Informaatioteknologian tiedekunnan julkaisuja
No. 59/2018

Jouni Pöyhönen, Viivi Nuojua

Tilannekuvatieto kriittisen infrastruktuurin yrityksen tietojärjestelmien tietoturvallisuudesta

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 59/2018

Editor: Pekka Neittaanmäki
Covers: Petri Vähäkainu ja Matti Savonen

ISBN 978-951-39-7555-5 (verkkoj.)
ISSN 2323-5004

Jyväskylä 2018

Tilannekuvatieto kriittisen infrastruktuurin yrityksen tietojärjestelmien tietoturvallisuudesta

Jyväskylän yliopisto
Informaatioteknologian tiedekunta
Tietotekniikan laitos

CIRP-tutkimusartikkeli
Tutkimusongelman kuvaus

2016

Jouni Pöyhönen
Viivi Nuojua

JYVÄSKYLÄN YLIOPISTO

KUVIOT

Sisällysluettelo

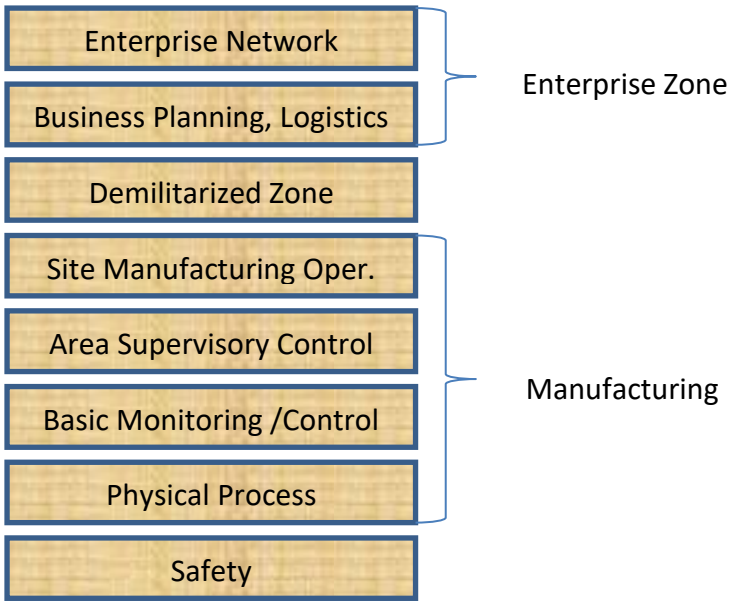
1. Johdanto tilannekuvaan

Modernin yhteiskunnan toiminta perustuu useiden kriittisten infrastruktuurien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu yhä enemmän luotettavista sähköjärjestelmistä, toimivista tiedonsiirtoverkostoista, tiedon luotettavuudesta, eheydestä ja käytettävyydestä toimintaympäristössä, joiden kyberturvallisuusriskejä digitaalisen maailman uhkakuvat jatkuvasti kasvattavat. Moderni yhteiskunta on täysin sidoksissa palveluiltaan dynaamiseen kybertoimintaympäristöön.

Kybertoimintaympäristö on sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kriittinen infrastruktuuri käsittää ne rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeille toiminnoille. Siihen kuuluu sekä fyysisiä laitoksia ja rakenteita, että sähköisiä toimintoja ja palveluja. (Turvallisuuskomitean sihteeristö, 2013, 12.)

Sähköjärjestelmä muodostaa perustan lähes kaikille yhteiskunnan palveluille. Toiminnan täytyy olla siten mahdollisimman keskeytymätöntä. Lyhyetkin sähkökatkot heijastuvat häiriöinä laajalle yhteiskunnan muihin kriittisiin palveluihin. Näitä kriittisiä palveluita tuottavia toimialoja kutsutaan yhdessä kriittiseksi infrastruktuuriksi. Kriittisen infrastruktuurin toiminnan jatkuvuuden turvaaminen ja nopea häiriötilanteista palautuminen on erityisen tärkeää, jotta palvelukatkosten heijastusvaikutukset pystytään pitämään mahdollisimman pieninä. Organisaatiokohtainen kyberturvallisuuden tilannetietoisuuden muodostaminen ja ylläpitäminen ovat toiminnan jatkuvuuden hallinnassa keskeisessä roolissa. Toiminnan ohjaaminen ja koordinoitujen tilannekohtaisten päätösten tekeminen edellyttävät reaaliaikaista tilannekuvaa omista tietojärjestelmistä ja tietovarannoista dynaamisesti muuttuvassa kybertoimintaympäristössä. Kriittisen infrastruktuurin sisältämät monitahoiset riippuvuussuhteet myös edellyttävät erityisesti sähköyhtiöiltä eri organisaatiotahoille ulottuvaa jatkuvaa tilannetietoisuuden aikaansaamista omasta kyberturvallisuustilanteestaan ja siihen vaikuttavista tekijöistä.

Tämän tilannekuvaselvitystyön tilaajana on kriittisen infrastruktuuriin lukeutuva energiayritys. Yritys pitää tärkeänä ITIL-palvelumallin (Information Technology Infrastructure Library, ITIL) mukaisten tietojärjestelmiensä ja tietojärjestelmävarantojensa reaaliaikaisen tilannekuvan aikaansaamista. Kuviossa 1 on esitetty tyypillinen tuotantoyrityksen kybertoimintaympäristön rakenne järjestelmätasolla, joka sopii esimerkiksi energiayrityksen tapaukseen.



KUVIO 1. Kybertoimintaympäristön rakenne järjestelmätasolla (Knowles, Prince, Hutchison, Ferdinand, Disso & Jones, 2015, 53)

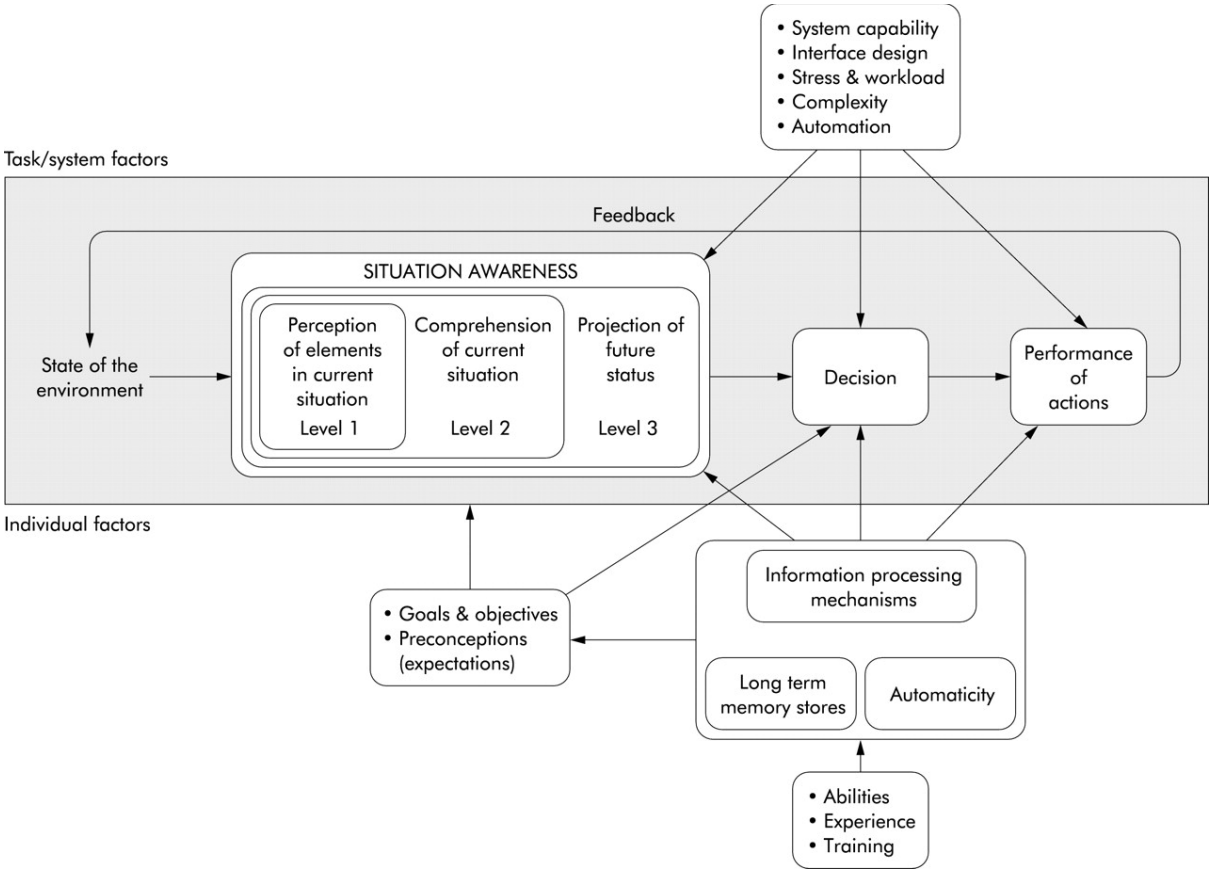
Kuviossa 1 hierarkkinen kyberympäristö koostuu yritystason ja tuotantotason tieto- ja automaatiojärjestelmistä. Ylimmällä tasolla hierarkiassa ovat yrityskohtaiset toimistojärjestelmät, toiminnanohjausjärjestelmä (Enterprise Resource Planning, ERP) ja internetin käytön mahdollistavat järjestelmät tiedonsiirtoverkkoineen. Seuraavalla tasolla ovat tuotannonohjausjärjestelmä (Manufacturing Execution System, MES) ja tuotantoprosessin ohjaukseen tarvittava teollisuuden automaatiojärjestelmä (Industrial Control System, ICS). Edellä mainitut järjestelmät eroavat toisistaan erityisesti rakenteeltaan, toiminnaltaan ja elinkaariltaan huomattavasti, joten tilannekuvan muodostamisen näkökulmasta katsottuna eroavaisuudet vaikuttavat toteutusratkaisun etsintään merkittävästi.

Teollisuuden automaatiojärjestelmiä voidaan luonnehtia siten, että ne ovat hyvin vakiintuneita ja niitä käytetään pitkään verrattuna esimerkiksi toimistojärjestelmiin, jotka ovat elinkaareltaan huomattavasti lyhempiä. Automaatiojärjestelmien elinkaaret voivat olla perusjärjestelmän osalta jopa useiden vuosikymmenien mittaisia. Automaatiojärjestelmät ovat myös resursseiltaan rajoittuneita, jolloin niissä ei ole voitu käyttää tyypillisiä teknillisiä tietoturvaratkaisuja eikä salaustekniikoita. Automaatiojärjestelmien tietovarastot sisältävät pääosin prosessin tietoja eikä niinkään liiketoimintojen kannalta salassa pidettävää tietoa. Suoraa yhteyttä internet-verkkoon ei tavallisesti tarvita, mutta MES-järjestelmien käytön lisääntyminen on lisännyt internet-liitännän tarvetta. Lisäksi automaatiojärjestelmien tietoteknisiä laitteita ei käytetä muihin tarkoituksiin, vaan ne ovat hajautettuina tuotantoprosessiin, sen mittaus- ja ohjaustehtäviin sekä turvatoimintoihin. Niihin tapahtuva pääsynhallinta on useimmiten tarkasti järjestetty. Automaatiojärjestelmien toimintojen ja

henkilöstön valvonta on hallittua muun muassa johtuen prosessin toiminnan käytettävyys- ja turvallisuusvaatimuksista. (Suomen Automaatioseura ry Turvallisuusjaosto, 2010, 89 - 90.)

Edellä mainituista syistä johtuen tässä selvityksessä kriittisen infrastruktuurin tilannekuvatiedon ulottaminen yrityksen tietojärjestelmiin rajataan yritystason järjestelmiin (ITIL-palvelut). Samalla rajaus parantaa tarkastelun yleistettävyyttä kriittisten infrastruktuurien osalta.

Endsley (1995) on kehittänyt tilannetietoisuuden mallia työskennellessään useissa eri tutkimustehtävissä Yhdysvaltojen ilmavoimien palveluksessa. Kuviossa 2 on esitetty mallin yleinen rakenne. Tilannetietoisuuden ydin koostuu kolmesta peruselementistä, jotka ovat havaitseminen (Level 1), tilanteen ymmärtäminen (Level 2) ja sen vaikutuksen arviointi tulevaisuuteen nähden (Level 3). Näin muodostettava tilannekuva antaa perusteet johtopäätöksiin ja niistä seuraavaan päätöksentekoon. Siihen vaikuttavat myös tilanteesta riippuen tehtävä- tai järjestelmäkohtaiset ominaisuudet sekä päätöksentekijän kokemukset ja arviointikyky. Päätöksenteko puolestaan ohjaa toimintaa, joka heijastuu takaisin havainnoitavaan toimintaympäristöön.



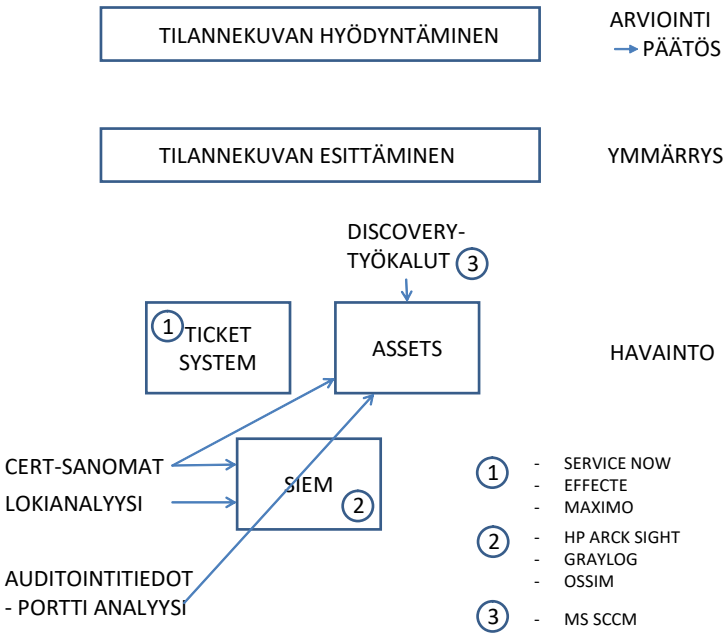
KUVIO 2. Tilannekuvajärjestelmä dynaamiseen päätöksentekoon (Endsley, 1995, 35)

Faber (2015) kiinnittää huomiota kybertoimintaympäristön tilannetietoisuuden merkitykseen erityisesti tiedonsiirtoverkkojen liikenteen valvonnan osalta. Tavoitteena on, että siellä esiintyvien tapahtumien seurantaan kehitetään työkaluja, joilla parannetaan verkon valvojan päätöksenteon edellytyksiä häiriötilanteissa. Hän pitää kehitystoimia tilannekuvakyvyn kehittämiseksi, niin julkisten kuin yksityisten organisaatioiden osalta, eräänä merkittävimmistä kyberturvallisuuden parantamiseen tähtäävistä lähiajan tavoitteista. Faber suosittaa Endsleyn kehittämän tilannekuvarakenteen soveltamista kybertoimintaympäristön seurantatarpeisiin. (Endsley,1995, 35; Faber, 2015.)

Endsleyn kehittämän tilannetietoisuuden mallin yleistä rakennetta voidaan soveltaa myös energiayrityksen tietojärjestelmien tilannekuvan muodostamiseen johdannossa mainituin rajauksin.

2. Yrityksen tietojärjestelmät, tietovarannot ja tietoturvan tilannekuva

Energiayrityksen selvityspyynnön mukainen tietojärjestelmiensä ja tietovarantojensa tietoturvan tilannekuvan muodostamisen viitekehys on esitetty kuviossa 3. Endsleyn tilannekuvan rakenteen havaintokohteita (Level 1) siinä edustavat tietojärjestelmät ja tietovarannot (Assets), palvelupyynnöt (Ticket system) sekä CERT-sanomat ja lokianalyysit SIEM-järjestelmän kautta (Security Information and Even Management, SIEM). Tavoitteena on aikaansaada niistä tietoturvaa kuvaava reaaliaikainen ilmaisu. Havainnoista muodostettavan tilannekuvan esittäminen on puolestaan edellytys havaintojen ymmärtämiseen (Level 2). Tämän jälkeen muodostuvat edellytykset havaintojen mukaisten vaikutusten arvioimiseksi tilannekuvaa hyväksi käyttäen sekä tilannekuvan tulkitsijan tietojärjestelmäkokoonpanon tuntemusta ja teknillistä osaamista hyödyntäen (Level 3). Lopullisena tavoitteena on luonnollisesti tilannekohtaisten oikeiden päätösten tekeminen ja päätösten mukaisten tietojärjestelmien ja tietovarantojen suorituskykyä ylläpitävien toimenpiteiden ohjaus. (Endsley, 1995, 35.)



KUVIO 3. Yrityksen tietoteknillisten järjestelmien tietoturvan tilannekuvan muodostamisen viitekehys

Tietojärjestelmiä ja tietovarantoja voidaan hallita konfiguraation hallinnan työkaluilla (Discovery-työkalut). Tyypillisesti niiden avulla saadaan selville tietojärjestelmissä toimivien palomuurien ominaisuudet ja tietojärjestelmissä toimivat palvelut. Yrityksen ITIL-palvelumallin mukaisten tietojärjestelmien ja tietovarantojen reaaliaikaisen käyttökokemuksen tilannetieto koostuu niihin kohdistuvista palvelun tukipyynnöistä (Ticket system). SIEM-järjestelmän avulla puolestaan muodostetaan tilannetietoisuutta tunnetuista uhkatekijöistä (CERT-sanomat) ja tarkastelun kohteena olevista tietojärjestelmien lokeista (Lokianalyysi). Jokainen edellä mainituista järjestelyistä tuottaa siis omalta osaltaan tilannetietoisuutta. Lopullisena tavoitteena on aikaansaada näiden tietojen automaattinen yhdistäminen, joka kohdistuu kohdeorganisaation ITIL-palvelujen mukaiseen tietojärjestelmäkokoonpanoon. Lähtökohtana pidetään avoimen lähdekoodin (ilmaiset) tuotteiden hyödyntämistä mahdollisimman pitkälle. Tutkimuskysymyksenä onkin: ”Miten saadaan aikaiseksi automaattisesti toimiva kohdeorganisaation tietojärjestelmien kyberturvallisuudesta kertova tilannekuvatieto edellä kuvatussa rakenteessa?”

Kuviossa 3 on lueteltu alustavasti joitakin avoimen lähdekoodin työkaluja, joita arvioidaan voitavan hyödyntää työssä.

Porttianalyysit ovat kertaluonteisia analyyseja, joten niiden käyttäminen dynaamisessa kyberympäristössä on tarkoituksenmukaisinta auditointiluonteisesti.

3. Kirjallisuuskatsaus

Lääperin, Rummukaisen & Vankan (2015) artikkeli ”Kriittisen infrastruktuurin tilannekuvajärjestelmä” on tehty osana Tekesin rahoittamaa DiSCI- (Digital Security of Critical Infrastructures) tutkimushanketta, jossa tutkitaan ratkaisuja suomalaisen kriittisen infrastruktuurin turvallisuuden parantamiseksi. Hankkeessa ovat tutkimuspartnereina Maanpuolustuskorkeakoulun lisäksi Aalto-yliopisto ja Stonesoft Oyj (nykyisin osa Intel/McAfee-konsernia). Artikkeli käsittelee datafuusiota eri kohdejärjestelmien tuottaman raa’an datan integroimiseksi tilannekuvan kehittämiseksi koko kriittisen infrastruktuurin osalta. Kohdejärjestelmien datasta muodostetaan toteutuksessa tilannekuva tapahtumaluokittain seuraavasti: luvaton pääsy, palvelunesto, haitallinen ohjelmakoodi, haitallinen käyttö, tiedustelu ja murtautumisyritys. Artikkeli ei kuitenkaan anna ratkaisua edellä mainittujen tietojen automaattiseksi havainnoimiseksi yrityksen tietojärjestelmästä datafuusion kohdejärjestelmänä. Tämän selvityksen mukaisen ratkaisun löytyminen tukee osaltaan myös koko kriittisen infrastruktuurin tilannekuvan datafuusion kehittämistoimenpiteitä.

Tietoturvayhtiö AlienVault on tutkinut SIEM-järjestelmiä ja ITIL-viitekehystä keksiäkseen ratkaisun nopeampaan tietoturvauhkiin reagointiin. SIEM:ssä sekä ITIL:ssä on omat hyvät ominaisuutensa, mutta niissä on myös puutteita. Näin ollen ne eivät yksinään riitä tarpeeksi nopean reagointikyvyn saavuttamiseen. AlienVaultin tutkimus ei varsinaisesti tähtää tässä raportissa kuvattuun tilannekuvajärjestelmään, mutta se oli ensimmäinen löydös, jossa käsiteltiin molempia, sekä SIEM-järjestelmiä että ITIL-prosesseja, samassa yhteydessä. Tutkimuksen lopputuloksena todetaan, että SIEM-järjestelmät ja ITIL-prosessit tulisi saada yhdistettyä jollain järkevällä tavalla parhaan reagointikyvyn saavuttamiseksi, mutta että tämä ei ole helppoa. Asiaan liittyen riittää tekemistä, mutta valitettavan usein, kuten AlienVaultin tapauksessa, resurssit tulevat vastaan. (Constantine 2011a, 2; Constantine 2011b, 20.)

Lähimmäksi luvussa 2 kuvattua SIEM-järjestelmän ja ITIL-viitekehyksen yhdistävää tilannekuvajärjestelmää pääsee Axxera-nimisen yrityksen tuote Axxera SIEM (Axxera Inc., 2013). Siitä löytyy kaikki tarvittavat aiemmin kuvatut tilannekuvajärjestelmän osaset: SIEM-järjestelmä, tietojärjestelmät ja tietovarannot, palvelupyyntöjärjestelmä ja ITIL-viitekehys integroituna. Tuotekuvauksen perusteella jää kuitenkin hieman epäselväksi, rajoittuuko järjestelmä ainoastaan turvallisuuspuolen palvelupyyntöihin. Lisäksi tuotteen hintaluokasta ja itse yrityksestä ei löydy tarpeeksi tietoa.

4. Yhteenveto

Esimerkiksi energiayhtiön kyberturvallisuuden tilannetietoisuuden muodostaminen ja ylläpitäminen ovat toiminnan jatkuvuuden hallinnassa keskeisessä roolissa. Tämän selvityksen perusteella voidaan sanoa, että asiaa on tutkittu melko vähän ja käyttökohteeseen sopivia ja täsmälleen halutun laisia tuotteita ei ole markkinoilla tarjolla. Tätä johtopäätöstä tukevat myös lausunnot Jyväskylän yliopiston yhteistyökumppaneiden asiantuntijahenkilöiltä.

Selvityksen lopputuloksena syntyi tutkimusongelman määrittyminen luvussa 2 kuvattuun muotoon. Koska valmiista tuotteista ei löytynyt sopivaa kokonaisuutta, jatkotoimenpiteenä esitetään, että ongelman ratkaisemiseksi paras vaihtoehto on rakentaa kuvatun lainen tilannekuvajärjestelmä pääosin avoimen lähdekoodin ratkaisuja yhdistelemällä.

Lähteet

Axxera Inc..(2013). Axxera SIEM. Axxera Inc:n internetsivusto. Saatavilla: 5.12.2016 http://axxerainc.com/products/isms/

Constantine, C. (2011a). AlienVault. Developing ITIL – Mature Security Incident Response With SIEM. A Plan for CSIRT Maturity Models via monitoring-driven Kanban, Part 1. Saatavilla: 16.5.2016 https://www.alienvault.com/blog-content/2011/11/SIEM-for-ITIL-Incident-Response-Part-1.pdf

Constantine, C. (2011b). AlienVault. Developing ITIL – Mature Security Incident Response With SIEM. A Plan for CSIRT Maturity Models via monitoring-driven Kanban, Part 2. Saatavilla: 16.5.2016 https://www.alienvault.com/blog-content/2011/12/SIEM-for-ITIL-Incident-Response-Part-2.pdf

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 37(1),* 32 - 64.

Faber, S. (2015). Flow Analytics for Cyber Situational Awareness. SEI Blog. Carnegie Mellon Universityn internetsivusto. Saatavilla: 16.5.2016 https://insights.sei.cmu.edu/sei_blog/2015/12/flow-analytics-for-cyber-situational-awareness.html

Knowles, W., Prince, D., Hutchison, D., Ferdinand, J., Disso, .J.F.P. & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection 9,* 52 - 80.

Lääperi, L., Rummukainen, L. & Vankka, J. (2015). Kriittisen infrastruktuurin tilannekuvajärjestelmä. *Tiede Ja Ase. 72*(1). Saatavilla: 16.5.2016 http://ojs.tsv.fi/index.php/ta/article/view/50158

Suomen Automaatioseura ry Turvallisuusjaosto. (2010). Teollisuusautomaation tietoturva – Verkottumisen riskit ja niiden hallinta. SAS julkaisusarja nro 29. 1.verkkopainos 2010. Saatavilla: 16.5.2016 https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf

Turvallisuuskomitean sihteeristö. (2013). Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. Saatavilla: 16.5.2016 http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit

Informaatioteknologian tiedekunnan julkaisuja
No. 59/2018

ISBN 978-951-39-7554-8 (nid.)
ISSN 2323-4997

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 59/2018

ISBN 978-951-39-7555-5 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO