jamk.fi

Tilannetietoisuuden kasvattaminen organisaation kybertoiminta-ympäristössä

Uudemman sukupolven SIEM-järjestelmien vertailu

Sara Sallinen

Opinnäytetyö
Joulukuu 2019
Tekniikan ala
Insinööri (AMK), Tieto- ja viestintätekniikka
Kyberturvallisuus

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Sallinen, Sara	Opinnäytetyö, AMK	Joulukuu 2019
	Sivumäärä 81	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: Kyllä

Työn nimi

Tilannetietoisuuden kasvattaminen organisaation kybertoimintaympäristössä

Uudemman sukupolven SIEM-järjestelmien vertailu

Tutkinto-ohjelma

Tieto- ja viestintätekniikka

Työn ohjaaja(t)

Tero Kokkonen, Sampo Kotikoski

Toimeksiantaja(t)

Organisaatio X

Tiivistelmä

Uhkien havainnointi kompleksista kybertoimintaympäristöstä aiheuttaa useille yrityksille ja organisaatioille haasteita. Tilannetietoisuuden kasvattamiseksi ja päätöksenteon tueksi vaaditaan erilaisia toimintatapoja ja havainnointivälineitä, joita ovat esimerkiksi erilaiset uudemman sukupolven SIEM-järjestelmät. SIEM-järjestelmien avulla kerätään, hallitaan ja analysoidaan lokitietoja ja kyberturvallisuustapahtumia.

Tavoitteena tutkimuksella oli tehdä toimeksiantajalle vertailu uudemman sukupolven SIEM-järjestelmistä ja löytää näistä sopivin Organisaatio X:n vaatimuksiin ja tarpeisiin nähden. Tutkittaviksi SIEM-järjestelmiksi valittiin kolme johtavaa tuotetta: Splunk Enterprise Security, IBM QRadar ja LogRhythm Next-Gen SIEM.

Tutkimus toteutettiin kehittämistutkimuksena yhdistellen laadullisen ja määrällisen tutkimuksen keinoja. Teoriaosuuteen ja SIEM-järjestelmien ominaisuuksien kartoittamiseen käytettiin laadullisia menetelmiä. Tuotteiden vertailussa taas käytettiin määrällistä menetelmää, jotta saatiin perustellusti valittua Organisaatio X:lle paras tuotevaihtoehto.

Tulokset saatiin toteuttamalla vertailu toimeksiantajan vaatimuksista ja tuotteiden ominaisuuksista sekä asiakasarvioiden perusteella. Tutkimustuloksena Splunk Enterprise Security oli ominaisuuksiensa ja käytettävyytensä puolesta paras vaihtoehto Organisaatio X:lle. Modulaarinen ja integroituva järjestelmä oli helppokäyttöinen monipuolisten lokienhallintaan sekä poikkeamien analysoimiseen liittyvien ominaisuuksiensa lisäksi.

Lopputuloksena saatiin koostettua Organisaatio X:lle tietoa tilannetietoisuuden tärkeydestä, uudemman sukupolven SIEM-järjestelmien arkkitehtuurista ja ominaisuuksista sekä vastattua tutkimuskysymykseen onnistuneesti eri tutkimusmetodeja hyödyntäen.

Avainsanat (asiasanat)

SIEM, tilannetietoisuus, kyberturvallisuus, lokienhallinta

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Sallinen, Sara	Bachelor's thesis	December 2019
		Language of publication: Finnish
	Number of pages: 81	Permission for web publication: Yes

Title of publication

Increasing situational awareness in an organization's cyber environment

Comparison of the next-gen SIEM systems

Degree programme

Information and Communications Technology

Supervisor(s)

Tero Kokkonen, Sampo Kotikoski

Assigned by

Organization X

Abstract

It is very challenging for many companies and organizations to detect threats from complex cyber environments. In order to increase situational awareness and support decision making, different strategies and observations tools are required, such as next-generation SIEM systems. The SIEM system is used to collect, manage and analyze log information and cyber security events.

The purpose of this study was to compare different next-generation SIEM systems and find the most appropriate one for Organization X's needs and requirements. Three leading products were selected for a more specific inspection: Splunk Enterprise Security, IBM QRadar and LogRhythm Next-Gen SIEM.

The research was conducted as a development study, combining qualitative and quantitative research methods. The qualitative methods were used in the theory section and for a survey of the features of the SIEM systems. Quantitative methods were used when products were compared in order to validate the result.

The result was obtained by comparing the requirements of Organization X and the features of the SIEM systems as well as taking customer reviews into account. The best option for the needs of Organization X was met with Splunk Enterprise Security due to its features and usability. Splunk Enterprise Security is a very modular, integrating system with ease of use with its versatile log management capabilities and anomaly analysis features.

Organization X got a completed study about the importance of situational awareness, architecture and features of next generation SIEM systems. In addition, the study also managed to successfully answer to the research question by using a variety of research methods.

Keywords/tags (subjects)

SIEM, situational awareness, cyber security, log management

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenneluettelo

AV	Antivirus
BI	Business Intelligence
CISA	Cybersecurity and Infrastructure Security Agency
DLP	Data Loss Prevention
DNS	Domain Name Services
EDR	Endpoint Detection and Response
FIM	File Integrity Monitoring
FTP	File Transfer Protocol
FW	Firewall
IDS/IPS	Intrusion Detection/Prevention System
IOC	Indicators of Compromise
IP	Internet Protocol
IR	Incident Response
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OT	Operational Technology

PII	Personally Identifiable Information
SA	Situational Awareness
SAAS	Software as a Service
SEM	Security Event Management
SIEM	Security Information and Event Management
SIM	Security Information Management
SOAR	Security Orchestration Automation and Response
SOC	Security Operations Center
SSH	Secure Shell
SVD	Singular Values Decomposition
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UEBA	User and Entity Behaviour Analytics
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAN	Wide Area Network

1 Johdanto

1.1 Työn taustat

Kyberturvallisuuden tärkeys korostuu päivittäin ympäri maailmaa erilaisten tietomurtojen ja jatkuvasti muuttuvien hyökkäysten vaikutusten myötä. Usein rahalliset tappiot kasvavat suuriksi ja erilaiset yritykset ja organisaatiot menettävät kallisarvoista tietoa niin asiakkaistaan kuin tuotteistaan. Näitä tapauksia on Suomessakin käynyt ilmi, esimerkiksi vuonna 2019 tapahtunut tietomurto Lahden kaupungin tietojärjestelmiin aiheutti suoraan noin 700 000 euron vahingot, eikä välillisten vahinkojen suuruutta ole vieläkään tiedossa (Karkimo 2019). IBM:n tutkimuksen mukaan keskimääräinen tietomurron hinta on ollut vuonna 2019 maailmanlaajuisesti noin 3,56 miljoonaa euroa ja murron havaitseminen kestää keskimäärin 279 päivää (Ponemon 2019). Nämä luvut korostavat havainnointikyvyn ja siten oman ympäristön tuntemisen tärkeyttä, jotta poikkeamat havaitaan mahdollisimman pian niiden tapahduttua. Tähän apuna voidaan käyttää uudemman sukupolven SIEM-järjestelmiä, jotka valvovat reaaliajassa kybertoimintaympäristön tilaa hyödyntäen muun muassa tekoälyä ja koneoppimista. Kun tietoisuus omasta kybertoimintaympäristöstä saadaan kasvatettua riittävälle tasolle, voidaan myös päätökset tehdä järkevin perustein, jotta mahdolliset tietomurrot sekä muut tunkeutumisyritykset saadaan havaittua ja estettyä.

1.2 Tutkimuskysymykset ja aiheen rajaus

Opinnäytetyön oli tarkoitus antaa yleiskuvaa Organisaatio X:lle uudemman sukupolven SIEM-järjestelmistä ja kuinka tilannetietoisuutta voidaan kasvattaa SIEM-järjestelmien avulla. Päällimmäiseksi tutkimusongelmaksi muodostuikin siten, kuinka tilannetietoisuutta voidaan kasvattaa Organisaation X:n kybertoimintaympäristössä SIEM-järjestelmän avulla. Pääasiallisena tutkimuskysymyksenä oli:

Minkälainen SIEM-järjestelmä on mahdollisesti sopiva toimeksiannon tehneelle organisaatiolle?

Tutkimuskysymystä täydentävät seuraavat alakysymykset:

Mitä tarkoittaa tilannetietoisuus ja miksi se on tärkeä huomioida osana organisaation turvallisuutta kybertoimintaympäristössä?

Mikä on uudemman sukupolven SIEM-järjestelmä ja miten sillä kasvatetaan kybertoimintaympäristön turvallisuutta?

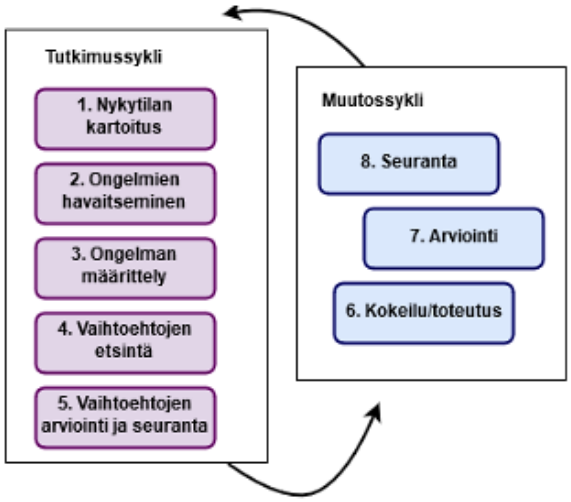
Päätutkimuskysymykseen etsittiin vastaus hyödyntäen toimeksiantajalta saatuja vaatimuksia tuotteelle sekä muita vapaasti saatavilla olevia tuotearviointeja, joiden pohjalta lähdettiin tekemään vertailuja valittujen tuotteiden välillä. Kahteen alakysymykseen vastatiin teoriaosuuden perusteella.

Koska aihe oli itsessään melko laaja, opinnäytetyön aihe rajattiin koskemaan ainoastaan SIEM-järjestelmän ominaisuuksia ja tilannetietoisuutta yleisesti. Lisäksi sopivan SIEM-järjestelmän löytämiseksi hyödynnetään yleisesti saatavilla olevia tietoja järjestelmien ominaisuuksista. Tutkimustyössä ei oteta kantaa siihen, minkä SIEM-järjestelmän Organisaatio X loppujen lopuksi tulee valitsemaan tai miten itse käyttöönotto toteutetaan. Parhaaksi vaihtoehdoksi valittu järjestelmä on kirjoittajan näkemys asiasta, jossa huomioitiin organisaation tarpeet. Myöskään tarkempia tietoja Organisaatio X:n toiminnasta tai vaatimuksista ei esitetä, koska tieto- tai kyberturvallisuuteen liittyvät hankintaratkaisut ovat salassa pidettävää tietoa niiden arkaluontoisuutensa vuoksi. Koska aihe liittyy erittäin vahvasti kyberturvallisuuteen, kirjoittaessa on pyritty myös huomioimaan koko tutkimustyön ajan turvallisuusnäkökulma.

1.3 Tutkimusmenetelmät

Tutkimusmenetelmäksi valikoitui kehittämistutkimus, koska päämääränä on muutos organisaation toiminnassa, ja tässä tapauksessa se toteutui SIEM-järjestelmän avulla. Yleensä kehittämistutkimus on sekoitus kvalitatiivista eli laadullista tutkimusta sekä kvantitatiivista eli määrällistä tutkimusta. Myös pelkästään kvalitatiivinen tutkimus on mahdollista toteuttaa määritelmän piirissä. Kehittämistutkimus eroaa kuitenkin perinteisimmistä tutkimusmenetelmistä, koska siinä tuotetaan ratkaisu tai poistetaan esitetty ongelma. Käytännössä kehittämissykli koostuu tutkimussyklistä ja muutossyklistä (ks. kuvio 1) sekä näiden toiminnan jatkuvuudesta. Tällöin kehitystutkimus

siirtyy jatkuvasti tutkimussyklistä muutossykliin, minkä jälkeen palataan jälleen nykytilan kartoitukseen ja edetään jälleen muutossykliin. (Kananen 2015, 39-42.)



Kuvio 1. Kehittämisyklin toimintaperiaate (Kananen 2015, 42)

Kehittämistutkimuksessa on tärkeää valita tavoitteet, joita kohti työssä edetään, ja mittarit, joilla saavutettuja tavoitteita mitataan (mts. 53). Tämän kehittämistyön tavoitteena on antaa ehdotus tavasta, jolla Organisaatio X voi kasvattaa kybertoimintaympäristönsä tilannetietoisuutta SIEM-järjestelmän avulla. Teoriaosuuden ja taustatutkimuksen konkreettisena tuloksena ovat erilaisten SIEM-järjestelmien vertailu ja parhaaksi valikoitunut vaihtoehto perusteluineen. Nämä toimenpiteet mahdollistavat Organisaatio X:n toimintatapojen ja työskentelymenetelmien tehostamisen tulevaisuudessa. Mittari työn onnistumiseksi on Organisaatio X:n kokema hyöty tutkimuksesta.

1.4 Aineistonkeruumenetelmät ja aiemmat tutkimukset

Laadullisen tutkimuksen aineistonkeruumenetelmiä ovat dokumentaatio, haastattelut sekä havainnointi. Määrällisessä tutkimuksessa hyödynnetään yleisesti esimerkiksi

kyselylomakkeita tai muita kuvausmenetelmiä, joiden avulla voidaan muodostaa erilaisia taulukoita, kaaviota ja muita vastaavia menetelmiä. (Kananen 2015, 24.) Tutkimuksen teoriaosuuden tiedot hankittiin laadullista menetelmää hyödyntäen, eli hyödyntämällä esimerkiksi erilaista dokumentaatiota ja havainnointia. Päätutkimuskysymykseen tuotettiin vaatimukset SIEM-järjestelmän ominaisuuksista toimeksiantajan haastattelujen avulla. Määrällistä tutkimusmenetelmää hyödynnettiin kerättäessä vertailtavat aineistot taulukkoon sekä määrittämällä pistemäärät ja asiakastyytyväisyyskyselyjen keskiarvot.

Aineistoa kerättiin tutkimuksessa mahdollisimman tuoreista lähteistä alan nopean kehityksen ja siten myös tietojen vanhenemisen johdosta. Tietolähteinä toimivat pääosin erilaiset korkeakoulujen tietokantojen kautta lainatut e-kirjat, kansainvälisesti arvostetut IEEE-julkaisut, tietoturva-asiantuntijoiden kirjaamat blogikirjoitukset sekä SIEM-valmistajien tuottama materiaali. Lisäksi tutkimuksessa hyödynnettiin erilaisia markkinointitutkimuksia ja käyttäjien arvosteluita eri verkkosivustoilta, joiden taustoihin perehdyttiin. Lainsäädäntöä, kansainvälisiä ISO-standardeja, KATAKRI-auditointikriteeristön sekä Valtionvarainministeriön tuottamia VAHTI-ohjeita käytettiin tutkimuksessa. Tutkimuksessa pyrittiin hahmottamaan myös laajempaa mittakaavaa ja soveltamaan tilannetietoisuuden vanhempia teorioita uudempiin näkökulmiin, joita käsitellään esimerkiksi Suomen kyberturvallisuusstrategiassa ja Suomen kansallisessa riskiarviossa. Opinnäytetyön kirjoittamisen aikana on myös keskusteltu tietoturva-asiantuntijoiden kanssa SIEM-järjestelmistä sekä Organisaatio X:n tarpeista.

SIEM-järjestelmistä ja niiden vertailusta on tehty useampia opinnäytetöitä, muttei ainakaan tutkimuksen kirjoittamishetkellä tilannetietoisuuden kasvattamisen tai uudemman sukupolven SIEM-järjestelmien ominaisuuksien näkökulmasta. Useimmat näistä on tehty pitkälti lokienhallinnan tai SIEM-järjestelmien perinteisempiä ominaisuuksia läpikäyden. Tässä opinnäytetyössä korostettiin nimenomaisesti uudemman sukupolven ominaisuuksia ja käytiin läpi teorioita tilannetietoisuudesta, sekä pohdittiin kuinka nämä kaksi ominaisuutta yhdistämällä saadaan kasvatettua kybertoimintaympäristön turvallisuutta. Tutkimustyön näkökulman tärkeyttä korostaa sen ajankohtaisuus Organisaatio X:n lisäksi myös yksilöllisellä ja yhteiskunnallisella tasolla. Ilman kyberturvallisuuteen liittyvää havainnointikykyä ja tilannetietoisuutta, ei voida

muodostaa kokonaisvaltaista kuvaa kybertoimintaympäristöstä, mikä altistaa erilaisille uhkatilanteille sekä kasvattaa niiden toteutumisen todennäköisyyttä.

2 SIEM

2.1 Yleistä SIEMistä

SIEMiä (Security Information and Management System) käytetään monitoroimaan reaaliajassa organisaation kybertoimintaympäristöä ja siihen sisältyviä järjestelmiä turvallisuustapahtumien ja uhkien havainnoimiseksi, kybertuvallisuuspoikkeamiin reagoimiseen sekä forensiikkaan. SIEM-termin kehittivät vuonna 2005 Mark Nicolett ja Amrit Williams heidän tutkiessaan uusia tietoturvajärjestelmiä. Käytännössä turvallisuuslokien hallinnointia ja analysointia hoitavat SIEM-järjestelmät ovat kuitenkin yhdistelmä vanhemman sukupolven SIM ja SEM-järjestelmistä. (SIEM-guide 2019, luku 1.) SIM (Security Information Management) sisältää muun muassa keskitettyä lokienhallintaa, lokidatan analysointia ja raportointia. SEM:llä (Security Event Management) taas hallinnoidaan ja valvotaan reaaliajassa IT-toimintaympäristön tapahtumia ja lokitietoja. (Pratt 2017; SIEM-guide 2019, luku 1.)

SIEMin yksi parhaista puolista on kyky käsitellä erityisten suuria määriä tapahtumia erilaisista lähteistä kybertoimintaympäristössä, koska mitä enemmän tapahtumia kerätään, sitä parempi näkyvyys organisaation tilannekuvasta saadaan muodostettua (Bhatt, Manadhata & Zomlot 2014, 37). Näitä tapahtumia voivat olla lokitiedot eri lähteistä sekä esimerkiksi käyttäjien haitallinen toiminta. Mitä suurempi IT-infrastruktuuri organisaatiolla on, sitä hankalampi sieltä on tunnistaa uhkia ja haavoittuvuuksia. Tämä johtuu muun muassa siitä, että laitteiden, palveluiden, sovellusten ja verkkojen määrä kasvaa valtavaksi ja siten myös niiden muodostama hyökkäyspinta-ala. (Canner 2019b; SIEM-guide 2019, luku 1.)

SIEMin tuottamia raportteja voidaan hyödyntää tapahtumien analysoinnissa ja auditoinneissa, sekä esimerkiksi forensiikkaa edellyttävissä tilanteissa. Hälytyksin tai järjestelmää tarkkailevan tietoturva-asiantuntijan toimesta voidaan toteuttaa poikkeamien analysointia. SIEMin avulla säästyy parhaassa tapauksessa organisaation resursseja, sekä tehokkuus ja havainnointikyky kasvavat, koska työntekijöiden työaika ei mene pelkkien lokitietojen läpikäymiseen. (Canner 2019a; SIEM-guide 2019, luku 1.) Lisäksi SIEMillä voidaan hallitusti valvoa organisaatiossa ilmenneitä haavoittuvuuksia, joiden lieventäminen ei esimerkiksi päivityksin tai konfiguraatiomuutoksin ole mahdollista (Canner 2019b).

SIEMin lukuisten hyvien puolien lisäksi järjestelmässä on tietysti myös omat haasteensa, kuten toimivien säännöstöjen luominen. Säännöstöjä tehtäessä ongelmaksi voivat muodostua niiden sopiva määrä. Mikäli sääntöjä luodaan liikaa, kyberympäristöstä ei saada välttämättä kaikkea olennaista tietoa tai jos sääntöjä on liian vähän, saadaan liikaa turhaa tietoa. Nämä omalla tavallansa estävät kunnollisen ja realistisen kokonaiskuvan luomisen, kun työntekijöiden aikaa menee hukkaan väärien positiivisten (engl. false positive) havaintojen käsittelyssä. (Saurabh 2017.) Myös SIEM-järjestelmän käyttöönotto, konfigurointi ja siihen liittyvät kustannukset voivat nousta ongelmiksi organisaatiossa.

2.2 SIEM-tyypit

SIEM-tyypit voidaan jaotella ainakin neljään eri ryhmään sen mukaan, miten niiden toteuttaminen, ylläpito ja hallinnointi on toteutettu. Kun palvelua harkitaan otettavaksi edes osittain ulkopuolisen palveluntarjoajan kautta, tulee määritellä tarkasti oikeudet ja vastuut.

SIEM-tyypit ovat seuraavat (SIEM-guide 2019, luku 1):

1. Talon sisällä hallinnoitu SIEM (In-house SIEM)
2. Pilvipohjainen SIEM (Cloud-based SIEM)
3. Ulkopuolella hallinnoitu SIEM (Managed SIEM)
4. Hybridi-SIEM (Hybrid-SIEM).

2.2.1 Talon sisällä hallinnoitu SIEM

Talon sisäisessä SIEMissä kaikki SIEMin suunnittelusta, toteutuksesta ja ylläpidosta lähtien on toteutettu organisaation sisällä. Tämä ratkaisu saattaa kuitenkin olla hyvinkin työläs ja aikaa vievä kaikkine työvaiheineen ja koulutuksineen, koska SIEMin integrointi ja käyttöönotto voi viedä paljonkin organisaation resursseja. Joskus kunnollisen näkyvyyden aikaansaamiseen saattaa mennä kuukausia ja joskus sitä ei ikävä kyllä saavuteta lainkaan. (Jyotiprakash 2017.) Kustannuksia voi kertyä työntekijöiden palkkojen lisäksi hankittavasta laitteistosta ja ohjelmistosta. Hyötynä oman organisaation sisäisestä SIEM-ratkaisusta on tietojen pysyminen omassa organisaatiossa, oman IT-infrastruktuurin ja käytäntöjen tunteminen, mikä helpottaa käyttöönottoa sekä päätösten tekemistä ja niiden vaikutuksien arvioimista kybertoimintaympäristöön (Pros and cons of outsourcing your Cyber Security - In-house, MSSP, or Virtual SOC? 2017).

2.2.2 Pilvipohjainen SIEM

Pilvipohjainen SIEM voidaan toteuttaa ulkopuolisena palveluna joko täysin tai osittain. Pilviratkaisuiden eroissa on oma hinnoittelunsa riippuen tavasta, millä ne on toteutettu sekä palvelun ominaisuuksista, eli ostetaanko pilvipalveluun kokonaan lisenssi, käytetäänkö mahdollisia omia konesaleja datan säilyttämiseen vai käytetäänkö näitä täysin palveluntarjoajan puolelta. Pilviratkaisussa tulee aina miettiä kuitenkin oman datan kriittisyyttä, halutaanko sitä jakaa mahdollisille kolmansille osapuolille, miten data on suojattu ja mitkä lait koskevat palveluntarjoajaa. (PiTuKri 2019, 9-16)

Tietoturvallisuuden näkökulmasta pilvipalveluihin liittyy ylipäätänsä monia riskejä. Traficomin Kyberturvallisuuskeskus on listannut Pilvipalveluiden turvallisuuden arviointikriteeristössä (PiTuKri 2019) lukuisia kohtia, joita tulee ottaa huomioon pilviratkaisuja harkitessa tietojen suojaustasosta riippuen. Hyvinä ominaisuuksina pilvipalveluna toteutetussa SIEMissä on kuitenkin sen nopea käyttöönotto, skaalautuvuus erilaisiin ympäristöihin ja kuluissa säästäminen esimerkiksi mahdollisen laitteistohankintojen osalta. Lisäksi kun palvelu otetaan muualta, voidaan säästää palkkakuluissa,

kun asiaan perehtynyt palveluntarjoaja hoitaa suurimman osan tehtävistä töistä. (Cloud SIEM Solutions 2019; Jyotiprakash 2017.)

2.2.3 Ulkopuolella ylläpidettävä SIEM

Mikäli SIEM-ratkaisu päädytään hankkimaan kokonaan tai edes osittain ulkopuoliselta palveluntarjoajalta, voidaan tämän avulla säästää aikaa ja kustannuksia, koska palveluntarjoajilla on useimmiten valmiiksi koulutettu henkilöstö toteuttamaan ja ylläpitämään SIEMiä. Lisäksi tarjolla on palveluita, joissa palveluntarjoaja voi monitoroida omassa tietoturvakeskuksessaan organisaation kybertoimintaympäristön tilannetta jopa vuorokauden ympäri. Kun palvelu ostetaan ulkopuoliselta taholta, voidaan organisaation työntekijät vapauttaa edes osittain hoitamaan muitakin työtehtäviä. Kuten pilvipalvelupohjaisten ratkaisujenkin yhteydessä mainittiin, myös tämä ratkaisu on skaalautuvampi kuin itse tuotettu SIEM-ratkaisu. Tässä ratkaisussa huonona puolena on tietojen päätyminen kolmansille osapuolille, joten palveluntarjoaja tulee miettiä tarkasti, jotta tietyt lait ja standardit on huomioitu palvelussa, sekä onko organisaatio valmis luovuttamaan omia tietojaan eteenpäin. (Pros and cons of outsourcing your Cyber Security - In-house, MSSP, or Virtual SOC? 2017.)

2.2.4 Hybridi-SIEM

Hybridi-SIEMissä käyttöönotto on toteutettu oman organisaation toimesta, mutta itse ylläpitoa ja hallinnointia hoitavat yhdessä oman organisaation työntekijät, sekä SIEM-palveluntarjoaja. Laitteistot ja ohjelmistot hankitaan talon puolesta, mutta palveluntarjoaja antaa tässäkin tapauksessa apua, mikäli omassa organisaatiossa ei ole osaamista SIEMin hallinnointiin. Tässä SIEM-tyypissä voi muutoin huomioida samat asiat kuin on aiemmin luvussa 2.2.2 mainitut. (SIEM-guide 2019, luku 1.)

2.3 SIEM-sukupolvet

SIEM-järjestelmät voidaan jakaa myös niiden ominaisuuksien ja julkaisuaikojen mukaisesti kolmeen eri sukupolveen. Näiden ominaisuudet on havainnollistettu tarkemmin taulukossa 1. Ensimmäisen sukupolven SIEM-järjestelmiin voidaan lukea aiemmin mainitut SIM ja SEM-järjestelmien yhdistelmät, joiden ominaisuudet ovat hyvin

rajalliset verraten nykyajan tarpeisiin. Dataa kyettiin varastoimaan, mutta vain osittain sekä lokitietojen rikastaminen oli hidasta ja manuaalista, kuten kaikki muutkin sen ajan SIEMin ominaisuudet. Toisen sukupolven SIEMin perustuessa datamassojen (engl. big data) käsittelyyn mahdollistaa se suurien datamäärien käsittelyn, jota voidaan rikastaa automaattisesti. Toisen sukupolven SIEM-ratkaisussakaan ei päästy täysin manuaalisuudesta eroon, vaan esimerkiksi uhkien havainnointi, hälytykset sekä ohjausnäkymää (engl. dashboard) käsitellään ja luodaan manuaalisesti. Poikkeamiin reagointiin liittyvät rajapinnat ja esimerkiksi visualisointitoiminteet ovat rajoitettuja. (SIEM-guide, SIEM-guide 2019, luku 1.)

Taulukko 1. SIEM-sukupolvet (SIEM-guide 2019, luku 1, muokattu)

SIEM (2005)	Next-Gen SIEM (2010)	Third-Gen SIEM (2017)
Skaalautuu vertikaalisesti	Skaalautuu horisontaalisesti, tuki massadatalle	Rajaton skaalautuvuus, perustuu tietoaltaisiin
Osittain historiallista dataa	Täysin pääsy historialliseen dataan suodatuksen kera	Rajaton pääsy historialliseen dataan mukaan lukien uudet datalähteet, kuten pilvi
Hidas manuaalinen lokien tutkiminen	Automaattinen datankeruu, rajoitetut tietolähteet	Automaattinen datankeruu mistä tahansa tietolähteestä
Uhkien analysointi manuaalisesti, hälytykset manuaalisesti luotu	Uhkien analysointi, hälytykset ja visualisointi manuaalisesti	Uhkien analysointi automaattista, perustuu koneoppimiseen ja UEBAan
Poikkeamien hallintaa vähän tai ei ollenkaan	Poikkeamien hallintaan rajattu rajapinta	Poikkeamien hallinta integroituu IT- ja turvallisuustyökalujen kanssa, täydet SOAR kyvykkyydet
Rajatut visuaaliset näkymät	Yleensä rajatut ja valmiiksi sisäänrakennetut näkymät	Täysi BI-tietojen etsiminen

Vuonna 2017 kehitetyssä kolmannen sukupolven SIEM-järjestelmässä on keskitytty pitkälti automatisointiin ja koneoppimiseen (SIEM-guide 2019, luku 1.). Koneoppimisella tarkoitetaan tekoälyä hyödyntävää sovellusta, jonka avulla voidaan automatisoida tiettyjä tapahtumia. Päätarkoituksena on, että koneoppimisen avulla tietokoneet voivat oppia automaattisesti toimenpiteitä, ilman ihmisen osallistumista tapahtumien käsittelyyn. Koneoppimista voidaan hyödyntää esimerkiksi vanhan datan pe-

rusteella tapahtuvaa tulevien tapahtumien ennustamista. (What is Machine Learning? A definition 2017.) Uhkilta suojautuminen pohjautuu juuri koneoppimiseen, jossa voidaan nauhoittaa tietynlaista käyttäytymistä ja näin ollen automatisoida datan analysointia sekä erottaa esimerkiksi käyttäjien poikkeava käyttäytyminen normaalista. Tietoturvapoikkeamiin reagoimisessa voidaan hyödyntää lukuisia eri turvallisuustyökaluja sekä esimerkiksi SOARia (Security Orchestration Automation and Response). Kolmannen sukupolven SIEM perustuu tietoaltaisiin, joissa tallennettavan tiedon määrä on lähes rajatonta, jolloin myös tietoja voidaan käsitellä ihan eri tavoin perinteiseen SIEMiin verrattuna. (SIEM-guide 2019, luku 1.)

2.4 SIEMiin liittyviä määritelmiä

2.4.1 Haavoittuvuus, uhka ja riski

Haavoittuvuudella tarkoitetaan esimerkiksi ohjelmistojen ja järjestelmien koodivirheitä, joista aiheutuu heikkouksia. Näitä heikkouksia hyväksikäyttämällä hyökkääjä voi aiheuttaa haittaa organisaatiolle. Tämä vaarantaa tietoturvallisuuden tunnetut kulmakivet eli tietojen luottamuksellisuuden, eheyden ja saatavuuden. (Vulnerabilities 2019.) Koodivirheiden lisäksi haavoittuvuuksia voidaan nähdä aiheutuvan muun muassa ihmisten toiminnasta, ohjeiden puutteellisuudesta, konfiguraatiovirheistä, sekä organisaation huonoista prosesseista. Haavoittuvuuksia aiheutuu useimmiten tahattomasti, mutta niitä voidaan tehdä myös tahallisesti. Esimerkkejä tahattomista tilanteista voi olla käyttäjän pääsy virheellisesti aineistoon, johon hänen käyttöoikeutensa ei pitäisi riittää. Tähän voi olla syynä tilanne, jossa vanhan työntekijän tunnuksia ei poisteta tai nykyiselle työntekijälle on jäänyt muuttuneen työnkuvan johdosta ylimääräisiä käyttöoikeuksia. Haavoittuvuuksia voi aiheutua myös päivittämättömistä ohjelmistoista, joiden vuoksi ohjelmistoon aiheutuu tietoturva-aukko. Tahallisesti aiheutettu haavoittuvuus voisi olla esimerkiksi takaporttien ohjelmoiminen koodiin. (VAHTI 2009, luvut 2.1-2.2.)

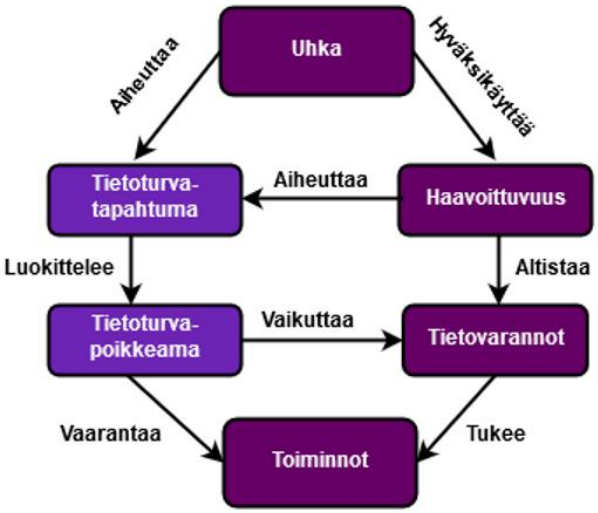
Uhkalla tarkoitetaan haittaa, joka aiheutuu hyödynnettäessä olemassa olevaa haavoittuvuutta. Riskillä tarkoitetaan uhkan ja haavoittuvuuden muodostamasta koko-

naisvaikutuksesta ja sen todennäköisyydestä aiheutuvaa negatiivista vaikutusta organisaatiolle. (Dunkerley & Rogers 2016.) Tämän vuoksi useimmiten erilaisissa riskianalyyseissä hyödynnetään juuri riskin toteutumisen todennäköisyyttä kerrottuna sen vaikutuksella organisaatioon ja riski pisteytetään saadun arvon mukaan (Calder & Watkins 2007). Riskienhallintaprosessissa riskit tunnistetaan, analysoidaan, arvotetaan sekä päätetään, minkälaisia hallintatoimenpiteitä tehdään (SFS-EN ISO/IEC 27001:2017, 8).

SIEM auttaa haavoittuvuuksien- ja riskienhallinnassa etsimällä kyberympäristöstä mahdolliset riskit siihen kuuluvien turvallisuusominaisuuksien ja työkalujen avulla (Tchesnokov 2016). Useimmiten SIEM-järjestelmiin kuuluu haavoittuvuusskanneri tai se on erikseen integroitavissa SIEMiin. Esimerkiksi haavoittuvuusskannauksesta saatujen tietojen avulla haavoittuvuudet arvioidaan kriittisyyden mukaan ja mikäli haavoittuvuutta ei voida poistaa tai lieventää, voidaan siitä aiheutuvaa riskiä monitoroida SIEM-järjestelmän avulla ja reagoida nopeasti, mikäli haavoittuvuutta yritetään hyödyntää hyökkäyksessä.

2.4.2 Tapahtumat ja poikkeamat

Tapahtumalla tarkoitetaan Miesslerin (2017) mukaan tilaa, jossa tarkkailtava kohde muuttuu jollakin tavalla johtuen esimerkiksi ihmisen tai toisen järjestelmän toiminnasta. Käytännössä tällainen tilanne voi olla esimerkiksi, kun järjestelmää päivitetään uudempaan versioon, jolloin järjestelmän tila muuttuu. SIEM-järjestelmän yhteydessä puhutaan myös välikohtauksista tai poikkeamista (engl. incident), jotka ovat negatiivisia tapahtumia. Käytännön esimerkkinä poikkeamasta voidaan mainita tilanne, jossa asiakastietoja vuodetaan hakkerin toimesta Internetiin ja tästä aiheutuu sekä organisaatiolle että asiakkaalle haittaa, kun arkaluontoiset tiedot ovat kaikkien saatavilla. (Miessler 2017.) Kuviossa 2 on esitelty yleisellä tasolla, kuinka tietoturvatapahtuma eskaloituu uhkan hyödyntämisestä tietoturvapoikkeamaksi ja kuinka tapahtumiin vaikuttavat riippuvuudet voidaan määritellä. Tummemmalla värillä merkittyjen laatikoiden kohteet ovat olleet jo aiemmin olemassa, niihin vaikuttavat vaaleammalla värillä merkittyjen laatikoiden sisältämät osa-alueet ja tämän lopputuloksena tapahtuu tietoturvapoikkeama (SFS-ISO/IEC 27035-1:2016, 3).



Kuvio 2. Tietoturvapoikkeama ja osa-alueiden riippuvuudet (SFS-ISO/IEC 27035-1:2016, 3, muokattu)

2.4.3 Lokidata

Yleisesti ottaen lokilla tarkoitetaan eri laitteiden, kuten tietokoneiden, verkkolaitteiden, älypuhelimien tai esimerkiksi erilaisten sovellusten keräämää tietoa niiden toiminnasta tai erilaisista virhetilanteista. Useimmiten lokiin tallennetaan tietoa, kuten milloin jokin asia tapahtui, kuka teki ja mitä teki. Lokitietoja kerätään, jotta voidaan selvittää esimerkiksi syitä johonkin virhetilanteeseen tai tietoturvapoikkeamaan. Tästä syystä SIEMissäkin hyödynnetään lokeista saatavaa tietoa joko reaaliajassa tai jälkikäteen forensiikassa. Lokitietoja voidaan koostaa erilaisista lähteistä ja riippuen niiden käyttötarkoituksesta, ne voidaan luokitella esimerkiksi ylläpitolokiin, käyttö- tai tapahtumalokiin, muutoslokiin, virhelokiin ja viestintälokiin. (Näin keräät ja käytät lokitietoja 2019.)

Viestintävirasto (2016) määrittää lokilta kerättäväksi vähintään seuraavia tietoja: aikaleima, tapahtuma, toimija, käyttöoikeus, tapahtuman lähde, tapahtuman kohde ja tapahtuman tila. Ilman näitä tietoja on vaikeaa lähteä hyödyntämään tai selvittämään virhetilanteessa mitä tehtiin tai yritettiin tehdä. Lokitietoihin pääsyä tulee ehdottomasti rajata sellaisilta tahoilta, jotka eivät työtehtävissään niitä tarvitse. Lokitietojen tulee säilyä muuttumattomina eikä kenelläkään pitäisi olla muokkausoikeutta

tietoihin, jotta oikeellisuus, muuttumattomuus ja luottamuksellisuus voidaan saavuttaa. (Lokien keräys ja käyttö 2016, 2-4.)

Vaikka lokienhallinta on yksi SIEMn ominaisuus, tulee kuitenkin ottaa huomioon, ettei se ole SIEMin päätarkoitus. Lokienhallinnassa pääpaino on lokituksen tekemisellä, varastoinnilla ja organisoinnilla, kun taas SIEMissä keskitytään turvallisuuslokien tai tapahtumien hyödyntämiseen tietoturvallisuuden kasvattamiseksi kyberympäristössä. (Blackstratus 2019.) Siten SIEMissä voidaan ajatella turvallisuuteen liittyvien toiminnallisuuksien olevan laajemmassa käytössä kuin perinteisemmässä lokienhallinnassa.

2.4.4 Kybertoimintaympäristö

Kybertoimintaympäristö määritellään ulkoministeriön julkaisussa (Kyberturvallisuus ja kybertoimintaympäristö 2019) ihmisen luomana digitaalisena rinnakkaistodellisuutena, mikä yhdistää ihmiset, laitteet, ja informaatioteknologian valtioiden rajojen yli. Toinen määritelmä kyseiselle termille on yksinkertaisesti ”yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö”, joka on määritelty Turvallisuuskomitean kyberturvallisuussanastossa (Kyberturvallisuuden sanasto 2018, 21). Koska termejä ja määritelmiä on yhtä paljon kuin näkökulmia maailmassa, tässä opinnäytetyössä viitataan kybertoimintaympäristöllä koko organisaation IT-infrastruktuuriin ja sen sisältämiin laitteisiin, tietoliikenneverkkoihin sekä tietojärjestelmiin.

3 Lainsäädäntö, tietoturvavaatimukset ja standardit

SIEM-järjestelmää koskettavat useat eri lait liittyen esimerkiksi turvalliseen tietojenkäsittelyyn, säilytykseen, lokienhallintaan tai mahdollisiin henkilörekistereihin. SIEM-ratkaisua valitessa tulee ottaa huomioon myös tietoaineistojen luokitteluun liittyviä vaatimuksia, kansainvälisiä standardeja ja lainsäädäntöä. Näiden lisäksi Suomessa on hyvä hyödyntää myös Valtionvarainministeriön luomia VAHTI-ohjeita, joiden sisältö

koostuu turvallisuuteen liittyvistä hyvistä käytännöistä. KATAKRI, eli tietoturvallisuuden auditointityökalu viranomaisille sisältää ohjeita eri suojaustason turvallisuuteen kohdistuvista vaatimuksista. Vaatimukset itsessään pohjautuvat Suomea koskevaan lainsäädäntöön, sekä kansainvälisiin tietoturvallisuuteen liittyviin velvoitteisiin. (KATAKRI 2015, 3.)

3.1 Lainsäädäntö

Riippuen organisaation toimialasta, eri lainsäädännön osa-alueet tulee huomioida esimerkiksi lokitietojen käsittelyssä ja keräämisessä sekä käsiteltäessä henkilötietoja. Alle on koottu esimerkkejä lainsäädännöstä, joita SIEM-hankinnassa tulee ottaa huomioon (Lokien keräys ja käyttö 2016, 7):

- Julkisuusasetus (621/1999)
- Henkilötietolaki (523/1999)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Tietoyhteiskuntakaari (7.11.2014/917)
- Sähköisen viestinnän tietosuojalaki (526/2004)
- Asetus Tietoturvallisuudesta valtionhallinnossa (1.7.2010/681)
- Julkisuusasetus (12.11.1999/1030)
- Laki tietoyhteiskunnan palveluiden tarjoamisesta (21.5.1999/621)
- Arkistolaki (23.9.1994/831)
- Pakkokeinolaki (22.7.2011/806)
- Poliisilaki (22.7.2011/872).

Tiedonhallintalaki (906/2019) astuu voimaan 1.1.2020. Laki sisältää tietoturvallisuuteen ja lokienhallintaan liittyviä vaatimuksia sekä muuttaa tai korvaa osittain tai kokonaan yllämainittuja säädöksiä, joten myös tämän säädöksen huomioiminen on tärkeää edellä mainittujen lisäksi. Tietosuojaan ja henkilötietojen käsittelyyn liittyen on huomioitava EU:n tietosuoja-asetus, eli GDPR (General Data Protection Regulation) ((EU) 679/2016).

3.2 Tiedon luokittelu

Tiedon luokittelun avulla saadaan pienennettyä tietoturvariskejä. Kun tiedot luokitellaan huolellisesti, säilytetään suojaustasoa vastaavalla tavalla, kartoitetaan riskit ja

pidetään yllä luetteloa salassa pidettävien tietojen käsittelyoikeuksista, saadaan näiden keinojen avulla kasvatettua organisaation tietoturvatasoa huomattavasti. (KATAKRI 2015; T04, 8; T12, 15.)

Suojaustasot on määritelty Valtioneuvoston asetuksessa julkisuuslain 621/1999 25§:ssä. Suojaustasot on määritelty salassa pidettävien asiakirjojen tietoturvallisuuteen liittyvien vaatimusten perusteella ja eri suojaustasot määräytyvät sen mukaan, kuinka suurta haittaa niiden oikeudettomasta paljastumisesta voi aiheutua joko yksilön, organisaation tai yhteiskunnan edulle. Taulukosta 2 on nähtävissä suojaustasot. Tiedonhallintalain myötä kyseiset suojaustasot kuitenkin poistuvat ja tilalle jäävät turvallisuusluokitukset.

Taulukko 2. Suojaustasot ja turvaluokitusmerkinnät (VAHTI 2010)

Oikeudeton paljastuminen voi aiheuttaa:	Salassapitomerkintä	Turvallisuusluokitusmerkintä
Haittaa yleiselle tai yksityiselle edulle	SALASSA PIDETTÄVÄ ST IV	KÄYTTÖ RAJOITETTU ST IV
Vahinkoa yleiselle tai yksityiselle edulle	SALASSA PIDETTÄVÄ ST III	LUOTTAMUKSELLINEN ST III
Merkittävää vahinkoa yleiselle edulle	SALASSA PIDETTÄVÄ ST II	SALAINEN ST II
Erityisen suurta vahinkoa yleiselle edulle	SALASSA PIDETTÄVÄ ST I	ERITTÄIN SALAINEN ST I

Mikäli esimerkiksi suojaustason IV tietoja kerätään SIEMin keskitettyyn tietokantaan suuria määriä, voi tämä tietokasautuma nostaa vaatimuksen huomioida suojaustason III vaatimukset tietojen käsittelylle ja ympäristölle (KATAKRI 2015; I01, 32.). Myös tietojen elinkaaren ajan tietoja tulee säilyttää ja käsitellä siten, että niiden eheys, luottamuksellisuus sekä saatavuus toteutuvat. Tämä voidaan varmentaa organisaatiossa teknisellä ja hallinnollisella tasolla, sekä varmistamalla jäljitettävyys tahoille, joilla on pääsy käsitellä esimerkiksi SIEM-järjestelmään liittyviä tietoja. (KATAKRI 2015; I18, 57.)

Myös fyysinen turvallisuus on tärkeä osa tietojen suojaamista. Tiedot tulisikin tämän vuoksi säilyttää oman suojaustasonsa luokituksen mukaisesti ja mieluusti fyysisesti erillään toisistaan, eli tehdä eri tasojen turvallisuusvyöhykkeitä. Tehokkaimpana keinona on suosia kerroksellista suojausta siten, että korkeimman tason tiedot säilytetään organisaation sisimmässä tilassa ja asiaton pääsy tiloihin on estetty. Tähän voivat olla apukeinona erilaiset videovalvontamenetelmät, vartiointi sekä pääsyoikeuksien rajaaminen ainoastaan henkilöille, jotka ovat oikeutettuja tietoon ja pääsevät sisään ainoastaan esimerkiksi rajoitetulla avainkortilla. (KATAKRI 2015; F01, 17.)

SIEM-järjestelmän käytössä tulee ottaa huomioon myös erityisesti käyttäjien oikeudet. Kun järjestelmään tallennetaan yksityiskohtaista tietoa esimerkiksi organisaation käyttäjien toiminnasta tai ylipäätänsä koko organisaation verkkoliikenteestä, tulee erityisen tarkasti huomioida tiedonvarastointimenetelmät, sekä miten tietoa siirretään luotettavasti ja turvallisesti. (Astakhova & Muravyov 2019.) Erityisesti käyttöoikeudet SIEM-järjestelmään tulee myöntää harkitusti, jotta tietoon pääsy on vain sellaisilla henkilöillä, joilla on siihen perusteltu tarve työtehtäviinsä nähden (KATAKRI: I06, 38).

3.3 Standardit

Tietoturvallisuuteen liittyvät kansainväliset standardit ohjaavat tietoturvallisten järjestelmien hankinnassa ja yleisesti saavuttamaan tietynlaisen tietoturvallisuuden tason organisaatiossa. Yleisimmät näistä tietoturvallisuuteen liittyvistä standardeista ovat ISO27000-sarjaa. Sarjassa on useita julkaisuja liittyen tietoturvallisuuden hallintajärjestelmiin ja yleisiin hallintakeinoihin, tietoturvahäiriöiden hallintaan, tietoturvariskeihin ja niin edelleen. Lisäksi on mahdollista hankkia erilaisia sertifikaatteja omalle organisaatiolle, joilla voidaan viestiä oman organisaation tietoturvallisuuden luotettavuutta. ISO27000-sarjassa on myös listattuja vaatimuksia sertifiointia ja auditointia varten. Kansainväliset alan ammattilaiset ovat pyrkineet luomaan malleja pohjaksi tietoturvalle huomioiden alan nopean kehittymisen. (SFS-EN ISO/IEC 27000:2017, 5.)

4 Tilannetietoisuus kybertoimintaympäristössä

4.1 Teoreettinen tausta

4.1.1 Endsleyn teoria

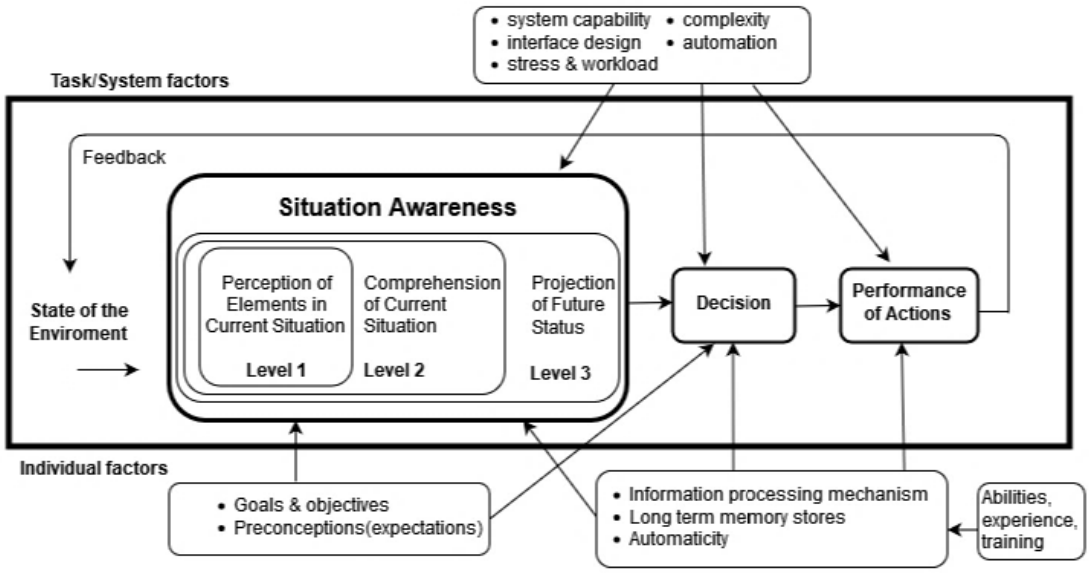
Tilannetietoisuuden (engl. situational awareness) juuret ulottuvat menneisyyteen ensimmäiseen maailmansotaan, jolloin toimintatapaa hyödynnettiin ilmavoimissa päätöksenteossa ilmatilan ollessa muuttuva tai jopa vaarallinen ympäristö. Useissa tutkimuksissa ja tietolähteissä viitataan Endsleyn (1995) kehittämään teoriaan tilannetietoisuudesta, jossa painotetaan teorian hyödyntämistä ihmisten päätöksenteossa monimutkaisissa ja dynaamisissa ympäristöissä. Endsley määrittelee tilannetietoisuuden yksinkertaisesti tilaksi, jolloin tiedetään mitä tapahtuu. Toinen hieman monipuolisempi määritelmä Endsleyltä (1995, 36) on *"Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"*. Tässä määritelmässä painottuvat ympäristön elementtien havainnoiminen yhdessä ajan ja tilan kanssa sekä niiden merkityksen ymmärtäminen lähitulevaisuuden kannalta.

Endsley jakaakin edellä mainitun määritelmänsä mukaisesti tilannetietoisuuden kolmeen eri tasoon, joiden pohjalta tehdään päätökset ja toimitaan niiden mukaisesti (Endsley 1995, 32-37):

1. Elementtien havaitseminen ympäristöstä
2. Nykyisen tilanteen ymmärtäminen
3. Tulevan tilan ennustaminen.

Kuviossa 3 on havainnollistettu Endsleyn malli tilannetietoisuudesta dynaamisessa päätöksenteossa. Yksilötasolla tilannetietoisuuteen ja tilannekuvan luomiseen vaikuttavat ympäristön elementit ja miten esimerkiksi stressi- tai muiden ulkoisten tekijöiden tai ympäristön kompleksisuuden vaikuttaessa yksilöön havaitaan oleelliset asiat. Tämän vuoksi toisessa tasossa pyritään tavoittelemaan syvällisempää ymmärrystä vallitsevasta tilasta aiemmin havaittujen elementtien perusteella. Toisessa tasossa

pyritään siis luomaan tavallaan kokonaiskuvaa senhetkisestä tilanteesta, jotta tietoa pystytään hyödyntämään tulevassa päätöksenteossa. Kolmannessa tasossa pyritään ennustamaan havaittujen elementtien (taso 1) ja niiden muodostaman tilanteen perusteella (taso 2) mitä tapahtuu tai voi tapahtua seuraavaksi. Tämän perusteella edetään varsinaiseen päätöksentekoon ja toimintaan näiltä kolmelta eri tasolta muodostettujen havaintojen ja johtopäätösten perusteella. (Endsley 1995, 36-37.)



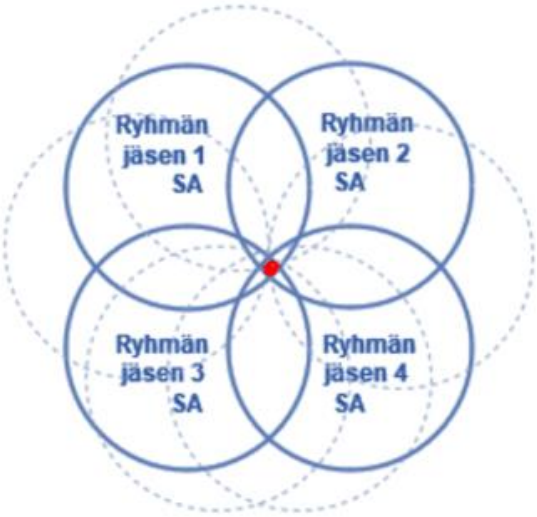
Kuvio 3. Endsleyn malli tilannetietoisuudesta (Endsley 1995, 35, muokattu)

Endsleyn teoriassa puhutaan pitkälti yksilöön liittyvänä tietoisuuden tilana, mutta kuten kuviossa 3 nähdään, vaikuttaa prosessiin paljon muitakin tekijöitä. Etenkin tarkisteltaessa tilannetietoutta digitaalisessa ympäristössä, vaikuttavat tilannetietoisuuteen esimerkiksi kybertoimintaympäristön monimutkaisuus ja laajuus. Endsley mainitsee myös muun muassa järjestelmiin liittyvinä tilannetietouteen vaikuttavina osa-alueina automaation, järjestelmän kyvykkyydet, rajapintojen suunnittelun, kompleksisuuden, stressin ja työkuorman (Endsley 1995, 35).

Endsleytä on kritisoitu useammassakin tutkimuksessa tästä perusmallista ja hän itse kumoaakin tämän teorian toimivuuden tutkimuksessaan *Situation Awareness*

Misconceptions and Misunderstandings (Endsley 2015, 8) täysin sellaisenaan kompleksisessa ja dynaamisessa ympäristössä. Perusteorian avulla voidaan kuitenkin tehdä päätöksiä tehokkaammin ja paremmin kuin perinteisessä ihmisen tekemässä kognitiivisessa päätöksentekoprosessissa (Endsley 1995, 32; Endsley 2015, 9-10). Koska Endsleyn vuonna 1995 kehittämää teoriaa on hyödynnetty lukuisissa tutkimuksissa vielä lähivuosinakin, voidaan tästä päätellä teorian pohjimmiltaan soveltuvan kuitenkin päätöksenteon tai vähintäänkin uudempien toimintamallien pohjaksi. Tämän tuottaman merkittävyyden vuoksi teoria nostettiin tutkimuksessa esiin.

Kun tavoitellaan kokonaisvaltaista tilannetietoisuutta kybertoimintaympäristössä, tavoitellaan oikeastaan enemmän ryhmän tai ryhmittymien muodostamaa kokonaisuutta kuin pelkästään yksilön näkökulmaa. Tällöin voidaan puhua ryhmän tilannetietoisuudesta. Kuviossa 4 on esitettynä Endsleyn näkemys kuinka ryhmän sisäinen tilannetietoisuus muodostuu (Endsley 1995, 39). Tiivistetysti ilmaistuna tässä teoriassa jokaisella yksilöllä on oma tilannetietoisuutensa, joista olennaisia osia jakamalla toisilleen saadaan koostettua oikeellisin kuva tilannetietoisuudesta (kirkkaanpunaisella merkitty osio kuviosta). Tähän voidaan laskea mukaan vielä kybertoimintaympäristön resurssit, eli esimerkiksi eri tietojärjestelmien tuottamat lokitiedot ja muut vastaavat. Tämä on havainnollistettu kuviossa 4 ulommaisilla katkoviivaisilla ympyröillä. Ryhmän muodostama tilannetietoisuus voidaan nähdä esimerkiksi siten, että tiimin jäsenillä on omat työtehtäviin kuuluvat osa-alueensa, eli esimerkiksi osaamisalueelle kuuluvat järjestelmät ja prosessit, jotka tuottavat tilannekuvaa kybertoimintaympäristöstä. Kaikkea, etenkään tarpeetonta tietoa ei tosin tarvitse jakaa kaikille, mutta myöskään olennaisia tietoja ei saa jättää kertomatta, koska siinä tapauksessa tilannekuva vääristyy (Endsley 1995, 39).



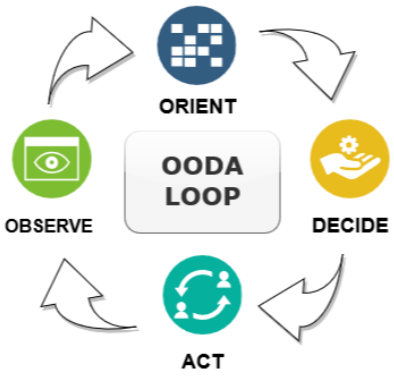
Kuvio 4. Ryhmän muodostama tilannetietoisuus (Endsley 1995, 39, muokattu)

Yhtenä riskinä tässä voidaan nähdä, ettei yksilö erota oleellista tietoa osaamisesta tai muusta puutteelliseen havainnointikykyyn liittyvästä seikasta johtuen, jolloin tilannekuvan koostaminen ja sitä kautta tilannetietoisuus on vaillinaista. Nykyaikana tuleekin siis huomioida yksilöiden lisäksi eri järjestelmien tai muiden resurssien tila, jolloin kybertoimintaympäristössä vallitseva tilanne saadaan tietyn ryhmän tietouteen ja koostettua näistä pienistä palasista tarvittava kokonaisuus. Tällaisessa tapauksessa turvallisuuden valvontajärjestelmä, kuten SIEM, on omiaan kasvattamaan tietoisuutta omasta kybertoimintaympäristöstä.

4.1.2 OODA-silmukka päätöksenteossa

Toinen tärkeä teoria päätöksentekoon liittyen on John Boydin kehittämä OODA-silmukka (engl. loop), jota on laajalti käytetty päätöksenteossa toimialasta riippumatta. Tätä päätöksenteon mallia hyödynnettiin muun muassa Yhdysvaltojen ilmavoimien operaatiossa Korean sodassa jo vuonna 1953 (Enck 2012). OODA-silmukka koostuu neljästä eri tilasta, eli havainnointi (observe), tilanteen arviointi (orient), päätöksenteko (decide) ja toiminta (act), kuten kuviosta 5 nähdään. Teorian mukaan onnistuneeseen päätöksentekoon vaaditaan jatkuvaa havainnointia, tunnistamista, sekä muuttuvien tilanteiden ennustamista tilan, ajan, sekä havaintojen yhteisvaikutuksen ymmärtämisen kautta, jotta osataan tehdä oikeanlaisia päätöksiä. Tämän

vuoksi vuorovaikutus näiden OODA-silmukan eri tilojen välillä on erityisen tärkeää. Silmukkamainen esitystapa kuvaa prossin jatkuvuutta. (Ilin & Rogova 2019, 34.)



Kuvio 5. OODA-silmukka (Ilin & Rogova 2019, 34, muokattu)

Havainnointivaiheessa huomioidaan ulkopuolinen informaatio sekä muuttuvat olosuhteet tarkkailtavasta ympäristöstä. Tilanteen arvioinnissa lähdetään syventämään havaittua tietoa päätöksentekoa varten, jolloin vaikuttavia tekijöitä myös tässä teoriassa ovat kulttuuriset perinteet, geneettinen perimä, uusi tieto, aiemmat kokemukset sekä erilaiset analyysimenetelmät tai synteesit. Päätöksentekovaiheessa hyödynnetään havainnoinnin ja tilanteen arvioinnin avulla saatua tietoa sekä luodaan hypoteeseja. Toimintavaihe toteutetaan edellisten tilojen perusteella ja palataan jälleen tarkkailemaan ympäristöä. (Bhat, Biesdorf, Manjunath, Matthes & Shumaiev 2018, 52-53.)

Kun sovelletaan OODA-silmukkaa kyberturvallisuuteen, voidaan ajatella SIEM-järjestelmän hoitavan kybertoimintaympäristön havainnointia poikkeavien tapahtumien osalta. Tilanteen arvioinnissa voidaan hyödyntää esimerkiksi erilaisia riski-uhka-haavoittuvuus-analyyseja tai esimerkiksi SIEM-järjestelmän valmistajan tuottamia reaaliaikaisia uhkasyötteitä. Myös aiemmin tapahtuneet poikkeamat ja niihin annettujen vasteiden toimivuus tulee huomioida. Kun on pohdittu mahdollisia vaikutuksia omaan kybertoimintaympäristöön, voidaan tehdä näiden ja muiden SIEM-

järjestelmästä saatujen tietojen pohjalta päätöksiä. Toiminnallisessa vaiheessa mahdollinen uhka tai haavoittuvuus lievennetään tai poistetaan, joten tämä vaihe on vaste poikkeamiin, minkä jälkeen voidaan jälleen palata normaalitilaan.

4.1.3 Uudemmat tilannetietoisuuden määritelmät ja vaikutukset

Uudempien määritelmien mukaan kybertoimintaympäristön tilannekuvalla tai tilannetietoisuudella tarkoitetaan Turvallisuuskomitean kyberturvallisuussanaston mukaan organisaation kybertoimintaympäristön tietojärjestelmien käytettävyyden ja turvallisuuden tilannetta tietyllä hetkellä (Kyberturvallisuuden sanasto 2018, 22). Jopa Suomen kyberturvallisuusstrategiassa (2013, 7) painotetaan toisena linjauksena tilannetietoisuuden ja tilanneymmärryksen parantamista. Tilannekuva on siis enemmänkin otanta tietyllä hetkellä vallitsevasta tilasta kyberympäristössä, kun taas tilannetietous on tilannekuvan avulla muodostettu ymmärryksen tila omasta ympäristöstä ja sen resursseista (Kuusisto 2005, 10-11).

Tilannetietoisuudessa huomioidaan ajan tasalla olevat tiedot ja analyysit haavoittuvuuksista tai poikkeamista sekä otetaan huomioon uhkien arvioiminen ja niiden ennustaminen, jotta pahimmilta häiriötilanteilta vältyttäisiin. Suomessa kyberturvallisuuden tilannekuvan ylläpitämisestä ja tilannekuvaan liittyvän tiedon jakamisesta muille organisaatioille vastaa Traficomin (Liikenne- ja viestintävirasto) Kyberturvallisuuskeskus. Traficomilta saatujen tietojen perusteella organisaatio voi toimia oman toimialansa mukaisesti poikkeavassa tilanteessa. (Suomen kyberturvallisuusstrategia 2013, 7.)

Kerrannaisvaikutukset yhteiskunnan kriittisten toimintojen menetysten kautta eri organisaatioihin voivat olla mittavia, koska suurin osa kaikesta tiedosta on nykyään tietoverkoissa. Esimerkiksi sähköyhteyksien katketessa, ei dataa saada siirrettyä, jolloin vaikutukset ulottuvat organisaation tietojen käytettävyyteen, eheyteen ja saatavuuteen. (Suomen kansallinen riskiarvio 2019. 2018, 18.) Yhteiskunnan ja organisaatioiden näkökulmasta puutteellisesti luotu tilannekuva voi pahimmillaan lamaannuttaa kriittisiä osa-alueita, kuten esimerkiksi energiatuotannon, sosiaali- ja terveysalan pal-

veluita, teollisuuden ohjausjärjestelmiä, sekä rahoitusalan maksuliikennettä tai organisaation kriittisiä järjestelmiä. Näistä voi aiheutua liiketoiminnan tai maineen menetyksen lisäksi pahimmillaan vakavia loukkaantumisia, ihmishenkien menetyksiä ja esimerkiksi materiaalista tuhoa eri toimijoille. (Suomen kansallinen riskiarvio 2015. 2016, 20.)

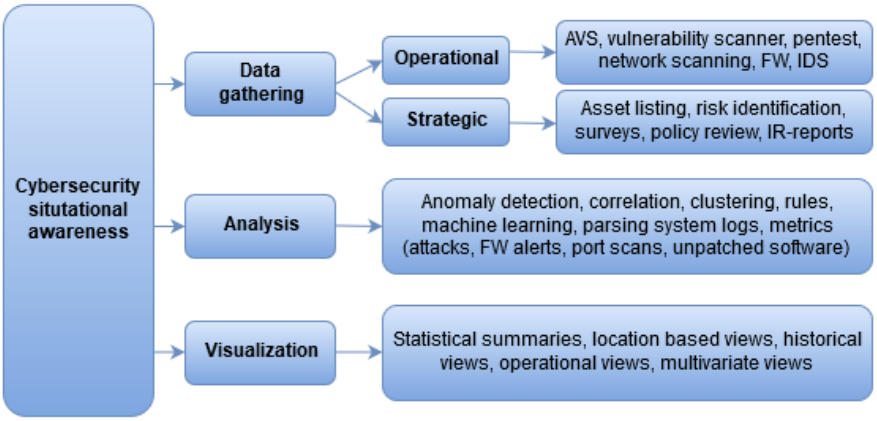
Tilannekuvan muodostamisen ja sitä kautta tilannetietoisuuden kasvattamisen tärkeyttä osana organisaation kyberturvallisuutta ei voi vähätellä, koska sen pohjalta muodostetaan poikkeustilanteessa tehtävät päätökset (Rantanen 2018, 3). Tilannetietoisuuden tärkeyttä korostaa myös sen huomioiminen kansallisissa turvallisuusstrategioissa useassa eri maassa, kuten esimerkiksi Suomessa ja Kanadassa (Suomen kyberturvallisuusstrategia 2013, 7; Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2018). Mikäli tilannekuva koostetaan puutteellisin keinoin, tehdään päätökset toimenpiteistä myös puutteellisesti, jolloin tällä voi olla suoraan negatiivisia vaikutuksia yhteiskuntaan, organisaation toiminnan jatkuvuuteen tai liiketoiminnan menetykseen.

4.2 Tilannekuvan muodostaminen

4.2.1 Tilannetietoisuuden luokittelu

Kuviossa 6 Evesti, Frantti ja Kanstrén (2017) ovat luokitelleet tutkimuksessaan *Cybersecurity Situational Awarness taxonomy* kyberturvallisuuden tilannetietoisuuden kolmeen eri tasoon, joita ovat datan kerääminen, analysointi, sekä visualisointi. Tutkimuksessa jaoteltiin tilannetietoisuus organisaatioille ja kansalliselle tasolle, mutta tässä opinnäytetyössä keskitytään organisaation näkökulmaan (ks. kuvio 6). Datan kerääminen on jaoteltu operatiiviseen ja strategiseen toimintaan. Operatiiviseen toimintaan sisältyvät tietolähteet, kuten haavoittuvuusskannausten tiedot, IDS/IPS, tietoturvatestaus ja niin edelleen, mitkä voidaan nähdä myös SIEM-järjestelmiin tai muihin turvallisuusjärjestelmiin sisältyvinä toiminnallisuuksina. Strategiselle puolelle taas sisältyvät esimerkiksi riskienhallintasuunnitelmat, tietoturvapoikkeamista koostuvat raportit ja tietoturvapolitiikkojen katselmoinnit, jotka ovat erittäin tärkeitä osa-alueita, kun halutaan kasvattaa ja ylläpitää organisaation kyber- tai tietoturvallisuutta.

Nämä ovat pitkäkestoisia ja ylläpidettäviä prosesseja, jotka tehdään manuaalisesti ihmisten toimesta. (Evesti, Frantti & Kanstrén 2017, 3.)



Kuvio 6. Tilannetietoisuuden luokittelumalli (Evesti, Frantti ja Kanstrén 2017, 5, muokattu)

Tarkasteltaessa analyysi- ja visualisointiluokkia, voidaan havaita SIEMin pitkälti sisältävän myös näistä useimmat ominaisuudet, kuten poikkeamien havainnoinnin, tietojen korreloinnin, lokitietojen parsinnan, säännöstöjen luomisen sekä näiden tietojen pohjalta muodostettujen visuaalisten näkymien luomisen ihmiselle ymmärrettävään muotoon. SIEM-järjestelmissä korostuvat tekninen, operatiivinen ja visuaalinen toiminta, kun taas tietoturva-asiantuntijoille jää käsiteltäväksi enemmänkin strateginen ja analyyttinen puoli, kun päätöksiä tehdään operatiivisesti kerättyjen tietojen pohjalta.

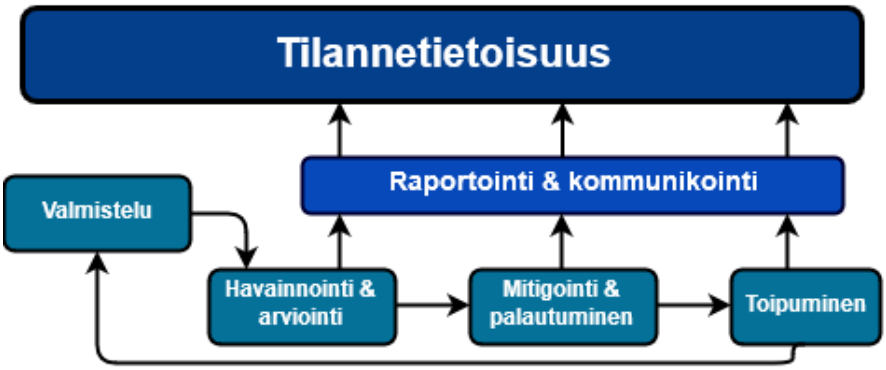
Operatiivisen puolen onkin tarkoitus helpottaa nopeiden päätösten teossa ja tietoa yleisesti ottaen hyödynnetään päivittäisessä toiminnassa. Operatiivisen tiedon perusteella voidaan myös tuoda strategiselle puolelle lisäarvoa, jolloin pidempiaikaisten suunnitelmien tekemiseen saadaan lisätietoja. (Evesti, Frantti & Kanstrén 2017, 3.) Operatiivisen tiedon hyödyntämisessä strategisessa päätöksenteossa voidaan antaa

havainnollistava esimerkki tilanteesta, missä haavoittuvuusskannauksen yhteydessä löydetään vakava haavoittuvuus, josta tehdään riskienhallintasuunnitelma. Riskienhallintasuunnitelman avulla päätetään jatkotoimenpiteet, eli haavoittuvuus joko lievennetään, poistetaan tai hyväksytään. Tällöin haavoittuvuudesta aiheutuva riski on tiedossa ja näin ollen sen käsittely on hallittua, eikä hyökkääjä todennäköisesti pääse hyödyntämään haavoittuvuutta samalla tavalla kuin ennen riskienhallintasuunnitelman tekoa.

Tilannetietoisuuden ollessa erittäin laaja ja moninainen kokonaisuus, saadaan luokittelulla jäsenneltyä mitä kaikkea tilannetietoisuuteen liittyy, sekä mitä turvallisuuden operatiivisia ja strategisia toiminnallisuuksia tulee ottaa huomioon pohdittaessa tilannetietoisuuden kasvattamista organisaatiossa. Tämä tutkimus helpottaa myös opinnäytetyössä tehtävää vertailua tilannetietoisuuden kasvattamisesta SIEM-järjestelmän avulla, koska sen avulla havainnollistetaan kuinka kytköksissä nämä kaksi osa-aluetta ovatkaan toisiinsa nähden.

4.2.2 Toimintaprosessit

Kuviossa 7 on esiteltynä Kanadan valtionhallinnon muodostama kuvaus tietoturvatapahtumien käsittelystä ja sen sisältämästä toimintaprosessista. Tämän perustella voidaan todeta, että tilannetietoisuuden kulmakivet ovat raportoinnissa sekä tiedon jakamisessa ja kommunikoinnissa. Kun kybertoimintaympäristön resursseja monitoroidaan monipuolisesti, saadaan helpommin havainnoitua poikkeamia sekä reagoitua niihin nopeammin ja tehokkaammin. Tämä edesauttaa palautumista normaalitilaan poikkeaman tapahduttua.



Kuvio 7. Malli tilannekuvasta ja tietoturvatapahtumien hallinnasta (Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2018, muokattu)

Yksi tärkeä osa tilannetietoisuuden ylläpitoa on ennakointi ja valmistautuminen. Tapahtumia ennakoidessa voidaan hyödyntää erilaisia uhka-analyysejä sekä esimerkiksi aiemmin tapahtuneiden poikkeamien analysointia, jolloin kasvatetaan ymmärrystä omasta ympäristöstä ja osataan varautua mahdollisesti toistuviin samankaltaisiin tai jopa yllättäviin poikkeamiin. (Kuusisto 2014, 67.) Kun mahdollisille uhka-arvioille luodaan haavoittuvuus- ja riskianalyysit, voidaan niiden avulla pienentää mahdollisten häiriöiden todennäköisyyttä. Nämä edesauttavat riskien hallittua käsittelyä ja kasvattavat siten mahdollisuuksia varautua uhkatilanteisiin, kun mahdollisia skenaarioita ja niihin kohdistettavia toimenpiteitä on jo käsitelty organisaatiossa. (Yhteiskunnan turvallisuusstrategia 2017, 25.)

Tilannetietoisuutta käsiteltäessä voidaan todeta, että kyseessä on prosessi muuttuvassa kybertoimintaympäristössä, jota tulee kehittää jatkuvasti. Vaikka kuviossa 7 on Kanadan valtionhallinnon muodostama kuva, voidaan sitä soveltaa myös muiden organisaatioiden osalta tilannetietoisuuteen liittyviin käytäntöihin toimintaprosessin ollessa yleisellä tasolla. Kuten myös tästä mallista voidaan huomata, on siinä samankaltaisuuksia esimerkiksi aiemmin käsiteltyjen Endsleyn teorian sekä OODA-silmukan kanssa, joissa painotettiin samankaltaisia osa-alueita tilannetietoisuuden kasvattamiseksi ja toimintamallia kuinka tietojen pohjalta tehdään päätökset. Samansuuntaisia ratkaisuja oli aiemmin mainitussa CISAn oppaassa (Situational Awareness 2016) sekä monissa muissa eri tietolähteissä.

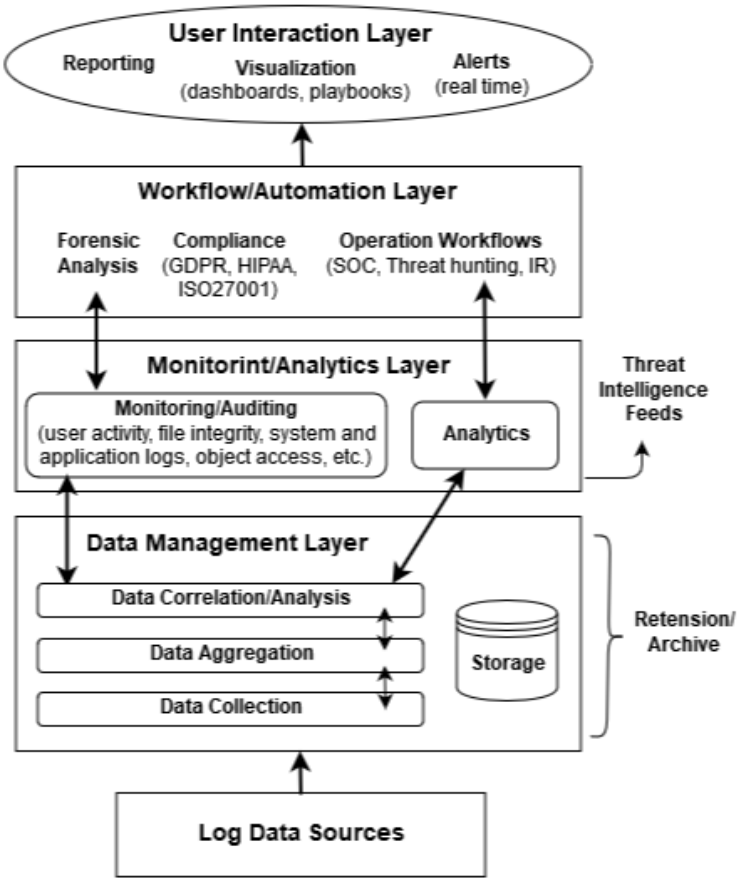
Tilannetietoisuutta voidaan ja sitä tuleekin kehittää yli organisaatioiden rajojen, jotta kokonaisvaltainen näkyvyys kansainvälisestä ja kansallisesta tilannekuvasta saadaan muodostettua. Nykyään Internetin käytön ja muun digitalisoitumisen yleistyessä organisaation palveluissa ei voida asettaa uhkille maantieteellisiä rajoja. EU:n kyberturvallisuusstrategiassa (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace 2013, 18) on korostettu tiedon jakamista sekä kansallisten tahojen välillä että yksityisellä puolella, jotta uhkiin ja esimerkiksi jatkuvasti muuttuviin hyökkäystekniikoihin voidaan varautua. Myös Suomen Yhteiskunnan turvallisuusstrategiassa (2017, 15) sekä Suomen Kyberturvallisuusstrategiassa (2019, 7) painotetaan hyvän johtamisen ja häiriötilanteiden hallinnan yhteydessä muun muassa tilannekuvan muodostamista ja arvioimista, kriisiviestintää, tiedonjakamista ja näiden pohjalta tehtäviä teknisiä päätöksiä, tietoturvauhkiin varautumista sekä jatkuvuudenhallintaa ja yhteistoimintaa.

5 SIEM-arkkitehtuuri

SIEMin tarkemman toimintavan tunteminen on välttämätöntä, kun suunnitellaan tietynlaiselle organisaatiolle sopivaa SIEM-ratkaisua. Kuviossa 8 nähdään esimerkki uudemman sukupolven SIEM-arkkitehtuurista. SIEMin toiminnallisuudet on jaoteltu neljään eri kerrokseen, joilla kaikilla on omat toiminnallisuutensa prosessissa. Kerrokset ovat: datanhallintakerros, monitorointi/analysointikerros, työnkulku/automatisointikerros ja käyttöliittymäkerros.

Käytännössä dataa kerätään ensiksi olennaisista lähteistä, joita voivat olla esimerkiksi verkkolaitteet, viruksentorjuntaohjelmisto, sovelluslokit ja muut vastaavat resurssit organisaation kybertoimintaympäristöstä. Toisin sanoen, kaikki liikenne tai tapahtumat mitä organisaatiossa halutaan valvoa. Erilaiset keräimet tai lokiagentit keräävät datan ja välittävät tiedot SIEMin keskitettyyn tietokantaan tai tietoaltaaseen. Joko lokiagentit tai itse SIEM-järjestelmä normalisoivat ja yhdistelevät lokiagenttien välittämän datan, jotta sitä voidaan prosessoida ja hyödyntää. Data analysoidaan yleensä korrelointisäännöstöjä hyödyntäen, jotta poikkeamia havaitessa generoidaan hälytys SIEM-järjestelmässä jatkotutkimuksia varten. SIEM-järjestelmä myös visualisoi ja

muodostaa raportteja, jolloin voidaan aloittaa reagointi poikkeamiin tai kuitata hälytys aiheettomaksi. (Petters 2019.) Seuraavissa alakappaleissa käydään nämä SIEMiin liittyvät toiminnallisuuksien eri kerrokset tarkemmin läpi.

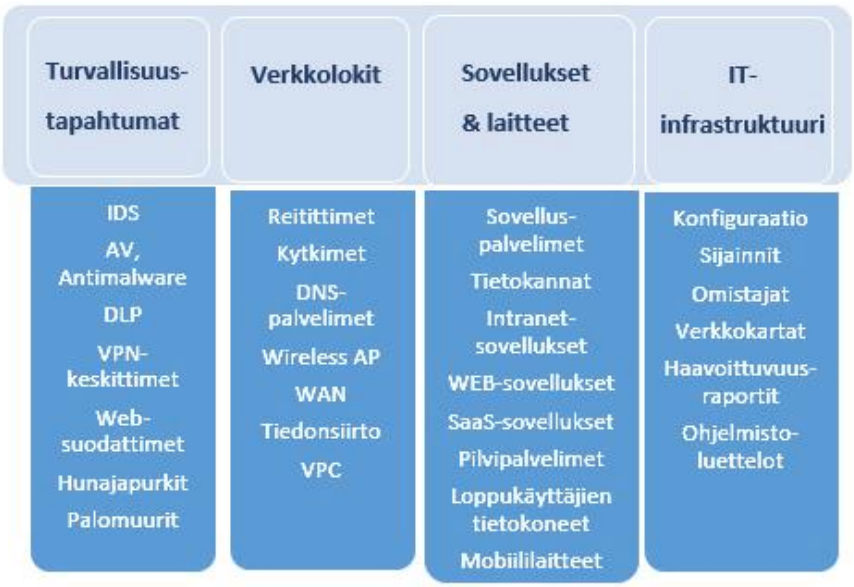


Kuvio 8. Uudemman sukupolven SIEM-arkkitehtuuri (Filkins 2019, 3, muokattu)

5.1 Datan kerääminen ja siirtäminen

SIEMin toiminnan perustuessa datan käsittelyyn ja analysoimiseen, organisaation tuleekin päättää mistä kaikkialta dataa kerätään. Mitä enemmän dataa kerätään tarpeellisista lähteistä, sitä parempi ja realistisempi näkyvyys organisaation tilannekuvasta saadaan muodostettua. Toisaalta, kuten aiemmin sääntöjä luodessa todettiin jo

luvussa 2.1, mikäli lokitietoja haetaan niin sanotusti tarpeettomista lähteistä, ei siitä pidemmällä tähtäimellä ole muuta kuin haittaa, koska työntekijäresurssit menevät esimerkiksi väärien positiivisten aiheuttamien hälytysten läpikäymiseen. Kuviossa 9 voidaan nähdä esimerkkejä mahdollisista lokiin tallentuvista tietolähteistä. (SIEM-guide 2019, luku 3.) Olennaista on siis miettiä tärkeät ja tarpeelliset kohteet ja lähteä käyttöönottovaiheessa pikkuhiljaa lisäämään lokilähteitä priorisoimalla tärkeimmät ensin (Näin keräät ja käytät lokitietoja 2019).



Kuvio 9. Esimerkkejä lokilähteistä (SIEM-guide 2019, luku 1, muokattu)

5.1.1 Tiedonsiirtomenetelmät

Kybertoimintaympäristön lokilähteiden ja muiden tapahtumien tiedonsiirtoon voidaan käyttää lukuisia eri protokollia ja tekniikoita erilaisten keräimien tai agenttien lisäksi. Syslog-protokollaa hyödynnetään datan yhdistelyssä, koska data on standardiformaatissa ja näin ollen käsittely helpottuu. Lisäksi tapahtumavirtaprotokollat, ku-

ten SNMP, Netflow tai IPFIX voivat toimia datan siirtämisessä. Kun lokitietoja halutaan välittää turvallisesti eteenpäin, voidaan käyttää tähän tarkoitukseen esimerkiksi TCP-protokollaa tai TLS/SSL-salausta. (SIEM-guide 2019, luku 2.) Alla on käyty läpi näistä yleisimmät protokollat tiivistetysti.

TCP/IP (Transmission Control Protocol / Internet Protocol)

TCP/IP-protokollapari on yksi yleisimmin käytössä olevista yhteiskäytännöistä ja sitä hyödynnetään esimerkiksi Internetin yli liikennöidessä. Esimerkiksi FTP, SMTP ja HTTP hyödyntävät TCP:tä. TCP/IP:n arkkitehtuuri koostuu neljästä eri kerroksesta: liittymiskerros, Internet-kerros, kuljetuskerros ja sovelluskerros, joille myös em. ja lukuisat muut protokollat sijoittuvat. TCP/IP on tilallinen protokolla, minkä suosio osittain perustuukin esimerkiksi datan eheyden- ja virheentarkistukseen. (Casad & Willsey 1999, 17-25.)

UDP (User Datagram Protocol)

UDP puolestaan on tilaton protokolla ja toisin kuin TCP/IP, se ei tee esimerkiksi pakettien uudelleenlähetystä tai virheentarkistusta. UDP:tä hyödynnetäänkin ensisijaisesti, kun vältetään suurempaa kuormitusta, eikä ole tarpeen tarkistaa paketin saapumista perille. UDP:n päätehtävänä on välittää datagrammeja sovelluskerrokselle. (Casad & Willsey 1999, 106-107.)

Syslog

Syslog-formaatissa dataa voidaan hakea vain suoraan datavarastosta, esimerkiksi käyttöjärjestelmän tiedoista datan ollessa valmiiksi standardimuodossa. Syslog-formaattia käyttävät useat verkkolaitteet, esimerkiksi palomuurit, reitittimet ja tulostimet. (SIEM-guide 2019, luku 2.) Syslog hyödyntää siirtämiseen UDP- ja TCP/IP-protokollia ja on yleisimmin käytössä UNIX-pohjaisissa käyttöjärjestelmissä (Chuvakin, Phillips & Schmidt 2013, luku 1).

SNMP (Simple Network Management Protocol)

SNMP on standardipohjainen protokolla, jota käytetään yleisesti verkkolaitteiden hallinnoimisessa suorittaen laitteille kyselyitä ja generoiden saatujen tietojen pohjalta esimerkiksi hälytyksiä. Protokollaa voidaan hyödyntää esimerkiksi tilanteissa, joissa vanhempien laitteiden ei ole mahdollista hyödyntää Syslog-protokollaa. SNMP hyödyntää UDP-protokollaa tiedonsiirrossa. (Chuvakin, Phillips & Schmidt 2013, luku 3.)

Windows Event Log

Windowsin tapahtumalokit pitävät sisällään erilaiset sovelluslokit, käyttöjärjestelmän omat lokit sekä turvallisuustapahtumien lokitiedot. Turvallisuuslokiin tallentuvat tiedot esimerkiksi onnistuneista ja epäonnistuneista sisäänkirjautumisista sekä pääsystä eri resursseihin, kuten esimerkiksi tiedostoihin tai muihin jaettuihin tietoihin. (Chuvakin, Phillips & Schmidt 2013, luku 3.)

SSH (Secure Shell)

SSH on kahden osapuolen kommunikointiin tarkoitettu ohjelmisto. Usein ohjelmaa käytetään esimerkiksi suorittamaan komentoja salatun etäyhteyden välityksellä asiakaskoneen ja palvelimen (tietokone, verkkolaite ym.) välillä. Yhteyden avulla voidaan hyödyntää muun muassa tiedostojen siirtoa turvallisella SFTP (Secure File Transfer Protocol)- protokollalla. SSH:n avulla kaikki kommunikointi salataan ja siinä käytetään kaksivaiheista todennusta. Siirretyn datan eheys voidaan tarkistaa digitaalisella allekirjoituksella. (Dwivedi 2004.)

SSL (Secure Sockets Layer) / TLS (Transport Layer Security)

SSL-protokolla perustuu kahden koneen tai laitteen väliseen turvattuun yhteyteen. SSL sisältää salausmenetelmät, jotka suojaavat siirrettävää dataa, todennuksen ja datan eheyden varmistamisen. TLS on käytännössä päivitetty ja turvallisempi versio vanhemmasta SSL-protokollasta. HTTPS-yhteyttä käytettäessä hyödynnetään juuri jompaakumpaa protokollaa SSL-sertifikaatilla. (What is SSL, TSL and HTTPS? 2019.)

API (Application Programming Interface)

API on ohjelmointirajapinta sovellusten ja järjestelmien välillä, joka usein sisältää pääsyn erilaisiin toiminnallisuuksiin tai prosesseihin. SIEMissä API-rajapintoja voidaan hyödyntää tiedonvälittämiseen automatisoidusti suoraan esimerkiksi sovelluksen ja SIEM-järjestelmän välillä. Kuka tahansa voi luoda haluamansa APIn sovellukseen, jolloin esimerkiksi organisaatio voi joustavasti toteuttaa juuri sellaisen kuin on tarpeen ja tämä mahdollistaa siten erilaisten resurssien integroimista SIEMin. APIen avulla voidaan kasvattaa turvallisuutta, kun voidaan itse määritellä mitä tietoa siirretään, kenellä on pääsy tietoon ja minkälaisia toimenpiteitä suoritetaan tämä jälkeen. (Iversen 2018.)

5.1.2 Lokiagentit

Lokiagentti tai keräin on ohjelmisto, joka kerää yhdestä lähteestä lokitietoja välittäen ne toiseen kohteeseen, kuten tässä yhteydessä SIEM-järjestelmään. Lokiagentteja on ns. agentillinen (engl. agent) ja agentiton (engl. agentless). Agentiton lokiagentti on yleensä valmiiksi asennettu alustalle, josta lokitietoa kerätään ja se käyttää tiedonsiirtoon usein SNMP-, WMI- tai Syslog-protokollia. (Koecher 2017.) WMI on Microsoftin kehittämä työkalu datan hallinnointiin ja operointiin Windows-pohjaisissa ympäristöissä, jolla dataa voidaan hallita etäyhteyksien avulla (About WMI 2018). Agentillisen keräimen avulla saadaan kerättyä ja muutoin käsiteltyä huomattavasti enemmän dataa halutusta lähteestä, koska agentit ovat usein alustojen valmistajien tarkoin tekemiä ja lokeja voidaan siirtää tehokkaasti API-rajapintojen avulla. (Koecher 2017.)

Yleisimmät lokiformaatit, kuten Syslog, ovat yleensä tuettuja. Uudemman sukupolvien SIEM-ratkaisuissa ei hyödynnetä aina lokiagentteja datan keräämiseen, vaan lokitiedot voidaan myös viedä suoraan SIEMiin. (SIEM-guide 2019, luku 2.) Lokiagenttien käyttö on kuitenkin turvallisempaa kuin datan lähettäminen esimerkiksi etäyhteydellä, jolloin hyökkääjällä on mahdollisuus hyväksikäyttää etäyhteyttä. Agenttien käytön etuna on se, että ne voivat myös säilöä tietoa välimuistiin, joten mikäli keskitetty datavarasto tai palvelin ei ole saatavilla, voidaan välimuistista lähettää dataa eteenpäin, kun yhteydenmuodostaminen on jälleen mahdollista. (Koecher 2017.)

5.2 Datan normalisointi

Datan normalisoinnilla tarkoitetaan dataformaatin muokkaamista yhteen haluttuun muotoon. Kun organisaation SIEM-järjestelmä hyödyntää erityisen suuria määriä tietolähteitä, on data useimmiten eri muodossa datankerääjän tai agentin saadessa tiedon. Tämän vuoksi data täytyy normalisoida, jotta sitä voidaan käyttää SIEMissä. Suodattamiseen ja normalisointiin määritellään tietyt tiedot (esimerkiksi aika, IP-osoite, tapahtuman tiedot ym.) joita halutaan tarkistella ja muut suodatetaan pois, eikä niitä lähetetä edelleen SIEMiin. (Canner 2019a.) Luvussa 5.1.2 mainitut lokiagentit voivat osaltaan tehdä valmiiksi datan normalisointia ennen tietojen edelleen lähetystä SIEMiin (Chuvakin, Phillips & Schmidt 2013, luku 1).

Käytännössä normalisoinnissa datasta erotellaan halutut asiat omiin ryhmiinsä, kuten voidaan havaita seuraavasta yksinkertaistetusta esimerkistä:

<;;5>devid=XSKDJDJ1891 devname=exampledevice date=2019-09-09 time=14:43:58 srcip=10.10.10.200 srcport=44000 dstip=172.217.15.206 dstport=443

Tästä lokimerkinnästä voidaan saada seuraavaa tietoa normalisoinnin avulla(Monge 2019):

- Laitteen ID
- Laitteen nimi
- Päivämäärä
- Kellonaika
- Lähdeosoite
- Lähdeportti
- Kohdeosoite
- Kohdeportti.

Lokitietojen käsittelyssä voidaan normalisoinnin lisäksi hyödyntää datan parsimista, kategorisointia, rikastamista, indeksoimista sekä varastoimista keskitettyyn tietokantaan (SIEM-guide 2019, luku 3). Indeksoimisen tai parsimisen avulla voidaan nopeuttaa merkittävästi hakujen tekemistä lokimassasta (Chuvakin 2016, 3).

5.3 Datan säilyttäminen

Vanhemmissa SIEM-ratkaisuissa useimmiten data on varastoitu perinteisiin tietovarastoihin, mutta uudemman sukupolven alustoissa hyödynnetään suurienkin datamassojen käsittelyyn tarkoitettuja tietoaltaita. Tietoaltaisiin voidaan säilöä erittäin suuria määriä raakadataa, eikä ole väliä onko se rakenteellista, ei-rakenteellista vai osittain rakenteellista. Tämä tekee tietoaltaista skaalautuvia ja verrattuna perinteisiin tietovarastoihin, data voidaan käsitellä raakamuodossa kasvattaen myös käsittelyn tehokkuutta. Perinteisissä datavarastoissa tietoa joudutaan käsittelemään ennen sen siirtoa varastoon ja sen sisältämä data on rakenteellista sekä mallinnettua, jolloin käsittely on hitaampaa. (Saurabh & Venkata 2018, luku 1.)

Tietoaltaat voidaan jakaa karkeasti kahteen eri kerrokseen: datan säilömiseen ja analysoimiseen. Säilömiskerroksella raakadataa säilötään ja tarvittaessa muunnetaan, jotta se voidaan analysoida. Lisäksi historiallinen data voidaan arkistoida ja säilöä tietoaltaaseen. Aktiivisessa käytössä oleva data voidaan säilöä toissijaiseen varastoon, jossa voidaan määritellä tietyt aikarajat, jolloin data siirretään historialliseen varastoon säilöön. Säilömiskerros toimii pohjana dynaamiselle analytiikkakerrokselle, missä erilaiset analytiikka- ja profilointimallit alkavat tuottaa erilaista metriikkaa ja visualisoida sitä. (Saurabh & Venkata 2018, luku 1.) Datan ryhmittelystä ja analysoinnista puhutaan seuraavissa luvuissa tarkemmin.

Dataa kerätään normaalin viitekehyksen mukaisesti datankerääjien (engl. collector) ja datan yhdistäjien (engl. integrator) avulla. (Saurabh & Venkata 2018, luku 2.) Näiden toiminta on vastaavaa kuin aiemmin mainittujen lokiagenttien. Kerätessä kriittistä dataa yhteen paikkaan, tulee tietysti huomioida tietojen suojaaminen. Tärkeitä suojausmenetelminä ovat esimerkiksi pääsynrajoittaminen käyttöoikeuksien hallinnan avulla, autentikointi hyödyntäen epäsymmetrisiä avaimia, digitaalisia allekirjoituksia ja tiivistefunktiota sekä IPsec- ja TLS-protokollia liikuteltaessa dataa. Lisäksi verkkopohjainen valvonta kasvattaa turvallisuutta, kuten palomuurit ja IDS/IPS-ratkaisut, klusterointi sekä solmupohjainen ryhmittely tietoaltaassa. Tietysti myös tietoallasta tulee valvoa sekä havainnoida siihen kohdistuvia poikkeamia, haavoittuvuuksia ja uhkia. (Saurabh & Venkata 2018, luku 6.)

5.4 Datan ryhmittely

Datan ryhmittelyvaiheessa raakadata kerätään yhteen, jotta se voidaan analysoida. Keräämisen ja normalisoinnin jälkeen tiedot leimataan (engl. tag) ja ryhmitellään riippuen tiedon tyypistä. (Chapman & Maymi 2018.) Näin saadaan tietoa esimerkiksi samankaltaisten tapahtumien lukumäärästä tai muuta haluttua statistiikkaa. Tietoa voidaan ryhmitellä tapahtuman ominaisuuksien perusteella, kuten esimerkiksi kuinka paljon tiettyä liikennettä tapahtuu tietyllä IP-osoitteella.

5.5 Datan analysointi ja poikkeamiin reagointi

Datan analysointivaihe on yksi tärkeimmistä, koska siinä tapahtuu mahdollisten poikkeamien havainnointi. Vanhemman sukupolvien SIEM-ratkaisussa datan analysointiin on käytetty lähinnä muutamaa eri tekniikkaa, jotka ovat korrelointisäännöt sekä haavoittuvuuksien ja riskien arviointi. Uudemman sukupolven SIEM-ratkaisuissa erilaisten säännöstöjen lisäksi korrelointiin voidaan hyödyntää myös koneoppimista erottamaan normaalit tapahtumat poikkeavista. UEBAn hyödyntämän koneoppimisen avulla voidaan havainnoida esimerkiksi epänormaali käyttäytyminen käyttäjien tai vaikkapa sovellusten toiminnassa. (Advanced Correlation Engine 2019.)

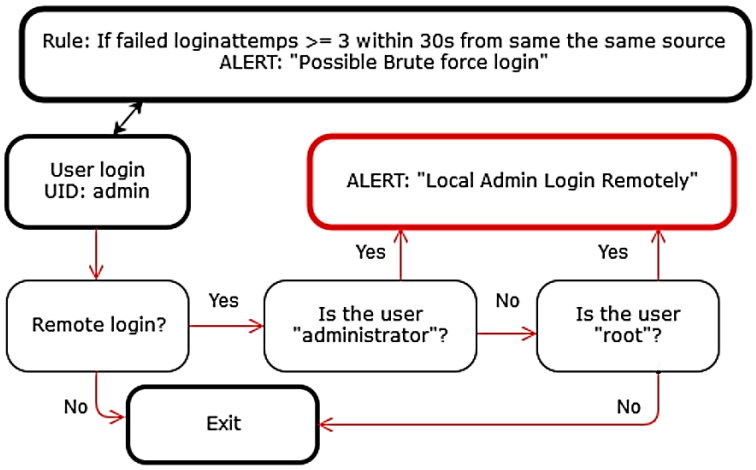
Dataa voidaan analysoida koneoppimisen lisäksi ns. ohjatun (engl. supervised learning) tai ohjaamattoman oppimisen kautta. Nämä hyödyntävät toiminnassaan muun muassa lineaarista regressiota, erilaisia luokittelutekniikoita, sekä klusterointia. Simulaatioiden avulla voidaan mallintaa tosielämään liittyviä tai hypoteettisia tapahtumia, jolloin voidaan tehdä optimointia sekä erilaisten entä jos -skenaarioiden testaamista. Tekstinlouhinnassa voidaan hyödyntää statistiikkaa, koneoppimista ja kielitiedettä, minkä tarkoituksena on löytää kaavoja tai tiettyjä trendejä rakenteettomasta datasta ja siten löytää arvokkaampaa tietoa tiettyyn skenaarioon datamassojen seasta. (Martin, McPherson, Miyamoto & Talabis 2015, luku 1.)

5.5.1 Datan korrelointi

Datan korrelointia voidaan suorittaa esimerkiksi sääntöpohjaisesti, staattisesti tai tekoälyn avulla, joilla saadaan yhdistettyä pisteet eri loki- tai tapahtumatietojen väliltä ja tämän perusteella generoida tai olla generoimatta hälytyksiä riippuen määritellyistä säännöstöistä tai niihin yhdistetyistä alisäännöistä. Nykyisissä SIEM-järjestelmissä tämä on jo varsin automatisoitua ja erilaisia uhkamalleja on luotu valmiiksi, jolloin haitalliset ja poikkeavat tapahtumat voidaan havaita helpommin. (Automated Correlation Engine 2019; Chuvakin 2016, 3; Dietz 2018.) Korreloinnin ongelmaksi voivat muodostua esimerkiksi tiuhaan muuttuvat IP-osoitteet tai muut tunnistetiedot, jolloin tapahtumia on vaikea liittää toisiinsa ja siten korrelointi ei toimi aina kuten pitäisi (Dietz 2018). Korrelointi voidaan toteuttaa joko reaaliajassa tai jälkikäteen hakemalla tietoja tietokannasta (Chuvakin 2016, 3).

Säännöstöjä luomalla on tarkoitus hälytysten tuottamisen lisäksi automatisoida tapahtumien analysointia SIEM-järjestelmässä ja siten helpottaa organisaation työntekijöiden tehtäviä. Esimerkiksi silloin kun yksittäisiä tapahtumia on miljoonia, näiden seasta poikkeamien havainnointi on lähes mahdotonta yksittäisten henkilöiden toimesta. Säännöstöjen luominen voi olla joko yksinkertaista tai yksinkertaisista osista muodostuvia monimutkaisia kokonaisuuksia, jotka perustuvat tapahtumista aiheutuviin vaikutuksiin. (Blask, Harper, Harris, Miller & VanDyke 2011.)

Otetaan käytännön esimerkiksi korreloinnista järjestelmävalvojan oikeuksilla tapahtuva kirjautuminen palvelimelle. Inhimillisten virheiden vuoksi salasana voidaan kirjoittaa useamman kerran väärin, mutta jos muutaman sekunnin aikana kirjautumisyrityksiä on kymmeniä, voidaan jo epäillä tämän olevan esimerkiksi väsytyshyökkäys (engl. brute force). Kuviossa 10 on esitettynä yksinkertaisen kaavion avulla, kuinka säännöstö voisi toimia tällaisessa tilanteessa tarkistaen järjestelmävalvojan tunnusten kirjautumisyritysten oikeellisuutta joko generoiden hälytyksen tai lopettamalla tarkistuksen, mikäli tapahtuma ei koske määriteltyä säännöstöä. (Mt.)



Kuvio 10. Kaavio hälytyksen generoimisesta säännön perusteella (Blask, Harper, Harris, Miller & VanDyke 2011, muokattu)

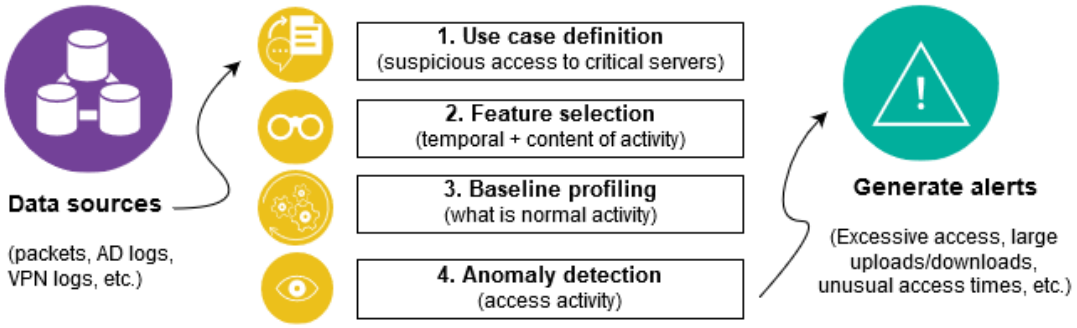
Korrelaatiomoottorin avulla voidaan hienosäätää säännöstöjen toimivuutta. Tätä voidaan havainnollistaa edellä mainitun esimerkin avulla siten, että hälytykset generoidaan vasta kun tietty määrä epäonnistuneita sisäänkirjautumisyrityskertoja on havaittu palvelimelle. Normaalitilanteessa olisi tietenkin myös suositeltavaa lukita tunnukset tietyn yritysmäärän jälkeen. Esimerkkikuviossa (ks. kuvio 10) hälytyksen laukaisemiseen riittää kolme tai enemmän yrityksiä. Tätäkin voisi hienosäätää vielä esimerkiksi lisäämällä sääntöön, että mikäli välissä ei ole ollut onnistuneita kirjautumisia, kyseessä voi olla mahdollinen väsytyshyökkäys, minkä oikeellisuuden tietoturva-asiantuntija tarkistaa. (Blask, Harper, Harris, Miller & VanDyke 2011.)

5.5.2 UEBA (User and Entity Behavior Analytics)

UEBAa voidaan hyödyntää SIEM-ratkaisussa, koska sen avulla voidaan havaita poikkeamia käyttäjien, sovellusten, verkkoliikenteen, verkkolaitteiden ja muiden tietolähteiden toiminnassa (Waitt 2019). Kuten kuviosta 11 nähdään, UEBAn toiminta perustuu kyberympäristön normaalin toiminnan tuntemiseen, jotta poikkeavat tapahtumat havaitaan. UEBA hyödyntää toiminnassaan koneoppimista, erilaisia algoritmeja ja staattisia analyysejä. (Brook 2018.) Näiden toiminnallisuuksien ansiosta jokaista asiaa ei tarvitse erikseen ohjelmoida tai opettaa. Näin erilaisten tapahtumien ja poikkeamien ennustaminen sekä tunnistaminen ovat mahdollisia valmiiksi määriteltyjen

tapahtumakaavojen ja käyttötapausten avulla. Tämän ansiosta käsittely automatisoituu ja manuaalinen työskentely vähenee. UEBAn etuna voidaan nähdä myös DLP (Data Loss Prevention), minkä avulla organisaation sensitiivinen data ei vuoda ulospäin. Jos näin tapahtuu, generoidaan hälytys jatkotutkimuksia varten. (SIEM-guide 2019, luku 4.)

Ensiksi UEBAssa kerätään dataa olennaisista tietolähteistä, kuten käyttäjien sisäänkirjautumisista tai tietoliikennepaketeista, minkä jälkeen (1. Use Case Definition) data suodatetaan, ryhmitellään ja valmistellaan seuraavaan vaiheeseen. Tämän jälkeen (2. Feature Selection) valitaan kerätystä ja suodatetusta datasta ominaisuuksien mukaan tärkeimmät, minkä jälkeen ne varastoidaan. Kolmannessa vaiheessa (3. Baseline Profiling) ominaisuudet ryhmitellään konfiguroiduiksi pohjaksi, minkä jälkeen koneoppimisen avulla, SVD:tä (Singular Values Decomposition) hyödyntäen, generoidaan käyttäytymisprofiileja tietolähteille, kuten käyttäjälle tai laitteelle. Neljäntenä vaiheena (4. Anomaly Detection) UEBA vertaa testiarvoihin luotua käyttäytymisprofiilia, minkä jälkeen pisteytetty tapahtuma luodaan. Mikäli tapahtuma ei täsmää luotuun profiiliin, UEBA tuottaa hälytyksen, jotta poikkeama voidaan tutkia ja analysoida tarkemmin. (Shashanka, Shen & Wang 2016, 6-7; Wang 2017.)



Kuvio 11. UABAn toimintamalli (Wang 2017, muokattu)

UEBA eroaakin itsessään muista turvallisuuden valvontajärjestelmistä, koska se ei keskity turvalokien tai tapahtumien analysointiin, vaan nimenomaisesti käyttäjien ja laitteiden toiminnan valvomiseen. UEBAn tärkeimpiä ominaisuuksia ovatkin uhkien havainnointi organisaation sisältäpäin, kuten haitallisen käyttäjän tunnistaminen, hyökkäyksien havainnointi, käyttöoikeuksiin tehdyt muutokset sekä pääsyn estäminen suojattuun dataan. (Brook 2018.)

5.5.3 SOAR (Security Orchestration, Automation and Response)

Yksi uudemman sukupolven SIEM-ratkaisujen ominaisuuksista on SOAR. SOARin päätoiminnallisuutena voidaan katsoa olevan uhkien havainnointi, analysointi sekä tietoturvapoikkeamiin reagoiminen. Orkestroinnin avulla voidaan koordinoida päätöksentekoa automatisoidusti tietoturvapoikkeamiin reagoinnissa. SOAR hyödyntää tähän erilaisia riskienhallintakeinoja ja ympäristön tilaan liittyviä analyysejä, lisäksi tietoturva-asiantuntijat voivat valita käyttöliittymän kautta minkälaisia toimenpiteitä tehdään. SOARin avulla poikkeamiin reagoiminen nopeutuu automatisoinnin vuoksi. Esimerkiksi LogRhythmin SOAR-tuotteessa voidaan automaattisesti asettaa päätelaitteita tai käyttäjiä karanteeniin, kerätä konedataa, katkaista verkkoyhteyksiä ja lopettaa prosesseja, mikäli havaitaan epäilyttävää käyttäytymistä. Ymmärrettävästi tämä voi vähentää huomattavasti manuaalista työtä. (Security Orchestration, Automation and Response 2019.)

5.5.4 Älykkäät uhkasyötteet

Uudemman sukupolven SIEM-järjestelmien yhtenä kulmakivenä on niin sanotut älykkäät uhkasyötteet (engl. threat intelligence feeds). Uhkasyötteet ovat usein SIEM-järjestelmien valmistajien omien tutkimusryhmien tuloksia tai erillisiä kolmansien osapuolien syötteitä kattavimman lopputuloksen aikaansaamiseksi. Yleensä uhkasyötteet päivittyvät automaattisesti ja niiden sisältämää tietoa verrataan SIEM-järjestelmän avulla omaan kybertoimintaympäristöön. Useimmiten uhkasyötteet sisältävät tietoa esimerkiksi epäilyttävistä domain-nimistä, haittaohjelmien tiivisteistä, haitallisista IP-osoitteista sekä esimerkiksi julkisesti jaetusta haitallisesta koodista.

Näitä IOCeiksi (engl. indicators of compromise) kutsuttuja tietoja tarvitaan muun muassa nollapäivähaavoittuvuuksien ja jatkuvasti muuttuvien uhkien havainnoimiseen. (Humphries 2019.)

5.6 Visualisointi

SIEMissä visualisoinnin avulla saadaan koostettua erilaisia näkymiä kyberympäristöstä lähestulkoon reaaliaikaisesti. Näkymiä voidaan hallita web-pohjaisen ohjausnäkymän kautta, johon voidaan määrittää näkyväksi esimerkiksi erilaisia tilastoja, käyriä ja muuta metriikkaa, jotka näyttävät senhetkisen ympäristön tilanteen. Yleensä lisäksi nähtävillä ovat myös tapahtumien historiatiedot, eli esimerkiksi mistä IP-osoitteesta on yritetty useamman kerran epäonnistuneesti kirjautua järjestelmävalvojana sisään tietylle palvelimelle tai työasemalle. Näitä voidaan hyödyntää tarvittaessa myös forensiikkatyössä. Yleensä hallintapaneeli on joko pilvipohjainen, jolloin se toimii valmistajan palvelimilla tai palvelinpohjainen, jolloin toiminta on keskittynyt organisaation omille palvelimille (Filkins 2019, 15). Visualisointia on havainnollistettu tarkemmin luvussa 6, kun käydään läpi valittujen SIEM-järjestelmien ominaisuuksia.

5.7 Raportointi

Raportointi mahdollistaa poikkeamien analysoinnin ja usein eri SIEM-ratkaisuissa on mahdollista hyödyntää valmiita raportteja tai luoda omia tarpeen mukaan. Raportointia voidaan tehdä esimerkiksi sisäänkirjautumista tai niiden yrityksistä, järjestelmien tai datan muutoksista, verkkoliikenteestä, haittaohjelmista ja ympäristössä tapahtuvista virheistä (Chuvakin, Phillips & Schmidt 2013, luku 12). Usein SIEM-järjestelmiin on generoitu valmiita raporttipohjia, esimerkiksi liittyen lainsäädäntöön tai standardeihin (esim. ISO27000-sarja, GDPR), joiden avulla voidaan verrata toteutuvatko vaaditut asiat omassa kybertoimintaympäristössä. Poikkeustilanteissa SIEM-järjestelmä voi generoida hälytyksen, kun rikkomuksia näihin säännöksiin tai standardeihin liittyen tapahtuu. (Compliance Solutions n.d.) Raporteista saadaan näkyville kyberympäristössä tapahtuvat trendit, eli esimerkiksi kuinka paljon tietyntyyppisiä hyökkäyksiä on tehty tiettyyn kohteeseen.

6 SIEM-tuotteiden vertailu

SIEM-tuotteita lähdettiin vertailemaan tarkemmin tilaajan puolelta asetettujen vaatimusten pohjalta. Yleisiä vaatimuksia tulevalle järjestelmälle koottiin taulukkoon 3 teemoittain. Valittavan järjestelmän tuli olla näiden ominaisuuksien lisäksi modulaarinen, eli integroitava muihin jo olemassa oleviin järjestelmiin, sekä sen tuli mukautua muuttuviin tulevaisuuden tarpeisiin. Vaatimuslista toimeksiantajan puolelta on koostettu keskustellen eri henkilöiden kanssa tarpeista ja vaatimuksista, joten samalla hyödynnettiin laadullisen tutkimuksen menetelmää, eli käytännössä haastateltiin työntekijöitä. Koostettu taulukko on dokumentti käydyistä keskusteluista.

Taulukko 3. Toimeksiantajan yleiset vaatimukset

Metriikka ja ohjausnäkymä	**Tapahtumien havainnointi, analytiikka ja visualisointi**
Mukautettujen näkymien luominen	Sääntöpohjainen korrelointi
Reaaliaikaiset päivitykset	Useiden laitteiden ja kompleksisten tapahtuminen korrelointi
Roolipohjaiset näkymät	Tulosten ja löydösten graafinen visualisointi
Monipuoliset hakutoiminnot	Uhkasyötteiden / IOCien reaaliaikainen päivittyminen
Intuitiivinen ja käytettävä	Tapahtumakaavojen havaitseminen datalähteestä tai tyypistä riippumatta
Lait, standardit ja säädökset	Käyttäytymisen analysointiin pohjautuva poikkeamien havainnointi
Valmiit raporttipohjat	Verkkoliikenteen nauhoittaminen ja varastointi
Valmiit korrelointisäännöt	**Työnkulun hallinta**
Hälytys, kun säännöstöä rikotaan	Ongelmatikettien generointi
Lokienhallinta	Mukautettujen työjonojen luominen
Lokitietojen kerääminen eri lähteistä	Automatisoidut/manuaaliset vasteet
Lokitietojen eheyden ylläpito	**Hälytykset ja ilmoitukset**
Agentiton/agentillinen keräin	Reaaliaikaiset hälytykset ja ilmoitukset
Lokien normalisointi ja aikaleimaus	Hälytysilmoitukset eri kanavien kautta
Vikasietoisuus	**Tukipalvelut**
Luotettava lokien välittäminen	Käyttöönotto, koulutus ja ylläpito
Lokitietojen käsittelystä jää merkintä	Asiakaspalvelu

Huomioon ottaen toimeksiantajan näkökulma ja vaatimukset, valikoitui näiden perusteella vertailtaviksi tuotteiksi Gartnerin markkinatutkimuksen kolme johtavaa toimijaa, eli Splunk, IBM Qradar sekä LogRhythm, jotka ovatkin olleet tutkimuksen kärkisijoilla jo useampia vuosia (Bussa, Kavanagh & Sadowski 2018). Seuraavissa luvuissa käydään tarkemmin läpi valittujen SIEM-järjestelmien ominaisuudet, vahvuudet ja heikkoudet sekä käyttöliittymien erilaisia näkymiä.

6.1 Splunk Enterprise Security

Splunk valmistaa SIEM-järjestelmien lisäksi myös muita työkaluja liittyen data-analytiikkaan, IoT-laitteisiin ja turvallisuuteen. Splunk Enterprise Security on Splunkin kaupallinen SIEM-tuote ja se on pääosin suunnattu keskisuurille ja suurille yrityksille. Käytännössä Splunk Enterprise -ohjelmisto toimii alustana turvallisuuteen liittyville lisäosille, joihin myös Splunk Enterprise Security kuuluu. Alustalle on mahdollista ostaa Splunk Enterprise Securityn lisäksi erikseen SOAR-työkalu eli Splunk Phantom tai UEBA-työkalu eli Splunk User Behavior Analytics. Nämä kolme moduulia yhdistämällä saadaan kokonaisvaltaisin näkyvyys omaan ympäristöön sekä Phantomin avulla hyödynnettyä automaatio-ominaisuuksia. Tuotetta on mahdollista ostaa pilvipalveluna, talon sisäisenä ja ulkoisena palveluna sekä hybridinä. (Bussa, Kavanagh & Sadowski 2018.)

Tuotteen lisensointimalli perustuu joko alustalle syötettyyn tapahtumien määrään (GB/päivä) tai vaihtoehtoisesti infrastruktuuripohjaiseen laskentatehon määrään. Jälkimmäinen voi olla järkevämpi ratkaisu, mikäli tapahtumia on paljon päivän aikana. Esimerkiksi Netflow- ja DNS-dataan on mahdollista saada alennuksia, kun kyseessä on tapahtumiin pohjautuva hinnoittelu. Asiakaspalvelun palvelun nopeudessa ja laajuudessa on erilaisia tasoja riippuen ostettavan paketin tasosta. (Splunk® Enterprise Security n.d., osio Splunk for Security.)

6.1.1 Ominaisuudet

Splunk Enterprise Securityn tärkeimpinä ominaisuuksina voidaan nähdä edistyneemmät sisäänrakennetut ja säännöllisesti päivittyvät käyttötapaukset, valmiit ohjausnäkymät ja haut, korreloidut hakutoiminnot, sisäänrakennetut korrelointisäännöt, hälytykset, raportit, reaaliaikainen monitorointi sekä poikkeamienhallinta. Splunk Enterprise Security sisältää Investigation Workbench -ominaisuuden, jonka avulla saadaan kokonaisvaltaisempi kuva tapahtuneista välikohtauksista ja poikkeamista sekä kyetään reagoimaan uhkiin parhaimmillaan reaaliajassa. (Adopting Splunk's analytics-driven security platform as your SIEM 2018, 6.)

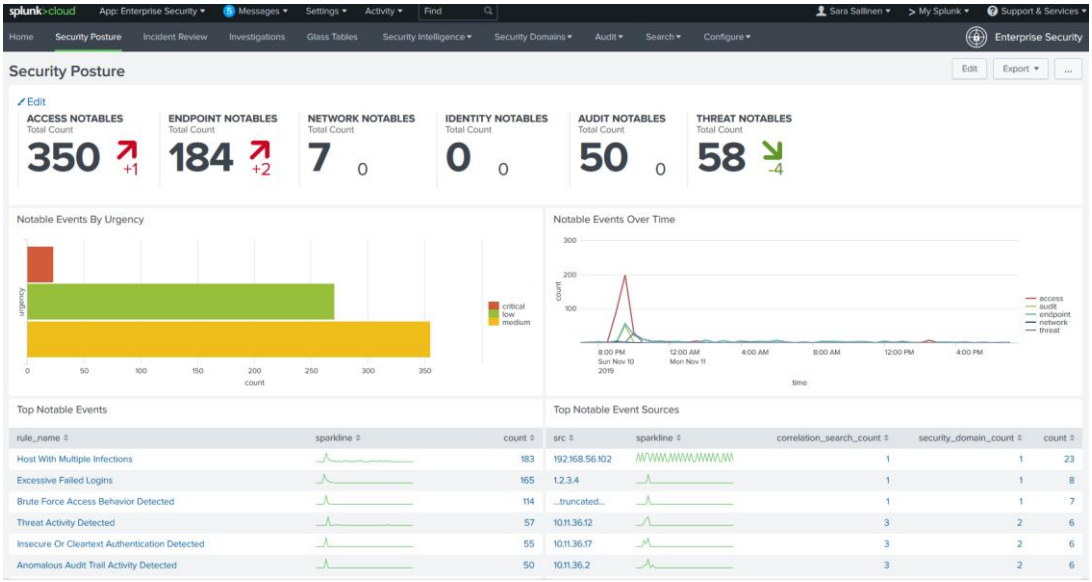
Valmiiden käyttötapausten avulla voidaan helpottaa ammatillisesti eri tasoisten työntekijöiden taakkaa, koska Splunkin oma tutkimusryhmä jakaa tietoaan uusimmista kyberturvallisuuteen liittyvistä trendeistä ja puolustustekniikoista. Splunkin web-alustalla on mahdollista hakea ilmaiseksi tai erikseen ostamalla yli 800 erilaista turvallisuusapplikaatiota, esimerkiksi uudemman sukupolven palomuureja, edistynyttä uhkien hallintaa ja niin edelleen. Splunk tukee myös useita kolmannen osapuolen valmistajien tuotteita, mikä tekeekin tuotteesta modulaarisen. (Mts. 6.) Taulukossa 4 on listattuna eri tietolähteistä yhdistettynä käyttäjien näkemyksiä järjestelmän vahvuuksista ja heikkouksista. Päätavoitteena oli saada Splunkin omien materiaalien lisäksi muita mielipiteitä, jotta tulokset olisivat luotettavampia.

Taulukko 4. Splunk Enterprise Securityn vahvuudet ja heikkoudet (Bussa, Kavanagh & Sadowski 2018; Security Information and Event Management Market 2019; Best Security Information and Event Management (SIEM) Software n.d.)

Vahvuus	Heikkous
Yksinkertaiset käyttötapaukset	Hinnoittelumallien vuoksi kustannukset suuria
Laajat integroitumismahdollisuudet	Riippuvuus 3-osapuolten tuesta OT-protokollille
Laaja sovelluskauppa	Asiakastuessa puutteita
Vahvat henkilötietojen (PII) suojausominaisuudet	Ei paikallista tukea FIM tai EDR-pohjaisille agenteille, onnistuu kuitenkin 3-osapuolien avulla
Helppokäyttöisyys	Täysi perehtyminen vie aikaa, koska todella paljon ominaisuuksia
Vaihtoehdot kuinka tarkkaa analytiikkaa halutaan (UBA + SOAR)	UBA saatavilla ainoastaan in-house ja pilvipohjaisesti
Kehittyneet korrelointisäännöt	Toteutusvaihe ja datan validointi on aikaa vievää

6.1.2 Käyttöliittymä

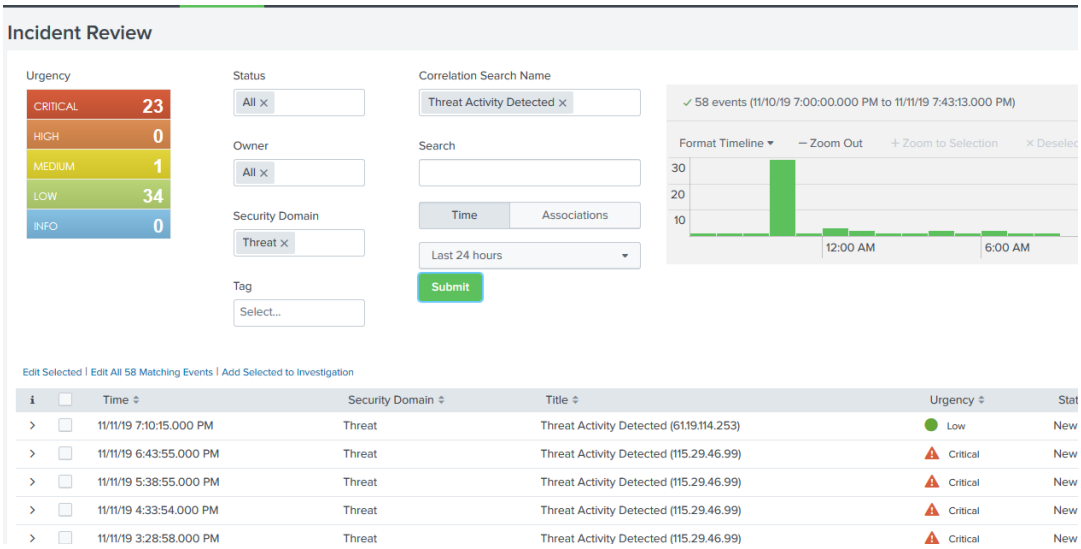
Splunkin verkkosivustolla on mahdollista testata Splunk Enterprise Securityä pilvipohjaisesti hiekkalaatikkoympäristössä ja sen avulla tutkittiin käyttöliittymän käytettävyyttä ja toiminnallisuuksia. Kuviossa 12 on Security Posture -perusnäkymä, joka käytännössä ilmaisee nopeasti huomionarvoisia asioita ympäristöstä, kuten esimerkiksi pääsynvalvontaan, loppukäyttäjien laitteisiin, verkkoon tai havaittujen uhkien määrään. Sivustolla on myös näkyvillä erilaista metriikkaa ja tarkempaa tietoa havainnoista saa helposti klikkaamalla tapahtumaa. Näkymää voi muokata omien tarpeiden mukaan tai käyttää valmiita pohjia.



Kuvio 12. Security Posture -näkymä

Incident Review -välilehdeltä pääsee tekemään erilaisia hakuja (ks. kuvio 13) ns. Extreme Searchin avulla. Määrittelyt saa tehtyä hyvinkin tarkasti, jotta saadaan luotettavampia ja rajatumpia hakutuloksia. Näkymästä pääsee myös hallinnoimaan poikkeamia, eli esimerkiksi muuttamaan niiden tilaa tai kriittisyyttä sekä siirtämään niitä esimerkiksi toisen työntekijän tehtäväksi. Kaikki tehdyt muutokset Splunkin tietoihin

tallennetaan Incident Review Audit -välilehdelle, jolloin muutokset ovat jäljitettävissä. Data varmennetaan luottamusketjun säilyttämiseksi allekirjoituksin. (Operationalize Security Intelligence 2019.)



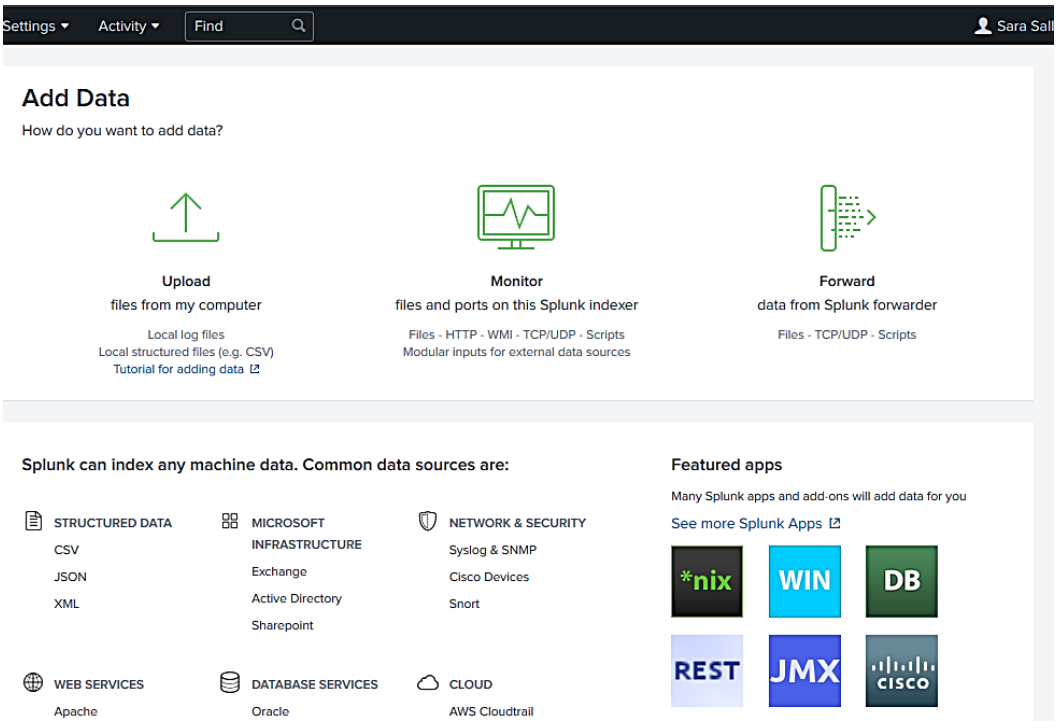
Kuvio 13. Incident Review -näkymä

Eri välilehtien rakenne oli itseään toistava, eli ne sisältävät metriikkaa ja erilaisia käyriä tapahtumista. Tästä syystä ei koettu mielekkääksi lisätä jokaisesta näkymästä erikseen kuvaa, vaan katsottiin järkevämmäksi luetella pääkohdat näistä ominaisuuksista. Sisäisten ja kehittyneiden uhkien havainnointiominaisuus sisältää toiminnallisuuksia Asset/Identity Centeristä, missä kaikki kybertoimintaympäristön resurssit ovat nähtävillä. Resursseista saadaan tiedot esimerkiksi niiden omistajasta, kriittisyydestä ja kenellä pitäisi olla pääsy näihin tietoihin. Tämä auttaa turvallisuustapahtumien priorisoinnissa.

Threath Activity -välilehdelle kootaan havaitut uhkat ja tältä välilehdeltä pääsee tekemään tarkempaa tutkimusta havaitusta poikkeavasta käyttäytymisestä sisältäen uusien DNS-domainien analyysit, http-kategoriat ja käyttäjäanalyysit, liikenteen määrään ja URLien pituuteen liittyvät analyysit sekä älykkäiden uhkasyötteiden artefaktit.

Myös muihin protokolliin, kuten SSL-liikenteeseen liittyvät havainnot ovat koottuna välilehdelle. Älykkäiden uhkasyötteiden viitekehityksen avulla saadaan automaattisesti kerättyä, ryhmiteltyä ja poistettua kaksoiskappaleita uhkasyötteistä. Splunkiin onkin integroitavissa huomattava määrä kolmansien osapuolien tarjoamia uhkatietoja.

Splunk Enterprise Security sisältää pääsynhallintaan liittyvää suojausta loppukäyttäjille, sovelluksille, laitteille sekä lukuisia kolmannen osapuolen sovelluksia on integroitavissa järjestelmään. Asetusten muokattavuus on melko yksinkertaista, ja tästä on esimerkkinä tietolähteen lisääminen Splunkiin kuviossa 14. Dataa voidaan lisätä erilaisissa muodoissa ja Splunk listaakin yleisimmät tuotteessaan. Lisäämisvaiheessa data luokitellaan ja näitä tietoja voidaan mukauttaa omien tarpeiden mukaan. Splunkissa Data Forwarderit ajavat samaa asiaa kuin lokiagentit. Splunkin ominaisuudet vaikuttivat yleiskuvaltaan melko helppokäyttöisiltä ja ohjatuilta toimenpiteiltä. Dokumentaatiota järjestelmästä on melko kattavasti saatavilla Splunkin verkkosivustolla.



Kuvio 14. Datan lisääminen Splunkiin

6.2 IBM QRadar SIEM

Valmistajana IBM on ollut alalla pitkään, joten myös turvallisuuteen ja analytiikkaan liittyvä valikoima on monipuolinen. IBM Security tarjoaa palveluita SIEMin ja muiden turvallisuustyökalujen lisäksi myös liittyen tietosuojaan, tekoälyyn, teollisuuteen sekä erilaisten lakien ja säännösten noudattamiseen. IBM QRadar SIEM -alustaan on lisättävissä monia lisäosia, kuten UEBA, tekoälyyn pohjautuvaa analytiikkaa (IBM QRadar Advisor with Watson), pilvipalveluiden analytiikkaa (IBM QRadar on Cloud), syvempää analyysiä verkkoliikenteestä (IBM QRadar Network Insights), haavoittuvuuksien hallintaa (IBM QRadar Vulnerability Manager), forensiikkaa IBM QRadar (Incident Forensics) sekä datan säilytysratkaisuja IBM QRadar (Data Store). (The IBM QRadar Security Intelligence Platform 2019.) Lisensointimalli perustuu tapahtumien määrään, eli paljonko tapahtumia on sekunnissa (EPS) tai tapahtumavirtoja sekunnissa (FPS). Tuotetta on saatavilla virtuaalikoneena ja ohjelmistona joko pilviratkaisuna tai hallinnoitavana organisaation itsensä toimesta (Bussa, Kavanagh & Sadowski 2018).

6.2.1 Ominaisuudet

IBM Security Intelligence -alusta jakautuu käytännössä kolmeen moduuliin: valvonta, havainnointi ja tutkinta. Valvonta-moduulissa kerätään tietoa eri tapahtumista kybertoimintaympäristössä mahdollisten uhkien tunnistamista ja analysointia varten. Erillisiä haavoittuvuusskannereita voidaan integroida alustaan, jolloin korjaustoimenpiteitä voidaan priorisoida tehokkaammin. Monitorointi-moduulissa hyödynnetään esimerkiksi koneoppimista pohjaprofiilin luomiseen, jotta ympäristöstä voidaan havaita poikkeavaa käyttäytymistä. Havainnointi toimii korreloinnin pohjalta allekirjoitus- tai käyttäytymispohjaisia metodeja noudattaen. Sääntöpohjalta, IOCeihin ja tiettyihin kaavoihin täsmäävien metodien avulla voidaan havaita sekä reaaliajassa että jälkikäteen havaittuja tunnettuja ja tuntemattomia uhkia. Näiden lisäksi kehittyneemmät verkkoanalysointiominaisuudet auttavat huomaamaan poikkeavaa kommunikointia. Riskipohjaisen havainnoinnin ja priorisoinnin avulla tehdään tapahtumien analysointia ja korrelointia tietolähteiden, käyttäjien, verkkoliikenteen, haavoittuvuuksien ja älykkäiden uhkatoimintojen pohjalta. (The IBM QRadar Security Intelligence Platform 2019.) Tutkinta-moduuli hyödyntää rikkomuskortteja automatisoidussa analytiikassa,

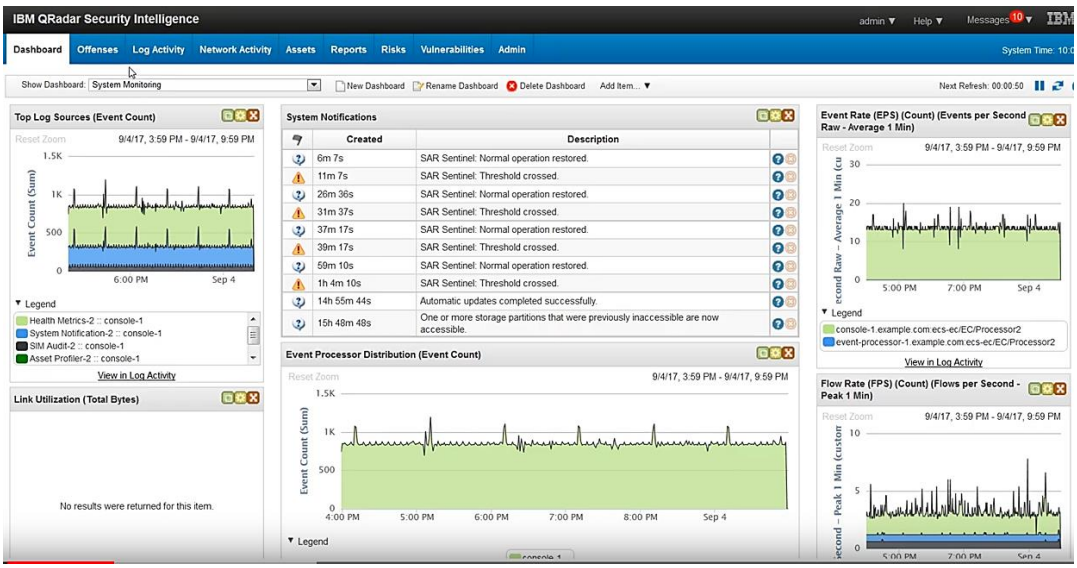
mikä nopeuttaa tietoturva-asiantuntijoiden työskentelyä. Advisor-ominaisuuden avulla voi hyödyntää tekoälyyn pohjautuvaa Watsonia alustaviin tutkimuksiin. (Mts. 6-7.) Taulukkoon 5 on koostettuna näkemyksiä Qradarin heikkouksista ja vahvuuksista asiakkaiden näkökulmasta.

Taulukko 5. IBM Qradar vahvuudet ja heikkoudet (Bussa, Kavanagh & Sadowski 2018; Security Information and Event Management Market 2019; Best Security Information and Event Management (SIEM) Software n.d.)

Vahvuus	Heikkous
Joustava ja vahva alusta	Käyttöliittymä ei ole helppokäyttöinen tai käyttäjäystävällinen
Laaja valikoima käyttötapauksia	Integraatio ja käyttöönotto on saanut muita valmistajia vähemmän pisteitä
Vahva ekosysteemi, helposti integroitavissa IBM:n omia lisäosia	Riskienarviointi vaatii osaamista rikkomusten käsittelemiseksi
Laaja tuki verkkoliikenteen valvomiselle	Riskien pisteytys ei ole muokattavissa UEBAssa
Selkeät, muokattavat raportit	Asiakaspalvelu ja tuki saanut muita vähemmän pisteitä
Lokilähteiden automaattinen tunnistaminen	Suodattimien luomisen jälkeen niitä ei voi muokata lainkaan

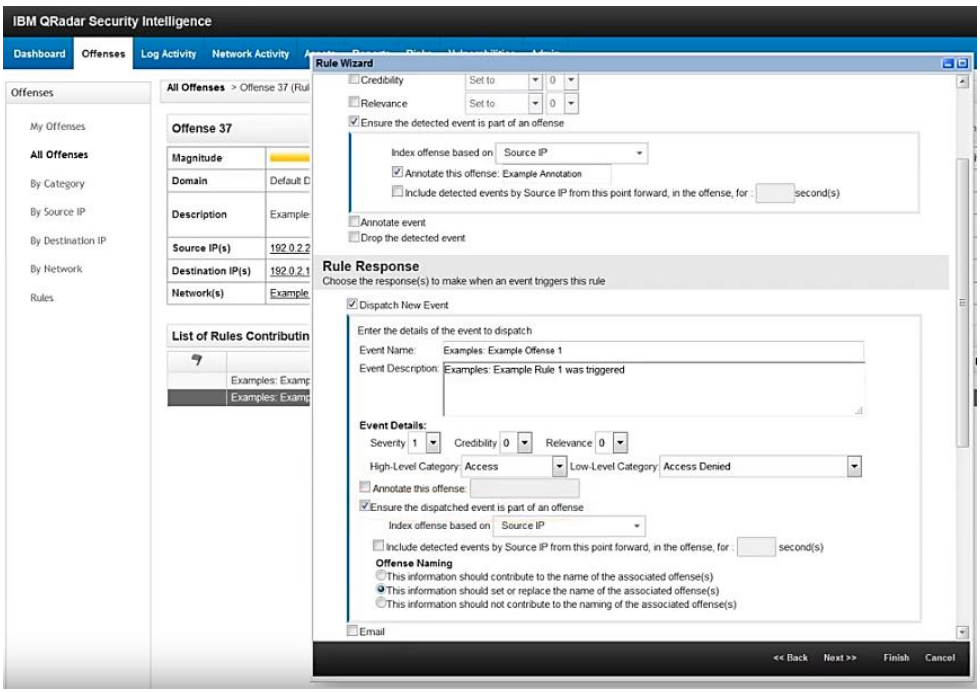
6.2.2 Käyttöliittymä

QRadarin SIEMin käyttöliittymää ei kyetty testaamaan testiympäristössä, joten tietoja näistä toiminnallisuuksista haettiin muun muassa IBM:n omasta dokumentaatiosta. QRadar Security Intelligence-alustan Dashboard-näkymä (ks. kuvio 15) sisältää erilaista metriikkaa ja sitä voi muokata haluamansa näköiseksi lisäämällä tai poistamalla sisältöä. Näkymä toimii käyttöoikeuspohjaisesti, joten tehdyt muutokset eivät vaikuta jokaiseen käyttäjään.



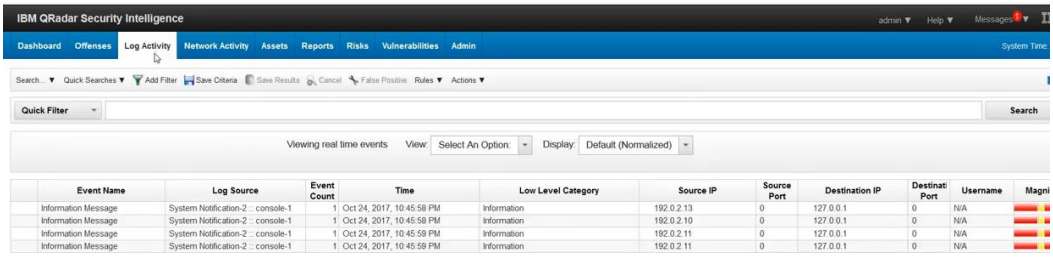
Kuvio 15. Qradar Dashboard -näkymä (IBM QRadar SIEM Tuning: Introduction to QRadar and Tuning 2017)

Tärkeä osa QRadarin toimintaa on niin sanotut rikkomukset, eli offenset (engl. offences). Järjestelmä generoi rikkomuksia eri tapahtumien välillä, joista ketjuttamisen avulla saadaan tuotettua kokonaismäärä generoiduista hälytyksistä. Koska tiedot ovat koottuna yhdelle sivulle, saa asiantuntija suoraan kuvan millaisesta tapahtumasta on kyse. Mikäli tapahtumaketjuun liittyy uusia tapahtumia, päivittyvät tiedot luodulle rikkomuskortille. Kortti sisältää tiedot kuinka suuri rikkomus kyseessä on omaan ympäristöön verrattuna sekä poikkeavuuden vakavuusasteen verrattuna haavoittuvaan kohteeseen. Offenses-välilehdeltä (ks. kuvio 16) voidaan tarkistella näitä rikkomuksia, sekä määritellä säännöstöt, milloin tietyt tapahtumat yhdistetään rikkomukseen. Rikkomuksista saa myös kasattua koosteita, joista pystyy suoraan näkemään tapahtumiin vaikuttavat tekijät ja esimerkiksi siihen liittyvät IP-osoitteet. (IBM Knowledge Center 2017.)



Kuvio 16. QRadarin Offenses -välilehti (IBM QRadar SIEM Tuning: Offense Basics 2018)

Log Activity -välilehti (ks. kuvio 17) sisältää perusnäkymän eri lokilähteisiin, joihin voi suorittaa hakuja ja lisätä erilaisia suodattimia. Hakuja ja niiden tuloksia on mahdollista tallentaa. Myös tälle välilehdelle on mahdollista tehdä mukautettuja säännöstöjä, mikäli käyttöoikeudet sen sallivat. Säännöstöjä voi luoda perustuen käyttäytymiseen, poikkeavuuteen sekä luotujen sääntöjen rikkomiseen. Lokitietoja voi tarkastella raakamuodossa, normalisoituna, ryhmiteltynä tai reaaliajassa.



Kuvio 17. Log Activity -näkymä (IBM QRadar SIEM Tuning: Offense Basics 2018)

Network Activity -välilehden avulla voidaan valvoa ja tutkia verkkoliikennettä erilaisin hakutoiminnoin ja luoden säännöstöjä vastaavasti kuin Log Activity -välilehdellä. Asset Managementin kautta hallitaan kybertoimintaympäristön resursseja. QRadar käyttää niin sanottuja mustia ja valkoisia listoja tunnistamaan onko jokin resurssi haitallinen vai ei. Reports -välilehdeltä nimensäkin mukaisesti pääsee muodostamaan erilaisia raportteja. Admin -välilehdeltä pääsee tekemään järjestelmävalvojan toimia, eli järjestelmän konfigurointiin, käyttäjien hallintaan, datan ja tapahtumien lähteisiin liittyviä toimenpiteitä. (IBM Knowledge Center 2017.) Myös IBM:llä on laajat dokumentatiot tuotteistaan verkkosivustollaan.

6.3 LogRhythm Next-Gen SIEM Platform

LogRhythm tunnetaan parhaiten muun muassa erilaisten SIEM-järjestelmien, lokienhallintaan, analysointiin ja verkonvalvontaan keskittyvien tuotteiden valmistajana. LogRhythmin Next-Gen SIEM -alustat ovat tarkoitettu lähinnä suurille tai keskisuurille organisaatioille. Next-Gen SIEMin XDR -alusta koostuu käytännössä kolmesta eri komponentista: AnalytiX (analytiikka), DetectX (havainnointi) sekä RespondX (vaste). Näiden lisäksi alustalle on ostettavissa erilaisia lisäturvallisuusominaisuuksia, kuten UEBA ja verkkoliikenteen analysointityökalu (NetworkXDR). (LogRhythm NextGen SIEM Platform n.d.) SIEM-järjestelmä on saatavilla ohjelmistona, virtuaalikoneena tai fyysisenä laitteistona. Järjestelmä on mahdollista toteuttaa organisaation itsensä hallinnoitavana, osittain organisaation ja osittain palveluntarjoajan hallinnoimana sekä hybridinä. Hinnoittelu toimii tässä tuotteessa sen perusteella, kuinka monta viestiä tapahtuu sekunnissa (MPS) keskimäärin päivän aikana. (Bussa, Kavanagh & Sadowski 2018.) Uudeksi hinnoittelumalliksi on kuitenkin lanseerattu vuoden 2019 lokakuussa rajoittamattomaan datan määrään perustuva malli, missä maksetaan ainoastaan vuosittainen maksu, jolloin muuttuvat datamäärät eivät nosta hintaa (LogRhythm Releases First True Unlimited Data Plan for SIEM 2019).

6.3.1 Ominaisuudet

LogRhythmin SIEM-ratkaisu perustuu tietoaltaiden käyttöön, minkä avulla saadaan keskitettyä lokitietoja yhteen paikkaan skaalautuvasti. Uhkien havainnointi, poikkeava käytös ja kriittiset tapahtumat voidaan havaita reaaliajassa LogRhythmin AI Enginen avulla. AnalytiX-komponenttiin sisältyy lokidatan ja muiden tapahtumien analysointi niin fyysisistä, virtuaalisista kuin pilvipohjaisistakin ympäristöistä. AnalytiX luokittelee, indeksoi, normalisoi sekä rikastaa datan, jotta esimerkiksi hakujen tekeminen nopeutuu. Hakuja voidaan toteuttaa laajalti rakeenteelliseen ja ei-rakenteelliseen dataan, sekä uusilla kyselykielillä (engl. query language). (LogRhythm NextGen SIEM Platform n.d., osio AnalytiX.)

DetectX-komponentti sisältää ominaisuudet havaita haitallista toimintaa jatkuvasti päivittyvien uhkatietojen sekä sisäänrakennettujen sisältöpohjaisten uhkienhavainnointitoimintojen avulla. Koneoppimisen hyödyntäminen ristiinkorreloinnilla edesauttaa havaitsemaan epäilyttävää käyttäytymistä. DirectX sisältää MITRE ATT&CK -moduulin, minkä avulla voi testata tietoturvavalvomon havainnointikykyä ja sen säännöstöjä erilaisin hyökkäystekniikoin. Sisäänrakennetun määräystenmukaisuuden varmistamiseen tarkoitettu moduuli havaitsee automaattisesti poikkeamia säädöksissä. (LogRhythm NextGen SIEM Platform n.d. , osio DetectX.)

RespondX-komponentti sisältää SOAR-ratkaisun, joka kykenee hoitamaan automatisoidusti poikkeamien ja tapahtumien hallinnan, tietoturvatapahtumien tutkinnan, sekä poikkeamiin reagoiminen helpottuu valmiiden pelikirjojen (engl. playbooks) avulla, joilla asiantuntijat voivat analysoida ohjatusti tapahtumia. Automatisointi on kuitenkin rajoittunut yksittäisiin toimiin, eikä monimutkaisten poikkeamien käsittelyyn. Erilaisen metriikan tuottaminen ja raportointi hoituvat tämän komponentin avulla. (LogRhythm NextGen SIEM Platform n.d., osio RespondX.) Taulukkossa 6 on koostettuna käyttäjien näkemyksiä LogRhythm SIEMin heikkouksista ja vahvuuksista.

Taulukko 6. LogRhythm vahvuudet ja heikkoudet (Bussa, Kavanagh & Sadowski 2018; Security Information and Event Management Market 2019; Best Security Information and Event Management (SIEM) Software n.d.)

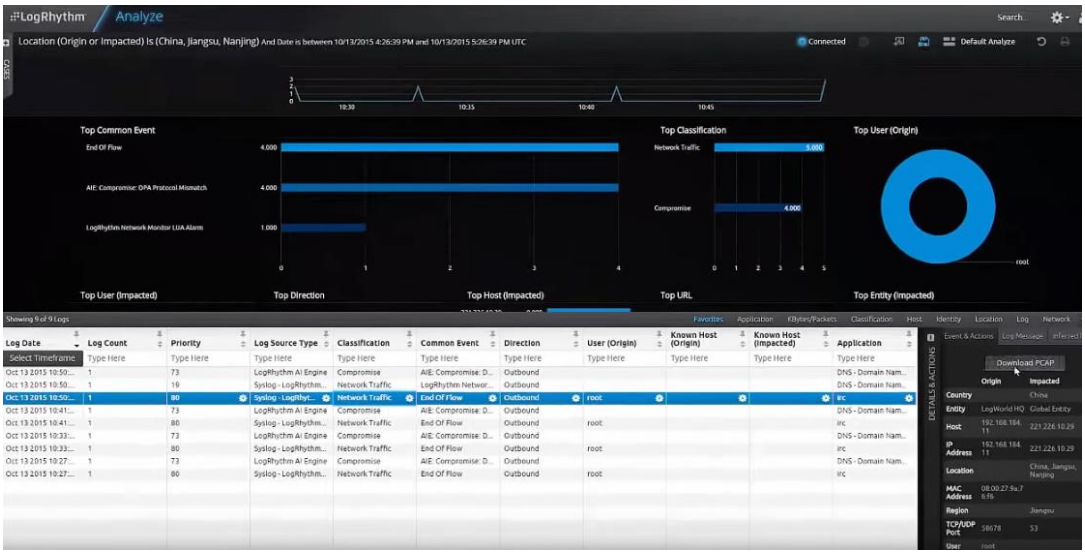
Vahvuus	Heikkous
Itsenäinen toimija, tarjoaa vaihtoehtoja verkko- ja host-tason seurannalle	Ei omaa sovelluskauppaa
Helppo käyttöönotto	Yksistään SOAR-ominaisuudet eivät ole vielä kovinkaan kehittyneitä
Käyttöliittymä helppokäyttöinen	Epäselvää markkinointia
Valmiit sisällöt päivittyvät jatkuvasti	Hinnoittelun ja sopimusten joustamattomuus
Hallinnointi helppoa	Raporttipohjia ei voi muokata luomisen jälkeen
Sisältöjen muokkausmahdollisuudet	Paljon menuja ja valikoita, joten opetteluun menee aikaa

6.3.2 Käyttöliittymä

Myöskään LogRhythmin SIEM-tuotetta ei ollut mahdollista testata konkreettisesti, joten aineistoa käyttöliittymästä piti kerätä saatavilla olevista lähteistä. Päänäkymä (ks. kuvio 19) eli Dashboards-välilehti sisältää jälleen erilaista metriikkaa tapahtumista ja näkymän saa muokattua haluamakseen. Klikkailemalla metriikoita saa avattua alareunaan analysointinäkymän, joka avaa tapahtumien tarkemmat tiedot ja jonka avulla voi suorittaa erilaisia hakuja.

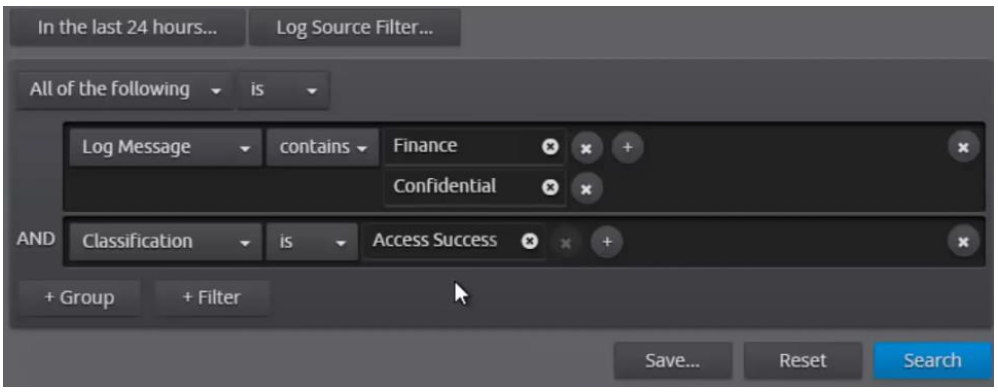
Kuvio 19. LogRythm SIEMin päänäkymä (Goldhammer 2016)

Analyze- välilehdellä (ks. kuvio 20) tehdään tapahtumien tarkempaa analysointia. Näkymään saadaan näkyville erilaista metriikkaa. Alareunaan saa näkymään lokitiedot samoin kuin Dashboard-välilehdeltäkin. Sivun oikeasta laidasta voi tarkastella tarkempia tapahtumatietoja valitsemalla lokilähteen listalta. Kyseistä tapahtumasta on mahdollista ladata esimerkiksi pcap-tiedosto tarkempaa tutkimusta varten.



Kuvio 20. Analyze -välilehti (Goldhammer 2016)

Hakujen toteuttaminen ja erilaisten suodattimien lisääminen on helppoa (ks. kuvio 21). Tehdyt haut voidaan tallentaa ja lisätä hakujen tulokset esimerkiksi Dashboardille. Hälytykset-välilehdelle on jaoteltuna erikseen uudet tapahtumat ja niiden tiedot. Hälytyksiä voidaan suodattaa ja muokata säännöstöin sekä lajitella erilaisin määrein.



Kuvio 21. Esimerkki hakutoiminnosta LogRhythmin SIEMillä (Goldhammer 2016)

Epäilyttävistä tapahtumista voidaan luoda ns. Case-kortteja, joihin kerätään tarkempaa tietoa tapahtumasta ja lisätä tapahtumiin tageja, joiden avulla voidaan suorittaa kohdennetumpia hakuja. Case-kortteihin voidaan määritellä niiden prioriteetti ja lisätä tarvittavia lokilähteitä sekä kerätä niille todistusaineistoa epäilyjen tueksi. Cases-välilehdelle on koottuna Case-kortit (ks. kuvio 22) ja näkymästä pääsee tarkastelemaan korttien historiatietoja, määriä ja avoimien Case-korttien sisältöjä.

Kuvio 22. Cases -välilehti (Goldhammer 2016)

7 Tutkimustulokset

Vastausta vaatimustenmukaiseen SIEM-järjestelmän etsimiseen hyödynnettiin kehittämistutkimuksen aineistonkeruu- ja analysointimenetelmien piiriin kuuluvan laadullisen tutkimuksen menetelmiä. Aineistonkeruuseen käytettiin SIEM-tuotteiden valmistajien verkkosivuja, arvosteluita, videoita, valokuvia, raportteja, manuaaleja sekä muuta saatavilla olevaa dokumentaatiota. (Kananen 2015, 77.) Itse tuotevertailussa kuitenkin käytettiin määrällisen, eli kvalitatiivisen tutkimusmenetelmän keinoja luomalla taulukoita, joissa paras vaihtoehto perusteltiin vertailemalla ominaisuuksien ja arvosteluiden perusteella koostettuja pistemääriä.

Puolueettomuus oli tärkeää tietolähteitä valitessa liittyen tuotteiden ominaisuuksiin, joten eräs tärkeä tietolähde oli Gartnerin tuottama Magic Quadrant (MQ) -markkinointitutkimus. Vastaavia tutkimuksia tehdään monien eri toimialojen tuotteista, mutta tässä tutkimuksessa on käytetty SIEM-järjestelmiin liittyvää tutkimusta vuodelta 2018. MQ:ssa tarkoituksena on antaa lukijalle ymmärrystä, minkälaisia tuotteita on markkinoilla sekä avata niiden ominaisuuksia. Valmistajat arvioidaan tuotteidensa perusteella neljään eri luokkaan, eli johtajat (engl. leaders), visionäärit (engl. visionaries), niche-pelaajat (engl. niche players) sekä haastajat (engl. challengers). Johtajat-osion tuotteet suoriutuvat hyvin heidän nykyisestä visiostaan sekä ovat varustautuneet hyvin tulevaisuutta varten. Visionäärit ovat menossa kohti oikeaa suuntaa ja ymmärtävät tämänhetkiset tarpeet markkinoilla, mutta eivät vielä toimi tarpeeksi hyvin. Niche-pelaajat keskittyvät pienempään segmenttiin onnistuneesti tai ovat toistaiseksi huonosti keskittyneitä, eivätkä ole innovatiivisia muita ylittäviä toimijoita. Haastajat suoriutuvat hyvin tai voivat hallinnoida suurta segmenttiä, mutta eivät vaikuta ymmärtävänsä markkinoiden suuntaa. (Bussa, Kavanagh & Sadowski 2018.)

Kaikki kolme valittua järjestelmää olivat Gartnerin tutkimuksen johtajat-osiossa, mikä vaikutti selvästi siihen, että myös näiden kolmen järjestelmän ominaisuudet olivat hyvin samankaltaisia keskenään. Ominaisuuksista koottiin toimeksiantajan vaatimuksia vastaava taulukko 7, johon on koostettu vaatimuksissa määritellyt ominaisuudet ja niitä vastaavat pistemäärät. Liitteessä 1 on nähtävillä täydentävä taulukko, missä

on eriteltynä jokainen ominaisuus omalle rivilleen. Näiden tietojen pohjalta Splunk Enterprise Security ja LogRhythmin SIEM sijoittuivat tasasijoille 28 pisteellä, kun taas IBM QRadar sai vain yhden pisteen näitä toimijoita vähemmän. Kokonaispistemäärä ominaisuuksille oli kaikkiaan 29.

Taulukko 7. Vertailutaulukko SIEM-tuotteiden ominaisuuksista

Ominaisuus (max pistemäärä)	Splunk ES	IBM Qradar	LogRhythm SIEM
Metriikka ja ohjausnäkymä (5)	5	4	5
Lait, standardit ja säädökset (3)	3	3	3
Lokienhallinta (8)	8	7	8
Tapahtumien havainnointi, analytiikka ja visualisointi (6)	5	5	5
Työkulun hallinta (3)	3	3	3
Hälytykset ja ilmoitukset (2)	2	2	2
Tukipalvelut (2)	2	2	2
YHTEENSÄ (29)	28	27	28

Tuotteiden ominaisuuksien ollessa niin lähellä toisiaan havaittiin, ettei tällainen lähestymistapa anna kokonaiskuvaa vielä yksittäisestä ominaisuudesta. Tällä tarkoitetaan sitä, että tuotteessa voi olla jokin ominaisuus, mutta tämä tieto ei vielä kerro, onko kyseinen ominaisuus toimiva vai ei. Koska kaikkia SIEM-järjestelmiä ei päästy testaamaan ja antamaan painoarvoa omalle havainnoinnille, päädyttiin tekemään vielä tutkimusta asiakaskokemuksista neljältä eri sivustoilta liittyen tuotteiden arviointeihin, jotka ovat koottuna taulukkoon 8.

Ensimmäinen lähde oli Gartner, josta mainittiinkin jo tämän luvun alkupuolella. Toinen lähde oli G2, joka pitää sisällään yli miljoona tuotearvostelua eri käyttäjiltä ja on toiminut vuodesta 2012 lähtien keräten käyttäjäkokemuksia (G2 n.d., osio About). Kolmantena hyödynnettiin IT Central Stationin verkkosivustoa, joka pitää sisällään lähes 400 000 tuotearvostelua (IT Central Station n.d.). Neljäntenä sivustona oli Trust Radius, joka taas määrällisesti sisältää yli 200 000 tuotearvostelua eri ohjelmistoista (Trust Radius n.d.). Arvostelut pitivät sisällään ominaisuuksia liittyen reaaliaikaiseen valvontaan, uhkatietoihin, datan ja käyttäjien valvonnan ominaisuuksiin, sovellusten

valvontaan, analytiikkaan, lokien hallintaan ja raportointiin sekä esimerkiksi käyttöönottoon ja asiakastuen toimintaan. Taulukkoon merkityt ominaisuudet ovat siten keskiarvoa näiden ominaisuuksien pisteistä.

Taulukko 8. Eri sivustojen arvioinnit (Security Information and Event Management Market 2019; G2 n.d., osio Security Information and..; IT Central Station 2019; TrustRadius n.d.)

	Splunk Enterprise Security	IBM Qradar	LogRhythm SIEM	Sivusto
Arvostelujen lkm	266	268	488	Gartner
Pisteet	**4,4/5**	4,1/5	**4,4/5**	
Arvostelujen lkm	322	37	34	G2
Pisteet	**4,3/5**	4,2/5	3,9/5	
Arvostelujen lkm	56	38	70	IT Central Station
Pisteet	**4,4/5**	4,2/5	4,1/5	
Arvostelujen lkm	254	86	42	Trust Radius
Pisteet	4,4/5	**4,5/5**	3,8/5	
Keskiarvo n.	**4,4/5**	4,3/5	4,1/5	

Taulukon perusteella voidaan pitää Gartnerin tutkimusta luotettavimpana, koska siinä arvostelujen lukumäärät ovat huomattavasti suuremmat kuin muilla sivustoilla. Näiden pohjalta päädyttiin kuitenkin laskemaan vielä erikseen sivustojen pisteytyksien keskiarvo, jolloin tuloksista voidaan päätellä kokonaisvaltaisesti paras vaihtoehto. Keskiarvoista parhaimman, eli 4,4/5 sai Splunk Enterprise Security. Lukujen perusteella Splunkia on muutenkin arvosteltu valmistajana enemmän verrattuna muihin, mikä kertonee todennäköisesti tuotteen markkinoinnista tai kuluttajien kiinnostuksesta tuotteeseen. Kun verrataan eri sivustoilta saatua keskiarvoa ja vaatimuslistauksen vertailusta saatuja pistemääriä, menee Splunk Enterprise Security näistä kolmesta perustellusti johtavaan asemaan.

8 Pohdinta

Tutkimustyön tarkoituksena oli tehdä kartoitus toimeksiantajalle uudemman sukupolven SIEM-järjestelmistä ja löytää mahdollisesti sopiva järjestelmä toimeksiantajan käyttöön. Tutkimusongelmana oli, kuinka tilannetietoisuutta voidaan kasvattaa Organisaation X:n kybertoimintaympäristössä SIEM-järjestelmän avulla. Päätutkimuskysymyksenä taas esitettiin, mikä SIEM-järjestelmä olisi sopivin Organisaatio X:n asettamiin vaatimuksiin. Tutkimusongelmaan- ja kysymykseen saatiin vastaus hyödyntämällä kehittämistutkimukselle ominaisia menetelmiä, eli yhdistämällä laadullista tutkimusta määrälliseen tutkimukseen.

Tutkimusmenetelmäksi valittiin kehittämistutkimus, koska katsottiin että tutkimusmenetelmän avulla saadaan ratkaistua edellä mainittu tutkimusongelma. Kehittämistutkimus tuki myös laadullisen- ja määrällisen tutkimusmenetelmien käyttöä samassa tutkimuksessa. Muitakin vaihtoehtoisia tutkimusmenetelmiä pohdittiin käytettäväksi, mutta sopivampaa menetelmää tutkimukselle ei löytynyt. Tämä johtunee tutkimuksen olemisesta nimenomaisesti alustava kartoitus, joka on ratkaisu ongelmaan, mutta ei kuitenkaan jatkuva kehittämissykli. Kehittämissyklin toista vaihetta, eli muutossykliä ei päästy sellaisenaan tekemään, koska tutkimuksen aikana ei voitu tietää minkä valinnan Organisaatio X tulee tekemään, eikä siten esimerkiksi toteutusvaiheeseen voitu ottaa kantaa näissä aikarajoissa. Toisaalta kehittämistyön toisena syklinä voidaan nähdä tutkimustyön varsinainen kehitysprosessi, jolloin saatiin ensimmäisen kehityssyklin toteuttamisen jälkeen esimerkiksi toimeksiantajalta tai ohjaajalta palautetta, minkä johdosta työn sisältöä muutettiin tarpeita vastaaviksi. Näiden kehittämistoimenpiteiden pohjalta valmistui loppuarviointiin työ, minkä jälkeen kehitystyötä voidaan jatkaa annettujen jatkokehitysideoiden pohjalta.

Tutkimuskysymyksen vastaukseksi saatiin parhaimmaksi vaihtoehdoksi Organisaatio X:n tarpeisiin Splunkin Enterprise Security -järjestelmä. Järjestelmä vastasi lähestulkoon täydellisesti Organisaatio X:n vaatimuksia, koska tuote oli modulaarinen ja helposti integroitavissa muihin järjestelmiin. Myös helppokäyttöisyys ja lokienhallintaan liittyvät ominaisuudet täsmäsivät vaatimuksiin. Päivittyvät uhkasyötteet sekä laajin

kolmansien osapuolten syötteiden integroitavuus olivat myös tärkeässä roolissa. Ainoa kohta vaatimuslistasta mikä ei sellaisenaan täyttänyt, oli poikkeavaan käyttäytymiseen liittyvät toiminnallisuudet (UEBA), mutta kyseinen moduuli on erikseen integroitavissa alustalle. Kaikki kolme järjestelmää olivat vahvoja vaihtoehtoja, eivätkä ominaisuudet sellaisenaan juurikaan eronneet toisistaan. Ainoa asia mikä selkeästi kävi ilmi SIEM-järjestelmiin perehtyessä, oli IBM QRadarin heikompi käytettävyys käyttöliittymän osalta. LogRhythm erosi muista tuotteista tarjotessaan suoraan SOAR-moduulia tuotteessaan, muissa se oli integroitavissa ja ostettavissa erikseen. Splunkin suosio ja kiinnostavuus kävi selkeästi ilmi asiakkaiden tyytyväisyydessä. Itse hiekkalaatikkoympäristössä Splunk Enterprise Securityä testanneena voin samaistua asiakkaiden antamaan palautteeseen omien havaintojen pohjalta. Uusi laskentatehoon perustuva hinnoittelumalli tulee toimimaan varmasti paremmin organisaatioille, joilla on todella paljon tapahtumia päivän aikana.

Tutkimustyötä tukivat pääkysymyksen lisäksi kaksi alakysymystä: mitä tarkoittaa tilannetietoisuus ja miksi se on tärkeä huomioida osana organisaation turvallisuutta kybertoimintaympäristössä, sekä mikä on uudemman sukupolven SIEM-järjestelmä ja miten sillä kasvatetaan kybertoimintaympäristön turvallisuutta. Näihin saatiin vastaukset laadullisella tutkimusmenetelmällä teoriaosuudessa. Tilannetietoisuus voidaan nähdä tietoisuuden tilana tietyssä ajanhetkessä, johon vaikuttavat ympäristön lukuiset eri elementit, kuten tietojärjestelmät sekä niiden tila. Näiden havaintojen pohjalta tehdään päätökset, esimerkiksi mukaillen Endsleyn teoriaa tai OODA-silmukkaa.

Tilannetietoisuus korreloi suoraan SIEM-järjestelmien toiminnallisuuteen, koska niiden ydintoimintona on havainnointikyvyn kasvattaminen tarkkailemalla kybertoimintaympäristöä, tutkimalla tarkemmin mahdollisia löydöksiä, tekemällä päätökset tältä pohjalta ja valitsemalla toimintatavat päätösten mukaisesti. Kun tilannetietoisuutta ajatellaan laajemmassa mittakaavassa, voidaan ymmärtää, että poikkeamiin voidaan reagoida vain niiden tietojen pohjalta mitä on saatu havainnoitua omasta kybertoimintaympäristöstä. Kun tietoisuus omasta ympäristöstä kasvaa ja tarvittavat valvontamekanismit ovat toteutettuna, saadaan kokonaisvaltaisesti kasvatettua kybertur-

vallisuutta. Uudemman sukupolven SIEM-järjestelmät eroavat vanhemmista ominaisuuksiltaan, eli yleensä nämä ovat kykeneviä suurien datamassojen käsittelyyn, koska tiedot tallennetaan skaalautuviin tietoaltaisiin. Lisäksi koneoppimisen avulla saadaan automatisoitua poikkeamiin reagointia sekä älykkäiden uhkasyötteiden avulla vaihdettua tietoa kansainvälisesti ilmenevistä uhkista ja siten ne voidaan havaita SIEM-järjestelmän avulla omasta ympäristöstä.

Tutkimusaineistoa valitessa pyrittiin käyttämään mahdollisimman tuoreita ja luotettavia lähteitä. Luotettavaksi lähteeksi voidaan nähdä kansainväliset IEEE-julkaisut, lait, standardit, vuosia hyödynnetyt teoriat eri tutkimuksissa ja alalla pitkään olleiden SIEM-valmistajien tuottama yleispätevä materiaali. Lisäksi tutkimuksessa hyödynnettiin Suomen omia kansalliseen- ja kyberturvallisuuteen liittyvää materiaalia, VAHTI-ohjeistuksia sekä KATAKRI-auditointikriteerejä. Käytetyissä blogimerkinnöissä tarkistettiin aina sivuston sekä kirjoittajan taustat. Kirjallisuudessa pyrittiin hyödyntämään myös kriittisyyttä kirjoittajien kesken. SIEM-järjestelmien valmistajien sivustoilta oli vaiheittain haastavaa löytää markkinointilauseiden seasta olennaista tietoa, mutta perehtymällä tarkempiin tuotedokumentaatioihin, videoihin ja manuaaleihin saatiin kuitenkin muodostettua oikeellisempaa kuvaa tuotteista. Tarkempia hinnoittelumallejakaan ei ollut saatavilla kaikista tuotteista suoraan ilman tarjouspyyntöjen lähettämistä, joten tähän ei sen suurempaa huomiota pystynyt kiinnittämään, vaikka se varmasti olisi ollut hyödyllinen tieto myös toimeksiantajalle.

Asiakaskokemuksia tutkiessa markkinointisivustoilla mainittiin, etteivät SIEM-järjestelmien valmistajat pääse vaikuttamaan aineistoihin ja mainitsivat tiedon olevan riippumatonta. Selvittäessä asiaa tarkemmin, piti sivustoille useimmiten kirjautua erikseen ja varmentaa käyttöehdoin etteivät annetut tulokset ole SIEM-järjestelmien edustajilta. Tämä lisää toki vaivaa, mutta mielestäni ei ole täysin absoluuttista, etteivätkö valmistajat halutessaan voisi vaikuttaa tuloksiin. Vertaillessa sivustojen välisiä keskiarvoja, ei niissä ollut kuitenkaan juurikaan vaihtelua, joten mielestäni tämän vuoksi tulokset ovat vähintäänkin suuntaa-antavia ja siten huomioitavan arvoisia. Luotettavin tutkimus näistä oli Gartnerin tuottama tutkimus, koska siinä

oli suurin määrä asiakasarvioita eri valmistajien kesken. Gartnerin tutkimuksia hyödynnetään laajalti myös muissa tutkimuksissa sekä toimijana sillä on vuosien kokemus vastaavista tutkimuksista.

Tutkimuksen luotettavuutta voidaan mitata esimerkiksi sen toistettavuudella, kun kyseessä on määrällinen tutkimus (Kananen 2015, 112). Vaatimustaulukon ja SIEM-järjestelmien ominaisuuksia voidaan verrata uudelleen samoin tuloksin. Tuotearvioinnit voivat tietysti ajan saatossa muuttua ja niihin vaikuttavat myös esimerkiksi tuotteiden ominaisuuksien päivittäminen sekä muut seikat. Tutkimustyön kirjoittamishetkellä kyseiset tutkimukset asiakkaiden kokemuksista kuitenkaan tuskin muuttuvat lyhyen aikavälin sisällä, joten mielestäni on perusteltua pitää tutkimusta luotettavana sen toistettavuuden kannalta. Asiakastyytyväisyyteen tai käyttökokemuksiin vaikuttavat oppiminen sekä tunne- ja kokemusperäiset asiat, jolloin arvio ei välttämättä ole aina sama. Tällaisen asian tutkimisen laajuus on kuitenkin ulkopuolella tästä tutkimuksesta. Laadullisessa tutkimuksessa luotettavuutta voidaan arvioida muun muassa tutkijan tulkinnan perusteella, ilmiön esiintymistavoilla ja tekijöiden määrillä, vahvistettavuudella sekä aineiston rakenteella (Kananen 2015, 94). Luotettavuutta arvioitiin tässä tutkimuksessa pitkälti tutkijan omasta näkökulmasta aineistojen keräämisen yhteydessä. Tietoperusta on tässä työssä laaja ja analysoitu, lisäksi dokumentaatiota on tuotettu perustellen työn eri vaiheissa. Työn vahvistettavuutta on tuettu antamalla tutkimus esimerkiksi toimeksiantajan arvioitavaksi. Nämä seikat ilmaisevat työn luotettavuutta.

Kokonaisuudessaan aihe oli laaja, jolloin aiheen rajaaminen työn alussa oli erittäin tärkeää ja siinä onnistuttiin. Kirjoittamisprosessi opetti tutkimuksesta ja sen menetelmistä paljon, lisäksi tutkimuksen teko antoi syvällisempää ymmärrystä tilannetietoisuuden tärkeydestä sekä uudemman sukupolven SIEM-järjestelmien ominaisuuksista. Omalta osaltaan täysi salassapito toimeksiantajaan liittyen vaikutti tutkimuksen sisältöön rajoittavasti, joten tarkkoja analyysejä esimerkiksi tutkimuksen taustoista ei voinut julkaista. Tutkimuksen eri vaiheissa pyrittiin huomioimaan kyberturvallisuusnäkökulma ja reflektoimaan teorian lisäksi myös omia havaintoja pitkin kirjoitusprosessia. Kirjoitusprosessi oli itsenäistä työtä ja mikäli tutkimustyötä tehtäisiin uudel-

leen, suunnittelisin ja aikatauluttaisin työvaiheet tarkemmalla tasolla, jotta työn tekeminen ei turhaan pitkittyisi. Vaatisin myös enemmän tukea toimeksiantajan puolelta, koska välillä oli haastavaa saada vastauksia tarkentaviin kysymyksiin, mikä osaltaan hidasti tutkimuksen tekemistä. Suorittaisin tarkempia testejä SIEM-järjestelmillä konkreettisesti, koska tässä työssä esimerkiksi käytettävyys jäi muiden kuin Splunk Enterprise Securityn kohdalla melko teoreettiselle tasolle.

Lopputuloksena tutkimustyöstä saatiin koostettu tietopaketti liittyen tilannetietoisuuden kasvattamiseen, uuden sukupolven SIEM-järjestelmien ominaisuuksiin ja arkkitehtuuriin sekä antamalla yleistietoa kolmesta johtavasta SIEM-järjestelmästä. Tutkimuskysymykseen ja sen alakysymyksiin vastattiin, sekä hyödynnettiin monipuolisesti erilaisia lähteitä ja käytettiin kehittämistutkimukselle ominaisia menetelmiä analysoiden lähteiden luotettavuutta. Toimeksiantaja sai itselleen kuvaukset eri SIEM-järjestelmistä toimeksiannon mukaisesti ja ilmaisi tyytyväisyytensä työn lopputulokseen. Myös muut aiheesta kiinnostuneet tai näiden johtavien SIEM-järjestelmien välillä pohtivat saavat tutkimuksesta hyötyä, koska tärkeimmät ominaisuudet ovat kiteytettynä yhteen paikkaan. Näin ollen voi sanoa, että tehtävänannon ja lopputuloksen summana on onnistunut tutkimustyö.

Jatkokehitysideana näkisin SIEM-järjestelmän tai järjestelmien testaamisen suuremmassa testiympäristössä ennen lopullista hankintapäätöstä, mikä ei tässä tapauksessa ollut mahdollista. Testiympäristön avulla saadaan laajempaa kuvaa toimintatavoista ja erilaisin käyttötapauksin voidaan testata soveltuvuus käytännön tasolla organisaation ympäristöön. SIEM-järjestelmän käyttöönoton jälkeen havainnointikyvyn ja tilannetietoisuuden kasvattamista voidaan mitata esimerkiksi haastattelemalla työntekijöitä siitä, onko poikkeamia havaittu normaalia enemmän sekä onko reagointinopeus kasvanut hankitun järjestelmän myötä. Oikein toteutettuna SIEM-järjestelmistä koituva lisäarvo ja tehokkuuden kasvaminen ovat tärkeitä ominaisuuksia laajoissa ja kompleksissa kybertoimintaympäristöissä, joista muutoinkin voi olla haastavaa havaita kyberturvapoikkeamia.

Lähteet

About WMI. 2018. Dokumentti WMI:stä Microsoftin verkkosivustolla 31.5.2018. Viitattu 4.9.2019. https://docs.microsoft.com/en-us/windows/win32/wmisdk/about-wmi.

Adopting Splunk's analytics-driven security platform as your SIEM. 2018. Improve your security posture by using Splunk as your SIEM, 6. Splunkin esittely SIEM-tuotteesta. Viitattu 11.11.2019. https://www.splunk.com/pdfs/white-papers/splunk-as-a-siem.pdf.

Advanced Correlation Engine. 2019. Radar Cyber Securityn artikkeli kehittyneistä korrelaatiomoottereista. Muokattu 30.7.2019. Viitattu 29.7.2019. https://www.radarservices.com/radarplatform/technology/advanced-correlation-engine/.

Astakhova, A. & Muravyov, N. 2019. A Data Collection and Analysis System for Managing the Vulnerabilities of Users of an Information System in a Small Business. IEEE, 2. doi: 10.1109/USBEREIT.2019.8736583. Viitattu 26.7.2019. https://janet.finna.fi, IEEE.

Astakhova. 2019. Radar Cyber Securityn artikkeli kehittyneistä korrelaatiomoottereista. Muokattu 30.7.2019. Viitattu 29.7.2019. https://www.radarservices.com/radarplatform/technology/advanced-correlation-engine/.

Automated Correlation Engine. 2019. Paloalto Networksin artikkeli automatisoiduista korrelaatiomoottoreista. Muokattu 30.7.2019. Viitattu 29.7.2019. https://www.paloaltonetworks.com/features/automated-correlation-engine.

Bhat, M., Biesdorf, A., Manjunath, A., Matthes, F. & Shumaiev, K. 2018. Decision Making and Cognitive Biases in Designing Software Architectures. 2018 IEEE International Conference on Software Architecture Companion (ICSA-C), 52-53. doi: 10.1109/ICSA-C.2018.00022. Viitattu 18.11.2019. https://janet.finna.fi, IEEE.

Bhatt, B., Manadhata, P. & Zomlot, L. 2014. The Operational Role of Security Information and Event Management Systems. IEEE Security & Privacy, 37. doi:10.1109/MSP.2014.103. Viitattu 26.7.2019. https://janet.finna.fi, IEEE.

Blackstratus. 2019. Guide to SIEM and Log Management Solutions-ohje SIEMien ja lokienhallinnan ratkaisuihin. Viitattu 16.8.2019. https://www.blackstratus.com/siem-log-management-solutions/.

Blask, C., Harper, A., Harris, S., Miller, R. & VanDyke, S. 2011. Security Information and Event Management (SIEM) Implementation. Luku 5: The Anatomy of a SIEM, 5. Viitattu 29.7.2019. https://janet.finna.fi, books24x7.

Brook, C. 2018. What is User and Entity Behavior Analytics? A Definition of UEBA, Benefits, How It Works, and More-blogikirjoitus Datainsiderin verkkosivustolla 5.12.2018. Viitattu 24.7.2019. https://digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more.

Bussa, T., Kavanagh, K. & Sadowski, G. 2018. Magic Quadrant for Security Information and Event Management-julkaisu Gartnerin verkkosivustolla 3.12.2018. Viitattu 8.10.2019. https://www.gartner.com/doc/reprints?id=1-5WGR9UB&ct=181205&st=sb.

Calder, A. & Watkins, S. G. 2007. Information Security Risk Management for ISO27001 / ISO17799: Implementing ISO27001. Ely: IT Governance Publishing. Luku 2: Risk Assessment Methodologies. Viitattu 19.9.2019. https://janet.finna.fi, books24x7.

Canner, B. 2019a. Here are the Top 5 Benefits of SIEM for Enterprises-artikkeli Information Security Solutions Reviewin verkkosivustolla. Viitattu 2.8.2019. https://solutionsreview.com/security-information-event-management/here-are-the-top-5-benefits-of-siem-for-enterprises/.

Canner, B. 2019b. What are Vulnerability Management Solutions? Why Do They Matter for SIEM?-artikkeli Information Security Solutions Reviewin verkkosivustolla. Viitattu 24.7.2019. https://solutionsreview.com/security-information-event-management/what-are-vulnerability-management-solutions-why-do-they-matter-for-siem/.

Casad, J. & Willsey, B. 1999. TCP/IP. Suomenkielisen version on kääntänyt Samela Juha Helsinki: IT Press. Englanninkielinen versio julkaistu nimellä Teach yourself TCP/IP in 24 hours, SAMS Publishing 1998. Osa 2, 22-107. Viitattu 19.9.2019.

Chapman, B. & Maymi, F. 2018. CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). Julkaistu 2018 McGraw-Hill Educationin toimesta. Kappale 13 Putting in Compensating controls, Data aggregation and correlation. Viitattu 22.8.2019. https://janet.finna.fi, books24x7.

Chuvakin, A. 2016. The Complete Guide to Log and Event Management. NetIQ:n kustantama julkaisu 2016 lokien- ja tapahtumienhallinnasta. Viitattu 30.8.2019. https://www.microfocus.com/media/white-paper/the_complete_guide_to_log_and_event_management_wp.pdf.

Chuvakin, A., Phillips, C. & Schmidt, K. 2013. Logging and Log Management, The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngressin julkaisu 2013. Viitattu 4.9.2019. Luvut 1 ja 3. https://janet.finna.fi, books24x7.

Cloud SIEM Solutions. 2019. Blogikirjoitus pilvipohjaisista SIEM-ratkaisuista Solarwindsin verkkosivustolla 13.3.2019. Viitattu 1.8.2019. https://www.solarwindsmsp.com/blog/cloud-siem-solutions.

Compliance Solutions. N.d. Esittely LogRhythmin SIEM-tuotteeseen sisältyvistä raporteista liittyen säädöksiin ja standardeihin. Viitattu 7.11.2019. https://logrhythm.com/solutions/compliance/.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 2013. Council of European Union, Bryssel 8.2.2013. Viitattu 21.8.2019. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206225%202013%20INIT.

Dietz, S. 2018. Beyond SIEM: Evolving Correlation-artikkeli kyberturvallisuuteen erikoistuneen Jask:in verkkosivustolla 13.6.2018. Viitattu 31.8.2019. https://jask.com/beyond-siem-evolving-correlation/.

Dunkerley, D. & Rogers, B. 2016. CRISC Certified in Risk and Information Systems Control All-in-One Exam Guide, McGraw-Hill Education. Luku 1: Risk Concepts. Viitattu 18.9.2019. https://janet.finna.fi, books24x7.

Dwivedi, H. 2004. Implementing SSH: Strategies for Optimizing the Secure Shell. Wiley Publishing, Inc. Luku 1. Viitattu 4.9.2019. https://janet.finna.fi, books24x7.

Enck, R.E. 2012. The OODA Loop. Artikkeli OODA-loopista. Julkaistu 21.3.2012, 1, 3, 123-124. doi: 10.1177/1084822312439314. Viitattu 18.11.2019. https://doi.org/10.1177/1084822312439314.

Endsley, M. 1995. Toward a Theory of Situtation Awarness in Dynamic Systems. Researchgaten verkkosivustolla, 8-64. doi: 10.1518/001872095779049543. Viitattu 15.8.2019. https://www.researchgate.net/publication/210198492_Endsley_MR_Toward_a_Theory_of_Situation_Awareness_in_Dynamic_Systems_Human_Factors_Journal_371_32-64.

Endsley, M. 2015. Situation Awareness Misconceptions and Misunderstandings-julkaisu 24.2.2015, 9, 1, 8-10. doi: 10.1177/1555343415572631. Viitattu 21.8.2019. https://doi.org/10.1177/1555343415572631.

Evesti, A., Frantti, T. & Kanstrén, T. 2017. Cybersecurity situational awareness taxonomy-tutkimus. IEEE International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) 2017, 3-5. doi:10.1109/CyberSA.2017.8073386. Viitattu 29.7.2019. https://janet.finna.fi, IEEE.

Filkins, B. 2019. SANS Institute, Information Security Reading Room. An evaluator´s Guide to NextGen SIEM, 3-15. Viitattu 15.8.2019. https://www.sans.org/reading-room/whitepapers/analyst/evaluator-039-s-guide-nextgen-siem-38720.

G2. N.d. Teknologioiden markkinointialusta. Tuotearvosteluja eri SIEM-tuotteista. Osiot: About, Security Information and Event Management (SIEM) Software. Viitattu 1.12.2019. https://www.g2.com/categories/system-security.

Goldhammer, S. 2016. A Day in the Life of an Analyst | LogRhythm Demo 22.12.2016. Verkkovideo LogRhythmin SIEM-tuotteesta SOC-analyytikon näkökulmasta. Lataaja LogRhythm. Viitattu 3.12.2019. https://www.youtube.com/watch?v=9TRqZuZqtKY.

Government of Canada Cyber Security Event Management Plan (GC CSEMP). 2018. Kanadan valtionhallinnon kyberturvallisuustapahtumien hallintasuunnitelma. Viitattu 29.7.2019. https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html.

Humphries, S. 2019. Threat Intelligence Feeds: Keeping Ahead of the Attacker-blogikirjoitus SIEMeihin erikoistuneen Exabeamin verkkosivustolla 15.10.2019. Viitattu 3.12.2019. https://www.exabeam.com/siem/threat-intelligence-feeds/.

IBM Knowledge Center. 2017. IBM QRadar Security Intelligence Platform V7.3.0 documentation. Dokumentaatio QRadarin toiminnallisuuksista IBM:n verkkosivustolla.

Viitattu 3.12.2019. https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/qradar_IC_welcome.html.

IBM QRadar SIEM Tuning: Introduction to QRadar and Tuning. 2017. Demo Qradarista. Lataaja: IBM Security Support. Viitattu 9.12.2019. https://www.youtube.com/watch?v=UL-2KDDGXJk.

IBM QRadar SIEM Tuning: Offense Basics. 2018. Demo Offences-korttien toiminnasta 27.3.2018. Lataaja: IBM Security Support. Viitattu 9.12.2019. https://www.youtube.com/watch?v=UL-2KDDGXJk.

Ilin, R. & Rogova, G. L. 2019. Reasoning and Decision Making under Uncertainty and Risk for Situation Management. 2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), 34. doi: 10.1109/COGSIMA.2019.8724330. Viitattu 18.11.2019. https://janet.finna.fi, IEEE.

IT Central Station. 2019. Compare IBM QRadar vs. LogRhythm NextGen SIEM vs. Splunk. Viitattu 1.12.2019. https://www.itcentralstation.com/products/comparisons/ibm-qradar_vs_logrhythm-nextgen-siem_vs_splunk.

Iversen, M. 2018. SIEM, meet APIs: Why APIs are critical for security operations-artikkeli TechBeaconin verkkosivustolla. Kirjoittaja on vanhempi tietoturvallisuuteen perehtynyt insinööri. Viitattu 2.10.2019. https://techbeacon.com/security/why-apis-are-critical-security-operations.

Jyotiprakash, S. 2017. Five Advantages of Cloud-Based SIEM for Security Intelligence and Operations-artikkeli Security Intelligencen verkkosivustolla 22.9.2017. Viitattu 1.8.2019. https://securityintelligence.com/five-advantages-of-cloud-based-siem-for-security-intelligence-and-operations/.

Kananen, J. 2015. Kehittämistutkimuksen kirjoittamisen käytännön opas. Miten kirjoitan kehittämistutkimuksen vaihe vaiheelta. Jyväskylän Ammattikorkeakoulun julkaisuja 212, 24-112. Jyväskylä: Jyväskylän ammattikorkeakoulu. Viitattu 12.11.2019. https://janet.finna.fi, booky.fi.

Kansallinen riskiarvio 2018. 2019. Sisäinen turvallisuus, sisäministeriön julkaisuja 2019:5, Helsingissä 20.1.2019, 18. Viitattu 13.8.2019. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161332/5_2019_Kansallinen%20riskiarvio.pdf.

Karkimo, A. 2019. ESS: Haittaohjelma aiheuttanut jo liki 700 000 euron laskun Lahdessa – tuskin riittää. Uutinen 9.8.2019 Tivin verkkosivustolla. Viitattu 1.12.2019. https://www.tivi.fi/uutiset/ess-haittaohjelma-aiheuttanut-jo-liki-700-000-euron-laskun-lahdessa-tuskin-riittaa/f0211b31-52a0-4743-94bd-758dbd4cfd17.

KATAKRI. 2015. Kansallinen turvallisuusauditointikriteeristö. Tietoturvallisuuden auditointityökalu viranomaisille, 3-57. Viitattu 26.7.2019. https://www.defmin.fi/files/1525/Katakri.pdf.

Koecher, I. 2017. Agent vs Agentless: Why you should monitor (event) logs with an agent-based log monitoring solution-blogikirjoitus lokiagenttien käytöstä. Viitattu 10.7.2019. https://www.eventsentry.com/blog/2017/03/agent-vs-agentless-why-you-should-monitor-event-logs-with-an-agent-based-log-monitoring-solution.html.

Kuusisto, R. 2005. Liikenne- ja viestintäministeriön julkaisuja 81/2005. Tilannekuvasta täsmäjohtamiseen, johtamisen tietovirrat kriisin hallinnan verkostossa, 10-11. Julkaistu Helsingissä 16.11.2005. Viitattu 22.8.2019. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78700/Julkaisuja_81_2005.pdf?sequence=1.

Kuusisto, T. 2014. Kybertaistelu 2020. Toim. Tuija Kuusisto Helsingissä 2014. Maanpuolustuskorkeakoulu, taktiikan laitos. Julkaisusarja 2, No. 1/2014, 67. Tampere: Juvenesprint. Viitattu 12.8.2019. http://www.doria.fi/bitstream/handle/10024/103034/Kybertaistelu2020%28net%29.pdf?sequence=2&isAllowed=y.

Kyberturvallisuuden sanasto. 2018. Turvallisuuskomitea. Sanastokeskus TSK ry:n julkaisu, 21-29. Viitattu 29.7.2019. http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf.

Kyberturvallisuus ja kybertoimintaympäristö. 2019. Ulkoministeriön verkkojulkaisu kyberturvallisuudesta. Viitattu 15.8.2019. https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto.

L (EU) 679/2016. GDPR (General Data Protection Regulation), EU:n tietosuoja-asetus henkilötietojen käsittelystä. Viitattu 15.11.2019. https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504.

L 906/2019. Laki julkisen hallinnon tiedonhallinnasta. Viitattu 29.11.2019. https://www.finlex.fi/fi/laki/alkup/2019/20190906.

LogRhythm NextGen SIEM Platform. N.d. Logrhythmin esittely heidän SIEM-tuotteestaan. Osiot: DetectX, RespondX, AnalytiX. Viitattu 14.11.2019. https://logrhythm.com/products/nextgen-siem-platform/.

LogRhythm Releases First True Unlimited Data Plan for SIEM. 2019. Artikkeli hinnoittelumallista LogRhythmin verkkosivustolla. Viitattu 12.12.2019. https://logrhythm.com/press-releases/logrhythm-releases-first-true-unlimited-data-plan-for-siem/.

Lokien keräys ja käyttö. 2016. Viestintäviraston ohje 4/2016 lokien keräämisestä ja käytöstä, 2-7. Viitattu 16.8.2019. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitusohje.pdf.

Martin, J.L., McPherson, R., Miyamoto, I. & Talabis, M. 2015. Information Security Analytics – Finding Security Insights, Patterns and Anomalies in Big Data. Waltham: Syngress 2015. Luku 1: Analytics defined. Viitattu 24.9.2019. https://janet.finna.fi, books24x7.

Miessler, D. 2017. The Difference Between Events, Alerts, and Incidents-artikkeli kyberturvallisuuteen erikoistuneen Daniel Miesslerin verkkosivustolla 15.11.2017. Viitattu 16.7.2019. https://danielmiessler.com/study/event-alert-incident/.

Monge, M. 2019. SIEM Event Normalization Makes Raw Data Relevant to Both Humans and Machines-artikkeli tapahtumien normalisoinnista 8.1.2019. Viitattu 9.9.2019. https://securityintelligence.com/siem-event-normalization-makes-raw-data-relevant-to-both-humans-and-machines/.

Näin keräät ja käytät lokitietoja. 2019. Liikenne- ja viestintäministeriö, Traficom, Kyberturvallisuuskeskus. Artikkeli lokitiedoista 5.7.2019 Traficomin verkkosivustolla. Viitattu 30.8.2019. https://www.kyberturvallisuuskeskus.fi/fi/nain-keraat-ja-kaytat-lokitietoja.

Operationalize Security Intelligence. 2019. Splunk Enterprise Security- tuotteen ominaisuudet. Muokattu 10.11.2019. Viitattu 11.11.2019. https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/features.html.

Petters, J. 2019. What is SIEM? A Beginner's Guide. Blogikirjoitus kyberturvaratkaisuihin erikoistuneen Varoniksen verkkosivustolla SIEMin perusteista 4.6.2019. Viitattu 28.7.2019. https://www.varonis.com/blog/what-is-siem/.

PiTuKRI. 2019. Pilvipalveluiden turvallisuuden audintointikriteeristö. Liikenne-ja viestintävirasto, Traficom, Kyberturvallisuuskeskus. Julkaistu huhtikuussa 2019, versio 1.0, 9-16. Viitattu 1.8.2019. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri.pdf.

Ponemon, L. 2019. What's New in the 2019, Cost of a Data Breach Report. IBM Security. Julkaistu Security Intelligencen verkkosivustolla 23.7.2019. Viitattu 2.12.2019. https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/.

Pratt, M.K. 2017. What is SIEM software? How it works and how to choose the right tool. Artikkeli CSO:n verkkosivustolla 28.9.2017. Viitattu 28.8.2019. https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html/.

Pros and cons of outsourcing your Cyber Security - In-house, MSSP, or Virtual SOC? 2017. Blogikirjoitus Comtactin verkkosivustolla organisaation sisäisen kyberturvallisuuden toteuttamiseen liittyviin hyötyihin ja haittoihin 22.9.2017. Viitattu 1.8.2019. https://www.comtact.co.uk/blog/pros-and-cons-of-outsourcing-your-cyber-security-in-house-mssp-or-virtual-soc.

Rantanen, H. 2018. Tilannekuvan tuottaminen, hyödyntäminen ja jakaminen. Kriittinen nykytilan tarkastelu. Aluehallintovirastojen julkaisuja 48/2018, 3. Vaasa 2018. Viitattu 29.7.2019. https://www.avi.fi/documents/10191/10616116/Julkaisu-42_20180713.pdf/52e3bb5b-f40d-4fcc-8a93-9ab735c3028e.

Saurabh, K. 2017. To rule or not to rule: SIEMs and their false positives-artikkeli CSO:n verkkosivustolla SIEMin säännöstöjen hyvistä ja huonoista puolista 18.10.2017. Viitattu 16.8.2019. https://www.csoonline.com/article/3233869/to-rule-or-not-to-rule-siems-and-their-false-positives.html.

Security Information and Event Management Market. 2019. Gartnerin Peer Insight-arvostelut eri SIEM-tuotteista. Viitattu 22.11.2019. https://www.gartner.com/reviews/market/security-information-event-management.

Security Orchestration, Automation and Response. 2019. Tietoa SOAR-tuotteesta LogRhythmin verkkosivustolla. Muokattu 19.8.2019. Viitattu 23.8.2019. https://logrhythm.com/solutions/security/security-automation-and-orchestration/.

SFS-EN ISO/IEC 27000:2017. Aihealueet: Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki: Suomen Standardisoimisliitto SFS, 5. Vahvistettu 3.3.2017. Viitattu 21.11.2019. https://janet.finna.fi, SFS Online.

SFS-EN ISO/IEC 27001:2017. Aihealueet: Informaatioteknologia, turvallisuustekniikat, tietoturvallisuuden hallintajärjestelmät, vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS, 8. Vahvistettu 3.3.2017. Viitattu 20.9.2019. https://janet.finna.fi, SFS Online.

SFS-ISO/IEC 27035-1:2016. Aihealueet: Informaatioteknologia, turvallisuustekniikat, tietoturvapoikkeamien hallinta. Osa 1: Principles of incident management, 3. Sveitsi: ISO copyright office. Viitattu 20.9.2019. https://janet.finna.fi, SFS Online.

Shashanka, M., Shen, M. & Wang, J. 2016. User and entity behavior analytics for enterprise security. 2016 IEEE International Conference on Big Data (Big Data), 6-7. doi: 10.1109/BigData.2016.7840805. Viitattu 26.7.2019. https://janet.finna.fi, IEEE.

SIEM-guide. 2019. Artikkeli kyberturvallisuuteen ja SIEM-järjestelmiin erikoistuneen Exabeamin verkkosivustolla. Luku 1: What is SIEM, luku 2: SIEM Architecture, luku 3: Events and logs, luku 4: UEBA. Viitattu 24.7.2019. https://www.exabeam.com/siem-guide/.

Situational Awareness. 2016. CRR Supplemental Resource Guide-julkaisu CISAn verkkosivustolla. Carnegie Mellon University, Vol. 10, Situational Awareness, Version 1.1. Viitattu 20.8.2019. https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-SA.pdf.

Splunk® Enterprise Security. N.d. Tuote-esittely Splunkin verkkosivustolla. Osiot: Splunk Enterprise Security, Splunk for Security. Viitattu 9.12.2019. https://www.splunk.com/en_us/software/enterprise-security.html.

Suomen kansallinen riskiarvio 2015. 2016. Sisäinen turvallisuus, sisäministeriön julkaisu 3/2016, Helsingissä 26.1.2016, 20. Viitattu 13.8.2019. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/64948/Kansallinen_riskiarvio_2015_fi_FINAL_4.pdf.

Suomen kyberturvallisuusstrategia. 2013. Valtioneuvoston periaatepäätös 24.1.2013, Turvallisuuskomitea, 7. Viitattu 29.7.2019. https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf.

Suomen kyberturvallisuusstrategia. 2019. Valtioneuvoston periaatepäätös 3.10.2019. Turvallisuuskomitea, 7. Viitattu 5.11.2019. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf.

Tchesnokov, S. 2016. Managing information security risks with a SIEM solution-artikkeli Continuity Centralin verkkosivustolla 13.9.2016. Viitattu 10.9.2019. https://www.continuitycentral.com/index.php/news/technology/1389-managing-information-security-risks-with-a-siem-solution.

The IBM QRadar Security Intelligence Platform. 2019. IBM Corporation, IBM Security. IBM QRadar SIEM-tuotteen esittely. Viitattu 15.11.2019. https://www.ibm.com/downloads/cas/W18VL4QG.

TrustRadius. N.d. Security Information and Event Management (SIEM) Software. SIEM-järjestelmien asiakasarvosteluja. Osiot: LogRhythm NextGen SIEM Platform, Splunk Enterprise, IBM QRadar. Viitattu 1.12.2019. https://www.trustradius.com/security-information-event-management-siem#products.

VAHTI. 2009. VAHTI-ohje: Tietoturvapoikkeamiin varautuminen, 2.1-2.2. Viitattu 9.9.2019. https://www.vahtiohje.fi/web/guest/tietoturvapoikkeamiin-varautuminen.

VAHTI. 2010. VAHTI-ohje: Tietoaineistelujen luokittelu. Viitattu 13.11.2019. https://www.vahtiohje.fi/web/guest/tietoaineistojen-luokittelu.

Waitt, T. 2019. SIEM, UEBA, and SOAR – What's the Difference?-artikkeli American Security Todayn verkkosivustolla 21.3.2019. Viitattu 24.8.2019. https://americansecuritytoday.com/siem-ueba-and-soar-whats-the-difference/.

Wang, J. 2017. Understanding IntroSpect's Modular, Data-Agnostic and Scalable UEBA Architecture-blogikirjoitus Aruban (Hewlet Packard Enterprise company) verkkosivustolla 31.10.2017. Viitattu 24.7.2019. https://blogs.arubanetworks.com/industries/understanding-introspects-modular-data-agnostic-and-scalable-ueba-architecture/.

What is Machine Learning? A definition. 2017. Artikkeli koneoppimisesta tekoälyyn keskittyneen Expert Systemsin verkkosivustolla 5.10.2017. Viitattu 16.8.2019. https://www.expertsystem.com/machine-learning-definition/.

What is SSL, TLS and HTTPS? 2019. Artikkeli SSL, TLS ja HTTPS-protokollista Symantecin verkkosivustolla. Muokattu 5.9.2019. Viitattu 6.9.2019. https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-https.

Vulnerabilities. 2019. NISTin määritelmä haavoittuvuudelle NVD-osiossa. Viitattu 10.9.2019. https://nvd.nist.gov/vuln.

Yhteiskunnan turvallisuusstrategia. 2017. Yhteiskunnan turvallisuus. Valtioneuvoston periaatepäätös 2.11.2017. Turvallisuuskomitea, 15-25. Viitattu 30.7.2019. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf.

Liitteet

Liite 1. Splunkin, IBM QRadarin ja LogRhythmin vertailu (Splunk® Enterprise Security n.d; IBM Knowledge Center 2017; LogRhythm NextGen SIEM Platform n.d.)

Ominaisuus	Splunk Enterprise Security	IBM Qradar	LogRhythm SIEM
Metriikka ja ohjausnäkymä			
Mukautettujen näkymien luominen	x	x	x
Reaaliaikaiset päivitykset	x	x	x
Roolipohjaiset näkymät	x	x	x
Monipuoliset hakutoiminnot	x	x	x
Intuitiivinen ja käytettävä	x		x
Lait, standardit ja säädökset			
Valmiit raporttipohjat	x	x	x
Valmiit korrelointisäännöt	x	x	x
Hälytys, kun säännöstöä rikotaan	x	x	x
Lokienhallinta			
Lokitietojen kerääminen eri lähteistä	x	x	x
Lokitietojen eheyden valvonta	x	x	x
Verkkoliikenteen nauhoittaminen ja varastointi	x	x	x
Agentiton/agentillinen keräin	x	x	x
Lokien normalisointi ja aikaleimaus	x	x	x
Vikasietoisuus	x	x	x
Luotettava lokien välittäminen	x		x
Lokitietojen käsittelystä jää merkintä	x	x	x
Tapahtumien havainnointi, analytiikka ja visualisointi			
Sääntöpohjainen korrelointi	x	x	x
Useiden laitteiden ja kompleksisten tapahtuminen korrelointi	x	x	
Tulosten ja löydösten graafinen visualisointi	x	x	x
Uhkasyötteiden / IOCien reaaliaikainen päivittyminen	x	x	x
Tapahtumakaavojen havaitseminen datalähteestä tai tyypistä riippumatta	x	x	x
Käyttäytymisen analysointiin pohjautuva poikkeamien havainnointi	(x)	(x)	(x)
Työkulun hallinta			
Ongelmatikettien generointi	x	x	x
Mukautettujen työjonojen luominen	x	x	x
Automatisoidut/manuaaliset vasteet	x	x	x
Hälytykset ja ilmoitukset			
Reaaliaikaiset hälytykset ja ilmoitukset	x	x	x
Hälytysilmoitukset eri kanavien kautta	x	x	x
Tukipalvelut			
Käyttöönotto, koulutus ja ylläpito	x	x	x
Asiakastuki	x	x	x