



SOC toiminnan osa-alueet ja Security Analystin rooli

Arttu Nurmela

Haaga-Helia ammattikorkeakoulu

Tradenomin tutkinto

AMK-Opinnäytetyö

2023

Tiivistelmä

Tekijä(t) Arttu Nurmela
Tutkinto Tradenomi
Raportin/Opinnäytetyön nimi SOC toiminnan osa-alueet ja Security Analystin rooli
Sivu- ja liitesivumäärä 20 + 3
<p>Tässä työssä perehdytään Security Analystin työhön ja työkaluihin. Lukemalla työtä opiskelija tai vastavalmistunut voi saada tarvittavia avaintietoja, joiden avulla voi saada työpaikan Security Operations Centeristä. Työssä esitellään tyypilliset työkalut, joita hyödyntämällä parannetaan kohteen tietoturvaa ja harjoitetaan sen valvontaa. Työkalujen lisäksi työssä kuvataan esimerkkiskenaarioita, joita nämä kyseiset työkalut voivat tuoda käsiteltäväksi.</p> <p>Security Analystin työkalut ovat tärkeässä osassa hänen arkeansa, joten niiden esittely on pyritty kirjoittamaan selkeästi ja antamaan hyvän yleiskuvan niiden toiminnasta. Työkalujen esittelyssä pyritään tuomaan esille, kuinka niitä voi hyödyntää organisaation tietoturvan valvonnassa ja kehityksessä. Nämä työkalut sisältävät monia teknisiä toiminnallisuuksia, joten niiden esittelyssä keskitytään vahvasti tietoturvalvonnalla kannalta oleelliseen toimintaan. Lukijan tulee kuitenkin huomioida, että koko toimintamallin ymmärtäminen vie aikaa ja vaati paljon opiskelua. Koulutussertifikaatit, joita työssä on tuotu esille vahvistaa näiden työkalujen kokonaisvaltaisen hallitsemisen.</p> <p>Opinnäytetyössä kerrotaan myös tyypillisistä verkossa tarjolla olevista harjoitusalueista, joiden avulla jokainen tietoturvasta kiinnostunut voi harjoittaa omaa osaamistaan laajoista verkko-labroista ja kokeilla miten tietoturvatestaajan työkalut sekä tietoturvan valvojan työkalut toimivat. Työssä myös kuvataan, miltä verkkopohjainen hyökkäysyritys voi näyttää lokienvallontatyökalun näkökulmasta.</p>
Asiasanat Tietoturvaopas, Kyberturvallisuus, tietotekniikka, tietoturvapuolustus, analytiikka

Sisällys

1	Johdanto	1
2	Ammattitehtävän esittely	3
2.1	SOC:n jäsenet	3
2.2	Kokonaiskuva liiketoimintamallista	4
3	Miten päästä Security Analystiksi?	6
3.1	Hackthebox, tryhackme	6
3.2	Koulutus taustalla	7
3.3	Oma tekninen osaaminen	8
4	Työkalut	9
4.1	IP-selvitykset	9
4.2	EDR	10
4.3	NDR	12
5	SOAR	14
5.1	Raportointi osana työtä	14
5.2	Tietoturvapoikkeaman raportointi ja selvitys	15
6	SIEM	16
6.1	Lokien hallinta	16
6.2	Hakulausekkeet	17
6.3	Automaatio ja tekoälyn vaikutuksia	18
7	Pohdinta	20
	Lähteet	21

1 Johdanto

Tietoturvan tärkeys korostuu yhä enemmän ja enemmän mediassa, yrityksissä ja lainsäädännössä. Useista uutismedioista ja artikkeleista on luettavissa tarinoita tietoturva-rikkomuksista ja väärinkäytöksistä. Suomessa lähivuosina yksi kohutuimmista tieturvarikkomuksista oli Vastaamon tapaus, jossa monien potilaiden kaikki kertomukset ja vuodettiin internetiin. Tämäkin, johtui vakavasta tietoturvahaavoittuvuudesta. Tällaiset tapaukset tuovat aina esille tietoturvan tärkeyden. Oma ammatillinen suuntautumiseni ohjautuu vahvasti tietoturvaan ja haluan tällä työllä selvittää, mitkä ovat ensimmäiset askeleet alalle ja millaisia taitoja sekä ominaisuuksia on hyvä hallita. Selviytyö koostuu kirjallisuuden, artikkelien ja toimenkuvien perusteella. Työ soveltuu IT- ja tietoturva-alan opiskelijoille ja vastavalmistuneille, ja tukee aloittelijan kasvamista ammatillisessa kehityksessä.

Työssä esitellään aluksi ammattitehtävää Security Analyst, sillä se on usein ensimmäinen askel tietoturvan uraa. Esittelyssä on myös mukana tyypillinen tiimi, joka työskentelee osana Security Operations Centeriä. Kun esittelyt on käyty, aletaan työssä syventyä Security Analystin rooliin ja työtehtäviin. Työssä kuvataan, millaista osaamista ja mielenkiintoa hakijalta voidaan vaatia, jotta pärjää työtehtävässä, tärkeää on toki muistaa, ettei kaikkia voi osata heti.

Seuraavana on vuorossa työkalujen esittely ja niihin perehtymistä. Teknisellä alalla on tärkeää osata ja kyetä oppimaan aina uusia työkaluja, joiden avulla työtehot kasvavat ja tietoturvan parissa valvonta tehostuu. Työssä esitellään avointen lähteiden työkaluja IP-osoite selvityksiin, työasemasuojausta EDR:llä, verkkomonitorointia NDR:llä, SOAR:in ja SIEM:n käyttöä alustana työelämässä. Aiheesta kiinnostaa monet tekniset työkalut, joilla tietoturvaa valvotaan. Työssä ei kuitenkaan huomioida, miten työkalut on rakennettu kooditasolla, eikä myöskään ota kantaa niiden kaupalliseen pärjäämiseen. Aihealue on kattava ja ajankohtainen, joten jokainen tietoturvasta innostunut voi saada siitä paljon irti.

Taulukko 1. Keskeinen termistö

NDR	Verkkoliikenteen valvontatyökalu
EDR	Päätelaitteiden valvontatyökalu
SIEM	Keskittetty lokienkeräys – ja hallintatyökalu

SOAR	Tietoturvalvonnin automatisointi ja orkestrointi alusta
SOC	Yksikkö, joka muodostuu usean eri osaamisalueen tietoturva-ammattilaisista
Security Analyst	Henkilö, joka on erikoistunut tietoturvalvontaan
IP-osoite	Verkkoon liitettyjen laitteiden yksilöintiin käytetty numerosarja, internet protokalla
Palomuuuri	Järjestelmä, joka valvoo verkkoliikennettä ja estää hyökkäämisyritykset verkosta
Blue Team	Ryhmä henkilöitä, jotka varmistavat tietoturvan toiminnan simuloitussa tilanteessa
Red Team	Ryhmä henkilöitä, jotka harjoittavat tietoturva hyökkäyksiä simuloitussa tilanteessa
Päätelaite	Laitteita, jotka on kytketty verkkoon. Esimerkiksi kannettava tietokone, työasema, puhelin
Raakaloki	Dataa, jonka päätelaite lähettää kerättäväksi
Tiedosto Hash	Tiedoston uniikki cryptograafinen tunnistetiet

2 Ammattitehtävän esittely

Security Analyst on osa Security Operations Centeriä eli SOC:ia. Ammattitehtävän ydin on tietoturvalvonta, jossa Security Analyst valvoo kohteen, esimerkiksi yrityksen tietoturvaa apunaan osaava tiimi ja kehittyneet työkalut. Security Analysti pyrkii löytämään yrityksen ohjelmistojen datasta tietoturvaa vaarantavia tekijöitä, joita kyberrikollinen voi hyödyntää. SOC on yleisesti ympäri vuorokauden toimiva yksikkö, sillä kysyntä jatkuvalla tietoturvalvonnalle on suuri. Ympäri vuorokautisella valvonnalla mahdollistetaan jatkuva saumaton reagointivalmius tietoturvauhkien torjuntaan ja niiden korjaustöiden aloittamiseen.

2.1 SOC:n jäsenet

Jokaisella jäsenellä on oma rooli ja työtehtävät Security Operations Centerissä, koska valvonnan kokonaisuus on ratkaiseva tekijä toimittamaan palveluita. Tectargetin kirjoittajan Ashwin Krishnanin mukaan osasto vaatii viisi avainhahmoa, jotta palvelun tarjoamisesta pystytään suoriutumaan. Ensimmäinen henkilö on Incident responder, jonka päävastuu on hallita ja monitoroida tietoturvalvontaan käytettyjä työkaluja. Tietoturva on nopeasti muuttuvaa, joten järjestelmien pitää jatkuvasti olla päivitettyinä. Päivitetyt järjestelmät pystyvät havaitsemaan tehokkaammin uusimpien uhkien trendiä ja vastaamaan niihin määritetyllä tavalla (Krishnan 2020). On huomioitavaa, että SOC:n koon mukaan samoissa rooleissa voi olla monia henkilöitä. Usein myös samat henkilöt edustavat useaa roolia. Yksikön koko voi siis vaihdella muutamasta henkilöstä useisiin kymmeneen tai jopa satoihin.

Toisena henkilönä listalla on Security investigator. Nimensä mukaisesti tämän hahmon vastuulla on tehdä syvällistä tutkintaa järjestelmien tunnistamista uhkista ja väärinkäytöksistä. Uhkan tai väärinkäytöksen ilmaantuessa Security investigatorin tehtävä on myös tehdä suunnitelma, kuinka uhka saataisiin poistettua (mitigation plan) ja tarvittaessa toteuttaa se yhteistyössä hänen tiiminsä kanssa. (Krishnan 2020).

Kolmas henkilö on Advanced security analyst. Verkkoartikkelissa todetaan, että tämä on vaativa ja pitkän kokemuksen tuoma asema. Työssään hänen tehtävänä on löytää uusia ennalta tunnettomia uhkia ja heikkouksia järjestelmistä. Tällainen hahmo toimii myös usein senior-roolissa, joten hän pyrkii myös ohjaamaan ja kouluttamaan uudempia SOC:in jäseniä esimerkiksi. Security analysteja. (Krishnan 2020).

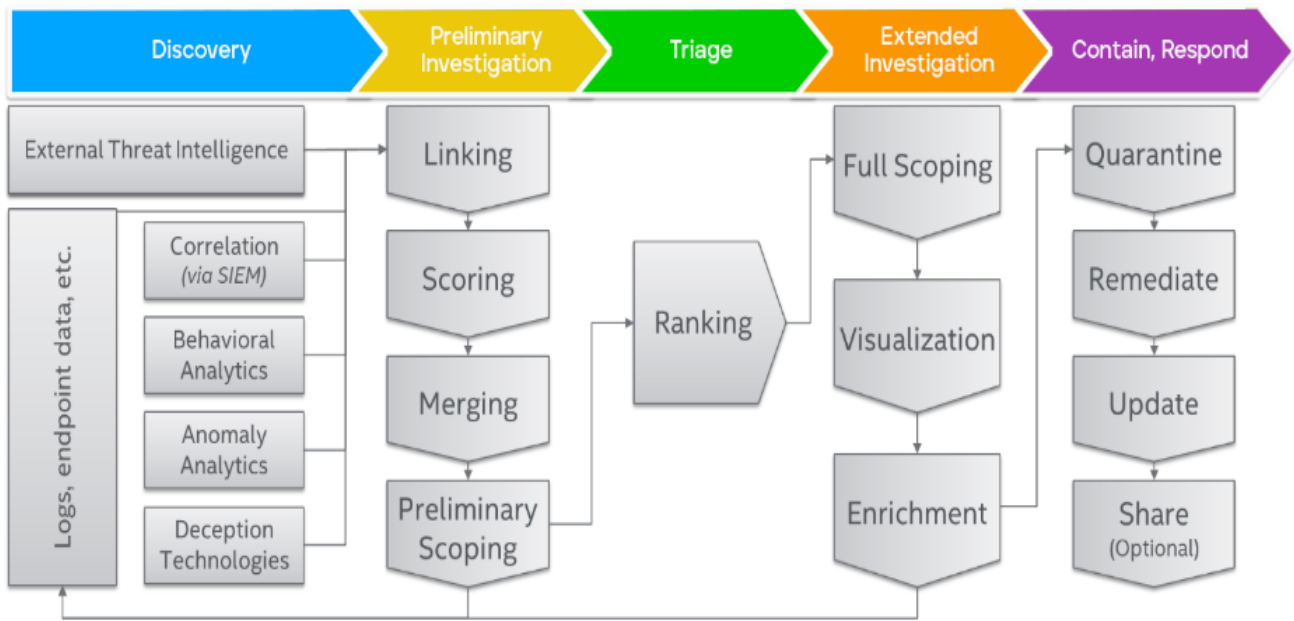
Neljäs henkilö on SOC manager. Johtohahmona manager on kuitenkin myös erittäin pätevä ja käytännön tunteva tietoturvalvonnassa. Hän pitää yhteyttä asiakkaidensa CISO:on eli tietoturvavastaavaan henkilöön ja muihin asiakkaiden tietoturvan henkilöstöön. SOC manager pyrkii myös kasvattamaan liiketoimintaa, joten hän tapaa uusia potentiaalisia asiakkaita. (Krishnan 2020).

Viimeinen henkilö on Security engineer/architect. Arkkitehti vastaa SOC:n toiminnan kannalta kriittisen tärkeistä valvontatyökaluista. Hän testaa ja valitsee parhaat työkalut toimittajilta. Arkkitehti toimii myös yhteistyössä kehittäjien ja ylläpitäjien kanssa, jolloin pitkäkestoinen infrastruktuuri on turvattu. (Krishnan 2020).

2.2 Kokonaiskuva liiketoimintamallista

Tietoturvan tärkeys on viime vuosien aikana noussut enemmän ja enemmän esille yritysten toiminnassa. Suuret yritykset pitävät hallussaan massiivisia määriä suojattavaa dataa, kuten talous- ja henkilötietoja. Resurssien ja osaajien ollessa vähissä turvaudutaan ulkoiseen tekijään ja ostetaan tietoturva palveluna. Tietoturva-ammattilaisten määrä kysyntään verrattuna on vähäinen (MTV-utiset 2022). MTV:n uutisartikkelin mukaan osaajia tarvitaan myös valtion tasolla, turvaamaan yhteiskunnan toiminnan kannalta kriittiset palvelut, mm. Sähkön, lämmön ja puhteen veden jakelu.

Security Operations Center onkin palvelu, joita tietoturvaan erikoistuneet toimijat myyvät asiakkaille. SOC:n asiantuntijat ovat koulutettuja ja työssä tietoturvan valvontaan perehtyneitä. Yllä mainittuja palveluita valvoo OT (operational Technology) asiantuntijat, jotka ymmärtävät kriittisten palveluiden valvonnan tarpeet. Lokidatan keräämisen avulla voidaan luoda kattava valvonta, jonka jatkuvalla kehityksellä ja ylläpidolla voidaan turvata yritysten tai valtion laitosten käyttämät laitteet tuottavat. Lokidatalla voidaan kerätä kaikki toiminta mukaan lukien myös merkit mahdollisesta Kyber-hyökkäyksestä. Laitteiden haavoittuvuudet ovat hyökkääjien hyväksikäytettäviä ja niistä kuvaus kappaleessa kuusi. Kuvassa yksi kuvataan Security Operations Centerin toimintaa ylätasolla.



Kuva 1. Mikä on Security Operations Center (Trellix)

Fool.com:n artikkelin mukaan ulkoistetulla SOC-palvelulla voidaan vähentää kustannuskuluja ja saavuttamaan parempi tietoturva. (Long 5.8.2022). Kyber hyökkäyksen aiheuttama palvelun alhaalla olo aikaa (Downtime) voi aiheuttaa yrityksellä mittavia taloudellisia tappiota sekä henkilötietojen menetyksen, jonka arvoa ei voi mitata rahalla. Lisäksi menetetyt tiedot voivat aiheuttaa yritykselle pitkään kestäviä tutkintoja myös lakipykälien mukaan, jolloin tutkitaan, onko yritys itse luistanut tietoturvavelvoitteistaan.

3 Miten päästä Security Analystiksi?

Security Analystin tehtävät ovat usein ensimmäinen askel tietoturva-asiantuntijan uralla. Monet suuremmat yritykset tarjoavat koulutuksen loppusuoralla oleville tai juuri valmistuneille harjoitteluhjelmia, jotka kestävät usein noin puoli vuotta. Harjoittelun aikana tuore asiantuntija oppii alan työtehtävissä tarvittavia taitoja, kuten työkalujen käyttöä, uhkatilanteiden ehkäisyä ja raportointia sekä asiakasrajapinnassa työskentelyä. Ominaisuuksia, joita toivotaan Security Analystille:

- Analyttistä ja tutkintaintoista otetta
- Tuntemusta tietoverkoista
- Halua kehittyä
- Kyky oppia uusia asioita alati muuttuvassa ympäristössä
- Tiimityöskentelytaitoja
- Osamista tietoturva-alalta. Verkon harjoittelu materiaaleista lisää työn muissa osioissa.

Suomessa ammattikoulut, ammattikorkeakoulut sekä yliopistot tarjoavat kattavan tutkinnon myös tietoturva-alalle. Tietoturva on IT-alalla katsottuna hyvin laaja ja jokaisen osa-alueen toiminta vaatii vankkaa osaamista esimerkiksi tietoverkoista ja pilvipalveluista. Koulutus tarjoaa hyvän yleiskuvan näistä, mutta työssä oppiminen on ehdottoman tärkeää, sillä niin kutsutun oikean elämän tilanteita ja ympäristöjä voi olla hyvin hankalaa simuloida. Etenkin korkeakoulututkinnot tarjoavat opiskelijalle kattavat pohjatiedot ymmärtää työtehtävissään tulevia haasteita.

Cybersecurityguiden Tietoturva-analyytikon työtehtäviin pääsyyn vaaditaan neljää askelta:

1. Kykyä pystyä hakemaan tietoa ja tulkita sitä (Research)
2. Koulutusta. Useimmat työtehtävissä omaavat tradenomin, kandidaatin, maisterin tai insinöörin koulutusta. (education)
3. Sertifikaatteja eli koulutustodistuksia. Yleisimpiä sertifikaatteja alalla on muun muassa Microsoftin sertifikaatit, kuten SC-200. (certificate)
4. Verkostoitumista. Usein työpaikat saadaan tuttujen kautta ja auttaa saamaan tietoa alan tapahtumista (Network). (cybersecurityguide 2023)

3.1 Hackthebox, tryhackme

Verkossa on monia palveluita, joiden avulla pystyy harjoittelemaan omaa osaamista virtuaaliympäristöissä suoraan verkkoselaimella. Näitä harjoituksia voi siis tehdä missä ja milloin vain. Tehtäviä on niin aloittelijoille kuin myös pidemmälle edenneille alan ammattilaisille.

tryhackme perustajan Ashu Savanin mukaan hän halusi tarjota helpomman tavan tulla kyberturvalle. (hostingadvice 2020). Tämän tyyppiset verkkoharjoitukset ovat hyviä ja ne antavat hyvän yleiskuvan, miten Kyber-hyökkäys voisi tapahtua. Usein tietoturvan parissa auttaa se, että puolustava puoli (Blue Team) osaa myös hyökätä (Red Team), sillä mikä olisikaan parempi tapa puolustautua kuin osaamalla ennakoita hyökkääjän aiheet ja tehdä hyökkäyksestä mahdotonta alun perin. Suuret yritykset tarjoavat erilaisia ohjelmia tätä varten. Ohjelmat kulkevat usein nimellä Bug Bounty ja niiden päämääränä on havaita ohjelmistojen haavoittuvuudet tai ongelmat, jotta ne voidaan korjata ennen kuin hyökkääjä sen tekee. Usein ongelman löytäjälle on tarjolla myös palkkio. Osa tietoturva-ammattilaisista saattaa tehdä tällaisia tehtäviä pelkästään.

3.2 Koulutus taustalla

Suomessa on havahduttu ongelmaan, että kyberturvallisuuteen perehtyneiden määrä ei riitä vastaamaan suureen kysyntään. Monet yliopistot, ammattikorkeakoulut ja ammattiopistot tarjoavat kattavaa koulutusta alalle. Alan opintojen suuri etu on, että opiskelijat saavat usein jo työharjoittelun kautta suoraan vakituisen tehtävän, jossa pääsee syventämään omaa osaamistaan. Lisäksi kansainvälisiä opiskelupaikkoja on myös bachelorsstudiesin mukaan paljon. Suomessa ammattikorkeakoulun opinnot kestävät 3–4 vuotta riippuen koulusta ja tutkinnosta (Bachelorstudies).

Tutkinnon aikana opiskellaan tietoturvan lisäksi myös tietoverkkoja ja koodaamista, joka helpottaa ymmärtämään monien eri järjestelmien toimintalogiikkaa. Tietoverkot on hyvä omaksua varhaisessa vaiheessa, sillä suuri osa hyökkäyksistä tapahtuu verkon yli ja näin vaatii myös ymmärrystä erityisesti verkkoprotokollista. Usein insinöörin opinnot kestävät hieman pidempään kuin esimerkiksi tradenomin tutkinto. Kaakkois-Suomen ammattikorkeakoulu tarjoaa Suomessa labratyöskentelyyn perustuvat tutkinnon, jonka avulla käytännön läheisyys on taattu (XAMK).

Taulukko 2. Kyberturvallisuuteen perustuvia koulutusohjelmia:

Oppilaitos / Korkeakoulu:	Tutkinnon nimi:
Kaakkois-Suomen ammattikorkeakoulu	Kyberturvallisuus, Ylempi AMK.
Turku AMK	Kyberturvallisuus, insinööri
Metropolia	Kyberturvallisuus, Ylempi AMK.
Jyväskylän yliopisto	Kyberturvallisuuden maisteri opinnot

JAMK	Sovellettu kyberturvallisuus
Helsinki Business College	SOC specialist- koulutus

3.3 Oma tekninen osaaminen

Työnantajat arvostavat suuresti alalla itse hankittua teknistä osaamista. Virtuaaliympäristöjen hallinta on loistava keino oppia, kuinka järjestelmät kommunikoivat keskenään ja miten niitä hallitaan tietoturvallisesti. Verkosta löytyy oppaita, videoita ja labramateriaalia, joilla harjoitella. Tietoturvasta kiinnostunut voi esimerkiksi asentaa virtuaalipalvelimen, joka on täynnä haavoittuvaisia sovelluksia. Metasploitable on tunnettu työkalu, jolla voi harjoitella erilaisilla hyökkäystyökaluilla. Tätä kutsutaan penetraatio testaukseksi eli tunkeutumistestaukseksi. Laitteelle on asennettu haavoittuvia eli esimerkiksi vanhentuneita sovelluksia ja hyökkäystyökalujen avulla niitä voi käyttää hyödyksi. Tunkeutumistestaus on täysin sallittua ja laillista, kunhan huomioi sen, että kohde on oma laite tai sen omistaja on antanut luvan testaukselle.

Penetraatiotestauksen lisäksi koodaustaidoista on suurta hyötyä. Usein kokeneet koodaajat ovat aloittaneet uransa harrasteprojektin kautta ja innostuneet kehittämään omia ohjelmointitaitoja. Arduino on aloittelijaystävällinen tuote, joka mahdollistaa ohjelmoinnin yhdistettynä elektroniikkakomponenttien kanssa toimimiseen (Arduino 2018). Arduino yhdistetään osaksi haluttua projektia, vaikka leditaulua ja se ohjelmoidaan näyttämään tiettyjä valo-ominaisuuksia. Esimerkiksi jouluvalot voidaan luoda Arduinon ohjeistuksilla helposti. Kyberturvallisuuskeskuksen mukaan yhteiskunta tarvitsee lisää ammattiosaajia digitaalisessa maailmassa ja onkin julkaissut melko kattavan kokoelman erilaisia oppaita tunnettujen väärinkäytös tekniikoiden hyödyntämiseen (Traficom 2022).

4 Työkalut

Avoimet työkalut ovat Security Analystille tärkeitä. Ne auttavat ymmärtämään, mistä erilaiset yhteydet tulevat ja miten eri komponentit ja ohjelmistot toimivat. Jos Analystin valvottavassa ympäristössä alkaa esiintymään yhteydenotto yrityksiä tuntemattomista osoitteista, niiden alkuperää voi etsiä IP-osoitteen avulla internetistä. Avoimia lähteitä ja työkaluja hyödynnetään päivittäin ja keskusteluforumit voivat auttaa ratkaisemaan ongelman. Security Analystin työkalut ovat usein myös kaupallisia ja niitä ylläpitävät ja kehittävät suuret organisaatiot, kuten esimerkiksi Microsoft. Tämä auttaa työkalujen havainnointikyvyssä, sillä suurilla yrityksillä on paljon sidosryhmiä ja resursseja. Kaupalliset työkalut ovat usein saman tyyppisiä ja niiden toimintalogiikka toisiaan, mutta käyttöliittymissä voi olla suuriakin eroavaisuuksia. Nyrkkisääntönä on kuitenkin hyvä tietää, että jos hallitsee yhden tarjoajan EDR-työkalun käytön, on siirtyminen toiseen huomattavasti helpompaa.

4.1 IP-selvitykset

Security Analystinä on hyvä tuntee, kuinka eri IP-osoitteita pitää analysoida. Työtehtävissä Security Analyst tulee huomaamaan, että erilaisia yhteydenotto yrityksiä tulee palomuurille lukuisia lähes taukoamatta. Vaikka yhteyksiä on lukuisia, se ei tarkoita, että kaikki olisivat haitallisia, ongelmana onkin tunnistaa haitalliset osoitteet ja niiden yhteydet palomuurilokeilta. Julkiset IP-osoitteet ovat uniikkeja. Kasperskyn artikkelin mukaan IP:n lyhenne tulee sanoista internet protocol ja niillä pystytään tunnistamaan mistä dataa lähetetään ja minne. (Kaspersky)



Kuva 2: Mikä on IP-osoite (Rafter, D. 2022)

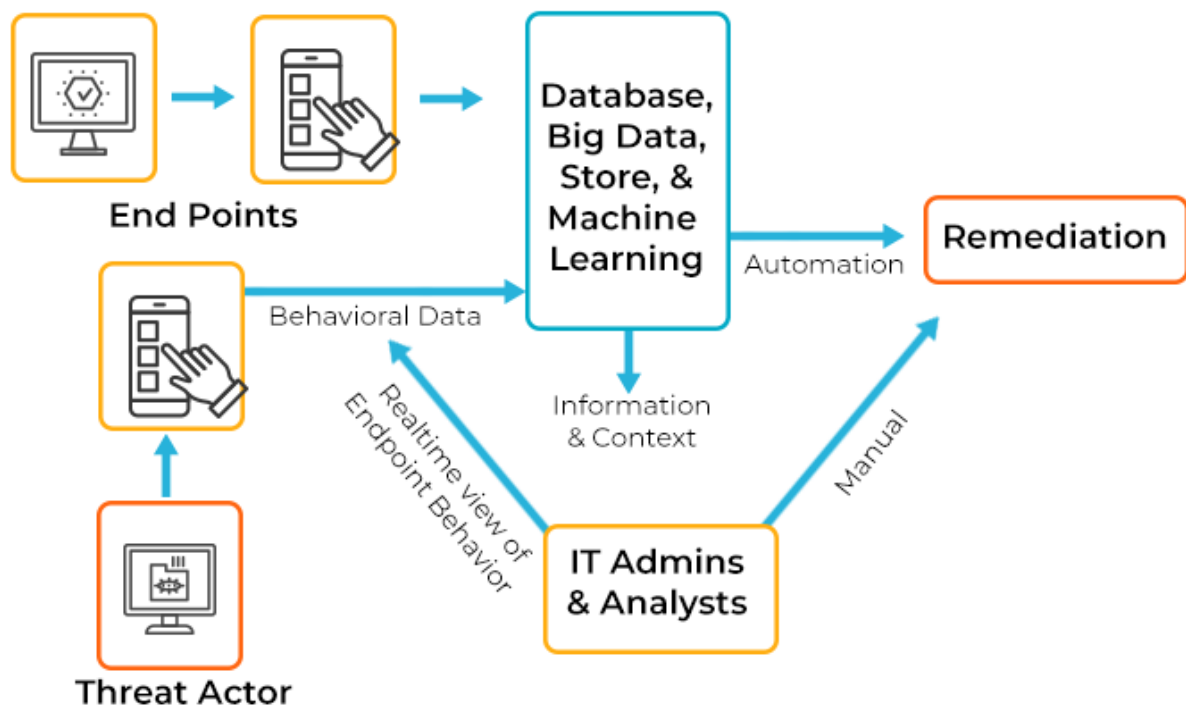
Verkossa on lukuisia työkaluja, joilla voidaan hakea osoitteita, joita palomuuuri on havainnut. Jos useita odottamattomia yhteydenottoja tulee tietystä osoitteesta, sitä voidaan hakea esimerkiksi abuseipdb:stä (AbuseIPDB 2023).

Abuseipdb on lukuisten käyttäjien luoma yhteisö, johon käyttäjät voivat merkata havaintoja tietyistä osoitteista. Kuvitteellisessa skenaariossa voisi olla tilanne, jossa on ulkomaalainen IP-osoite, joka yrittää ottaa yhteyttä haitallisella sisällöllä (Payload). Palomuurille asetetut tunnisteet (signaturet) tunnistavat osoitteesta tulleen paketin sisällön haitalliseksi ja torjuvat sen. Tietoturva-asiantuntijat huomaavat nämä yhteydenotot ja tutkivat tilannetta. IP-osoite ajetaan abusedbip:n tietokantaan, jolloin huomataan, että sama osoite on merkattu ja se lähettää eri kohteisiin yrityksiä murtautua sisään verkkoon. Tuntematon osoite on siis todettu haitalliseksi ja se voidaan palomuurilla laittaa mustalle listalle ja jatkossa kaikki samasta osoitteesta tulleet yhteydenotot estetään automaattisesti.

4.2 EDR

EDR tarjoaa suojaa käyttäjien päätelaitteille. Lyhenne tulee sanoista Endpoint Detection and Response. (CrowdStrike 2023) Yritysten käyttäjät ovat usein hyökkääjien kohteena, sillä heitä pidetään usein tietoturvan näkökulmasta helpoimpana kohteena. EDR:nän tehtävä on jatkuvasti ja automaattisesti seurata päätelaitteella tapahtuvaa toimintaa, joilla mahdolliset hyökkäykset voivat tapahtua. EDR voi olla alustana paikallisesti asennettu tai pilvipalvelun portaalina käyttötapauksesta riippuen. Usein suuren turvaluokituksen ympäristö voi vaatia paikallisen asennuksen, joka ei ole yhteydessä internettiin. Kuvassa kaksi on esitelty EDR:n toimintaketku. Dataa haetaan siis päätelaitteilta, joita tulkitaan järjestelmän automaatiolla.

HOW EDR WORKS

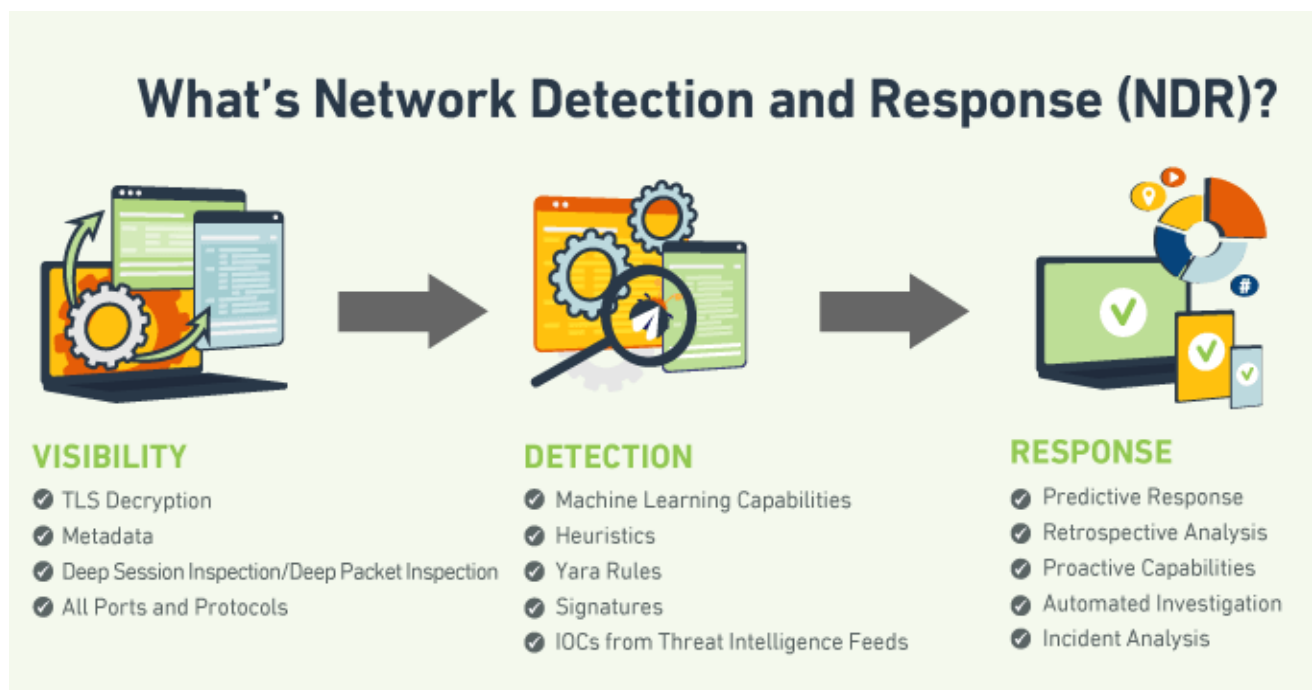


Kuva 2: Mikä on EDR? (BasuMallick, C, 2022)

Esimerkki skenaariona EDR:lle on tiedoston lataus. Käyttäjä tarvitsee hänen työkoneelleen ohjelman, jolla voi ottaa kuvankaappauksen näytöltä. Hän hakee verkosta avainsanaa "ilmainen kuvankaappausohjelma" ja hakukone tarjoaa lataussivun. Käyttäjä lataa ohjelman suoritettavan ohjelman, mutta se ei käynnisty koneella. Tämän takana on EDR:n suorittama valvonta, joka on ladatun tiedoston suoritusyrityksen aikana huomannut, että kyseessä on haittaohjelma, jolla pyritään saastuttamaan tietokone. EDR tarjoaa siis ehkäiseviä ominaisuuksia. Kyseessä voisi olla myös vastavasti sähköpostin liitetiedostoon piilotettu haittaohjelma.

4.3 NDR

NDR eli Network Detection and Response on järjestelmä, jota voidaan hyödyntää osana verkkoliikenteen valvontaa. NDR:n voi asentaa paikallisesti tai pilvipalveluna, kuten EDR:kin. Työkalu on usein teknisesti edistynyt ja se ei hyödynnä palomuurin tavoin “signatuureja” eli tietynlaisia avainmerkintöjä vaan se pyrkii tunnistamaan liikenteestä normaalista poikkeavaa toimintaa koneoppimisen turvin. Ciscon kuvauksen mukaan NDR pyrkii luomaan yrityksen verkkoliikenteestä normaalin kuvan (baseline) ja tulkitsemaan siitä poikkeavan toiminnan. Kuvassa esitellään NDR:n toimintaa. Kuvassa kolme kuvataan, miten NDR toimii.



Kuva 3: Mikä on NDR? (Mancine, G, 2020)

Esimerkki skenaario NDR:n toiminnasta.

Yrityksen tuotantolaitoksen verkkoliikenne on vähäistä ja NDR:n normaalitilan tunnistus on tehty. Liikenteestä alkaa kuitenkin näkymään poikkeamia kahden laitteen välisessä liikenteessä, jota ei ole aikaisemmin havaittu. NDR tulkitsee tämän poikkeavuutena ja nostaa siitä hälytyksen, jonka tietoturvatimi vastaanottaa. Tutkinnan aikana käy ilmi, että toiselle laitteelle on päätyntä haittaohjelma, koska se on yhteydessä internetiin ja se pyrkii louhimaan dataa toiselta laitteelta. Eli tässä tapauksessa NDR toi tarvittavan tiedon verkkoanomaliasta, jolla pystyttiin pysäyttämään tärkeiden tietojen vuotaminen, jolla voi olla kalliit seuraukset yritykselle. NDR:n toiminnallisuuteen voi lisätä myös torjuvia toimenpiteitä (preventive actions). Esimerkitapauksessa NDR olisi voinut

automaattisesti estää laitteiden välisen kommunikoinnin tutkimuksen ajaksi. Tällaiset toimenpiteet voivat kuitenkin aiheuttaa liiketoimintaan häiriöitä, mikäli hälytys olisi ollut turha (false positive). Tästä syystä normaalitilan kalibrointi on ehdottoman tärkeää, sillä tietoturvatutkinnat voivat olla aikaa vieviä ja vaativat paljon resursseja.

5 SOAR

SOAR eli Security orchestration, automation and response (SOAR) on järjestelmä, jota Security Analyst käyttää päivittäin osana työtään. Tämä alusta kerää yhteen tärkeimmät tiedot eri lähteistä ja prosessoi sitä käytettävään muotoon. SOAR:n automaatiokyvykkyydet ovat oikein käytettynä Security Analystin hyvä ystävä. Swimlanen artikkelin mukaan SOAR säästää tietoturvatimiä aikaa vieviltä manuaalisilta tehtäviltä ja auttaa priorisoimaan päivittäisen tekemisen. (Swimlane 2022)

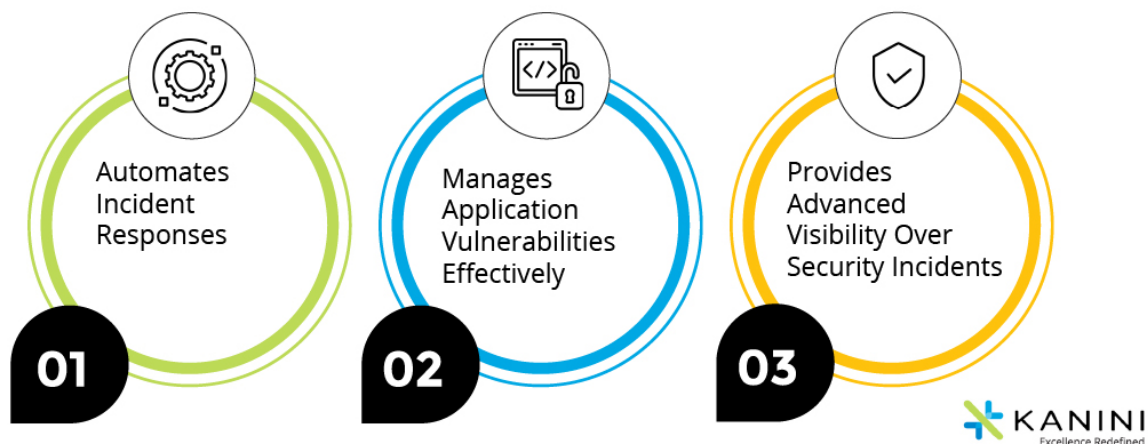
SOAR:iin on usein integroitu useita järjestelmiä, kuten SIEM, EDR ja NDR. Se kerää yhteen näiden järjestelmien tuottaman materiaalin (muun muassa käyttäjätiedot, lokidatan, hälytykset, laite-tiedot, verkkotiedot). Security Analyst voi siis tutkia esimerkiksi EDR:n tuottaman hälytyksen ja käsitellä sen suoraan SOAR:lta, jolloin hänen ei tarvitse avata EDR:n konsolia tai portaalia ollenkaan. Tämä säästää arvokasta työaikaa ja tehostaa tutkintaa. Havaintoja eri tietoturvatapahtumista voi tulla useasta tietolähteestä. SOAR pystyy tulkitsemaan tämän ja kostaa niistä yhdistetyn hälytyksen, jolle asettuu korkea käsittelyn priorisointiaste. Näin täyttyy järjestelmän tärkeä tehtävä, nopeuttaa vasteaikaa tietoturvatapahtumille. Usein tietoturvapoikkeamien käsittelylle määritetään sopimuksessa SLA (Service Level Agreement) aikaikkuna, jolloin sovitut toimenpiteet tulee olla tehtynä. Toimenpiteitä sovitaan tapauskohtaisesti, mutta niihin kuuluu muun muassa hälytyksen käsittelyn, raportoinnin ja selvityksen aika vastine.

5.1 Raportointi osana työtä

SOC:n palveluihin kuuluu myös säännöllinen asiakasraportointi. Raporttien esittelystä sovitaan palvelun tarjouksentekovaiheessa ja myös mitä tietoja raporttiin tulee. Raportin sisältöä on yleiskuva tietoturvasta, poikkeamien määrästä ja muista tärkeistä havainnoista. Raportoinnin tärkeä osa on käydä asiakkaan kanssa läpi tietoturvapoikkeamat, joita on esiintynyt raportointikauden aikana. Tällöin niiden jatkotoimenpiteistä ja kehityksestä voidaan keskustella, miten poikkeamia voi ehkäistä ja mitä voidaan tehdä ensikerralla paremmin. SOC palvelu kehittyy koko ajan ja uusia palveluita tuodaan mukaan jatkuvasti. Näistä keskusteleminen yhdessä asiakkaan kanssa voi tuoda lisämyyntiä ja kasvattaa liiketoimintaa. SOAR-alustat tarjoavat raportointimahdollisuuden. Se kykenee jalostamaan raportointijakson datasta kaavioita, yhteenvetoja ja paljon muuta dataa, joita voidaan esitellä asiakkaalle. SOAR:n tuottama sisältö säästää näinkin aikaa, koska SOC:n jäsenen ei tarvitse itse hakea dataa useasta eri lähteestä, vaan ne saadaan valmiina kootusti yhdestä paikasta.

5.2 Tietoturvapoikkeaman raportointi ja selvitys

SOC:n päätehtävä on havaita ja paikata tietoturvaan liittyviä uhkia ja poikkeamia. Usein nämä poikkeamat tulevat ilmi vasta uhkan sattuessa. Eri tietojärjestelmissä on useita haavoittuvuuksia ja niiden haitallista käyttöä ei voi aina ennustaa. NCSC:n artikkelin mukaan haavoittuvuus on heikkous it-järjestelmässä, jota hyödyntämällä hyökkääjä saa pääsen järjestelmään (National Cyber Security Centre, 2015) Järjestelmien tietoturvaan liittyviä havaintoja on siis tärkeää raportoida asiakkaalle, jotta ongelma voidaan korjata. Raportoinnin lisäksi poikkeaman ilmoittamisesta on tärkeää seurata poikkeaman kulkua ja valmistumista. SOAR:sta lähetettyä ilmoitusta kutsutaan usein tiketiksi. Tikein vastaanottavia kokonaisvaltaisia järjestelmiä on useita, mutta markkinoilla yksi suosituimmista on ServiceNow. ServiceNow yhdistää monet IT-alan tärkeät palvelut yhteen alustaan ja näin helpottaa tiedon käsittelyä päivittäisessä työssä. Se on rakennettu palvelemaan yrityksen työskentelyä ja tekee tikkettien seurannasta ja käsittelystä helpompaa. Palvelun pystyy integroimaan suoraan toiminaan SOAR-alustan rinnalla ja poikkeamailmoituksen seuranta on saumatonta.



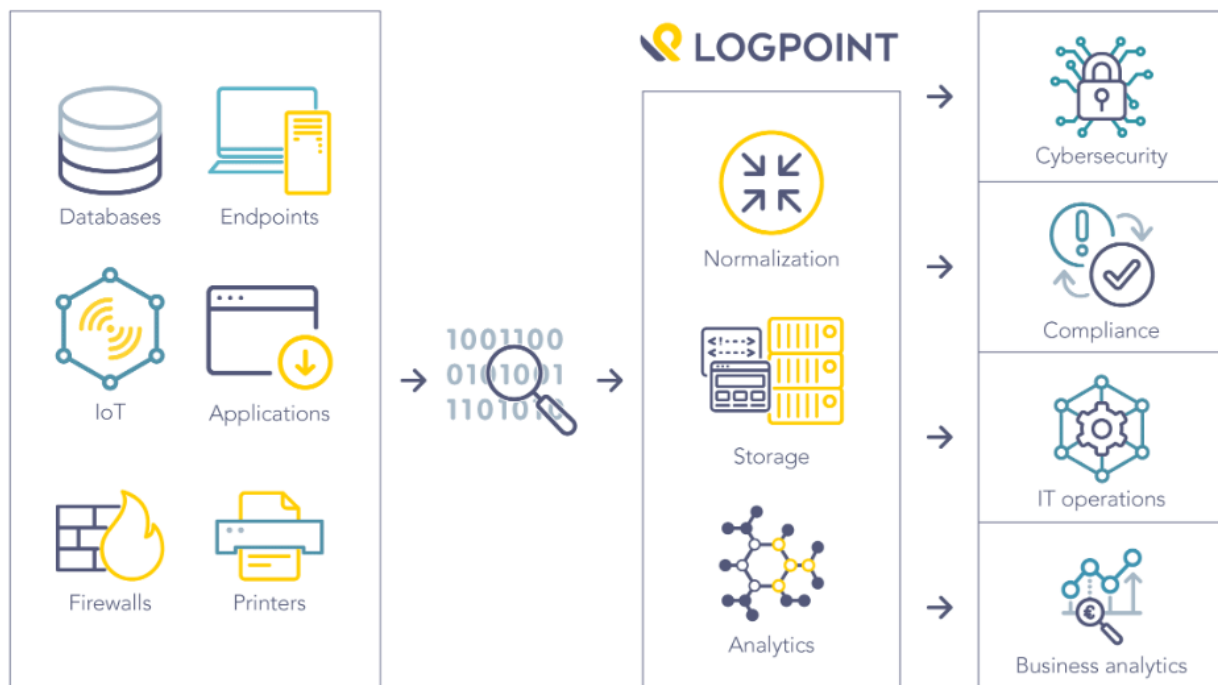
Kuva 4: ServiceNow ominaisuudet (Smith, J.)

Kaninin sivuilla kirjoitetun artikkelin mukaan ServiceNow auttaa nopeuttamaan tietoturvapoikkeaman reagointi ja selvitysaikaa. Automatisoidut palvelut auttavat yritystä selvittämään tapauksia nopeammin. (Joshua Smith).

6 SIEM

SIEM eli Security Information and Event Management. Tämä järjestelmä kerää lokidataa laitteista, joihin on asetettu lokitus päälle. Lokidataa on monenlaista, mutta karkeasti ilmaistuna se tarkoittaa kerättyä dataa laitteiden toiminnasta. Lokidatan kerääminen on olennainen osa tietoturvalvontaa, koska sillä voidaan jäljittää esimerkiksi käyttäjien tekemät muutokset järjestelmiin. Suomessa Katakri 2020 vaatii lokivalvontaa tietoturvakriittisiin ympäristöihin. (Katakri 2020, F-08.3) Kuvassa viisi esitellään SIEM:n kokonaisuutta.

SIEM at a glance



Kuva 5: Mikä on SIEM? (Logpoint, 2023)

6.1 Lokien hallinta

Lokien kerääminen on nykyjärjestelmissä helppoa. Logsignin artikkelin mukaan Windows ja Linux järjestelmät pystyvät keräämään lokitietoa mm. Systeemin- ja applikaatioiden toiminnasta ja niitä voi tarkastalla Event Viewer työkalulla (Logsign 2020).

Lokityyppejä on monenlaisia ja valvonnan tarpeita katselmoidessa päätetään, mitä lokia halutaan mistäkin järjestelmästä kerätä. Tässä kohtaa SIEM-järjestelmä tulee mukaan lokien valvontaan. Infrastruktuurista voidaan kerätä useiden laitteiden tuoma lokivirta yhteen ja lähettää ne kootusti ja pakatusti palvelimelle, jolle SIEM on asennettu. SIEM kykenee vastaanottamaan nämä paketit ja

sille voidaan asettaa normalisointipolitiikka. Tämä tarkoittaa NXlogin dokumentaation mukaan sitä, että tuotu lokidata muutetaan yleisesti luettavaan muotoon, esimerkiksi JSON:ksi. (Nxlog) Tämä mahdollistaa lokidatan luettavuuden ja käsittelyn SIEM-työkalulla mahdollisimman helpoksi.

Kuvassa kuusi nähdään sinisessä laatikossa lähteen lähettämä Syslog raakaloki, joka on normalisoitu punaiseen laatikkoon. Punaisen laatikon data on helpommin luettavaa ja vihreitä kenttiä kuten action, voidaan käyttää hakulausekkeessa datan suodattamiseen.

Tässä esimerkissä palomuuuri on torjunut liikenteen (action=Deny) URL-osoitteeseen, joka on yhdistetty uhkapelaamiseen.



Kuva 6: Lokinormalisointi (Have, T. 2016)

6.2 Hakulausekkeet

SIEM:n toiminnallisuuteen kuuluu myös edellä mainitut hakulausekkeet. Lokidatasta voidaan haakea tietyillä hakulausekkeilla niitä tapahtumia, joita halutaan valvoa. Näitä lausekkeitä kutsutaan Hälytyssäännöiksi (Alert rule, Use case). Kuten yllä olevassa kuvassa, palomuuuri tuottaa lokitietoa verkkoliikenteen tapahtumista ja sitä on miltein mahdoton seurata ilman spesifejä lausekkeitä, sillä palomuuuri voi tuottaa miljoonia rivejä lokia päivässä. Palomuurilla voi olla vakioituja torjuntasääntöjä tai torjuntasääntöjä voidaan mukauttaa tarpeen mukaan. Esimerkkikuvassa kuusi on estetty liikenne uhkapelisivustolle ja se ei vaadi toimenpiteitä, paitsi silloin kun liikenne olisi sallittua.

Tallaiselle toiminnalle voisi luoda säännön, jossa

```
url_category=gambling and action=allow
```

Näin saadaan hälytyssäännöllä ilmoitus, jos uhkapelaamiseen yhdistetty liikenne on sallittua. Valvonnassa on olennaista tietää mitä halutaan valvoa ja miksi. Tässä esimerkissä voisi syynä olla,

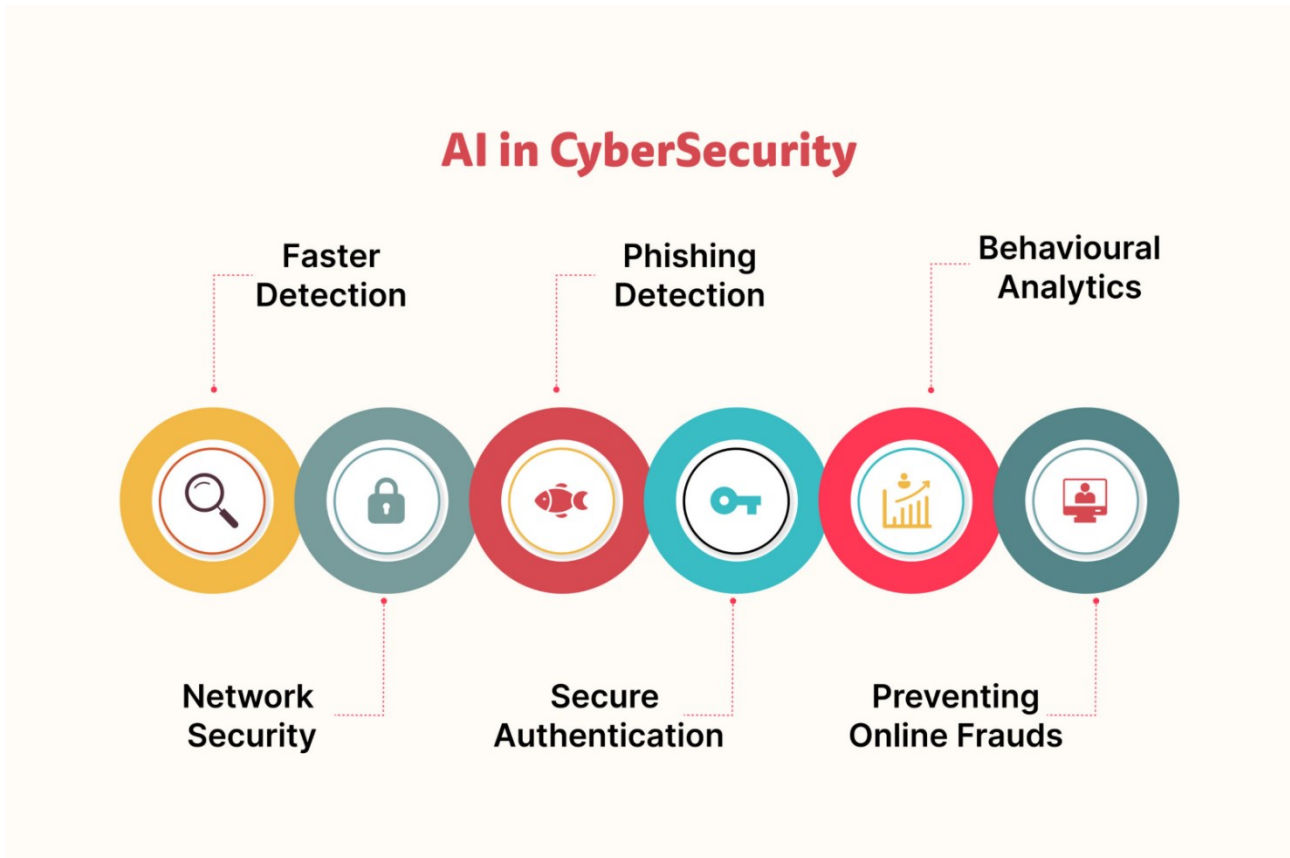
että organisaation politiikka kieltää uhkapelaamisen verkossaan ja työasemillaan. SIEM:n hälytys-sääntöjen tuottamat ilmoitukset voidaan kerätä SOAR-alustalle, josta Security Analystit ottavat sen käsittelyyn.

6.3 Automaatio ja tekoälyn vaikutuksia

Automaatiota ja tekoälyä hyödynnetään jo monissa tietoturva-järjestelmissä, kuten esimerkiksi EDR-työkaluissa. Tekoälylle annetaan näissä työkaluissa oppimisjakso, jossa koneoppimisella pyritään tunnistamaan järjestelmien ja verkkojen normaalitila. Työkalun asennusvaiheessa työkalu tarkkailee työasemien, palvelimien ja myös käyttäjien reaaliaikaista toimintaa ja oppii normaalitilan. Oppimisjakso voi kestää päivistä kuukauteen riippuen mitä työkalun sensoria opetetaan. Oppimisjakson jälkeen työkalun automaatio tunnistaa ja asetusten mukaan myös ehkäisee mahdollisia tietoturvapoikkeamia. Ehkäisevän toimenpiteen, kuten esimerkiksi työaseman eristämisen verkosta vaati ihmisen hyväksynnän tai varmistuksen. Automaatio seuraa tauotta laitteiden ja käyttäjien toimintaa, joka on ihmistyönä raskasta. Oppimisjakson normaalitilasta poikkeaminen, kuten uuden järjestelmälle tuntemattoman ohjelmiston asennus (Usein järjestelmä myös tutkii asennuksen tunnisteita, kuten tiedoston tunnisteiden hash-arvoa ja vertaa sitä uhkatietoon) ja nostaa siitä hälytyksen tutkittavaksi, jos se todetaan aiheuttavan vaaraa. Ohjelma voi esimerkiksi ottaa yhteyttä johonkin palvelimeen ja pyrkiä tuomaan sieltä uuden tiedoston laitteelle. Kyseisen toiminnan tunnistaminen on yksittäiselle henkilölle vaivalloista ja tallainen jää helposti huomaamatta. Automaatiolta kyseinen tunnistus vie joitakin sekunteja ja asennuksen ehkäisy, mikäli tiedosto on tunnistetusti haitallinen, tapahtuu millisekunneissa ja vaara pystytään ehkäisemään. IBM:n artikkelin mukaan EDR etsii kahdenlaista indikaattoria hyökkäyksestä.

1. IOC (Indicator Of Compromise) eli tunniste, joka voi olla esimerkiksi tiedosto-hash tai IP-osoite.
2. IOA (Indicator Of Attack) eli toimenpiteitä tai tapahtumia, jotka tunnistetaan hyökkäyksen tekniikoihin tai hyökkääjiin.

Artikkelissa myös ilmenee, että yllä olevia indikaattoreita ylläpidetään "Threat Intelligence" palvelussa, jossa jatkuvasti päivitetään ja ylläpidetään tietoa eri hyökkääjistä, hyökkäystavoista ja hyökkäysvälineistä (IBM, 2023). Tietoturvaa voi ajatella kissa ja hiiri leikkinä. Tärkeintä on pysyä edellä vastustajaa, tässä tapauksessa hyökkääjää. Jatkuva järjestelmien päivitys ja hyökkääjien tekniikoiden selvittäminen auttaa turvaamaan ympäristöt tehokkaasti. Kuvassa seitsemän nähdään, kuinka tekoälyä on valjastettu mukaan tietoturvaan.



Kuva 7: AI Kyberturvallisuudessa (OrangeMantra, 2022)

7 Pohdinta

Opinnäytetyön tavoitteena on olla tietoturva-alaa harkitseville opiskelijoille ja alalla työskenteleville oppaana ja tiedonlähteenä. Työssä kuvataan millaisia odotuksia, taitoja ja ominaisuuksia Security Analystiltä odotetaan ja auttaa antamaan ymmärryksen Security Operations Centerin toiminnasta sekä Security Analystin roolista. Security Analystin rooli on tässä työssä ensisijaisena ja työn edessä selviää, mitä työtehtävässä edellytetään. Työssä tuodaan esille myös Security Analystin tyypillisiä työkaluja, jotta niihin voi perehtyä ja tehdä harjoituksia verkossa. Työssä selvitetään myös tietoturvan tärkeyden kasvu valtakunnallisesti vuosittain ja tietoturva-asiantuntijan työtehtävät ovatkin sitä myöten merkityksellisiä.

Opinnäytetyötä tehdessä minun tuli ensimmäisenä kasata selkeät rajaukset työlleni. Tietoturva-ala on valtava kokonaisuus ja useat tämän työn aihealueet voisivat olla kokonainen työ jo itsessään. Tämän vuoksi työssä on kuvattu eri aiheiden keskeisimmät tiedot ja kertoa esimerkiksi tiettyjen työkalujen ominaisuuksista. Niiden teknistä toimintaa ei ole sen tarkemmin kuvattu, sillä se on rajattu pois. Onnistuin tuomaan esille keskeisimmän työn sisällön, josta lukija voi kerryttää omaa tietoisuutta hyödyntäen esimerkiksi lähdeluetteloja. Lähdeluettelo on pyritty kasaamaan palvelun- ja tuotteiden toimittajien omista artikkeleista ja dokumentaatiosta, sillä niitä ylläpidetään ja päivitetään. Lähteiden jatkuvuus on näin taattu varmemmin. Opin työssä myös tuottamaan informatiivista sisältöä, joka voi edesauttaa lukijaa ammatillisessa kasvussa, joka on myös tämän työn päätarkoitus. Tavoitteena oli myös tuoda esille ammatillista ymmärrystä aihealueesta.

Työ on tehty verkosta löytyvän materiaalin pohjalta. On tärkeää ymmärtää, että jokainen organisaatio toimii omalla tavallaan ja niiden käytänteet voi erota toisistaan, tämä työ on kuvattu mielestäni hyvin ylätasolla ja yksilöityä organisaatiota tai yksikköä ei ole otettu mukaan. Tietoturva-alan ammattilaisen on tärkeä hallita verkon materiaalin kriittinen hallinta ja osata löytää oikeat lähteet massasta.

Tietoturva-ala on jatkuvasti kehittyvää ja muuttuvaa. Työssä voisi myös kuvata tulevaisuuden näkymiä, tehdä vertailua tietoturvauhkien kehityksestä lähivuosien aikana. Työssä voisi myös kuvata eri työkalujen sensorien toimintalogiikkaa ja asennuksissa huomioitavia seikkoja, kuten järjestelmävaatimuksia ja tietoteknisten ympäristöjen skaalauksia. Tietoturvavalvonnan tarpeen kuvaaminen ja uhkakartoitus voisi myös olla mukana työn jatkokehityksessä.

Lähteet

AbuseIPDB 2023. About AbuseIPDB. Luettavissa:

<https://www.abuseipdb.com/about.html> .

Luettu 4.5.2023

arduino 2018. What is Arduino?

Luettavissa: <https://www.arduino.cc/en/Guide/Introduction>.

Luettu: 2.2.2023

Bachelorstudies 2023. Kandidaattiohjelma Kyberturvallisuudessa 2023.

Luettavissa: <https://www.bachelorstudies.fi/Kandidaatti/Kyberturvallisuus/>.

Luettu: 26.1.2023

BasuMallick, C, 2022. What is Endpoint Detection and Response? Definition, Importance, Key Components, and best practises.

Luettavissa: <https://www.spiceworks.com/it-security/endpoint-security/articles/what-is-edr/#lg=1&slide=0>

Luettu 1.5.2023

CrowdStrike 2023. WHAT IS ENDPOINT DETECTION AND RESPONSE (EDR)?

Luettavissa: <https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/>

Luettu 4.5.2023

cybersecurityguide 2023. How to become a cybersecurity analyst: A complete guide.

Luettavissa: <https://cybersecurityguide.org/careers/security-analyst/>.

Luettu: 2.3.2023

Have, T. 2016. Normalization.

Luettavissa: <https://www.logpoint.com/en/blog/normalization/>

Luettu 1.5.2023

Hostingadvice 2020. Learn Cybersecurity with TryHackMe.

Luettavissa: <https://www.hostingadvice.com/blog/learn-cybersecurity-with-tryhackme/>.

Luettu: 28.1.2023

IBM, 2023. EDR (Endpoint Detection and Response)

Luettavissa: <https://www.ibm.com/topics/edr/>

Luettu: 3.5.2023

Long, M.R, 5.8.2022. A Small Business Guide to the Security Operations Center (SOC).

Luettavissa: <https://www.fool.com/the-ascent/small-business/it-management/articles/soc/>.

Luettu: 26.1.2023

Logsign 2020. Logging of security events in SIEM

Luettavissa: <https://www.logsign.com/blog/logging-of-security-events-in-siem/>

Luettu 4.5.2023

Logpoint 2023. What is SIEM?

Luettavissa: <https://www.logpoint.com/en/what-is-siem/>)

Luettu: 1.5.2023

Kaspersky. What is an IP Address – Definition and Explanation.

Luettavissa: <https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address>.

Luettu 4.5.2023

Krishnan, A. 09.2020. 5 key enterprise SOC team roles and responsibilities, Techtarget Blog

Luettavissa: <https://www.techtarget.com/searchsecurity/tip/5-key-enterprise-SOC-roles-and-responsibilities>.

Luettu: 20.1.2023

Mancini, G. 2020. Why Fidelis is a Leading Provider of network detection and response

Luettavissa: <https://fidelissecurity.com/threatgeek/network-security/why-fidelis-is-a-leading-provider-of-network-detection-response/>

Luettu 1.5.2023

MTV-uutiset. Kuinka polvilleen Suomen voisi saada kyberiskulla? Osaajista tarvitaan lisää, erityisesti valtion tehtäviin

Luettavissa: <https://www.mtvuutiset.fi/artikkeli/kuinka-polvilleen-suomen-voisi-saada-kyberiskulla-osaajista-tarvitaan-lisaa-erityisesti-valtion-tehtaviin/8375816#gs.rnwhjo>.

Luettu: 24.1.2023

NCSC 2015. understanding vulnerabilities.

Luettavissa: <https://www.ncsc.gov.uk/information/understanding-vulnerabilities>

Luettu 26.4.2023

Nxlog. NXLog Documentation.

Luettavissa: <https://docs.nxlog.co/userguide/configure/normalization.html>.

Luettu 4.5.2023

OrangeMantra, 2022. How AI In Cybersecurity Reimagines Cyberthreat.

Luettavissa: <https://www.orangemantra.com/blog/how-ai-in-cybersecurity-reimagines-cyberthreat/>

Luettu 3.5.2023

Rafter, D. 2022. What is IP-address.

Luettavissa: <https://us.norton.com/blog/privacy/what-is-an-ip-address#>

Luettu 1.5.2023

SwimLane 2022. The Benefits of SOAR for your SOC Team

Luettavissa: <https://swimlane.com/blog/benefits-of-soar>

Luettu 4.5.2023

Smith, J. How ServiceNow SecOps helps organizations transform their IT security operations.

Luettavissa: <https://kanini.com/blog/servicenow/transformation-of-security-operations/>

Luettu 26.4.2023

Traficom 2022. Ohjeet ja oppaat tietoturva-ammattilaisille Luettavissa: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-tietoturva-ammattilaisille>.

Luettu: 3.2.2023

Trellix, 2023. What is SOC. Luettavissa:

<https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html>

Luettu 1.5.2023

xamk 2023. INSINÖÖRI (AMK), KYBERTURVALLISUUS. Luettavissa: <https://www.xamk.fi/koulutukset/insinööri-amk-kyberturvallisuus/>.

Luettu: 26.1.2023