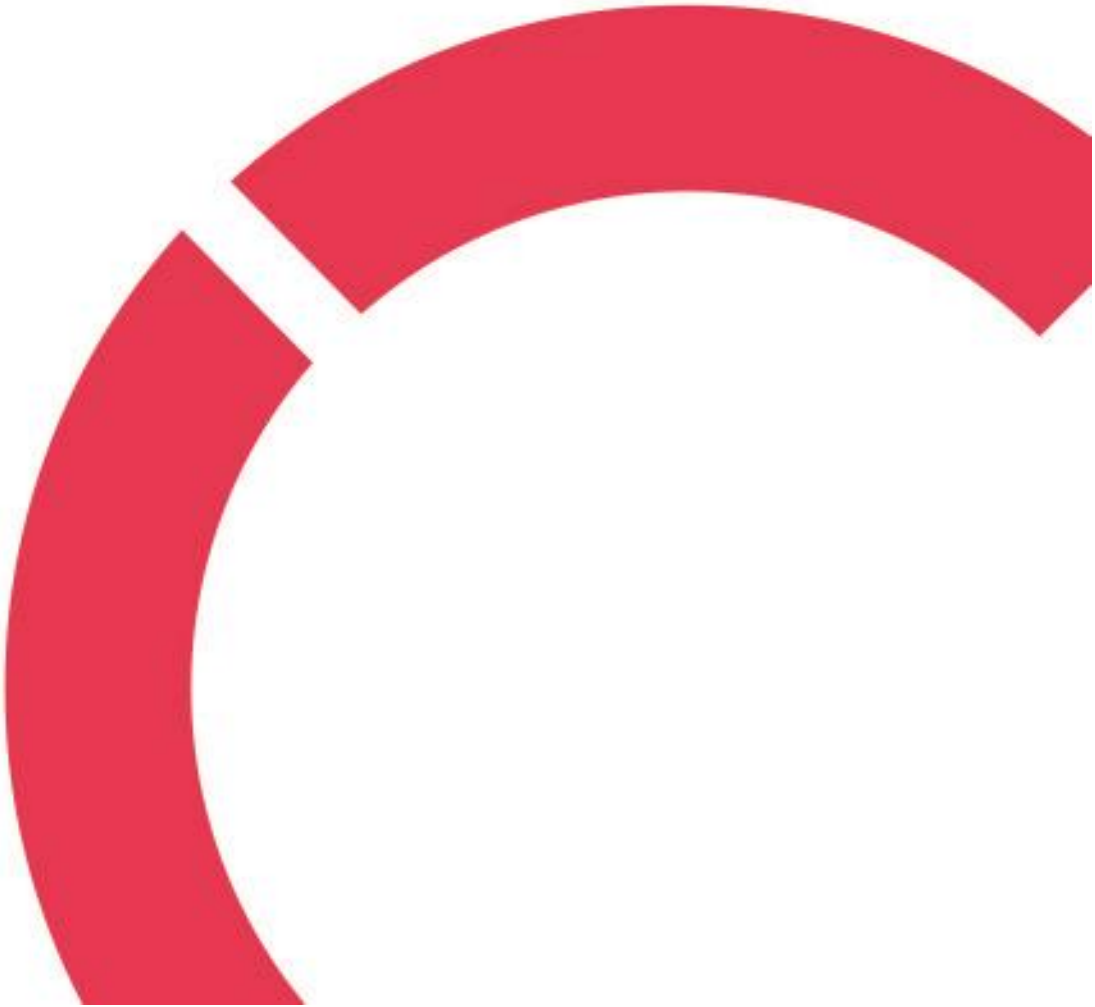
Robert Mustajärvi

SOC-PILOTOINNIN VAIKUTUS TILANNEKUVAAN

Analyysi ja soveltaminen tietoturvan hallintaan

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutus
Elokuu 2023



TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** elokuu 2023	**Tekijä/tekijät** Robert Mustajärvi
Koulutus Tieto- ja viestintätekniikka		☒ AMK ☐ YAMK
Työn nimi SOC-pilotoinnin vaikutus tilannekuvaan: Analyysi ja soveltaminen tietoturvan hallintaan		
Työn ohjaaja Sari Lipsanen		**Sivumäärä** 37 + 2
Työelämäohjaaja Juha Matilainen		

Tämä opinnäytetyö käsitteli DigiTyy-hankkeessa suoritetun SOC-pilotoinnin (Security Operations Center) vaikutusta tietoturvallisuuden tilannekuvaan. Tietoturvan tilannekuva merkitsee organisaation kykyä ymmärtää ja reagoida aktiivisesti uhkiin ja haavoittuvuuksiin, joihin organisaation tiedot ja järjestelmät saattavat olla alttiita. SOC-pilotointi on prosessi, jossa uusi toimintamalli otetaan käyttöön koeluontoisesti ennen laajamittaisempaa käyttöönottoa.

Työssä analysoitiin SOC-pilotoinnin vaikutusta tietoturvan hallintaan ja sitä, miten tämä pilotointi parantaa organisaatioiden tilannekuvaa. Työ tarkastelee erityisesti, kuinka SOC-pilotointi voi parantaa organisaation reagointikykyä, tunnistaa haavoittuvuuksia ja torjua uhkia ja miten se mahdollistaa nopeamman toiminnan tietoturvan kannalta kriittisissä tilanteissa.

Lisäksi opinnäytetyössä tutkittiin, miten SOC-pilotointia voidaan tehokkaasti soveltaa tietoturvan hallintaan. Työssä käsitellään SOC-pilotointiprosessin suunnittelua, toteuttamista ja sen tulosten arviointia, ja tarjotaan käytännön suosituksia SOC-pilotointiprojektien onnistuneeseen läpiviemiseen.

Opinnäytetyön tuloksena saatiin kattava ymmärrys siitä, kuinka SOC-pilotointi voi parantaa tietoturvan tilannekuvaa organisaatioissa, sekä konkreettisia työkaluja SOC-pilottiprojektin suunnitteluun ja toteuttamiseen.

Kalajoen kaupunki hyödyntää tämän opinnäytetyön tuloksia loppuraportoinnin yhteydessä DigiTyy-hankkeen päättyessä.

Asiasanat
DigiTyy-hanke, julkishallinto, Kalajoen kaupunki, organisaatio, pilotti, SOC, tilannekeskus.

ABSTRACT

Centria University of Applied Sciences	**Date** August 2023	**Author** Robert Mustajärvi
Degree programme Information technology		
Name of thesis Impact of SOC Pilot Implementation on Situational Picture: Analysis and Application to Security Management		
Centria supervisor Sari Lipsanen		**Pages** 37 + 2
Instructor representing commissioning institution or company. Juha Matilainen		

This thesis explored the impact of SOC (Security Operations Center) piloting on the situational picture of information security. The situational picture for information security signifies an organization's ability to understand and actively respond to threats and vulnerabilities that the organization's data and systems may be exposed to. SOC piloting is a process where a new information security strategy is trialed on a small scale before wider implementation.

The study analyzed the impact of SOC piloting on information security management and how this piloting enhances the situational picture. The study particularly examined how SOC piloting can improve an organization's response capacity, identify vulnerabilities, ward off threats, and enable quicker action in critical situations regarding information security.

Additionally, the thesis investigated how SOC piloting can be effectively applied to information security management. The study covered the planning, implementation, and evaluation of the SOC piloting process, and offered practical recommendations for successful completion of SOC piloting projects.

As a result of the thesis, a comprehensive understanding of how SOC piloting can improve the situational picture of information security was gained, as well as concrete tools for planning and implementing a SOC pilot project.

The City of Kalajoki will utilize the results of the thesis work in their final report at the conclusion of the DigiTyy project.

Key words
City of Kalajoki, DigiTyy project, organization, pilot, public administration, situation center, SOC.

KÄSITTEIDEN MÄÄRITTELY

Azure AD

Azure AD (Azure Active Directory) on Microsoftin pilvipohjainen hakemisto- ja identiteetinhallinta-palvelu. Käyttäjän kirjautuessa johonkin Office 365-palveluun, tunnistautuu hän samalla Azure AD:tä vasten. Azure AD ei kuitenkaan rajoitu ainoastaan käyttäjien identiteetteihin, vaan sitä voidaan käyttää myös sovelluksien ja laitteiden identiteettien hallintaan.

Digiturva

Yleisesti ottaen digiturvalla tarkoitetaan käytäntöjä ja toimenpiteitä, joiden avulla pyritään suojaamaan tietotekniikkaa, digitaalisia tietoja sekä verkko-omaisuutta. Digiturva voi sisältää vahvojen salasanojen käyttöä, säännöllisiä ohjelmistopäivityksiä, tietosuojakäytäntöjen noudattamista ja varmuuskopioiden luomista tärkeille tiedoille.

EDR

Endpoint Detection and Response (EDR) on järjestelmä, joka keskittyy verkkotietokoneiden tai yleisemmin päätelaitteiden suojaamiseen uhkia vastaan. Uhkia voivat olla virukset, haittaohjelmat ja muut kyberhyökkäykset. EDR-ratkaisu on osa laajempaa tietoturvastrategiaa, joka auttaa suojaamaan organisaation tietoverkkoa ja -järjestelmiä. EDR-järjestelmät keräävät ja tallentavat jatkuvasti dataa päätelaitteilta. Kun jotain epäilyttävää havaitaan, EDR voi automaattisesti ryhtyä toimenpiteisiin, kuten eristämään päätelaitteen muusta verkosta tai lähettämään hälytyksen tietoturvatiimille.

Efecte

Opinnäytetyössä puhuttaessa Efectestä tarkoitetaan sillä eurooppalaista palvelunhallinnan ratkaisua. Efecte tarjoaa asiakkailleen useita eri palvelunhallinnan työkaluja, kuten myös tiketöinti- ja palvelupyynnön hallintajärjestelmiä. SOC-pilotoinnin aikana Efecte toimi ennen kaikkea tikeitöintijärjestelmänä, johon tiketit häiriöistä tehtiin.

Endpoint

Endpoint tarkoittaa suomennettuna päätelaitetta. Se viittaa tietoverkon loppupisteeseen, jossa tietoliikenne alkaa tai päättyy. Päätelaitteita voivat olla mitkä tahansa laitteet, jotka ovat yhteydessä verkkoon ja jotka voivat lähettää ja vastaanottaa tietoa. Yleisimpiä päätelaitteita ovat työasemat ja kannettavat tietokoneet, älypuhelimet ja tabletit, palvelimet sekä IoT-laitteet.

False-positive

Termillä false-positive tarkoitetaan tietoturvassa ja analytiikassa tilannetta, jossa järjestelmä tai työkalu antaa virheellisen ilmoituksen positiivisesta tapahtumasta tai havainnosta, vaikka todellisuudessa kyse ei ole aidosta uhasta tai poikkeamasta. False-positive-ilmoitukset voivat aiheuttaa haittoja ja haasteita. Niiden erottaminen todellisista uhkista vie resursseja ja aikaa. Niitä saatetaan myös tästä syystä jättää huomiotta, joka voi johtaa todellisten uhkien ohittamiseen. False-positive-ilmoitusten vähentämiseksi on tärkeää tehdä järjestelmien ja algoritmien asianmukaisia asetuksia, päivityksiä ja hienosäätöjä.

IDS

Intrusion Detection System (IDS) on tunkeutumisen havaitsemisjärjestelmä, joka valvoo verkkoliikennettä ja tunnistaa epäilyttäviä toimintoja tai uhkia, kuten esimerkiksi tietoturvahyökkäyksiä tai järjestelmän väärinkäyttöä. IDS-järjestelmän toiminta perustuu siihen, että se analysoi jatkuvasti verkkoliikennettä ja vertaa sitä tunnettujen hyökkäysten malleihin tai normaalin liikenteen profiileihin. Liikenteen poiketessa merkittävästi normista tai vastatessa tunnettua hyökkäystä, IDS tuottaa hälytyksen.

Inhouse yhtiö

Inhouse yhtiöllä tarkoitetaan yleisesti osakeyhtiötä, joka on valtion, kunnan tai kuntayhtymän omistuksessa sekä niiden määräysvallan alla. In-house yhtiöiltä tehdyt hankinnat voidaan toteuttaa ilman hankintalain mukaista kilpailutusta.

Insidentti

Insidentti (eng. incident), toisin sanoen tapahtuma voidaan liittää esimerkiksi tietoturvaan. Tällöin puhutaan tietoturva-insidentistä, jolla tarkoitetaan jotakin havaittua tapahtumaa tietoturvan osalta, joka vaatii mahdollista reagointia.

IPS

Intrusion Prevention System (IPS) on tietoturvaratkaisu, joka ei ainoastaan havaitse, vaan myös torjuu aktiivisesti erilaisia kyberhyökkäyksiä ja tunkeutumisyrityksiä. Verrattuna IDS:ään, IPS toimii dynaamisemmin. Havaitessaan mahdollisen uhan, se voi ryhtyä toimenpiteisiin sen torjumiseksi. Toimenpiteitä voivat olla esimerkiksi kyseenalaisten pakettien hylkääminen, yhteyden katkaiseminen hyökkääjään, tai hyökkäyksen tietojen raportointi tietoturva-analyytikolle.

Julkisverkko

Julkisverkko viittaa laajaan verkkoinfrastruktuuriin, joka on saatavilla ja jaettu useiden eri käyttäjien kesken. Julkisverkko toimii vastakohtana yksityiselle verkolle. Internet on yleisin esimerkki julkisverkosta. Se on maailmanlaajuinen julkisverkko, johon miljardit käyttäjät ja organisaatiot ovat yhteydessä. Julkisverkot ovat avoimia ja kaikkien saatavilla olevia verkkoympäristöjä. Julkisverkoissa tieto ja viestintä kulkevat verkon eri solmupisteiden kautta ja voivat olla alttiita tietoturva- ja yksityisyysriskeille.

Kypsyystaso

Organisaatioiden kypsyystasolla tarkoitetaan yksinkertaistettuna sitä, kuinka kehittynyttä, tehokasta ja kattavaa organisaation tietoturvan hallinta ja käytännöt ovat. Kypsyystason määrittämiseen on olemassa erilaisia malleja ja mittareita, joita voivat olla esimerkiksi ISO 27001-standardi tai CMMI (Capability Maturity Model Integration). Kypsyystasoa voidaan korottaa muun muassa selkeiden tietoturvan hallintaprosessien luomisella, tietoturvakoulutuksilla, jatkuvalla seurannalla ja arvioinnilla sekä tietoturvan teknisten ratkaisujen kehittämisellä.

Lokitus

Lokituksella tarkoitetaan tietojen tallentamista tapahtumista tai toiminnoista tietyssä järjestelmässä, sovelluksessa tai verkossa. Tämä on tärkeä tietoturvatoimenpide, joka auttaa tallentamaan ja dokumentoimaan tapahtumia, jotta niitä voidaan myöhemmin tarkastella, analysoida tai tutkia. Tyypillisiä asioita, joita lokitusprosessi tallentaa ovat tietoa ja järjestelmän tiloja tai virheilmoituksia. Tapahtumatieto tallennetaan yleensä lokitiedostoihin tai lokitietokantoihin. Myöhemmin tätä voidaan käyttää tietoturvan valvontaan, ongelmien vianmääritykseen, suorituskyvyn seurantaan, sääntöjen noudattamisen tarkistamiseen tai mahdollisten tietoturvaloukkausten tutkimiseen.

Palomuuri

Palomuurilla tarkoitetaan ohjelmistoa, joka tietokoneeseen asennetaan. Palomuurin tehtävänä on estää haitallinen verkkoliikenne. Näin voidaan estää häiritsevien ja sopimattomien IP-osoitteiden pääsy laitteeseen sekä tietokonetta voidaan suojata viruksilta.

Pilotointi

Pilotoinnilla tarkoitetaan jonkin asian kokeilemista ja validointia mahdollisesti pienemmässä mittakaavassa ennen sen täydellistä käyttöönottoa. Kyseinen asia voi olla esimerkiksi uusi järjestelmä.

SOC

Security Operations Center (SOC) on turvallisuusoperaatiokeskus, joka vastaa organisaation suojaamisesta kyberuhkilta.

Tietoturva

Tietoturva on hieman laajempi käsite verrattuna digiturvaan. Se kattaa kaikenlaisen tietojen ja tietojärjestelmien suojaamisen. Tietoturvan pyrkimyksenä on suojata tietoja luottamuksellisina, varmistaa tietojen eheys ja säilyttämään tietojärjestelmien saatavuus. Usein digiturvaa sekä tietoturvaa käytetään vuorovaikutuksessa toistensa kanssa, vaikka ne ovatkin hieman erillisiä käsitteitä.

Tilannekuva

Tilannekuva viittaa organisaation tai tilanteen kokonaiskäsitykseen tai ymmärrykseen tietystä tilanteesta tai asiayhteydestä. Se perustuu tietoon, joka on kerätty eri lähteistä ja joka auttaa hahmottamaan tilanteen nykytilaa, kehityssuuntia ja mahdollisia uhkia tai haasteita.

Verkkosegmentointi

Verkkosegmentoinnilla tarkoitetaan käytäntöä, jossa suuri verkkoympäristö jaetaan pienempiin osiin tai segmentteihin. Jokainen segmentti toimii erillisenä verkkona, jossa on omat säännöt asetukset ja turvallisuusmekanismit. Tällä tavoin se parantaa verkon turvallisuutta, hallittavuutta sekä suorituskykyä. Verkkosegmentoinnin pääideana on rajoittaa verkossa tapahtuvaa liikennettä ja estää haitallisen liikenteen leviäminen koko verkkoon. Koko verkkoon leviämisen sijaan haitallinen liikenne jää vain yhteen verkon osa-alueeseen.

VPN

Virtual Private Network (VPN) on verkkojen turvallisuustekniikka, jonka avulla yhteys voidaan muodostaa yksityisen verkon ja julkisen verkon välillä. Sen tärkeimpiä tehtäviä on luoda salattu ja turvallinen yhteys käyttäjän laitteen ja VPN-palvelimen välille. Suosituimpia käyttötarkoituksia VPN:lle ovat: Yksityisyyden suojaaminen, tietoturva julkisessa Wi-Fi-verkossa, käyttörajoitusten kiertäminen sekä liiketoiminnalliset tarpeet.

TIIVISTELMÄ

ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

1 JOHDANTO 1

2 TIETOTURVAN HALLINTA JA TILANNEKUVA 3
2.1 Tietoturvan hallinnan perusteet 4
2.2 Tilannekuvan käsite ja merkitys tietoturvan hallinnassa 5

3 SOC-TYÖSKENTELYN PERUSTEET 6

3.1 ERILAISET SOC-TASOT 8
3.2 SOC-järjestelmiä 9

4 PILOTOINNIN JA KOKEILUN EROAVAISUUDET 13

5 SOC-PILOTOINNIN TEORIA JA TOTEUTUS 14
5.1 SOC-palveluun vaaditut prosessit ja toimintamallit 16

6 SOC-PILOTOINTI NUMEROINA 20
6.1 Toimittajan huomiot SOC-pilotoinnista 21
6.2 SOC-pilotoinnin hyödyt 21

7 HAASTATTELUOSIO 22
7.1 Toimittajan haastatteluosio 22
7.2 Organisaatioiden haastatteluosio 26

8 POHDINTA JA JOHTOPÄÄTÖKSET 28
8.1 Pohdinta 28
8.2 Johtopäätökset 29

LÄHTEET 30

1 JOHDANTO

Tietoturvan rooli on noussut yhä keskeisemmäksi organisaatioiden toiminnassa digitalisaation ja tietoverkkojen käytön merkittävän lisääntymisen seurauksena. Tietoverkkoihin kohdistuvia uhkia ja tietomurtoja on enemmän kuin ennen, mikä vaatii organisaatioilta edelleen vahvemman tietoturvan hallinnan ja reagointikyvyn. Security Operations Center (SOC) on toimintakeskus, jonka avulla tietoturvaa on helpompi hallita laajalla skaalalla. SOC vastaa organisaation tietoturvan valvonnasta, uhkien torjumisesta ja niihin reagoinnista.

Tämä opinnäytetyö on tehty Kalajoen kaupungille. Opinnäytetyössä keskitytään DigiTyy-hankkeessa suoritetun SOC-pilotoinnin vaikutukseen tilannekuvan osalta. Opinnäytetyössä käsitellään SOC-pilotointiin osallistuneiden organisaatioiden ajatuksia pilotoinnista ja sitä, kuinka heidän tilannekuvansa on muuttunut SOC-pilotoinnin myötä. Yksityisyyden varmistamiseksi kutsutaan pilotointiin osallistuneita organisaatioita kirjaimilla A, B, C ja D. Organisaatio A on alueella toimiva inhouse yhtiö, joka toimi pilotoinnissa toimittajan roolissa. Organisaatiot B ja C ovat julkishallintoja ja organisaatio D on oppilaitos. Mukana olleiden organisaatioiden tilannekuvaa selvitettiin haastattelemalla kyseisiä organisaatioita SOC-pilotoinnista. Pilottiin osallistuneet organisaatiot ovat tunnistaneet tarpeen vahvistaa tietoturvaa, ja ne pyrkivät parempaan tilannekuvaan uhkien havaitsemiseksi ja niihin reagoimiseksi.

SOC-pilotoinnilla tarkoitetaan SOC:n testaamista ja validointia pienemmässä mittakaavassa ennen sen laajempaa käyttöönottoa. Tämän opinnäytetyön tavoitteena on analysoida SOC-pilotoinnin vaikutusta tilannekuvaan tietoturvan hallinnassa. Tutkimuksessa ja haastatteluissa selvitetään, miten SOC-pilotointi on parantanut Kalajoen kaupungin ja muiden mukana olleiden organisaatioiden tietoturvatilannetta ja mitä haavoittuvuuksia tai poikkeamia pilotoinnin aikana havaittiin. Lisäksi tavoitteena on tarjota suosituksia ja toimenpide-ehdotuksia tietoturvan hallinnan kehittämiseksi mukana olleissa organisaatioissa.

DigiTyy-hanke on valtiovarainministeriön rahoittama hanke, joka on Kalajoen kaupungin ja 18 muun organisaation yhteishanke. Tavoitteena hankkeella on kehittää digitaalisen turvallisuuden prosesseja ja hallintamalleja. Digitaalinen turvallisuus käsittää tietosuojan, tietoturvan, toiminnan jatkuvuuden hallinnan ja varautumisen sekä riskien hallinnan. Hankkeella on digiturvaryhmä, jonka tavoitteina on edistää kuntien ja kuntayhtymän lakisääteisiä velvollisuuksia digitaalisen turvallisuuden osalta. Hankkeen toteutusaika oli 2021–2023 ja hankebudjettina oli 643 100 €.

DigiTyy-hankkeeseen osallistuneita kuntia ja organisaatioita olivat Joki ICT Oy, Jokilaaksojen koulutuskuntayhtymä JEDU, Kalajoki, Kannonkoski, Kempele, Kivijärvi, Koulutuskuntayhtymä Brahe, Kärsämäki, Liminka, Muhos, Nivala, Oulainen, Pyhäjoki, Pyhäjärvi, Raahe, Siikajoki ja Ylivieska. Aiemmin mukana olivat myös Peruspalvelukuntayhtymä Kallio ja Perusturvaliikelaitos Saarikka, jotka siirtyivät hyvinvointialueelle. (Kunta-akkuna 2022.)

2 TIETOTURVAN HALLINTA JA TILANNEKUVA

Tietoturvan hallinta on organisaation prosessi, jonka tarkoituksena on suojata tietoja, tietojärjestelmiä ja tietoverkkoja erilaisilta tietoturvariskeiltä. Tietoturvan hallinnassa hyödynnetään erilaisia käytäntöjä, prosesseja, teknologioita ja toimenpiteitä, joiden avulla pyritään tunnistamaan, estämään, havaitsemaan sekä reagoimaan tietoturvapoikkeamiin ja uhkiin.

Keskeinen osa tietoturvan hallintaa on tilannekuva, joka tarkoittaa organisaation käsitystä sen hetkisestä kokonaisavaltaisesta tietoturvatilanteesta. Tilannekuva perustuu tietoon, joka on kerätty eri lähteistä, kuten tietoturvahälytyksistä, tapahtumalokeista, haavoittuvuusanalyyseistä ja muusta tietoturvadatasta. Tämä tieto auttaa organisaatiota ymmärtämään nykyisen tietoturvatilanteen, havaitsemaan poikkeavuuksia ja mahdollisia uhkia sekä reagoimaan niihin.

Tilannekuva tietoturvan hallinnassa tarjoaa organisaatiolle kokonaisvaltaisen näkymän sen tietoturvaympäristöön. Se auttaa organisaatiota havaitsemaan ja analysoimaan tietoturvapoikkeamia, tunnistamaan haavoittuvuuksia ja riskejä sekä reagoimaan nopeasti mahdollisiin hyökkäyksiin tai uhkiin. Tilannekuvan avulla organisaation on helpompi myös suunnitella ja toteuttaa tietoturvan parantamistoimenpiteitä sekä valvoa niiden tehokkuutta. Tilannekuvan ylläpitäminen ja päivittäminen edellyttää jatkuvaa valvontaa, analyysiä sekä raportointia. Organisaation on kerättävä ja analysoitava tietoa eri tietolähteistä, ja sen on kyettävä korreloimaan ja tulkitsemaan kyseisiä tietoja laajan kokonaiskuvan saamiseksi.

Laajan tilannekuvan saamiseksi organisaatioiden on myös hyödynnettävä teknologioita, kuten tietoturvajärjestelmiä, lokien analysointityökaluja ja keskitettyjä hallintaratkaisuja, kuten SIEM- ja SOC-järjestelmiä. Lisäksi organisaatioiden on kehitettävä ja noudatettava selkeitä tietoturvakäytäntöjä, koulutettava henkilöstöä tietoturvasta ja varmistettava tietoturvakäytäntöjen tehokas täytäntöönpano.

Tietoturvan hallinta ja tilannekuva eivät ole kertaluonteisia toimenpiteitä, vaan jatkuva prosessi, joka vaatii organisaation sitoutumista ja jatkuvaa kehittämistä. Organisaatioiden on pysyttävä ajan tasalla uusista tietoturvauhkista, tekniikoista ja parhaista käytännöistä sekä säännöllisesti arvioitava tietoturvatoimenpiteidensä tehokkuutta.

Tietoturvan hallinta ja tilannekuva ovat elintärkeitä organisaation tietoturvatoimien menestykselle. Ne tarjoavat mahdollisuuden havaita, reagoida ja ennaltaehkäistä tietoturvapoikkeamia sekä pitää organisaation tieto ja järjestelmät turvassa. Vahva tietoturvan hallinta ja kattava tilannekuva luovat perustan luottamuksella, kestävälle liiketoiminnalle ja vastuulliselle tietoturvatoiminnalle.

2.1 Tietoturvan hallinnan perusteet

Tietoturvan hallinnan perusteet keskittyvät organisaation tietovarojen suojaamiseen, sekä tietoturvariskien tunnistamiseen, arviointiin ja hallintaan. Sen tarkoitus on varmistaa tiedon luottamuksellisuus, eheys ja saatavuus. Seuraavana listattuna joitakin tietoturvan hallinnan perusteita:

1. **Tietoturvastrategia:** Tämä on suunnitelma siitä, kuinka organisaatio aikoo suojata tietovaransa ja hallita tietoturvariskejä. Strategian pitäisi sisältää suunnitelmat erityyppisten uhkien, kuten hakkeroinnin, haittaohjelmien, fyysisten uhkien ja sisäisten uhkien varalle. Strategia tulisi myös päivittää säännöllisesti, jotta se pysyy ajan tasalla uusien uhkien ja tekniikoiden suhteen.

2. **Tietoturvakäytännöt ja -protokollat:** Nämä ovat ohjeita siitä, kuinka henkilöstön tulee käsitellä tietoa ja teknologiaa turvallisesti. Tähän voi kuulua esimerkiksi ohjeet siitä, miten luodaan turvallisia salasanoja, miten tunnistetaan huijausviestit tai miten käytetään turvallisia yhteyksiä.

3. **Tietoturvakoulutus:** Henkilöstön tietoturvakoulutus on tärkeä osa tietoturvan hallintaa. Koulutus voi auttaa ihmisiä ymmärtämään tietoturvariskit ja oppimaan, kuinka suojautua niiltä. Koulutus voi auttaa ihmisiä ymmärtämään tietoturvariskit ja oppimaan, kuinka suojautua niiltä. Koulutus voi myös auttaa luomaan tietoturvallisen kulttuurin organisaatiossa.

4. **Tekniset tietoturvatoimet:** Teknisten tietoturvatoimien tarkoitus on suojata tietoa teknisesti. Tämä voi sisältää esimerkiksi palomuurit, haittaohjelmien torjuntaohjelmat, tunkeutumisen havaitsemisjärjestelmät ja kryptaus.

5. **Säännöllinen tarkistus ja auditointi:** Tietoturvan hallintaan tulisi sisältyä säännöllinen tarkistus ja auditointi, jotta voidaan varmistaa, että tietoturvastrategiat ja -toimet ovat tehokkaita. Auditointi voi paljastaa mahdollisia heikkouksia tai aukkoja, jotka voidaan korjata.

6. **Tietoturva-insidenttien hallinta:** Tämä viittaa prosessiin, joka seuraa ja hallitsee tietoturva-insidenttejä. Sen tavoitteena on minimoida vahingot ja palauttaa normaali toiminta mahdollisimman nopeasti. (Kyberturvallisuuskeskus 2020.)

2.2 Tilannekuvan käsite ja merkitys tietoturvan hallinnassa

Tilannekuva on termi, jota käytetään useissa eri yhteyksissä, mutta tietoturvan hallinnassa se tarkoittaa yleensä kykyä nähdä ja ymmärtää organisaation koko tietoturvatilanne reaaliajassa. Tämä sisältää kaiken, mukaan lukien nykyiset tietoturvauhat, mahdolliset tietoturvauhat ja organisaation kyvyn vastata niihin. Tilannekuvan ymmärtäminen on välttämätöntä tehokkaan tietoturvan hallinnan kannalta, koska se auttaa organisaatiota tunnistamaan ja reagoimaan tietoturvatapahtumiin ja -uhkiin.

Tietoturvan hallinnassa tilannekuva voi koostua seuraavista osatekijöistä:

1. **Uhkatietoisuus:** Tällä tarkoitetaan sitä, että organisaatio ymmärtää erilaisia tietoturvariskejä ja -uhkia, joita se saattaa kohdata. Tähän voi kuulua esimerkiksi tietoja erilaisista hakkerointitekniikoista, haittaohjelmista ja muista uhista, jotka saattavat vaarantaa organisaation tietoturvan.

2. **Välikohtaisten ja loppupisteen suojausten tila:** Tämä kuvastaa organisaation tietoturvaratkaisujen nykyistä tilaa. Tämä voi sisältää esimerkiksi tietoja palomuurien tilasta, virustorjuntaohjelmien päivitystilasta ja muista tietoturvatoimenpiteistä.

3. **Haavoittuvuustiedot:** Tämä tarkoittaa tietoa mahdollisista haavoittuvuuksista organisaation järjestelmissä, sovelluksissa tai laitteissa, jotka voivat mahdollistaa tietoturvaiskun.

4. **Insidenttien hallinta ja vaste:** Tämä viittaa organisaation kykyyn tunnistaa, seurata ja reagoida tietoturvatapahtumiin tai -insidentteihin. (DigiTyy-hanke 2023.)

3 SOC-TYÖSKENTELYN PERUSTEET

Security Operations Center (SOC) on tärkeä osa organisaation tietoturvan ekosysteemiä. SOC:n tärkeimpiä tehtäviä ovat organisaation verkkojen, palvelimien, päätelaitteiden, tietokantojen ja muiden järjestelmien tietoturvavalvonnan järjestäminen, tietoturvaloukkausten ennaltaehkäiseminen ja tietoturvatapahtumien hallinta ja vastaaminen. (Logpoint 2020.)

SOC:ssa työskentelee erityisesti tietoturvallisuuden asiantuntijoita, joihin kuuluu tietoturvainsinöörejä, analyytikoita ja johtajia. Yleisimpiä perustehtäviä SOC:n parissa työskenteleville ovat:

1. **Valvonta ja havainnointi:** SOC:n henkilöstö valvoo jatkuvasti organisaation tietojärjestelmien turvallisuustilannetta. He käyttävät usein tietoturvavalvontaan tarkoitettuja työkaluja ja ohjelmistoja, jotka auttavat tunnistamaan mahdollisia uhkia tai epäilyttävää toimintaa.

2. **Uhkien havaitseminen ja analysointi**: Havaitessaan mahdollisen tietoturvatapahtuman SOC:n analyytikot arvioivat sen vakavuuden, laajuuden ja vaikutuksen. Tämä sisältää usein uhkien tarkemman analyysin, kuten miten hyökkäys toteutettiin, mihin järjestelmiin se vaikutti ja miten hyökkäystä voidaan ehkäistä tulevaisuudessa.

3. **Vaste toimenpiteet:** Jos tietoturvatapahtuma havaitaan, SOC:n tehtävä on johtaa tilanteeseen vastaamista, mukaan lukien hyökkäyksen lopettaminen, sen vaikutusten minimointi, järjestelmien palauttaminen normaalitilaan ja parannusten tekeminen järjestelmien suojauksessa.

4. **Raportointi ja viestintä:** SOC:n tehtävänä on myös raportoida tietoturvatilanteesta organisaation johdolle ja muille sidosryhmille. Tämä sisältää tietoa uhkista, tietoturvatapahtumista, niiden vaikutuksista ja toteutetuista vastatoimenpiteistä.

5. **Jatkuva parantaminen:** SOC:n tulee jatkuvasti parantaa tietoturvatoimintojaan. Tämä voi sisältää uusien tietoturvatyökalujen ja -tekniikoiden tutkimista, tietoturvakäytäntöjen ja -prosessien päivittämistä, henkilöstön koulutusta ja tietoturvavalvontatoimintojen tehostamista. (Microsoft 2023.)

SOC:ssa työskentely edellyttää laaja-alaista osaamista tietoturvan, verkkojen ja järjestelmänhallinnan alueilta. Henkilökunnan tulee olla taitavia monimutkaisessa ongelmanratkaisussa, ja heidän on kyettävä reagoimaan nopeasti ja tehokkaasti uhkiin. Tämän lisäksi heidän on ymmärrettävä tietoturvan perusperiaatteet ja -käytännöt, erityyppiset tietoturva- ja hyökkäystekniikat sekä erilaiset tietoturvatyökalut ja -tekniikat.

Työskentely SOC:ssa voi olla stressaavaa, koska tehtävät voivat olla kiireellisiä ja työskentelyaikataulu voi olla epäsäännöllinen, varsinkin jos organisaation tietoturvauhkien torjuminen tapahtuu 24/7, eli kellonympäri. Samalla työskentely SOC:ssa tarjoaa mahdollisuuden oppia uusinta tietoturvatekniikkaa, tehdä tiivistä yhteistyötä muiden tietoturva-asiantuntijoiden kanssa ja toimia ensilinjan puolustajana organisaation tietoturvauhkia vastaan. (Crowdstrike 2022.)

SOC itsessään kasvattaa organisaation reagointikyvykkyyttä huomattavasti. Palvelua tai pilotointia suunnitellessa kannattaa huomio kiinnittää kuitenkin myös näihin asioihin:

- Tiedon jakaminen ja viestintä
- Joustavat toimintamallit
- Teknologian hyödyntäminen
- Henkilöstön koulutus ja kehitys
- Riskienhallinta ja ennakoiva suunnittelu

Ainakin nämä asiat huomioitaessa organisaation reagointikyvykkyys on parempaa. Oikeanlaisella viestinnällä ja tiedonjakamisella kaikki ymmärtävät tavoitteet paremmin. Joustavilla toimintamalleilla organisaation on helpompaa mukautua muuttuviin olosuhteisiin nopeammin. Uusimmilla teknologioilla organisaatio voi tehostaa prosessejaan. Henkilöstön jatkuvalla kouluttamisella saadaan parempi mukautuvuus uusiin työtehtäviin, jolloin organisaation reagointikyky nopeutuu edelleen. Riskienhallinta ja ennakoiva suunnittelu on tärkeä osa reagointikyvykkyyden saavuttamista, koska organisaation on helpompi ennakoida ja valmistautua tuleviin mahdollisiin haasteisiin. Hätätilanteen sattuessa vastuut ja tehtävät ovat selvillä, jolloin itse ongelmaan pystytään keskittyä paremmin. (DigiTyy-hanke 2023.)

3.1 ERILAISET SOC-TASOT

3.1.1 Taso 1

Taso 1 SOC:ssa työskentelee useimmiten niin kutsutut etulinjan työntekijät. Tämä tarkoittaa sitä, että nämä työntekijät ovat vastuussa ensimmäisestä vasteesta ja uusien hälytyksien seurannasta. Usein Taso 1 SOC:ssa työskentelevät käyttävät automatisoituja työkaluja, joiden avulla he seuraavat ja analysoivat tapahtumia. Tapahtuman havainnoinnin jälkeen he tekevät alustavan tarkastelun ja luokittelun tapahtumille.

Taso 1:n työntekijät usein raportoivat haastavammat ja lisää selvitystä vaativat ongelmat tai tapahtumat ylemmille SOC-tasoille. Taso 1:llä työskentelevien henkilöiden tittelit ovat useimmiten SOC-analyytikko tai Security Analyst I. Taso 1:n käyttämät työkalut ovat usein erilaiset SIEM-työkalut. Näitä voivat olla esimerkiksi IBM QRadar, Splunk, Microsoft Sentinel tai LogRhythm.

3.1.2 Taso 2

Taso 2 SOC-tiimin jäsenet ovat kokeneempia analyytikoita, jotka käsittelevät ja ratkaisevat monimutkaisempia tehtäviä. Heidän tehtävänään on suorittaa syvällisempiä analyyseja ja tutkimuksia niistä tapahtumista, joita Taso 1:n työntekijät ovat havainneet. Taso 2:lla on käytössä edistyneempiä työkaluja, menetelmiä ja teknologioita tietoturvaongelmien ratkaisemista varten.

Yleisimpiä titteleitä tällä tasolla työskentelevillä ovat Senior Security Analyst tai Security Analyst II. Tällä tasolla työskentelevillä on yleensä enemmän kokemusta ja tietotaitoa kuin taso 1-analyytikoilla. Tällä tasolla käytetään usein samoja työkaluja, kuin alemmallakin tasolla, mutta tehokkaammin tai laajemmin ja syvällisemmin. Heillä voi olla käytössä työkaluja, kuten FireEye tai CrowdStrike, jotka havaitsevat kehittyneempiä uhkia, joita ei välttämättä voi havaita perinteisemmillä työkaluilla. Ohjelmistot, kuten: FTK tai EnCase auttavat tutkimaan tietoturvahyökkäyksiä ja auttavat myös keräämään todisteita tapahtumista.

3.1.3 Taso 3

Taso 3:ssa työskentelevät henkilöt ovat SOC-tiimin asiantuntijoita, joilla on yleensä kaikista tasoista syvin ja laajin tietoturvaosaaminen. He käsittelevät kaikkein monimutkaisimpia ja vakavimpia tietoturvaongelmia. Töiden ohessa he myös suunnittelevat ja toteuttavat strategisia tietoturvatoimenpiteitä ja

parannuksia sekä tekevät myös ennaltaehkäiseviä tietoturvatoimia. Heillä on myös kyky johtaa tapahtuneiden tietoturvaloukkausten tutkimista ja selvittämistä.

Tällä tasolla työskentelevät usein Lead Security Analystit, Security Engineerit tai Security Analyst III:set. Nämä työntekijät ovat SOC-tiimin kaikkein kokeneimpia ja asiantuntevimpia jäseniä. Usein on mahdollista, että tiimissä työskentelee myös SOC-päällikkö (SOC Manager), joka vastaa koko SOC-tiimin toiminnasta ja suorituskyvystä. Tällä tasolla työskentelevillä henkilöillä on käytössään kaikkein edistyneimmät työkalut. Taso 3:n työntekijät käyttävät myös samoja työkaluja, kuin alemmilla tasoilla, mutta edelleen tehokkaammin, kuin taso 2:lla. Taso 3:n työntekijöillä on käytössä myös erilaisia ohjelmia, kuten Cuckoo Sandbox tai VirusTotal, jotka auttavat analysoimaan haittaohjelmia. Tällä tasolla voidaan käyttää myös SOAR:a ja penetraatiotyökaluja, kuten Kali Linux. Kali Linuxin avulla työntekijät voivat testata tietoturvajärjestelmien haavoittuvuuksia ja suunnitella sen avulla parempaa suojautumista. (Letsdefend 2022.)

3.2 SOC-järjestelmiä

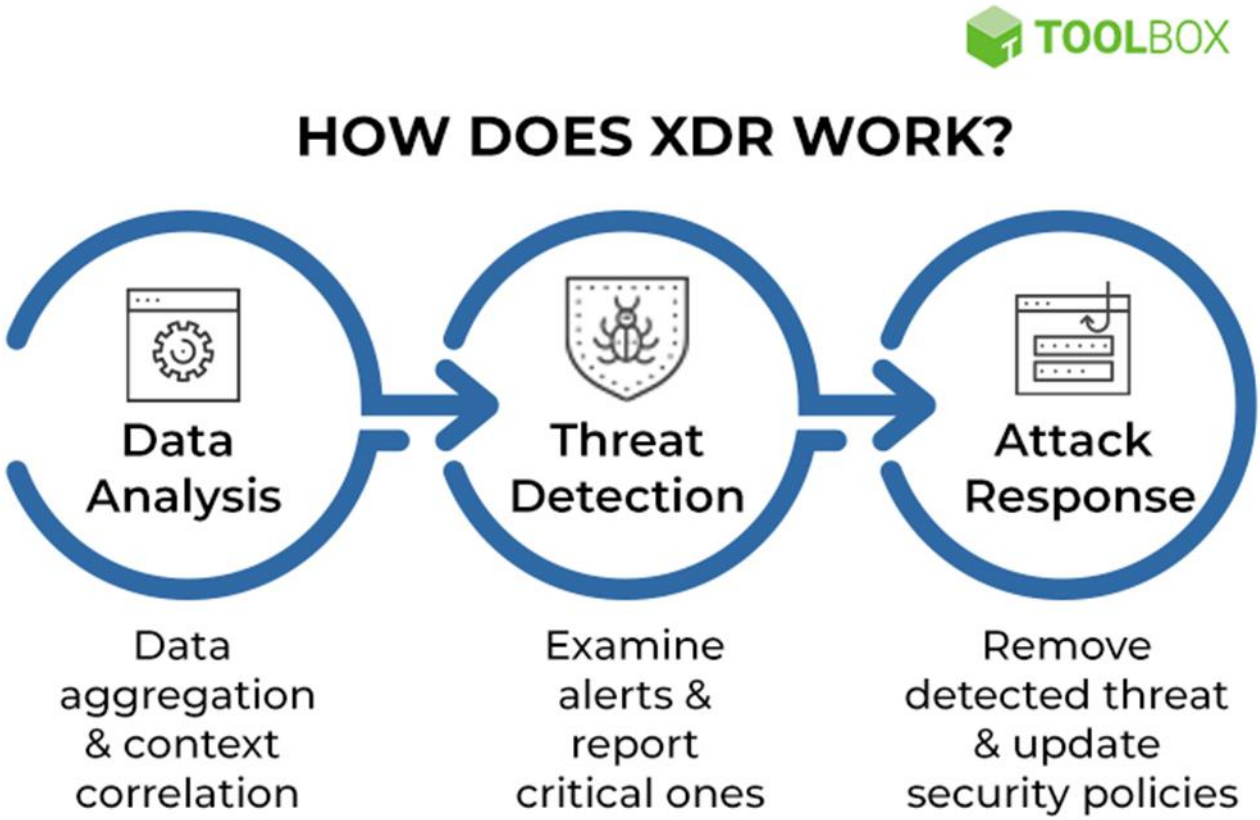
3.2.1 XDR

XDR (Extended Detection and Response) on kehittyneempi versio EDR:stä ja se onkin nyt käytännössä korvannut EDR:n tietoturva-alalla. XDR on suunniteltu olemaan helppo ottaa käyttöön ja ylläpitää. XDR-ohjelmisto auttaa tietoturvatiimejä ratkaisemaan tietoturva tapahtumia keskittämällä, standardoimalla sekä korreloimalla erilaisia turvatietoja useasta eri lähteestä. Tällä tavalla saadaan lisää havainnointikykyä verrattuna EDR:n. XDR tarjoaa täydellisemmän näkyvyyden käyttäen verkkoaineistoa haavoittuvien päätelaitteiden seurantaa varten. EDR-työkalut eivät löydä tällaisia haavoittuvuuksia joko yhtä laajasti tai lainkaan. XDR analysoi tietoja useista eri lähteistä, kuten: sähköposteista, päätelaitteista, palvelimista, verkoista, pilvipalveluista, AzureAD:sta. XDR:n skannatessa tietoturva tapahtumia näin laajasti, se parantaa tietoturvatiimien tehokkuutta huomattavasti. (Orangecyberdefense 2023.)

Mitä tapahtuu, jos XDR havaitsee uhan, jota se ei tunne entuudestaan, eikä sillä ole ennalta määriteltyjä protokollia kyseistä uhkaa varten? Tällaisissa tilanteissa XDR kuitenkin tunnistaa epänormaalia tai epäilyttävää toimintaa, vaikka uhka ei olisikaan aiemmin tunnettu. Ensimmäisenä XDR tekee hälytyksen havaitusta riskistä tai uhasta. Hälytyksessä on yleensä tiedot siitä, mitä on havaittu, missä on havaittu ja milloin on havaittu. Hälytyksessä saattaa olla myös tarkempia tietoja havainnosta, joita voivat

olla IP-osoitteet, käyttäjätiedot tai muut teknisemmät tiedot. Hälytyksen luomisen jälkeen XDR kuitenkin yrittää vielä estää uhkaa automaattisesti, ennen SOC-työntekijän asiaan puuttumista. Uhan estämiseen liittyviä toimintoja ovat monesti: kyseenalaisten prosessien tappaminen, epäilyttävien tiedostojen eristäminen tai pääsyn estäminen verkko-osoitteisiin, jotka kyseiseen uhkaan on liitetty.

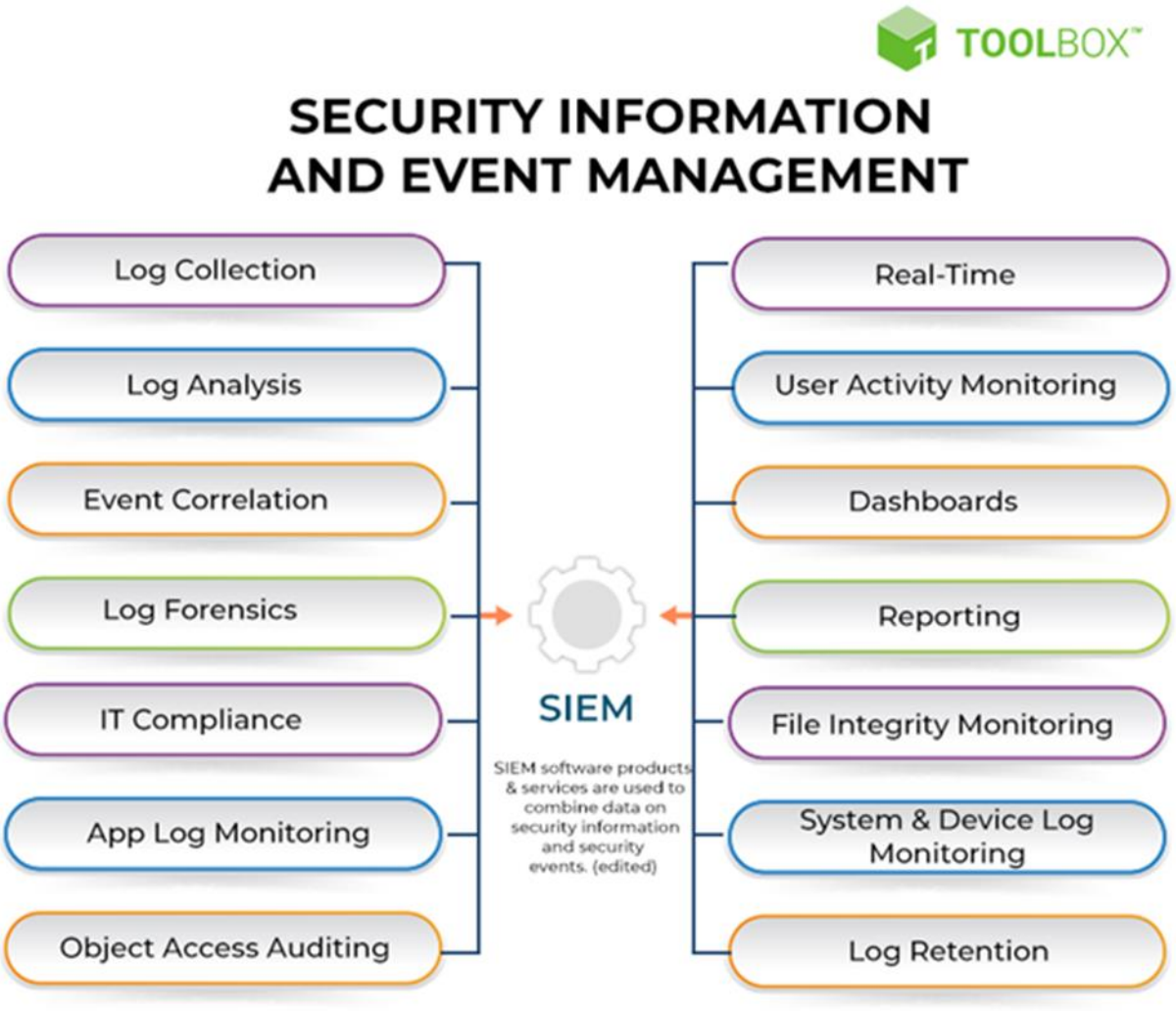
XDR:ssä on puutteena se, että siinä on usein valmiiksi määriteltyjä sääntöjä ja hälytyksiä, jotka toimivat oikein hyvin useimmissa perustilanteissa, mutta se ei välttämättä tarjoa samankaltaista syvää ja yksityiskohtaisempaa mukauttamista, joita SIEM-työkalulla voisi mahdollisesti saavuttaa. Mikäli organisaatiolla on tarpeellista säätää ja mukauttaa järjestelmää tarpeidensa mukaan, voisi SIEM olla tähän hyvä ratkaisu. Nopea ja helpompi, mutta samalla kalliimpi ratkaisu on XDR, joka tarjoaa hyvää suojausta suurimmalle osalle tietoturvariskejä. Lyhyesti sanottuna, SIEM toimii enemmän niin sanotusti käsipelillä, kun taas XDR toiminta on sisäänrakennettujen valmiiden protokollien vuoksi automaattista ja nopeampaa. (Kanade, V 2022.)



Kuva 1. Miten XDR toimii? (Spiceworks 2023.)

3.2.2 SIEM

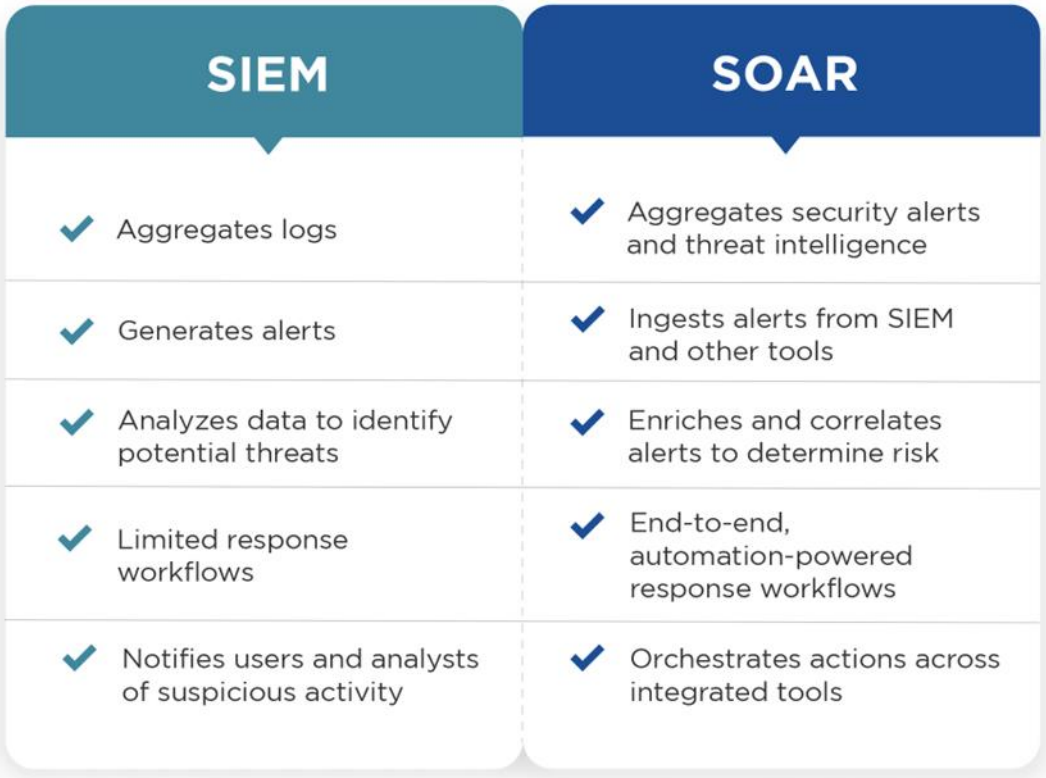
SIEM (Security Information and Event Management) on järjestelmä, joka mahdollistaa monien turvallisuustyökalujen lokitietojen standardoidun käytön, mutta myös laajennettua valvontaa räätälöityjen sovellusten avulla. SIEM on teknologia, joka ei toimi itsenäisesti, vaan vaatii aina ihmisen analysoimaan sen eri lähteistä keräämää dataa. SIEM-järjestelmä on hieman vaativampi ottaa käyttöön ajallisesti, se on myös vaativampi ylläpitää verrattuna XDR:n. SIEM kuitenkin on mukautettavissa organisaation tarpeiden mukaan ja siitä syystä se voikin olla monelle todella hyvä työkalu. SIEM vaatii aina tietyn määrän resursseja, jotta sen hyödyt ovat maksimaaliset. Työntekijöiden on sitouduttava seuraamaan SIEM:ä säännöllisesti tai organisaation on perustettava oma tiiminsä valvomaan SIEM:n keräämiä lokitietoja. (Spiceworks 2022.)



Kuva 2. Miten SIEM toimii? (Spiceworks 2022.)

3.2.3 SOAR

SOAR (Security Orchestration, Automation and Response) on erilaisista yhteensopivista ohjelmistoista muodostuva järjestelmä, jonka avulla organisaatiot voivat kerätä tietoa tietoturvauhista ja näin ollen reagoida tapahtumiin joko pienellä ihmisen avustuksella tai kokonaan ilman ihmisen avustusta. Tämän alustan tavoitteena on parantaa digitaalisen turvallisuuden toimintojen tehokkuutta. Nimensäkin perusteella SOAR:lla on kolme pääkomponenttia, joita ovat turvallisuuden orkestrointi, turvallisuuden automatisointi ja turvallisuusvaste. Orkestroinnilla tarkoitetaan prosessia, jonka avulla tietoja voidaan jakaa eri järjestelmien välillä. Tämän avulla voidaan havaita tehokkaammin tietoturvatapahtumia sekä niihin voidaan reagoida ja niitä voidaan analysoida tehokkaammin. (Benard, W 2022.)



Kuva 3. SIEM vs. SOAR (D3Security 2023.)

4 PILOTOINNIN JA KOKEILUN EROAVAISUUDET

Kokeilu ei ole sama asia kuin pilotti. Siinä missä kokeilun päämääränä on tuottaa merkittävään uutta tietoa ideaan liittyen, pilotin päämääränä on tehdä viimeinen validaatio ja varmistus siitä, että asiat toimivat niin kuin pitääkin. ”*Onnistunut kokeilu on sellainen, jossa mahdollisimman pienellä vaivalla ja resursseilla opitaan mahdollisimman paljon kehitettävän idean kannalta oleellista uutta tietoa”.*

Lähtökohtaisesti kokeilun voidaan sallia epäonnistuvan, monesti jopa odotetaan, että se epäonnistuu. Pilotissa taas odotukset onnistumisen suhteen ovat lähes sataprosenttiset. Vaikka pilotti epäonnistuisi, eli tietty ratkaisu ei välttämättä toimi odotetulla tavalla, saatetaan projektin kanssa silti päästä eteenpäin alun perin laaditun suunnitelman mukaan.

Kokeilusta saatava tieto vaikuttaa monesti oleellisella tavalla kehitysprojektin etenemiseen. Pilotin eteen usein tehdään paljon enemmän töitä verrattuna kokeiluun, ei radikaaleille muutoksille juuri jää tilaa. Kokeilun jälkeen muokkaaminen on kaikin puolin mahdollista. Pilotoinnin jälkeen mahdollisuuksia jää lähinnä hienosäätöön. Kehitettävä idea sisältää aina tietyn joukon olettamuksia, joita pilotissa testataan kaikkia kerralla. Tämän takia pilotin tekeminen on hitaampaa, kalliimpaa ja siinä on isompia riskejä, kuin kokeilu. (Paju, S 2016.)

5 SOC-PILOTOINNIN TEORIA JA TOTEUTUS

SOC-pilotoinnin organisaatioille kehitti alun perin organisaatio A. Se on toiminut toimittajan sekä vastaanottajan roolissa monissa eri piloteissa, joita DigiTyy-hankkeessa mukana oleville organisaatioille on esitelty hankkeen aikana. Pääsääntöisesti pilotointeihin pääsevät mukaan kaikki halukkaat organisaatiot, mutta joissakin piloteissa on myös vaatimuksia mukaan pääsemiselle. SOC-pilotoinnin vaatimuksena oli esimerkiksi olemassa oleva SIEM-järjestelmä. Ilman SIEM-järjestelmää organisaation olisi hankala aloittaa SOC-pilotointi, sillä SIEM kerää tarpeellisen datan, jota SOC-työskentely edellyttää. Organisaatioissa SIEM-järjestelmän hankkiminen olisi vienyt paljon aikaa ennen kuin varsinainen SOC-pilotointi olisi voitu edes aloittaa. SOC-pilotoinnissa mukana olleita organisaatioita oli neljä kappaletta, opinnäytetyössä nimiltään A, B, C ja D.

SOC-pilotointiin päädyttiin, sillä DigiTyy-hankkeen suunnitteluvaiheessa järjestettävässä ryhmätyöskentelyssä havaittiin, että on tunnistettu useita lähteitä, joista organisaatioiden tulisi seurata syötettä sekä lokitietoja. Lähteet, joista havaintoja tulee ovat esimerkiksi tikettijärjestelmä, työasemat, Microsoftin Office 365 palvelusta, NAC-palvelusta, palomuurista, VPN-yhteyksistä, palvelimista sekä organisaation käyttämästä DNS-palvelusta. Myös kyberturvallisuuskeskuksen tuottama kybersää, Traficomin tuottamat NCSC-raportit ja alueen muiden vastaavien organisaatioiden havainnot ovat osa tätä lähdekokonaisuutta. Pilotoinnin avulla haluttiin kuitenkin ennen kaikkea selvittää, mitä prosesseja, toimenpiteitä ja muita asioita pilotoinnin tai palvelun käyttöön ottaminen vaatii organisaatiolta.

DigiTyy-hankkeessa järjestettävissä riskirekisteri ja ryhmätyöskentely työpajoissa on tunnistettu useita eri tapahtumia, joihin organisaatioiden on hyvä reagoida. Tunnistettuja tapahtumia ovat esimerkiksi tietojenkalastelut, digiturvallisuuteen liittyvät poikkeamat, palvelunestohyökkäykset, laajamittaiset häiriöt sekä tietomurron tai tietosuojan vaarantuminen. (DigiTyy-hanke 2023.)

Monesti varsinkin digiturvallisuuteen liittyvät poikkeamat jäävät organisaatioissa herkästi huomioimatta. Yleensä tapaukset hoidetaan normaalin vikailmoituksen kautta. Esimerkkinä Office 365:n osalta huomataan outo kirjautuminen, reagoidaan ainoastaan tämän yhden käyttäjän kohdalla ja vaihdetaan tarvittaessa salasanaa ym. Laajempi vaikutus jää herkästi huomioimatta.
Organisaatioiden oman toimintaympäristön tilannekuva on todella heikko digiturvallisuuden näkökulmasta. Isojen ongelmien läpikäynti ja viestintä organisaatioiden mielestä on huonolla tasolla. Tehtävien vastuuttaminen vaikuttaa hankalalta, tai ainakaan niistä ei ole tehty dokumentteja, joista vastuut

ilmenevät, esim. RACI-taulukko. Tilanteissa, joissa ICT on ulkoistettu palveluntarjoajalle, voi ajatuksena olla ”Kyllä joku muu hoitaa tämän ongelman”. RACI-taulukko on hyödyllinen ja helppokäyttöinen tapa selvittää vastuut nopeasti. RACI-taulukon avulla on myös helppo ohjeistaa muita siitä, mitkä asiat ovat heidän vastuullaan.

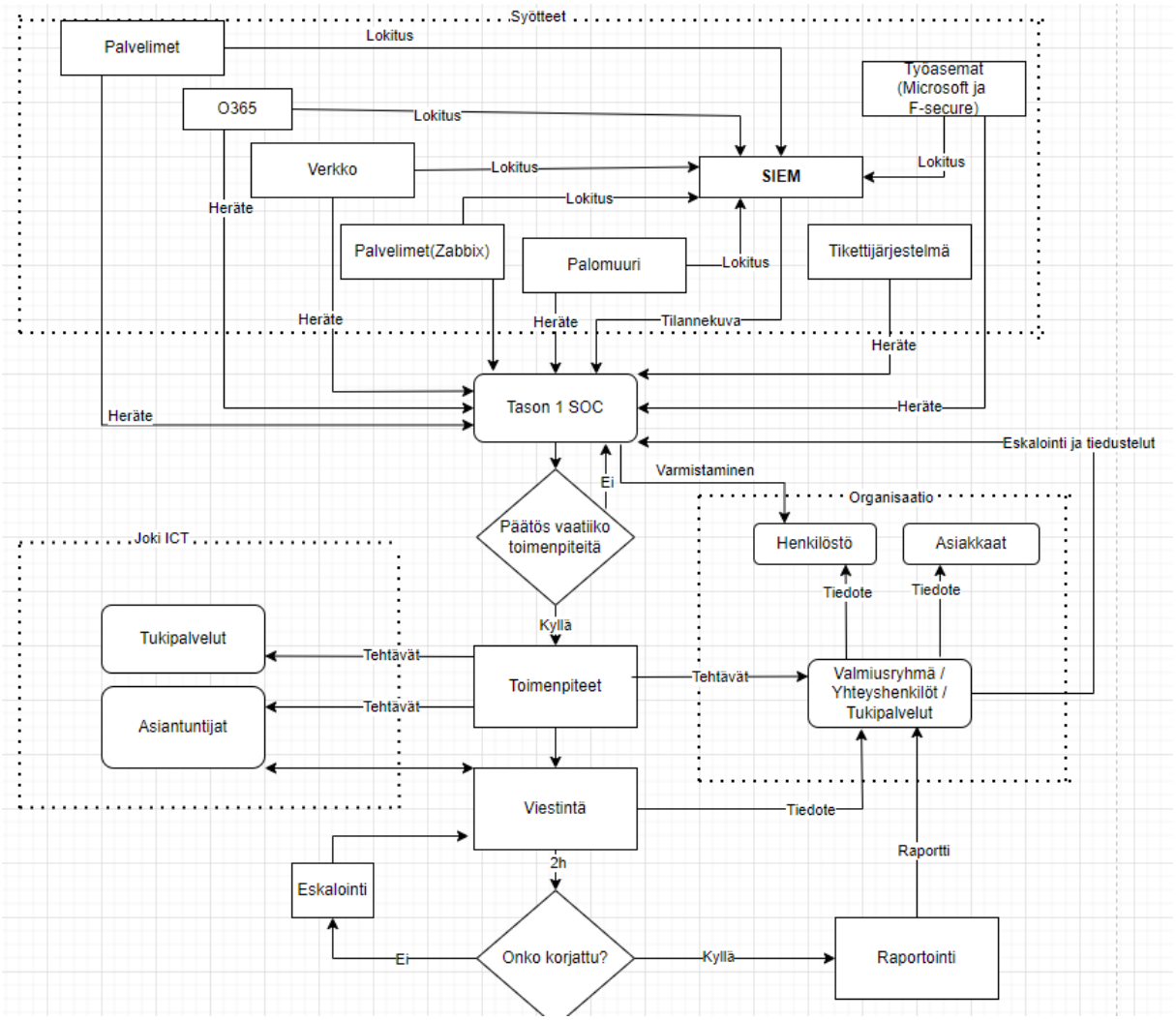
Rooli/vastuu	**Kuvaus**
R (Responsible)	Kenellä on vastuu tehtävistä
A (Accountable)	Kuka lopulta vastaa asian hoitumisesta
C (Consulted)	Keneltä kysytään ja saadaan lisätietoa
I (Informed)	Kenelle tiedotetaan

Taulukko 1. *RACI-taulukko, vastuut ja tehtävät.*

Vastuualue	Tietohallinto	Pääkäyttäjä	Järjestelmän toimittaja	Tukipalvelut	Asiantuntijapalvelut	Operaattori	Teleoperaattori
Tietoliikenne (ulos)	A	I	C	C	C	R	
Tietoliikenne (sisäinen)	A	I	C	R	R	I	
Etäyhteydet (VPN)	A	I	C	R	R		I
Palvelimet + ylläpito	A	I	C	R	R		
Sovelluskonfiguraatiot	I	A	C/I	R	R		
Työasemat	A	I	C	R	R		
Oheislaitteet	A	I	C	R	R		

Resurssit eivät ole riittäviä organisaatioissa, jotta voitaisiin seurata tilannetta monesta eri lähteestä systemaattisesti. Selvityksen ja keskustelun perusteella pääkäyttäjät käyvät läpi lokeja sekä eri syötteitä,

kun sille on aikaa muiden töiden salliessa. Nykytilanne on sellainen, että reagointi tapahtumiin reagointi tapahtuu paljon jäljessä ja käytännössä organisaatioiden tarkoituksena on vain palauttaa normaali tilanne. (DigiTyy-hanke 2023.)



KUVA 4. SOC-prosessikaavio *(DigiTyy-hanke).*

5.1 SOC-palveluun vaaditut prosessit ja toimintamallit

SOC-pilotoinnin avulla kerättiin tietoa myös siitä, millaisia prosesseja ja toimintamalleja sekä mahdollisia muita asioita SOC-palvelun käyttöönotto vaatii palvelun toimittajalta sekä asiakasorganisaatiolta. Pilotointia varten toimittajan sekä asiakasorganisaatioiden oli valmisteltava prosesseja ja toimintamalleja, joista selviää vastuut ja toimintatavat eri tilanteissa sekä ohjeistuksia ja muita dokumentteja. DigiTyy-hanke on valmistellut suuren määrän erilaisia dokumentteja, jotka kaikki ovat hyödyllisiä tai jopa välttämättömiä SOC-pilotointia/palvelua varten. DigiTyy-hankkeen valmistelemat dokumentit ovat

hankkeessa mukana olevien organisaatioiden vapaassa käytössä, jotta jokaisen organisaation ei tarvitse valmistella jo olemassa olevia dokumentteja.

Hankkeen tärkeimpiä dokumentteja koskien SOC:n prosesseja, toimintamalleja sekä toimenpiteitä ovat:

- MIM-prosessi, jota voidaan hyödyntää organisaatioiden reagointiprosesseihin. MIM on lomakepohja, joka täytetään laajamittaisen häiriön sattuessa. Lomakkeeseen merkitään tiketin numerot, tapahtuman tila, vetovastuu, kuvaus tapahtumasta, juurisyy vialle, IT-vaikutus, toiminnallinen vaikutus, suunnitellut ja toteutuneet toimenpiteet. MIM-lomakkeen loppuvaiheessa kysytään vielä yhteensä viisi kertaa ”miksi”. Tällä tavalla kasvatetaan ymmärrystä miksi häiriö ylipäätään pääsi tapahtumaan. MIM-prosessi helpottaa organisaatioiden reagointia tietomurtoon tai muuhun vastaavaan poikkeustilanteeseen.

- ICT-valmiussuunnitelma, jota käytetään kaikissa häiriö- ja poikkeustilanteissa. Suunnitelma kattaa ennaltaehkäisyn, kriisijohtamisen, viestinnän, uhka-analyysin, tehtävien toteutuksen, vastuut ja käytettävät voimavarat, sekä myös lainsäädännöllisen perustan. Tämä suunnitelma valmistaa organisaatioita varautumaan tietomurtoon. Tietomurron tai muun poikkeuksen sattuessa on suunniteltu ennakkoon, miten tilanteeseen vastataan.

- Käyttövaltuushallinta dokumentin tavoitteena on mallintaa ja yhtenäistää käyttövaltuusprosessit kaupunkitasolla niin, että niiden käyttö on mahdollista jokaisella toimialalla sekä liikelaitoksilla. Käyttöoikeuksien hallinnassa noudatetaan vähimpien oikeuksien periaatteita, jolloin järjestelmien käyttäjille, ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet ja valtuudet, jotka ovat tehtävien suorittamiseksi välttämättömiä. Dokumentin avulla vähennetään tunnusten väärinkäytöksiä, jolloin SIEM hälytteet vähenevät sekä tietomurron riski pienenee.

- MFA (Multi Factor Authentication) otettiin käyttöön, koska se vähentää merkittävästi epäilyttäviä onnistuneita kirjautumisia järjestelmiin. Käyttäjän kirjautuessa järjestelmään, käyttäjä saa puhelimeensa viestin, jonka avulla hänen pitää todentaa kirjautumisyrityksensä.

- Ulkomailta kirjautumisen esto, jonka avulla ulkomailta kirjautuminen ei onnistu. Tällä tavalla voidaan yhdessä MFA:n kanssa vähentää merkittävästi luvattomia kirjautumia ulkomailta.

- Muutoksenhallinta-dokumentilla kartoitetaan tulevien muutosten vaikutusta sekä sillä voidaan ennaltaehkäistä epäonnistuneen muutoksen selvitystyöstä aiheutuvia kustannuksia suunnittelun avulla. Muutoksenhallinta kyselylomake auttaa hahmottamaan asioita, joita on otettava huomioon kussakin muutoksessa.

- Tietoturvarikkomus työntekijänä dokumentin läpikäymällä ja käyttöönottamalla organisaatiolla on mahdollisuus vaatia tietoturvallista toimintaa. Dokumentissa kerrotaan esimerkkejä tietoturvarikkomuksista työntekijänä sekä toimenpiteitä rikkomuksen sattuessa. Työntekijöiden tietäessä rikkomusten seuraukset, on riski rikkomuksiin pienempi.

- Tietomurto, tietovuoto ja tietosuoja dokumentissa käydään läpi organisaation tapahtumaketjut tietomurron tai tietovuodon sattuessa ja tietosuojan vaarantuessa. Prosessin läpiviemiseksi suositellaan myös MIM-lomakkeen käyttöä. Mikäli SOC havaitsee epäilyttäviä kirjautumisia tai tietomurron, on siihen jo olemassa valmiit tapahtumaketjut, jolloin reagointi nopeutuu ja mahdolliset vahingot jäävät pienemmiksi.

- Palvelunestohyökkäys, josta tapahtumaketjun pääkohdat hyökkäykseen reagointiin. Prosessikuvaus mahdollistaa raportointia, dokumentointia ja johtaa hyvään kehittämiseen.

- Digiturvallisuuden poikkeama voi olla esimerkiksi tilanne, jota organisaatiossa ei ole aiemmin kohdattu, ohjeistusta tai päätöstä ei ole tehty organisaatiossa tai riski, jota ei ole huomioitu uhka-analyysissa. MIM-lomakkeen hyödyntäminen on suositeltavaa myös tässä osiossa.

- Hankintamenettelyn tavoitteena on ehkäistä suunnittelemattomia, hallitsemattomia sekä ennakoivasti huomioida hankintoihin liittyvien tietoteknisten käyttöympäristöjen muutoksista toimintamalleihin ja liitännäisiin. Hankintamenettelyn tavoitteena on myös, että tietohallinto ja muut tarvittavat kohderyhmät ovat tietoisia ICT-ympäristön muutoksista. (DigiTyy-hanke 2023.)

- Tiedonhallintalaki tuli voimaan 1.1.2020 ja sen tarkoituksena on varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely. Tiedonhallintalakia sovelletaan valtion virastoissa ja laitoksissa, tuomioistuimissa, eduskunnan virastoissa,

valtion liikelaitoksissa, kunnissa, kuntayhtymissä, itsenäisissä julkisoikeudellisissa laitoksissa, yliopistolaissa tarkoitetuissa yliopistoissa ja ammattikorkeakoululaissa tarkoitetuissa ammatti-koreakouluissa. (Laki julkisen hallinnon tiedonhallinnasta 2019.)

- *”Vaikutuksen arviointi, jonka tavoitteena on arvioida jäljelle jääneestä riskistä, onko se oikeutettu ja hyväksyttävissä sen hetkisissä olosuhteissa. Vaikutustenarviointi helpottaa ja auttaa rekisterinpitäjää tietosuojalainsäädännön vaatimusten noudattamisessa, sen dokumentoinnissa ja osoittamisessa”.* (Tietosuojavaltuutetun toimisto.)

- TAISTO-harjoitus on hyvä tapa varautua laajoihin hyökkäyksiin. TAISTO-harjoitus on Digi- ja väestötietoviraston järjestämä maksuton harjoitus, joka on suunniteltu erityisesti julkiselle sektorille, mutta muutkin toimijat voivat osallistua. Harjoituksessa keskitytään häiriötilanteiden hallintaan, johtamiseen ja viestintään, ja sen tapahtumat peilaavat ajankohtaisia uhkia. (Digi- ja väestötietovirasto 2023.)

Yllä luetuilla dokumenteilla ja toimenpiteillä katetaan tiedonhallintalakiin pohjautuvia vaatimuksia, joita ovat ainakin:

- Järjestelmien tunnistaminen
- Järjestelmässä käsiteltävän tiedon tunnistaminen
- Tiedon ja järjestelmän kriittisyyden tunnistaminen
- Järjestelmään liittyvän infrastruktuurin tunnistaminen
- Infrastruktuurin kriittisyyden määrittäminen järjestelmäroolin perusteella
- Lokien keräämisen ja hallinnan käyttöönotto alustoilla kriittisyysjärjestyksessä
- Toiminnan jatkuvuuden suunnittelu kriittisyysasteittain
- Toiminnan palautumisohjeiden ja toimenpiteiden määrittäminen kriittisyyden perusteella.
- Jatkuvuudenhallinnan harjoittelu (TAISTO-harjoitukset, yhteinen harjoittelu)
- Käyttäjätunnusten hallinta ja lisensointi (Laki julkisen hallinnon tiedonhallinnasta 2019.)

6 SOC-PILOTOINTI NUMEROINA

Toimittajan puolella on pidetty kirjaa erilaisten hälytyksien ja muiden tapahtumien lukumäärästä. Kirjanpito ei kuitenkaan ollut automaattista, vaan enemmänkin tukkimiehen kirjanpitoa käsipelillä. Tästä syystä luvuissa saattaa olla pientä heittoa, mutta pyrkimyksenä oli, että kaikki hälytykset kirjattaisiin ylös.

Taulukko 2: *SOC-pilotoinnin hälytteet numeroina.*

	Helmikuu	Maaliskuu	Huhtikuu	Yhteensä
SIEM-hälytykset	249	273	215	737
Raportit	2	4	0	6
Yhteydenotot organisaatioihin	35	25	11	71
Yhteydenotot organisaatioista	24	16	2	42
Muita käsiteltyjä herätteitä	28	21	13	62

Taulukosta 2 selviää, kaikkien organisaatioiden yhteenlasketut lukemat. SIEM keräsi hälytyksiä lukuisista eri lähteistä yhteensä 737 kappaletta, joista 249 helmikuussa, 273 maaliskuussa ja 215 huhtikuussa. False-positiveja näistä hälytyksistä oli selkeästi suurin osa, jopa 689 kappaletta, joista 230 helmikuussa, 253 maaliskuussa ja 206 huhtikuussa. Aiheellisia selvityksiä jäi siis 48 kappaletta, joista 19 helmikuussa, 20 maaliskuussa ja 9 huhtikuussa. Tapauksista on laskettu prosentuaalisesti 6,5 % kaikista tapauksista olevan aiheellisia. Laajempia raportteja tapahtumista tehtiin 2 kappaletta ja 4 raporttia riskikäyttäjistä.

Toimittajan organisaatioihin ottamia yhteydenottoja eri hälytyksiä ja lisäselvityksiä koskien oli yhteensä 71 kappaletta, joista helmikuussa 35, maaliskuussa 25 ja huhtikuussa 11. Organisaatioiden yhteydenotot toimittajalle vastaavista asioista oli yhteensä 42 kappaletta, joista 24 helmikuussa, 16 maaliskuussa ja 2 huhtikuussa. Muita käsiteltyjä herätteitä oli yhteensä 62 kappaletta, joista 28 helmikuussa, 21 maaliskuussa ja 13 huhtikuussa. Aikaa SOC-työskentelyyn pilotoinnin aikana käytettiin yhteensä 250 tuntia ja seurantapalaverien aikana saatiin käsiteltyä huomioita yhteensä 72 kappaletta. (DigiTyy-hanke. 2023. *SOC-pilotointi numeroina*).

6.1 Toimittajan huomiot SOC-pilotoinnista

Työaika oli yksi suurimmista haasteista, SOC-pilotointia suoritettiin 8–16 aikavälillä, virka-aikana. Työtä tehtiin siis oman työn ohella, joka tietysti lisäsi työtaakkaa ja kiirettä organisaatioissa. Toimittajan puolella sekä organisaatioissa on huomioitu, että tulevaisuudessa käynnistyvässä SOC-palvelussa tulisi olla 5 henkilön työpanos, pilotoinnissa työpanos oli 3 henkilöä. Suunnittelussa on myös, että vuorot jaettaisiin aamu- sekä iltapäivävuoroihin. Toimittaja huomioi myös, että SOC-tiimissä olisi hyvä olla edustusta jokaisesta toimittajan palvelusta. Tällä tavalla pystyttäisiin ratkaisemaan ongelmia jo sisäisesti SOC-tiimillä ja tieto kulkee henkilöiden kautta palvelukohtaisiin tiimipalavereihin.

Toimittajan puolen haastatteluosiossakin oli mainittu pelikirjoista, niistä sopiminen yhteisissä palavereissa on tärkeää, koska se nopeuttaa päätöksentekoa ja on helpompi tunnistaa false-positive tapauksia ilman, että resursseja kuormitetaan liikaa. Isona huomiona havaittiin myös, että tiedonhallintamallin ajantasaisuus kohdeorganisaatiossa tukee SOC-toimintaa, koska sen avulla pystytään tarkistamaan asiat ilman resurssien varaamista yhteyshenkilöiltä. Työasemien seurantaan ja hälytyksien saamiseksi on havaittu, että tarvitaan parempi työkalu. Tästä syystä tulevassa SOC-palvelussa tulee olemaan Lansweeper-työkalu, jolla voidaan esimerkiksi peilata sidosryhmiltä tulevia haavoittuvuuksia ympäristöön.

6.2 SOC-pilotoinnin hyödyt

SOC-pilotoinnille asetetut tavoitteet saavutettiin ja organisaatioiden tilannekuva ja reagointikyvykkyys on kasvanut merkittävästi. Organisaatioiden perusedellytykset digiturvallisuuteen liittyvien poikkeamien havainnointi, reagointi, käsittely ja niistä palautuminen on tehostunut organisaatioiden haastattelujen perusteella. Viestinnästä on tullut reaaliaikaisempaa. Organisaatiot osaavat hyödyntää saatavilla olevia resursseja tehokkaammin, jolloin vikojen korjausaika tehostuu. Pilotointi vahvisti organisaatioiden yleistä ICT-tilannekuvaa. Poikkeamiin, häiriöihin ja uhkakuviin reagoiminen pystytään tekemään vain havainnoinnilla. Pilotoinnin aikana esiin nousseita konkreettisia huomioita on helpompi havainnollistaa organisaatioille, jolloin myös kustannuksien esittäminen on paljon helpompaa. Laajempien vikojen läpikäynti tehostui luonnollisesti ja esimerkiksi Efectestä saatavan tiedon laatua kehitetään. Erityisesti organisaatioiden digiturvallisuuden kypsyystaso on saatu huomattavaan nousuun pilotoinnin ansiosta.

7 HAASTATTELUOSIO

Haastatteluprosessi alkoi siitä, että selvitin SOC-pilotoinnin toimittajalta pilotointiin mukaan lähteneet organisaatiot, joita voisin haastatella asiaan liittyen. Lisäksi selvitin, ketkä kyseisessä organisaatiossa olivat osallisina SOC-pilotoinnin toteutumisessa heidän organisaationsa osalta. Lähetin organisaation kaikille osallisille sähköpostia, jossa kutsuin heidät noin tunnin mittaiseen Teams-haastatteluun. Haastateltavia henkilöitä toimittajan puolelta oli yksi, organisaatiossa B kaksi, organisaatiossa C yksi, organisaatio D ei koskaan vastannut yhteydenottoihin. Tästä syystä myöskään kommentteja ei ole saatu, jolloin turvaudutaan organisaatioiden A, B ja C vastauksiin.

Valmistelin haastattelukysymyksiä etukäteen, jonka jälkeen haastattelin mukaan lähteneitä organisaatioita SOC-pilotoinnista. Haastatteluni käsitti kysymyksiä resursseista, aikatauluista sekä kuinka organisaatiot kokivat SOC-pilotoinnin yleisesti. Kaikki organisaatiot eivät päässeet mukaan pilottiin, koska heillä ei ollut ennakkoon SIEM-järjestelmää tai omasta tahdostaan eivät halunneet lähteä mukaan. Haastatellessani toimittajaa tuli hyvin selväksi myös se, että minkälaisia haasteita tai esteitä organisaatiot kokivat SOC-pilotointiin mukaan lähtemisessä.

Seuraava osio käsittelee haastattelukysymykseni ja yhteenvedon mukana olleiden organisaatioiden vastauksista. Vastauksista oli helppo luoda yhteenveto, sillä kaikki mukana olleet organisaatiot vaikuttivat olevan hyvin pitkälti samaa mieltä aiheista. Kysymykset olivat kaikille organisaatioille samoja, jotta on helpompi selvittää poikkeamia tai yhtäläisyyksiä organisaatioiden kokemuksien välillä. Tarkoituksena oli haastatella ensin toimittajaa ja sen jälkeen organisaatioita heidän kokemuksistaan.

7.1 Toimittajan haastatteluosio

Ensimmäinen kysymys toimittajalle käsitteli millaisia toiminnallisuuksia ja työkaluja SOC-pilotointi tarjoaa tietoturvan hallinnassa.
Analysointi, keskustelu, oikeat henkilöt keskustelevat keskenään, asiantuntijuus tilannekuvan muodostumiseen. Nämä asiat tulivat toimittajan edustajan suusta lähes välittömästi kysymyksen esittämisen jälkeen. Tilaajana organisaatioita kiinnostaa tämänhetkinen kuva yleistilanteesta. Toimittajana saadaan laajempi käsitys yleisturvallisuudesta meidän sekä muiden organisaatioista. Toimittaja pystyy reagoimaan nopeasti, jolloin varautuminen paranee alueellisesti.

Miten organisaatiot ovat vastaanottaneet SOC-pilotin? Mitkä ovat yleisimpiä haasteita tai esteitä, joita organisaatiot kohtaavat SOC-pilotin käyttöönotossa?

SOC-pilotointi oli niin sanotusti helppo myydä läpi, koska DigiTyy-hanke toimi osittain kustantajana, jolloin organisaatioiden oli helppo lähteä mukaan. SOC-pilotointia määrittäessä ajateltiin, että kyllähän tätä normaalisti tehdään. Organisaatioiden yksi yleisimpiä haasteita SOC-pilotoinnissa oli resurssivaje, toisin sanoen SOC-pilotointia oli suoritettava oman työn ohella, jolloin se koitui aikataulullisesti hyvin haastavaksi.

Ennakkoluulot ja valmiit mielipiteet SOC:sta olivat osalla luotuina, mutta kattavan pilotoinnin läpikäynnin jälkeen yhä useammat alkoivat ymmärtämään asian tärkeyden. Aikaisemmin Suomessa tapahtuneet tietomurtotapaukset lisäsivät kiinnostusta SOC-pilotointiin. Uhkakuvat ja tietomurrosta johtuvat kustannukset täytyy käydä esittelyssä läpi. Tämä lisää edelleen ymmärrystä SOC:in hyödyistä.

Kaikkia DigiTyy-hankkeessa mukana olleita organisaatioita ei ollut tarkoituskaan saada mukaan, liian suurella laajuudella tuloksia olisi ehkä hankalampi seurata. Tämä laajuus oli riittävä. Lähtövaatimuksena SOC-pilotointia varten oli, että organisaatiolla täytyy olla SIEM-järjestelmä käytössä valmiiksi. Organisaatiossa C SIEM otettiin käyttöön juuri ennen kuin pilotointi alkoi.

Miten SOC-pilotointi integroituu organisaation nykyiseen tietoturva-arkkitehtuuriin ja prosesseihin? Onko siinä vaikutusta olemassa olevien järjestelmien tai työnkulun muutoksiin?

Prosessien kannalta ICT painottuu tietohallinnon alaisuuteen. Toimittajan näkökulmasta pyritään, että osallistuvat pystyvät tekemään omat työt, mutta silti sitoutuvat tekemään SOC:a. Reagointiprosessit kehittyvät pilotoinnin aikana, ”tällainen syöte, keneltä kysyn asiasta” tyyppisesti. In-house yhtiöillä asiantuntijatyöt sekä neuvojat käytettävissä. Organisaation päätöksentekoa ja sopimusmuutoksia pitää mahdollisesti muuttaa hieman riippuen jo olemassa olevien prosessien laadusta.

Miten SOC-pilotin tehokkuutta ja vaikutuksia mitataan? Millaisia mittareita käytetään arvioimaan SOC-pilotin onnistumista tietoturvan hallinnassa?

SIEM-pohjainen SOC on käsityötä, mahdollista automatiikkaan olisi. Tällöin hinta olisi huomattavasti korkeampi (XDR SOC). Organisaatioiden kanssa käytiin kuukausipalavereja säännöllisesti, palavereissa käytiin läpi esimerkiksi, montako tikettiä keretään käsitellä Efecte-tikettijärjestelmässä. Aiheina olivat myös false-positive ilmoitusten määrä verrattuna aiheellisiin insidentteihin. Organisaatiokohtaisesti seurattiin myös laajempia raportteja sekä työaikaa.

Minkälaista tukea ja koulutusta toimitatte organisaatioille SOC-pilotoinnin aikana? Millainen on jatkuvan tuen ja ylläpidon malli SOC-pilotin jälkeen?

Hankkeen puolelta on tehty ohjeistuksia organisaatioiden käytettäviksi. Hanke työsti SIEM-oppaan organisaatioille. Toimittajan roolissa seurantapalaverit, tieto välitettiin mahdollisimman pureksittuna organisaatioille ja tarjottiin asiantuntijapalveluita, mikäli tarpeellista. Periaatteena oli, että selitys sen verran valmis, että organisaatio voi sanoa vain kyllä tai ei. Organisaatioille tehty siis helpoksi ymmärtää asiat.

Miten SOC-pilotin toimittaja vastaa organisaatioiden erityistarpeisiin ja vaatimuksiin? Onko järjestelmä skaalautuva ja muokattavissa organisaation tarpeiden mukaan?

Pilotoinnissa käytettiin SIEM:iä ja pilotoinnissa se oli hyvin yksioikoinen, pilotoinnissa laskettiin mukaan lähinnä palvelimet ja Office 365. SOC-palvelusta voidaan räätälöidä tarvittaessa hyvinkin laaja kokonaisuus. Organisaatioille on mahdollista tehdä tiekartta siitä, mitä toivoisivat lisäyksinä. Rajapinnat mahdollistavat tietojen tuomisen muista palveluista SIEM:iin. Identiteetinhallinta on saatu paremmin haltuun SOC lähtötilanteessa. Hälytyksienkäsittelystä on jäänyt velkaa, joka tarkoittaa sitä, että kymmeniä tai jopa satoja hälytyksiä on jäänyt kuittaamatta. Tämä velan umpeen kurominen hidastaa organisaatioiden kykyä reagoida uusiin jatkuvasti esiin nouseviin uhkiin. Ihanne tilanne olisi se, ettei hälytysvelkaa olisi lainkaan.

Millaisia tietoturva-analyysejä ja raportointia SOC-pilotin toimittaja tarjoaa? Miten nämä auttavat organisaatioita saamaan paremman tilannekuvan tietoturvatapahtumista?

Seurantapalavereissa tulee tärkeimmät nostot esille. Tulevaisuutta ajatellen palaverit vievät paljon aikaa, tilalle kaavaillaan tiivistettyjä PowerPoint-esityksiä, jolloin tieto on nopeasti saavutettavissa. SIEM:stä on mahdollista saada QRadarin raportteja, vaikkakin ne ovat hieman alkukantaisia. FortiAnalyzer raportit myös saatavilla toimittajalta, josta nähdään palomuurin estämää liikennettä. Automatiikalla pystyy seuraamaan asioita, nostaa mahdollisia uhkia esille, joille käsittelijä voi tehdä tarvittavat toimenpiteet. Tukkijätkän kirjanpidolla voidaan seurata esimerkiksi, montako kontaktia tai uhkaa organisaatio tai henkilö kohtaa. Yhteinen toimintamalli sekä yhteiset prosessit ovat tärkeitä, jotta saadaan organisaatiot päätöksenteko kykyisiksi. Yhteinen pelikirja täytyy siis löytyä.

Millaisia oppimis- tai parannusehdotuksia olette saaneet organisaatioilta, jotka ovat osallistuneet SOC-pilotointiin? Miten nämä palautteet on huomioitu SOC-pilotin kehittämisessä?

Palautetta tuli ripotellen seurantapalaverien aikana. Palautteet käsiteltiin sisäisesti toimittajan näkökulmasta. SOC-pilotoinnista tulleita organisaatioiden nostoja:
Tilannekuvaan toivottiin parempaa kuvaamista toimittajalta. Pystyisi käymään uhka-analyysia läpi ja tekemään päätöksiä perustuen selkeään uhkakuvaan. Jos tapahtuu tietoturvamuutos tai havainto, miten se parantaa tietoturvaa, miten se havaitaan.

Mikä on ollut yleinen vaikutus SOC-pilotoinnin käyttöönotolla organisaatioiden tietoturvan hallintaan? Voitteko jakaa esimerkkejä onnistuneista tuloksista tai tapausesimerkkejä?
Yleinen viesti, että pilotille asetetut kaikki tavoitteet saavutettu, positiivinen yleisfiilis. Mukana olleet organisaatiot ovat toimineet sanansaattajina tulevaisuudessa jatkuvalle SOC-palvelulle. Vaatimusmäärittelyt tehty tavoitteiden mukaisesti toimittajan osalta. Pilotoinnista on tuotu kehitysideat ilmi, jotta pystytään laittamaan virallinen SOC-palvelu käyntiin. Riskikäyttäjiä on saatu kuriin, jotka mahdollisesti on pidempäänkin ollut väärissä käsissä. Työasemille parempia hälytteitä, miten pystytään paremmin havaitsemaan.

Yhteiskäyttötunnukset saatu nostettua tapetille, että ovatko järkeviä vai ei. Palomuurien säännöllinen katselmointi. Kiristysviesti tullut, että muokataan nettisivunne, vaaraa ei kuitenkaan tästä koitunut. Kohdennetummin ja omaa tietoturvaa parantaen nettisivujen äärellä. Julkisverkkojen ajattelu noussut pintaan. Tarvitseeko VPN-yhteydet ja aivan kaikkien mahdollisten toimintojen onnistua, mikäli asiakkaalla julkisverkkojen käyttömahdollisuus.

Yleisesti voi siis todeta, että yleinen tietoisuus on lisääntynyt valtavasti. Organisaatioiden heikkoja kohtia on havaittu ja niitä lähdetty kehittämään. Moni organisaatio oli pilotoinnista positiivisesti vaikuttunut, jolloin he haluavat myös sitoutua toimittajan tarjoamaan tulevaan SOC-palveluun. Organisaatioista osa, jotka pilotointiin eivät osallistuneet, kokevat palvelun niin tärkeäksi ja hyväksi, että sitoutuvat siihen nyt, kun heillä on SIEM-järjestelmä hankittuna.

7.2 Organisaatioiden haastatteluosio

Organisaatioiden haastatteluprosessi toteutettiin samalla tavalla kuin toimittajankin haastatteluprosessi. Kysymykset poikkesivat hieman toimittajalle esitetyistä kysymyksistä, koska vain toimittajalla on oikeat vastaukset tiettyihin kysymyksiin. Kysymyksien tarkoituksena oli saada selvyyttä siitä, kuinka onnistuneeksi organisaatioiden edustajat kokivat SOC-pilotoinnin. Kysymyksillä tavoiteltiin myös sitä, kuinka pilotointi auttoi organisaatiota parantamaan tilannekuvaansa ja kypsyystasoansa digiturvallisuuden osalta. DigiTyy-hanke laati useita erilaisia dokumentteja ja toimenpiteitä SOC-pilotointia varten, joita muut organisaatiot voivat hyödyntää vapaasti. Tällöin organisaatioiden ei tarvinnut itse erikseen alkaa valmistelemaan omia prosessejaan. Kaikilla mukana olleilla organisaatioilla ei kuitenkaan ollut käytössä esimerkiksi MFA:ta.

Ensimmäinen kysymys käsitteli sitä, millainen organisaation tietoturvatilanne oli ennen SOC-pilotointia, mitä haasteita siinä oli ja auttoiko pilotointi ratkaisemaan näitä haasteita.
Organisaatiot kokivat työvoiman ja ajan suurimpana haasteena. SIEM/lokitukset olivat juuri tulleet käyttöön ennen SOC-pilotointia. Kuva tietoturvan kokonaisuudesta oli ennen pilotointia suppeampi kuin nykyään, sitä saatiin siis nostettua huomattavasti. Negatiivista liikennettä ei kuitenkaan kovin paljon havaittu. Organisaatioissa luotettiin paljon toimittajan puoleen, sillä heillä oli enemmän resursseja käytössä. Tietoturvatilanne ei ole vielä täydellinen, joten työtä riittää paljon. DigiTyy-hanketta sekä pilotointia kehuttiin, sillä se on tehostanut tietoturvatilannetta paljon ja esimerkiksi ilman hanketta organisaatioiden olisi ollut todella hankalaa lähteä perehtymään asioihin, kun työaika ja tietämys ei välttämättä ollut riittävällä tasolla.

Mitä odotuksia organisaatioilla oli SOC-pilotoinnin suhteen? Täyttyivätkö odotukset?
Odotuksia ei ollut kovin paljon, koska SOC ei ollut etukäteen kauhean tuttu, mutta siihen lähdettiin mukaan avoimin ja oppivaisin mielin. Toimittajan esitys pilotoinnista vaikutti hyvältä ja selkeältä, joka edesauttoi mukaan lähtemisen helppoutta. Pilotoinnin varrella esiin tuli muutamia kehitysideoita, joista toimittaja ottikin hyvin koppia. Odotuksista voidaan kertoa sen verran, että ne ylittyivät pilotoinnin ollessa hetken aikaa käynnissä.

Miten SOC-pilotointi on vaikuttanut organisaationne tietoturvatilanteeseen? Onko asioita lähdetty korjaamaan/muuttamaan havaintojen jälkeen?

Pilotointi koettiin sen verran onnistuneeksi, että toimittajan pilotoinnin pohjalta valmistelema SOC-palvelu tullaan ottamaan käyttöön. Toimittajan kanssa on myös järjestetty palavereja, joissa keskustellaan tarkemmin ja laajemmin organisaatioiden tietoturvatilanteesta.

Millaisia hyötyjä tai haittoja SOC-pilotoinnin laajempi käyttöönotto toisi organisaatioonne?

SOC-palveluun haluttaisiin suurin piirtein sama mittakaava kuin pilotissakin oli, laajempaan ei koeta tarvetta. Haittoina koetaan ehkä työaika, esimerkiksi false-positive tapauksissa, kun ei ole varmuutta tarvitseeko tilanteeseen reagoida vaiko ei. Tällaisten tapausten läpikäynti vaatii paljon aikaa ja vaivaa.

Miten SOC-pilotointi integroitui organisaationne nykyiseen tietoturva-arkkitehtuuriin ja prosesseihin?

Pilotointi integroitui oikein hyvin, pieniä tarkistuksia tehtiin, että löytyykö kaikki tarpeelliset asiat, joita pilotointiin vaaditaan. Kokonaisuutta läpikäytiin, jotta saadaan selkeä kuva kaikesta mitä pitää muokata ja mitä on jo olemassa. DigiTyy-hankkeen tekemät dokumentit auttoivat ymmärtämään mitä pitää ottaa huomioon. M365 on tulossa käyttöön myöhemmin.

Millaisia oppimis- tai parannusehdotuksia lähetitte SOC-pilotoinnin toimittajalle, jos koitte parannettavaa.

Viestinnässä koettiin pieniä haasteita, ei välttämättä toiminut täysin niin kuin suunniteltiin. Asioiden huolellinen dokumentointi havaittiin hyödylliseksi.

Millaisia muita huomioita teillä on SOC-pilotoinnista?

8–16 aikavälillä toteutettu SOC toiminta on hyvin järkevä, tällä hetkellä ei tarvetta 24/7 toiminnalle. SOC:n seuraaminen sujui hyvin, riippumatta siitä kuka oli vuorossa. Palaverikäytänteistä tykättiin, ne olivat hyviä. Alueellisesti tehdyt väliaikatiedotteet olisivat hyviä. Toimittajan puolella valmiustaso koettiin hyväksi.

8 POHDINTA JA JOHTOPÄÄTÖKSET

8.1 Pohdinta

Tässä opinnäytetyössä on tutkittu SOC-pilotoinnin vaikutusta osallistuvan organisaation tilannekuvaan. Tutkimuksessa saatiin kerättyä tietoa SOC järjestelmistä ja tasoista sekä osallistuneiden organisaatioiden käytännön kokemuksia pilotoinnista ja sen vaikutuksista tilannekuvaan. Tutkimus oli hyödyllinen sekä tekijälle, että sen tuleville hyödyntäjille. Tekijä oppi aiheesta ja organisaatioiden tarpeista sekä toiminnoista paljon, tämä edesauttaa tekijän tietotaitoa tietoturvallisuuden osalta tulevaisuudessa. Tulevien hyödyntäjien ei tarvitse alkaa miettimään itsenäisesti, mitä kaikkia prosesseja tai toimenpiteitä SOC-palvelun käyttöönottaminen vaatii, vaan he voivat opiskella tutkimuksesta mitkä asiat ovat tarpeellisia palvelua käyttöön otettaessa. Tutkimuksessa lueteltuja prosesseja ja toimenpiteitä voidaan tilanteen ja tarpeen mukaan myös hyödyntää muissakin tilanteissa, kuin SOC-palvelua käyttöön otettaessa.

Tulosten analysointi:
SOC-pilotoinnilla oli merkittävän suuri vaikutus organisaatioiden tietoturvan parantamisessa. Haastatteluissa esiin tulleet käytännön kokemukset korostivat SOC-ratkaisujen merkitystä. Haastatteluista selvisi myös organisaatioiden oppimiskokemuksia sekä mahdollisia kehitysehdotuksia. Organisaatioiden reagointikyvykkyys parantui merkittävästi pilotoinnin myötä toimittajan kertomuksien mukaan.

Menetelmien arviointi:
Haastattelumenetelmä osoittautui tarjoamaan syvällistä tietoa pilotointiin osallistuneiden organisaatioiden näkökulmista. Menetelmänä käytettiin noin tunnin mittaista Teams-haastattelua jokaiselle osallistuneelle organisaatiolle. Toimittajan edustaja oli haastatteluissa myös mukana, jolloin keskustelu oli entistäkin syvällisempää ja laajempaa.

Teoria ja käytäntö:
Tutkimuksessa saatiin yhdistettyä SOC-järjestelmien ja työkalujen teoreettiset taustat sekä käytännön sovellukset. Tällä tavalla tutkimukseen saadaan sekä niin akateeminen, kuin ammatillinenkin näkökulma aiheeseen.

8.2 Johtopäätökset

Yhteenveto:

SOC-pilotoinnin vaikutus organisaation tilannekuvaan on monitahoinen. Se ei ole ainoastaan tekninen työkalu, vaan se on myös strateginen osa organisaatioiden tietoturva-arkkitehtuuria. Miten hyvin SOC-pilotoinnissa menestytään, määräytyy organisaatioiden valmiuksien ja tarpeiden mukaan. SOC-pilotointia tai SOC-palvelua varten on organisaation käytävä läpi toimintamallejaan sekä luoda tarpeellisia prosesseja pilotointia varten. Tietyt tietoturvan parantamistoimenpiteet ovat myös monesti erittäin hyödyllisiä otettaessa SOC käyttöön, koska ne vähentävät false-positive ilmoitusten määrää ja työaikaa jää enemmän aitoihin hälytyksiin reagoimiseen.

Merkitys ja vaikutukset:

Tämä tutkimus korostaa SOC-pilotoinnin keskeistä roolia nykyaikaisen tietoturvan hallinnassa. Se voi auttaa muita organisaatioita ymmärtämään ja arvioimaan tarvettaan SOC-ratkaisuille ja antaa viitekehystä niiden käyttöönottoon. Tutkimuksessa kerrotaan avoimesti pilotoinnin hyödyistä ja haastatellaan siihen jo osallistuneita organisaatioita, jotka jakavat kokemuksiaan asiasta. Kyseistä tutkimusta tullaan käyttämään Kalajoen kaupungin omistaman DigiTyy-hankkeen loppuraportissa hyödyksi. Tutkimuksen tarkoituksena on myös helpottaa SOC-palvelua suunnittelevien organisaatioiden käyttöönottoa palvelun osalta. Organisaatiot hyötyvät tutkimuksesta ymmärtämällä minkälaisia prosesseja tai toimenpiteitä SOC-palvelun käyttöön ottaminen vaatii. Prosessien ja toimenpiteiden jälkeen käyttöönotto sujuu kivuttomammin sekä tietomurron tai muun ongelman sattuessa prosessien mukaan toimiminen helpottaa paineen alla työskentelyä sekä auttaa tilanteen aiheuttamiin epäselvyyksiin.

Loppukommentit:

Tutkimus tehtiin työn ohessa Kalajoen kaupungille. Erityisinä haasteina oli yhteisen ajan löytyminen haastateltavien organisaatioiden kanssa sekä ajan löytäminen tutkimuksen tekemiselle. Tutkimuksen tekeminen oli opettavaista, sillä tietoa tuli runsaasti eri lähteistä, jolloin vankan kokonaiskuvan muodostaminen aiheesta on helpompaa. Oma mielenkiinto aihetta kohtaan edesauttoi tutkimuksen edistymistä huomattavasti.

LÄHTEET

Kunta-akkuna. 2022. *Hankekortti*
Saatavissa: Microsoft Word - Kunta-Akkuna hankekortti s (kalajoki.fi) Viitattu 20.06.2023

Kanade, V. 2022. *What is Extended Detection and Response (XDR)? Definition, Components, Advantages, and Best Practices. Spiceworks.*
Saatavissa: What Is Extended Detection and Response (XDR)? Definition, Components, Advantages, and Best Practices - Spiceworks Viitattu 08.07.2023

Banerd, W. 2022. *SIEM versus SOAR: How they Differ and Why they Work Well Together. D3Security.*
Saatavissa: SIEM vs. SOAR: How they Differ and Why they Work Well Together | D3 Security Viitattu 10.07.2023

Paju, S. 2016. *Mitä eroa on kokeilulla ja pilotilla? Filosofian Akatemia Oy.*
Saatavissa: Mitä eroa on kokeilulla ja pilotilla? - Filosofian Akatemia Oy Viitattu 10.07.2023

Niinistö, S. & Lintilä, M. 2019. Laki julkisen hallinnon tiedonhallinnasta 906/2019 *Euroopan parlamentin ja neuvoston direktiivi. Finlex.*
Saatavissa: Laki julkisen hallinnon tiedonhallinnasta 906/2019 - Säädökset alkuperäisinä - FINLEX ®
Viitattu 12.07.2023

Vaikutusten arviointi. Tietosuojavaltuutetun toimisto.
Saatavissa: Vaikutustenarviointi | Tietosuojavaltuutetun toimisto Viitattu 23.07.2023

Taisto-harjoitus. Digi- ja väestötietovirasto.
Saatavissa: TAISTO-harjoitus | Digi- ja väestötietovirasto | Digi- ja väestötietovirasto (dvv.fi) Viitattu 24.07.2023

DigiTyy-hanke tuotokset.
Ei vielä julkisesti saatavissa. Viitattu 01.08.2023

SOC Analyst Career Without a Degree. 2022.

LetsDefend Blue Team Blog. Saatavissa:

SOC Analyst Career Without a Degree (letsdefend.io). Viitattu 03.08.2023

Microsoft. 2023. *Security operations analyst associate*

Saatavissa: Microsoft Certified: Security Operations Analyst Associate - Certifications | Microsoft Learn Viitattu 07.08.2023

Logpoint. 2020, päivitetty 4/2023. *What is a security operations center?*

Saatavissa: What is a Security Operations Center (SOC)? (logpoint.com) Viitattu 20.08.2023

Crowdstrike. 2022. *What is a Security Operations Center?*
Saatavissa: What is a Security Operations Center? [SOC Security Guide] (crowdstrike.com) Viitattu 23.08.2023

Kyberturvallisuuskeskus. 2020. *Tietoturva.*
Saatavissa: Tietoturva | Kyberturvallisuuskeskus Viitattu 23.08.2023

Orangecyberdefense. 2023. *SOC, SIEM, MDR, EDR, XDR... What are the differences?*
Saatavissa: SOC, SIEM, MDR, EDR, XDR... what are the differences? (orangecyberdefense.com) Viitattu 27.08.2023