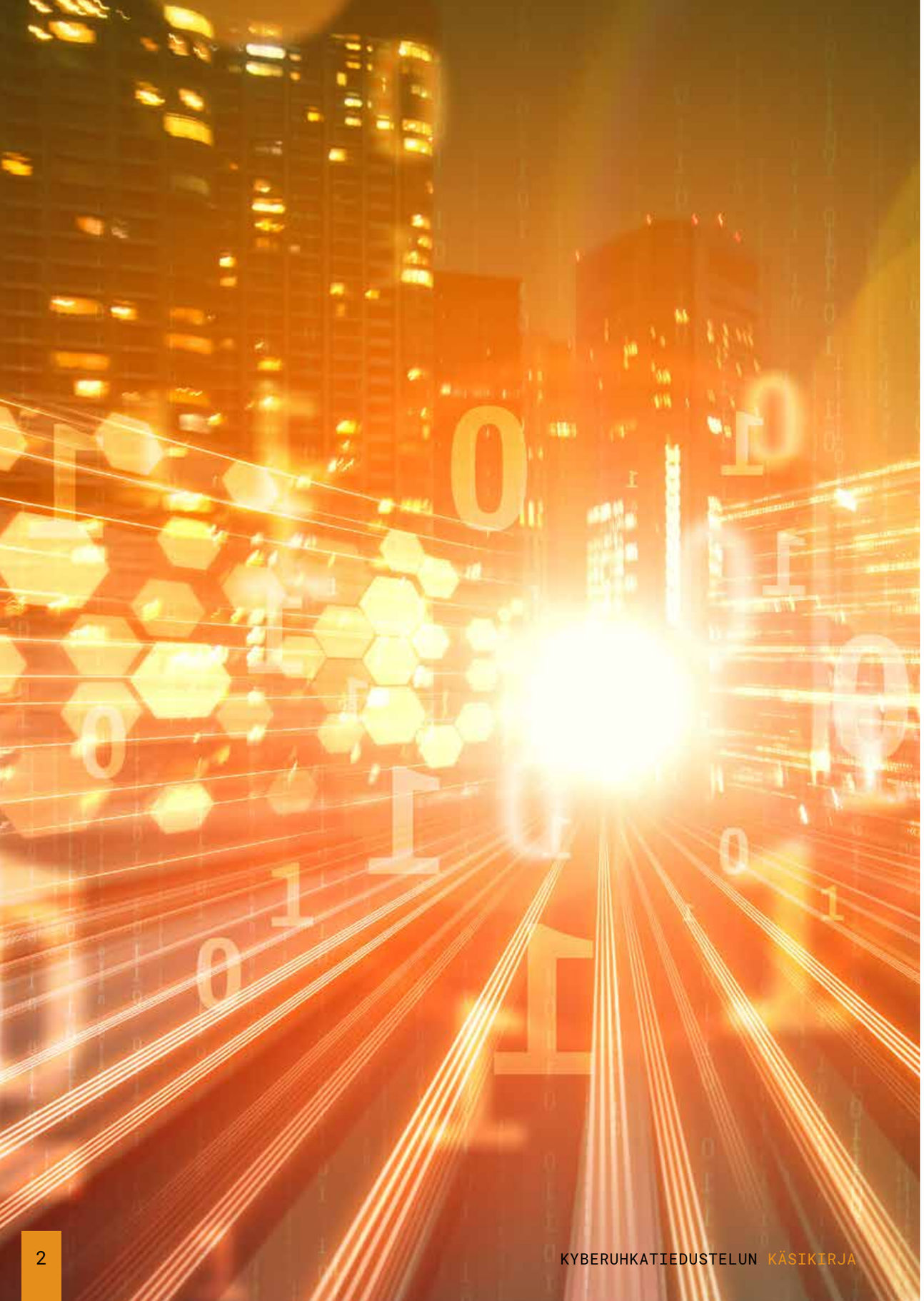
Cyberwatch Finland

DNV CYBER

KYBERUHKATIEDUSTELUN KÄSIKIRJA



ESIPUHE

Kyberuhkat muuttuvat ja kehittyvät jatkuvasti, ja organisaatioilta on alettu edellyttämään yhä enemmän kykyä omaksua ja hyödyntää kyberuhkia koskettavaa tietoa. Tämä korostuu paitsi nykyisistä käytännön tarpeista kuin myös lainsäädännön vaatimuksista. Vaikka EU:n verkko- ja tietoturvadirektiivi NIS2-direktiivi (EU2022/2555) ja sen kansallisesti sovellettavat versiot (Kyberturvallisuuslaki, Laki julkisen hallinnon tiedonhallinnasta ja Laki sähköisen viestinnän palveluista) eivät suoraan velvoita nimenomaan kyberuhkatiedon hankintaan tai hyödyntämiseen, velvoittaa se arvioimaan ja hallitsemaan kyberuhkia, muodostamaan näiden pohjalta organisaation kyberriskienhallinnan toimintamallin ja raportoimaan merkittävistä poikkeamista valvovalle viranomaiselle. Käytännössä tämän toteuttaminen vaatii kyberuhkatietoa. Samoin useissa yrityksissä käytössä oleva ISO/IEC 27000 Tietoturvallisuuden standardisarja edellyttää hallintakeinojen muodossa uhkatiedon keräämistä ja analysointia. Esimerkiksi ISO 27001:2022-standardin hallintakeino 5.7 (uhkatiedustelu) vaatii organisaatioita keräämään, analysoimaan ja tuottamaan tietoa tietoturvauhkista.

Yrityksen johto on uuden kyberturvallisuuslain myötä entistä velvoittavammassa roolissa, ja uusissa velvoitteissa korostuu johtohenkilöstön henkilökohtaisen vastuun kasvaminen riskienhallinnan toimenpiteiden toteuttamisessa – ja toteuttamatta jättämisessä. Kyberriskienhallinnan toimenpiteitä on käytännössä mahdotonta toteuttaa ilman reaaliaikaista uhkatietoa, jolloin käytännössä näkyvyys uhkakuvaan on hyvin rajallinen ja epätodenmukainen. Mitä laajempi ja kattavampi kyberuhkatieto yrityksellä on, sen paremmin valmistautumisaikaa yrityksellä myös on.

Tämän käsikirjan tavoitteena on avata tarkemmin sitä, mitä tämä kyberuhkatieto voi olla, mistä sitä saadaan sekä tarjota erilaisia menetelmiä, eli käytännön työkaluja kyberuhkatiedon hyödyntämisen prosessia suunnitteleville organisaatioille. Kirja on jaettu johdanto-osaan, jota seuraa neljään vaiheeseen (ohjaus; keräys / prosessointi; analyysi; ja jakelu) jaettu kyberuhkatiedon hyödyntämisen prosessi. Jokaisessa vaiheessa on erikseen esitelty, mitkä ovat organisaation johdon vastuut, mitä käytännössä tehdään (operatiiviset toimenpiteet) ja mitä konkreettisia työkaluja on mahdollista hyödyntää tässä työn vaiheessa.

Käsikirja on ensisijaisesti tarkoitettu suomalaisille kyberturvallisuuslain piiriin kuuluville kriittisen- tai puolustusalan toimijoille, mutta sen sisältö on hyödynnettävissä myös laajemmin organisaation toimialaan tai kokoon katsomatta.

Tämän käsikirjan on laatinut yhteistyössä Cyberwatch Finland ja DNV Cyber. Se on laadittu osana suomalaisten epäsuoran teollisuuden yhteistyön konsortion SOW275 Knowledge Mining for Intelligence -projektia. Tämän käsikirjan tavoitteena on lisätä suomalaisten kriittisten alojen organisaatioiden ymmärrystä, ja kykyä hyödyntää kyberuhkatietoa. Lähteinä on käytetty vastaavia kansainvälisiä teoksia, eritoten Recorded Futuren julkaisemaa Threat Intelligence Handbook:n 4:ttä painosta. Kirjan ohjeissa on pyritty ottamaan huomioon suomalainen toimintaympäristö ja kriittisten toimialojen vaatimukset sekä tarpeet.

Käsikirjan toimituskunta,
Helsingissä 2026

SISÄLTÖ

LUKIJALLE

Kyberuhkaympäristö on muuttunut perustavanlaatuisesti. Enää ei riitä, että haavoittuvuuksia korjataan viikkojen tai kuukausien aikajänteellä – todellinen mittari on aika. Useissa viimeaikaisissa tapauksissa olemme nähneet saman kaavan: haavoittuvuus tulee julki, exploitit ilmestyvät tunneissa tai päivissä ja massaskannaus sekä opportunistinen hyväksikäyttö alkaa lähes välittömästi. Hyökkääjät hyödyntävät haavoittuvuuksia ennen kuin organisaatiot edes ymmärtävät olevansa altistuneita niille. Erityisesti julkiseen verkkoon näkyvät palvelut ja legacy-ratkaisut muodostavat jatkuvan riskin.

Kyberuhkatiedustelu tarkoittaa, että ennakoidaan mitä voidaan käyttää hyväksi, ei vain teoriassa haavoittuvaa. Tämä on keskeinen osa operatiivista riskienhallintaa. Kyberuhkatiedustelun tehtävä on siirtää organisaatio reaktiivisesta puolustuksesta ennakoivaan – ja juuri nyt, kilpajuoksussa aikaa vastaan, tämä on ratkaisevan tärkeää.

Käsikirja antaa kattavan ja ymmärrettävän kokonaiskuvan Kyberuhkatiedustelusta (CTI) ja valmistaa organisaatiot määrämuotoiseen ja suunnitelmalliseen tapaan toteuttaa velvoitteitaan, ja parantaa heidän toimintaedellytyksiään.

Niko Candelin, Chairman, Board of Directors,
Finnish Information Security Cluster, FISC

Kyberala ry (FISC) edustaa Suomessa toimivaa kyberturvallisuusalaa. Yhdistyksen tarkoituksena on edistää digitaalisten teknologioiden riskienhallintaa, digitaalista turvallisuutta sekä toimialan edellytyksiä Suomessa ja EU:ssa yhteistyössä julkishallinnon, yritysten ja kansalaisyhteiskunnan kanssa. FISC suosittelee Kyberuhkatiedustelun käsikirjaa organisaatioille (2026) kaikille organisaatioille, jotka haluavat vahvistaa kyberturvallisuuttaan ja vastata kasvaviin sääntely- ja riskienhallintavaatimuksiin. Käsikirja tarjoaa käytännönläheisen ja suomalaiseen toimintaympäristöön sovitetun kokonaiskuvan kyberuhkatiedon (CTI) hyödyntämisestä johdon päätöksenteosta operatiiviseen toteutukseen. Käsikirja tukee erityisesti EU:n NIS2- ja DORA-säädösten sekä ISO/IEC 27001 -standardin tietojohtoisuuden periaatetta sekä auttaa organisaatioita kehittämään kypsyystasoaan hallitusti. Opas soveltuu niin kriittisille toimijoille kuin laajemminkin kaikille, jotka tavoittelevat parempaa tilannekuvaa, ennakointia ja vaikuttavia toimenpiteitä muuttuvassa kyberuhkaympäristössä.

Peter Sund, CEO,
Finnish Information Security Cluster, FISC

1 JOHDANTO

1.1 Tarpeet kyberuhkatiedolle

Modernissa tietoyhteiskunnassa jokainen organisaatio joutuu varautumaan kyberuhkiin – joko suoraan tai välillisesti. Kyberuhka on potentiaalinen tilanne, tapahtuma tai toiminta, joka voi vahingoittaa tai häiritä viestintäverkkoja ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti.[1] Uhkat ovat samaan aikaan uniikkeja, tiettyä organisaatiota tai toimialaa kohtaan, että yleisiä, organisaation kokoon tai toimintamalleihin katsomatta. Näihin uhkiin on pakko varautua ja vastata. Liian usein organisaatioiden varautumisen aste ei ole sillä tasolla, että kyberuhkan realisoitumiseen osattaisiin suhtautua riittävällä vakavuudella. Edelleen toimintamalleissa korostuu reaktiivinen ote proaktiivisen sijaan ja toimenpiteitä toteutetaan vasta, kun kyberuhka on realisoitunut, mainehaittaa on ehtinyt syntymään ja viranomaiset ovat kiinnostuneet tapahtuneesta. Merkityksellinen ja oikea-aikainen uhkatieto pyrkii tuomaan toimenpiteisiin ennakoitavuutta ja tehokkuutta, samalla minimoiden vahinkojen kustannukset. Kyberuhkatiedolla on pyrkimys saada aika ja taustatieto päätöksentekoon. Jotta uhkatiedosta on organisaatiolle hyötyä, pitää organisaation johdolla olla myös riittävä kyky tehdä siihen pohjautuvia päätöksiä viedäkseen organisaatiota oikeaan suuntaan. Kyberuhkatiedolla yksinään ei tee mitään, jos sitä ei osata käyttää oikein.

Kyberuhkatiedolla tarkoitetaan toimintaympäristöstä hankittua tai sitä koskevaa tietoa siitä, mitkä tai minkälaiset uhkat ovat kaikkein todennäköisimpiä ja miten niiltä voidaan suojautua. Käytännössä se on tietoa, joka ohjaa organisaation päätöksiä kyberturvaan tehtävistä investoinneista, toimintamalleista tai teknisistä ratkaisuista. On täysin mahdollista tehdä näitä päätöksiä ja ratkaisuja myös ilman uhkatietoa, mutta tällöin toimitaan käytännössä sokkona ja riski vääriin päätöksiin, tai mikä pahempaa, tärkeimpien uhkien huomiotta jäämiseen kasvaa merkittävästi. Kyberuhkatieto on siis edellytys entistä kehittyneempään ja tarkempaan tiedolla johtamiseen, kun suunnitellaan ja toimeenpannaan kybersuojausta.

Kyberuhkatieto, ja sen tuottamisen prosessi, on hyvin samankaltainen tiedustelutiedon ja –prosessin kanssa. Perinteinen tiedusteluprosessi on jatkuva, vaiheittainen toimintamalli, jolla kerätään, analysoidaan ja toimitetaan tietoa päätöksenteon tueksi. Tiedusteluprosessi jakautuu neljään vaiheeseen, joita ovat 1) ohjaus ja suunnittelu, 2) tiedonhankinta, 3) käsittely ja analyysi sekä 4) jakelu ja raportointi. Kyberuhkatiedon tuottamiseen kuuluu samoja vaiheita ja sen tavoite on myös samankaltainen: tiedon tuottaminen päätöksenteon tueksi. Kyberuhkatiedon kohdalla tavoite on erityisesti tuottaa lisäaikaa päätöksentekoon ja muuttaa reaktiivinen toiminta proaktiiviseksi eli ennakoivaksi. Käytännössä tavoitteena on havaita ja vastata uhkiin ennen niiden realisoitumista, jolloin torjunta on helpompaa ja vahinkoja ei pääse syntymään.

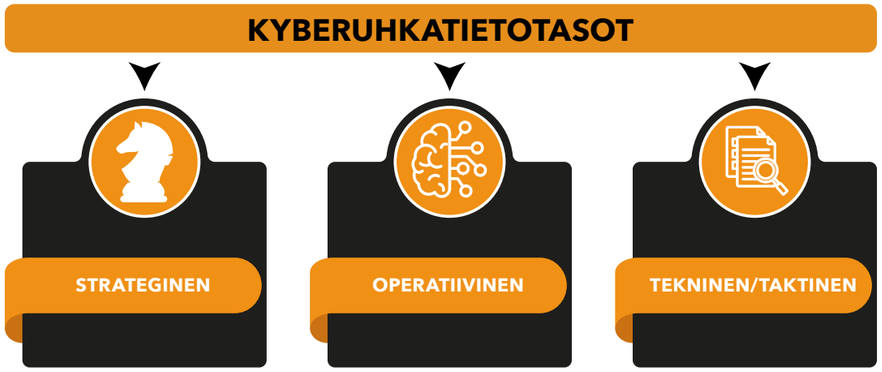
Käsitteenä kyberuhkatieto on laaja. Se käsittää esimerkiksi ymmärryksen uhkatoimijoiden motiiveista, yleisimmistä ja suosituimmista hyökkäysmuodoista, tiedot tunnistetuista haittaohjelmista tai listauksen IP-osoitteista, jotka ovat yhdistetty rikolliseen toimintaan. Juuri tiedon monipuolisuus ja toisaalta runsas saatavuus tekee sen käsittelystä haastavaa. Moni organisaatio ei tiedä mitä kaikkea tietoa sen tulisi kerätä, mistä sitä saadaan tai mitä sillä pitäisi tehdä. Suurimmalta osalta puuttuu myös kyky ja ymmärrys siitä, miten kyberuhkatietoa voidaan analysoida ja käyttää johtamisen ja ennakoinnin välineenä.

Uudet kansainväliset ja kansalliset lait, kuten jo aiemmin mainittu NIS2 sekä esimerkiksi DORA (Digital Operational Resilience Act) ja kyberkestävyyssäädös (Cyber Resilience Act) edellyttävät jatkuvasti valvotumpaa kyberriskien hallintamallin luomista, jossa pohjana täytyy olla arvio kyberriskien todennäköisyydestä ja vaikutuksista. Strukturoitu kyberuhkatiedon prosessi on kehitetty vastaamaan tähän ongelmaan. Se auttaa organisaatiota ymmärtämään miten kyberuhkatiedosta saadaan paras mahdollinen hyöty irti ja miten resursseja ei tuhlata epäolennaisen tai ei-relevantin tiedon hankintaan tai käsittelyyn. Se on myös luonteeltaan iteratiivinen ja itseään kehittävä. Tämä tarkoittaa, että se on helppo aloittaa käytännössä tyhjästä mutta samalla se luonnostaan kehittää itse itseään ja sitä toteuttavaa organisaatiota kohti korkeamman kypsyystason toimintaa ja parempaa kykyä tunnistaa, varautua ja reagoida kyberuhkiin. Parhaimmillaan hyvä kyberuhkatiedusteluprosessi myös mahdollistaa sen hyödyntämisen markkinoinnissa tai ulkoisessa viestinnässä. Organisaation omaama yksityiskohtainen ja ajantasainen kuva itseä ja omaa toimialaa koskevista kyberuhkista voi toimia etuna kilpailutustilanteessa sekä luotettavan toimijan maineen saamisessa ja ylläpitämisessä.

[1] Suomen kyberturvallisuusstrategia 2024–2035, käsitteet ja määritelmät, ss. 48–49.

1.2 Uhkatiedon tasot

Organisaatioiden ja etenkin ylimmän johdon on tärkeä ymmärtää, minkälaista erilaista uhkatietoa on saatavilla. Kyberuhkatieto jaetaan usein kolmeen tasoon auttamaan hahmottamista (kuva 1). Nämä tasot ovat strateginen uhkatieto, operatiivinen uhkatieto ja tekninen (joskus myös taktinen) uhkatieto.



Kuva 1. Kyberuhkatiedon tasot.

STRATEGINEN UHKATIETO

Yleinen tieto kybermaailman uhkatoimijoista, niiden toimintatavoista, muutoksista ja vallalla olevista trendeistä. Esimerkiksi katsaukset kybermaailman ilmiöistä tai tunnistettujen uhkatoimijoiden toiminnasta. Vastaanottajina organisaation ylin johto, tai yritystoiminnan riskeistä vastaava taho. Aikaväli harvempi, esimerkiksi kuukausittain tai kvartaaleittain tuotettava.

OPERATIIVINEN UHKATIETO

Organisaatiota itseään oleellisesti koskeva ja poikkeuksellisia, ei automatisoituja toimenpiteitä edellyttävä tieto. Esimerkiksi indikaatio itseen tai alihankkijaan kohdistuvasta uhkasta. Operatiivisessa uhkatiedossa analysoidaan muun muassa hyökkääjän motiiveja. Vaikuttaa päivittäiseen työhön. Keräys jatkuvaa, mutta todennäköisesti toimenpiteitä aiheuttavaa tietoa muutamia kertoja kuukaudessa.

TEKNINEN/ TAKTINEN UHKATIETO

Tekninen data, jonka avulla uhkatoimijoita, haittaohjelmia tai käynnissä olevia operaatioita voidaan tunnistaa tai estää. Esimerkiksi listaukset pahoista IP-osoitteista, CVE-haavoittuvuuksista tai muu mahdollinen IoC-data (ts. Indicators of Compromise, uhkatunnisteet). Päivittäistä ja jatkuvaa tiedon keräämistä ja suojausjärjestelmien päivittämistä. Usein koneluettavaa. Uhkatietoa kutsutaan taktiseksi silloin, kun tekninen uhkatieto muutetaan päivittäisiksi aktiivisiksi teknisiksi puolustautumistoimenpiteiksi konkreettisia uhkaindikaattoreja etsimällä.

Vaikka tason mukaan tehtävä luokittelu on hyödyllinen ja auttaa prosessin suunnittelussa, ei organisaatioiden kannata lukkiutua liikaa siihen käytännön prosessia valmisteltaessa. On kannattavampaa pohtia minkälaista tai mistä lähteistä saatavaa tietoa tarvitaan, kuin ajatella pelkästään tarvitaanko strategista tietoa ja kuinka paljon. Tärkein kriteeri, jota uhkatiedolle voidaan määrittää, on sen **käyttökelpoisuus**. Tällä tarkoitetaan sitä, että uhkatieto, jota organisaatio tuottaa tai hankkii, on luonteeltaan ja sisällöltään sellaista, että se vastaa tarpeisiin, johtaa suoriin toimenpiteisiin tai vahvistaa jo tehtyjen toimenpiteiden oikeellisuutta. Tällöin ei ole väliä minkä tason uhkatieto on kyseessä, mutta tasojen kautta pohtiminen auttaa silti hahmottamaan eri tiedonlähteitä ja tietotarpeita.

Uhkatietoprosessin ollessa käynnissä, tuotettua dataa tai informaatiota voidaan luokitella myös sen vakavuuden mukaan. Vakavuuteen perustuva luokittelu tarkoittaa sitä, kuinka merkittävästä uhkasta tai sellaisen indikaatiosta on kyse ja vaikuttaa siihen, miten tietoa käsitellään ja kuinka nopeasti siihen reagoidaan.

1.3 Uhkatietoprosessin kehittäminen ja arviointi

Kyberuhkatietoa voidaan tuottaa ja hyödyntää monella eri tasolla mutta useinkaan vähimmäisvaatimustaso, eli perustaso, ei riitä loputtomasti. Uhkatietoprosessin eri tasoja ja niiden ulottuvuuksia on hahmotettu alla olevassa taulukossa (taulukko 1). Taulukko toimii tiekarttana uhkatietoprosessia kehittäville organisaatioille, mutta sitä ei tule ymmärtää suorana ohjeena siitä, mitä tulee tavoitella. Jokaisella organisaatiolla on omat resurssit ja tavoitteet, jotka määrittävät sen, minkä laajuiseen uhkatietoprosessiin pyritään, ja missä suhteessa oma toiminta ja kumppanien hyödyntäminen tapahtuu. Uhkatietotasot jaetaan tässä neljään tasoon: 1) minimitaso, 2) kehittyvä prosessi, 3) kyberuhkatiedon tehokas hyödyntäjä sekä 4) ajatusjohtaja/innovaattori. Huomionarvoista on, että kaikkien ei tarvitse tulla ajatusjohtajiksi tai innovaattoreiksi tämän asian suhteen, vaan usein hyvä perustaso riittää. Kaikkien toimintaa on kuitenkin mahdollista kehittää ja parantaa.

Kyberuhkatietoprosessin laajuutta ja laatua on mahdollista arvioida myös yrityksen muilla työkaluilla mitattavan kypsyystason eli kybermaturiteetin kautta. Kypsyystaso kertoo sen, millainen kyberkyvykkyys organisaatiolla on suojautua kyberuhilta ja varmistaa liiketoiminnan jatkuvuus häiriötilanteissa. Kypsyystason voi määritellä erilaisten työkalujen (kuten Kyberturvallisuuskeskuksen Kybermittarin) avulla ja tasot suhteutetaan joko omaan toimialaan peilaten tai määritellään organisaatiokohtaisesti tavoitetasot. Kuitenkin suoran muihin tehtävän vertailun sijaan, organisaation on tärkeä ymmärtää, mikä taso juuri sille on tavoiteltava ja riittävä, mutta vertaileminen voi silti monella tavoin olla hyödyllistä. Kypsyystasoa voidaan verrata samalla alalla toimiviin vertaisiin yleisen tason määrittämiseksi ja kilpailuedun säilyttämiseksi. Usein kyberturvaan tai -uhkatietoon tehtävä investointi on helpompaa perustella sillä, mitä muut tekevät, kuin sillä, miten paljon alkuun vaikeasti hahmotettavaa hyötyä se tuottaa. Tämä voi olla tarpeen etenkin uhkatietoprosessin alkuvaiheessa, kun konkreettisia sen tuottamia hyötyjä ei vielä ole nähty.

	TASO 1: Perustaso	TASO 2: Kehittyvä prosessi	TASO 3: Kyberuhkatiedon tehokas hyödyntäjä	TASO 4: Ajatusjohtaja/innovaattori/edelläkävijä
Päätös: Mihin päätöksiin kyberuhkatietoa käytetään	Uhkatieto jää teknisten asiantuntijoiden tasolle	Uhkatietoa jaetaan organisaatiossa, mutta sen hyödyntäminen on vaihtelevaa ja suunnitelmatonta	Uhkatieto ohjaa päätöksentekoa sekä hankintoja ja sitä hyödynnetään laajasti organisaation eri toiminnoissa	Organisaatio tunnistetaan tuottamansa kyberuhkatiedon myötä ajatusjohtajaksi omalla toimialallaan
Toimintamallit: Tiedon saavuttamisen kyky	Uhkatiedon keräys on vähäistä ja lähteet yksipuolisia, tiedon keräys voi olla ulkoistettua	Uhkatiedon keräys on tavoitehakuista ja lähteet vaihtelevia	Uhkatiedon keräys ja j akaminen on monipuolista ja aktiivista, sitä tuetaan verkostojen avulla	Uhkatiedon keräys ja jakaminen on organisoitua ja johdettua, verkostoja hyödynnetään aktiivisesti
Työkalut: Teknologinen maturiteetti	Kyky käyttää erilaisia työkaluja on rajattu: esimerkiksi tietoturvakomponenttien valmistaja lähettää uhkatietoa suoraan laitteen estolistalle	Kyky hyödyntää parhaita työkaluja ja uutta teknologiaa on muutamien työntekijöiden hallussa ja resursseja vähäisesti	Uusien innovaatioiden arvo tunnistetaan ja niitä pyritään hyödyntämään, mutta toiminta on ad-hoc pohjaista eli tapauskohtaista tai suunnittelematonta	Uusien teknologioiden hyödyntämistä suunnitellaan ja siihen panostetaan, organisaatio testaa ja on edelläkävijä innovaatioiden hyödyntämisessä
Tavoite: Jatkuvan parantaminen	Kyberuhkatietoa kerätään ja hyödynnetään oppaiden ja käytänteiden neuvomalla tavalla	Kyberuhkatietoprosessi on kehittynyt organisaation itse tunnistamien omien tarpeiden ja tavoitteiden myötä	Kyberuhkatieto prosessi on uniikki ja kehittyy jatkuvasti verkostoissa opitun pohjalta	Organisaatio on kyberuhkatiedon edelläkävijä ja tuottaa sekä jakaa yhdessä kumppaneiden kanssa uusia menetelmiä, tietoa ja toimintatapoja, ts. opettaa muita

Taulukko 1: Uhkatietoprosessin eri tasot ja ulottuvuudet.

Samoin oman kypsyystason mittaaminen voi olla tarpeen toimittajia ja muita yhteistyökumppaneita, kuten liittoumia, tiedonjakorinkejä tai ei-kaupallisia kumppaneita, valittaessa. Mittaamista voi lähestyä usealla eri tavalla, mutta yleisimmin käytössä on erilaiset itsearviointilomakkeet, viralliset standardit tai kyberuhkatiedon operatiiviseen hyötyyn (kuinka usein uhkatiedon pohjalta tehdään päätöksiä) nojaavat mittarit. Etenkin usein alihankkijoiden kohdalla on hyödyllistä arvioida näiden teknologisia valmiuksia, eli mitä järjestelmiä he käyttävät tai minkälaisiin tietolähteisiin heillä on pääsy. Mittaustapoja valittaessa on tärkeä muistaa, että eri mittareilla saadut tulokset ovat vain harvoin vertailukelpoisia keskenään. Kumppaneita valittaessa organisaation on syytä keskittyä enemmän nimenomaan omiin tarpeisiin ja riskiarvioihin vastaamiseen, kuin sen kannalta vähäisesti merkittävien mittareiden tuloksiin. Lisäksi tiettyä tasoa tai tiettyjä toimintoja voidaan ja kannattaa vaatia alihankkijoilta, vaikka mitään konkreettista maturiteettimittaria ei edes käytettäisi.

Kypsyystason mittauksen ensisijaisena tavoitteena on organisaation kypsyyden selvittäminen ja sitä kautta sen kehittäminen. Uhkatietoprosessin tason mittaaminen on hyödyllistä myös prosessin kehittyessä, organisaation seuraavien askeleiden tunnistamisessa ja oman luotettavuuden varmistamisessa. Kun alkutilanne on kartoitettu ja dokumentoitu, on myöhemmin kehitys helpompi nähdä. Vertailu muihin saman toimialan kilpailijoihin ja sen tuloksena syntynyt kilpailuetu auttaa perusteltaessa investointien tarpeellisuutta ja hyödyllisyyttä. Juuri prosessin kehittymistä ja sitä, kuinka hyvin se vastaa asetettuihin tavoitteisiin ja tunnistettuihin tarpeisiin, voidaankin pitää yhtenä tärkeimmistä kyberuhkatietoprosessiin liittyvistä mittatavista asioista.

Organisaation kybermaturiteetin kasvattaminen on prosessi, jossa organisaatio siirtyy sattumanvaraisesta tietoturvasta enemmän systemaattiseen, riskipohjaiseen ja ennakoivaan toimintatapaan, jossa yhdistyy ihmiset, prosessit ja teknologia. Organisaation kybermaturiteettia eli -kypsyyttä voidaan kasvattaa arvioimalla aluksi organisaation nykytilanne, eli lähtötilanne eri menetelmiä (esimerkiksi myöhemmin kuvattu Gap-analyysi) hyödyntäen. Tämän jälkeen tunnistetaan keskeiset riskit ja määritetään niille hallintatoimet, johon johto laatii toimintasuunnitelman ja resurssit. Maturiteetin kasvattaminen alkaa perusasioiden kuntoon saattamisella, mistä yksi keskeisimmistä on kyberturvallisen organisaatiokulttuurin luominen kouluttamalla henkilöstöä. Toinen keskeinen toimenpide on sellaisten teknisten toimenpiteiden käyttöönotto, jotka parantavat päivittäistä tietoturvallista toimintaa. Kyberkypsyys kasvaa sitä mukaan, kun toimintatapoja ja prosesseja kehitetään jatkuvan palautteen ja muuttuvan kybertoimintaympäristön mukaan.

1.4 Ulkoistaminen ja yhteistyökumppanien luotettavuus

Kyberuhkatietoprosessi perustuu lähes aina enemmän tai vähemmän tiedon jakamiseen ja yhteistyöhön. Se on luonteeltaan niin laaja ja monipuolinen kokonaisuus, että parhaimminkaan resursoidun organisaation ei ole järkevää pyrkiä tuottamaan ja tekemään kaikkea itse, vaan tärkeä osa onnistunutta prosessia on myös oikeanlaisten yhteistyökumppanien hankinta. Kaikkea ei myöskään tänä päivänä ole kannattavaa tehdä itse: jos yrityksen omat kybertiedot- ja taidot ovat vajavaiset, on usein investointi luotettavaan kyberturvallisuuskumppaniin enemmän kuin perusteltu. Kumppanuudet voivat olla niin tasavertaisia tiedonjakoverkostoja kuin alihankkija- tai toimittajasuhteita, joiden kautta hankitaan tietoa tai osaamista kyberuhkatietoprosessia tukemaan. Paras kumppanuus on sellainen, jossa molemmat osapuolet voivat antaa ja saada tietoa. Tämä mahdollistaa molemmin puolisen kasvun ja kehityksen.

Kumppaneita valittaessa on tärkeä arvioida, mitä ne voivat tuottaa ja kuinka ne vastaavat organisaation tarpeisiin. On harvoin järkevää hankkia kumppania, joka tuottaa täysin samoja asioita, vaan yleensä kannattaa keskittyä omien tieto- tai osaamisaukkojen paikkaamiseen. Tämä tapahtuu tiettyyn kyberuhkatiedon tyyppiin tai sen tuottamisen prosessiin erikoistuneita kumppaneita hankkimalla. Tietyt uhkatiedon prosessin vaiheet vaativat myös kokemusta ja osaamista, ja tämä on usein helpompaa etenkin alkuvaiheessa hankkia ulkopuolelta kuin kehittää itse. Kumppanuussuhteita, olivat ne sitten alihankintaa tai tiedonvaihtoa, ei tule kuitenkaan ymmärtää staattisina. Niiden on tarkoitus kehittyä, ja ennen kaikkea kehittää, molempia osapuolia. Optimitilanteessa alihankkijalta ostettu osaaminen siirtyy omaan henkilöstöön, ja tiedonjakosopimukset kehittyvät eri osapuolten tullessa paremmiksi hyödyntämään kumppanien tuomaa tietoa sekä ymmärtämään, minkälaista dataa tämä kaipaa. Oikein valittu kumppani auttaa lisäämään organisaation kypsyyttä: jos organisaatio on kypsyytensä suhteen vielä alkuvaiheessa, paras kumppani on sellainen, joka kasvattaa organisaation omaa kyvykkyyttä yhteistyön edetessä.

Toinen tärkeä arvioinnin kohde on kumppanin luotettavuus. Kyberuhkatiedossa käytettävien kumppaneiden kohdalla luottamusta on kahdenlaista: palveluntarjoajan itsensä ja sen tuottaman tiedon luotettavuus. Molemmat ovat kriittisiä onnistuneelle uhkatietoprosessille. Palveluntarjoajan itsensä luottamus tarkoittaa samaa auditointivelvollisuutta, joka organisaatiolla on minkä tahansa IT-palveluntarjoajan kohdalla. Kyberhyökkäykset kohdistuvat yhä useammin alihankkijoihin ja, koska kyberuhkatietoa tuottavilla alihankkijoilla on usein pääsy useiden organisaatioiden järjestelmiin, ovat ne houkutteleva kohde kyberhyökkäyksille.

Organisaation luotettavuuden arviointi voi perustua esimerkiksi sertifikaatteihin, alihankkijoilla täytettäviin kyselylomakkeisiin tai yleiseen maineeseen. Kyberuhkatiedon tuottajien kohdalla on syytä muistaa, että kaikkien ei välttämättä tarvitse läpäistä niitä auditointikriteerejä, mitä esimerkiksi IT-palveluntuottajilta odotetaan. Mikäli ulkoinen taho esimerkiksi vain hankkii uhkatietoa eikä ikinä yhdistä omia järjestelmiään tai muutenkaan pääse organisaation tietojärjestelmiin käsiksi, ei vaatimusten tarvitse olla niin kovat. Näissäkin tapauksissa luotettavuuden taso kuitenkin vaikuttaa esimerkiksi siihen, minkälaista ja kuinka arkaluontoista tietoa organisaatio itse voi tämän toimittajan kanssa jakaa. Monessa tapauksessa prosessin läpäissyt uhkatieto saattaa sisältää suoria viittauksia itse organisaatioon tai paljastaa jotain sen suojaus- ja tunnistuskapasiteetista. Tämä tieto voi olla arvokasta myös pahantahtoisille toimijoille. Ulkoisten toimittajien luotettavuuden tulee määrittää paitsi sitä, miten syvään yhteistyöhön eri tahojen kanssa voidaan ryhtyä, myös sitä kuinka arkaluontoista tietoa näiden kanssa voidaan jakaa.

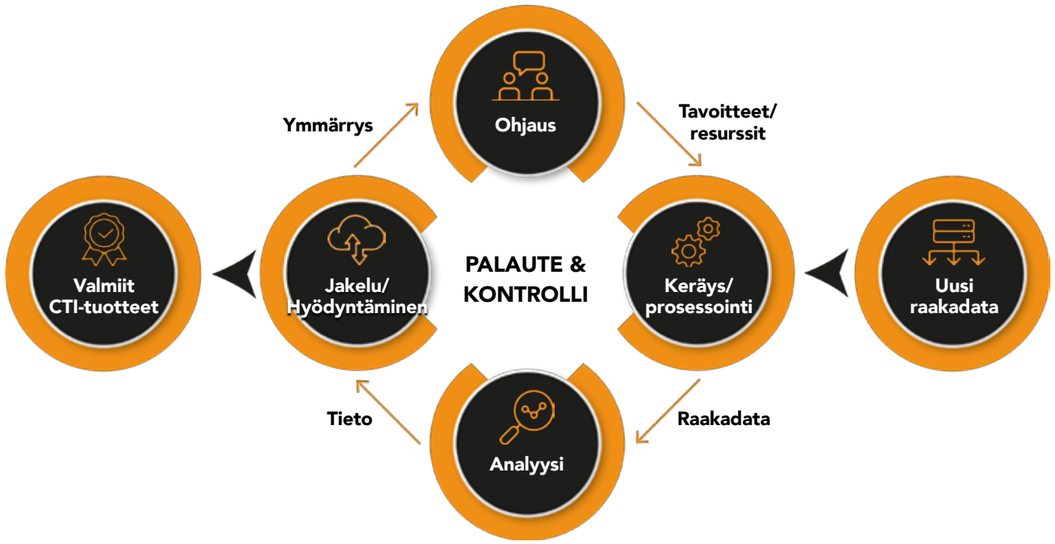
Toinen tärkeä luotettavuuden aspekti on ulkoisten toimijoiden tuottaman uhkatiedon varmuustaso. Tällä tarkoitetaan sitä, kuinka tarkkaa, ajankohtaista ja oikeaa sen tuottama tieto on. Huono uhkatieto voi pahimmillaan aiheuttaa paitsi uhkien huomiotta jättämisen, myös valheellisen turvallisuuden tunteen, jolloin juuri pahimmat vahingot yleensä tapahtuvat. Ulkoisesti, ilman ennakkotietoja voi olla vaikea arvioida sitä, kuinka luotettavaa tietoa tietty toimittaja tuottaa. Tiedon laatua on helpoin arvioida vasta sitten, kun sitä on saatu lähteestä hetken aikaa ja yleensä verrattu muihin samasta aiheesta tietoa tuottaviin lähteisiin. Luottamus ei myöskään jakaudu joko/tai (luotettava/ei-luotettava) arviointiasteikkoon, vaan luotettavuutta ohjaa usein motiivit ja jaetut intressit. Kumppanien valinnassa, usein kuitenkin joudutaan nojaamaan toimittajien maineeseen tai tämän olemassa olevien asiakkaiden määrään ja laatuun. Kriittisille toimijoille tietoa pitkään toimittaneen yrityksen tuottama data on todennäköisesti melko luotettavaa, kun taas tuntemattomampien tahojen tietoihin on syytä suhtautua varauksella.

Riippuen siitä, kuinka paljon dataa organisaatio kykenee prosessoida, voi myös epävarmemman luottamustason datan kerääminen olla silti hyödyllistä. Tietolähde, jota kukaan muu alalla ei käytä, voi muodostua hyvinkin arvokkaaksi, mikäli sen luotettavuus voidaan varmistaa pitkän aikavälin seurannalla. Yksikin kriittinen signaali kokonaan uudesta lähteestä voi olla juuri se, mikä tarjoaa mahdollisuuden havaita muutoin tutkan alapuolelta lähestyvä uhka etukäteen ja näin olla usein se kaikista merkityksellisin tietolähde. Usein epävarmojen tietolähteiden käyttö on kuitenkin järkevää vain uhkatiedon keräämiseen erikoistuneille organisaatioille, mutta se on luonnollisesti mahdollista kenelle tahansa, joka siihen haluaa panostaa tarpeeksi resursseja. Organisaation tulee ymmärtää eri luottamustasojen tiedon arvo, ja omien resurssien ja tarpeiden mukaan määrittää minkälaisilta ja minkä tasoisilta kumppaneilta sen kannattaa tietoa hankkia.

2 KYBERUHKATIEDON PROSESSI

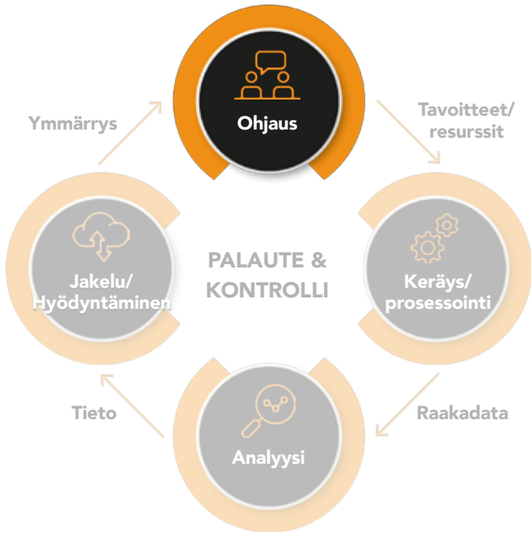
Kyberuhkatiedon hyödyntämistä kutsutaan kyberuhkatiedon prosessiksi (CTI-prosessi, Cyber Threat Intelligence -process). Syklisen uhkatietoprosessin avulla johdon kyvykkyyksiä ymmärtää kyberuhkatietoa on mahdollista kehittää ja ohjata. Se sisältää kaikki vaiheet ensimmäisestä suunnitelmasta alkaen tiedon keräämiseen ja hyödyntämiseen sekä toiminnasta saatujen kehittämistarpeiden toimeenpanoon seuraavaa keräyskertaa varten. Prosessin aikana kerätty raakadata muokkautuu informaatioksi ja lopulta päätöksentekoa tukevaksi tai ohjaavaksi tiedoksi. Se on luonteeltaan syklinen ja jatkuva, ja sitä on helppo kuvata tiedustelumaailmasta tutun tiedusteluympyrän kautta. Tiedusteluympyrä on kuvaus tiedustelutiedon keräämisen, analysoinnin ja hyödyntämisen prosessista, ja se on jaettu neljään tai viiteen vaiheeseen. Kyberuhkatiedon kohdalla neljän vaiheen ympyrä on käyttökelpoisin (kuva 2). Ympyrä jaetaan tässä käsikirjassa ohjauksen, keräyksen, analysoinnin ja jakelun vaiheisiin. Ympyrää ei tule käsittää prosessikaavioksi, jossa ensimmäisestä vaiheesta siirrytään aina linjassa seuraavaan. Todellisuudessa ympyrän jokainen vaihe on käynnissä samanaikaisesti muiden vaiheiden kanssa rinnakkain, ja useita CTI-prosesseja voi olla samanaikaisesti käynnissä. ”Ympyrä” kuvaakin lähinnä sitä, mitä uhkatiedolle tapahtuu missäkin vaiheessa ja miten se jalostuu raakadatasta päätöksentekoa tukevaksi ymmärrykseksi.

Tässä käsikirjan luvussa CTI-prosessin eri vaiheita käsitellään yksitellen, jakaen ne kolmeen eri näkökulmaan. Jokaisen vaiheen alussa käsitellään organisaation johdon vastuita ja toimenpiteitä. Tämän jälkeen käsitellään operatiivisen tason toimenpiteitä ja operatiivisen johdon velvollisuuksia. Lopuksi käsitellään käytännön ja teknisen tason työkaluja, joita kyseisessä vaiheessa on mahdollista hyödyntää. Tarkoituksena on, että jokaisen näkökulman edustajat saavat konkreettista hyötyä käsikirjan sisällöstä niin, että kokonaisuus hahmottaa mahdollisimman laajasti ja läpileikkaavasti koko kyberuhkatiedon prosessia.



Kuva 2: Kyberuhkatiedusteluympyrän yksittäinen prosessi.

2.1 Ohjaus



CTI-prosessin ohjaus on usein tärkein vaihe prosessin onnistumisessa. Ohjauksessa määritellään prosessin tavoitteet sekä resurssit ja mandaatti tavoitteiden saavuttamiseksi. Ilman huolellisesti tehtyä ohjausta, on todennäköistä, että resursseja hukataan vääränlaisen tiedon keräämiseen tai käsittelyyn, tai kaikkea saatavilla olevaa ja tarpeellista tietoa ei kerätä tai hyödynnetä. Johdon vastuulla onkin hyvin tehdyn ohjauksen avulla myös suojata yrityksen IT omaisuus erilaisilta uhkatoimijoilta, koska jo yksikin laiminlyönti voi johtaa merkittävään tietoturvatapahtumaan. Yksinkertaistettuna ohjausvaiheessa on kyse uhkatiedon keräämisen ja hyödyntämisen suunnittelemisesta sekä suunnitelmien käytännön toteuttamisen valmistelusta. CTI-prosessissa on loppukädessä kysymys turvallisuuteen tehtävästä investoinnista, kuten IT-omaisuuden suojaamisesta, ja mikäli sijoitukselle halutaan vastinetta, on se syytä suunnitella ja valmistella huolella.

2.1.1 Johdon vastuu

Ohjausvaiheessa organisaation johdon vastuu on merkittävä. Johto määrittää tavoitteet, uhkatiedon tarpeet ja käytettävissä olevat resurssit. Johto tekee myös päätökset esimerkiksi yhteistyökumppanien käytöstä prosessin eri vaiheissa. Se, kuinka suuren osan tästä toteuttaa strateginen johto ja mikä osuus lankeaa heille, jotka vastaavat operatiivisesta toiminnasta, vaihtelee organisaatioittain. Ideaalitilanteessa molemmat osapuolet ovat tiukasti mukana prosessissa. Prosessissa hyödynnetään ja konsultoidaan myös muita organisaation osia, eli kaikkia, jotka mahdollisesti tulevat kerättyä kyberuhkatietoa hyödyntämään. On luonnollista, että mikäli CTI-prosessi käynnistetään täysin tyhjästä, voi tämä tehtävä tuntua haastavalta. Tässä vaiheessa on jopa suositeltavaa konsultoida ulkopuolisia asiantuntijoita, mikäli kokemusta aiheesta ei ole riittävästi.

Käytännössä CTI-prosessin ohjauksessa on kaksi tehtävää:

1. Suojattavan omaisuuden tunnistaminen ja siihen kohdistuvien uhkavektoreiden kartoittaminen.
2. Tarvittavan tiedon ja sen tason (strateginen, operatiivinen, tekninen) määrittäminen, jotta päätöksentekoon saadaan tarvittava informaatio.

Ensimmäiseen kuuluu omaisuuden tunnistamisen lisäksi siihen kohdistuvien hyökkäysten tai häiriöiden vaikutusten kartoittaminen sekä suojauskohteiden priorisointi. Jälkimmäiseen kuuluu kysymykset, kuten ”minkälaista uhkatietoa tarvitaan”, ”kuka sitä voi tuottaa” ja ”missä muodossa kerätty tieto on parhaiten hyödynnettävissä”. On tärkeää ymmärtää ketkä kaikki omassa organisaatiossa kyberuhkatietoa tarvitsevat, missä muodossa ja laajuudessa sitä tarvitaan sekä mitkä ovat organisaation kyvyt hankkia ja käsitellä tietoa. Näiden ja muiden kysymysten perusteella organisaation johto määrittää tietotarpeen sekä sen täyttämisessä käytettävissä olevat resurssit (käytännössä usein henkilöstön ja pääoman). Hyvä lopputulos tässä vaiheessa on erilaiset konkreettiset kysymykset, joihin vastaaminen on loppuprosessin tehtävä. Tavoitteena on valita kysymykset, joihin halutaan vastaus, ja tunnistaa uhkat, joista halutaan ennakkovaroitus.

Kaikki organisaatiot eivät välttämättä tarvitse jokaisen eri tason tietoa, ja kysymyksiä voi olla mitä tahansa muutamista kymmeniin. Se, mitä käytännössä tarvitaan, eli minkälaisiin kysymyksiin halutaan vastaus, on jokaisen organisaation kohdalla yksilöllistä. On myös hyvä tunnistaa, että tietopyynnöt eivät ole ilmaisia, joten siksikin organisaation sen hetkiselle tietotarpeelle vastaavat kysymykset ovat olennaisia osata listata ja määrittää, ja karsia muut niin sanotusti turhat, mutta ”hyvä tietää” -kysymykset. Juuri tämän kartoittaminen on ohjausvaiheen tärkein tehtävä ylimmän johdon osalta.

Ohjauksen onnistumisen edellytyksenä on myös edellä mainittujen lisäksi ennakkovaroituksen määrittelyn tekeminen. Tämä tarkoittaa sitä, että johdon tulee määritellä ne asiat, joista se haluaa CTI-prosessin tuottavan organisaatiolle ennakkovaroitusta. Tätä kautta organisaation on myös helpompi määritellä ne triggerit eli ärsykkeet, jotka laukaisevat ilmoituksen tai muun välittömän reaktion, johon reagoida.

ESIMERKKIKYSYMYKSIÄ CTI-PROSESSISSA, RIIPPUEN ORGANISAATIOSTA JA SEN UNIIKISTA KONTEKSTISTA

Strategisen tason kysymyksiä:

"miten kyberuhkakenttä tulee kehittymään seuraavan vuoden kuluessa",

"miten geopolitiikka tulee vaikuttamaan meistä kiinnostuneiden uhkatoimijoiden operaatioihin",

"mistä asioista tai kehityksestä halutaan saada ennakkovaroitus",

"minkä trendin muutos voisi merkittävästi vaikeuttaa organisaation toimintaa tulevaisuudessa"

Operatiivisen tason kysymyksiä:

"minkälaiset hyökkäysmuodot ovat tällä hetkellä suosituimpia tunnettujen uhkatoimijoiden operaatioissa",

"missä kyberhyökkäyksiin liittyvää tietoa jaetaan"

Teknisen tason kysymyksiä:

"millä keinoin voidaan tunnistaa ja rajoittaa haittaohjelmien leviäminen tai tarttuminen omiin laitteisiin",

"mitkä IP-osoitteet on tunnistettu kuuluvan tietyille uhkatoimijoille, ja mistä tätä tietoa saadaan"

2.1.2 Operatiiviset toimenpiteet

Kun johto on määrittänyt strategiset tavoitteet, kysymykset ja tarpeet kyberuhkatiedolle, on operatiivisen tason vastuulla päättää, miten ne käytännössä saavutetaan ja minkälaisia työkaluja ja tukea tarvitaan näiden tavoitteiden saavuttamiseksi. Tämä tarkoittaa päätöksiä henkilöstöstä, yhteistyötahoista, investoinneista, käytettävistä menetelmistä sekä työkaluista. Kyseessä onkin tavallaan investointihanke kyberriskien hallintaan – jos investointiin ei ole mitoitettu oikeanlaisia resursseja, niin tulokset ja tätä kautta myös hyöty voi jäädä hyvinkin vaatimattomaksi. Tyypillisesti tässä vaiheessa käydäänkin vielä monipuolisesti keskusteluja ylimmän johdon kanssa tavoitteista ja mahdollisista keinoista.

Kun lopullinen suunnitelma on saatu valmiiksi, määrittää operatiivinen johto ne toimenpiteet, jotka on toteutettava ennen tiedonkeräysvaiheen aloittamista. Tämä voi käsittää esimerkiksi uuden henkilöstön palkkaamista, työkalujen hankintaa tai yhteistyösopimusten tekemistä kumppaneiden ja alihankkijoiden kanssa. Tässä vaiheessa käytännön toimenpiteet ovat yhä lähinnä kartoittamista ja suunnitelmien laatimista. Tarkoituksena on kuitenkin tuottaa konkreettisia, toteuttavissa olevia suunnitelmia, eikä enää ylätason tavoitelistauksia tai kysymyksiä, jotka kaipaavat vastausta.

Osaamisen ja henkilöstön kartoittaminen

Tärkeä osa ohjausvaiheen konkreettisia toimenpiteitä, on tarvittavan osaamisen kartoittaminen. Strategisen tason kyberuhkatietoa voi toisinaan tuottaa paremmin kyberasiantuntijan sijaan geopolitiikan tai kansainvälisten suhteiden ammattilainen. Oleellista on varmistua siitä, että henkilöstöä löytyy paitsi uhkatiedon keräämiseen ja käsittelyyn, myös sen jakamiseen. Teknisen tason uhkatiedon kerääjä ja analysoija ei välttämättä ole paras henkilö kommunikoimaan tehtyjä havaintoja ei-teknisille henkilöille tai olemaan yhteydessä organisaation ulkopuolisiin tahoihin tiedonjakoa varten. Organisaation koko ja prosessin laajuus puolestaan määrittävät sen, kuinka paljon henkilöstöä kukin työvaihe sitoo, ja käytetäänkö samaa henkilöstöä prosessin eri vaiheissa. Ohjausvaiheessa organisaation tulee päätettyjen tiedonhankintakysymysten perusteella määrittää minkälaista osaamista ja mitä henkilöstöä prosessin toteuttaminen edellyttää.

Yhteistyökumppanien valinta

On luonnollista, että läheskään jokainen organisaatio ei kykene tai koe tarpeelliseksi koko CTI-prosessin läpikäymistä pelkästään omalla henkilöstöllä. On muistettava, että kyberuhkatieto on osa laajempaa rihmastoista uhkatietokokonaisuutta, eikä sitä tule ymmärtää tai nähdä irrallisena entiteettinä esimerkiksi ympärillä vaikuttavista geopoliittisista tapahtumista tai muusta organisaation omaan liiketoimintaan koskettavista uhkatiedoista. Uhkatiedon jakaminen ja sen vastaanottaminen organisaatiorajat ylittäen ovatkin varsin tärkeä osa CTI-prosessia. Tiedonjakoverkostoihin osallistuminen, alihankkijoiden käyttäminen joissain CTI-prosessin vaiheissa ja uhkatiedon jakaminen ovat tehokkaita keinoja parantaa lopputuloksia, etenkin mikäli oma kyvykkyys tiedonkäsittelyyn tai sen keräämiseen on omalla organisaatiolla rajallinen. Esimerkiksi kansalliset ISAC-tiedonvaihtoryhmät ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä, joissa käsitellään erilaisia alakohtaisia kyberuhkia ja hyviä käytäntöjä niiltä suojautumiseen. Onkin hyvä ymmärtää, että tiedonjako kyberuhkia koskien on lähes aina vastavuoroista. Pelkästään hyödyn etsimisen sijaan, organisaatioiden tuleekin pohtia, miten ne voivat itse tuottaa lisäarvoa millekäkin verkostolle, sillä tämä usein johtaa myös vastaanotettavan tiedon laadun parantumiseen.

Yhteistyökumppanien valitsemista ja auditoimista on käyty tarkemmin läpi luvussa 2.4, mutta mikäli valmiiksi valikoituja kumppaneita ei vielä ole, on se luonnollista tehdä prosessin tässä vaiheessa. Kun yhteistyötahot ovat selvillä, päätetään tässä vaiheessa prosessia siitä, miten niitä käytetään. Ulkoistetaanko esimerkiksi osa tiedon keräyksestä tai analysoinnista kokonaan? Kuinka paljon eri kumppaneilta tai verkostoista saatavaan dataan luotetaan? Tekeekö organisaatio itse muuta, kuin vastaanottaa tietoa ja jakaa sen sisäisesti tarpeellisille tahoille? Miten yhteistyötä konkreettisesti tehdään, eli mitä laitteita ja verkostoja käytetään? Nämä ovat muun muassa niitä kysymyksiä, joihin tässä prosessin vaiheessa pyritään saamaan vastaus.

Operatiivisten toimenpiteiden työkalut

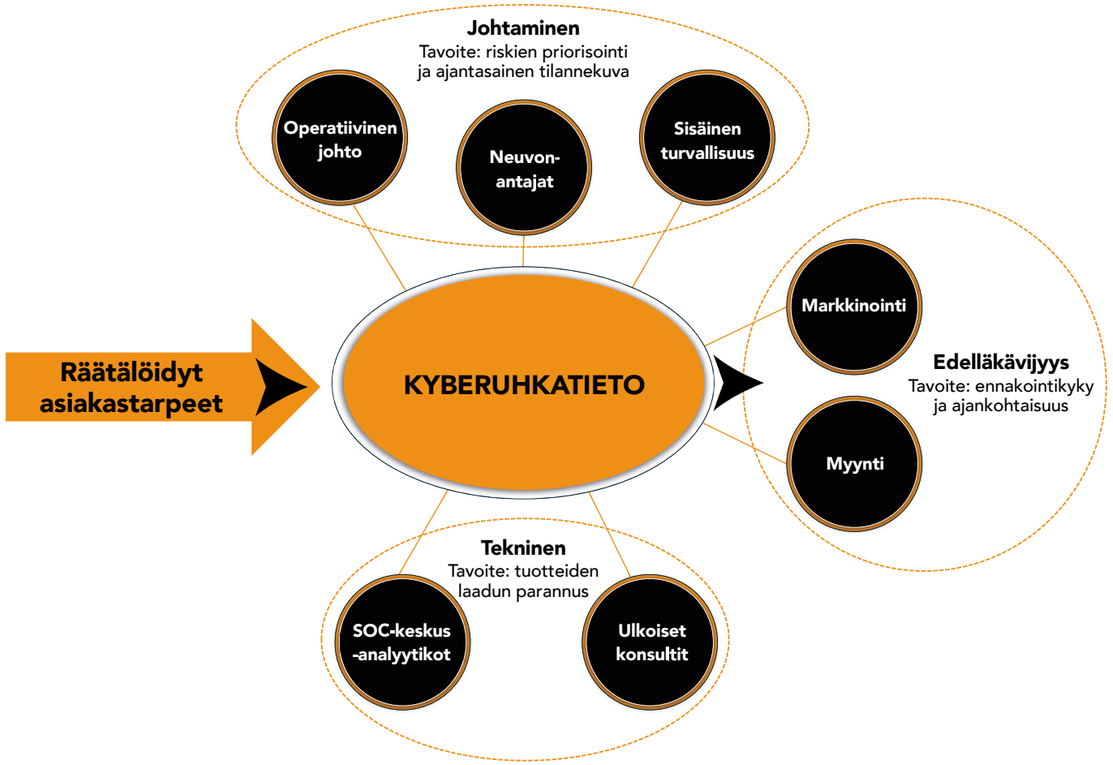
Ohjausvaiheessa tulee luoda suunnitelma työkaluista, joita CTI-prosessissa halutaan käyttää ja joihin on varaa resursoida. Vaikka käytännössä se, mitä ja miten työtä tehdään, muokkautuu usein prosessin aikana, on suunnitteluvaiheessa hyvä kartoittaa mahdollisia sovellus- tai välinehankintoja. Kun tiedetään mitä halutaan tehdä, on usein helppo seuraavaksi määrittää, minkälaisia työkaluja toteuttaminen vaatii, kuinka paljon näistä ratkaisuista on valmiiksi jo olemassa ja mitä pitää vielä hankkia. Käytettävät työkalut määrittävät jonkin verran sitä, missä muodossa ja minkälaista uhkatietoa tuotetaan. Työkalujen valinnassa onkin hyvä ottaa huomioon mitä muut alan toimijat tai yhteistyötahot käyttävät, ja ohjata valintoja yhteensopivuuden ja tiedonjaon helpottamiseksi. Tärkeää on pitää mielessä organisaation oma konteksti ja käytössä olevat resurssit, ja arvioida jokaisen työkalun tarpeellisuutta erikseen. Automaattisesti ei tule valita alalla suosituinta tai eniten käytettyä ratkaisua, vaan on hyvä ymmärtää se, mitä oma organisaatio tarvitsee. Tärkeää onkin ymmärtää sekä oman alan että spesifisti oman toimintakentän luomat erityisvaatimukset ja valita työkalut sekä kumppanit sen mukaisesti. Hyvä on myös huomioida, että isommilla organisaatioilla on mahdollisuus käyttää optimoidumpia ja kehittyneempiä työkaluja, kuin mitä keskisuurilla tai pienillä organisaatioilla.

Mikäli CTI-prosessissa käytetään alihankkijoita, on syytä varmistua siitä, mitä teknisiä ratkaisuja tai muita työkaluja näillä on käytössään. Tämä on syytä tehdä paitsi luotettavuuden ja kybermaturiteetin arvioimiseksi, mutta myös siksi, että alihankkijoiden käyttämät työkalut tulisi olla yhteensopivia omien työkalujen kanssa. Alihankkijoita valitessa on hyvä myös huomioida se, että niiden tuottaman tiedon tulisi olla luettavaa ja ymmärrettävää organisaation käytössä olevilla menetelmillä ja järjestelmillä.

Hyödyntämisen suunnittelu

Koko suunnitteluvaiheessa on tärkeää pitää mielessä se lopputulos ja lopputuote, jota CTI-prosessissa tavoitellaan. Kun tehdään valintoja henkilöstöstä tai työkaluista, on ne tehtävä sen perusteella, minkälaista tietoa lopulta halutaan tuottaa ja miten se parhaiten on hyödynnettävissä. Hyödyntämisen kannalta on esimerkiksi kriittistä, että saatu tieto on ymmärrettävässä muodossa ja kaikkien niiden henkilöiden ja tahojen saavutettavissa, jotka sitä tarvitsevat. CTI:n perusteella on tarkoitus tehdä sellaisia päätöksiä, jotka tukevat joko suoraan tai välillisesti yrityksen ydintoimintaa. Käytännössä tämä tarkoittaa organisaation sisäistä kartoitusta siitä, mitkä tahot ja missä muodossa uhkatietoa voivat hyödyntää. On prosessin tuloksena saatu uhkatieto sitten listaus tunnistetuista uhkatoimijoille kuuluvista IP-osoitteista tai monisivuinen analyysi siitä, miten kvanttiteknologia tulee vaikuttamaan käytössä oleviin salausjärjestelmiin viiden vuoden kuluessa, on oltava tiedossa, mitä lopputuotteelle tehdään.

Kyberuhkatietoa hyödynnetään jatkuvasti laajemmin ja useampiin eri tarkoituksiin (kuva 3). Räätälöidyt asiakastarpeet ohjaavat sitä, minkälaista kyberuhkatietoa organisaation tulisi kerätä. Saatujen suorien kyberuhkatietojen hyödyntämiskohteiden (kuten tieto kulkeutuu johdolle päätöksenteon tueksi ja toimenpiteitä ohjaavaksi tekijäksi tekniselle puolelle) lisäksi tuotettua tietoa, osaamista tai materiaalia voidaan hyödyntää esimerkiksi organisaation omassa markkinoinnissa tai omissa julkaisuissa, mikä luo edelläkävijän tai ajatusjohtajan asemaa organisaatiolle. Kyberuhkatiedustelun lopputuotteista onkin mahdollista saada varsinaisen tavoitellun hyödyn lisäksi muitakin sivutuotteita. Tulevaisuudessa on todennäköistä, että hyödyntäminen monipuolistuu entisestään. Kaikkien organisaatioiden ei tarvitse kuitenkaan heti suunnitella luovia tai yllättäviä käyttötarkoituksia. On luonnollista, että alkuvaiheessa käyttötarkoitukset ovat hyvinkin suoraviivaisia. Kun kokemusta uhkatiedon hankinnasta ja hyödyntämisestä kertyy, on helpompi muokata ja kehittää prosessia tuottamaan laajemmin hyödynnettävissä olevia tuotteita.



Kuva 3: Kyberuhkatiedon monipuoliset käyttötarkoitukset.
Lähde: kuva perustuu Pietari Sarjakiven luonnokseen (2025).

2.1.3 Käytännön työkalut

Ohjauksessa on kaikista CTI-prosessin vaiheista vähiten tarjolla selkeitä, konkreettisia työkaluja tai menetelmiä. ”Työkaluilla” tässä vaiheessa tarkoitetaankin enemmän keskustelu- ja listauspohjaista tekemistä. Suunnitteleminen tapahtuu yleensä aivoriihi- tai palaverityöskentelynä, joka voi olla hyvinkin vapaamuotoista. Käytettävissä on kuitenkin myös tutkittuja strukturoituja menetelmiä, jotka voivat tehostaa prosessia, parantaa sen luotettavuutta ja helpottaa kehittymistä. Lisäksi suojattavan omaisuuden ja siihen kohdistuvien uhkavektoreiden kartoittamiseksi on mahdollista käyttää laajasti erilaisia skannereita, tai verkko-omaisuutta kartoittavia teknisiä työkaluja. CTI-prosessi tuottaakin sitä arvokkaampaa tietoa, mitä paremmin yrityksen IT-omaisuus ja siihen kohdistuvat uhkat on kyetty tunnistamaan. Onnistunut CTI-prosessi voi parhaimmillaan antaa ennakkovaroituksen siitä, kuka iskee, mihin ja milloin isketään, ja miten se olisi mahdollista estää. Alla on esitelty kaksi erilaista työkalua, GAP-analyysi ja suojattavan omaisuuden kartoittamisen -malli, jotka ovat esimerkkejä menetelmistä toteuttaa ohjausvaiheen toimintoja strukturoidusti. Nämä eivät kuitenkaan ole ainoita eikä myöskään jokaiseen tilanteeseen soveltuvampia tapoja.

GAP-analyysi

Suosittu tapa lähestyä CTI-prosessia on GAP-analyysi. GAP-analyysi on menetelmä, jossa verrataan nykytilaa ja tavoitetilaa ja tunnistetaan niiden välinen kuilu (gap). Sen avulla organisaatio näkee, mitä puuttuu, mitä pitää kehittää ja millaisilla resursseilla tai prosesseilla tavoitetila saavutetaan. Tavoitteena on sitoa tietotarve yrityksen strategiaan ja liiketoimintaan. Analyysimenetelmänä se on monipuolinen ja eri malleja löytyy useita. Alla on listattuna esimerkki, miten GAP-analyysiä voidaan käyttää CTI-prosessin ohjausvaiheessa.

Nykytilan kartoitus:
- Mitä uhkatietolähteitä on jo käytössä?
- Miten tiedot kerätään, analysoidaan ja jaetaan?
- Käytetäänkö standardeja (esim. STIX/TAXII-teollisuusstandardit kyberuhkatiedon kuvaamiseen ja jakamiseen)?
  - STIX (Structured Threat Information eXpression): Standardisoitu kieli, jolla kuvataan uhkia, kuten haittaohjelmia, toimijoita, hyökkäystapoja ja indikaattoreita, tehden tiedosta koneluettavaa
  - TAXII (Trusted Automated eXchange of Intelligence Information): Protokolla, joka määrittelee, miten STIX-muotoista tietoa jaetaan automaattisesti, mikä tekee jakamisesta tehokasta ja turvallista
- Mitkä ovat henkilöstön osaamiset ja tekniset kyvykkyydet?

Tavoitetilan määrittely:
- Halutaanko uhkatiedon keruu automatisoida?
- Tarvitaanko integraatioita SIEMiin, SOC:iin tai muihin järjestelmiin?
- Millainen uhkatiedon hyödyntämisprosessi organisaatiolla pitäisi olla (esim. reagointi, analyysi, jakaminen)?

Puutealueiden tunnistaminen:
- Mitkä työkalut, prosessit, datalähteet tai osaaminen puuttuvat?
- Onko lainsäädännöllisiä, sopimuksellisia tai tietosuojahaasteita tai -vaatimuksia?
- Onko nykyinen kyvykkyys riittämätön tietyn uhkamallin osalta (esim. ransomware-toimijat, haavoittuvuusvaroitukset)?

GAP-analyysin avulla voidaan laatia konkreettinen kehityssuunnitelma:
- Mitä hankitaan, mitä kehitetään sisäisesti, mitä automatisoidaan
- Mihin prosesseihin tarvitaan ohjeistuksia
- Mikä koulutus tai osaaminen on tarpeen

Kyvykkyyden mittaaminen ja jatkuva parantaminen:
- Kun lähtötaso ja tavoite ovat tiedossa, voidaan mitata edistymistä ja tehdä uhkatiedonhallinnasta jatkuva prosessi

GAP-analyysi on hedelmällisin, kun siihen osallistuu laajasti henkilöstöä organisaation eri osa-alueilta. Pelkästään strategisen johdon lisäksi, on tärkeää, että mukana on käytännössä toiminnasta vastaavia henkilöitä ja teknisen tason asiantuntijoita. Mukana voi olla myös ulkoisia asiantuntijoita, etenkin mikäli osia prosessista on tarkoitus ulkoistaa tai kokemusta CTI-prosessista ei organisaation sisältä löydy. Yllä oleva esimerkki voi toimia mallina, jonka mukaisesti organisaatio rakentaa oman GAP-analyysinsä, mutta sitä ei tule käsittää yksiselitteisenä tai muuttumattomana mallina, johon ei voisi lisätä omia kysymyksiä tai pohdittavia asioita.

Suojattavan omaisuuden kartoittamisen -malli

Ohjausvaiheessa toinen käyttötarkoitus konkreettisille työkaluille on GAP-analyysiinkin kuuluva suojattavan omaisuuden kartoitus. Tähän on tarjolla erilaisia valmiita tarjolla olevia työkaluja ja malleja, joita voi hyödyntää toimialakohtaisten omaisuuksien kartoittamiseen. Mallilla tarkoitetaan oman suojattavan omaisuuden tunnistamista, mutta usein myös priorisointia ja mahdollisten uhkavektorien kartoittamista. Mitä suuremmasta organisaatiosta on kyse, sitä hankalampi tämä prosessi on. IT-omaisuus on jatkuvasti muuttuva, joten ajantasaisen kuvan ylläpitäminen on lähes mahdotonta ja suojattavien kohteiden määrä niin loputon, ettei mitenkään ole mahdollista kartoittaa kaikkiin kohdistuvia uhkia. Etenkin näissä tilanteissa toiminnan kannalta kriittisimpien omaisuuksien tunnistaminen ja niiden suojauksen priorisointi on tärkeää. Alla esitelty yksi menetelmä suojattavan omaisuuden ja siihen kohdistuvien uhkien kartoittamiseen.

Omaisuuden kartoitus:
- Valmiit listaukset omasta IT-infrastruktuurista
- Automaattiskannerit sisään ja ulospäin näkyvästä omaisuudesta

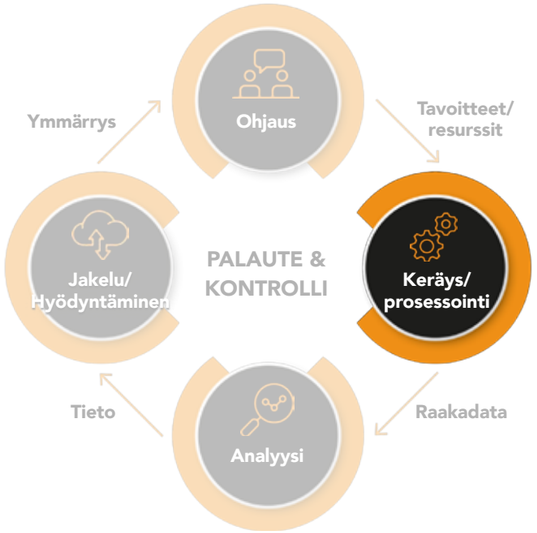
Tärkeimpien kohteiden tunnistaminen:
- Mitkä järjestelmät tai laitteet ovat kriittisiä toiminnan jatkuvuuden kannalta, onko niille olemassa vaihtoehtoa tai varmuuskopioita?
- Missä kriittisimpiä tai arkaluontoisimpia tietoja säilytetään ja kenellä niihin on pääsy?

Uhkien ja uhkatekijöiden kartoittaminen:
- Hyökkäyspinta-alan kartoittaminen: Miten tärkeimpiin tunnistettuisiin kohteisiin voitaisiin hyökätä: avoin verkkoportti, haavoittuva palvelin, heikosti konfiguroitu pilviympäristö?
- Haavoittuvuuksien hallinta: Miten hyökkääjä voisi edetä järjestelmästä toiseen? Mitkä ovat sisäiset yhteydet, joiden kautta kriittisimpään omaisuuteen voitaisiin päästä käsiksi?
- Uhkamallinnus: Kuinka todennäköisiä erilaiset uhkakuvat tai hyökkäysmuodot ovat? Mikä on todennäköisyys valtiollisesti motivoituneelle vaikuttamiselle omaa organisaatiota kohtaan? Kuinka houkutteleva kohde on ransomwaretoimijan näkökulmasta?
- Tämän kartoitusvaiheen tuottama tieto on olennainen osa yrityksen kokonaistietoturvan prosesseja

Näiden kysymysten avulla tuotetaan arvotettu tai luokiteltu lista suojattavasta omaisuudesta, jakaen se esimerkiksi kriittiseen, tärkeään ja ei-kriittiseen omaisuuteen. Tätä listaa verrataan tunnistettuihin uhkiin ja niiden todennäköisyyksiin. Kriittisimpien kohteiden kohdalla voidaan rakentaa tarkempia skenaarioita, miten eri uhkat juuri niihin voisivat vaikuttaa. Lopuksi listataan käytännön toimenpiteitä, miten näitä voitaisiin rajoittaa. Kartoitus on myös syytä toistaa ja päivittää säännöllisesti, se voi olla myös joltain osin jatkuvaa.

CTI-prosessin kannalta tärkeää on tunnistaa se, minkälaista tietoa tarvitaan suojauksen ylläpitämiseksi ja minkä tasoiset tai miten motivoituneet uhkatoimijat hyökkäävät todennäköisimmin organisaatiota kohtaan.

2.2 Keräys/prosessointi



Ohjausta seuraava vaihe on tiedon keräys ja sen prosessointi. Tässä luvussa käsitellään molemmat toiminnot, painopisteen ollessa keräysvaiheesta. Keräyksellä tarkoitetaan eri vaiheissa prosessointia olevan tiedon (raakadatan tai valmiiksi analysoidun tiedon) hankkimista edellisessä vaiheessa tehtyjen suunnitelmien mukaisesti. Prosessoinnilla tarkoitetaan kerätyn tiedon muuntamista yhtenäiseksi, käyttökelpoiseksi ja kontekstuaaliseksi uhkainformaatioksi, myöhempää analyysiä ja hyödyntämistä varten. Toisin sanoen, jotta tietoa on mahdollista hyödyntää, tulee se ensiksi löytää ja kerätä. Vasta, kun tämä kerätty tieto on jalostettu, on se käyttökelpoista.

Tämä vaihe on edellisen kanssa yhtä lailla kriittinen ja siinä tehdyt virheet vaikuttavat merkittävästi lopputulokseen. Etenkin uutta kyberuhkatiedon prosessia käynnistäessä keräysvaiheessa sorrutaan usein virheeseen, jossa tietoa kerätään yksinkertaisesti mahdollisimman paljon ja mahdollisimman monesta lähteestä. Vaikka runsas tietomäärä on periaatteessa hyvä, johtaa tämänkaltainen toiminta yleisemmin tilanteeseen, jossa syötettä on liikaa käsiteltäväksi ja tietoturvatiimit lamaantuvat turhien hälytyksien ja manuaalista läpikäyntiä vaativan tietomassan kanssa. Keräysvaiheessa onkin tärkeä muistaa edellisessä vaiheessa määritellyt tarkat tarpeet, ja ohjata toimintaa sen mukaan. Liiallinen tietomäärä voi johtaa yhtä herkästi virheisiin kuin puutteellinenkin keräys. Vain edistyneimpien ja eniten resursseja kyberuhkatietoprosessiin sijoittaneiden toimijoiden kannattaa kerätä kaikki mahdollinen saatavilla oleva tieto.

2.2.1 Johdon vastuu

Keräysvaiheessa organisaation johdon vastuu on pienempi kuin ohjausvaiheessa. Tärkeä keräysvaiheeseen liittyvä johdon vastuu on kumppanuussuhteiden luominen ja ylläpitäminen. Nykyisin merkittävä osa uhkatiedosta saadaan kumppaneilta tai verkostojen kautta, ja johdon tehtävä ylläpitää ja vahventaa näitä suhteita. Yksikään organisaatio ei yksin voi kerätä tai tuottaa kaikkea mahdollista tietoa, joten etenkin tämä on tärkeässä roolissa onnistuneessa CTI-prosessissa.

Keräyksessä toteutetaan niitä suunnitelmia, joita aiemmassa vaiheessa on asetettu ja ylimmän johdon tehtäväksi jää lähinnä toiminnan seuranta ja raporttien vastaanottaminen tai tarpeen vaatiessa vaatiminen. Tässä vaiheessa raporttien ei ole tarkoitus sisältää varsinaista uhkatietoa, vaan enemmänkin seurattava on sitä, miten hyvin asetetut tavoitteet voidaan käytännössä saavuttaa, ja tuleeko kesken keräyksen mieleen uusia aiemmin huomioimattomia tiedonlähteitä tai -tarpeita. Näiden huomioiminen on pääosin toteuttavien osien vastuulla, mutta organisaation johdon on syytä pysyä kartalla siitä, mitä tehdään ja miten prosessi sujuu, jotta esimerkiksi seuraavalla iteraatiokerralla voidaan ohjausvaiheessa ottaa huomioon nyt esiin nousseet puutteet tai haasteet. Yksinkertaisimmillaan tämä seuranta voi olla palautteen tai väliaikatiedotteiden pyytämistä ja parhaimmillaan kaikki sujuu suunnitelmien mukaisesti ja tiedotteet ovat hyvin lyhyitä.

Johdon vastuulla on pitää itsensä tietoisena keräykseen liittyvistä kustannuksista ja toiminnan tehokkuudesta. Keräystä toteuttaessa on helppo syntyä eräänlainen vauhtisokeus, kun dataa ja tietoa on saatavilla lähes loppumaton määrä, mutta sen liiallinen haaliminen ilman kykyä tai aikomusta hyödyntää sitä lähinnä syö tehoja prosessista. Tähän liittyy olennaisesti myös mahdollisten vinoumien tunnistaminen ja niiden hallinta: toisinaan ennakkoasetelmat voivat ohjata keräystä jo lähtökohtaisesti väärään suuntaan. Johdon tulee huolehtia, että organisaation tavoite on selkeä ja toimintaa toteutetaan suunnitelmien mukaisesti ja järkevissä mittasuhteissa organisaation kykyihin sekä tarpeisiin nähden.

2.2.2 Operatiiviset toimenpiteet

Keräys- ja prosessointivaiheen käytännön toimenpiteet jakautuvat raakadatan hankkimiseen valikoituja tiedonhankintaväyliä pitkin ja sen prosessointiin jatkokäsittelyä varten. Organisaatiosta ja toiminnan laajuudesta riippuen datalähteitä voi olla muutamista satoihin, ja ne voivat luonteeltaan olla mitä tahansa uutismedioista sisäisiin lokitietoihin. Alla esitettynä muutamia tyypillisimpiä datalähteitä mutta käytännön työssä on syytä muistaa, että mikä tahansa lähde, joka vaikuttaa tuottavan ohjauksessa määritettyihin tietotarpeisiin vastaavaa tietoa, on hyödynnettävissä.

ULKOISET EI-TEKNISET LÄHTEET
Laajempi ympäristötieto, joka vaikuttaa uhkakuvaan.

OSINT-lähteet (Open-Source Intelligence):
- Uutiset, blogit, tietoturvatutkimukset
- GitHub / Pastebin (vuodot, työkalut)
- Sosiaalinen media
- Akateemiset paperit
- MITRE ATT&CK-tietokanta (TTP-tiedot)

Yhteisöt ja verkostot:
- ISAC-verkostot (esim. finanssi- tai terveydenhuolto)
- CERT/CSIRT-yhteisöt
- Kansalliset kyberturvakeskukset
- Suljetut Slack/Discord/Telegram-tietoturvaryhmät

Valmiit tietoturvatuotteet:
- Trendianalyysit (esim. Gartner, Forrester)
- Tietoturvatalojen uhka-analyysit
- Palveluntuottajien tiedotteet (Microsoft, Checkpoint)

Dark web- ja rikollisfoorumit:
- Tor-foorumit
- Markkinapaikat
- Vuotopalvelut (data dumps)
- Ransomware-ryhmien vuotosivut

SISÄISET EI-TEKNISET LÄHTEET
Ei-puhtaasti teknistä tietoa, joka voi paljastaa haavoittuvuuksia tai riskialueita.

- Sisäiset turvallisuusraportit
- Riskianalyysit
- Red team / pentest -raportit
- Incident response -raportit
- Henkilöstön havainnot (esim. phishing-ilmoitukset)

ULKOISET TEKNISET LÄHTEET
Dataa, jota saadaan organisaation ulkopuolisista teknisistä syötteistä.

Uhkatieto-syötteet (Threat Feeds):
- IOC-feedit (IP:t, hashit, domainit)
- Maksulliset kuratoidut syötteet (Recorded Future, Mandiant, CrowdStrike, Anomali jne.)
- Ilmaiset syötteet (Abuse.ch, Spamhaus, CERTit)

Haavoittuvuustietokannat:
- NVD, CVE-tietokannat
- CERT/CC julkaisut
- Tuotevalmistajien tiedotteet (Microsoft, Cisco, Adobe…)

Haittaohjelmatietokannat:
- VirusTotal
- Hybrid Analysis
- Joe Sandbox
  URL- ja domain-reputaatiojärjestelmät

SISÄISET TEKNISET LÄHTEET
Nämä perustuvat organisaation omaan infrastruktuuriin.

Lokitiedot:
- Palomuurilokit
- IDS/IPS- ja NDR-lokit
- Proxy- ja DNS-lokit
- VPN- ja autentikaatiolokit
- Endpoint-lokit (EDR/XDR)

Verkkoliikennemittaukset:
- NetFlow / sFlow
- Packet capture –data

Palvelin- ja sovelluslokit:
- Web-palvelimet (Apache, Nginx)
- Tietokannat
- Pilvipalveluiden audit-lokit (Azure, AWS, GCP)

Turvajärjestelmät:
- SIEM
- DLP-järjestelmät
- Honeypotit ja honeynetit (hyökkäysindikaattorien keruu)

Keräys

Raakadatan keräystä voidaan kohdistaa heterogeeniseen joukkoon tietolähteitä. Samoin se voidaan keskittää tuottamaan tietoa niin potentiaalisista, vuosien päässä odottavista, kuin jo käynnissä olevista organisaatioon kohdistuvista hyökkäyksistä. Juuri tietomassojen helppo saavutettavuus ja monipuolinen tarjonta on se ansa, johon moni uusi kyberuhkatietoa keräävä organisaatio sortuu. On yhtä tärkeää ymmärtää, mitä tietoa ei tarvita tai ehditä käsitellä oman prosessin piirissä, kuin se, minkälaista tietoa tarvitaan. Keräysvaihe kehittyy jokaisella prosessin iteraatiokerralla ja saattaa muuttua merkittävästi uusien tietolähteiden myötä.

Keräysvaihe on mahdollista ulkoistaa käytännössä kokonaisuudessaan. Tällöin palveluntarjoaja hoitaa keräyksen, prosessoinnin ja seuraavan työvaiheen eli analyysin. Tyypillisempää on kuitenkin oman tiedonhankinnan ja ulkoisten lähteiden yhdistäminen. Verkostojen merkitys korostuukin keräysvaiheessa. Etenkin uhkatietoprosessin kehityksen kannalta on tärkeää, että organisaatio selvittää minkälaisia oman toimialan tai alueen verkostoja on olemassa ja mitä niihin liittyminen edellyttää. Ulkoisten lähteiden ja oman tiedonhankinnan yhdistämisessä on äärimmäisen tärkeä varmistua siitä, että tieto kulkee eri kerääjien toimesta yhteen paikkaan prosessointia ja myöhempää analyysia varten. Oli prosessoinnin toteuttaja sitten alihankkija tai organisaatio itse, on varmistuttava siitä, että kaikki kerätty tieto päätyy organisaation käyttöön, eikä verkoston järjestämistä tiedonjakopalavareista saatava tieto jää kokoukseen osallistuneen henkilön pöydälle.

Mikäli organisaation tavoitteena on oman uhkatietoprosessin kehittäminen tai maturiteetin parantaminen, on suositeltavaa, että kaikkea uhkatiedon keräystä tai varsinkaan prosessointia ei ulkoisteta. On luonnollista, että etenkin alkuvaiheessa luotetaan paljon ulkoisiin asiantuntijoihin. Se voi myös olla paras keino ymmärtää miten ja mistä tietoa kannattaa hankkia monikirjavien lähteiden joukosta. Oman osaamisen kehittäminen ulkoisen palveluntarjoajan tuella on pitkällä tähtäimellä järkevää ja usein taloudellista.

Prosessointi

Ennen kuin kerättyä raakadataa voidaan alkaa analysoimaan, on se muokattava käsittelyn mahdollistavaan muotoon. Tätä kutsutaan raakadatan prosessoinniksi. Erilainen raakadata vaatii eri verran prosessointia muuttuakseen hyödynnettäväksi. Joskus kerätty data voi olla valmista lähes sellaisenaan, esimerkiksi uuden haittaohjelman tunnusmerkit tai lista pahoista IP-osoitteista, joista kummatkin voidaan syöttää käytännössä suoraan palomuureihin tai SIEM-järjestelmiin. Toisinaan kerätty data vaatii paljonkin käsittelyä ja abstraktiotason säätämistä, että sen analysointi olisi paitsi tehokasta, mutta myös mahdollista. Käytännössä prosessointi voi olla datan siirtämistä samaan formaattiin, ylimääräistä ”kohinan” ja kaksoiskappaleiden poistoa sekä datan selkeyttämistä ja kielen yhtenäistämistä. Usein se sisältää metadatan luomista prosessin jäljitettävyyden parantamiseksi tai datan rikastamista yhdistelemällä useiden eri lähteiden syötteitä. Mitä se käytännössä pitää sisällään, riippuu organisaation itselleen asettamista tavoitteista ja tiedustelukohteista. Prosessointi on kokemuksesta ja asiantuntemuksesta hyötyvä vaihe, sillä onnistuessaan se vähentää työmäärää seuraavissa vaiheissa. Toisaalta siinä epäonnistuminen voi aiheuttaa tärkeiden tietojen jäämisen huomiotta.

Itse kerätyn tiedon lisäksi prosessointi usein koskee ulkoapäin, esimerkiksi mainittujen verkostojen tai yhteistyökumppanien, tuottamaa dataa. On hyvin tyypillistä, että tämä data vaatii jonkun verran muokkausta, jotta se voidaan yhtenäistää organisaation itse keräämänsä tiedon kanssa tai syöttää analyysiohjelmistoon tai tietokantaan. Etenkin organisaatioilla, joilla uhkatietoprosessi on hyvin laaja, ja kerättyä dataa vastaanotetaan laajasti ulkopuolelta, prosessointikyvyn on oltava korkea. Kyky vastaanottaa käytännössä missä tahansa muodossa olevaa dataa ja pystyä hyödyntämään eri tiedostomalleja, on sekä hyödyllistä että kriittistä tämänkaltaisessa ympäristössä toimiville organisaatioille. Vähimmillääkin kaikilla uhkatietoprosessia pyörittävillä organisaatioilla tulisi olla valmius yksinkertaisimpien ja yleisimpien tietomuotojen vastaanottamiseen. Prosessoinnin painetta voidaan kuitenkin vähentää pohtimalla jo etukäteen missä muodossa dataa todennäköisesti tullaan saamaan ja miten sen käsittely on yksinkertaisinta. Jos analyysityökalut on valittu ottaen huomioon se, minkälaista dataa tullaan keräämään, ei muokkausta välttämättä tarvita niin paljoa.

Joka tapauksessa prosessointi on vähintäänkin yhtä tärkeä vaihe kuin itse raakadatan keräys. Ilman sitä analyysissä tuhlataan resursseja epäollennaisten duplikaattien läpi kahlaamiseen ja tärkeät yhteydet saattavat jäädä huomaamatta. Oli analyytikkona sitten automaattinen työkalu tai ihminen, hyötyvät molemmat siitä, mitä paremmin data on jo keräysvaiheessa prosessoitu.

2.2.3 Käytännön työkalut

Uhkatiedon keräämisessä käytettävät työkalut vaihtelevat huomattavasti sen mukaan minkälaista ja mistä lähteestä dataa kerätään. Keräämistä voidaan tehdä manuaalisesti yksittäisten analyytikkojen toimesta, ja esimerkiksi strategisen analyysin raakadataa etsiessä se on yhä erittäin suosittua. Käytettävissä on kuitenkin jatkuvasti enemmän ja parempia automatisoituja keräystyökaluja, joita voidaan hyödyntää monenkin erilaisen datan keräämiseen. Nykyisin suurin osa automatisoiduista hakukoneista hyödyntää tekoälyä, yleisimmin kielimalleja, ja suorittaa pelkän keräämisen tai kaavinnan lisäksi myös jonkin verran prosessointia esimerkiksi poistaen duplikaatteja tai muokaten tulokset tiettyyn tyyppiin tai kielelle.

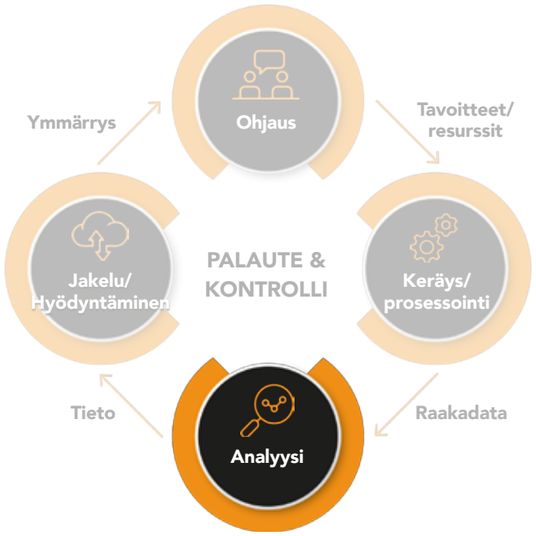
DATAN KERUUN TYÖKALUJA

- Automatisoidut hakukoneet/ kerätyt syötteet - esimerkiksi Google Alerts, Talkwalker ja Feedly
  - Mahdollistavat tiettyjen hakusanojen tai -ehtojen automatisoidun seurannan ja tuottavat ilmoituksia
- Tiedon poiminta- ja kaavintatyökalut – esimerkiksi Python-pohjaiset BeatifulSoup ja Scrapy
  - Automatisoituun verkkokaavintaan
- Pimeän verkon seurantatyökalut – Osana muita sovellusperheitä, kuten Crowdstriken X Recon, tai erikoistuneet alustat, kuten Cyber Intelligence House
  - Tuottavat raakadataa pimeästä ja syvästä verkosta, joko suoraan hyödynnettäväksi tai analyysin työstettäväksi
- Indeksointityökalut – esimerkiksi Splunk ja Elastisearch
  - Keräävät ja prosessoivat konetuotettua dataa lukuisista eri lähteistä, mahdollistavat sen tallentamisen ja tietomassoista tehtävät haut
  - Tarjoavat mahdollisuuksia kerätyn datan visualisointiin ja voivat toimia analyysialustoina

Keräystyökaluiksi voidaan myös mieltää suositut tiedonjakoalustat, joiden kautta organisaatio voi sekä vastaanottaa että jakaa uhkatietoa. Näistä esimerkiksi MISP (Malware Information Sharing Platform) on ilmainen ja avoimen lähdekoodin alusta, jota useat viranomaiset ympäri maailmaa käyttävät uhkatiedon koostamiseen ja jakamiseen. MISP-tarjoaa mahdollisuuden liittyä verkostoihin, joissa jaetaan standardoitua ja usein varmennettua uhkatietoa, helposti hyödynnettävässä muodossa. Sen lisäksi käytetään usein ilmaista ja avoimen lähdekoodin OpenCTI-työkalua, joka tarjoaa osittain samoja toimintoja, mutta toimii enemmänkin analyysiprosessia tukevana työkaluna. OpenCTI on myös työkaluna uudempi ja osittain myös päällekkäisien ominaisuuksien vuoksi haastajan asemassa, mutta parhaiten työkalut toimisivat rinnakkain.

Raakadatan prosessointiin käytettävät työkalut ovat datan mallintamiseen käytettäviä standardeja ja indeksointiin tai järjestämiseen suunniteltuja sovelluksia. Standardit, kuten STIX ja TAXII, mahdollistavat uhkatiedon jakamisen tarjoten strukturoidun tavan tallentaa tietoa. Riippuen raakadatan lähteestä tai tyypistä, sen konvertoiminen näihin standardeihin voi vaatia jonkin verran työtä, mutta lähtökohtaisesti molempia voidaan käyttää huomattavan erilaisen tai eri tasoisen uhkatiedon prosessointiin. Tekoälyllä on tulevaisuudessa myös yhä merkittävämpi rooli tämänkaltaisten kyberuhkatiedusteluprosessien raakadatan jatkojalostamisessa. Tekoälyä voi hyödyntää muun muassa etenkin datan esikäsittely- ja jäsennysvaiheessa, sen rikastamisessa sekä ylimääräisen kohinan poistamisessa. Kustomoidut tekoälyratkaisut tulevatkin entisestään helpottamaan analyytikon tai käsittelijän prosessointitaakkaa ja mahdollistavat usein lähes täyden automatisoinnin rutinoituneiden tietolähteiden datan prosessoinnissa.

2.3 Analyysi



Kolmas vaihe on analyysi. Analyysivaiheessa kerätty raakadata muokataan analyysiprosessin myötä uhkatiedoksi. Riippuen kerätyn datan laadusta, tämä voi olla hyvinkin yksinkertaista tai vaatia paljon työstämistä. Tavoitteena on lisätä raakadataan merkityksiä, yhdistellä eri lähteistä saatavaa tietoa johtopäätösten tekemiseksi ja lopulta tuottaa ymmärrettävää tietoa päätöksenteon tueksi ja näin konkreettisiksi toimenpiteiksi. Oleellista lopputuloksen kannalta on prosessin alkuvaiheessa selkeästi määritellyt tiedustelukysymykset ja tiedon tarpeet. Kyberuhkatiedustelussa analyysistä voi vastata yhtä hyvin niin ihminen kuin järjestelmä. Automaatio ja tekoälyn hyödyntäminen etenkin teknisen datan analysoinnissa kehittyy jatkuvasti, mutta ihmisanalyytikoilla on yhä merkittävä rooli etenkin strategisen tason analyysissä.

2.3.1 Johdon vastuu

Analyysivaiheessa johdon vastuu on valvomista, kontekstin syventämistä, tarvittaessa ohjaamista ja lopputuotteen hyödyntämisen valmistelua. Johdon tulee varmistaa, että analyysissä tarvittavat resurssit ja työkalut ovat saatavilla ja uusiin esille tulleisiin tarpeisiin pystytään vastaamaan. Suurin osa varsinaisesta ohjauksesta on lähtökohtaisesti tehty jo aiemmin siihen keskittyvässä työvaiheessa, mutta usein käytännön työssä tässä vaiheessa esiin nousee uusia tarpeita tai mahdollisuuksia. Henkilöt tai järjestelmät, jotka varsinaista analyysia tekevät, eivät välttämättä ole olleet mukana ohjausvaiheessa, eikä heillä välttämättä ole tarkkaa tietoa siitä, minkälaista ja mihin tarpeeseen tietoa on tuotettu. Johdon tehtävä on pysyä mukana prosessissa ja ohjata sitä tavoitteiden mukaiseen suuntaan, jotta siitä on paras hyöty myöhemmässä päätöksenteossa.

Tärkeä osa analyysivaihetta on tiedon raportointi. Analyytikoiden vastuulla on tuottaa raportteja siinä muodossa, että ne ovat ymmärrettäviä ja niiden sisältämä tieto hyödynnettävissä raportoinnin kohteelle. Usein tämä on organisaation johto. Etenkin uudenlaisen tiedon tai uusien lähteiden kanssa työskennellessä analyytikoiden voi olla vaikea alkuun ymmärtää minkälaisessa muodossa tieto tulee esittää. Tällöin johdon tehtävä on antaa palautetta ja vaatia raportoinnilta enemmän. Mikäli raportit, joita uhkatietoprosessi tuottaa, eivät johda käytännön toimenpiteisiin, tulee prosessia kehittää. Vaikka raportointimuoto ja muut seikat pitäisi olla sovittuna jo ohjausvaiheessa, on jatkuva palautteen antaminen ja pyrkimys kehittää prosessia tärkeää myös analyysivaiheessa. Dialogi analyytikoiden ja raportteja hyödyntävien tahojen välillä tulee olla avointa, ja molempien osapuolten on ymmärrettävä minkälainen tieto ja missä muodossa on tavoitteena.

Johdon ei kuitenkaan tule puuttua varsinaiseen analyysityöhön. Vaikka on suotavaa, että johto tietää mitä analyytikot tekevät ja mitä käytännön työ on, ei sen tule osallistua tai ohjata prosessia liian intensiivisesti vaan pikemminkin valvoa, että analyysi on mahdollisimman objektiivisesti toteutettu. Liiallinen mukana olo voi vähentää analyytikoiden vapautta tai ohjata johtopäätöksiä etenkin strategisen tason analyysissa, joten vaikka ohjaaminen ja ymmärrys on tärkeää, ei johdon tule puuttua liikaa itse prosessiin.

Käytännössä johdon vastuu analyysivaiheessa on sen varmistaminen, että työ on menossa oikeaan suuntaan. Kyberuhkatieto, tai sen tuotanto, ei saa “politisoitua”, eli sen ei pidä ohjautua organisaation (tai sen johtohenkilöiden) tavoitteiden, toiveiden tai mieltymysten mukaan. Jos organisaation johto on liian intensiivisesti mukana prosessissa, kasvaa riski, että analyysin tekijät pyrkivät mahdollisesti alitajuisesti tuottamaan tietoa, jota johtaja toivoisi näkevänsä tai piilottelemaan havaintoja, joiden ei uskota miellyttävän johtajaa. Tästä muodostuu prosessiin helposti ajatusvinoumia. Myös tässä on kyse kehittyvästä ja iteratiivisesta prosessista. Kun uhkatietoprosessia käydään läpi ensimmäisiä kertoja, on johdon osallistuminen todennäköisesti suurempaa. Tämä on usein hyvä, mutta sen rooli tässä työn vaiheessa ideaalitilanteessa vähenee sen mukaan, kun parhaat käytänteet selviävät ja ongelmakohdat ratkeavat toistojen myötä.

2.3.2 Operatiiviset toimenpiteet

Käytännön toimenpiteiden vaihtoehtoja on analyysivaiheessa lukemattomia. Se, miten dataa analysoidaan, riippuu siitä, minkälaista dataa organisaatio on kerännyt ja mitkä ovat tavoitteet tai asetetut tietotarpeet. Analyysivaiheessa pyrkimyksenä on erottaa tapahtumien tarkoitus kohinasta ja sattumasta. Yleensä analyysi tarkoittaa datan merkityksen määrittämistä, sen validointia eli luotettavuuden määrittelyä ja priorisointia eli kiireellisyysasteen päättämistä. Alla on esitetty yleisimpiä toimenpiteitä kyberuhkatiedon analyysiprosessissa. Listausta ei tule pitää kaiken kattavana tai yleispätevänä. Käytännön elämässä organisaation on tärkeä ymmärtää, miten kerätystä raakadatasta saadaan mahdollisimman paljon käytännön hyötyä. Usein analyysiprosessissa voidaan hyödyntää ulkoisia asiantuntijoita.

Poikkeamien tunnistus

Poikkeamien tunnistus on äärimmäisen tärkeä osa teknisen uhkatiedon analyysiä. Sitä voivat suorittaa ihmisanalyytikot mutta yhä enemmän osa-alueita tästä prosessista voidaan automatisoida. Poikkeamien tunnistuksessa usein massiivisesta määrästä lokitietoa etsitään poikkeamia mahdollisten tunkeutumisyritysten havaitsemiseksi tai jo järjestelmiin päässeen uhkatoimijan tunnistamiseksi. Lokitietoja kerätään joko osana normaalia tietoturvavalvontaa tai uhkatietoprosessin osana tiedon keräysvaiheessa. Analyysissä siitä etsitään joko mitä tahansa poikkeavaa tai ennalta tiedettyjä merkkejä uhkatoiminasta. Lisäksi analyysissä etsitään kampanjoiden välisiä teknisiä yhteneväisyyksiä, kuten samankaltaisia haittaohjelmia, komentokanavia, infrastruktuuriratkaisuja tai hyökkäysketjuja, joiden avulla yksittäiset havainnot voidaan yhdistää laajemmaksi kokonaiskuvaksi uhkatoimijoiden toimintatavoista.

Uhkamallinnus ja attribuutio

Uhkamallinnuksessa ja attribuutiossa on kyse havaitun ulkoisen toiminnan, usein tunkeutumisyritysten tunnistamisesta sekä syy-seuraussuhteiden ymmärtämisestä. Uhkamallinnuksessa ja attribuutiossa pyritään raakadataan perustuen ymmärtämään kuka tai ketkä ovat havaitun toiminnan takana ja mitkä ovat toimijoiden mahdolliset motiivit. Uhkamallinnus tarkoittaa havaittujen viitteiden perusteella päätelmien tekemistä toiminnan tavoitteista, eli miten uhkatoimija esimerkiksi pyrkii tunkeutumaan kriittisimpään omaisuuteen. Uhkamallinnusta on tarkoitus tehdä jatkuvasti ja ennakoivasti, ja sen tarkoituksena on olla proaktiivista. Jo ennen kyberuhkatiedusteluprosessin aloittamista organisaation ensimmäinen tavoite on tunnistettavan omaisuuden ja etenkin toiminnan kannalta kriittisten järjestelmien tunnistaminen ja mahdollisten hyökkäysvektorien kartoittaminen (käsitelty luvussa 3.1.3). Analyysivaiheessa onkin enemmän kyse siitä, että kerätyn datan perusteella tunnistetaan missä vaiheessa hyökkäystä ulkoinen toimija on ja noudattaako operaatio tunnistettuja uhkavektoreita. Oli vastaus tähän kysymykseen mikä tahansa, ohjaa se välittömästi tehtäviä vastatoimenpiteitä, jotka voivat olla joko etukäteen suunniteltuja (tunnistetut uhkavektorit) tai kokonaan uusia.

Attribuutiossa havainnot ulkoisesta toiminnasta yhdistetään ennakkotietoihin eri uhkatoimijoiden tai uhkatoimijatyyppien operaatiosta, pyrkien tunnistamaan kuka toiminnan takana on. Attribuution tavoitteena ei välttämättä ole tunnistaa uhkatoimijatasolla, mistä ryhmästä on kyse, vaan usein riittävää on ymmärtää, onko toiminta esimerkiksi opportunistista, automatisoitua vai kohdennettua. Pelkästään tämä tieto voi auttaa reagoinnissa käynnissä olevaan uhkaan, ja auttaa varautumaan vastaaviin operaatioihin tulevaisuudessa.

Vaikutus- ja riskianalyysi

Jos uhkamallinnuksen tavoitteena on selvittää, miten hyökkääjä voisi päästä käsiksi kriittiseen omaisuuteen, on vaikutusanalyysin tarkoitus hahmottaa, minkälaista vahinkoa aiheutuu, jos niin käy. Mikäli taas todetaan, että tunkeutuja ei seuraa mitään tunnistettua uhkavektoria tai kohdista hyökkäystä kriittisimpään omaisuuteen, on vaikutusanalyysin tehtävä tunnistaa, mitä hyökkääjä mahdollisesti etsii. Samoin tarkoitus on nimen mukaisesti ymmärtää, minkälaista vahinkoa uhkatoimija voisi aiheuttaa jo saavuttamillaan jalansijoilla tai mihin tietoihin sillä on mahdollisesti jo ollut pääsy.

Vaikutusanalyysi on tärkeä toteuttaa etenkin akuutin uhkan kohdalla. Sitä helpottaa mahdollisimman yksityiskohtainen ja ajantasainen kuva omasta IT-omaisuudesta, yhteyksistä ja siitä, mitä tietoa missäkin säilytetään. Vaikutusanalyysia on mahdollista tehdä etukäteen, ja mielellään kriittisen omaisuuden kohdalla näin toimittaisiinkin. Usein hyökkäys on jollain tavoin erilainen, kuin ennakoitu tai se saatetaan esimerkiksi onnistua rajoittamaan vain tiettyyn osaan verkkoa. Tällöin vaikutusanalyysin merkitys korostuu. Se auttaa vastaamaan uhkaan, helpottamaan esimerkiksi kriisiviestintää ja voi parhaillaan ehkäistä mainehaitan syntymistä. Esimerkkejä tapauksista, joissa kyberhyökkäyksen kohteeksi joutunut organisaatio on viestinyt epäselvästi tai virheellisesti perustuen heikosti toteutettuun vaikutusanalyysiin, löytyy helposti. Usein seurauksena on ollut merkittävä isku luotettavuudelle. Organisaatiot ovat voineet antaa ymmärtää, että yhteistyökumppanien tai asiakkaiden data ei ole vaarantunut hyökkäyksessä ja, kun näin jälkikäteen paljastuu tapahtuneen, on julkinen tulkinta usein epärehellisyys, vaikka taustalla saattaisi olla virhe vaikutusanalyysissä.

Strateginen analyysi

Aiemmat esitellyt toiminnot keskittyvät pitkälti teknisen uhkadatan analysointiin. Strategisen ja operatiivisen datan analysointi on huomattavasti erilaista ja usein sykliltään hitaampaa. Tämän analyysimuodon tavoitteena voi olla esimerkiksi ymmärtää toimintaympäristöä, ennakoida sen tulevia muutoksia tai arvioida uusien kehittyvien uhkien todennäköisyyksiä ja vaikutuksia. Strategisen ja operatiivisen uhkatiedon analyysissä voidaan käyttää strukturoituja analyysityökaluja, jotka ovat alkujaan tiedusteluanalyysiin kehitetty menetelmäperhe. Strukturoituja analyysityökaluja ovat esimerkiksi erilaiset skenaariotyökalut, kilpailevien hypoteesien analyysi ja voimakenttäanalyysi. Näistä kilpailevien hypoteesien analyysi (Analysis of Competing Hypothesis, ACH) on esiteltynä myöhemmin tässä luvussa. Strukturoitujen analyysityökalujen käytön tarkoitus on vähentää virheitä analyysissä ehkäisten intuitiivisia ansoja ja kognitiivisia virheitä. Niiden käyttäminen pakottaa lähestymään käsiteltäviä ilmiöitä useista eri näkökulmista ja kriittisesti ennakkokäsityksiin nähden.

Strukturoitujen analyysityökalujen käyttö, kuten muukin strategisen tason analyysi vaatii usein kokemusta ja osaavia analyytikoita. Läheskään jokaisen organisaation ei kannata investoida strategisen analyysin tuotantoon, mutta sen tuottaman ymmärryksen arvo on syytä tiedostaa. Ymmärrys toimintaympäristön muutoksista auttaa ennakoivissa investointipäätöksissä. Uhkien tunnistaminen ennen niiden vakaviksi muuttumista on aina taloudellisempaa, kuin niihin reaktiivinen vastaaminen. Lisäksi ”yleissivistys” kyberuhkista voi olla arvokasta tietoa suhteita luodessa ja kumppaneiden kanssa käytävissä vapaamuotoisissakin keskusteluissa. Strategista uhkatietoa ja valmiita raportteja on kannattavaa hyödyntää ja hankkia, vaikka niiden omaan tuotantoon ei välttämättä ole aina järkevää tai mahdollista panostaa. Strategisten kyberuhkien ymmärrys on osa johdolla oltavaa tilannekuvaa, jota tulee ylläpitää tavalla tai toisella.

Analyysin dokumentointi ja raportointi

Lopullinen ja ehkä tärkein operatiivinen vaihe on analyysissä saavutettujen johtopäätösten siirtäminen eteenpäin, eli jakaa valmista tietoa tarvitsevalle taholle. Analysoitu tieto voi olla mitä tahansa tekstimuotisesta raportista suullisesti annettuun lausuntoon tai suoraan palomuuriin syötettävään listaan varmasti pahantoisiksi tunnistetuista IP-osoitteista.

Raportit tulee tuottaa eri kohdeyleisöille sopivassa muodossa:

- C-taso tarvitsee selkeän yhteenvedon vaikutuksista ja suosituksista.
- SOC-tiimi tarvitsee tekniset artefaktit, indikaattorit ja hyökkäysketjun kuvaukset.
- Arkkitehtuuritiimi hyötyy pitkäaikaisemmista TTP-trendeistä (Tactics, Techniques and Procedures) ja suosituksista.

Laadukas raportti erottaa selkeästi havainnot, johtopäätökset ja suositellut toimenpiteet, ja sisältää analyytikon luottamusasteikon eli sen, miten luotettavana analyytikko tietoa pitää. Joissain tilanteissa myös alkuperäisen raakadatan lähteen mainitseminen voi tulla kysymykseen, mutta tämä ei aina ole tarpeen. Nyrkkisääntönä voidaan pitää, että etenkin raporttimuotoisia analyysituotteita tulee toimittaa loppukäyttäjälle mahdollisimman vähän ja mahdollisimman tiiviissä muodossa. Turhan, ei toimintaa aiheuttavan tiedon raportointi lisää työmäärää eikä yleensä tuota mitään hyödyllistä. Kyberturvallisuudesta vastaavat henkilöt joutuvat muutenkin painimaan päivittäisen informaatiotulvan kanssa, joten vain relevanttia ja oikeasti merkitsevää tietoa tuottava analyysi on äärimmäisen arvokas. Ylimääräiset tai liian pitkät raportit, etenkin toistuvina, usein vähentävät vastaanottajan kiinnostusta, jolloin sen kerran, kun raportti sisältäisikin arvokasta tai reagointia vaativaa tietoa, jää se huomaamatta.

Analyysin loppuvaiheessa tärkeää on tehdyn työn dokumentointi. Tämä tarkoittaa tiedon tallentamista siitä, minkälaista dataa on analysoitu ja mitä johtopäätöksiä siitä on tehty. Dokumentointi helpottaa samanlaisen analyysityön toistamista, mutta on arvokasta tilanteissa, missä huomataan analyysin johtaneen virheelliseen lopputulokseen. Hyvin dokumentoidusta analyysityöstä on helppo jäljittää, missä kohtaa virhe tapahtui ja välttää se jatkossa. Dokumentointi on arvokasta, kun arvioidaan eri lähteistä tai yhteistyökumppaneilta saatavan datan luotettavuutta. Vaikka analyysiprosessin lopputuote, oli se sitten raportti tai SIEM:iin syötettävä indikaattori, ei sisällä alkuperäisen tiedon lähdettä, on jäljitettävyyden vuoksi tärkeää, että tieto on tallennettuna jossain. Jos tietyn tiedon tuottajan data on jatkuvasti virheellistä tai puutteellista, voi sen havaitseminen tai erottaminen lopputuotteesta itsestään olla vaikeaa. Huolellinen dokumentointi onkin tärkeää.

ACH-menetelmä (Analysis of Competing Hypotheses)

ACH on strukturoitu analyysimenetelmä, jossa rinnakkaisia hypoteeseja arvioidaan systemaattisesti saatavilla olevaa tietoa vasten. Sen keskeinen hyöty on kognitiivisten harhojen vähentäminen ja analyysin läpinäkyvyyden parantaminen. Menetelmää hyödynnetään erityisesti strategisessa ja operatiivisessa uhka-arvioinnissa, esimerkiksi arvioitaessa hyökkäyksen tekijää, motiivia tai todennäköistä jatkokehitystä epävarman tai ristiriitaisen tiedon pohjalta.

Red Team / Blue Team -ristiintarkastus

Red Team / Blue Team -lähestymistapaa käytetään analyysin laadunvarmistukseen ja vaihtoehtoisten tulkintojen tunnistamiseen. Red Team haastaa analyysin oletukset ja johtopäätökset hyökkääjän näkökulmasta, kun taas Blue Team edustaa puolustavaa, organisaation todellisuuteen nojaavaa tulkintaa. Menetelmä parantaa analyysin luotettavuutta ja auttaa tunnistamaan puutteita tai virheellisiä päätelmiä, erityisesti operatiivisessa ja taktisen tason CTI:ssä.

Aikajanan mallintaminen hyökkääjän todennäköisestä etenemisestä

Aikajanan avulla jäsennetään hyökkäyksen tapahtumat loogiseen ja kronologiseen järjestykseen. Tämä tukee ymmärrystä siitä, miten hyökkäys on edennyt, missä vaiheessa hyökkääjä on tällä hetkellä ja mitkä seuraavat toimenpiteet ovat todennäköisiä. Menetelmä auttaa myös epäloogisuuksien tunnistamisessa. Aikajanoja hyödynnetään erityisesti tapauskohtaisessa analyysissä, incident response -tukena sekä ennakoivassa uhka-arvioinnissa.

Hyökkäysketjun mallinnus (Cyber Kill Chain)

Kill Chain -malli tarjoaa rakenteen hyökkäyksen vaiheiden tunnistamiseen tiedustelusta vaikutusten saavuttamiseen. Sen avulla analyytikko voi paikantaa, missä vaiheessa hyökkäys on havaittu ja mihin puolustustoimenpiteet kannattaa kohdistaa. Mallia käytetään yleisesti taktisen ja operatiivisen tason analyysissä puolustuksen aukkojen tunnistamiseen ja havaintokyvykkyyksien kehittämiseen.

Hyökkääjien TTP-mallinnus (MITRE ATT&CK)

MITRE ATT&CK tarjoaa standardoidun viitekehyksen hyökkääjien tekniikoiden, taktiikoiden ja toimintatapojen (TTP = Tactics, Techniques and Procedures) kuvaamiseen. Sen keskeinen hyöty on yhteinen kieli analyytikoiden, SOC-tiimien ja johdon välillä sekä analyysin vertailtavuus eri tapausten ja uhkatoimijoiden välillä. Mallia sovelletaan taktisen analyysin tukena sekä uhkahavaintojen ja uhkatoimijoiden profiloinnissa.

Diamond Model -rakenne

Diamond Model jäsentää kyberuhkat neljän keskeisen elementin kautta: uhkatoimija, infrastruktuuri, kyvykkyys/toiminta ja motiivi tai uhri. Malli auttaa ymmärtämään uhkan kokonaiskuvaa ja eri elementtien välisiä suhteita. Sitä hyödynnetään erityisesti operatiivisessa ja strategisessa CTI:ssä, kun pyritään yhdistämään tekninen havaintodata laajempaan kontekstiin ja uhkatoimijan tavoitteisiin.

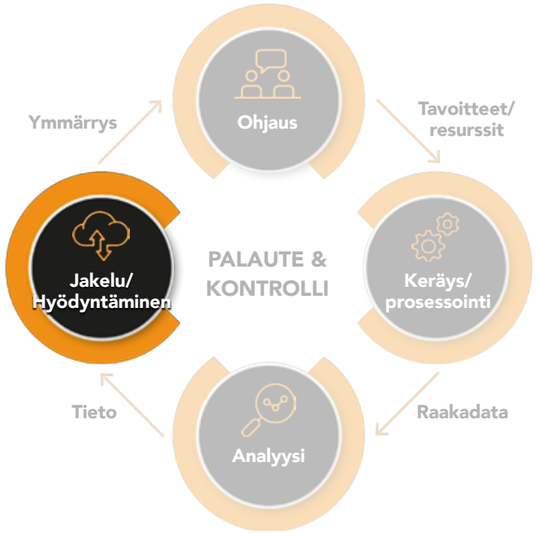
Skenaarioharjoitukset ja työpajat

Strategisen tason skenaarioharjoitukset auttavat hahmottamaan uhkien vaikutuksia organisaation ydintoimintoihin ja saattavat paljastaa aiemmin huomioimattomia heikkouksia varautumisessa. Operatiivisen tason harjoitukset harjoituttavat ja kehittävät varautumista konkreettisten häiriötilannetoimenpiteiden myötä.

2.3.3 Käytännön työkalut

Erilaisia kyberuhkatiedustelussa hyödynnettäviä analyysityökaluja on olemassa monipuolisesti. Niiden käyttö riippuu huomattavasti analysoitavan datan laadusta ja analyysiprosessin tavoitteesta. Alla esitettynä muutamia työkaluja, joita hyödynnetään strategisen ja operatiivisen kyberuhkatiedon analysoinnissa.

2.4 Jakelu



Jos aiemmat vaiheet ovat olleet tärkeitä sen takaamiseksi, että CTI-prosessi onnistuu parhaalla mahdollisella tavalla, on viimeinen jakelun ja hyödyntämisen vaihe edellytys sille, että työstä on jotain käytännön hyötyä. Kuten ohjausvaiheessa todettiin, tärkein kriteeri sille minkälaista uhkatietoa organisaation tulee pyrkiä hankimaan, on sen käytettävyys ja juuri käytettävyyden realisoimisesta on tässä vaiheessa kysymys. Oli uhkatiedon lopullinen vastaanottaja sitten järjestelmä, henkilö tai organisaation osasto, on tämän vaiheen tehtävä varmistaa, että kerätty ja analysoitu tieto päätyy sinne ja, että vastaanottaja tietää, mitä on saamassa ja mitä sen kanssa tulee tehdä.

Kyberuhkatiedon jakelu koskee sekä omaa organisaatiota että ulkoisia kumppaneita. Verkostojen toiminta perustuu siihen, että sen kaikki osapuolet sekä tuottavat että vastaanottavat tietoa, joten kyberuhkatiedon kanssa työskentelevien organisaatioiden tulee varautua myös jakamaan hankkimaansa ja käsittelemäänsä uhkatietoa muille. Tässä on otettava huomioon etenkin se, minkä laatuista tietoa halutaan jakaa ja, että jaettu tieto on luotettavaa ja hyödyllistä. Väärän tiedon jakaminen paitsi heikentää koko kentän turvallisuuden tasoa, voi aiheuttaa mainehaittaa organisaatiolle. Etenkin jaettavan uhkatiedon laadusta tulee olla täysi varmuus tai vaihtoehtoisesti epävarmuus pitää pystyä ilmaisemaan. Tässä toimii esimerkiksi Suojelupoliisin (Supo) määrittelemät epävarmuuden arviointimenetelmät tiedon lähteen ja sisällön luotettavuuden määrittämiseksi. Määritelmän mukaan epävarmuuden arviointi koostuu keskeisesti kahdesta osa-alueesta: tiedon lähteen luotettavuuden arvioinnista (lähteen historia, pätevyys ja aiempi paikkansapitävyys) sekä informaatiosisällön luotettavuuden arvioinnista (tiedon eheys, vahvistettavuus ja konteksti). Luotettavuuden arviointiin vaikuttaa myös tiedon luokittelu sen turvaluokitus ja salassapitotarpeen mukaan: kappalekohtaiset turva- ja luotettavuusluokat määritetään usein riskienhallinnan ja seurauksien perusteella (TL I-IV).

Tärkeä pohdittava asia onkin se, minkälaista tietoa organisaatio pystyy jakamaan ja kenelle. Uhkatiedon kriittisyys tulee olla määritetty organisaation sisäisesti, ja eri tiedonjakoverkostot tai kumppanit luokiteltuja sen mukaan, kenelle minkäkin tasoista tietoa voidaan jakaa. Tietojen käsittelijät eli analyytikot harvoin tietävät, mihin ja milloin tietoa tullaan todellisuudessa käyttämään sen jakelun jälkeen.

Periaatteessa kyberuhkatiedon jakelu ja hyödyntäminen tulisi olla suunniteltu jo projektin alkuvaiheessa mutta, kuten missä tahansa projektissa, suunnitelma on hyvä lähtökohta, joka usein kuitenkin muuttuu käytännössä. Uusia datalähteitä tai tietomuotoja keksitään kesken projektin tai yllättävä ja nopeasti syntynyt yhteistyö tuottaa uudenlaista, hyödylliseksi todettua tietoa. Jakelu ja hyödyntämisvaiheen tärkein tehtävä on varmistaa, että suunnitelmat toteutuvat, muokata niitä tarvittaessa ja pitää huolta siitä, että myös niiden ulkopuolinen uhkatieto hyödynnetään mahdollisimman tehokkaasti.

2.4.1 Johdon vastuut

Kyberuhkatietoprosessin viimeisessä vaiheessa johdon vastuut ovat kaksijakoiset. Ensimmäinen vastuu, jota on jo sivuttu, on sen varmistaminen, että uhkatieto päätyy kaikkialle, missä sitä tarvitaan. Toinen, kenties merkityksellisempi, on sen varmistaminen, että tietoa hyödynnetään ja sen perusteella tehdään päätöksiä tulevaisuudesta tai kehitetään nykyistä toimintaa. Uhkatietoprosessin tavoite ei ole tuottaa tietoa sen itsensä vuoksi, vaan nimenomaan päätöksenteon tueksi tai sen ohjaamiseksi. Johdon vastuulla on mahdollistaa raakadatan muutos tiedoksi, tiedon kehittyminen ymmärrykseksi ja lopulta erilaisten kyberuhkien riskien pienentämiseen johtavaksi toiminnaksi. Paraskaan uhkatietoprosessi ei tuota konkreettista hyötyä, ellei sen tuottamaa ymmärrystä osata implementoida tehokkaasti. Johdon vastuulla on sekä itse tehdä päätöksiä uhkatiedon pohjalta että varmistaa, että muut organisaation osat, joille tietoa jaetaan, hyödyntävät sitä oikein.

Käytännössä toiminnot voivat olla resurssien uudelleen kohdentamista, uusia investointeja tai poikkeustilanteiden hallintaa. Johdon toinen keskeinen vastuu onkin valmistella, toteuttaa, vastuuttaa ja varmistaa, että nämä toimenpiteet toteutuvat. Paras tapa on johtaa esimerkillä ja näyttää, että kyberuhkat käsitellään liiketoimintariskeinä eikä pelkästään IT-asioina. Hyödyllistä on kerätä ja vaatia palautetta organisaation eri osilta kyberuhkatiedon hyödyllisyydestä. Jos tiedon laadussa tai muodossa havaitaan puutteita, voidaan näitä käyttää jatkossa keräyksen ja analyysin ohjaamiseen. Oli kyse sitten teknisestä uhkatiedosta tai strategisista raporteista, johdon vastuulla on varmistaa, että prosessilla, johon on investoitu, on todellista vaikuttavuutta organisaation toimintaan. Ilman aktiivista johtamista kyberuhkatieto jää usein raporteiksi ja dataksi. On johdon vastuulla muuttaa kyberuhkatieto toiminnaksi ja riskienhallinnaksi.

Johdon vastuulla on myös organisoida ja resursoida uhkatiedon jakaminen ulkoisille sidosryhmille. Käytännössä tämä saatetaan hoitaa jopa analyytikkotasolla, mutta johto yleensä vastaa tiedonjakosopimusten tekemisestä, niihin käytössä olevista resursseista ja sopimusten ylläpidosta. Aktiivinen ote on tärkeää, ja sopimusten ja käytäntöjen tulee olla toimivia. Mikäli jonkin tiedon tai tietotyypin jakamista rajoittaa byrokratia tai epävarmuus siitä, mitä kaikkea voimassa olevat sopimukset kattavat, heikentää se merkittävästi verkostojen toimivuutta. Tämä vaikuttaa usein siihen, kuinka mielellään ulkoiset toimijat jakavat omia tietojaan.

2.4.2 Operatiiviset toimenpiteet

Jos organisaation ylimmän johdon tehtävä on varmistaa, että uhkatieto johtaa konkreettisiin toimenpiteisiin, on operatiivisen johdon vastuulla käytännössä valita, priorisoida ja toteuttaa ne. Toimenpiteet voivat olla hyvinkin yksinkertaisia (esimerkiksi uusien IOC:ien tai pahaksi tunnistettujen IP-osoitteiden syöttäminen palomuuriin tai SIEM:iin) tai monimutkaisia pitkän aikavälin muutoksia (prosessien muokkaamien tai uusien järjestelmien hankinta). Operatiivisen johdon vastuulla on yleensä ymmärtää, mitä nämä toimenpiteet ovat ja kuka ne käytännössä suorittaa. On esimerkiksi mahdollista, että uhkatieto koskee organisaation käyttämää, mutta kokonaan ulkoisen palveluntuottajan tuottamaa ja ylläpitämää järjestelmää, jolloin operatiiviselle johdolle lankeaa vastuu viestinnästä ja koordinoinnista alihankkijan kanssa. Koordinointi on tärkeää myös oman organisaation sisällä, sillä usein käytännön toimenpiteet edellyttävät panostusta usealta eri toimialueelta tai organisaation eri osastoista.

UHKATIEDON KÄYNNISTÄMIÄ KONKREETTISIA TOIMENPITEITÄ

- Paikkaus- ja kovennustoimet
- Valvontasääntöjen päivitykset
- Käyttöoikeuksien tarkistukset
- Uusien järjestelmien käyttöön ottaminen
- Henkilöstön tiedottaminen ja/tai kouluttaminen
- Väliaikainen kohotettu valmius ja tiukennetut turvatoimet

Kun tarvittavat toimenpiteet on valittu, on seuraavana tehtävänä priorisoida ne. Tässä yleensä auttaa analyysivaiheen tuottama uhkien tai haavoittuvuuksien vakavuusluokitus, mutta sen ei tule olla ainoa ohjenuora toimenpidejärjestystä valittaessa. Vakava haavoittuvuus merkityksettömässä kohteessa ei välttämättä ole yhtä kiireellinen korjattava, kuin mahdollisesti käytössä oleva hyökkäysmuoto, joka kohdistuu kriittisimpään omaisuuteen. Tehtävät tulee priorisoida ottaen huomioon eri toimintojen kriittisyys, käytössä olevat resurssit ja muut akuutit tehtävät. Tietoturvatiimejä vaivaa lähes aina jatkuva ylityöllistäminen ja priorisointia ajaa usein pakko. Onkin tärkeää, että se taho, joka priorisoinnista vastaa, ymmärtää sen käytössä olevat resurssit ja kohteiden suojattavuuden tärkeysjärjestyksen.

Seuranta ja raportointi

Pelkkä toimenpiteiden käynnistäminen ei riitä. Etenkin uudenlaisen uhkatiedon kanssa työskennellessä on äärimmäisen tärkeää seurata, että toimenpiteet etenevät ja ovat toteuttamiskelpoisia sekä hyödyllisiä. Kaikki poikkeamat, hankaluudet ja viiveet on syytä nostaa esiin mahdollisimman nopeasti, jotta niihin voidaan reagoida ja tarpeen vaatiessa muokata joko käynnissä olevaa prosessia tai saada oppeja jatkoon. Tilanneraportointia on vaadittava kaikista niistä projekteista, joihin ei voida itse suoraan osallistua tai joiden edistymistä ei voida tarkkailla. Tämä koskee niin omia kuin alihankkijoille ja kumppaneille vastuutettuja toimenpiteitä. Lisäksi operatiivisen johdon vastuulla on yleensä raportoida ylöspäin toimintojen edistymisestä.

Kaikki tämä edellyttää hyvän ja tarkan tilannekuvan ylläpitämistä käynnissä olevista toimenpiteistä. Tilannekuvan ylläpitoon kuuluu myös sen tarvittavilta osin välittäminen toimiville osilla, jotta nämä ymmärtävät, mitkä ovat prioriteetit, ja miksi tietyt uhkat ovat arvioitu kriittisemmiksi kuin toiset.

Palautteen antaminen ja toimintamallien päivittäminen

Samalla, kun ylläpidetään tilannekuvaa ja seurataan toimenpiteiden edistymistä, on tärkeää antaa palautetta uhkatiedon tuottajille. Palautetta tulee antaa uhkatiedon sisällöstä ja muodosta, mutta erityisesti myös sen ajoituksesta. On äärimmäisen tärkeä huomata, mikäli jokin uhkatieto tulee liian myöhään ja joka olisi pitänyt saada aikaisemmin pitkän implementaatioprosessin vuoksi. Tällöin on perusteltua harkita niin sanotusti mutkien oikomista analyysivaiheessa tai raakadatan suoraa hyödyntämistä.

Kyberuhkatiedon on tärkeää olla relevanttia, luotettavaa ja hyödynnettävää. Vaikka tähän tähdätään prosessin jokaisessa vaiheessa, aina silti jonkin verran turhaa tietoa kulkeutuu prosessin läpi. Näiden kohdalla on syytä arvioida, kuinka paljon resursseja ylimääräisen tiedon tuottaminen vei ja syntyikö se jonkin tarpeellisen tiedon ”sivutuotteena”, jolloin sen muodostumiselta on vaikea välttyä. Tämän selvittämiseksi dokumentoitu analyysityö ja vuoropuhelu toteuttavien osien ja operatiivisen johdon välillä on tärkeää.

Palautteen antamisen tavoitteena tulisi olla toiminnan kehittäminen. Kyberuhkatietoprosessi on jatkuva ja käytännön elämässä yksi organisaatio suorittaa sen kaikkia vaiheita usein samanaikaisesti. Tällöin jatkuva palautteen kerääminen ja sen antaminen on tärkeää, jotta toimintaa voidaan kehittää ja, jotta toiminta pysyy tehokkaana. CTI-prosessilla tulee olla selkeä tavoite ja päämäärä, jottei prosessi ala pyörimään taustalla ikään kuin automaattisesti, tuottaen päätöksentekoon lopulta varsin vähän relevanttia informaatiota. Tällöin on vaarana, että CTI-prosessista syntyy lähinnä itseään työllistävä kehä vailla todellista käytännön arvoa.

Varsinaista ”palautteenantojaksoa” ei tosielämässä yleensä voida järjestää, joten asiat on nostettava esiin, kun huomataan puutteita tai mahdollisuuksia kehittää toimintaa. Työohjeiden ja käytäntöjen päivittäminen on etenkin uhkatietoprosessin alkuvaiheessa varsin yleistä ja siihen tulee varautua. On tärkeää pitää huolta, että jatkuvasti saadut opit hyödynnetään siten, että ne muuttuvat pysyviksi toimintatavoiksi, eikä ole vain kertaluontoisia muutoksia toiminnassa. On tärkeää, että kyberuhkatiedon prosessilla on omistaja, joka kerää palautetta ja on vastuussa prosessin jatkuvasta kehittämisestä.

2.4.3 Käytännön työkalut

Konkreettisia työkaluja jakeluvaiheessa on verrattain vähän. Riippuen uhkatiedon laadusta ja tyypistä, jakelu ja hyödyntäminen saatetaan toteuttaa yksittäisillä teknisten kyberturvauhkatietojen jakelualustoilla, kuten esimerkiksi Splunk tai MISP (Malware Information Sharing Platform). Se voi yhtä hyvin olla raporttien välittämistä organisaatiossa sähköpostin liitteenä. Samat jakelumenetelmät toimivat myös tiedon jakamiseen organisaation ulkopuolelle. Tähän käytettävät työkalut ovat pitkälti samoja kuin tämän käsikirjan keräysvaiheessa esitellyt tiedonjaon kanavat ja uhkatietostandardit, jotka auttavat yhtenäistetyn tiedon välittämisessä.

TIEDONJAON KANAVIA JA TYÖKALUA
MISP/OpenCTI uhkatiedon jakamiseen ja käsittelyyn tarkoitettuja sovelluksia, jotka mahdollistavat nopean ja standardoidun datan jakamisen.
Standardit, kuten STIX ja TAXII, ovat käytössä jakoalustoilla mutta mahdollistavat tiedon siirtämisen niiden ulkopuolelle ja hyödyntämisen muilla, ei suoraan yhteydessä olevilla työkaluilla.
Organisaation sisäinen tiedonjako, kuten sisäverkkojen tiedonjakokanavat, viikkopalaverit, johtoryhmän uhkaesittelyt, säännölliset uhka- ja kriisinjohtamistyöpajat sekä hallitus- ja muu säännöllinen raportointi.
Vapaamuotoiset uhkatietoverkostot voivat olla esimerkiksi kuukausittaisia tiedonjakopalavereja, joissa viranomaiset tai alan suurimmat toimijat jakavat suullisesti tietoa viime aikoina kohtaamistaan kyberuhkista tai vallalla olevista trendeistä. Näistä hyvänä esimerkkinä toimii kansallisen Kyberturvallisuuskeskuksen, Traficomin, ISAC-tiedonvaihtoryhmät, joiden päätarkoituksena on jakaa toimialakohtaisia tietoa ja kokemuksia ja tätä kautta lisätä organisaatioiden ja toimialojen kykyä suojautua digitaalisia uhkia vastaan sekä hallita häiriötilanteita. (Lisätietoa ISAC-toiminnasta saat sähköpostiosoitteesta ktk-verkostot@traficom.fi.)

Myöskään uhkatiedon hyödyntämiseen ei ole tarjolla kovinkaan kattavia listoja konkreettisista työkaluista. Se, minkälaisiin toimintoihin uhkatieto ohjaa, on hyvin kontekstiriippuvaista. Esimerkiksi edellisessä kappaleessa esitellyt koventamistoimet tai valvontasääntöjen muutokset perustuvat niihin alustoihin ja sovelluksiin, joita organisaatiolla on jo ennestään käytössä.

3 CTI – JATKUVASTI KEHITTYVÄ PROSESSI

Kyberuhkatiedon tärkein tehtävä on tuottaa aikaa ja tietoa päätöksentekoa varten, kuten jo tämän käsikirjan johdannossakin on todettu. Aikaa on tarkoitus antaa uhkien ennalta tunnistamiseen ja niihin reagointiin, ennen niiden realisoitumista. Tämä aika on jatkuvasti käymässä lyhyemmäksi ja ennakkovaroituksen hankkiminen yhä vaikeammaksi. Uhkatoimijoiden operaatiot ovat nopeutuneet ja uusien haavoittuvuuksien julkaisun ja hyödyntämisen välinen aika on lyhentynyt. Tällä hetkellä puhutaan usein minuuteista haavoittuvuusjulkaisun ja sitä hyödyntämään pyrkivien hyökkäysten välillä. Teknologinen kehitys suosii hyökkääjiä, ja esimerkiksi tekoäly on jo nyt tuottanut merkittävää etua kyberhyökkäysten toteuttajille. Vaikka puolustuksellistakin hyötyä tekoälystä on saatu ja uusia innovaatioita nousee sen myötä jatkuvasti, on etumatka huomattava hyökkääjillä, joiden ei tarvitse auditoida tai varmistaa, että tekoälyä hyödyntävä hyökkäystyökalu toimii varmasti ja kaikissa tilanteissa. Yksikin onnistuminen riittää ja, jos työkalu ei toimikaan, ei vahinkoa tapahdu.

Toisin sanoen jatkuvaksi yhä intensiivisemmäksi käyneen kybervaikuttamisen seurauksena tarve ajantasaisen kyberuhkatiedon saamiselle on kasvanut entisestään. Organisaation kriittisimmän omaisuuden suojaamiseen tarvittavat kontrollikeinot tarvitaan yhä nopeammin, kuin mitä ihminen pystyy niitä yksin toteuttamaan. Tämä puolestaan on kasvattanut tekoälyn merkitystä uhkatiedon keräämisessä, käsittelyssä ja jatkojalostamisessa. Kasvanut tiedon tarve samalla kuin lisääntynyt erilaisen uhkainformaation määrä onkin pakottanut organisaatiot omaksumaan yhä nopeammin käyttöönsä erilaiset prosessia helpottavat tekoälyagentit ja -työkalut. Tekoälyn kohdalla kuitenkin edelleen haasteena on sen luotettavuuden takaaminen. Yhdessä ihmisanalyytikko ja tekoälytyökalu voivat tulevaisuudessa parhaiten vastata tähän kasvaneeseen relevantin kyberuhkatiedon saamisen tarpeeseen.

Akuutin ja nopealla aikataululla hyödynnettävän tiedon lisäksi strategiselle ja operatiiviselle tiedolle on suurempi tarve yleisen turvallisuustilanteen heikentyessä ja valtiollisen kybervaikuttamisen yleistyessä. Organisaatioiden tarve kyberuhkatiedolle tulee lisääntymään ja regulaatiotrendin ollessa kasvava, on todennäköistä, että myös sitä kautta nousevat velvoitteet tilannekuvan ja uhkatiedon ylläpitämiseen tulevat lisääntymään. Tämä edelleen kasvattaa kyberuhkatiedon arvoa tulevaisuudessa.

Kyberuhkatiedon tarve koskee jokaista organisaatiota, mutta ei samalla tavalla. Jokaisen organisaation käytettävissä olevat resurssit ja tarpeet määrittävät ne yksilölliset olosuhteet, joissa organisaatio toimii. Kaikkia koskevien yleispätevien ohjeistuksien luominen on lähes mahdotonta. Tässä käsikirjassa on pyritty tarjoamaan mahdollisimman laajasti ja monipuolisesti hyödynnettävissä olevia neuvoja kyberuhkatietoprosessin käynnistämiselle, käytölle ja kehittämiselle.

Kyberuhkatiedon hankkimisen ja hyödyntämisen prosessi on varsin laaja ja monipuolinen, sekä jatkuvasti päivittyvä ja kehittyvä. Sen toteuttaminen onnistuneesti vaatii motivaatiota, resursseja ja kokemusta. Paras tapa kehittää prosessia, on sen laajentaminen suhteutettuna oman organisaation kasvaneisiin tiedontarpeisiin. Uusien tietolähteiden, prosessien tai analyysityökalujen jatkuva implementointi on tärkeää paitsi muuttuvien uhkien kanssa mukana pysymiseksi, myös toiminnan kehittämiseksi. Kyberuhkatiedon prosessi tulee ymmärtää jatkuvasti käynnissä olevaksi ja kehittyväksi toiminnoksi. Ympyrän tulee pyöriä ja palautetta tulee kerätä eri vaiheiden toteutumisesta. Tärkein tekijä kehittyvän prosessin kannalta on intressi kehittää sitä. Kyberuhkatietoprosessi ei tule olla vain pakolliseksi miellettävä toimenpide, vaan lisäarvoa tuottava sijoitus, joka voi pelastaa organisaation lamauttavalta vahingolta sekä tarjota markkina- ja ajatusjohtajan aseman.

Esimerkkitapaukset kyberuhkatiedon eri tasoille

Käsikirjan johdannossa viitattiin kyberuhkatiedon eri tasoihin (strateginen, operatiivinen ja tekninen) ja eri luvuissa on sivuttu sitä, miten eri tason tieto edellyttää erilaisia toimenpiteitä ja käsittelyä. Tässä esimerkkitapauksissa on esitelty muutamia malleja siitä, mitä eri tason uhkatiedon kohdalla minkäkin vaiheen käytännön toimenpiteet ovat. Esimerkit on tarkoitettu helpottamaan hahmottamaan sitä, miten eri tason tieto edellyttää erilaisia toimenpiteitä ja mitä nämä voivat olla.

O = OHJAUS **K = KERÄYS / PROSESSOINTI** **A = ANALYYSI** **J = JAKELU / HYÖDYNTÄMINEN**

STRATEGINEN UHKATIETO (ESIMERKKICASE 1):
Kriittisen toimialan organisaatioon kohdistuu valtiollista kybervaikuttamista

- **O** Organisaatio, joka toimii kriittisellä alalla, tiedetään kohdistuvan ulkomaisten kyberuhkatoimijoiden kiinnostusta.
- **O** Todetaan tarve hankkia tietoa toimialaa koskevista kyberuhkista ja niiden kehityksestä globaalisti.

  Organisaatio kartoittaa omia kykyjään hankkia tätä tietoa mutta päätyy siihen, että kustannustehokkainta on hyödyntää alihankkijaa, jonka kanssa sovitaan uhkatiedon hankinnasta.
- **K** Organisaatio alkaa vastaanottamaan alihankkijan keräämää ja valmiiksi analysoimaa, tasaisin väliajoin toimitettua uhkatietoa koskien omaa toimialaa, joita täydentää erikseen tilatut raportit kriittisistä aiheista.
- **K** Organisaatio tallettaa saadun tiedon omiin järjestelmiinsä ja varmistaa, että se on saatavissa ja luotettavasti säilytettynä.
- **A** Organisaation tietoturvasta vastaava taho perehtyy raportteihin, vertaa niitä omaan ymmärrykseen ja muodostaa yhteenvedon tilannekuvasta.
- **A** Tilannekuvasta kirjoitetaan muutaman lauseen tiivistelmä esitettäväksi johtoryhmälle. Lisäksi raportit ja lähteet, joiden perusteella tilannekuva on muodostettu, talletetaan. Tiivistelmästä säilytetään versio, josta näkyy selvästi mistä mikäkin tieto on peräisin.
- **J** Tilannekuva esitellään kuukausittaisessa johtoryhmän kokouksessa ja sitä jaetaan saman toimialan organisaation yhteisessä tilannekuvapalaverissa.
- **J** Saadun ymmärryksen pohjalta varaudutaan piikkeihin uhkatoimijoiden aktiivisuudessa ja reagoidaan uudenlaisiin hyökkäysmuotoihin tai yleistyviin trendeihin.

OPERATIIVINEN UHKATIETO (ESIMERKKICASE 2):
Kyberriskianalyysissa esille noussut kasvanut riski

- **O** Organisaatio tunnistaa riskianalyysissa siihen kohdistuvan monipuolisia kyberuhkia ja toteaa, että näihin varautuminen vaatii proaktiivista toimintaa ja ajantasaisen uhkatiedon hankkimista.
- **O** Todetaan tarve hankkia tietoa käynnissä olevista kyberhyökkäyskampanjoista, uusista haittaohjelmista ja uhkatoimijoiden työkalujen kehityksestä.
- **O** Kartoitetaan käytössä olevat keinot hankkia tietoa ja päädytään hankkimaan uhkatietoa tuottava, prosessoiva ja analysoiva ulkoinen SOC-palvelu ja ajankohtaista IOC-uhkatietoa verkostojen kautta.
- **O** Määritetään, mitä tietoa halutaan kerätä, kenen toimesta ja miten hankittu data hyödynnetään.
- **K** Organisaatio auditoi ja vertailee eri palveluntuottajia ja sopii toimittajan kanssa SOC-toimintojen tuottamisesta. Sopimuksessa käydään läpi, miten toimittaja kerää tietoa organisaation rajapinnasta, miten siihen reagoidaan ja kenelle poikkeamista ilmoitetaan. Samalla varmistetaan, että tiedonjako organisaation ja SOC-keskuksen välillä on sujuvaa ja toimii molempiin suuntiin eli, että esimerkiksi verkostosta saatava uhkatieto kulkeutuu SOC-keskukseen prosessoitavaksi ja uusia tietotarvevaatimuksia esitettään SOC-toimittajalle.
- **K** Organisaatio liittyy kansalliseen ISAC-verkostoon, jossa jaetaan ajankohtaista tietoa kyberuhkista.
- **K** Organisaatio varmistaa, että kaikki relevantti tieto, jota eri kanavia pitkin saadaan, päätyy analysoitavaksi. Käytännössä varmistetaan, että tiedonjakotilaisuuksiin osallistuva henkilö joko osaa arvioida, mikä on relevanttia ja välittää nämä tiedot eteenpäin organisaatiossa (tai ulkoiselle SOC-tuottajalle) tai vaihtoehtoisesti kaikki tieto otetaan vastaan ja prosessoidaan myöhemmin.
- **A** Ulkoistettu SOC-palvelu analysoi omalta osaltaan kerättyä uhkatietoa ja ylläpitää suojausta vastaamaan muuttuviin tai kehittyviin uhkiin. Organisaation oma henkilöstö puolestaan analysoi ISAC-ryhmistä saatua tietoa yhdistäen sitä SOC-analyysiin. Organisaation tulee pysyä kartalla siitä, mitä tehdään ja miksi. Yhteydenpitoa ja tiedonvaihtoa SOC-palveluntarjoajaan tulee ylläpitää aktiivisesti.
- **J** Organisaatio vastaanottaa tietoa SOC-palvelusta ja varmistaa, että samalla sen muista lähteistä saama uhkatieto päätyy keskuksen (ja muun organisaation) hyödynnettäväksi.
- **J** Organisaatio jakaa SOC-palvelun tuottamia havaintoja torjutuista hyökkäyksistä tai tunkeutumisyrityksistä alan muille toimijoille, joiden tiedetään käyttävän samankaltaisia iskun kohteena olleita sovelluksia. Organisaatio tiedottaa myös viranomaisia mahdollisista poikkeamista.
- **J** Jakelussa muistetaan tiedon luokittelu ja se, minkälaista tietoa ulospäin voidaan jakaa. Organisaation toiminnasta tai havainnointikyvystä kertovaa tietoa ei jaeta ulkopuolisille tahoille ilman sen "puhdistamista" ja turvallista jakelukanavaa.

TEKNINEN UHKATIETO (ESIMERKKICASE 3):
Organisaation teknisen tietoturvan parantaminen

- **O** Organisaatio toteaa riskiarvoissa, että todennäköisyys kyberhyökkäyksen kohteeksi joutumiselle on korkea ja päättää parantaa teknisen tietoturvan tasoa.
- **O** Turvatason parantamiseen ohjataan resursseja ja osana sitä päätetään lisätä teknisen uhkatiedon hankintaa.
- **O** Organisaatio tunnistaa kriittisimmän suojattavan omaisuuden ja kartoittaa ulkoisia ja sisäisiä lähteitä, joista näihin sovelluksiin liittyvää relevanttia uhkatietoa voidaan saada.
- **O** Määritetään, mitä tietoa halutaan kerätä, kenen toimesta ja miten hankittu data hyödynnetään.
- **K** Organisaatio laajentaa teknisen uhkatiedon hankintaansa lisäämällä lähteiden joukkoon uusia haavoittuvuustietokantoja ja -syötteitä. Data kerätään ja koostetaan Splunk-alustalla, johon ohjataan myös olemassa olevista MISP-verkostoista saatava tieto.
- **K** Splunkissa data yhdenmukaistetaan ja sovellus konfiguroidaan antamaan hälytys kriittisimpiin kohteisiin liittyvien uhkien tunnistamisesta.
- **A** Raakadataa analysoidaan jatkuvasti hyödyntäen poikkeamien havainnointiin erikoistuneita tekoälymalleja ja muita vastaavia työkaluja. Hälytyskynnystä säädetään ja muokataan tuottamaan vain relevantteja ja todellisia toimenpiteitä vaativia ilmoituksia.
- **J** Hälytyksistä tiedotetaan tarpeen mukaan organisaation sisällä ja johto vastaa poikkeamatilanteista tiedonjakoon organisaation ulkopuolelle.

TIETOA DNV CYBERISTA

DNV Cyber on johtava kyberturvallisuuspalvelujen tarjoaja. Autamme yrityksiä niiden monitahoisissa tarpeissa tehden niistä turvallisempia ja sietokykyisempiä. Yli 500 asiantuntijan maailmanlaajuisella tiimillämme on yli 30 vuoden kokemus IT- ja teollisuuden ohjausjärjestelmien kyberturvallisuudesta. Autamme asiakkaitamme useilla toimialoilla suoriutumaan helpommin ja paremmin.

Tunnistamme, priorisoimme ja viestimme riskeistä, ohjaamme yrityksiä säädösten vaatimuksissa ja yhdistämme kyberturvallisuuden asiakkaidemme liiketoimintatavoitteisiin. Kyberturvallisuuspalvelujen tarjoajana hyödynnämme tehokasta teknologiaa ja uhkatietoa, autamme turvaamaan kyberinvestoinnit ja toteuttamaan kustannustehokkaita toimenpiteitä. Havaitsemme uhat ja reagoimme niihin sekä varmistamme toimintojen jatkuvan parantamisen ja nopean palautumisen.

Esitämme kysymyksiä ja kuuntelemme sekä puhumme toimialasi kieltä. Teemme yhteistyötä ja jaamme näkemyksiä, kehitämme alan standardeja ja luomme parhaita käytäntöjä turvaten sen, mikä on kriittistä, samalla mahdollistaen yritysten menestymisen.

DNV Cyber muodostettiin yhdistämällä Nixu, Applied Risk ja DNV vuonna 2024.

TIETOA DNV:STÄ

DNV on riippumaton varmennuksen ja riskienhallinnan asiantuntija, joka toimii yli 100 maassa ja jonka tehtävä on suojella ihmishenkiä, omaisuutta ja ympäristöä. Monien maailman menestyneimpien organisaatioiden luotettuna puolestapuhujana autamme tarttumaan mahdollisuuksiin ja kohtaamaan globaalien muutosten aiheuttamia riskejä. Hyödynnämme laajaa osaamistamme ja syvää asiantuntemustamme turvallisuuden ja suorituskyvyn edistämiseksi, kehitämme alan standardeja ja luomme uusia ratkaisuja.

DNV Cyber suojaa sinulle kriittistä.

CYBERWATCH FINLAND

Yritys on perustettu helmikuussa 2017.

Cyberwatch Finland liittyi osaksi Netum Groupia 21.4.2026.

Cyberwatch Finland palvelee yrityksiä ja muita organisaatioita vahvistamalla ja kehittämällä niiden kyberturvallisuuskulttuuria ja kykyä estää kyberhyökkäyksiä.

Tavoitteenamme on strategisen kybertietoisuuden ja –kyvykkyyden parantaminen toiminnan kaikilla tasoilla, yksittäisistä henkilöistä organisaatioiden ylimpään johtoon asti. Kerromme tämän hetken kyberturvallisuusilmiöistä ja niihin vaikuttavista tekijöistä.

Asiantuntijatiimimme koostuu strategisen kyberturvallisuuden monipuolisesta osaamisesta, jota täydentää laaja-alainen kokemus johtamisesta, kokonaisturvallisuudesta ja toiminnasta kansainvälisessä yritysympäristössä.

Tavoitteena kyberkyvykkäämpi maailma.


AI