Uhkien metsästys

1st Jonni Nurminen
University of Jyväskylä
KYBS1201
Jyväskylä, Finland
jonnurmi@student.jyu.fi

***Tiivistelmä*—Uhkien metsästys on viime aikoina ollut trendaava aihe kyberturvallisuudessa ja tutkimuksen kohteena. Uhkien metsästys on proaktiivinen metodi, jossa uhkia pyritään löytämään ennen kuin niitä ehditään hyödyntämään haitalliseen toimintaan. Lisäksi uhkien metsästys mahdollistaa reaktiivisten turvatoimien, kuten palomuurin ohittaneiden kehittyneiden uhkien löytämisen. Tämän esseen tarkoitus on selvittää lukijalle, mitä uhkien metsästys on, mikä sen rooli ja merkitys on, hyödyt ja haasteet, siihen liittyvät työkalut ja metodit sekä aiheeseen liittyvää aiempaa tutkimusta. Uhkien metsästys tarvitsee tulevaisuudessa tutkimusta liittyen tekoälyn käyttöön sekä metsästyksen haasteisiin, kuten vääriin hälytyksiin ja ihmisten taitoihin.**

***Avainsanat*—Uhkien metsästys, kyberuhkien metsästys, kyberturvallisuus, uhkatieto, tekoäly**

I. Johdanto

Internet on merkittävä osa nyky-yhteiskuntaa ja siellä liikkuu valtavia määriä arvokasta dataa sekä rahaa. Tämän vuoksi kyberturva on päivästä toiseen tärkeämpää kuin koskaan ennen. [1] Eräs uusi ja suosiotaan kasvattava metodi [1] kyberuhkien torjunnassa on etsiä ja paikata uusia kyberuhkia etukäteen, ennen kuin ulkopuolinen ehtii hyödyntämään uhkaa hyökkäämiseen [2]. Tällaista proaktiivista lähestymistapaa kyberuhkien torjuntaan kutsutaan uhkien metsästykseksi (eng. threat hunting / cyber threat hunting) [1] [3].

Vuonna 2018 tehdyssä tutkimuksessa 60% vastaajista ilmoitti aikeistaan ryhtyä proaktiiviseen uhkien metsästykseen, 43,2% kertoi suorittavansa sitä jatkuvasti ja 16,7% kertoi suorittavansa sitä säännöllisin väliajoin [4]. Eräässä tutkimuksessa [5] proaktiivisen uhkien metsästyksen todettiin olevan 60% nopeampi uhan löytämisessä verrattuna perinteisiin reaktiivisiin menetelmiin.

Uhkien metsästys on proaktiivista [1] [3], joka tarkoittaa ennakoivaa [6]. Perinteinen uhkien tunnistus taas on reaktiivista, eli uhkiin reagoidaan niiden ilmetessä [4], kun vahinko on jo päässyt tapahtumaan. Uhkien metsästyksessä pyritään löytämään ja paikkaamaan näitä uhkia ennakoivasti, ennen kuin ulkopuolinen taho on niitä ehtinyt hyödyntämään ja päässyt tekemään vahinkoa [4]. Tässä tuleekin uhkien metsästyksen ja perinteisen uhkien tunnistuksen oleellisin ero sekä uhkien metsätyksen oleellisin etu.

Tämän esseen tavoitteena on, että sen lukija kykenee vastaamaan seuraaviin kysymyksiin uhkien metsästyksestä:

- Mitä uhkien metsästys on?
- Mikä sen rooli ja merkitys kyberuhkien torjunnassa on?
- Mitä haasteita siihen liittyy?
- Miten ja millaisilla työkaluilla sitä tehdään?
- Miten aihetta on tutkittu?

Esseessä ei lähdetä syvällisesti tarkastelemaan esimerkiksi uhkien metsästyksen haasteita, niiden syitä ja ratkaisuja, vaan tarkoitus on kertoa lukijalle, minkätyylisiä haasteita aiheeseen liittyen on havaittu. Uniikin ja tarpeellisen esseestä tekee se, että se on suomenkielinen. Uhkien metsästyksestä on hyvin vaikeaa löytää suomenkielisiä julkaisuja. Uhkien metsästyksen suosio ja rooli kyberuhkien torjunnassa on ollut merkittävässä kasvussa lähivuosina, minkä vuoksi aihetta on hyvä kartoittaa.

Seuraavassa luvussa II on lyhyt kirjallisuuskatsaus käsiteltävään aiheeseen. Kirjallisuuskatsauksessa perehdytään aiheeseen liittyvään aiempaan tutkimuskirjallisuuteen, jota internetistä löytyi. Tavoitteena on luoda lukijalle kuva siitä, millaista tutkimusta aiheesta löytyy. Luvussa III tarkastellaan tarkemmin uhkien metsästyksen määritelmää ja tavoitteita sekä siihen liittyviä tekniikoita, työkaluja ja teknologioita. Luvussa IV listataan tehtyjä havaintoja, tässä tapauksessa uhkien metsästyksen haittoja ja hyötyjä. Luku V on keskustelu, jossa pohditaan ja analysoidaan uhkien metsästystä ja sen tulevaisuutta. Luvussa VI on yhteenveto tästä esseestä. Yhteenvedossa tiivistetään esseen sisältö sekä pohditaan uhkien metsästyksen tulevaisuuden tutkimustarvetta. Lopuksi on vielä esseessä hyödynnettyjen lähteiden luettelo.

II. Kirjallisuuskatsaus

A. Tiedonhaku

Tämän esseen lähdekirjallisuus on etsitty hyödyntämällä tieteellisten julkaisujen hakupalvelu Google Scholar:ia. Google Scholar:ssa haut tehtiin englannin kielellä. Hakuprosessissa hakusanoina toimivat threat hunting, techniques, tools, challenges, review ja technologies. Haut toteutettiin näiden sanojen yhdistelmillä. Uhkien metsästyksestä on hyvin vaikeaa löytää suomenkielisiä artikkeleita.

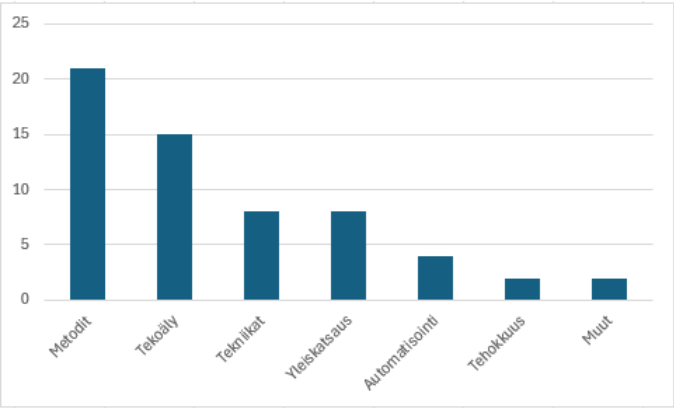
Pelkästään haku ”threat hunting” ilman lainausmerkkejä tuottaa Google Scholar:ssa noin 2 miljoonaa tulosta. Kun käytetään lainausmerkkejä, tuloksia saadaan noin 5600. Lainausmerkit tarkoittavat, että lainausmerkkien sisällön pitää löytyä hakutuloksien otsikoista. Aiheeseen liittyvää kirjallisuutta on siis valtava määrä, jos hakua ei rajata otsikoihin. Kuitenkin suuren tulosmäärän takia hakuprosessissa päädyttiin hakemaan ainoastaan otsikoista, koska tuloksien määrä väheni muutamiin tuhansiin ja kun hakusanat löytyvät otsikosta,

ovat löytyneet artikkelit todennäköisimmin mieleekkäämpiä esseen aiheen kannalta ja soveltuvat näin lähteiksi. Kuitenkin kun hakusanakomboa ”threat hunting” käytettiin yhdessä muiden aiemmin lueteltujen hakusanojen kanssa, ei muissa sanoissa käytetty lainausmerkkejä. Haussa siis etsittiin otsikoista sanakomboa ”threat hunting” ja lisäksi artikkelien sisällöstä muita hakusanoja.

B. Aiempi tutkimuskirjallisuus

Google Scholar:in tuloksista löytyneet tutkimukset olivat suurilta osin tuoreita. Kun haku kohdistettiin otsikoihin hakulauseella ”threat hunting”, saadusta noin 5600:sta tuloksesta noin 1400 julkaisua oli julkaistu tämän vuoden (2024) aikana. Tämä tarkoittaa, että noin 25% julkaisuista on julkaistu alle vuosi sitten.

Hakutuloksista valittiin 60 ensimmäistä tulosta ja ne kategorioitiin julkaisujen otsikon ja tiivistelmän perusteella karkeasti eri teemoihin. Teemat jakautuivat metodeihin, tekoälyyn, tekniikoihin, yleiskatsaukseen, automatisointiin, tehokkuuteen ja muihin. Metodit sisältävät myös kehykset ja mallit, joita tutkimuksissa ehdotettiin. Tekoälyyn sisältyy kaikki tekoälyn osa-alueet kuten koneoppiminen, neuroverkot ja syväoppiminen. Tekniikoihin sisältyy myös teknologiat sekä työkalut. Automatisoinnissa käsiteltiin uhkien metsästyksen automatisointia ilman tekoälyä. Julkaisujen teemat ja niiden jakauma ovat seuraavassa kuvassa 1.



KUVA 1. Hakutulosten jakauma teemoittain

Suosituin tutkimuksen kohde pienen otoksen perusteella näyttää olevan metodit ja toiseksi suosituin tekoälyn hyödyntäminen. Tekoälytutkimukset keskittyvät suurimmaksi osaksi koneoppimiseen. Koneoppimisen hyödyntämiseen uhkien metsästyksessä keskittyvät muun muassa tutkimukset [7] [8] ja [4]. Lisäksi [9] käsittelee koneoppimisen ja syväoppimisen hyödyntämistä Ransomware-hyökkäysten löytämisessä.

Metodeihin luokitellut tutkimukset käsittelivät muun muassa erilaisia kehyksiä ja malleja, joiden avulla uhkien metsästystä voidaan suorittaa, siitä saadaan tehokkaampaa tai se soveltuu paremmin tiettyyn kohdealueeseen, kuten teollisuuden ohjausjärjestelmien verkkojen suojaukseen. Tästä esimerkkinä Jadidin ja Lun [10] tutkimus, jossa he esittelevät uhkien metsästys -kehyksen teollisuuden ohjausjärjestelmien (eng. Industrial Control System, ICS) verkkoon, koska heidän mukaansa nykyiset uhkien metsästyksen metodit eivät suoraan sopineet ko. verkoissa metsästykseen. Tutkimuksen tuloksena he esittelivät kolmivaiheisen uhkien metsästys -kehyksen, joka soveltuu ICS-verkoissa metsästämiseen. Kehys hyödyntää aiempia MITRE ATT&CK Matrix ja timantti -mallien yhdistelmää haitallisen toiminnan tunnistamisessa. Näistä malleista kerrotaan lisää seuraavassa luvussa III. Tutkimuksen lopuksi Jadidi ja Lu [10] testaavat kehystä kolmella erilaisella skenaariolla, joista esimerkkinä yksi oli vedenpuhdistamon prosesseja mallintava tietoaineisto. Tuloksena tutkimuksessa todettiin kehyksen soveltuvan teollisuusyrityksien käyttöön ICS-verkoissa tehtävään uhkien metsästykseen. Muita vastaavia tutkimuksia ovat muun muassa [11] [12] ja [13]. Esimerkiksi Puzis, Zilberman ja Elovici [12] esittelevät tutkimuksessaan ATHAFI:n, joka on ketterä uhkien metsästys -malli.

Tekniikkateemaan kuuluivat tutkimukset, joissa esiteltiin tai kehitettiin alustoja, tekniikoita tai järjestelmiä uhkien metsästykseen. Tällaisia tutkimuksia ovat muun muassa [14] [15] ja [16]. Yleiskatsauksissa, kuten [1] ja [17] tarkasteltiin yleisesti uhkien metsästystä ja sen käyttöä esimerkiksi kirjallisuuskatsauksen tai kyselytutkimuksen avulla. Automatisointi käsittää uhkien metsästyksen automatisointia ilman tekoälyä käsittelevät tutkimukset, kuten [18]. Tehokkuuteen kuuluvissa tutkimuksissa esiteltiin keinoja, joilla uhkien metsästyksestä saadaan tehokkaampaa, esimerkiksi [19]. Kategoriaan muut taas lukeutuivat tutkimukset, joiden ei ajateltu sopivan mihinkään muuhun teemaan ja olivat yksittäisiä tapauksia otoksessa. Esimerkiksi tutkimuksessa [20] käsitellään uhkien metsästykseen tarvittavia oleellisia taitoja ja miten niitä voitaisiin opettaa yliopistossa.

III. Uhkien metsästys

Tässä luvussa sukelletaan syvemmälle uhkien metsästyksen määritelmään, sekä pohditaan uhkien metsästyksen tavoitteita. Lisäksi listataan lähdekirjallisuudesta esiin nouseita uhkien metsästyksen menetelmiä, työkaluja ja teknologioita. Luvussa esitellään myös, miten uhkien metsästys tyypillisesti toteutetaan ja miten tekoälyä hyödynnetään uhkien metsästyksessä.

A. Määritelmä ja tavoitteet

Kuten jo aiemmin todettiin, uhkien metsästyksellä tai kyberuhkien metsästyksellä (eng. threat hunting tai cyber threat hunting) tarkoitetaan proaktiivista lähestymistapaa tuntemattomien ja korjaamattomien uhkien identifiointiin organisaation verkossa [3]. Uhkien metsästyksessä ei keskitytä tunnettujen uhkien havaitsemiseen, vaan ideana on kehittää uusia, aiemmin tuntemattomia hyökkäyskeinoja. Kun uusi hyökkäyskeino löydetään, siltä voidaan puolustautua ennen kuin ulkopuoliset hyökkääjät (eng. attacker tai threat actor tai adversary) hyödyntävät kyseistä keinoa hyökkäämiseen organisaatiota vastaan. [2] Leikkimielisesti voidaan sanoa, että saaliista tehdäänkin metsästäjä [21]. Vaikka uhkien metsästyksen mielletään yleisesti olevan proaktiivista, jotkin

lähteet, kuten [22] ja [7] jakavat sen proaktiiviseen ja reaktiiviseen lähestymistapaan. Badva ym. [22] mieltävät proaktiivisen osan olevan uhkatiedon hyödyntämistä hypoteesien tai käyttötapausten muodostamiseen mahdollistaen aktiivisen potentiaalisten uhkien etsimisen, ennen kuin ne aiheuttavat vahinkoa. Reaktiivinen puolestaan keskittyy rikostekniseen tutkintaan ja uhkahälytyksiin vastaamiseen uhan havaitsemisen jälkeen. Shan ja Meyong [7] käyttämä jako vastaa tätä.

Uhkien metsästyksessä on tärkeää kyetä ymmärtämään hyökkääjien käytöstä. Tähän sisältyy ymmärrys hyökkääjien taktiikoista (miksi), tekniikoista (miten) ja menettelytavoista (erikoisuudet). Lähdekirjallisuudessa tulee usein vastaan tätä tarkoittava lyhenne TTP, joka tulee englanninkielen sanoista Tactics, Techniques ja Procedures. Jatkuvasti kehittyvän ja muuttuvan hyökkääjien TTP:n takia staattisten, reaktiivisten suojausmekanismien on vaikeaa pysyä hyökkääjien kehityksen mukana. [4]

1) Tyypit: IBM [3] jakaa uhkien metsästyksen kolmeen tyyppiin. Nämä ovat strukturoitu metsästys, strukturoimaton metsästys sekä tilanne- ja kokonaisuuskohtainen metsästys. Bhardwaj ym. [23] tyytyvät luokittelussa kahteen ensimmäiseen.

Strukturoitu metsästys pohjautuu hyökkäyksen indikaattoreihin ja aiemmin mainittuun TTP:hen. Strukturoidussa metsästyksessä metsästäjä kykenee tunnistamaan uhkatoimijan ennen kuin se on kerennyt aiheuttamaan vahinkoa ympäristöön. Tässä metodissa käytetään MITRE ATT&CK -kehystä. [3] MITRE ATT&CK -kehys puolestaan on globaalisti saatavilla oleva tietopohja, joka perustuu todellisen maailman havaintoihin hyökkääjän TTP:stä. Kyseistä kehystä käytetään perustana uhkamallien ja -menetelmien kehittämiseen yksityisellä sektorilla, hallituksessa ja kyberturvallisuuden tuote- ja palveluyhteisöissä. [24]

Strukturoimattoman metsästyksen aloitus perustuu laukaisijaan (eng. trigger), joka on yksi lukuisista vaaran indikaattoreista (eng. Indicator of Compromise, IoC). Laukaisija aktivoi metsästäjän etsimään havaitsemista edeltäviä ja sen jälkeisiä malleja. Lähestymistapaa ohjatakseen metsästäjä voi tutkia malleja niin kauan, kuin tietojen säilytysaika laissa sallii. [3] Strukturoimaton metsästys tuottaa uusia vaaran indikaattoreita ja se on pääasiassa dataperustaista [23].

Tilanne- ja kokonaisuuskohtaisessa metsästyksessä tilannehypoteesi saadaan yrityksen sisäisestä riskiarviosta tai sen IT-ympäristön trendi- ja haavoittuvuusanalyysistä. Kokonaisuuskohtaiset johtolangat tulevat joukkoihin perustuvasta hyökkäysdatasta, joka paljastaa nykyisten tarkasteltavissa olevien hyökkääjien TTP:t. Näiden avulla uhkien metsästäjä voi etsiä näitä käyttäytymismalleja ympäristöstä. [3] Bhardwaj ym. [23] sisällyttävät tämän strukturoituun metsästykseen.

2) Uhkien metsästäjät: Uhkien metsästystä suorittavat uhkien metsästäjät. Organisaatiolla voi olla oma uhkien metsästäjien tiimi tai uhkien metsästys on voitu ulkoistaa sitä tarjoaville palveluille, kuten CrowdStrike, Cisco ja Booz Allen Hamilton [25]. Uhkien metsästävät tutkivat verkkoja ja laitteita proaktiivisesti havaitakseen tuntematonta ja haitallista käytöstä aiheuttavia uhkia [10]. Esimerkiksi F-Securella uhkien metsästäjät sitoutuvat hyökkäyskoulutukseen ja monilla F-Securen metsästäjillä on jo aiempaa kokemusta hyökkäämisestä. F-Securen mukaan aiempi kokemus hyökkäysmetodien testauksesta on merkittävä etu, sillä se mahdollistaa uhkien metsästäjän operoida hyökkääjälle ominaisella ajattelutavalla. Lisäksi perustuntemus hyökkäämisestä kertoo uhkien metsästäjälle, mistä ja mitä etsiä, vaikka hyökkääjän tekniikat eivät olisi ilmeisiä. [2]

3) Uhkatieto: Uhkien metsästykseen liittyy oleellisesti myös uhkatieto (eng. Threat Intelligence / Cyber Threat Intelligence, CTI). Uhkatiedon tavoite on saavuttaa tietoetu uhkatoimijoihin nähden. Uhkatieto nopeuttaa haitallisen käytöksen aikaista havaitsemista ja voi mahdollistaa sen havaitsemisen jo ennen kuin hyökkääjä on päässyt verkkoon. [26] Uhkatietoa kerätään, prosessoidaan ja analysoidaan todellisista tapauksista, jotta ymmärretään hyökkääjän motiiveja, hyökkäyskäytöstä sekä hyökkäyskohteita [27]. Uhkatietoa voidaan jakaa erilaisilla alustoilla muiden saataville. Esimerkki tällaisesta alustasta on MISP (Malware Information Sharing Platform) [10]. Uhkatieto myös muodostaa pohjan koneoppimis- ja tekoälymallien kouluttamiselle [28].

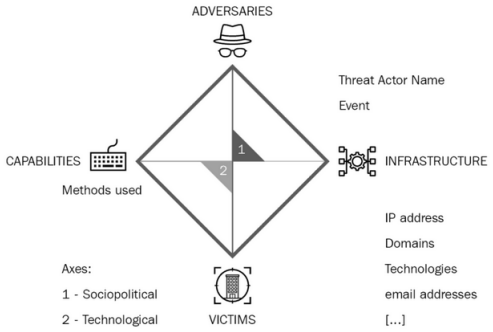
B. Metodit

Uhkien metsästykseen on olemassa lukuisia erilaisia metodeja, mutta erityisesti kolme metodia on laajasti käytössä. Nämä kolme metodia ovat timanttimalli (eng. Diamond model), kyberhyökkäysketju (eng. cyber kill chain) ja MITRE ATT&CK [10]. Huomioitavaa on, että uhkien metsästystä ei ole vakinaistettu ja sen suorittajat tekevät metsästystä erilaisilla metodeilla riippuen tarpeista ja resursseista [22]. Tarkastellaan seuraavaksi tarkemmin kolmea edellä mainittua metodia.

MITREn ATT&CK -kehys on kuvaileva malli, jonka avulla tutkitaan hyökkääjän aktiviteetteja, joita hyökkääjä pystyy toteuttamaan saadakseen jalansijaa ja operoidakseen esimerkiksi yritys- tai pilviympäristössä, älypuhelimissa tai ICS-järjestelmissä. Kehys tarjoaa yleisen taksonomian kyberturvallisuusyhteisölle, joiden avulla voidaan selittää hyökkääjän toimintaa. Kehys käyttää 14:ää eri taktiikkaa, joita käytetään käsittämään erilaisten menetelmien sarjoja. Jokainen taktiikka kuvaa taktista tavoitetta, eli miksi hyökkääjän käytös on tietynlaista. Esimerkiksi taktiikka ”isku” (eng. impact) tarkoittaa yritystä estää kohteen pääsy hänen omaan järjestelmäänsä. Taktiikka sisältää myös järjestelmän manipuloinnin tai tuhoamisen. [29] Tarkemmin ATT&CK-kehyksen taktiikoita ja niihin sisältyviä tekniikoita voi tarkastella MITRE:n nettisivulta.

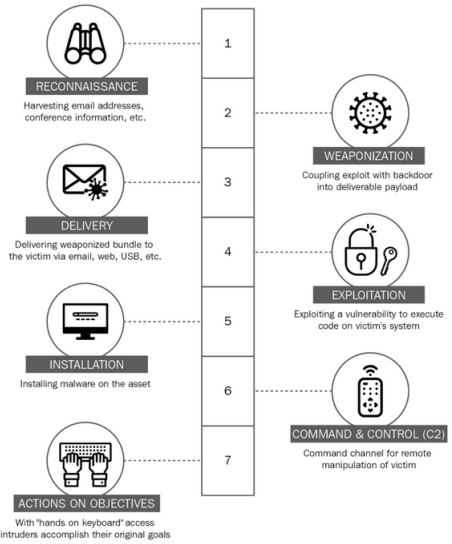
Timanttimalli (eng. Diamond model) on yksinkertainen keino seurata tunkeutumisrikkomuksia, sillä se auttaa määrittämään niihin liittyvät pienetkin yksityiskohdat. Se sisältää neljä pääominaisuutta: hyökkääjät, infrastruktuuri, kyvyt ja uhrit. Nämä ominaisuudet on yhdistetty sosiopoliittisilla ja teknisillä akseleilla. [25] Timanttimallia esittää kuva 2.

Kyberhyökkäysketju on Lockheed Martinin kehittämä 7 askeleen keino, jonka avulla voidaan tunnistaa vaiheet, joita hyökkääjän pitäisi seurata saavuttaakseen tavoitteensa. Tämän avulla voidaan rajata kohtia, joissa hyökkäys voidaan



KUVA 2. Timanttimalli [25]

pysäyttää. Ketju on saanut kritiikkiä siitä, että se ei selitä tarpeeksi hyvin sitä, miten nykyaikaiset hyökkäykset toimivat. [25] Hyökkäysketjua esittää kuva 3.



KUVA 3. Lockheed Martinin kehittämä kyberhyökkäysketju [25]

C. Metsästyksen toteuttaminen

Uhkien metsästyksen toteuttaminen tapahtuu tyypillisesti neljässä tai viidessä eri vaiheessa, riippuen lähteestä ja toteuttajasta. Esimerkiksi Badva ym. [22] jakavat metsästyksen neljään vaiheeseen ja Hillier ja Karroubi [21] taas viiteen vaiheeseen. Vaiheiden lukumäärästä riippumatta perusidea vaikuttaa olevan aina sama. Aluksi rakennetaan metsästystä edeltävä suunnitelma eli hypoteesi. Sen jälkeen analysoidaan ja luokitellaan uhka. Tämän jälkeen suunnitellaan ja toteutetaan tehtäviä, joilla uhkaa voidaan hallita, ts. toteutetaan uhkien metsästys. Metsästyksen jälkeen uhka määritellään ja tunnistetaan. Lopuksi uhka paikataan ja siitä raportoidaan. [22] [21] Tämän lisäksi Hillier ja Karroubi [21] lisäävät vielä viidennen vaiheen, uhkien seurannan. Uhkien metsästystä voidaan toteuttaa erilaisissa ekosysteemeissä, kuten kriittisessä infrastruktuurissa, käyttöjärjestelmissä ja IoT-laitteissa ja uhkia voidaan metsästää esimerkiksi lokeista, verkkoliikenteestä, binäärikoodista, dokumenteista ja järjestelmien konfiguraatioista [21].

D. Työkalut ja teknologiat

Lähdekirjallisuudessa tulee vastaan monia erilaisia työkaluja ja teknologioita, joita voi hyödyntää uhkien metsästyksen eri vaiheissa. Riippuu myös hyvin paljon tutkimuksesta, mitä työkaluja on käytössä. Tämä taas kertoo siitä, miten paljon erilaisia työkaluja on saatavilla ja miten eri tavalla organisaatiot ja yksilöt toteuttavat uhkien metsästystä. Yleisesti ennen metsästystä käytetään turvallisuusanalyytiikkatyökaluja, kuten HELK:ä [4]. Metsästysvaiheessa etsitään uhkia ATT&CK-kehyksen ja timanttimallin avulla joko manuaalisesti tai käytetään työkaluja, joilla tunnistetaan uhkia. Tällaisia työkaluja ovat muun muassa Splunk, VirusTotal ja ReliaQuest/Greymatter. [22] Mahboubi ym. puolestaan listaavat työkalut Caldera, Caret, Car, ATT&CK Navigator ja Tram. Uhkien metsästyksen jälkeen uhkasta luodaan uhkatietoa ja se päivitetään turvallisuusanalytiikkatyökaluihin sekä uhkatiedonjakoalustalle, kuten MISP:iin [4]. IBM [3] listaa metsästäjän tärkeisiin työkaluihin MDR:n, SIEM:n ja turvallisuusanalytiikkatyökalut. Näiden lisäksi voidaan hyödyntää myös muita työkaluja, kuten paketinanalysointityökaluja [3].

E. Tekoäly uhkien metsästyksessä

Tekoälyn povataan olevan yhä merkittävämpi työkalu uhkien metsästyksessä. Hillier ja Karroubi [21] toteavat, että tekoäly tulee laajentamaan uhkien metsästystä ja lisäämään sen automatisointia, joka tukee uhkien metsästäjiä. Tekoälyn hyödyntämisestä uhkien metsästyksestä löytyykin jo paljon tutkimusta.

Tekoälyä, erityisesti koneoppimista on käytetty aiemmissa tutkimuksissa metsästyksen automatisointiin ja hybridijärjestelmiin, jossa tekoäly tukee uhkien metsästäjää. Tekoäly voidaan valjastaa esimerkiksi päätöksen tekoon, mallien luomiseen sekä uhkatiedon keräämisen ja analysointiin avoimista lähteistä [1]. Tekoälyn etu uhkien metsästyksessä on sen kyky käsitellä valtavia määriä dataa nopeasti ja tarkasti [4].

Koneoppimismallien hyödyntämistä on tutkittu muun muassa kriittisen infrastruktuuriin suojaamisessa uhkien metsästyksen avulla [8] [7] ja mallit ovat saavuttaneet hyviä tuloksia. Esimerkiksi tutkimuksessa [7] onnistuttiin saavuttamaan satunnaismetsämallilla 95% tarkkuus ja AdaBoost-mallilla 95.7% tarkkuus.

IV. Havainnot

A. Haasteet

Vaikka uhkien metsästyksen voidaan todeta olla merkittävä uusi keino kyberuhkien torjunnassa, liittyy siihenkin useita haasteita. Badva ym. [22] kategorioivat tyypillisimmät uhkien metsästyksen haasteet metodeihin, dataan sekä organisaatioon ja ihmisiin liittyviin haasteisiin. Metodeihin liittyvät haasteet ovat tutkimuksen [22] tulosten perusteella yleisin haaste, jossa metsästäjien on vaikeaa yrittää identifioida, varmistaa ja paikata uhkia. Sindiramutty ym. [30] nostavat tutkimuksessaan merkittävimmiksi haasteiksi liiallisen datan, näkyvyyden,

datan laadun, havaitsemisen viiveen, hyökkääjien taktiikat sekä väärät positiiviset ja metelin. Hillierien ja Karroubin [21] listaamat haasteet liittyvät kysymyksiin mitä metsästää ja mistä metsästää sekä jatkuvasti kehittyviin uhkiin (eng. Advanced Persistent Threats, APTs). Kirjallisuudessa haasteita esitellään hyvin eri tavalla ja eri tärkeyksillä. Haasteet voidaan kuitenkin luokitella seuraavasti:

- Teknologiset haasteet: Dataa voi olla liikaa, se voi olla epätäydellistä ja monimutkaista ja sen laatu voi olla huonoa [22] [30] [4]. Järjestelmät ja työkalut voivat hajota [22].
- Ihmisten haasteet: puute ammattilaisista [4] [22], riittämätön osaaminen [22], käyttötapausten rakentaminen ja TTP:n monimutkaisuus [22], uhkien metsästyksen vaativuus ja monimutkaisuus [22]
- Prosessin haasteet: Uhkien metsästykseen liittyvät toimet laukaisevat usein virheellisesti turvallisuushälytyksiä kohdejärjestelmässä aiheuttaen ”meteliä”, joka vie huomiota oikeilta hälytyksiltä [30] [22]. Viive uhkien havainnoinnissa (manuaalinen analyysi) [30]
- Hyökkääjien aiheuttamat haasteet: Hyökkääjien taktiikat ja tekniikat kehittyvät jatkuvasti, joka vaikeuttaa uhkien metsästystä. [30] [4] [21] [22]

B. Hyödyt

Uhkien metsästys parantaa yleisesti kyberturvaa ja sen tarjoamia hyötyjä ovat:

- Potentiaalisten uhkien tunnistaminen ajoissa: uhkien metsästys mahdollistaa uhkien havaitsemisen ennen uhkien eskalaatiota [4]. Uhkien havaitseminen ajoissa myös vähentää hyökkääjien aiheuttaman vahingon määrää [3].
- Algoritmien ja mallien päivittäminen: uhkien metsästyksestä saatu tieto vaaran indikaattoreista ja TTP:stä ovat tärkeitä anomalioiden havaitsemisjärjestelmien algoritmien ja konfiguraatioiden sekä koneoppimismallien päivittämisessä, joka mahdollistaa niiden sopeutua paremmin muuttuviin uhkiin [4].
- Havaitsemattomien, staattisten turvallisuusjärjestelmien ohittaneiden uhkien havaitseminen: uhkien havaitsemisaika hyökkäyksen aloituksesta sen löytymiseen pienenee [3].

V. Keskustelu

A. Proaktiivinen uhkien metsästys täydentää reaktiivisia metodeja

Perinteisiä reaktiivisia metodeita uhkien torjunnassa ovat muun muassa palomuurit, virustentorjunta sekä turvallisuusinformaation ja -tapahtumien hallinta (eng. Security Information and Event Management, SIEM). Tällaiset reaktiiviset metodit auttavat verkkoja havaitsemaan hyökkäyksiä ja ehkäisemään toistuvia hyökkäyksiä parantamalla suojausstrategioita. Reaktiivisten metodien erityinen heikkous on, että ne eivät osaa ennakoida uhkia ja ennustaa niiden tulevia hyökkäyksiä. Taitavat hyökkääjät ovat myöskin hyvin tietoisia reaktiivisista metodeista ja osaavat ohittaa ne. Nämä ovat merkittävimpiä rajoitteita perinteisissä reaktiivisissa metodeissa, jonka takia useat organisaatiot ovat alkaneet metsästää uhkia proaktiivisesti. [10] Proaktiivinen lähestymistapa parantaa merkittävästi kyberturvallisuutta ja on viimeaikoina ollut trendaava aihe. Kuten myös IBM [3] on todennut, jopa 20% uhkista kykynee ohittamaan reaktiiviset turvallisuusmenetelmät ja uhkien metsästys on hyvä keino kukistaa nämä uhat, täydentäen reaktiivisia metodeja.

B. Uhkien metsästyksen tulevaisuuden näkymät

Uhkien metsästystä pyritään tulevaisuudessa varmastikin automatisoimaan entistä enemmän, tekoälyn avulla ja ilman. Tekoälyn rooli tulee myös korostumaan uhkien metsästyksessä, sillä tekoäly on omiaan valtavien datamäärien nopeassa käsittelyssä. Metsästyksen täysi automatisointi ei kuitenkaan ole mahdollista, sillä se vaatii dynaamista päättelyä, kuten intuitiota, luovuutta ja strategista ajattelua, jota ei ainakaan vielä pystytä paikkaamaan koneilla tai tekoälyllä [22]. Myös aiemmalla kokemuksella on merkittävä rooli metsästyksessä [2] [22] ja jotkut uhat on jopa löydetty ainoastaan metsästäjän aiemman kokemuksen avulla [22]. Lisäksi tekoälymallit vaativat jatkuvaa opettamista uudella datalla ja täysin uudenlaisen, ennennäkemättömän uhan löytäminen voi olla tekoälylle haastavaa, jopa mahdotonta. Tämä siksi, että tekoälylle ei ole opetettu koskaan vastaavaa uhkaa, joten se ei osaa etsiä sitä. Tekoäly ei myöskään kykene samanlaiseen dynaamiseen ajatteluun kuten ihminen, sillä ne perustuvat todennäköisyysmatematiikkaan ja algoritmeihin. Tästä huolimatta, tekoäly on jo nyt ja tulee olemaan entistä tärkeämpi apulainen metsästäjälle, erityisesti datan käsittelyyn liittyvissä tehtävissä. Tekoälyn ja automaation lisäksi oleellista on keskittyä tutkimaan uhkien metsästyksen nykyisiä haasteita, sillä ne laskevat merkittävästi metsästyksen tehokkuutta. Uhkien metsästyksen on todettu myös olevan sen toteuttajille kuormittavaa ja haastavaa, joten ihmisten kouluttamista ja metsästystyökaluja on syytä pohtia, jotta metsästys helpottuisi.

VI. Yhteenveto

Uhkien metsästys on proaktiivinen lähestymistapa kyberuhkien torjuntaan, jossa potentiaaliset uhat pyritään tunnistamaan ja paikkaamaan ennen kuin niitä ehditään hyödyntämään haitallisissa tarkoituksissa. Uhkien metsästyksellä pystytään havaitsemaan kehittyneitä uhkia, jotka osaavat kiertää ja piiloutua perinteisiltä staattisilta, reaktiivisilta turvallisuusmenetelmiltä, kuten palomuureilta. Tässä esseessä tarkastelimme aihetta syvällisemmin ja vastasimme kysymyksiin mitä uhkien metsästys on, mikä sen rooli ja merkitys kyberuhkien torjunnassa on, mitä haasteita siihen liittyy, miten ja millaisilla työkaluilla sitä tehdään ja miten aihetta on tutkittu. Uhkien metsästys on viime vuosina ollut trendaava aihe myös tutkimuksen kohteena ja tutkimuksen määrä sekä uhkien metsästyksen rooli kyberturvallisuudessa tulee varmasti kasvamaan entisestään hyökkääjien taktiikoiden ja tekniikoiden alati kehittyessä.

Lisäksi tulevaisuuden trendinä uhkien metsästyksessä on selkeästi havaittavissa tekoälyn hyödyntäminen, joka mah-

dollistaa lisääntyvän automatisaation ja laajemman toiminta-alan. Tekoäly tulee myös helpottamaan turvallisuusammattilaisten työtä monimutkaisessa uhkien metsästyksessä. Tulevaisuudessa aiheeseen liittyvät tutkimukset voisivat keskittyä tekoälyyn ja yleisesti haasteisiin, kuten ihmisten kouluttamiseen ja vaaran indikaattoreihin. Tekoälyä on selkeästi saatu jo hyvin kehitettyä, mutta edelleen tekoälymallit pitää saada tarkemmiksi. Unelmatavoite alalla olisi varmasti täysi automaatio esimerkiksi tekoälyn avulla, mutta siitä ollaan vielä kaukana, eikä sitä välttämättä koskaan saavuteta. Tämä siksi, että uhkien metsästys vaatii dynaamista ajattelua, joihin koneet eivät toistaiseksi pysty. Kun tekoäly vielä kehittyy, on myös syytä selvittää, miten ihmisistä koulutetaan tehokkaita ja taitavia metsästäjiä, jotta työ ei olisi niin raskasta ja vaikeaa sekä saadut tulokset paranisivat. Vaaran indikaattorit tarvitsevat tutkimusta, sillä väärät positiviiset hälytykset nousivat keskeiseksi haasteeksi uhkien metsästyksessä, kun turvallisuushälytyksiä aiheutuu turhaan vaarattomasta metsästystoiminnasta. Nämä kaikkinensa tehostaisivat uhkien metsästystä, jonka on todettu olevan vielä liian tehotonta [1].

LÄHTEET

[1] Z. Wang, "A systematic literature review on cyber threat hunting," 2022. [Online]. Available: https://arxiv.org/abs/2212.05310

[2] F-Secure. (9.2.2020) Meet the real threat hunters. [Online]. Available: https://blog.f-secure.com/meet-the-real-threat-hunters/

[3] IBM. (ei pvm.) What is threat hunting? [Online]. Available: https://www.ibm.com/topics/threat-hunting

[4] A. Mahboubi, K. Luong, H. Aboutorab, H. T. Bui, G. Jarrad, M. Bahutair, S. Camtepe, G. Pogrebna, E. Ahmed, B. Barry, and H. Gately, "Evolving techniques in cyber threat hunting: A systematic review," *Journal of Network and Computer Applications*, vol. 232, p. 104004, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804524001814

[5] A. B. Ajmal, M. Alam, A. A. Khaliq, S. Khan, Z. Qadir, and M. A. P. Mahmud, "Last line of defense: Reliability through inducing cyber threat hunting with deception in scada networks," *IEEE Access*, vol. 9, pp. 126 789–126 800, 2021.

[6] K. kielten keskus. (2024) Haku: proaktiivinen. [Online]. Available: https://www.kielitoimistonsanakirja.fi/#/proaktiivinen?searchMode=all

[7] A. Shan and S. Myeong, "Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application," *Sensors*, vol. 24, no. 15, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/15/4888

[8] M. Aragonés Lozano, I. Pérez Llopis, and M. Esteve Domingo, "Threat hunting architecture using a machine learning approach for critical infrastructures protection," *Big Data and Cognitive Computing*, vol. 7, no. 2, 2023. [Online]. Available: https://www.mdpi.com/2504-2289/7/2/65

[9] F. Aldauiji, O. Batarfi, and M. Bayousef, "Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art," *IEEE Access*, vol. 10, pp. 61 695–61 706, 2022.

[10] Z. Jadidi and Y. Lu, "A threat hunting framework for industrial control systems," *IEEE Access*, vol. 9, pp. 164 118–164 130, 2021.

[11] H. Rasheed, A. Hadi, and M. Khader, "Threat hunting using grr rapid response," in *2017 International Conference on New Trends in Computing Sciences (ICTCS)*, 2017, pp. 155–160.

[12] R. Puzis, P. Zilberman, and Y. Elovici, "Athafi: Agile threat hunting and forensic investigation," 2020. [Online]. Available: https://arxiv.org/abs/2003.03663

[13] K. Wafula and Y. Wang, "Carve: A scientific method-based threat hunting hypothesis development model," in *2019 IEEE International Conference on Electro Information Technology (EIT)*, 2019, pp. 1–6.

[14] K. Subramanian and W. Meng, "Threat hunting using elastic stack: An evaluation," in *2021 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 2021, pp. 1–6.

[15] P. Karuna, E. Hemberg, U.-M. O'Reilly, and N. Rutar, "Automating cyber threat hunting using nlp, automated query generation, and genetic perturbation," 2021. [Online]. Available: https://arxiv.org/abs/2104.11576

[16] D. Hermawan, N. G. Novianto, and D. Octavianto, "Development of open source-based threat hunting platform," in *2021 2nd International Conference on Artificial Intelligence and Data Sciences (AiDAS)*, 2021, pp. 1–6.

[17] L. Chen, R. Jiang, C. Lin, and A. Li, "A survey on threat hunting: Approaches and applications," in *2022 7th IEEE International Conference on Data Science in Cyberspace (DSC)*, 2022, pp. 340–344.

[18] M. Arafune, S. Rajalakshmi, L. Jaldon, Z. Jadidi, S. Pal, E. Foo, and N. Venkatachalam, "Design and development of automated threat hunting in industrial control systems," in *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, 2022, pp. 618–623.

[19] D. Javeed, M. T. Khan, I. Ahmad, T. Iqbal, U. M. Badamasi, C. O. Ndubuisi, and A. Umar, "An efficient approach of threat hunting using memory forensics," *International Journal of Computer Networks and Communications Security*, vol. 8, no. 5, pp. 37–45, 2020.

[20] M. N. S. Miazi, M. M. A. Pritom, M. Shehab, B. Chu, and J. Wei, "The design of cyber threat hunting games: A case study," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, 2017, pp. 1–6.

[21] C. Hillier and T. Karroubi, "Turning the hunted into the hunter via threat hunting: Life cycle, ecosystem, challenges and the great promise of ai," 2022. [Online]. Available: https://arxiv.org/abs/2204.11076

[22] P. Badva, K. M. Ramokapane, E. Pantano, and A. Rashid, "Unveiling the Hunter-Gatherers: Exploring threat hunting practices and challenges in cyber defense," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 3313–3330. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/badva

[23] A. Bhardwaj, K. Kaushik, A. Alomari, A. Alsirhani, M. M. Alshahrani, and S. Bharany, "Bth: Behavior-based structured threat hunting framework to analyze and detect advanced adversaries," *Electronics*, vol. 11, no. 19, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/19/2992

[24] MITRE. (ei pvm.) Homepage. [Online]. Available: https://attack.mitre.org/

[25] W. P. Maxam III and J. C. Davis, "An interview study on third-party cyber threat hunting processes in the us department of homeland security," *arXiv preprint arXiv:2402.12252*, 2024.

[26] K. Oosthoek and C. Doerr, "Cyber threat intelligence: A product without a process?" *International Journal of Intelligence and CounterIntelligence*, vol. 34, no. 2, pp. 300–315, 2021. [Online]. Available: https://doi.org/10.1080/08850607.2020.1780062

[27] CrowdStrike. (2023) What is cyber threat intelligence? [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/

[28] P. Rodriguez and I. Costa, "Artificial intelligence and machine learning for predictive threat intelligence in government networks," *Advances in Computer Sciences*, vol. 7, no. 1, pp. 1–10, 2024.

[29] V. Costa-Gazcón, *Practical Threat Intelligence and Data-Driven Threat Hunting: A hands-on guide to threat hunting with the ATT&CKTM Framework and open source tools*. Packt Publishing Ltd, 2021.

[30] S. R. Sindiramutty, N. Jhanjhi, and S. K. Ray, "Threat hunting and behaviour analysis," *Utilizing Generative AI for Cyber Defense Strategies*, p. 235, 2024.