jamk.fi

SOARin käyttöönotto ja sen vaikutukset SOC:n toimintaan

Saku Hopponen

Opinnäytetyö
Joulukuu 2019
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Hopponen, Saku	Opinnäytetyö, AMK	Joulukuu 2019
	Sivumäärä 55	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

SOARin käyttöönotto ja sen vaikutukset SOC:n toimintaan

Tutkinto-ohjelma

Insinööri (AMK), tieto- ja viestintätekniikka

Työn ohjaaja(t)

Jani Immonen, Matti Mieskolainen

Toimeksiantaja(t)

Viria Security Oy

Tiivistelmä

Opinnäytetyön toimeksiantajana toimi Viria Security Oy. Opinnäytetyön tavoitteena oli tehdä Security Orchestration, Automation and Response (SOAR) -alustan käyttöönotto ja havainnoida sen vaikutuksia Security Operations Center (SOC) -tiimin toimintaan ja suorituskykyyn valvontatyössä. SOC:n suorituskykyä haluttiin parantaa nopeuttamalla poikkeaman hallinnan manuaalisia työvaiheita automatisoimalla ja orkestroimalla työkaluja yhdestä alustasta, SOARista.

Opinnäytetyön teoriaosuudessa pyrittiin esittelemään SOC ja siihen liittyvät keskeiset aiheet kuten työkalut, poikkeaman hallinta ja SOAR. Toteutusvaiheessa käsiteltiin alustan käyttäjiin liittyvät asetukset, SOC:n työkalujen integrointi alustaan pelikirjoineen ja poikkeaman käsittelyn tekeminen SOARilla.

Tuloksissa havaittiin, että joitain SOARin hyötyjä pystyttiin havaitsemaan jo tärkeimpien työkalujen integroimisen jälkeen. SOC-valvonnan tekeminen yhdestä järjestelmästä sekä hälytystietojen haun automatisointi pelikirjoilla nopeutti analyysiprosessia ja mahdollisti paremman kokonaiskuvan saamisen poikkeaman hallinnassa. Alustan käyttöönotto todettiin hyvin laajaksi ja jatkuvasti kehittyväksi projektiksi. Alusta on modulaarinen ja sen muovaaminen toimeksiantajan tarpeisiin vaatii aikaa.

Lopputuloksena todettiin, että opinnäytetyössä käsitelty osuus oli SOARin alkuaskelia. Projekti on pitkä ja automatisoitavia prosesseja on paljon, mutta SOARin tuoma lisäarvo SOC:n suorituskyvylle prosessien automatisoinnilla ja kokonaiskuvan parantamisella oli jo huomattavissa. Todettiin myös, että vaikutusten mittaaminen opinnäytetyön käsittelemässä vaiheessa käyttöönottoa oli vielä hankalaa, koska mm. tiketöintiä ei ehditty integroida alustaan.

Avainsanat (asiasanat)

SOC, SOAR, orkestrointi, automatisointi, poikkeaman hallinta

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Hopponen, Saku	Bachelor's thesis	December 2019
		Language of publication: Finnish
	Number of pages 55	Permission for web publication: x

Title of publication

Deployment and effects of SOAR on SOC

Degree programme

Information and Communications Technology

Supervisor(s)

Jani Immonen, Matti Mieskolainen

Assigned by

Viria Security Oy

Abstract

The thesis was assigned by Viria Security Oy. The objective was to deploy Security Orchestration, Automation and Response (SOAR) platform and observe its effects on actions and performance of Security Operations Center (SOC) team. The aim was to improve SOC's performance by speeding up the manual tasks of incident management and response using automation and orchestration of SOC's tools from SOAR.

The theory section of the thesis aims to introduce SOC and its fundamental concepts, including tools, incident handling and SOAR. The implementation section covers the settings involving users of the platform, integrations of SOC's other tools and incident handling on SOAR.

Results showed that some benefits of SOAR can be seen after integrating the most important tools and building simple playbooks. Concentrating the SOC's monitoring on one user interface and automating information gathering with playbooks helped the analysis process and enabled gaining better situational awareness during incident handling. The deployment of SOAR platform was noted to be very large, time consuming and project under constant development.

The part of deployment covered in the thesis presented only first steps of SOAR. There are plenty of processes to be automated and the project takes time; however, the value SOAR offers to SOC-team's performance can be seen. It was also noted that measuring the effects of SOAR was difficult at an early state of deployment as in the thesis, because there was no time to integrate the ticketing system.

Keywords/tags (subjects)

SOC, SOAR, incident handling, security orchestration, security automation

Miscellaneous (Confidential information)

Sisältö

Kuviot

Lyhenteet

2FA	Two-factor Authentication
AD	Active Directory
API	Application Programming Interface
APT	Advanced Persistent Threat
ATD	Advanced Threat Detection
CEF	Common Event Format
CRUD	Create, Read, Update and Delete
DNS	Domain Name System
EDR	Endpoint Detection and Response
EPP	Endpoint Protection Platform
HTTPS	Hypertext Transfer Protocol Secure
HIDS	Host-based Intrusion Detection System
IDS	Intrusion Detection System
IOC	Indicator of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LEEF	Log Event Extended Format
MSSP	Managed Security Service Provider
MTTD	Mean Time to Detection
MTTR	Mean Time to Resolution
NIDS	Network-based Intrusion Detection System
NTA	Network Traffic Analysis
RBAC	Role Based Access Control
REST	Representational State Transfer
SLA	Service Level Agreement
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center

SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network

1 Lähtökohdat

1.1 Toimeksiantaja

Toimeksiantajana opinnäytetyölle toimi Viria Security Oy. Viria Security Oy kuuluu suomalaiseen Viria Oyj -konserniin, joka kuuluu Suomen suurimpiin kokonaisvaltaisen yritysturvallisuuden toimittajiin (Virian liiketoiminnat n.d.). Viria Security Oy on konsernissa emoyhtiö Viria Oyj:n tytäryhtiö. Se kuuluu turvaliiketoimintaan ja tuottaa sekä digitaalisen että fyysisen turvallisuuden ratkaisuja. Yrityksen tarjoamiin digitaalisen turvallisuuden palveluihin kuuluvat mm. kyberturvapalvelut, kuten kyberturvakeskus (CSOC) -valvontapalvelu. Lisäksi yhtiö tarjoaa yritysverkkoratkaisuja. Kantavana ajatuksena Virialla on ”vain yksi turvallisuus”, joka käsittää turvallisuuden kokonaisuutena, kattaen fyysisen ja digitaalisen turvallisuuden. (Vuosikertomus 2018.)

Virian juuret ovat Vaasan Läänin Puhelin Oy:ssa, josta tuli Anvia ja sittemmin Viria, teleliikenneyhtiö Elisan ostaessa suuren osan yrityksen toiminnoista 2016 (Toivonen 2017). Viria on sen jälkeen lähtenyt voimakkaaseen kasvuun merkittävien yrityskauppojen myötä. Vuonna 2018 Virian liikevaihto oli 104,9 M€ ja henkilöstön lukumäärä konsernissa oli 516. (Vuosikertomus 2018.)

1.2 Toimeksianto ja tavoitteet

Toimeksiantona oli ottaa käyttöön CSOC-tiimille uusi työkalu, Security Orchestration, Automation and Response (SOAR) -alusta. Työn tavoitteena oli konfiguroida käyttöön SOAR-alusta, liittää siihen Security Operations Centerin (SOC) käyttämät muut työkalut, kuten Security Information and Event Management (SIEM)- ja Advanced Threat Detection (ATD) -teknologiat, ja tarkastella SOARin vaikutuksia SOC:n toimintaan ja suorituskykyyn. Lisäksi tavoitteena työssä oli syventyä paremmin SOC-toimintaan ja siihen vaikuttaviin tekijöihin, joihin toimiva SOAR myönteisesti vaikuttaisi. Käyttöönotettu SOAR tuo toimeksiantajalle lisäarvoa poistamalla ylimääräistä manuaalista työtä täten myös nopeuttaen poikkeamien käsittelyä.

Käyttöönotetun SOARin tarkoituksena on keskittää tietoturvavalvonnan käyttö yhdelle alustalle, josta voidaan hallita poikkeamia ja vastata niihin nopeammin sekä tehokkaammin. SOAR tuo mukanaan myös SOC-toiminnan tehostamiseksi automatisointia pelikirjojen (engl. playbook) avulla sekä tilanteiden (engl. case) hallinnan ominaisuuksia nopeamman reagointikyvyn saavuttamiseksi.

2 Security Operations Center

2.1 Yleistä

Tänä päivänä kyberuhat, kuten hakkerit ja haittaohjelmat, ovat entistä kehittyneempiä, ja yritykset ovat heränneet tarpeeseen parantaa tietoturvaansa suojatakseen arkaluontoiset tietonsa (Zimmerman 2014, 1). Security Operations Center (SOC) eli tietoturvahallintakeskus on organisaation osa, jossa asiantuntijoista koostuva tiimi valvoo organisaation tietoverkkojen, järjestelmien ja laitteiden turvallisuustilannetta. Sen tehtävänä on havaita ja analysoida kyberturvallisuuspoikkeamia sekä vastata niihin erilaisia tietoturvateknologioita ja prosesseja käyttäen. SOC vastaa siitä, että tietoturvapoikkeamat tunnistetaan, tutkitaan ja niistä raportoidaan oikealla tavalla. SOC-tiimi koostuu pääosin analyytikoista, jotka yhdessä pitävät yllä tilannekuvaa valvottavan organisaation tietoverkkojen ja järjestelmien turvallisuustilasta. (Mts. 9-10.) Toimiva SOC muodostuu ihmisistä, teknologioista ja prosesseista ja niiden tehokkaasta yhteistoimivuudesta (ks. kuvio 1) (Torres 2015, 3).

Kuvio 1. SOC:n osat (Torres 2015, 3)

Organisaatioilla voi olla oma sisäinen SOC, tai se voi olla ulkoisen tahon, MSSP:n, tarjoama. Managed Security Service Provider (MSSP) on palveluntarjoaja, joka tuottaa tietoturvalaitteiden ja järjestelmien valvontaa ja hallintaa palveluna organisaatioille. Sen tarjoamiin palveluihin voivat kuulua esim. palomuurin hallinta, tunkeutumisen havaitseminen, antivirus-palvelut ja Virtual Private Network (VPN) -hallinta. (Managed Security Service Provider (MSSP) n.d.) Sisäinen SOC antaa täyden kontrollin työkaluille, prosesseille ja henkilöstölle, mutta ulkoistamalla palvelu MSSP:lle yritykset saavuttavat kustannustehokkuutta ja voivat keskittyä omaan ydinliiketoimintaansa. Tämä kuitenkin vaatii, että SOC:n ulkoistamisessa tietoturvapalveluita tarjoava kumppani tekee tiiviisti yhteistyötä palveluja ostavan yrityksen kanssa. (In-house SOC or MSSP 2019.)

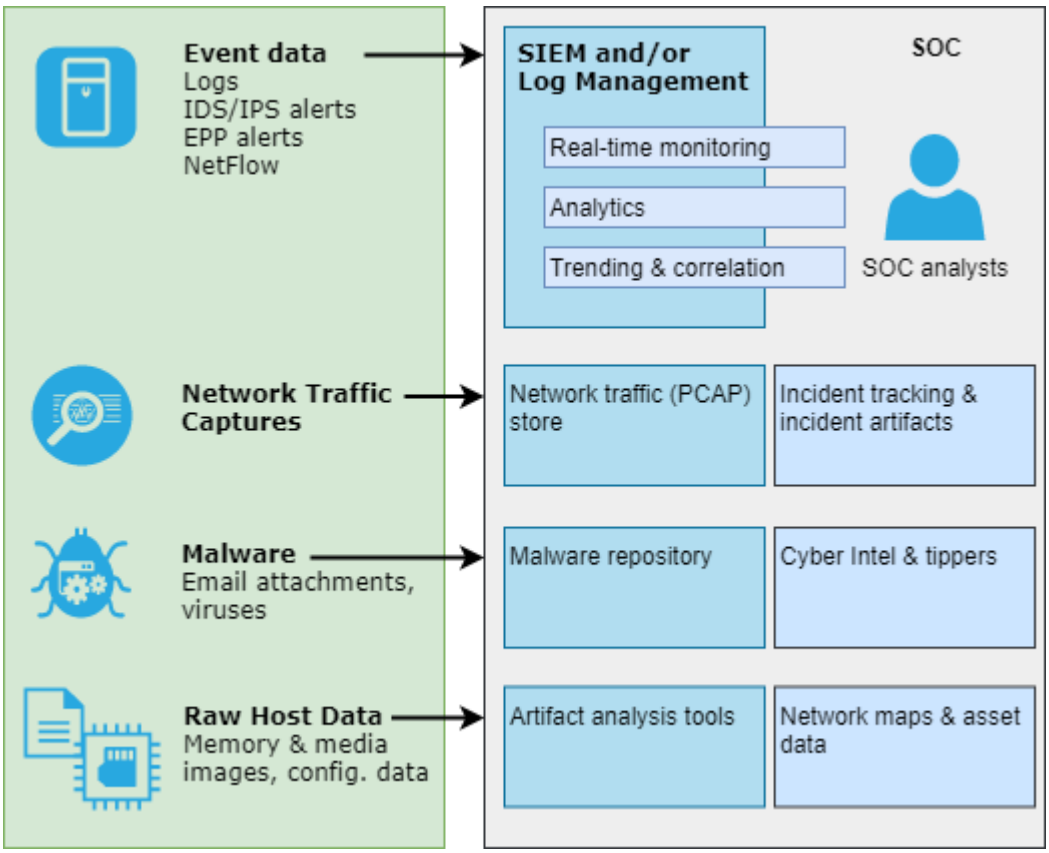
SOC-tiimi jakaantuu tyypillisesti eri tasoille (engl. tier). Tason 1 analyytikot suorittavat hälytysjonon jatkuvaa valvontaa ja luokittelevat hälytyksiä. Havaitessaan tarkempaa analysointia vaativan poikkeaman taso 1 eskaloi poikkeaman tason 2 analyytikoille. Tasolla 2 toimivat analyytikot, jotka kykenevät tutkimaan tietoturvapoikkeamia syvemmin ja korreloimaan eri lähteistä kerättyä dataa ymmärtääkseen, mistä on kyse.

Tällä tasolla tapahtuvan analyysin perusteella pyritään määrittämään poikkeaman vaikutukset ja tarvittavat korjaustoimenpiteet. Tasolta 2 voidaan tilanne vielä eskaloida 3. tasolle, kun kyseessä on esimerkiksi liiketoimintakriittinen poikkeama. Taso 3 pitää yleensä sisällään perusteellista osaamista mm. tietoverkoista, digitaalisesta forensiikasta ja haittaohjelmien takaisinmallinnuksesta. Näitä kaikkia tasoja johtaa SOC manageri, joka valvoo ja ohjaa tiimin toimintaa. (Torres 2015, 4.)

Sovitun palvelutasosopimuksen (engl. Service Level Agreement (SLA)) mukaan SOC voi työskennellä esimerkiksi 8x5, 12x5 tai 24x7 palveluajoilla. Työskentelyajan tarpeeseen vaikuttavat mm. asiakasorganisaation koko, vaatimukset ja SOC:n henkilöstön määrä. Koska hyökkääjät ”työskentelevät” kellon ympäri, 24x7 valvonnalla organisaation aika reagoida mahdolliseen hyökkäykseen saadaan minimoitua, mutta sen ylläpitäminen tulee luonnollisesti kalliimmaksi. (Zimmerman 2014, 291-294.)

2.2 Työkalut

SOC käyttää työkaluinaan tyypillisesti laitteiden ja verkon valvonnan sekä hallinnan työkaluja kuten palomuureja, Intrusion Detection System/Intrusion Prevention System (IDS/IPS) -järjestelmiä, verkkoliikenteen analysointijärjestelmiä, Security Information and Event Management (SIEM) -järjestelmiä sekä päätelaitesuojauksen ratkaisuja. Analysoitavaksi dataksi valvottavasta ympäristöstä kerätään esim. datavirtaa, pakettikaappauksia ja lokidataa, joita korreloimalla SOC voi havaita ja analysoida poikkeamia. SOC:n yleisimpien työkalujen arkkitehtuuri on esitetty kuviossa 2. (Zimmerman 2014, 34-35.)

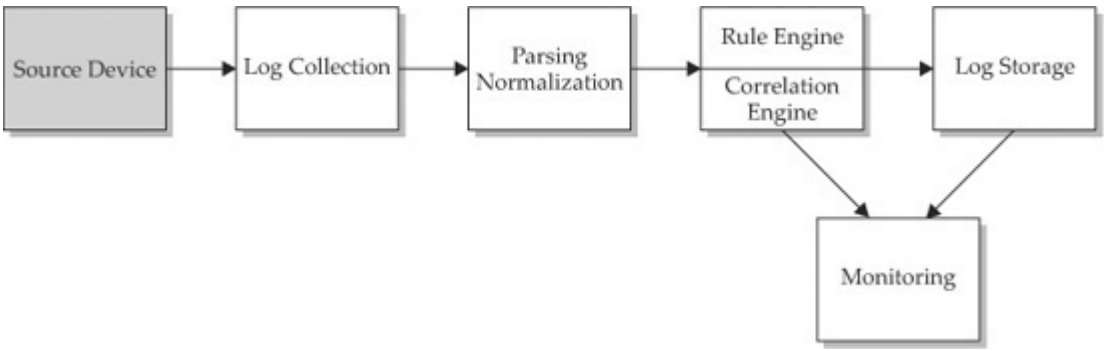


Kuvio 2. SOC-työkalujen arkkitehtuuri (mukaillen Zimmerman 2014, 33)

2.2.1 SIEM

SIEM on työkalu, joka lähes jokaisella SOC:lla on käytössään. SIEMin tehtävä on koota suuri määrä lokidataa ja muuttaa se informaatioksi, jota analyytikot voivat käyttää. SIEM kerää, kokoaa yhteen, suodattaa, varastoi, luokittelee, korreloi ja esittää tietoturvaan liittyvää lokidataa. SIEM mahdollistaa analyytikoille reaaliaikaisen sekä historiallisen näkyvyyden datasta. (Zimmerman 2014, 154-157.)

Yksinkertainen SIEM voidaan jakaa karkeasti kuuteen eri osaan, jotka toimivat itsenäisesti, mutta yhdessä muodostavat toimivan SIEM kokonaisuuden. Nämä osat on esitetty kuviossa 3. (Miller, Harris, Harper, Vandyke & Blask 2011.)



Kuvio 3. SIEMin osat (Miller, Harris, Harper, Vandyke & Blask 2011.)

Lähdelaite

Ensimmäinen osa, lähdelaite, on laite tai sovellus, joka syöttää dataa SIEMille. Data voi olla lokidataa tai jotain muuta dataa, jota laitteelta voi saada. SIEMiin kuuluva komponentti, joka kerää lokidataa lähdelaitteilta, on nimeltään kollektori. (Mt.)

Lokien keruu

Seuraava vaihe on lokien kerääminen, joka voidaan toteuttaa kahdella menetelmällä. Lähdelaite voi lähettää lokidataa SIEMin kollektorille, jolloin SIEM toimii vastaanottajana. Tästä yleinen esimerkki on syslog-protokolla, jonka avulla lähdelaite automaattisesti lähettää lokidataa vastaanottajalle. Vastaavasti SIEM voi kerätä lokidataa lähdelaitteelta noutamalla. Tällöin SIEM aloittaa yhteyden lähdelaitteelle ja aktiivisesti noutaa lokidatan sieltä. (Mt.)

Parsinta ja normalisointi

Kun lokidata on kerätty SIEMiin, kolmantena tapahtuu lokien parsinta ja normalisointi. Koska eri laitteet ja laitevalmistajat käyttävät lokeissaan eri formaattia, täytyy SIEMin parsia sille hyödyllinen tieto irti raa'asta lokidatasta ja normalisoida kerätty data yhdenmukaiseksi, jotta se voi hyödyntää erilaisia lokeja eri lähteistä. (Mt.)

Säännöt ja korrelointi

Neljäs osa käsittää SIEMin toiminnallisuuden tehdä ja käyttää sääntöjä sekä korreloida tapahtumia niiden perusteella. Säännöissä määritellään ehdot, joiden toteutuessa tapahtumasta luodaan poikkeama. Ehtoina voi olla esim. epäonnistunut kirjautuminen järjestelmänvalvojan tunnuksilla tai palomuurin estämien yhteyksien suuri määrä lyhyessä ajassa. Korrelointimoottori on osa sääntömoottoria ja sen tehtävänä on tutkia useampien eri lähteiden tapahtumien yhtyettä toisiinsa ja muodostaa niistä yksi tapahtuma/poikkeama. Korrelointimoottorilla saadaan logiikan avulla yhdistettyä hyvin erilaisia kriteereitä muodostamaan organisaatioiden turvallisuustarpeisiin vastaavia poikkeamahälytyksiä. (Mt.)

Lokien varastointi

Jotta SIEMistä voidaan tehdä kyselyjä aiemmin tapahtuneista tapahtumista, täytyy lokien olla varastoituna. Yleisin tapa lokien säilytykseen on tietokanta, kuten MySQL, Oracle, Microsoft SQL tai jokin muu tietokanta-alusta. (Mt.)

Valvonta

Viimeinen vaihe, monitorointi, käsittää SIEMiin tallennettujen lokien käyttämisen ja hyödyntämisen valvonnassa. SIEM-järjestelmässä on konsolirajapinta, joko web- tai sovelluspohjainen, jota analyytikot tai muut SIEMin käyttäjät käyttävät datan käsittelyyn ja SIEMin hallintaan. Koska SIEM normalisoi datan (kohta 3), tapahtumien käsittely ja analysointi kaikelle kerätylle lokidatalle onnistuu käyttöliittymän kautta. Sitä kautta hallitaan myös sääntöjä ja suoritetaan valvonta, sekä reaaliaikainen että menneiden tapahtumien. (Mt.)

2.2.2 IDS/IPS

Tunkeilijan havaitsemisjärjestelmä (engl. Intrusion Detection System (IDS)) on laitteisto/ohjelmisto tai niiden yhdistelmä, joka havaitsee järjestelmään tai verkkoon ta-

pahtuvat tunkeutumiset. Palomuuri ei välttämättä tarkista sen läpikulkemien pakettien datasisältöä, joten se voi sallia paketin läpi, vaikka se sisältäisi haitallista koodia. IDS tarkastaa jokaisen verkon läpi kulkevan paketin purkamalla sen ja tarkastamalla sen datan haitallisen koodin varalta, jonka jälkeen se kokoaa paketin alkuperäiseen muotoonsa ja lähettää eteenpäin. (Rao & Nayak 2014.)

IDS-järjestelmät voidaan jakaa kahteen eri tyyppiin: konepohjaisiin (HIDS) ja verkkopohjaisiin (NIDS). HIDS on yleensä ohjelmistopohjainen, tietokoneelle asennettava agentti, joka monitoroi ja raportoi sovellusten toimintaa. Se valvoo pääsyä järjestelmään ja sen sovelluksiin monitoroiden mm. lokeja ja luo hälytyksiä epätavallisista toimista, jotka se lähettää esim. SIEM-järjestelmään. NIDS suojaa puolestaan verkkoa ja sen resursseja verkon näkökulmasta. NIDS tarkastaa jokaisen verkkoon saapuvan paketin haitalliselta sisällöltä vertaamalla sitä tunnettuihin tunnisteprofiileihin ja havaitessaan poikkeavuuden verkkoliikenteessä se laukaisee hälytyksen hallintakonsoliin, kuten SIEMiin. (Mt.)

Tunkeilijan estämisjärjestelmä (engl. Intrusion Prevention System (IPS)) on laajennus IDS:lle. IDS:n kyetessä pelkästään havaitsemaan hyökkäyksiä, pystyy IPS aktiivisesti myös estämään hyökkäyksiä ja suojaamaan verkkoa pudottamalla paketteja tai blokkaamalla yhteyksiä. Nykyään verkkopohjainen tunkeutumisen havainnointi sekä estäminen ovat yhdistetty samaan järjestelmään. IDS/IPS-järjestelmien havainnointi perustuu erilaisiin mekanismeihin. Kaksi ensisijaista tekniikkaa ovat tunnisteisiin perustuva havainnointi ja poikkeavuuksiin perustuva havainnointi. (Mt.)

Tunnistepohjainen havainnointi on yksinkertaisin ja auttaa suojaamaan verkkoa tunnetuilta uhilta. Havainnointi tapahtuu vertaamalla verkkoliikennettä tietokannasta löytyviin, jo tunnettuihin hyökkäystunnisteisiin. Koska hyökkäyksen pitää tarkasti täsmätä tiedettyyn tunnisteeseen, pienikin muutos tunnetusta uhkatunnisteesta voi ohittaa järjestelmän huomaamatta, jonka takia tunnistetietokantaa täytyy päivittää jatkuvasti. (Mt.)

Poikkeavuuksiin perustuva havainnointi suojaa verkkoa tuntemattomilta uhilta. IDS/IPS-järjestelmä luo ensin normaalista verkkoliikenteestä vertailukohdan opiskelemalla normaaliliikennettä eri kellonaikoina ja muodostaen siitä lähtötason, johon se vertaa liikennettä havaiten siitä poikkeavuuksia ja laukaisten tarvittaessa hälytyksen. Poikkeavuuksiin perustuvan havainnoinnin yksi ongelmista on, että se tuottaa helposti virheellisiä positiivisia tuloksia (engl. false positive), joiden analysointi on SOC-tiimille ylimääräistä työtä. (Mt.)

2.2.3 Network Traffic Analysis

Hyökkäyspinta-alan kasvaessa erittäin suureksi yritysverkoissa, on avuksi kehitetty Network Traffic Analysis (NTA) eli verkkoliikenteen analysointityökalut. Vuonna 2017 kansainvälinen tutkimus- ja konsultointiyritys Gartner nimesi NTA-työkalut yhdeksi kasvavista teknologioista ja viime vuosina tuotetoimittajat ovat integroineet NTA-toiminnallisuuksia osaksi kokonaisvaltaisia uhkien torjunta-alustoja. (Yu 2019.)

NTA mahdollistaa SOC-tiimille uutta näkyvyyttä sekä havainnointi- ja tutkintakyvykkyyttä valvottavan organisaation verkkoon tarkastellen verkkoliikennettä ja analysoiden verkon sisällä tapahtuvia toimia, havaiten hyökkäyshavaintoja etenkin laitteilta ja sovelluksilta, joita on muuten hankala varustaa valvottavaksi tai jotka eivät lokita (Hein 2019). Pelkästään tunnisteita vasten tarkastamisen sijaan, NTA jatkuvasti valvoo ja kerää verkkoliikennettä ja pakettidataa. Ajan mittaan NTA muodostaa liikenteestä normaalin verkkokäyttäytymisen lähtötason, jonka jälkeen se havaitsee liikenteestä poikkeamia ja epätavallisuuksia vertaamalla liikennevirtaa lähtötasoon ja analysoimalla liikennettä matemaattisilla tai koneoppimisen algoritmeilla. Tyypillisen NTA-alustan tärkeimmät osat ovat liikenteen kollektori, datavarasto, analysointimoottori ja käyttöliittymä. (Yu 2019.)

SOC:lle NTA on tärkeä työkalu sen tarjotessa näkyvyyttä reaaliaikaisesta verkko- ja sovellusliikenteestä etenkin vaakasuunnassa, eli organisaation verkon laitteiden välillä, josta hyökkääjän sivuttaisliikkuminen (engl. lateral movement) tai mahdollinen tiedon vuotaminen kyetään havaitsemaan (mt). Gartnerin mukaan yritysten kannat-

taisi vahvasti harkita tunniste- ja hiekkalaatikkopohjaisten havainnointikeinojen täydentämistä NTA:lla, sillä se voi havaita verkon reunalla olevien tietoturvateknologioiden ohi päässeitä uhkia (Hein 2019).

2.2.4 Endpoint Protection Platform

Endpoint Protection Platform (EPP) -ratkaisu on päätelaitteille asennettava ohjelmisto, jonka tehtävänä on estää tiedostomuotoiset haittaohjelmat, havaita laitteelta haitallisia toimia, sekä tarjota tarvittavat tutkinta- ja korjaustoiminnot poikkeamiin reagoimiseen. Tänä päivänä tuotetoimittajat ovat ottaneet EPP-tuotteisiin mukaan päätoiminnallisuuksia Endpoint Detection and Response (EDR) -ratkaisuista, tavoitteenaan luoda kokonaisvaltaisempia ratkaisuja, joka yhdistää molempien kategorioiden höydyt. EDR:n tavoitteena on estämistoimenpiteiden sijaan havaita tietoturvapoikkeamia ja hallita niitä, ja kerätä niistä dataa, tarjoten SOC:lle erittäin tärkeää näkyvyyttä. (The Evolution of Endpoint Protection 2018.)

Kehittyneillä EPP-ratkaisuilla valvova SOC-tiimi saa näkyvyyttä suoraan työasemiin. EPP:n avulla työasemilta voidaan valvoa mm. käynnissä olevia prosesseja, verkkoyhteyksiä, tiedostojen suorittamista ja muokkaamista ja rekisterimuutoksia. Monissa tuotteissa haitallisen toiminnan tunnistamisessa ja analysoinnissa käytetään koneoppimista ja tekoälyä perinteisten tunnettujen uhkatietojen lisäksi. (Henderson 2019.) EPP-ratkaisut tehostavat SOC-tiimin poikkeamien tutkintaa tarjoamalla dataa päätelaitteiden tietoturvasta, jota voidaan korreloida muualta verkosta havaittuun dataan (Jablonska 2017).

2.3 Haasteet

Tänä päivänä kyberhyökkäykset ovat arkipäivää, hyökkäykset ovat entistä kehittyneempiä ja kysymys ei ole enää ”jos se tapahtuu” vaan ”koska se tapahtuu”. Tämän myötä SOC kohtaa monia haasteita pystyäkseen turvaamaan organisaation tietoverkon havaiten poikkeamat nopeasti ja vastaten uhkiin. SOC:n vastaanottamien hälytysten ja tapahtumien määrä kasvaa, kun valvottavaa on enemmän, ja tämä on yksi yleisimmistä haasteista. (Tillyard 2018.)

SANS:n tekemän vuoden 2019 SOC-katsauksen mukaan suurin haaste SOC:ssa on osaavan henkilöstön puute. Kaikista 272:sta kyselyyn vastanneesta 157:n mielestä tämä vaikuttaa eniten SOC:n kyvykkyyteen. Seuraavaksi suurimmat haasteet olivat automatisoinnin ja orkestroinnin puute sekä erilaisten keskenään integroimattomien työkalujen määrä. Tulokset olivat lähes samat kuin edeltävänä vuonna (ks. kuvio 4). (Crowley & Pescatore 2019, 19.)

Table 4. Challenges to Full Integration and Utilization of a Centralized SOC Service Model Year-over-Year

	2019		2018	
Lack of skilled staff	57.7%	157	61.9%	148
Lack of automation and orchestration	49.6%	135	52.7%	126
Too many tools that are not integrated	43.0%	117	47.7%	114
Lack of management support	37.1%	101	37.2%	89
Lack of processes or playbooks	36.8%	100	42.7%	102
Lack of enterprisewide visibility	36.0%	98	41.8%	100
Too many alerts that we can't look into (lack of correlation between alerts)	32.0%	87	33.9%	81
Silo mentality between security, IR and operations	30.2%	82	30.1%	72
Lack of context related to what we are seeing	25.4%	69	18.8%	45
High staffing requirements	25.0%	68	27.2%	65
Regulatory or legal requirements	9.2%	25	12.6%	30
Other	4.8%	13	8.8%	21
Answered		**272**		**239**

Kuvio 4. SOC:n suurimmat haasteet SANS:n tutkimuksessa 2019 (Crowley & Pescatore 2019, 19)

Osaavan henkilöstön puutteen perimmäisenä syynä on SOC analyytikoilta vaadittava laaja pohjatieto ja -osaaminen, jonka lisäksi tarvitaan analyyttistä ajattelutapaa (mt.). Pula tietoturva-asiantuntijoista on kasvava, ja International Information System Security Certification Consortiumin (ISC^2) vuoden 2018 tutkimuksen mukaan pula on lähes kolmesta miljoonasta kyberturvallisuuden ammattilaisesta maailmanlaajuisesti (Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens 2018). Tämän arvioidaan kasvavan 3,5 miljoonaan vuoteen 2021 mennessä (Morgan 2017).

Analyytikoiden apuna toimii aina tekniikka. Automatisoinnin ja orkestroinnin puute ja siihen sidoksissa olevien työkalujen integraatioiden ja pelikirjojen puute kertoo mm.

manuaalisen työn määrästä. Fideliksen Velocity360:lta vuonna 2018 tilaaman tutkimuksen mukaan tärkeimpiä automatisoinnin kohteita SOC:ssa olivat hälytysten luokittelu ja priorisointi, relevantin informaation ja datan kerääminen tutkittavaan tapahtumaan liittyviltä verkko- ja päätelaitteilta tai SIEMiltä, yleiset toistuvat tehtävät (tiketin luonti, raportointi jne.) ja muut tutkimustyöhön liittyvät logiikat. Automatisointi mahdollistaa paremman tehokkuuden ja vähentää uhkatoimijan havaitsemiseen kuluvaa aikaa johtaen parempaan SOC:n suorituskykyyn. Raportissa muita ilmi nousseita haasteita olivat myös päätelaitteiden ja verkkojen havaintojen integroiminen tutkintavaiheessa sekä vanhat ja tehottomat mittarit SOC:n toiminnan arvioinnissa. (Wang, Clark & Wilcox 2018, 6.)

2.4 Toiminnan mittarit

On tärkeää, että SOC kerää dataa poikkeaman hallinnan ja tiimin toiminnan tehokkuudesta ja suorituskyvystä. Tärkeimmistä tehokkuuden mittareista käytetään nimeä Key Performance Indicator (KPI). KPI on tapa mitata jonkin tavoitteen tai funktion onnistumista tai epäonnistumista, ja se tarjoaa tietoa, johon erilaiset päätökset nojautuvat. Laadukkaat KPI:t toimivat SOC:n jatkuvan kehittymisen edesauttajana ja ohjaajana, ja ne auttavat varmistamaan tietoturvahallinnan prosessien tehokkaan toimivuuden ja asianmukaisen käsittelyn. Tärkeitä huomioitavia asioita näitä mittareita valitessa on, että niiden tulisi olla helposti mitattavia, joko kvantitatiivisesti tai kvalitatiivisesti, niitä pystyy käyttämään toiminnan ja päätösten pohjana, ja että ne ovat oleellisia tehtävälleen. Lisäksi niiden tulisi ajan mittaan kyetä näyttämään muutoksia. (Moran 2018.)

SOC-tiimin toiminnan tehokkuuden mittaamisen pääaiheina käytetään yleensä analyytikoiden taitoja, havainnoinnin onnistumista, suurimpien riskien arviointia, poikkeamien mitigoimisen onnistumista, prosessien onnistumista ja työtaakan määrää. SOC voi käyttää KPI-mittareinaan esimerkiksi

- Käsiteltyjen poikkeamien määrä.
- Mean Time to Detection (MTTD), eli aika, joka SOC:lla kestää havaita poikkeama hälytysten joukosta.
- Mean Time to Resolution (MTTR), eli aika, joka SOC:lla kestää neutralisoida uhka.

- Poikkeamien määrä eri tyyppien mukaan, kuten webhyökkäykset, sähköposti jne.
- Rahallinen menetys per poikkeama. (The Modern Security Operations Center, SecOps and SIEM: How They Work Together n.d.; Moran 2018.)

Käsiteltyjen poikkeamien määrä mittaa, kuinka kiireinen valvottava ympäristö on ja paljonko toimia se SOC:lta vaatii. MTTD mittaa, kuinka tehokas SOC on prosessoimaan hälytyksiä ja havaitsemaan niiden seasta oikeat poikkeamat, ja MTTR mittaa, kuinka tehokas SOC on keräämään poikkeamiin liittyvää dataa, koordinoimaan toimenpiteitä ja tekemään niitä. (The Modern Security Operations Center, SecOps and SIEM: How They Work Together n.d.; Moran 2018.)

Hyödyllistä metriikkaa tiimin menestymisestä saadaan lisäksi tiimin jäseniltä kerätyillä itsearvioilla ja asiakasorganisaation tai palvelun omistajan tyytyväisyyden arviosta (Cichonski, Millar, Grance & Scarfone 2012, 40-41).

3 Poikkeaman hallinta

Tietoturvapoikkeaman hallinta käsittää toimenpiteet, joilla poikkeamiin varaudutaan ja reagoidaan minimoiden vahingot ja toipuen normaalitilaan mahdollisimman tehokkaasti (Kyberturvallisuuden sanasto 2018).

3.1 Tapahtuma ja poikkeama

3.1.1 Tapahtuma

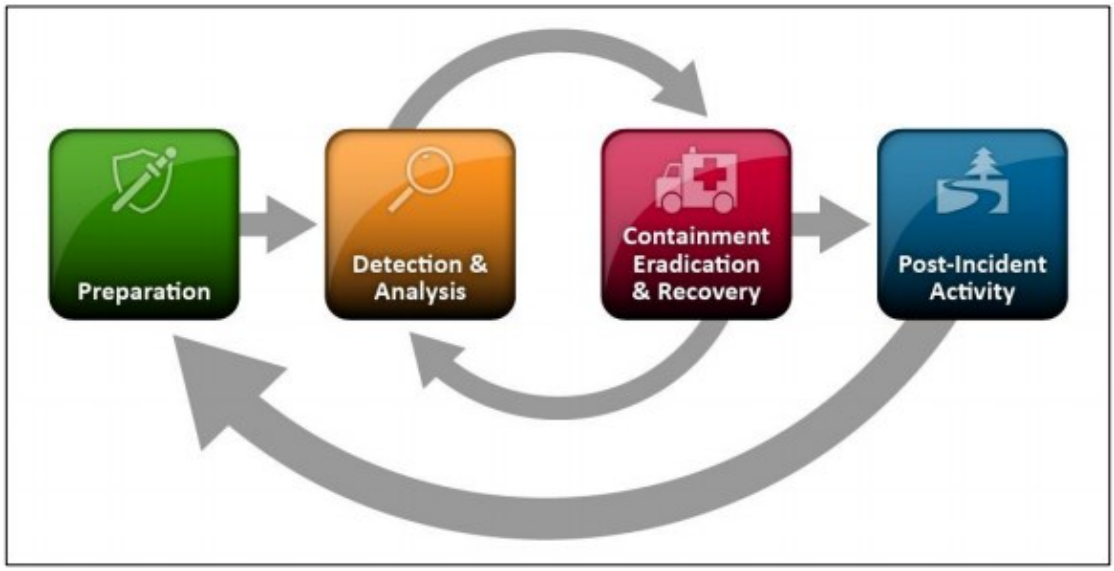
Tapahtuma (engl. event) on mikä tahansa havaittavissa oleva tapahtuma järjestelmässä tai verkossa. Tapahtuma on esim. käyttäjän yhteydenotto tiedostojakoon, palvelimen vastaanottama pyyntö verkkosivusta, käyttäjän sähköpostin lähettäminen tai palomuurin estämä yhteys. Tapahtumat ovat raakaa dataa, joita työkalut kuten SIEM-järjestelmä analysoi sääntöjensä avulla. (Cichonski, Millar, Grance & Scarfone 2012, 6; Zimmerman 2014, 10-11.)

3.1.2 Poikkeama

Tietoturvapoikkeama (engl. security incident) on tietoturvapolitiikan tai hyväksyttyjen käytänteiden loukkaus tai sen välitön uhka, joka mahdollisesti vaarantaa tietojärjestelmän luotettavuuden, saatavuuden tai eheyden. Poikkeamia ovat esim. palvelimen kaatava palvelunestohyökkäys, käyttäjän tietokoneen saastuminen sähköpostin liitteestä avatulla haittaohjelmalla tai käyttäjän tekemä arkaluotoisen materiaalin tietovuoto tiedostonjakopalveluun. Yksi tapahtuma voi muodostaa poikkeaman, mutta monesti poikkeamaan liittyy monta tapahtumaa. (Cichonski ym. 2012, 6; Zimmerman 2014, 10-11.)

3.2 Käsittelyn vaiheet

Poikkeamien käsittely voidaan jakaa vaiheisiin, jossa käydään läpi poikkeaman hallinnan elinkaari. National Institute of Standards and Technologyn (NIST) mallin mukaan nämä päävaiheet ovat valmistautuminen, havainnointi ja analyysi, hallinta, hävittäminen ja palautuminen ja poikkeaman jälkeiset toimenpiteet (ks. kuvio 5). Hallinta-, hävittämis- ja palautumisvaiheen toimet kiertävät monesti takaisin havainnointiin ja analyysiin esimerkiksi tilanteessa, jossa selvitetään, onko haittaohjelma levinnyt muihin tietokoneisiin hävittämisprosessin aikana. Lopuksi poikkeaman jälkeisten toimenpiteiden, kuten poikkeamasta tehdyn raportin, tulisi heijastua valmisteluvaiheeseen, jotta vastaavilta poikkeamilta vältyttäisiin. (Cichonski ym. 2012, 21.)



Kuvio 5. Poikkeaman hallinnan elinkaari (Cichonski, Millar, Grance & Scarfone 2012, 21)

3.2.1 Valmistautuminen

Ensimmäinen vaihe käsittää valmistautumisen poikkeaman hallintaan, johon kuuluu sen tekemisen kyvykkyyden lisäksi poikkeamien estäminen varmistamalla, että verkot, järjestelmät ja sovellukset ovat tarpeeksi hyvin suojattu. Resurssit ja työkalut, jotka on syytä ottaa huomioon poikkeaman hallintaan valmistautumisessa ovat mm. käytettävät kommunikointimekanismit ja käytettävät tilat, tarvittavat laitteistot ja ohjelmistot, ja analyysiin tarvittavat dokumentaatiot, kuten esim. verkkokuvat. (Mts. 21-23.)

Mitä vähemmän poikkeamia on, sen parempi. Riittämättömät tietoturvakontrollit kasvattavat poikkeamien lukumäärää, joka voi olla liikaa hallintaa suorittavalle tiimille. Tällöin on todennäköisempää, että poikkeamiin vastataan vajavaisesti tai liian hitaasti, joka taas vaikuttaa negatiivisesti organisaation liiketoimintaan. (Mts. 23.)

3.2.2 Havainnointi ja analyysi

Poikkeamat voivat ilmentyä lukemattoman monella eri tavalla, ja ne vaativat erilaisia strategioita niihin vastaamiseen. Vaikka yleisesti ottaen mitkä tahansa poikkeamat tulisi pystyä käsittelemään, organisaatioiden tulisi keskittyä erityisesti yleisimpiin

hyökkäysvektoreihin. Myös riskienhallinta on tärkeässä osassa, jotta SOC voi havaita juuri kyseisen valvottavan organisaation keskeisimmät riskit. Erilaisia hyökkäysvektoreita ovat esim. irrotettava ulkoinen media, sähköposti, websivut ja -sovellukset, palvelunestohyökkäykset ja organisaation käytänteiden rikkomukset. (Mts. 25.)

Mahdollisten poikkeamien tarkka havaitseminen ja arvioiminen on monesti haastavin vaihe prosessissa. Poikkeamat voidaan havaita usealla eri tavalla, eikä tieto havainnosta ole aina yksityiskohtainen tai täsmällinen. Osaa poikkeamista on jopa lähes mahdotonta havaita, toisten ollessa helposti havaittavia selkeistä merkeistä. Mahdollisen poikkeaman havainnointia hankaloittaa myös vastaanotettujen hälytysten tyypillisesti suuri määrä. Tässä vaiheessa korostuu myös henkilöstöltä vaadittava syvä tekninen osaaminen ja kokemus. (Mts. 26.)

Merkit poikkeamasta voivat olla ennakoivia tai suoria indikaattoreita, että poikkeama on tapahtunut tai tapahtumassa. Jos ennakkomerkkejä poikkeamasta havaitaan, tulisi mahdollinen kohde ottaa vähintäänkin tarkempaan valvontaan. Koska nämä merkit eivät ole takuuvarmasti tarkkoja, on ihmisen tekemä analyysi oltava prosessissa mukana. Poikkeaman hallintaa suorittavan tiimin tulisi nopeasti analysoida ja tarkistaa kunkin poikkeaman paikkansapitävyys seuraten ennalta määritettyä prosessia ja dokumentoida kaikki siihen kuuluvat vaiheet. Analyysin alkuvaiheessa olisi tärkeää saada pikaisesti selville poikkeaman laajuus ja mihin se vaikuttaa, mistä poikkeama on peräisin ja miten poikkeama tapahtuu (mm. millä työkaluilla tai hyökkäysmenetelmillä). Koska poikkeamia ei pidä käsitellä sillä periaatteella, että mikä on havaittu ensin, myös käsitellään ensin, on priorisointi tehtävä perustuen poikkeaman vaikutuksiin organisaation toiminnallisuuteen, tietoon ja palautumiseen tarvittaviin resursseihin. Näillä tiedoilla tiimi voi paremmin priorisoida poikkeaman käsittelyn seuraavia toimenpiteitä. Priorisoinnin lisäksi organisaatioilla tulisi olla myös prosessi, jossa määritellään poikkeaman eskalointi ylemmälle tasolle käsiteltäväksi. (Mts. 27-29, 32-33.)

Kaikki vaiheet heti poikkeaman havaitsemisesta aina sen lopulliseen ratkaisuun saakka tulisi dokumentoida selkeästi aikaleimoineen. Esimerkiksi lokikirjan pitäminen

havaittujen tapahtumien ja tiedoston muutosten dokumentointiin johtaa tehokkaampaan ja systemaattisempaan käsittelyprosessiin. Kaikki poikkeamaan liittyvä tieto tulisi säilyttää ja pääsy siihen rajoittaa, sillä tietoa voi mahdollisesti käyttää mm. todistusaineistona oikeudessa. (Mts. 30-31.)

Poikkeaman hallintaa tekevän tiimin täytyy tiedottaa asiaankuuluvia sidosryhmiä ja henkilöitä poikkeamasta. Poikkeaman hallintapolitiikassa tulisi olla määritelty vähintään kenelle täytyy ilmoittaa ja milloin. Tiedottamiseen käytettävät kommunikointiyhteydet tulisi olla määritelty ja suunniteltu siten, että tieto saadaan perille. (Mts. 33-34.)

3.2.3 Hallinta, hävittäminen ja palautuminen

Hallinta- ja rajaustoimenpiteisiin poikkeamalle voi kuulua esimerkiksi järjestelmän sammuttaminen, verkosta irrottaminen tai joidenkin toimintojen poistaminen käytöstä. Strategiat poikkeamien hallintaan ja rajaamiseen vaihtelevat kuitenkin poikkeaman tyypin mukaan ja siksi organisaatiolla pitäisi olla määritelty strategiat merkittäville poikkeamatyypille. Strategian suunnittelussa tulisi huomioida palvelun saatavuus, mahdolliset vahingot, tarve todistusaineiston säilymiseen, implementoimiseen tarvittava aika ja resurssit, sekä korjaavan ratkaisun väliaikaisuus. Joissain tapauksissa hyökkäyksen rajaaminen voi aiheuttaa lisävahinkoa, kuten esimerkiksi tilanteessa, jossa haittaohjelma ottaa yhteyttä toiseen palvelimeen tasaisin väliajoin ja yhteyden katkettua käynnistää prosessin, joka salaa kaiken datan käyttäjän kovalevyltä. (Mts. 35-36.)

Kun poikkeama on hallinnassa, siihen kuuluvien osien hävittäminen voi olla tarpeen. Tämä tarkoittaa esim. haittaohjelman poistamista tai murrettujen käyttäjätunnusten poistamista käytöstä. Joissakin poikkeamatilanteissa haitallisten osien hävittäminen tapahtuu palautumisen ohessa. Poikkeamasta palautuminen käsittää järjestelmien ja toiminnan palauttamisen normaalitilaan ja haavoittuvuuksien korjaamisen vastaavien poikkeamien tapahtumisen estämiseksi, jonka lisäksi yleensä järjestelmien ja verkon valvonnan tasoa myös korotetaan. Muita toimenpiteitä voivat myös olla esim.

salasanojen vaihtaminen, päivitysten ajaminen tai palomuurisääntöjen tiukentaminen. Poikkeamasta palautuminen voi kestää kauan, laajemmissa poikkeamatilanteissa kuukausia. (Mts. 37.)

3.2.4 Poikkeaman jälkeiset toimenpiteet

Viimeiseen, muttei vähäisimpään vaiheeseen kuuluu kokemusten ja opittujen asioiden läpikäynti ja hyödyntäminen. Suuremman poikkeaman jälkeen olisi aina hyvä pitää ”mitä opittiin”-tapaaminen, jossa käydään läpi mitä tapahtui, kuinka hyvin henkilöstö pärjäsi, mikä meni hyvin ja mitä olisi voinut tehdä eri tavalla, ja miten vastaavat poikkeamat estetään tai havaitaan jatkossa. Asioiden reflektointi tapaamisessa auttaa poikkeaman hallintatiimiä ja muita osallisia kehittymään, jonka lisäksi myös poikkeaman hallintapolitiikkaa ja käytänteitä saadaan päivitettyä entistä paremmiksi. Osana tätä vaihetta on myös loppuraportin kirjoittaminen kustakin poikkeamasta, joka voi olla hyödyksi samankaltaisia poikkeamia käsitellessä. (Mts. 38-39.)

4 Security Orchestration, Automation and Response

4.1 Yleistä

Security Orchestration, Automation and Response (SOAR) on kokoelma erillisiä teknologioita, joka mahdollistaa datan ja tietoturvahälytysten keräämisen eri lähteistä yhteen paikkaan. Organisaatioilla on implementoitu monia eri tietoturvateknologioita, joiden datan integroiminen keskenään vaatii aikaa ja resursseja niiden generoimien hälytysten määrän kasvaessa liian suureksi valvovalle SOC-tiimille. (Why Gartner’s SOAR Model is the Future of IT Security 2018.) SIEM-järjestelmästä SOAR eroaa siinä, että SOAR kerää hälytykset eri tietoturvateknologioista ja kykenee vastaamaan niihin automatisointipelikirjojen avulla. SIEM-ratkaisut vain nostavat hälytyksen, mutta SOAR mahdollistaa myös niihin reagoimisen. (Tillyard 2019.)

SOAR mahdollistaa tehokkaamman työnkulun soveltamalla koneen älykkyyttä poikkeamien havaitsemisen ja niihin vastaamisen virtaviivaistamiseksi ja automatisoimiseksi (SOAR - Security Orchestration, Automation and Response n.d.). Se tehostaa analyytikoiden työtä ja keventää manuaalisen työn määrää yhdistämällä kolme aiemmin erillistä osa-aluetta: orkestroinnin ja automaation, uhkatiedon ja poikkeaman hallinnan. (Imam 2019.)

SOAR-termin on keksinyt kansainvälinen tutkimus- ja konsultointiyritys Gartner vuonna 2015, jonka jälkeen SOAR-markkinat ovat lähteneet kasvuun. Viimeisen kolmen vuoden aikana SOAR-toimittajien määrä on kasvanut yrityskauppojen myötä, ja Gartner ennustaa, että vuoden 2022 loppuun mennessä 30% organisaatioista, joilla on tietoturvatiimissä enemmän kuin viisi henkilöä, hyödyntävät SOAR-työkaluja tietoturvahallinnassaan. Tänä päivänä osuus on alle 5%. (Neiva, Lawson, Bussa & Sadowski 2019.)

4.2 Orchestration

Orkestroinnilla tarkoitetaan erillisten tietoturvateknologioiden ja -työkalujen integroimista ja yhdistämistä, jotta ne yhdessä parantavat poikkeaman hallinnan prosessien työnkulkua. Automatisointi on osa orkestrointia, joten orkestrointi myös käsittää toistuvien aikaa vievien ja manuaalisten tehtävien helpottamisen koneen avustamalla päätöksenteolla ja korjaustoimenpiteillä loppukäyttäjän kuitenkin valvoen ja toimien mukana. Orkestrointi on siis järjestelmien ja palveluiden automatisoitua koordinointia yhdistäen ihmiset, prosessit ja teknologian. (Security Orchestration and Automation n.d.)

Esimerkiksi, jos SOC-tiimi saa käsittelyyn haitallisen sähköpostiviestin, analyytikot tarkistavat lähettäjän maineen uhkatiedoista ja viestin lähteen Domain Name System (DNS) -työkalulla. Viestin sisältämien Uniform Resource Locator (URL) -osoitteiden maineet ja puhtaus tarkistetaan työkalulla, kuten VirusTotalilla, ja mahdolliset liitetiedostot ajetaan sandbox-työkalussa. Tässä tapauksessa orkestroinnilla voidaan automatisoida datan keruu SOARissa integroimalla uhkatietotyökalut järjestelmään, jotta analyytikon ei tarvitse erikseen käsin ajaa tarkastuksia kussakin eri työkalussa.

Orkestroinnilla voidaan automatisoida esim. IP-osoitteiden tietojen hakua, Indicators of compromise (IOC) -tietojen rikastamista ja poikkeamien vakavuustason määrittämistä. (Imam 2019.)

4.3 Automation

Automatisointi SOARissa tarkoittaa tietoturvahallintaan liittyvien tehtävien automaattista käsittelyä. Se on prosessi tehtävien, kuten haavoittuvuusskannausten tai hälytysten eskaloimisen, suorittamiseen ilman ihmisen väliintuloa. (What is Security Automation? 2017.) Automatisoimalla tehtäviä, poikkeaman hallintaa suorittava SOC-tiimi voi standardisoida työnkulun eri vaiheita, päätöksentekoa, toimenpiteitä ja tilan seuraamista. Automatisoinnin tehokkuuden takaamiseksi automatisoitavien tehtävien ja prosessien tulisi kuitenkin olla hyvin määritelty. (Imam 2019.)

Automatisointi nojaa pelikirjoihin, jotka sisältävät suoritettavat vaiheet. Niillä voidaan toteuttaa automatisointia sekä reaktiivisesti että proaktiivisesti. Reaktiivisesti automaatiopelikirja voi suorittaa poikkeaman hallinnan tehtäviä, kerätä metriikoita tai tehdä poikkeamille tilanteen (engl. case) hallintaa. Proaktiivisesti taas pelikirjoilla voi hoitaa uhkien metsästämistä (engl. threat hunting) ja muita poikkeamia ennaltaehkäiseviä tietoturvahallintatoimia. (Mt.)

4.4 Response

Poikkeamiin vastaamiseen liittyvät teknologiat auttavat analyytikoita hallitsemaan, koordinoimaan ja seuraamaan tietoturvapoikkeamia ja niihin reagointia. Näihin toimiin kuuluvat mm. tiketin luominen tai suoremmat vastetoimenpiteet, kuten IP-osoitteen estäminen palomuurisäännöllä. SOARin poikkeaman hallinta -toiminnallisuus auttaa analyytikoita hälytysten luokittelussa ja prosessoinnissa sekä tapausten hallinnassa mahdollistaen SOC-tiimille tukea yhteistyöhön kommunikoimalla, jakamalla tietoa ja hallitsemalla eri työtehtäviä järjestelmän sisällä. Tapausten hallintaan, jonka eri vaiheita järjestelmä virtaviivaistaa, kuuluvat poikkeamiin liittyvän tiedon kerääminen, sen jakaminen ja analysointi. Lisäksi osa SOARin ominaisuuksia on kerätä

mahdollisiin uhkiin liittyvät uhkatiedot ja tarjota se SOC-tiimin käytettäväksi, jonka perusteella tiimi voi tehdä ennakoivia toimenpiteitä. (Imam 2019; Neiva ym. 2019.)

SOAR-työkalut mahdollistavat myös raporttien ja kojelautanäkymien generoimisen eri sidosryhmille. Raportit ja näkymät voivat olla esim. teknisempiä analyytikkotason raportteja tai ylemmälle johtotasolle sopivampia, kokonaiskuvaa esittäviä raportteja, joista käy ilmi SOC:n suorituskyvyn mittareita ja mahdollisia pullonkauloja toiminnassa. (Incident Response Automation and Security Orchestration with SOAR n.d.)

5 Ongelman määrittely

Opinnäytetyön kehittämistehtävän tarkoituksena oli selvittää, kuinka SOAR-alusta otetaan tehokkaasti käyttöön sekä havainnoida, kuinka se vaikuttaa SOC-tiimin suorituskykyyn erilaisia suorituskykymittareita käyttäen. Työssä tavoitteena oli integroida tiimin käytössä jo olevat tietoturvateknologiat SOARiin, kuvata poikkeamien käsittelyä SOAR-alustan ominaisuuksia hyödyntäen ja tutkia vaikutuksia, kuten kuinka paljon sillä pystyy nopeuttamaan tiimin toimintaa orkestroimalla eli integroimalla työkalut samaan alustaan ja automatisoimalla poikkeamien käsittelyä sekä muita manuaalisia tehtäviä. SOC-tiimi tavoittelee nopeaa reagointiaikaa ja virtaviivaisempaa hälytysten sekä poikkeamien käsittelyä.

Työssä käydään läpi SOAR-järjestelmään konfiguroitavat vaiheet ja SOC-valvontaan kuuluvien toimenpiteiden tekeminen SOARin avulla. Aluksi käydään läpi järjestelmän käyttäjien hallinnointi ja integraatioyhteyksien tekeminen muiden ulkoisten järjestelmien ja SOARin välillä sekä niistä saatavien hälytysten siirtäminen SOARin tietueiksi. Integraatioyhteyksien jälkeen suoritetaan hälytysten ja poikkeamien käsittelyä SOARissa sekä havainnoidaan sen nopeutta ja tehokkuutta. Lopuksi työkalu otetaan tiimin analyytikoiden testikäyttöön ja tarkastellaan käytön jälkeistä palautetta.

Opinnäytetyön tuotosta voidaan hyödyntää esittämään SOAR-alustan mahdollistamat hyödyt SOC-tiimin käytössä ja osoittamaan se suorituskykymittareilla. Alustan

käyttöön ja ylläpitoon liittyvän osaamisen kehittyminen hyödynnetään kouluttamalla se muille SOC-tiimin jäsenille.

6 Käyttöönotto

Toteutusvaiheen alussa käsitellään käyttäjien hallintaan liittyviä konfiguraatioita ja SOARin tiimirakenteita. Tämän jälkeen läpikäydään vaiheet integraatioyhteyksien tekemiseen ja hälytysten rikastamiseen pelikirjoineen. Lopuksi suoritetaan hälytysten ja poikkeamien käsittelyä SOARista sekä tarkastellaan alustan vaikutuksia valvontatyöhön mittareiden kautta.

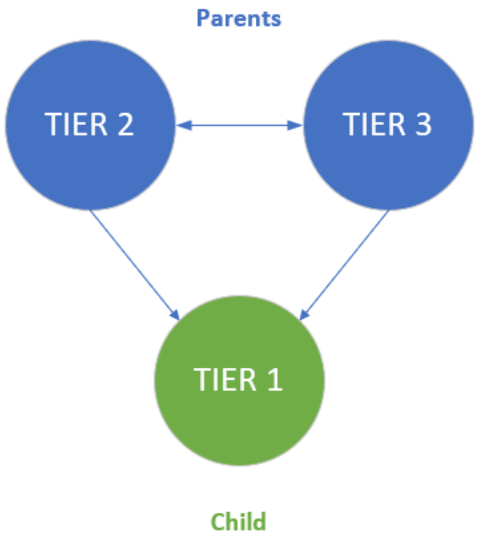
6.1 Käyttäjät

6.1.1 Tiimirakenne

Alkuvaiheessa SOAR-alustaa tulee käyttämään SOC-tiimistä tasot 1 ja 2, eli tier 2 ja tier 3. Käyttäjänhallinta rakennetaan keskitetysti Active Directorylla (AD) tai vastaavalla käyttäjänhallintajärjestelmällä käyttäen autentikointiin Lightweight Directory Access Protocollaa (LDAP) sitoen siihen myös kaksivaiheisen tunnistautumisen (engl. two-factor authentication (2FA)). AD:ssa käyttäjien pääsy sallitaan käyttäjäryhmillä, jolloin vain oikeutetut käyttäjät pääsevät kirjautumaan CSOC-palveluihin kuten SOARiin. Käyttäjät täytyy myös erikseen tuoda käyttäjänhallinnasta SOARiin, joten sinne pääsevät vain käyttäjät, jotka ovat molemmista päistä sallittu.

SOARissa voi luoda omia tiimejä ja muokata niiden suhteita toisiinsa tiimihierarkian hallinnassa. Tiimit edustavat ryhmiä ”omistajista”, ja tiimiin kuuluvat voivat käsitellä oman tiiminsä omistamia tietueita määritettyjen käyttäjälle määritettyjen roolien mukaan. SOARiin ei saanut tuotua tiimirakenteita suoraan käyttäjähallinnasta, joten ne lisättiin järjestelmään erikseen. Oletuksena järjestelmässä olevan ”SOC Team” -tiimin lisäksi luotiin tiimit Tier 1, Tier 2 ja Tier 3. Vaikka alkuvaiheessa järjestelmää käyttää ainoastaan Tier 2, luotiin tiimit muille SOC:n tasoille jo valmiiksi.

SOAR-alustan pääasialliset käyttäjät kuuluvat Tier 2 -tiimiin, joten muiden tiimien suhteet rakennettiin sen ympärille. Tier 2 on sisarussuhteessa Tier 3:n kanssa, mikä tarkoittaa, että ne näkevät toistensa tietueet ja voivat käsitellä niitä. Jos poikkeama eskaloidaan Tier 3:lle, on olennaista, että siihen kuuluvat henkilöt pääsevät käsittelemään tietueita. Tier 1 on lapsisuhteessa Tier 2:een ja Tier 3:een nähden, eli nämä tiimit ovat sen vanhempia. Tier 1:een kuuluvat eivät näe tai voi käsitellä Tier 2 ja Tier 3 -tiimin tietueita, mutta Tier 2 ja 3 voivat käsitellä Tier 1:n omistamia tietueita. Koska Tier 1 suorittaa jatkuvaa hälytysten läpi käymistä luokitellen ja priorisoiden, ei heidän tarvitse eskaloinnin jälkeen nähdä eskaloituja hälytyksiä. Luotujen tiimien Tier 1, 2 ja 3 välinen suhde on esitetty kuviossa 6.



Kuvio 6. Tietuiden omistussuhteiden tiimihierarkia

6.1.2 Käyttöoikeudet

SOARissa käyttöoikeudet määritetään roolien avulla eli Role Based Access Control (RBAC) -mallin mukaan. Rooleja voi itse luoda mukana tulevien oletusroolien lisäksi, ja niille voi määrittää käyttöoikeudet kuhunkin SOARin moduuliin Create, Read, Update ja Delete (CRUD) -periaatteella. Käyttöoikeuksien määrittämisessä päätettiin noudattaa least privilege -periaatetta eli käyttäjille annetaan vain ne oikeudet, joita

he tarvitsevat analysointityönsä tekemiseen. SOARin ylläpito- ja hallintatoimista vastaa Tier 2, joten tarvittaessa heillä on pääsy järjestelmän lokaalille järjestelmänvalvoja-tunnukselle, jolla merkittävät muutokset tehdään. Admin-tunnuksella tehdyt toimet voidaan kohdentaa kuhunkin käyttäjään auditlokin, ja sieltä näkyvän IP-osoitteen perusteella.

SOARiin luotiin kaksi uutta roolia: T1 Analyst ja T2 Analyst kuvaamaan Tier 1 ja 2-käyttäjien tarpeisiin sopivia käyttöoikeuksia. T1 Analyst -roolille määritettiin luku-, luonti- ja päivitysoikeudet vain tarvittaviin moduuleihin, mm. alerts, incidents ja indicators moduuleihin. Tärkeintä on, että Tier 1 pystyy tekemään hälytysten nopeaa käsittelyä ja eskaloimaan lisätutkintaa vaativat hälytykset Tier 2:lle. Koska Tier 2 -analyytikot ovat järjestelmän pääasialliset käyttäjät, määritettiin T2 Analyst -roolille vähintään lukuoikeus kaikkiin moduuleihin ja laajemmin muokkausoikeuksia kuin T1-analyytikolla. T2 Analyst -roolilla on esimerkiksi muokkausoikeudet playbook-moduuliin pelikirjojen käsittelyä varten. Tier 1:lle riittää, että he voivat suorittaa pelikirjoja. Yksittäisille pelikirjoille voi myös määrittää suoritusoikeudet vain tietyille tiimeille, joten vaikuttavimpien pelikirjojen suorittamisen rajoittaminen pystyttiin eväämään esim. Tier 1:ltä.

6.2 Integraatiot

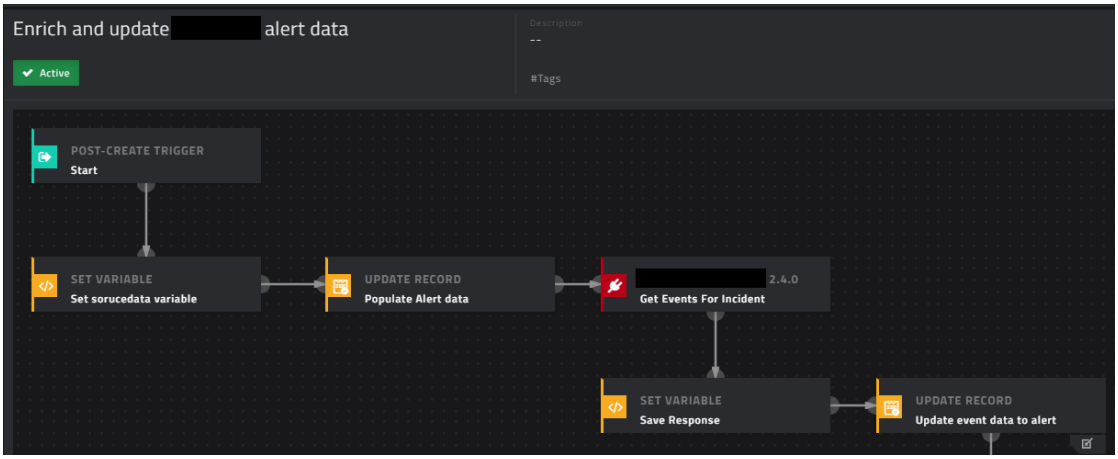
Tässä luvussa käydään läpi SIEM-järjestelmän, ATD-palvelun sekä verkkopalveluiden, kuten VirusTotalin integraatioihin tehdyt toimenpiteet ja konfiguraatiot.

SOARin ja SOC-tiimin käyttämien työkalujen väliset integraatioyhteydet toteutetaan pääasiassa suojattuna Hypertext Transfer Protocol Secure (HTTPS) -protokollan yli, jota suurin osa SOARin liitosohjelmistoista (engl. connector) käyttävät. Tarvittaessa integraatioita varten luotaville palvelukäyttäjille (engl. service user) annetaan vain ne käyttöoikeudet, joita ne tarvitsevat. Application Programming Interface (API) -rajapintaa käyttäviä integraatioita varten SOARiin voi myös luoda appliance-käyttäjiä, jotka käyttävät API-avainpareja.

6.2.1 SIEM

Integraatio SIEM-järjestelmään haluttiin olevan kaksisuuntainen. SIEM lähettää SOARille nostamansa hälytykset (SIEMissä poikkeamat) ja hakee SOARista muutokset SIEMille, kun hälytys on käsitelty ja selvitetty. Tällaista integraatioyhteyttä varten tuotetoimittaja oli kehittänyt SIEMille asennettavan sovelluksen, joka suorittaa sekä datan lähettämisen, että sen hakemisen SOARilta. Applikaatio asennettiin SIEMille, avattiin palomuurilta HTTPS-yhteys SOARin ja SIEMin välille, luotiin integraatioasetukset ja määritettiin ne osoittamaan SOARiin käyttäen integraatioyhteyttä varten SOARiin luotua käyttäjää. Koska käytössä oleva SIEM oli MSSP-versio, ohjattiin myös SIEMin integraatioasetuksissa kunkin organisaation hälytykset SOARissa luotuihin, organisaatioita vastaaviin Tenants-moduulin tietueisiin lisäämällä kunkin tietueen API-polku. Tenants-moduuliin on lisätty jokainen asiakasorganisaatio omana tietueenaan. SIEM saatiin määritettyä lähettämään uudet hälytykset automaattisesti SOARille luomalla uusi notifikaatiomääritys.

Kun uudet hälytykset saapuivat SOARiin, niiden data oli lähes kokonaan hälytyksen Source data -kentässä JSON-formaatissa. SOARissa tietojen ”mappaaminen” tehtiin luomalla kuvion 7 mukainen pelikirja.

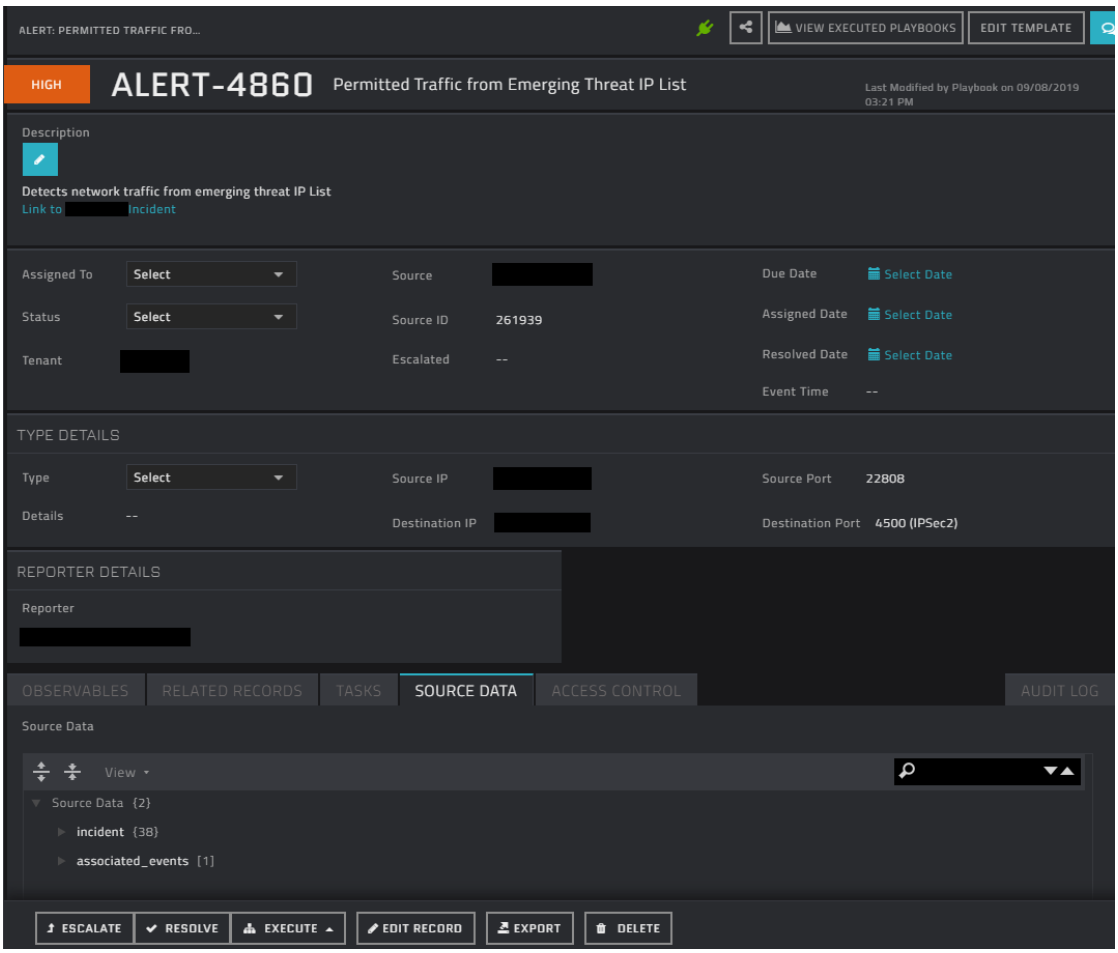


Kuvio 7. Pelikirja SIEMin hälytysten rikastamiseen

Laukaisijaksi pelikirjalle asetettiin post-create trigger, jolla määritettiin pelikirja ajettavaksi aina, kun järjestelmään luotiin uusi hälytys, jonka lähteenä on SIEM. Suorituksen ehtona käytettiin siis hälytyksen Source-kentän arvon tarkastamista. Set variable -vaiheessa määritetään pelikirjan sisäisiä muuttujia ja mm. tallennetaan saapuneen hälytyksen Source Data -kentän sisältö muuttujaan. Sen jälkeen päivitetään hälytyksen kenttiin sen sisältämän JSON-datan sisältämiä tietoja, kuten lähde- ja kohde IP-osoite, portit, raportoiva laite ja vakavuustaso (low-high) Update record -vaiheessa.

Hälytykseen liittyvät SIEM-tapahtumat eli lokidata saatiin haetttua asentamalla tuotetoimittajan kehittämä SIEM-liitosohjelmisto, jossa on funktio tapahtumien hakemiseen SIEMin poikkeaman ID:n perusteella. Tämä liitosohjelmiston funktio lisättiin vaiheeksi pelikirjaan ja määritettiin se hakemaan SIEMin poikkeamaan liittyvät tapahtumat parametreinään muuttujilla määritetty organisaatiokohtainen konfiguraatio ja poikkeaman ID. SOAR käyttää pelikirjoissaan Jinja-mallia, joka on Pythonille kehitetty mallinnuskieli. Esim. {{vars.tenant_config}} viittaa pelikirjan sisällä määritetyn ”tenant_config”-muuttujan sisältöön.

Liitosohjelmiston funktion palauttama vastaus on JSON-rakenne hälytykseen liittyvistä tapahtumista ja se tallennetaan muuttujaan ja lopuksi päivitetään tietueeseen mahdollisista tapahtumista löytyvät lisätiedot. Tämän pelikirjan suoritettua SIEMin lähettämästä raa’asta JSONista on parsittu informatiiviset tiedot hälytyksen kenttiin ja SIEMin poikkeaman sekä tapahtumien raakadata on yhdistetty ja tallennettu Source data -kenttään. Esimerkki pelikirjan rikastamasta hälytyksestä on esitetty kuviossa 8.



Kuvio 8. Pelikirjan käsittelemä hälytys SIEMistä. Raa'asta datasta on parsittu tiedot hälytys-tietueen datakenttiin.

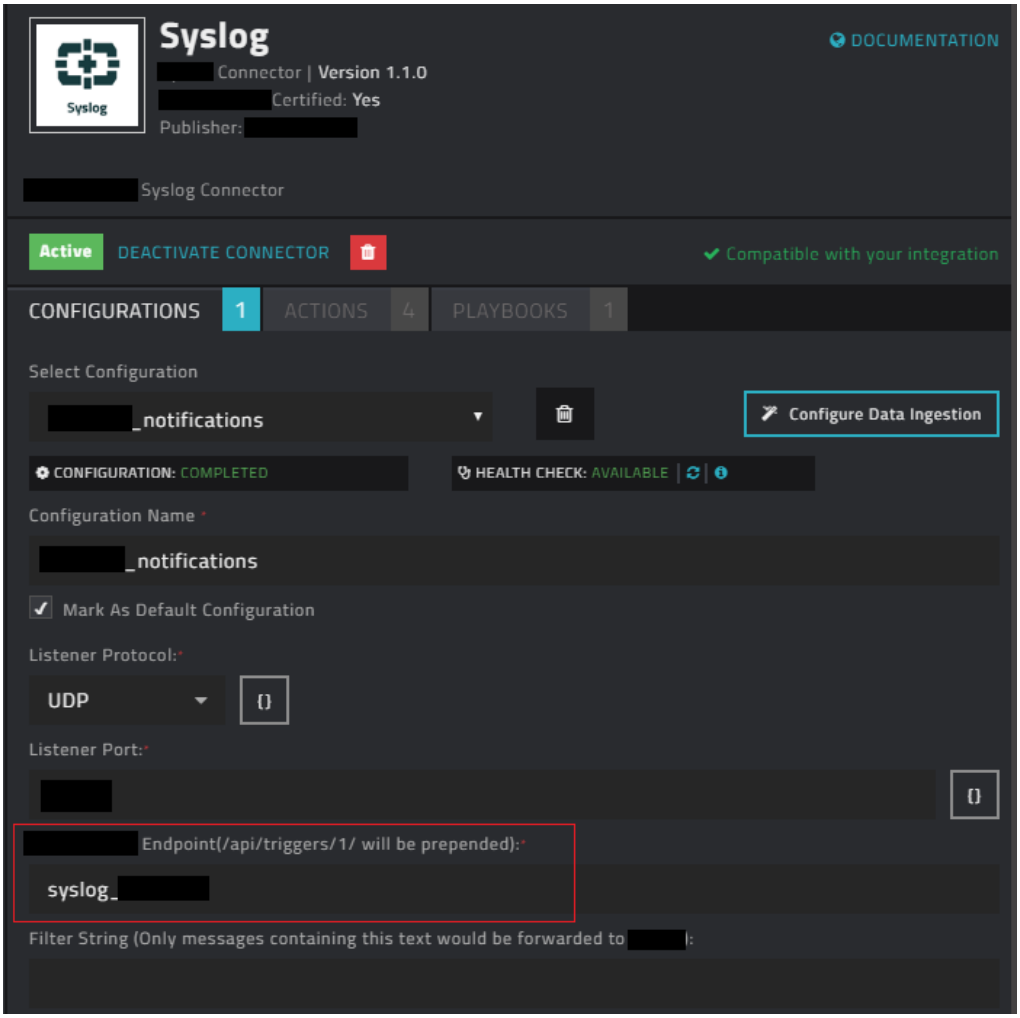
6.2.2 ATD-palvelu

Advanced Threat Detection (ATD) -palvelussa on SIEMin tavoin syöte havaituista tapahtumista valvottavassa verkossa, jotka haluttiin saada SOARiin hälytyksiksi. Tuotetoimittajalta löytyi liitosohjelmisto tuotteelle, mutta sillä pystyi ainoastaan lähettämään tiedostoja ja verkko-osoitteita ATD:n sandboxiin ja hakemaan sen analyysiraportin. Hälytysten suhteen integraatio päätettiin toteuttaa käyttämällä syslogia, johon SOARista löytyi liitosohjelmisto.

ATD-palveluun luotiin notifikaatioasetus, joka lähettää havaitut tapahtumat syslogilla SOARiin. Notifikaatioasetuksessa määritettiin ATD-palvelu lähettämään syslog UDP-protokollaa käyttäen SOARiin. Portin täytyi olla suurempi kuin 1024, koska SOARissa

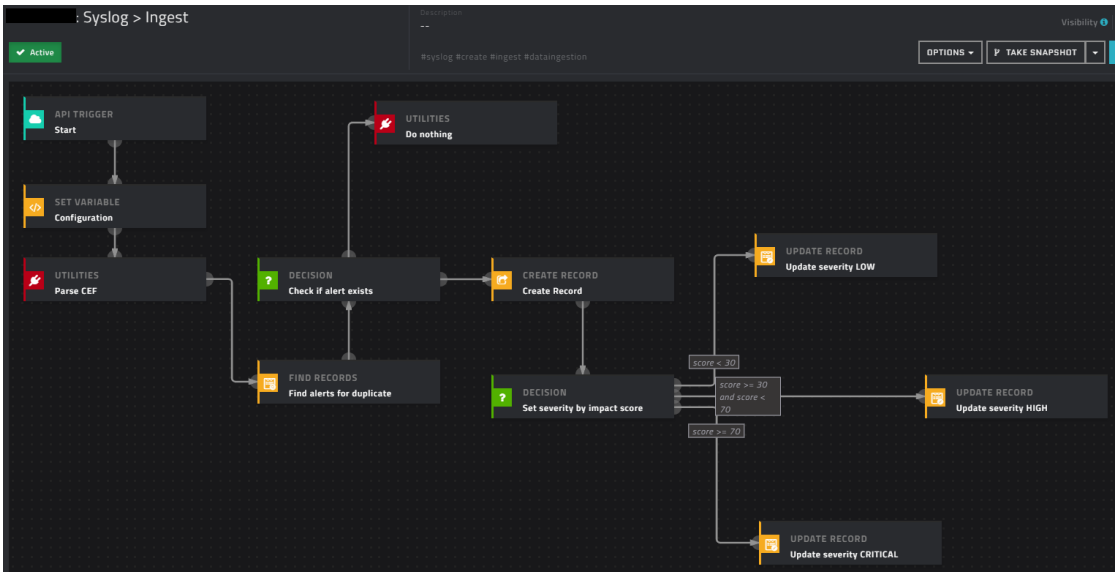
syslog-kuuntelija käynnistetään ei-root käyttäjänä. Lokiformaatiksi määritettiin Common Event Format (CEF), koska SOAR ei tukenut Log Event Extended Format (LEEF) -formaattia, joka olisi mahdollistanut myös mahdollisten pakettikaappausten lähetyksen lokin mukana.

Kun integraatioasetus ATD-palveluun oli luotu ja tarvittavat palomuuriavaukset tehty, asennettiin SOARiin syslog-liitosohjelmisto ja luotiin sille konfiguraatio ATD-palvelua varten. Liitosohjelmiston konfiguraatiossa määritettiin SOAR kuuntelemaan käytettyä UDP-porttia ja määritettiin polku API:in, jota käytetään pelikirjassa API-laukaisijana. Tällä voidaan identifioida eri syslog-integraatiot ja ajaa haluttu pelikirja juuri tietylle konfiguraatiolle. ATD-palvelun integraation laukaisijan päätepisteeksi annettiin yksilöllinen nimi (ks. kuvio 9).



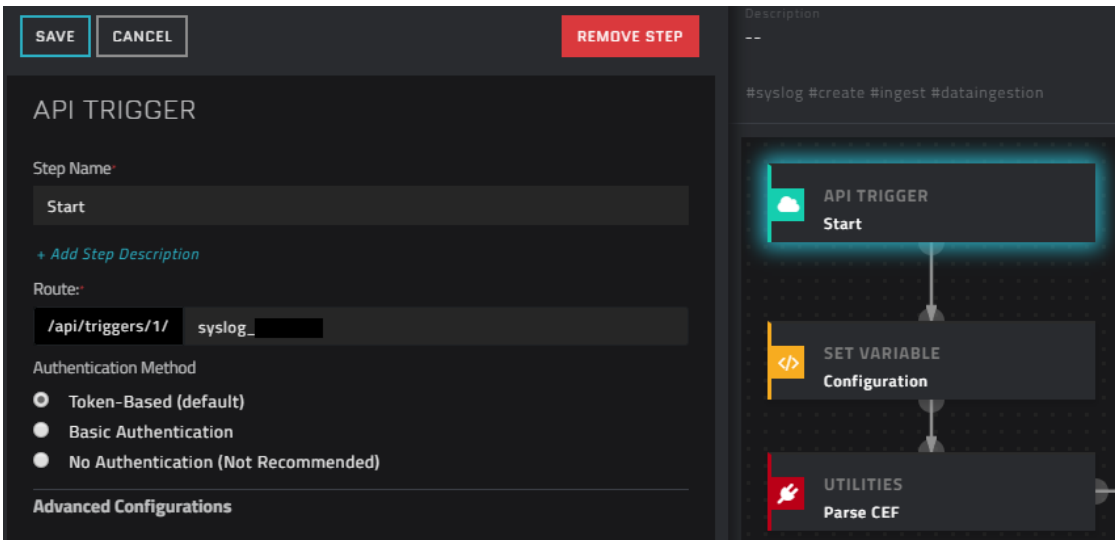
Kuvio 9. Syslog-liitosohjelmiston ATD-palvelun konfiguraatio. Endpoint osoittaa haluttuun API-laukaisijaan.

SOAR käynnisti syslog-kuuntelijan, kun liitosohjelmiston konfiguraatio oli tallennettu. Jotta vastaanotetusta syslogista saatiin luotua hälytys, luotiin kuvion 10 mukainen pelikirja parsimaan CEF-loki ja luomaan uusi alert-tietue.



Kuvio 10. Pelikirja ATD:n hälytysten luomiseen ja rikastamiseen

SIEMiä varten luodusta pelikirjasta poiketen syslogilla vastaanotettu hälytys ei automaattisesti muodostu SOARissa alert-tietueeksi, joten laukaisijaksi täytyi valita API-pohjainen laukaisin ja luoda tietue pelikirjalla. Laukaisinvaiheen konfiguraatiossa määritettiin päätepiste, johon saapuva Representational State Transfer (REST) API POST-pyyntö käynnistää pelikirjan suorituksen. Laukaisevaksi päätepisteeksi määritettiin aiemmin luodun syslog-liitosohjelmiston konfiguraation päätepisteen nimi, joten pelikirja käsittelee vain ATD-palvelun lähettämät hälytykset. Autentikoimiseen käytetään suositeltua token-pohjaista metodia, joka käyttää JSON Web Tokeneita (JWT) (ks. kuvio 11).



Kuvio 11. API-laukaisijan konfiguraatio

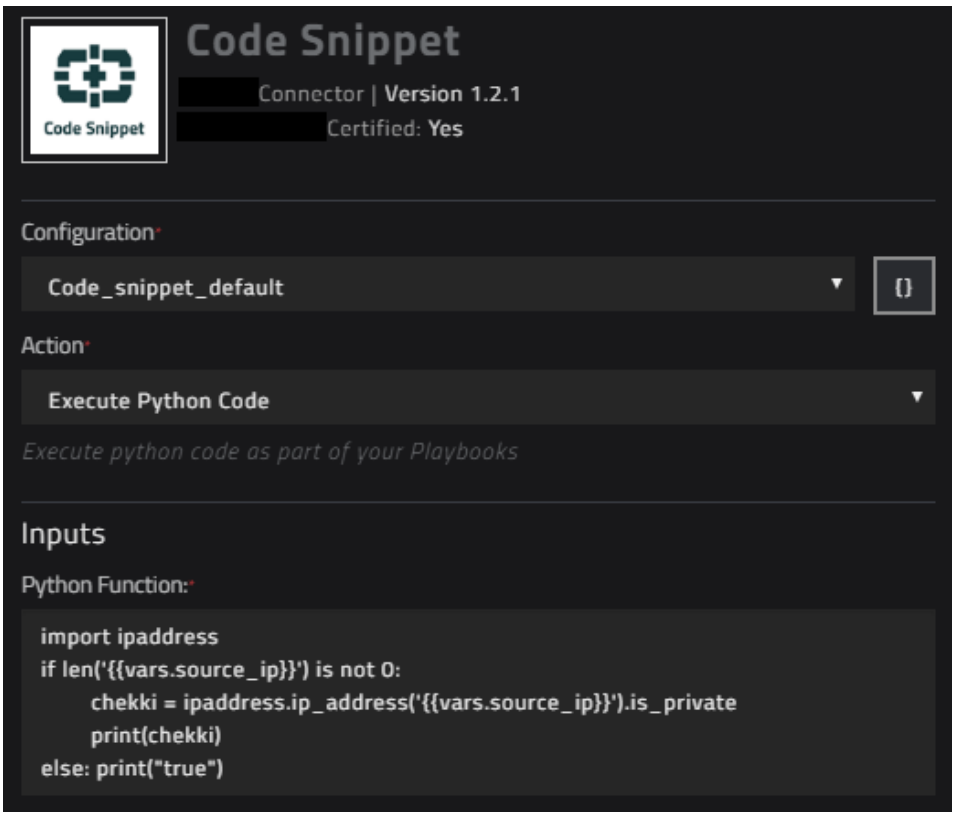
Pelikirjan seuraavissa vaiheissa tallennetaan pelikirjan sisäiseen muuttujaan vastaanotettu CEF-muotoinen syslog-data, parsitaan se SOARin omalla Utilities-liitosohjelmiston funktiolla ja luodaan uusi alert-tietue täydentäen sen kenttiin tiedot parsitusta datasta. SIEMin pelikirjasta poiketen ATD-palvelun pelikirjaan lisättiin myös tarkastus duplikaattien varalta hakemalla hälytyksistä osumia vastaavalla ID:llä. Jos samalla ID:llä oleva hälytys löytyy, lopettaa pelikirja suorituksen siihen. Lisäksi vakavuustason määrittämistä varten täytyi luoda päätösvaihe, jonka mukaan tietueen tasoksi päivitetään low, high tai critical, koska ATD-palvelu käyttää vakavuuden määrittämiseen pistearvoa skaalalla 0-100.

6.2.3 Analysoinnissa hyödynnettävät verkkopalvelut

Hälytyksiä analysoidessa SOC-tiimi käyttää erilaisia verkkopalveluita esimerkiksi IP-osoitteiden tietojen ja maineen tarkastamiseen. Tällaiset palvelut haluttiin integroida SOARiin siten, että niiden tulokset ja/tai linkit niihin ovat nopeasti ja helposti tarkasteltavissa kustakin hälytyksestä. IP-osoitteiden tietojen hakuun hyödynnetään mm. Whois, VirusTotal, GreyNoise ja Cisco Talos -palveluita.

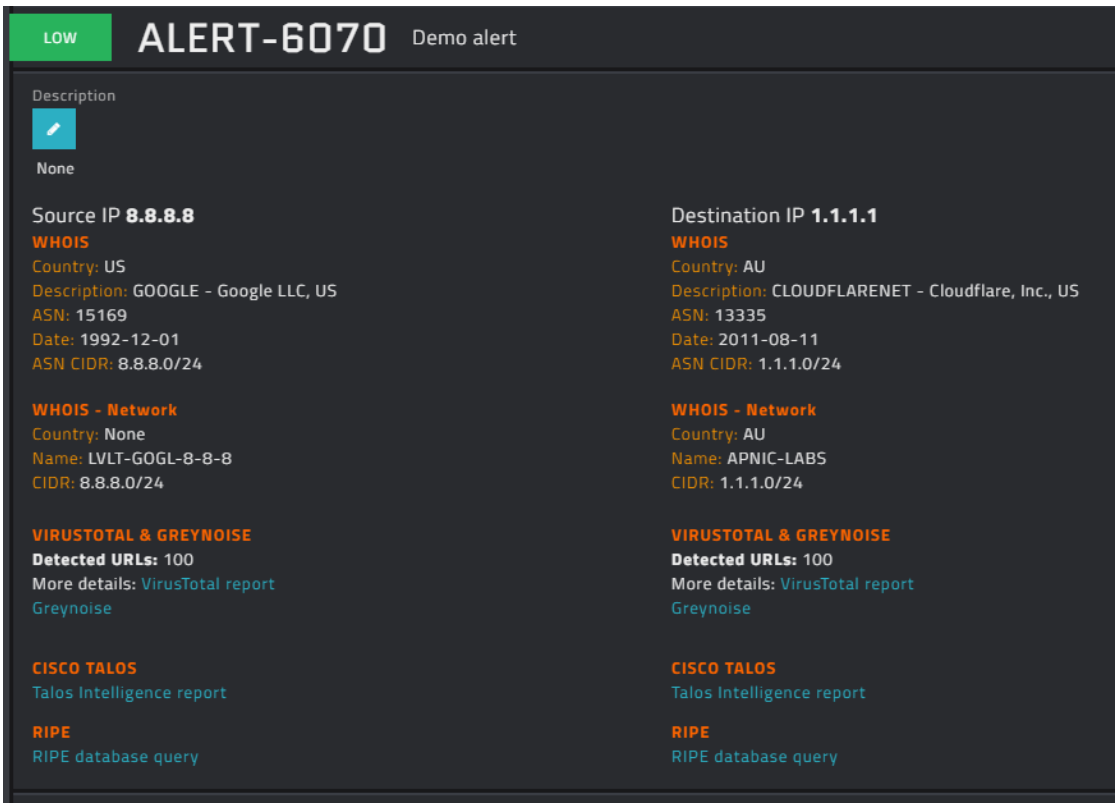
Palveluista Whois:lle ja VirusTotalille löytyi SOARiin valmis liitosohjelmisto. Liitosohjelmistot asennettiin ja tehtiin palomuuriavaukset, jonka jälkeen niille tehtiin konfiguraatiot, kuten muillekin liitosohjelmistoille aiemmin. VirusTotal käyttää yhteyteen API-avainta, kuten suurin osa muistakin vastaavista palveluista, joka syötetään liitosohjelmiston konfiguraatioon. VirusTotalin liitosohjelmistossa oli funktiot tiedostojen ja URL-osoitteiden lähettämiselle sekä IP-, domain-, URL- ja tiedosto-mainetietojen hakemiselle.

IP-osoitetietojen hakemiselle ja tulosten lisäämiselle alert-tietueeseen tehtiin pelikirja. Koska hälytyksissä ei välttämättä ole lähde ja kohde IP-osoitetta tai vain toinen niistä, täytyi pelikirjan sallia suorittaminen loppuun asti, vaikka jokin näistä kentistä olisi tyhjä. Tärkeänä huomiona oli myös tarkistaa, onko IP-osoite yksityinen vai julkinen, jottei kyselyjä suoriteta turhaa. SOARissa on valmiiksi asennettu Code Snippet -liitosohjelmisto, jolla voi ajaa Python-koodia suoraan pelikirjan vaiheena. Kuviossa 12 on esitetty pelikirjaan tehty Code Snippet -vaihe, joka tarkistaa onko IP-osoite yksityinen yksinkertaisella Python-koodin pätkällä. Tämän vaiheen palauttamaa vastausta käytetään sittemmin pelikirjassa päätöskohdassa määräämään, suoritetaanko kysely IP-osoitteesta VirusTotalissa.



Kuvio 12. IP-osoitteen tarkistus Code Snippet -pelikirjavaiheessa

Pelikirjan laukaisijana käytettiin aluksi manuaalista käynnistämistä, jotta testiajoja pystyttiin ajamaan aina halutessa. Kun pelikirja oli testattu toimivaksi ja käyttövalmis, vaihdettiin laukaisija automaattiseksi suorittamaan pelikirja aina uuden alert-tietueen luomisen yhteydessä. Kuviossa 13 on esitetty esimerkki pelikirjan rikastaman hälytyksen description-kentästä.



Kuvio 13. Esimerkki pelikirjalla rikastetuista IP-osoitetiedoista hälytyksessä

6.2.4 Muut työkalut

SOC:n käyttämistä työkaluista EPP-palvelun ja tiketöintijärjestelmän integraatiot eivät valmistuneet tähän työhön mennessä. EPP:n liitosohjelmisto on tuotetoimittajalla työn alla, sillä nykyinen liitosohjelmisto ei tue palvelun uutta API-rajapintaa.

Toimeksiantajan käytössä olevan tiketöintijärjestelmän integraatioyhteys tehdään yrityksen sisäisten kehittäjien toimesta. Integraatioyhteys tullaan tekemään kaksisuuntaisesti, jotta SOARista saadaan luotua tiketti järjestelmään ja päivitettyä tikettiin liittyvät viestit ja tiedot takaisin SOARiin.

6.3 Hälytysten ja poikkeamien käsittely

Kun tärkeimmät käytettävät työkalut oli integroitu SOAR-alustaan, tavoitteena oli tehdä hälytysten ja poikkeamien käsittely suoraan SOARissa, tarvitsematta käydä itse

integroiduissa työkaluissa erikseen, paitsi silloin tällöin, kun kaikkea tarvittavaa tietoa ei näe suoraan SOARista.

6.3.1 Havainnointi ja analysointi

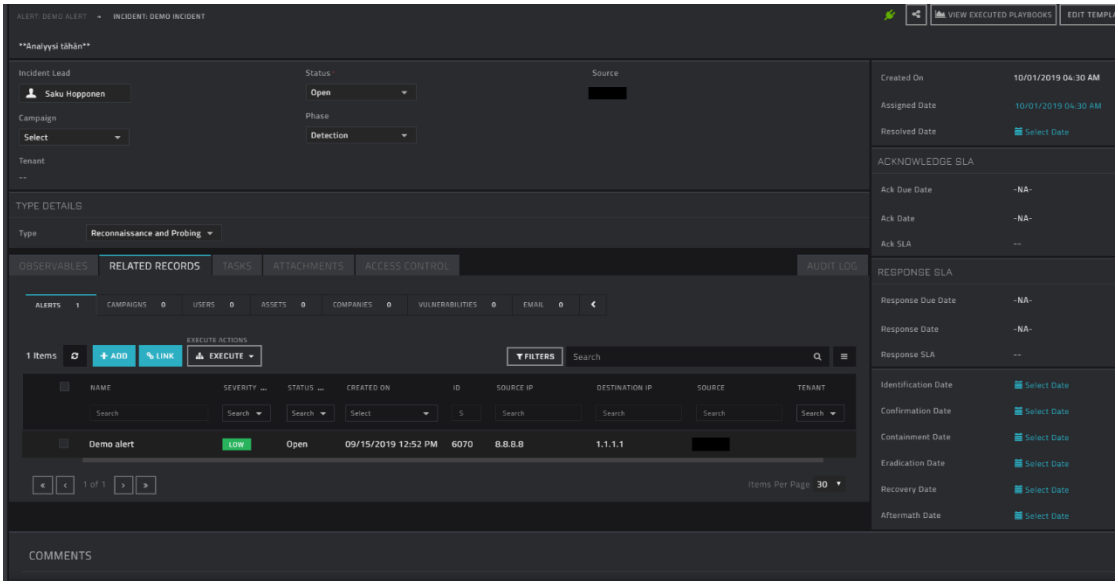
Hälytysten ja poikkeamien havainnointi muuttuu SOARin myötä analyytikolle helpommaksi. Kun eri työkalujen lähettämät hälytykset ovat samassa alustassa ja samalla hälytyslistalla, analyytikko voi suoraan nähdä korrelaatiota eri järjestelmien lähettämien hälytysten välillä, jos sellaista on. Kun analyytikko suorittaa valvontaa SOARista, ei hänen tarvitse valvoa useamman eri työkalun käyttöliittymää, joka lisää riskiä, että analyytikolta jää jotain havaitsematta tai yhteyttä kahden tai useamman eri järjestelmän tuottaman hälytysten välillä ei huomata. Kun uusi hälytys saapuu SOARiin, merkitsee valvontaa suorittava analyytikko sen statuksen itselleen käsiteltäväksi ja aloittaa tutkinnan. Pelikirjat, jotka ovat luotu automaattisesti ajettaviksi uuden hälytyksen saapuessa, rikastavat hälytyksen tiedot ja hakevat mm. IP-osoitteiden mainetiedot automaattisesti, jolloin tiedot ovat lähes välittömästi analyytikon nähtävillä hälytyksen saapumisesta. Myös hälytyksistä löytyvät indikaattorit (IP-osoitteet, tiedostojen tiivistesummat ja URL-osoitteet) poimitaan hälytyksistä pelikirjalla, joka luo niistä tietueet indicators-moduuliin.

Eri moduulien, kuten alerts, incidents ja indicators, väliset yhteydet linkittyvät valmiiksi olevien pelikirjojen avulla ja kaikista tietueista on nähtävillä, mitkä muut tietueet liittyvät kuhunkin hälytykseen, joka helpottaa analyytikkoa hahmottamaan kokonaiskuvaa, sekä havaitsemaan aiempia esiintymiä tapahtumasta. Koska SOAR mahdollistaa omien moduulien tekemisen ja olemassa olevien muokkaamisen, on uusia yhteyksiä moduulien välille helppo lisätä tarpeen mukaan. Lisäksi tietueiden ulkonäköä ja esittämiä kenttiä voi vapaasti muokata, joten esim. hälytykset voi muokata näyttämään juuri haluamiltaan, joka on modulaarisen SOARin etuja.

Tutkinnan ja analyysin perusteella hälytys joko suljetaan tai eskaloidaan poikkeamaksi. Hälytys voidaan sulkea vääränä hälytyksenä, tai todellisena positiivisena. Sulkemisen voi suorittaa nappulalla käynnistettävällä yksinkertaisella pelikirjalla, joka pyytää käyttäjältä sulkemisen syyn ja automaattisesti päivittää ratkaisun aikaleiman,

sekä hälytyksen sulkeneen henkilön tietueeseen. Jos joitain selkeästi vääriksi hälytyksiksi tunnistettuja hälytyksiä ei voida niitä lähettävän järjestelmän päässä sääntömuutoksilla suodattaa, SOARin pelikirjalla voidaan myös suorittaa automaattista sulkemista määritetyillä ehdoilla.

Jos havaittu hälytys on analyysin perusteella tietoturvapoikkeama, eskaloidaan se, jolloin SOAR luo siitä incident-tietueen ja linkittää siihen kuuluvat hälytyksen siihen. Kuten hälytykset, ovat poikkeamat myös muokattavissa moduulin kautta. Poikkeaman tietueeseen analyytikko kirjaa analyysinsa tuloksen, tarvittavat toimenpiteet ja määrittää muut tiedot poikkeamalle, esimerkiksi tyypin. Kuviossa 14 on esitetty esimerkki hälytyksestä eskaloidusta poikkeamasta SOARissa.



Kuvio 14. Incident-tietue, johon on liitettynä siihen liittyvät muut tietueet eri moduuleista

Toimeksiantajan käytössä olevan tiketöintijärjestelmän integroiminen SOAR-alustaan tunnistettiin alusta asti yhdeksi tärkeimmistä automatisoinnin ja nopeuttamisen kohteeksi. Tiketöinnin integraatio suunniteltiin tapahtuvan siten, että analyytikko voi suoraan incident-tietueesta luoda uuden tiketin järjestelmään pelikirjalla, joka myös täyttäisi automaattisesti mm. asiakkaan ID:n ja muita aiemmin manuaalisesti täytettäviä kenttiä nopeuttaen tiketöintiprosessia ja vähentäen inhimillisiä virheitä.

6.3.2 Reagointi

Joidenkin tietoturvateknologioiden, kuten EPP-työkalujen tai palomuurien, liitosohjelmistot mahdollistavat SOAR-alustassa reagoimisen poikkeamiin toimenpiteillä kuten eristämällä halutun laitteen verkosta tai blokkaamalla tietyn IP-osoitteen. Tällainen SOC-tiimin käytössä oleva työkalu oli esimerkiksi EPP-palvelu, mutta koska tuotetoimittajan liitosohjelmisto oli vanha, ei integraatiota saatu mukaan tähän työhön.

Päivitetty liitosohjelmisto ja toimiva integraatioyhteys mahdollistaa esim. suojattujen päätelaitteiden, niissä käynnissä olevien prosessien ja muiden tietojen listaamisen lisäksi skannausten ajamisen päätelaitteille tai laitteen verkosta eristämisen. Näitä toimenpiteitä voi käyttää pelikirjoissa vaiheina ja incident-tietueista voi suorittaa näitä vastatoimenpiteitä ajamalla pelikirjoja. Tällä hetkellä SOC-tiimi toistaiseksi vain havaitsee ja analysoi poikkeamia, ilmoittaen niistä asiakkaille suositellen tarvittavat vastatoimenpiteet. Tästä syystä incidents-moduulin kustomointi jäi tässä vaiheessa hyvin vähäiseksi, incident-tietueiden sisältäessä lähinnä analyytikon kirjoittaman analyysin ja poikkeamaan liittyvät alert-tietueet.

6.4 Mittarit

SOC-tiimin suorituskyvyn määrittely on haastavaa, eivätkä kaikki mittarit sovellu välttämättä kaikille SOC:eille. Yleisesti kuitenkin voidaan ajatella, että mittarit, jotka ovat selkeästi sidoksissa liiketoimintaan, ovat jokaiselle tietoturvavalvontaa tekevälle organisaatiolle tärkeitä. Tällaisia mittareita ovat esimerkiksi aiemmin mainitut havainnointi- ja ratkaisuaikaa mittaavat MTTD ja MTTR. Käyttöönottoa tehdessä kuitenkin huomattiin, että SOARin vaikutukset eivät olleet vielä tässä vaiheessa selkeästi esillä.

Aluksi mittareiksi suunniteltiin käsittelyaikoja, mutta todettiin, että muuttuvia tekijöitä on liikaa. SOAR-alustan käyttöönotto ei ollut vielä tarpeeksi pitkällä, jotta hälytysten ja poikkeamien käsittelyaikoja ja muiden vastaavien ajallisten mittareiden arvoja olisi voinut pitää vertailun kohteina ilman SOARia tehdyn valvontatyön ja poikkeaman hallinnan tuloksiin. Käsittelyajoissa vaikuttavia muuttuvia tekijöitä ovat esimerkiksi hälytyksen tyyppi, kohde, sen toistuvuus ja aiemmat havainnot, ja tutkinut

analyytikko. Pelikirjoilla automaattinen IP-osoitetietojen hakeminen ja linkkien luominen tietueiden välille nopeuttaa analysointityötä, mutta sen tarkka ajallinen mittaaminen ei ollut kannattavaa, sillä se on hyvin pieni osa prosessia. Tiketöinnin integraatioyhteyden puuttuminen tämän työn vaiheessa käyttöönottoa oli lisäksi huomattava puute, joten esim. MTTR:n mittaaminen ei ollut järkevää. Lisäksi hälytysten määrän ollessa vielä niin pieni, todettiin MTTD:n mittaaminen myös tarpeettomaksi, koska kaikki saapuneet hälytykset kyettiin käsittelemään heti kun ne saapuivat. Täten SLA:n aika havainnoinnin osalta oli käytännössä nollassa.

Vaikutusten mittaukseen tässä vaiheessa soveltui parhaiten analyytikoiden testikäytön jälkeinen palaute ja odotukset SOAR-alustasta, sen käytöstä, ja valvontatyön tekemisestä sen kautta (ks. Liite 1). Analyytikoilta kysyttiin vapaamuotoista palautetta SOARista ja huomioita valvontatyön tekemisestä SOARilla.

7 Tulokset

Käyttöönotossa tehtyjen työkaluintegraatioiden avulla valvonta saatiin yhteen käyttöliittymään ja luoduilla pelikirjoilla saatiin toistaiseksi automatisoitua pientä osaa hälytysten käsittelyn vaiheista.

Liitteessä 1 esitetty analyytikoilta kerätty palaute lyhyehkön SOARin testikäytön perusteella jakoi mielipiteitä. SOARin käytön koulutus ja testikäytön pituus ei aikataulun puitteissa ollut yhtä riittävä syvempään palautteeseen muilla SOC-tiimin jäsenillä, kuin järjestelmän parissa enemmän työskennelleillä.

Tiketöintijärjestelmän integraation puuttuminen tunnistettiin palautteissakin huomattavaksi puutteeksi, jonka takia ”kopioi ja liitä” -toimintaa joutui edelleen tekemään poikkeamia eskaloidessa asiakkaille. Integraation valmistuessa tulee tiketöintiprosessikin nopeutumaan huomattavasti.

Käyttöliittymä todettiin ulkoisesti hyvän näköiseksi ja sen kustomointimahdollisuudet nostettiin etuna, mutta käytettävyyteen liittyi osalla ongelmia. Tätä selittää SOAR-

alustan käyttöön liittyvän koulutusosuus, jota ei oltu vielä ehditty kattavasti pitää tiimille näin alkuvaiheessa, erillisen tarkemman koulutuksen tapahtuessa pidemmällä käyttöönotossa. Paljon enemmän järjestelmää käyttänyt tuntee itse helposti alustan käytön yksinkertaiseksi, mutta se ei välttämättä sitä muille ole ennen kattavaa koulutusta. Ongelmaksi palautteissa nousi yleispätevän näkymän tekeminen, sillä toistaiseksi listanäkymät ovat kaikille samanlaiset. Koska kaikissa hälytyksissä ei ole esimerkiksi lähde- ja kohde IP-osoitetta, ei listanäkymän IP-osoitesarakkeet palvele täysin hälytysten käsittelytyötä. Ongelmana on, että kun hälytyksiä tulee usealta eri laitteelta ja ne ovat eri tyyppisiä, ei yksi sapluuna näkymästä voi toimia yleispätevänä kaikille hälytyksille. Tämä ongelma voidaan jatkossa ratkaista luomalla useampi näkymä, joista valita mitä käyttää tai jakamalla hälytykset integroitujen järjestelmien lähteen mukaan.

Perinteiseen SIEMistä tehtyyn valvontaan verrattuna automaation tekemä tiedonhaku ja linkit uhkatietopalveluihin ja IP-osoitetietojen hakuun havaittiin nopeuttavan käsittelyä palautteidenkin perusteella. Mitä vähemmän joutuu manuaalisesti tekemään vastaavia hakuja, sitä nopeammin käsittely etenee. Tehtävien automatisointi pelikirjoilla huomattiin hyvin potentiaaliseksi avuksi ja todettiin, että kun manuaalisia prosesseja saadaan enemmän automatisoitua, tulee työnkulku paranemaan. Tällöin aikaa saadaan käytettyä tehokkaammin itse analysointityöhön, kun tarvittava tieto on valmiiksi esillä.

Indikaattoreiden kerääminen ja niiden ylläpitäminen SOARissa havaittiin tehokkaaksi apuvälineeksi valvontatyössä. Epäkohtina indikaattoreista nousi, ettei mainetietoa voi valita suoraan sitä manuaalisesti luodessa. Nämä ongelmat kyetään korjaamaan muokkaamalla moduulia ja siihen liittyviä oletuspelikirjoja halutun näköiseksi. Moduulia ei tämän työn aikana ehditty muokata täysin valmiiksi, hälytysten ollessa ensisijainen hiomisen kohde. Tulevaisuudessa indikaattoreiden tavoitteena on tarjota helposti ja suoraan näkyviin sen tila ja maine, sekä aiemmat esiintymiset hälytyksissä, jotta vastaavat havainnot ovat nähtävillä ja mahdollinen poikkeama helpommin havaittavissa kokonaiskuvasta.

SOAR-järjestelmän käyttöönottoprojekti on pitkä ja jatkuvan kehityksen alla. Modulaarisen SOARin muokkaaminen mahdollisimman analyytikkoa palvelevaksi, manuaalisten työtehtävien korvaaminen pelikirjoilla ja työnkulun hiominen vievät aikaa ja alusta muovautuu toimeksiantajan tarpeiden näköiseksi ajan mittaan. SOAR-järjestelmällä on saavutettavissa työnkulun yhdenmukaisuutta, kun pelikirjoja erilaisista prosesseista ja vaiheista tehdään lisää. Toistuvia tehtäviä automatisoidaan pelikirjoilla ja ihmisen tekemiä virheitä minimoidaan esim. pelikirjan suorittamilla tarkastuksilla ja automaattisesti täyttämällä datakenttiä, jotka aiemmin analyytikko on joutunut kirjoittamaan käsin.

Orkestroinnilla ja automatisoinnilla voidaan jatkossa korvata manuaalinen työ esimerkiksi tapauksessa, jossa käyttäjä lataa haittaohjelman työasemalleen: Palomuuri havaitsee tapahtuman, muttei kykene estämään sitä. Tästä tulee hälytys SIEM-järjestelmään, että haittaohjelma on läpäissyt palomuurin. Työaseman antivirusohjelmisto pysäyttää haittaohjelman ja ilmoittaa siitä. ATD-järjestelmä kaappaa tapahtumaan liittyvän liikenteen ja haittaohjelman, ja tekee haittaohjelmalle analyysin ajamalla sen hiekkalaatikossa, joka kertoo haittaohjelman toiminnallisuudesta ja mm. mitä se yrittää suoritettuna tehdä. Kaikki nämä vaiheet olisivat SOAR-alustassa nähtävillä, jolloin tilanteesta saa muodostettua kokonaiskuvan. Integroituina järjestelmien hälytykset ovat koottuna SOARiin ja niiden toiminnot, kuten haittaohjelman analysointi hiekkalaatikossa, olisivat ajettavissa SOAR-alustan pelikirjojen käskyttämänä, yhtenä prosessina. Analyytikon on helpompi ja nopeampi tehdä analyysi ja päätös tilanteen vakavuudesta. Esimerkin mukainen automatisointi nopeuttaa analyysityötä, joka lyhentää poikkeaman käsittelyaikaa, joka taas tarkoittaa SOC-tiimin kyvykkyyttä käsitellä hälytyksiä nopeammin, pitäen kiinni sovituista vasteajoista hälytysmäärien kasvaessa.

Kasvavan hälytysmäärän ongelmiin liittyy olennaisesti virheellisten positiivisten eli väärien hälytysten määrä. Kun analysoitavia hälytyksiä tulee nopeammin kuin analyytikko ehtii niitä käsitellä, on väärät hälytykset kitkettävä pois. Jos havaittavissa hälytyksissä toistuu paljon samanlaisia tapahtumia ja niissä on kaavamaisuutta, pelikirja kykenee suorittamaan analysoinnin mahdollisimman pitkälle ihmisen puolesta ja jois-

sain tilanteissa merkitä hälytyksiä virheellisiksi positiivisiksi automaattisesti, jos lähdetyökalun säännöillä sitä ei pystytä tekemään. Tämä vaikuttaa suoraan SOC-tiimin havainnointikykyyn, joka on oleellinen osa SOC:n suorituskykyä. Myös hälytysten priorisointi automatiikalla on tätä havainnointikykyä tehostava toiminto. SOAR-alustalla kyetään esimerkiksi muuttamaan hälytyksen vakavuustasoa tai lähettämään sähköpostilla ilmoituksen, jos hälytys koskee asiakkaalle kriittistä laitetta ja hälytys nostetaan käsittelylistan kärkeen.

8 Pohdinta

Opinnäytetyön tavoitteena oli ottaa käyttöön SOAR-alusta ja tarkastella sen vaikutuksia SOC:n toimintaan valvontatyössä. Työssä käyttöönottoon kuului käyttäjien ja tiimien luominen alustaan sekä integraatioyhteydet muihin SOC:n työkaluihin. Tavoitteet saavutettiin, muttei aivan niin kattavasti kuin itse odotin, koska työn edetessä kävi entistä selvemmäksi, että projekti on kuitenkin paljon pidempi työ, kuin mitä tähän opinnäytetyöhön ehdittiin tekemään. Tästä johtuen myös vaikutusten mittaaminen osoittautui haastavaksi, koska kaikkia haluttuja integraatioita ei ehditty tekemään eikä poikkeaman hallinnan prosesseja vielä tarkemmin automatisoimaan. SOARin vaikutuksia kyettiin kuitenkin havaitsemaan.

Lopputuloksena työkaluista SIEM- ja ATD-järjestelmät saatiin integroitua SOAR-alustaan ja niiden lähettämät hälytykset rikastettiin pelikirjoilla, mutta kaikkia SOC-tiimin käytössä olevia työkaluja ei saatu integroitua SOARiin niiden liitosohjelmistojen ollessa vasta kehitettävänä. SOARin vaikutuksia valvontatyöhön havaittiin orkestroinnin ja automatisoinnin osalta, kun valvonta saatiin keskitettyä yhteen järjestelmään ja luotua pelikirjoja tietojen rikastamiseen. SOAR-alustan huomattiin nopeuttavan analysoinnin alkuvaihetta, kun IP-osoitetiedot ovat valmiiksi haettu hälytystietueeseen. Tämän lisäksi eri työkalujen hälytysten saaminen samaan alustaan auttoi analyytikoiden työskentelyä, kun ei tarvinnut valvoa useampaa eri käyttöliittymää. Myös hälytyksiin kuuluvien indikaattoreiden ja niiden tai hälytysten aiempien havaintojen seuraaminen oli SOARissa helpompaa, kun tietueiden väliset linkitykset olivat automaattisia. Poikkeaman hallinta ja hälytysten käsittelyn vaiheet

saatiin SOARissa eriteltyä selkeämmäksi, kun hälytyksiin saatiin käsittelevän henkilön nimi ja eskalointi poikkeamaksi suoritettiin pelikirjalla.

Mielestäni työssä onnistuttiin kuvaamaan SOC, SOAR, ja niihin liittyvät aiheet ja haasteet tarpeeksi kattavasti työn toteutusvaiheen tueksi. Toteutuksessa käyttöönotto saatiin työn aikana hyvälle uralle, kun tuotteen erilaisia ominaisuuksia päästiin käyttämään ja testaamaan, ja tietoperustassa esitellyt SOARin tärkeimmät ominaisuudet ja vaikutukset olivat havaittavissa myös SOAR-alustan parissa työskennellessä. SOARin modulaarisuus ja muokattavuus oli jopa yllättävää, joka myös toi haasteita hahmottaa, millaiseksi alusta ja sen eri moduulit kannattaisi rakentaa, jotta ne tukisivat parhaiten analyytikoiden työtä. Ongelmia totetutuksessa ilmeni mm. AD-käyttäjien tuonnin ja SIEM-integraation kohdalla, kun korjauksia niihin jouduttiin odottamaan tuotetoimittajalta useampia viikkoja, joka hidasti työn etenemistä. Vaikutusten mittaamisessa useammat erilaiset suorituskykymittarit olisivat antaneet kattavamman kuvan vaikutuksista SOC:n suorituskykyyn, mutta käyttöönotto ei ollut vielä tarpeeksi pitkällä, jotta niitä olisi voitu käyttää vaikutusten tarkkaan mittaamiseen. SOC:n suorituskyvyn määrittely ei ole määritettävissä yksinkertaisesti eikä vain tiettyjen määrällisten mittareiden perusteella, vaan se muodostuu kunkin organisaation itse asettamien mitattavien tulosten pohjalta. Mittarina analyytikoiden mielipiteet ovat subjektiivisia ja niissä on eroavaisuuksia, mutta ne ovat yhtä tärkeitä kuten muutkin suorituskykymittarit.

Tulosten perusteella voidaan todeta, että SOARilla on saavutettu jo osittain, ja tullaan saavuttamaan SOC:n suorituskykyä tehostavaa manuaalisen työn automatisoimista, havainnointikyvyn paranemista korreloimalla, työnkulun ja prosessien virtaviivaistamista ja yhdenmukaistamista, hälytysten automaattista luokittelua ja poikkeaman hallinnan vaiheiden nopeuttamista. Nämä parantavat tilannekuvan hahmottamista valvottaviin ympäristöihin ja mahdollistavat kasvavan hälytysmäärään reagoimisen nopeammin ja vasteajan puitteissa. Kokonaisuudessaan vaikutukset vähentävät tiimin työtaakkaa ja lisäävät tiimin tuottavuutta. Tuloksia voidaan hyödyntää SOARin positiivisten vaikutusten osoittamiseen ja alustan hankkinnan perusteluna.

SOAR-alustan käyttöönotto jatkuu tämän työn jälkeenkin. Muokattavaa, integroitavaa ja automatisoitavaa on vielä paljon ja projekti on pitkä sekä jatkuvasti kehittyvä. Tässä työssä ehdittiin toteuttaamaan ja käsittelemään pintaraapaisu alustan käyttöönotosta ja mahdollisuuksista. SOC-tiimin valvontatyön kehittäminen on yleisestikin jatkuvaa, niin prosessien, työkalujen kuin henkilöstön osaamisen suhteen. SOC:n työkaluista SOAR tulee olemaan tiimin ensisijainen valvontatyössä käytetty alusta, joten ei voi sanoa, että se olisi välttämättä koskaan täysin valmis.

Lähteet

Cichonski, P., Millar, T., Grance, T. & Scarfone, K. 2012. Computer Security Incident Handling Guide. National Institute of Standards and Technology (NIST). Viitattu 15.7.2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Crowley, C. & Pescatore, J. 2019. Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey. SANS Institute. Viitattu 17.7.2019. https://www.sans.org/reading-room/whitepapers/analyst/common-practices-security-operations-centers-results-2019-soc-survey-39060

Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens. 2018. (ISC)²:n tutkimus kyberturvallisuusalan työvoimasta 2018. Viitattu 23.7.2019. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

Hein, B. 2019. The 5 Cybersecurity Takeaways From Gartner's NTA Market Guide. ExtraHopin artikkeli Forbes-lehden verkkosivustolla 25.3.2019. Viitattu 30.7.2019. https://www.forbes.com/sites/extrahop/2019/03/25/the-5-cybersecurity-takeaways-from-gartners-nta-market-guide/#6da378c470fd

Henderson, J. 2019. Passive Isn’t Good Enough: Moving into Active EDR. SANS Institute. Viitattu 17.7.2019. https://www.sans.org/reading-room/whitepapers/analyst/passive-isn-039-t-good-enough-moving-active-edr-38965

Imam, F. 2019. Security Orchestration, Automation and Response (SOAR). Artikkeli Infosec Instituten verkkosivustolla 12.3.2019. Viitattu 27.6.2019. https://resources.infosecinstitute.com/security-orchestration-automation-and-response-soar/

Incident Response Automation and Security Orchestration with SOAR. N.d. Artikkeli Exabeam-verkkosivustolla. Viitattu 27.6.2019. https://www.exabeam.com/siem-guide/incident-response-and-automation/

In-house SOC or MSSP. 2019. Artikkeli Avertiumin verkkosivuilla 27.2.2019. Viitattu 21.6.2019. https://www.avertium.com/in-house-soc-of-mssp/

Jablonska, M. 2017. Proactive or Reactive Endpoint Security? A Critical Crossroads for SOC Analysts. Artikkeli SecurityIntelligence-verkkosivustolla. Viitattu 17.7.2019. https://securityintelligence.com/proactive-or-reactive-endpoint-security-a-critical-crossroads-for-soc-analysts/

Kyberturvallisuuden sanasto. 2018. Sanastokeskus TSK ry. Helsinki: Huoltovarmuuskeskus. Viitattu 12.7.2019. http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Managed Security Service Provider (MSSP). N.d. Artikkeli Gartnerin IT-sanaston verkkosivuilla. Viitattu 21.6.2019. https://www.gartner.com/it-glossary/mssp-managed-security-service-provider

Miller, D., Harris, S., Harper, A., Vandyke, S. & Blask, C. 2011. Security Information and Event Management (SIEM) Implementation. Viitattu 24.6.2019. https://library.books24x7.com/

Moran, J. 2018. Key Performance Indicators (KPIs) for Security Operations and Incident Response. DFLabsin dokumentti. Viitattu 25.7.2019. https://www.dflabs.com/wp-content/uploads/2018/03/KPIs_for_Security_Operations_and_Incident_Response-2.pdf

Morgan, S. 2017. Cybersecurity Jobs Report 2017 Edition. Cybersecurity Ventures:n raportti. Viitattu 23.7.2019. https://www.herjavecgroup.com/wp-content/uploads/2018/07/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf

Neiva, C., Lawson, C., Bussa, T. & Sadowski, G. 2019. Market Guide for Security Orchestration, Automation and Response Solutions. Gartner. Viitattu 10.7.2019. https://www.gartner.com/doc/reprints?id=1-10ID63MZ&ct=190701&st=sb

Rao, U. H. & Nayak, U. 2014. The InfoSec Handbook: An Introduction to Information Security. Viitattu 15.7.2019. https://library.books24x7.com/

Security Orchestration and Automation. N.d. Artikkeli Demiston verkkosivustolla. Viitattu 27.6.2019. https://www.demisto.com/security-orchestration/

SOAR - Security Orchestration, Automation and Response. N.d. Artikkeli Optiv-verkkosivustolla. Viitattu 26.6.2019. https://www.optiv.com/cybersecurity-dictionary/soar

The Evolution of Endpoint Protection. 2018. Symantecin julkaisema tutkimus. Viitattu 17.7.2019. https://www.gartner.com/imagesrv/media-products/pdf/symantec/symantec-1-4SNI36O.pdf?es_p=6816496

The Modern Security Operations Center, SecOps and SIEM: How They Work Together. N.d. Artikkeli Exabeam-verkkosivustolla. Viitattu 25.7.2019. https://www.exabeam.com/siem-guide/the-soc-secops-and-siem/

Tillyard, J. 2018. The Top 5 Challenges Faced by Security Operations Centers. Artikkeli DFlabs-verkkosivustolla 21.3.2018. Viitattu 1.7.2019. https://www.dflabs.com/blog/the-top-5-challenges-faced-by-security-operations-centers/

Tillyard, J. 2019. The Difference Between SIEM and SOAR (Why Do I Need SOAR, If I Have SIEM?). Artikkeli DFlabs-verkkosivustolla 27.6.2019. Viitattu 17.11.2019. https://www.dflabs.com/blog/the-difference-between-siem-and-soar-why-do-i-need-soar-if-i-have-siem/

Toivonen, J. 2017. Vaasan Läänin Puhelimesta tuli Anvia, josta tuli Viria, jolla on 100 miljoonaa euroa muttei puhelimia tai verkkoa – puhelinyhtiöt ovat muuttuneet totaalisesti. Artikkeli Ylen uutisten verkkosivustolla 17.7.2017. Viitattu 25.6.2019. https://yle.fi/uutiset/3-9715405

Torres, A. 2015. Building a World-Class Security Operations Center: A Roadmap. SANS Institute. Viitattu 19.6.2019. https://finland.emc.com/collateral/white-papers/rsa-advanced-soc-solution-sans-soc-roadmap-white-paper.pdf

Virian liiketoiminnat. N.d. Infosivu Virian verkkosivustolla. Viitattu 25.6.2019. https://www.viria.fi/viria-konserni/liiketoiminnat/

Vuosikertomus 2018. 2018. Virian vuosikertomus. Viitattu 25.6.2019. https://www.viria.fi/wp-content/uploads/2019/04/Viria_vuosikertomus_2018.pdf

Wang, C., Clark, J. & Wilcox, D. 2018. The State of the SOC: An Enterprise Study on Threat Detection and Response. Fideliksen tilaama ja 360Velocityn tekemä tutkimus. Viitattu 2.7.2019. http://www.ace-pac.com/download/Fidelis/RS-State-of-SOC-0315-2018.pdf

What is Security Automation? 2017. Artikkeli Rapid7:n blogisivustolla 18.5.2017. Viitattu 27.6.2019. https://blog.rapid7.com/2017/05/18/security-automation/

Why Gartner’s SOAR Model is the Future of IT Security. 2018. Artikkeli Technologent-verkkosivustolla 25.7.2018. Viitattu 26.6.2019. https://blog.technologent.com/gartner-soar-model-future-it-security

Yu, D. 2019. Network Traffic Analysis (NTA). Artikkeli Hillstone Networksin verkkosivustolla 18.3.2019. Viitattu 30.7.2019. https://www.hillstonenet.com/blog/network-traffic-analysis-nta/

Zimmerman, C. 2014. Ten Strategies of a World-Class Cybersecurity Operations Center. MITRE. Viitattu 19.6.2019. https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

Liitteet

Liite 1. SOC-tiimin analyytikoiden palautteet SOARista

• Vapaa indikaattoreiden määrittely
• Alert listalla näkyy pelkästään ip tietoa
  ○ puuttuu osasta alerteista
  ○ valvonta vaatii alertien avaamista, hidastaa toimintaa
• Tämän hetkisessä prosessissa, jossa tiketit asiakkaille tehdään copy-pastella tikettijärjestelmään, tieto pitäisi kaivaa useasta eri paikasta
• Päättömyyksiä käyttöliittymässä
  ○ Esim. Indikaattorille ei voida antaa reputationia luotaessa, vaan se pitää lisätä erikseen???

• Indikaattorit osio on erittäin hyvä KB SOC:n kohtaamista IoC:sta
  ○ Hyvä IoC kategoriointiin ja TI:n jakamiseen
  ○ Ongelmana se että pitäisi saada tehokas ja aktiivinen käyttö ominaisuudelle analysoinnin yhteydessä
• Automaation mahdollisuudet melkein rajattomat playbookkien avulla
  ○ Ongelmana automaation säätämiseen menevä työ, ns. loputon työmaa
  ▪ Säätöä pitäisi tehdä samalla kun analysoi, löytää tutkinnassa jotain jota automatisoida -> toteuttaa sen tai ainakin dokumentoi idean
• SOAR:n näkymien kustomisaatio erittäin vahva
  ○ Helpottaa huomattavasti workflowta, kun tarpeelliset kentät, playbookit ja muut toiminnallisuudet yhdessä paikassa
  ○ Ongelmana hyvän ”yleispätevän” näkymän toteuttaminen
  ▪ Mahdollista personalisoida tätä jokaisen omaan käyttäjään parantamaan henk. koht. Workflowia?

• Ehkä isoin juttu miulle on tuo et incidentistä löytyy suoraan linkit esim. cisco talos, greynoise ja virustotaliin. Nopeuttaa käsittelyä kun löytyy nuo palvelut kätevästi incidentin alta. • Sit oon saanu sellaisen kuvan että tolla soarilla pystyy aika paljon automatisoimaan asioiden käsittelyä ja playbookeilla voi tehdä vaikka mitä. Tämä taas varmasti helpottaa SOCin työtä sit kun saadaan homma pyörimään. • Jos jotain negatiivista pitää sanoa, niin UI on minusta vähän sekava. Selkeesti on panostettu ulkoasuun mutta ehkä se menee käytettävyyden edelle. Tosin tämäkin ”ongelma” varmaan poistuu kun tottuu käyttämään.

- Pikaohje: tykkäsin, paitsi:
    - kohta jossa Alert-listasta saa alertin lisätietoja näkyviin täpästä:
        - Korvaa sen suoraan kohdalla, jossa klikataan hälytyksen otsikkoa ->
        - -> Avaa tarkemmat tiedot
        - -> Avaa suoraan Virustotalin, Graynoisen ja Tallos intelligence-linkit
        - Tykkään, helppo! Ei tartte enää copy-pastata!!
- Fiilis: sitä ehkä vastustetaan koska vaikeudet integroida nykyiseen työskentelymalliin (multiorganisaatio)
  Tarttis ehkä opastettua käyttöä//syventymistä sen käyttöön
- SOAR:
    - Nätti
    - Jouheva
    - Pitäisi yhteensovittaa meidän työskentelymetodien kanssa.
        - Nyt ongelmana on että Tier1 on vain SIEMissä

- SOAR:n potentiaali on hyvä, mutta toisaalta haastellinen runsaan muokattavuuden vuoksi.
- Kaikkia automatisaation mahdollisuuksia ei ole vielä kartoitettu. Tämä tarkoittaa sitä, että potentiaalisen automatisoinnin mahdollisuuksia ei vielä tiedetä tarkalleen.
- Haasteena jatkuvasti muuttuva threatlandscape ja toisaalta valvottavien laitteiden päivitykset, asiakkaiden käytön muuttuminen. Käytännössä kaikki elementit valvonta-segmentillä elää ja muuttuu.
- SOAR vaatii hyvää ja nopeaa muutoksenhallintaprosessia. Pyörää ei kuitenkaan tarvitse keksiä uudelleen vaan ongelma on ratkaistavissa lainaamalla jatkuvan ohjelmistokehityksen tekniikoita soveltuvin osin ja yhdistämällä yrityksen muutoksenhallinta-prosessin osuudet yhteen.
- - Kokonaisuutena SOAR on hyvä mahdollisuus automatisoida prosessimaisen työnosuutta tietoturvavalvonnassa. Tämä ei tarkoita, että koko prosessi automatisoidaan havainnoista raportointiin. Hyvin hyödynnettynä SOAR tuo kokonaisnäkyvyyden tapahtumiin ja rikastaa tietoa eri järjestelmien, IoC:n ja ThreatIntelin avulla. Tämä kaikki tieto tuodaan "pakettina", jonka perusteella analyytikko voi tehdä tarvittavat ratkaisut ja reagoida nouseviin uhkiin nopeasti. Tämä myös palvelee asiakkaita nopeutuneina vasteaikoina ja lisää tehokkuutta esim. haittaohjelmien leviämisen estämisessä/eristämisessä ja asiakkaan liiketoiminnan jatkuvuuden varmistamisessa. Lopputuloksena on siis entistä parempaa palvelua ja parempia päätöksiä kokonaisnäkyvyyden ollessa parempi.