

Pauli Pietikäinen

Kulunvalvonnan yhdistäminen CSOC- valvontaan

LOIHDE TRUST

Tradenomi (AMK)

Tietojenkäsittelyn
koulutusohjelma

Syksy 2021



**KAMK • University
of Applied Sciences**

Tiivistelmä

Tekijä(t): Pauli Pietikäinen

Työn nimi: Kulunvalvonnan yhdistäminen CSOC-valvontaan

Tutkintonimike: Tradenomi (AMK), tietojenkäsittelyn koulutusohjelma

Asiasanat: SIEM- ja SOAR-järjestelmät, kulunvalvonta, fyysinen- ja digitaalinen turvallisuus, CSOC

Toimeksiantona oli liittää kulunvalvontajärjestelmä Security Incident and Event Management (SIEM)-järjestelmään. Tällä liitoksella oli tarkoitus tuoda fyysisen turvallisuuden kulunvalvontadataa osaksi Cyber Security Operations Center (CSOC)-toiminnassa toteutettavaa tietoturva- ja valvontaa. Toimeksiantaja halusi selvittää, miten fyysisen ja digitaalisen turvan yhdistämisellä voitaisiin tehostaa kyberturvallisuuden valvonnassa suoritettavaa identiteetin turvaamista, ja siten tuottaa lisäarvoa asiakkaille. Tästä aiheesta ei olla vielä tehty monia julkaisuja tai ratkaisuja suomen kielellä, ja aihe on muutenkin tuore tietoturvatoinnissa.

Opinnäytetyön toimeksiantaja on Loihde Trust Oy, joka on osa Loihde-konsernia. CSOC on Loihde-konsernin kyberturvallisuuden valvontaa tuottava tiimi. Opinnäytetyö tehdään osana toimeksiantajan yksi turvallisuus-kehitysprojekti ja sisäistä kehitystyötä.

Teoriaosuudessa esitellään kulunvalvontateknologian ja digitaalisen turvallisuuden periaatteita CSOC-toiminnan näkökulmasta, sekä mitä lisäarvoa niiden yhdistäminen SIEM-järjestelmässä voi tuottaa. Tarkemmin perehdytään myös siihen, miten kulunvalvontadataa voidaan auttaa CSOC-analyytikkoja tutkimaan ja reagoimaan tietoturvatapahtumiin.

Käytännönsuosuuksia kuvaa prototyyppitaso toteutusta lokiliitoksesta järjestelmien välillä, joka luotiin toimeksiantajan testiympäristössä. Kulunvalvontajärjestelmästä luotiin yhteys SIEM-järjestelmään. Kulunvalvontadatan pohjalta luotiin alustavia tietoturvasääntöjä, joilla havainnollistettiin liitoksen toimintaa. Lisäksi opinnäytetyön tekemisessä otettiin huomioon dokumentaatio jatkokehityksen kannalta. Dokumentaatiota tullaan käyttämään jatkokehityksessä, jos toimeksiantaja kokee sen mielekkääksi.

Opinnäytetyön käytännönsuosuuksissa esiintyvät tuotteet (kulunvalvonta ja SIEM-järjestelmät) on määritellyt toimeksiantaja eikä niitä esitellä nimellä salassapitosyistä. Myöskään toimeksiantajalle tuotettua tarkempaa dokumentaatiota ei esitetä opinnäytetyön yhteydessä.

Abstract

Author(s): Pauli Pietikäinen

Title of Publication: Integrating Physical Access Control Data into CSOC-Monitoring

Degree Title: Bachelor of Business Administration, Business Information Technology

Keywords: SIEM- and SOAR- platforms, Access Control, Physical security, Information security, CSOC

The objective of this Bachelor's thesis was to develop an integration between a physical access control system and Security Incident and Event Management-platform (SIEM). The purpose of this integration was to bring data from the physical access control systems to be used in information security monitoring performed by Cyber Security Operations Center (CSOC). The client wanted to investigate how the combination of physical and digital security could be used to enhance identity protection efforts carried out by a cybersecurity team. There are not many Finnish publications or solutions about this subject, and it is rather new in the cybersecurity space overall.

The thesis was commissioned by Loihde Trust Oy, which is part of Loihde Group. Loihde Trust has cybersecurity team that produces cybersecurity monitoring services. The thesis was made as a part of Loihde Trust's "yksi turvallisuus"-development project.

The theoretical part presents principles of physical access control and digital security and how much added value combining their data can create, from the viewpoint of a cyber security operations center. The more in-depth focus is on how data from physical access control system can be used to help a CSOC analyst to investigate and respond to information security incidents.

The practical part illustrates how a proof of concept was made of the log integration between the two systems. This was implemented with tools and demo environment that Loihde Trust provided. The log from the physical access control system was used to make preliminary rules to demonstrate the functionalities of this integration. Part of the thesis was also to provide documentation of the project that can be used in further development.

Most of the products and solutions that appear in the proof of concept, as well as the documentation about it, will be obfuscated or not named due to the secrecy requirements of the project.

Sisällysluettelo

| | | |
|-------|--|----|
| 1 | Johdanto..... | 4 |
| 2 | Toimeksianto ja kehitysongelma..... | 5 |
| 2.1 | Kehitysongelma..... | 5 |
| 3 | Kyberturvallisuus tänä päivänä | 7 |
| 3.1 | Kyberrikollisuuden torjunta | 8 |
| 4 | Järjestelmien ja käsitteiden esittely..... | 10 |
| 4.1 | SIEM | 10 |
| 4.2 | SOAR | 12 |
| 4.3 | Kulunvalvonta | 13 |
| 4.4 | Pääsynvalvonta | 13 |
| 4.5 | Käyttöoikeuksien hallinta | 14 |
| 4.5.1 | Autentikointi | 14 |
| 4.5.2 | Auktorisointi | 15 |
| 4.5.3 | Käytön tilastointi..... | 16 |
| 4.6 | Kulunvalvontakäytäntö..... | 16 |
| 4.7 | MITRE ATT&CK..... | 17 |
| 5 | Toteutussuunnitelma käytännönsuudessa..... | 18 |
| 5.1 | Integraatit | 18 |
| 5.2 | Kulunvalvontajärjestelmän yhdistäminen SIEM-järjestelmään..... | 19 |
| 5.3 | Tavoitteita | 20 |
| 5.3.1 | Ehdollinen pääsy | 20 |
| 5.3.2 | Esimerkki säännöt | 21 |
| 5.3.3 | Datan esitys analyytikolle | 21 |
| 5.3.4 | Dokumentaatio | 22 |
| 6 | Käytännönsuuden toteutus | 23 |
| 6.1 | Valittu tapa toimia ja sen kuvaus..... | 23 |
| 6.2 | Logstash -keräin | 24 |
| 6.2.1 | Lokin kohde..... | 24 |

| | | | |
|-----|-------|---|----|
| | 6.2.2 | Lokin lähde | 25 |
| | 6.2.3 | Lokiliikenteen salaus | 26 |
| 6.3 | | Lokituksen toimivuuden testaus | 27 |
| | 6.3.1 | Denied entries in different locations -sääntö | 27 |
| 7 | | Tulokset | 29 |
| 8 | | Pohdinta | 30 |
| | 8.1 | Opinnäytetyön onnistumisen arviointi | 30 |
| | 8.2 | Kannattavuus | 30 |
| | 8.3 | Jatkosuunnitelmat | 30 |
| | 8.4 | Mitä opittiin ja mitä tekisin eri tavalla | 31 |

Symboliluettelo

- AAD Azure Active Directory. Microsoftin laajentama versio perinteisestä Active Directory-palvelusta, joka kattaa myös Microsoftin Azure-pilvipalvelun toiminnallisuudet.
- AD Active Directory. Microsoftin Windows-ympäristöjen käyttäjätietokanta ja hakemistopalvelu.
- CSOC Cyber Security Operations Center valvoo organisaation digitaalista tietoturvaa.
- IOC Indicators of Compromise. Tietoturvauhista tiedetyt vaarantumisen merkit.
- Playbook SOC-toiminnassa yleisesti käytetty nimitys SOAR-järjestelmän, tai muun automaatiojärjestelmän automaatioista.
- SIEM Security Information and Event Management. Järjestelmä, jolla etsitään haitallista toimintaa sinne vietävästä lokidatasta.
- SOAR Security Orchestration, Automation and Response. Järjestelmä, jolla voidaan automatisoida tietoturvalvontaa ja toimia.

1 Johdanto

Opinnäytetyön aiheena oli liittää kulunvalvontajärjestelmä Security Incident and Event Management (SIEM)-järjestelmään. Tällä liitoksella oli tarkoitus tuoda fyysisen turvallisuuden kulunvalvontadataa osaksi Cyber Security Operations Center (CSOC)-toiminnassa toteutettavaa tietoturva- ja valvontaa. Toimeksiantaja halusi selvittää, miten fyysisen ja digitaalisen turvan yhdistämisellä voitaisiin tehostaa kyberturvallisuuden valvonnassa suoritettavaa identiteetin turvaamista, ja siten tuottaa lisäarvoa asiakkaille. Tästä aiheesta ei ole vielä tehty monia julkaisuja tai ratkaisuja suomen kielellä, ja aihe on muutenkin tuore tietoturva- ja valvontatoiminnassa.

Teoriaosuudessa esitellään kulunvalvontateknologian ja digitaalisen turvallisuuden periaatteita CSOC-toiminnan näkökulmasta, sekä mitä lisäarvoa niiden yhdistäminen SIEM-järjestelmässä voi tuottaa. Tarkemmin perehdytään myös siihen, miten kulunvalvontadatalle voidaan auttaa CSOC-analyytikkoja tutkimaan ja reagoimaan tietoturvatapahtumiin.

Käytännönosuus kuvaa prototyyppitason toteutusta lokiliitoksesta järjestelmien välillä, joka luotiin toimeksiantajan testiympäristössä. Kulunvalvontajärjestelmästä luotiin yhteys SIEM-järjestelmään. Kulunvalvontadatan pohjalta luotiin alustavia tietoturvasääntöjä, joilla havainnollistettiin liitoksen toimintaa. Lisäksi opinnäytetyön tekemisessä otettiin huomioon tuleva jatkokehitys dokumentaation kannalta. Dokumentaatiota tullaan käyttämään jatkokehityksessä, jos toimeksiantaja kokee sen mielekkääksi.

2 Toimeksianto ja kehitysongelma

Toimeksiantaja on Lohde Trust Oy. Lohde Trust Oy on fyysisen ja digitaalisen turvallisuuden palveluita tuottava suomalainen Lohde-konserniin kuuluva yritys. Vuonna 2020 Lohde-konsernin henkilöstön lukumäärä oli 714 ja liikevaihto 106,8 M€. Lohde-konserniin kuuluu Lohde Trustin lisäksi Lohde Advisory-, Lohde Analytics ja Lohde Factor -tytäryhtiöt, jotka tuottavat mm. digitaalisen kehittämisen palveluita, kuten data-analytiikan ja tiedolla johtamisen palveluita sekä konsultointia. Lohde-konserni suoritti syksyllä 2021 brändimuutoksen vanhasta Viria-brändistä. (Viria Oyj Tilinpäätöstiedote 2021.)[1]

Opinnäytetyön toimeksianto tulee Lohde Trust -yhtiön ”Yksi turvallisuus” -hankkeesta, jossa pyritään helpottamaan tietoturvan toteutusta yhdistämällä tietoturvan fyysisiä ja digitaalisia puolia helpommaksi kokonaisuudeksi. Näin parannetaan toimeksiantajan kykyä turvata asiakkaiden henkilöstöä sekä digitaalisia ja fyysisiäkin resursseja kokonaisuutena.

Toimeksiantona oli kehittää toimeksiantajan Cyber Security Operations Centerin (CSOC) Security Information and Event Management eli SIEM-järjestelmään prototyyppitason ominaisuus, jolla CSOC-tiimin näkyvyys saadaan yltämään myös fyysistä kulunvalvontaa koskevaan dataan. Tälle datalle luodaan havainnollistavia esimerkkikäyttötarkoituksia SIEM-järjestelmään. Lisäksi tehtävänä oli arvioida käyttötarkoitusten hyödyllisyyttä SOC-valvonnan näkökulmasta.

Toimeksianto toteutettiin kokonaisuudessaan toimeksiantajan määräämillä järjestelmillä, toimeksiantajan tarjoamassa testiympäristössä. Tämän toimeksiannon tulosten pohjalta toimeksiantaja harkitsee jatkokehityksen mahdollisuuksia.

2.1 Kehitysongelma

Toimeksiantaja haluaa kehittää asiakkaille tarjoamansa palvelun laatua. Samalla voidaan tutkia, voidaanko fyysisten ja digitaalisten turvallisuustuotteiden keräämää dataa yhdistämällä luoda tarkempaa uhkakuvaa asiakkaan ympäristöstä, sekä selvittää millaisia etuja se tuo tietoturvatapahtumien tutkintaan. Aihe on varsin tuore, koska kulunvalvonta dataa ei yleisesti

käsitellä suoraan SIEM-järjestelmässä, tai kyseistä dataa ei käytetä sääntötasolla yhdessä tavanomaisen digitaalisen tietoturvadatan kanssa.

Käyttäjien identiteettiin perustuvien riskien tunnistus on keskiössä CSOC-toiminnassa, koska se on yleisimpiä hyväksikäyttökohteita. Käyttäjien identiteettien hyväksikäytöllä voidaan saavuttaa ensimmäinen jalansija kohdeympäristössä, jonka kautta jatkohyväksikäyttö mahdollistuu. Tällaiset hyväksikäyttöyritykset pyritään torjumaan mahdollisimman varhaisessa vaiheessa ja kulunvalvontadatasta, eli fyysisenturvallisuuden datasta, voidaan mahdollisesti havaita jotain, mikä muilta järjestelmiltä jää huomaamatta.

3 Kyberturvallisuus tänä päivänä

Kyberturvallisuus on viime vuosina noussut yhä enemmän esille valtamediassa. Erityisesti koronapandemian aiheuttama etätyötrendi on laittanut organisaatiot pohtimaan digitaalisenturvallisuuden menettelyjä uudestaan. Kyberrikollisuus on myöskin noussut kasvuun mm. ”Cybercrime as a service” (Suom. Kyberrikollisuus palveluna) toimintamallien takia, jossa kyberrikolliset myyvät kehittämiään haittaohjelmia eteenpäin muille rikollisille.

Ransomware- eli kiristykseen käytettävät haittaohjelmat ovat lisänneet kyberrikollisuustoimintaa rahallisen kannattavuutensa takia. Kiristyshaittaohjelman onnistuneesti levittänyt taho estää uhrin pääsyn omiin tietojärjestelmiin, ennen kuin tämä on maksanut kiristäjän vaatimat lunnaat. Kiristyshaittaohjelmat voivat pysäyttää kokonaisen organisaation toiminnan, mikäli ne pääsevät leviämään onnistuneesti. Tästä voidaan nostaa esimerkeiksi Colonial Pipeline Yhdysvalloista ja Coop-kauppaketju naapurimaastamme Ruotsista.

Colonial Pipeline toimittaa bensiiniä 5 500 mailin pituisen putkistojärjestelmänsä avulla jopa 50-miljoonalle amerikkalaiselle. Kiristyshaittaohjelma iski yrityksen verkkoon 29. huhtikuuta 2021, jonka jälkeen yritys joutui sulkemaan toimituksensa useammaksi päiväksi ja päätyi maksamaan kiristäjän vaatiman 4,4 miljoonan dollarin lunnaat. Hyökkäyksellä oli suuri vaikutus bensiinin hintaan ja Yhdysvaltojen itärannikon infrastruktuurin toimivuuteen. [2]

Coop Sweden on ruotsissa toimiva kauppaketju, joka joutui heinäkuussa 2021 myöskin kiristyshaittaohjelman uhriksi. Haittaohjelma levisi yritykseen ohjelmistoyritys-Kaseyan välittämän ohjelmiston kautta, jota hyökkääjät käyttivät haittaohjelmisto levitykseen. Kauppaketju joutui sulkemaan yli 800 liikettä Ruotsissa hyökkäyksen takia.[3]

Suomessakaan ei olla säästytty kyberrikollisuudelta. Loppuvuodesta 2020 tuli ilmi tietomurto, jossa Psykoterapiakeskus Vastaamolta varastettiin sensitiivistä dataa, jota käytettiin kiristykseen. Tämä tapaus on vaikuttanut sittemmin myöskin asiakastietolain kiristämiseen Suomessa, eli sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevaan lakiin. [4]

Kiristyshaittaohjelmat näkyvät helposti normaalinkin ihmisen arjessa yllä kuvattujen esimerkkien mukaisesti. Ne keräävät myös paljon uutisotsikoita laajamittaisten vaikutusten takia. Kiristyshaittaohjelmien kohdalla pitää muistaa, että ne ovat kyberhyökkäyksen viimeisimpiä

vaiheita. Näihin ei ole yleensä helppo päästä, vaan tätä on edeltänyt pitkälinen ”hyökkäysketjuksi” kutsuttu prosessi. Hyökkäysketjun suunnittelu ja toteutus voivat vaatia paljon aikaa ja onnea hyökkääjän puolelta, mikäli kohdeorganisaation tietoturvaasiat ovat ajan tasalla. Hyökkäysketjujen tunnistamiseen perehdytään seuraavassa osiossa.

3.1 Kyberrikollisuuden torjunta

Tietoturvahkien kasvun myötä tietoturvaa joudutaan jatkuvasti kehittämään. Jatkuvassa kehityksessä ovat mukana niin tietoturvapalveluja tarjoavat yritykset kuin myös avoimien lähteiden tiedustelu -yhteisöt (Eng. Open Source Threat Intelligence, OSINT). Näiden yhteisöjen peruseriaatteena on jakaa ilmaista dataa omista tietoturvalöydöksistä ja -havainnoista muille yhteisön jäsenille ja saada samalla itse ilmaista tietoa muiden havainnoista. Tällaisten laajojen jakeluverkostojen ansiosta uudet tietoturvaohjelmat, kuten haittaohjelmat ja haavoittuvuudet, on entistä helpompi tunnistaa nopeasti ja maailmanlaajuisesti.

Yleisimpiä jaettuja tietoja ovat vaarantumisen merkit (Eng. Indicators of compromise, IOC) [5]. Ne ovat merkkejä, joita käytetään forensiikassa tunnistamaan tietoturvaloukkauksissa käytettyjä haittaohjelmia, tekniikoita tai tietoturvahaavoittuvuuksia. Perinteisesti nämä voivat olla esimerkiksi: IP-osoitteita, joista lähetetään tai jotka vastaanottavat tietoliikennettä; tiedostopolkuja, joihin tehdään muutoksia; kirjautumistietoja tai mitä tahansa anomaliaita infrastruktuurin toiminnassa. Tietoturvatapahtumien tutkimuksessa tämä nopeuttaa huomattavasti haitallisten tapahtumien tunnistusta, koska tiedetään muidenkin joutuneen samanlaisen tapauksen kohteeksi. Tämä myös voi nopeuttaa vastatoimien tekoa, jos tekijä voidaan tunnistaa samaksi hyökkääväksi tahoksi, jonka lisäksi ennakolta tiedetään miten he yleensä toimivat. Myös maksullisia tietoturvapalveluja tarjoavat yritykset ovat useasti mukana jossain määrin avoimien lähteiden tiedustelussa.

Tietoturvaluotteita tuottavat yritykset pyrkivät kehittämään omia järjestelmiään tunnistamaan uhkia entistä tehokkaammin ja varmemmin. Tekoälyä on pyritty valjastamaan poikkeavuuksien etsintään niin verkkoliikenteestä kuin ohjelmien toiminnasta. Tekoäly on osoittautunut tehokkaaksi etenkin uusien uhkien tunnistuksessa, koska se ei vaadi ennalta tiedettyjä merkkejä

vaarantumisesta, vaan pystyy näin käsittämään suojeltavan alueen kokonaisuutena paremmin kuin perinteiset ratkaisut.

Kyberrikollisuuden torjumisessa on tärkeää kouluttaa henkilöstöä tietoturva-asioissa ja toteuttaa tehokasta tietoturvasuunnitelmaa. Omaa ympäristöä joutuu myöskin suojaamaan tietoturvatyökaluilla, kuten: ajantasaisilla päätelaitesuojausohjelmilla (Eng. EDR. Endpoint detection and response) (esimerkiksi antivirusohjelmat), palomureilla (Eng. Firewall), verkon havainnointi- ja vastaiskutyökaluilla (Eng. Network Detection and response, NDR). Näiden lisäksi on monia muita ratkaisuja eri käyttötarkoituksiin, ja yleensä tietoturvaohjelmistoja tuottavat yrityksen yhdistelevät ja tarjoavat suojausta useammassa eri kategoriassa.

Päätavoite laaja-alaiselle suojaukselle on kerätä mahdollisimman laaja näkymä organisaatiosta, jotta uhkien tunnistaminen on mahdollista hyökkäystavasta riippumatta. Tietoturvasovellusten lukumäärän kasvaessa niiden valvontaan vaadittavien resurssien määrä kasvaa. Tätä ongelmaa varten on luotu SOAR- ja SIEM-järjestelmiä, jotka mahdollistavat tietoturvatapahtumien tutkinnan automatisoinnin ja useamman eri järjestelmän yhdistämisen samaan näkymään. SOAR- ja SIEM-järjestelmiä kuvataan syvemmin kappaleissa 3.1 ja 3.2.

Suurien organisaatioiden tietoturvan valvontaan ei edes tehokkaalla SOAR-järjestelmällä riitä aikaa perinteisen IT-osaston puolelta, vaan valvonnasta vastaamaan perustetaan erikseen SOC-tiimi, jonka tehtävä on erityisesti tietoturvan valvonta. Erillisen SOC-tiimin pyörittäminen voi olla kuitenkin taloudellisesti organisaation koosta riippuen kallista, joten olemassa on myöskin SOC-palvelun tarjoajia, jotka valvovat useamman organisaation tietoturvaa yhtäaikaaisesti.

Aktiivisten toimien lisäksi yhteiskuntatasolla tietoturvaan vaikuttaa lainsäädäntö, jolla voidaan vaatia tietyllä alalla toimivia organisaatioita täyttämään tietyt vaatimukset tietoturvan suhteen. Lisäksi on myöskin olemassa tietoturvasertifiointejä, joita varten organisaation tietoturvatoteutus auditoidaan eli tarkistetaan täyttääkö se sertifiointin asettamat vaatimukset. Sertifioinneilla voidaan osoittaa yhteistyökumppaneille, että organisaatio on todistetusti hoitanut tietoturvansa tietyllä tasolla kriteereiden mukaisesti.

4 Järjestelmien ja käsitteiden esittely

Digitaalisen ja fyysisen turvallisuuden järjestelmät ovat alkaneet muistuttaa toisiaan enemmän maailman digitalisaation myötä. Kummallakin järjestelmällä kerätään tietoja, jotka voivat liittyä samoihin tietoturvatapahtumiin. Tietoturvatapahtuma on tietojärjestelmän tai organisaation toimintojen tapahtuma, jonka seurauksena tietojen tai palvelujen tila on muuttunut ja joka saattaa vaikuttaa tietoturvaan. Tämän takia on tärkeää organisaation tietoturvan kannalla luoda yhtenäisempää tietoturvapoliittikkaa, jotta organisaation toimintaan vaikuttavissa tietoturvatapahtumissa saadaan uusin tieto niin tarkasti ja niin helppossa muodossa kuin mahdollista.

Fyysisen turvallisuuden laitteistot vaativat itsessään jo digitaalisen turvallisuuden valvontaa, koska ne toimivat tietokoneilla ja käyttävät yrityksen tietoliikenneverkkoja, jotka on syytä turvata. Toisaalta myös digitaalisen turvallisuuden käyttämät konesalit vaativat fyysisen turvan tarjoamaa suojaa estämään asiattonta kulkua. Lyhyesti sanottuna fyysisillä ja digitaalisilla järjestelmillä on suhde, jossa toista voidaan päästä hyväksikäyttämään toisen kautta ja molempien suojaus vaatii täten toinen toistaan.

Toimeksiantajan CSOC-tiimi tekee tietoturvalvontaa asiakkaille. CSOC-tiimi kerää tietoturvaan liittyvää dataa asiakkailta useiden eri tuotteiden ja ratkaisujen avulla. Yksi näistä ratkaisuista on SIEM-järjestelmä, jolla voidaan suorittaa tehokasta lokitietoihin perustuvaa tietoturvalvontaa. SIEM-järjestelmään perinteisesti lähetetään digitaalisten tuotteiden tietoturva-lokeja, joista etsitään tietoturvapoikkeamia erilaisten sääntöjen avulla.

4.1 SIEM

SIEM-järjestelmä eli Security Information and Event Management (tietoturva -informaation ja -tapahtumien hallinta) mahdollistaa reaaliajassa tapahtuvan laajan tietoturvalvonnin toteutuksen, tietoturvatapahtumien visualisoinnin ja tutkimisen. SIEM-järjestelmä on tietoturvajärjestelmä, mihin kerätään keskitetysti lokitietoja erilaisista tietojärjestelmä lähteistä.

Esimerkkilähteitä ovat mm. Erilaiset palvelimet, palomuurit ja päätelaitteet. Myöskin mahdollisista tietoturvasovelluksista, kuten antivirusohjelmista, voidaan ottaa lokeja talteen. [6]

Loki on tekstimuotoon tallennettu tieto siitä, mitä tietojärjestelmässä on tehty tai tapahtunut. Esimerkiksi kun tietokoneelle kirjautuu kirjoittamalla käyttäjätunnuksen ja salasanan, syntyy lokimerkintä onnistuneesta sisäänkirjautumisesta auditointilokiin. Jos salasanan kirjoittaa väärin, syntyy erilainen lokimerkintä väärällä salasanalla tehdystä epäonnistuneesta kirjautumisyrityksestä. Lokidataa on mahdollista tuottaa lähes kaikista tapahtumista erilaisten lokiasetusten avulla. Lokiviestit pystyvät yleensä myöskin vastaamaan viestiin liittyviin kysymyksiin: milloin, kuka, mitä, mistä ja mihin.

Alla olevassa kuvassa (kuva 1) näkyy tavanomainen lokiviesti käyttäjän sisäänkirjautumisesta Windows-päätelaitteelle. Merkittynä on mielenkiintoisimmat tiedot lokista. Lokiviesteistä muodostetaan tapahtuma (Eng. Event).

An account was successfully logged on.

Subject:

Security ID: SYSTEM
Account Name: DESKTOP-DEMO\$
Account Domain: TESTAAJAT
Logon ID: 0x3E7

Logon Information:

Logon Type: 7
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: No

Impersonation Level: Impersonation

New Logon:

Security ID: EsimerkkiAD\TopiTestaaaja
Account Name: topi.testaaaja@testaus.fi
Account Domain: EsimerkkiAD
Logon ID: 0xFD5213F
Linked Logon ID: 0xFD5212A
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

Process ID: 0x30c
Process Name: C:\Windows\System32\lsass.exe

Network Information:

Workstation Name: DESKTOP-DEMO
Source Network Address: -
Source Port: -

Detailed Authentication Information:

Logon Process: Negotiate
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

Kuva 1. Lokiviesti onnistuneesta sisäänkirjautumisesta Windows-laitteelle

Tällaista lokia nimitetään yleensä raakalokiksi (Eng. Raw log). Raakalokin saapuessa SIEM-järjestelmä parsii sen, eli erottelee lokista kaikki attribuutit. Attribuutit koostuvat tietotyypistä (esimerkiksi Account name) ja arvoalueesta (esimerkiksi topi.testaaaja@testaus.fi), joiden avulla

voidaan tapahtumat hakea myöhemmin. SIEM-järjestelmillä myöskin rikastutetaan eli lisätään lisäattribuutteja. Yksinkertainen rikastuttaminen voisi olla esimerkiksi IP-osoitteiden maantieteellisten sijaintitietojen lisääminen, jolla kerrotaan tutkijalle minkä maan IP-alueeseen IP-osoite kuuluu ilman, että se pitää käsin tarkistaa. [7]

SIEM-järjestelmä mahdollistaa lokidatan tallentamisen useasta eri lähteestä samaan paikkaan, jossa niistä luotuja tapahtumia voidaan verrata ja korreloida keskenään nopeasti ja helposti, käyttäen attribuutteja ja niiden arvoalueita. SIEM-järjestelmään luodaan myöskin sääntöjä erilaisille tapahtumille ja niiden kombinaatiolle, joista syntyy hälytyksiä säännön ehtojen täytyessä. Tietoturva-asioihin perehtynyt SOC-analyytikko, tai muu digitaalisen forensiikan osaaja, joka on perehtynyt tutkimaan organisaation tietoturvaa, tutkii hälytykset niiden syntyessä.

Esimerkkinä voisi olla sääntö, joka vertaa käyttäjien suorittamia onnistuneita ja epäonnistuneita kirjautumisia. Esimerkki poikkeavasta käytöksestä voi olla tapahtumaketju, jossa käyttäjä kirjoittaa salasanan 50 kertaa väärin ennen kuin pääsee lopulta kirjautumaan sisään. Epäilyttävää tästä tekee se, että keskiverto henkilö olisi ottanut yhteyttä IT-tukeen paljon aikaisemmin, unohtettuaan oman salasanansa. Siispä SOC-analyytikko tutkii säännön luoman tietoturvahälytyksen esimerkiksi IP-osoitteesta pääteltävien tietojen ja tilin muun historian perusteella. Analyytikko tarvittaessa ilmoittaa tapahtumasta eteenpäin eskalointimenettelyn mukaisesti. Mahdollisesta onnistuneena väsytyshyökkäyksestä (Eng. Brute Force), jossa tietokoneavustuksella koitetaan sattumanvaraisesti arvata käyttäjätilin salana.

4.2 SOAR

Security Orchestration, Automation and Response (SOAR) on järjestelmä, jota hyödynnetään tietoturvakeskus- eli SOC-toiminnassa. SOAR-järjestelmän avulla yhdistetään automatiikalla tehtävät toimet, tietoturvatapausten tutkinta ja hallinta sekä mahdolliset tapahtumien korjaustoimet samaan sovellukseen. SOAR-järjestelmällä pyritään näyttämään kaikki tarpeellinen data analyytikoille yhdessä ikkunassa, jotta työnkulku olisi mahdollisimman nopeaa ja vaivatonta. Tämä mahdollistetaan luomalla automaatioita kaikkiin toistuviin toimiin. Esimerkkejä näistä automaatioista voivat olla lisäinformaation haku tapahtumista, tekoälyn luomat tulkinnot

tapahtumasta, vastatoimien, kuten prosessien eristäminen tai verkkoyhteyksien katkaiseminen kohdelaitteelta. Automaatiot luodaan yleisesti käyttäen playbook-nimisiä kirjastoja.

SOAR-järjestelmää voidaan kuvata ”kohtaamispaikkana” kaikille tietoturvatuotteille joita organisaatiossa käytetään esimerkiksi päätelaitesuojaus, SIEM-järjestelmä ja verkonseuranta-järjestelmät. SOC-toiminnasta yleisesti puhuttaessa on tärkeää tietää, mikä SOAR on.

4.3 Kulunvalvonta

Kulunvalvontajärjestelmällä tarkoitetaan fyysisen turvallisuuden laitteistoa, jolla valvotaan organisaation kiinteistöjä. Kulunvalvontajärjestelmillä voidaan valvoa ja rajata ihmisten kulkua alueella. Kulunvalvontajärjestelmillä voidaan myöskin auditoida, mistä ovista käyttäjät ovat kulkeneet aikaisemmin.

Kulunvalvonta on todennäköisesti vanhin turvallisuuden muoto. Jo kauan ennen nykyaikaisia järjestelmiä kulunvalvontaa toteutettiin vartijoilla, lukoilla ja muureilla, jotka mahdollistivat ihmisten kulun seuraamisen tai pääsyn rajoittamisen haluttuihin paikkoihin. Lukollinen ovi on esimerkki perinteisen kulunvalvonnan toteutuksesta.

Digitalisoidussa maailmassa ihmisvartijoista ja perinteisistä fyysisistä avaimista on jo suurelta osin luovuttu. Nykyaikaiset kulunvalvontajärjestelmät käyttävät kameroita ja liikkeentunnistimia vartijoiden sijaan. Fyysiset avaimet on vaihdettu kulkutunnisteisiin, joiden käyttöoikeuksia voidaan muuttaa tarvittaessa helposti. Digitalisointi on muuttanut kulunvalvontaa muun muassa helpottamalla kulkulokien keräämistä sekä kulkulupien rajaamista ja peruuttamista.

4.4 Pääsynvalvonta

Pääsynvalvonta on tietotekniikka maailmassa yleinen käsite ja siihen voi liittyä monia muita termejä, kuten roolipohjainen pääsynvalvonta (Eng. Role Based Access Control, RBAC). Idea pääsynvalvonnalla on sama kuin fyysisellä kulunvalvonnalla. Tietotekniikan puolella sillä vain määritellään mihin tietoteknisiin palveluihin ja resursseihin kunkin henkilön käyttäjätillä on

minkäkin tasoinen käyttöoikeus. Esimerkiksi pääsynvalvonnalla voidaan rajata mihin tietoon, työasemiin, tietoverkkoihin tai järjestelmiin, käyttäjän tilillä voi kirjautua tai päästä käsiksi.

Roolipohjainen pääsynvalvonta perustuu periaatteeseen, jossa yksittäisille käyttäjille ei suoraan myönnetä oikeuksia, vaan käyttäjät lisätään ryhmään. Ryhmille on myönnetty roolin tehtäviin kuuluvat oikeudet, jotka käyttäjä perii ryhmään kuulumalla. Täten voidaan muuttaa jopa tuhansien henkilöiden oikeuksia helposti muokkaamalla ryhmän käyttöoikeuksia. [9]

4.5 Käyttöoikeuksien hallinta

Kulunvalvonan ja pääsynvalvonan määrittelyä ja auditointia hallitaan pääsynhallinnalla (Eng. Access management; AM) eli menettelyllä, joilla varmistetaan, että käyttäjät, laitteet, sovellukset ja järjestelmät pääsevät käyttämään tietojärjestelmissä olevaa tietoa roolinsa mukaisesti. Pääsynhallintaa toteutetaan puolestaan käyttöoikeuksien hallinnalla (Eng. Access Control). Puhekielessä pääsynhallintaa ja käyttöoikeuksien hallintaa saatetaan kuitenkin käyttää sekaisin, koska ne helposti mieleltään samaksi asiaksi.

Käyttöoikeuksien hallinta voidaan jakaa kolmeen eri pääalueeseen: autentikointi, auktorisointi ja käytön tilastointi (Eng. Three A's of Access Control: Authentication, Authorization ja Accounting). Nämä alueet esitellään seuraavissa kappaleissa.

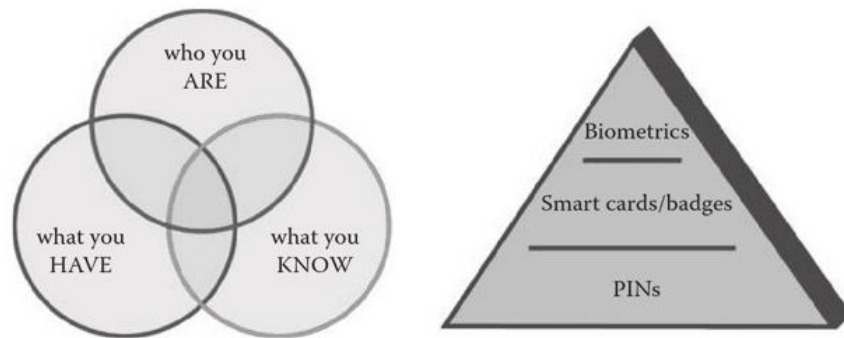
4.5.1 Autentikointi

Autentikoinnilla eli todentamisella varmistetaan, että kirjautuja on juuri se henkilö, jolle kohdetili kuuluu. Autentikaatiolla yleensä tarkoitetaan sisäänkirjautumista tietojärjestelmään. Tämä voidaan toteuttaa monella eri tavalla. Seuraavalla sivulla on kuvaaja (kuva 2) liittyen tähän.

Yleisimpiä autentikointi tapoja ovat:

- Salasanat ja koodit eli salasana pohjainen tunnistautuminen eli jotain mitä käyttäjä tietää
- Sormenjälki ja kasvotunnistus eli biometrinen tunnistautuminen eli jotain mitä käyttäjä on

- Autentikaatio-sovellukset ja koodilaitteet eli token-pohjainen tunnistautuminen eli jotain mitä käyttäjällä on



Kuva 2. Autentikaation kolme kulmakiveä, [8]

Autentikointiin voidaan käyttää mitä tahansa näistä tavoista tai yhdistää useampaa yhteen autentikointiin, jolloin puhutaan monivaiheisesta tunnistautumisesta (Eng. Multi Factor Authentication, MFA). Tunnistautumistavat sekä mahdollisten monivaihteistunnistautumisten määrä vaihtelee tunnistauduttavan kohteen välillä. Esimerkiksi yleensä fyysinen kulku rakennuksessa vaati vain autentikaatiotokenin (kulkulätkä) käyttöä oviin, mutta turvasoa voidaan nostaa vaatimalla PIN-koodi kulkulätkän käytön yhteydessä. Tällöin autentikaatioon vaaditaan jotain, mitä käyttäjällä on ja jotain, minkä hän tietää.

4.5.2 Auktorisointi

Auktorisointi eli valtuuttaminen on lupien antamista ryhmille tai käyttäjille. Kun käyttäjä on autentikoituna järjestelmään, tarkastetaan, onko autentikoitua käyttäjää auktorisoitu käyttämään järjestelmää missä määrin.

Autentikointi ja auktorisointi ovat tapahtumia, joiden pohjalta voidaan muodostaa monenlaisia tietoturvatapahtumaketjuja. Näiden tapahtumien tilastointi onkin äärimmäisen tärkeää tietoturvalvonnan kannalta.

4.5.3 Käytön tilastointi

Tilastoinnilla varmistetaan luottamuksellisuutta eli sitä, että pystytään tarkistamaan, että vain auktorisoidut henkilöt ovat päässeet käyttämään tiettyjä resursseja. Kulunvalvonta- ja pääsynvalvontadata tallennetaan tietokantaan, josta myöhemmin voidaan tarkistaa, mistä joku tietty henkilö on kulkenut tai kirjautunut. Tilastointia ovat esimerkiksi SIEM-järjestelmään lähetetyt kirjautumislokit.

Tilastoidusta tapahtumasta voidaan myöskin etsiä tapahtumia, joilla tunnistetaan käyttäjiin kohdistuneita tietoturvahyökkäyksiä, kuten käyttäjätilien kaappauksia. Kulunvalvonnan ja pääsynvalvonnan dataa ei yleensä suoraan käytetä yhdessä tunnistamaan tietoturvapoikkeamia, mutta mahdollisuuksia sillekin on.

4.6 Kulunvalvontakäytäntö

Kulunvalvonnan (niin digitaalisen kuin fyysisenkin) toteuttamisen, valvonnan ja toiminnan takaamiseksi pitää luoda kulunvalvontaa koskevat käytännöt. Kulkulupien jaon pitäisi perustua organisaation toiminnallisiin tarpeisiin, salassapitovaatimukset huomioon ottaen. Henkilöllä kuuluu olla oikeudet vain tietoihin ja paikkoihin, johon hänen pitää päästä käsiksi suorittaakseen häneltä vaaditut tehtävät. Tätä lähestymistapaa kulunvalvontaa kutsutaan vähimpien oikeuksien periaatteeksi (Eng. Principle of least privilege). [9. s.69]

Tilien tietoturvavaatimuksia voi myöskin nostaa antamalla rooleille omia tietoturvavaatimuksia rooliin liittyviä tietoja käyttäessä, esimerkiksi lisäautentikointien muodossa.

Palvelun tai järjestelmän omistajien kuuluu hyväksyä pyydetty kulkuluvat, kun ne ovat organisaation kulunvalvontakäytänteiden mukaiset, sekä säännöllisesti tarkistaa voimassa olevat kulkuluvan haltijat. Jos henkilön toimenkuva organisaatiossa muuttuu, kuuluu kulkulupia muuttaa vastaamaan henkilöiden uusia rooleja sekä poistaa vanhan roolin oikeudet, joihin henkilöllä ei enää ole selvää tarvetta muuttuneen roolinsa suorittamiseen. [9 s.69]

Kulunvalvonnan käytäntöjen oikea toteutus tehostaa tietoturvaa sekä helpottaa SOC-valvontaa, kun tiedetään tarkalleen, mitkä oikeudet kullakin käyttäjällä pitäisi olla. Lisähyötyä tuottavat

myöskin ominaisuudet, jotka estävät käyttäjää näkemästä käyttöoikeuksien ulkopuolisia asioita graafisissa käyttöjärjestelmissä. Tällöin käyttöoikeuksien väärinkäyttöyritykset on helpompi havaita, koska käyttäjä ei voi vahingossa yrittää käyttää oikeuksiensa ulkopuolisia resursseja. Varsinainen hyöty kulunvalvontakäytäntöjen oikeaoppisesta toteutuksesta tietoturvamielessä saadaankin tilanteessa, jossa käyttäjätili joutuu vaarannetuksi, mutta tilillä päästään toteuttamaan vain rajoitettuja toimintoja. Rooleilta, joilla on laajemmat käyttöoikeudet, kuuluukin vaatia vahvempia autentikaatio tapoja, jolloin vaarantumisriski pienenee.

4.7 MITRE ATT&CK

MITRE ATT&CK Framework on amerikkalaisen voittoatavoittelemattoman Mitre -yhtiön luoma ilmainen tietopohja, josta löytyy matriiseja kyberhyökkäyksien yleisistä vaiheista ja niiden tunnistuksesta. ATT&CK Matrix for Enterprise -matriisi kattaa 14 hyökkäysvaihetta, joihin on jaettu 188 hyökkäystekniikkaa, joilla voi olla vielä omia alatekniikoitaan. MITRE ATT&CK on kehittynyt standardiksi tietoturva-alalla, ja monet tietoturva tuotteet voivat lisätä ATT&CK Framework -tiedot löydöksiinsä analysoinnin helpottamiseksi. [10]

ATT&CK Framework on hyödyllinen, koska sitä käyttämällä voidaan määritellä, mihin vaiheeseen kyberhyökkäystä tietoturvatapahtumat liittyvät. Sen avulla löytää lisätietoa havaitusta tekniikasta sekä sen seurauksista ja käyttötarkoituksista. ATT&CK Framework helpottaa myös yleisen keskustelun kulkua tietoturvayhteisöissä, kun osallisilla on sama tietopohja. Silloin on helpompi ymmärtää, mistä tarkalleen puhutaan.

5 Toteutussuunnitelma käytännönsuudessa

Toimeksiantaja määräsi tässä opinnäytetyössä käytettävän SIEM- ja kulunvalvontajärjestelmän. Toimeksiantaja ei halunnut, että järjestelmien nimiä suoraan mainitaan tässä opinnäytetyössä salassapitosyistä. Opinnäytetyö koostuu suunnittelemisvaiheesta ja käytännönsuudesta, jossa suunnitelman pohjalta luodaan prototyyppi (Eng. Proof of Concept, POC) toimeksiantajan testiympäristöön.

5.1 Integraatiot

Kulunvalvontajärjestelmä, myöhemmin KV-järjestelmä, on integroitu jo aikaisemmin Azure Active Directory:n (AAD) toimeksiantajan toimesta. Tätä integraatiota käytetään luomaan KV-järjestelmään jo olemassa oleville AAD-käyttäjille kulkutunnisteet ja hallitsemaan käyttäjien kulkuoikeuksia Active Directoryn käyttöoikeuksien hallinnan kautta. Tämä opinnäytetyö nojaa vahvasti tähän integraatioon, koska käyttöoikeuksien käytön valvonta on oleellinen osa SOC-työtä. Integraation tuoma yhtenäisyys KV-järjestelmän ja Active Directoryn välille helpottaa SIEM-järjestelmän päässä tehtävää työtä, koska käyttäjien käyttäjätiliattribuutit voidaan yhdistää suoraan toisiinsa ja ne pysyvät ajantasaisina automaattisesti.

Azure AD mahdollistaa hyvin vahvan SSO-tunnistuksen, johon voi liittää kohteita useista eri lähteistä, kuten On Premises Active Directorystä, joten siihen yhdistäminen on hyvä vaihtoehto keskitetyn käytönvalvonnan seuraamiseksi.

Azure AD:n kanssa voidaan myös käyttää mm. Azure identity protection-palvelua, jolla voidaan valvoa käyttöä tehokkaasti [11]. Tai voidaan käyttää Conditional Access- palvelua, jolla voidaan määritellä ehtoja eri kirjautumisille niin fyysisessä kuin digitaalisessa maailmassa [12]. Tämä tuottaa lisäarvoa liitokselle myöskin SIEM-valvonnan ulkopuolelta. SIEM-järjestelmällä voidaan valvoa Identity protection- ja Conditional access- palveluita. Identity Protection ja Conditional Access Conditional Access -tapahtumat ovat erittäin hyödyllisiä tietoturvapoikkeusten tutkinnassa.

AD-käyttäjä on se identiteetti, jota halutaan seurata SIEM-valvonnassa. Tavoitteena on yhdistää kaikki mahdolliset kirjautumiset eri ympäristöistä tähän identiteettiin. Tämä helpottaa myöskin käyttäjää, kun on vain yksi tili, jota käytetään joka paikassa. Myöskin vastatoimien suoritus kaapattuja käyttäjätilejä vastaan helpottuu ympäristössä, jossa on yksi käyttäjätili henkilöä kohden helpottuu.

5.2 Kulunvalvontajärjestelmän yhdistäminen SIEM-järjestelmään

KV-järjestelmän lokit pitää lähettää SIEM-järjestelmään, jotta säännöt ja hälytysten tutkinta voidaan tehdä yhdestä paikasta. KV-järjestelmä kerää lokeja SQL-tietokantaan, josta lokit voidaan vetää SIEM-järjestelmän tietokantaan. Ratkaisuna tässä projektissa toimii erillinen Logstash-palvelin, jolla voidaan suorittaa SQL-kyselyitä suoraan SQL-tietokannasta, sekä parsia haetut viestit valmiiksi [13].

Logstash-palvelin oli testiympäristössä jo valmiina, joten sille vain konfiguroidaan uusi konfiguraatio lokien hakemiseen KV-järjestelmästä. Logstahs-sovellus muuttaa SQL-kyselyt suoraan XML muotoon, jota SIEM-järjestelmä osaa lukea. KV-järjestelmän SQL-tietokannassa sarakkeet vastaavat SIEM-järjestelmän attribuutteja, ja ne on nimetty selkokielellä, joten niitä ei kannata jäsentää uudelleen. Tämä helpottaa myöskin sääntöjen luomisvaiheessa, koska attribuuttien nimiä ja tarkoituksia voidaan tarkistaa suoraan KV-järjestelmän dokumentaatiosta.

Logstash on Elastic-yrityksen luoma avoimen lähdekoodin (Eng. Open source) työkalu lokien keräämiseen, parsimiseen eli jäsentämiseen, suodattamiseen ja muuttamiseen. Elastic-yritys on tunnettu Elasticsearch-tietokantaklusterista, jolla voidaan ylläpitää suuria tietokantoja. Logstash-ohjelmaa voidaan kuitenkin käyttää hyvin laajasti lähettämään dataa paikasta toiseen, avoimen lähdekoodin suoman kehitysyhteisönsä ansiosta.

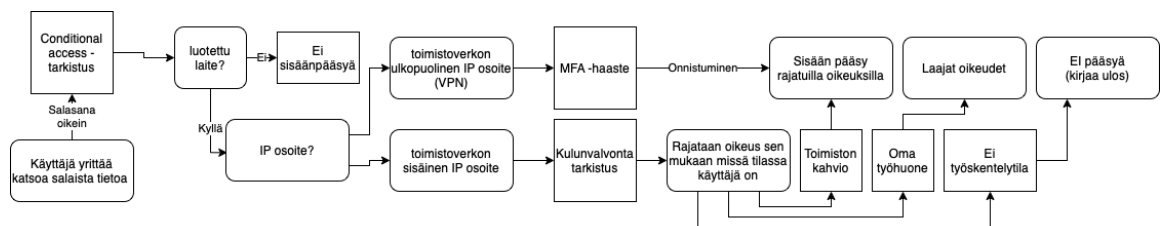
5.3 Tavoitteita

Kun AAD-integraatio ja lokiviestien toimitus SIEM-järjestelmään toimivat, voidaan ruveta toteuttamaan projektille toimeksiantajan puolesta antamia tavoitteita. Tavoitteita käsitellään seuraavissa kappaleissa.

5.3.1 Ehdollinen pääsy

Ehdollinen pääsy (Eng. Conditional Access) on Microsoftin Azure -pilvipalveluun kuuluva pilvipohjainen identiteetin suojeluratkaisu. Ehdollinen pääsy nimensä mukaisesti mahdollistaa ehtopohjaisen kulunpääsyn resursseihin. Ehdollista pääsyä käytetään nostamaan autentikaatiovaatimuksia arkaluontoisille materiaaleille tai oikeuksille. Ehdollinen pääsy voidaan konfiguroida vaatimaan lisätunnistautumista esimerkiksi MFA-tunnistautumisen muodossa tai luotetun laitteen käyttöä, kun käyttäjä tekee korkeaa käyttöoikeutta vaativia toimia [12].

KV-järjestelmän AAD-integraatiolla voitaisiin luoda ylimääräisiä ehtoja tunnistautumiselle, kun käyttäjä työskentelee toimistolla. Alla olevassa kaaviossa (Kuva 3) havainnollistetaan, miten KV-järjestelmän tiedot voitaisiin tuoda MFA-tunnistautumisen rinnalle toimistotyössä. KV-järjestelmä myöskin voisi mahdollistaa käyttäjän tietokoneen automaattisen lukitsemisen, jos tämä lähtee tilasta.



Kuva 3. KV-datan toimiminen ehdollisen pääsyn kanssa.

5.3.2 Esimerkkisäännöt

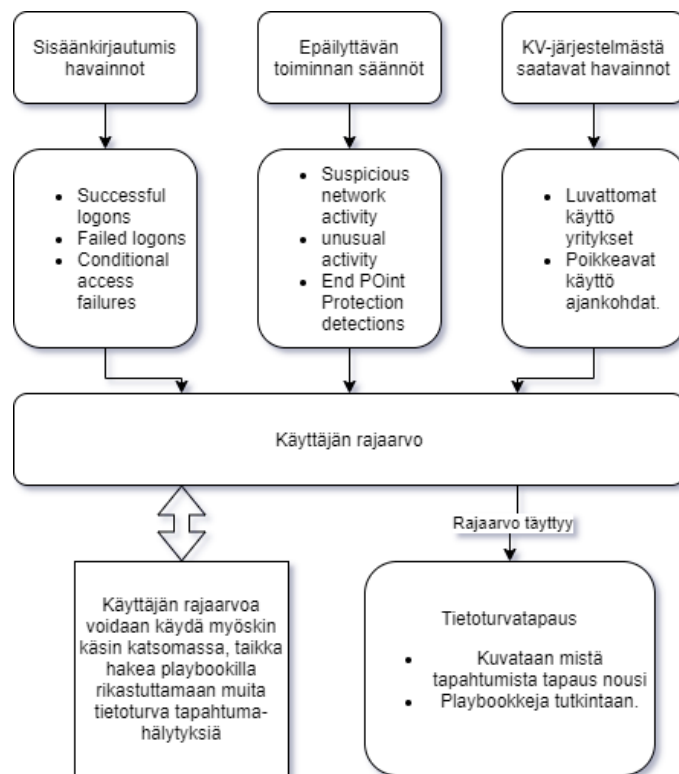
Luodaan ensiksi yksinkertaisia sääntöjä, jotka perustuvat vain KV-järjestelmästä saatavaan dataan. Kun yksinkertaisten sääntöjen todetaan toimivan halutulla tavalla, voidaan tutkia mahdollisia ehdollisen pääsyn mahdollistamia sääntöjä käyttäen AAD-integraatiota.

Esimerkki yksinkertaisesta säännöstä voisi olla sääntö, joka hälyttää, kun käyttäjän kulkulupaa koitetaan käyttää useisiin auktorisoimattomiin kulkupisteisiin useita kertoja.

5.3.3 Datan esitys analyytikolle

Analysointia auttavat merkinnät voivat nopeuttaa analyytikkojen työtä. Esimerkiksi kun kulunvalvonta ja käytönvalvonta datasta muodostuu epäilyttäviä tapahtumaketjuja, voidaan tehdä merkintä käyttäjään, jos sama käyttäjä esiintyy/ synnyttää joitain muita hälytyksiä. Tämä auttaisi analyytikkoja huomiomaan käyttäjän muut tietoturvatapahtumat paremmin, ja muodostamaan mahdollisen tapahtumaketjun, jos SIEM-järjestelmä ei ole sellaista vielä synnyttänyt.

Datan esityksen apuna voidaan käyttää esimerkiksi käyttäjän epäilyttävistä tapahtumista arvoja seuraavaa SOAR-playbookkia, sääntöä tai visualisointia, joka rikastutetaan haluttuihin tietoturvatapahtumiin lisätiedoksi SOAR-playbookin avulla. Esimerkki tällaisesta ratkaisusta on esimerkiksi Microsoftin AAD Identity Protection -platform. Sen avulla voidaan selvittää käyttäjäkohtaisia riskejä. Alla kuvaus (Kuva 4), miltä kyseisenlaisen ratkaisun laajennus KV-järjestelmän datan kanssa näyttäisi logiikaltaan.



Kuva 4. KV- Järjestelmän datan lisäys käyttäjä kohtaista riskiä mittavaan ratkaisuun

5.3.4 Dokumentaatio

Toimeksiantaja haluaa, että käytännönsuutta dokumentoidaan sitä tehdessä, ja että kaikki tärkeät asiat kirjataan ylös. Tulen käyttämään tätä dokumentaatiota myöskin pohjana käytännönsuuden kirjoittamiselle. Dokumentaatio on yksi salassa pidettävistä liitteistä.

Dokumentaatiolta vaaditaan selkeyttä, ja sen avulla pitäisi pystyä kopiomaan työn tulokset. Yksityiskohtaista ohjeistusta ei kuitenkaan tarvitse luoda, vaan voidaan viitata esimerkiksi olemassa oleviin muihin dokumentaatioihin tai ohjeisiin, mikäli niitä noudattamalla ei syntynyt ongelmia.

6 Käytännönsuuden toteutus

Käytännönsuuden suoritusta aloittaessa todettiin, että aikaisemmin fyysisen kulunvalvonnan ja AAD:n välille luotu integraatio oli tämän projektin tarpeet huomioon ottaen puutteellinen. Toimeksiantaja päätti, että AAD:n integraation käyttö ohitetaan kokonaan opinnäytetyön osalta. KV-järjestelmä yhdistetään pelkästään SIEM-järjestelmään. AAD-puolen ratkaisuita selvitetään, kun AAD-liitos tehdään myöhemmin.

AAD- tai AD-integraatiota voidaan simuloida SIEM-järjestelmän päässä sääntötasolla luomalla SIEM-järjestelmän sääntöihin yksittäisiä parituksia käyttäjille. Parituksella tarkoitetaan AAD-käyttäjän ja KV-järjestelmän käyttäjän tietojen etsimistä erikseen saman identiteetin alle. Tällä voidaan simuloida maksimissaan muutaman käyttäjän toimintaa. Tuotantokäytössä pitää olla jokin oikea tapa toteuttaa vastaava identiteettiin liittäminen, esimerkiksi aikaisemmin suunniteltu AAD-integraatio.

Simuloimalla AD-integraatiota kierretään tarve käyttää aikaa opinnäytetyön tekemisestä integraation korjaustoimiin. Integraation tekeminen ei myöskään kuulunut alkuperäiseen toimeksiantoon, joten se kannattaa jättää opinnäytetyön ulkopuolelle, jotta aihealue ei laajennu liikaa.

6.1 Valittu tapa toimia ja sen kuvaus

Käytännönsuudessa prototyyppitason ratkaisuun luotiin siis KV-järjestelmästä lokiliikenne SIEM-järjestelmään. SIEM-järjestelmässä testattiin liitoksen toimivuus ja luotiin alustavia sääntöjä, joissa käytettiin KV-järjestelmän dataa.

AAD-integraation puutteesta huolimatta pyrittiin noudattamaan kohdassa 4 esiteltyä toteutussuunnitelmaa. Aikaa toteutusvaiheessa ei kuitenkaan ollut kaikkien kohtien toteuttamiselle. Esimerkiksi SOAR-playbook-ratkaisuja ei päästy kokeilemaan.

6.2 Logstash-keräin

Keräin on ympäristössä toimiva kohdennuspiste, jonka kautta voidaan lähettää lokidataa keskitettyyn paikkaan helpommin. Esimerkiksi ei jouduta tekemään kuin yhdet palomuuriauvaukset keräimelle. Kaikki muurialueen sisällä olevat laitteet lähettävät samalle keräimelle lokinsa, joka lähettää ne eteenpäin SIEM-järjestelmään esimerkiksi VPN-putken läpi. KV-järjestelmästä haettiin lokit Logstash -nimisen keräinratkaisun avulla

Logstash-palvelin oli jo valmiina testiympäristössä. Logstash toimii hyvin suurelta osalta pluginien - eli lisäosien avulla, joita palvelimeen voi liittää oman tarpeensa mukaan. Ensimmäisenä piti tarkistaa, oliko palvelimella jo vaadittavat lisäosat lokin hakemiseen kohde KV-palvelimelta. Lisäosat oli asennettu jo aikaisemmin samanlaiseen käyttötarkoitukseen.

Seuraavaksi piti lisätä konfiguraatiotiedostot, joissa määriteltiin seuraavat asiat: kohde, lähde sekä salaukseen ja autentikaatioon liittyvät asiat. Nämä kohdat kuvataan alakappaleissa tarkemmin.

6.2.1 Lokin kohde

Lokit lähetetään yleisesti konfiguroimalla vastaanottajajärjestelmän tiedot ja sertifikaatit, jolloin Logstash pystyy lähettämään sinne lokia turvallisesti. Salassapitosyistä tätä konfiguraatiota ei esitellä tarkemmin.

Lokin lähettämisessä on tiettyjä asioita, joita pitää ottaa huomioon, kun sitä tehdään SOC-palveluntuottajana. Lokit pitää pystyä määrittämään koskemaan vain lähettävän asiakkaan sääntöjä, mikäli ne lähetetään jaettuun SIEM-järjestelmään. SIEM-järjestelmät mahdollistavat useamman alaorganisaation luonnin, joihin voi lähettää erikseen omat lokinsa, ja tällöin lokit eivät voi mennä sekaisin asiakkaiden välillä. Alaorganisaatiot voivat käyttää esimerkiksi kokonaan erillisiä tietokantoja tai klustereita datojen erottamiseen. Joissain tapauksissa asiakkailla voi olla oma SIEM-järjestelmä, jolloin he itse vastaavat datansäilytyksestä.

Tuotannossa tällaista liitosta monen asiakkaan jakamaan SIEM-järjestelmään voidaan varmistaa luomalla testitapahtuma arvottomalla datalla Logstash -palvelimella, joka lähtee SIEM-

järjestelmässä konfiguroituun alaorganisaatioon. Kun lokin kulku oikeaan kohteeseen on varmistettu, voidaan lokin hakua koskeva konfiguraatio viimeistellä hakemaan oikeaa tietoa.

6.2.2 Lokin lähde

Lähdetietokantaan luotiin tunnukset, jotta Logstash pääsee käsiksi tietokantaan. Näillä tunnuksilla ei saa olla muuta kuin lukuoikeudet haluttuun informaatioon, kuten aikaisemmin mainittiin vähimpien oikeuksien periaatteesta (3.4). Tiedot kopioidaan ja Logstash ei muokkaa lähdelaitteella mitään tietoja. Riippuen Logstash-palvelimen ja lähdejärjestelmän lokaatiosta, voi olla tarpeellista tehdä palomuuuriavaukset liikenteelle. Testiympäristössä tätä tarvetta ei kuitenkaan ollut.

Lisäksi hakukonfiguraatiossa määriteltiin SQL-kysely, joka lähteenä toimivasta KV-järjestelmän SQL-tietokannasta haluttiin hakea. Logstash muuttaa kaikki kyselyn tulokset lokiviesteiksi. Siispä kyselyssä määritettiin, mistä asti tietoa haettiin, jotta Logstash ei hakisi joka kerta samaa tietoa. Tämä on ratkaistu käyttämällä tracking saraketta, jolla voidaan ottaa talteen jonkin muun sarakkeen sisältö ja käyttää sitä sitten jatkamaan kyselyä seuraavalla kerralla siitä, mihin jäätiin. Alla on esimerkki konfiguraatiosta (kuva 5).

```

input {
  jdbc {
    jdbc_driver_library => "/usr/share/sqljdbc_9.4/enu/mssql-jdbc-9.4.0.jre11.jar"
    jdbc_driver_class => "com.microsoft.sqlserver.jdbc"
    jdbc_connection_string => "jdbc:sqlserver://KANTAPALVELIN.domain.com\INSTANSSI
      ;databaseName=TIETOKANTA
      ;user=USER
      ;password=PASSWORD
      ;trustServerCertificate=true
      ;hostNameInCertificate=*.domain.com
      ;loginTimeout=30
      ;domain=domain.com
      ;Trusted_Connection=true
      ;authenticationScheme=NTLM
      ;authentication=NotSpecified
      ;integratedSecurity=true
      ;encrypt=true;"
    jdbc_user => "USER"
    jdbc_password => "PASSWORD"
    # serialnum sarakkeessa on KV-järjestelmän kasvava liukunumero, jolla voidaan eritellä jokainen tapahtuma toisistaan.
    tracking_column => "serialnum"
    tracking_column_type => "numeric"
    use_column_value => true
    #schedule käyttää Cron ajastusta. Nyt se on ajastettu hakemaan tapahtumat kerran minuutissa.
    schedule => "* * * * *"
    #last_run_metadata_path tämä avulla voidaan tallentaa tracking_column tieto jokaisen toiston jälkeen talteen.
    last_run_metadata_path => "/usr/share/logstash/metadata/testiKV.metadata"
    #Lopussa suoritetaan SQL kysely joka haetaan SQL tietokannasta
    #Huom. kysely ottaa huomioon aina edellisen kerran viimeisen serialnum arvon, jolloin samoja tapahtumia ei haetaan uudestaan.
    #SERIALNUM > xx ei muutu, mutta määritetään käyttöön otossa mikäli ei haluta hakea koko taulun tulosta.
    #( tämän vois alussa käydä lisäämässä myös testiKV.metadata -tiedostoon)
    statement => "
      use accesscontrol
      SELECT * FROM events
      WHERE SERIALNUM > :sql_last_value AND
      SERIALNUM > 1635403720
      ORDER BY EVENT_TIME_UTC ASC
    "
  }
}

```

Kuva 5. Esimerkki konfiguraatiotiedostosta, jolla haetaan tietoja Microsoft SQL-tietokannasta

6.2.3 Lokiliikenteen salaus

Lokiliikenne haluttiin myöskin salata järjestelmien välillä. Yleensä liikenne laitetaan alustavasti kulkemaan VPN-putken läpi. Lisäksi tehdään TLS (Transport Layer Security) salaus Certificate Authority's certifiikaateilla. Näin varmistetaan liikenteen kattava salaus. TLS salauksella voidaan varmistaa, että dataa vaihtavat osapuolet ovat keitä heidän pitäisi olla, ja että dataan ei ole koskettu siirron yhteydessä. Logstahille tuleva ja lähtevä liikenne voidaan salata erikseen. Prototyypissä salaus toteutettiin TLS-salauksella.

6.3 Lokituksen toimivuuden testaus

Loituksen toimivuutta testattiin luomalla SIEM-järjestelmään sääntö ja luomalla sääntöä vastaavia testitapahtumia KV-järjestelmään. Vasteajalla, eli sillä kuinka nopeasti sääntö hälyttää testitapahtumien tapahtumisen jälkeen, voidaan tutkia, toimiiko liitos reaaliajassa. Testauksen päätteeksi säännöt laukesivat aina minuutin sisällä, niin kuin Logstashin päässä oli konfiguroitu. Prototyyppi siis toimi halutulla tavalla.

Lopuksi selvitettiin myöskin, olivatko sääntöön kuulumattomat tapahtumat tulleet SIEM-järjestelmään oikein. Tämä tehtiin vertaamalla tietyn ajan sisällä tulleiden tapahtumien summaa KV-järjestelmän omassa lokitietokannassa olevien tapahtumien summaan samalta ajalta. Nämä täsmäsivät, joten lokiliitos näyttäisi olevan toiminnallinen.

6.3.1 Denied entries in different locations -sääntö

Tämä testisääntö käyttää pelkkää KV-järjestelmästä kerättyä dataa. Sillä myöskin suoritettiin lokien lähetyksen testaaminen KV-järjestelmästä. Sääntö on nimetty englanniksi, koska SIEM-järjestelmässä pyritään käyttämään englantia yhtenäisyyden takia.

Sääntö on osiota 5.3.2 kuvatun säännön mukainen, ja hälyttää, kun käyttäjän kulkulupaa koitetaan käyttää useisiin auktorisoimattomiin kulkupisteisiin useita kertoja.

Säännön logiikka:

1. Annetaan säännölle attribuutti `Max_deny_count`, jonka arvoaluetta muuttamalla voidaan määritellä hälytyksen raja-arvoa eli korkeinta sallittua epäonnistunutta kulkuluvan käyttömäärää.
2. Määritellään tapahtumat eli lokiviestit, joita sääntö valvoo, eli vain KV-järjestelmästä tulevat tapahtumat.
3. KV-järjestelmästä tulevasta datasta haetaan Event type attribuutteja, joiden arvoalue viittaa epäonnistuneeseen kulkuyritykseen, joiden syynä on auktorisoimaton kulkuyritys. Salassapitosyistä tarkkaa Event type arvoa ei kerrota.

4. Kohdan 3. hausta luodaan listaus kaikista löydetyistä erillisistä Device-attribuutin arvoalueista eli eri tunnistautumispisteistä.
5. Verrataan 4. kohdan listaus 1. kohdan raja-arvoon. Mikäli tunnistautumispaikkojen määrä, joilla tunnistautuminen on epäonnistunut ylittää raja-arvon, nousee hälytys.

Sääntö on yksinkertainen, mutta sitä voitaisiin sellaisenaan hyödyntää osion 5.3.3 kaavion esittämässä käyttäjän seurausratkaisussa, keräämään tietoja epäilyttävästä toiminnasta.

7 Tulokset

AAD-integraation puutteellisuus aiheutti ongelmia opinnäytetyön etenemiselle. KV-järjestelmän liittäminen SIEM-järjestelmään kuitenkin onnistui hyvin ja sen kautta saatava data vaikutti testausten perusteella luotettavalta. Tämän datan perusteella myöskin pystyttiin luomaan sääntöjä SIEM-järjestelmään. Tämä osuus työstä voidaan katsoa onnistuneeksi ja täyttävän toimeksiantajan asettamat tavoitteet.

Dokumentaation osalta prototyypin luonnissa ei esiintynyt mitään mielenkiintoista, ja suurin osa työstä pystyttiin tekemään noudattamalla järjestelmien omia dokumentaatioita ja ohjeita. Dokumentaatiossa kuvataan kuitenkin testaustavat, konfiguroinnit sekä muistiinpanot, jotka helpottavat vastaavan liitoksen uudelleen tekemistä.

Datanesitys analyytikoille ja ehdollisen pääsyn -osuudet jäivät toteuttamatta AAD-integraation puutteiden takia. KV-järjestelmän lokidata voi kuitenkin olla SOC-toiminnassa arvokasta DFIR-tilanteissa (Digital Forensics and Incident Response), joissa tutkitaan tietoturvatapahtumia laajemmin tietoturvarikkeen seurauksena.

8 Pohdinta

Opinnäytetyön käytännönsuuden jälkeistä pohdintaa arvioinnin, kannattavuuden, jatkosuunnitelmien ja oman oppimisien näkökulmista.

8.1 Opinnäytetyön onnistumisen arviointi

Opinnäytetyö ei yltänyt kaikkiin toimeksiantajan tavoitteisiin, mutta se kuitenkin edisti aiheen käsittelyä sisäisesti ja toi uusia ideoita esille. Koska SIEM-järjestelmän ja KV-järjestelmän liitos on varmistettu mahdolliseksi, voidaan hankkeen edistämistä miettiä uudesta näkökulmasta.

Siihen kuinka kannattavaksi tällainen liitos tulisi, ei vielä voida vastata.

8.2 Kannattavuus

Opinnäytetyön tulosten pohjalta ei vielä voida sanoa, tulisiko tämän liitos olemaan kannattava AAD-integraation kanssa. Pelkkä SIEM-järjestelmään liittäminen ei riitä kannattavien säännösten luontiin CSOC-valvonnan osalta, eikä tätä ratkaisua kannattaisi ottaa käyttöön prototyyppitoteutuksen mittakaavassa.

Kaikki säännöt ja tapahtumat voitaisiin luoda/lähetää SIEM-järjestelmään mitä KV-järjestelmässäkin voidaan luoda, mutta niiden tekeminen on käytännöllisempää KV-järjestelmän sisällä. Pelkkien lokien liittäminen SIEM-järjestelmään voisi olla hyödyllistä yllä kuvatussa DFIR-tilanteessa, mikäli on epäily, että hyökkääjät ovat fyysisesti käyneet paikan päällä

8.3 Jatkosuunnitelmat

Käytännönsuudessa jäi paljon asioita toteuttamatta puutteellisen Azure Active Directory integraation vuoksi. Alustavaa suunnittelua oli kuitenkin tehty AAD:n integraatio

mahdollisuuksista. Jatkokehitystä kannattaa jatkaa korjaamalla AAD-integraatio ja testaamalla jo suunniteltuja ratkaisuja sen kanssa.

Myöskin rahallisiin kustannuksiin pitäisi luoda jokin arvio. Opinnäytetyön yhteydessä tutustuin KV-järjestelmän lisenssimaksuihin ja maksukäytäntöihin, ja ne vaikuttivat kalliilta tämän käyttötarkoituksen osalta. En niihin itse perehtynyt syvemmin tai maininnut tässä opinnäytetyössä tämän enempää, koska niiden käsitteleminen laajentaisi aihealuetta liikaa. Rahalliset kustannukset voivat ajaa tämän kokonaisuuden hyvin kapeaan markkinarakoon, jolloin sen kehitys ei välttämättä olisi taloudellisesti kannattavaa. Tämän takia niiden selvitys olisi yhtä arvokasta kuin AAD-integraation korjaus.

8.4 Mitä opittiin ja mitä tekisin eri tavalla

Projekti oli omasta mielestäni liian laaja-alainen. Aihealue ja tekninen toteutus olivat kohtuullisesti rajattuja, mutta tietämystasoni ei ollut aivan riittävällä tasolla fyysisen turvallisuuden menetelmien suhteen. Minun olisi pitänyt hyödyntää toimeksiantajan fyysisen turvallisuuden ammattilaisten tietotaitoa työssä enemmän. Jatkokehityksessä kannattaisi luoda erillinen kehitysryhmä sekä digitaalisen-, että fyysisen turvan osaajista, jolloin osaaminen olisi kattavampaa.

Oma ymmärrykseni tietoturvasta kehittyi hyvin paljon fyysisestä turvallisuudesta oppimieni uusien näkökulmien kautta. Myöskin tiedonetsintätaidot kehittyivät, kun jouduin tutustumaan itselleni vieraaseen aiheeseen. Työn tekemisen aikatauluttaminen osoittautui päivätöiden ohella hankalaksi, mutta sen kautta opin myös päätöksentekotaitoa ja laittamaan asioita tärkeysjärjestykseen.

Lähteet

1. Loihde tilinpäätös tiedote 2020. Viitattu: 9.11.2021.
<https://www.loihde.com/wp-content/uploads/sites/2/2021/03/Viria-Oyj-Tilinpäätöstiedote-2020.pdf>
2. William Turton and Kartikay Mehrotra. Bloomberg. Artikkel Colonial pipeline kyberhyökkäyksestä. Viitattu: 12.11.2021
<https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>
3. Joe Tidy. BBC. Artikkel Coop-kauppaaketjun kyberhyökkäyksestä. Viitattu: 12.11.2021
<https://www.bbc.com/news/technology-57707530>
4. Jesse Mäntysalo. YLE. Voisiko Vastaamon kaltainen tietomurto toistua? Maanantaina voimaan tuleva laki tekee siitä erittäin epätodennäköistä, sanovat asiantuntijat. Viitattu: 12.11.2021
<https://yle.fi/uutiset/3-12162669>
5. Crowdstrike. Indicators of Compromise Explained. Viitattu: 12.11.2021
<https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/>
6. IBM. Why is SIEM important? Viitattu 12.11.2021
<https://www.ibm.com/topics/siem>
7. Jacobs J, Rudis B. Data-Driven Security : Analysis, Visualization and Dashboards. New York: John Wiley & Sons, Incorporated; 2014.
Created from kajaani-ebooks on 2021-11-10 09:19:15.
8. Baker PR, Benny DJ. The Complete Guide to Physical Security. London: Auerbach Publishers, Incorporated; 2012.
Created from kajaani-ebooks on 2021-08-03 07:28:19.
9. Kenyon B. ISO 27001 Controls - a Guide to Implementing and Auditing. Ely: IT Governance Ltd; 2019.
Created from kajaani-ebooks on 2021-07-23 12:42:52
10. MITRE. MITRE ATT&CK Framework Enterprise Techniques. Viitattu: 14.11.2021
<https://attack.mitre.org/techniques/enterprise/>
11. Microsoft. Azure Active Directory and Identity Protection documentation. Viitattu. 29.7.2021
<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

12. Microsoft. Azure Active Directory and Conditional Access documentation. Viitattu.
29.7.2021
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>
13. Elastic. Logstash Reference dokumentation. Viitattu: 11.11.2021
<https://www.elastic.co/guide/en/logstash/current/index.html>