Sampo Bredenberg

Uhkatietojen rikastus julkisten lähteiden tiedustelutiedoilla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tutkinto-ohjelman nimi

Insinöörityö

31.12.2024

Tiivistelmä

Tekijä: Sampo Bredenberg

Otsikko: Uhkatietojen rikastus julkisten lähteiden tiedustelutiedoilla

Sivumäärä: xx sivua + x liitettä

Aika: 31.12.2024

Tutkinto: Insinööri (AMK)

Tutkinto-ohjelma: Tieto- ja viestintätekniikka

Ammatillinen pääaine: Ohjelmistotuotanto

Ohjaajat: Tehtävänimike Etunimi Sukunimi  
Tehtävänimike Etunimi Sukunimi

**Tiivistelmä**

Avainsanat: avainsana, avainsana

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tämän opinnäytetyön alkuperä on tarkastettu Turnitin Originality Check -ohjelmalla.

Abstract

Author: First Name Last Name

Title: Title of the Thesis

Number of Pages: xx pages + x appendices

Date: 1 March 2021

Degree: Bachelor of Engineering

Degree Programme: Name of the degree programme

Professional Major: Name of the professional major

Supervisors: First name Last name, Title (e.g., Project Manager)

First name Last name, Title (e.g., Principal Lecturer)

Tiivistelmän tekstiosuus kirjoitetaan niin, että se mahtuu sivulla käytössä olevaan tilaan. Tekstiosuudessa käytetään Leipäteksti ilman välistystä-tyyliä.

Keywords: Keyword, Keyword

Sisällys

Lyhenteet

[1 Johdanto 1](#_Toc68862316)

[2 Pääluvun otsikko 1](#_Toc68862317)

[2.1 Alaluvun otsikko 1](#_Toc68862318)

[2.2 Alaluvun otsikko 2](#_Toc68862319)

[3 Asiakirjan rakenteet 3](#_Toc68862320)

[3.1 Taulukot 3](#_Toc68862321)

[3.1.1 Taulukon tekeminen Wordissä 4](#_Toc68862322)

[3.1.2 Alaluvun alaotsikko 5](#_Toc68862323)

[3.2 Lainaukset 5](#_Toc68862324)

[3.3 Luetelmat 5](#_Toc68862325)

[3.4 Ohjelmakoodi 6](#_Toc68862326)

[3.5 Kaavat 6](#_Toc68862327)

[4 Kuvan ja taulukon vaihtoehtoinen teksti 7](#_Toc68862328)

[4.1 Vaihtoehtoisen tekstin lisääminen kuvalle 7](#_Toc68862329)

[4.2 Vaihtoehtoisen tekstin lisääminen taulukolle 8](#_Toc68862330)

[5 Saavutettava asiakirja 9](#_Toc68862331)

[5.1 Asiakirjan ominaisuuksien viimeistely 9](#_Toc68862332)

[5.2 Insinöörityön saavutettavuuden tarkistus 9](#_Toc68862333)

[5.3 Word-tiedoston tallentaminen saavutettavaksi PDF-tiedostoksi 10](#_Toc68862334)

[Lähteet 12](#_Toc68862335)

Liitteet

Liite 1: Liitteen nimi

Liite 2: Liitteen nimi

Lyhenteet

ORM: *Object-relational mapping*. Ohjelmiston oliomallin mukaisen esityksen kuvaaminen relaatiotietokantamallin mukaiseksi esitykseksi ja kääntäen.

Tietoturvaloukkaus:

Uhkatekijä:

Digitaalinen tunnistetieto:

SIEM:

Brute-force:

# Johdanto

Uhkatiedot ovat todisteita haitallisesta toiminnasta IT-ympäristöissä. Uhkatietoja keräämällä ja niitä tutkimalla pyritään paljastamaan aktiivinen väärinkäyttö, sekä väärinkäyttöyritykset.

* Aidon datan kerääminen rajoitettua, yleensä vain oikeista ympäristöistä dataa
* Työlästä tunnistaa suuria määriä haitallista toimintaa
* Hyötyä muiden tehdystä ja automatisoidusta työstä

# Lähtökohdat

Tietoturva on tärkeä osa tietojärjestelmiä, jolla turvataan järjestelmien luotettava toiminnallisuus. Tietoturvan tärkeyttä korostetaan ja tietoisuutta jaetaan laajemmin kuin koskaan. Tässä luvussa pohjustetaan tietoturvapoikkeamien ja haitallisten uhkien tutkimiselle olennaisia käsitteitä, jotka ovat digitaalisia tunnistetietoja. Opinnäytetyön lopputuloksena on sovellus ratkaisu, joka mahdollistaa uhkatietojen keskitetyn rikastamisen. Sovelluksen avulla tietoturva-ammattilaiset voivat tehostaa työtään oleellisiin kohteisiin ja havaita tietoturvapoikkeamat nopeammin.

## Uhkatiedot

Uhkatiedot ovat tapoja ja tunnistettavia tietoja, joita on käytetty tietoturvaloukkauksissa ja väärinkäyttöyrityksissä. Niitä kerätään prosessoimalla tutkimalla tietoturvaloukkauksista ja tunnistamalla mitä hyökkääjä on tehnyt. Tässä opinnäytetyössä rajataan uhkatiedot digitaalisiin tunnistetietoihin, joita ovat:

* IPv4- ja IPv6-osoitteet
* Verkkotunnisteet (domain)
* Verkko-osoitteet (URL) **Vaihda verkko-osoitteet -> URL:it**
* Tiedostojen hajautusarvot (hash) **tarkistelaskenta?**

Digitaalisia tunnistetietoja löytyy palomuuri- ja kirjautumislokeilta lähtö- tai kohdeosoitteina, sekä laitteiden toiminnasta verkkoliikenteenä sekä tiedostoina. Uhkatiedot ovat ennestään tunnistettuja uhkatoimijoiden käyttämiä haitallisia tiedostoja, sekä tietoverkko liikennettä uhkatoimijoiden hallitsemiin verkko-osoitteisiin. Uhkatietojen avulla pyritään paljastamaan aktiivisia tietoturvaloukkauksia tai jopa torjumaan hyökkäyksiä ennakoivasti, kun uhkatekijöille ominaisia toimintatapoja valvotaan ennestään tunnistetuilla digitaalisilla tunnistetiedoilla.

Haittaohjelmia käytetään saavuttamaan jokin tavoite. Ennen lopullista tavoitetta, haittaohjelma pyrkii usein tunkeutumaan syvemmälle ympäristöön, saamaan salasanoja haltuun ja korottamaan käyttöoikeuksia, kunnes tavoite on mahdollista toteuttaa. Tavoitteen edellytyksenä voi olla jokin tietty laite, verkkoympäristö tai saamaan tietyn tasoiset käyttöoikeudet. Tiedostoja voidaan tunnistaa hajautusarvojen perusteella.

Verkkotunnisteet isännöivät haitallisia tiedostoja tai muita resursseja kuten kalastelu sisältöä, joiden kautta saadaan ensimmäinen pääsy ympäristöön. Ne toimivat myös osoitteina, joihin viedään luvattomasti tietoaineistoa ympäristöstä, ja komentokeskuskina, joiden kautta voidaan komentaa haittaohjelmia toimimaan halutulla tavalla.

### Digitaaliset tunnistetiedot

IP-osoitteet toimivat tietoliikenteen perustana. Kun tietoa halutaan lähettää, vastaanottaa tai hakea toiselta laitteelta, täytyy laitteen osoittaa mistä liikenne liikkuu mihin. IP-osoitteet toimivat lähtö- ja kohdeosoitteina, joiden avulla voidaan reitittää mikä laite lähettää tietoja, minne. IP-osoitteet voidaan jakaa neljään tyyppiin:

* Julkiset IP-osoitteet
* Yksityiset IP-osoitteet
* Dynaamiset IP-osoitteet
* Staattiset IP-osoitteet

Uhkatiedoille oleelliset IP-osoitetyypit ovat julkiset IP-osoitteet. Julkiset IP-osoitteet ovat yleensä pysyviä, aina ainutlaatuisia ja ne toimivat tunnisteina julkisessa internetissä. Uhkatietojen kontekstissa IPv4 ja IPv6 eivät juurikaan eroa. IP-osoitteet ovat yleensä aina osana tietoturvaloukkauksia, sillä kaikki verkkoliikenne tarvitsee aina IP-osoitteen.

[IP-osoite tyypit] <https://nordvpn.com/fi/blog/types-of-ip-addresses/> 17.11

Verkkotunniste on usein ihmisymmärrettävä merkkijono, joka tarvitsee aina IP-osoitteen, jonka takana jotain palvelua pidetään yllä. Verkkotunnisteet toimivat hierarkialla, jossa tasot erotetaan pisteellä. Ylätason verkkotunnusta (top-level domain) hallitsee aina jokin organisaatio, joka jakaa toisen tason verkkotunnisteita organisaatioille sekä yksityishenkilöille. Uhkatiedot koskevat toisen tai jopa kolmannen tason verkkotunnisteita, joissa uhkatoimija ylläpitää haitallista toimintaa. Usein koko toisen tason verkkotunniste osallistuu haitalliseen toimintaan.

Verkko-osoitteilla tarkoitetaan tarkkaa osoitetta verkkotunnisteella, joka johtaa tiettyyn resurssiin. Verkko-osoitteessa voi olla mukana myös kysely parametrejä.

Kaikkiin verkkoliikenteeseen liittyvien tunnistetietojen kautta voidaan suorittaa samoja haitallisia toimia, koska IP-osoite, verkkotunniste ja osoite ovat kaikki jokseenkin riippuvaisia toisistaan. Näiden tunnistetietojen takana voidaan isännöidä haitallisia tiedostoja, joita huijataan laitteen käyttäjä lataamaan, tai mahdollistetaan aktiivisen haittaohjelman käydä lataamassa jatkotoimenpiteiden suorittamiseksi. Verkossa isännöidään myös erilaisia huijauksia, joiden tavoitteena on yksinkertaisimmillaan seurata käyttäjän toimintaa, tai varastaa henkilökohtaisia tietoja.

IP-osoitteet ja verkkotunnisteet ovat hallittuja tunnisteita. Eri organisaatiot hallinnoivat verkkoliikenteeseen liittyviä tunnisteita ja jakavat osia alemmille organisaatioille käyttöön. Tämän hallinnollisen rakenteen takia, IP-osoitteet sekä verkkotunnisteet eivät ole pysyviä uhkatietoja. IP-osoitteiden ja verkkotunnisteiden käyttö voidaan mitätöidä, jos niistä tunnistetaan suoritettavan haitallista toimintaa. Näitä samoja tunnisteita voidaan jakaa myöhemmässä vaiheessa toiselle toimialle, joka käyttää niitä laillisiin toimiin.

Tiedostojen hajautusarvot ovat matemaattisia laskentatuloksia tiedoston sisällöstä. Tiedostojen nimet ovat mielivaltaisia ja niitä pystytään muuttamaan ilman että tiedoston sisältöön tarvitsee tehdä muutoksia. Tiedostonimi ei tällöin toimi tunnisteena tiedostoille. Hajautusarvot ovat uniikkeja merkkijonoja, jotka tehdään erilaisten laskenta algoritmien avulla ja kuvaavat tiedoston sisältöä. Vertaamalla tiedoston hajautusarvoa voidaan varmistaa, onko tiedoston sisältö muuttunut, jolloin voidaan varmistaa, onko ennestään tunnettua tiedostoa muutettu esimerkiksi hyökkääjän toimesta. Tiedoston toiminta voidaan analysoida, sen haitallisuus arvioida ja tulokset julkaista tai tallentaa. Hajautusarvot pysyvät samana, jos tiedoston sisältö pysyy täysin saman, joten tallennettuja tuloksia voidaan käyttää arvioimaan tiedostoa, jos se huomataan uudestaan. Useat virustentorjuntaohjelmat käyttävät osana toimintaansa hajautusarvoja tunnistaakseen ennestään löydettyjä haittaohjelmia.

[Microsoft PowerShell Get-FileHash, hyvää dokumentaatiota mihin hasheja käytetään] <https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-7.4> 16.11

### Uhkatietojen **kerääminen/löytäminen**

**Tarkoituksena kertoa mistä uhkatietoja nostetaan ensimmäisen kerran.**

Uhkatiedot ovat reaktiivisia luonteeltaan. Niitä kerätään joko osana teknistä tutkimusta tapahtuneen tietoturvaloukkauksen jälkeen, tai todettujen väärinkäyttöyritysten perusteella tunnistamalla digitaaliset tunnistetiedot, jotka olivat osallisina yritykseen. Nämä digitaaliset tunnistetiedot tallentuvat valvottavien ympäristöjen digitaalisiin lokeihin.

Lokit ovat sovellusten ja käyttöjärjestelmien tuottamia tietoja kyseisen tuotteen toiminnasta, jotka tallennetaan tai tulostetaan laitteelle. Niiden muoto ja sisältö vaihtelevat tuotteista toisiin. Lokien tarkoituksena on kertoa tuotteen toiminnasta ja ne voivat sisältää merkintöjä esimerkiksi sovelluslogiikasta, muutoksista, virheistä ja mitkä toiminnot ovat johtaneet kyseisiin tapahtumiin. Palomuurin tehtävänä on määritellä verkkoliikennettä ja suojella sisäverkkoa haitallisilta toimijoilta. Palomuurit yleensä tallentavat tiedot verkkoliikenteestä, kuten mikä lähdeosoite otti yhteyttä mihin kohdeosoitteeseen, millä portilla, kuinka monta tavua lähetettiin ja otettiin vastaan. Jos palomuuri estää yhteyden, se saattaa ilmoittaa tämän ja syyn, miksi yhteys estettiin.

[Palomuuri on] <https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html> 28.11

Jäsennellyillä lokeilta, joilla on jokin standardi tiedostomuoto, tunnistetiedot kuten IP-osoitteet ovat aina tietyssä kohtaa, jolloin tunnisteet voidaan erottaa helposti lokeilta ohjelmallisesti. Ohjelmointi- ja skriptauskielet tarjoavat usein valmiita ratkaisuita yleisimpien tiedostomuotojen, kuten JSON-, XML- ja CSV-tiedostojen jäsentelyyn.

Lokeilta, joilla ei ole struktuuria, voidaan digitaaliset tunnistetiedot erottaa käyttämällä säännöllisiä lausekkeita (regex). Säännöllisillä lausekkeilla voidaan poimia tekstistä tietyn mallisia tekstijonoja. Kaikki digitaaliset tunnistetiedot noudattavat tietynlaista mallia, joka mahdollistaa niiden poimimisen.

Tekninen tutkimus seuraa tietoturvaloukkausta. Sen tarkoituksena on käydä systemaattisesti läpi digitaalista todistusaineistoa, kuten tietoliikennelokeja, järjestelmälokeja ja haittaohjelmia. Sen tavoitteena on usein jäljittää mitä tietoturvaloukkauksessa on tapahtunut, mitä hyökkääjä on saanut aikaan ja miten laajalle toiminta on ulottunut. Tutkimuksen tavoitteena voi myös olla uhkatietojen kerääminen. Tuloksena on listaus digitaalisista tunnistetiedoista, mitä tietoturvaloukkauksessa on käytetty. Nämä toimivat uhkatietoina, joita voidaan käyttää muissa ympäristöissä uhkien löytämiseen ja torjumiseen.

Aktiivisen valvonnan ja tehokkaiden turvallisuusmenetelmien kautta voidaan tunnistaa väärinkäyttöyrityksiä. Brute-force hyökkäyksessä hyökkääjä pyrkii pakottamaan itsensä sisään, esimerkiksi kokeilemalla jokaista salasanaa, kunnes jokin onnistuu. Tunnistamalla normaalista toiminnasta poikkeavia tapauksia voidaan tietoturvaloukkaukset estää ennenaikaisesti. Tapahtumien pohjalta voidaan myös kerätä digitaaliset tunnistetiedot ja koostaa ne uhkatiedoiksi.

Erityinen tapa kerätä uhkatietoja, on jättää ympäristöön näkyvälle laite, joka houkuttelee hyökkääjiä yrittämään tunkeutua siihen. Näitä laitteita kutsutaan hunajapurkeiksi (honeypot). Niiden tarkoituksena on esittäytyä helppoina kohteina, joiden annetaan tahallaan joutua väärinkäytön uhriksi. Nämä laitteet toimivat ansoina, ja ovat eristettynä muusta verkosta. Hyökkääjän toimintoja voidaan seurata ja saadaan tietoja aitojen uhkien käyttämistä tekniikoista ja tunnisteista.

[Threat intelligence] <https://www.ibm.com/topics/threat-intelligence> 21.11

[What is a honeypot] <https://www.fortinet.com/resources/cyberglossary/what-is-honeypot> 19.11

### Uhkatietojen käyttö

Ympäristöissä on normaalia toimintaa, johon liittyy paljon verkkoliikennettä ja tiedostojen toimintaa. Vertaamalla tunnettuja uhkatietoja ympäristön toiminnassa esiintyviin tunnisteisiin, voidaan aktiiviset tietoturvaloukkaukset ja hyökkäys yritykset, tunnistaa ajoissa. Kehittyneissä tietoturva-järjestelmissä voidaan esimerkiksi verkkoliikenteen kohdeosoitteita ja prosessien toimintaa verrata suoraan tunnettuihin uhkatietoihin. Virustorjuntaohjelmat perustuvat usein siihen, että ne vertaavat laitteen toimintaa tunnettuihin uhkatietoihin. Uhkatietoja käytetään myös manuaalisessa analysoinnissa.

Poikkeavan toiminnan ilmetessä, tietoturva-tiimi suorittaa usein manuaalista analysointia, jossa lokien pohjalta pyritään tunnistamaan haitallinen toiminta ja löytöjen perusteella tekemään vastatoimenpiteitä. Analysoinnissa käsitellään usein lokeja, jotka sisältävät useita erilaisia digitaalisia tunnisteita. Tunnisteiden rikastaminen uhkatiedoilla nopeuttaa mahdollisen haitallisen toiminnan löytämistä ja tehostaa toimintaa, kun tutkintaa voidaan keskittää pois normaalista toiminnasta. Uhkatietoja voidaan siis käyttää tutkinnan tukena, antaen syvempää kontekstia haitalliselle toiminnalle. Niiden avulla voidaan tehdä lähteisiin perustuvia päätöksiä tilanteissa, joissa pitää selvittää onko jokin toiminta haitallista.

Kehittyneemmissä ympäristöissä lokeja viedään SIEM-alustoille, jotka toimivat keskitettyinä lokien hallinta alustoina. SIEM-alusta mahdollistaa tietoturvatapahtumien keskitetyn monitoroinnin, analysoinnin ja hallinnan. Alustalle viedään tietoturvatapahtumien valvontaan tarvittavia lokeja, kuten palomuuri-, käyttäjienhallinta alusta- ja laite tapahtumalokia. Useat SIEM-alustat jäsentelevät lokit automaattisesti sellaiseen muotoon, joka mahdollistaa tehokkaan uhkatietojen keräämisen sekä niiden analysoinnin.

## Julkisiin lähteisiin perustuva tiedustelutieto

Koska uhkatietojen kerääminen on reaktiivista, IP-osoitteet ja verkkotunnisteet usein lyhytkestoisia ja uhka tekijöitä on useita, yksittäisen tahon on hankala pitää ajantasaista uhkatieto tietokantaa yksin pystyssä.

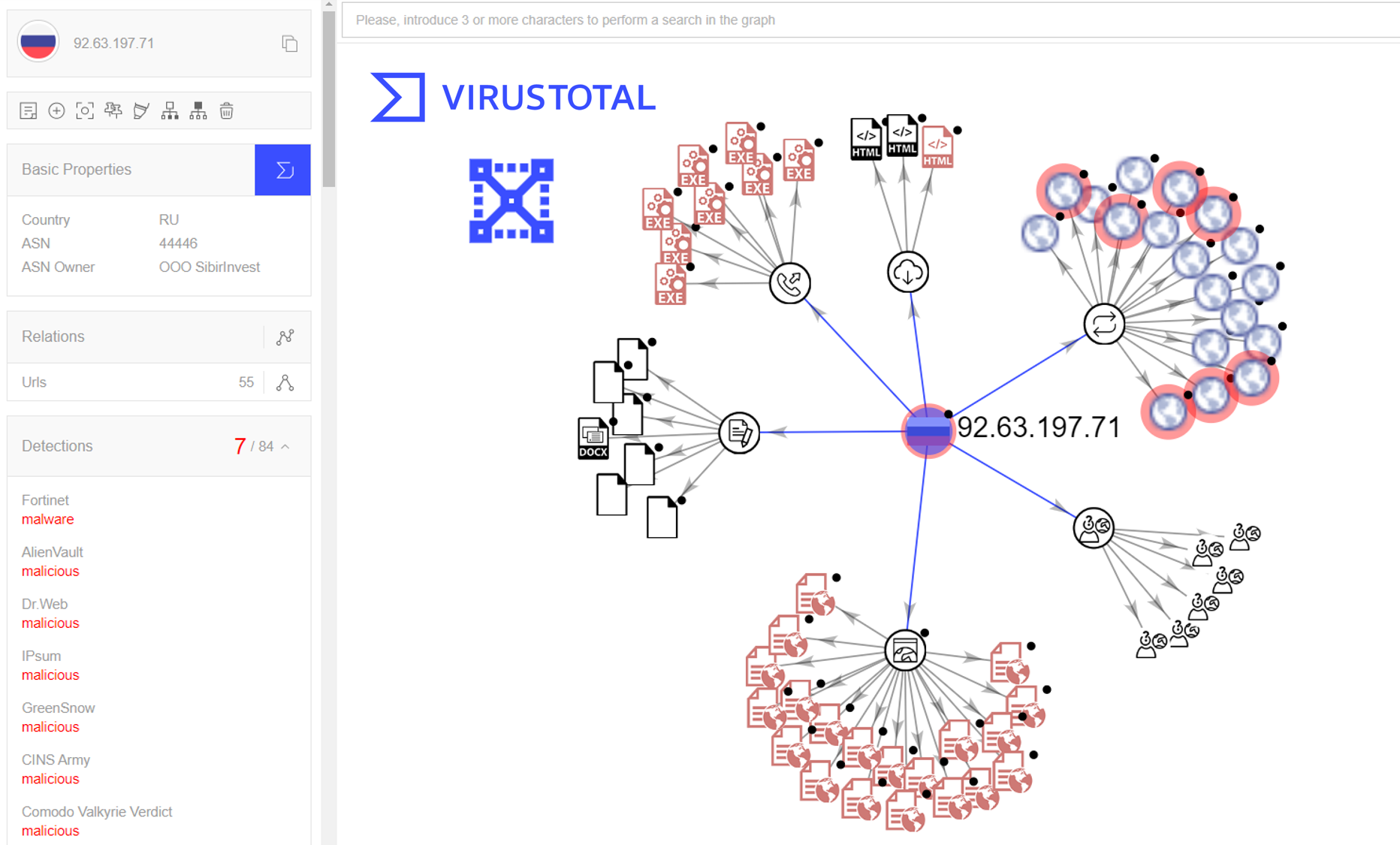
Kyberturvallisuus yhteisö on hyvin avoin jakamaan tietoja aktiivisista uhista. Uhkatietoja julkaistaan yksityisten tutkijoiden ja ammattilaisten, sekä organisaatioiden ja yritysten toimesta niin vapaasti, kuin kaupallisesti. Monet organisaatiot, yhteisöt ja yritykset erikoistuvat uhkatietojen keräykseen, analysointiin ja niiden julkaisuun. Uhkatietojen jakamisessa on usein tavoitteena lieventää tietoturvaloukkausten vaikutuksia, havaita aktiiviset hyökkäykset nopeammin ja ennaltaehkäistä niitä. Julkisten lähteiden uhkatietojen käyttäminen mahdollistaa ajantasaisen uhkien seurannan. Vertaamalla monia lähteitä keskenään, saadaan tarkka kuva uhkatietojen todenmukaisuuksista ja nopeutetaan analysointia, kun haitallinen toiminta on jo löydetty.

Monet alustat tarjoavat API ratkaisun alustojen ominaisuuksien, kuten uhkatietojen hakemisen käyttöön.

### Avoimet lähteet

Avoimet toimijat julkaisevat sekä mahdollistavat uhkatietojen hakemisen alustoiltaan vapaasti. Moni avoin toimija perustuu joukkoistettuun tiedustelutiedon keräämiseen, eli yhteisöön kuuluvien henkilöiden tai organisaatioiden nostamiin havaintoihin.

VirusTotal on yksi suosituin ja tunnetuin julkisiin lähteisiin perustuvien tiedustelutietojen alustoista. Se tarjoaa paljon erilaisia ominaisuuksia ja sen toiminnallisuus on integroitu moneen tietoturva-tuotteeseen. VirusTotal kokoaa eri tietoturva-toimijoiden virustorjuntaohjelma moottoreita, verkkosivu skannereita ja muita havaintoja tuottavia tuotteita alustalleen. Alusta mahdollistaa kenen tahansa syöttää tiedosto, verkkotunnus, URL tai IP-osoite, joka arvioidaan näillä tuotteilla ja tulokset jaetaan vapaaseen käyttöön. Havainnot eri toimijoiden tuotteista, antavat kattavan näkymän tunnisteiden toiminnasta ja onko niiden toiminnassa havaittu haitallisuutta. Alustalta löytyy esimerkiksi tiedostojen skannaamiseen tunnetuimmat virustentorjuntaohjelma toimittajat, kuten McAfee, WithSecure, Microsoft ja CrowdStrike.

VirusTotal sisältää myös yhteisö ominaisuuksia. Rekisteröityneet käyttäjät pystyvät äänestämään (-1 tai +1) tunnistetietoja sekä jättämään vapaan kommentin tunnisteille. Yhteisön määrittämä yhteispistemäärä sekä kommentit näytetään tunnisteen yhteydessä. Käyttäjät voivat luoda omia uhkatieto kokoelmia, ominaisuus mahdollistaa mind-map tyylisen kanvaasin, jossa voi luoda yhteyksiä tunnisteiden ja uhkatietojen välille. Näitä kaavioita voi jakaa muulle yhteisölle. Alusta mahdollistaa kaikkien tietojen hakemisen API:n avulla. Ilmainen API on rajoitettu 500 kyselyyn päivässä, 4 kyselyä minuutissa. Hinnoitellussa API:ssa ei ole kyselyrajoituksia, eikä sen hinnasta ole julkista tietoa. 

**VAIHDA KUVA, JOKU RANDOM GOOGLESTA ATM**

AbuseIPDB tarjoaa alustan, jossa rekisteröitynyt ja varmistettu käyttäjä pystyy ilmoittamaan IP-osoitteiden suorittaneen haitallista toimintaa. IPv4- tai IPv6-osoitteen lisäksi, täytyy väärinkäyttö kategorisoida ainakin yhteen valmiista kategorioista ja vapaa muotoinen kommentti liittää ilmoitukseen. Alustalta voi etsia IP-osoitetta, jonka sivulla mahdolliset ilmoitukset ja niiden tiedot näkyvät. Ilmoitusten perusteella alusta laskee "Confidence of Abuse" arvon IP:lle, joka kuvaa kuinka varmoja alustan ylläpitäjä organisaatio on siitä, että IP-osoite suorittaa väärinkäyttöä asteikolla 0–100. Alusta tarjoaa API:n, jonka kautta voi tehdä ilmoituksia, sekä hakea IP-osoitteiden tietoja ilmoituksista. Ilmainen API mahdollistaa 1000 kyselyä päivässä. Varmistetut käyttäjät rajoitetaan 5000 kyselyyn päivässä. Maksullisilla sopimuksilla kyselyiden rajoituksia voi kasvattaa 50000 kyselyyn asti.

[AbuseIPDB FAQ] <http://www.abuseipdb.com/faq.html> 17.11

Open Threat Exchange on yksi suurimmista avoimista uhkatieto yhteisöistä. Alusta mahdollistaa uhkatietojen jakamisen ”Pulse” raporttien muodossa. ”Pulset” ovat yhteisön jäsenten postauksia, joissa on lähde ja listaus tähän lähteeseen liittyvistä uhkatiedoista. Yhteisön jäsenet ovat yksittäisiä tietoturva-ammattilaisia tai organisaatiota, jotka keräävät ja julkaisevat uhkatietoja esimerkiksi tutkintojen tai hunajapurkkien tulosten perusteella. Alustalla voi seurata tiettyjä jäseniä ja saada heidän julkaisemia pulseja suoraan. Tämän avulla voi luoda syötteen itselleen oleellisista toimijoista tai toimialoista. Pulsejen lisäksi yksittäisiä tunnisteita voi etsiä ja alusta antaa näkymän, jossa siihen liittyviä pulseja ja muita liittyviä tunnisteita voi seurata. Open Threat Exchange tarjoaa rajattoman API:n jonka avulla alustan toimintoja voi käyttää.

Tranco on listaus, joka mittaa verkkotunnisteiden suosiota. Se yhdistää viiden eri toimijan kokoamat verkkotunniste suosio sijoitukset, luoden listauksen miljoonasta suosituimmasta viimeiseltä 30 päivältä. Yhdistämällä eri toimijoiden sijoituksia, tavoitteena on luoda vakaan listaus, jota vaikea manipuloida keinotekoisesti. Tranco listaus antaa kontekstia verkkotunnusten toiminnasta. Aidot verkkotunnisteet ovat yleensä vakiintuneita palveluita, joita käytetään jatkuvasti. Uudet verkkotunnisteet tai sellaiset, joille ei ole paljoa liikennettä, voi muiden todisteiden avulla kertoa mahdollisesti haitallisesta toiminnasta. Tranco tarjoaa rajattoman API:n, jonka avulla voi saada tiedot verkkotunnisteen sijoituksista viimeisen 30 päivän ajalta.

**Stop Forum Spam**

**ThreatMiner**

**URLhaus**

**ThreatFox**

### Kaupalliset toimijat

**GreyNoise**

**Mandiant**

**Maltiverse**

**Intelligence X**

### Joukkoistettu tiedustelutieto

Moni alusta mahdollistaa julkaisun tai jopa perustuu yksittäisten käyttäjien tekemiin havaintoihin. Itsenäiset tietoturva ammattilaiset voivat kerätä ja suorittaa omia tutkimuksia ja julkaista löydökset vapaasti muiden käyttöön. Yksittäisen henkilön johtopäätökset jonkin tunnisteen haitallisesta toiminnasta ei usein ole luotettava lähde, mutta jos kymmenet käyttäjät tuovat esiin samanlaisia nostoja, voi näitä verrata omiin huomioihin luotettavammin.

Joukkoistetut alustat voivat yksinkertaisimmillaan antaa käyttäjien tehdä ilmoituksia haitallisesta toiminnasta tai vain äänestää tunnisteen luotettavuudesta. Syvempää kontekstia löytyy alustoilta, kuten Open Threat Exchange. Käyttäjät julkaisevat raportteja löytämästään haitallisesta toiminnasta, joissa mukana tunnisteita ja lähteitä tai raportteja.

## Uhkatietojen rikastaminen

Uhkatietojen rikastamisessa tavoitteena on tuoda lisäkontekstia digitaalisen tunnisteen toiminnasta tutkintaan.

Järjestelmien tunnistettua epänormaali toiminta, tietoturva-tiimi tutkii mitä tämän toiminnan takana on ja pyrkii selvittämään, onko se asiallista vai onko sen takana haitallinen toimija. Toiminnassa on melkein aina jokin digitaalinen tunniste mukana, joka voi johdattaa tutkintaa oikeaan suuntaan. Edistyneissä järjestelmissä voi olla integraatioita alustoille, joista haetaan automaattisesti lisätietoja tunnisteista, jotka liittyvät tunnistettuun toimintaan.

Tutkinnan edetessä tunnisteiden määrä usein lisääntyy, mitä enemmän toimintaa selvitetään. Näiden tunnisteiden rikastaminen uhkatiedoilla tehostaa tutkintaa, kun normaali toiminta voidaan erotella ja löytää aikaisempien tutkintojen perusteella todettu haitallinen toiminta. Jotta tutkija saisi mahdollisimman laajan kontekstin ja moninaisen näkemyksen tunnisteista, tarvittaisiin rikastukseen useita lähteitä. Alustat, kuten VirusTotal, yhdistävät jo valmiiksi monien toimijoiden analyysejä. Yksinkertaisessa käytössä tämä usein riittää lisäkontekstin rakentamisessa. VirusTotal antaa kuitenkin **hyvin binäärin vastauksen**. Toimijoiden analysointi moottorit antavat ilmoille vain tiedon siitä, pitävätkö ne tunnistetta haitallisena, eivätkä miksi se on haitallinen. Moninaisen näkemyksen rakentaminen edellyttää useamman lähteen käyttöä, joiden erilainen toiminnallisuus ja näkökulmat antavat paremman kokonaiskuvan mahdollisesta haitallisesta toiminnasta.

Opinnäytetyön tuloksena on alusta, joka yhdistää eri uhkatietolähteet yhteen paikkaan, ja mahdollistaa digitaalisten tunnisteiden moninaisen rikastamisen yhdestä paikasta. Tämä poistaa tarpeen käyttää eri palveluiden verkkosivuja, kun niitä voidaan käyttää yhdestä paikkaa. Alusta käyttää esiteltyjen alustojen API ominaisuuksia, ja tuottaa yhdenmukaista dataa niiden antamista tiedoista.

# Teknologiat

Opinnäytetyön tuloksena rakennettuun alustaan käytettiin monia yleisiä ohjelmiston kehitykseen tarvittavia teknologioita. Teknologiat valittiin halutun käyttötarkoituksen puitteissa ja niitä lisättiin sitä mukaan, kun tarve toiminnallisuuteen tuli. Perusteena oli helposti käyttöönotettava, REST API pohjainen sovellus. Tämän perusteella työ toteutettiin Pythonin Flask frameworkillä ja käyttöönotossa sovellus muutetaan kontiksi Docker työkalulla.

## Python

Työn ohjelmointi kielenä käytetään python 3.11. Python tarjoaa laajan valikoiman kehittyneitä kirjastoja, joiden käyttäminen nopeuttaa kehittämistä. Työ perustuu erilaisten API alustojen käyttöön ja niiden tuomista yhteen, uusien API alustojen lisääminen haluttiin tehdä helpoksi ja modulaariseksi. Pythonin yksinkertaisuus mahdollistaa ylläpitämisen ja uusien yhteyksien luonnin minimaalisella perehtymisellä alustan syvempään toimintaan.

Kirjastojen käyttö on yksinkertaista pythonilla. Toiminnallisuuden rakentaminen ja toisten teknologioiden tuominen sovellukseen on helppoa, kun integroimiseen ja perusteiden rakentamiseen ei tarvitse käyttää aikaa.

Kehityksen aikana käytettiin Pythonin virtuaalista ympäristöä (Python virtual environment). Virtuaalinen ympäristö sisältää vain määritetyt kirjastot ja tietyn Python version, jonka avulla kehitys on yhtenäistä eri alustoilla ja käyttöönotto prosessi helppoa, kun kehitys tehdään aina identtisessä kehitysympäristössä.

### Flask

Flask on web-applikaatio framework kirjasto, joka mahdollistaa yksinkertaisten http-pohjaisten applikaatioiden rakentamisen. Flaskia käytetään työssä määrittämään API-rajapinnat, joita kutsumalla sovelluksen toiminnallisuuksia käynnistetään ja määritetään.

Flaskin ominaisuuksista työssä käytetään Blueprinttejä yhtenäisten toiminnallisuuksien kuten virheilmoitusten määrittämiseen, route dekoraattoreita rekisteröimään URL osoitteet, jotka käynnistävät sovelluksen eri toimintoja, sekä valmiita tietokanta liittimiä ja apu funktioita. Tietokanta liittimiä käyttämällä Redis ja SQLite yhteyksien rakentamisen hoitaa Flask automaattisesti.

Tekemällä kutsuja määritettyihin URL osoitteisiin, sovellus käynnistää tausta prosesseja ja palauttaa JSON formatoituja vastauksia.

@main.route("/health", methods=["GET"])

def health\_check():

    return jsonify({"status": "running"}), 200

Esimerkki /health URL osoitteesta, joka palauttaa JSON vastauksen palvelun statuksesta.

<https://flask.palletsprojects.com/en/stable/>

### Gunicorn

Gunicorn on Web Server Gateway Interface (WSGI) http-palvelin. Sen tehtävänä on välittää http-pyynnöt web-applikaatiolle. Vaikka Flask tarjoaa http-palvelimen kehitys tarpeisiin, eivät sen ominaisuudet ja tehokkuus ole niin kehittyneitä, kuin projektin, joka keskittyy toimimaan täysin http-palvelimena. Gunicorn toimii monisäikeisenä, pystyy prosessoimaan useita pyyntöjä yhtäaikasesti ja mahdollistaa erilaisten asetusten asettamisen, joilla voidaan tehostaa http-palvelimen nopeutta sekä turvallisuutta.

Gunicorn mahdollistaa alustan joustavan konfiguraation sekä käyttöönoton. Alustaa voidaan käyttää sellaisenaan Gunicorn toimien palvelimena, tai yhdistää käänteiseen välityspalvelimeen (reverse proxy). Kehittyneemmissä ympäristöissä Gunicornin toiminnan voi helposti yhdistää välityspalvelimeen, kuten Nginx tai Apache.

### Celery

Celery on asynkroninen, hajautettu tehtäväjono. Tehtäväjonoon pusketaan tehtäviä, joita Celery työntekijät (workers) suorittavat. Jonoksi ja tehtävien välittämiseksi tarvitaan message broker, joka on tässä työssä Redis. Rediksen ylläpitämään jonoo lisätään dynaamisesti tehtäviä, jotka Redis välittää työntekijöille. Celery työntekijät ovat erillisiä prosesseja, joita voidaan määrittää useita toimimaan samanaikaisesti ja ne suorittavat funktion toiminnallisuuden.

Sovelluksessa API-rajapinnan kautta tehdyt kutsut lisäävät tehtäviä Redis tehtävä jonoon, jonka kautta Celery työntekijä saa tarkat parametrit tarvittaville toimille. Työntekijät ovat erotettuna muusta sovelluksesta, ja ne hoitavat raskaammat tehtävät. Lisäämällä työntekijöiden määrää, voidaan sovellusta skaalata helposti ottamaan vastaan suuriakin määriä pyyntöjä, ilman toiminnan hidastumista.

A diagram of a task

Description automatically generated

Celery tehtävä prosessi.

## Redis

Redis on keskusmuistipohjainen varastointi palvelin alusta. Redis on erityisen tehokas varastoimaan ja lukemaan tallennettua dataa, koska se säilyttää kaiken keskusmuistissa (RAM). Se soveltuu toimimaan tietokantana, message brokerina sekä välimuistina. Tässä työssä Redis toimii samaan aikaan message brokerina Celerylle, sekä välimuistina tuloksille.

Välimuistiin voidaan tallentaa tiettyyn avainsanaan arvoja, joiden hakeminen vie aikaa tai on muuten raskasta. Redis vähentää näiden hitaiden ja raskaiden toimintojen määrää, kun niiden tuloksia voidaan tallentaa ja myöhemmin hakea tehokkaasti Rediksen välimuistista. Arvoille voidaan määrittää vanhentumisaika, jonka tultua täyteen arvo poistuu välimuistista ja näin pidetään se ajantasaisena. Välimuisti tehostaa sovelluksen toimintaa, vähentää vastausaikoja ja mahdollistaa skaalautumisen.

Redis toimii myös Celeryn tehtävä jonona. Celery kirjasto sisältää valmiin toiminnallisuuden Rediksen käyttöön. Celery määritettyjä tehtäviä voidaan ohjelmallisesti puskea Rediksen tehtävä jonoon helposti, josta työntekijät saavat ne käsittelyyn. Tehtävä jono toimii first in, first out periaatteella.

## Docker

Docker on virtualisointi alusta, joka tekee kehittämisestä, testauksesta ja lopulta käyttöönotosta yksinkertaista ja yhtenäistä. Dockeriin määritetään infrastruktuuri, jonka päällä kehitetty sovellus pyörii. Docker rakentaa määritysten perusteella ”kontin”, joka sisältää sovelluksen, sen tarvitsemat kirjastot, konfiguraatiot ja alustan, joka käynnistetään eristetysti laitteen käyttöjärjestelmästä. Dockerin toimintaa voidaan verrata virtuaalikoneeseen, mutta Docker virtualisoi vain sovelluksen toiminnan kannalta tärkeät palvelut, jonka takia Docker käyttää yleensä vähemmän laitteen resursseja. Dockeria käyttämällä voidaan käynnistää ja hallinnoida useita erilaisia palveluita ja sovelluksia helposti.

Docker Compose on Dockerin työkalu, joka soveltuu määrittämään suurempia, useiden Docker konttien kokonaisuuksia, joiden monitorointi sekä hallinnointi voidaan yhtenäistää. Docker Composen avulla voidaan rakentaa laajempi sovellus, joka sisältää kehitetyn sovelluksen, sille oman tietokannan sekä web-palvelimen. Jokainen palvelu pystytetään yhden konfiguraatio tiedoston avulla, docker-compose.yml. Konfiguraatioon määritetään jokainen haluttu, yksittäinen Docker palvelu ja niiden erityisominaisuudet. Konfiguraatio tiedoston avulla yksittäisen palvelun, kuten tietokannan vaihtaminen ei vaadi muuta, kuin konfiguraatio muutosta ja uudelleen käynnistämistä. Docker Compose tukee myös skaalausta. Yksittäisiä Docker palveluita voidaan käynnistää useita käynnistysvaiheessa, jolloin esimerkiksi Celery työntekijöitä voidaan määrittää useita.

Työssä Docker Composella erillisiä Docker kontteja hallinnoidaan yhtenäisesti. Sovelluksen eri osat eritellään yksittäisiin Docker kontteihin, joita hallinnoidaan tarvittavien palveluiden kanssa Docker Composella. Tuloksena alusta, joka on itsenäinen kokonaisuus.

# Työn toteutus

Työn tavoitteena oli luoda yksittäinen sovellus kokonaisuus, joka rikastaa sille syötettyjä digitaalisia tunnistetietoja, tekemällä useita API hakuja uhkatieto lähteisiin. Sovelluksen tarkoitus on siis yhdistää uhkatietojen rikastus yhteen paikkaan, näin poistaa tarve käydä useissa eri paikoissa hakemassa uhkatietoja. Sovelluksen täytyi täyttää seuraavat ominaisuudet:

* API avainten tallentaminen
* Digitaalisten tunnisteiden tunnistaminen ja kategorisointi
* Useiden ulkoisten API rajapintojen käyttäminen

Sovelluksen haluttiin myös toimia niin, että uusien uhkatieto lähteiden lisääminen olisi mahdollisimman yksinkertaista. Toteutus pyrittiin pitämään yksinkertaisena ja monipuolisena, että alustan sisällyttäminen valmiisiin toteutuksiin sekä yhdistäminen muihin komponentteihin olisi helppoa ja samalla toimisi myös itsenäisenä.

Rakenteeltaan työssä päädyttiin ratkaisuun, jossa toiminnallisuutta ohjataan Flaskilla toteutetun API rajapinnan kautta, joka käynnistää Celery työntekijöille tehtäviä. Näin erotellaan rajapinnan toiminta, raskaammista tehtävistä, joissa käydään hakemassa uhkatietoja ulkoisista API rajapinnoista ja sovelluksen API rajapinnan käyttö ei hidastu.

Sovellusta kehittäessä, ominaisuuksia tarkennettiin ja lisättiin sitä mukaan, kun tarve niille tuli. Kehitykseen käytettiin Visual Studio Code koodi editoria Python laajennuksilla, kehityksen tukena Docker Composea ja versionhallintana GitHub alustaa. API rajapinnan toiminnallisuuden testaamiseen käytettiin Postman sovellusta. Docker mahdollisti uusien palveluiden helpon lisäämisen ja jatkuvan testauksen. Kehittäminen tapahtui useilla laitteilla ja käyttöjärjestelmillä, Windows 10, Windows 11 ja Ubuntu, riippuen siitä mikä oli sillä hetkellä kätevintä. Docker mahdollisti yhtenäisen, alusta riippumattoman kehityksen ja jatkuvan testauksen.

Sovellusta lähdettiin rakentamaan tekemällä perusta API rajapinnan ja Celery työntekijöiden toiminnallisuudelle, jossa kutsu API rajapintaan käynnistää Celery työntekijän taustalle.

Lähdekoodin löytää työn tekijän henkilökohtaisesta GitHub reposta: <https://github.com/Sampob/threat-lense>

## Flask API

Flask toimii välittäjänä, jonka kautta kaikkia sovelluksen toiminnallisuuksia käynnistetään ja määritetään. Flask kirjasto määritetään ja käynnistetään Flaskin dokumentaation mukaisesti. Määrittelyssä käytetään apuluokkaa ”Config”, joka sisältää koko sovellukselle tärkeitä arvoja, kuten Redis tietokannan osoitteen ja kuunneltavat portit. Config luokan muuttujat voidaan määrittää ympäristömuuttujina esimerkiksi Dockerilla, joka mahdollistaa toiminnallisuuksien helpon mukautumisen.

Flask määritetään ja luodaan \_\_init\_\_.py moduulissa, jota kutsutaan ensimmäisenä koko sovelluksen käynnistyessä. Flask varmistaa ja käynnistää kaikki tietokantayhteydet, joita käytetään koko sovelluksen toiminnassa.

### API kehitys

API:n kehityksessä pyrittiin noudattamaan RESTful-periaatteita. Flaskin Blueprint moduulia käytettiin yhtenäistämään API:n toiminnallisuuksia, ja varmistettiin simppeli skaalautuminen, jos uusia toiminnallisuuksia täytyy lisätä.

### API reitit

API rajapinnan reitit määritetään routes.py moduulissa Blueprint dekoraattorilla, joka yhdistetään Flaskiin. Reitin rekisteröiminen ja toiminnallisuuden liittäminen siihen toimii kuin normaaleiden funktioiden määrittäminen. Esimerkiksi seuraava koodi rekisteröi Flaskiin reitin ”/search”, joka ottaa vastaan ”GET” pyyntöjä, ja suorittaa funktion ”search” toiminnallisuuden.

@main.route("/search", methods=["GET"])

def search():

print(“Performing search...”)

Sovelluksen koko toiminnallisuus haluttiin pystyä hallitsemaan API:n kautta, joten jokaiselle toiminnalle määritettiin API rajapintaan reitti, jonka kautta niitä pystytään käynnistämään.

RESTful-periaatetta ”Uniform interface” (Yhdenmukainen rajapinta) käytettiin reittejä suunnitellessa.

### Palautusmuoto

## Celery workers

### Celery tasks

## Julkisiin lähteisiin perustuva tiedustelutieto

### BaseSource

## Tiedon varastointi

### Välimuisti

### Salaus

## Docker compose

### Containers

### Networking

### Healthchecks

### Logging

## Testaus

### API endpoint testaus

# Tulokset

## Toiminnallisuus

## Käyttöönotto

### Yksinkertaisessa ympäristössä

### Kehittyneemmässä ympäristössä

## Käyttö

## Jatkokehitys

# Yhteenveto