SOC-organisaatiomalli

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Poikkeamien hallinta ja kyberturvakeskukset TTC6060-3007
3.12.2024
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

Taulukot

1 Johdanto

Tässä harjoitustyössä perehdytään SOC (Security Operations Center) -organisaatiomallin suunnitteluun ja toteutukseen. SOC eli tietoturvakeskus on organisaation keskeinen yksikkö, joka vastaa tietoturvauhkien havaitsemisesta, analysoinnista ja niihin reagoimisesta. Tietoturvakeskuksen avulla yritys pystyy hallitsemaan ja suojaamaan digitaalista ympäristöään jatkuvasti kehittyviltä kyberuhilta.

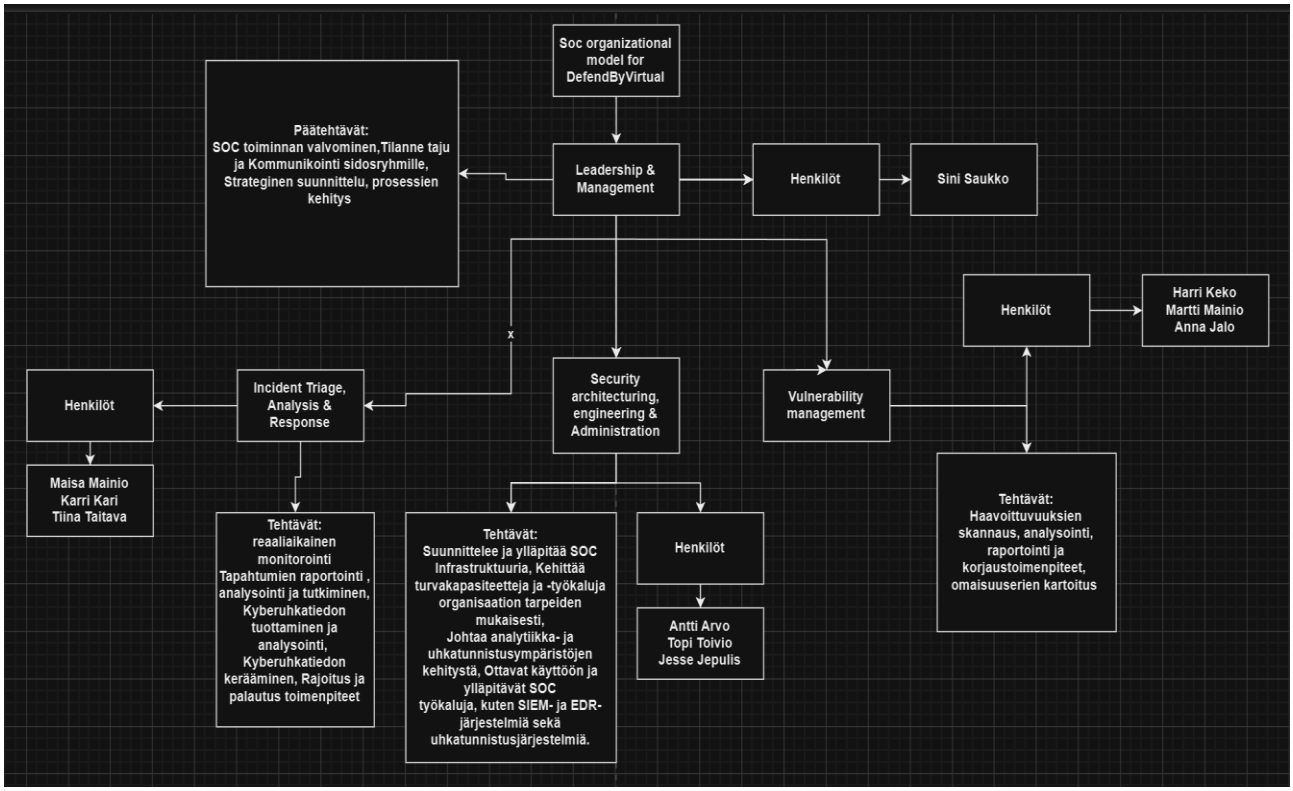
Tämän työn tavoitteena on luoda SOC-organisaatiomalli kuvitteelliselle DefendByVirtual-yritykselle. Työssä määritellään SOC rakenne, keskeiset tehtävät ja vastuualueet huomioiden yrityksen tarpeet ja resurssit. Koska DefendByVirtualilla on tällä hetkellä viisi työntekijää, tietoturvakeskuksen perustamiseksi on sallittu palkata kymmenen henkilöä, joille määritellään tarkat roolit ja vastuut.

2 SOC organisaatiomalli

Tietoturvakeskuksen suunnittelu alkaa yrityksen tietoturvatarpeiden kartoituksesta. Organisaation koko, toimiala ja asiakaskunta vaikuttavat siihen, millainen SOC-rakenne on sopivin. Pienemmälle yritykselle, kuten DefendByVirtual, keskitetty SOC (Centralized SOC) tarjoaa tehokkaan ja selkeän toimintamallin, jossa kaikki tietoturvatoiminnot hoidetaan yhdestä keskusyksiköstä käsin. Näin voidaan varmistaa johdonmukainen toiminta ja resurssien tehokas käyttö.

SOC-rakenteen suunnittelussa on keskeistä määritellä kunkin roolin päätehtävät ja vastuualueet. Tämä takaa, että jokainen työntekijä tietää omat tehtävänsä ja voi keskittyä niihin täysipainoisesti.

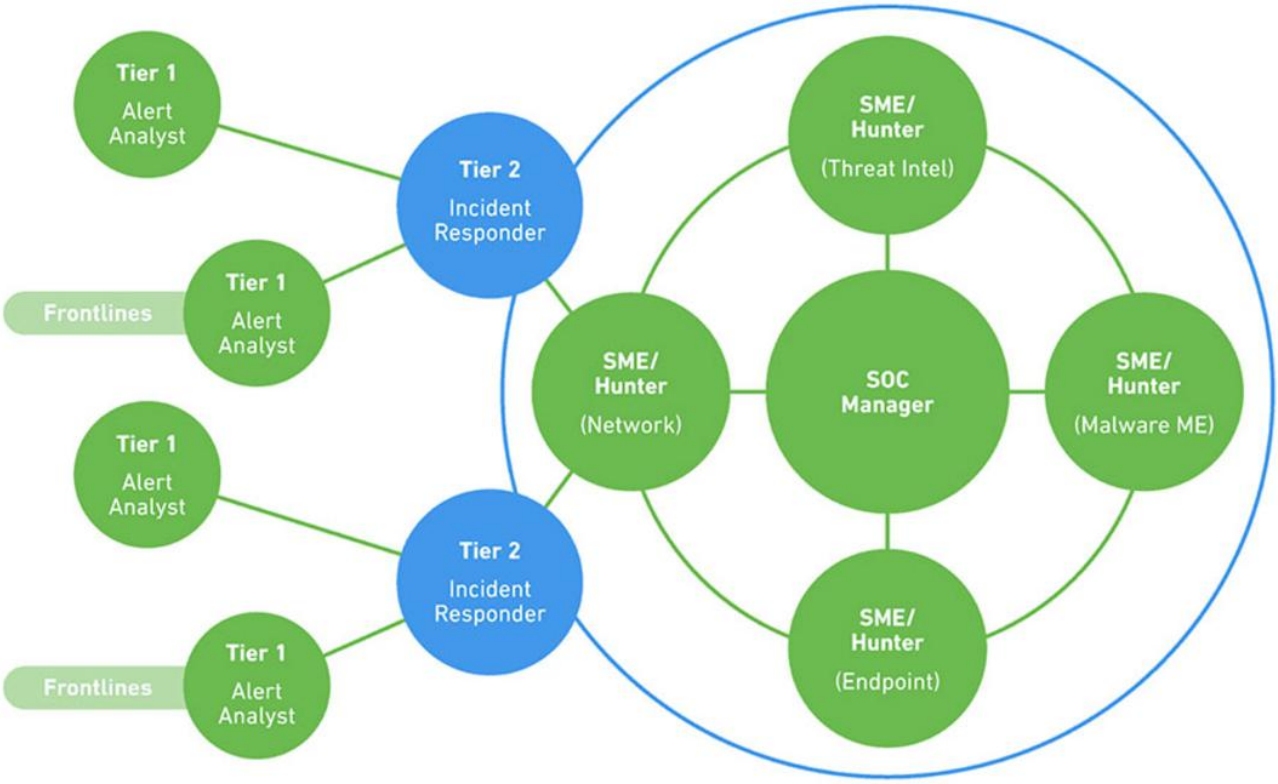
Toteutetaan pieni keskitetty SOC organisaatiomalli MITREn ohjeistusten mukaan, joka on toimiva yrityksille, joissa on noin 5–20 työntekijää. (Kuvio 1)



Kuvio 1. Organisaatiomalli

2.1 SOC roolit

SOC-tiimi voidaan jakaa neljään tasoon (Kuvio 2) tehokkaan uhkien prosessoinnin ja hallinnan takaamiseksi. Tasoilla on kyberpuolella erilaisen taustan omaavia työntekijöitä, jotka reagoivat kyberuhkiin, ja tarvittaessa siirtävät ne seuraavalle tasolle esimerkiksi kyseisen uhan asiantuntijalle. Tier 1 tasolla monitoroidaan SIEM-järjestelmää, analysoidaan ja priorisoidaan hälytyksiä. Tier 2 tason analyytikot saavat tason 1 oikeaksi havaitut uhat. Tämän tason henkilöstöllä on syvempi kyberosaaminen. Tier 3 vastaa kriittisten tietoturvaloukkausten hallinnasta ja myös uhkien jatkuvasta metsästyksestä (Threat Hunting) organisaatiossa. Tasolla 3 olevalla henkilöstöllä on syvempää osaamista jostakin tietystä kyberuhasta, esimerkiksi tietoverkon uhista tai haittaohjelmista.



Kuvio 2. Soc-tiimin roolit. (Orion Cassetto. 2022).

Tauluko 1. Soc-tiimin vastuut ja roolit. (Orion Cassetto. 2022)

Rooli	**Osaaminen**	**Tehtävät**	**Henkilöt (SOC)**
Tier 1 – Analyytikko **(Hälytyksien analysointi)**	Henkilöt päteviä järjestelmänhallinnassa, ohjelmoinnissa (kuten Python, Ruby,	SIEM-monitorointi, tietoturvamonitorointityökalujen hallinta ja konfigurointi. Hälytysten priorisointi ja arviointi	Maija Mainio, Karri Kari, Tiina Taitava

	PHP), skriptauskielissä. Sertifikaatit (CISSP, SANS SEC401).	todellisten tietoturvaloukkausten tunnistamiseksi.	
Tier 2 – Analyytikko **(Reagoi tietoturvapoikkeamiin)**	Kokemus vastaavista taidoista kuin tasolla 1. Syvempi kokemus esim. haittaohjelmista, forensiikasta ja uhkien tiedustelusta. Mahd. eettisen hakkeroinnin osaaminen etu.	Saa oikeat uhat tasolta 1. Reagoi niihin uhkatiedustelun avulla selvittääkseen hyökkäyksen luonteen ja sen vaikutuksen. Tekee strategian uhkan rajaamiseen ja poistamiseen, jotta järjestelmä saadaan normaalitilaan.	Harri Keko, Martti Mainio, Anna Jalo
Tier 3 - Analyytikko (Asiantuntija ja uhkien metsästäjä)	Tason 2 taitojen lisäksi syvällisempi kokemus haittaohjelmista, penetraatiotestauksesta ja uusien uhkien tunnistamisesta. Ymmärrys uhkista ylemmällä tasolla, ja tietojen visualisoinnista esim. johdolle.	Metsästää aktiivisesti uhkia ja aukkoja järjestelmässä. Kriittiset tapaukset tulevat tasolta 2 tälle tasolle. Päivittäinen järjestelmän skannaus, penetraatiotestaus uhkatiedon etsiminen ja viimeisimpien kyberuhkatietojen ymmärrys.	Antti Arvo, Topi Toivio, Jesse Seppälä
Tier 4 - SOC-johtaja	Kokemusta projektinhallinnasta, tietoturvapoikkeamien hallinnasta ja viestinnästä.	Rekrytoi ja kouluttaa SOC-henkilöstöä, vastuussa strategioista hyökkäyksessä ja puolustuksessa. Organisaation yhteyshenkilö turvallisuudessa, vaatimuksien vastaamisessa ja tietoturvapoikkeamissa.	Sini Saukko

Lähteet

Orion Cassetto. Security Operations Center Roles and Responsibilities. Exabeam artikkeli. 2022. Viitattu 20.11.2024. https://www.exabeam.com/blog/security-operations-center/security-operations-center-roles-and-responsibilities