoittaa. Kahdesta tiketistä löysin RMA-numeron. Molemmat RMA:t olivat tehty saman toimipisteen kytkimistä, josta asiakas tiketillä mainitsi. Toisella tiketillä asiakas kertoi, että olivat saaneet laitevalmistajalta vaihtokytkimen, mutta toisen RMA:n kytkin ei ollut vielä saapunut. Löysin sähköpostin laitevalmistajalta, jossa luki, että tämän puuttuvan vaihtokytkimen pitäisi saapua juuri tänään asiakkaalle. Merkitsin löydökset tiketille ja kysyin asiakkaalta, oliko toinenkin vaihtokytkin saapunut.

Asiakkaan kahdella ISE-palvelimella Radius oli alhaalla. Kirjauduin ISE-palvelimelle ja menin katsomaan lokeista, jos siellä näkyisi onnistuneita autentikointeja näiden radius-palvelimien kautta. Onnistuneita autentikointeja näkyi, eli kyseessä oli ollut hetkellinen häiriötilanne. Merkitsin tutkinnat tiketille ja laitoin tiketin kiinni.

Keskiviikko 1.7.2020

Päivän tavoitteena oli oppia ratkaisemaan tiketti, jota en ennen osannut ratkaista.

Palvelimella valvontrobotti oli sammunut. Yhdellä palvelimella on yleensä kaksi nimeä; yksi talon antama ja asiakkaan oma. En löydä palvelinta asiakkaan palvelinnimellä kannasta, joka aiheutti hieman hämmennystä. Löysin palvelimen nimellä keskitetystä palvelinmonitorointipalvelusta palvelimen IP-osoitteen. IP-osoitteen avulla löysin IPAM:sta meidän nimen tälle palvelimelle. Pystyin päättelemään palvelimen nimestä, että kyseessä on meidän oma labrapalvelin. Hälytys oli kuittaantunut tutkinnan aikana eli häiriötilanne oli poistunut. Merkitsin tutkinnat tiketille ja suljin tiketin.

Asiakkaan Oracle-palvelimelta on tullut hälytys deadlockista. Yritin kirjautua palvelimelle tuloksetta. Kaivoin ohjeistuksen auki ja huomasin, että asiakkaan palvelimiin pääsee kiinni hyppypalvelimen kautta. Kirjauduin hyppypalvelimelle, josta pääsin onnistuneesti kirjautumaan palvelimelle. Oracle-palvelimilla on skripti, jolla pystyy tarkastamaan, onko palvelimella aktiivista deadlockia. Tällä kertaa skripti valitti virhettä rivillä 1, mitä en ennen

ollut nähnyt. Vertasin skriptiä ohjeistuksessa olevaan skriptiin ja huomasin niiden olevan erilaiset. Tein uuden skriptin ohjeissa olevan skriptin mukaiseksi, mutta se toimi vielä huonommin. Kirjoitin tekemisten tulokset tiketille ja laitoin tiketin databasetiimin jonoon jatkotutkintoja varten.

Suljin tikettejä, jotka olivat pidemmän aikaa odottaneet asiakkaan vastausta. Edistin monia tikettejä, joissa asiakkaalta piti tiedustella lisätietoja sähköpostitse.

Torstai 2.7.2020

Päivän tavoitteena oli oppia uutta.

Vastasin puheluun, jossa asiakas heti alkoi selittämään ongelmatilannetta, joka heillä oli päällä. Yhtäkkiä toinen ihminen alkoi selittämään samaa ongelmaa syvemmin, jolloin tajusin, että minut oli lisätty tämän ongelman tutkimista varten luotuun palaveriin. Eräällä toimipisteellä verkko ei toimi kunnolla, koska yksi verkko ei mainostu toimipisteelle. En ollut hirveästi verkko-ongelmia tutkinut, joten kysyin apua kollegoilta. Kollega nopeasti tutki asiaa kanssani ja totesimme, että palveluntarjoaja ei mainosta tätä puuttuvaa verkkoa, vaikka sen pitäisi. Ilmoitin asiakkaalle, että loin ongelmasta tiketin meille ja päivitämme heille lisätietoja sen kautta. Avasin palveluntarjoajalle tiketin, jotta verkko saataisiin mainostumaan. Asiakas soitteli parin tunnin sisään kolme kertaa ja pyysi, että ongelmaa tutkittaisiin korkeammalla prioriteetilla. Ilmoitin asiakkaalle joka kerta, että ongelma oli palveluntarjoajalla tutkinnassa eikä sitä voisi tämän enempää nopeuttaa.

Otin työn alle tiketin, jossa asiakas pyytää uuden CNAME-tietueen. Kirjauduin IPAM:in ja etsin asiakkaan DNS:tä oikean A-tietueen, jonne loin halutun CNAME-tietueen.

Asiakkaan SSLVPN-laitteesta tehty tiketti, jossa eräs LDAP-palvelin ei vastannut. En tiedä yhtään, miten tämä pitäisi ratkaista, joten menin asiakkaan ohjeistuksesta lukemaan heidän SSLVPN-palvelustansa. Löysin osoitteen, jolla pääsin selaimella kirjautumaan tälle laitteelle. Sivustolla pystyi testaamaan, onko LDAP-palvelin tavoitettavissa. Hälyttävä palvelin ei vastannut vielä, joten monitoroin tilannetta hetken, jos se alkaisikin vastaamaan. Palvelin ei alkanut vastaamaan, joten lähetin asiakkaalle sähköpostia, jotta he tarkastaisivat palvelimen tilan.

Viikkoanalyysi

Tavoitteisiin päästiin helposti, sillä vastasin koko yövuoron aikana vain muutamaan puheluun ja sain tehtyä monia tikettejä ja palvelupyyntöjä. Viikon aikana ratkaisin todella

paljon sellaisia tikettejä, joita en ennen osannut ratkaista. Lähes jokaisen tiketin myötä tuli opittua uutta jostain teknologiasta tai järjestelmästä.

3.6 Seurantaviikko 6

Perjantai 10.7.2020

Päivän tavoitteena oli selvitä yöstä.

Tänä yönä pääsin toimimaan hälymiehenä. Puheluja ja hälytyksiä tuli niin vähän, että minulla oli aikaa etsiä tikettijonoista tikettejä, joita pystyin sulkemaan heti. Hiljaisina hetkinä edistin tikettejä, jotka eivät vaatineet laajaa tutkintaa.

Sain puhelun, jossa soittaja kertoi, että hän ei pääse kirjautumaan palvelimelle. Kollega tutki tilannetta ja huomasi, että palvelimen hostin datastore on täynnä. Jostain syystä palvelinta ei voitu siirtää toiselle datastorelle, joten soitin CDC-päivystäjälle. Päivystäjä teki taikojaan ja häiriötilanne poistui.

Tiketti, jossa asiakas kertoi, että heillä oli mahdollisia palomuurausongelmia, sillä yksi tulostin ei toiminut. Asiakas oli antanut ongelmatulostimen ja yhden toimivan tulostimen IP-osoitteen. Toimipisteellä on Checkpointin palomuurit, joiden lokeja pääsee Checkpointin omasta keskistetystä hallintaportaalista, SmartConsolesta, lukemaan. Lokeista näin, että käyttäjiltä kulki liikennettä tulostuspalvelimelle, tulostuspalvelimelta kulki liikennettä tulostimille ja tulostimien IP-osoitteisiin kulki liikennettä. Molemmat tulostimet olivat samassa aliverkossa, joten ne saivat samat muuraussäännöt. Lähetin asiakkaalle tutkinnan tulokset ja kysyin, oliko tulostuspalvelimella kaikki hyvin ja oliko tulostin konfiguroitu oikein.

Asiakkaan Oracle-palvelimen osiosta tiketti, jossa osion tila on loppumassa. Osio täyttyi erään sovelluksen vanhoista lokeista. Oli viikonloppu, jolloin talon Oracle-asiantuntijat olivat viikonlopun vietossa, joten delegoin tiketin kolmannelle osapuolelle tutkintaa varten. Kolmannen osapuolen asiantuntija laittoi sähköpostia, että hän ei päässyt kirjautumaan palvelimelle. Aloin ihmettelemään kollegojen kanssa, mistä tämä voisi johtua. Hetken päästä asiantuntija ilmoitti, että hän oli vaihtanut selainta ja pääsi kirjautumaan palvelimelle. Levyllä, jolla osio sijaitsi, tuli I/O-virhettä, joten delegoin ongelman CDC-päivystäjälle.

Lauantai 11.7.2020

Päivän tavoitteena oli oppia jotain uutta.

Toimin tänään taas hälymiehenä ja luultavasti tulen toimimaan koko viikon. Vuoron alkuun suljin rutiininomaisia tikettejä, jotka eivät vaatineet erityisempiä toimenpiteitä.

Lisäsin Windows-palvelimen levylle tilaa. Tämän palvelimen laajennuksen pystyi suorittamaan vCenteristä. Kirjauduin palvelimelle ja avasin disk managementin, jonka kautta löysin laajennettavan levyn SCSi-numeron, etten vahingossa laajentaisi väärää levyä. Etsin palvelimen vCenteristä ja lisäsin laajennettavalle levylle asiakkaan haluaman määrän tilaa. VCenter lisäsi levylle allokoimatonta tilaa, jonka kävin disk managementin kautta allokoimassa levylle.

Palvelimelta oli tullut outo tiketti, jonka otin työn alle. Otsikossa luki, että palvelimen yhdeltä levyltä oli tullut virhettä. Avasin palvelimen tapahtumienvalvonnan, jossa navigoin tieni järjestelmälokiosioon. Tiketin otsikon mukaista hälytystä oli tullut sekunnin sisään muutaman kerran siihen aikaan, kun levy oli alkanut hälyttämään. Laitoin tiketin kiinni pitkällä sulkeutumisajalla sen varalta, että virhettä tulisi lisää.

Yö oli todella rauhallinen hälytysten osalta.

Sunnuntai 12.7.2020

Päivän tavoitteena oli pysyä virkeänä.

Toimin tämänkin yön hälymiehenä.

Asiakas pyysi tekemään ajastetun tietoturvapäivityksen ja hiljentämään päivitettävien palvelimien valvonnat päivitysten ajaksi. Jouduin aluksi luomaan tunnukset järjestelmään, josta tietoturvapäivityksen sai ajastettua. Valitsin oikeat palvelimet ja ajastin päivityksen halutulle ajalle. Tämän jälkeen loin ajastetun valvontojenhiljennyksen kaikille päivitettäville palvelimille.

Erään palvelimen prosessorin hälytysrajaa täytyi muuttaa. Valvontoja voi muuttaa helposti keskitetystä valvontajärjestelmästä. Kirjauduin järjestelmään ja etsin palvelimen. Muutin prosessorin hälytysrajaa haluttuun arvoon ja suljin tiketin.

Asiakas soitti ja kertoi, että hänen toimipisteellään oli muutama tukiasema, joiden kaiutusalueella ei verkko toimi. Soittaja kertoi epäilevänsä, että kaiutusalueen kattavissa

tukiasemissa olisi jotain vikaa. Kirjauduin toimipisteen WLAN-kontrollerille ja käynnistin soittajan ilmoittamat tukiasemat uudestaan. Varmistin soittajan kanssa tukiasemien käynnistyttyä, että ne kaiuttavat verkkoa. Tämä häiriö johtui myös muistivuodosta, joka korjaantuu käynnistämällä tukiasema uusiksi.

Viikkoanalyysi

Hälymiehenä oli vaikempi oppia uutta, sillä hälytaulun parissa työskennellessä ei kerkeä tikettejä ratkomaan. Taulu oli kuitenkin tarpeeksi hiljainen ajoittain, jonka ansioista kerkesin työstämään tikettejä ja palvelupyyntöjä. Tämä oli seuranta-ajan ensimmäinen viikko kun tavoitteisiin ei aivan päästy.

3.7 Seurantaviikko 7

Perjantai 17.7.2020

Päivän tavoitteena oli ratkaista uusi tiketti.

Asiakas pyysi palauttamaan tiedostokansiosta tiedoston, jonka hän oli vahingossa poistanut. Tiedustelin asiakkaalta tiedoston sijaintia, sillä sitä ei ollut tiketillä ilmoitettu. Löysin heti perään toisen samanlaisen tiedostonpalautustiketin, jossa kansion osoite oli ilmoitettu. Asiakkaan hyppykoneelta avasin resurssienhallinnan ja liitin kansion osoitteen resurssienhallinnan osoiteriviin, jonka jälkeen löysin kansion, josta tiedosto piti palauttaa. Asiakas ei ollut ilmoittanut palautettavan tiedoston nimeä tai versiota, joten kysyin sitä. Kun asiakas oli vastannut, kopioin halutun tiedoston ja liitin sen asiakkaan nykyiseen kansioon.

Tiketti, jossa asiakas kertoi, että kun hän käynnistää tietokoneen, selain ja tietty sivu aukesi. Aloitin tutkinnan etsimällä käyttäjän tunnuksen. Epäilin, että käyttäjä kuului sellaiseen AD-ryhmään, jossa oli GPO, joka aukaisee selaimen ja tämän sivun tietokoneen auettua. Löysin GPM:stä ryhmän, jolla on GPO, joka aukaisi selaimen, mutta avattava sivu ei ollut sama, kuin tällä käyttäjällä. Konsultoin asiantuntijoilta tästä ja heidän mielestään ongelma oli myös AD:ssa, joten pyysin asiakasta tarkastamaan käyttäjän AD-ryhmät.

Asiakas oli pyytänyt yhdelle työntekijälle admin-oikeudet eräälle palvelimelle. Pyytäjällä ei ollut oikeuksia pyytää muutosta, joten pyysin asiakkaan muutoskontaktilta luvitusta

oikeuksien lisäykselle. Muutoskontakti oli käynyt itse lisäämässä työntekijälle oikeudet palvelimelle, joten suljin tiketin.

Lauantai 18.7.2020

Päivän tavoitteena oli oppia jotain uutta.

Toimin tänään taas hälymiehenä.

Asiakkaan SD soitti, että heillä oli DDoS päällä ja että hän oli juuri laittanut sähköpostia tästä. Löysin sähköpostin ja tein siitä tiketin. Kirjauduin SmartConsoleen ja menin tarkastelemaan kohdemuurilta, minkälaista liikennettä siellä näkyy. Hyökkäys oli tullut Afrikassa sijaitsevista IP-osoitteista. Asiakas oli pyytänyt estämään kaikki nämä osoitteet, joita oli yhteensä satoja. Lokeista huomasin, että hyökkäys oli loppunut ennen kuin SD oli ongelmasta meille ilmoittanut. SD:llä ei ollut oikeuksia pyytää muutosta, joten ilmoitin SD:lle, että tarvitsemme muutoskontaktilta luvituksen tähän muutokseen.

Oracle-palvelimelta oli tullut tiketti, joka kertoi, että palvelimen arkistoloki oli liian vanha. Tämä voi tarkoittaa sitä, että varmistus ei toimi kunnolla. Hälytys generoitui siitä, kun kuukausittaisessa varmistuksen ottamisessa oli mennyt liian kauan ja järjestelmä ei ollut poistanut vanhoja varmistuslokeja. Tiketin varmistuksen ottamisessa oli kestänyt liian kauan, joten delegoin ohjeiden mukaisesti tiketin tietokanta-asiantuntijoille.

Asiakkaan Palo Alto palomuurilla oli BGP-peeraus katkennut. Kirjauduin asiakkaan Panoramaan ja valitsin oikean palomuurin, jonka järjestelmälokeista pystyin haarukoimaan BGP-lokit. Lokit näyttivät, että peering yhteys oli muodostunut, eli häiriötilanne oli poistunut. Merkitsin tutkinnat tiketille ja suljin sen.

Meidän tikettijärjestelmämme lakkasi toimimasta. En ollut ennen tätä ongelmaa korjannut, joten aloin selvittämään, miten ongelman saisi ratkaistua. Kirjauduin palvelimelle, jossa tikettijärjestelmä pyörii. Ohjeiden mukaan ongelma ratkeaa sammuttamalla oikea prosessi, jolloin prosessi käynnistyy itse uudestaan. Löysin oikean prosessin ja sammutin sen. Prosessi käynnistyi lähes heti itsestään ja tikettijärjestelmä alkoi taas toimimaan.

Sunnuntai 19.7.2020

Päivän tavoitteena oli oppia jotain uutta.

Sain kunnian toimia tänäänkin hälymiehenä.

Yhden palvelimen taulutila hälytti vähästä tilasta. Tein tiketin tästä ja kollega otti sen työn alle. Hän huomasi, että tietokannassa oli muitakin taulutiloja, joissa oli tila loppumassa. Tarkastin, että näistä muista taulutiloista ei ollut aiempia tikettejä. Tikettejä etsiessäni huomasin, että yhden toisen palvelimen osio hälytti vieläkin valvonnassa. Hälytyksestä löysin tiketin, jolla häiriötä oli tutkittu. Tiketille oli merkitty, että tästä ei tarvitse välittää ja valvonnat oli poistettu. Koska hälytys oli vieläkin aktiivinen, päättelin, että valvontojen poisto oli mennyt pieleen. Keskitetystä valvontajärjestelmästä huomasin, että valvonnat oli poistettu väärin, joten korjasin tilanteen ja poistin valvonnat oikein.

Asiakkaan SSL VPN täytyi käynnistää uudelleen. Muutoskalenteriin oli laitettu hyvät ohjeet, miten tämän saa tehtyä. Kirjauduin SSL VPN:lle ja laitoin järjestelmän käynnistymään uudelleen. Kun uudelleenkäynnistys oli valmis, kirjauduin laitteelle ja varmistin palvelun toiminnallisuuden.

Kytkinportti fläppäili eli portti sammui ja meni takaisin päälle jatkuvasti. Avasin toimipisteen verkkokuvan, josta huomasin, että portin takana oli tukiasema. Tukiasema sai virran kytkinportin kautta. Monesti fläppäilevän tukiasemaportin saa korjattua sillä, että kytkinportin virransyöttö katkaistaan hetkeksi ja laitetaan takaisin päälle. Katkaisin portin virransyötön ja laitoin sen takaisin päälle. Hetken monitoroinnin jälkeen huomasin, että häiriötilanne oli poistunut.

Viikkoanalyysi

Sain opittua yllättävän paljon, vaikka toimin hälymiehenä osan viikosta. Paljon tuli kaikkea pientä opittua. AD-ongelmien tutkiminen oli täysin uutta. Sain kollegoilta ja asiantuntijoilta paljon neuvoja, miten AD toimii ja miten siellä olevia häiriöitä pystyy tutkimaan. Palomuurien hallintasovellukset käyvät tutummaksi päivä päivältä, sillä olen alkanut tutkimaan yhteysongelmahäiriöitä entistä enemmän.

3.8 Seurantaviikko 8

Tiistai 21.7.2020

Päivän tavoitteena oli oppia jotain uutta.

Asentaja soitti toimipisteeltä eräästä muutostiketistä, jossa toimipisteen kytkimen kaksi porttia piti liittää tiettyyn VLANin. Muutostiketillä oltiin konfiguroitu monia asiakkaan eri toimipisteiden kytkinportteja. Tarkastin, että kytkimen konfiguraatio näytti oikealta, jotta

pystyin porttimuutoksen suorittamaan onnistuneesti. Konfiguroin portit oikeaan VLANin ja ilmoitin asentajalle, että työ oli tehty. Merkitsin tiketille muutostyöhön kuluneen ajan ja tekemäni porttikonfiguraatiot.

Sain käsiteltäväkseni tiketin eräästä palvelimen palvelusta, joka ei vastannut valvonnassa. Palvelimella huomasin, että siellä ei ole kyseistä palvelua. Kyselin sähköpostitse asiakkaalta, oliko palvelu tarkoituksella poistettu.

Esimies pyysi minua ottamaan työn alle tiketin, jolla tutkittiin erään toimipisteen verkkoongelmaa. Toimipisteellä oli SD WAN -toteutus, jossa pääyhteytenä oli MPLS ja varayhteytenä oli 4G-liittymä. Ongelmana oli, että tällä hetkellä kaikki liikenne kulki varaliittymän kautta. SD WAN-reitittimellä ei näkynyt verkkoliikennettä portissa, mistä MPLS-yhteyden pitäisi tulla. Avasin palveluntarjoajalle tiketin, jotta he tarkastaisivat, oliko MPLS-liittymän reititys kunnossa.

Keskiviikko 22.7.2020

Päivän tavoitteena oli oppia jotain uutta.

Yksi prosessi ei vastaa palvelimella. Tarkastin palvelimelta, että prosessi oli käynnissä, eli hälytys oli false positive. Laitoin monitorointitiimille viestiä, jotta he tarkastaisivat palvelimen valvonnat.

Tiketti vCenteristä, jossa eräällä hostilla hälytti jokin laiteobjekti. VCenteristä huomasin, että hostilla ei ollut yhtään aktiivista hälytystä ja kaikkien laiteobjektien kunto näytti vihreää. Olin menossa kirjoittamaan tutkinnat tiketille, mutta tiketti oli jo itsestään sulkeutunut.

Opettelin tänään komentoja, joilla Windowsin PowerShellin kautta saisi haettua palvelimesta tietoja, esim. top 5 eniten muistia käyttävää prosessia ja sen, kuinka paljon tehoa jokainen prosessoriydin käytti.

Asiakas pyysi käyttäjälle uuden RSA-tokenin aktivointilinkin. Löysin ohjeistuksesta täydelliset ohjeet, miten linkin sai lähetettyä. Vanha token oli vielä voimassa, joten uutta ei tarvinnut tehdä. Ensiksi etsin RSA Security Consolesta käyttäjän, jolle token piti lähettää. Monien klikkailujen jälkeen sain aktivointilinkin, jonka lähetin asiakkaalle, joka lähetti sen käyttäjälle.

Viikkoanalyysi

En koe, että olisin päässyt viikkotavoitteisiin. Kesälomakausi oli parhaimmillaan, joten puheluita tai tikettejä tuli paljon vähemmän, kuin yleensä. Kulunut viikko oli erittäin rauhallinen. Vaikka opin uutta, aiempiin viikkoihin verrattuna opittua oli paljon vähemmän. En ollut ennen käyttänyt PowerShell-komentoja. Niiden avulla nopeutan ja helpotan omaa työtäni.

3.9 Seurantaviikko 9

Maanantai 27.7.2020

Päivän tavoitteena oli oppia jotain uutta.

Huomasin tiketin, jossa eräs host oli kaatunut. Tämän hostin ympäristössä oli monia virtuaalikoneita. Hostin kaatuminen on huono asia, sillä vaikka kaikki hostilla olevat virtuaalikoneet siirtyisivät toiselle hostille, ne sammuvat ennen siirtymistä. Sillä on pahimmassa tapauksessa suora vaikutus asiakkaiden, kenen virtuaalikoneita hostilla on, tuotantoon. Huomasin Teamsissa viestin, jossa asiantuntija kertoi tekevänsä päivityksiä hostille eli häiriötilannetta ei ole.

Asiakkaan Linux-palvelimella osio oli täyttymässä. Lähetin palvelimesta vastaavalle asiakkaan yhteyshenkilölle sähköpostin, mutta sain heti vastausviestin, jossa henkilö ilmoitti olevansa vielä kuukauden lomalla. Osion täyttyminen ei välttämättä näy asiakkaalle mitenkään, mutta se voi pahimmassa tapauksessa pysäyttää koko palvelimen toiminnan. Lähetin sähköpostia asiakkuuden myyntipäällikölle ja tekniselle päällikölle, jos he tietäisivät korvaavan henkilön lomailevalle yhteyshenkilölle.

Vastaanotin puhelun, jossa asiakas kertoi, että hänen eräs VPN-tunneli oli alhaalla. Kerroin asiakkaalle tekeväni häiriöstä tiketin ja tutkivani asiaa. Asiakkaan palomuurilta tarkastin, että tunneli oli alhaalla. Käynnistin tunnelin avaintenvaihtoprotokollan vaiheen kaksi uudestaan, jonka jälkeen tunnelin tila muuttui aktiiviseksi. Varmistin vielä asiakkaalta, että tunneli toimii.

Palvelimelta oli tullut hälytys, jossa Citrix broker servicen ja tietokannan välinen yhteys oli katkennut. Citrix XML broker [2] toimii Citrix-palvelinfarmin ja www-käyttäjäliittymän välikätenä. Esim. kun käyttäjä kirjautuu Citrixillä applikaatioon, kirjautumistiedot menevät XML brokerille, joka välittää ne tietokantaan, jossa tiedot autentikoidaan. Palvelimen

tapahtumienhallinnasta näin, että yhteys oli katkeamisen jälkeen palautunut viiden sekunnin kuluttua takaisin.

Sain puhelun asiakkaan help deskiltä, joka ilmoitti, että eräällä toimipisteellä ei verkko toimi. Hälymies kertoi, että toimipisteeltä ei ollut tullut yhtäkään hälytystä. Tarkastin, että kaikki toimipisteen verkkolaitteet vastasivat valvonnassa ja ettei toimipisteestä ollut auki olevia tikettejä. Kysyin soittajalta tarkentavia tietoja häiriöstä, mutta hänellä ei niitä ollut antaa. Tulimme soittajan kanssa siihen lopputulokseen, että hän on yhteydessä häiriön ilmoittajaan ja jos häiriötilanne on aktiivinen, lähettää hän meille sähköpostilla tarkan viankuvauksen.

Eräällä toimipisteellä langaton verkko ei toiminut tietyssä kohtaa taloa. Etsin toimipisteen verkkokuvasta tukiaseman, jonka katvealueella verkko ei toiminut. Tukiasemalta huomasin, että siihen yhdistyneet laitteet eivät päässeet liittymään mihinkään WLAN-verkkoon. Tukiaseman uudelleenkäynnistyksen jälkeen havaitsin, että siihen liittyneet päätelaitteet pääsivät nyt eri WLAN-verkkoihin. Tein händerin päivävuorolle, jotta asiakkaalta varmistettaisiin, oliko häiriötilanne yhä aktiivinen.

Tiistai 28.7.2020

Päivän tavoitteena oli pysyä hereillä.

Otin työn alle tiketin, jossa asiakas kertoi samanlaisesta WLAN-ongelmasta, jota jo eilen tutkin. WLAN-kontrollerilta tarkastin asiakkaan ilmoittamien virheilevien tukiasemien tilan, mutta en löytänyt mitään virheitä tai häiriöitä. Tämän WLAN-verkon ongelmat toistuvat monilla toimipisteillä ja joskus ne olivat hetkellisiä häiriötilanteita, jotka korjaantuvat itsestään. Lähetin asiakkaalle tiivistelmän tutkinnan tuloksista ja kysyin, oliko häiriötilanne vielä aktiivinen.

Sain händerin, jossa piti tehdä failover SQL-palvelimelta toiselle. SQL-palvelin 1 oli käynnistynyt uudelleen, jolloin aktiivisuus oli kääntynyt SQL palvelin 2:lle. Eräs jobi epäonnistuu jatkuvasti, joten aktiivisuus täytyi siirtää takaisin palvelimelle 1. Olin menossa suorittamaan failoveria, kun huomasin, että palvelin 1 oli jo aktiivinen. Historiatiedoista näin, että palvelin 2 oli käynnistynyt kolme tuntia sitten uudestaan ja aktiivisuus oli kääntynyt takaisin palvelin 1:lle. Jobi ajettiin kaksi kertaa päivässä, kello 7 ja 23. Pyysin aamulla kollegaa, joka antoi minulle tämän händerin, tarkastamaan, että jobi oli onnistunut.

Asiakas kertoi, että PDF:n tulostus SAP:sta ei onnistu ja hän epäili Cortex XDR:n estävän tulostuksen. Minulla tai yhdelläkään vuorossa olevalla kollegalla ei ole aiempaa

kokemusta Cortexista ja ohjeistuksesta siitä ei ollut. Kysyin tietoturvapuolen yövuorolaiselta apua. Hän ei nähnyt mitään tulostukseen viittaavaa ongelmaa Cortexissa. Tein händerin aamuvuorolle, jotta häiriöstä voitaisiin kysyä asiantuntijoilta.

Asiakkaalla oli jaetun tunneloinnin tunneli alhaalla. Tiketillä ei ollut mainittu, minkä palomuurin kautta tunneli meni. Löysin Panoramasta pienen etsinnän jälkeen oikean palomuurin. Palomuurilta näin, että tunneli oli ylhäällä. Palomuurin CLI:ltä näin, että tunnelin läpi meni paketteja koko ajan. Merkitsin tiketille tutkinnat ja suljin tiketin. Epäilin, että palveluntarjoajalla oli ollut hetkellinen häiriö, koska tunneli oli vain hetken tavoittamattomissa.

Keskiviikko 29.7.2020

Päivän tavoitteena oli oppia jotain uutta.

Sain eilisen Cortex-tiketin takaisin. Kollega oli kysellyt asiantuntijoilta neuvoja, mutta kukaan ei osannut kertoa, miksi tulostus ei toiminut. Loin Palo Altolle TAC-tiketin ja ilmoitin asiakkaalle, että häiriö oli laitevalmistajalla tutkinnassa.

Tiketti, jossa asiakkaan DHCP-palvelu oli sammunut. En tiedä, mistä DHCP-palvelun tilan näkee, joten otin ohjeistuksen auki ja aloin etsimään, mistä DHCP-palvelun tilan pystyy tarkastamaan. Hetken pähkäilyn jälkeen tajusin, että IPAM:sta näki esim. DNS-palveluiden tilan, joten DHCP:n pitäisi olla siellä myös. IPAMista näin, että asiakkaan DHCP-palvelu on päällä.

Erään toimipisteen operaattorireititin ei vastannut valvonnassa, mutta kaikki muut verkkolaitteet vastasivat. Valvomme operaattorireitittimillä yleensä reitittimen loopback-osoitetta. Epäilen, että toimipisteellä oli palveluntarjoajan puolella tapahtunut muutos, jonka takia loopback-osoite oli vaihtunut. Kirjauduin yhdelle toimipisteen kytkimistä ja sen ARP-taulusta sain operaattorireitittimen IP-osoitteen. IP-osoite oli eri, kuin kannassa, mutta osoite vastasi ICMP-kyselyyn. Tarkastin IP-osoitteen skriptillä, joka kertoi osoitteesta tietoja mm. palveluntarjoajan ja liittymän tunnuksen. Skriptin tuloste kertoi, että kyseessä oli sama reititin, kuin meillä kannassa oli. Toimipisteellä oli luultavasti tapahtunut liittymän nopeuden korotus ja IP-osoite oli tästä syystä vaihtunut. Päivitin uuden IP-osoitteen kantaan ja suljin tiketin.

Otin työn alle tiketin operaattorireitittimestä, joka ei vastannut valvonnassa. Huomasin samalla, että toimipisteen muutkaan verkkolaitteet eivät vastanneet. Verkkolaitteiden palvelutasosta näin, että niitä ei oltu vielä otettu käyttöön. Löysin toimipisteeseen liittyvän

muutostiketin laitteiden käyttöönotosta. Tiketillä oli merkintä, että käyttöönottoa ei ollut vielä tehty. Lähetin sähköpostin asiakkaalle, jossa tiedustelin ajankohtaa, jolloin laitteet otetaan käyttöön.

Torstai 30.7.2020

Päivän tavoitteena oli oppia jotain uutta ja pysyä hereillä.

Löysin aikaisemmin tutkimani Cortex-tiketin. TAC kertoi, että jos Acrobat Readerissa oli suojaustila päällä, Cortex XDR estää SAPista tulostamisen. Välitin asiakkaalle TAC:n viestin ja heidän suosittelemat toimenpiteet.

Edistin kymmeniä tikettejä, joissa asiakkaalta piti tiedustella lisätietoja häiriön ratkaisemista varten.

Sain kollegalta händerin, jossa eräs palvelin piti käynnistää uudestaan. Palvelimen valvontarobotti ei oli päällä. Kollega oli yrittänyt käydä käynnistämässä robotin uudestaan, mutta palvelin kävi niin hitaalla, että edes task manageria ei saanut auki. Asiakkaalta oli pyydetty lupa käynnistää palvelin uudestaan. Käynnistin palvelimen uudestaan ja aloin etsimään juurisyytä palvelimen hitaudelle. Järjestelmälokeissa oli runsaasti virheitä muistin loppumisesta. Keskitetystä palvelimienvalvontajärjestelmästä näin, että palvelimen muistin käyttö oli ollut 98–99 %. Valvontarobotti ei toiminut kunnolla korkean muistin käytön takia. Lähetin asiakkaalle tiedot tutkinnasta ja suljin tiketin.

Asiakkaan Oracle-palvelimella osio oli täyttymässä ja sieltä piti poistaa trace-tiedostoja. Sain kollegalta hyvät ohjeet, miten tracetiedostoja sai poistettua. Palvelimella tarkastin, kuinka paljon minkäkin instanssin trace-tiedostot veivät tilaa. Poistin kolmesta eniten tilaa vievästä instanssista tracetiedostot, joka vapautti 30 % lisää tilaa osiolle.

Löysin tiketin reitittimestä, jonka portti oli mennyt alas. Toimipisteen verkkokuvaan ei ollut merkitty laitetta, joka oli yhdistetty tähän porttiin. Tiketillä ei lukenut, mikä portti oli mennyt alas, joten tarkastin reitittimen lokeista, mistä portista hälytys oli generoitunut. Löysin oikean portin, mutta en vieläkään tiennyt, mikä laite portin takana oli. Tarkastin CDP:llä viereisten porttien laitteet. Viereisessä portissa olleen laitteen MAC-osoite indikoi, että kyseessä olisi Canonin laite, eli mitä luultavimmin tulostin. Viereinen portti oli myös samassa VLANssa, kuin alhaalle mennyt portti. Löysin identtisen tiketin toiselta toimipisteeltä ja sen toimipisteen verkkokuvan mukaan saman portin takana oli tulostin. Merkitsin tutkinnat tiketille ja kysyin asiakkaalta, oliko portin takana oleva laite tarkoituksella sammutettu.

Viikkoanalyysi

Pääsin viikon tavoitteisiin jälleen kerran. Tämän yöviikon aikana kerkesin tutkimaan monia ongelmia. Opin ratkaisemaan Palo Alton häiriöitä enemmän ja viikon aikana ratkaisin enemmän verkko-ongelmia, mitä yleensä. Eniten kehitystä tapahtui verkko-ongelmien ratkaisussa.

3.10 Seurantaviikko 10

Perjantai 7.8.2020

Päivän tavoitteena oli ratkaista ongelma, mitä en ennen osannut ratkaista.

Olin tänään vuoron ainoa palvelinosaaja. Huomasin vuoron aikana myös, että olen ainoa, joka osasi käyttää uutta tikettijärjestelmää.

Asiakkaalta oli tullut vastaus Cortex-tiketille. Hän oli konfiguroinut GPO:hon asetuksen, joka kytkee Acrobat Readerin suojaustilan pois päältä, niin kuin TAC suositteli. Asiakas kertoi, että häiriötilanne oli ratkennut tällä korjauksella ja tiketti voitiin sulkea.

Asiakas pyysi ottamaan kolmesta heidän virtuaalikoneestaan snapshotin ennen kuin hän suoritti päivityksiä palvelimille. Otin snapshotit ja pyysin asiakasta ilmoittamaan, kun snapshotit voidaan poistaa.

Minun työkannettavan webbikamera ei toimi. Asensin kameran ajurit uudestaan ja yritin tuloksetta selvittää, miksi kamera ei toimi. Lähetin IT-tukeen viestin ongelmasta ja kuvasin lyhyesti, mitä olin tehnyt ongelman selvittämiseksi.

Asiakas kertoi, että heidän toimipisteellään oli tulostin, joka ei tulosta, kun tulostin oli langattomassa verkossa. Aloitin tutkinnan etsimällä asiakkaan ohjeistuksesta linkkejä asiakkaan järjestelmiin. Ohjeistuksessa ei oikeastaan ollut kirjotettu asiakkaan WLAN:sta mitään, joten aloin epäilemään, kuuluiko asiakkaan WLAN-ylläpito meille. Kysyin asiakkuuden myyntipäälliköltä sähköpostilla, kuuluivatko WLAN-palvelut asiakkaan sopimukseen. Lähetin myös asiakkaalle lisätietopyynnön, sillä tiketillä ei ollut mitään teknisiä tietoja annettu.

Yhdellä käyttäjällä Cortex XDR esti erään applikaation käynnistämisen. Kirjauduin Cortexiin ja huomasin siellä hälytykset, mitä oli generoitunut joka kerta, kun asiakas oli yrittänyt käynnistää applikaation. En osannut sanoa, kuuluiko sovelluksen olla estetty.

Lähetin asiakkaan yhteyshenkilölle viestin, jossa kysyin, kuuluiko applikaatio olla estettyjen listalla vai voitiinko se sallia.

Lauantai 8.8.2020

Päivän tavoitteena oli oppia jotain uutta.

Tiketti, jossa palvelimella oli levy täyttymässä. Tämänlaiset tiketit kuuluvat rutiininomaisiin tiketteihin, koska yleensä ne ovat helppoja ja nopeita ratkaista. Tiketin palvelin oli Exchange-palvelin, jonka ylläpito kuului täysin meidän vastuulle. Huomasin, että levyn pitäisi tyhjentää itseään automaattisesti viikon välein, mutta nyt levy oli kolme viikkoa putkeen jatkanut täyttymistään. Juurisyy saattoi olla, että palvelimella ei varmistukset toimineet kunnolla, jolloin transaction lokeja ei poistettu. Ohjeistus kertoi, että palvelu oli erittäin kriittinen asiakkaan liiketoiminnan kannalta, joten soitin konesalipäivystäjälle ja kerroin ongelmasta. Lähetin tikettinumeron päivystäjälle ja hän jatkoi häiriön tutkintaa.

Suljin muita rutiininomaisia tikettejä, kun vastaan sattui tiketti palvelimen korkeasta muistin käytöstä. Palvelimen muistin käyttö laski historiatietojen mukaan joka sunnuntai kello 18. Selasin palvelimesta luotuja tikettejä ja yhdeltä aikaisemmalta tiketiltä löysin syyn säännölliselle tyhjenemiselle. Palvelimella pyöri prosessi, jonka muistin käyttö kasvoi koko ajan ja prosessi käynnistettiin uudestaan sunnuntaisin, sitä varten tehdyllä taskilla kello 18. Käynnistin taskin, jonka jälkeen muistin käyttö laski. Lähetin asiakkaalle viestin, että palvelimesta oli tullut muistinkäyttöhälytys ennen kuin task oli ajettu.

Tänä yönä yksi konesalin palomuuri vaihdettiin uuteen, joka olisi pahimmassa tapauksessa saattanut aiheuttaa paljon hälytyksiä esim. palvelimista, joiden verkkoliikenne kulki tämän palomuurin läpi. Olin vuoron ainoa palvelinosaaja, joka lisäsi vastuuta ja paineita entisestään. Vaihto sujui onnistuneesti ja mitään ei hajonnut. Lähetin kaikille CDC-asiakkaille tiedotteen, että muutostyö oli suoritettu onnistuneesti.

Asiakkaan Elasticsearch-palvelimelle oli kertynyt runsaasti lokeja. Ohjeistuksessa kerrotaan, että lokeja sai poistaa vanhimmasta lokitiedostosta alkaen. Palvelimella oli skripti, jolla lokitiedostoja sai siivottua. Palvelimelle kirjautuminen osoittautui vaikeaksi, sillä en meinannut löytää toimivia tunnuksia. Pienen tunnusrallin jälkeen pääsin kirjautumaan palvelimelle. Listasin kaikki lokit ja otin ylös muutamien tiedostojen nimiä, jotka halusin ensimmäiseksi poistaa. En ollut ennen käyttänyt tätä siivousskriptiä, joten en tiedä, miten sitä pitäisi käyttää. Yritin poistaa yhden tiedoston, mutta skripti ei toiminut. Googlasin

ohjeita, miten skriptiä käytetään ja löysin hyvät ohjeet [3]. Sain skriptin toimimaan ohjeiden avulla ja poistin vanhimpia lokeja sen verran, että hälytysraja alittui reilusti.

Viikkoanalyysi

Tällä viikolla tuli vastaan tikettejä, jotka yleensä ovat rutiininomaisia, mutta tällä kertaa häiriötilanne oli oikeasti päällä. Viikon aikana tuli vastaan paljon pieniä uusia asioita opittua. Koen osaavani ratkaista Cortexiin liittyviä ongelmia, mitä meille saattaa ratkaistavaksi tulla. Viikon aikana käytin ohjeistusta ja googlea avuksi ongelmien ratkaisuissa enemmän, mitä aiemmin olin käyttänyt.

4 POHDINTA

Päiväkirjaraportointia aloittaessani tavoitteeni oli ratkaista joka päivä sellainen tiketti, jota en ennen osannut ratkaista. Käytän päivittäin työssäni kymmeniä eri järjestelmiä ja teknologioita. Haastan itseäni viikottain tutkimalla ongelmia, joita en ole ennen tutkinut. Tätä kautta kartutan osaamistani aktiivisesti ja pyrin opettelemaan uutta. Raportoinnin alussa jouduin kyselemään kollegoilta apuja ongelmatilanteissa. Opinnäytetyön alussa en ollut varma, saanko kirjoitettua tarpeeksi erilaisista työtehtävistä. Nopeasti kuitenkin huomasin, että aiheista tai erilaisista tiketeistä ei tule pulaa.

Päiväkirjamuotoisen opinnäytetyön tehtyäni huomasin, että kykenen ratkaisemaan haastavampiakin häiriötilanteita itsenäisesti, joten huomattavaa ammatillista kehitystä on tapahtunut seurantajakson aikana. Olen oppinut, miten monien asiakkaiden järjestelmät toimivat ja miten niiden ympäristöt on rakennettu. Asiakkaiden suuren määrän vuoksi tämä ei kuitenkaan päde kaikkiin asiakkaisiin. On monia asiakkaita, joiden ympäristöjä en edelleenkään tunne lainkaan. Opeteltavaa ITOC:ssa on runsaasti, joten pääsen varmasti tulevaisuudessa tutkimaan kaikkien asiakkaiden ympäristöjen häiriöitä ja ongelmia. Tietotekniset taitoni ovat kasvaneet seurantajakson aikana. Aluksi jouduin kyselemään paljon neuvoja, mutta tällä hetkellä kykenen vastaamaan kollegoiden kysymyksiin.

Asiakaspalvelutaitoini ovat kehittyneet seurantajakson aikana. Suullinen kommunikointi on kehittynyt enemmän kuin kirjallinen, joka oli jo aloittaessani hyvässä kunnossa. Mitä enemmän vastailen asiakkailta tuleviin puheluihin, sitä enemmän kehitystä tapahtuu. Haluan kehittyä lisää asiakaspalvelijana, jotta voin toivottavasti jatkossa tarjota laadukasta ja asiantuntevaa palvelua asiakkaille.

Asettamani tavoitteet olivat hyvin maltillisia, mutta realistisia. Viikkoanalyysin ansiosta huomasin, että pääsin lähes joka viikko itselleni asettamiin tavoitteisiin. Huomaan nyt jälkeen päin, kuinka paljon kehitystä on tapahtunut näinkin lyhyen ajan sisään. Tämä kannustaa minua jatkossa oppimaan uutta ja kehittämään ammatillisia taitojani.

LÄHTEET

[1] M. Flinck 2019. MBR vs. GPT: Mitkä ovat erot? Viitattu 22.11.2020. https://koti-mikro.fi/oheislaitteet/kiintolevy/mbr-vs-gpt-mitka-ovat-erot/

[2] Apttech 2012. Understanding Citrix XML Broker and troubleshooting one XML broker issue. Viitattu 1.11.2020. https://apttech.wordpress.com/2012/02/08/understanding-citrix-xml-broker-and-troubleshooting-one-xml-broker-issue/

[3] Richard Chesterwood 2019. How to delete old ElasticSearch logs? Viitattu 23.11. https://blog.chesterwood.io/2019/06/how-to-delete-old-elasticsearch-logs.html

Telia Cygate Oy 2020. Kotisivut. Viitattu 22.11.2020. https://www.teliacygate.fi/fi/