DIGI- JA VÄESTÖTIETO-VIRASTO

Digitaalisen turvallisuuden havainnoinnin kehittäminen

VAHTI hyvät käytännöt tukimateriaali

16.1.2023

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Sisällysluettelo

Digitaalisen turvallisuuden havainnoinnin kehittäminen

1 Yleistä

Tämä asiakirja on tarkoitettu vapaasti hyödynnettäväksi ja sovellettavaksi tukimateriaalina. Oppaan tarkoituksena on avata yleisesti digitaalisen turvallisuuden havainnointiin ja havainnointikyvyn kehittämiseen liittyviä aiheita.

Toivomme, että annat palautetta tästä tukimateriaalista:

https://response.questback.com/dvv/digiturvahyvatkaytannotpalaute

Muut yhteydenotot koskien tätä tukimateriaalia:
digiturva@dvv.fi

2 Johdanto

Tässä oppaassa käydään läpi digitaalisen turvallisuuden havainnointiin liittyviä yleisiä periaatteita, joiden avulla julkisen hallinnon organisaatiot voivat kehittää ja tehostaa omaa digitaalisen turvallisuuden havainnointia erilaisissa toimintaympäristöissä. Oppaassa keskitytään erityisesti siihen, millä toimenpiteillä organisaatio voi rakentaa toimivan pohjan varsinaisen havainnoinnin toteuttamiselle hyödyntäen erilaisia palvelumalleja. Opas sisältää myös vinkkejä havainnointipalveluiden tarkasteluun ja hankintaan.

Digitaalisessa ympäristössä ajantasainen tilannekuva ympäristön turvallisuudesta koostuu useista eri lähteistä saaduista tiedoista ja syötteistä. Näiden tietojen ja syötteiden havainnointi, sekä siihen liittyvät toimenpiteet ja tekniset ratkaisut, ovat keskeisessä roolissa tilannekuvan muodostumisessa.

Kattavan digitaalisen ympäristön tilannekuvan muodostamiseen vaaditaan sekä organisaation oman, kuin myös organisaation ulkopuolisen toimintaympäristön havainnointia. Käytännössä tämän toteuttamiseen tarvitaan sekä automaattista havainnointia järjestelmien, palveluiden ja päätelaitteiden tapahtumista, työntekijöiden ja muiden käyttäjien itsensä tekemiä havaintoja, kuin myös erilaisista ulkoisista lähteistä kerättyä uhka- ja tilannetietoa. Ulkoisista lähteistä kerätty tieto voi olla esimerkiksi ajankohtaisten tapahtumien, viranomaistiedotteiden sekä relevanttien teknologiatoimittajien viestinnän seurantaa.

Havainnoinnilla pyritään ensisijaisesti havaitsemaan ja ehkäisemään mahdolliset turvallisuuteen liittyvät poikkeamat normaalitilanteesta, mutta havainnointitiedot tukevat organisaatiota myös poikkeamatilanteissa. Kerättyä tietoa voidaan käyttää poikkeamatilanteen mahdollisimman tehokkaaseen normalisointiin ja poikkeaman syiden selvittämiseen. Organisaation tulisi myös oppia havaituista poikkeamista, virheistä sekä kehittää omaa toimintaa havaintojen kautta.

3 Havainnoinnin merkitys

Havainnointikyvyllä organisaatio mahdollistaa suojattavien kohteiden tietoturvallisuuteen sekä tietosuojaan liittyvän valvonnan. Organisaatio kykenee tunnistamaan negatiiviset tapahtumat kuten poikkeamat ja väärinkäytökset, sekä selvittämään esimerkiksi näiden tapahtumien laajuuden. Havainnoinnilla mahdollistetaan myös tiedonkäsittelyyn liittyvien päivittäisten tapahtumien ja tapahtumaketjujen osapuolten yksiselitteisen selvittämisen, kiistämättömyyden, jäljitettävyyden, sekä tätä kautta varmistetaan tietoa käsittelevien henkilöiden oikeusturvan toteutumista.

Lisäksi havainnoinnilla helpotetaan häiriöiden selvittämistä sekä nopeutetaan organisaation toiminnan palauttamista häiriötilanteista normaalitasolle. Organisaatio kykenee myös valvomaan ja seuraamaan organisaation toiminnalle oleellisten toiminteiden käyttöä, suorituskykyä ja käytettävyyttä.

Voidaankin sanoa, että havainnointi mahdollistaa ja tukee organisaation reaaliaikaisen digitaalisen turvallisuuden tilannekuvan muodostamista, sekä mahdollistaa oikea-aikaisen reagoinnin havaittuihin tapahtumiin, vikatilanteisiin ja poikkeamiin. Lisäksi havainnointi mahdollistaa laadukkaan raportoinnin ja tilastoinnin, sekä tukee yleisesti organisaation lainmukaisuuden sekä mahdollisten muiden regulaatioiden toteutumista.

Toisin sanoen, havainnointi mahdollistaa muun muassa:

- poikkeamien ja väärinkäytösten selvittämisen,
- poikkeamiin reagoinnin ja toiminnan palauttamisen normaalitasolle,
- suorituskyvyn ja käytettävyyden seurannan,
- digitaalisen turvallisuuden tilannekuvan muodostamisen,
- raportoinnin ja tilastoinnin,
- lainmukaisuuden sekä mahdollisten muiden regulaatioiden toteutumisen,
- digitaalisen turvallisuuden kehittämisen havainnoituun tietoon perustuen.

4 Havainnointi osana digitaalisen turvallisuuden arkkitehtuuria

Digitaalisen turvallisuuden arkkitehtuuri koostuu organisaation digitaalisen turvallisuuden rakennusosista kuten toimintatavoista ja teknisistä ratkaisuista sekä niiden suhteesta organisaation tavoitteisiin ja toimintaan.

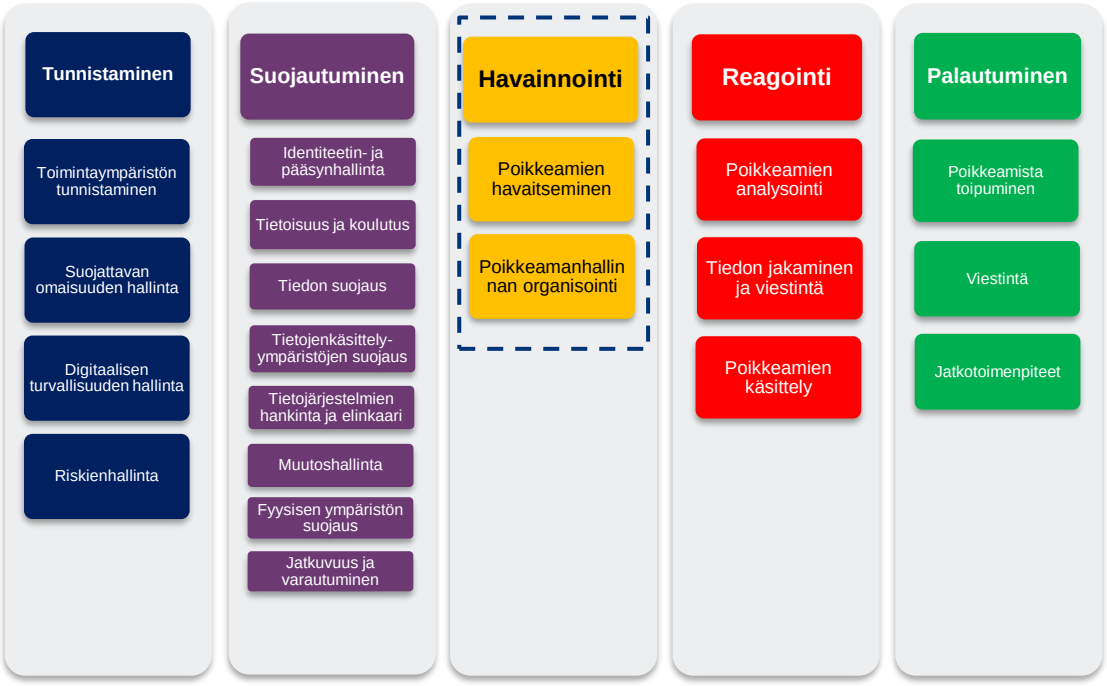
Havainnointi ja siihen liittyvät tekniset ratkaisut sekä prosessit muodostavat olennaisen osan digitaalisen turvallisuuden arkkitehtuuria, sillä sen avulla poikkeamat digitaalisen turvallisuuden perustasosta havaitaan mahdollisimman varhaisessa vaiheessa ja niihin voidaan reagoida valmiiksi määritellyn prosessin mukaisesti.

Poikkeavien tapahtumien havaitseminen digitaalisissa toimintaympäristöissä vaatii usein etenkin päätelaitteiden, verkkolaitteiden ja palveluiden tuottamaa tietoa ja sen analysointia ja havainnoinnin tuleekin kohdistua sekä organisaation itse ylläpitämiin, että ulkoistettuihin tai palveluina ostettuihin organisaation toiminnalle olennaisiin kohteisiin.

Digitaalisen turvallisuuden havainnoinnin suunnittelu lähtee liikkeelle oman toiminnan ymmärtämisestä, ja erityisesti seuraavat kysymykset auttavat pääsemään alkuun havainnoinnin suunnittelussa:

- Mitä suojattavia kohteita, kuten digitaalisia palveluita tai tietoa, organisaatiolla on?
- Millaisia uhkia tai riskejä organisaation toimintaan kohdistuu?

Edellä mainitut kysymykset tukevat havainnoinnin suunnittelua asettamalla tavoitteet toimintamallille, joka perustuu organisaation itsensä muodostamaan realistiseen käsitykseen siitä, mitä kohteita tulee suojata ja millainen uhkaprofiili organisaatiolla on, eli millaiset uhkat voisivat todennäköisimmin kohdistua organisaatioon.



Kuva 1. Havainnointi ja reagointi osana digitaalisen turvallisuuden arkkitehtuuria

Yllä olevan kuvan mukaisesti havainnointi osana digitaalisen turvallisuuden arkkitehtuuria käsittää poikkeamien havaitsemiseen tarvittavat prosessit, tekniset ratkaisut ja toimintamallit sekä näiden organisoinnin.

Keskeisenä tekijänä poikkeamien havaitsemisessa on tilannekuvan muodostamiseen erikoistuneet tietoturvavalvomotoiminnot, joiden toimintamalleja ja käyttöä tämä opas avaa.

Tietoturvavalvomotoiminto voi olla organisaation sisäisesti järjestämä, tai ulkoisesti hankkima palvelu.

5 Organisaatiolta vaadittavat valmiudet

Riippumatta siitä, toteutetaanko havainnoinnin osalta varsinainen operatiivinen toiminta, kuten järjestelmien valvonta ja uhkatiedon seuranta, organisaation itsensä vai ulkopuolisen palveluntuottajan toimesta, organisaatiolla itsellään on oltava tiettyjä valmiuksia sekä tuottaa, että vastaanottaa tietoa.

Organisaatiolla tulisi olla kyky itsenäisesti tai havainnointipalvelua tarjoavan toimijan kanssa yhteistyössä:

1. Tunnistaa suojattavat kohteet
2. Tunnistaa organisaatioon kohdistuvat keskeisimmät uhat
3. Tunnistaa suojattavien kohteiden tuottama havainnointia tukeva tieto
4. Vastaanottaa tilannekuvaa analysoidun havainnointitiedon pohjalta
5. Hallita poikkeamia
6. Tunnistaa eri toimijoiden roolit havainnoinnissa ja tilannekuvan muodostumisessa
7. Perustaa tai ottaa käyttöön valvontaan sekä havainnointiin liittyvät organisaatiorakenteet ja tekniset kyvykkyydet

Ensimmäiseksi organisaation on tunnistettava organisaation toiminnalle kriittiset suojattavat kohteet. Tunnistamisessa tulee myös huomioida organisaation toiminnalle kriittinen tieto, ja erityisesti se, missä järjestelmissä ja palveluissa tietoa käsitellään ja säilytetään. Lisäksi suojattaville kohteille sekä tiedolle tulee määrittää omistajuus, jotta organisaatio kykenee kohdistamaan ja resursoimaan havainnointikyvyn oikeisiin kohteisiin.

Suojattavia kohteita voi sijaita esimerkiksi:

- Organisaation itse tuottamassa infrastruktuurissa
- Organisaation kapasiteetti- tai palvelutoimittajan tuottamassa palvelussa
- Organisaation käyttämissä pilvipalveluissa
- Organisaation käyttämissä tietoturvapalveluissa

Suojattavien kohteiden on tuotettava organisaation määrittelemää lokitietoa, ja lokitieto tulee olla mahdollista välittää tai siirtää organisaation määrittelemään paikkaan sellaisessa muodossa, joka mahdollistaa lokitiedon hyödyntämisen.

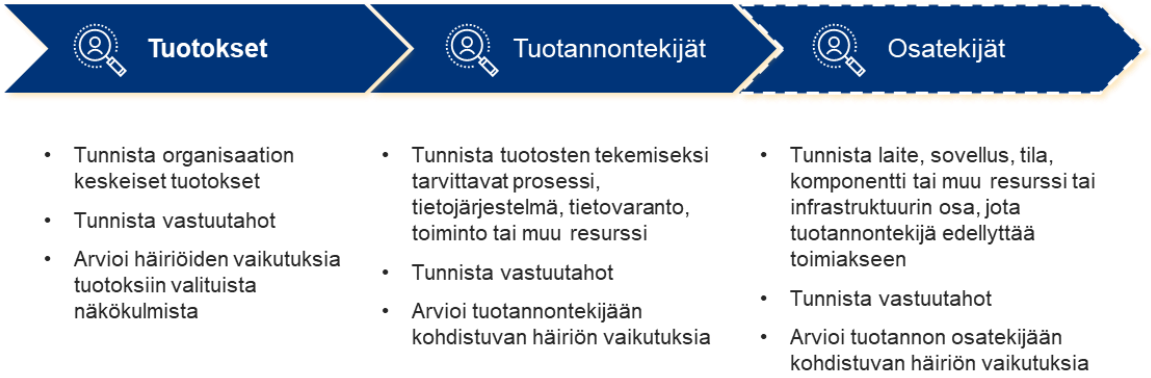
Organisaation on lisäksi kyettävä vastaanottamaan tuotettua, ja mahdollisesti analysoitua havainnointitietoa ja reagoimaan poikkeamiin sekä tekemään päätöksiä poikkeamien hallinnasta sen perusteella.

5.1 Suojattavien kohteiden tunnistaminen

Organisaation oman toimintaympäristön, arkkitehtuurin ja rakenteiden tunteminen on avainasemassa myös havainnoinnin suunnittelussa. Kun suojattavat kohteet ja oma toimintaympäristö tunnetaan, on helpompi määritellä teknisiä toteutuksia ja prosesseja havainnoinnille.

Jotta havainnoinnin toimenpiteitä, kuten esimerkiksi teknistä valvontaa, voidaan kohdistaa oikein, organisaation tulee tunnistaa toimintaympäristönsä suojattavat kohteet. Digitaalisen turvallisuuden kannalta erityisesti organisaation tärkeitä toimintoja tukevat tietojärjestelmät, tietovarannot, infrastruktuuri ja käytön mahdollistavat päätelaitteet ovat eräitä keskeisiä esimerkkejä suojattavista kohteista. Suojattavat kohteet voivat siis olla organisaation itse tuottamia, ulkoistettuja tai palveluina ostettuja.

Organisaatiosta riippuen suojattavia kohteita voi olla hyvinkin suuria määriä. Tästä syystä saattaa olla tarpeellista priorisoida kohteita sen mukaisesti, mitkä kohteet ovat organisaation toiminnan kannalta kaikkein tärkeimpiä ja keskittää varsinkin alkuvaiheessa havainnointitoimia erityisesti niihin kohteisiin.



Kuva 2. Kriittisten kohteiden luokittelu

Suojattavien kohteiden tunnistamisessa ja niiden priorisoinnissa on suositeltavaa hyödyntää menetelmää, joka kuvataan Digi- ja väestötietoviraston julkaisemassa oppaassa kriittisten kohteiden luokittelusta[1].

5.2 Keskeisten uhkien tunnistaminen

Havainnoinnin kannalta ei kuitenkaan riitä pelkästään se, että tunnistetaan suojattava omaisuus. Sen lisäksi on syytä kiinnittää huomiota siihen, millaisia uhkia organisaatioon kohdistuu ja millaisen riskin ne muodostavat organisaation toiminnalle.

Organisaation omaa uhkaprofiilia selvitettäessä on otettava huomioon sekä uhkatoimijat, että niiden digitaaliselle toimintaympäristölle muodostamat konkreettiset uhat.

Euroopan kyberturvallisuusviraston (ENISA) julkaisemien raporttien[2] mukaan yleisimpiä uhkatoimijoita digitaalisessa toimintaympäristössä voivat olla esimerkiksi

[1] Kriittisten kohteiden luokittelu. VAHTI hyvät käytännöt tukimateriaali. 2022.
[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

- järjestäytynyt rikollisuus,
- valtiollisten toimijoiden muodostamat uhat tai
- poliittisen tai sosiaalisen aktivismin eri muodot.

Edellä mainittujen toimijoiden muodostamat yleisimmät uhat ovat tyypillisimmin;

- Kiristyshaittaohjelmat
- Haittaohjelmat
- Käyttäjien manipulointi, mukaan lukien käyttäjätunnusten kalastelu
- Ohjelmistohaavoittuvuudet
- Palvelunestohyökkäykset
- Disinformaatio
- Toimitusketjuun kohdistuvat uhat

Yksittäiseen organisaatioon kohdistuvien uhkien tunnistaminen saattaa olla haastavaa erityisesti siinä tapauksessa, mikäli organisaatio toteuttaa useaa erilaista tehtävää. Tästä syystä onkin suositeltavaa ottaa mahdollisimman kattavasti huomioon erilaisia uhkia monipuolisesti eri lähteisiin perustuen.

Tietoturvavalvomoiden toiminta perustuu uhkatiedon keräämiseen, analysointiin ja tämän tiedon perusteella toteutettavaan digitaalisen ympäristön valvontaan. Uhkatiedon lähteinä voi olla muun muassa tiedonvaihtoverkostot, kaupalliset uhkatietolähteet ja avoimet lähteet kuten media ja erityisesti uhkatiedonvaihtoon kehitetyt standardit ja prosessit.

5.3 Havainnointia tukevan tiedon kerääminen ja analysointi

Viimekädessä havainnoinnin tarkoitus on tuottaa tilannekuvaa operatiivisen toiminnan ja johtamisen tueksi. Havaitsemalla poikkeamat ja häiriöt niihin voidaan reagoida, mikä toisaalta mahdollistaa myös korjaavien toimenpiteiden tekemisen digitaalisen turvallisuuden kehittämiseksi.

Tiedon kerääminen tarkoittaa saatavilla olevan tiedon kokoamista erilaisia tietolähteitä hyödyntäen. Tietolähteet voivat sisältää muun muassa teknisiä valvontatoimia, käyttäjien ilmoittamia havaintoja sekä myös tietoa ja tiedotteita ulkoisista lähteistä, kuten esimerkiksi kansallisista turvallisuusviranomaisilta saatavilla olevaa tietoa. Alla olevassa taulukossa on listattu erilaisia tietolähteitä, joita havainnoinnissa voidaan hyödyntää:

Sisäiset tietolähteet	Ulkoiset tietolähteet	Tiedonvaihto ja verkostot
Sovellusten käyttö- ja lokitiedot	Organisaation palvelutuottajien tarjoama raportointi ja näkymä palveluihin	Viranomaisten raportit ja tilannekuvapalvelut, esimerkiksi

		Kyberturvallisuuskeskuksen katsaukset
Päätelaitteiden ja käyttöjärjestelmien lokitiedot	Laite- ja sovellusvalmistajien tiedotteet muun muassa haavoittuvuuksista ja tietoturvaparannuksista	Tiedonvaihtoverkostot, kuten esimerkiksi VAHTI
Tietoliikenneinfrastruktuurin, kuten palomuurien ja reitittimien käyttö- ja lokitiedot	Tarkastukset ja auditoinnit	Organisaatioiden väliset yhteiset hankkeet ja kehittäminen
Pilvipalveluiden käyttö- ja lokitiedot	Organisaation muiden sidosryhmien tarjoamat tiedot tai analyysit	Tilaisuudet ja katsaukset liittyen digitaaliseen turvallisuuteen
Henkilöstön poikkeamailmoitukset	Laite- ja sovellusvalmistajien tarjoamat tiedotteet muun muassa haavoittuvuuksista	
Keskitetyn käyttövaltuushallinnan valvonta- ja lokitiedot		
Tarkastukset ja auditoinnit		

Riippuen organisaation koosta ja suojattavien kohteiden määrästä, edellä esitetyistä tietolähteistä saattaa kertyä valtava määrä tietoa, jolloin tiedon käsittely manuaalisin toimenpitein on käytännössä mahdotonta. Siksi onkin tärkeää tietää, mitkä tiedot ovat havainnoinnin kannalta olennaisia ja käyttää apuna automaattisia järjestelmiä havainnoinnin tukemiseksi. Havainnoinnin tukena voidaan hyödyntää muun muassa seuraavia teknisiä ratkaisuja:

- **Lokitietojen** automaattisen keräyksen ja analysoinnin, esimerkiksi SIEM-järjestelmän (engl. Security Information and Event Management), avulla voidaan havainnoida poikkeamia siten, että järjestelmä tutkii automaattisesti tapahtumia määritettyjen käytäntöjen mukaisesti ja hälyttää perustasosta poikkeavista tapahtumista. Usein tietoturvavalvomo operoi keskitettyä lokienhallintajärjestelmää. Lisäksi lokitietojen tallentaminen ja helppo etsittävyys ovat tärkeitä ominaisuuksia, kun tietoturvapoikkeaman sattuessa selvitetään jälkikäteen mitä on tapahtunut, missä on tapahtunut, milloin on tapahtunut ja kuka on tehnyt.

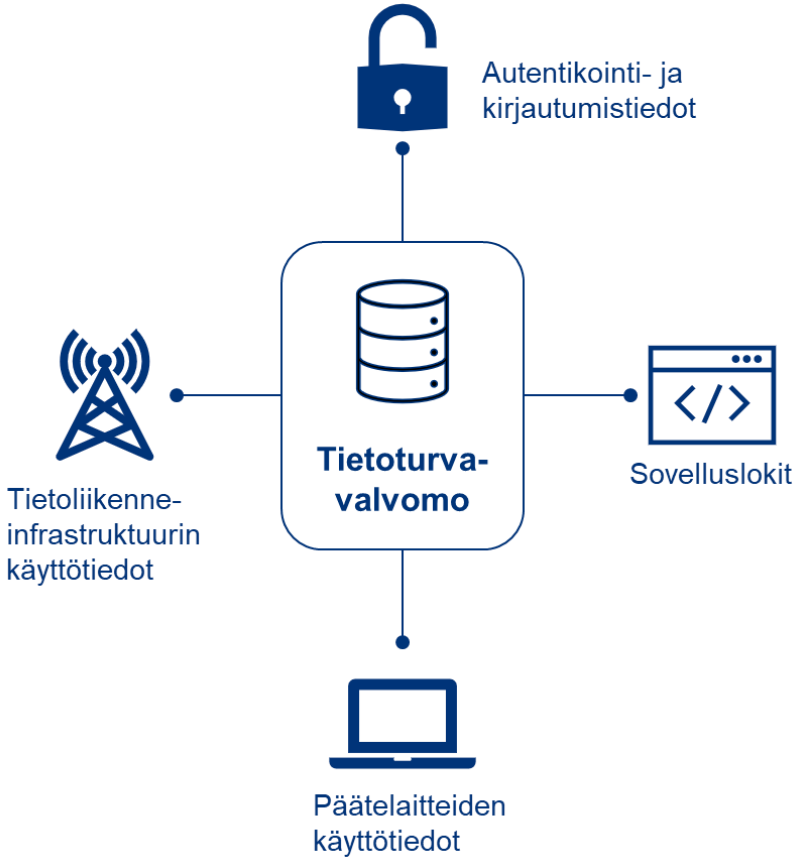
- **Tietoliikenneratkaisujen,** kuten palomuurien tai tunkeutumisen havaitsemis- tai estämisjärjestelmät (engl. Intrusion Detection System, IDS tai Intrusion Prevention System, IPS) avulla voidaan havainnoida tietoverkoissa tapahtuvaa verkkoliikennettä. Palomuuriteknologioiden avulla tietoverkot voidaan

eriyttää omiksi kokonaisuuksiksi ja niissä tapahtuvat luvattomat pääsy-yritykset voidaan havaita ja jopa estää resurssien luvaton käyttö automaattisesti.

- **Päätelaitesuojausta** (engl. Endpoint detection and response, EDR) käytetään päätelaitteiden ja palvelinten käyttöjärjestelmien valvontaan ja niissä tapahtuvan epäilyttävän toiminnan tunnistamiseen. Päätelaitesuojaus kerää kattavasti käyttötietoa päätelaitteista kuten tietokoneista, palvelimista ja mobiililaitteista sekä vertaa tätä tietoa ennalta määritettyihin tunnisteisiin. Päätelaitesuojauksen toiminta perustuu sovellustoimittajien keräämään tietoon haittaohjelmista ja muista uhkatekijöistä, jolloin päätelaitteelta kerättyä tietoa voidaan verrata muualla tehtyihin havaintoihin.

  Päätelaitesuojaus voi toimia myös reaktiivisesti eristämällä päätelaitteen haittaohjelmatartunnan tai uhkaavaa toimintaa tunnistaessaan. Päätelaitesuojauksen tuottama tieto on avainasemassa myös tietoturvavalvomoiden keräämän tiedon analysoinnissa ja valvonnassa.

- **Autentikointi ja kirjautumistiedot,** joita palvelut, järjestelmät ja sovellukset tuottavat ovat myös avainasemassa, kun valvotaan digitaalisen ympäristön käyttöä. Kirjautumistiedot voivat paljastaa luvattoman kirjautumisen sekä tiedon siitä, mistä ja mihin aikaan luvaton kirjautuminen on tehty.



Kuva 3. Tietoturvavalvomo kerää ympäristön havainnointitietoja

Tiedon keräämisen ja käsittelyn osalta on hyvä huomioida, että lokitietojen tuottamiseen, keräämiseen, analysointiin ja hyödyntämiseen liittyy myös lakisääteisiä velvollisuuksia, joiden toteutumisesta vastaa aina pääsääntöisesti tiedon tai järjestelmän omistaja.

Havainnoinnin osalta olennaisia tiedon keräämistä ja käsittelyä ohjaavia säädöksiä:

- *Laki julkisen hallinnon tiedonhallinnasta 906/2019*
- *Tietosuoja-asetus, GDPR – 2016/679* henkilötietojen käsittelyn osalta
- *Laki yksityisyyden suojasta työelämässä 759/2004* työnantajan suorittaman teknisen valvonnan osalta

5.4 Poikkeamien havaitseminen

Poikkeavan toiminnan havainnointia voidaan toteuttaa tehokkaasti, jos suojattavat kohteet ja niiden käyttötarkoitus sekä toimintaympäristö tunnetaan riittävän hyvin. Lisäksi poikkeamien tehokas havaitseminen edellyttää organisaation digitaalisen ja fyysisen ympäristön teknistä valvontaa ja tähän erikoistuneita ratkaisuja. Valvonta voidaan toteuttaa itsenäisesti tai se voidaan ulkoistaa palveluntuottajalle, mutta kummassakin tapauksessa organisaatiolla itsellään on oltava käsitys siitä, mitä kohteita valvotaan ja miksi.

Huomionarvoista on myös se, että digitaalisen turvallisuuden havainnointia tukevat teknisten ratkaisujen ja valvonnan lisäksi myös käyttäjien poikkeavuuksista tekemät ilmoitukset. Siksi onkin tärkeää, että organisaatio on toteuttanut toimintamallin ilmoitusten raportointiin ja vastaanottamiseen. Lisäksi organisaation henkilöstö tulee kouluttaa havaitsemaan ja ilmoittamaan organisaation toimintaan kohdistuvista uhkista, haavoittuvuuksista ja poikkeamista.

Poikkeavien tapahtumien havaitsemisen edellytyksenä on, että organisaatio ymmärtää suojattavan kohteen käytön normaalin, tyypillisen toiminnan. Organisaation tavoitteena onkin muodostaa käsitys normaaleista tapahtumista, jotta saadaan vertailukohta epätavallisille tapahtumille, eli poikkeamille. Suojattavan kohteen toiminnan ymmärtämisessä voidaan esimerkiksi käyttää alla olevia menetelmiä:

- tapahtuman tyyppi (onko kyse esimerkiksi tiedon muuttamisesta vai tiedon katselusta)
- tapahtuman esiintymisen harvinaisuus tai uutuus (tapahtumaa ei ole koskaan ennen nähty, tai se on todella harvinainen)
- lähde- ja kohdeosoitteet (onko lähde ja/tai kohde esimerkiksi ns. mustalla/valkoisella listalla)
- kellonaika ja viikonpäivä (tapahtuuko tapahtuma poikkeukselliseen tai huomiota herättävään ajankohtaan?)
- tapahtuman esiintymisen tiheys (esimerkiksi hyvin tiheästi, tai tietyllä aikavälillä ilmenevät tapahtumat)

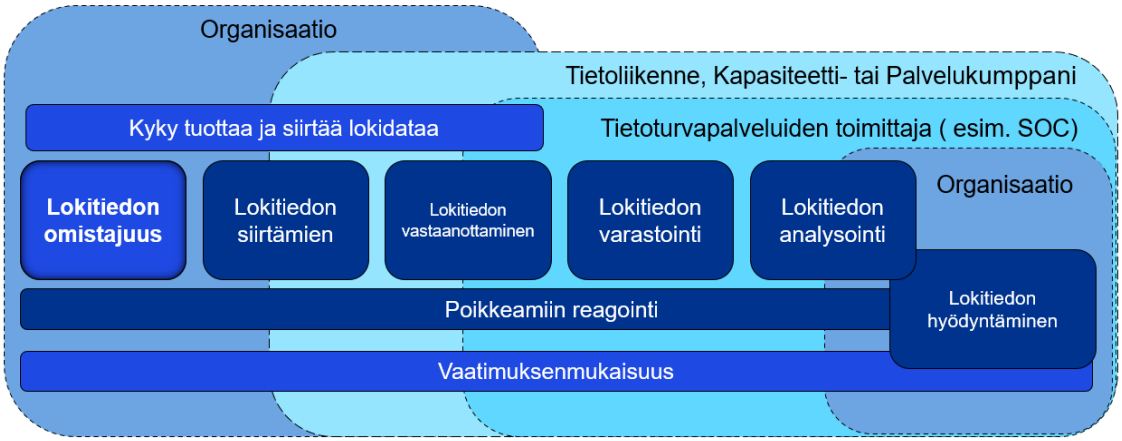
Havaitut poikkeamat, joilla on negatiivinen vaikutus organisaation toimintaan, pyritään estämään kokonaan, tai syntyneitä haittoja tulee kyetä pienentämään siten että organisaation toimintakyky pystytään palauttamaan. Poikkeamien estäminen ja haittojen pienentäminen perustuvat riskilähtöiseen ennakointiin, sekä oikea-aikaiseen reagointiin.

5.5 Eri toimijoiden roolit havainnoinnissa

Organisaation käyttämät palvelutuottajat, esimerkiksi perinteiset toimisto-, kapasiteetti- ja konesalipalveluita, sekä erilaisia pilvipalveluita tuottavat kumppanit ovat myös olennaisia havainnointiin liittyvien syötteiden tuottajia.

Usein tiedonhallinnan ympäristöt muodostuvat usean eri toimittajan palveluista sekä ratkaisuista ja saattavat sisältää myös useita erilaisia palvelumalleja aina valmiista ohjelmistopalveluista puhtaaseen konesalikapasiteettiin. Tästä syystä havainnoinnin kannalta onkin ensiarvoisen tärkeätä kyetä kokoamaan eri ympäristöistä kerätyt havainnot yhteen, siten että se muodostaa digitaalisen turvallisuuden kannalta merkityksellistä tilannekuvan kokonaisuutta.

Tästä syystä organisaation tulisikin mahdollistaa yhteistyö eri toimijoiden välillä esimerkiksi integroimalla keskitetty lokienhallinta ja tietoturvavalvomo lokilähteisiin sekä huomioida myös mahdolliset integraatiotarpeet organisaation oman toiminnanohjausjärjestelmän sekä palvelutuottajien toiminnanohjausjärjestelmien välillä. Laadukkaat integraatiot mahdollistavat tehokkaan palveluidenhallinnan, sekä tehokkaan poikkeamienhallinnan ja välittömän reagoimisen havaittuihin poikkeamiin.



Kuva 4. Eri toimijoiden roolit havainnointitiedon tuottamisessa ja käsittelyssä

5.6 Roolit ja vastuunjako

Aiemmin käsiteltyjen teknisten ratkaisujen lisäksi havainnointiin liittyvä toiminta pitää organisoida laadittujen prosessien ja toimintamallien mukaisesti. Organisoituminen tarkoittaa sitä, että havainnointiin ja poikkeamien käsittelyyn liittyvät roolit, vastuut ja viestintä eri roolien välillä on määritetty.

Tässä kappaleessa on kuvattu tyypillisiä digitaaliseen turvallisuuteen liittyviä rooleja ja vastuita havainnoinnin ja tilannekuvan muodostamisen kontekstissa. Roolit ja vastuut voivat kuitenkin poiketa organisaatiokohtaisesti tässä kappaleessa esitetystä.

Strategisella tasolla digitaalisen turvallisuuden toteutumisesta ja vaatimuksenmukaisuudesta vastaa organisaation ylin johto. Ylin johto vastaa siitä, että muun muassa havainnointiin liittyvät toimet ovat linjassa lakien ja asetusten sekä organisaation strategian kanssa. Ylimmän johdon rooli on mahdollistaa toiminta ja toimia päätöksien hyväksyjänä.

Koordinoivan tai taktisen tason vastuulla on koostaa, välittää ja raportoida tietoa strategiselle tasolle päätöksenteon tueksi. Tietoturvapäällikkö tai palvelun omistaja vastaa useimmiten koordinoivan tason toimenpiteistä. Koordinoiva taso vastaa yleensä myös havainnoinnin periaatteiden määrittämisestä sekä havainnointiin liittyvien sisäisten ja ulkoisten yhteistyökumppanien toiminnan ohjauksesta. Koordinoivan tason vastuulla on kerätä ja vastaanottaa tietoa operatiiviselta tasolta.

Operatiivisen tason rooli on tehdä varsinainen tiedon kerääminen lokilähteisiin ja muihin lähteisiin perustuen. Operatiivisella tasolla toimivan tietoturvavalvomon asiantuntijoiden tehtäviin kuuluu muun muassa havainnoida poikkeamia sekä reagoida poikkeamiin käsittelemällä ja analysoimalla eri lähteistä kerättyä tietoa. Operatiivinen taso vastaanottaa taktiselta tasolta havainnoinnin suorittamiseen tarvittavat periaatteet ja vaatimukset.

Tietoturvapäällikkö

Vastaa havainnoinnin periaatteiden ja ohjeistuksen päivittämisestä ja ylläpidosta, hankkeiden ja –toimenpiteiden eteenpäin viennistä, menettelytapojen valvonnasta ja edistämisestä. Seuraa havainnoinnin toteutusta ja tekee ehdotuksia vastuutahoille. Vastaa osaltaan havainnoinnin tueksi kerättävien tietojen tarpeiden ja perusteiden määrittelystä.

Tietosuojavastaava

Vastaa osin sekä tukee organisaatiota henkilötietoa sisältävien havainnointitietojen keräämisen perusteiden määrittelystä.

Järjestelmän omistaja

Järjestelmän omistaja vastaa omistamansa järjestelmän osalta havainnoinnin vaatimuksenmukaisesta toteuttamisesta, sekä järjestelmän kyvystä tuottaa ja kerätä havainnointitietoa.

Tietohallinto

Vastaa vastuullaan olevien järjestelmien ja palvelujen osalta havainnoinnin vaatimuksenmukaisesta toteuttamisesta. Useimmiten tietohallinto myös vastaa havainnointiin liittyvien operatiivisten palveluiden koordinoinnista, tuottamisesta sekä hankinnoista, sopimuksista ja niiden hallinnasta.

Tietoturva- tai tietosuojaryhmän jäsen

Osallistuu ryhmän kokouksiin ja välittää tarpeellista havainnointiin ja sen toteuttamiseen liittyvää tietoa omille toimialueilleen. Tukee omalla toiminnallaan havainnoinnin toteutumista ja kehittämistä.

Henkilöstö

Henkilöstön vastuulla on omalta osaltaan seurata ja tunnistaa poikkeavia tapahtumia omassa työympäristössään ja käyttämissään järjestelmissä, ja raportoida näistä poikkeamista eteenpäin määritettyjen käytäntöjen mukaisesti.

Palveluntuottajat

Vastaavat ylläpitämiinsä organisaation järjestelmiin liittyvän havainnoinnin toteutuksesta ja raportoinnista tilaajan määrittelemien vaatimusten ja käytäntöjen mukaisesti. Palveluntuottajan tulee lisäksi seurata ja valvoa oman palvelutuotantonsa digitaalisen turvallisuuden tilaa.

6 Toteutus- ja palvelumallit

Organisaatiolla on mahdollisuus toteuttaa havainnointiin liittyviä toimintoja eri tavoilla ja palvelukonsepteilla. Alla on kuvattu erilaisia toimintamalleja, joita organisaatio voi hyödyntää havainnointikyvyn kehittämisessä ja käyttöönotossa.

6.1 Erilaisia toteutusmalleja

Organisaatio toteuttaa itsenäisesti havainnointipalvelut

Organisaatio voi kehittää ja luoda digitaalisen turvallisuuden havainnointiin ja reagointiin vaadittavat kyvyt kokonaan organisaation omin resurssein.

Tämä toimintamalli vaatii organisaatiolta pitkäjänteisyyttä ja sitoutumista tehdä investointeja, sekä erittäin hyvän kypsyystason henkilökunnan osaamisen, prosessien, integraatioiden sekä teknologioiden suhteen. Organisaatiolla tulee olla kykyä kehittää ja luoda uusia toimintaan liittyviä prosesseja, integraatioita sekä erittäin hyvä ymmärrys omasta toimintaympäristöstä ja kriittisistä toiminteista.

Malli sitoo merkittävästi organisaation omia resursseja, mutta myös tuottaa pitkällä aikajänteellä tarkasteltuna laadukasta havainnointi- ja reagointikykyä täysin organisaation omiin lähtökohtiin sopivalla tavalla.

Havainnointipalveluiden, kuten tietoturvavalvomon hankkiminen palveluna

Organisaatio voi hankkia digitaalisen turvallisuuden havainnointiin ja reagointiin vaadittavat kyvyt kokonaispalveluna, joka toteutetaan ja jota operatiivisessa mielessä tuotetaan organisaation ulkoisin resurssein.

Tämä toimintamalli vaatii organisaatiolta hankintavaiheessa ymmärrystä ja osaamista hankittavan palvelukokonaisuuden määrittelyssä, sekä kohtalaisen kypsyystason digitaalisen turvallisuuden havainnoinnista vastaavien tahojen osaamisessa. Organisaatiolla tulee olla halua sekä kykyä kehittää ja luoda uusia toimintaan liittyviä prosesseja, integraatioita, ohjeita sekä olla ymmärrys omasta toimintaympäristöstä ja toiminnalle kriittisistä palveluista.

Malli sitoo jonkin verran organisaation omia palvelua hallinnoivia sekä suojattavia kohteita omistavia resursseja; erityisesti näitä resursseja tarvitaan palvelun käyttöönottovaiheessa. Kokonaispalvelu tuottaa laadukkaasti hankittuna havainnointi- ja reagointikykyä, joka palveluntuottajan skaalaetujen vuoksi saattaa olla hyvinkin kustannustehokasta.

Itsenäisesti toteutetun ja ulkoistetun havainnointipalvelun yhdistelmä (hybridimalli)

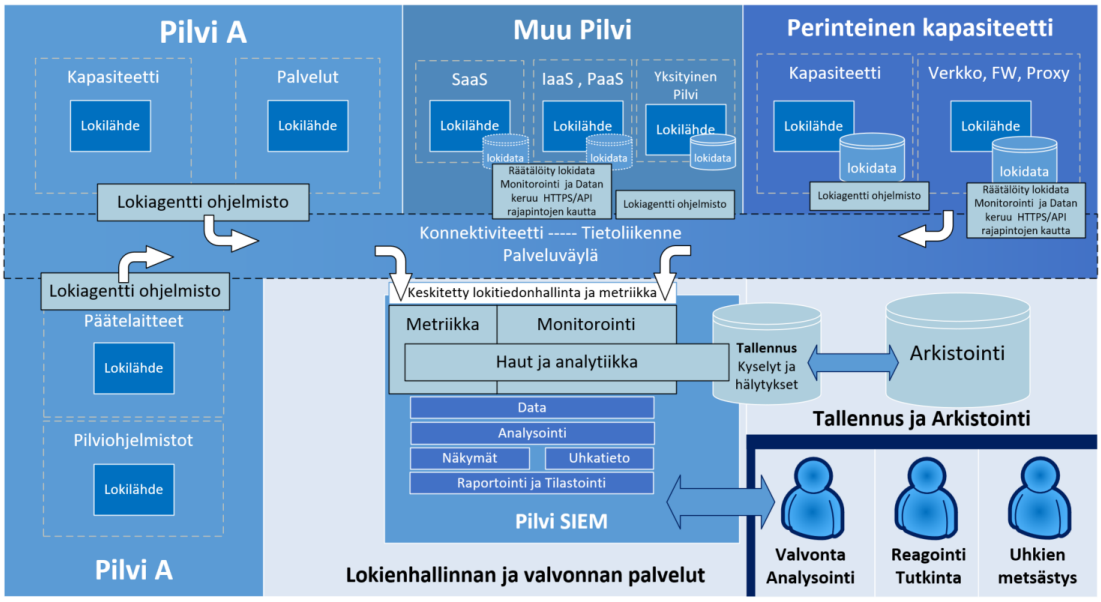
Organisaatio voi hankkia digitaalisen turvallisuuden havainnointiin ja reagointiin vaadittavat kyvykkyydet yhdistellen omia resurssejaan hankittavaan palveluun. Palvelu toteutetaan organisaatiolla jo olemassa olevan teknologian tai muiden kyvykkyyksien tukemana siten että, kokonaispalvelua tarkasteltaessa palvelukomponentteja tuotetaan myös organisaation ulkoisin resurssein.

Tämä toimintamalli vaatii organisaatiolta hankintavaiheessa laajaa ymmärrystä ja osaamista hankittavien palvelukomponenttien, ja niiden integraatioiden määrittelyissä, sekä hyvän kypsyystason digitaalisen turvallisuuden havainnoinnista vastaavien tahojen osaamisessa sekä monitoimijaympäristön hallinnassa. Organisaatiolla tulee olla halua sekä kykyä kehittää ja luoda uusia toimintaan liittyviä prosesseja, integraatioita, ohjeita sekä olla kattava ymmärrys omasta toimintaympäristöstä ja toiminnalle kriittisistä palveluista.

Malli sitoo organisaation omien palveluiden ylläpitäjiä ja palveluita hallinnoivia sekä suojattavia kohteita omistavia resursseja; erityisesti näitä sekä palvelukumppanien resursseja tarvitaan palvelun käyttöönottovaiheessa. Yhdistelmä tuottaa laadukkaasti hankittuna laadukasta, kustannustehokasta ja vaatimukset täyttävää havainnointi- ja reagointikykyä siten, että organisaatiolla on pelivaraa myös muokata palvelua omien tarpeidensa mukaisesti.

Esimerkki pilvipalveluna toteutetusta valvontapalvelusta

Organisaatiolle on valikoitunut palvelukumppaniksi yksi pääsääntöinen pilvipalveluita ja tietoturvapalveluita tuottava palvelukumppani. Organisaatio käyttää myös useita erilaisia valmisohjelmistopalveluita sekä tukeutuu osittain myös toiseen pilvipalvelutarjoajaan. Organisaatiolla on infrastruktuuria myös perinteisen paikallisen verkko-, sekä kapasiteettialustojen muodossa.



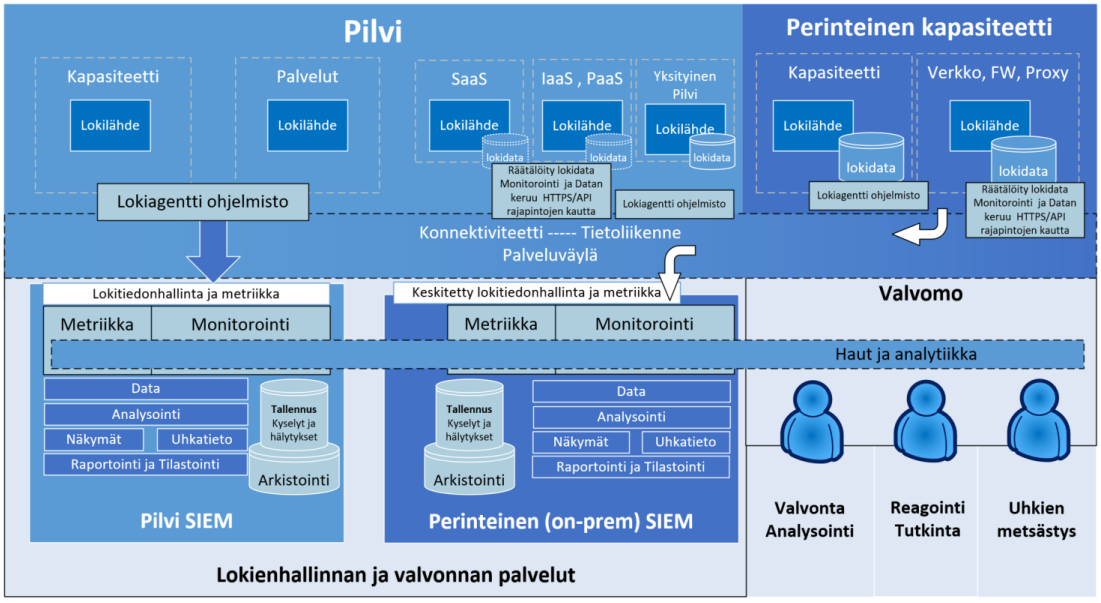
Kuva 5. Esimerkki pilvipalveluna toteutetusta valvontapalvelusta

Organisaatio on keskittänyt lokienhallinnan ja sitä kautta tuotettavan havainnointi kyvykkyyden pilvipalveluna hankittuun keskitettyyn valvonta-alustaan ja tässä esimerkissä valvoo, reagoi sekä tuottaa myös itse poikkeamienhallinnan. Poikkeamienhallinta on myös ulkoistettavissa kolmannelle osapuolelle, jolloin ulkopuolinen taho käytännössä jollain tasolla hallinnoi sekä operoi organisaation pilvessä olevaa valvonta-alustaa. Valvonta-alustan hälytykset voidaan myös edelleen lähettää, tai mahdollistaa seuranta ja analysointi kolmannelle osapuolelle rajapintojen sekä integraatioiden kautta.

Esimerkki paikallisen ja pilvipalveluna tuotetun valvonnan yhdistelmästä

Organisaatio on hankkinut ulkoisen tietoturvavalvomopalvelun. Organisaatiolla on oma paikallisesti tuotettu keskitetty lokienhallintajärjestelmä, joka on palvelukokonaisuudessa integroitu osaksi tietoturvavalvomon tuottamaa palvelua. Organisaatio on myös käyttänyt huomattavan määrän aikaa suunnitellakseen ja toteuttaakseen sujuvaan poikkeamienhallintaan liittyvät integraatiot ja työnkulun eri kumppanien välillä.

Organisaatio on arvioinut riskilähtöisesti, että pilvipalvelupohjaista valvonta-alustaa, ja siihen tarjottua tallennuspalvelua ei voida hyödyntää kaikessa organisaation lokitietojen analysoinnissa sekä tallennuksessa johtuen tiedon luottamuksellisuudesta, joten organisaatio käyttää paikallista lokienhallintajärjestelmäänsä luottamuksellisen lokitiedon säilyttämiseen ja analysointiin.



Kuva 6. Esimerkki paikallisen ja pilvipalveluna tuotetun valvonnan yhdistelmästä

6.2 Palveluiden hankinta

Organisaation tulee ennen palvelun hankintaa tunnistaa ja määritellä omat tarpeensa, kuten esimerkiksi se, tarvitseeko havaintoihin pystyä reagoimaan mihin vuorokauden aikaan tahansa, sekä arvioida kohdistuuko hankinta palvelukokonaisuuteen vai vain tiettyyn havainnointikyvykkyyteen, jota organisaatio itse tai organisaation palvelukumppani operoi, tai johonkin näiden yhdistelmään. Hankittavan palvelun sisältö riippuu myös siitä, millainen kyky organisaatiolla itsellään on palvelun käyttöön. Ei välttämättä ole tarpeellista pyrkiä heti ensimmäisenä ottamaan käyttöön ympärivuorokautista valvomopalvelua, jos organisaatiolla itsellään ei ole valmiuksia toimia vuorokauden ympäri.

Tietoturvapalveluita tuottavilla toimijoilla on usein erilaisia palvelukokonaisuuksia tarjolla. Alla on esitetty esimerkki havainnointi- tai tietoturvavalvomopalvelussa mahdollisesti hankittavista palvelu- ja/tai teknologiakokonaisuuksista, joista voidaan tarpeen mukaan muodostaa palvelukokonaisuus tai yksittäisiä havainnointikykyjä.

Esimerkiksi tietoturvatapahtumien valvonta saattaa olla pitkälle automatisoitua toimintaa, jossa asiantuntijat analysoivat ja selvittävät automaation poimimia havaintoja toimistoaikojen puitteissa tai vastaavasti asiantuntijat voivat aktiivisesti valvoa tietoturvatapahtumia vuorokauden ympäri vuoden jokaisena päivänä.

Palveluiden sisältö vaihtelee palvelun ja toimittajan mukaan, joten on syytä pyytää palvelukuvaukset nähtäville ja varmistua siitä, mitä kyseinen palvelu käytännössä sisältää.

Tietoturvavalvomopalvelut	Käyttöönottoprojekti	Havainnointia tukevat asiantuntijapalvelut
Tietoturvatapahtumien valvonta	Tietolähteiden kartoitus	Hallintamallien kehittäminen
Tietoturvatapahtumien analysointi	Valvontaan tarvittavan teknologian käyttöönotto	Tietoturva- ja tietoliikennearkkitehtuurin kehittäminen
Haavoittuvuuksien kartoitus ja hallinta	Toimintamallien laatiminen	Havainnoinnin ja poikkeamahallinnan prosessien kehittäminen
Uhkien tunnistaminen ja uhkatiedon kerääminen	Integraatioiden rakentaminen	Havainnointiteknologioiden käyttöönotto
Poikkeamien hallinta ja tietoturvaloukkausten tutkinta	Palvelumallin suunnittelu vasteaikoineen ja viestintäkanavineen.	

6.3 Havainnointipalvelun suunnittelun ja käyttöönoton tarkastuslista

Tässä kappaleessa on kuvattuna esimerkinomainen havainnointipalvelun hankinnan suunnittelun ja käyttöönoton tarkastuslista. Lopullinen käyttöönoton suunnittelu riippuu pitkälti käyttötapauksesta, eli esimerkiksi siitä kuinka laajasti organisaation järjestelmiä ja kohteita on tarkoitus saattaa keskitetyn havainnoinnin piiriin.

Useimmiten havainnointipalvelun hankkiminen ulkoiselta palveluntoimittajalta on kuin mikä tahansa muu hankinta, kuitenkin sillä erotuksella, että keskitetty havainnointipalvelu, kuten esimerkiksi tietoturvavalvomo, kerää havainnointitietoa laajasti kaikista sen piiriin lisättävistä järjestelmistä ja siten saattaa vaatia integraatioita ja suunnittelua myös organisaation eri palvelu- tai järjestelmätoimittajien välillä.

Käyttöönottoprojektin osalta riittävä suunnittelu ja ennalta valmistautuminen on erityisen tärkeää, kuten yleensäkin palveluiden hankinnoissa.

6.3.1 Tarkastuslista suunnittelun tueksi

- Tunnista ja määrittele organisaation tarpeet havainnoinnille
- Tunnista organisaation reunaehdot (juridiset, tekniset sekä muut velvoitteet)
- Varmista että organisaatiolla on kyky hyödyntää käyttöönotettavaa havainnointipalvelua täysimääräisesti
- Varmista palvelutarjoajan kyky tuottaa yhtenäinen palvelukokonaisuus
    - Kokonaisuuden palvelut, teknologiat ja mahdolliset alihankintana tuotettavat ratkaisut näkyvät palvelua käyttävälle organisaatiolle yhtenäisenä kokonaisuutena.
- Varmista, että palveluntarjoajalla on tarjottavista palveluista ajantasaiset ja päivitetyt palvelukuvaukset.
- Varmistaa että palveluntarjoaja esittää ja kuvaa toimintamallin, joka sisältää muun muassa vastuunjaon ja viestinnän palveluntarjoajan ja tilaajan välillä.
- Varmista palveluntarjoajan kyky tuottaa tarvittavat tietoliikenneyhteydet, infrastruktuuri ja integraatiot havainnointitiedon keräämiseksi ja välittämiseksi
- Selvitä, miten organisaation tietojen sekä kehitettyjen toiminnallisuuksien kanssa toimitaan palveluntarjoajan vaihdon yhteydessä.

6.3.2 Tarkastuslista käyttöönoton tueksi

Organisaatiossa tulee varmistua, että:

- Käyttöönottoprojektille on ennen projektin aloitusta määritelty tavoitteet, aikataulu ja hyväksymiskriteerit.
    - Kriteerit voivat olla esimerkiksi tiettyjen järjestelmäkokonaisuuksien saamista kokonaisuudessaan keskitetyn havainnointipalvelun piiriin.

- Käyttöönottoprojektin tarvitsemat organisaation omat resurssit on tunnistettu ja varattu, yleisimmin:
    - Käyttöönottoprojektin projektipäällikkö
    - Käyttöönottoprojektin ohjausryhmä
    - Hankittavan havainnointipalvelun omistaja
    - Havainnointi- tai lokitietoa tuottavien järjestelmien omistajat
    - Integraatioista ja prosesseista vastaavat asiantuntijat
    - Tietoliikenteestä vastaavat asiantuntijat
- Käyttöönottoprojektin hallinnan ja tekemisen vastuut ovat määritelty ja selkeitä sekä tilaajalle että havainnointipalvelua toimittavalle taholle. Tilaaja on varannut omat sekä muiden tarpeelliseksi tunnistettujen palveluntuottajien resurssit käyttöönottoprojektille.
- Palveluun liitettävät havainnointi- tai lokitietoa tuottavat kohteet on tunnistettu ja kohteiden liittämisjärjestys on määriteltynä.
    - Organisaatio on myös varmistanut, ettei havainnointiin liittämiseen tai lokitietojen käyttöön ole sopimuksellisia, tai palvelutuotantomallin tuomia esteitä.
- Projektiryhmän tulee varmistaa, että organisaation muut palvelutoimittajat ovat tietoisia käyttöönotosta, jotta heidän ylläpitämänsä tietolähteiden liittäminen keskitettyyn havainnointipalveluun onnistuu ja liittämisen kustannuksiin on varauduttu.
- Käyttöönottoprojektin hyväksymiskriteereinä kannattaa käyttää hankintavaiheessa määriteltyjä (pakollisia) vaatimuksia. Samoja vaatimuksia tulisi käyttää käyttöönottoprojektin tehtäviä muodostettaessa. Vaatimusten täyttymistä kannattaa myös seurata koko käyttöönottoprojektin ajan.

Liite 1 Esimerkki rooleista ja vastuista RACI-mallin mukaisesti

Vastuunjakotaulukko toimii vastuiden ja roolien selkeyttäjänä useamman toimijan kokonaisuudessa. Taulukkoa voidaan käyttää esimerkiksi palvelusopimuksen liitteenä tai käyttöönotto- ja suunnitteluvaiheen työvälineenä silloin, kun pohditaan millaisia tehtäviä palveluun sisältyy.

Alla esimerkinomainen vastuunjakotaulukko, joka kuvaa havainnointipalvelun vastuita hankkivan organisaation ja palvelutoimittajan välillä. Listausta kannattaa hyödyntää muokkaamalla se omaan käyttötapaukseen sopivaksi.

Selitteet:

Responsible – osapuoli, joka tekee työn asian suorittamiseksi. Tehtävänä toiminnan loppuun saattaminen ja/tai päätöksien tekeminen.

Accountable – osapuoli, joka on vastuussa toiminnasta

Consulted – tiedot antava osapuoli. Tämä ryhmä koostuu yleensä aiheasiantuntijoista.

Informed – Osapuolet, joihin toiminnan tulos vaikuttaa ja jotka on pidettävä ajan tasalla.

Aihe	Havainnoinnin palvelutoimittaja	Organisaatio tai sen alihankkija
Suunnittelu ja Ohjaus		
Organisaation tiedonhallinnan, tiedon käsittelyn, tiedon omistajuuden sekä jakamisen suunnittelu ja määrittely.	**I**	**R**
Digitaalisen turvallisuuden havainnoinnin organisointi ja seuranta	**C**	**R**
Organisaation digitaalisen turvallisuuden havainnointitarpeiden, -käyttötapausten ja suojattavien kohteiden määrittely	**C**	**R**
Palvelutoimittajan tuottaman havainnointipalvelun vaatimien tietolähteiden määrittely ja käyttöönotto	**R**	**C**
Havainnointipalvelun palveluhallinta		
Palvelutoimittajan tuottaman havainnointipalvelun hallinta ja raportointi	**R**	**I**
Palvelutoimittajan tuottamaan havainnointipalveluun kohdistuvien muutosten hallinta ja toteutus	**R**	**I**
Palvelutoimittajan tuottaman havainnointipalvelun jatkuvuuden ja käytettävyyden hallinta	**R**	**I**
Havainnointi		
Palvelutoimittajan tuottaman palvelukokonaisuuden havainnointikomponenttien (esimerkiksi lokienhallinta, SIEM, IDS/IPS,	**R**	**I**

EDR, haavoittuvuuksien hallinta) käyttöönotto ja ylläpito		
Palvelutoimittajan tuottaman havainnointipalvelun operatiivinen toteuttaminen	**R**	**I**
Palvelutoimittajan tuottaman havainnointipalvelun tuottaman tiedon analysointi ja havainnointi	**R**	**I**
Organisaation kohdistuvien uhkien tunnistaminen	**C**	**R**
Havaittujen poikkeamien selvittäminen ja toimenpiteet poikkeamien ratkaisemiseksi	**R**	**A**
Analysointi		
Organisaation poikkeamienhallinnan prosessin laatiminen	**C**	**R**
Tapahtumien ja poikkeamien luokittelumallin laatiminen ja toteuttaminen	**C**	**R**
Tapahtumien ja poikkeamien tutkinta ja analysointi	**R**	**I**
Reagointi		
Palvelutoimittajan tuottaman palvelukokonaisuuden poikkeamiin reagointi	**R**	**A**
Organisaation toimintaa koskevat viranomaisilmoitukset		**R**