Playbookin toteuttaminen

Ryhmä 13

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

Poikkeamienhallinta ja kyberturvakeskukset TTC6060 - 3007
6.12.2024
Tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

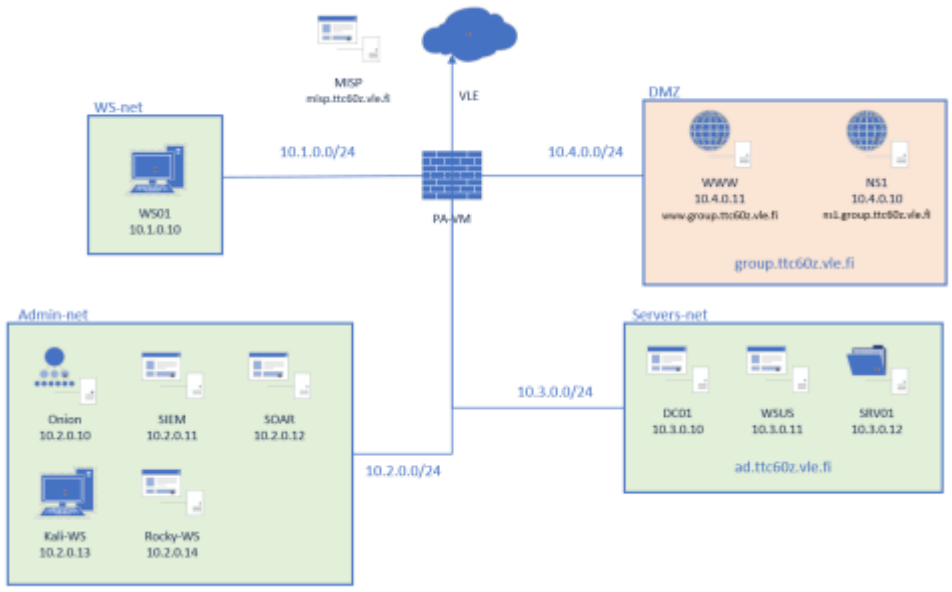
Kuviot

Taulukot

1 Johdanto

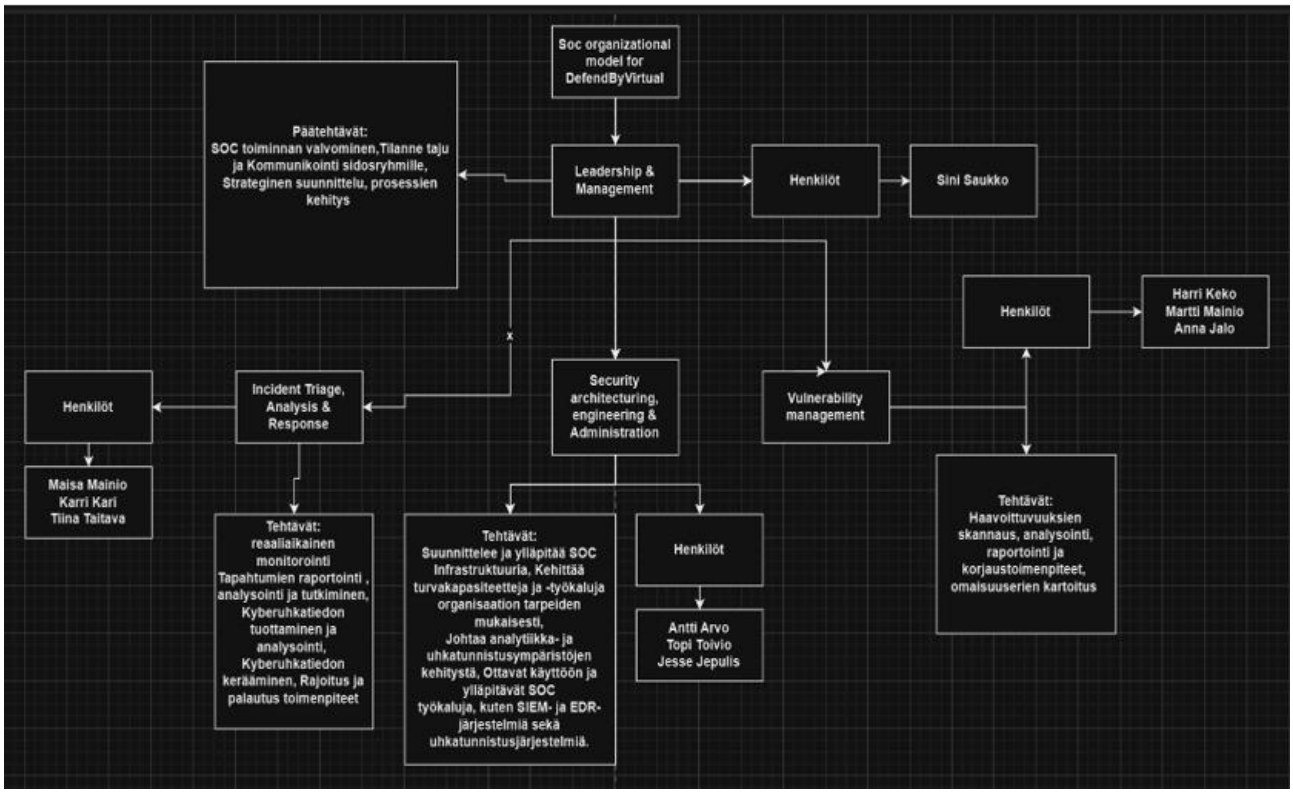
Tämän harjoitustyön tarkoituksena on tutustua playbook käsitteeseen SOC ympäristössä. Playbookilla tarkoitetaan toimintasuunnitelmaa, joka määrittelee toimenpiteet ja prosessit tiettyjen tilanteiden hallintaan, kuten kyberuhkan toteutuminen.

Playbook toteutetaan harjoituksessa kuvitteellisen DefendByVirtual yrityksen VLE ympäristöön, joka kuvattu kuviossa 1.



Kuvio 1. VLE

Playbook toteutetaan harjoituksessa 2 tehdylle SOC-organisaatiolle. (Kuvio 2).



Kuvio 2. SOC-organisaatiomalli

2 Uhka-analyysi

Toteutamme playbookin kiristysohjelmahyökkäyksen (ransomware) varalta.

Ransomware on haittaohjelma, joka salaa organisaation tiedostot ja vaatii lunnaita niiden vapauttamiseksi. Hyökkäykset voivat aiheutua haitallisista sähköposteista, haavoittuvuuksien hyväksikäytöstä, haitallisista verkkosivustoista tai vaarantuneista etäyhteyksistä. Todennäköisyys ransomware-hyökkäykselle altistumiselle on keskikorkea, kiristynyt kybervaikuttamisen tilanne voi nostaa riskiä huomattavasti.

Ominaisuudet:

- Nopea leviäminen organisaation verkossa.
- Tiedostojen salaaminen ja pääsyn estäminen.
- Ransomnote-viesti, jossa vaaditaan maksua.
- Voidaan käyttää kaksivaiheista kiristystä (tiedot varastetaan ennen salausta ja uhataan julkaista ne).

Vaikutus:

- Liiketoiminnan keskeytyminen.
- Maineen heikkeneminen.
- Mahdolliset juridiset seuraamukset.
- Taloudelliset tappiot (lunnaat, palautumiskustannukset, sakot).

3 Playbook

Playbook on ennalta laadittu toimintasuunnitelma, joka ohjaa organisaation toimintaa erityistilanteissa, kuten kyberuhkien ilmetessä. Sen tarkoituksena on kuvata selkeästi ja yksityiskohtaisesti toimenpiteet, joita tulee noudattaa eri vaiheissa – uhkien havaitsemisesta niiden torjuntaan ja tilanteen jälkeiseen palautumiseen. Playbook parantaa organisaation kykyä reagoida tehokkaasti, minimoida vahingot ja palauttaa normaali toiminta mahdollisimman nopeasti. Kyberuhkien varalta laadittu playbook sisältää myös vastuut ja aikataulut, jotka varmistavat sujuvan yhteistyön eri toimijoiden välillä. Lisäksi playbook toimii koulutus- ja viestintätyökaluna, joka auttaa henkilöstöä ymmärtämään roolinsa ja tehtävänsä kriisitilanteissa. (Ransomware Incident Playbooks: A Comprehensive Guide. 2024).

3.1 Playbookin vaiheet NIST:n suosituksien mukaan

Preparation:

- Roolit ja vastuut: Määrittele avainhenkilöt ja heidän tehtävänsä. Roolit tulee olla selvillä SOC-tiimillä, jotta toiminta on ransomware- tilanteessa tehokasta ja tieto saadaan oikeille henkilöille.

- Tietoturvakoulutus: Kouluta henkilöstöä tunnistamaan uhkia ja raportoimaan ne. Henkilöstön tulee osata huomata mahdolliset kiristyshaittaohjelmat ja ne tulee raportoida SOC-tiimille.

- Varotoimet: Varmuuskopioi data ja testaa palautusprosessit säännöllisesti. Varmuuskopioilla voidaan varmistaa tärkeiden tietojen pysyminen organisaatiolla, vaikka kiristyshaittaohjelma kohdistettaisiin niihin.

- Päätelaitteiden ja verkon suojaus: Käytä ajantasaisia suojausohjelmia, monivaiheista tunnistautumista (MFA) ja verkon valvontaratkaisuja. Ohjelmat ja automatisoidut valvontaratkaisut voivat huomata ja estää ohjelman ennen sen pääsyä päätelaitteisiin.

- Dokumentaatio ja harjoitukset: Kirjaa palautusprosessit ja harjoittele ennakoivasti niitä. Palautus tulee olla mahdollisimman nopea, jotta liiketoiminta saadaan taas käyntiin hyökkäyksen jälkeen.

Detection and Analysis:

- Uhkan tunnistus: Tarkkaile yleisiä hyökkäystapoja, kuten haitallisia sähköposteja, selainhaavoittuvuuksia ja USB-laitteita. Voidaan selvittää esimerkiksi MITRE:n APT toimijoiden (PPT) avulla, mitä mahdollisia haittaohjelmia voitaisiin organisaatioon kohdistaa.

- Priorisointi: Arvioi tapahtumien kriittisyys luokittelumatriisin avulla (kriittinen, korkea, kohtalainen, matala). Priorisointi ja väärien positiivisten arvioiminen on tärkeä osa analyysiä, jotta saadaan seuraavat askeleet tietoturvapoikkeamassa selville.

- Viestintä ja toimenpiteet: Määritä prosessi tapahtumien raportointiin ja tarvittaviin toimenpiteisiin. Kun uhka on tunnistettu ja priorisoitu, voidaan mennä toimenpiteisiin.

Containment, Eradication, Recovery:

- Eristäminen (Containment): Katkaise tartunnan saaneet järjestelmät verkosta ja estä hyökkäyksen leviäminen. Heti, kun saadaan selville kiristyshaittaohjelman olevan järjestelmässä, tehdään tarvittavat eristystoimenpiteet.

- Poistaminen (Eradication): Poista haittaohjelma, sulje vaarantuneet tilit ja korjaa hyökkäyksessä käytetyt haavoittuvuudet. Poistetaan hyökkäyksessä järjestelmään tuotu ohjelma ja varmistetaan kaikkien vaarantuneiden tilien ja ohjelmien toimenpiteet, jotta hyökkääjä ei voi näitä hyväksikäyttää.

- Palautus (Recovery): Palauta tiedot ja järjestelmät varmuuskopioista vasta kun se on eristetty, sekä haittaohjelma on poistettu, ja haavoittuvuudet paikattu.

Post-Incident Response:

- Juurisyyanalyysi: Tunnista hyökkäyksen alkuperä ja estä vastaavat tulevat hyökkäykset. Analyysillä voidaan varmistaa tällaisten hyökkäyksien estäminen, tai ainakin parempi varautuminen jatkossa.

- Parannukset: Korjaa tekniset puutteet, virheet prosessissa ja viestintäongelmat. Tämän avulla voidaan parantaa prosessia jatkon kannalta. Kaikkia prosessin kulkuun ja järjestelmän palauttamiseen, negatiivisesti vaikuttaneita asioita pyritään parantamaan ennen seuraavia kertoja.

- Koulutus: Päivitä henkilöstön tietoturvakoulutus ja tarkenna toimintakäytäntöjä. Koulutuksen päivittäminen voi olla tarpeen, kun saadaan uutta tietoa organisaatioon vaikuttavista uhista ja siitä, miten prosessit toimivat niitä vasten.

- Tietoturvapolitiikan vahvistaminen: Varmista, että koko organisaatio noudattaa päivitettyjä tietoturvapolitiikkoja. Huomattujen parannusmahdollisuuksien avulla tehdyt uudet politiikat tietoturvassa tulee olla kaikilla selvillä.

(Liite 1. Ransomware incident response playbook framework. 2023.)

3.2 Uhkan tunnistaminen ja analysointi

Ransomware-hyökkäyksen tunnistaminen alkaa epäilyttävän toiminnan havaitsemisesta järjestelmissä. SOC-tiimi käyttää SIEM-järjestelmää ja EDR-työkaluja analysoidakseen hälytyksiä, jotka voivat viitata tiedostojen salaukseen, luvattomiin prosesseihin tai verkkoliikenteen poikkeavuuksiin. Incident Triage -ryhmä analysoi ja priorisoi hälytykset ja kerää tilannekuvan uhkan etenemisestä. He hyödyntävät reaaliaikaista monitorointia ja tutkimusraportteja uhkan tyypin ja laajuuden määrittämiseksi.

Tunnistuskeinot:

- **Haitalliset prosessit ja ohjelmat:** Esimerkiksituntemattomat salausohjelmat tai epänormaalit resurssien käytöt
- **Poikkeava verkkoliikenne:** Liikenne tuntemattomiin IP-osoitteisiin ja verkkopalvelimet, jotka liittyvät haittaohjelmaan
- **Järjestelmämuutokset:** Tiedostojen uudelleennimeämiset, salausprosessit sekä mahdollinen ransomnote-tiedosto järjestelmässä

Havainnon käsittely:

- Aktivoi SOC-tutkijatiimi ja määrittele havaitun haittaohjelman laajuus
- Tarkista lokitiedostot ja järjestelmähälytykset, joissa näkyy epäilyttävää toimintaa, kuten suuria määriä tiedostojen uudelleen nimeämisiä tai merkkejä salauksesta
- Selvitä, onko tapahtunut tiedon ulosvientiä
- Dokumentoi havaintojen perusteella alustava tilannekuva ja priorisoi jatkotoimenpiteet

3.3 Uhkan torjuminen & lieventäminen

Ransomware-hyökkäyksen torjuminen vaatii nopeita ja koordinoituja toimia. Security Engineering -tiimi eristää tartunnan saaneet järjestelmät välittömästi verkosta estääkseen uhan leviämisen. Lisäksi he varmistavat, että varmuuskopiotiedostot ovat turvassa ja käytettävissä palautustoimenpiteitä varten.

Toimenpiteet uhkan torjumiseksi:

- **Eristäminen:** Tartunnan saaneiden laitteiden poistaminen verkosta ja muiden kriittisten järjestelmien suojaaminen
- **Haittaohjelmien tunnistus ja poisto:** Haittaohjelmat analysoidaan ja poistetaan
- **Palautus:** Tietojen palautus viimeisimmästä varmuuskopiosta ja tarvittaessa järjestelmien uudelleen alustaminen.
- **Tilanteen dokumentointi:** Kaikki toimenpiteet kirjataan tarkasti ja ne raportoidaan organisaation johdolle

Samanaikaisesti Vulnerability Management -tiimi suorittaa riskinarvioinnin organisaation muille järjestelmille ja omaisuuserille varmistaakseen, ettei muita heikkouksia ole.

3.4 Tiimien vastuut ja viestintä

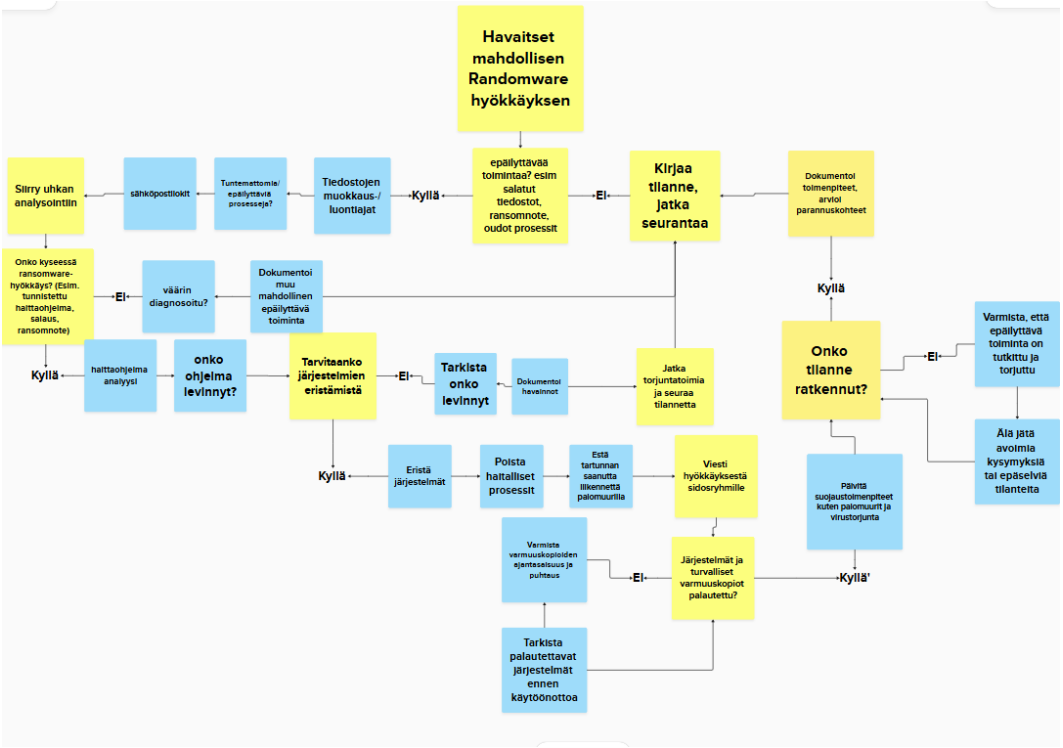
SOC:n toimintaa johtaa Leadership & Management -tiimi, joka vastaa strategisesta päätöksenteosta ja resurssien ohjauksesta. Jokaisella SOC-tiimillä on omat tarkasti määritellyt vastuunsa:

- **Incident Triage -tiimi:** Uhkan havaitseminen, analysointi ja ensimmäiset torjuntatoimenpiteet
- **Security Engineering -tiimi:** Tekniset toimet, kuten järjestelmien eristäminen ja haittaohjelmien poistaminen
- **Vulnerability Management -tiimi:** Omaisuuserien kartoitus, analysointi ja pitkäaikaiset korjaustoimenpiteet

Viestintä organisaation sisällä ja ulkopuolisten sidosryhmien, kuten asiakkaiden tai viranomaisten, kanssa tapahtuu erillisen, dokumentoidun viestintäprotokollan mukaisesti. Näin varmistetaan tiedon oikea-aikaisuus, tarkkuus ja johdonmukaisuus.

3.5 Toimintakartta

Playbookin toteutusta voidaan selkeyttää entisestään luomalla jonkinlainen visuaalinen toiminta-kartta kuvaamaan toteutusjärjestystä. Toimintakartta ransomwaren havaitsemiseen ja hallintaan liittyvistä toimenpiteistä on esitetty kuviossa 3.



Kuvio 3. Toimintakartta

4 Testaus ja ylläpito

Playbookin tehokkuus varmistetaan säännöllisillä testauksilla ja jatkuvalla ylläpidolla. Testauksessa käytetään simuloituja ransomware-hyökkäyksiä, jotka antavat realistisen kuvan tiimien reaktioky-vystä.

Testauksen vaiheet:

- **Harjoitusten järjestäminen:** Simulaatiot, kuten Red Team -hyökkäykset, joissa arvioidaan käytän-nön toimenpiteiden ja päätöksenteon toimivuutta
- **Tulosten analysointi:** Harjoitusten tulokset dokumentoidaan ja niiden perusteella tehdään tarvitta-via parannuksia.

Ylläpidon osalta SOC-tiimit tarkistavat ja päivittävät käytettävät työkalut, kuten SIEM- ja EDR-järjestelmät, sekä varmistavat, että tiimin jäsenillä on ajan tasalla oleva koulutus uhkien torjunnasta. Tämä varmistaa organisaation valmiuden myös uusien uhkien ilmetessä.

Lähteet

Ransomware Incident Playbooks: A Comprehensive Guide. 2.2.2024. Cyber Management Alliance. Viitattu 3.12.2024. https://www.cm-alliance.com/cybersecurity-blog/ransomware-incident-playbooks-a-comprehensive-guide.

Liitteet

Liite 1. Ransomware incident response playbook framework

Liite 2. Liitteen otsikko