jamk

Tietoturvavalvomon raportoinnin kehittäminen ja automatisointi

Lassi Halkosaari

Opinnäytetyö, AMK
Marraskuu 2021
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Halkosaari, Lassi

Tietoturvavalvomon raportoinnin kehittäminen ja automatisointi

Jyväskylä: Jyväskylän ammattikorkeakoulu. Marraskuu 2021, 54 sivua.

Tietojenkäsittely ja tietoliikenne. Tieto- ja viestintätekniikka. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Kyberturvallisuuden ongelmat ovat osa päivittäistä kamppailua yrityksille. Hyökkäysmäärien kasvaessa tietoturvavalvomoilla on tärkeä rooli organisaatioiden kyberuhkien hallinnassa jatkuvan valvonnan ja reagoinnin avulla.

Opinnäytetyön toimeksiantajana toimi Insta Advance Oy. Opinnäytetyön toimeksiantona oli kehittää ja automatisoida tietoturvavalvomon asiakkailleen kuukausittain toimitettavia palveluraportteja. Työn tavoitteena oli kehittää käytössä olevia palveluraportteja antamaan asiakkaille parempi kuva omien järjestelmiensä tietoturvan tilanteesta. Toisena tavoitteena oli automatisoida kuukausittain toimitettavien palveluraporttien luontiprosessia, jonka tavoitteena oli raporttien tekemiseen käytetyn työajan huomattava väheneminen.

Opinnäytetyö toteutettiin soveltavana tutkimuksena. Tietoperustassa tarkasteltiin yleisellä tasolla mitä tietoturvavalvomo, raportointi ja automatisointi pitivät sisällään. Tietoperustan jälkeen tarkasteltiin käytettyjä datalähteitä ja teknologioita. Tarkastelujen jälkeen käytiin läpi tietoturvavalvomon raportoinnin kehittäminen tapaustutkimuksena, jossa ensin kehitettiin käytössä ollutta palveluraporttia paremmaksi ja sen jälkeen kehitettiin teknisesti raportin luontiprosessia.

Opinnäytetyön lopputuloksena oli uusi kehitetty kuukausittain asiakkaille toimitettava palveluraportti sekä pitkälle automatisoitu raportin luontiprosessi. ActiveDocs-ohjelmiston ja datalähteisiin tehtyjen liitosten ansiosta suurin osa palveluraportille tulevista tiedoista saatiin haettua automaattisesti sen luonnin yhteydessä. Uudella kehitetyllä palveluraportilla tuotiin asiakasta varten selkeämmin esille heidän omien järjestelmiensä tietoturvan tilanne.

Merkittävä tulos oli raportointiin käytettävän ajan väheneminen noin kahdesta tunnista noin puoleen tuntiin, jolloin raportoinnin tekijät pystyivät käyttämään säästyneen työaikansa muiden työtehtävien tekemiseen. Tuloksista voi päätellä, että tietoturvavalvomo tarvitsee jatkuvaa kehittämistä ja automatisointia pysyäkseen ketteränä ja tehokkaana jatkuvasti muuttuvassa ympäristössä. Kehitettävää riittää aina, joten kehitystyö ei välttämättä koskaan ole täysin valmis.

Avainsanat (asiasanat)

SOC, kehittäminen, automatisointi, raportointi, integraatio, API, ohjelmointi, ActiveDocs

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Halkosaari, Lassi

Development and automation of Security Operations Center reporting

Jyväskylä: JAMK University of Applied Sciences, November 2021, 54 pages.

Engineering and technology. Degree Programme in Information and Communication Technology. Bachelor's thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

Cyber security issues are part of the daily struggle for businesses. As the number of attacks increases, Security Operations Centers play an important role in managing organizations' cyber threats through continuous monitoring and response.

The thesis was commissioned by Insta Advance Oy. The assignment of the thesis was to develop and automate the service reports delivered monthly to the customers of the Security Operations Center. The aim of the work was to develop the service reports in use to give customers a better picture of the security situation of their own systems. Another goal was to automate the process of creating monthly service reports, which aimed to significantly reduce the time spent on reporting.

The thesis was carried out as an applied research. At the general level, the knowledge base examined what the Security Operations Center, reporting and automation contained. After the knowledge base, the data sources and technologies used were examined. Following the reviews, the development of the Security Operations Center's reporting was reviewed as a case study, in which the service report used was first developed to be better and then the report creation process was technically developed.

The end result of the thesis was a new developed monthly service report delivered to customers and a highly automated report creation process. Thanks to the ActiveDocs software and the connections made to the data sources, most of the information coming to the service report was retrieved automatically when it was created. The newly developed service report highlighted the security situation of their own systems for the customer.

A significant result was a reduction in the time spent on reporting from about two hours to about half an hour, when the reporters were able to use their saved working time to perform other work tasks. From the results, it can be concluded that the Security Operations Center needs continuous development and automation in order to remain agile and efficient in an ever-changing environment. There is always plenty to develop, so development work may never be complete.

Keywords/tags (subjects)

SOC, development, automation, reporting, integration, API, programming, ActiveDocs

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenteet ja käytetyt termit

ActiveDocs	Asiakirjojen automatisointiohjelmisto suurille organisaatioille (Welcome to ActiveDocs n.d.)
API	Application Programming Interface
APT	Advanced Persistent Threat
Automaatio	Tehtävän suorittamista ilman ihmisen väliintuloa (Nanopoulos 2017)
Automatisointi	Manuaalisen työn muuttamista automaattiseksi (Nanopoulos 2017)
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Central Informatics Security Officer
CSIRT	Computer Security Incident Response Team
EDR	Endpoint Detection and Response
IDE	Integrated Development Environment
IDS	Intrusion Detection System
Incident Responder	Tietoturvavalvomon työntekijän rooli, jossa vastataan tapahtumista
IPS	Intrusion Prevention System
JSON	JavaScript Object Notation
Kyberhyökkäys	Kybertoimintaympäristöön ja mahdollisesti sen fyysisessä maailmassa ohjaamiin toimintoihin kohdistuva hyökkäys (Tietotekniikan termitalkoot 2014)
Kyberturvallisuus	Kybertoimintaympäristön tavoitetila, johon voidaan luottaa ja sen toiminta on turvattu (Kyberturvallisuuden sanasto 2018, 22)
MSSP	Managed Security Service Provider
NDR	Network Detection and Response
PDF	Portable Document Format
REST	Representational State Transfer
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Center (Tietoturvavalvomo)
Tier	Taso, jolla henkilö työskentelee tietoturvavalvomossa
TLS	Transport Layer Security

Triage Specialist	Tietoturvavalvomon uuden tapahtuman ensivasteen tekijän rooli
UEBA	User and Entity Behaviour Analytics
UTF-8	Unicode Transformation Format - 8 bits

1 Työn lähtökohdat

1.1 Taustaa ja toimeksiantaja

Kyberturvallisuuden ongelmat ovat osa päivittäistä kamppailua yrityksille. Vuonna 2007 tehdystä tutkimuksesta ilmeni, että hakkerit hyökkäsivät tietokoneita ja verkkoja vastaan yhdellä hyökkäyksellä 39 sekunnin välein. Uudemmassa Internetin rikollisuusvalituskeskuksen (Internet Crime Complaint Center) vuoden 2020 raportista ilmeni, että onnistuneita hyökkäyksiä tapahtui koko vuoden aikana 465177 kappaletta. Tämä tarkoittaa onnistunutta hyökkäystä 1,12 sekunnin välein. Todellisuudessa hyökkäysten määrä kuitenkin on vielä suurempi, sillä tässä ei ole huomioitu hyökkäysyrityksiä eikä raportoimattomia tapahtumia. (Zaharia 2021.) Cyber-edgen tuottaman raportin mukaan 86 prosenttia yrityksistä on ollut onnistuneen kyberhyökkäyksen kohteena vuonna 2020 (Cyberthreat Defense Report n.d.).

Koronaviruspandemia siirsi työntekijöitä etäkonttoreille. Samanaikaisesti kyberhyökkäyksien määrä lisääntyi merkittävästi (Sobers 2021). Hyökkäysmäärien kasvaessa tietoturvavalvomoilla (engl. Security Operations Center, SOC) on tärkeä rooli organisaatioiden kyberuhkien hallinnassa jatkuvan valvonnan ja reagoinnin avulla. Jatkuvan valvonnan ansiosta tietoturvavalvomot pystyvät tuottamaan raportteja asiakkailleen heidän järjestelmiensä tietoturvan tasosta. (Gurman 2020.) Raportointi voi kuitenkin muodostua ongelmaksi organisaatioilla, joilla on useita asiakkaita, sillä työntekijöiden aikaa kuuluu paljon raporttien tekemiseen käsin. Tämä on yksi syy raportoinnin automatisoinnin kehittämisen tärkeyteen. Automatisoidulla raportoinnilla parannetaan tehokkuutta, vähennetään monotonista työtä ja säästetään rahaa. (How report automation can improve your reporting process n.d.)

Crowleyn ja Pescatoren (2019) tekemän tutkimuksen mukaan vain 10,7 prosentilla vastaajista on täysin automatisoitu ja integroitu näkymä ajantasaisiin tietoturvavalvomon suorituskyvyn mittareihin. Vuorostaan 27,3 prosentilla on käytössä pääosin automatisoitu, vähäisesti manuaalista työtä vaativa toteutus raportointiin. Suurimmalla osalla eli 44 prosentilla on osittain automatisoitu tietojen hakeminen, mutta manuaalista työtä tarvitaan edelleen raportoinnin loppuunsaattamiseksi. Viimeiseksi 18 prosentilla raportointi on täysin manuaalista, jolloin tietoa haetaan useasta eri järjestelmästä ja laskenta tehdään manuaalisesti. (Crowley & Pescatore 2019, 18.)

Työn toimeksiantajana oli Insta Advance Oy, joka on osa Insta Group Oy -konsernia. Insta Advance Oy on kyberturvallisuuden ja turvallisen digitalisaation erikoisosaaja. Instan tärkeimpiä arvoja ovat ”Teemme kerralla kunnollista”, ”Pidämme lupauksemme” ja ”Osaamme ja onnistumme yhdessä”. Vuonna 2020 Insta-konsernin liikevaihto oli 138 miljoonaa euroa ja henkilöstön lukumäärä yli 1000. Insta on suomalainen perheyritys, joka palvelee asiakkaitaan teollisuusautomaation, teollisen digitalisaation, kyberturvan ja puolustusteknologian parissa. Konserniin kuuluu emoyhtiö Insta Group Oy:n lisäksi kolme toimialayhtiötä, jotka ovat Insta Advance Oy, sähköautomaation ratkaisutoimittaja ja elinkaarikumppani Insta Automation Oy ja avioniikan, miehittämättömän ilmailun ja korkeateknologian asiantuntija Insta ILS Oy. (INSTA ON TURVALLISEN JA KILPAILUKYKYISEN YHTEISKUNNAN RAKENTAJA JA KEHITTÄJÄ n.d.)

1.2 Tavoitteet ja toimeksianto

Opinnäytetyön toimeksiantona oli kehittää ja automatisoida tietoturvavalvomon asiakkailleen kuukausittain toimitettavia palveluraportteja. Työn tavoitteena oli kehittää käytössä olevia palveluraportteja antamaan asiakkaille parempi kuva omien järjestelmiensä tietoturvan tilanteesta. Toisena tavoitteena oli automatisoida kuukausittain toimitettavien palveluraporttien luontiprosessia. Valmiissa työssä tavoitellaan tietoturvavalvomon työntekijöiden kuukausittain toimitettavien palveluraporttien luomiseen käytetyn työajan huomattavaa vähenemistä automatisoimalla luontiprosessia, sillä suurin osa raporteille tulevasta tiedosta saadaan ActiveDocs-ohjelmistoon tehtyjen liitosten kautta muutamaa painiketta painamalla.

Toimeksianto toteutettiin aluksi selvittämällä tietoja, joita käytössä olevissa tietoturvavalvomon kuukausittain toimitettavissa palveluraporteissa on. Toisessa vaiheessa selvitettiin raporteille lisättäviä osioita – kuvioita, kaavioita ja kuvia. Kolmannessa vaiheessa tutkittiin muita raportointiosioita, joista asiakas voisi hyötyä raporteilla. Lopuksi kuukausittaisten palveluraporttien luontiprosessi automatisoitiin käyttämällä ActiveDocs-ohjelmistoa. Luontiprosessin automatisointia varten tehtiin useita liitoksia eri järjestelmiin ja tietokantoihin.

1.3 Tutkimusmenetelmä

Opinnäytetyö toteutettiin soveltavana tutkimuksena, jonka tavoitteena on tähdätä ensisijaisesti käytännön sovellukseen uusien menetelmien ja keinojen avulla (Tutkimus- ja kehittämistoiminta n.d.). Soveltavalla tutkimuksella tavoitellaan usein teknistä tai taloudellista hyötyä uusien ratkaisujen kautta (Soveltava tutkimus n.d.). Opinnäytetyö on jaettu kahteen osaan, jotka ovat teoria ja tekninen toteutus. Teoriaosassa pohjustettiin teknisessä toteutuksessa käytettäviä käsitteitä. Teknisessä toteutuksessa toteutettiin taloudellista hyötyä tavoitteleva ratkaisu.

Opinnäytetyötä rajattiin kolmen tutkimuskysymyksen avulla, jotka olivat:

1. Mitä tekijöitä hyvä tietoturvavalvomon tietoturvaraportti sisältää?
2. Miten tietoturvavalvomon raportointia voidaan kehittää?
3. Miksi tietoturvavalvomon raportointia kannattaa automatisoida?

Opinnäytetyöhön tietoa hankittiin kirjallisuudesta, internetistä löytyvistä artikkeleista ja toimeksiantajan edustajien eli työntekijöiden kanssa käydyistä keskusteluista. Tutkija on aikaisemmassa työssään parin vuoden aikana kehittänyt raportointia ja automatisoinut erilaisia raportteja. Opinnäytetyössä pystyttiin hyödyntämään tutkijan aikaisempaa osaamista ja kokemusta raportoinnin kehittämisestä, työkaluista ja automatisoinnista. Opinnäytetyössä on kiinnitetty tutkimuseettisesti erityistä huomiota, ettei opinnäytetyössä kerrota asiakkaiden tai tietoturvavalvomon työntekijöiden nimiä eikä liikesalaisuuksia. Tämän lisäksi työssä on huomioitu hyvä tieteellinen käytäntö. Opinnäytetyön reliabiliteettia ja validiteettia käsitellään pohdintaosuudessa.

2 Tietoturvavalvomo, raportointi ja automatisointi

Tässä luvussa määritellään käsitteet tietoturvavalvomo, raportointi ja automatisointi. Teoreettinen viitekehys koostettiin useista artikkeleista, kirjoista ja muista asiantuntijateksteistä. Tämän luvun teoreettinen viitekehys esittää mallin, jota tarkastellaan käytännönläheisemmin seuraavissa pääluvuissa.

2.1 Tietoturvavalvomo (Security Operations Center, SOC)

Tietoturvavalvomo tunnetaan yleisemmin englanninkielisten termien Security Operations Center (SOC) ja Cyber Security Operations Center (CSOC) mukaan. Tietoturvavalvomo voi olla osa organisaatiota tai tietoturvavalvomon palvelut voidaan ostaa ulkopuoliselta palveluntarjoajalta, jota kutsutaan Managed Security Service Provider (MSSP) toimijaksi (Kyberturvallisuuden sanasto 2018, 16). Tietoturvavalvomo on järjestäytynyt ja korkeasti koulutettu tiimi tai organisaatio, joka käyttää kehittyneitä tietoturvaloukkauksen tutkintaan tarkoitettuja työkaluja estääkseen, havaitakseen ja reagoidakseen organisaation kyberturvallisuuden häiriötilanteisiin (Demertzis, Kikiras, Tziritas, Sanchez & Iliadis 2018, 2, 35). Työkalujen lisäksi tietoturvavalvomossa on hyvin määritellyt prosessit ja menettelytavat häiriötilanteita varten (Sampat 2019).

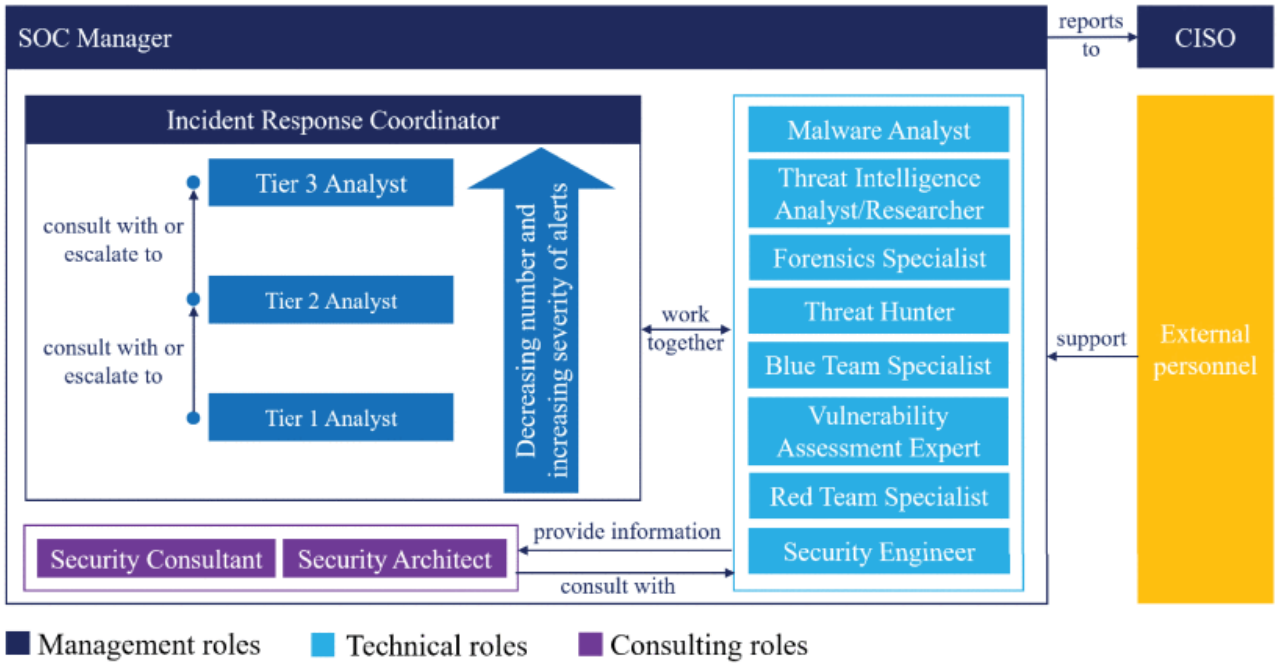
Ponemon Instituutin (2021) tekemän vertailututkimuksen mukaan tietomurron keskimääräiset kustannukset ovat 3,78 miljoonaa dollaria. Summa voi kuitenkin vaihdella riippuen murron perimmäisistä syistä, verkoston koosta ja organisaation mukaan. Keskimääräiset ulkopuolisen palveluntarjoajan tietoturvavalvomon kustannukset ovat noin 5,31 miljoonaa dollaria vuodessa. (Second Annual Study on the Economics of Security Operations Centers… 2021, 2.) Tietoturvavalvomon työntekijät varmistavat, että käytössä on organisaatiolle sopivat työkalut tietoturvapoikkeamien valvontaan, jolloin rajallisia resursseja ei käytetä tehottomiin työkaluihin. (What is a Security Operations Center (SOC)? n.d.c.)

2.1.1 Tietoturvavalvomon tehtävä ja toiminta

Tietoturvavalvomon tehtävänä on havaita, analysoida, vastata, raportoida ja estää kyberhäiriötilanteita (Zimmerman 2014, 9). Tietoturvavalvomon keskeisenä toiminnan osana on kyky käsitellä tietoturvauhkia ja poikkeamia. Erityisesti 2020-luvulla, kun uhkat muuttuvat ja kehittyvät nopeasti,

tarve ajantasaiselle kyvylle puolustautua kohdistettuja hyökkäyksiä sekä kehittyneitä haittaohjelmia vastaan kasvaa. Näissä tapauksissa tutut puolustusmekanismit, kuten virustorjunta ja palomuuri ei välttämättä riitä. Tällöin tarvitaan lisäksi jatkuvaa ympäristön valvontaa, uhkatilanteen seurantaa ja koulutettuja ammattilaisia uhkien havaitsemiseksi ja torjumiseksi. (Mikä on SOC ja miksi sellainen tarvitaan? 2017.) Tietoturvavalvomon työntekijät tekevät tiivistä yhteistyötä organisaation häiriötilanteiden reagointiryhmien (engl. Computer Security Incident Response Team, CSIRT) kanssa varmistaakseen, että turvallisuusongelmat korjataan nopeasti löydön jälkeen (De Groot 2020). Tietoturvavalvomon yhtenä tehtävänä on raportoida löydöksiään organisaation tietojärjestelmien tietoturvavastaavalle (engl. Central Informatics Security Officer, CISO), joka puolestaan raportoi joko tietohallintojohtajalle (engl. Chief Information Officer, CIO) tai suoraan toimitusjohtajalle (engl. Chief Executive Officer, CEO) (What is a Security Operations Center (SOC)? n.d.a.).

Tietoturvavalvomoa johtaa yleensä CISOn alaisuudessa SOC manageri, joka valvoo kaikkia tietoturvavalvomon osa-alueita, sen työvoimaa ja toimintaa. Hänen alaisuudessaan työskentelee analyytikot: Tier 1, Tier 2 ja Tier 3 (Tier-sanalla kuvataan tasoa, jolla henkilö työskentelee) (ks. Kuvio 1). Tier 1 analyytikon eli Triage Specialistin tehtävä on luokitella ja priorisoida hälytykset sekä eskaloida tapahtumia Tier 2 analyytikoille, mikäli häiriötilanteen selvittäminen kestää muutamia minuutteja kauemmin. Tier 2 analyytikko eli Incident Responder tutkii syvällisesti eskaloituneet tapahtumat, tunnistaa kohteena olevat järjestelmät ja hyökkäyksen laajuuden. Tier 2 analyytikko käyttää tiedossa olevaa uhkatietoa hyökkääjän paljastamiseksi. Tier 3 analyytikko eli uhkienmetsästäjä (engl. Threat Hunter) etsii ennakoivasti epäilyttävää käyttäytymistä verkosta, toteuttaa penetraatiotestausta ja arvioi verkon turvallisuutta havaitakseen edistyneitä uhkia ja tunnistaakseen haavoittuvuusalueet tai riittämättömästi suojatut resurssit. Suuren häiriötilanteen sattuessa Tier 3 analyytikko siirtyy Tier 2 analyytikon avuksi vastaamaan ja pitämään häiriötilannetta kurissa. Tietoturvavalvomolla voi olla myös turvallisuusarkkitehti (engl. Security Architect), jonka tehtävänä on suunnitella ja kehittää järjestelmiä sekä prosesseja integroimalla eri teknologioita toimimaan keskenään. Turvallisuusarkkitehti tekee myös tehtävien automatisointia, jolloin tietoturvavalvomon tehokkuus kasvaa toiminnan laajentuessa. Turvallisuusarkkitehtia voidaan myös kutsua turvallisuusinsinööriksi (engl. Security Engineer). (The Modern Security Operations Center… n.d.; Zimmerman 2014, 11, 45; Vielberth, Böhm, Fichtinger & Pernul 2020, 227761–227762.)



Kuvio 1. Tietoturvavalvomon roolitukset ja niiden keskenäinen vuorovaikutus (Vielberth ym. 2020, 227763)

Tietoturvavalvomo voi toimia eri valvontamalleilla, joista Suomessa toimivilla yrityksillä yleisin malli on jatkuvasti operoitava ympärivuorokautinen tietoturvavalvomo. Toisaalta tietoturvavalvomo voi toimia normaalien toimistojen aukioloaikoina esimerkiksi arkisin kahdeksan tai 12 tunnin työvuoroissa. Ensimmäinen malli tarkoittaa kahdeksaa tuntia viitenä päivänä viikossa, yleensä nämä viisi päivää ovat maanantaista perjantaihin. Toinen malli voi tarkoittaa esimerkiksi kahta kahdeksan tunnin työvuoroperiaatteella toimivaa toimipistettä eri aikavyöhykkeillä, jolloin saadaan neljän tunnin limitys molempiin suuntiin. (Zimmerman 2014, 63–64.)

Jatkuva ympärivuorokautinen palvelumalli tuo organisaatioille etulyöntiaseman puolustautuessa häiriötilanteilta ja tunkeutumisilta, sillä puolustautuminen ei ole riippuvaista kellonajasta (De Groot 2020). Ympärivuorokautinen malli kuitenkin maksaa huomattavasti enemmän sekä vaikuttaa työntekijöihin ja muuhun logistiikkaan (What is a Security Operations Center (SOC)? n.d.c.).

2.1.2 Tietoturvavalvomon haasteet

Tietoturvavalvomolla on useita haasteita, jotka pitäisi pystyä voittamaan. Ensimmäinen haaste on osaajapula. Kyberturvallisuuden ammattilaisista on puute olemassa olevien kyberturvallisuuden avoimien työpaikkojen täyttämisessä (What is a Security Operations Center (SOC)? n.d.b.). Esimerkiksi vuonna 2019 osaajapula oli 4,07 miljoonaa ammattilaista ((ISC)² Finds the Cybersecurity Workforce Needs to Grow 145%... 2019). Tämä aiheuttaa korkean riskin työntekijän ylikuormittumiselle. Ratkaisuna tietoturvavalvomon osaajapulaan on paikallisesti kouluttaa jokaiselle työntekijälle varahenkilö, jolla on tarvittava asiantuntemus hoitaa kyseisiä työtehtäviä, mikäli paikka yhtäkkiä vapautuu. (What is a Security Operations Center (SOC)? n.d.b.)

Toisena haasteena on edistyneet hyökkääjät kuten esimerkiksi edistyneet pitkäkestoiset uhat (engl. Advanced Persistent Threat, APT). Keskeinen osa organisaation kyberturvallisuusstrategiaa on verkon puolustus. Siihen on kiinnitettävä erityistä huomiota, koska edistyneillä toimijoilla on palomuurien ja päätelaitteiden puolustusten välttämiseksi tarvittavat välineet ja tietotaito. Tätä voidaan hallita ottamalla käyttöön poikkeamien havaitsemis- ja/tai koneoppimisominaisuudet sisältäviä työkaluja, joilla voidaan tunnistaa uusia uhkia. (What is a Security Operations Center (SOC)? n.d.b.)

Kolmantena haasteena on runsas data- ja verkkoliikenne. Keskimääräisen organisaation käsittelemän verkkoliikenteen ja datan määrä on suuri, jolloin kaikkea tietoa on vaikea analysoida. Tällöin pitääkseen manuaalisen analyysin minimissään tietoturvavalvomon työntekijöiden täytyisi luottaa automaattisiin työkaluihin tietojen suodattamiseksi, jäsentämiseksi, kokoamiseksi ja korreloimiseksi. (What is a Security Operations Center (SOC)? n.d.b.)

Neljäntenä haasteena on hälytysväsymys (engl. Alert Fatigue). Tietoturvavalvomon ei tulisi aina luottaa suodattamattomiin poikkeamahälytyksiin, hälytysten määrä voi silloin olla helposti musertava. Suuri ylimääräisten hälytysten määrä häiritsee tiimejä löytämästä oikeita ongelmia. Hälytysväsymystä voidaan helpottaa automaatiolla, jaottelemalla valvottavaa sisältöä ja sijoittamalla hälytyksiä eri prioriteeteille, jossa korkeamman prioriteetin hälytykset tulisi käsitellä ensimmäiseksi. (What is a Security Operations Center (SOC)? n.d.b.)

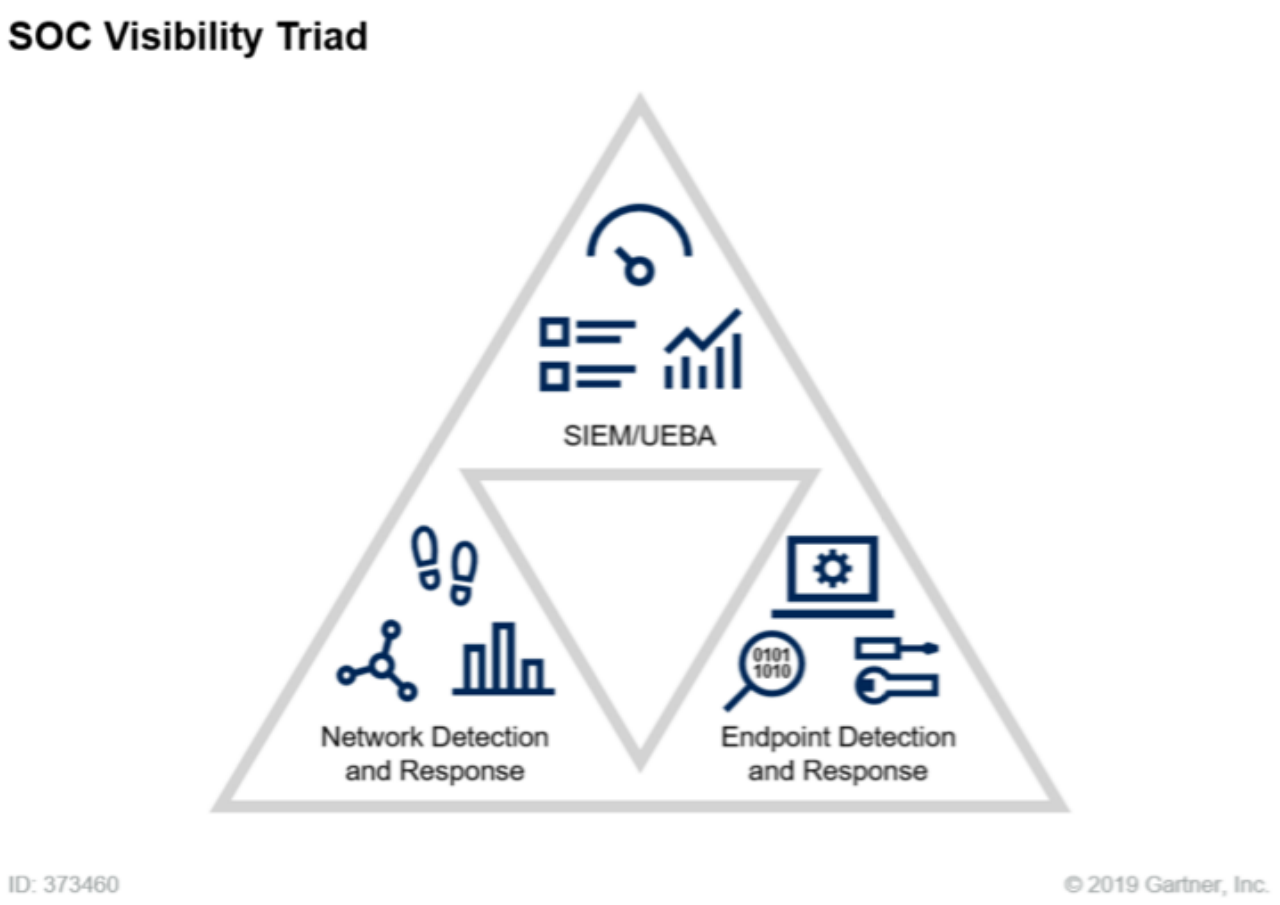
Viidentenä haasteena on tuntemattomat uhat. Tuntemattomia uhkia ei pystytä tunnistamaan perinteisiin tunnusmerkkeihin perustuvilla tunnistuksilla, päätelaitteiden tunnistuksilla ja palomuureilla. Ongelmaa pystyy lieventämään kehittämällä käyttäytymisanalyysiä epätavallisen käyttäytymisen löytämiseksi. (What is a Security Operations Center (SOC)? n.d.b.)

Kuudentena haasteena on työkalujen ylikuormitus. Organisaatiot usein hankkivat monia toisistaan irrotettuja työkaluja tarttuakseen kaikkiin mahdollisiin uhkiin, jolloin ne eivät välttämättä toimi keskenään muodostaen monimutkaisia uhkia. Kiinnittämällä huomiota keskitetyn seuranta- ja hälytysalustan avulla tehokkaisiin vastatoimiin pystytään vähentämään työkalujen ylikuormitusta. Työkalujen ylikuormitusta pystytään myös vähentämään erilaisten työkalujen integraatioiden avulla, jolloin työkaluja saadaan paremmin toimimaan keskenään. (What is a Security Operations Center (SOC)? n.d.b.)

Tietoturvavalvomon toiminnan kehittymisen ja tehokkuuden kannalta haasteeksi nousee vielä vähäinen raportoinnin automatisointi. Esimerkkinä tästä nähdään Crowleyn ja Pescatoren (2019) tekemä tutkimus, jonka mukaan alle puolella tietoturvavalvomoista on täysin tai pitkälle automatisoitu raportointi ajantasaisen suorituskyvyn mittaamiseen (Crowley & Pescatore 2019, 18).

2.1.3 Tietoturvavalvomon työkalut

Tietoturvavalvomon tärkeimpiä työkaluja ovat Security Information and Event Management (SIEM), Network Detection and Response (NDR) ja Endpoint Detection and Response (EDR). Käyttämällä näitä työkaluja yhdessä suuret tapahtumat eivät jää huomaamatta häiriötilanteiden tutkimisprosessin aikana (ks. Kuvio 2). (Chuvakin 2020.)



Kuvio 2. SOC Visibility Triad (Barros, Chuvakin & Belak 2019)

SIEM

Tietoturvavalvomon tärkeimpänä elementtinä pidetään yleensä modernia Security Intelligence -järjestelmää, jolla saadaan ajantasainen tilannekuva valvottavan kohdeympäristön kyberturvallisuuden tilasta (Mikä on SOC ja miksi sellainen tarvitaan? 2017). Security Information and Event Management (SIEM) -järjestelmällä tarkoitetaan tuotetta, joka tarjoaa reaaliaikaisen analyysin verkon laitteistojen ja sovellusten tuottamista turvallisuushälytyksistä. SIEM voi olla ohjelmisto, laite tai hallittu palvelu, jota käytetään sekä turvallisuustietojen lokittamiseen, että raporttien luomiseen joissain tapauksissa. (Vacca 2014, 20–21.) Taulukko 1 SIEM-työkalun ominaisuuksista.

Taulukko 1. SIEMin ominaisuudet (Vacca 2014, 20–21, muokattu)

Ominaisuus	**Selite**
Tietojen yhdistäminen	SIEM kerää tietoa monista lähteistä ja tarjoaa mahdollisuuden yhdistää tietoja, joka auttaa välttämään tärkeiden tapahtumien menettämistä.
Korrelointi	SIEM etsii tapahtumista yhteisiä ominaisuuksia ja yhdistää ne sen jälkeen samaan nippuun.
Hälytykset	SIEM tekee automaattista analyysiä korreloituneista tapahtumista ja tuottaa hälytyksiä helpottamaan tietoturvavalvomon toimintaa.
Koontinäkymät	SIEM-työkalut osaavat muuttaa tapahtumatiedot informaatiotaulukoiksi ja erilaisiksi visuaalisiksi näkymiksi, jotka auttavat tunnistamaan poikkeavaa toimintaa.
Yhteensopivuus	SIEM-sovelluksia voidaan automatisoida keräämään vaatimusten mukaista tietoa ja tuottamaan raportteja erilaisiin tarkoituksiin, esimerkiksi raportoida asiakkaille tietoturvapoikkeamien määrää.
Tietojen säilyttäminen	SIEM käyttää historiallisen tiedon säilyttämiseen pitkäaikaista tallennusta helpottaakseen tietojen korrelointia pitkällä aikavälillä ja vastatakseen erilaisiin vaatimuksiin tiedon säilyttämisajasta.

IDS & IPS

Tunkeutumisenhavaitsemisjärjestelmä (engl. Intrusion Detection System, IDS) ja tunkeutumisenestojärjestelmä (engl. Intrusion Prevention System, IPS) ovat suunniteltu havaitsemaan merkkejä hyökkäyksistä ja epätavallisesta liikenteestä verkossa. IDS- ja IPS-järjestelmät voivat olla verkkolaitteina, verkkokytkinten ja reitittimien moduuleina sekä edistyneinä ominaisuuksina verkkolaitteissa ja eri käyttöjärjestelmissä. IDS-järjestelmä lähettää hälytyksen, kun se havaitsee tiettyä kuviota noudattavaa poikkeuksellisen epätavallista liikennettä tai tunnetun allekirjoituksen liittyen tunnettuihin hyökkäyksiin. IPS-järjestelmä pystyy tekemään hälytyksien lisäksi korjaavia toimenpiteitä. (Sheikh 2020, luku 2.)

EDR

Endpoint Detection and Response (EDR) on suunniteltu kehittyneiden kyberuhkien jatkuvaan valvontaan ja niihin reagoimiseen. Tämä saavutetaan asentamalla agenttiohjelmia tai tunnistimia päätelaitteisiin keräämään toimintaa koskevia tietoja ja lähettävät niitä keskitettyyn tietokantaan analysoitavaksi. Analytiikkatyökalujen avulla EDR-ratkaisut pystyvät tunnistamaan poikkeavuuksia ja toimintamalleja. Näistä voidaan lähettää automaattisia hälytyksiä korjaustoimia tai jatkotutkimuksia varten. (ENDPOINT DETECTION AND RESPONSE n.d.)

NDR

Network Detection and Response (NDR) täydentää EDR- ja SIEM-työkaluja. NDR-ohjelmisto antaa tietoturvavalvomolle laajemman näkyvyyden koko verkkoon havaitakseen fyysisesti, virtuaalisesti ja pilvi-infrastruktuuriin kohdistuvien mahdollisesti piilossa olevien hyökkääjien käyttäytymistä. Laajempi havaitsemisympäristö voi paljastaa hyökkäyksen täyden laajuuden sekä mahdollistaa nopeammat ja kohdennetummat vastatoimet. (SOC, SIEM, MDR, EDR… what are the differences? 2021.)

UEBA

Tietoturvavalvomolla voi olla myös käytössä käyttäjien ja entiteettien käyttäytymisen analytiikkaa (engl. User and Entity Behaviour Analytics, UEBA). UEBA käyttää suuria määrää tietoa ihmisten ja koneiden tyypillisen ja epätyypillisen käyttäytymisen mallintamiseen verkossa. Tällä tavalla se pystyy tunnistamaan epäilyttävän käyttäytymisen, mahdolliset uhat ja hyökkäykset, joita perinteinen virustorjunta ei välttämättä havaitse. Esimerkiksi UEBA tunnistaa hyökkäykset, jotka eivät pohjaudu haittaohjelmiin analysoimalla käyttäytymismalleja. UEBA voi nykyään käyttää koneoppimista normaalin käyttäytymisen tunnistamiseen ja varoittaa riskialttiista poikkeamista, jotka voivat viitata verkossa tapahtuviin sivuttaisliikkeisiin (engl. lateral movement), sisäpiirin uhkiin, vaarantuneisiin tileihin ja erilaisiin hyökkäyksiin. UEBA täydentää vanhojen SIEM-työkalujen puutetta käyttäytymisanalytiikasta. (What is UEBA? Definition and Benefits n.d.)

2.2 Raportointi

2.2.1 Raportointi yleisesti

Raportointi on osa viestintää ja sen tarkoitus on dokumentoida tapahtumia. Raportointi voi olla kertovaa, kuvailevaa ja erittelevää. Tyypillisesti raportointi tapahtuu menneessä aikamuodossa ja tekstin rinnalla on usein havainnollistavia kuvaajia ja taulukoita. Raportoinnin avulla pystytään välittämään tietoa muille. (Hopeavuori n.d.) Tietoturvavalvomo pystyy raportoinnin avulla välittämään asiakkailleen tietoa heidän tietojärjestelmiensä tilasta (Gurman 2020).

Raporteilta lukija saa arvokasta tietoa organisaation toimintansa kannalta sekä mahdollisia uudistus- ja parannusehdotuksia toimintansa tueksi (Hopeavuori n.d.). Kurittun (2018) mukaan hyvän raportin kolme tärkeintä tunnusmerkkiä ovat:

1. kirkkaat ydinviestit
2. helppolukuisuus
3. luotettavat tiedot.

Kirkkailla ydinviesteillä tarkoitetaan oleellisimpien tietojen tuontia esille, joka samalla selkeyttää raportin rakennetta. Helppolukuisuudella pyritään siihen, että raporttia olisi helppo lukea ja sen asiat ovat helposti ymmärrettävissä. Luotettavilla tiedoilla varmistetaan, että raportin vastaanottajaa ei ohjata väärään suuntaan oikeasta tilanteesta ja epäluotettaviin tietoihin ei pohjata päätelmiä. (Kurittu 2018.)

2.2.2 Tietoturvavalvomon raportti

Gurmanin (2020) mukaan tietoturvavalvomon raportin tulisi sisältää ainakin seuraavat kohdat. Ensimmäiseksi keskeisimmät havainnot, joka toimii yhteenvetona raportin tärkeimmistä kohdista. Kohdan pitäisi tarjota selkeä kuva organisaation tietojärjestelmien turvallisuuden tasosta ja riskiprofiilista raporttia lukeville johtajille ja hallituksen jäsenille. Keskeisimpiä havaintoja voidaan selkeyttää erilaisilla visualisoinneilla ja mittareilla. Toisena seurannan yhteenveto, joka sisältää yhteenvedon raportilla seurattavista verkoista, laitteista ja palvelimista. Yhteenvedosta tulisi käydä ilmi seurattavat kohteiden määrä ja sijainti sekä tarkastamattomien laitteiden määrä, jotta johtajat

tietävät mahdollisien aukkojen syyt. Kolmantena häiriötilanteiden yhteenveto, joka on luettelo havaituista ja ratkaistuista häiriötilanteista raportointijakson aikana. Osiossa toimitetaan lisätietoa häiriötilanteista, kuten niiden tyypeistä, ajasta, kauanko kunkin ongelman havaitseminen ja ratkaiseminen kestivät, kunkin tapahtuman vakavuudesta ja tietoturvavalvomon tekemistä toiminnoista ongelman ratkaisemiseksi. (Gurman 2020.)

Neljäntenä osiona on yhteenveto uhkista. Tässä osiossa käsitellään vain raportointijakson aikana tapahtuneita vakavimpia uhkia. Osiossa vakavia uhkia tarkastellaan tarkemmin, selitetään mitä ne ovat ja miten niitä on käsitelty sekä asetetaan tapaukset uudelleen asiayhteyteen seuraavien kysymyksien avulla. Onko kyseinen hyökkäys riskitrendien mukainen? Oliko sillä vaikutusta liiketoimintaan? Odotetaanko samanlaisia tapauksia lisää? Voidaanko samanlaisiin uhkiin valmistautua paremmin? Viimeisenä kohtana suositukset, jossa keskitytään organisaation kyberturvallisuuden tasoa parantaviin toimenpiteisiin. Toimenpiteitä voivat olla tietoturvavalvomon talousarvion suurentaminen tai investointipyyntö tiettyihin kyberturvallisuuden työkaluihin. Osiossa voidaan myös suositella koko organisaatiolle järjestettävää kyberturvallisuuden tietoisuuskoulutusta tai erityisiä suunnitelmia tietojen ja liiketoiminnan prosessien suojaamiseksi, mikäli tietomurto tapahtuu. (Gurman 2020.)

2.2.3 Erilaisia raportointitapoja

Raportointia voidaan toteuttaa PowerPoint-, Word- ja PDF-muodossa, sähköpostina, infograafina tai verkkosivuna. PowerPoint toimii hyvin, mikäli dioilla näkyvät tiedot selitetään selkeästi asiakkaalle tapaamisen yhteydessä. Word-dokumentti kannattaa muuttaa PDF-dokumentiksi, mikäli asiakkaalta ei odoteta kommentteja suoraan raportille. PDF-raportti luodaan yleensä, kun lukija haluaa säilyttää raportin ja raportti on liian monimutkainen asetettavaksi verkkosivulle. PDF-muodossa raportille saadaan aseteltua paljon tietoa, mutta raporttia luodessa täytyy kiinnittää erityistä huomiota tiedon asetteluun ja esilletuonnin selkeyteen. Lisäksi raportointia voidaan toteuttaa luomalla verkkosivulle erilaisia näkymiä raportoitavista järjestelmistä. Verkkosivulta asiakkaat voivat vapaasti katsoa joko reaaliajassa tai tietyn ajanjakson välein päivitettävää sivua, josta nähdään kyseisen organisaation järjestelmiensä tila tarkastushetkellä. (Clippinger 2017, 29–79.) Erilaisia verkkosivunäkymiä varten on kehitetty useita ohjelmia, joita voidaan hyödyntää raportoinnissa esimerkiksi DashThis, D3security ja ServiceNow (How report automation can improve your reporting process. N.d.; CISO dashboard n.d.; Cybersecurity Incident Reporting & Dashboards n.d.).

2.2.4 Palvelutasosopimus (SLA)

Raportoinnin osana raportoidaan palvelutasosopimuksen määrittelemä palvelutaso, jota palvelun tuottajalta odotetaan. Tämä sopimus on kriittinen osa jokaista teknologiasopimusta. Palvelutasosopimuksessa määritellään mittarit, joilla palvelua mitataan sekä korjaustoimenpiteet tai seuraamukset mikäli kyseistä palvelutasoa ei saavuteta. Näiden lisäksi sopimuksessa määritellään vastuut ja odotukset, jotta sopimuksen molemmat osapuolet ymmärtävät vaatimukset samalla tavalla, jos palvelussa ilmenee ongelmia. (Overby, Greiner & Paul 2017.)

2.3 Automatisointi

Automatisoinnilla tarkoitetaan manuaalisen työn muuttamista automaattiseksi. Automaatiolla suoritetaan tehtäviä ilman ihmisen väliintuloa. Automaatiolla voidaan kattaa kyberturvallisuuden puolustukselliset ja hyökkäykselliset osa-alueet. (Nanopoulos 2017.)

Puolustus hyödyntää automaatiota tapahtumien ennaltaehkäisyssä, havaitsemisessa ja reagoinnissa. Hyökkäyspuolella punaiset tiimit (engl. Red Team) eli vihollista simuloivat tiimit ja muut hyökkääjät voivat käyttää automaatiota haavoittuvuuksien arvioinnin suorittamiseen tai tavoitteiden saavuttamiseen. Automatisoinnista on hyötyä, sillä manuaalisten tehtävien tekemisen sijaan tiimit ja muut ammatinharjoittajat voivat käyttää enemmän aikaa perusteellisemman analyysin tekemiseen ja ennakoivien turvatoimien toteuttamiseen. Automatisoinnin keskeisenä etuna on, että se helpottaa ammatinharjoittajien elämää ja antaa heille mahdollisuuden työskennellä tehokkaammin. (Nanopoulos 2017.)

Seuraavat kolme asiaa kertovat, kannattaako jokin tehtävä automatisoida vai ei. Ensimmäiseksi selvitetään, onko tehtävä rutiininomainen eli tehdäänkö se tietyin aikavälein. Esimerkiksi tietoturvavalvomo voi kuukausittain tehdä ja lähettää tietoturvaraportin asiakkaalle. Toiseksi tehtävän yksitoikkoisuus eli pitääkö tehtävä tehdä aina samalla tavalla ja pitääkö tietoja hakea aina samoilla ohjeilla. Esimerkiksi tietoturvavalvomo voi kerätä raportille tietoa eri järjestelmistä aina tietyllä tavalla. Viimeiseksi tehtävän aikakriittisyys eli työn tekijä ei ehdi käyttää aikaansa tärkeämpien töiden tekemiselle. Esimerkiksi manuaalisesti kaiken tiedon kerääminen tietoturvavalvomon raportille saattaa kestää useita tunteja. (Nanopoulos 2017.)

Kaikkea ei kuitenkaan kannata automatisoida: Ennen tietoturvavalvomon kuukausittaista palveluraportin lähettämistä halutaan yleensä varmistaa raportille tulevien tietojen ulkoasun selkeys ja korostaa joitain erityistapahtumia merkittävyyttä kirjoittamalla niistä lisätietoja auki. Tällöin ei haluta automatisoida raportin kaikkia vaiheita. (Nanopoulos 2017.)

3 Työssä käytetyt datalähteet ja teknologiat

Tässä luvussa määritellään työssä käytetyt datalähteet ja teknologiat. Luvun lopussa vertaillaan ja esitellään lyhyesti raportoinnin automatisointiin valittua työkalua.

3.1 Datalähteet

3.1.1 Tiketöintijärjestelmä

Tiketillä tarkoitetaan tiketöintijärjestelmään kirjattua palvelupyyntöä, joka voi sisältää yhteydenottoja, ongelmia tai molempia. Tiketillä voidaan seurata tietyn tapahtuman käsittelyä tiketöintijärjestelmässä. Tiketille asetetaan oma tunnistenumero sekä sen tilaa ja käsittelijää voidaan seurata tunnistenumeron perusteella. (Miksi tiketöinti? n.d.) Tiketöintijärjestelmä toimii tikettien käsittely- ja asiakaspalvelujärjestelmänä sekä toiminnanohjausjärjestelmänä. Sähköpostin yhdistäminen tiketöintijärjestelmän osaksi on tärkeää. Tällöin sähköpostin hallinta osana tikettien käsittelyä on sulavaa, eikä asiakkaan tarvitse käyttää useita sähköpostiosoitteita kommunikointiin. Järjestelmästä kuvataan tikettien tila sekä yhtä asiaa koskeva viestiketju ja historia. Näin asiakokonaisuus pysyy helposti seurattavana yhdellä tiketillä. (Mikä on tiketöinti? n.d.)

Tiketöintijärjestelmässä tiketti voidaan osoittaa tietylle tiimille tai asiakaspalvelijalle. Tällöin eri tiimit ja henkilöt voivat työpäivän aikana seurata omaa työjonoansa ja ottaa sieltä tikettejä itselleen käsiteltäväksi. Järjestelmässä samanlaisia tikettejä voidaan yhdistää tai liittää toisiinsa. Yhdistäessä tikettejä kaksi tai useampi eri tiketti sulautuu yhdeksi tiketiksi. Alitiketöinnissä tiketeistä valitaan päätiketti ja sen alle voidaan luoda alitikettejä. Alitiketöintiä voidaan käyttää esimerkiksi, jos asiakkaalta on tullut tehtävä, joka voidaan jakaa useisiin tehtäviin ja eri vastuualueille. Tiketöintijärjestelmästä saadaan haettua tiketeiltä tietoa raportteja varten. Raporteilla voidaan seurata tiketin tietojen perusteella esimerkiksi palvelutasosopimuksissa sovittujen vastausaikojen toteutumista

sekä raportointijaksolla kertyneitä tikettimääriä. Hyvin tehdystä järjestelmästä saadaan tehtyä laajaa raportointia - lisäksi se on kytkettävissä ulkoisiin raportointijärjestelmiin. (Mikä on tiketöinti? n.d.)

3.1.2 Security Information and Event Management (SIEM)

SIEM-järjestelmästä saadaan reaaliaikaista tietoa sinne asetetuista lokilähteistä. Lisäksi sillä voidaan muodostaa hälytyksiä tapahtumista tai tapahtumasarjoista, jotka noudattavat luotuja sääntöjä korrelaatioon perustuen. Tämän jälkeen hälytyksiä voidaan ohjata keskitettyyn tiketöintijärjestelmään tietoturvavalvomon työntekijöiden käsiteltäväksi. Joissain tapauksissa SIEM-järjestelmästä voidaan luoda erillisiä raportteja tuottamaan tärkeää lisätietoa tietoturvavalvomon palveluraportille tuotteesta ja lisäosista riippuen. (Vacca 2014, 20–21, 103.)

3.1.3 Verkonvalvontapalvelin

Verkonvalvontapalvelin seuraa jatkuvasti verkossa olevien järjestelmien suorituskykyä ja niiden välisten verkkoyhteyksien tilaa. Palvelimelle voidaan asettaa aikavälejä, jolloin hälytyksiä lähetetään verkonvalvojalle esimerkiksi tiketöintijärjestelmään, kun tietyssä aikaikkunassa johonkin verkossa olevaan järjestelmään ei saada yhteyttä tai yhteys toimii hitaasti. Mikäli verkonvalvontaa tuotetaan palveluna, palvelimelta saatavalla tiedolla pystytään laskemaan, toteutuuko palvelulle sovittu palvelutasosopimus (engl. Service Level Agreement, SLA). (IT-alan kehitys on johtanut n.d.)

3.1.4 Tunkeutumisenhavaitsemisjärjestelmä (IDS)

HAVARO on Kyberturvallisuuskeskuksen huoltovarmuuskriittisille yrityksille ja valtionhallinnolle tarjoama palvelu, joka toimii tietoturvaloukkausten havainnointi- ja varoitusjärjestelmänä. Palvelussa eri lähteistä peräisin olevien tietoturvallisuusuhkatunnisteiden perusteella organisaation verkkoliikenteestä tunnistetaan haitallinen ja normaalista poikkeava liikenne. Ensisijaisesti kyberturvallisuuskeskus vastaanottaa poikkeamien tiedot ja analysoi ne. Toisaalta palvelua tuotetaan tietoturvavalvomoiden kanssa yhteistyössä, jolloin SOC hoitaa osan tapahtumien käsittelystä ja raportoinnista. HAVARO-järjestelmän tietojen perusteella voidaan varoittaa muita organisaatioita havaitusta uhasta. Tällöin järjestelmän avulla pystytään muodostamaan kokonaiskuva suomalaisten tietoverkkojen tietoturvauhista. (HAVARO-palvelu 2021.)

3.2 Teknologioita

3.2.1 Visual Studio -kehitysympäristö

Visual Studio on Microsoftin omistama integroitu kehitysympäristö (engl. Integrated Development Environment, IDE), jota voidaan käyttää sekä koodin muokkaamiseen, korjaamiseen ja rakentamiseen, että sovelluksen julkaisemiseen. Integroitu kehitysympäristö on monipuolinen ohjelma, jota voidaan käyttää ohjelmistokehityksen moniin osa-alueisiin. Visual Studio sisältää tavanomaisen editorin ja virheenkorjauksen lisäksi kääntäjät, koodin viimeistelytyökalut, graafiset suunnittelijat ja monia muita ominaisuuksia helpottamaan ohjelmistokehitysprosesseja. (Welcome to the Visual Studio IDE 2021.)

3.2.2 C# -ohjelmointikieli

C# on yleiskäyttöinen ja moderni olio-ohjelmointikieli, jota kutsutaan nimellä ”C sharp”. Ohjelmointikielen kehitti Microsoft. Anders Hejlsberg ja hänen tiiminsä johtivat kielen kehitystä .Net -aloitteen puitteissa ja sen ovat hyväksyneet Euroopan tietokonevalmistajien yhdistys (ECMA) ja kansainvälinen standardointijärjestö (ISO). C# on yhteisen kieli-infrastruktuurin (engl. Common Language Infrastructure, CLI) joukossa. Lisäksi se on syntaksiltaan samankaltainen kuin Java ja helppo käyttäjille, jotka tuntevat jonkin kielistä C, C++ tai Java. C# on korkean tason kieli ja sen takia se on helposti opittava. C# on laajasti käytetty työpöytä- ja verkkosovellusten kehittämiseen. (Intoduction to C# 2019.)

3.2.3 .NET ja ASP.NET -alustat

.NET on kehittäjäalusta, joka koostuu työkaluista, ohjelmointikielistä ja kirjastoista monenlaisten sovellusten rakentamiseen. Perusalusta tarjoaa komponentteja kaikenlaisiin sovelluksiin. Perusalustan lisäkehykset, kuten ASP.NET, laajentavat .NET -komponentteja tietyntyyppisiin sovelluksiin. ASP.NET tuo seuraavia asioita lisää .NET alustalle: (What is ASP.NET? n.d.)

- Peruskehyksen verkkopyyntöjen käsittelyyn C# -kielellä
- Verkkosivujen mallinnussyntaksin (Razor), dynaamisten verkkosivujen luomiseen C# -kielellä
- Kirjastot yleisille verkkomalleille, kuten mallinäkymäohjain (engl. Model View Controller, MVC)
- Todennusjärjestelmän, joka sisältää kirjastot, tietokannan ja mallisivut kirjautumisen käsittelyä varten, mukaan lukien ulkoinen ja monivaiheinen todennus
- Muokkauslaajennukset syntaksin korostukseen, koodin viimeistelyyn ja muita toimintoja verkkosivujen kehittämiseen (What is ASP.NET? n.d.)

3.2.4 Internet Information Services (IIS) -verkkopalvelin

Internet Information Services tunnetaan lyhenteellä IIS. IIS-verkkopalvelin toimii Microsoftin .NET -alustalla Windows -käyttöjärjestelmässä. IIS voidaan myös ajaa Linuxilla ja Macilla, tätä ei kuitenkaan suositella sen epävakaisuuden vuoksi. Toisaalta Windowsilla IIS on vakaa, monipuolinen ja sitä on käytetty laajalti useita vuosia tuotannossa. IIS-verkkopalvelin toimii prosessina verkkosovellusten isännöintiin. IIS on täynnä ominaisuuksia ja sitä käytetään yleisimmin ASP.NET -verkkosovellusten ja staattisten verkkosivujen isännöintiin. Sitä voidaan käyttää myös tiedostonsiirtopalvelimena ja isäntänä Windowsin kommunikoinnin perustan (engl. Windows Communication Foundation, WCF) palveluille. Lisäksi sitä voidaan laajentaa isännöimään verkkosovelluksia, jotka on rakennettu muilla alustoilla, kuten PHP:llä. Vuolletin (2018) mukaan IIS tukee seuraavia todennusvaihtoehtoja:

1. Basic
2. ASP.NET
3. Windowsin todennusta.

3.2.5 JavaScript Object Notation (JSON) -tiedonsiirtoformaatti

JavaScript Object Notation eli JSON on kevyt tiedonsiirtoformaatti, jota ihmisen on helppo lukea ja kirjoittaa sekä koneiden on helppo jäsentää ja luoda. Se perustuu osaan JavaScript-ohjelmointikielen standardia ECMA-262, kolmas painos joulukuussa 1999. JSON on täysin kieliriippumaton tekstimuoto, joka käyttää C-kieliryhmän ohjelmoijille tuttuja käytäntöjä. Nämä ominaisuudet tekevät JSON-tiedonsiirtoformaatista hyvän tiedonsiirtotavan. Esimerkki koodipätkä JSON muodosta: '{"nimi":"Testi", "ikä":20, "puhelin":null}'. (Introducing JSON n.d.)

3.2.6 Representation State Transfer (REST) -rajapinta

Representation State Transfer eli REST tarkoittaa alun perin arkkitehtuurityyliä hajautetuille hypermediajärjestelmille. Nykyään puhutaan myös REST-rajapinnoista. REST ei ole protokolla tai standardi, vaan joukko arkkitehtuurisia rajoituksia. WWW (World Wide Web) on hyvä esimerkki kyseiseen arkkitehtuurityyliin perustuvasta järjestelmästä. Ensimmäisen kerran REST esiteltiin vuonna 2000 Roy Fieldingin väitöskirjassa. Sovelluksen on täytettävä seuraavat kuusi ohjaavaa rajoitusta (ks. taulukko 2), että sitä voidaan kutsua RESTfuliksi: (Fielding 2000, 76–85.)

Taulukko 2. REST-rajapinnan ohjaavia rajoituksia (Fielding 2000, 76–85, muokattu)

Rajoitus	**Selite**
Asiakas-Palvelin (engl. Client-Server)	Erottamalla käyttöliittymäongelmat tietojen tallennusongelmista parannetaan käyttöliittymän siirrettävyyttä useilla alustoilla sekä skaalautuvuutta yksinkertaistamalla palvelinkomponentteja.
Tilaton	Jokaisen asiakkaan palvelimelle lähettämän pyynnön on sisällettävä kaikki pyynnön ymmärtämiseksi tarvittavat tiedot, eikä se voi hyödyntää palvelimelle tallennettuja yhteyksiä. Istunnon tila pysyy siis täysin asiakkaan varassa.
Mahdollisuus välimuistille	Välimuistin rajoitukset edellyttävät, että pyyntöön annetun vastauksen tiedot ovat implisiittisesti tai nimenomaisesti merkitty asetettavaksi välimuistiin tai ei ollenkaan. Jos vastaus on välimuistissa, asiakkaan välimuistilla on oikeus käyttää kyseistä vastaustietoa uudelleen vastaavia pyyntöjä varten.
Yhtenäinen käyttöliittymä	Soveltamalla ohjelmistosuunnittelun yleisperiaatetta komponenttiliittymään, järjestelmän arkkitehtuuri yksinkertaistuu ja vuorovaikutusten näkyvyys paranee. Yhdenmukaisen käyttöliittymän saamiseksi tarvitaan useita arkkitehtuurisia rajoituksia komponenttien käyttäytymisen ohjaamiseksi. REST määritellään neljällä rajapintarajoituksella: resurssien tunnistaminen, resurssien manipulointi edustusten kautta, itsekuvaavat viestit ja hypermedia sovellustilan moottorina.
Kerrostettu järjestelmä	Kerrostettu järjestelmätyyli mahdollistaa arkkitehtuurin muodostamisen hierarkkisista kerroksista rajoittamalla komponenttien käyttäytymistä siten, että yksikään komponentti ei voi nähdä sen välittömän kerroksen ulkopuolelle, jonka kanssa ne ovat vuorovaikutuksessa.
Koodi tarvittaessa	REST mahdollistaa asiakkaan toimintojen laajentamisen lataamalla ja suorittamalla koodin sovelmien tai komentosarjojen muodossa. Tämä yksinkertaistaa asiakkaita vähentämällä valmiiksi toteutettujen ominaisuuksien määrää.

3.2.7 Open Data Protocol (OData) -protokolla

Open Data Protocol eli OData on kansainvälisen standardisoimisjärjestön (engl. International Organization for Standardization, ISO) ja kansainvälisen sähkötekniikan komission (engl. International Electrotechnical Commission, IEC) hyväksymä OASIS (Organization for the Advancement of Structured Information Standards) -standardi, joka määrittelee joukon parhaita käytäntöjä RESTful-ohjelmointirajapintojen (engl. RESTful API) rakentamiseen ja käyttöön. OData RESTful ohjelmointirajapinnat ovat helppoja käyttää ja sen metatiedot, voidaan koneellisesti lukea kuvaus ohjelmointirajapintojen tietomalleista, mahdollistavat tehokkaiden asiakkaan välityspalvelimien ja työkalujen luonnin. (OData n.d.)

3.2.8 GitLab -alusta

GitLab on yhtenä sovelluksena toimitettava ainutlaatuinen DevOps -alusta, jonka avulla luodaan ohjelmistotyön virtaviivainen kulku samalla vapauttaen organisaation yhteen liitetyn työkaluketjun rajoituksista. Yhtenä sovelluksena GitLab tarjoaa hyvän näkyvyyden ja tehokkuuden sähköisten palvelujen tuotantoon, sen kaikissa vaiheissa. (What is GitLab? n.d.) Työssä GitLab ympäristöä käytetään koodin versionhallintatyökaluna.

3.3 Raporttien automatisointityökalu

3.3.1 ActiveDocs-ohjelmiston valinta

Työssä raporttien automatisointiin käytettiin ActiveDocs-ohjelmistoa. ActiveDocs on asiakirjojen automatisointiohjelmisto suurille organisaatioille (Welcome to ActiveDocs n.d.). ActiveDocs-ohjelmisto valikoitui raporttien automatisointiin syistä, jotka on avattu taulukossa kolme.

Taulukko 3. ActiveDocs-ohjelmiston valintaan johtaneita syitä

Syy	**Selite**
Yhteensopivuus olemassa olevien järjestelmien kanssa	1. Integroitui hyvin Microsoftin tuotteiden kanssa. 2. Word-muodossa olevat raporttipohjat pystyttiin viemään ActiveDocs-ohjelmistoon. 3. Yhteydet tietokantoihin olivat mahdollisia. 4. Erinäiset tiedostot, joista tietoa haettiin, voitiin liittää datalähteiksi. 5. REST-rajapintayhteydet olivat mahdollisia.
Laajennettavuus	Ohjelmistoon voitiin liittää lisää datalähteitä. Lisäksi ohjelmistoon voitiin liittää ohjelmointirajapinnan kautta kaikkea mahdollista.
Loppukäyttäjän käytettävissä	Palveluraportin luominen oli yksinkertaista loppukäyttäjälle.
Sulauttaminen	Tietoa ei tarvitse hakea käsin monesta eri datalähteestä.
Dokumentaatio	Ohjelmiston mukana tuli kattava dokumentaatio.
Tuki	Vastaan tulleissa ongelmissa pystyttiin saamaan tukea ActiveDocsin tuotetuesta.

Muita testattuja työkaluja, jotka eivät kuitenkaan sopineet haluttuun käyttötarkoitukseen olivat JasperReports, Crystal Reports, jsreport ja monet muut liiketoimintatiedon hallintatyökalut (engl. Business intelligence, BI). Näistä työkaluista Crystal Report ei päässyt konseptin todennusvaiheeseen (engl. Proof of Consept, PoC) siitä puuttuvan demon ja sen sekavuuden vuoksi. JasperReports raportointityökalu ei sopinut käyttötarkoitukseen, sillä:

1. Raportoinnin kuvauskieli oli staattista, jolloin dynaamisia datalähteitä ei pystytty lisäämään.
2. Työkalulla oli puutteellinen ja huono dokumentaatio sekä se käytti vanhentuneita rajapintoja.
3. Työkalu ei ollut yhteensopiva olemassa olevien järjestelmien kanssa, tärkeimpänä: Word-tiedostoa ei pystynyt luomaan vaan olisi pitänyt käyttää JasperReportsin omaa JRXML-kuvauskieltä.

Jsreport työkalu oli hyvä vaihtoehto ActiveDocs-ohjelmistolle, mutta se ei kuitenkaan sopinut käyttötarkoitukseen, sillä:

1. Jokainen raportti olisi jouduttu rakentamaan alusta alkaen uudestaan, tämä vaatisi Hypertext Markup Language (HTML) kielen osaamista, jolla vanhat Word-palveluraportit pitäisi luoda käsin samanlaisiksi, joka puolestaan olisi vaatinut paljon työtä.
2. Verrattuna ActiveDocs-ohjelmistoon jsreport oli teknisempi ratkaisu loppukäyttäjille.
3. Helppokäyttöinen käyttöliittymä olisi pitänyt tehdä itse.
4. Käyttää node.js kirjastoa, joten tulevaisuudessa Node Package Manager (NPM) riippuvuuksien määrä olisi mahdollisesti ongelma.

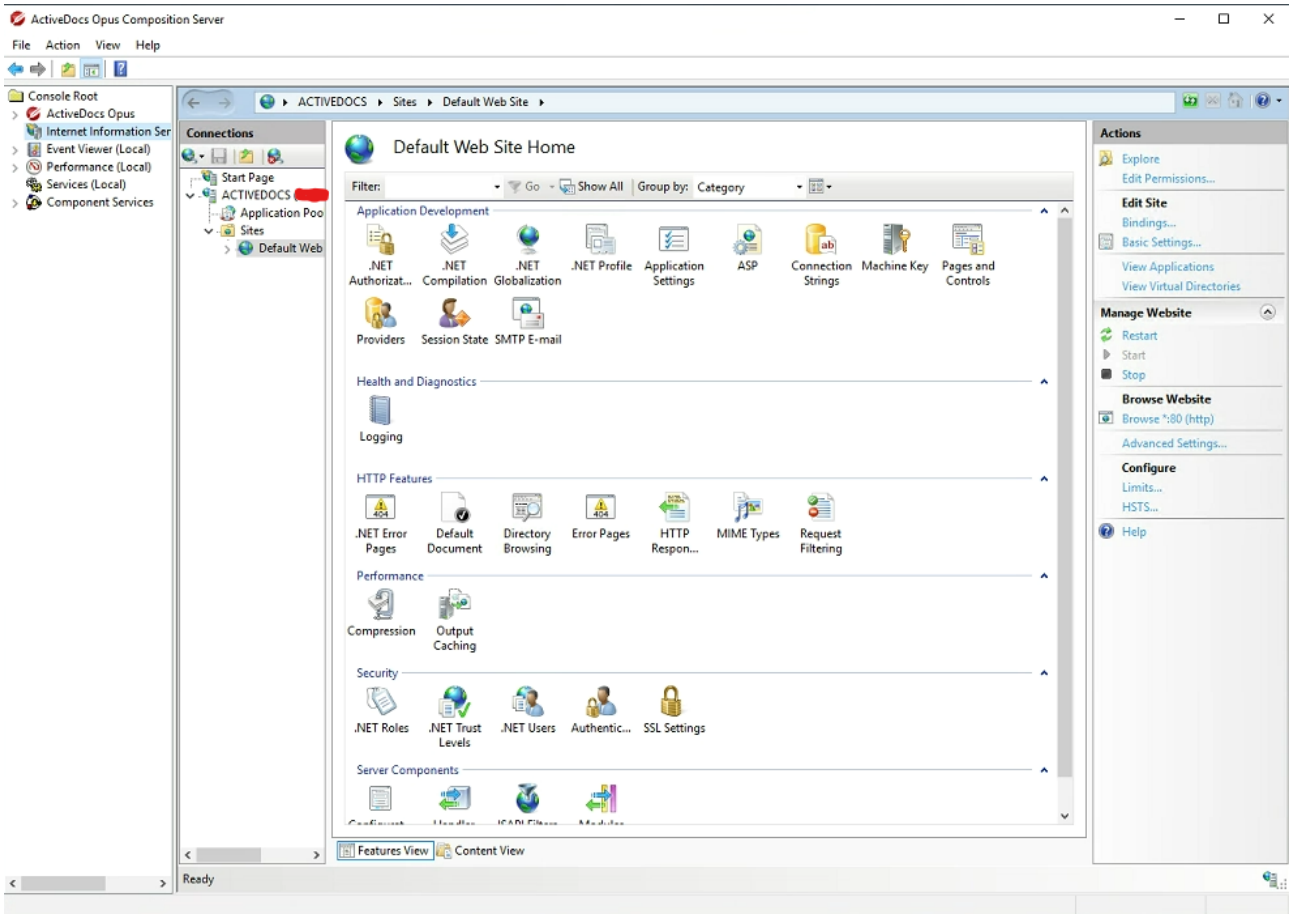
Lisäksi selvitettiin mahdollisuuksia käyttää erilaisia BI-työkaluja. Nämä työkalut olisivat soveltuneen suuremman mittakaavan ratkaisuiksi, johon tarvittaisiin monipuolisempaa tilannetietoa järjestelmistä. Kuitenkaan haluttuun käyttötarkoitukseen BI-työkalut eivät olleet yhteensopivia, sillä ne eivät soveltuneet Word-muotoiseen raportointiin.

3.3.2 ActiveDocs-ohjelmisto

ActiveDocs-ohjelmisto koostuu useasta eri komponentista, mutta tässä työssä käytetään Active-Docs Opus Composition Server -ja ActiveDocs Opus Content Manager -ohjelmistoja.

ActiveDocs Opus Composition Server

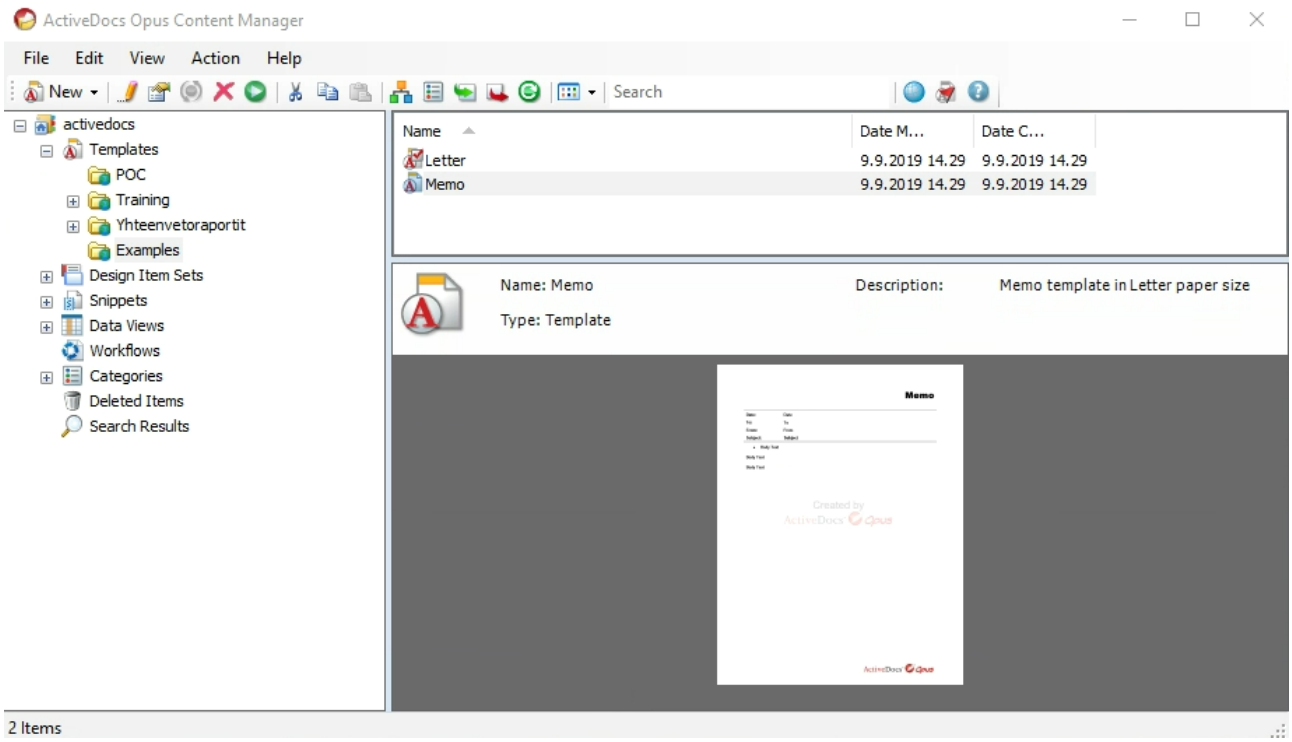
ActiveDocs Opus Composition Server -ohjelmiston näkymää (ks. Kuvio 3) käytetään ainoastaan, kun luodaan uudelle asiakkuudelle oma DataView. DataView tarkoittaa tiedon kokoelmaa tietyltä asiakkaalta. Composition Server -ohjelmistoon linkitetään IIS-palvelussa luotavat verkkosivut. Näiltä verkkosivuilta voidaan sen jälkeen hakea tietoa REST-rajapinnan kautta ActiveDocs Opus Content Manager -ohjelmistolla.



Kuvio 3. ActiveDocs Opus Composition Server -ohjelmiston näkymä

ActiveDocs Opus Content Manager

Content Manager -ohjelmiston näkymä toimii pääasiallisena näkymänä loppukäyttäjälle (ks. Kuvio 4). Content Manager -ohjelmistossa tiedon hakeminen Composition Server -ohjelmistolta tapahtuu luomalla DataView, johon määritetään Composition Server -ohjelmiston verkko-osoite tiedonhakusijaintia kuvaavine parametreineen. Tämän jälkeen määritetään tarkemmat haetun tiedon käsittelyarvot, kuten esimerkiksi mitkä kentät näkyvät DataViewillä ja kauanko tiedon hakeminen DataViewille saa kestää.



Kuvio 4. ActiveDocs Opus Content Manager -ohjelmiston näkymä

Content Manager -ohjelmistossa voidaan luoda Word-muotoisista palveluraporteista Word-mallipohjia. Luomisen jälkeen näitä mallipohjia voidaan muokata Microsoft Word -työkalulla, johon ActiveDocs on luonut Word-laajennuksen ActiveDocs-ohjelmiston työkalujen käyttöä varten. Kyseisen Word-laajennuksen avulla mallipohjiin voidaan tuoda ja muokata tietoja DataVieweiltä.

4 Case: Tietoturvavalvomon raportointi

4.1 Raportoinnin kehittämistarpeet ja kehitys

Tässä luvussa käydään läpi, mitä käytössä olevat kuukausittain toimitettavat palveluraportit sisältävät, mitä niissä halutaan kehittää, kuinka niitä tehdään ja kuinka niiden tekemistä haluttaisiin automatisoida.

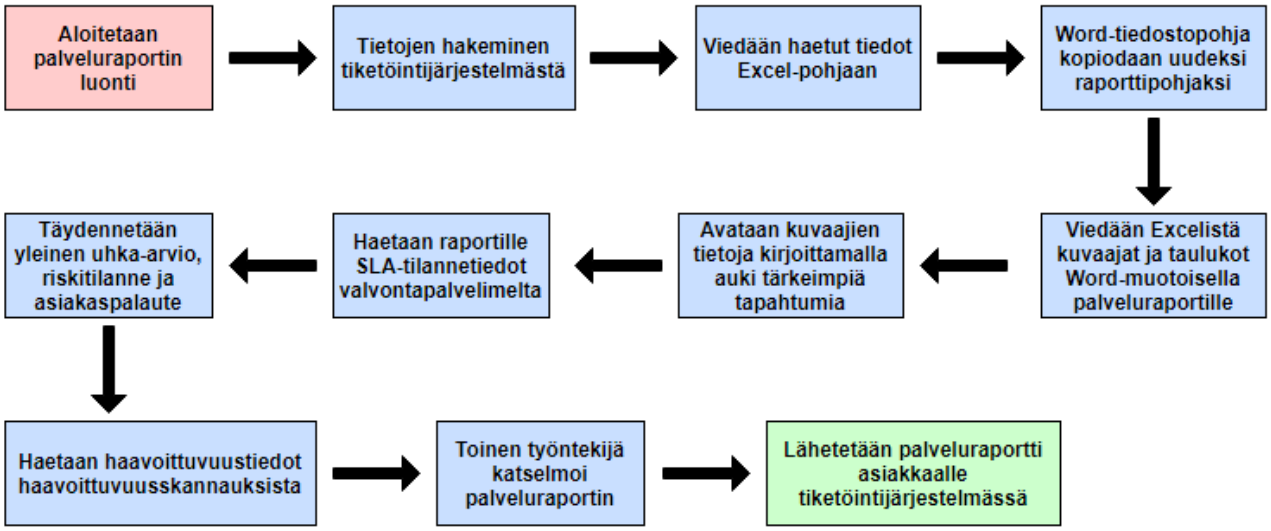
4.1.1 Käytössä oleva palveluraportti

Käytössä oleva palveluraportti sisältää raportointijaksolta eli pääasiassa edelliseltä kuukaudelta tai vuosineljännekseltä seuraavat tiedot:

1. Palvelujakson saavutettu SLA-tilanne, joka sisältää valvontapalvelimilta saatavan SLA-tilannetiedon, jota verrataan SLA-tavoitteeseen.
2. Jakson palvelupyynnöt, joka sisältää kuvaajan häiriöstä ja palvelupyynnöistä tiketin tilan mukaan: käsittelyssä tai suljettu. Tarkemmat tiedot raportointijaksolla ratkaistuista muutos- tai palvelupyynnöistä.
3. Jakson tietoturvatilanne, joka sisältää yleisen uhkatilanteen asiakkaan järjestelmistä. Voidaan käydä läpi esimerkiksi yleisiä haavoittuvuuksia. Jakson tietoturvatapahtumat vakavuuksittain, tyypeittäin sekä vakavuuksittain edellisen 90 päivän ajalta ryhmiteltynä viikkonumeroittain.
4. Riskitilanne, joka sisältää mahdolliset riskit, kuten esimerkiksi suorituskyvyn- tai levytilan puute.
5. Eskaloinnit ja asiakaspalaute, joka sisältää tarkemmat tiedot eskaloinneista, joihin kuuluu pääasiassa vakavat ja kriittiset tapahtumat sekä mahdollisen asiakaspalautteen.
6. Avoimet muutokset, joka sisältää raportointihetkellä olevat avoimet muutos- ja palvelupyynnöt.
7. Haavoittuvuudet, joka sisältää asiakkaan ympäristöstä löytyvät tärkeimmät uudet haavoittuvuudet sinne tehtyjen haavoittuvuusskannauksien perusteella.

4.1.2 Käytössä oleva palveluraportin prosessikuvio

Käytössä oleva kuukausittain asiakkaalle toimitettava palveluraportti luodaan suurimmaksi osaksi käsin. Raportin luomisessa käytetään apuna Excel-työkaluun tehtyjä makroja, jotka muuttavat tiketöintijärjestelmästä haetut tikettitiedot kuvaajiksi ja taulukoiksi. Tämän jälkeen kopioidaan Word-tiedostopohja uudeksi raporttipohjaksi ja viedään Excel-työkalussa tehdyt kuvaajat ja taulukot raportille. Kuvaajien ja taulukkojen viennin jälkeen tiettyjä kohtia raportilla kirjoitetaan auki tarkemmin. Auki kirjoittamisen jälkeen haetaan SLA-tilannetiedot valvontapalvelimelta. Viimeiseksi SIEM-tuotteelta haetaan haavoittuvuustietoja haavoittuvuusskannauksien raporteilta ja katselmoidaan toisen työntekijän toimesta, että palveluraportilla ei ole selkeitä virheitä (ks. Kuvio 5).



Kuvio 5. Käytössä oleva raportoinnin prosessikuvio

Palveluraporttia tekevien asiantuntijoiden mukaan paljon aikaa vievä ja muuten turha vaihe on tietojen hakeminen tiketöintijärjestelmästä raportille. Yhden kuukausittaisen palveluraportin tekemiseen kuluu asiantuntijalla aikaa noin kaksi tuntia.

4.1.3 Automatisoinnin mahdollisuudet

ActiveDocs-ohjelmiston avulla raportointia voidaan nopeuttaa automatisoimalla tiedonhakuvaiheita, joista tärkein ja työläin vaihe on tiketöintijärjestelmästä saatavan tiedon hakeminen ja sen vieminen palveluraportille oikeaan muotoon. Hakemisen automatisoinnin jälkeen voidaan haetut tiedot muokata oikeaan muotoon ja viedä ne ActiveDocs-ohjelmistolle, jossa ne liitetään automaattisesti palveluraportille luonnin yhteydessä.

4.1.4 Uusi kehitetty palveluraportti

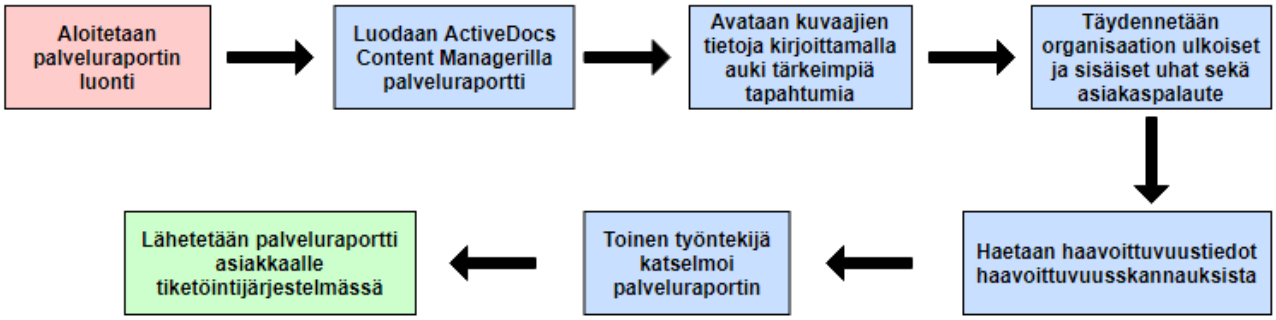
Osa palveluraportille tulevasta tiedosta määritellään asiakkaan ja organisaation välisessä palvelukuvauksessa. Muut raportille tulevat tiedot voidaan itse määritellä sen perusteella mistä tiedosta asiakas voisi hyötyä. Uusi palveluraportti sisältää pääosin samat tiedot kuin käytössä oleva palveluraportti. Kuitenkin ActiveDocs-ohjelmiston rajoitteiden ja asiakkaan paremman tiedottamisen vuoksi omien järjestelmien tilasta on raportin kenttiä ja sisältöä muokattu paremmiksi. Uusi kehitetty palveluraportti sisältää raportointijaksolta eli pääasiassa edelliseltä kuukaudelta tai vuosineljännekseltä seuraavat tiedot:

1. Raportointijakson saavutettu palvelutasotilanne, joka sisältää valvontapalvelimilta saatavan SLA-tilannetiedon, jota verrataan SLA-tavoitteeseen. Lisäksi kohta sisältää palvelusopimuksissa määritetyt SLA-tavoitteet ja niiden toteumataulukon sekä lisätietoa SLA-tavoitteen ylittävistä tiketeistä raportointijaksolla.
2. Raportointijakson kaikki tapahtumat, joka sisältää kuvaajan häiriöstä, muutos- ja palvelupyynnöistä tiketin tilan mukaan onko se käsittelyssä vai suljettu. Tarkemmat tiedot raportointijaksolla ratkaistuista ja avoimista muutos- tai palvelupyynnöistä.
3. Raportointijakson tietoturvatilanne, joka sisältää organisaation ulkoiset ja sisäisit uhat. Ulkoisissa uhissa voidaan käydä läpi esimerkiksi yleisiä haavoittuvuuksia. Sisäisissä uhissa voidaan mainita esimerkiksi suorituskyvyn- tai levytilan puute. Jakson tietoturvatapahtumat omina kuvaajina vakavuuksittain, tyypeittäin sekä vakavuuksittain edellisen kolmen kuukauden ajalta ryhmiteltynä viikkonumeroittain. Lisäksi avataan tarkemmat tiedot laajemmin raportoitavista tapauksista, joihin kuuluu pääasiassa vakavat ja kriittiset tapahtumat.
4. HAVARO-tapausten lukumäärät ja tiedot, joka sisältää HAVARO-tunkeutumisenhavaitsemisjärjestelmästä eriteltynä tarkempia tietoja tapahtumien lukumääristä verrattuna edellisiin jaksoihin sekä kuvaajan niiden laadusta.
5. Palaute, joka sisältää mahdollisen asiakkaan antaman palautteen palvelusta sekä mahdollisen palveluntarjoajan palautteen asiakkaalle.
6. Haavoittuvuudet, joka sisältää asiakkaan ympäristöstä löytyvät tärkeimmät uudet haavoittuvuudet sinne tehtyjen haavoittuvuusskannauksien perusteella.

Uudessa palveluraportissa tietoja on uudelleenjärjestelty ja joitain uusia tietoja, kuten HAVARO-tapausten lukumäärät ja tiedot, on lisätty antamaan parempi kokonaiskuva asiakkaan omien järjestelmien tapahtumamääristä.

4.1.5 Uuden kehitetyn palveluraportin prosessikuvio

Uusi kehitetty kuukausittain asiakkaalle toimitettava palveluraportti luodaan suurimmaksi osaksi ActiveDocs-ohjelmistoon tehdyillä automatisoinneilla. Uuden raportin luontiprosessissa jää monia vaiheita pois verrattuna käytössä olleeseen luontiprosessiin. Uudessa prosessissa palveluraportin luonti aloitetaan ActiveDocs Opus Content Manager -ohjelmistossa. Ohjelmistosta valitaan halutun asiakkaan palveluraportti. Ajetaan raportti, jonka jälkeen avataan kuvaajien tietoja kirjoittamalla auki tärkeimpiä tapahtumia. Auki kirjoittamisen jälkeen täydennetään organisaatioon kohdistuvat ulkoiset ja sisäiset uhat sekä mahdollinen asiakaspalaute. Viimeiseksi SIEM-tuotteelta haetaan haavoittuvuustietoja haavoittuvuusskannauksien raporteilta ja katselmoidaan toisen työntekijän toimesta, että palveluraportilla ei ole selkeitä virheitä (ks. Kuvio 6).



Kuvio 6. Uuden kehitetyn palveluraportin prosessikuvio

4.2 Tekninen toteutus

Tässä luvussa käydään läpi teknistä toteutusta ja kuinka se toteutettiin. Ensin käydään läpi toteutusta yleisesti sen jälkeen tarvittavien ohjelmistojen asennuksia ja tehtyjä integraatioita eri järjestelmiin.

4.2.1 Toteutus yleisesti

Koko tekninen prosessi menee tiivistetysti seuraavalla tavalla. Visual Studio -ympäristöä käytetään C#-koodin kirjoittamiseen ja sen kokoamisessa IIS-palvelimelle verkkosivuksi, joka hakee tietoa eri datalähteistä ja muuttaa ne JSON-muotoon verkkosivulle ActiveDocs-ohjelmistoa varten. Kyseiseltä verkkosivulta tiedot haetaan ActiveDocs-ohjelmiston DataViewille, joka viedään lopuksi palveluraportin mallipohjaan. DataViewillä olevat tiedot luetaan raportin luonnin yhteydessä Document Wizard -työkalussa.

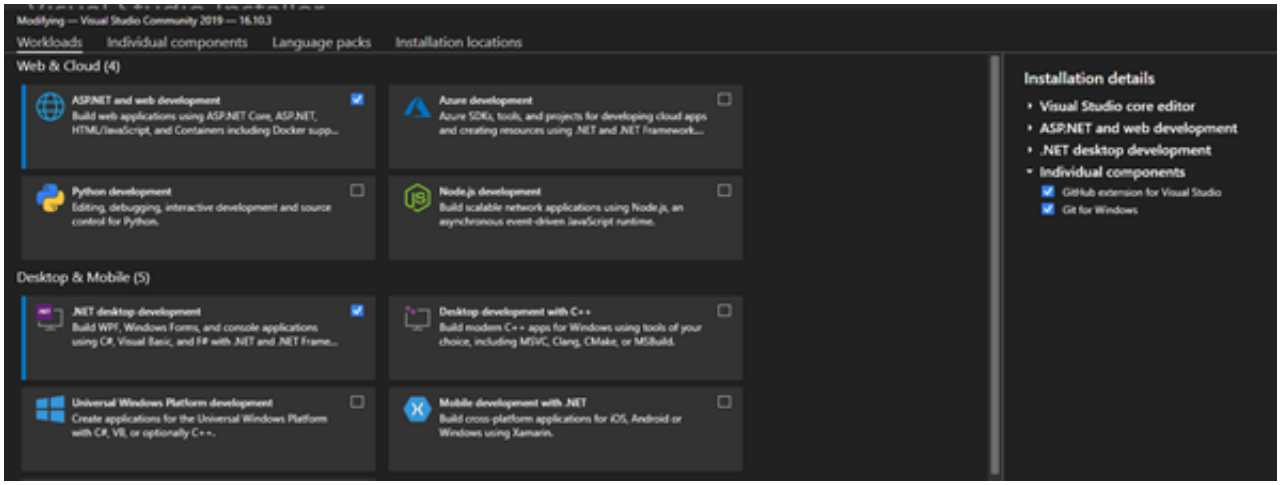
Toteutus aloitettiin tutkimalla erilaisia toteutusmahdollisuuksia ActiveDocs-tuotteen tarjoamista Visual Studion esimerkkiratkaisuista. Ottamalla mallia esimerkeistä tehtiin OData-mallia käyttävä C#-koodipohja eli .cs-tiedosto, johon luotiin integraatioita eri järjestelmien välille. Verkkosivulle tulevat tiedot jäsenneltiin ja tyypiteltiin .xml-tiedostossa OData-mallin mukaan ActiveDocs-ohjelmiston DataViewejä varten. ActiveDocs Opus Content Managerissa DataViewin luonnin yhteydessä lisätietoihin asetetaan Datatype-arvo. Datatype-arvo määrittelee C#-koodissa if-ehtolauseilla mitä tietoa DataView saa. Esimerkiksi CaseSLAYlitykset arvolla saadaan haettua SLA-tavoitteen ylittäneet tapahtumat.

4.2.2 Tarvittavat ohjelmistot ja niiden asennukset

Visual Studio -kehitysympäristö

Visual Studiosta voidaan ladata tuotteen omilta verkkosivuilta, joko ilmainen Community-versio tai maksullinen Business- tai Enterprise-versio. Työssä käytettiin Visual Studio Community 2019 -versiota. Toteutusta varten asennettiin Visual Studio oletusasetuksilla ja seuraavilla komponenteilla (ks. Kuvio 7):

1. ASP.NET and web development
2. .NET desktop development
3. Git for Windows
4. GitHub extension for Visual Studio.



Kuvio 7. Visual Studioon asennettavat komponentit

Visual Studioon asennettiin myös seuraavat NuGet-paketit, jotka sisältävät muiden kehittäjien uudelleenkäytettävää koodia:

1. Newtonsoft.Json ja Json.Linq
2. Microsoft.AspNet.WebApi
3. Microsoft.AspNet.WebApi.Client
4. Microsoft.AspNet.WebApi.Core
5. Microsoft.AspNet.WebApi.WebHost
6. Nager.Date
7. System, josta haettiin paketit Collections.Generic, Data, Globalization, IO, Linq, Net, Net.Http, Text, Text.RegularExpressions, Web, Web.Http ja Xml.

ActiveDocs-ohjelmistot

Toteutushetkellä ActiveDocs Opus Composition Server ja ActiveDocs Opus Content Manager -ohjelmistot olivat valmiiksi asennettuja, sillä niitä oli käytetty aikaisemmin erilaisten raporttien automatisointiin. Uutta ActiveDocs-ohjelmistoa asennettaessa asennusohjeet saadaan ActiveDocs-tuotetuelta tuotteen oston yhteydessä.

4.2.3 Integraatiot eri järjestelmistä

Tiketöintijärjestelmä

Tiketöintijärjestelmään tulee suurin osa palveluraportille haluttavista tiedoista, jotka käsitellään tietoturvavalvomon henkilöstön toimesta. Järjestelmään tulee hälytykset SIEM-, IDS-palvelulta ja verkonvalvontapalvelimelta, joten tähän tehtiin ensimmäiseksi integraatio. Yhteys tiketöintijärjestelmään saatiin järjestelmään luodun REST API -rajapintayhteyden kautta. Yhteyden luontiin käytettiin .cs-tiedostossa C#-kirjastoa System.Net.WebClient. Yhteyden luontia ja tietojen hakua varten asetettiin verkko-osoite parametreineen tiketöintijärjestelmän REST API -rajapintaan GET-metodilla. Parametrit määräytyivät tiketöintijärjestelmän REST API -rajapinnan mukaan, tässä tapauksessa parametreiksi asetettiin eri käyttötapausten mukaan seuraavia arvoja:

1. Asiakkaan tunnistenumero tiketöintijärjestelmässä.
2. Päivämäärät miltä väliltä tikettien tiedot haluttiin (pääasiassa edellisen kuukauden ensimmäisestä päivästä nykyisen kuukauden ensimmäiseen päivään).
3. Tiketin tyypin määritys sen perusteella haluttiinko häiriöt, palvelupyynnöt, muutospyynnöt vai useampi vaihtoehto näistä.
4. Päivämäärät milloin tiketti tulisi olla ratkaistu.
5. Tiketin tietoturvatapahtumakentän arvon määritys, onko tietoturvatapahtuma vai jokin muu.
6. Tiketin vakavuuden määritys, onko tiketin vakavuus merkityksetön, vähäinen, kohtalainen, vakava, kriittinen vai useampi vaihtoehto näistä.

Joissain tapauksissa tiketin eri välilehdiltä täytyi hakea lisätietoa, silloin täytyi parametreihin asettaa tiketin tunnistenumero ja välilehden numero, jolta tietoja haluttiin. Parametrien asettamisen jälkeen täytyi asettaa merkistökoodaus UTF-8 sekä yhteyspyynnön otsikkoon erillinen käyttäjäkohtainen salausavain, joka haettiin jokaisella tiedonhakukerralla uudestaan.

Tiketöintijärjestelmästä haluttujen tikettien tiedot tuotiin merkkijonona, joka muutettiin heti JArrayksi käyttämällä metodia JsonConvert.DeserializeObject. JArraystä voitiin hakea for-silmukassa jokaisen halutun tiketin tietyt tiedot ja muokata niitä haluttuun muotoon kuten esimerkiksi, kuinka monta vakavuudelta kriittistä tapahtumaa luotiin raportointijakson aikana tai päivämäärä voitiin muuttaa tiettyyn muotoon. Nämä tiedot lisättiin muokkauksien jälkeen uuteen JObjectiin, joka lisättiin myöhemmin verkkosivulle menevään julkiseen JArrayhyn samassa silmukassa. For-silmukassa tehtiin myös viimeiset tikettien suodatukset if-ehtolauseilla, jolloin valittiin tiettyyn raportin osaan sopivat tiketit haetuista tiketeistä.

Esimerkiksi mikäli palveluraportille haluttiin saada raportointijakson häiriöt ja palvelupyynnöt, joiden SLA-tavoite on ylittynyt, ensin asetettiin verkko-osoitteen parametreihin asiakkaan tunnistenumero tiketöintijärjestelmässä, tiketin luontiaikaväli eli raportointijakso (tässä tapauksessa edellinen kuukausi) ja tiketin tyyppi oli oltava häiriö tai palvelupyyntö. Myöhemmin for-silmukassa haettiin vielä lisätietoja eri välilehdeltä koskien tiketin luokitteluaikaa ja viestin lähetysaikaa, joista koostuivat tikettien SLA-tavoiteajat. Lisätietojen haun jälkeen kaikista haetuista tiketeistä valittiin if-ehtolauseella raportille vain ne tiketit, joiden SLA-tavoiteajat eivät ole toteutuneet. Tähän raportin osaan haettiin tiketiltä seuraavat tiedot: tunnistenumero, otsikko, tila, tyyppi, vakavuus, vasteaika ja ensitiedotusaika.

Verkonvalvontapalvelin

Verkonvalvontapalvelimelta saadaan hälytyksiä tiketöintijärjestelmään, mutta sieltä saadaan myös tarkempaa tietoa palvelimien käytettävyyksistä eli SLA-arvoista. Verkonvalvontapalvelimella ei ollut REST API -rajapintaa käytössä, mutta sieltä saatiin käytettävyystiedot haettua suoraan JSON-muotoiselta verkkosivulta GET-metodilla. Käytettävyystiedot haettiin C#-koodissa samalla tavalla kuin tietojen hakeminen tiketöintijärjestelmän REST API -rajapinnasta. Eri asiakkaiden tietojen hakemisen erottamisessa käytettiin eri verkko-osoitetta, jonka parametreihin määriteltiin halutun asiakkaan id-arvo. Lisäksi yhteyspyynnön otsikkoon kirjoitetaan erilainen käyttäjäkohtainen salausavain, joka pysyy aina samana tietoa hakiessa.

Tiedot palautuvat jälleen merkkijonona ja merkkijono muutetaan JArrayksi käyttämällä metodia JsonConvert.DeserializeObject. Muuttamisen jälkeen jokainen JSON objekti käydään läpi ja sen arvot (hostname, selite ja käytettävyys) tallennetaan yhteen JObjectiin. Samaan JObjectiin tallennetaan SLA-tilanteen teksti, joka saadaan vertaamalla käytettävyyttä SLA-tavoitearvoon. Mikäli kyseisen palvelimen käytettävyys on pienempi kuin SLA-tavoite, saadaan arvo Selvitys alapuolella, muussa tapauksessa saadaan arvo OK. Arvon ollessa Selvitys alapuolella, palveluraportille tulee manuaalisesti selvittää syyt, jotka johtivat SLA-tavoitearvon rikkoutumiseen.

Tunkeutumisenhavaitsemisjärjestelmä (HAVARO)

Tunkeutumisenhavaitsemisjärjestelmästä – HAVARO – saadaan hälytyksiä tiketöintijärjestelmään. HAVARO-palvelusta saadaan hälytyksien lisäksi tarkempia lukumääriä tapahtumista ja niiden vakavuuksista rajapinnan kautta. Tarkoituksena oli hakea palveluraportille tapausten lukumäärä raportointijaksolla ja vuoden sisällä sekä vuoden sisällä olevat tapahtumat vakavuuksittain. Rajapintayhteyden parametrit oli asetettu erillisellä automaatiopalvelimella, jossa sijaitsi toimiva automaatio-ohjelmisto. Automaatio-ohjelmisto toimii välittäjänä HAVAROn rajapinnan ja C#-koodin välillä. C#-koodissa määritettiin verkko-osoite salausavaimineen, josta automaatio-ohjelmisto välitti tiedot HAVAROn rajapinnalle. Rajapintaa käytettiin noudattaen HAVAROn omaa rajapinnan käyttöohjetta.

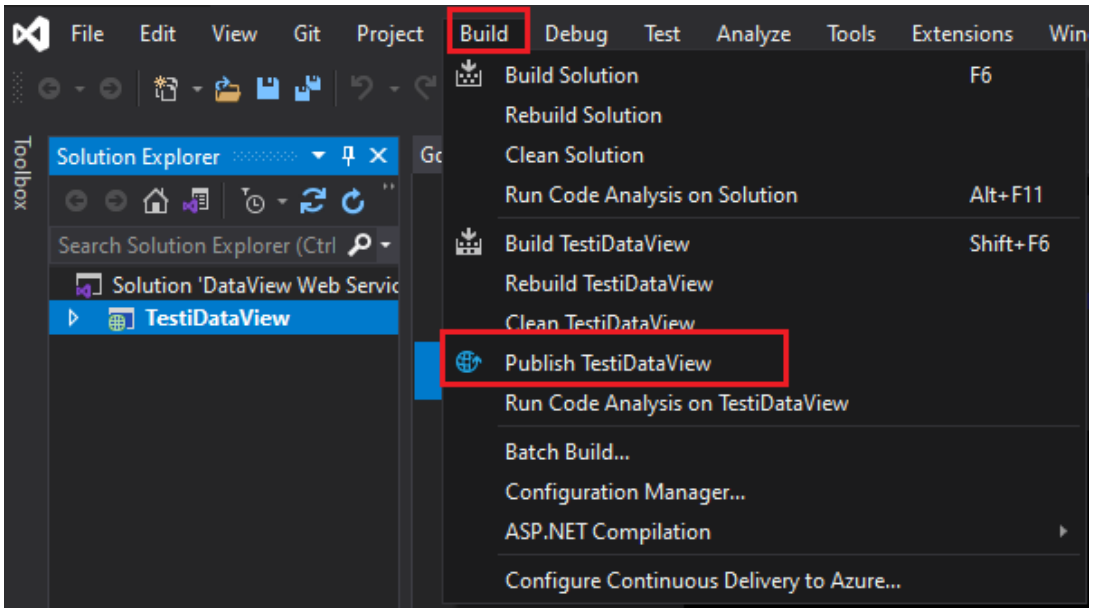
Yhteydenluontia HAVAROa varten C#-koodissa käytettiin kirjastoa System.Net.WebRequest. Ensin luotiin TLS (Transport Layer Security) protokollaa noudattava uusi httpRequest. Seuraavaksi syötettiin aikaisemmin luotu haku uuteen StreamWriter instanssiin, joka lähetti kutsun kohti HAVAROa. HAVAROn vastaus saatiin käyttämällä StreamReader instanssia, jossa voitiin käyttää funktiota ReadToEnd() lukemaan vastaus kokonaan. Tämä vastauksena tullut merkkijono muutettiin JArrayksi käyttämällä metodia JsonConvert.DeserializeObject.

HAVAROn hakua varten luotiin while-silmukka, joka suoritettiin, kunnes tapauksia kaikki tapaukset oli haettu. While-silmukassa haun alkupäivämäärä muutettiin aina viimeisimmän haetun tuloksen alkupäivämääräksi, joten kaikki tietyn aikavälin tapaukset saatiin haettua. Joka haun palautuessa kyseinen JArray käytiin JTokeneittain läpi ja jokainen JToken asetettiin talteen uuteen JArrayhyn, koska hakemisessa vanha JArray aina ylikirjoitettiin. Haettua kaikki tapahtumat, uuden JArrayn jokainen arvo käytiin läpi for-silmukassa kolmen if-ehtolauseen läpi, jotka tutkivat oliko kyseinen

arvo tapahtunut raportointijaksolla, vuoden sisällä ja luokiteltu vakavuuksittain. Mikäli arvo meni läpi jostakin if-ehtolauseesta, lisättiin kyseiseen muuttujaan yksi tapahtuma lisää. Käytyä läpi jokainen JArrayn arvo, nämä lukumääriä sisältävät arvot lisättiin JObjectiin. Lopuksi JObjectin arvot lisättiin verkkosivulle menevään julkiseen JArray muuttujaan.

4.2.4 ActiveDocs Opus Composition Server -ohjelmiston käyttäminen

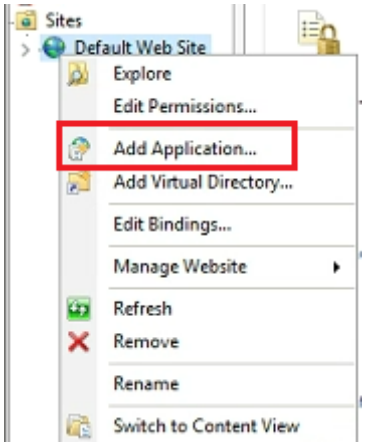
Ensimmäiseksi uutta raporttia varten Visual Studio -ympäristössä koottiin ja julkaistiin projekti painamalla Visual Studion Publish-painiketta (ks. Kuvio 8).



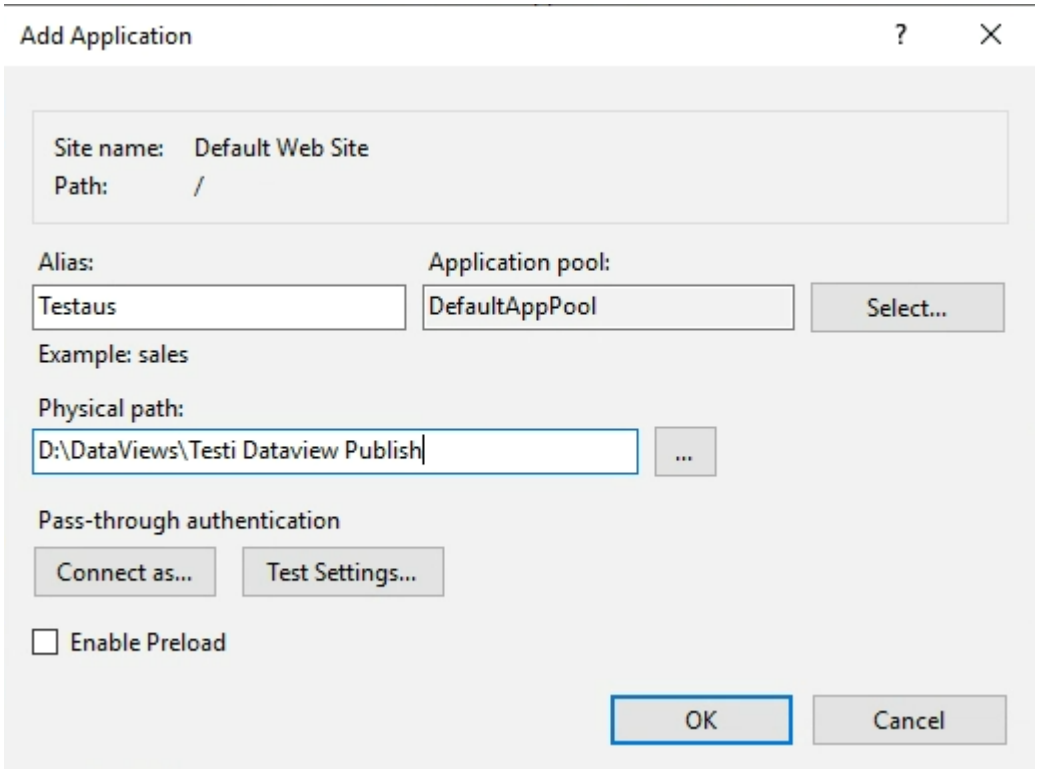
Kuvio 8. Visual Studio -ympäristössä projektin julkaiseminen

Julkaistusta projektista luotiin verkkosivu ActiveDocs Opus Composition Server -ohjelmiston IIS-palvelimella. Verkkosivu luotiin käynnistämällä ActiveDocs Opus Composition Server ja seurattiin seuraavia kohtia (ks. Kuvio 3):

1. Navigoitiin kohtaan ACTIVEDOCS ja valittiin Sites.
2. Painettiin hiiren kakkospainikkeella kohtaa Default Web Site.
3. Valittiin valikosta Add application (ks. Kuvio 9).
4. Täytettiin kenttä Alias ja valittiin kohtaan Physical path Visual Studiossa julkaistu projektikansio (ks. Kuvio 10).



Kuvio 9. IIS-palvelussa uuden verkkosivun lisäys



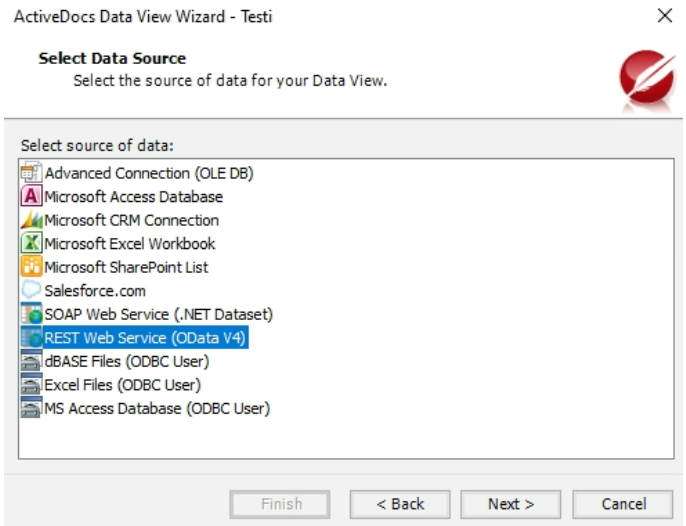
Kuvio 10. IIS-palvelussa uuden verkkosivun lisäyksen yhteydessä täytettävät kentät

IIS-palvelimen asetuksista voitiin tarvittaessa muuttaa tunnusten varmennustapaa. ActiveDocs-ohjelmisto vaati, että julkaistulla projektikansiolla oli tietyt oikeudet käyttäjälle IIS_IUSRS tietojen lukemista varten, joten ne asetettiin oikein. Mikäli päivitettiin olemassa olevalle raportille tietoja, voitiin projektikansio julkaista ylikirjoittamalla vanhassa projektikansiossa olevat tiedostot.

4.2.5 ActiveDocs Opus Content Manager -ohjelmiston käyttäminen

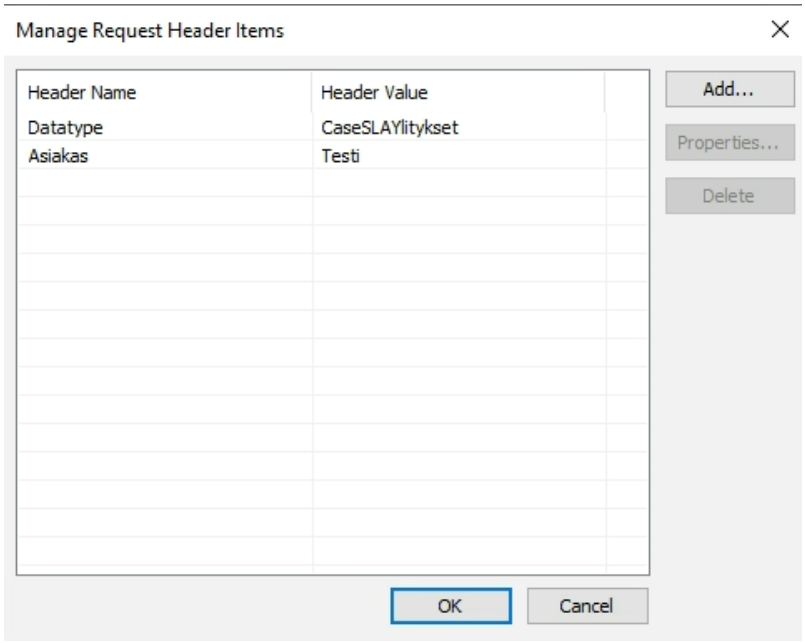
Avattaessa ensimmäistä kertaa ActiveDocs Opus Content Manager -ohjelmistoa täytyi asettaa Composition Server -ohjelmiston verkko-osoite ja nimi. Tämän jälkeen täytyi ActiveDocs-pääkäyttäjän asettaa oikeudet Content Managerissa tyypiksi Designer User. Tällöin pystyttiin muokkaamaan ja luomaan uusia raporttipohjia ja niihin liittyviä muita osia.

Content Managerissa luotiin ensimmäiseksi uutta palveluraportti varten uusi DataView. Luodessa uutta DataViewiä valittiin tietolähteeksi REST Web Service (OData V4) (ks. Kuvio 11).



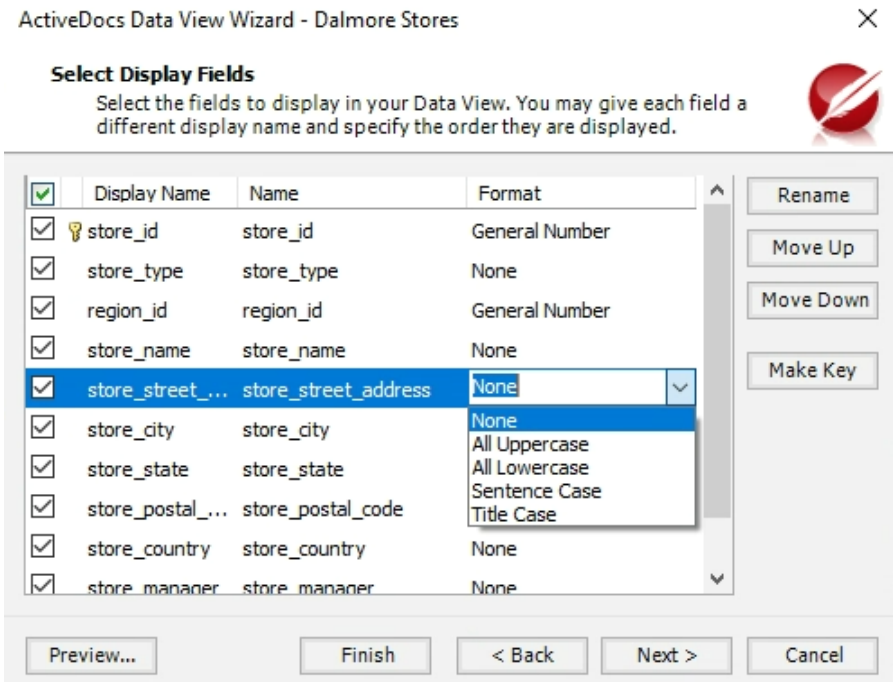
Kuvio 11. Content Managerissa DataViewin asetuksissa tietolähteen valinta

Seuraavaksi asetettiin verkkosoite, jonka alkuosa määräytyi Composition Server -ohjelmiston verkkosijainnin mukaan. Verkkosoitteen loppuosa määräytyi C#-koodissa asetettavan RoutePrefix-arvon mukaan. Verkko-osoitteen asettamisen jälkeen voitiin tarvittaessa asettaa tunnukset yhteyden luontia varten. Testailujen aikana tätä ei kuitenkaan käytetty. Verkko-osoitteen asettamisen jälkeen lisättiin otsikkoarvot (Datatype ja Asiakas), joiden avulla saatiin haettua vain tietty data tietyltä asiakkaalta verkkosivulta (ks. Kuvio 12).



Kuvio 12. Content Managerissa DataViewin asetuksissa lisätyt otsikkoarvot

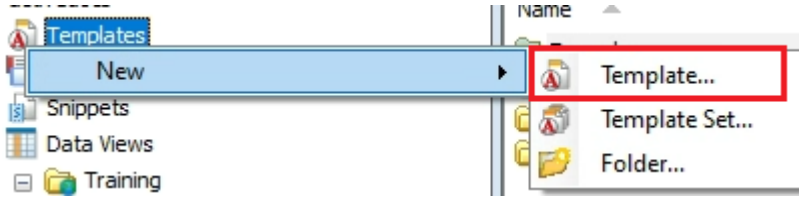
Otsikkoarvojen lisäämisen jälkeen valittiin .xml -tiedostossa asetetun datan kohde. Seuraavaksi asetettiin DataViewissä näytettävät kentät ja niiden muoto esimerkiksi All uppercase tai All lower-case (ks. Kuvio 13).



Kuvio 13. Content Managerissa DataViewissä näytettävät kentät ja niiden muoto

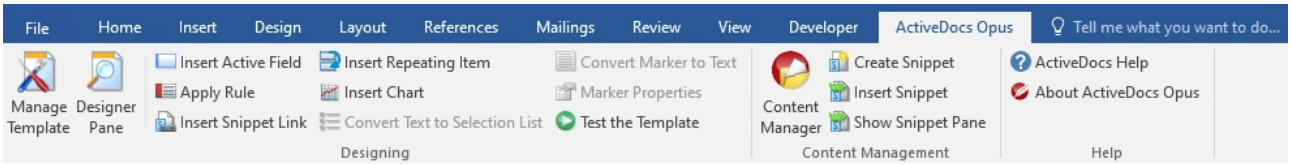
Lopuksi asetettiin vielä tarvittaessa suodatin- ja lajittelujärjestysarvot sekä DataViewin aikakatkaisun arvo halutun kokoiseksi. Yhteen DataViewiin tuotiin vain yhden tyyppistä dataa, joten DataViewejä luotiin niin monta erilaista kuin dataa haluttiin raportille.

Itse palveluraportti luotiin Content Managerin Templates -kohdassa (ks. Kuvio 14).



Kuvio 14. Content Managerissa uuden mallipohjan teko

Uuden palveluraportin pohjaksi vietiin import-toimintoa käyttäen jo käytössä ollutta palveluraporttia Word-muodossa. Tätä luotua mallipohjaa muokattiin sen jälkeen painamalla sen kohdalla hiiren oikeaa näppäintä ja valitsemalla Edit, tällöin mallipohja avautuu muokattavaksi Word-muodossa. DataViewien tiedot lisättiin mallipohjaan käyttämällä Wordiin lisättyä ActiveDocs Add-in-välilehteä (ks. Kuvio 15).



Kuvio 15. ActiveDocs Add-in-välilehti

Välilehdeltä käytettiin Manage Template -työkalua, jossa pystyttiin käyttämään Import from DataView -toimintoa DataViewien tietojen tuontiin. Tietojen tuonnin jälkeen käytettiin toimintoja Insert Active Field, Insert Repeatin Item, Insert Chart ja Apply Rule, että palveluraportti saatiin halutun näköiseksi. Lopuksi muokkaukset tallennettiin ja mallipohja julkaistiin käytettäväksi toiminnolla Check In.

Julkaistu mallipohja voitiin tämän jälkeen ajaa valmiiksi palveluraporttipohjaksi Content Managerissa komennolla Run, jolloin ActiveDocs Document Wizard avautui verkkoselaimeen. Document Wizardissa käytettiin Next-toimintoa ja tarkasteltiin raportille syötettäviä DataViewien tietoja. Lopuksi raportti luotiin Finish-toiminnolla ja ladattiin Word-muodossa jatkotäydennettäväksi. Palveluraporttipohjan sisällysluettelo ei päivittynyt automaattisesti raportin luonnin jälkeen, joten sitä varten luotiin, seuraavanlainen Word-makro (ks. Kuvio 16).

```
Sub Document_Open()
    '
    ' UpdateTableOfContents Macro
    ' Updates the first table of contents in the document
    '
        Dim toc As TableOfContents
        Dim tof As TableOfFigures
        With ActiveDocument
            .Range.Fields.Update
            For Each toc In .TablesOfContents
                toc.Update
            Next toc
            For Each tof In .TablesOfFigures
                tof.Update
            Next tof
        End With
End Sub
```

Kuvio 16. Word-makro sisällysluettelon automaattiseen päivitykseen

5 Tulokset

Työn alussa olevassa tietoperustassa tutkimuskysymyksiä käsiteltiin yleisellä tasolla ja itse tehdyssä tapaustutkimuksessa kysymyksiin vastattiin monipuolisesti. Työssä saatiin vastattua kaikkiin kolmeen aihetta rajaavaan tutkimuskysymykseen:

1. Mitä tekijöitä hyvä tietoturvavalvomon tietoturvaraportti sisältää?
2. Miten tietoturvavalvomon raportointia voidaan kehittää?
3. Miksi tietoturvavalvomon raportointia kannattaa automatisoida?

Hyvän tietoturvavalvomon tietoturvaraportin tulisi sisältää ainakin seuraavat viisi kohtaa raportointijaksolta. Ensimmäisenä keskeisimmät havainnot, sisältäen yhteenvedon tärkeimmistä tapahtumista. Toisena seurannan yhteenveto, sisältäen mitä verkkoja, laitteita ja palvelimia oli seurattu. Kolmantena häiriötilanteiden yhteenveto, sisältäen luettelon havaituista ja ratkaistuista häiriötilanteista. Neljäntenä yhteenveto uhkista, sisältäen vain vakavimmat uhat. Viidentenä suositukset, sisältäen organisaation kyberturvallisuuden tasoa parantavat toimenpiteet.

Tietoturvavalvomon raportointia voidaan kehittää selkeyttämällä raportteja, automatisoimalla, yksinkertaistamalla prosessia ja lisäämällä uutta mielenkiintoista tietoa asiakkaiden järjestelmistä. Tietoturvavalvomon raportointia kannattaa automatisoida, koska palveluraporttien tekeminen on kuukausittain toistuva työ, joka tehdään aina samaa kaavaa noudattaen. Tämä tekee työstä yksitoikkoisen. Lisäksi palveluraporttien tekijöillä on usein tärkeämpiäkin töitä, jotka tulisi hoitaa samaan aikaan työläiden raporttien kanssa.

Työn lopputuloksena oli uusi kehitetty kuukausittain asiakkaille toimitettava palveluraportti sekä pitkälle automatisoitu raportin luontiprosessi. ActiveDocs-ohjelmiston ja datalähteisiin tehtyjen liitosten ansiosta suurin osa palveluraportille tulevista tiedoista saatiin haettua automaattisesti raportin luonnin yhteydessä. Merkittävänä lopputuloksena uusi palveluraportti ja automatisoitu raportointitapa otettiin vanhan raportoinnin rinnalle käyttöön ja se tulee syrjäyttämään vanhan raportoinnin työn valmistumisen jälkeisinä kuukausina, kun mahdolliset vastaan tulevat ongelmat on korjattu.

Uudella kehitetyllä palveluraportilla tuotiin asiakasta varten selkeämmin esille heidän omien järjestelmiensä tietoturvan tilanne. Lisäksi raportilla parannettiin tärkeitä kohtia rikastamalla ja selkeyttämällä tiedon esitystapoja, erityisesti tikettien SLA-laskennan sisältävää kohtaa. Yleistä raportin tietojen järjestystä muutettiin johdonmukaisemmaksi ja täysin uutena kohtana lisättiin HAVARO-tapausten lukumäärät ja tiedot. Työllä saatiin tuotettua haluttua lisäarvoa asiakkaalle.

Osana raportoinnin kehittämistä kuului automatisointi. Automatisoimalla raportointia pystyttiin tehostamaan tietoturvavalvomon työtä. Ennen raportointiin kului aikaa noin kaksi tuntia jokaista palveluraporttia kohden. Automatisoidulla raportoinnin luontiprosessilla ja kehitetyllä palveluraportilla, raportin tekemiseen kului aikaa noin puoli tuntia. Esimerkiksi jos tehtäisiin viidelle asiakkaalle palveluraportti vanhalla tavalla, työhön kuluisi yhdeltä henkilöltä noin kymmenen tuntia ja automatisoidulla tavalla koko työhön kuluisi kaksi ja puoli tuntia. Säästetty aika suurenee, mitä enemmän asiakkaita on. Mikäli tehtäisiin 20 asiakkaalle, työhön kuluisi vanhalla tavalla noin 40 tuntia ja automatisoidulla tavalla kymmenen tuntia.

Vuodessa työn säästämät summat ovat merkittäviä. Esimerkiksi vuodessa viidelle asiakkaalle tehtävien kuukausittain toimitettavien palveluraporttien tekoon kului noin 120 tuntia ja automatisoidulla tavalla noin 30 tuntia. Viikkotyöajan ollessa 37,5 tuntia vuodessa säästyisi työaikaa kaksi viikkoa ja kaksi päivää. Vuorostaan laskiessa 20 asiakkaalla vuodessa raportointiin kului ennen noin 480 tuntia ja automatisoidulla tavalla noin 120 tuntia. Tämä tarkoittaa 37,5 tunnin viikkotyöajalla yhdeksän viikon ja kolmen päivän säästöä. Käytännössä työllä saatiin tehostettua tietoturvavalvomon raportointia merkittävästi.

6 Pohdinta

Kehitystyön tavoitteena oli kehittää käytössä olevia palveluraportteja antamaan asiakkaille parempi kuva omien järjestelmiensä tietoturvan tilanteesta sekä automatisoida kuukausittain toimitettavien palveluraporttien luontiprosessia. Työn tuloksena saatiin uusi kehitetty kuukausittain asiakkaille toimitettava palveluraportti sekä pitkälle automatisoitu raportin luontiprosessi. Tulokset olivat kokonaisuudessaan onnistuneita, kaikki asetetut tavoitteet palveluraporttien kehittämisen ja automatisoinnin suhteen saavutettiin ja toimeksiantajan palaute työstä oli kiitettävää. Merkittävä tulos oli yhdelle asiakkaalle raportointiin käytettävän ajan väheneminen noin kahdesta tunnista noin puoleen tuntiin. Laskiessa konkreettista säästön määrää, 20 asiakkaalla raportointiin vuodessa käytettävää työaikaa säästyisi kehitystyön ansiosta yhdeksän kokonaista viikkoa ja kolme päivää, joka on huomattava ajan säästö.

Ajallisen säästön seurauksena raportointia tekevien työntekijöiden työn mielekkyys kasvoi, koska turhaa manuaalista työtä vähentyi huomattavasti. Lisäksi kehitettyä palveluraporttia ei jatkossa luoda monimutkaisen luontiprosessin mukaisesti vaan suurin osa tiedoista tulee raportille automaattisesti. Kyseiset työntekijät pystyvät jatkossa käyttämään oman aikansa tehokkaammin muihin työtehtäviin ja ottamaan itselleen lisää työtehtäviä säästyneen työajan tilalle.

Opinnäytetyön aiheen valinta onnistui hyvin, sillä sitä pystyttiin rajaamaan tutkimuskysymysten avulla sopivan laajoiksi ja selkeiksi kokonaisuuksiksi. Aihe on myös jatkuvasti ajankohtainen ja tuo uutta koko alalle, sillä jatkuvasti uudet yritykset huomaavat tarvitsevansa tietoturvavalvomoa palveluna ja tällöin nykyisten olemassa olevien tietoturvavalvomoiden on pystyttävä skaalautumaan jatkuvasti suurempaan valvonnan tarpeeseen.

Työn luotettavuutta tarkasteltiin reliabiliteetin ja validiteetin avulla. Reliabiliteetilla tarkoitetaan tulosten toistettavuutta eli voidaanko työ toistaa ja päästä samaan lopputulokseen (Kananen 2015, 349). Validiteetilla tarkoitetaan oikeiden asioiden tutkimista (Kananen 2015, 343). Työssä reliabiliteetti on korkea, sillä tutkimusprosessi on kuvattu tarkasti, kattavasti ja riittävän yksityiskohtaisesti toistettavuuden näkökulmasta. Lisäksi työn reliabiliteettia nostaa lähteiden koostuminen pääasiassa luotettavista verkkolähteistä ja ammattialan tutkimusjulkaisuista. Työn validiteetti on myös korkea, koska tehdyllä tutkimuksella ja tutkimuskysymyksillä saatuihin tuloksiin oli tarkoitus päästä. Työssä tutkittiin oikeita asioita tarpeeksi laajasti.

Tutkimuseettisesti työssä onnistuttiin olemaan kertomatta asiakkaiden tai tietoturvavalvomon työntekijöiden nimiä ja liikesalaisuuksia. Erityistä huomiota täytyi kiinnittää teknisen toteutuksen tekemiseen, jotta työhön saatiin riittävän kattavasti tietoa, mutta kuitenkaan ei paljastettu organisaatioista liian yksityiskohtaisia tietoja.

Kehitystyön aikana aikaa kului huomattavasti SLA-laskujen tekemiseen koodissa, koska tiketöintijärjestelmästä oli hankalaa hakea aikamääreitä tietyille tapahtumille. Tämän lisäksi paljon aikaa kului vanhan raportin selvittelyyn ja siihen millä määrityksillä jotkin raportille tulevat tiedot on otettu. Kehitystyön kanssa samaan aikaan paranneltiin tiketöintijärjestelmän kenttien nimiä ja tämä aiheutti jonkin verran arvojen uudelleen määrittämistä integraatiota varten.

Työn aikana huomattiin, että ei välttämättä ole olemassa täysin oikeaa vastausta kysymykseen mikä on tärkeää palveluraporteilla, koska se riippuu paljon näkökulmasta mitä raportilla halutaan tietää. Esimerkiksi toiselle voi olla tärkeää saada tietoon tikettien lukumäärä ja toiselle on tärkeää tietää minkä vakavuusluokan tikettejä on tullut. Monipuolisella raportilla saadaan tuotettua paljon erilaista tietoa, mutta riski liialliselle tietomäärälle kasvaa mitä laajempi raportti on. Tällöin ei välttämättä sisäistetä tärkeimpiä kohtia raportilta, joten on tärkeää pitää myös se mielessä lisätessä uutta tietoa raportille.

Raportointia tehdään pääasiassa asiakastarpeisiin. Työn aikana kuitenkin ilmeni, että raportointia voidaan tehdä myös organisaation omiin tarkoituksiin. Tiketöintijärjestelmästä voidaan mitata tikettien käsittelyyn kuluvaa aikaa ja tämän raportoinnin avulla pystytään kehittämään ja ohjaamaan omaa toimintaa. Esimerkiksi käsittelystä luokitteluun kuluvaa aikaa voidaan mitata Tier 1 -työntekijän ensivasteen tekoajan mukaisesti, vuorostaan SLA-tavoitteiden kannalta on tärkeää tietää, kauanko aikaa kuluu kokonaisuudessaan uuden tiketin luokitteluun.

ActiveDocs-ohjelmistolla pystytään tällä hetkellä tekemään vain edellisen kuukauden palveluraportti, mutta kehityskohteena olisi muokata C#-koodia ja raportoinnin logiikkaa tukemaan minkä tahansa kuukauden palveluraportin tekoa. C#-koodissa nykyiset kovakoodatut kuukausimääritykset tulisi asettaa dynaamisiksi, jolloin kuukauden määritys tapahtuu dokumenttia luodessa ActiveDocs -ohjelmiston Document Wizard -työkalussa. Kuukauden määrityksen jälkeen kyseinen kuukausi pitäisi tuoda C#-koodiin, jossa se asetetaan dynaamiseksi kuukausimuuttujaksi, johon

voidaan sitoa kaikki koodissa olevat kellonajat. Kuukauden määritys voitaisiin toteuttaa osana C#-koodin refaktorointia eli lähdekoodin sisäisen rakenteen muuttamista toiminnallisuus säilyttäen. Tässä tapauksessa refaktorointia tehtäisiin luettavuuden sekä ohjelmakomponenttien työnjaon selkeyttämiseksi.

Myöhemmin työstettäessä useampia samantapaisia palveluraportteja eri asiakkailla voidaan tekstien ylläpidettävyyttä helpottaa ActiveDocs-ohjelmistolla. Ohjelmistossa voidaan käyttää katkelmia, jotka löytyvät ActiveDocs Opus Content Manager -ohjelmistossa englanninkielisellä nimellä Snippet. Lisäksi tietoturvavalvomon raportointia voitaisiin automatisoida vielä pidemmälle, esimerkiksi ActiveDocs-ohjelmisto tukee mahdollisuutta luoda ja lähettää dokumentti automaattisesti tiettynä päivänä. Kuitenkin niin kauan, kun palveluraportille halutaan tuottaa lisäarvoa manuaalisesta analyysistä tätä ominaisuutta ei pystytä hyödyntämään.

Jatkokehityskohtana ilmeni tarve automatisoida tekniseen kuukausittain toimitettavan palveluraportin lisäksi raportti johtotason kvartaaleittain pidettäviin kokouksiin. Tämän raportin automatisointi vaatii lisäselvittelyä ActiveDocs-ohjelmiston soveltuvuudesta luoda PowerPoint-raportti, mikäli ohjelmistolla pystytään luomaan PowerPoint-muotoinen raportti, sen tekeminen noudattaisi suurimmalta osin samaa kaavaa kuin Word-muotoisen raportin luominen. Toisena kehityskohteena olisi SIEM-tuotteelta saatavien tapahtumien hakeminen REST API -rajapinnalta ja luoda taulukoita sekä kuvaajia kategorisoimalla haettua dataa.

Palveluraporttien kehittäminen ja automatisointi jatkuu joustavasti työssä tehtyjen kehitystoimenpiteiden jälkeenkin esiin tulleiden kehitysehdotusten mukaisesti. Kehitystyön päätteeksi voidaan todeta, että tietoturvavalvomo tarvitsee jatkuvaa kehittämistä ja automatisointia pysyäkseen ketteränä ja tehokkaana jatkuvasti muuttuvassa ympäristössä. Kehitettävää riittää aina, joten kehitystyö ei välttämättä koskaan ole täysin valmis.

Lähteet

(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide. 2019. Artikkeli (ISC)²:n www-sivuilla. Viitattu 29.8.2021. https://www.isc2.org/News-and-Events/Press-Room/Posts/2019/11/06/ISC2-Finds-the-Cybersecurity-Workforce-Needs-to-Grow--145.

Barros, A., Chuvakin, A. & Belak, A. 2019. Applying Network-Centric Approaches for Threat Detection and Response. Gartnerin julkaisema tutkimus, ID G00373460. Viitattu 9.9.2021. https://www.gartner.com/en/documents/3904768.

Chuvakin, A. 2020. Back in 2015, while working on a Gartner SOC paper. Blogikirjoitus Mediumin www-sivuilla 10.9.2020. Viitattu 9.9.2021. https://medium.com/anton-on-security/back-in-2015-while-working-on-a-gartner-soc-paper-i-coined-the-concept-of-soc-nuclear-triad-8961004c734.

CISO dashboard. N.d. ServiceNow:n www-sivuilla. Viitattu 3.9.2021. https://docs.servicenow.com/bundle/rome-security-management/page/use/dashboards/application-content-packs/ciso-dashboard.html#d1300031e279.

Clippinger, D. 2017. Producing written and oral business reports: Formatting, illustrating, and presenting. New York: Business Expert Press. Viitattu 2.9.2021. https://janet.finna.fi, Ebook Central Academic Complete International Edition.

Crowley, C. & Pescatore, J. 2019. Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey. SANS Instituutin toteuttama kysely. Viitattu 8.9.2021. https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf.

Cybersecurity Incident Reporting & Dashboards. N.d. Artikkeli D3Securityn www-sivuilla. Viitattu 3.9.2021. https://d3security.com/platform/reporting-dashboards/.

Cyberthreat Defense Report. N.d. Raportti CyberEdgen www-sivuilla. Viitattu 26.8.2021. https://cyber-edge.com/cdr/.

De Groot, J. 2020. What is a Security Operations Center (SOC)? Artikkeli Digitalguardianin www-sivuilla. Viitattu 29.8.2021. https://digitalguardian.com/blog/what-security-operations-center-soc.

Demertzis, K., Kikiras, P., Tziritas, N., Sanchez, S. & Iliadis, L. 2018. The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence. Big data and cognitive computing, 2, 35. Julkaistu verkossa 22.11.2021. Viitattu 29.8.2021. https://doi.org/10.3390/bdcc2040035.

ENDPOINT DETECTION AND RESPONSE. N.d. Artikkeli F-Securen www-sivuilla. Viitattu 31.8.2021. https://www.f-secure.com/fi/business/resources/endpoint-detection-and-response.

Fielding, R. 2000. Architectural Styles and the Design of Network-based Software Architectures. Irvine: University of California, 76–85. Viitattu 12.9.2021. https://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf.

Gurman, S. 2020. A Security Operations Center (SOC) Report Template for the C-Suite. Blogikirjoitus Securityscorecardin www-sivuilla 2.9.2020. Viitattu 20.8.2021. https://securityscorecard.com/blog/security-operations-center-report-template-for-the-c-suite.

HAVARO-palvelu. 2021. Artikkeli Kyberturvallisuuskeskuksen www-sivuilla. Viitattu 12.9.2021. https://www.kyberturvallisuuskeskus.fi/fi/havaro-palvelu.

Hopeavuori, T. N.d. Raportoinnin tarkoitus. Oulun ammattikorkeakoulun opetusmateriaali. Viitattu 31.8.2021. http://www.oamk.fi/~thopeavu/materiaalit/raportoinnin_tarkoitus.html.

How report automation can improve your reporting process. N.d. Blogikirjoitus DashThis yrityksen www-sivuilla. Viitattu 20.8.2021. https://dashthis.com/blog/how-report-automation-can-improve-your-reporting-process/.

INSTA ON TURVALLISEN JA KILPAILUKYKYISEN YHTEISKUNNAN RAKENTAJA JA KEHITTÄJÄ. N.d. Instan www-sivuilla. Viitattu 16.10.2021. https://www.insta.fi/tietoa-meista.

Intoduction to C#. 2019. Artikkeli Geeksforgeeksin www-sivuilla. Päivitetty 17.12.2019. Viitattu 12.9.2021. https://www.geeksforgeeks.org/introduction-to-c-sharp/.

Introducing JSON. N.d. JSONin www-sivuilla. Viitattu 10.9.2021. https://www.json.org/json-en.html.

IT-alan kehitys on johtanut. N.d. Blogikirjoitus Motadatan www-sivuilla. Viitattu 12.9.2021. https://www.motadata.com/fi/blog/network-monitoring-basics/.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas: Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylän ammattikorkeakoulu, 343, 349. Viitattu 28.10.2021. https://janet.finna.fi, Booky.

Kurittu, K. 2018. Yritysvastuuraportointi: Kiinnostavan viestinnän käsikirja. Toinen painos. Helsinki: Alma Talent Pro, 154. Viitattu 2.9.2021. https://janet.finna.fi, Alma Talent Pro.

Kyberturvallisuuden sanasto. 2018. Sanastokeskuksen sanastojulkaisu TSK 52. Helsinki: Huoltovarmuuskeskus. Viitattu 29.8.2021. https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf.

Mikä on SOC ja miksi sellainen tarvitaan? 2017. Combitech Finlandin artikkeli Mediumin www-sivuilla. Viitattu 24.9.2021. https://medium.com/@combitech/mik%C3%A4-on-soc-ja-miksi-sellainen-tarvitaan-a0df93609118.

Mikä on tiketöinti? N.d. Tiketöinnin www-sivuilla. Viitattu 24.9.2021. https://tiketointi.fi/mika-on-tiketointi/.

Miksi tiketöinti? N.d. Tiketöinnin www-sivuilla. Viitattu 2.10.2021. https://tiketointi.fi/miksi-tiketointi/.

Nanopoulos, R. 2017. What Is Security Automation? Artikkeli Rapid7:in www-sivuilla 8.11.2017. Viitattu 1.9.2021. https://www.rapid7.com/resources/wbw-security-automation/.

OData. N.d. ODatan www-sivuilla. Viitattu 12.9.2021. https://www.odata.org/.

Overby, S., Greiner, L. & Paul, L. 2017. What is an SLA? Best practices for service-level agreements. Artikkeli CIO:n www-sivuilla 5.7.2017. Viitattu 12.9.2021. https://www.cio.com/article/2438284/outsourcing-sla-definitions-and-solutions.html.

Sampat, P. 2019. Cyber Security Operations Center (CSOC), What it might bring to an organisation - the rudiments! Artikkeli LinkedIn www-sivuilla 30.6.2019. Viitattu 29.8.2021. https://www.linkedin.com/pulse/cyber-security-operations-center-csoc-what-might-bring-payal-sampat/.

Second Annual Study on the Economics of Security Operations Centers: What is the True Cost for Effective Results? 2021. Ponemon Instituutin julkaisema tutkimusraportti, 2. Viitattu 7.11.2021. https://ss-usa.s3.amazonaws.com/c/308480999/media/17666138faf35490806660815230382/rpt-ponemon-institute-second-annual-study-economics-of-the-soc-2021.pdf.

Sheikh, A. 2020. Comptia security+ certification study guide: network security essentials. Berkeley, California: Apress L. P. Viitattu 31.8.2021. https://janet.finna.fi, Skillsoft Books ITPro.

Sobers, R. 2021. 134 Cybersecurity Statistics and Trends for 2021. Artikkeli Varonis -yrityksen www-sivuilla 16.3.2021. Viitattu 20.8.2021. https://www.varonis.com/blog/cybersecurity-statistics/.

SOC, SIEM, MDR, EDR… what are the differences? 2021. Blogikirjoitus Orange Cyberdefensen www-sivuilla 5.1.2021. Viitattu 31.8.2021. https://orangecyberdefense.com/be/blog/managed-detection-response/soc-siem-mdr-edr-what-are-the-differences/.

Soveltava tutkimus. N.d. Käytännön fysiikan www-sivuilla. Viitattu 21.8.2021. http://www04.edu.fi/kaytannonfysiikka/fysiikka_soveltava_tutkimus.asp.

The Modern Security Operations Center, SecOps and SIEM: How They Work Together. N.d. Artikkeli Exabeamin www-sivuilla. Viitattu 30.8.2021. https://www.exabeam.com/siem-guide/the-soc-secops-and-siem/.

Tietotekniikan termitalkoot. 2014. Sanastokeskuksen www-sivuilla. Viitattu 26.8.2021. http://www.tsk.fi/tsk/termitalkoot/fi/haku-266.html.

Tutkimus- ja kehittämistoiminta. N.d. Tilastokeskuksen www-sivuilla. Viitattu 21.8.2021. https://www.stat.fi/meta/kas/t_ktoiminta.html#tab2.

Vacca, J. 2014. Network and system security. Toinen painos. Waltham, Mass: Academic Press, 20–21, 103. Viitattu 31.8.2021. https://janet.finna.fi, ProQuest Ebook Central.

Vielberth, M., Böhm, F., Fichtinger, I. & Pernul, G. 2020. Security Operations Center: A Systematic Study and Open Challenges. Kahdeksas painos. Institute of Electrical and Electronics Engineers IEEE. Viitattu 9.9.2021. https://doi.org/10.1109/ACCESS.2020.3045514.

Vuollet, P. 2018. Artikkeli Stackifyn www-sivuilla. Viitattu 12.9.2021. https://stackify.com/iis-web-server/.

Welcome to ActiveDocs. N.d. ActiveDocsin www-sivuilla. Viitattu 20.8.2021. https://www.active-docs.com/product/.

Welcome to the Visual Studio IDE. 2021. Artikkeli Microsoftin www-sivuilla. Viitattu 12.9.2021. https://docs.microsoft.com/en-us/visualstudio/get-started/visual-studio-ide?view=vs-2019.

What is a Security Operations Center (SOC)? N.d.a. Artikkeli McAfeen www-sivuilla. Viitattu 30.8.2021. https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html.

What is a Security Operations Center (SOC)? N.d.b. Artikkeli Microfocuksen www-sivuilla. Viitattu 29.8.2021. https://www.microfocus.com/en-us/what-is/security-operations-center.

What is a Security Operations Center (SOC)? N.d.c. Artikkeli Splunkin www-sivuilla. Viitattu 30.8.2021. https://www.splunk.com/en_us/data-insider/what-is-a-security-operations-center.html.

What is ASP.NET? N.d. Artikkeli Microsoftin www-sivuilla. Viitattu 12.9.2021. https://dotnet.microsoft.com/learn/aspnet/what-is-aspnet.

What is GitLab? N.d. GitLabin www-sivuilla. Viitattu 23.9.2021. https://about.gitlab.com/what-is-gitlab/.

What is UEBA? Definition and Benefits. N.d. Artikkeli FireEye:n www-sivuilla. Viitattu 31.8.2021. https://www.fireeye.com/products/helix/what-is-ueba.html.

Zaharia, A. 2021. 300+ Terrifying Cybercrime and Cybersecurity Statistics (2021 EDITION). Artikkeli Comparitech:n www-sivuilla, päivitetty 29.6.2021. Viitattu 26.8.2021. https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/.

Zimmerman, C. 2014. Ten Strategies of a World-Class Cybersecurity Operations Center. MITRE. Viitattu 30.8.2021. https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf.