Riskiperusteinen tietoturvatapahtumien koneellinen kiireellisyysluokittelu

Ville Salmela

2019 Laurea

Laurea-ammattikorkeakoulu

Riskiperusteinen tietoturvatapahtumien koneellinen kiireellisyysluokittelu

Ville Salmela
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Kesäkuu, 2019

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma
Tradenomi (AMK)

Ville Salmela

Riskiperusteinen tietoturvatapahtumien koneellinen kiireellisyysluokittelu

Vuosi 2019 Sivumäärä 42

Tietoturvavalvonnan kysyntä on kasvussa, minkä ansiosta tietoturvavalvomoiden työkuorma lisääntyy. Jotta toimeksiantaja pystyisi paremmin vastaamaan kasvavaan kysyntään, tässä työssä pyritään tehostamaan tietoturvavalvomon toimintaa luomalla menetelmä tietoturvatapahtumien koneelliseen kiireellisyysluokitteluun.

Kiireellisyysluokittelua varten on tarpeen määrittää jokaisen tietoturvatapahtuman riskitaso, perustuen sen piirteisiin. Opinnäytetyön tavoitteena oli tunnistaa piirteistä oleellisimmat ja luoda systemaattinen malli niiden mittaamiseen. Kun kiireellisyysluokittelu koneellistetaan, tietoturvavalvonnan prosessista poistuu yksi manuaalinen työvaihe, jonka ansiosta työn tehokkuus kasvaa ja inhimillisten tekijöiden vaikutus toimintaan vähenee.

Työn toteuttaminen tehtiin neljässä vaiheessa. Ensimmäisessä vaiheessa tunnistettiin sille asetettavat vaatimukset työn tavoitteiden ja toimeksiantajan tarpeiden pohjalta. Toisessa vaiheessa tunnistettiin erilaisia tietoturvatapahtumia kuvailevia piirteitä käyttäen menetelminä dokumenttianalyysiä ja miellekarttoja. Kolmannessa vaiheessa piirteet luokiteltiin kategorioihin, joka mahdollistaa riskitason koneellisen laskemisen. Neljännessä vaiheessa muodostettiin asteikot mittaamista varten.

Työn tuloksena tunnistettiin 12 mitattavaa piirrettä ja muodostettiin asteikot, joiden perusteella tietoturvatapahtuman riskitaso voidaan arvioida koneellisesti. Riskitason määritysmenetelmän käyttöönoton jälkeen tietoturvavalvomon on vielä sovitettava arviointikriteerit käytettävissä oleviin resursseihin ja tavoitteisiin siten, että tietyn kiireellisyysluokan tietoturvatapahtumat on mahdollista käsitellä tavoiteajassa.

Työn aikana tunnistettiin jatkokehityskohteita, joita on määrä seurata ja kehittää menetelmän käyttöönoton yhteydessä ja sen jälkeen. On selvitettävä, kuinka hyvin koneellisesti laskettu arvio tietoturvatapahtuman riskitasosta vastaa ammattilaisen arviota. Lisäksi on pyrittävä kehittämään tietoturvatapahtuman piirteiden mittausmenetelmiä tarkemmiksi, mieluiten kohti objektiivista mittausta.

Asiasanat: mittaus, priorisointi, SIEM, tietoturva

Laurea University of Applied Sciences
Degree Programme in Security Management
Bachelor's Thesis

Ville Salmela

Abstract

Automated Risk-based Prioritization of Information Security Events

Year 2019 Pages 42

In today's computerized operating environment, an increasing number of enterprises is willing to protect their digital assets by subscribing to an information security monitoring service from a security operations center (SOC). This trend is straining the resources of one particular SOC, and as a commission for them, this thesis aims to alleviate the strain by increasing the efficiency of handling information security events.

It was identified that in order to increase the efficiency, the prioritization of information security events needs to be automated. For that to be possible, first it is necessary to accurately calculate risk levels for each event based on its attributes. Therefore, the thesis had the objective to identify those information security event attributes, which are most relevant in relation to the risk level. The second objective was to develop a measuring model for systematic measuring of the previously identified event attributes. It is estimated that automating the prioritization process has two main advantages. It is faster, and it reduces the influence of human factors, thus providing more speed and consistent quality.

The thesis was completed in four phases. In the first phase, requirements for the work were defined based on the commissioner's needs and thesis objectives. During the second phase, information security event attributes were identified using the document analysis and mind mapping techniques. The third phase classified the attributes into different categories, as required by the supporting systems. In the fourth and final phase, scales for measurement were defined and documented.

As a result, 12 information security event attributes were identified and a measurement scale for each one was defined. After the new automated prioritization method has been deployed, there will still be tasks that need to be completed so that the method can be utilized effectively. The calculated risk levels must be aligned with priority decision criteria, taking into account available resources and target handling times for each priority.

After the deployment of the new prioritization method, there remain issues that require further attention. Firstly, the commissioner should closely monitor the accuracy of automatically calculated risk levels and compare them with ones estimated by security professionals. Secondly, it was identified that the chosen subjective measurement methods should be developed to be more accurate, preferably so that objective measurements can be reached.

Keywords: information security, measurement, prioritization, SIEM

Sisällys

1 Johdanto

Liiketoimintaympäristön digitalisoitumisen edetessä organisaatioiden toiminnot muuttuvat yhä enemmän riippuvaisiksi tietoverkoista ja -järjestelmistä. Suojellakseen toimintansa jatkuvuutta ja lieventääkseen tieto-omaisuuteen kohdistuvia riskejä, yhä useampi organisaatio päättää ostaa tietoturvahäiriöiden hallintapalvelua tietoturvapalveluita tarjoavalta yritykseltä.

Tämä toiminnallinen opinnäytetyö tehtiin yhteistyössä tietoturvapalveluita tarjoavan yrityksen kanssa. Yritys esiintyy tässä työssä anonyymisti, ja siihen viitataan sanalla toimeksiantaja.

Opinnäytetyölle asetettu strategisen tason tavoite oli parantaa tietoturvahäiriöiden hallintapalvelun tehokkuutta, jotta toimeksiantaja pystyy paremmin vastaamaan palvelun kasvavaan kysyntään.

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantaja tarjoaa asiakkailleen tietoturvavalvontaa jatkuvana palveluna. Tietoturvavalvontaa suorittaa toimeksiantajan operoima tietoturvavalvomo, jossa työskentelevät tietoturva-analyytikot vastaavat palvelun ympärivuorokautisesta toiminnasta.

Tietoturvavalvontaan kuuluu tietoturvatapahtumien tunnistaminen ja arviointi, ja se on osa tietoturvahäiriöiden hallintapalvelua, johon sisältyy myös tietoturvavalvonnan suunnittelu, valvonnassa käytetyn järjestelmän ylläpito, sekä tunnistettujen tietoturvahäiriöiden raportointi ja hallinta.

1.2 Kehitystarve

Tietoturvavalvontaa käytetään tietoturvariskien hallintakeinona. Jotta hallintakeinon tehokkuus saadaan maksimoitua, on tarkoituksenmukaista reagoida havaittuihin tietoturvatapahtumiin niiden riskitason perusteella siten, että ensimmäisenä käsitellään korkeariskiset tapahtumat.

Kun arvioimista odottavia tietoturvatapahtumia on useampi kuin yksi, tietoturvavalvomon henkilökunnan tulee päättää, missä järjestyksessä ne käsitellään. Opinnäytetyötä edeltävässä tilanteessa käsittelyjärjestyksen muodostamiseen on käytetty manuaalista menetelmää, jossa tietoturva-analyytikko arvioi riskitason tapauskohtaisesti. Arvio on tehty tietoturvatapahtuman metatietojen perusteella, hyödyntäen kokemuksen kautta karttunutta subjektiivista arviointikykyä.

Tietoturvatapahtumien määrän kasvaessa merkittävästi, subjektiivisen arviointimenetelmän tarkkuus laskee, sillä ihmisen tiedonkäsittelykapasiteetti ei riitä kaiken saatavilla olevan

tiedon käsittelyyn tällä manuaalisella menetelmällä. Kun tietoturvatapahtumia ei voida luotettavasti asettaa järjestykseen riskin suuruuden perusteella, korkeariskisten tapahtumien käsittelyn aloittamiseen saattaa kulua tarpeettoman kauan aikaa.

1.3 Tavoitteet

Tämän opinnäytetyön tavoitteena oli kehittää menetelmä tietoturvatapahtumien koneelliseen kiireellisyysluokitteluun. Koneellista kiireellisyysluokittelua varten on tarpeen määrittää jokaisen tietoturvatapahtuman riskitaso, ja tätä varten on tunnistettava tarkoitukseen sopivat tietoturvatapahtuman piirteet sekä luotava edellytykset niiden automaattiseen mittaamiseen.

Siirtymällä tietoturvatapahtumien riskitason koneelliseen arviointiin, pyritään saavuttamaan seuraavia tehokkuuteen liittyviä hyötyjä:

- tietoturvatapahtumien määrän kasvaminen ei heikennä riskitasoarvion luotettavuutta,
- riskitasoarvion tekemiseen kuluu nykyistä vähemmän työaikaa.

Lisäksi tunnistettiin yksi palvelun laatuun liittyvä hyöty:

- inhimillisten tekijöiden vaikutus riskitasoarvioon vähenee, joten tuotettu palvelu on nykyistä tasalaatuisempaa.

Jotta opinnäytetyö vastaisi asetettuihin tavoitteisiin, luotiin tavoitteita vastaavat tutkimuskysymykset:

- Mitä tietoturvatapahtuman piirteitä tulee tarkastella, jotta voidaan luotettavasti arvioida sen riskitaso?
- Millainen mittausmalli soveltuu edellä mainittujen piirteiden koneelliseen mittaamiseen?

Kun tietoturvatapahtuman riskitaso on luotettavasti määritelty, sitä voidaan käyttää koneelliseen kiireellisyysluokitteluun. Kiireellisyysluokittelun tehostuminen tukee strategisen tason tavoitetta, eli sen ansiosta tietoturvavalvomo pystyy paremmin vastaamaan palvelun kasvavaan kysyntään.

Yhdessä toimeksiantajan kanssa tarkensimme tavoitteita siten, että kehitettävän menetelmän on oltava hyvin skaalautuva, mahdollisimman automaattinen, ja sen on hyödynnettävä toimeksiantajalla käytössä olevan valvontajärjestelmän ominaisuuksia.

Oheinen taulukko (Taulukko 1) kokoaa yhteen opinnäytetyön tavoitteet, tutkimuskysymykset ja toimeksiantajalle syntyvät hyödyt.

Strategisen tason tavoite	Parantaa tietoturvahäiriöiden hallintapalvelun tehokkuutta, jotta toimeksiantaja pystyy paremmin vastaamaan kasvavaan kysyntään.
Päätavoite	Kehittää menetelmä tietoturvatapahtumien koneelliseen kiireellisyysluokitteluun riskitason perusteella.
Alitavoitteet	Tunnistaa ne tietoturvatapahtuman piirteet, jotka oleellisesti vaikuttavat sen riskitasoon.
	Kehittää mittausmalli edellä mainittujen piirteiden mittaamiseen.
Tutkimuskysymykset	Mitä tietoturvatapahtuman piirteitä tulee tarkastella, jotta voidaan luotettavasti arvioida sen riskitaso?
	Millainen mittausmalli soveltuu edellä mainittujen piirteiden koneelliseen mittaamiseen?
Hyödyt	Tietoturvatapahtumien lukumäärän kasvaminen ei heikennä riskitasoarvion luotettavuutta.
	Riskitaso-arvion tekemiseen kuluu nykyistä vähemmän työaikaa.
	Inhimillisten tekijöiden vaikutus riskitasoarvioon vähenee, joten tuotettu palvelu on nykyistä tasalaatuisempaa.

Taulukko 1 - Opinnäytetyön tavoitteet

1.4 Rajaus

Tässä opinnäytetyössä keskitytään riskitason määrittämismenetelmän kehittämisprosessin raportointiin. Menetelmän tarkka tekninen kuvaus jätetään työn ulkopuolelle toimeksiantajan toivomuksesta, sillä se on liikesalaisuus.

1.5 Rakenne

Tämän opinnäytetyön toisessa luvussa määritellään työssä esiintyvät keskeisimmät käsitteet. Käsitteiden määrittely luo pohjan toimintaympäristön sekä teoreettisen viitekehyksen ymmärtämiselle. Toimintaympäristö kuvataan luvussa kolme ja teoreettinen viitekehys luvussa neljä.

Viidennessä luvussa esitellään opinnäytetyön toteutuksessa käytetyt menetelmät sekä kuvataan opinnäytetyöprosessin eri vaiheet. Kuudennessa luvussa kuvaillaan opinnäytetyössä kehitettyä tietoturvatapahtumien riskitason määritysmenetelmää.

Seitsemännessä luvussa arvioidaan toimeksiantajalta saadun palautteen perusteella opinnäytetyön onnistumista ja sitä, kuinka hyvin se vastaa sille asetettuihin tavoitteisiin. Lopuksi kootaan yhteen työn aikana esiin nousseet jatkokehitystarpeet.

2 Keskeiset käsitteet

Tässä luvussa määritellään työssä esiintyvät keskeiset käsitteet ja esitellään niiden merkitys tämän opinnäytetyön asiayhteydessä. Käsitteet on jaettu kolmeen eri aihealueeseen: tietoturvavalvonta, riskienhallinta ja mittaaminen. Käsitteiden määrittelyn apuna on käytetty ISO27000 standardisarjaa, VAHTI-julkaisuja ja SIEM-järjestelmän valmistajan dokumentaatiota.

2.1 Riskienhallinta

Tietoturvavalvonta on osa organisaatioiden riskienhallintaa. Seuraavaksi on kuvattu tärkeimpiä riskienhallinnan käsitteitä tämän työn näkökulmasta.

Uhka

Uhka on ”mahdollinen syy epätoivottuun tapahtumaan, josta voi seurata haittaa järjestelmälle tai organisaatiolle” (SFS-ISO/IEC 27000:2016, 16).

Eri tyyppisiä tietoturvauhkia, jotka aiheuttavat tieto-omaisuuteen kohdistuvan riskin, ovat muun muassa:

- Tekeytyminen, eli toisena esiintyminen
- Tiedon peukalointi, eli luvaton muuttaminen
- Kiistäminen, eli aiheeton väite, että tieto tai tapahtuman kuvaus ei pidä paikkaansa
- Paljastus, eli luottamuksellisen tiedon joutuminen ulkopuolisen tietoon luvatta
- Palvelun esto, eli tietojärjestelmän käytettävyyden heikkeneminen
- Käyttöoikeuksien luvaton laajentaminen
- Sivuttainen liike, eli kaapattujen valtuustietojen käyttäminen järjestelmästä toiseen etenemiseen

Uhkat ovat peräisin Lockheed Martinin STRIDE-LM mallista, suomentamiseen käytetty VAHTI sanastoa. (Muckin, M. & Fitch, S. 2019,13; Valtionhallinnon tietoturvallisuuden johtoryhmä 2008.)

Riski

Riski on ”todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon” (Valtionhallinnon tietoturvallisuuden johtoryhmä 2008, 80).

Tässä työssä riskiä kuvataan tapahtuman seurausten ja riskin toteutumisen todennäköisyyden yhdistelmänä.

Riskitaso

Riskitaso kuvaa riskin suuruutta (SFS-ISO/IEC 27000:2016, 11). Tässä opinnäytetyössä käsitellään tietoturvatapahtumien suhteellista riskitasoa. Suhteellisuudella tarkoitetaan sitä, että riskitasolle laskettu arvo on merkityksellinen ainoastaan järjestelmän sisällä osoittamassa tietoturvatapahtumien välisiä eroja.

Tässä työssä tietoturvatapahtuman riskitasoa verrataan arviointikriteereihin, jolloin saadaan selville sen kiireellisyysluokka.

2.2 Tietoturvavalvonta

Toimeksiantajan tietoturvavalvomossa valvotaan asiakasorganisaatioiden tieto-omaisuutta. Seuraavaksi käsitellään tietoturvavalvonnan keskeisiä käsitteitä.

SIEM

SIEM on lyhenne englanninkielisestä termistä Security Incident and Event Management, joka tarkoittaa tietoturvahäiriöiden ja -tapahtumien hallintaan käytettyä järjestelmää (Ilkka ym. 2017, 54). Järjestelmään syötetään ajankohtaista uhkatietoa, tietoa valvottavista laitteista ja käyttäjistä, sekä lokitietoa valvottavilta laitteilta. Järjestelmä tunnistaa tietoturvatapahtumia ja tarjoaa tietoturvavalvomon henkilökunnalle käyttöliittymän niiden arvioimiseen. (IBM 2019d, 3.)

Tässä työssä SIEM -järjestelmällä viitataan nimenomaan IBM Security QRadar SIEM v.7.3.1 -tuotteeseen ja kehitettävä riskitason määritysmenetelmä laadittiin sen kanssa yhteensopivaksi.

Tietoturvatapahtuma

Tietoturvatapahtuma on ”tapahtuma, joka kertoo, että tietoturvallisuus tai hallintakeinot ovat mahdollisesti pettäneet” (SFS-ISO/IEC 27035-1:2016, 6).

SIEM-järjestelmässä käytetään samasta asiasta englanninkielistä termiä ”offense”, jonka järjestelmän valmistaja on määritellyt tarkoittamaan viestiä, joka tarjoaa tietoa esimerkiksi

siitä, että tietoturvaperiaatteissa määriteltyä toimintatapaa on rikottu tai tietoverkko on hyökkäyksen kohteena. (IBM 2019a.)

Kaikki tietoturvatapahtumat eivät tarkoita sitä, että tieto-omaisuuteen kohdistunut hyökkäys olisi onnistunut tai, että tietoturvallisuus on vaarantunut (SFS-ISO/IEC 27035-1:2016, 7).

Tässä työssä tietoturvatapahtumalla tarkoitetaan ensisijaisesti SIEM-järjestelmän laukaisemaa viestiä (offense), jonka tietoturvavalvomon henkilökunta arvioi. Tietoturvatapahtuma voidaan arvioinnin seurauksena luokitella tietoturvahäiriöksi.

Tietoturvahäiriö

Tietoturvahäiriö on ”yksi tai useampi epätoivottu tai odottamaton tietoturvatapahtuma, joka suurella todennäköisyydellä vaarantaa liiketoiminnot ja uhkaa tietoturvallisuutta” (SFS-ISO/IEC 27000:2016, 10).

Tietoturvavalvomo raportoi tunnistetut tietoturvahäiriöt ja käynnistää häiriövasteen, eli ”toimenpiteet, joilla lievennetään tai ratkaistaan tietoturvahäiriö…” (SFS-ISO/IEC 27035-1:2016, 7).

Lokitapahtuma

Valtionhallinnon tietoturvasanasto määrittelee vastaavan termin: lokitieto on ”automaattisesti kirjautuva tapahtumatieto, joka voi sisältää muun muassa erilaisia tunnistamistietoja, välitystietoja ja tietoja virhetilanteista” (Ilkka ym. 2017, 54).

Lokitapahtumat ovat peräisin lokilähteiltä, josta ne siirretään SIEM-järjestelmään käsittelyä ja tallennusta varten. Lokilähteitä esitellään tarkemmin luvussa kolme.

Lokitapahtumasta käytetään SIEM-järjestelmässä englanninkielistä termiä ”event”.

Skenaario

Tässä työssä skenaariolla tarkoitetaan sellaista tapahtumaa tai tapahtumaketjua, joka vaikuttaa valvottavaan tieto-omaisuuteen, ja joka pyritään havaitsemaan valvontasäännöllä.

Valvontasääntö

Valvontasääntö on kokoelma ehtolausekkeita, jonka avulla SIEM-järjestelmä tunnistaa tietyn skenaarion toteutumisen. Valvontasääntö voi myös laukaista automaattisen vasteen, kuten tietoturvatapahtuman kirjaamisen tai lokitapahtuman piirteiden muokkaamisen. (QRadar SIEM).

SIEM-järjestelmä arvioi kaikki lokitapahtumat valvontasääntöjen avulla.

Tieto-omaisuus

ISO 27000 standardin mukaan tieto-omaisuus ”voi olla esimerkiksi taloudellista tietoa, aineetonta omaisuutta, työntekijöiden henkilötietoja tai asiakkaiden tai kolmansien osapuolten organisaatiolle antamia tietoja” (SFS-ISO/IEC 27000:2016, 4).

Esimerkiksi verkkoasemille tallennetut asiakirjat, käyttäjien sähköpostit, järjestelmien asetustiedostot ja kaikenlaiset tietokannat ovat tieto-omaisuutta.

Suojattavat toiminnot

Suojattavilla toiminnoilla tarkoitetaan niitä asiakkaan liiketoimintoja, jotka ovat riippuvaisia valvottavasta tieto-omaisuudesta.

Suojattavia toimintoja voivat olla esimerkiksi verkkokauppa, tuotekehitys tai asiakkuudenhallinta.

Luotettavuus (credibility)

Lokitapahtuman, skenaarion tai tietoturvatapahtuman luotettavuus ilmaistaan SIEM -järjestelmässä käyttäen englanninkielistä termiä ”credibility”. Järjestelmän valmistajan määritelmän mukaan se on arvo, joka osoittaa tietoturvatapahtuman integriteetin (IBM 2019a). Integriteetillä tarkoitetaan käytännössä luotettavuuden suuruutta, joka ilmaistaan kokonaislukuna asteikolla 0-10.

Tässä opinnäytetyössä luotettavuus määritellään seuraavasti: todennäköisyys, että lokitapahtuma, skenaario tai tietoturvatapahtuma liittyy tietoturvahäiriöön. Luotettavuus muodostuu ensisijaisesti lokilähteen tai valvontasäännön ominaisuuksien perusteella.

Luotettavuus on suuri, jos lokitapahtuma, skenaario tai tietoturvatapahtuma esiintyy tietoturvahäiriön yhteydessä usein, mutta muissa yhteyksissä vain harvoin. Tietoturvatapahtuman luotettavuus rinnastetaan tietoturvariskin todennäköisyyteen.

Olennaisuus (relevance)

Lokitapahtuman, skenaarion tai tietoturvatapahtuman olennaisuus ilmaistaan SIEM -järjestelmässä käyttäen englanninkielistä termiä ”relevance”. Järjestelmän valmistajan määritelmän mukaan se on arvo, joka osoittaa tapahtuman suhteellisen vaikutuksen valvottavaan verkkoon (IBM 2019a). Olennaisuudella tarkoitetaan käytännössä suhteellisen vaikutuksen suuruutta, joka ilmaistaan kokonaislukuna asteikolla 0-10.

Tässä opinnäytetyössä termi määritellään seuraavasti: suojattavien toimintojen alttius lokitapahtuman, skenaarion tai tietoturvatapahtuman vaikutuksille. Olennaisuus muodostuu ensisijaisesti tieto-omaisuuden ominaisuuksien perusteella.

Olennaisuus on suuri, jos tapahtumaan liittyvä tieto-omaisuus on suojattavien toimintojen kannalta tärkeä ja tieto-omaisuus on altis tapahtuman vaikutuksille. Olennaisuus on pieni, jos tapahtumaan liittyvä tieto-omaisuus ei ole merkittävä suojattavien toimintojen kannalta, tai tieto-omaisuus on hyvin suojattu tapahtuman vaikutuksilta.

Vakavuus (severity)

Lokitapahtuman, skenaarion tai tietoturvatapahtuman vakavuutta merkitään SIEM -järjestelmässä englanninkielisellä termillä ”severity”. Järjestelmän valmistajan määritelmän mukaan se on arvo, joka kuvaa lähteen kohteelle aiheuttamaa suhteellista uhkaa (IBM 2019a). Vakavuudella tarkoitetaan käytännössä suhteellisen vakavuuden suuruutta, joka ilmaistaan kokonaislukuna asteikolla 0-10.

Tässä opinnäytetyössä termi määritellään seuraavasti: tapahtuman tai tietoturvatapahtuman potentiaalinen vaikutus tieto-omaisuuden tietoturvallisuuteen. Vakavuus muodostuu ensisijaisesti tapahtuman tai tietoturvatapahtuman ominaisuuksien perusteella.

Vakavuus on suuri, jos vaikutus tietoturvallisuuteen on luonteeltaan negatiivinen ja tasoltaan suuri. Vakavuus on pieni, jos vaikutus tietoturvallisuuteen on tasoltaan pieni tai luonteeltaan positiivinen. Tietoturvatapahtuman olennaisuuden ja vakavuuden yhdistelmä rinnastetaan tietoturvariskin seurauksiin.

Tietoturvatapahtuman suhteellinen tärkeys (magnitude)

SIEM -järjestelmä laskee automaattisesti tunnistamilleen tietoturvatapahtumille arvon, joka tunnetaan järjestelmän sisällä englanninkielisellä nimellä ”magnitude”. Tämä arvo kuvastaa tietoturvatapahtuman suhteellista tärkeyttä (verrattuna muihin samaan järjestelmään kirjattuihin tietoturvatapahtumiin) ja se muodostetaan laskemalla painotettu keskiarvo tietoturvatapahtuman luotettavuudesta, olennaisuudesta ja vakavuudesta (IBM 2019a). Laskemiseen käytetty algoritmi on valmistajan liikesalaisuus (IBM 2019b).

Määrittäessään tietoturvatapahtuman luotettavuutta, olennaisuutta ja vakavuutta, SIEM-järjestelmä ottaa huomioon siihen liittyvien skenaarioiden ja lokitapahtumien vastaavat arvot.

Lisäksi suhteelliseen tärkeyteen vaikuttaa dynaamisia tekijöitä, kuten tapahtumaan liittyvän lokitiedon määrä ja tietoturvatapahtuman ikä. Dynaamiset tekijät määräytyvät tapauskohtaisesti tilanteen mukaan, eikä niiden muodostumiseen voi vaikuttaa asetuksilla. (IBM 2019c.) Tämän vuoksi dynaamiset tekijät on tässä työssä jätetty tarkastelun ulkopuolelle.

Samoin kuin riskitaso muodostuu tapahtuman seurausten ja todennäköisyyden yhdistelmänä, niin vastaavasti tärkeys muodostuu vakavuuden ja olennaisuuden, sekä luotettavuuden yhdistelmänä. Oheinen taulukko (Taulukko 2) havainnollistaa rinnastamista.

Riskin muodostuminen	Tietoturvatapahtuman tärkeyden muodostuminen QRadar SIEM -järjestelmässä
Todennäköisyys	Luotettavuus (Credibility)
Seuraukset	Olennaisuus (Relevance) Vakavuus (Severity)
= Riski	= Tärkeys (Magnitude)

Taulukko 2 - Riskin ja tietoturvatapahtuman tärkeyden rinnastaminen

2.3 Mittaaminen

Jotta tietoturvatapahtuman riskitaso voidaan määrittää luotettavasti, on mitattava siihen liittyvien lokitapahtumien ja skenaarioiden piirteitä. Seuraavaksi määritellään tämän työn kannalta keskeiset mittaamisen käsitteet.

Piirre

Piirre on ”kohteen ominaisuus tai määrite, jonka ihminen tai automaattinen järjestelmä voi erottaa laadullisesti tai määrällisesti” (SFS-ISO/IEC 27004, 12).

Mittauksen kohteen piirrettä mitataan mittausmenetelmällä, jonka seurauksena muodostuu perusmittari (SFS-ISO/IEC 27004, 24).

Tässä työssä piirteitä ovat muun muassa lokilähteen tyyppi, lokilähteen laatu, käyttäjän, laitteen tai verkon painoarvo, tapahtuman turvallisuusvaikutus, uhkatiedon luotettavuus ja havaitsemismenetelmän luotettavuus.

Mittauksen kohde

Mittauksen kohde on ”kohde, jota kuvataan sen piirteiden mittauksen avulla” (SFS-ISO/IEC 27004, 16).

Tässä työssä mittauksen kohteita ovat lokitapahtuma ja skenaario.

Perusmittari

Perusmittari on ”mittari, joka on määritelty jonkin piirteen ja sen suuruuden määrittämiseen käytettävän menetelmän avulla” (SFS-ISO/IEC 27004, 12).

Tässä työssä perusmittareita ovat muun muassa lokitiedon luotettavuuden perusarvo ja tarkennearvo, sekä skenaarion olennaisuuden ensimmäinen ja toinen lisäarvo. Perusmittareita käsitellään tarkemmin myöhemmissä luvuissa.

Johdannaismittari

Johdannaismittari on kahden tai useamman perusmittarin yhdistelmä (SFS-ISO/IEC 27004, 26).

Tässä työssä johdannaismittareita ovat lokitiedon ja skenaarion luotettavuus, olennaisuus, sekä vakavuus.

Mittausmenetelmä

Mittausmenetelmä on ”johdonmukainen toimintojen ketju, joka on esitetty yleisellä tasolla ja jota käytetään piirteen suuruuden määrittämiseen tietyllä asteikolla” ja se voi olla subjektiivinen tai objektiivinen (SFS-ISO/IEC 27004, 14). Tässä työssä käytettävät mittausmenetelmät ovat subjektiivisia. Subjektiivinen mittausmenetelmä tarkoittaa sitä, että määrän ilmaiseminen perustuu ihmisen arviointikykyyn (SFS-ISO/IEC 27004, 14).

Asteikko

Asteikko on ”järjestetty arvojoukko, joka voi olla jatkuva tai epäjatkuva, tai niiden luokkien joukko, joihin piirre kuvautuu” (SFS-ISO/IEC 27004, 16).

Tässä työssä käytetään ainoastaan järjestysasteikkoja. Järjestysasteikon käyttäminen tarkoittaa, että mittaustulosten arvot voidaan järjestää, mutta arvojen välisillä etäisyyksillä ei ole merkitystä (Tilastokeskus 2019).

Mittausfunktio

Mittausfunktio on ”algoritmi tai laskelma, jolla yhdistetään kaksi tai useampia perusmittareita” (SFS-ISO/IEC 27004, 14).

Esimerkki mittausfunktiosta on: tapahtuman luotettavuuden perusarvo + tapahtuman luotettavuuden lisäarvo = tapahtuman luotettavuus.

Analyysimalli

Analyysimalli on "algoritmi tai laskelma, joka yhdistää yhden tai useamman perus- tai johdannaismittarin ja niihin liittyvät arviointikriteerit” (SFS-ISO/IEC 27004, 12).

Tässä työssä on yksi analyysimalli, SIEM-valmistajan algoritmi, joka yhdistää tapahtuman ja skenaarion luotettavuuden, olennaisuuden ja vakavuuden sekä dynaamiset piirteet määrittääkseen tietoturvatapahtuman suhteellisen riskitason.

Indikaattori

Indikaattori on ”analyysimallista johdettu mittari, joka antaa täsmennettyjen tietotarpeiden mukaisen arvon tai arvion halutuille piirteille” (SFS-ISO/IEC 27004, 14). ”Indikaattorit saadaan soveltamalla analyysimallia perus- tai johdannaismittariin ja yhdistämällä ne arviointikriteereihin” (SFS-ISO/IEC 27004, 28).

Tässä työssä indikaattori ilmaisee tietoturvatapahtuman kiireellisyysluokituksen arviointikriteerien mukaan, perustuen analyysimallilla laskettuun riskitasoon.

Arviointikriteerit

Arviointikriteerit, eli ”raja-arvot, tavoitteet tai mallit, joilla määritetään toimenpiteiden tai lisätutkimusten tarve tai jotka kuvaavat tietyn tuloksen luottamustasoa” (SFS-ISO/IEC 27004, 14).

Indikaattorin arvoa verrataan arviointikriteereihin, jolloin saadaan selville mittaustulos (SFS-ISO/IEC 27004, 30).

Esimerkki arviointikriteereistä esitetään luvussa kuusi, Taulukko 3.

Mittaustulokset

Mittaustuloksilla tarkoitetaan yhtä tai useampaa tietotarpeeseen vastaavaa indikaattoria ja niihin liittyviä tulkintoja (SFS-ISO/IEC 27004, 14).

Esimerkki mittaustuloksesta: ”Tietoturvatapahtuma X kuuluu kiireellisyysluokkaan 1, se täytyy arvioida ensimmäisenä.”

Tietotarve

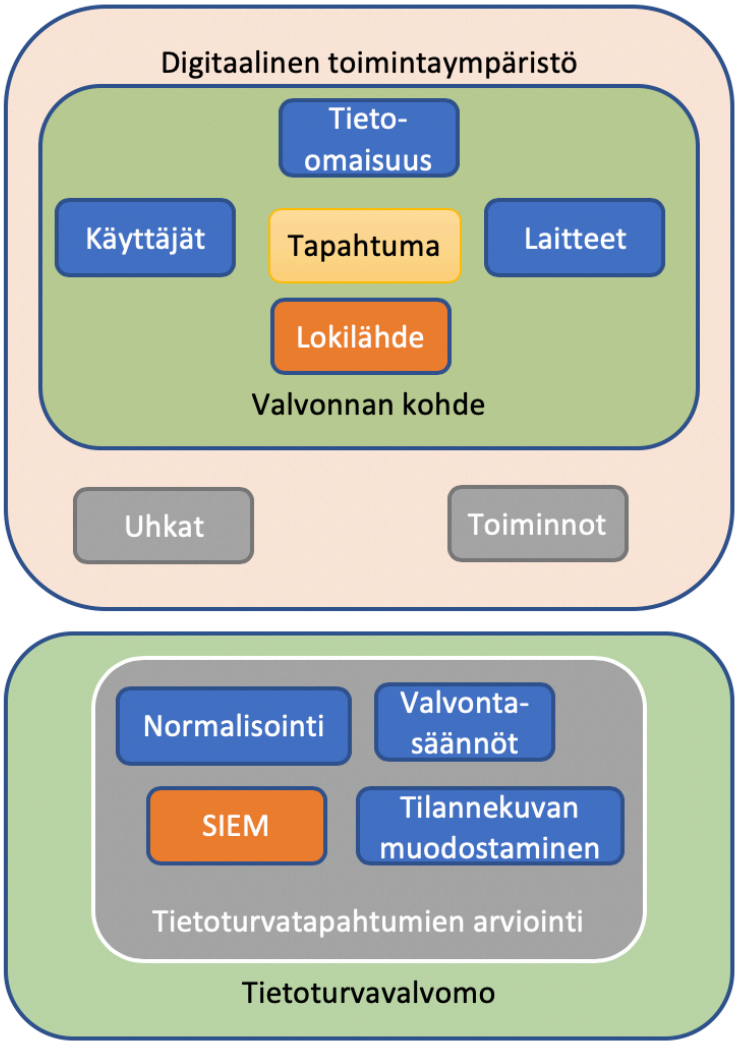
Tietotarpeella tarkoitetaan tavoitteiden, riskien ja ongelmien hallintaan tarvittavaa näkemystä (SFS-ISO/IEC 27004, 14).

Tämän työn keskeinen tietotarve on: missä järjestyksessä tietoturvatapahtumat tulee arvioida?

3 Toimintaympäristö

Tietoturvavalvonnan toimintaympäristö kattaa sekä tietoturvavalvomon että valvottavan tieto-omaisuuden. Näiden keskinäinen yhteys on se, että tietoturvavalvomossa tunnistetaan tieto-omaisuuteen kohdistuvia uhkia ja arvioidaan näistä aiheutuvia tietoturvatapahtumia.

Oheinen kuvio (Kuvio 1) havainnollistaa toimintaympäristön keskeisimpien elementtien yhteyksiä.



Kuvio 1 - Toimintaympäristön keskeisimmät elementit

Asiakasorganisaatioilla on digitaalisessa toimintaympäristössä toimintoja, jotka ovat riippuvaisia tieto-omaisuudesta. Digitaalisessa toimintaympäristössä olevia uhkia vastaan suojaudutaan tietoturvavalvonnalla.

Tietoturvavalvonnan kohteena on asiakasorganisaation tieto-omaisuus. Asiakkaan tietoverkoissa on lokilähteitä, jotka tallentavat tieto-omaisuuteen kohdistuvia tapahtumia kirjaten muun muassa tapahtumiin liittyvät laitteet ja käyttäjät. Lokilähteet lähettävät kirjaamansa tapahtumat SIEM-järjestelmään.

Tietoturvavalvomon henkilökunta vastaa tietoturvatapahtumien arvioinnista. Arvioinnin apuna käytetään SIEM-järjestelmää, jonka muodostaa tietoturvatapahtumat kolmivaiheisella prosessilla, johon kuuluu lokitapahtumien normalisointi, niiden arviointi valvontasäännöillä, sekä lopuksi tilannekuvan muodostaminen.

3.1 Tietoturvavalvomo

Tietoturvavalvonnan tavoitteena on nopeuttaa uhkien havaitsemista ja mahdollistaa nopea reagointi. Nopea reagointi lieventää tietoturvahäiriön vaikutusta suojattaviin toimintoihin. Lisäksi tietoturvavalvomon tuottaman tiedon avulla voidaan edistää tietoturvahäiriöistä oppimista, ja jatkuvan parantamisen kautta ennaltaehkäistä tulevia häiriöitä.

Tietoturvavalvonnan keskeisenä komponenttina on tietoturvahäiriöiden ja -tapahtumien hallinnassa käytetty järjestelmä, eli SIEM. Järjestelmä saa tarvittavat tiedot keräämällä asiakkaan tietoverkkoon kytketyiltä laitteilta lokitietoja. SIEM normalisoi lokitiedot yhteismitalliseen muotoon, ja luokittelee samalla jokaisen tapahtuman tiettyyn kategoriaan. Normalisointi mahdollistaa sen, että eri lähteistä vastaanotettuja tapahtumia voidaan käyttää tilannekuvan rakentamiseen yhteisillä valvontasäännöillä.

SIEM arvioi normalisoituja tapahtumia monien valvontasääntöjen avulla, jotka on ohjelmoitu laukaisemaan hälytys, kun tietty tapahtuma tai tapahtumaketju havaitaan. Tätä hälytystä kutsutaan myös tietoturvatapahtumaksi.

Tietoturvavalvomossa työskentelevät tietoturva-analyytikot analysoivat tietoturvatapahtumat, arvioiden asiakkaalle aiheutuvan riskin suuruutta. Mikäli arvion mukaan tietoturvatapahtuma suurella todennäköisyydellä vaarantaa tietoturvaa merkittävästi, kirjataan se tietoturvahäiriöksi raportointijärjestelmään, sekä käynnistetään häiriövaste.

3.2 Valvottava tieto-omaisuus

Toimeksiantajan asiakkaina on suuryrityksiä, jotka ostavat tietoturvavalvontaa jatkuvana palveluna. Tietoturvavalvonta kohdistetaan asiakkaan tieto-omaisuuteen. Tieto-omaisuuden tilasta ja siihen kohdistuvista toimista kerätään tietoa ja se tuodaan SIEM-järjestelmään tallennusta ja käsittelyä varten.

Lokitieto sisältää pääsääntöisesti viittä eri tietotyyppiä:

- Identiteettitieto: keitä käyttäjiä tapahtumaan liittyy
- Laitetieto: mitä laitteita on osallisena tapahtumassa

- Tapahtumatieto: mitä toimintoa yritettiin ja miten se onnistui
- Tilatieto: miten tieto-omaisuuden tilaa on muutettu tai yritetty muuttaa
- Metatieto: mistä tieto on peräisin, milloin se kirjattiin, mihin kategoriaan se kuuluu

3.2.1 Lokilähteet

Lokitietoa kerätään monista erilaisista lähteistä. Seuraavaksi on kuvailtu joitakin erilaisia lokilähteitä, sekä minkä tapaista tietoa niiltä tyypillisesti kerätään ja miksi.

Sisäverkon turvalaitteet

Sisäverkon turvalaitteilta kuten palomuureilta, tietomurtohälyttimiltä (IDS), tietomurron estojärjestelmiltä (IPS), tietovuodon estojärjestelmiltä (DLP) ja suodattavilta välipalvelimilta kerätään tietoja muodostetuista yhteyksistä ja niiden sisällöstä. Yhteyksistä tallennetaan muun muassa lähde- ja kohdeosoitteet, kesto, käytetty protokolla, ja muita metatietoja. Joidenkin yhteyksien sisällöt voidaan analysoida, ja verrata niitä uhkatietokantaan.

Sisäverkon turvalaitteiden lokitiedolla muodostetaan yleiskuva verkkoliikenteestä, tunnistetaan haitallisia yhteyksiä sekä havaitaan luottamuksellisen tiedon tarkoittamatonta tai luvatonta siirtoa.

Verkkoasemat

Verkkoasemilta, kuten käyttäjien päätelaitteilta, palvelimilta ja kytkimiltä kerätään käyttöjärjestelmälokia, joista käy ilmi laitteen asetuksiin tehdyt muutokset ja pääsytapahtumat. Työasemilta ja palvelimilta kerätään myös virustorjuntaohjelmien ja paikallisten valvontasensoreiden lokia.

Verkkoasemilta saadulla lokitiedoilla valvotaan tietoverkkoon kytkettyjen laitteiden tilaa ja eheyttä, sekä tunnistetaan haittaohjelmia tai haavoittuvuuksien hyväksikäyttöä. Verkkoasemat myös tuottavat tietoa käyttäjien toimista.

Pilvipalvelut

Erilaisista pilvipalveluina tarjottavista sovelluksista kuten sähköposti, tiedostojenjako ja webportaalit, kerätään pääsytapahtumia, järjestelmälokia ja sovelluskohtaista tapahtumalokia.

Pilvipalveluista kerätyn lokin perusteella valvotaan sovellusten käyttöä, tarkoituksena tunnistaa väärinkäyttötilanteet. Lisäksi pyritään tunnistamaan muun muassa käyttäjien epänormaalia toimintaa, joka saattaa olla merkki valtuustietojen luvattomasta käytöstä.

Taustajärjestelmät

Taustajärjestelmistä kuten tietokannoista, toiminnanohjausjärjestelmistä ja pääsynhallintajärjestelmistä kerätään sovelluskohtaisia tapahtumatietoja, järjestelmälokia sekä tunnistustapahtumia.

Taustajärjestelmien eheyttä ja saatavuutta valvotaan järjestelmälokien avulla. Tapahtuma- ja tunnistustietoja käytetään usein yhdessä muista järjestelmistä kerätyn tiedon kanssa kokonaiskuvan rikastamiseen.

3.2.2 Tieto-omaisuuteen kohdistuvat uhat

Tieto-omaisuuteen kohdistuvat uhat ja niiden merkittävyydet vaihtelevat yrityskohtaisesti. Erilaisten uhkien esittely ei ole keskeisessä osassa tässä opinnäytetyössä, mutta yleiskuva uhkamaisemasta auttaa hahmottamaan seuraavassa luvussa esiteltävää teoreettista viitekehystä. Hyvän yleiskuvan uhista saa esimerkiksi Euroopan unionin verkko- ja tietoturvavirasto ENISA:n tammikuussa 2019 julkaisemasta uhkamaisemasta. Raportissa esitellään 15 merkittävintä kyberuhkaa ja uhkatoimijaa.

Yleisellä tasolla, toimintaympäristön merkittävimpiä uhkia ovat: haittaohjelmat, verkkosivuihin pohjautuvat hyökkäykset, verkkosovelluksiin kohdistuvat hyökkäykset, kalasteluhyökkäykset, palvelun esto, roskaposti, bottiverkot, tietomurrot, sisäinen uhka, fyysinen vahinko, tietovuoto, identiteettivarkaus, kryptolouhinta, kiristäjävirukset ja kybervakoilu (ENISA 2019).

Näiden uhkien taustalla olevat merkittävimmät toimijat ovat: kyberrikolliset, sisäpiiriläiset, valtiolliset toimijat, kilpailevat yritykset, haktivistit, kyberterroristit ja skriptarit (ENISA 2019).

4 Teoreettinen viitekehys

Tässä luvussa esitellään teoreettinen viitekehys, johon tukeutuen tietoturvatapahtumien riskitason määrittämismenetelmä on kehitetty. Viitekehystä tarkastellaan kolmesta näkökulmasta: tietoturvavalvonta osana riskienhallintaa, SIEM-järjestelmän toimintaperiaate ja systemaattinen mittaaminen.

4.1 Tietoturvavalvonta osana riskienhallintaa

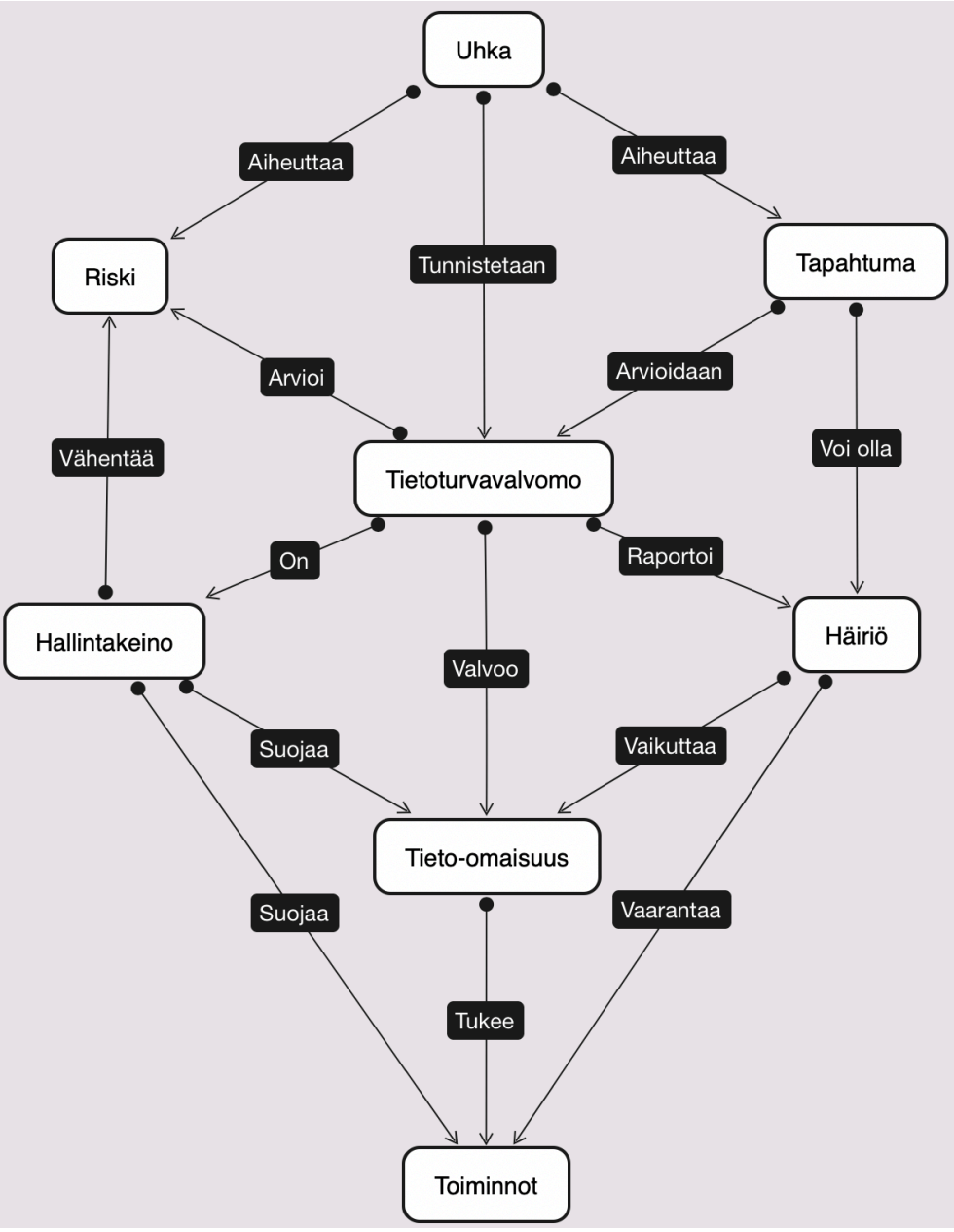
Tieto-omaisuuteen kohdistuu uhkia, jotka voivat toteutuessaan aiheuttaa tietoturvahäiriöitä. Tietoturvahäiriöt vaarantavat yrityksen suojattavia toimintoja, vaikuttamalla niitä tukeviin tietoverkkoihin ja -järjestelmiin. Uhkista aiheutuvia riskejä voidaan lieventää tietoturvavalvonnalla.

Riskienhallinnan näkökulmasta tietoturvavalvontaan sisältyvä tietoturvatapahtumien arviointi ja luokittelu on hallintakeino, joka kuuluu tietoturvahäiriöiden hallinnan kokonaisuuteen (SFS-

ISO/IEC 27001, 40, 42). Tietoturvahäiriöiden hallinta, yhdessä muiden hallintakeinojen kanssa, suojaa yrityksen tieto-omaisuutta ja siten myös siitä riippuvaisia liiketoimintoja.

Tieto-omaisuuteen kohdistuviin riskeihin on tärkeää varautua, sillä liiketoiminnot ovat digitalisaation ja lisääntyneen verkottumisen johdosta yhä enemmän riippuvaisia tietojärjestelmistä (SFS-ISO/IEC 27000:2016, 20).

Oheinen kuvio (Kuvio 2) esittää tietoturvahäiriöiden hallintaan liittyvien termien yhteyksiä tietoturvavalvonnan näkökulmasta. Kuvio perustuu osittain SFS-ISO/IEC 27035-1:2016 -standardin vastaaviin kuviin (SFS-ISO/IEC 27035-1:2016, 8-9).



Kuvio 2 - Tietoturvavalvonnan käsitteet riskienhallinnan viitekehyksessä

4.2 SIEM -järjestelmän toimintaperiaate

Kuten luvussa kaksi kuvattiin, niin SIEM-järjestelmä laskee tietoturvatapahtuman suhteellisen tärkeyden luotettavuuden, olennaisuuden ja vakavuuden yhdistelmänä. Tämän työn asiayhteydessä luotettavuus rinnastetaan riskin todennäköisyyteen, olennaisuuden ja vakavuuden yhdistelmä vastaavasti riskin seurauksiin. Kun hyväksytään nämä oletukset, voidaan tehdä johtopäätös, että tietoturvatapahtumien asettaminen järjestykseen käyttäen SIEM -järjestelmän laskemaa suhteellista tärkeyttä, vastaa opinnäytetyön tavoitetta suorittaa tietoturvatapahtumien kiireellisyysluokittelu riskitason perusteella.

Seuraavaksi käsitellään suhteellisen tärkeyden määräytymistä SIEM-järjestelmässä. Määräytyminen voidaan jakaa kolmeen eri vaiheeseen: normalisointi, tapahtumien arviointi ja tilannekuvan muodostaminen. Esitellyt vaiheet eivät täsmällisesti vastaa teknisen toteutuksen vaiheita, vaan ne kuvaavat sen sijaan loogisia kokonaisuuksia.

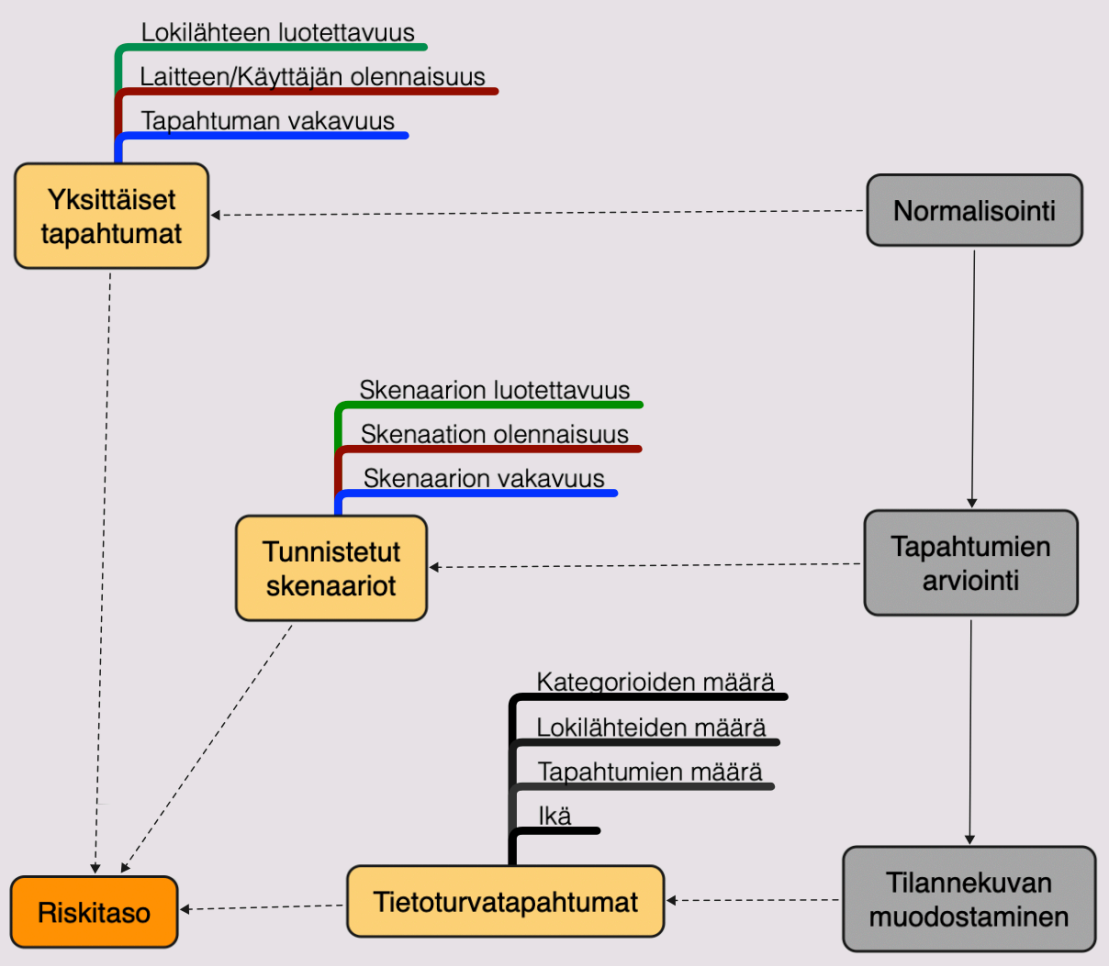
Normalisointivaiheessa eri lokilähteiltä saapuvat tapahtumat muutetaan yhteismitalliseen muotoon. Samalla tapahtumalle annetaan arvot lokilähteen luotettavuuden, tapahtuman vakavuuden ja tapahtumaan liittyvän tieto-omaisuuden olennaisuuden perusteella. Näiden arvojen määräytymiseen voi vaikuttaa järjestelmän asetuksia muuttamalla. (QRadar SIEM.)

- Lokilähteen asetuksissa voi määrittää luotettavuuden, jonka jälkeen kaikki siitä lokilähteestä saapuvat tapahtumat perivät asetetun luotettavuusarvon (QRadar SIEM).
- Jokaista lokilähdetyyppiä kohden järjestelmässä on moduuli, joka vastaa tapahtumien muuttamisesta yhteismitallisiksi. Moduulin asetuksista voi asettaa tapahtumakohtaisen vakavuusarvon, jonka jälkeen kaikki saman tyyppiset tapahtumat perivät asetetun vakavuusarvon (QRadar SIEM).
- Jokaisesta tapahtumasta tunnistetaan siihen liittyvät verkkoasemat. Järjestelmä sisältää tietokannan, johon on tallennettu tietoja verkkoasemista, mukaan lukien niiden suhteellinen tärkeys organisaatiolle. Järjestelmä hakee tietokannasta tapahtumaan liittyvän verkkoaseman suhteellisen tärkeysarvon, jonka perusteella se asettaa tapahtuman olennaisuusarvon (QRadar SIEM).

Tapahtumien arviointivaiheessa SIEM-järjestelmä vertaa tapahtumia valvontasääntöihin. Mikäli tapahtuma tai tapahtumaketju täsmää valvontasäännössä määriteltyyn skenaarioon, kirjataan tapauksesta tietoturvatapahtuma. Tässä vaiheessa täsmäävien tapahtumien luotettavuutta, olennaisuutta ja vakavuutta voidaan muokata. Samoin kuin normalisointivaiheessa, niin näiden arvojen määräytymiseen voi vaikuttaa järjestelmän asetuksia muuttamalla.

Tilannekuvavaiheessa SIEM-järjestelmä pitää kirjaa tietoturvatapahtumiin liittyvistä dynaamisista piirteistä, kuten kuluneesta ajasta sekä tapahtumien ja lokilähteiden määrästä. Näiden arvojen laskemista tai vaikutusta ei voi muuttaa järjestelmän asetuksilla.

SIEM laskee yhteen normalisointivaiheen ja tapahtumien arviointivaiheen tulokset ja huomioi vielä dynaamiset piirteet. Algoritmin tuloksena on tietoturvatapahtuman suhteellinen tärkeys, joka tämän työn asiayhteydessä rinnastetaan riskitasoon. Riskitason perusteella tapahtumat voidaan luokitella eri kiireellisyysluokkiin, ja ne siirtyvät tietoturvavalvomon henkilökunnan arvioitavaksi.



Kuvio 3 - Tietoturvatapahtuman suhteellisen riskitason määräytyminen SIEM-järjestelmässä

SIEM-järjestelmä tarjoaa siis puitteet tietoturvatapahtumien suhteellisen tärkeyden laskemiselle: se sisältää algoritmin, joka ottaa huomioon tapahtuman luotettavuuden, olennaisuuden, vakavuuden ja dynaamiset piirteet, ja laskee tärkeyden niiden perusteella. Lisäksi SIEM tarjoaa rakenteet edellä mainittujen arvojen muokkaamiseen. (IBM 2019c.)

Yleisimpien lokilähdetyyppien tapahtumien vakavuus tunnistetaan automaattisesti, mutta muuten jää tietoturvavalvomon vastuulle määrittää tärkeyteen vaikuttavien tekijöiden arvot.

4.3 Systemaattinen mittaaminen

Systemaattisen mittausmallin perustana on tietotarve, joka osoittaa mittauksen tavoitteen. Yleisesti mittauksen tavoitteena on antaa merkityksellistä tietoa päätöksenteon tueksi, ja tietotarpeen määrittelyllä tarkennetaan, millaista tukea päätöksentekoon tarvitaan.

Mittaamisen rakenne koostuu kolmesta elementistä: perusmittarit, johdannaismittarit ja indikaattorit. Perusmittarille saadaan arvo mittaamalla mittauksen kohteen piirteitä, käyttäen mittausmenetelmää. Tämän jälkeen mittausfunktiolla voidaan yhdestä tai useammasta perusmittarista jalostaa johdannaismittari. Analyysimallin avulla johdannaismittareista ja perusmittareista johdetaan indikaattoreita.

Arviointikriteerien avulla määritellään, miten indikaattoreiden arvoja tulee tulkita. Kun indikaattorin arvoa on tulkittu arviointikriteerien avulla, syntyy mittaustulos. Jos mittaaminen on hyvin suunniteltu ja toteutettu, mittaustulos vastaa tietotarpeeseen, ja tarjoaa merkityksellistä tietoa päätöksenteon tueksi.

5 Opinnäytetyön toteutus

Tässä luvussa kerrotaan kehittämistarpeen tunnistamisesta, sekä kuvaillaan opinnäytetyön vaiheita ja niissä käytettyjä menetelmiä.

5.1 Kehittämistarpeen tunnistaminen

Idea kehittämistarpeeseen syntyi havainnoinnin kautta. Tietoturvavalvomossa työskentelevien tietoturva-analyytikoiden työskentelyä seuraamalla havaittiin, että palvelun kysynnän kasvamisen johdosta tietoturvavalvomon kuorma kasvaa siten, että lähestytään tilannetta, jossa kapasiteetti ei riitä tietoturvatapahtumien arvioimiseen tavoiteaikojen puitteissa.

Jotta laadukasta tietoturvavalvontaa voidaan jatkossakin tarjota yhä kasvavalle asiakasjoukolle, on tarpeen reagoida lisäämällä resursseja ja tehostamalla prosesseja. Tietoturvavalvomon prosesseista tehostamisen kohteeksi valittiin tietoturvatapahtumien arviointi, sillä se on toiminnan kannalta keskeinen ydinprosessi, joka myös vaatii paljon resursseja.

Tehostamisessa kyse on siitä, että pyritään saamaan samoilla resursseilla aikaan enemmän hyötyä, ja yksi tapa saada aikaan toivottu vaikutus on kohdistamalla työtä sinne, missä sillä on suurin vaikutus. Näin ollen päädyttiin tarkastelemaan tietoturvatapahtumien priorisointia.

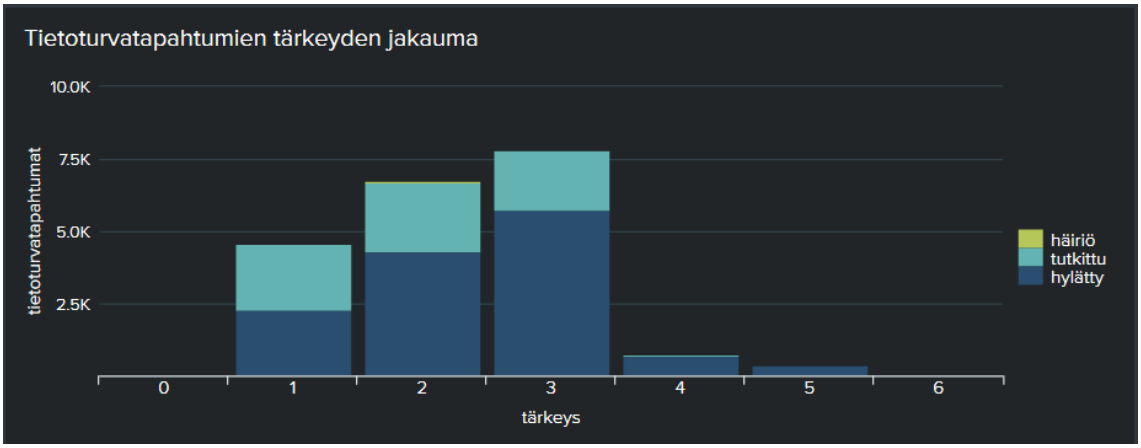
Tietoturvatapahtumia priorisoidaan, eli niitä jaetaan erilaisiin kiireellisyysluokkiin monien tekijöiden perusteella; muun muassa asiakkaalle luvattu palvelutaso, muut sopimukselliset asiat ja tapahtuman riskitaso vaikuttavat.

Tarkastellessa tietoturvatapahtumien priorisointiprosessia havaittiin, että merkittävin pullonkaula tietoturvatapahtumien määrän kasvaessa on riskitason arviointi, sillä se on manuaalisesti suoritettava tehtävä, joka vaatii tapauskohtaista harkintaa, eikä siihen ole yksiselitteistä oikeaa tapaa. Koneellistamalla tietoturvatapahtumien riskitason arviointi, pyritään siis tehokkaampaan ja tasalaatuisempaan kiireellisyysluokitteluun, joka osaltaan tehostaa koko tietoturvatapahtumien arviointiprosessia.

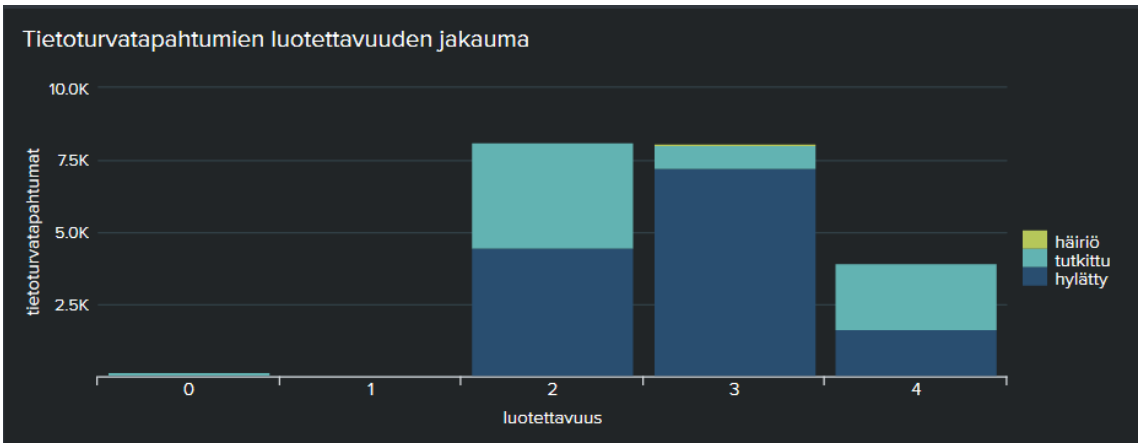
Riskitason arvioinnin kehittämismahdollisuuksiin tutustuminen aloitettiin dokumenttianalyysillä, joka kohdistettiin SIEM-järjestelmän dokumentaatioon. Dokumentaatiosta käy ilmi, että SIEM-järjestelmä tarjoaa puitteet priorisointiin laskemalla tietoturvatapahtumille suhteellisen tärkeyden, joka muodostuu suurelta osin kolmen eri piirteen yhteenlasketuista arvoista: luotettavuus, olennaisuus ja vakavuus.

Seuraavaksi selvitettiin millaisia arvoja tietoturvatapahtumien suhteelliseen tärkeyteen vaikuttavilla piirteillä on nykyisillä asetuksilla. Tätä varten rakennettiin alustavat mittarit (Kuviot 4-7) niiden tarkastelemiseen. Oheisiin mittauksiin on käytetty tilastotietoa useasta SIEM-järjestelmästä yli kuukauden ajanjaksolla.

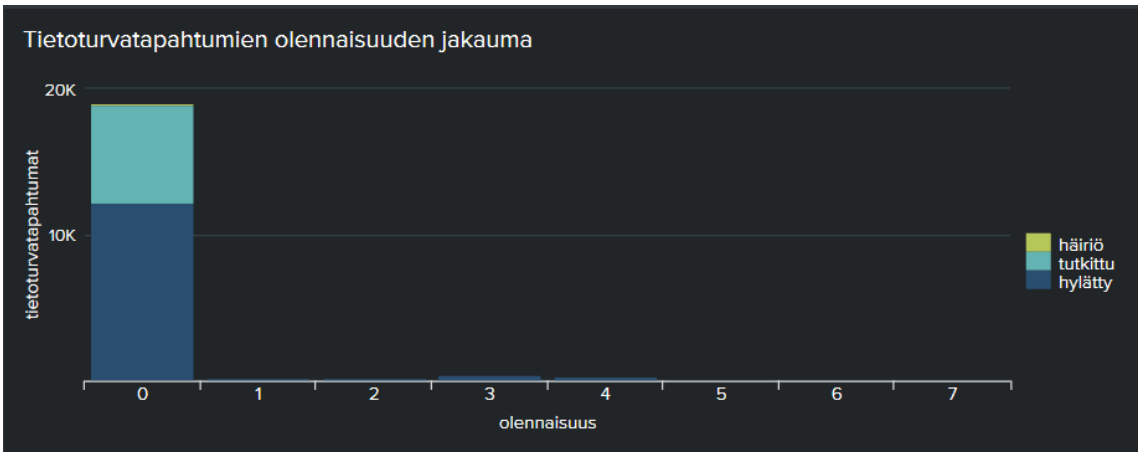
Mittareista voidaan lukea piirteiden arvojen jakauma asteikolla 0-10, jonka lisäksi värikoodi osoittaa tietoturvahäiriöiden, sekä tutkittujen ja hylättyjen tietoturvatapahtumien jakautumisen tietyn arvon sisällä. *Häiriöt* kuvaa raportoitujen tietoturvahäiriöiden määrää, *tutkittu* merkitsee että arvion jälkeen tietoturvatapahtuma todettiin vääräksi hälytykseksi tai luonteeltaan merkityksettömäksi, *hylätyt* puolestaan on metatietojen perusteella karsittu merkityksettöminä pois ennen varsinaista arviointia.



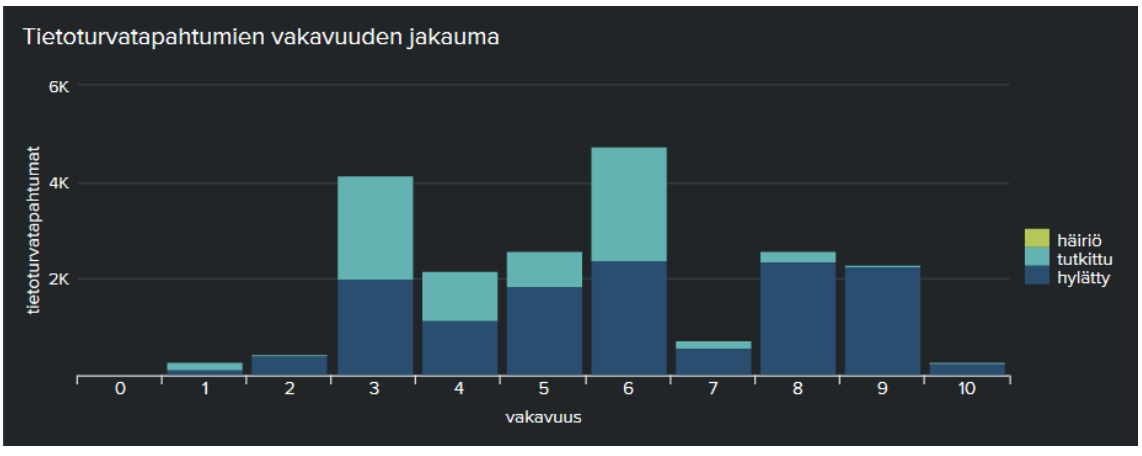
Kuvio 4 - Tietoturvatapahtumien tärkeyden jakauma



Kuvio 5 - Tietoturvatapahtumien luotettavuuden jakauma



Kuvio 6 - Tietoturvatapahtumien olennaisuuden jakauma



Kuvio 7 - Tietoturvatapahtumien vakavuuden jakauma

Mittareista tehtiin seuraavat havainnot:

1. Tilastollinen todennäköisyys, että tietoturvatapahtuma hylätään metatietojen perusteella merkityksettömänä lisääntyy, kun sen tärkeys kasvaa.

2. Luotettavuus- ja olennaisuusarvoja esiintyy kapealla asteikolla ja pienillä lukuarvoilla, eli suurin osa asteikosta ei ole käytössä.

3. Tietoturvahäiriöiden osuus tässä otoksessa on niin pieni, ettei niistä voi tehdä luotettavia johtopäätöksiä

Ensimmäisen havainnon perusteella todettiin, että SIEM-järjestelmän laskema tärkeysarvo ei nykyisellään vastaa tietoturva-analyytikoiden näkemystä. Keskimäärin, tietoturva-analyytikoiden tärkeäksi arvioimat tietoturvatapahtumat saivat SIEM-järjestelmältä alhaisen tärkeysarvon, ja päinvastoin.

Toisen havainnon perusteella todettiin, että nykytilanteessa SIEM-järjestelmät eivät tunnista olennaisuutta ja luotettavuutta oikein, joten arvot jäävät kaikissa tapauksissa mataliksi.

Havaintojen perusteella tarkennettiin kehitystyön tavoitteita. Jotta SIEM-järjestelmän laskemaa suhteellista tärkeyttä voitaisiin käyttää riskitason kaltaisesti tietoturvatapahtumien priorisointiin, on siis muokattava SIEM-järjestelmän asetuksia siten, että sen laskemat luotettavuus-, olennaisuus- ja vakavuusarvot vastaavat paremmin todellista tilannetta.

5.2 Kehittämisprosessin vaiheet

Kehittämisprosessissa oli useita eri vaiheita. Ensimmäisessä vaiheessa tunnistettiin sille asetettavat vaatimukset työn tavoitteiden ja toimeksiantajan tarpeiden pohjalta.

Toisessa vaiheessa tunnistettiin erilaisia tietoturvatapahtumia kuvailevia piirteitä käyttäen menetelminä dokumenttianalyysiä ja miellekarttojen luomista.

Kolmannessa vaiheessa piirteet luokiteltiin SIEM-järjestelmän mukaisiin luokkiin, eli luotettavuuden, olennaisuuden tai vakavuuden alle. Luokittelun yhteydessä yhdistettiin samankaltaisia piirteitä yhteen, ja valittiin jokaisesta luokasta muutama työn tavoitteita parhaiten tukeva, vaatimukset täyttävä piirre jatkoon. Tämän jälkeen jaettiin piirteet SIEM-järjestelmän ominaisuuksien mukaisesti normalisointivaiheeseen ja tapahtumien arviointivaiheeseen.

Neljännessä vaiheessa muodostettiin asteikot piirteiden mittaamista varten.

5.2.1 Vaatimuksien selvittäminen

Opinnäytetyön tavoitteiden asettamisvaiheessa tunnistettiin yhdessä toimeksiantajan kanssa, että kehitettäessä koneellista riskitason arviointimenetelmää, on tärkeää huomioida seuraavat seikat:

- Skaalautuvuus: menetelmän tarkkuus tai tehokkuus ei saa merkittävästi laskea tietoturvatapahtumien tai palveltavien asiakkaiden lukumäärän kasvaessa.
- Objektiivisuus: riskitason arvioiminen ei vaadi subjektiivisia arvioita tietoturva-analyytikoilta kehitystyön valmistuttua.
- Automaattisuus: SIEM-järjestelmällä on oltava käytössään kaikki tarvittava tieto, jotta se voi arvioida riskitason itsenäisesti.
- Toteuttamiskelpoisuus: arviointiin käytettävien piirteiden on oltava riittävän helposti mitattavissa, jotta menetelmän toimeenpanoon ei kulu kohtuuttomasti resursseja. Lisäksi menetelmän on oltava yhteensopiva käytössä olevan SIEM-järjestelmän ominaisuuksien kanssa.

Vaikka SIEM-järjestelmä tarjoaa puitteet riskitason laskemiseen, siihen vaikuttavien luotettavuus-, olennaisuus-, ja vakavuusarvojen määrittäminen jää pitkälti tietoturvavalvomon tehtäväksi. Opinnäytetyön tehtävänä on siis kehittää menetelmä näiden arvojen koneelliseen mittaamiseen siten, että edellä asetetut vaatimukset skaalautuvuuden, objektiivisuuden, automaattisuuden ja toteuttamiskelpoisuuden suhteen täyttyvät.

5.2.2 Piirteiden tunnistaminen

Tämän vaiheen tarkoituksena oli tunnistaa piirteitä, joita voidaan mitata lokitiedosta, skenaarioista ja tietoturvatapahtumista. Näiden piirteiden arvoja tullaan käyttämään luotettavuuden, olennaisuuden ja vakavuuden koneelliseen mittaamiseen. Tunnistamisvaiheessa käytettiin ensisijaisesti dokumenttianalyysia ja täydentävänä menetelmänä luotiin miellekarttoja käsitteiden välisten yhteyksien hahmottamiseksi.

Dokumenttianalyysissä tutkittiin kahden eri valmistajan SIEM-järjestelmien dokumentaatioita: IBM QRadar ja Splunk Enterprise Security. Lisäksi hyödynnettiin ETSI (European Telecommunications Standards Institute) standardia GS ISI 008, joka kuvaa miten SIEM otetaan käyttöön osaksi kokonaisvaltaista kyberpuolustusta. Toisenlaista näkökulmaa haettiin VERIS-projektista, jonka tavoitteena on kehittää tietoturvahäiriöiden kuvaamiseen käytettyä mittaristoa.

Miellekarttamenetelmän tarkoituksena oli tuottaa luovia ideoita dokumenttianalyysin tueksi. Dokumenttianalyysillä tunnistettuja piirteitä jaoteltiin erilaisiin ryhmiin, jotta nähtäisiin, onko syntyvää kokonaiskuvaa mahdollista täydentää vielä tunnistamattomilla piirteillä.

ETSI 008 SIEM standardin mukaan tietoturvatapahtuman kriittisyystaso rakentuu kahdesta elementistä: tapahtuman vakavuudesta ja siihen liittyvän tieto-omaisuuden herkkyydestä. Tieto-

omaisuuden herkkyyttä arvioitaessa on otettava huomioon sen arvo organisaatiolle luottamuksellisuuden, eheyden ja käytettävyyden näkökulmasta. (ETSI 2018.)

Tapahtuman vakavuus muodostuu kolmesta tekijästä: vaarallisuus, huomaamattomuus ja sovellettavuus. Vaarallisuuteen vaikuttavia ominaisuuksia ovat: uhkan suorittamisen tai leviämisen nopeus, vaikuttavuus, vaikutuksen laajuus, etähallintakyky, sitkeys, kontrollien puute ja suojaustasojen läpäisy. Huomaamattomuutta arvioidessa tulee ottaa kantaa tietoturvatapahtuman naamiointiin ja hyökkääjän anonymiteettiin. Sovellettavuuden osatekijöitä ovat hyökkääjän motivaatio, vaadittavat resurssit sekä käytettävissä olevat haavoittuvuudet. (ETSI 2018.)

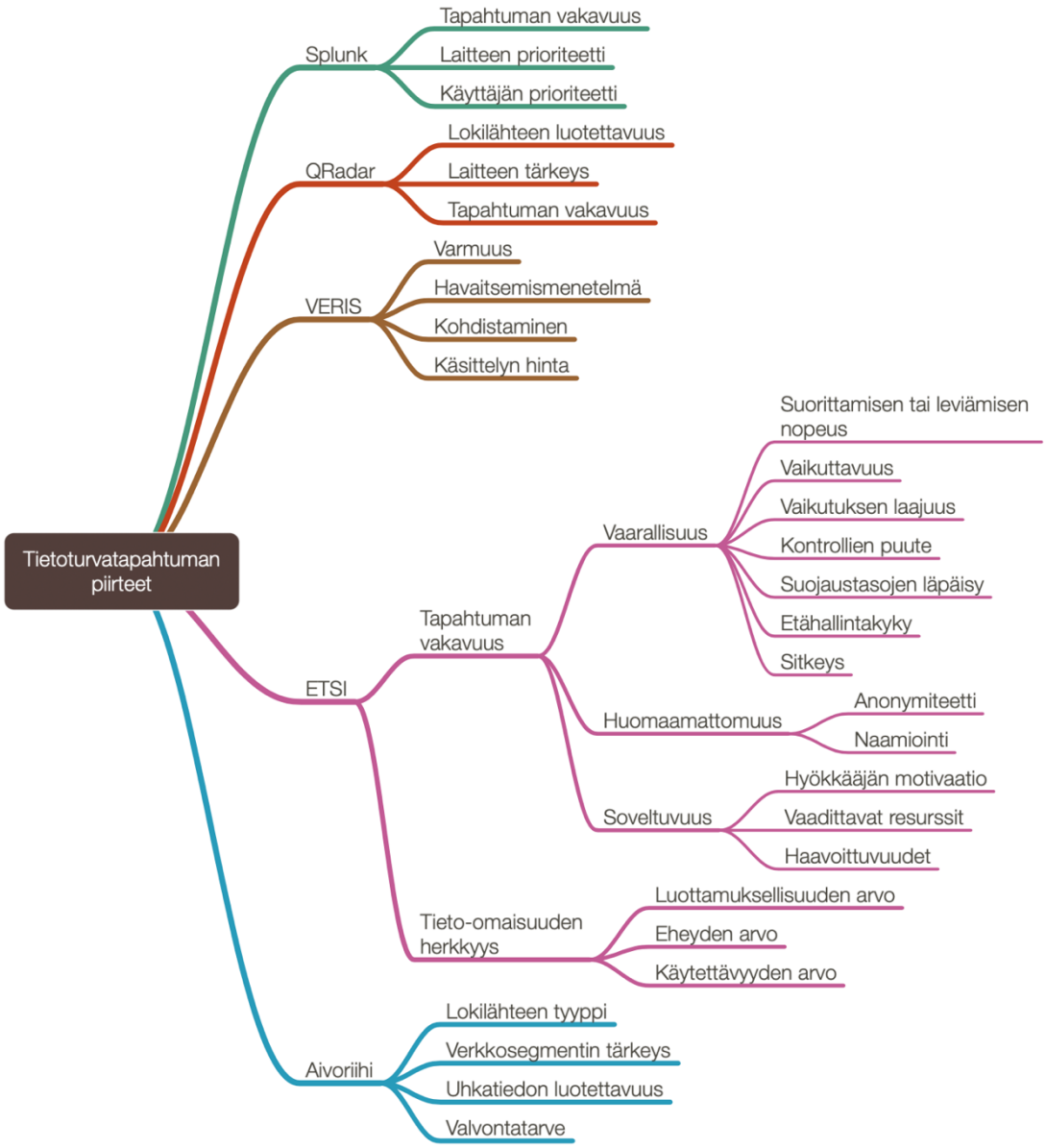
IBM QRadar dokumentaation mukaan tietoturvatapahtuman suhteelliseen tärkeyteen vaikuttaa lokilähteen luotettavuus, tapahtumien vakavuus sekä niihin liittyvien laitteiden tärkeys. Lisäksi huomioidaan tietoturvatapahtuman alusta kulunut aika, tapahtumien ja lokilähteiden lukumäärä, sekä tapahtumien kategoriat. (IBM 2019c.)

Splunk Enterprise Security dokumentaation mukaan kiireellisyyden määrittämiseen käytetään kolmea arvoa: tapahtuman vakavuus, laitteen prioriteetti ja käyttäjän prioriteetti. Mikäli sekä laitteen että käyttäjän prioriteetti on määritelty, ainoastaan suurempi huomioidaan. (Splunk 2019.)

VERIS skeemassa tietoturvahäiriötä kuvataan seuraavilla attribuuteilla: varmuus, havaitsemismenetelmä, kohdistaminen ja käsittelyn hinta (VERIS 2019).

Miellekarttojen luomisen tuloksena tunnistettiin vielä neljä uutta attribuuttia: lokilähteen tyyppi, verkkosegmentin tärkeys, uhkatiedon luotettavuus ja skenaarion valvontatarve.

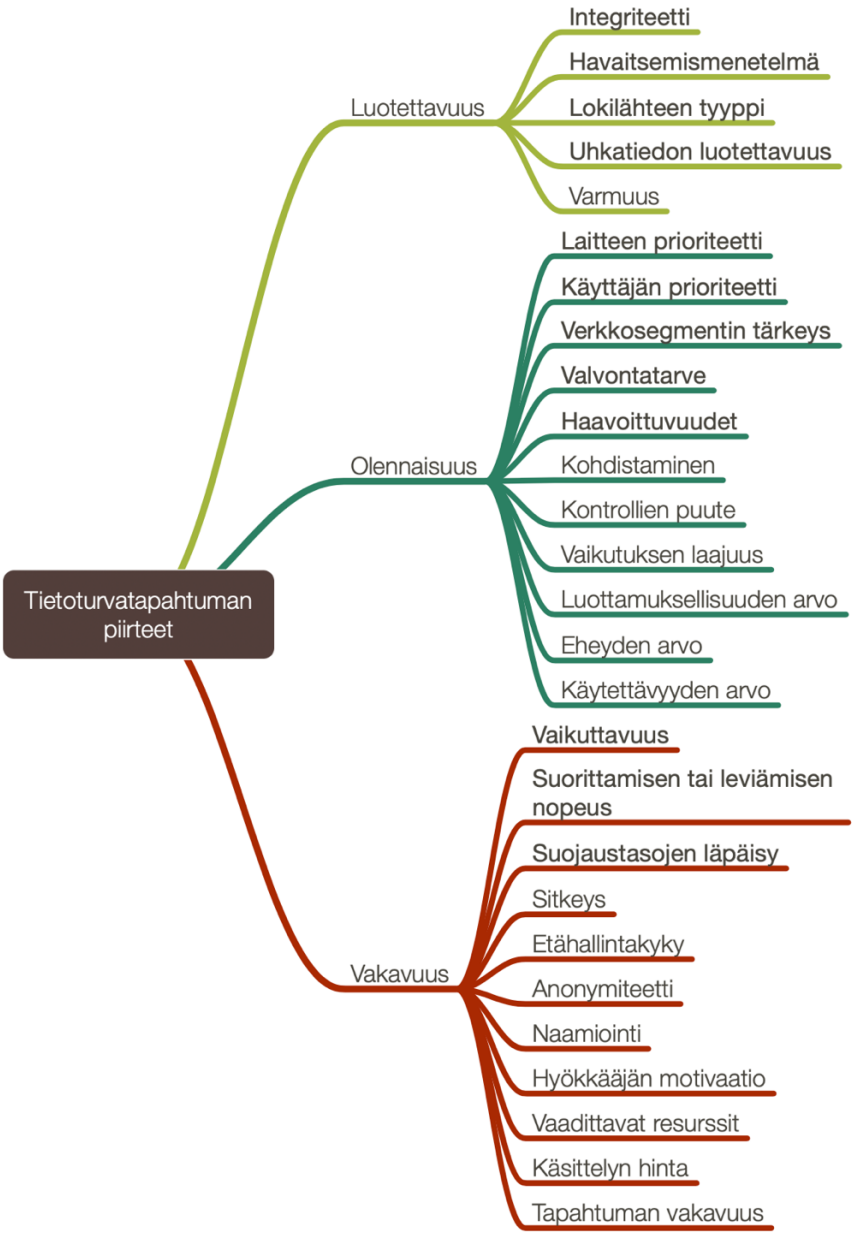
Kuvio 8 havainnollistaa tunnistamisvaiheen tulokset.



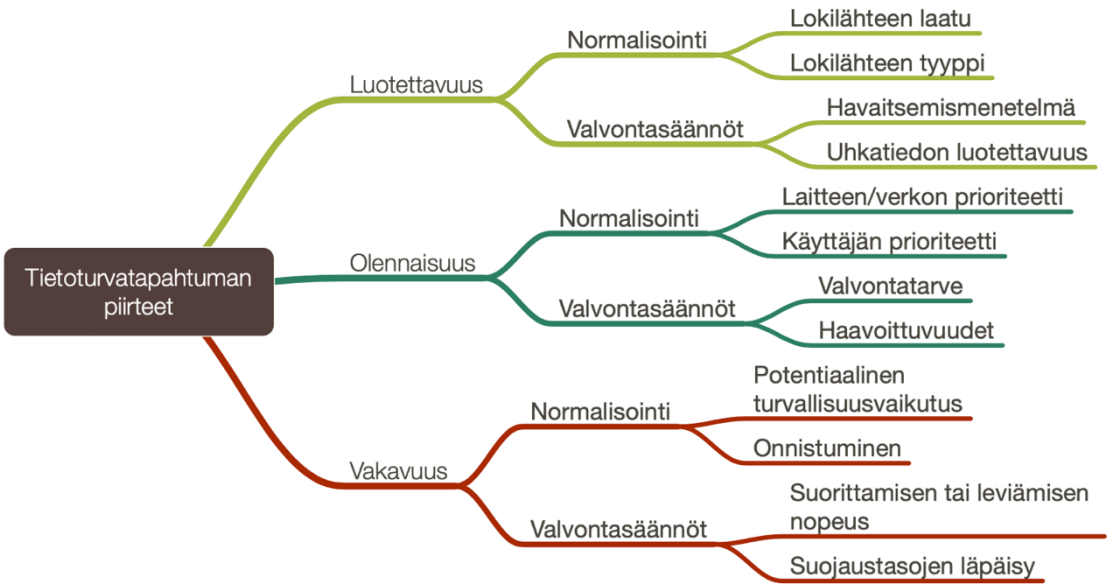
Kuvio 8 - Tunnistamisvaiheen käsitekartta

5.2.3 Piirteiden luokittelu

Tunnistettujen piirteiden luokittelu suoritettiin kahdessa vaiheessa. Ensimmäiseksi tavoitteena oli luokitella tunnistetut piirteet siten, että ne sijoitettiin joko luotettavuuden, olennaisuuden tai vakavuuden yhteyteen, sen mukaa mihin ne ominaisuuksiltaan parhaiten sopivat (Kuvio 9). Toisessa vaiheessa piirteet luokiteltiin edelleen käytettäväksi normalisointivaiheessa ja tapahtumien arviointivaiheessa (Kuvio 10). Jotta menetelmä säilyisi toteuttamiskelpoisena, piirteiden määrä rajoitettiin kahteentoista.



Kuvio 9 - Luokitteluvaiheen käsitekartta, ensimmäinen vaihe



Kuvio 10 - Luokitteluvaiheen käsitekartta, toinen vaihe

5.2.4 Asteikkojen muodostaminen

Asteikkoja muodostettaessa huomioitiin, että tavoitteena on suhteellisen riskitason käyttäminen kiireellisyysluokitteluun, joten arvojen välimatka ei ole olennaista, vain järjestys on merkitsevää. Lisäksi järjestysasteikolla mittaaminen on yksinkertaisempaa verrattuna suhteelliseen asteikkoon, ja siten nopeampaa suorittaa. Näin ollen päädyttiin käyttämään kaikkien piirteiden kohdalla järjestysasteikkoa.

Asteikot ovat viisiportaisia ja jokaiseen portaaseen on liitetty sanallinen kuvaus, josta käy ilmi piirteen tila ja sitä vastaava kokonaisluku. Mittaamisen yhteydessä, eli kun SIEM-järjestelmän asetuksia konfiguroidaan, verrataan piirteen tilaa asteikkoon ja valitaan sitä parhaiten kuvaava arvo asteikosta.

6 Tuotos

Tämän opinnäytetyön tuotoksena tunnistettiin lokitapahtumasta 6 ja skenaariosta 6 mitattavaa piirrettä, joiden perusteella tietoturvatapahtuman riskitaso voidaan arvioida koneellisesti. Jotta kaikki tarvittavat tiedot ovat saatavilla, SIEM-järjestelmään siis syötettävä:

- Lokilähteen tyyppi ja suhteellinen tarkkuus
- Käyttäjien, laitteiden ja verkkojen suhteellinen painoarvo
- Tapahtumien potentiaalinen suhteellinen vaikutus turvallisuuteen sekä tapahtuman onnistuminen/epäonnistuminen
- Skenaarioiden havaitsemismenetelmien suhteellinen tarkkuus
- Uhkatiedon suhteellinen tarkkuus
- Skenaarioiden valvontatarpeen tärkeys asiakkaalle

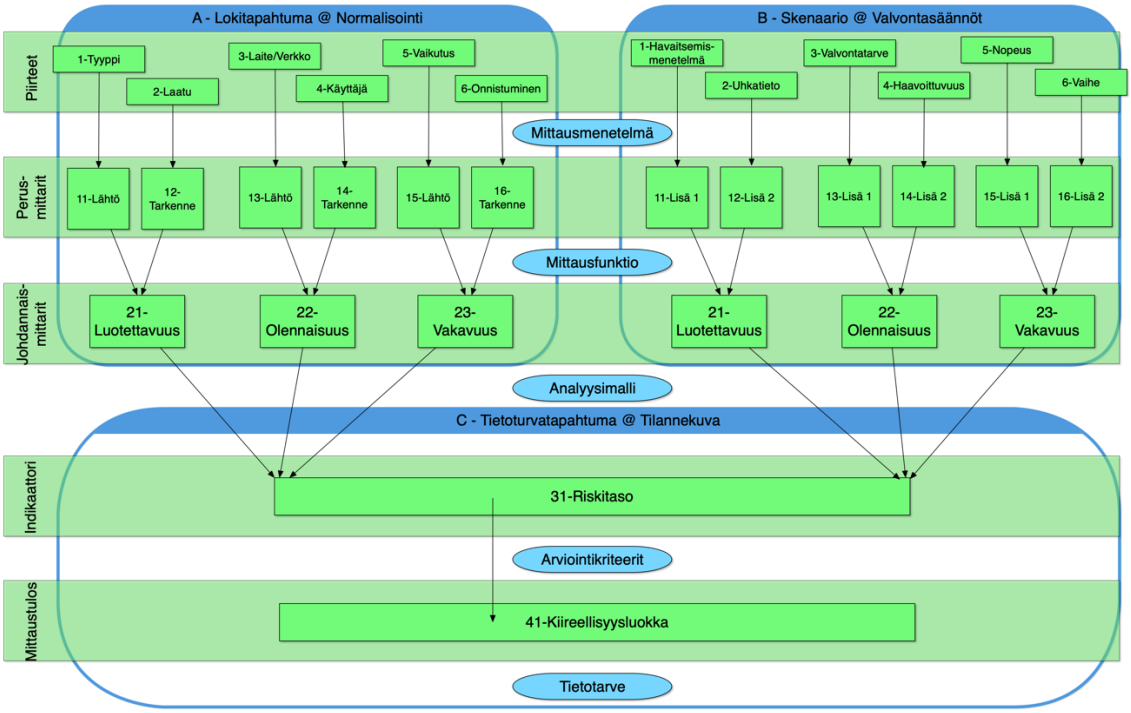
- Valvottavan ympäristön haavoittuvuus skenaarion häiriölle
- Tunnistettujen skenaarioiden vaiheet
- Tunnistettujen skenaarioiden oletetut kehitysnopeudet

Piirteiden mittaamista helpottamaan on luotu Excel-työkalu, joka tukee piirteiden arvojen määrittämistä sanallisilla kuvauksilla ja antaa tuloksena johdannaismittarin arvon.

Piirteiden mittaaminen on osa laajempaa mittausmallia, jonka tavoitteena on vastata tietotarpeeseen, eli tuottaa vastaus kysymykseen: ”Missä järjestyksessä tietoturvatapahtumat tulee arvioida?”.

6.1 Mittausmalli

Oheinen kuvio (Kuvio 11) esittää yleiskuvan tietoturvatapahtumien kiireellisyysluokitteluun käytetyn mittausmallin elementeistä. Elementtejä kuvataan tarkemmin liitteessä 1 (Mittausmallin elementtien kuvaukset).



Kuvio 11 – Yleiskuva tietoturvatapahtumien kiireellisyysluokitteluun käytetyn mittausmallin elementeistä

Lokitapahtuman piirteiden mittaaminen suoritetaan normalisointivaiheessa, skenaarion piirteiden mittaaminen suoritetaan siinä vaiheessa, kun lokitapahtumat arvioidaan valvontasäännöillä. Tietoturvatapahtumaan liitetty indikaattori ja mittaustulokset määräytyvät tilannekuvan muodostamisvaiheessa.

Normalisointivaiheen johdannaismittarit muodostuvat kahden erilaisen perusmittarin — lähtöarvon ja tarkennearvon — yhdistelmänä. Lähtöarvolla on merkittävämpi painoarvo, tarkennearvoa käytetään hienosäätämiseen.

Valvontasääntövaiheen johdannaismittarit muodostuvat kahden samanlaisen perusmittarin — lisäarvo 1 ja lisäarvo 2 — yhdistelmänä.

Mittausmallin rakenteelliset elementit, eli käytetty mittausmenetelmä, mittausfunktio, analyysimalli, arviointikriteerit ja tietotarve esitellään seuraavaksi.

Mittausmenetelmä

Subjektiivista arviointia käyttäen suoritetaan mittaaminen kaikkien piirteiden osalta kerran, jonka jälkeen ohjelmoidaan SIEM-järjestelmä tunnistamaan vastaavat tapaukset tulevaisuudessa.

Mittausfunktio

Johdannaismittarin arvo muodostuu kahden perusmittarin yhdistelmänä.

Analyysimalli

SIEM-järjestelmän algoritmi laskee indikaattorin arvon kaikkien johdannaismittareiden yhdistelmänä.

Arviointikriteerit

Arviointikriteerien avulla katsotaan mihin kiireellisyysluokkaan tietyn riskitason tietoturvatapahtuma kuuluu. Arviointikriteereitä ei ole vielä määritelty, mutta ne voitaisiin määritellä esimerkiksi näin:

Riskitaso	Kiireellisyysluokka
10	1
8-9	2
5-8	3
3-5	4
0-3	5

Taulukko 3 - Esimerkki arviointikriteereistä

Tietotarve

Mittauksen tietotarve on: missä järjestyksessä tietoturvatapahtumat tulee arvioida?

7 Arviointi

7.1 Onnistuminen

Strategisen tason tavoitteena oli parantaa tietoturvahäiriöiden hallintapalvelun tehokkuutta, jotta toimeksiantaja pystyy paremmin vastaamaan kasvavaan kysyntään. Tätä tavoitetta ei ole vielä saavutettu, mutta kun tietoturvatapahtumien koneellinen kiireellisyysluokittelu otetaan käyttöön, sillä toivotaan olevan positiivinen vaikutus palvelun tehokkuuteen.

Konkreettisena päätavoitteena oli kehittää menetelmä tietoturvatapahtumien koneelliseen kiireellisyysluokitteluun riskitason perusteella. Päätavoitetta tukemaan asetettiin kaksi alitavoitetta:

- Tunnistaa ne tietoturvatapahtuman piirteet, jotka oleellisesti vaikuttavat sen riskitasoon.
- Kehittää mittausmalli edellä mainittujen piirteiden mittaamiseen.

Tietoturvatapahtumalle tunnistettiin 12 sen riskitasoon oleellisesti vaikuttavaa piirrettä, joiden mittaamiseksi muodostettiin mittausmalli. Mittausmalli on dokumentoitu ja sen käyttöön on luotu työkalu. Arvioni mukaan päätavoite ja alitavoitteet on saavutettu.

Toimeksiantajan palautteen mukaan kehityskohde oli hyvin valittu, ja riskitason määrittelemiseksi luotu menetelmä on lupaava. Ennen menetelmän käyttöönottoa, on kuitenkin vaikea arvioida sen vaikutuksia ja todellista toteuttamiskelpoisuutta.

7.2 Yleistettävyys

Työ on osittain riippuvainen siitä, että SIEM-järjestelmänä käytetään IBM QRadar tuotetta, sillä tietoturvatapahtumien piirteet on luokiteltu sen mukaisesti luotettavuuden, olennaisuuden ja vakavuuden yhteyteen.

Työ on tehty vastaamaan toimeksiantajan tarpeeseen, joten riippuen toisten toimijoiden lähtötilanteesta, heidän kehitystarpeensa saattavat olla hyvin erilaisia, jolloin tämän opinnäytetyön tulokset eivät välttämättä ole yhtä lailla hyödyllisiä.

7.3 Jatkokehitystarpeet

Nyt kun on kehitetty menetelmä tietoturvatapahtumien koneelliseen kiireellisyysluokitteluun riskitason perusteella, on seuraavaksi ryhdyttävä suunnittelemaan sen teknistä toteutusta, eli käytännössä SIEM-järjestelmän konfiguraatiomuutoksia. Kun muutokset on suunniteltu, on mitattava 12 tunnistetun piirteen arvot ja syötettävä ne järjestelmään.

Menetelmän käyttöönoton vaikutusta on syytä seurata tarkasti, ja arvioida seuraavista näkökulmista:

- Kuinka hyvin koneellisesti laskettu riskitaso vastaa manuaalisesti arvioitua riskitasoa?
- Kasvaako riskitason ja tietoturvahäiriön todennäköisyyden välinen korrelaatio?

- Jakautuvatko luotettavuuden, olennaisuuden ja vakavuuden arvot riittävän tasaisesti asteikolle 0-10?
- Onko mahdollista kehittää tarkempia subjektiivisia mittausmenetelmiä piirteiden mittaamiseen? Entä objektiivisia?

Riskitason määritysmenetelmän käyttöönoton jälkeen arviointikriteerit täytyy sovittaa käytettävissä oleviin resursseihin ja kiireellisyysluokalle asetettuihin käsittelyn tavoiteaikoihin siten, että kiireellisyysluokkaan osuvat tietoturvatapahtumat on mahdollista käsitellä annetun ajan kuluessa. Tämän jälkeen on mahdollista käyttää automaattisesti laskettua riskitasoa koneelliseen kiireellisyysluokitteluun.

Lähteet

ENISA. 2019. ENISA Threat Landscape Report 2018. Viitattu 28.4.2019. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

ETSI. 2018. ETSI GS ISI 008 V1.1.1. Description of an Overall Organization-wide Security Information and Event Management (SIEM) Approach. Viitattu 29.4.2019. https://www.etsi.org/deliver/etsi_gs/ISI/001_099/008/01.01.01_60/gs_ISI008v010101p.pdf

IBM. 2019a. Glossary. Viitattu 22.4.2019. https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/r_qradar_product_glossary.html

IBM. 2019b. How Magnitude Calculation Works. Viitattu 29.4.2019. https://developer.ibm.com/answers/questions/366514/how-magnitude-calculation-works.html

IBM. 2019c. Offense prioritization. Viitattu 28.4.2019. https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_ug_offense_magnitude.html

IBM. 2019d. Data Sheet. Viitattu 23.4.2019. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGD03097USEN&

Ilkka, J., Sahlman, A., Mäntylä, H., Hartikainen, J., Janhunen, K., Grönroos, K., Raappana, M., Kinnunen, P., Heikkinen, P., Niinikorpi, S., Lehtinen, T., Törmälä, J. & Pajunen, K. 2017. Tietoturvapoikkeamatilanteiden hallinta. Valtiovarainministeriö. Viitattu 29.4.2019. http://urn.fi/URN:ISBN:%20978-952-251-930-6

Muckin, M. & Fitch, S. 2019. A Threat-Driven Approach to Cyber Security. Lockheed Martin Corporation. Viitattu 29.4.2019. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf

SFS-ISO/IEC 27000:2016. 2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Suomen Standardisoimisliitto.

SFS-ISO/IEC 27001. 2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto.

SFS-ISO/IEC 27004. 2010. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallinta. Mittaaminen. Suomen Standardisoimisliitto.

SFS-ISO/IEC 27035-1:2016. 2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvahäiriöiden hallinta. Osa 1: Tietoturvahäiriöiden hallinnan periaatteet. Suomen Standardisoimisliitto.

Splunk. 2019. How urgency is assigned to notable events in Splunk Enterprise Security. Viitattu 29.4.2019. https://docs.splunk.com/Documentation/ES/5.3.0/User/Howurgencyisassigned

Tilastokeskus. 2019. Järjestys- eli ordinaaliasteikko. Viitattu 22.4.2019. http://www.stat.fi/meta/kas/ordinaaliasteik.html

Valtionhallinnon tietoturvallisuuden johtoryhmä. 2008. Valtionhallinnon tietoturvasanasto. Viitattu 23.4.2019. https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto

VERIS. 2019. Incident description enumerations. Viitattu 29.4.2019. http://veriscommunity.net/enums.html#section-incident_desc

Julkaisemattomat lähteet

QRadar SIEM. 2019. Tietokoneohjelma. IBM.

Kuviot

Taulukot

Liitteet

Elementti	Kuvaus	Piirteellä korkea arvo	Piirteellä matala arvo
A1 piirre: lokilähteen tyyppi	Eri tyyppiset lokilähteet on asetettu järjestykseen sen perusteella, kuinka usein ne tuottavat tietoturvahäiriöön liittyvää tietoa.	Suuri osa lokilähdetyypin lokitapahtumista liittyy tietoturvahäiriöön.	Pieni osa lokilähdetyypin lokitapahtumista liittyy tietoturvahäiriöön.
A2 piirre: lokilähteen laatu	Lokilähteen laatuun vaikuttaa sen tuottaman tiedon oikeellisuus, ajankohtaisuus ja kattavuus.	Lokilähde tuottaa laadukasta tietoa.	Lokilähde ei tuota laadukasta tietoa.
A3 piirre: laitteen tai verkon painoarvo	Asiakas määrittelee laitteiden ja verkkosegmenttien suhteellisen tärkeyden organisaatiolle.	Laite tai verkko on tärkeä.	Laite tai verkko ei ole tärkeä.
A4 piirre: käyttäjän painoarvo	Asiakas määrittelee käyttäjien suhteellisen tärkeyden organisaatiolle.	Käyttäjä on tärkeä.	Käyttäjä ei ole tärkeä.
A5 piirre: lokitapahtuman vaikutus tietoturvallisuuteen	Tapahtuman potentiaalinen vaikutus tieto-omaisuuden tietoturvallisuuteen.	Potentiaalisesti suuri negatiivinen vaikutus.	Potentiaalisesti pieni negatiivinen tai mikä tahansa positiivinen vaikutus.
A6 piirre: lokitapahtuman onnistuminen/epäonnistuminen	Tapahtuman tulos.	Tapahtuman vaikutukset realisoituivat.	Tapahtumalla ei ollut vaikutusta.
A11 perusmittari: lokilähteen luotettavuuden lähtöarvo	Arvo saadaan mittaamalla piirteen A1 suuruus.	N/A	N/A
A12 perusmittari: lokilähteen luotettavuuden tarkennearvo	Arvo saadaan mittaamalla piirteen A2 suuruus.	N/A	N/A
A13 perusmittari: tieto-omaisuuden olennaisuuden lähtöarvo	Arvo saadaan mittaamalla piirteen A3 suuruus.	N/A	N/A
A14 perusmittari: tieto-omaisuuden olennaisuuden tarkennearvo	Arvo saadaan mittaamalla piirteen A4 suuruus.	N/A	N/A
A15 perusmittari: lokitapahtuman vakavuuden lähtöarvo	Arvo saadaan mittaamalla piirteen A5 suuruus.	N/A	N/A
A16 perusmittari: lokitapahtuman vakavuuden tarkennearvo	Arvo saadaan mittaamalla piirteen A6 suuruus.	N/A	N/A
A21 johdannaismittari: lokitapahtuman luotettavuus	Arvo saadaan perusmittareiden A11 ja A12 yhdistelmänä.	N/A	N/A
A22 johdannaismittari: lokitapahtuman olennaisuus	Arvo saadaan perusmittareiden A13 ja A14 yhdistelmänä.	N/A	N/A
A23 johdannaismittari: lokitapahtuman vakavuus	Arvo saadaan perusmittareiden A15 ja A16 yhdistelmänä.	N/A	N/A
B1 piirre: skenaarion havaitsemismenetelmän luotettavuus	Valvontasäännön luotettavuus vaihtelee monien tekijöiden perusteella.	Valvontasääntö havaitsee oikeat tapahtumat yleensä ja vääriä tapahtumia harvoin.	Valvontasääntö havaitsee oikeita tapahtumia harvoin ja vääriä tapahtumia usein.
B2 piirre: skenaarion liittyvän uhkatiedon luotettavuus	Uhkatiedon luotettavuus vaihtelee monien tekijöiden perusteella.	Uhkatiedon mukainen tapahtuma liittyy usein tietoturvahäiriöön.	Uhkatiedon mukainen tapahtuma liittyy harvoin tietoturvahäiriöön.
B3 piirre: skenaarion valvontatarve	uhkakuvista.	Skenaariolla on suuri merkitys asiakasorganisaatiolle.	Skenaariolla on pieni merkitys asiakasorganisaatiolle.
B4 piirre: skenaarioon liittyvä haavoittuvuus	Haavoittuvuuden vaikutus riippuu muun muassa sen hyväksikäytön helppoudesta ja alttiiden kohteiden määrästä.	Haavoittuvuudelle alttiita kohteita on paljon ja haavoittuuden hyväksikäyttö on helppoa.	Haavoittuvuudelle alttiita kohteita on vähän tai haavoittuvuuden hyväksikäyttö on vaikeaa.
B5 piirre: skenaarion suorittamisen tai leviämisen nopeus	Skenaarion vakavuuteen vaikuttaa se kuinka nopeasti se leviää toisiin kohteisiin.	nopeasti.	Skenaarion negatiivinen vaikutus ei leviä.
B6 piirre: skenaarion toteutumisen vaihe	Skenaarion vakavuuteen vaikuttaa se kuinka pitkälle se on edennyt.	Negatiiviset vaikutukset ovat realisoituneet täysin.	Negatiiviset vaikutukset on torjuttu.
B11 perusmittari: skenaarion luotettavuuden ensimmäinen lisäarvo	Arvo saadaan mittaamalla piirteen B1 suuruus.	N/A	N/A
B12 perusmittari: skenaarion luotettavuuden toinen lisäarvo	Arvo saadaan mittaamalla piirteen B2 suuruus.	N/A	N/A
B13 perusmittari: skenaarion olennaisuuden ensimmäinen lisäarvo	Arvo saadaan mittaamalla piirteen B3 suuruus.	N/A	N/A
B14 perusmittari: skenaarion olennaisuuden toinen lisäarvo	Arvo saadaan mittaamalla piirteen B4 suuruus.	N/A	N/A
B15 perusmittari: skenaarion vakavuuden ensimmäinen lisäarvo	Arvo saadaan mittaamalla piirteen B5 suuruus.	N/A	N/A
B16 perusmittari: skenaarion vakavuuden toinen lisäarvo	Arvo saadaan mittaamalla piirteen B6 suuruus.	N/A	N/A
B21 johdannaismittari: skenaarion luotettavuus	Arvo saadaan perusmittareiden B11 ja B12 yhdistelmänä.	N/A	N/A
B22 johdannaismittari: skenaarion olennaisuus	Arvo saadaan perusmittareiden B13 ja B14 yhdistelmänä.	N/A	N/A
B23 johdannaismittari: skenaarion vakavuus	Arvo saadaan perusmittareiden B15 ja B16 yhdistelmänä.	N/A	N/A
C31 indikaattori: riskitaso	Arvo saadaan analyysimallin tuloksena.		
C41 mittaustulos: kiireellisyysluokka	Arvo saadaan vertaamalla indikaattorin arvoa arviointikriteereihin.		