LAPIN AMK
Lapland University of Applied Sciences

PALO ALTO NETWORK CORTEX XDR -JÄRJESTELMÄN LOKIEN INTEGROINTI- JA HALLINTAMAHDOLLISUUDET

Manninen Ismo

Opinnäytetyö

Tietojenkäsittelyn koulutus
Tradenomi (AMK)

2023

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tietojenkäsittely koulutus
Tradenomi (AMK)

Tekijä	Ismo Manninen	Vuosi	2023
Ohjaaja(t)	Marko Leinonen		
Toimeksiantaja	Monialayritys		
Työn nimi	Palo Alto Networks Cortex XDR -järjestelmän Lokien integrointi- ja hallintamahdollisuudet		
Sivu- ja liitesivumäärä	46		

Opinnäytetyön aiheena oli tietoturvatapahtumien hallintajärjestelmän integraatioprosessien dokumentointi. Tavoitteena oli luoda käytännön ohjeistus integraatioprosessista lokitietojen keräämisen ja hallinnan näkökulmasta. Nopea kehittyminen tietoteknologia-aloilla vaatii yrityksiä ymmärtämään uusia palvelukokonaisuuksia, johon opinnäytetyöllä yritettiin löytää ratkaisua. Tutkimuksessa selvitettiin, miten lokitapahtumia kerätään, käsitellään ja tallennetaan sekä mitä mahdollisuuksia järjestelmä tarjoaa. Toimeksiantajayritystä ei yksilöity tässä opinnäytetyössä kilpailuedun ja riskitekijöiden vuoksi.

Opinnäytetyössä käytiin lokilähteiden ja -tapahtumien perusteet läpi niiden rakenteiden ja termistöjen osalta. Lisäksi tutkittiin päätelaitteiden valvonta- ja ohjausjärjestelmän toimintaa sekä osittain siihen liitettävää automaatiojärjestelmää. Tutkimuksella pyrittiin vastaamaan kysymyksiin, mitä, mistä ja miten lokitapahtumia Palo Alto Network Cortex XDR -järjestelmään voidaan liittää. Tutkimuksellisen kehittämistyön menetelmänä käytettiin konstruktiivista tutkimusotetta. Ohjeistuksen luontiin aineistona käytettiin palveluntarjoajan hallinto- ja käyttöönotto-oppaita sekä asiantuntijoiden haastatteluja, jotka analysoitiin teemoittelun avulla. Ohjeistuksen rakenne rakennettiin Kotimaisten kielten keskuksen julkaisemasta viitekehyksestä. Opinnäytetyössä syvennyttiin aiheeseen lokilähdeintegraation toteutuksen näkökulmasta.

Opinnäytetyön tuloksena saatiin luotua toimeksiantajayritykselle käytännöllinen ohjeistus, mikä paransi työntekijöiden ymmärrystä lokilähdeintegraation perusteista. Ohjeistuksen sisältö opastaa lukijalle dataformaattien, tietojoukkojen ja XQL-kyselykielen hallintaa käytännön hallinnassa, ja se tarjoaa perustaidot asiakastyöstä selviytymiseen. Positiivinen tulos oli ohjeistusmalli, joka lisää työntekijöille itsevarmuutta uuden järjestelmän käyttöönotossa ja hallinnassa asiakkaiden lokilähdeintegraatioissa ja niiden ylläpidossa.

Avainsanat: lokitiedot, lokilähde, kerääminen, jäsentäminen, normalisointi, kyselykieli, käytännönohjeistus

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

Business Information Technology
Bachelor of Business Administration

Author	Ismo Manninen	Year	2023
Supervisor	Marko Leinonen		
Commissioned by	Multi-industry company		
Subject of thesis	Palo Alto Networks Cortex XDR system Log integration and management capabilities		
Number of pages	46		

The thesis revolved around documenting integration processes for a security event management system. The objective was to create practical instructions for the integration process from the perspective of collecting and managing log source data. The rapid evolution in technology sectors required companies to understand new service ecosystems, to which the thesis provided insights. The research explained how log events were gathered, processed, stored, and the potential that the system offered. The commissioning company was not explicitly identified in the thesis due to competitive advantages and risk factors.

The thesis covered the fundamentals of log sources and events, including their structures and terminology. It also investigated the functionality of endpoint monitoring and control systems and, to some extent, the associated automation system. The research aimed to answer questions regarding what, where, and how log events could be integrated into the Palo Alto Network Cortex XDR system. The method employed for this research and development work was a constructive research approach. The material for creating the instructions consisted of administrative and deployment guides from the service provider, as well as interviews with experts, which were analyzed thematically. The structure of the instructions was based on a framework published by the Institute for the Languages of Finland.

The thesis resulted in the creation of a practical guide for the commissioning company, which enhanced the employees' understanding of the fundamentals of log source integration. The content of the guide instructed the reader on the practical management of data formats, datasets, and XQL query language, providing the basic skills needed to cope with customer work. A positive outcome was the guide model, which increased the employees' confidence in the adoption and management of a new system in customer log source integrations and their maintenance.

Key words: log information, log source, collection, parsing, normalization, query language, practical instructions

SISÄLLYS

KÄYTETYT LYHENTEET

API	Application Programming Interface
BIOC	Behavioral Indicators of Compromise
CEF	Common Event Format
CSV	Comma-separated values
EDR	Endpoint Detection and Response
IOC	Indicators of Compromise
IT	Information Technology
IOT	Internet of Things
JSON	JavaScript Object Notation
LEEF	The Log Event Extended Format
PANW	Palo Alto Networks
SIEM	Security Information and Event Management
SOC	Security Operations Center
SYSLOG	System Logging Protocol
XDR	Extended Detection and Response
XSIAM	Extended Security Intelligence and Automation Management
XSOAR	Security Orchestration, Automation and Response

1 JOHDANTO

1.1 Opinnäytetyön aihe

Yhteiskunnan ja yritysmaailman digitalisoitumisen myötä kyberuhkien määrä on kasvanut huomattavasti. Suojelupoliisin ja Traficomin mukaan kyberhyökkäykset ovat kasvaneet ja erityisesti kohdistetut hyökkäykset valituille organisaatioille ovat yleistyneet (Marjatta 2024). Viime aikoina on havaittu uusi trendi, jossa Suomen .fi-verkkotunnusten alla on ilmestynyt ammattimaisia huijaussivustoja, joissa sivustot ovat kohdistaneet hyökkäyksensä verkkopankkitunnusten varastamiseen. Tämän tyypin hyökkäyksillä tehdään merkittävää taloudellista ja inhimillistä vahinkoa. (Kyberturvallisuuskeskus 2023a.) Kyberturvallisuuskeskus, joka on liikenne- ja viestintävirasto Traficomin alainen viranomainen, vahvistaa, että kyseessä on kansainvälinen ongelma: ”Global Information Security Workforcen tekemän tutkimuksen mukaan pelkästään Euroopassa tulee olemaan vuoteen 2022 mennessä 350 000 kyberturvallisuusammattilaisen saatavuusvaje” (Kyberturvallisuuskeskus 2020a, 14).

Opinnäytetyön aiheena on PANW Cortex XDR -lokitapahtumien integraatioprosessin ohjeistus. Palvelun valmistaja tarjoaa yrityksille Cortex-nimistä palvelukokonaisuutta. Tämä palvelukokonaisuus on rakennettu useasta eri tietoturvaohjelmistosta yhdeksi ohjelmistoratkaisuksi. Palvelukokonaisuuden ominaisuuksiin kuuluu uhkien havaitseminen, ennaltaehkäisy, hyökkäyspinnan hallinta ja erilaisten tietoturva-automaatioiden käyttö. Kaikki nämä toiminnot on integroitu yhteen alustaan, mikä tekee tietoturvan hallinnasta tehokkaampaa ja yhtenäisempää. (Palo Alto Networks 2019.) Cortex XDR eli laajennettu päätelaitteiden tunnistus ja vastaus -järjestelmä on palvelukokonaisuus, jolla kerätään, hallitaan ja analysoidaan tietoa useista eri lokilähteistä, kuten verkkolaitelokeista, palvelinlokeista tai päätelaitelokeista. Cortex XDR:n avulla voidaan integroida muiden tietoturvapalveluiden lokitapahtumia ja käyttää niitä yhdessä muiden Cortex-palveluiden kanssa. (Palo Alto Networks 2023a.)

Aihe on itsessään erittäin tärkeä ja mielenkiintoinen, minkä vuosi sen ympäriltä löytyy monipuolisesti myös erilaisia opinnäytetöitä. Esimerkiksi Rissasen (2012)

tekemä opinnäytetyö käsittelee integraatiota verkkotoimintojen konfiguroinnin näkökulmasta. Uutta palomuuria varten yritykseen rakennettiin laboratorioympäristö, jossa Palo Alton palomuuria voitiin testata ja konfiguroida erillään yrityksen omasta sisäverkosta. Vastaavanlainen opinnäytetyö lokilähteiden integraatiosta on tehty toiselle palveluntarjoajalle, ja siinä käsitellään muun muassa Atlassian-tuotteiden lokitapahtumien keräämistä ja lähettämistä Splunk-nimisen valmistajan tarjoamaan SIEM-järjestelmään (Niiranen 2018).

1.2 Toimeksianto

Tietoteknologia-aloilla lokitiedot ovat aina olleet erittäin keskeisessä asemassa. Lokitiedot vastaavat, mitä, miksi ja milloin jotain on tapahtunut, minkä vuosi lokien keräämisessä on yleensä jokin tarve taustalla, josta halutaan saada tietoa. Järjestelmiin saattaa syntyä virheitä tai virhetilanteita, jolloin lokitiedoilla varmistetaan niiden laatu, ajankohta ja oikeellisuus. (Viestintävirasto 2016, 2.) Koska kehittyminen on nopeaa alalla, on myös uusien palvelukokonaisuuksien dokumentointi ja haltuun ottaminen haastavaa käytännön tasolla, mikä todennäköisesti saattaa olla syy osaajapulaan. Halunen pohtii, että osaajapula voi johtua siitä, ettei pysytä ympäristön muuttumisen perässä tai ettei osata tunnistaa tarvittavaa osaamista alalle (Petäjäkangas 2023). Toimeksiantajayritys onkin kiinnostunut kehittämään tätä osa-aluetta, minkä vuoksi tällä opinnäytetyöllä pyritään rakentamaan selkeä ja kokonaisvaltainen ohjeistus käytännönläheisyyttä silmällä pitäen.

Opinnäytetyön päämääränä on auttaa lokienkäsittelystä kiinnostuneita henkilöitä ymmärtämään ja hallitsemaan käytännöntasolla tietoturvatapahtumien hallintajärjestelmää ja siihen liittyviä lokien integraatioprosesseja. Työ toteutetaan laadullisena tutkimustyönä, joka pyrkii ymmärtämään tutkittavan kohteen ominaisuuksia ja merkityksiä (Lähdesmäki ym. 2021c). Tämä opinnäytetyö keskittyy uuden tietotekniikan käyttöönottoon ja hallintaan tutkimuksellisen kehittämistyön kautta, jossa samalla luodaan Cortex XDR -järjestelmän lokienhallinnasta ohjeistus toimeksiantajayritykselle. Ohjeistuksen avulla yrityksen henkilöstöä pystytään perehdyttämään paremmin ohjelmiston haltuunotossa, jolloin yritys saa enemmän tukea ja edellytyksiä tuleville asiakaspalveluille. Ohjeistuksen luomiseksi tutkitaan PANW:n tarjoamasta dokumentaatiosta, millaisia lokilähteitä palveluun

voidaan liittää ja miten lokitietoja voidaan hallita sekä hyödyntää järjestelmän avulla, josta lopulta koostetaan käytännönläheiset ohjeet toimeksiantajalle heidän parhaaksi katsomallaan tavalla. Työskentelyn parissa kuullaan toimeksiantajan asiantuntijoita, millaisia tarpeita ja toiveita heillä on ohjeistuksen mallista sekä mihin ihannetavoitteeseen pyritään tuotoksen avulla.

Prosessikehittämiseen liittyvät suunnitelmat ja toteutukset koetaan strategisena kilpailuetuna sekä riskitekijänä, minkä vuoksi opinnäytetyön toteuttaminen ja sen tarkat tulokset ovat osa yrityksen liikesalaisuuksia. Tämän vuoksi toimeksiantajayritystä, sen henkilöitä ja prosessiketjuja ei tulla yksilöimään tässä opinnäytetyössä. Tietoturva-aiheisessa opinnäytetyössä yrityksen nimen, henkilöiden ja tuotantoprosessien paljastamatta jättäminen on tärkeää useista syistä. Ensinnäkin yksityisyyden suoja on keskeinen tekijä. Yrityksen nimen tai tuotantoprosessien paljastaminen voi altistaa yrityksen merkittäville kyberuhkille, jotka voivat johtaa tuotannon keskeytymiseen, taloudellisiin menetyksiin ja asiakastietojen vaarantumiseen (Hillary 2023). Toiseksi prosessien avoimuus voi paljastaa päätöksentekoon liittyviä tietoja ja auttaa tunnistamaan prosessien sisällä tai välillä olevat pullonkaulat (IBM 2023b). Lopulta kyberrikollisuuden suuri kasvu on johtanut siihen pisteeseen, että organisaatiot ovat haluttomia julkaisemaan tietoja hakkerointitapauksista, mikä rajoittaa saatavilla olevia tietoja kyberturvallisuuden riskeistä (Cremer ym. 2022, 718–719).

1.3 Työn tavoitteet ja tutkimuskysymykset

Internetissä on nykyään kytketty monenlaisia laitteita, kuten verkkolaitteita (hubit, kytkimet, reitittimet, sillat, portit, modeemit, toistimet ja tukiasemat), matkapuhelimia ja tietokoneita. Kaikki nämä laitteet tuottavat lokitietoja, jotka ovat tärkeitä tietolähteitä järjestelmän toiminnan ymmärtämiseksi. Lokitiedot, usein kutsuttuna ”lokit”, ovat tietokonejärjestelmän tapahtumien kirjauksia, jotka voivat tapahtua käyttöjärjestelmässä tai muussa ohjelmistossa. Ne ovat olennaisia ongelmien vianmäärityksessä ja tarkastuksessa. (Kyberturvallisuuskeskus 2023b.)

Opinnäytetyöllä pyritään selvittämään, miten eri palveluntarjoajien lokitietoja liitetään Cortex XDR -järjestelmään ja mitä järjestelmällä voidaan tehdä lokitapahtumien kanssa. Opinnäytetyön tavoitteena on tuottaa kattavaa käytännönläheistä

tietoa lokilähdeintegraation prosessista ja siihen liittyvän järjestelmän käytöstä. Tuotoksen ohessa aktivoidaan organisaatiolle toimiva PANW Cortex XDR -testiympäristö, jossa voidaan harjoitella integraatioprosesseja sekä testata tulevan ohjeistuksen toimivuutta. Ohjeistuksesta pyritään rakentamaan selkeä ja helppolukuinen dokumentaatio, jolla saadaan työntekijät oppimaan integraatioprosessin avaintekijät ja viitekehykset.

Opinnäytetyön päätutkimuskysymys on:

- Miten lokitapahtumia tuodaan, käsitellään ja tallennetaan yrityksen hankkiman PANW Cortex XDR -järjestelmän avulla?

Tukikysymykset ovat:

- Millaisia käytäntöjä ja haasteita lokitapahtumien käsittelyyn liittyy?
- Miten lokitietoja voidaan suodattaa ja muokata?

Päätutkimuskysymys on erityisen tarkastelun kohteena, koska se määrittää, miten Cortex XDR -järjestelmä hyödyntää innovatiivisia ratkaisuja lokitietojen hallitsemiseksi ja hyödyntämiseksi. Cortex XDR on ollut kaikkien yritysten saatavilla vuodesta 2019 lähtien, joten kyseessä on tuore palvelukokonaisuus, josta löytyy seuraavan sukupolven kyvykkyyksiä tietoturvauhkien havaitsemiseen ja torjuntaan (Palo Alto Networks 2019). Tämän kysymyksen avulla voidaan osoittaa, millaisesta tietokokonaisuudesta lokienhallinta ja -käsittely koostuu, kun tarkastellaan integraatioprosessin vaiheita alusta loppuun. Opinnäytetyön tukikysymykset ovat tärkeitä, koska lokitietojen monimuotoisuus ja erilaiset standardit vaativat joustavia ratkaisuja niiden yhdistämiseen ja muuntamiseen. Kysymykset auttavat myös selvittämään, mitä työkaluja ja toimintoja järjestelmä tarjoaa lokitietojen eheyden ja saatavuuden näkökulmasta. On olemassa tilanteita, että lokitapahtumia ei voida hyödyntää sellaisenaan asiakkaan ympäristöstä, jolloin niitä täytyy usein muokata, yhdistää tai täydentää tapahtuman laadun varmistamiseksi.

2 JÄRJESTELMÄINTEGRAATIO JA KYBERTURVALLISUUSRATKAISUT

2.1 Tietoturva

Tietoturva muodostaa olennaisen osan tämän päivän digitaalista ympäristöä. Käsitteenä tietoturva viittaa tiedon säilyttämiseen kolmessa pääpiirteessä: sen saatavuudessa, luottamuksellisuudessa ja eheydessä. Tietoturva kattaa tiedon suojelemisen niin lepotilassa kuin sen siirron eri laitteiden välillä. Tietoturvaan liittyviä osa-alueita ovat muun muassa työasemien, palvelinten ja tietokoneverkon suojaaminen, lisäksi ympäristön ja sovellusohjelmien turvallisuus muodostavat keskeisen osan kokonaisuudesta. (Kyberturvallisuuskeskus 2020b.)

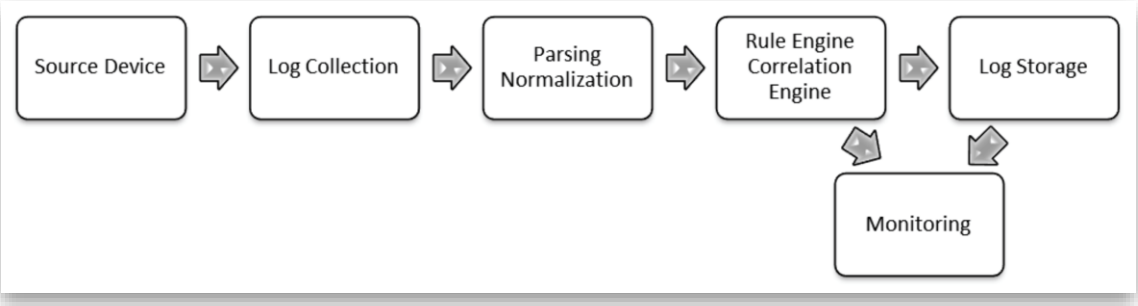
Tietoturvan perusperiaatteet voidaan tiivistää CIA-malliin (kuvio 1), joka on laajasti käytetty periaate tietoturvassa. Luottamuksellisuus (Confidentiality) tarkoittaa, että ainoastaan ne henkilöt, joilla on siihen oikeus, voivat käsitellä tietoa. Eheys (Integrity) merkitsee sitä, että tiedon alkuperäisyys säilyy, eikä se muutu tahattoman tai hyökkäyksen seurauksena. Mahdolliset muutokset tietoon tulisi myös pystyä havaitsemaan. Saatavuus (Availability) puolestaan takaa, että tiedot ja tietojärjestelmät ovat niiden käyttöoikeuden omaavien henkilöiden tai laitteiden käytettävissä, kun he niitä tarvitsevat. (Kyberturvallisuuskeskus 2020b.)

Kuvio 1. CIA-malli (Walkowski 2019)

Tietoturvan kannalta lokitiedot ovat keskeisessä asemassa. Ne tarjoavat yksityiskohtaisen tilannekatsauksen, mitä, milloin ja miksi on tapahtunut. Lokitietoja kerätään monista eri lähteistä, kuten tietokonejärjestelmistä, verkkolaitteista ja mobiilipalveluntarjoajilta. Nämä tiedot siis auttavat varmistamaan järjestelmän normaalin toiminnan ja tunnistamaan mahdolliset poikkeamat. Lisäksi lokitietojen avulla voidaan seurata järjestelmän käyttöä ja tiedonkulkua, mikä on erittäin tärkeää henkilötietojen tai muiden luottamuksellisten tietojen käsittelyssä (Kyberturvallisuuskeskus 2023b.) Yritykset ja henkilöt käyttävät erilaisia teknologioita ja järjestelmiä tietojen käsittelyyn ja säilyttämiseen. Näiden tietojen suojaaminen on välttämätöntä niin yksityisyyden, liikesalaisuuksien kuin lainsäädännönkin näkökulmasta. (Kyberturvallisuuskeskus 2020b.)

2.2 Lokilähdeintegraatio

Opinnäytetyön keskeisin käsite on lokilähdeintegraatio (kuvio 2). Lokienlähdeintegraatio on tapahtumasarja, jossa kerätään, muokataan, tallennetaan ja analysoidaan lokilähteistä tulevia lokitapahtumia keskitetyssä lokienhallintajärjestelmässä. Lokitapahtumien avulla seurataan sovellusten ja infrastruktuurin suorituskykyä, turvallisuutta ja tiedon saatavuutta. (Viestintävirasto 2016, 10.)



Kuvio 2. Lokilähdeintegraatio (González-Granadillo, González-Zarzosa & Diaz 2021)

Lokilähde on tietolähde, joka tuottaa lokitapahtumia eli tietojärjestelmän tapahtumia, jotka kirjataan lokitiedostoon (em. lokit) (IBM 2023a). Esimerkiksi palomuurit tai tunkeutumisenestojärjestelmät kirjaavat turvallisuuteen liittyviä tapahtumia, kun taas kytkimet tai reitittimet kirjaavat verkkoon liittyviä tapahtumia (Kybertur-

vallisuuskeskus 2023b). Lokilähteitä ovat myös sovellukset, palvelimet, tietokannat, käyttöjärjestelmät ja laitteet, jotka tuottavat lokitietoja omasta toiminnastaan (TEK-TOOLS 2020). Kaikille ominaista on lokitapahtumien sisältö eli lokiviestit, jotka sisältävät hyödyllistä tietoa tapahtumasta, kuten esimerkiksi aikaleiman, tapahtuman, tekijän, lähteen, kohteen, ja niin edelleen (Viestintävirasto 2016, 4).

Lokitapahtumien keräämisessä lokitapahtumat toimitetaan keskitettyyn lokienhallintajärjestelmään (Viestintävirasto 2016, 8). Tämä voidaan tehdä esimerkiksi lokitiedostojen replikoinnilla, API:lla tai suoralla lokitapahtumien kirjoittamisella lokienhallintajärjestelmään. Lokien keräämisessä tai niiden lähettämisessä voidaan käyttää erilaisia työkaluja, kuten agentteja, agentittomia ratkaisuja sekä kolmannen osapuolen palveluita. Keräämisen yhteydessä lokitapahtumia myös suodatetaan (TEK-TOOLS 2020). Suodatus tarkoittaa lokitapahtumien sisällyttämistä tai poissulkemista lokiviestin sisällön perusteella (Chuvakin, Schmidt & Phillips 2013, 9).

Lokitapahtumien muokkauksessa puhutaan yleisesti lokiviestien jäsentämisestä ja normalisoinnista. Jäsentäminen (Parsing) käsittelee ”raakalokitapahtumia” eli ei eroteltujen lokiviestien ottamista ja ominaisuustietojen poimimista niistä eri tietokenttiin. Jäsentämisessä siis erotellaan lokitapahtuman viestisisällöt erillisiksi viestikentiksi, jotka listataan hauissa tietokenttien alapuolelle. Näin voidaan luoda paremmin lokiviestin tietoihin perustuvaa analysointia ja raportointia. Normalisointi tarkoittaa, että siinä poimitaan lokitapahtumasta jäsennellyt viestikentät, jotka muunnetaan yhteisesti sovittuun muotoon (Chuvakin ym. 2013, 122, 148). Toisin sanoen lokiviesti tai tietokenttä muunnetaan mielekkäämmäksi informaatioksi tai tietomuodoksi. Esimerkiksi lokiviesti voi sisältää "ID = 6856" -kohdan. Tämä voi tarkoittaa esimerkiksi kirjautumisvirhettä, joten normalisointivaiheessa tämä numerosarja muutetaan tekstimuotoon ”Login Failure”, joka on paljon informatiivisempi (Chuvakin ym. 2013, 146).

Lokien tallennuksessa lokitiedot säilytetään keskitetyssä tietovarastossa. Lokien tallennuksessa voidaan käyttää erilaisia ratkaisuja, kuten relaatio- tai dokumenttitietokantoja, tiedostopohjaisia järjestelmiä tai pilvipalveluita. Käytännössä loki-

tallennus tarkoittaa tietojärjestelmän tapahtumien tallentamista ja seurantaa käytettävän lokitiedoston luomista. (TEK-TOOLS 2020; Valtiovarainministeriö 2009, 13.)

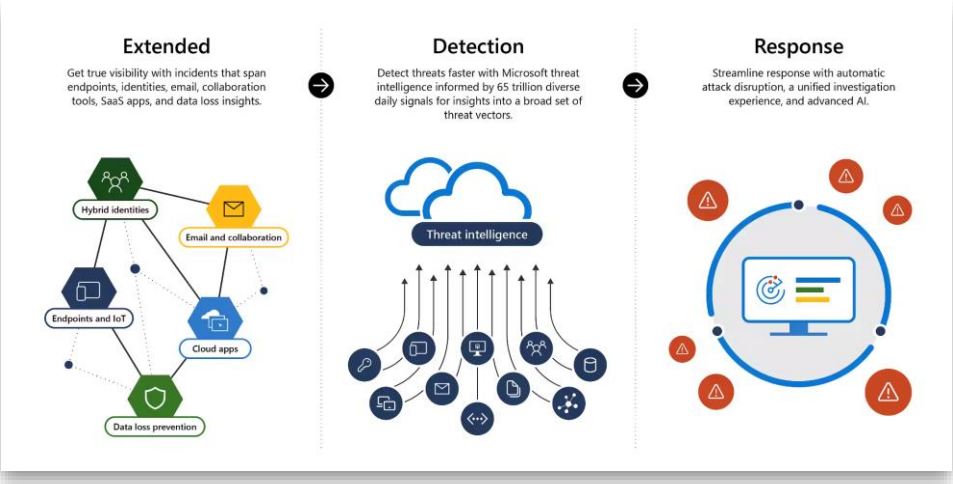
Lokien analysointi tarkoittaa lokitietojen läpikäyntiä ja tarkastelua mahdollisten tietoturvaongelmien ja muiden poikkeamien havaitsemiseksi. Analysoinnin avulla tunnistetaan ja ratkaistaan ongelmia, optimoidaan resursseja, havaitaan poikkeamia ja uhkia sekä tuotetaan raportteja ja hälytyksiä. (Valtiovarainministeriö 2009, 47.) Lokien analysointiin tarvitaan uusia menetelmiä ja työkaluja, joiden avulla monimuotoisista lokilähteistä kertynyt data voidaan järjestää ja analysoida tehokkaasti (Kyberturvallisuuskeskus 2023b, 10–11).

2.3 Cortex XDR

Yritykset käyttävät päätelaitteiden tunnistamiseen ja hallintaan EDR-ratkaisuja (Endpoint Detection and Response) tietojärjestelmiensä suojaamiseksi kyberuhkilta. Se on osa nykyaikaista tietoturvaa, joka yhdistää ennaltaehkäisevän suojauksen jatkuvaan havainnointiin ja reagointiin. EDR:n avulla voidaan nopeasti havaita, analysoida, estää ja torjua käynnissä olevia prosesseja ja hyökkäyksiä. Se hyödyntää pilvipohjaista lähestymistapaa saadakseen välittömästi uusimmat uhkatiedot ja seuraa jatkuvasti kaikkia tiedostoja ja sovelluksia, jotka tulevat verkkoon. EDR:n avulla voidaan merkittävästi parantaa tietoturvaa ja nopeuttaa uhkien havaitsemista ja korjaamista. (Cisco 2023.)

Kyberrikolliset ovat kehittäneet uusia strategioita, mikä vaikeuttaa tietomurtojen havaitsemista ja torjumista. Tämä vaatii entistä parempia suojakeinoja. Monet organisaatiot hyödyntävät XDR-ratkaisuja (Extended Detection and Response) turvatakseen sekä tunnetut että tuntemattomat uhat. Esimerkiksi Microsoft tarjoaa laajan valikoiman tietoturvaratkaisuja, kuten Microsoft 365 Defender ja Azure Defender. Näillä suojataan päätelaitteita, identiteettejä ja pilviympäristöjä. Microsoft 365 Defender on älykäs XDR-ratkaisu (kuvio 3), joka luo yhtenäisen näkymän identiteetteihin, päätelaitteisiin, sähköpostiin, sovelluksiin ja pilvipalveluihin. Se on integroitu osaksi Windows-käyttöjärjestelmää ja muihin Microsoftin turvatuotteisiin, kuten SIEM- ja SOAR-ominaisuuksiin sekä Outlookiin, Teamsiin,

SharePointiin ja Exchangeen. Tämä mahdollistaa mukautetun hälytysten analysoinnin ja tarjoaa kattavan suojan päätelaitteille. (Microsoft 2023.)



Kuvio 3. Microsoftin laajennettu havaitseminen ja reagointi (Microsoft 2023)

XDR-ratkaisu eroaa perinteisestä EDR-ratkaisusta siten, että se hyödyntää koneoppimista kaikissa yrityksen tiedon lähteissä, kuten verkko-, pilvi- ja päätelaitetiedoissa, tunnistaakseen uhkat ja reagoidakseen niihin ennaltaehkäisevällä tavalla. Cortex XDR käyttää Data Layer -dataa eli koottua tietovarastoa tarjotakseen pilvipohjaisen tallennuksen asiakasorganisaation sisällä, joka sisältää kaikki Cortex XDR:ään syötetyt lähteet, kuten päätelaitelokit, palomuurilokit, pilvilokit tai kolmannen osapuolen lokilähteet. Sovellus tarjoaa täyden näkyvyyden kaikkiin tietoihin Data Layerissa, ja sen avulla voidaan tutkia hälytyksiä, toteuttaa korjaustoimenpiteitä ja määritellä politiikkoja tulevaisuuden haitallisen toiminnan havaitsemiseksi. Tämä mahdollistaa myös välittömät toimenpiteet, joka antaa mahdollisuuden ennaltaehkäisevien sääntöjen määrittämiseen hyökkäysten estämiseksi. (Palo Alto Networks 2023a.)

Lokien yhdistäminen XDR:n avulla tehostaa havainnointia ja nopeuttaa reagointiaikaa vähentämällä manuaalisen analyysin tarvetta eri mittauspisteissä. Tietojen yhdistäminen palomuureista ja päätelaitteista antaa sensoritiedot yhtenäisessä näkymässä, ja jokainen sensori lisää näkyvyyttä sekä analyysikapasiteettia. Esimerkiksi, kun yhteys havaitaan sekä palomuurin että päätelaitteen kautta, päätelaite voi tarjota tietoa prosesseista ja tapahtumaketjusta. Samaan aikaan

palomuuri voi tarjota tietoa yhteyden aikana siirretystä datamäärästä ja eri sovellustunnisteista. (Palo Alto Networks 2023a.)

2.4 Cortex XSOAR

Cortex XSOAR on suunniteltu tukemaan tietoturvaoperaatiokeskuksia (SOC) tietoturvapoikkeamien standardoinnissa ja automatisoinnissa, jolla nopeutetaan tietomurtojen käsittelyaikoja. XSOAR yhdistää yli 700 tuotetta ja palvelua tarjoten “playbook”-ratkaisuja eli automaatioita, jotka kattavat useita toimintamalleja, tuotteita ja käyttötapauksia. Nämä mahdollistavat standardoidun, automatisoidun ja koordinoidun vastauksen erilaisiin tietoturvatuotteisiin. Cortex XSOAR:n avulla voidaan esimerkiksi luoda, päivittää ja poistaa “lippuja” eli tikettejä suoraan Cortex XSOAR -komentoriviä hyödyntäen. Tarvittaessa tikettejä voidaan myös rikastaa tapaukseen liittyvillä lisätiedoilla. XSOAR toimii pääasiassa tietoturva-analyytikoille työkaluna, joka tarjoaa mahdollisuuden luoda automaatioita tapausten ja uhkien hallintaan sekä niiden jatkokäsittelyyn. (Palo Alto Networks 2023b.)

Cortex XDR ja Cortex XSOAR ovat kaksi voimakasta tietoturva-alustaa, jotka yhdistämällä saadaan useita merkittäviä etuja tietoturvan hallinnassa ja torjunnassa. Esimerkiksi näiden avulla voidaan vähentää hälytysten turhaa toisteisuutta ja keskittyä yrityksen kannalta merkittäviin uhkiin ja riskeihin, mikä tekee tietoturvan hallinnasta paljon mielekkäämpää ja tarkoituksenmukaisempaa. Cortex XDR tarjoaa automatisoituja toimintoja, kuten valmiita tietoturva-automaatioita. Toiminnot, kuten tiedostojen estäminen, karanteeniin asettaminen ja päätelaitteiden eristäminen, voivat käynnistyä heti havaittujen uhkien vallitessa tai Cortex XSOAR -käyttöliittymän kautta. Tämä nopeuttaa tietomurtoon reagointia ja vähentää manuaalisten toimenpiteiden tarvetta. Rikastetun uhkatiedustelun avulla voidaan hyödyntää omia ainutlaatuisia uhkatiedustelupolitiikkoja parantaen hälytysten tarkkuutta ja laatua. (Cross 2021.) Näin ollen järjestelmien avulla voidaan tunnistaa ja priorisoida tietoturvauhkia nopeammin ja tarkemmin, miksi näiden palvelujen käyttöönotosta on paljon hyötyä eri yrityksien tietoturvassa.

3 TUTKIMUSASETELMA

3.1 Tutkimuksellinen kehittämistyö

Opinnäytetyössä käsitelty lokienhallintaohjeistus toteutetaan käytännössä organisaatiolle, jolloin työ tulkitaan kehittämistutkimuksena. Opinnäytetyön päämääränä on ymmärtää Cortex XDR:n laatua, ominaisuuksia ja merkityksiä kokonaisvaltaisesti, jolloin kyseessä on laadullinen tutkimus (Lähdesmäki ym. 2021c). Tutkimuksella pyritään ratkaisemaan käytännön ongelma ja samalla tuottamaan ammattialalle uutta tietoa (Humak 2022). Kehittämistutkimus tarkoittaa uuden tiedon rakentamista joko tutkimuksen tai käytännön kautta ja sen hyödyntämistä uusien tai olemassa olevien tuotteiden, tuotantotapojen, prosessien tai järjestelmien luomiseen tai niiden merkittävään parantamiseen (Anttila 1998). Kehittämistutkimuksen tulokset eivät välttämättä aina ole yleistettävissä, koska ne perustuvat yksittäistapauksiin. Opinnäytetyössä kerrottua ohjeistusta voidaan kuitenkin tässä tapauksessa hyödyntää myös muiden organisaatioiden ohjeistusmallina, kun ympäristöt ovat luotu samoilla palvelukokonaisuuksilla eli hankittu Cortex XDR Pro gigatavua ja päätelaitetta kohden olevat lisenssit.

Kehittämistutkimuksen valinta lähestymistavaksi perustuu sen kyvykkyydestä yhdistää sekä akateeminen kirjallisuus että työpaikalla kerätty tieto. Tavoitteena on tuottaa ohjeistus, joka on suunnattu erityisesti ammattialalle ja yritykselle. Ohjeistus koskee Cortex XDR -järjestelmän lokilähdeintegraatiota ja sen hallintaa. Kehittämistutkimuksessa voidaan käyttää monenlaisia menetelmiä, kun tavoitteena on tuottaa konkreettisia parannuksia tai mahdollistaa uusia ratkaisuja. Kehittämistyössä on tyypillistä käyttää useita menetelmiä eri vaiheissa, mikä lisää tutkimusprosessin joustavuutta ja monipuolisuutta. (Humak 2022.)

Valitsin kehittämistutkimukselle konstruktiivisen tutkimusmenetelmän lokilähdeintegraation ohjeistuksen kehittämiseen, koska tavoitteenani on rakentaa ongelman ratkaiseva tuotos, eli uusi toimintatapa tai -malli. Konstruktiivinen tutkimus tarjoaa mahdollisuuden luoda jotain uutta ja innovatiivista, mikä sopii erinomaisesti teknologiaan liittyvään kehitystyöhön. Konstruktiivinen tutkimusote mahdollistaa organisaatioiden liiketoimintaongelmien syvällisen ja kriittisen ana-

lyysin tarjoten teoriaan pohjautuvaa tietämystä, joka on puolueettomampaa ja syvällisempää kuin konsulttien auttaen kaventamaan käytännön ja tutkimuksen välistä kuilua (Lukka 2001). Vaihtoehtoisia tutkimusmenetelmiä olisivat olleet esimerkiksi toimintatutkimus ja tapaustutkimus.

Opinnäytetyön tarvittava tutkimusaineisto koostuu Cortex-järjestelmän hallintaoppaista, jotka liittyvät lokitapahtumien keräämiseen ja käsittelyyn. Dokumentteja ovat esimerkiksi Cortex-järjestelmän käyttöohjeet, lokitapahtumalähteiden tekniset tiedot, lokitapahtumien analysointiin liittyvät raportit ja artikkelit. Palveluntarjoajan aineiston käyttäminen ohjeistuksen luontiin on järkevää useista syistä. Ensinnäkin ne ovat valmiita dokumentteja, jotka sisältävät jo tarvittavat tiedot Cortex XDR -järjestelmän käytöstä ja hallinnasta. Tämä säästää aikaa ja resursseja, koska minun ei tarvitse tuottaa uutta aineistoa tutkimuksen aikana, vaan voin luoda ohjeistusta samalla kun perehdyn aineistoon. Toiseksi nämä oppaat ovat luotettavia lähteitä, koska ne ovat tuotettu itse järjestelmän kehittäjien toimesta. Ne tarjoavat tarkat ja ajantasaiset tiedot järjestelmän toiminnoista ja ominaisuuksista, mikä on tärkeää ohjeistuksen toiminnallisuuden kannalta. Kolmanneksi näiden oppaiden käyttö vähentää tekijänoikeuskysymyksiin liittyviä riskejä. Koska oppaat ovat julkisesti saatavilla ja tarkoitettu käyttäjien avuksi, niiden käyttö tutkimusaineistona ei riko tekijänoikeuksia (Lähdesmäki ym. 2014).

Ohjeistusrakenteen yleistiedon keräämiseksi valitsin puolistrukturoidut haastattelut aineistonkeruumenetelmäksi, koska ne mahdollistavat työntekijöiden kokemusten, näkemysten ja asiantuntemuksen hyödyntämisen aiheeseen liittyen (Lähdesmäki ym. 2021a). Menetelmän avulla saan syvällisen ymmärryksen toimeksiantajan lokilähdeintegraation haasteista ja mahdollisuuksista käytännön näkökulmasta. Haastatteluiden avulla pystyn ymmärtämään paremmin yrityksen prosesseja ja tarpeita, mikä auttaa minua suunnittelemaan ohjeistuksen, joka palvelee heidän tavoitteitaan. Vaihtoehtoisia menetelmiä olisivat voineet olla esimerkiksi strukturoidut haastattelut tai kyselyt. Nämä menetelmät voivat olla hyödyllisiä tiettyjen tietojen keräämisessä, mutta ne eivät välttämättä tarjoa samaa syvyyttä ja yksityiskohtaisuutta kuin puolistrukturoidut haastattelut (Humak 2022).

Dokumenttien ja haastatteluiden analysointi tapahtuu teemoittelun avulla. Tämä menetelmä mahdollistaa tutkimusaineiston jakamisen merkityksellisiin teemoihin

ja aihealueisiin, jotka vastaavat tutkimuskysymyksiin (Lähdesmäki ym. 2016). Teemoittelua voidaan käyttää tutkimuksessa, jossa pyritään selvittämään ihmisten näkemyksiä, mielipiteitä, tietoja, kokemuksia tai arvoja. Teemat auttavat järjestämään ja ryhmittelemään tietoja selkeästi, mikä helpottaa niiden ymmärtämistä ja hyödyntämistä. (Caulfield 2023.) Tämän avulla saan rajattua ohjeistuksen laajuutta ja sen rakennetta. Etsin aineistosta selkeitä ohjeistuksen kohteita, joita korostetaan käytännöntasolla, ja jotka nousevat haastatteluissa esiin aiempien lokilähdeintegraatioiden pohjalta. Näin ollen tulevan ohjeistuksen avulla työntekijät ymmärtävät, mitkä toimet ja aiheet ovat tärkeitä hallita lokilähdeintegraatiossa.

Kehittämistehtävän toimintaympäristönä on yritys, joka ylläpitää Cortex-järjestelmän palveluja muille yrityksille tietoturvallisuuden parantamiseksi. Palveluntarjoaja haluaa saada käsityksen siitä, miten se voi toteuttaa lokilähdeintegraatioita Cortex-järjestelmällä, jolloin he tarvitsevat kattavan dokumentaation niin teorian kuin käytännön tasolla asiakaspalvelun tarjoamiseksi. Lokilähdeintegraatiot ovat konsultointipalveluja, joissa yhdistetään eri laitteiden ja sovellusten lokilähteitä keskitettyyn lokientallennusjärjestelmään. Yritysympäristössä työskentelee kattavasti eri alan asiantuntijoita, joille ohjeistus tulee antamaan viitteitä integraatioprosessin työn kulusta, vaiheista ja sisällöstä. Tämän vuoksi ohjeistukseen dokumentoidaan myös asiakastyöhön liittyvää tietoa, jolloin kaikkia ohjeistuksen osia ei voida tietoturvasyistä sisällyttää opinnäytetyön raportille.

3.2 Konstruktiivinen tutkimus

Opinnäytetyössäni sovellan konstruktiivista tutkimusmenetelmää. Tämä menetelmä tarjoaa käytännöllisen viitekehyksen todellisten ongelmien ratkaisemiseen ja uuden tiedon luomiseen. Konstruktiivisen tutkimuksen keskiössä on “konstruktio”, joka viittaa ihmisen luomiin artefakteihin, kuten diagrammeihin, suunnitelmiin, tuotteisiin, organisaatiorakenteisiin tai tietojärjestelmämalleihin (Lukka 2001). Opinnäytetyössäni luon uuden konstruktion – tässä tapauksessa ohjeistuksen. Ohjeistus tulee ratkaisemaan tiedonhankinnan, perehdytyksen ja ajankäytön ongelmat tuottaen arvoa yritykselle sekä käytännön että teorian näkökulmasta. Tutkijana ja kehittäjänä luon ohjeistuksen rakenteen sekä sisällön ja osal-

listun tiiviisti yhteistyöhön työntekijöiden kanssa olemassa olevan tiedon hankkimiseksi. Lukka (2001) suosittelee tämän kaltaista lähestymistapaa sekä käytännön että teorian näkökulmasta, jolloin ongelmanratkaisuprosessit tuottavat runsaasti kokemuksellista oppia ja kontribuutioita.

Konstruktiivinen tutkimus koostuu seitsemästä eri vaiheesta (kuvio 4). Ensin löydetään kehitettävä kohde, josta on mahdollisuus tuntemattomien vaikutusmekanismien ja niiden toiminnan kuvaamiseen eli teoreettiseen kontribuutioon. Selvitetään kohteen laajuus ja tutkimusyhteistyön mahdollisuudet, jonka jälkeen hankitaan monipuolista ymmärrystä aiheesta teorian ja käytännön kautta. Jos kehitettävään kohteeseen löydetään yhteistyöllä ratkaisumalli, luodaan siitä konstruktio, josta siirrytään käytännön toteutukseen eli luomaan haluttua rakennelmaa. Lopulta työ tuottaa jonkinlaisen lopputuloksen, jonka jälkeen alkaa tarkasteluvaihe. Tarkasteluvaiheessa pohditaan, miten lopputulos vastaa suunnitelmia, luotiinko mahdollisesti teoreettisia kontribuutioita, kuinka laajasti ja millä muunnoksilla tuotos voidaan mahdollisesti siirtää muille soveltamisaloille. (Lukka 2001.)

Kuvio 4. Konstruktiivinen tutkimusprosessi (Lukka 2001)

4 TUTKIMUKSEN TOTEUTUS JA TULOKSET

4.1 Tutkimusaineisto, sen hankinta ja analysointi

Opinnäytetyön tarvittava tutkimusaineisto koostuu Cortex-järjestelmän hallinta-oppaista ja asiantuntijahaastatteluista, jotka liittyvät lokitapahtumien keräämiseen ja käsittelyyn. Opinnäytetyön aikana haastateltavana oli muutama toimeksiantajan asiantuntija, joilla on pitkä kokemus IT-alalta ja SIEM-järjestelmien integroimisesta. Heidän kanssaan työskenneltiin koko projektin ajan tiiviissä yhteistyössä niin sisäisissä Cortex XDR töissä kuin asiakastöissäkin, jossa he osallistuivat käytännön toteutukseen ja ohjeistuksen tavoitteen määrittelyyn. Ohjeistuksen paikaksi valitsimme yrityksen sisäisen verkkosivuston, josta tulevaisuudessa aineisto siirretään lähdekoodille ja toiselle palveluntarjoajan alustalle. Haastateltavat kertoivatkin tämän olevan väliaikainen ratkaisu, kunnes uusi alusta on valmis käyttöönotettavaksi.

> "Tekninen dokumentaatio olisi hyvä olla Markdown-muodossa. Ihan ok laittaa Wikii. Vältetään PDF-tiedostojen käyttöä, koska ne vaikeuttavat tulevaisuudessa tietojen siirtoa."

Heidän mielestään työntekijöiden on tärkeää ymmärtää, millaista dataa asiakkaan järjestelmästä tulee. Haastatteluissa nousi myös toistuvasti esiin lokitietojen laadun ja eheyden varmistaminen, että analyytikot saavat oikean käsityksen tapahtumasta tai hälytyksestä. Näiden lisäksi on ymmärrettävä tietojen poimimisen merkitys tapahtumasta, jolloin tulee lähetettyä oikeaa tietoa oikeassa kentässä.

> ”Pitää tietää, mitä integroidaan, että ovatko ne hälytyksiä vai tapahtumia? Asiakkaalta voi tulla erillisiä tapahtumia, johon tarvitsee rakentaa oma logiikka luomaan hälytyksiä. Voi myös tulla suoraa hälytyksiä. Tärkeä ymmärtää, millaista dataa tulee ja ymmärtää sen merkitys, eli että tulee oikeassa muodossa ne kentät. Jos on monta samaa tietoa liittyen yhteen kenttään, pitää luoda niistä lista ja lähettää SOAR:iin. Kaikki hälytyksen tarkastelutoiminnot halutaan SOAR:ssa tehdä, mutta analysti joutuu välillä käydä katsomassa tarkempaa informaatiota SIEM:stä.”

Toisin sanoen integrointivaiheessa on tiedot asetettava oikeisiin tietokenttiin, koska muuten automaatiot eivät anna oikeita tuloksia ja analyytikolle muodostuu enemmän työtä hälytysten jatkoselvittämiseksi. Toimeksiantajalla on käytössä erilaisia tietopohjia, joiden avulla viestitään ryhmille toimenpiteitä esimerkiksi, miten kriittisen sattuman kanssa kannattaa toimia.

> ”Konfiguraation tiedostosta tulee tietoa analyytikoille ja SOAR:lle. Siinä selviää, miten esimerkiksi toimitaan, kun tietynlainen hälytys tulee esiin. Siinä myös määritellään niitä rikastushakuja, joissa on esimerkiksi ne tapahtumakentät.”

Lopuksi kysyin yleisiä haasteita, mihin on törmätty integraatiovaiheissa tai niiden jäljiltä. Syitä on muutamia, kuten epäselkeästi määriteltyjen laitteiden määrä tai paikka, tulosraportointi ja tietojen poiminta.

> ”Scope on huonosti määritelty eli saattaa olla tilanne, että tulee lokia väärästä tenantista. Ohjeistuksessa olisi hyvä olla tietoa, jossa tämän tyyppiset virheet poissuljetaan kaikista lähteistä. Samoin pitää tietää, kuinka paljon integroitavia lähteitä on kyseessä, ettei käy sillä tavalla, että integroidaan 2 palvelinta ja asiakkaalla on 20 käytössä. Scopesta hyvä myös olla dokumentaatio ja arkkitehtuurikuva, jossa varmistetaan lähteiden määrä ja paikka. Olisi hyvä ymmärtää hakujen vaikutus ja virheiden mahdollisuus, kun kerätään tietoa esim. payloadista, joka sisältää paljon eri tietokenttiä. Parempi vaihtoehto olisi käyttää parsittua-kenttää virheiden välttämiseksi.”

Haastattelujen pohjalta integraatiotyöstä selviytymiseen nousee esille kolme pääteemaa: dataformaatit, IT-resurssit sekä uhkamallit ja -menetelmät. Näiden avulla työntekijä ymmärtää tiedonkäsittelyn laitteiden sekä sovellusten välillä, joissa piilee erilaisia haavoittuvuuksia tai riskejä. Cortex XDR:n dokumentaatiossa on myös nostettu esille jäsentelyvirheitä liittyen odotettuihin tietotyyppeihin, kuten CEF, LEEF tai JSON, ja niiden sisältämiin tietoihin, kuten TEXT tai CSV (Palo Alto Networks 2023a). Samoin järjestelmänvalvojille suunnatussa oppaassa on laajasti ja yksityiskohtaisesti kirjoitettu, millaisia IT-resursseja voidaan liittää järjestelmään, miten ne asennetaan, missä muodossa data lähetetään ja mihin tietojoukkoon data lopulta päätyy. Cortex XDR pystyy vastaanottamaan verkkoyhteyslokit, todennuspalvelu- ja tarkastuslokit, käyttö- ja järjestelmälokit, pilviresurssilokit ja muut mukautetut lokilähteet (Palo Alto Networks 2023a). Lopuksi työstä selviytymiseen ja analyytikon työn helpottamiseksi vaaditaan tietämystä tietomurto taktiikoista ja tekniikoista, jotka lisätään hälytyksen tietokenttiin mukaan niin kutsuttuna ”laukaisutietona” (Palo Alto Networks 2023a). Cortex XDR käyttää lähteenä yleisesti tunnettu ATT&CK-sivustoa, jonka löytää osoitteesta https://attack.mitre.org.

4.2 Ohjeistuksen rakenne

Ohjeiden luomisessa hyödynnän Kotimaisten kielten keskuksen julkaisemaa "Ohjeita ohjeiden tekijöille" -sivustoa. Sivuston mukaan laadukkaan ohjeistuksen laatimisessa korostuu kolme keskeistä tekijää. Ensimmäinen niistä on käskymuodon käyttö, joka tekee ohjeista suoraviivaisia ja selkeitä, helpottaen ohjeiden noudattajaa ymmärtämään odotetut toimenpiteet. Käskymuoto on erityisen tärkeä monimutkaisten tai teknisten ohjeiden yhteydessä, missä selkeys on avainasemassa. (Kotimaisten kielten keskus 2023.)

Toinen keskeinen tekijä on olennaisten toimintojen ja vaiheiden tunnistaminen ohjattavalle. Ohjeiden kirjoittajan on ymmärrettävä, mitkä tiedot ovat välttämättömiä ohjeiden käyttäjälle ja mitkä vaiheet tekijän on vähintään suoritettava. Tämä auttaa varmistamaan ohjeiden kattavuuden ja tarjoamaan kaikki tarvittavat toimenpiteet tekijälle. Kolmas keskeinen tekijä on ohjeiden esittäminen selkeästi hahmotettavassa muodossa. Ohjeiden tulee olla jäsenneltyjä ja helposti luettavia, jotta ne olisivat mahdollisimman ymmärrettäviä samalla edistäen uusien asiayhteyksien luomista ja aiempien vahvistamista. Tämä voi tarkoittaa esimerkiksi ohjeiden jakamista selkeisiin osiin tai alaotsikoiden käyttöä eri ohjeosien erottamiseksi toisistaan. (Kotimaisten kielten keskus 2023.)

Ohjeistuksessa tullaan hyödyntämään kaikkia edellä mainittuja tekijöitä. Ohjeistus tulee ohjaamaan lukijaa oikealle tiedonlähteelle, josta lukija voi syventyä kiinnostuksen mukaan kehittämään tietoisuuttaan dataformaateista, IT-resursseista tai uhkamalleista ja -menetelmistä. Päämääränä pidetään käytännönläheistä ohjeistusmallia, jossa konkreettisesti myös havainnollistetaan kuvien avulla integraatioprosessin vaiheita ja kulkua. Ohjeistuksen rakenne jäsennellään prosessivaiheiden mukaan osiin. Lokien keräys, käsittely ja säilyttäminen toimivat pääotsikkoina, jotka sisältävät tarkempia alaotsikoita käytännön prosessista. Alaotsikoissa lukijaa ohjataan käskymuodossa suorittamaan vaadittavia osatehtäviä, jotta kyseisen luvun tavoitteet saavutetaan.

4.3 Lokien kerääminen

Cortex XDR tarjoaa laajan näkyvyyden verkkoliikenteestä, käyttäjien käyttäytymisestä ja päätelaitteiden toiminnasta (kuvio 5). Järjestelmä voi vastaanottaa minkä tahansa muotoisia lokiviestejä niin kutsutussa ”raaka”-muodossa, mutta lokitietomuotona suositellaan lähettämään JSON-, CEF- tai LEEF-tiedostomuotoa tiedon jatkokäsittelyn helpottamiseksi. JSON (JavaScript Object Notation) on kevyt tiedostomuoto, joka on tarkoitettu datan tallentamiseen ja siirtämiseen. Sitä käytetään, kun tietoa lähetetään tietokoneiden välillä, palvelimelta verkkosivulle, yms. Sen syntaksissa tieto esitetään avainarvo-pareina, jossa data erotellaan pilkuilla. JSON:ssa aaltosulkeet pitävät sisällään objekteja ja hakasulut taulukoita. (W3Schools 2023.)

Kuvio 5. Kuvankaappaus liitettävistä lokilähteistä

Yleinen tapahtumamuoto (Common Event Format, CEF) on vakiintunut tiedostomuoto, joka on suunniteltu helpottamaan tietoturvaan liittyvien tapahtumien lokitusta. CEF perustuu syslog-muotoon, jota tukee suurin osa verkkolaitteista ja käyttöjärjestelmistä. CEF käyttää rakenteellista tiedostomuotoa, joka sisältää val-

miiksi määriteltyjä kenttiä, joissa on osatietoa tapahtumasta. CEF koostuu kahdesta osasta: otsikosta ja viestistä. Otsikko sisältää metatietoa, kuten aikaleiman, lähde IP-osoitteen ja laitteen isäntänimen, kun taas viesti sisältää yksityiskohtaiset tietokentät tapahtumasta, kuten tapahtumatyypin, vakavuustason ja muut asiaankuuluvat tiedot. (Watts 2023.) LEEF eli ”Log Event Extended Format” on rakenteellisesti samanlainen kuin CEF. Molemmissa otsikon data erotellaan pystyviivan (|) avulla ja viesti sisältö erotellaan tabulaattorilla.

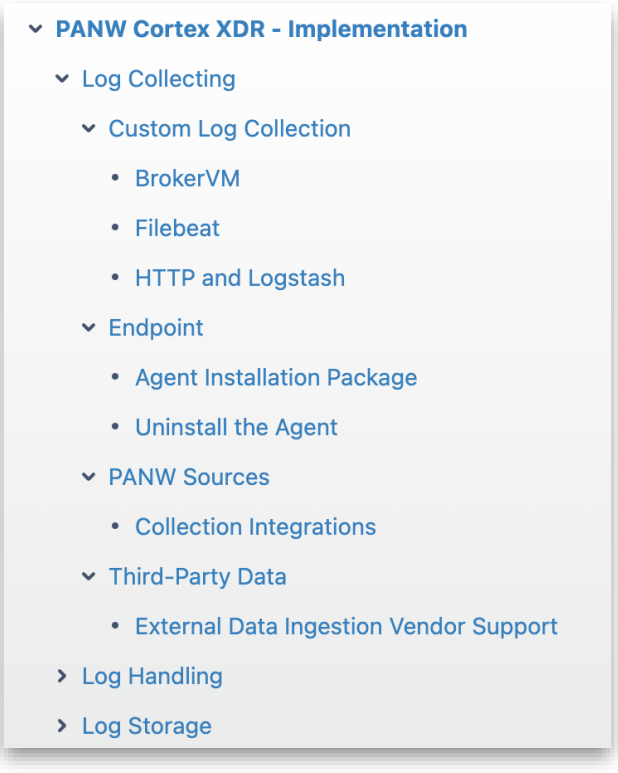
Cortex XDR käyttää käyttöliittymän rinnalle luotua datakerrosta kerätäkseen tietoa ja tarjotakseen pilvipohjaista tallennustilaa Cortex XDR -käyttäjille. Tähän tallennustilaan kerätään kaikki lokitapahtumatiedot tietojoukkoina, jotka tulevat Cortex XDR:ään eri lähteistä, kuten päätelaitteista, palomuureista, pilvipalveluista ja kolmannen osapuolen tietolähteistä. Cortex XDR voi siten analysoida ja yhdistää näitä tietoja, mikä auttaa tunnistamaan ja selvittämään tapahtumien syy-seuraussuhteet loogisessa aikajärjestyksessä. (Palo Alto Networks 2023a.)

Lokien keräämisen kannalta Cortex XDR tarjoaa kattavan tietoturvapalvelupaketin, jota tarkastellaan seuraavaksi. Ensisijaisesti sen analytiikkamoottori hyödyntää verkkotietoja ja päätelaitetietoja havaitakseen ja raportoidakseen automaattisesti mahdolliset uhkat hyökkäyksen jälkeen. Tämä toteutuu tarkkailemalla verkon normaalia ja poikkeavaa toimintaa IOC- ja BIOC-sääntöjen avulla. Cortex XDR tukee myös Palo Alto Networksin seuraavan sukupolven palomuureja, jotka valvovat suojauskäytäntöjä monilla verkon osa-alueilla. Kun laajennetaan suojauskäytäntöjä mobiili- ja etäkäyttäjille Prisma Accessin ja GlobalProtectin avulla, liikennelokit, mukaan lukien IoT-lokit, voidaan siirtää Cortex Data Lakeen, missä Cortex XDR -analytiikkamoottori voi analysoida niitä ja hälyttää epänormaalista toiminnasta. (Palo Alto Networks 2023a.)

Cortex XDR pystyy vastaanottamaan liikennelokit myös ulkopuolisilta palomuuritoimittajilta, esimerkiksi Check Pointilta, ja hyödyntämään analytiikkamoottoria näiden lokiensa tarkasteluun sekä epänormaalin toiminnan hälytysten generointiin tarjoten lisäkontekstin tapahtumille. Cortex XDR -agentit tarjoavat päätelaitteille suojaa ja analysoivat mahdollisia uhkaavia käytöksiä paikallisesti laitteelta. Ne raportoivat päätelaitetoiminnasta tietokerrokseen, jossa sitä analytiikkamoottoria avulla analysoidaan. Tämän jälkeen ulkoisia tai Cortex XDR -hälytyslähteitä

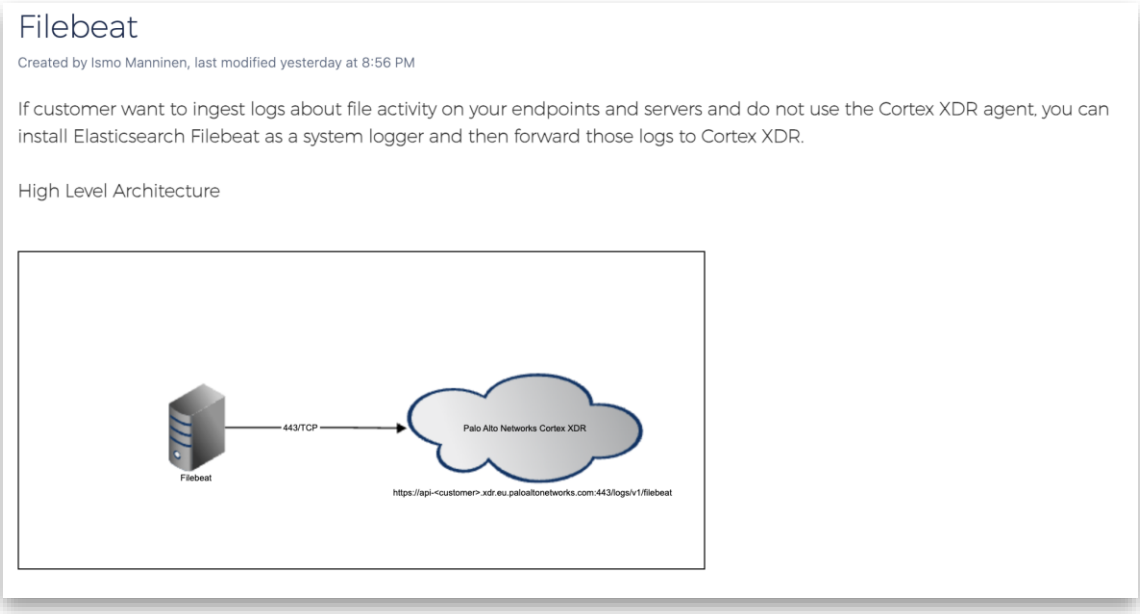
välitetään SOAR:lle API:n avulla, jolloin saadaan automatisoitua toimintoja ja tietoa tapahtumien kulusta SOC:lle jatkokäsiteltäväksi. (Palo Alto Networks 2023a.)

Kuten huomataan, on kyseessä hyvin monipuolinen järjestelmä lokitapahtumien keräämisen näkökulmasta. Lokitapahtumien keräämisestä luotiin ohjeistussivusto nimeltä ”Log Collecting”, jossa järjestelmätyökalujen toiminnot on jaettu kuvion 6 mukaisesti alaotsikoihin. Jokaisen sivuston alussa työntekijälle kerrotaan taustatietoa aiheesta, joka lopulta johtaa käytännönläheisiin ohjeisiin. Ohjeistuksessa erottelin 3 osapuolen lokilähteistä mukautetuista lokilähteistä, sillä ne vaativat enemmän konkreettisia toimenpiteitä toimeksiantajan työntekijöiltä kuin asiakkaalta. Päätelaitteiden agenttien asentaminen ja poistaminen suoritetaan asiakkaan toimesta pääsääntöisesti mutta prosessista haluttiin luoda avunantamisen näkökulmasta ohjeet myös toimeksiantajayrityksen työntekijöille.



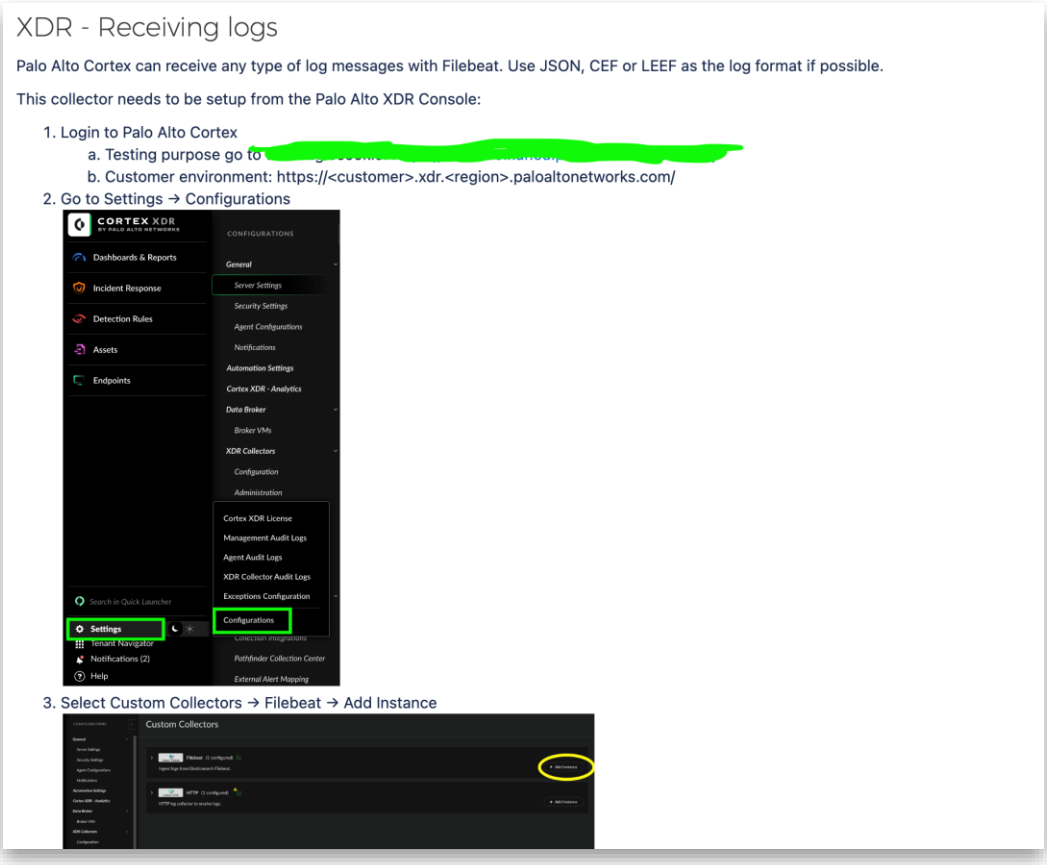
Kuvio 6. Lokikeräyksen ohjeistusrakenne

Jokaisessa alaluokan alussa on johdanto (kuvio 7), jossa lukijalle kerrotaan, millaisessa tapauksessa lokikeräysmenetelmä voi olla hyödynnettävissä. Sen jälkeen osoitetaan arkkitehtuurikuvalla ratkaisumalli, jota voidaan hyödyntää esimerkiksi asiakasdokumentaation arkkitehtuurikuvassa.



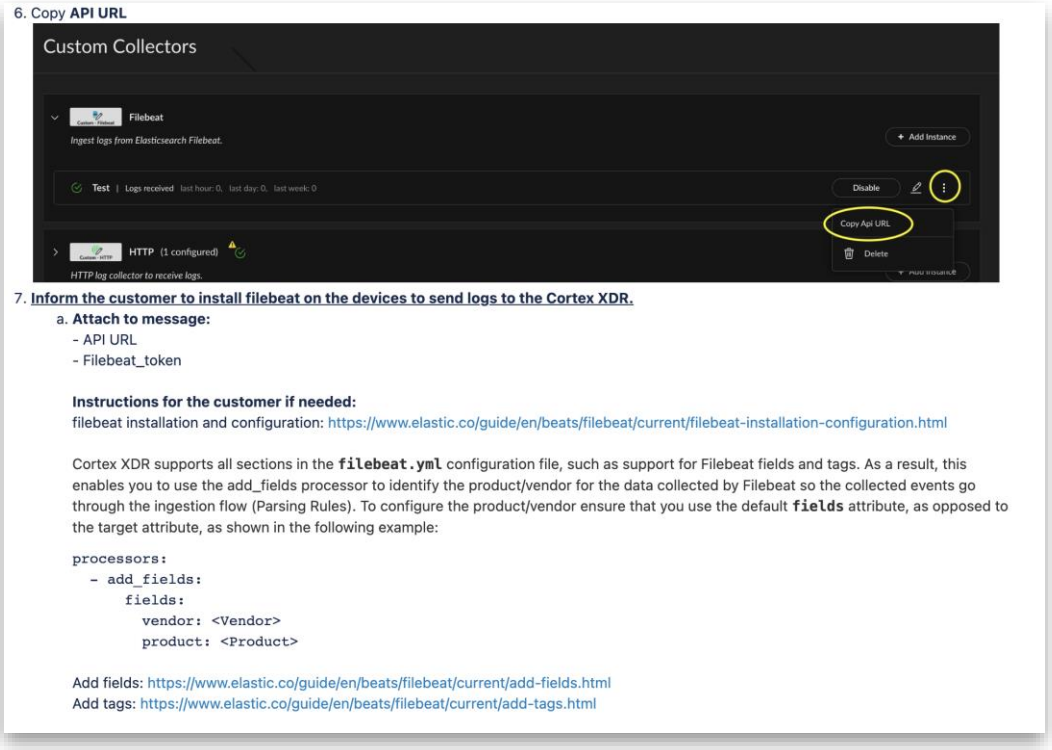
Kuvio 7. Filebeat – johdanto

Näistä siirrytään varsinaiseen käytännön toteutukseen (kuvio 8). Siinä lukijaa ohjataan käskymuodoilla tekemään käyttöliittymässä toimintoja, joiden avulla järjestelmä voi alkaa vastaanottamaan kohdelaitteista lokitapahtumia.



Kuvio 8. Filebeat – käytännönohjeet

Ohjeistus sisältää myös kohtia, joissa asiakkaan on tehtävä tarvittavia muutoksia ympäristöön. Tällaisissa tapauksissa ohjeistuksen noudattajalla ei ole pääsyä kohdejärjestelmään, jossa muutokset on suoritettava. Näissä tilanteissa ohjeiden seuraajalle annetaan tarvittavat tiedot (kuvio 9), jotka hänen tulee kerätä ja välittää asiakkaalle.



Kuvio 9. Filebeat – asiakasohjeistus

4.4 Lokien käsittely

Cortex XDR:ään liittyvien lokitapahtumien käsittely tehdään sen tietohallintavälineessä. Lokiviestien tehokasta käsittelyä varten on ymmärrettävä Cortex XDR:n käyttämän XQL-kyselykielen perusteet. XQL on XML-kyselykieli, joka mahdollistaa monivaiheisen kyselyjen tekemisen tietojoukkoihin kerätyistä lokitapahtumista, jotka on tallennettu järjestelmään. Tietojoukko koostuu erilaisista sarakkeista ja arvoista, ja siihen voidaan ladata lisää lokitietoja CSV-, TSV- tai JSON-tiedostojen muodossa. Jos erityistä tietojoukkoa ei ole määritetty lokien keräämisen yhteydessä, Cortex XDR käyttää oletuksena oletustietojoukkoa nimeltä "xdr_data", joka sisältää kaikki järjestelmän tukemat lokitapahtumat. (Palo Alto Networks 2023a.)

XQL on samanlainen toiminnaltaan kuten muidenkin SIEM ratkaisujen kyselykielet. XQL rakentaa kyselyt vaiheittain, ja jokainen vaihe suorittaa tietyn kyselytoimenpiteen aiemmalle vaiheelle. Vaiheet erotetaan toisistaan pystyviivalla (|). XQL-kyselyn alussa määritellään tietojoukko, kiinnostavat tietokentät ja niihin liittyvät toimenpiteet. Kyselyjä voidaan suorittaa joko tietojoukkoihin, kuten oletuksena oleva "xdr_data", tai ennalta määriteltyihin Preset-joukkohin. Preset-joukoissa yhdistetään XDR-tapahtumat ja kolmannen osapuolen lokit yhteisiin skeemoihin, joita kutsutaan tarinoiksi. Näistä tarinoista yleisimmät ovat "authentication_story" ja "network_story". (Palo Alto Networks 2023d.)

Kyselykielen oppiminen on helppoa, koska jokainen komento (kuvio 10) on jaettu selkeisiin johdanto-, kuvaus- ja esimerkkiosiin Cortex XDR XQL Language Reference -sivustolla. Jokainen komento-ohjeistus alkaa selkeällä syntaksin esittelyllä, joka antaa lukijalle ymmärryksen siitä, miten komentoa tulisi käyttää. Tämän jälkeen seuraa kuvaus, joka selittää komennon merkityksen ja sen, miten se vaikuttaa kyselyn suorituskykyyn. Komento-ohjeistuksen lopussa on käytännön esimerkki, joka näyttää, miten komentoa voidaan käyttää todellisessa tilanteessa. XQL:n avulla lokitapahtumia siis käsitellään sekä sisällytetään niihin informatiivista tietoa analyytikon työn tueksi. Kaikki lokien jatkokäsittely tapahtuu XQL-kyselykielen avulla, jolloin kyselykielen oppiminen ja hallitseminen on kriittinen haaste työntekijälle työstä selviytymiseen.

replace

Syntax

```
replace (<field>, "<old_substring>", "<new_string>")
```

Description

The `replace()` function accepts a string field, and replaces all occurrences of a substring with a replacement string.

Examples

If '.exe' is present on the `action_process_image_name` field value, replace that substring with an empty string. This example uses the if and lowercase functions, as well as the contains operator to perform the conditional check.

```
dataset = xdr_data
| fields action_process_image_name as apin
| filter apin != null
| alter remove_exe_process = if(lowercase(apin) contains ".exe",
                              replace(lowercase(apin),".exe",""),
                              lowercase(apin))
| limit 10
```

See also the trim function example.

Kuvio 10. XQL Replace-komennon ohjeistus (Palo Alto Networks 2023d)

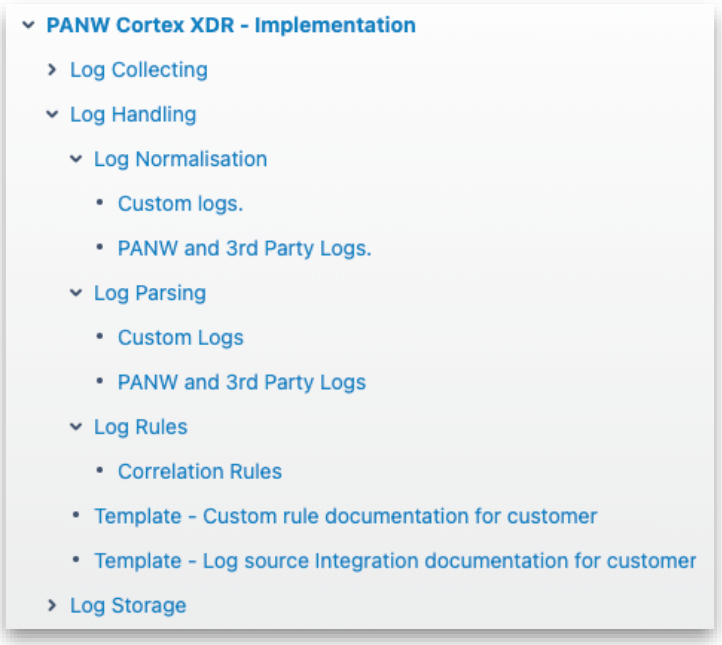
Cortex XDR jäsentelee lähtökohtaisesti kaikki Cortex-järjestelmien ja kolmansien osapuolien lokit automaattisesti, kun lokitapahtumien kerääminen on asennettu Cortex XDR -ohjeistuksen mukaisesti. Lokitapahtumat jäsentyvät ja normalisoituvat xdr_data-tietojoukkoon ja/tai network- sekä authentication-tarinoihin. Palo Alto Network tarjoaa valmiiksi jäsennellyt ja normalisoidut tietojoukot suurten pilvipalveluntarjoajien palveluista, kuten Amazon Web Services, Google Cloud Platform, Microsoft Azure ja Office 365 lokilähteistä. Kuitenkaan kaikki järjestelmälokit eivät ole Cortex XDR:ssä tuettuja, jolloin siitä tarvitsee luoda uusi tietojoukko sekä oma jäsentelysääntö tietojen jäsentämiseksi ja normalisoimiseksi.

Jäsentelysääntöjä luodaan XQL-kyselykielen avulla, jolla voidaan nimetä, muokata ja prosessoida lokitapahtumista saatuja tietokenttiä ja kenttäarvoja. Jäsentelysääntöjä hallitaan tietohallintavälineen kautta, jonka avulla voidaan luoda käyttäjän määrittelemiä sääntöjä lokitapahtumien jäsentämiseksi. Määrittelyssä käytetään kahta erillistä jäsentelysääntöosaa: INGEST ja COLLECT. INGEST-osiossa määritellään lopullinen tietojoukko, johon lokitapahtumat lopulta jäsentäytyvät. COLLECT-osa on valinnainen ja sillä voidaan rajoittaa tarpeettomien lokitapahtumien välittämistä INGEST-osalle. Molempiin näistä osista voidaan asettaa parametrit lokien käsittelyä varten seuraavasti: "vendor" määrittää, mihin alustaan säännöt liittyvät, "product" tarkentaa sovellettavan tuotteen ja "dataset" on pakollinen tietojoukolle asetettu nimi, johon jokainen lokitapahtuman rivi lopulta lisätään. INGEST- ja COLLECT-osien, "no_hit"-kohdan käyttö on valinnainen. Se ohjaa, miten toimia, jos sääntöryhmä ei tuota odotettuja tuloksia. Vaihtoehdot ovat "drop", mikä poistaa kyseisen lokitietueen, ja "keep", mikä säilyttää sen "_raw_log"-kentässä. Lisäksi INGEST-osan "ingestnull" asettaa, pitäisikö tyhjät arvot sisällyttää lokitietueelle. (Palo Alto Networks 2023a.)

Kaikki lokitiedot, jotka sisältyvät lokitapahtumalle, voidaan muokata XQL-kyselykielen avulla myös myöhemmässä vaiheessa. XQL-kyselykielellä määritellään kaikkiin Cortex XDR:n hälytyssääntöihin laukaisuehdot, joiden avulla lokitapahtuman arvot tarkistetaan ja luodaan tarvittaessa niiden seurauksena hälytys. Käyttäjät voivat itse määritellä, tehdäänkö tietomuutokset ennen lokitapahtuman tallennusta tietojoukkoon vai vasta hälytyksen yhteydessä. Esimerkiksi korrelaatiosäännön Drill-Down Query -vaiheessa, kun lokitapahtumatiedot ovat aiheuttaneet hälytyksen, ne lähetetään SOAR:iin lisätutkimuksia varten, jolloin voi suorittaa

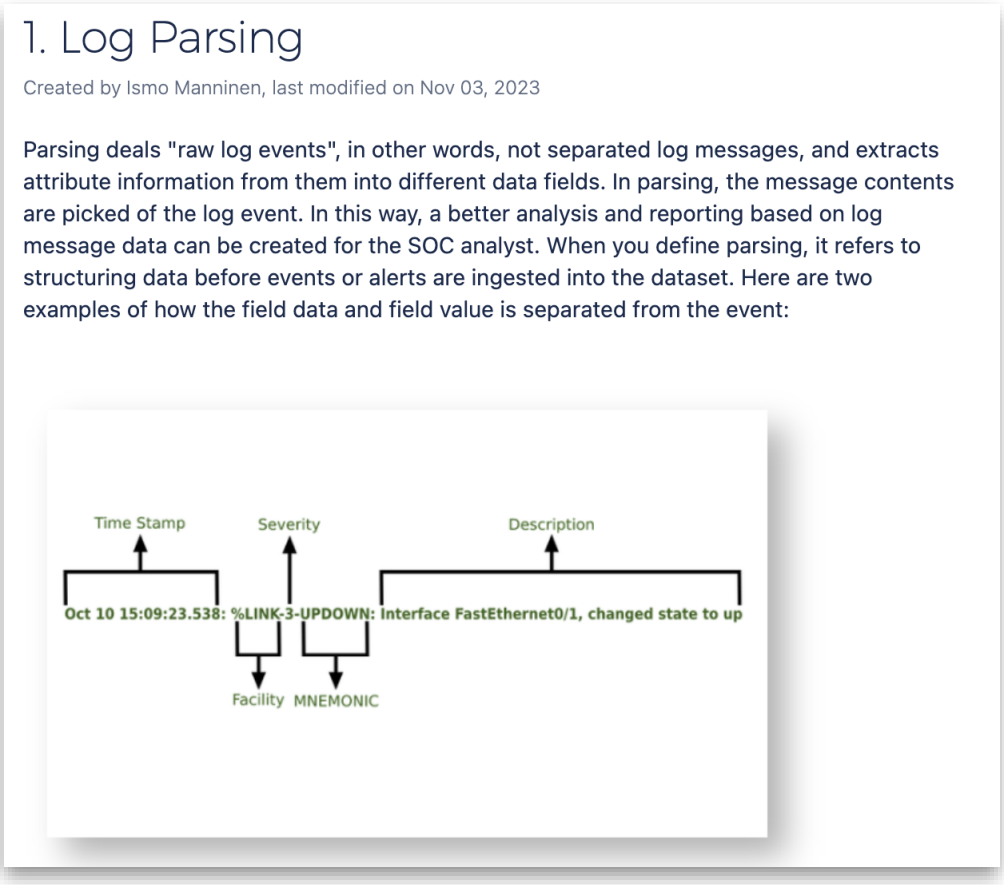
tarvittavat normalisoinnit ja muokkaukset tietokenttiin (Palo Alto Networks 2023a). Tässä vaiheessa viimeistään on varmistettava, että lokitapahtuman kenttien nimet ja arvot ovat yhteisesti sovitussa muodossa eli käytetään yhteisesti määriteltyä tietomallia.

Jokaisesta edellä mainitusta lokitapahtumien käsittelyosista tein sivustot, joissa päätoiminnot on jaettu kuvion 11 mukaisesti alaluokkiin. Näistä työntekijät löytävät taustatietoa aiheesta sekä käyttöohjeet. Kun työntekijä käsittelee asiakkaan custom-lokeja tai Palo Alton sekä kolmannen osapuolen lokilähteitä, hän näkee ohjeistuksesta lokilähteiden tilanteen ja tarvittavat menettelyt. Jos lokilähteet ovat yhä Palo Alton kautta hoidettuja, työntekijän tehtävä on suhteellisen yksinkertainen. Sen sijaan custom-lokilähteissä työntekijän on noudatettava ohjeistusta tarkasti ja tehtävä tarvittavia muutoksia. Näiden jälkeen luodaan korrelaatio- ja/tai hakusääntöjä, jotka laukaisevat hälytyksen. SOAR-järjestelmälle poimitaan Drill-Down-haun avulla tietokenttiä, josta analyytikko saa tarvittavaa tietoa tapahtumasta. Lopuksi työntekijä kirjoittaa raportin suoritetuista integraatioista luoden asiakkaalle dokumentaation räätälöidystä säännöistä sekä lokilähteistä. Raportoinnin avulla varmistetaan, että asiakkaat saavat tarvitsemansa tiedot oletusasetuksista ja toiminnallisuuksista, jolloin voidaan nopeasti palauttaa järjestelmä takaisin toimintavalmiiksi järjestelmävirheiden tai laiterikkojen yllättäessä.



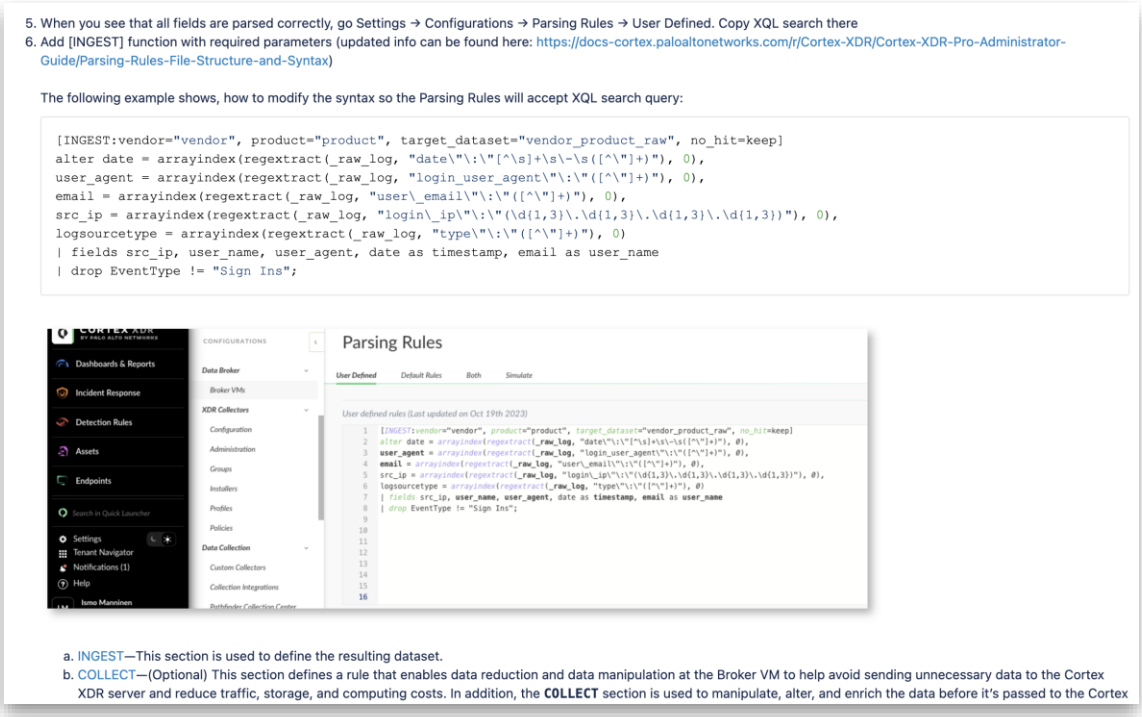
Kuvio 11. Lokienkäsittelyn ohjeistusrakenne

Jokaisen alaluokan alussa on johdanto (kuvio 12), joka selittää, millainen lokien käsittely on tarkoitus toteuttaa mahdollisille lokilähteille. Tässä kerrotaan, miksi työtä tehdään ja kenelle se on hyödyksi. Lisäksi esitellään prosessia havainnollistavalla kuvalla, joka näyttää tapahtuman lopputuloksen.



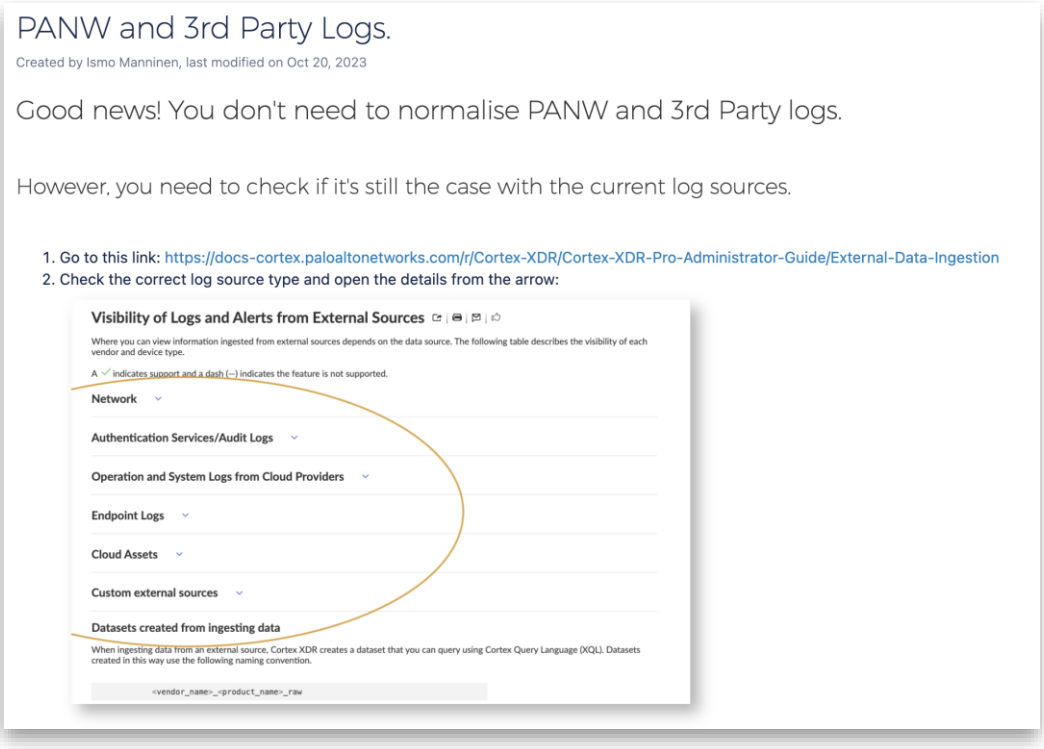
Kuvio 12. Jäsentämisen johdanto

Sen jälkeen esim. custom-lokeissa ohjeistuksessa tehdään käytännön jäsentelyä (kuvio 13), jossa lukijaa käskymuodoilla ohjataan tekemään tarvittavia toimintoja. Jokainen vaihe on numeroitu, jolloin suoritusjärjestys on lukijalle mahdollisimman selkeä. Lisätiedot tehtäväkohdasta ovat ohjeistuksessa sisennetty.



Kuvio 13. Jäsentämissäännön käyttöönotto

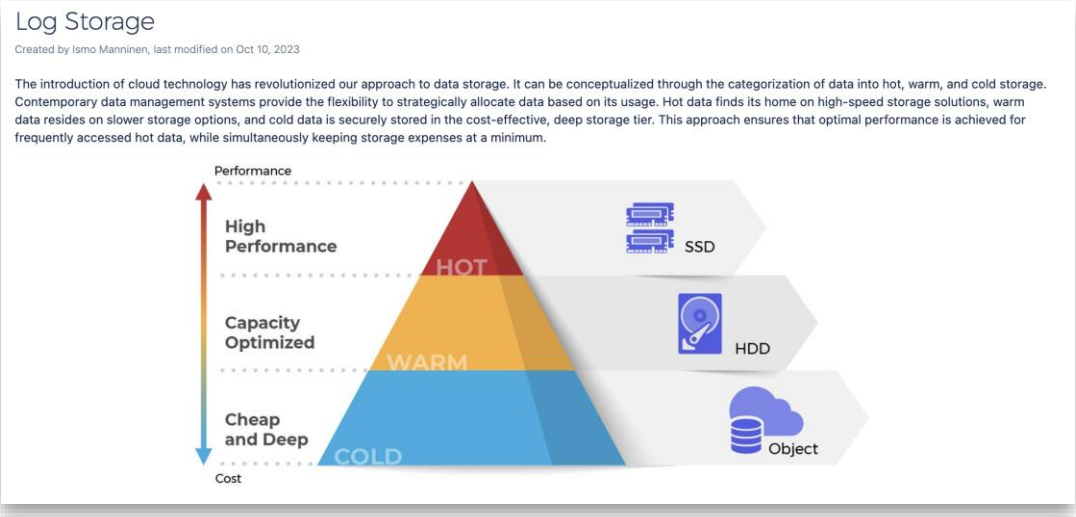
Ohjeistus auttaa lukijaa hyödyntämään alkuperäislähteitä, joista hän voi syventyä aiheeseen ja laajentaa omaa osaamistaan tarvittaessa. Palveluntarjoajan mukaan järjestelmä ja sen oppaat kehittyvät jatkuvasti, minkä vuoksi on järkevää viitata suoraan heidän luomiin tietoihin ja toimintamalleihin. Tämä tarkoittaa sitä, että ohjeistuksen noudattajalle käytännönvaihe saattaa sisältää pelkästään tarkastuksia, joiden avulla selvitetään, onko esimerkiksi kyseisestä lokilähteessä jo valmiiksi olemassa normalisoituja tietojoukkoja tai tarinoita (kuvio 14).



Kuvio 14. Normalisoinnin ohjeet

4.5 Lokien tallentaminen

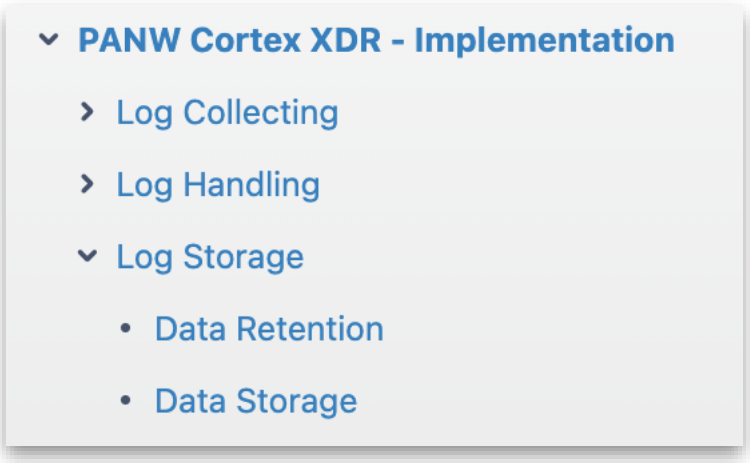
Pilviteknologian käyttöönotto on mullistanut lähestymistavan erilaisten tietojen tallentamiseen. Työntekijän on asiakaspalvelun näkökulmasta hyvä ymmärtää, missä ja miten tietoa Cortex-järjestelmällä oikein tallennetaan. Ohjeistuksen johdannossa kerrotaan, miten data luokitellaan järjestelmällä kuumaan, lämpimään ja kylmään varastointiin (kuvio 15). Kuumaa dataa käytetään nopeissa tallennusratkaisuissa, lämmintä dataa keskinopeissa tallennusvaihtoehdoissa ja kylmää dataa tallennetaan turvallisesti kustannustehokkaaseen syvään tallennustasoon. Tämä lähestymistapa varmistaa, että optimaalinen suorituskyky saavutetaan usein käytettäville kuumille tiedoille, samalla kun säilytyskustannukset pysyvät minimissä kylmällä datalla. (Sharma 2021.) Näiden avulla saadaan priorisoitua ajanjaksollisesti tärkeitä tapahtumia ja skaalattua suorituskykyä tärkeiden tapahtumien tai hälytysten tutkimiseksi. XQL-hakuja suoritetaan eri lämpötiloissa oleville tietojoukoille, jolloin hakuajoissa ja kustannuksissa esiintyy eroavaisuuksia. Lähtökohtaisesti oletuslisenssit sisältävät kuuman ja lämpimän varastoinnin mutta kylmä varastointi täytyy erikseen hankkia. (Palo Alto Networks 2023a.)



Kuvio 15. Datan eri säilöntämuodot

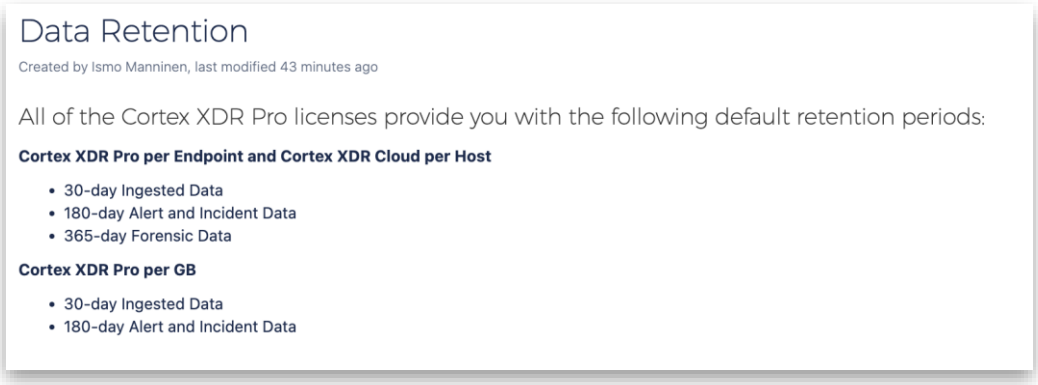
Kuuma data kattaa tietoja, joita käytetään usein ja jotka ovat ajankohtaisia. Nopean noudon varmistamiseksi se vaatii nopeita säilytysratkaisuja. Lämmin data puolestaan koskee tietoja, joita käytetään harvemmin ja joita käytetään tyypillisesti raportointi- tai analyyttisiin tarkoituksiin myöhemmässä vaiheessa. Se ei vaadi yhtä nopeaa käytettävyyttä kuin kuuma data, joten se voidaan sijoittaa hieman hitaampiin tallennusmuotoihin, jotka on optimoitu kapasiteetille. Kylmä data sisältää tietoja, joiden käsittely kuluttaa paljon aikaa ja jotka usein säilytetään arkistointiin liittyvistä syistä. Vähäisen käytön vuoksi ne voidaan sijoittaa siksi turvallisesti hitaammalle ja kustannustehokkaammalle säilytystasolle. (Sharma 2021.)

Tallennusmuodoista tein ohjeistussivustot, joissa lähteet on jaettu kuvion 16 mukaisesti säilytys- ja tallennusosiin. Nämä sisältävät informatiivista tietoa työntekijöille, kuinka pitkät ovat datan säilytysajat ja minne data tallennetaan. Nämä tiedot auttavat pääasiassa työntekijöitä asiakaspalvelussa ja asiakastyön raportoinnissa.



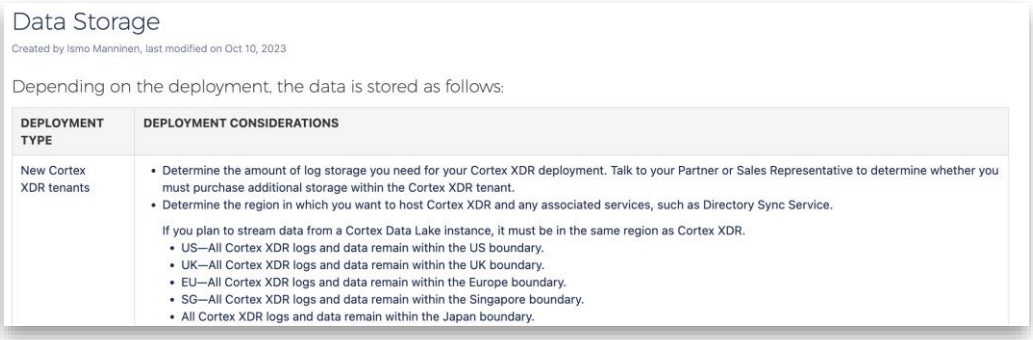
Kuvio 16. Lokivaraston ohjeistusrakenne

Näillä tiedoilla pystytään opastamaan ja tarkistamaan tarvittavia ratkaisuja Cortex XDR -ympäristön perustamisen ja ylläpidon näkökulmasta asiakkaalle. Ne myös tarjoavat perustiedot siitä, millaisia tallennusmahdollisuuksia Cortex XDR -lisenssit tarjoavat yrityksen palveluihin (kuvio 17). Oletuksena vastaanotetut tiedot säilyvät 30 päivää, hälytys- ja poikkeustiedot puoli vuotta ja rikostekniset tiedot kokonaisen kalenterivuoden (Palo Alto Networks 2023a).



Kuvio 17. Datan säilytysajat

Cortex XDR tallentaa kaiken datan perusajatuksena siihen käyttöönottoalueeseen, johon se on aktivoitu (Palo Alto Networks 2023a). Ohjeissa on useita taulukoita, joista yksi on esitetty kuviossa 18. Näissä taulukoissa näytetään jokaisen hallintakonsolin hallintoalueet sekä niihin liittyvät IP- ja URL-osoitteet. Lisäksi taulukoissa esitetään, millaisia verkkotunnuksia eri resursseille on ja miten hallintoalue ja resurssi otetaan huomioon URL-osoitteessa.



Data Storage

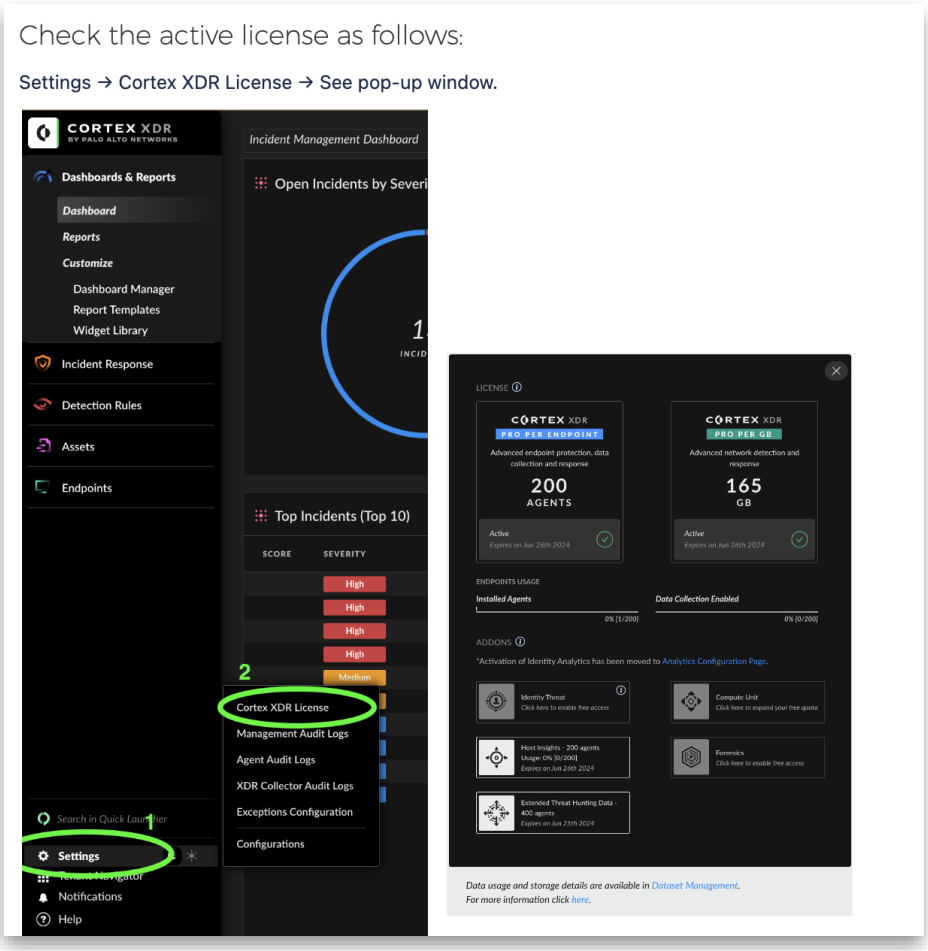
Created by Ismo Manninen, last modified on Oct 10, 2023

Depending on the deployment, the data is stored as follows:

DEPLOYMENT TYPE	DEPLOYMENT CONSIDERATIONS
New Cortex XDR tenants	• Determine the amount of log storage you need for your Cortex XDR deployment. Talk to your Partner or Sales Representative to determine whether you must purchase additional storage within the Cortex XDR tenant. • Determine the region in which you want to host Cortex XDR and any associated services, such as Directory Sync Service. If you plan to stream data from a Cortex Data Lake instance, it must be in the same region as Cortex XDR. • US—All Cortex XDR logs and data remain within the US boundary. • UK—All Cortex XDR logs and data remain within the UK boundary. • EU—All Cortex XDR logs and data remain within the Europe boundary. • SG—All Cortex XDR logs and data remain within the Singapore boundary. • All Cortex XDR logs and data remain within the Japan boundary.

Kuvio 18. Datan säilytyspaikat

Ohjeiden lopussa on käytännönohjeita, joiden avulla työntekijät voivat tarkistaa esimerkiksi järjestelmän käytössä olevat lisenssit (kuvio 19). Lisenssienhallinta-sivustolla näkyy, kuinka monta agenttia lähettää lokitapahtumia ja kuinka monta tiedonkeruutoimintoa on otettu käyttöön. Sivustolta voi myös aktivoida riittävillä käyttöoikeuksilla lisäosia järjestelmälle käyttöön (Palo Alto Networks 2023a).



Kuvio 19. Lisenssin tarkastusohje

4.6 Ohjeistuksen testaus

Kaikki integraatioiden parissa työskentelevät jäsenet, erityisesti uudet työntekijät, saivat mahdollisuuden osallistua ohjeistuksen testaukseen. Testauksen aikana he saivat lähettää testilokiviestejä testiympäristöön ja suorittaa vaadittavat toimenpiteet ohjeistuksen mukaisesti, että lokiviestit tulevat kerättyä ja käsiteltyä oikein. Testauksen jälkeen he antavat palautetta ohjeistuksen laadusta ja sen selkeydestä. Testauksen tavoitteena oli parantaa ohjeistuksen laatua ja arvioida, kuinka hyvin se vastaa toimeksiantajayrityksen tarpeita.

Testaukseen osallistui toimeksiantajayrityksestä muutamia henkilöitä, joista osa kävi ohjeistuksen läpi ja osa testasi ohjeistusta käytännössä. Ohjeistuksen testaus meni hyvin, ja se sai positiivista palautetta. Testaajien mukaan ohjeistus auttoi heitä ymmärtämään lokilähdeintegraation perusteet paremmin, ja antoi heille selkeämmän kuvan koko prosessista. Käyttäjät arvostivat erityisesti ohjeistuksen visuaalisia elementtejä ja sitä, miten se esitteli aiheen taustatietoineen. Ohjeistuksen avulla käyttäjät oppivat uutta ja tunsivat olonsa varmemmaksi aloittaessaan tulevia asiakasprojekteja. Ohjeistus oli heidän mielestään erinomaista.

Vaikka ohjeistus sai positiivista palautetta, palautteissa nousi esiin myös kehityskohteita. Testaajat toivoivat, että ohjeistus olisi yksityiskohtaisempi ja että jokainen vaihe olisi selkeästi kirjattu. Esimerkiksi “run”-napin painaminen oli oletettu toimenpide, joka olisi hyvä mainita ohjeistuksessa. Tämä selkeyttäisi toimintaa erityisesti niille käyttäjille, jotka eivät ole aiemmin käyttäneet vastaavia järjestelmiä. Lisäksi testaajat huomasivat, että ohjeistuksen rakenne ei ollut looginen, sillä normalisointiosio oli ennen parsintaosiota. Tämä aiheutti hämmennystä lukijassa, mikä voidaan ratkaista päivittämällä ohjeistuksen järjestystä.

Ohjeistuksen yksityiskohtaisuutta tarkennettiin kirjaamalla jokainen vaihe selkeämmin ylös, mukaan lukien oletetut toimenpiteet, kuten “run”-napin painaminen. Lisäksi ohjeistuksen rakenne tuli päivitettyä loogisemmaksi ja samalla tarkastettua sisältöjen johdonmukaisuus. Normalisointiosio on nyt sijoitettu oikeaan kohtaan eli parsintaosion jälkeen. Käyttäjäpalautteen perusteella nämä korjaukset ovat olleet hyviä ja ohjeistus on nyt entistä parempi.

5 JOHTOPÄÄTÖKSET

Opinnäytetyön tuloksena saatiin luotua tavoitteen mukainen ohjeistus lokien integroinnista ja hallinnasta, jossa kerrotaan, millaisia eri palveluntarjoajien lokilähteitä voidaan hyödyntää, mitä niille voidaan tehdä ja miten lokitapahtumia tuodaan, käsitellään ja tallennetaan PANW Cortex XDR -järjestelmään. Ohjeistuksen avulla työntekijät saivat varmemman käsityksen integraation oletetuista vaiheista ja työn kulusta. Ohjeistus on onnistunut uusi konstruktio, joka säästää perehdytykseen kuluvaa aikaa, joka antaa perustiedot työstä selviytymiseen. Kun uusi rakenne on osoitettu toimivan alkuperäisessä käyttöympäristössä, tämä tulisi nähdä käytännöllisenä työkaluna, joka tuo lisäarvoa tietylle tavoitteelle edistäen työskentelyn tehokkuutta ja hyödynnettävyyttä (Lukka 2001).

Toimeksiantajayrityksessä on olemassa monipuolisia ohjeistusmalleja, jonka vuoksi opinnäytetyön haastavin osuus oli löytää heille sopiva ohjeistusrakenne. Asiantuntijahaastatteluiden avulla ohjeistukseen saatiin rajattua tarpeita, mitä tulisi lokilähdeintegraation kautta vähintään saavuttaa, että hälytysjärjestelmästä on enemmän hyötyä kuin haittaa. Samoin Palo Alto Network hallintaoppaat eivät antaneet suoria ratkaisuja toteuttaa lokienkäsittelyyn liittyvää ohjeistusta, vaan niistä täytyi räätälöidä heidän tapoihinsa ja toimintamalleihinsa sopivia ratkaisuja.

Aluksi ohjeistuksen laatiminen uudella palvelukokonaisuudella oli haastavaa, koska toimeksiantajayrityksellä ei ollut selkeää käsitystä siitä, mitkä kaikki järjestelmäpalvelut tarvitaan asiakkaiden palvelemiseksi. Tämän vuoksi päätettiin jättää Data Lake- ja XSIAM-lokilähdeintegraatiot ohjeistuksen ulkopuolelle, koska kaikkea ei voitu sisällyttää vuoden 2023 kehitystyöhön. Tämä päätös auttoi hallitsemaan työmäärää ja antoi mahdollisuuden joustavampaan aikatauluun ohjeistuksen luomisessa asiakastyön ohessa. Lisäksi keskittyminen yhden järjestelmän opiskeluun mahdollisti syventymisen aiheeseen paremmin.

Ohjeiden laatiminen ja esimerkkien testaaminen veivät odotettua enemmän aikaa, sillä kaikkiin hälytyskäsittelyihin ei löytynyt suoria ratkaisuja olemassa olevista hallintaoppaista. Erityisesti haasteita tuotti väärien positiivisten hälytysten poissulkeminen ja lokilähteiden saatavuuden mittaus XQL-hakujen avulla. Näihin ongelmiin ei löytynyt valmiita ratkaisuja oppaista, joten oli tarpeen olla yhteydessä Palo Alton palvelupisteeseen sähköpostitse. Sain näihin haasteisiin heiltä

väliaikaisen ratkaisun ja tiedon palvelupisteeltä, että lokilähteiden saatavuuden mittaus tullaan automatisoimaan uudessa versiopäivityksessä ainakin tuetuille lokilähteille.

Erityisen mielenkiintoista oli oppia ohjeita luodessa, kuinka XDR ratkaisu eroaa perinteisistä SIEM ratkaisuista. Keskeinen ero XDR:n ja SIEM:n välillä on suojaustietojen laajuus ja integrointi. XDR kattaa laajemman valikoiman tietoturvatietoja, sisältäen päätelaite, verkkoliikenne ja pilvipohjaiset lähteet, kun taas SIEM keskittyy lokitietoihin verkon eri lähteistä ilman automaattista korrelaatiota lähteiden välillä (Palo Alto Networks 2023c). XDR tarjoaa yhtenäisemmän näkemyksen organisaation tietoturva tilasta ja mahdollistaa tasojen välisen uhkien havaitsemisen ja niihin reagoinnin. SIEM-vastatoimenpiteet rajoittuvat yleensä tietoturvavaroitusten lähettämiseen SOC:lle, kun taas XDR pystyy tietoturvavaroitusten lisäksi tekemään kontekstitietoisia muutoksia verkko- ja päätelaitteiden suojauksiin uhkien neutraloimiseksi (BlackBerry 2023). Nämä asiat tuntuvat sekoittuvan alalla helposti samaksi järjestelmäksi, mutta on tärkeä ymmärtää, että ne ovat kaksi erillistä palvelukokonaisuutta, joita voidaan hyödyntää yhdessä tai erikseen.

Opinnäytetyöraportti lokitapahtumien integroinnista ja hallinnasta on erittäin hyödyllinen, koska se auttaa ymmärtämään Cortex XDR:n toimintaa ja sen käyttöönottoa. Ohjeistus on räätälöity juuri toimeksiantajayrityksen tarpeisiin, mutta siitä voi saada käytännönläheisen malliesimerkin muiden alustojen tulevissa ohjeistuksissa ja aiheiden opiskeluissa. Kun yritys harkitsee eri tietoturvaratkaisujen käyttöönottoa, tämä opinnäytetyö tarjoaa nopean yleiskuvan siitä, mitä lokilähdeintegraatio tarkoittaa ja mihin aihealueisiin työntekijöiden kannattaa kiinnittää huomiota. Kuten jo aiemmin mainittiin, kyberturva-alan tarvittavan osaamisen tunnistaminen voi olla haastavaa, ja tämä puute saattaa vaikuttaa kyberturvallisuusasiantuntijoiden saatavuuteen. Opinnäytetyö antaa perustiedot siitä, mitä tietoteknologia-alalla niin kutsutut "lokit" oikein ovat, millaisessa ympäristössä niitä käsitellään ja mitä niiden hallinta pitää sisällään.

6 POHDINTA

Työn tarkoituksena oli tarkastella PANW Cortex XDR:n hallinto- ja käyttöönotto-oppaita kehittämistutkimuksen kautta ja ratkaista toimeksiantajayrityksen ongelman konstruktiivisen tutkimusmenetelmän avulla. Toimeksiantajayritys otti uuden palvelukokonaisuuden tarjontaansa, joka käyttöönotettiin heidän sekä asiakkaan ympäristöissä. Tavoitteena oli saada luotua toimeksiantajayritykselle käytännönläheinen ohjeistus järjestelmän käytöstä lokilähdeintegraation näkökulmasta. Työssäni tein aineistonhankintatyötä yrityksen ja palveluntarjoajan dokumentaatioista sekä asiantuntijoiden haastatteluista. Näitä analysoimalla päädyin käyttämään Kotimaisten kielten keskuksen julkaisemaa ohjeistusmallia, koska sen avulla pyritään tunnistamaan järjestelmän olennaiset toiminnot, esittämään asiat selkeästi hahmoteltavassa muodossa ja käyttämään käskymuotoa odotettujen toimenpiteiden osalta.

Opinnäytetyön keskeisenä tavoitteena oli selvittää, miten yrityksen hankkima PANW Cortex XDR -järjestelmä mahdollistaa lokitapahtumien tuonnin, käsittelyn ja tallentamisen. Päätutkimuskysymys keskittyi tarkastelemaan tätä prosessia, tuoden esiin tukikysymyksiä, kuten lokitapahtumien käsittelyyn liittyviä käytäntöjä, haasteita ja mahdollisuuksia lokitietojen suodattamiseen ja muokkaamiseen. Tutkimuksessani selvisi, että tämä järjestelmä tarjosi laajan näkymän verkkoliikenteeseen ja päätelaitteiden toimintaan. Se suositteli ja tuki yleisesti käytettyjä tiedostomuotoja lokitapahtumien käsittelyssä. XQL-kyselykieli mahdollisti lokitietojen jäsennyksen ja normalisoinnin luoden erilaisia tietojoukkoja ja niihin sääntöjä hälytysten luomiseksi. Näitä tietojoukkoja analysoimalla voitiin havaita poikkeavuuksia ja tunnistaa syy-seuraussuhteita käyttäen IOC-, BIOC- ja korrelaatiosääntöjä. Lisäksi tiedon tallennus perustui kuuman, lämpimän ja kylmän varastoinnin periaatteisiin priorisoiden datan tallentamista sen käyttötarkoituksen ja ajantasaisuuden mukaan.

Tutkimustuloksistani koostin kattavan ohjeistuksen eri palveluntarjoajien lokitapahtumien integroimisesta ja käsittelystä järjestelmään. Ohjeistuksesta rakentui kaiken kaikkiaan perustavanlaatuinen dokumentti toimeksiantajayritykselle. Siinä lokilähdeintegraatio jaetaan selkeisiin osa-alueisiin, jotka sisältävät aihealueista johdanto- ja toimenpideosia. Ohjeistus osoittautui testauksen kautta positiiviseksi

dokumentiksi, joka perehdyttää asiantuntijoita integraatioprosessin perusteisiin ja jossa saa käytännönläheistä perustietoa järjestelmän käytöstä. Lisäksi ohjeistuksella saatiin toimeksiantajalle selvitettyä tarvittavat viitekehykset, millainen ohjeistusmalli tukee heille käytännönläheistä työskentelyä. Ohjeistuksella saatiin lisättyä työntekijöille tunnetta selviytyä tulevista asiakasprojekteista. Saavutettiin siis teoreettinen kontribuutio, jossa ohjeistusmallilla voidaan lisätä työntekijöille lisää itsevarmuutta ja osallistumista uuden järjestelmän käyttöönotossa. Tämä itsessään oli erittäin positiivinen tulos opinnäytetyöstä.

Opinnäytetyössä on salattavaa ja suojeltavaa tietoa, joten eettisiä kysymyksiä ilmeni tässä yhteydessä. Ohjeistus laadittiin julkisesti saatavilla olevista asiakirjoista, jotka räätälöitiin asiantuntijahaastattelujen avulla ja joista kerättiin korjausideoita suullisen palautteen perusteella. Haastateltaville kerrottiin, että keskustelut tallennetaan toimeksiantajayrityksen tietojärjestelmään, eikä heidän henkilötietojaan kirjata opinnäytetyöhön tietoturvariskien ja identiteettisuojan vuoksi. Jokaisella on oikeus saada tietää tutkimuksen sisältö, henkilötietojen käsittely ja mitä tutkimukseen osallistuminen käytännössä tarkoittaa (Tutkimuseettisen neuvottelukunta 2019, 8). Kaikille henkilöille tehtiin selväksi, että osallistuminen on vapaaehtoista ja että he voivat kieltäytyä osallistumasta tai peruuttaa sen milloin tahansa. Tutkimuksessa keskityttiin ensisijaisesti haastateltavien kertomuksiin yrityksen tarpeista uuden tietotekniikan ja palvelun hallinnassa kuin itse haastateltavien.

Laadullisen tutkimuksen olennaisia näkökohtia ovat uskottavuuden ja luotettavuuden arviointi sekä käytettyjen käsitteiden ja menetelmien sopivuus tutkimusongelman ja aineiston kanssa. Luotettavuutta voidaan arvioida monin eri tavoin, esimerkiksi yleistettävyyden tai siirrettävyyden näkökulmasta, joka tarkastelee tulosten sovellettavuutta eri kohteisiin tai tilanteisiin. (Lähdesmäki ym. 2021b.) Tämä opinnäytetyö on luotettava, koska se perustuu palveluntarjoajan ja muiden yritysten lokienkäsittelyyn liittyvään dokumentaatioon. Tämä tarkoittaa, että ohjeistuksessa esitetyt prosessit ja sisällöt ovat peräisin luotettavista lähteistä, joiden soveltaminen ohjeistuksessa on osoittautunut toimivaksi yritysympäristöissä asiantuntijoiden palautteen kautta. Vaikka työ keskittyi tiettyyn tietoturvatapahtumien hallintajärjestelmään, sen periaatteet ja menetelmät ovat sovellettavissa

laajasti myös muilla alustoilla. Henkilöille saadaan tuotettua käytännöntyöhön liittyvää itseluottamusta, kun ohjeistus esittelee lukijalle aihetta, ilmaisee relaatioita kuvien avulla ja antaa selkeät vaihevaiheelta käytävät toimintaohjeet.

Jatkotutkimusmahdollisuuksina tämän opinnäytetyön pohjalta voisi tarkastella erilaisten ohjeistusten soveltuvuutta eri tietoturvatapahtumien hallintajärjestelmiin. Erityisesti voisi tutkia lokienkäsittelyn ja integraation laajentamista muihin vastaaviin järjestelmiin, vertaillen eri ratkaisujen toimivuutta ja soveltuvuutta erilaisiin organisaatioihin. Mahdollinen jatkotutkimus voisi keskittyä syvemmälle organisaatioiden tarpeisiin sekä laajempien käytännön ohjeistusten kehittämiseen integraatioprosessien hallinnassa. Toisaalta olisi kiinnostavaa tutkia tietoteknologisten ratkaisujen soveltuvuutta eri toimialoilla ja yrityskokoluokissa. Lisäksi jatkokehityksessä voitaisiin syventyä ohjeistuksen käyttäjäkokemuksen arviointiin ja kehittämiseen laajemmalla asiantuntijaotannalla, jolloin ohjeistus olisi vieläkin selkeämpi ja helpommin omaksuttavissa myös eri käyttäjäryhmille.

LÄHTEET

Anttila, P. 1998. Pirkko Anttila: Tutkimisen taito ja tiedon hankinta. Metodix – Metoditietämystä kaikille. Viitattu 8.9.2023 https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/.

BlackBerry 2023. XDR vs SIEM: What's the Difference. Viitattu 8.11.2023 https://www.blackberry.com/us/en/solutions/endpoint-security/extended-detection-and-response/xdr-vs-siem#differences.

Caulfield, J. 2023. How to Do Thematic Analysis | Step-by-Step Guide & Examples. Scribbr 22.6.2023. Viitattu 1.11.2023 https://www.scribbr.com/methodology/thematic-analysis/.

Chuvakin, A., Schmidt, J. & Phillips, C. 2013. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Waltham: Syngress. Viitattu 23.8.2023 https://books.google.fi/books?hl=en&lr=&id=Rf8M_X_YTUoC&oi=fnd&pg=PR1&dq=Log+management+systems+information+security&ots=ZRwnHVJ1ea&sig=34PIJKMk5gJCtHYBba8xEl9HqoM&redir_esc=y#v=onepage&q&f=false.

Cisco 2023. What Is Endpoint Detection and Response (EDR)? Viitattu 1.11.2023 https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html.

González-Granadillo, G., González-Zarzosa, S. & Diaz, R. 2021. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Crit-ical Infrastructures. Sensors, Vol 21 No 14, 4759. Viitattu 29.11.2023 https://doi.org/10.3390/s21144759.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F. & Materne, S. 2022. Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, Vol 47 No 3, 698–736. Viitattu 2.11.2023 https://doi.org/10.1057/s41288-022-00266-6.

Cross, K. 2021. Cortex XDR and Cortex XSOAR Bring the X-Factor to Security Operations. Palo Alto Networks 8.3.2021. Viitattu 28.9.2023 https://www.paloaltonetworks.com/blog/security-operations/xdr-xsoar/.

Hillary 2023. Securing the Future: The Vital Role of Cybersecurity in Manufacturing Processes. 21.8.2023 TechBullion. Viitattu 13.12.2023 https://techbullion.com/securing-the-future-the-vital-role-of-cybersecurity-in-manufacturing-processes/.

Humak 2022. Tutkimuksellisen kehittämistyön lähestymistavat ja menetelmät. Humanistinen ammattikorkeakoulu. Viitattu 8.9.2023 https://humak.libguides.com/c.php?g=688355.

IBM 2023a. Introduction to Log Source Management. Viitattu 23.8.2023 https://www.ibm.com/docs/en/dsm?topic=management-introduction-log-source.

– 2023b. What is process mapping? Viitattu 1.11.2023 https://www.ibm.com/topics/process-mapping.

Kotimaisten kielten keskus 2023. Ohjeita ohjeiden tekijöille. Helsinki. Viitattu 6.10.2023 https://www.kotus.fi/ohjeet/hyvan_virkakielen_ohjeita/millaisia_ovat_toimivat_ohjeet_ja_kysymykset/ohjeita_ohjeiden_tekijoille.

Kyberturvallisuuskeskus 2020a. Kyberturvallisuus ja yrityksen hallituksen vastuu. Viitattu 20.8.2023 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf.

– 2020b.Tietoturva. Viitattu 20.8.2023 https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva.

– 2023a. Kyberturvallisuuskeskuksen Viikkokatsaus - 32/2023. Viitattu 20.8.2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-322023.

– 2023b. Näin keräät ja käytät lokitietoja. Viitattu 21.8.2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja.

Lukka, K. 2001. Konstruktiivinen tutkimusote. Metodix Oy. Viitattu 6.9.2023 https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/.

Lähdesmäki, T., Hurme, P., Koskimaa, R., Mikkola, L. & Himberg, T. 2014. Valmiit dokumentit ja tuotetut dokumentit. Jyväskylän yliopisto, humanistinen tiedekunta. Viitattu 23.8.2023 https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmat/valmiit-dokumentit-ja-tuotetut-dokumentit.

– 2016. Teemoittelu. Jyväskylän yliopisto, humanistinen tiedekunta. Viitattu 24.8.2023 https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/teemoittelu.

– 2021a. Haastattelut. Jyväskylän yliopisto, humanistinen tiedekunta. Viitattu 24.8.2023 https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmat/haastattelut.

– 2021b. Tutkimuksen toteuttaminen. Jyväskylän yliopisto, humanistinen tiedekunta. Viitattu 15.11.2023 https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/tutkimusprosessi/tutkimuksen-toteuttaminen.

– 2021c. Laadullinen tutkimus. Jyväskylän yliopisto, humanistinen tiedekunta. Viitattu 28.11.2023

https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus.

Marjatta, R. 2023. Supon ja Traficomin arvio: Kyberturvallisuuden uhkataso pysynyt kohonneena ja kohdistettujen hyökkäysten määrä Suomessa noussut. Yle 21.4.2023. Viitattu 12.11.2023 https://yle.fi/a/74-20028240.

Microsoft 2023. Tehosta tietoturvatoimintojasi. Viitattu 1.12.2023 https://www.microsoft.com/fi-fi/security/business/solutions/extended-detection-response-xdr#diagram-cta-popup.

Niiranen, V. 2018. Atlassia tuotteiden lokitapahtumien saaminen SIEM-järjestelmään. Opinnäytetyö, Turun ammattikorkeakoulu. Viitattu 18.8.2023 https://urn.fi/URN:NBN:fi:amk-2018121120875.

Palo Alto Networks 2019. Palo Alto Networks Introduces Cortex, the Industry's Only Open and Integrated, AI-Based Continuous Security Platform. Viitattu 23.8.2023 https://www.paloaltonetworks.com/company/press/2019/palo-alto-networks-introduces-cortex-the-industrys-only-open-and-integrated-ai-based-continuous-security-platform.

– 2023a. Cortex XDR Pro Administrator Guide. Viitattu 23.8.2023 https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide.

– 2023b. Security Operations Workflow Automation. Viitattu 23.8.2023 https://www.paloaltonetworks.com/cortex/security-operations-automation.

– 2023c. What is the Difference Between XDR vs. SIEM. Viitattu 8.11.2023 https://www.paloaltonetworks.com/cyberpedia/what-is-xdr-vs-siem.

– 2023d. Cortex XDR XQL Language Reference. Viitattu 17.11.2023 https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-XQL-Language-Reference/Get-Started-with-XQL.

Petäjäkangas, H. 2023. Kyberuhkien torjuntaan koulutetaan lisää osaajia, mutta nyt ollaan jo myöhässä, sanoo professori. Yle 6.4.2023. Viitattu 15.8.2023 https://yle.fi/a/74-20026230.

Rissanen, J. 2012. Seuraavan sukupolven palomuuri yrityksessä. Opinnäytetyö. Lahden ammattikorkeakoulu. Viitattu 25.8.2023 https://urn.fi/URN:NBN:fi:amk-201205148149.

Sharma, A. 2021. Cold vs. Hot Data Storage: What's the Difference? Dataversity 9.9.2021. Viitattu 13.11.2023 https://www.dataversity.net/cold-vs-hot-data-storage-whats-the-difference/.

TEK-TOOLS 2020. How to Monitor Your Logs: Best Practices and Top Log Monitoring Software. Viitattu 23.8.2023 https://www.tek-tools.com/apm/log-monitoring-best-practices-and-tools.

Tutkimuseettisen neuvottelukunta 2019. Ihmiseen kohdistuvan tutkimuksen eettiset periaatteet ja ihmistieteiden eettinen ennakkoarviointi Suomessa –

Tutkimuseettisen neuvottelukunnan ohje 2019. Helsinki 2019. Viitattu 15.12.2023 https://tenk.fi/sites/default/files/2021-01/Ihmistieteiden_eettisen_ennakkoarvioinnin_ohje_2020.pdf.

Valtiovarainministeriö 2009. Lokiohje. Valtiovarainministeriön julkaisuja 3/2009. Viitattu 14.8.2023 https://www.suomidigi.fi/sites/default/files/2020-06/pdf_3_2009.pdf.

Viestintävirasto 2016. Lokien keräys ja käyttö. Ohje lokitietojen tallentamiseen ja hyödyntämiseen. Ohje 4/2016. Viitattu 14.8.2023 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitusohje.pdf.

Walkowski, D. 2019. What is the CIA Triad. F5 Labs 8.7.2019. Viitattu 15.12.2023 https://www.f5.com/labs/learning-center/what-is-the-cia-triad.

Watts, S. 2023. Common Event Format (CEF): An Introduction. Splunk 3.3.2023. Viitattu 6.11.2023 https://www.splunk.com/en_us/blog/learn/common-event-format-cef.html.

W3Schools 2023. JSON – Introduction. Viitattu 6.11.2023 https://www.w3schools.com/js/js_json_intro.asp.