Tampereen yliopisto

Erno Seppälä

ÄLYKKÄÄN TIETOTURVARATKAISUN HYÖDYT AUTOMAATIOSSA

Kandidaatintyö
Tekniikan ja luonnontieteiden tiedekunta
Toukokuu 2022

TIIVISTELMÄ

Erno Seppälä: Älykkään tietoturvaratkaisun hyödyt automaatiossa

Kandidaatintyö

Tampereen yliopisto

Teknisten tieteiden kandidaatin tutkinto-ohjelma

Toukokuu 2022

Tämä kandidaatintyö tutkii älykkään tietoturvaratkaisun hyötyjä automaatioympäristöissä kirjallisuuskatsauksen muodossa. Tutkimuksen kohteena oleva tietoturvaratkaisu on nimeltään SIEM (engl. Security Information and Event Management, SIEM). SIEM toimii lokienhallintajärjestelmänä ja analysoi lokimassoja. Työ aloitettiin tutkimalla, miten SIEM-järjestelmä käytännössä toimii, jonka jälkeen esiteltiin kohteena oleva automaatioympäristö ominaisuuksineen. Kohteena on yleisesti automaatioympäristö, joten varsinaista yksityiskohtaista kohdetta ei ollut saatavilla. Lopuksi selvitetään SIEM-ratkaisusta saatavia hyötyjä automaatiossa, sekä tutkitaan ratkaisun nykytilaa sekä mahdollista tulevaisuutta.

Merkittävimmät edut SIEM-järjestelmän käyttämisestä liittyvät uhkien yhä monipuolisempaan sekä älykkäämpään tunnistamiseen, johon perinteiset ratkaisut eivät täysin pysty. Tietoturvauhat kehittyvät jatkuvasti, joten myös niiltä suojaavat järjestelmät joutuvat kehittymään. Tietoturvaratkaisujen kehittäminen ei ole aina kuitenkaan niin yksinkertaista käytännön tai teknologian puolesta. Myös SIEM-järjestelmään liittyy haasteita sen elinkaaren aikana, ja myös näitä asioita sivutaan kandidaatintyössä.

Vaikka älykäs tietoturvaratkaisu tuo monia oleellisia etuja uhkantunnistamiseen, ei kyseisiä ratkaisuja ole vielä juurikaan käytössä teollisuudessa. SIEM-ratkaisun kaltaisia kilpailijoita on useita, mutta niiden ympärillä vallitseva asiantuntijuus ei ole riittävällä tasolla teollisuuden keskuudessa. Tämä johtaa osittain siihen, että myös ratkaisujen hinnoittelu on perinteisiä ratkaisuja huomattavasti korkeampaa. Teollisuudessa tietoturvallisuus ja sitä ylläpitävät järjestelmät kuluineen nähdään myös usein toissijaisina järjestelmän muun toiminnallisuuden ohella.

Vaikka älykkäät tietoturvaratkaisut eivät ole teollisuuden automaatiossa vielä nykypäivää, niiden voidaan olettaa yleistyvän, sillä IT-ympäristöissä (engl. Information Technology) ne ovat jo arkipäivää. Automaatio tulee tiedettävästi jäljessä teknologioiden kehittymisessä verrattuna IT-ympäristöihin.

Avainsanat: Security Information and Event Management, SIEM, Automaation tietoturvallisuus

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

AIC-malli	Availability, Integrity & Confidentally Model, automaation keskuudessa vallitseva malli, joka kiteyttää automaation perusvaatimukset. Tärkein mainitaan ensin.
CSV	Comma-separated values
CIA-malli	Confidentally, Integrity & Availability Model, IT-ympäristöjen malli, joka kiteyttää tärkeimmät tietoturvavaatimukset. Tärkein mainitaan ensin.
DCS	Distributed Control Systems, hajautettu ohjausjärjestelmä, nykyajan automaatiokokonaisuus, jossa yhdistyy IT-järjestelmien tiedon saatavuus ja OT-järjestelmien ominaisuudet.
ERP	Enterpise Resource Planning, liiketoiminnan toiminnanohjausjärjestelmä.
ICS	Industrial Control Systems, teollisuuden ohjaus -ja automaatiojärjestelmät.
IDS	Intrusion Detection System, automaatiossa yleisesti käytössä oleva mekanismi tietoturvauhkia vastaan.
IT	Information Technology
MES	Manufacturing Execution Systems, tuotannonohjausjärjestelmä.
OT	Operational Technology
PLC	Programmed Logic Controller, ohjelmoitava logiikka. Komponentti, joka on useasti osa systeemiä.
SCADA	Supervisory Control And Data Acquisition, valvovan tason tiedonkeruu- ja säätöjärjestelmä.
SIEM	Security Information and Event Management, lokien hallintajärjestelmä, joka pyrkii etsimään tietoturvauhkia ja tunnistamaan niitä.
SIEM 2.0	Security Information and Event management 2.0, SIEM-ratkaisujen uusi sukupolvi.
SIEM 3.0	Security Information and Event management 3.0, SIEM-ratkaisujen uusi sukupolvi.
SNMP	Simple Network Management Protocol

1. JOHDANTO

Digitalisaatio on kehittynyt viime vuosikymmenten aikana nopeasti. Teknologian kehitys on ulottunut myös automaatioon. Päivittynyt teknologia automaatiossa on tuonut runsaasti uusia huomioon otettavia asioita automaatiojärjestelmää suunniteltaessa. Nykyisin automaatiojärjestelmät ovat verkottuneita kokonaisuuksia, joilla on vastassaan samankaltaisia haasteita kuin IT-järjestelmilläkin (engl. Information Technology). Yksi isoimmista haasteista sekä tärkeimmistä osa-alueista automaatiojärjestelmää suunniteltaessa on turvallisuus ja luotettavuus.

Tämän työn tarkoituksena on perehtyä SIEM-järjestelmän (engl. Security Information and Event Management system) käytöstä saamiin hyötyihin automaatiossa. SIEM-järjestelmä on yksi niistä ratkaisuista, joilla tietoturvaa parannetaan niin IT-puolella kuin nykyään myös OT-puolella (engl. Operational tecnology). Aihe rajataan käsittelemään OT-puolen automaatiojärjestelmiä ja niissä käytössä olevia SIEM-järjestelmiä.

Automaatiojärjestelmiin liittyvissä tietoturvaratkaisuissa on aina myös tietynlaisia haasteita, ja niitä on myös SIEM-ratkaisujen käyttämisessä. Vaikka haasteita on olemassa, tämä työ käsittelee niitä vain pintapuolisesti. Sen sijaan tämän työn tarkoitus on keskittyä hyötyihin ja arvioida niitä yhdessä tietoturvallisuuden kanssa.

Automaatio kehittyy huomattavalla nopeudella, ja osittain siitä syystä automaation tietoturvallisuudesta löytyy paljon jo vanhentunutta materiaalia. Kirjallisuus on myös pääosin englanniksi, joten tässä työssä kootaan artikkeleista ja muusta kirjallisuudesta ajantasainen selvitys suomeksi. Tämän kandidaatintyön lukemalla lukija, esimerkiksi automaatiojärjestelmän hankintaa aikova taho, saa hyvän perustietämyksen SIEM-ratkaisujen hyödyistä automaatiossa sekä tietoa automaatiojärjestelmien nykytilasta sekä tietoturvahaasteista yleisesti.

Aluksi työssä käsitellään SIEM-ratkaisujen rakennetta sekä niiden perusideaa. SIEM-ratkaisut on alun perin suunniteltu IT-ympäristöihin, mutta tässä työssä niitä käsitellään teollisuuden automaatioympäristöihin sijoitettuna, vaikkakin myös IT-järjestelmät voivat olla tähän kokonaisuuteen yhteydessä. Tämän jälkeen työssä käsitellään automaatiojärjestelmiä ja määritellään automaatiossa vaadittava tietoturva. Kun työhön liittyvät pääkohteet on käsitelty, siirrytään tutkimaan SIEM-ratkaisujen tuomaa hyötyä

automaatioympäristöissä. Lopuksi työssä kerrotaan vielä päätelmistä sekä tutkimuksen tuloksista.

Työ tehdään erilaisia aiheeseen liittyviä artikkeleita hyväksikäyttäen. Suurin osa käytetyistä artikkeleista on vertaisarvioitu ja saatavilla internetissä. Lähdekirjallisuutena käytetään myös kirjoja sekä SIEM-järjestelmien jälleenmyyjien internetsivustoja. Kaikki käytetyt lähteet työn kirjoittaja on tarkasti arvioinut niiden soveltuvuuden kannalta.

2. SECURITY INFORMATION AND EVENT MANAGEMENT

Tässä luvussa käsitellään Security Information and Event Management -järjestelmää (SIEM). Jatkossa järjestelmästä käytetään sen lyhennettä SIEM, jotta työ pysyy mahdollisimman selkeänä käsittelyn aikana. Muutamat termit ovat englanniksi, sillä niille ei löytynyt sopivia käännöksiä suomen kielestä.

Ensimmäisessä alaluvussa kerrotaan SIEM:n rakenteesta ja sen perusideasta toimintaympäristössään. Sen jälkeen SIEM:n funktionaalisuus jaetaan viiteen alalukuun. Näissä luvuissa käsitellään järjestelmän toiminnallisuutta. Vaikka SIEM:n toimintaan osana lokienhallintaa kuuluu paljon muutakin, tämän työn tutkimuksessa käytetään vain tässä luvussa esiteltyä viittä osaa työn rajauksen vuoksi.

2.1 Yleistä

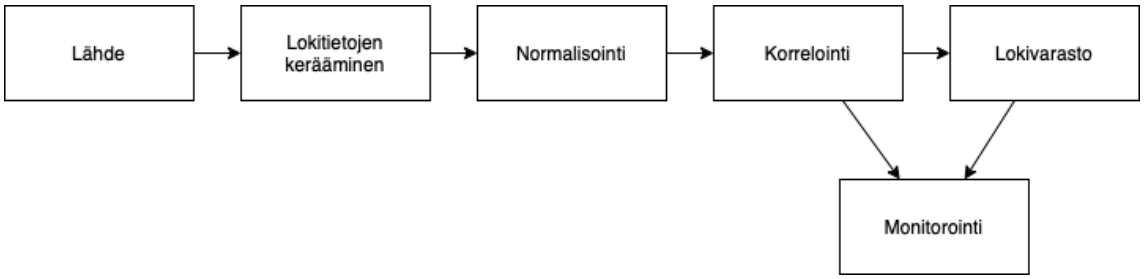
SIEM-järjestelmä on edistynyt tietoturvaratkaisu, jota käytetään usein IT-maailmassa. Sen päätehtävä on lokimassan hallinta, monitorointi sekä analysointi (Kostrekova & Binova 2015). SIEM-ratkaisut ovat usein myytäviä palveluja, joten niiden ylläpito saattaa olla ulkoistettua.

SIEM-ratkaisujen asiantuntijoita on vielä suhteellisen vähän OT-ympäristöissä, joten niiden ylläpito ja käyttöönotto saattaa olla kallista. Kattavan analysoinnin luominen vaatii myös pitkää valmistelua ja usein suuria kustannuksia, sillä analysoinnin toiminta vaatii ylläpitoa (Michelberger & Dombora 2016). SIEM-järjestelmä toimii useasti tavallisten tietoturvaratkaisujen ohella niin, ettei kumpikaan järjestelmä häiritse toisen toimintaa. SIEM-järjestelmiä tavataan OT-ympäristössä huomattavasti vähemmän, jos edes ollenkaan.

OT-ympäristöön liittyvät haasteet saattavat viitata esimerkiksi tietoturvaan varattuun budjettiin tai esimerkiksi automaatiojärjestelmien vanhaan ikään ja täten herkkyyteen. Myös erityisen reaaliaikaiset ja monimutkaiset ICS-järjestelmät (engl. Industrial Control Systems) voivat luoda haasteita, sillä SIEM-järjestelmä hyödyntää niissä liikkuvaa dataa. Tämä taas voi luoda viiveitä, sekä komponenttien kapasiteetin kantokyvyn ylitystä. (Salmenperä 2021)

2.2 Rakenne ja toimintaperiaate

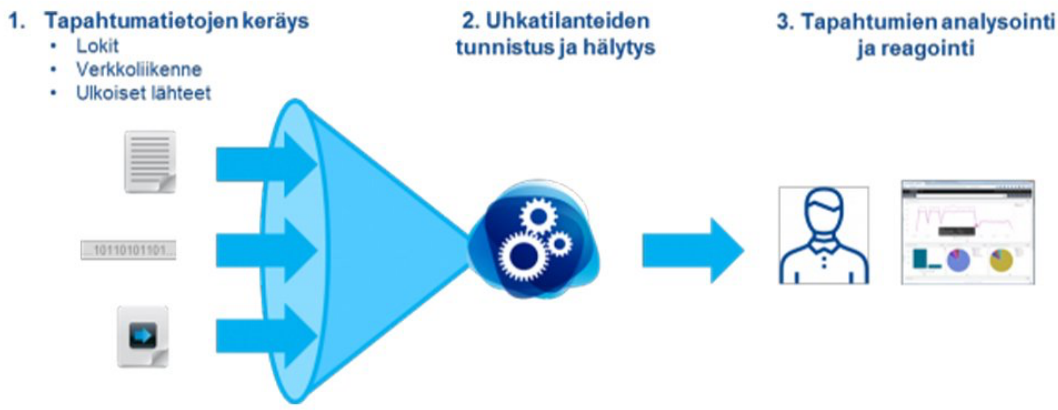
SIEM:iä voidaan luonnehtia monimutkaiseksi koneeksi, jossa on useita liikkuvia osia, joilla kaikilla on oma tehtävänsä. Jos yksikin koneen osa toimii väärin, koko systeemi toimii väärin. (Miller et al. 2011) SIEM-järjestelmä on usein siis hyvin monimutkainen, mutta sen toiminta voidaan silti jakaa karkeasti kuvan 1 tavalla kuuteen osaan.



Kuva 1. *SIEM-järjestelmä jaettuna kuuteen alisysteemiin (Miller, et al. 2011, s.81).*

Kuvassa 1 prosessi toimii niin, että ensin lähdelaitteelta, joka SIEM-järjestelmässä voi olla esimerkiksi palvelin, kerätään tietoa, jota kutsutaan lokitiedoksi. Tämän jälkeen lokitieto normalisoidaan ja jäsennellään jatkokäsittelyä varten. Jokaisessa SIEM-järjestelmässä jäsentelyn jälkeen tietoa korreloidaan ja tämän jälkeen se voidaan tallentaa lokivarastoon seurantaa varten. Osana järjestelmää lähdelaitteen lokitietoa voidaan monitoroida jopa reaaliajassa. Kuvassa 1 oleva lohkokaavio on purettu osiin tässä luvussa, ja jokaista alisysteemiä käsitellään tarkemmin omassa alaluvussaan.

SIEM-järjestelmän toiminta voidaan kuvata lohkokaavion ohella myös toisella kuvalla. Kuvassa 2 on esitetty SIEM:n toiminta käytännössä, kun se on liitetty esimerkiksi johonkin jo olemassa olevaan automaatiojärjestelmään.



Kuva 2. *SIEM:n periaatekuva (Kinnunen 2017).*

Kuvassa 2 on esitetty prosessi, jota SIEM käytännössä suorittaa. Prosessi on jaettu kolmeen eri vaiheeseen. Ensin kerätään tapahtumatietoja eli lokitietoja. Tapahtumatietoja voidaan kerätä periaatteessa mistä tahansa emojärjestelmän komponentista, josta dataa on mahdollista saada (Kotenko et al. 2013). Kun dataa on kerätty riittävästi, SIEM-järjestelmä suorittaa uhkatilanteiden tunnistusta sekä tarvittaessa hälytyksiä, jos tilanne niin vaatii. Mikäli hälytyksistä on aihetta ilmoittaa, kolmannessa vaiheessa esimerkiksi operaattori näkee kyseisen hälytyksen ja analysoi vielä manuaalisesti tilannetta, jonka jälkeen mahdollisesti reagoi siihen. Kuvasta 2 nähdään siis, että SIEM-järjestelmä on hyödyllinen työkalu, jolla pystytään tunnistamaan erilaisia uhkia ja analysoimaan jatkuvasti ja automaattisesti prosessin toimintaa. Sen etuna on kuvan 1 mukainen kyky tallentaa lokitietoja pidemmälle aikavälille, jotta esimerkiksi hitaasti näkyvät tunkeutumiset huomataan.

2.3 Lokitietojen kerääminen lähdelaitteelta

Kuvasta 1 havaittiin, että SIEM-järjestelmän prosessi alkaa lokitietojen keräämisellä lähdelaitteelta. Lokitiedolla tarkoitetaan jonkin tapahtuman tunnistamista tärkeäksi ja sen seurauksena sen tallentamista (Sandeep et al. 2014). Lokitiedot ovat tärkeässä asemassa SIEM-järjestelmän toiminnan kannalta, sillä ne toimivat analysoinnin

lähteinä ja pohjana jatkuvasti, kun lokeja prosessoidaan. Lokeja tai tapahtumatietoja kerätään järjestelmästä, jota halutaan suojata. Tietoa voidaan kerätä esimerkiksi antureilta tai muilta järjestelmän komponenteilta. (Coppolino et al. 2016) Lähdelaite ei kuitenkaan varsinaisesti kuulu SIEM-järjestelmään, vaan suojattavaan järjestelmään, mutta se on SIEM:n kannalta oleellinen osa kokonaisuudessa.

Loki- ja tapahtumatietojen keräämistavat vaihtelevat riippuen SIEM-toteutuksesta, mutta yleisesti tietojen kerääminen voidaan jakaa kahteen eri metodiin. Nämä metodit ovat tiedonlähetys (engl. Push Log Collection) ja tiedonhakeminen (Engl. Pull Log Collection). Jatkossa käytetään englanninkielisiä versioita metodeista, sillä varsinaisia suomenkielisiä käännöksiä ei löytynyt.

2.3.1 Lokitietojen lähettäminen lähdelaitteelta

Push Log Collection -metodia käytettäessä lähdelaite lähettää lokitietoja SIEM-järjestelmälle suoraan. Toteutuksena *Push Log* on huomattavasti helpompi ja sen konfigurointi on suoraviivaisempaa, sillä lähdelaitteelle ei tarvitse kertoa muuta kuin SIEM-serverin IP-osoite. Yleisimmät lähdelaitteelta automaattisesti lähetettävät datamuodot ovat SYSLOG, SNMP (engl. Simple Network Management Protocol) ja Windows Event Log. (Moukafih et al. 2019)

Mikäli louhinta suoritetaan tätä metodia hyödyntäen, täytyy lähdelaitteen tukea tunnettuja protokollia, kuten SYSLOG:ia. Lähdelaitteen logiikkaan voi myös olla toteutettuna agentti, jonka vastuulla on lokitietojen välittäminen SIEM:lle. Näiden seikkojen lisäksi louhinta voi olla myös integroituna tietovirtaan. (Vielberth & Pernul 2018)

2.3.2 Lokitietojen hakeminen lähdelaitteelta

Lokitietojen hakeminen eroaa edellisestä metodista sen toteutustavan puolesta. Kun Syslog-palvelin vastaanottaa lokitietoja lähdelaitteelta ja jakaa sitä eteenpäin SIEM-järjestelmälle, se ei pysty erikseen tarkastelemaan sitä, saapuvatko lähdelaitteelta lähteneet syslog-viestit palvelimelle ja ovatko viestit hyödyntämiskelpoisia (Miller et al. 2011, s.82). Lokitietojen hakemisessa ideana on, että palvelin hakee tiedot itse lähdelaitteelta (Moukafih et al. 2019).

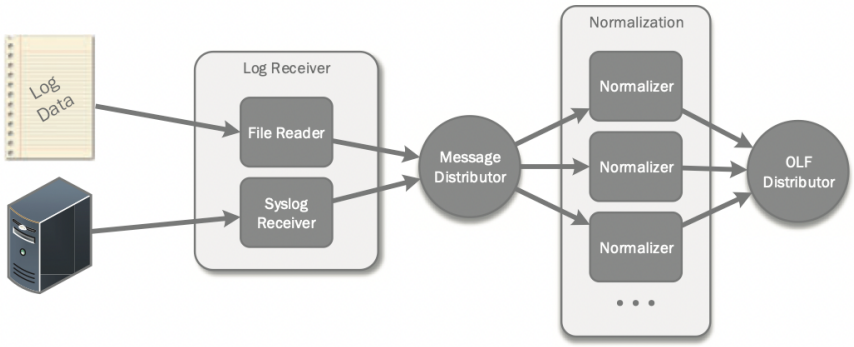
Kun palvelin hakee lokitietoa lähdelaitteelta, se tunnistaa lähdelaitteen ennen tiedon vastaanottamista ja näin ollen on tietoinen hyödyllisestä lokitiedosta. Tämän metodin ongelmana voidaan kuitenkin yleisesti pitää sitä, että se ei ole ainakaan automaattisesti reaaliaikainen. Tiedon lähettäjä lähettää lokitietoa automaattisesti heti, kun sitä

regeneroituu lähdelaitteelta, mutta tätä tapaa hyödynnettäessä tiedot täytyy noutaa aika ajoin itse, josta voi tulla viivettä. (Miller et al. 2011 s.82)

2.4 Lokitietojen jaottelu ja normalisointi

Lokitiedot esiintyvät järjestelmissä usein monessa eri muodoissa. Jotta SIEM-järjestelmä pystyy prosessoimaan ja hyödyntämään saamaansa lokitietoa, ne täytyy ensin muuttaa tiettyyn muotoon. Lokitietoa voidaan saada monesta eri lähteestä, joten jokainen tapahtumatieto täytyy saada eroteltua ja muutettua samaan muotoon. Usein Windows-pohjaisissa järjestelmissä käytetään CSV-muodossa (engl. comma-separated values) olevaa parsittua lokitietoa. (Coppolino et al. 2016)

Tapahtumalokien normalisointi on hankala prosessi, mutta usein se on integroituna SIEM:iin. Esimerkiksi järjestelmään kirjautuminen voidaan joissakin tapauksissa tehdä käyttäjätunnusten eri ilmentyminä. Tällöin tärkeää on normalisoida tieto niin, että SIEM ymmärtää näiden kaikkien kirjautumisten takana olleen sama taho riippumatta kirjoitusasusta. (Coppolino et al. 2016) Alla olevassa kuvassa 3 on esitetty datan normalisointi lohkokaavioiden avulla.



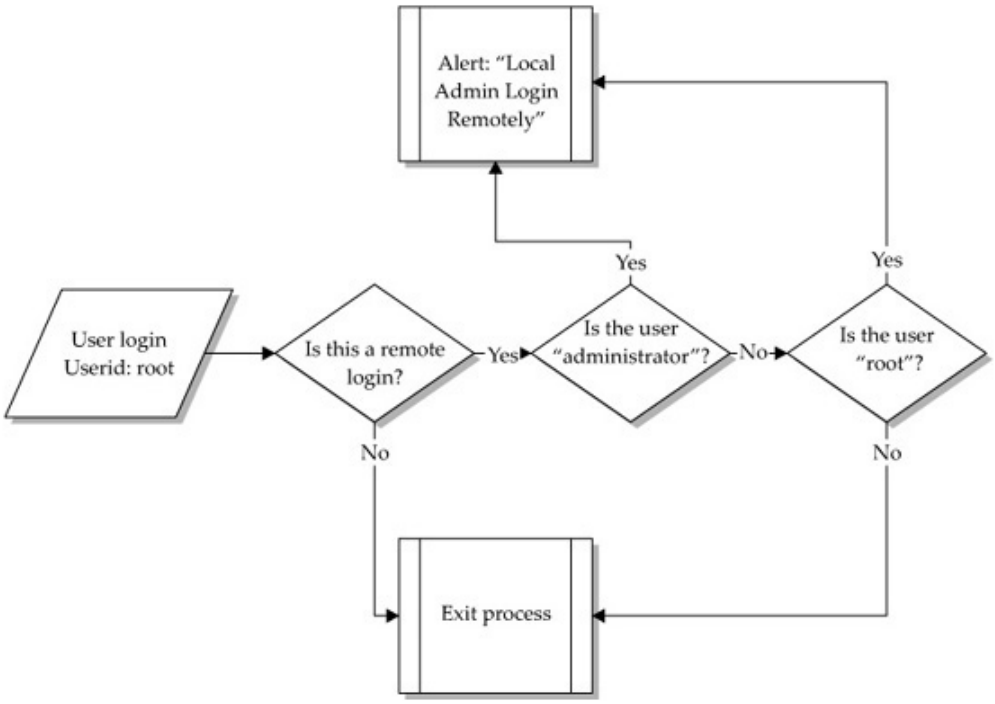
Kuva 3. *Datan normalisointi (Jaeger et al. 2015)*

Kuvassa 3 on esitetty normalisoinnin työnkulku. Ensin dataa tuotetaan ja se hankitaan SIEM-järjestelmää varten. Kun halutut tiedot on kerätty eri komponenteilta, ne tallennetaan väliaikaisesti lokitietoja vastaanottavalle komponentille. Kun tiedon louhinta on valmis, kerätyt lokitiedot jaetaan tapahtumien mukaan omiin tietorakenteisiin. Nämä erilliset tietorakenteet, jotka siis sisältävät jokainen tietoa yhdestä tapahtumasta, johdetaan seuraavaksi komponentille, joka hoitaa varsinaisen normalisoinnin. Normalisoinnilla tarkoitetaan siis prosessia, jossa tapahtumatiedot yhdenmukaistetaan sekä

jaotellaan tiettyjen sääntöjen mukaan, jotta niitä pystyttäisiin tulkitsemaan yhdestä paikasta yhden elimen toimesta (Sandeep et al. 2014).

2.5 Korrelaatio ja ehdollinen käsittely

Korrelointi on metodi, jolla SIEM-järjestelmä yhdistää useita eri lähteistä saatuja lokitapahtumia yhdeksi suureksi tarkasteltavaksi tapahtumaketjuksi, jota on tarkoitus katsoa yhtenä kokonaisuutena (Miller et al. 2011 s.87). Korrelaation aikana SIEM-järjestelmä pyrkii löytämään tapahtumien yhteyksiä toisiinsa hyödyntäen monimutkaista matemaattista mallinnusta (Michelberger & Dombora 2016). Kuvassa 4 on havainnollistettu, kuinka korrelaatio voidaan esimerkiksi toteuttaa.



Kuva 4. *Korrelaation esimerkki (Miller et al. 2011 s.87).*

Kuvassa 4 on esitettynä tilanne, jossa SIEM tarkastelee samanaikaisesti Linux-käyttöjärjestelmän sekä Windows-käyttöjärjestelmän kirjautumisyrityksiä. Korrelaation avulla pystytään löytämään eri tapahtumien välille yhteyksiä ja luomaan näistä tapahtumista isompia kokonaisuuksia. Tämän tiedon avulla tapahtumat voidaan muuttaa hyödylliseen tiedostomuotoon, josta kokonaisuuden tilaa pystytään tarkastelemaan. Mikäli järjestelmä havaitsee automatisoidun analysoinnin yhteydessä jotakin epäilyttävää, se kykenee ilmoittamaan siitä käyttäjälle (Kostrekova & Binova 2015).

SIEM-järjestelmässä on myös muita ohjelmoituja ominaisuuksia, joiden perusteella järjestelmän toimintaa ohjataan. Yleinen käytössä oleva suojausmenetelmä ja seurantakohde on sisäänkirjautumisyritysten lukumäärä. Sen mukaan voidaan esimerkiksi laskea ja seurata, kuinka monta kertaa samasta IP-osoitteesta yritetään kirjautua suojattuun järjestelmään sisään. (Miller et al. 2011 s.87)

Tapahtumien oikeanlainen tunnistaminen edellyttää onnistunutta korrelaatiota. Korrelaation oikeanlainen konfigurointi on siis tärkeässä asemassa järjestelmän kokonaisuuden toiminnan kannalta. (Gonzalez-Granadillo et al. 2021) Korrelaatio vaatii paljon laskentatehoa, jonka vuoksi se usein suoritetaan esimerkiksi aina tiettynä aikana päivästä.

2.6 Lokitietojen tallentaminen

Lokitietojen tallentaminen tapahtuu usein joko tietokantaan, tekstitiedostoon kuten CSV-tiedostoon tai binääritiedostoon. Tallennusmuoto riippuu SIEM-järjestelmän suunnitteluvaiheessa tehdyistä päätöksistä sekä mahdollisesti käyttötarkoituksista. Esimerkiksi tekstitiedostoa käytettäessä usein pyritään siihen, että lokitiedot ovat selkeästi luettavissa. (Miller et al. 2011 s.90)

Lokitietoja voidaan tallentaa fyysiseen sijaintiin kiintoasemalle, mutta yhä useammin vaihtoehtona on myös pilvipalveluiden käyttäminen, jolloin tiedon organisointi on saatavuutensa vuoksi helppoa. Automaatiojärjestelmän tuottama lokimassa voi olla kooltaan hyvin suurta, joten tiedontallennukseen liittyvät teknologiset kysymykset ovat tärkeitä.

2.7 Monitorointi

Kun kaikki prosessin esivaiheet on suoritettu, voidaan tarkastella lokitietoja sekä niistä saatavia analyyseja. Monitorointia voidaan suorittaa yleensä järjestelmän oman sovelluksen kautta. Sovelluksesta voidaan tarkastella erilaisia asioita visuaalisesti, joita järjestelmän on tarkoitus esittää (Kostrekova & Binova 2015).

Varsinkin automaatiossa monitorointi sekä sen mahdollistaminen on tärkeää, sillä erilaisten tapahtumien tila- ja lokitietoja täytyy päästä tarkastelemaan. Vaikka monitorointia voidaan suorittaa myös manuaalisesti, SIEM-järjestelmä analysoi myös automatisoidusti lokitietoja muodostaen tiedoista esimerkiksi raportteja (Kostrekova & Binova 2015).

Visuaalinen esitystapa tapahtumatietojen tilasta ja tietoturvatilasta on informatiivinen ja sen ymmärtäminen voi olla muita esitystapoja helpompaa. Se on myös paljon

havainnollistettavampi verrattuna muihin esitystapoihin. Tutkinnan osalta raakatieto on kuitenkin oleellisessa asemassa, eikä visuaalisuus välttämättä paljasta tietoa yhtä yksityiskohtaisesti.

3. AUTOMAATIO JA TIETOTURVA

Yleisesti automaatiojärjestelmiä on monissa eri kohteissa. Tässä työssä automaatiojärjestelmillä kuitenkin viitataan vain teollisuudessa esiintyviin automaatio- ja ohjausjärjestelmiin. (engl. Industrial Control Systems, ICS)

Tässä luvussa käsitellään automaatiojärjestelmiä sekä oleellisesti niiden työhön vaikuttavia osa-alueita. Ensin käsitellään automaatiojärjestelmien taustaa yleisesti, jonka jälkeen tutkitaan hieman järjestelmien toteutusta ja niiden merkitystä teollisuudessa. Tämän pääluvun lopuksi tutkitaan vielä automaatiojärjestelmien turvallisuusvaatimuksia teollisuudessa.

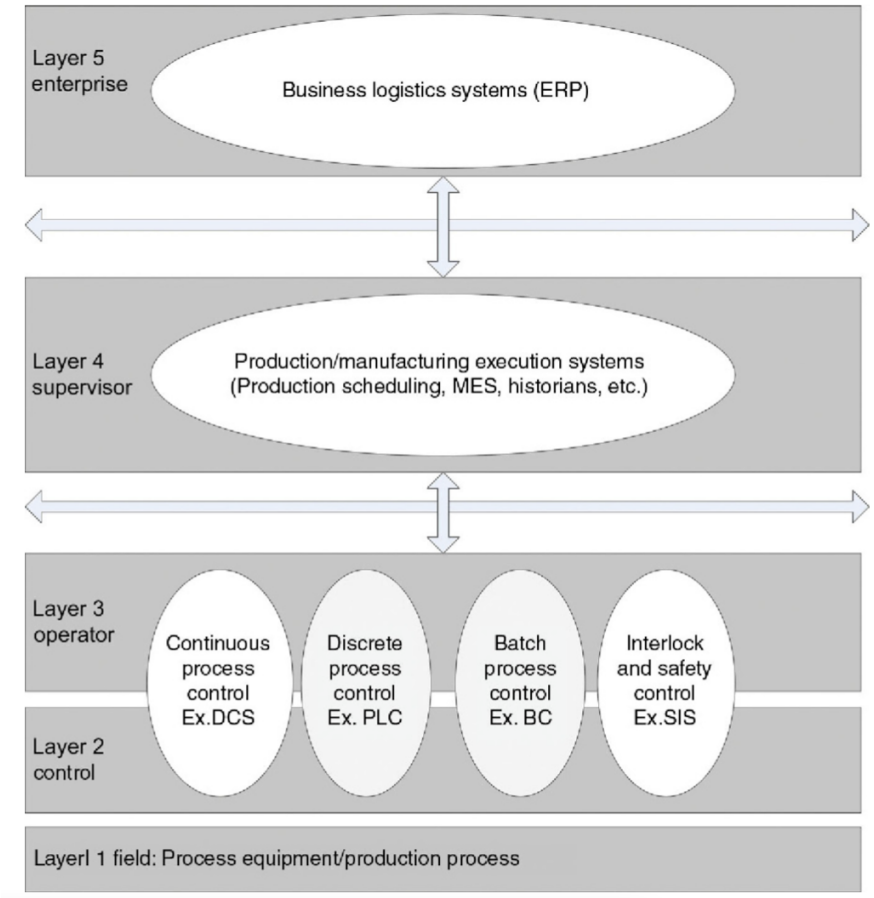
3.1 Automaatiojärjestelmät

Automaatiojärjestelmä on verkottunut pitkän elinkaaren ohjelmistotuote. Sen tehtävä on fyysisen prosessin automaattinen hallinta ja ihmiselle ongelmanratkaisuun tarvittavan valvontatiedon tuottaminen. (Seppälä 2022) Automaatiojärjestelmät siis toteuttavat erilaisia tehtäviä ihmisen puolesta. Vaikka automaatio tuo helppoutta prosessien hallintaan, se tuo myös tarkkuutta prosessien valvontaan. Joitakin mittauksia ei välttämättä pystytä edes suorittamaan ihmisen toimesta turvallisesti, kuten esimerkiksi sellaisia mittauksia, jotka joudutaan suorittamaan korkeassa lämpötilassa tai hapettomassa tilassa. Turvattomien mittausten toteuttaminen ei siis olisi edes mahdollista ilman automaatiota.

3.1.1 Rakenne

Automaatiossa olevat tietoliikenneratkaisut sekä ohjelmistot, jotka toteuttavat tai tukevat automaatiota ovat määrällisesti kasvaneet koko ajan. Tyypillistä edellä mainituille osakokonaisuuksille on myös se, että niitä harvoin toimittaa ja ylläpitää yksi toimittaja. (Ahonen et al. 2021, s.170) Automaation eri tasoilla on siis useita eri toimijoita, mutta myös teknologioita, jotka tekevät samoja tai eri asioita suuressa mittakaavassa. Tästä voidaan päätellä, että kompleksisuus on tyypillistä automaatiossa.

Automaatiojärjestelmät voidaan jakaa viiteen eri tasoon niiden toiminnallisuuksien perusteella. Kuvassa 5 on havainnollistettu automaation tasoja.

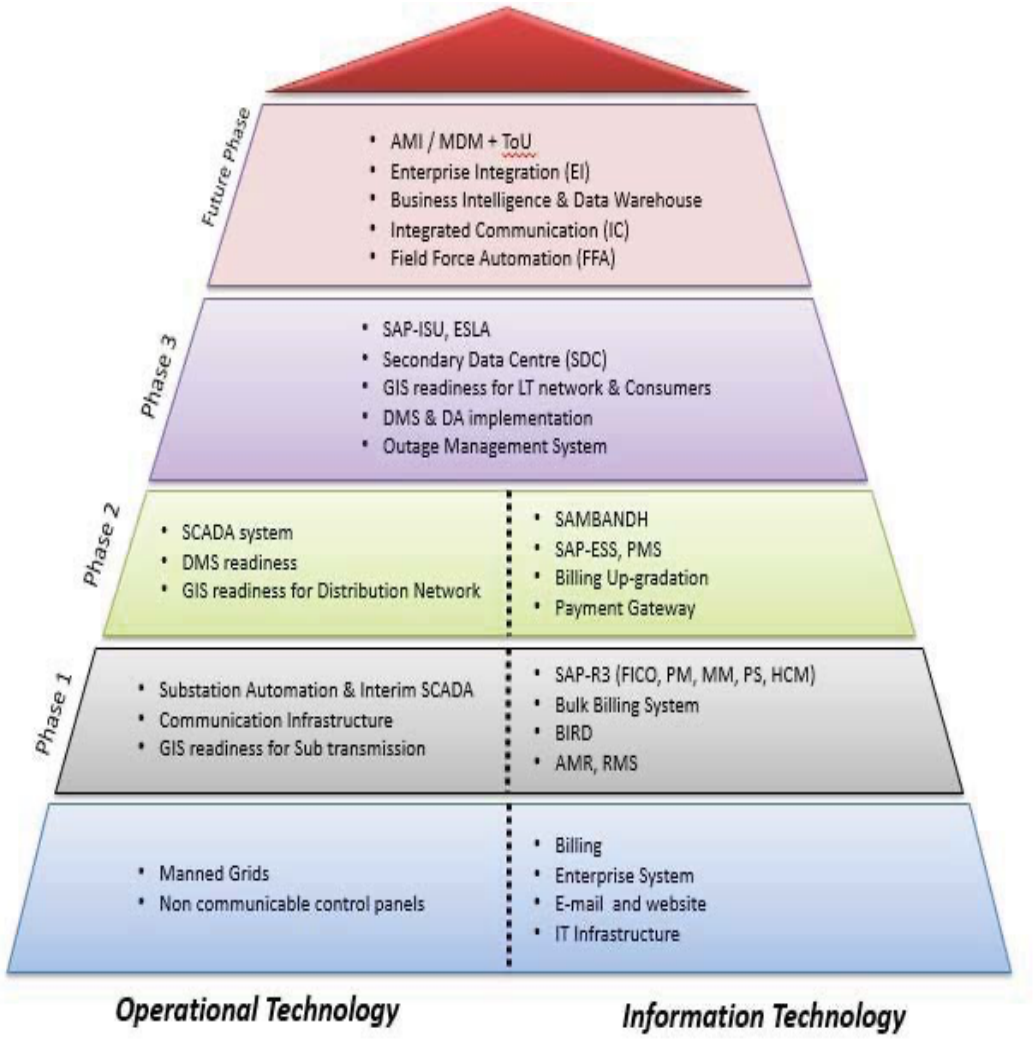


Kuva 5. *Automaation tasot (Di Sarno et al. 2016).*

Alimmalla tasolla on itse prosessi, johon automaatio on yhteydessä. Tasolla kaksi ja kolme sijaitsee ohjelmoitavat logiikat (engl. Programmed Logic Computer, PLC) sekä hajautetut järjestelmät. (engl. Distributed Control Systems, DCS) Näitä järjestelmiä hallinnoi pääsääntöisesti operaattorit, joilla on pääsy ainoastaan näiden tasojen järjestelmiin. Esimerkiksi PLC:ssä on ohjelmoituna toimintoja, joilla se ohjaa prosessia automaattisesti tai operaattorin avustuksella. Tasolla kolme sijaitsee myös valvontaan erikoistuneet automaatiojärjestelmät (engl. Supervisory Control and Data Acquisition, SCADA), jotka tuottavat operoinnissa tarvittavaa tietoa. Tasolla neljä sijaitsee tuotannonohjausjärjestelmät (engl. Manufacturing Execution Systems, MES) sekä tasolla viisi toiminnanohjausjärjestelmät (engl. Enterpise Resource Planning, ERP).

3.1.2 Automaation merkitys

Automaation merkitys teollisuudessa on kasvanut ajan saatossa huomattavasti. Nykyajan teollisuudessa yhdistyvät IT-järjestelmät sekä OT-järjestelmät, jotka muodostavat kuvan 6 kaltaisen kokonaisuuden.



Kuva 6. *IT- ja OT-järjestelmien yhteensulautuminen (Montesino et al. 2012).*

Kuvasta 6 huomataan, että IT-järjestelmät ovat liittyneinä internettiin. OT-järjestelmät ovat taas yhteydessä IT-järjestelmiin. Täten esimerkiksi hakkerit voivat hyödyntää tätä integraatiota hyökkäyksissään ja päästä käsiksi myös OT-järjestelmien tietoihin (Gonzalez-Granadillo et al. 2021). Vaikka IT- ja OT-järjestelmät ovat sulautuneet yhteen, OT-järjestelmät keskittyvät pääosin prosessien monitorointiin ja säätämiseen (Hahn 2016).

Automaatiojärjestelmien ominaisuuksia voidaan analysoida monilla eri tavoilla. Yksi tapa oikean suunnitteluperiaatteen löytämiseen on tunnistaa kolme tärkeintä ominaisuutta: tiedon saatavilla oleminen (engl. Availability), järjestelmien ja tiedon eheys (engl. Integrity) sekä tiedon luottamuksellisuus (engl. Confidentiality). Nämä kolme muodostavat yhdessä AIC-mallin, (engl. Availability, Integrity & Confidentally Model) joka on anagrammi IT-järjestelmien keskuudessa esiintyvästä CIA-mallista (engl. Confidentally, Integrity & Availability Model). (Salmenperä 2021) Tästä voidaan päätellä, että automaatioympäristöissä korostuu erilaiset ominaisuudet. Vaikka IT- ja OT-järjestelmät sisältävätkin samoja vaatimuksia, ei eri ympäristöjen keskuudessa painoteta ominaisuuksia samalla tavalla. Automaatiojärjestelmien tärkein ominaisuus on havaittavuus, sillä sen avulla ylimääräiset viiveet sekä tuottavuuden heikentyminen saadaan minimoitua (Sadeghi et al. 2015).

Automaation kannalta tärkeää on reaaliaikaisuus ja sen toteutuminen. Joidenkin prosessien ohjaus vaatii tarkkuutta ja reaaliaikaisuutta järjestelmältä. Reaaliaikaisuudella tai tosiaikaisuudella pyritään prosessin tehokkuuteen. Automaatiojärjestelmät myös suunnitellaan pitkälle toiminta-ajalle, jolloin järjestelmien toimintavarmuus jopa vuosien päästä täytyy olla luotettavalla tasolla. (Automaatioseura 2005, s.57-62)

3.2 Turvallisuus

Teollisuuteen suunniteltujen automaatiojärjestelmien suunnittelu on keskittynyt enimmäkseen järjestelmän eri toiminnallisuuksiin ja niiden kehittämiseen. Usein järjestelmien laitteisto ei ole uusinta sukupolvea, eikä täten kykene suoraan vastaamaan tietoturvauhkiin. (Gonzalez-Granadillo et al. 2021)

Automaation kannalta tietoturva on nykyään yhä tärkeämmässä asemassa. Teollisuuden automaatiojärjestelmiin kohdistuvat tietoturvariskit ovat kasvaneet viime vuosien aikana valtavasti. Suurin syy tietoturvariskien lisääntymiseen on ollut valtioiden sekä kyberrikollisten lisääntynyt liikkuvuus. (Gonzalez-Granadillo et al. 2021)

Automaation tietoturvallisuuden merkityksen ymmärtämiseksi on hyvä ymmärtää, millaisia eroja OT-järjestelmillä on verrattuna IT-järjestelmiin. IT-järjestelmien keskuudessa olleita ratkaisuja sovelletaan nyt myös OT-ympäristöissä. OT-ympäristöissä turvallisuus on kuitenkin yhdessä saatavuuden kanssa niin tärkeässä asemassa, että se aiheuttaa rajoitteita tietoturvallisuuden hyödyntämisessä. Myös fyysinen turvallisuus aiheuttaa haasteita, sillä IT-järjestelmissä ei ole fyysisiä prosesseja, joita tulisi ottaa huomioon. (Hahn 2016)

Tässä luvussa käsitellään turvallisuuden merkitystä teollisuudessa. Turvallisuus kattaa myös tietoturvallisuuden ohella prosessin turvallisuuden. Tietoturvallisuus voidaan jakaa eri osa-alueisiin, mutta tässä työssä perehdytään SIEM:n kannalta tärkeisiin osa-alueisiin, eli fyysiseen tietoturvaan sekä ohjelmistojen kannalta vaadittavaan tietoturvaan. Oleellisien tietoturvakatsauksien jälkeen käsitellään teollisuudessa jo tapahtuneita tietoturvaiskuja ja sitä, miten niiden tapahtuminen on vaikuttanut oleellisesti tietoturvallisuuden tilanteeseen.

3.2.1 Fyysinen tietoturva

Fyysinen tietoturva ottaa kantaa sellaisiin asioihin, joihin ihmiset vaikuttavat omalla toiminnallaan. Fyysinen tietoturva käsittelee nimensä mukaisesti fyysisiä asioita, jotka aiheuttavat uhkia. Esimerkiksi luvaton fyysinen pääsy järjestelmään tai tiedon joutuminen esimerkiksi puhuttuna vääriin käsiin ovat tämän kaltaisia uhkia. (Gonzalez-Granadillo et al. 2021)

Fyysisen tietoturvan ylläpito on haastavaa, sillä perinteiset ratkaisut eivät kykene tarkkailemaan yksilön toimia järjestelmän ulkopuolella. Fyysinen tietoturva pitää sisällään myös monia eri muuttujia, joten turvallisuuden mallintaminen ei ole yksiselitteistä. Fyysinen turvallisuus on kuitenkin tärkeä osa kokonaisvaltaista tietoturvallisuutta.

3.2.2 Ohjelmistoihin ja toiminnallisuuksiin liittyvä tietoturva

Automaatioympäristön suurin uhka on nykypäivänä ohjelmistoihin ja toiminnallisuuksiin liittyvä tietoturva. Ohjelmistot ja toiminnallisuudet liittyvät siinä määrin yhteen, että ohjelmistoilla toteutetaan erilaisia toiminnallisuuksia. Tämä tarkoittaa sitä, että ylemmän tason järjestelmä voi ohjata alemman tason järjestelmää, joka taas ohjaa kenttälaitteita, jotka tekevät toiminnallisuuksia.

Ohjelmistoihin liittyvä tietoturva on siis erittäin tärkeä osa kokonaisvaltaista tietoturvallisuutta. Automaatioympäristössä sijaitsevat ohjelmistot toteuttavat usein tarkkuutta vaativia toimintoja, joten niiden manipuloiminen voi aiheuttaa suurta häiriötä prosessille. Ne eivät siis kestä paljoakaan kaltoinkohtelua ilman negatiivisia vaikutuksia järjestelmän toiminnassa.

Automaatiojärjestelmiin liittyvien AIC-mallin mukaisten vaatimusten lisäksi myös tietoturvalta vaaditaan samankaltaisia ominaisuuksia. Tietoturvaratkaisujen tulee pystyä tunnistamaan poikkeuksia dataliikenteessä reaaliaikaisesti, jotta esimerkiksi haittaohjelmat havaitaan aikaisessa vaiheessa. Tietoturvaloukkauksen tapahtuessa tilanteista

pitäisi pystyä myös palautumaan mahdollisimman suoraviivaisesti ja nopeasti. Tietoturvalta edellytetään myös älykästä visuaalista ilmentymää, josta pystytään tunnistamaan kaikki verkkoon liitetyt komponentit ja niiden välillä tapahtuva liikennöinti suoraviivaisesti. (Gonzalez-Granadillo et al. 2021)

3.2.3 Haavoittuvuuksien kautta asenteiden muutoksiin

Aiemmin automaatioympäristöjen yksi suurimmista tietoturvallisuusuhkista oli fyysisen tietoturvan pettäminen. Viimeisen 20 vuoden aikana teollisuuden vallankumous on kuitenkin näyttänyt, että teollisuudessa vakavaksi ja suureksi uhaksi on muodostunut ohjelmistojen pettäminen internetissä käytettyjen tietoliikenneratkaisujen avustuksella.

Teollisuus ja sen sisällä oleva automaatio kehittyy erittäin hitaasti verrattuna IT-maailman tietojärjestelmiin. Yksi syy tähän on se, että automaatio käsittää usein hyvin monimutkaisen ja monitasoisen suuren kokonaisuuden, jonka päivittäminen vaatii ennen kaikkea järjestelmän luotettavaa toimintaa myös jatkossa. Tämä taas vaatii todella paljon erilaista käytännön testausta ohjelmistojen osalta, koska jokainen automaatiojärjestelmä on oma integraationsa, ei yleispätevää testausta ainakaan yleisesti voida tehdä.

Vuonna 2010 Iranin teollisuudesta löydettiin ensimmäinen haittaohjelma, joka oli sijoitettu SCADA-järjestelmään. Tämä kyseinen haittaohjelma oli nimeltään Stuxnet, ja se ei ainoastaan vakoillut kohdettaan, vaan pyrki myös uudelleenohjelmoimaan sitä. Stuxnet tunkeutui Siemensin suunnittelujärjestelmään, joka toimi työkaluna prosessinohjauksen muuttamisessa. Suunnittelujärjestelmät ovat automaation ohjelmoiintiin ja suunnitteluun käytettäviä erikoisohjelmistoja sisältäviä IT-järjestelmiä. Tästä johtuen Stuxnet-vakoiluohjelmalla oli kyky manipuloida kenttätason laitteiden toimintaa. (McMillar 2010)

Nykyaikaiset haittaohjelmat, jotka toimivat verkon ylitse, ovat siis uhkia myös automaatiolle. Stuxnet on hyvä esimerkki siitä, että vasta haavoittuvuuden löytymisen jälkeen siihen osattiin varautua. Järjestelmiä kohtaan oleva asenne siitä, että automaatioympäristö ei tarvitsisi samankaltaista huomiota tietoturva-asioissa on muuttunut. 2010-luvulla kyberturvallisuusuhat teollisuusjärjestelmissä olivat jo suuren yleisön tiedossa, joten niiden vakavuus on omaksuttu ainakin Suomessa (Ahonen et al. 2019).

4. ÄLYKKÄÄN TIETOTURVARATKAISUN KÄYTTÄMISESTÄ SAADUT HYÖDYT AUTOMAATIOSSA

Tässä luvussa keskitytään tutkimaan kandidaatintyön päätutkimuskysymystä, eli millaisia hyötyjä SIEM-ratkaisun käyttämisestä saavutetaan. Hyötyjä on monia ja ne on siksi erotettu väliotsikoin toisistaan.

4.1 Lokien jatkuva analysointi

Automaatiojärjestelmä tallentaa lokitietoja jatkuvasti monista eri lähteistä. Tästä johtuen lokitiedot voivat sijaita monessa eri tallennuspaikoissa, johon ne saattavat hukkua helposti. Lokitiedot taltioidaan usein erilaisille servereille, josta niihin pääsee myöhemmin käsiksi. Tiedot voivat kuitenkin olla toisiinsa nähden erilaisissa tiedostomuodoissa, jolloin niiden tulkitseminen ei ole yksiselitteistä. Lokien analysointi ainakaan automatisoidusti ei ole helposti toteutettavissa tästä syystä. (Qingrong et al. 2017)

SIEM-järjestelmä kykenee tallentamaan kaikki sen taltioimat lokitiedot samaan sijaintiin, jolloin niiden analysointi automatisoidusti on huomattavasti helpompaa. SIEM-järjestelmän ansiosta dataa pystytään analysoimaan jatkuvasti ja tunnistamaan mahdolliset uhat yhä nopeammin.

Automaatiokomponentit tuottavat suuren määrän lokitietoa, joka on vaikeasti tulkittavaa ja täten vaikeasti analysoitavissa automaattisesti (Ahonen et al. 2021, s.175). SIEM toimii työkaluna lokienhallinnassa ja sen ominaisuuksiin lukeutuu myös lokien automatisoitu analysointi.

4.2 Nopeus ja kyky tunnistaa haittaohjelmia

SIEM-järjestelmä kykenee tekemään lähes reaaliaikaista analyysiä saamastaan tapahtumatiedosta. Automaatiojärjestelmä, joka käyttää esimerkiksi IDS-ratkaisuja (engl. Intrusion Detection System, IDS) kykenee tunnistamaan tietoturvauhkia, mutta se ei kykene automaattisesti niin nopeaan toimintaan, kuin SIEM-järjestelmä. Tämä on SIEM:n normalisoinnin ansiota, joka muuntaa lokivirtaa yhtenäiseen muotoon, jonka ansiosta erilaiset vaikutukset voi olla helpompaa havaita koko prosessin mittakaavassa. Tämän ansiosta haittaohjelmien havaitseminen on nopeampaa, sillä yhden lokilähteen

tuottama tieto ei välttämättä kerro uhkasta tarpeeksi ajoissa. SIEM- järjestelmällä on kyky analysoida miljoonia tapahtumia reaaliajassa, sekä tehdä välittömiä toimia uhan löytyessä. (Gonzalez-Granadillo et al. 2021)

Automaatiojärjestelmiin kohdistuvat tietoturvauhat kuten haittaohjelmat eivät välttämättä aiheuta aggressiivista tuhoa järjestelmän toiminnan kannalta. Hitaasti eteneviä uhkia saattaa olla siitä syystä haasteellista havaita. Lokitiedon analysointi voi myös olla paikallista (Ahonen et al. 2021, s.82). Paikallinen lokienhallinta voi myös vaikuttaa uhkien tunnistusnopeuteen. SIEM-järjestelmästä saatava hyöty on kyky suorittaa kohdejärjestelmän tilan normalisointi, jonka johdosta se kykenee tunnistamaan haittaohjelmien toiminnan helpommin. Se kykenee havaitsemaan tilojen pienet muutokset ja ilmoittamaan muutoksista järjestelmän käyttäjälle, mikäli niihin ei löydy järkevää selitystä.

Haittaohjelmia vastaan on saatavilla useita eri ratkaisuja, kuten virustorjuntaohjelmistot, mutta niiden käyttäminen automaatiojärjestelmässä ei ole itsestäänselvyys, koska automaatiojärjestelmät ovat usein hyvin tarkasti ja rajoitetuin kapasiteetein rakennettu (Automaatioseura 2005, s.24). Muun muassa tästä syystä haittaohjelmien tunnistaminen ja eliminointi ei ole aina yksinkertaista automaatiojärjestelmässä. SIEM pystyy tunnistamaan prosessiin vaikuttavat haittaohjelmat automatisoidusti, koska se tarkkailee järjestelmän kokonaistilaa jatkuvasti mallintaen prosessin muutoksia.

4.3 Kohdejärjestelmän väärinkäytön seuranta

Automaatiojärjestelmän pääsy vääriin käsiin on estettävissä myös perinteisin ratkaisujen avulla. Tällöin käytössä voi olla vain ohjelmisto, joka lukitsee järjestelmään pääsyn, kun käyttäjätiedot on annettu riittävän monta kertaa virheellisesti. Väärinkäytön seuranta on yksi SIEM:n oleellisimmista hyödyistä, sillä SIEM tarjoaa myös sellaisen ominaisuuden. Kaikki SIEM-järjestelmässä tapahtuva analysointi ja siitä muodostuva analyysi on saatavilla ja hallittavissa yhdestä keskitetystä sijainnista.

Automaatiojärjestelmään voidaan päästä käsiksi myös verkosta, jolloin ainut digitaalinen tunnusmerkki voi olla IP-osoite. IP-osoite ei itsessään ole riittävä tieto tietoturvariskin arvioimiseen. (Ahonen et al. 2021, s.174) SIEM-järjestelmään voidaan luoda niin sanottu sallitut arvot sisältävä listaus, (engl. white list) joka tarkoittaa IP-osoiteavaruutta, joiden kautta natiiviin automaatiojärjestelmään myönnetään pääsy. Perinteinen palomuuri mahdollistaa myös sallitun IP-osoite-avaruuden luomisen, mutta heikkoutena tässä on se, että kaikki perinteiset väärinkäyttöä seuraavat työkalut eivät ole ainakaan automaattisesti linkitettyinä toisiinsa. Tässäkin tapauksessa SIEM-ratkaisun

edut on sen keskitetty hallinta, jonka avulla pystytään hyödyntämään kaiken sisään tulevan lokimassan tietoa kokonaisvaltaisessa analyysissä, joka seuraa mahdollisesti koko järjestelmän tilaa. Tietoturvaiskut voivat ilmentyä myös useita kanavia pitkin, jolloin perinteinen tietoturvatyökalu ei välttämättä kykene pysäyttämään hyökkäystä kokonaisuudessaan tai ainakaan tarpeeksi ajoissa.

4.4 Kohdelaitteilta saatavan datan analysointi

Automaatiojärjestelmissä liikkuu valtava määrä lokitietoa, jotka tulevat useista eri lähteistä ja jotka voivat olla yhtä monissa eri tietomuodoissa (Ahonen et al. 2021, s173). Lokitietoa tulee järjestelmistä useilta eri tasoilta, josta tässä työssä tärkeimmät ovat käyttöjärjestelmä, automaatiojärjestelmä, automaation tukijärjestelmät ja automaatiosovellus. Jokaisella tasolla tarvitaan suunnittelua, jotta lokitus olisi riittävää sekä mahdollisimman informatiivista. Erityisesti automaatiosovelluksesta saatava lokitieto voi olla vaikeasti jalostettavissa, sillä lokitietoa ei aina saada helposti ulkoisiin lokijärjestelmiin.

Perinteisen lokienhallinnan yksi suurimmista ongelmista on lokitiedon tulkitseminen. Perinteiset lokienhallintateknologiat eivät kykene hyödyntämään lokitietoa kokonaisuudessaan. Lokitiedon moninainen esittämistapa automaatioympäristössä vaatii usein manuaalista työtä, jotta lokitiedosta saatava potentiaali olisi saavutettavissa. Edellä mainittuun ongelmaan tai pikemminkin haasteeseen SIEM kykenee tarjoamaan ratkaisuja.

SIEM-järjestelmä kykenee jalostamaan lähdetiedosta melkein mitä tahansa parametria, kunhan se on konfiguroitu järjestelmään asianmukaisesti. Oleellinen hyöty on se, että riippumatta lähteestä lokitieto saadaan johdettua järjestelmän palvelimelle, ja sitä pystytään käsittelemään ja tarkastelemaan yhdestä paikasta. SIEM-järjestelmän serverillä sijaitseva tietomassa on johdettu samaan muotoon lähteestä riippumatta.

Haasteena lokitiedon yhdenmukaistamisessa on se, että tietoa on todella monessa eri muodossa ja kaikkien tietomuotojen muuttaminen ei ole universaalia. Tämä tarkoittaa sitä, että SIEM-järjestelmän käyttöönotossa lokitiedon yhdenmukaistaminen saattaa ja usein vaatiikin käsityötä. Ainoat varsinaiset rajoitteet lokitiedoille on kohteena olevan automaatiojärjestelmän rajoitteet ja kapasiteetin kantokyvyn riittävyys. Nämä seikat ovat usein kriittisiä, joten jo automaatiojärjestelmää suunniteltaessa olisi hyvä ottaa huomioon mahdollisesti tulevaisuudessa vaadittavat ominaisuudet tietoliikennetekno-logioista.

4.5 Kehityspotentiaali

Jokainen SIEM-implementaatio on oma toteutuksensa, kuten edellisessä luvussa selvisi. Myös jokainen automaatioympäristö on oma ratkaisunsa, vaikkakin niistä löytyisi samoja laitteita tai samojen toimittajien järjestelmiä. Kompleksisuutensa vuoksi automaatiossa ei ole universaalia tapaa hyödyntää SIEM-ratkaisua. SIEM-järjestelmä on potentiaalinen, sillä automaatioympäristön muuttuessa, SIEM voidaan sopeuttaa muutoksiin. Jos automaatiojärjestelmää tai sen osaa päivitetään uudempaan, on SIEM-järjestelmää mahdollista myös kehittää vastaamaan päivitettyjä vaatimuksia huomattavasti helpommin, kuin perinteisiä järjestelmiä, jotka toimivat osana käyttöjärjestelmää.

Tietoturvauhat muuttuvat ja tietoturvahyökkäysten metodit kehittyvät kerta toisensa jälkeen yhä älykkäämmiksi. Älykäs tietoturvaratkaisu, kuten SIEM, pystyy kehittymään myös, jotta uudet yhä älykkäämmät tietoturvaiskut kyetään myös jatkossa tunnistamaan. SIEM-järjestelmän kehitys perustuu siihen, että järjestelmän toimintaa ja lokitietoihin liittyvää analysointia voidaan muuttaa tarvittavalla tavalla.

SIEM-ratkaisujen keskuudessa on esiintynyt jo SIEM 2.0, (engl. Security Information and Event management 2.0) joka on ominaisuuksiensa puolesta valmis teollisuuteen. Sen parannukset ovat liittyneet esimerkiksi yhä laajempaan tukeen lähdelaitteiden keskuudessa, sekä automatisoidun raportoinnin kehittymiseen. Kehitteillä on myös SIEM 3.0 (engl. Security Information and Event management 3.0), joka pyrkii olemaan yhä kehittyneempi reaaliaikaisuudessa sekä skaalautuvuudessa. Sen pohjalla toimisi lohkoketjuteknologia, joka mahdollistaisi kompleksisen tiedon analysoinnin tehokkaasti. (Miloslavskaya 2018)

5. ÄLYKÄS TIETOTURVA OSANA JOKAPÄIVÄISTÄ AUTOMAATIOTA

Tässä luvussa käsitellään SIEM-ratkaisun yleistymistä automaatiojärjestelmien keskuudessa. Tällä hetkellä uutena implementaationa SIEM saattaa vaikuttaa automaatiojärjestelmän reaaliaikaisuuteen ja kuormittaa tietoliikenneväyliä liikaa. Tarkoituksena on siis tehdä pienimuotoinen tulevaisuuden katsaus liittyen toteutettavaan kokonaisuuteen.

5.1 Tarjonta 2020-luvulla

SIEM:n kaltaiset älykkäät tietoturvaratkaisut ovat tuttuja IT-maailmassa, mutta OT-maailmassa eivät niinkään. IT-ympäristöissä nähtävät ratkaisut nähdään huomattavalla viiveellä OT-järjestelmissä.

Älykkäiden tietoturvaratkaisujen, kuten SIEM:n käyttöönotto tulee lisääntymään, mutta todennäköisesti hitaasti. Tietoturvaratkaisujen kehitys suuresti kiinni asenteista, joihin vaikuttanee ainakin todelliset uhkat ja niiden realisoituminen. Älykkäiden tietoturvaratkaisujen asiantuntemus OT-järjestelmien keskuudessa on tällä hetkellä vielä heikkoa, mutta sen voidaan olettaa kasvavan vuosien saatossa. OT-ympäristöihin SIEM-ratkaisuja tarjoaa ainakin Insta Oy, jonka internet-sivuilta voi lukea lisää aiheesta (Kinnunen 2017).

SIEM-ratkaisuja tarjoavia yrityksiä on kuitenkin jo olemassa paljon, vaikkakin ne ovat keskittyneet enemmänkin IT-ympäristöihin tarjottaviin SIEM-ratkaisuihin. Eräitä yrityksiä, jotka tarjoavat SIEM-ratkaisuja palveluina, ovat esimerkiksi HP, IBM, Intel ja McAfee. Edellä mainittujen toimittajien ratkaisuihin voi tutustua esimerkiksi internetissä tarjoajien kotisivuilla. Toimintaperiaate eri palveluntarjoajilla on kuitenkin sama. (Gonzalez-Granadillo et al. 2021)

Vaikka toimintaperiaate on sama eri ratkaisujen kesken, painottavat eri ratkaisut kuitenkin eri ominaisuuksia. Jotkin SIEM-ratkaisut eivät käsittele koko lokimassaa säilyttääkseen reaaliaikaisuutensa. Tämän kaltaiset ratkaisut sopivat lähtökohtaisesti automaatiojärjestelmien tueksi. Toisaalta SIEM-ratkaisut voivat myös suorittaa kattavaa analysointia, jolloin ne käsittelevät lokimassaa hyvin kattavasti. Tällöin kyky reagoida turvallisuusuhkiin ei pysy reaaliaikaisena. (Michelberger 2016)

Useita eri SIEM-ratkaisuja on jo saatavilla. Uusien ratkaisujen päätavoite on lisätä ratkaisujen älykkyyttä, kuten myös joustavuutta sekä tehokkuutta ja saatavuutta. (Suarez-Tangil et al. 2015) Erilaisia vaihtoehtoja SIEM-ratkaisujen kesken on tarjolla siis yleisesti. OT-ympäristöjen keskuudessa tarjonta saattaa olla suppeampi.

5.2 Haasteet

Älykkään tietoturvaratkaisun kuten SIEM:n käyttöönotto ei ole yksinkertaista. Koska automaatiojärjestelmät ovat usein kompleksisia, monitasoisia ympäristöjä, on lokitietoa usein monessa eri muodossa. Tiedon muuttaminen yhteiseen muotoon onkin yksi SIEM-implementaation suurimmista haasteista, sillä valmista ratkaisua tietotyypin yhdenmukaistamiseen ei ole saatavilla (Ahonen et al. 2021, s.173, s.175).

Haasteita tuottavat myös järjestelmässä käytetyt toimilaitteet, jotka voivat olla iältään jo 20 vuotta vanhoja. Vanhat toimilaitteet saattavat olla jo ilman SIEM:n käyttöäkin äärirajoilla kapasiteettiensa puolesta. Ne eivät välttämättä kestä lisärasitusta enempää, sillä liikakuormitus voi häiritä toimilaitteiden toimintaa.

SIEM:n käyttöönottoa haittaa myös osittain sen korkeat kustannukset ympäristössään. Automaatiomuutos on aina liiketoimintapäätös, joten investointiin kuluvalla rahalla täytyy olla tuottava vaikutus liiketoiminnalle. Tämän asian perustelussa voi olla kuitenkin haasteita vaikuttaen oleellisesti SIEM-ratkaisujen investointipäätöksiin. Automaatioympäristössä tietoturva ja sen ymmärrys ei ole vielä samalla tasolla kuin IT- maailmassa, joten myöskään varattu budjetti ei ole samalla tasolla IT-puolen kanssa. OT-puolella kokonaisvaltainen tietoturva voidaan kokea ylimääräisenä kuluna, eikä niinkään tarpeellisena osana kokonaisuutta (Ahonen et al. 2021, s.23).

Vaikka SIEM:n käyttämisellä pystytään tunnistamaan huomattavasti tietoturvauhkia, ne eivät silti kykene vastaamaan jokaiseen uuteen uhkaan, sillä hyökkääjät kehittyvät myös hyökkäystavoissaan (Gonzalez-Granadillo et al. 2021). Tämä ongelma ei liity suoraan SIEM-ratkaisun käyttämiseen vaan on yleisesti tietoturvallisuushaaste. Tietoturvallisuuden kannalta on kuitenkin tärkeää olla ajan tasalla uhkien potentiaalista.

5.3 Järjestelmien uusiminen

Automaatiojärjestelmä, johon on yhdistetty lokienhallintajärjestelmä raskauttaa prosessia huomattavasti. Nykyiset käytössä olevat tietoliikenneväylät ovat tarkasti suunniteltu vastaamaan automaatiojärjestelmän vaatimuksiin, mutta kun tähän liitetään toinen järjestelmä rinnalle, vaaditaan usein lisää suorituskykyä.

Järjestelmän uusimisvaiheessa olisi syytä ottaa huomioon mahdollinen tiedonsiirtokuorman kasvaminen jo suunnitteluvaiheessa. Näin ollen uhkien ja vaatimusten kasvaminen ei tuota ongelmia SIEM-järjestelmän analysoinnissa.

SIEM-järjestelmä on itsessään skaalautuva, sillä sen kyky kasvattaa lokitiedon käsittelymäärää ei välttämättä ole sitoutunut toimilaitteiden kapasiteettiin, vaan myös SIEM:n arkkitehtuuriin (Gonzalez-Granadillo et al. 2021).

5.4 Uhkien jatkuva vakavoituminen

Teollisuus käy tällä hetkellä läpi suurta internetin vallankumousta. Vanhat ja suljetut järjestelmät joutuvat vastaamaan uusien ja avoimien järjestelmien uhkiin. Jo tapahtuneet hyökkäykset, kuten Stuxnet ovat vasta pintaraapaisu siitä, mihin internetin kautta tapahtuva tietoliikenne voi pahimmillaan johtaa. Toistaiseksi uhkien vaikutukset ovat olleet lähinnä taloudellisia, mutta tulevaisuudessa realisoituu se tosiasia, että myös fyysisiä vahinkoja kuten henkilövahinkoja voidaan saada aikaiseksi.

Näistä syistä SIEM-järjestelmän jatkuva kehittäminen ja sen käyttäminen korostuu tietoturvan parantumisessa. Kun haavoittuvuuksia paljastuu, SIEM-järjestelmä pystytään konfiguroimaan niitä vastaan jatkossa yhä paremmin. Konfigurointi ei vaadi jokaisen ohjelmiston erillistä testaamista vaan siihen riittää ainoastaan SIEM- järjestelmän oikeanlainen konfiguraatio, mikäli SIEM toimii hyödyntäen automaatiojärjestelmän olemassa olevaa lokitietoa ja lokitiedon hankintaa. Konfigurointi edellyttää kuitenkin sitä, että lokitiedon kuvaama toiminta ymmärretään, sillä ymmärryksen avulla pystytään tukemaan päätöksentekoa.

6. YHTEENVETO JA JOHTOPÄÄTÖKSET

Tämän kandidaatintyön tarkoituksena oli perehtyä älykkään tietoturvaratkaisun ominaisuuksiin sekä sen käyttämisestä saatuihin hyötyihin automaatioympäristöissä. Älykkäällä tietoturvaratkaisulla tarkoitetaan tässä työssä älykästä lokienhallintajärjestelmää, joka kykenee tekemään jatkuvaa analyysia automaatiojärjestelmän tuottamasta lokitiedosta. Saatua lokitietoa käsitellään, rikastetaan ja analysoidaan jatkuvasti lähes automatisoidusti. Automaatiojärjestelmä tuottaa suuren määrän lokitietoa, mutta yhtä tapaa sen tietomassan tulkitsemiseen ja analysoimiseen ei ole tarjolla perinteisten tietoturvaratkaisujen joukossa.

Älykäs lokienhallintajärjestelmä tuo suuria turvallisuushyötyjä automaatioympäristöön, sillä sen avulla lokitiedoista pystytään hyödyntämään täysi potentiaali uhkia tunnistaessa. Automaatiojärjestelmässä olevia lokitietoa tuottavia elementtejä on todella monia ja niiden tuottama lokitieto voi olla useassa eri muodossa. Älykkään lokienhallinnan etuja on sen kyky muuttaa lokimassa yhtenäiseen muotoon ja sijoittaa se yhteen sijaintiin, jotta järjestelmäkokonaisuuden tarkastelu onnistuu helpommin.

Älykkään lokienhallintajärjestelmän käyttäminen tuo etuja myös siihen, että mikään lokitiedosta saatava tieto ei ole irrallisesti analysoitava osa, vaan jokainen lokitietoa tuottava lähde otetaan mukaan analyysiin. Sillä on myös kyky reagoida uhkiin nopeasti sekä tunnistaa haittaohjelmien toiminta aikaisessa vaiheessa, jos haittaohjelmat pyrkivät esimerkiksi manipuloimaan automaatiojärjestelmän toimintaa. Tämän kaltainen tietoturvaratkaisu on myös kehitettävissä vastaamaan tulevaisuuden tietoturvahaasteisiin, sillä tietoturvauhat kehittyvät jatkuvasti.

Vaikka älykäs tietoturvaratkaisu tarjoaa monia oleellisia hyötyjä, ei sen käyttö ole automaatiojärjestelmien keskuudessa vielä kovin yleistä. Osittain tähän liittyy kustannukset, jotka ovat pääpiirteittäin suuremmat kuin perinteisillä ratkaisuilla, mutta älykkään tietoturvaratkaisun käyttöönottaminen automaatioympäristössä sisältää kuitenkin useita erilaisia haasteita.

Tämän kandidaatintyön tarkoitus oli esitellä keskeisen tietoturvaratkaisun ominaisuudet pääpiirteittäin. Älykkään tietoturvaratkaisun ominaisuuksiin perehtyminen onnistui hyvin. Tietoa oli hyvin saatavilla ja sen perusteella oli mahdollista perehtyä ratkaisun ominaisuuksiin. Haasteita tuotti hyötyjen arviointi, sillä työtä varten ei ollut saatavilla mitään tiettyä automaatioympäristöä. Tarkempia hyötyjä arvioidessa tarvittaisiin kohde,

jonka integraatio olisi tiedossa, jolloin kokonaisuuden toimintaa voitaisiin myös mallintaa. Vaikka varsinaista kohdeympäristöä ei ollut tiedossa, tämä työ tarjosi kuitenkin tietopaketin kyseisestä tietoturvaratkaisusta kiinnostuneelle taholle.

LÄHTEET

Ahonen, P., Seppälä, J. & Pärssinen, J. (2019). KYBER-ENE Energia-alan kyberturvaaminen 1-2. Julkaisija: Huoltovarmuuskeskus.

Ahonen, P., Seppälä, J., Suortti-Myyry, E. & Tyynelä M. (2021). Automaation tietoturva: Kriittisen tuotannon turvaaminen. Julkaisija: Suomen Automaatioseura RY.

Automaatioseura RY. (2005). Teollisuusautomaation tietoturva. Verkottumisen riskit ja niiden hallinta.

Coppolino, L., D'Antonio, S., Formicola, V. & Romano, L. (2016). A framework for mastering heterogeneity in multi-layer security information and event correlation. Julkaisija: Elsevier B.V Sivut 78-88.

Jaeger, D., Sapegin, A., Ussath, M., Cheng, F. & Meinel, C. (2015). Parallel and distributed Normalization of security events for instant attack analysis. Julkaisija: IEEE. Sivut 1-8

Miller, D., Harris, S., Harper, A., Vandyke, S., Blask, C. (2011). Security Information and Event Management (SIEM) Implementation. Julkaisija: Mc Graw Hill.

Di Sarno, C., Garofalo, A., Matteucci, I. & Vallini, M. (2016). A novel security information and event management system for enhancing cyber security in a hydroelectric dam. Julkaisija: Elsevier B.V. Sivut 39-51.

Gonzalez-Granadillo, G., Gonzalez-Zarzosa, S. & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Julkaisija: BASEL:MDPI. Sivut 1-28.

Hahn, A. (2016). Operational Technology and Information Technology in Industrial Control Systems. Julkaisija: Cham: Springer International Publishing. Sivut 51-68.

Kinnunen, Y. (2017). SIEM-järjestelmä on organisaation kyberturvallisuuden hermokeskus. Julkaisija: Insta Oy. Saatavilla: https://www.insta.fi/ajankohtaista/siem-järjestelmä-on-organisaation-kyberturvallisuuden-hermokeskus. (5.3.2021)

Kostrecova, E. & Binova, H. (2015). Security Information and Event Management. Julkaisija: Indian Journal of Research. Sivut 19-20.

Kotenko, I., Polubelova, O., Chechulin, A. & Saenko, I. (2013). Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM Systems. Julkaisija: Basel: MDPI AG. sivut 356-359.

McMillan, R. (2010). Siemens: Stuxnet worm hit industrial systems. Julkaisija: IDG News Service. https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html. (22.12.2021)

Michelberger, P. & Dombora, S. (2016). A Possible tool for development of information security: SIEM system. Julkaisija: Nis: Drustvo Ekonomista Ekonomika. Sivut 125-140.

Miloslavskaya, N. (2018). Designing blockchain-based SIEM 3.0 system. Julkaisija: Emerald Publishing Limited. Sivut 491-512.

Montesino, R., Fenz, S. & Baluja, W. (2012). SIEM-based framework for security controls automation. Julkaisija: Bradford: Emerald Group Publishing Limited. Sivut 248-263.

Moukafih, N., Orhanou, G. & Elhajji, S. (2019). Mobile agent-based SIEM for event collection and normalization externalization. Julkaisija: Bringley: Emerald Group Publishing Limited. Sivut 15-34.

Sadeghi, A., Wachsmann, C. & Waidner, M. (2015). Security and Privacy Challenges in Industrial Internet of Things. Julkaisija: ACM. Sivut 1-6.

Salmenperä, M. (2021). Automaation turvallisuus, luentodiat. ASE-7610. Julkaisija: Moodle.

Sandeep, B., Pratyusa, K. & Loai, Z. (2014). The Operational Role of Security Information and Event Management Systems. Julkaisija: LOAS ALAMITOS: IEEE. Sivut 35-41.

Seppälä, J. (2022). Automaation turvallisuus, luentodiat. AUT.440. Julkaisija: Moodle.

Suarez-Tangil, G., Palomar, E., Ribagorda, A. & Sanz, I. (2015). Providing SIEM systems with self-adaptation. Julkaisija: AMSTERDAM: Elsevier B.V. Sivut 145-158

Vielberth, M. & Pernul, G. (2018). A Security Information and Event Management Pattern. Julkaisija: SLPLop. Sivut 1-12.

Wu Qingrong, J., Xuan Zhu, S., Kuei-Chi Kuo, E. & Cong Lu, M. (2017). Light SIEM for Semiconductor Industry. Julkaisija: IEEE. Sivut 2331-2335.