Tietoturvavalvomon (SOC) käyttöönoton tarkastuslista

VAHTI hyvät käytännöt
10/2023

DIGI- JA VÄESTÖTIETO-VIRASTO

Yleistä

- Tämä opas on tarkoitettu vapaasti hyödynnettäväksi ja sovellettavaksi tukimateriaalina. Oppaan tarkoituksena on helpottaa tietoturvavalvomon käyttöönottoa ja hankintaa avaamalla yleisimpiä konsepteja ja toimenpiteitä.

- Toivomme, että annat palautetta tästä tukimateriaalista lähettämällä sähköpostia osoitteeseen digiturva@dvv.fi.

- Opas on laadittu usean eri organisaation ja asiantuntijan yhteistyönä VAHTI ICT-palveluiden digitaalisen turvallisuuden kehittäminen (ICT) -työryhmässä.

1. Poikkeamanhallinnan järjestäminen
2. Tarpeen ja tavoitetilan määrittely
3. Sidosryhmien tunnistaminen
4. Tietoturvauhkien tunnistaminen
5. Valvottavien kohteiden tunnistaminen
6. Tietoturvavalvomon kilpailutus ja hankinta
7. Vastuiden ja toimivaltuuksien määrittely
8. Käyttöönottoprojekti
9. Jatkuva kehittäminen

1 Poikkeamanhallinnan järjestäminen

Mitä tulee huomioida poikkeamanhallinnassa?

Toimiva poikkeamanhallinnan prosessi on usein edellytys tietoturvavalvomon menestyksekkäälle toiminnalle. Poikkeamanhallinnassa tulee huomioida muun muassa:

- ❑ Suunnitelmat, reagointiohjeet ja varajärjestelyt poikkeamatilanteita varten
- ❑ Poikkeamien luokittelu ja vaikutusten arviointi, erityisesti laajavaikutteisten ja kriittisten poikkeamien osalta
- ❑ Organisaation yhteyshenkilöiden ja sidosryhmien tunnistaminen sekä määrittely
- ❑ Viestintäsuunnitelmien sekä häiriöviestintäohjeistuksen luonti
- ❑ Säännöllinen seuranta ja raportointi poikkeamista organisaation johdolle
- ❑ Laajavaikutteisten ja merkittävien poikkeamien käsittelystä vastaavan kriisiorganisaation määrittely
- ❑ Poikkeamatilanteiden ennalta harjoittelu
- ❑ Toimintatapojen säännönmukainen kehittäminen jälkianalyysien pohjalta

Lisätietoa poikkeamanhallinnan kehittämisestä löydät seuraavista lähteistä:

- eOppiva: Turvaa digitaalinen toiminta häiriötilanteissa
- VAHTI: Tietoturvapoikkeamatilanteiden hallinta

2 Tarpeen ja tavoitetilan määrittely

Miksi tietoturvavalvomoa tarvitaan organisaatiossasi? Millaista lisäarvoa sen odotetaan tuovan?

Tarve tietoturvavalvomon käyttöönotolle lähtee useimmiten tavoitteesta parantaa digitaalisen turvallisuuden havainnointia ja reagointia. Tietoturvavalvomo vastaa seuraaviin tarpeisiin:

- ❑ Tilannekuvan muodostaminen ja ympärivuorokautinen seuranta
- ❑ Tilannekuva ja ymmärrys organisaatiossa kehittyy, kun nähdään mitä ympäristössä oikeasti tapahtuu
- ❑ Reagointi poikkeamiin
- ❑ Poikkeamatilanteiden analysointi ja korjaavat toimenpiteet
- ❑ Tietoturvauhkien tunnistaminen
- ❑ Laajan uhkatiedon hyödyntäminen
- ❑ Hyökkäyspinnan kartoittaminen
- ❑ Teknologia tietoturvan valvontaan
- ❑ Lainsäädännön vaatimusten toteuttaminen

2 Sidosryhmien tunnistaminen

Millaisia sidosryhmiä tietoturvan valvonnassa tulee huomioida?

Tietoturvan valvontaan liittyviä sidosryhmiä voi tunnistaa esimerkiksi oheisen kehäkuvion avulla seuraavasti;

- **Sisäiset sidosryhmät.** Esimerkiksi organisaation muut sisäiset toiminnot
- **Verkostosidosryhmät.** Esimerkiksi organisaation palveluntarjoajat
- **Ulkoiset sidosryhmät.** Esimerkiksi asiakkaat, kansalaiset, viranomaiset

Tässä yhteydessä on hyvä lisäksi tunnistaa mikä on kunkin sidosryhmän rooli tietoturvan valvonnassa. Roolien ja vastuiden kartoituksessa kannattaa hyödyntää esimerkiksi RACI-matriisia.

4 Tietoturvauhkien tunnistaminen

Tunnista millaisia tietoturvauhkia organisaatioon kohdistuu, mitä valvonnalla halutaan havaita?

Uhkien tunnistamisessa voi käyttää apuna esimerkiksi seuraavia lähteitä:

- ❑ Kyberturvallisuuskeskuksen tilannekuvatuotteet
- ❑ Euroopan Unionin kyberturvallisuusvirasto ENISA:n tilannekuvaraportit
- ❑ Muut viranomaisraportit
- ❑ Teknologiatoimittajien raportit ja havainnot
- ❑ MITRE ATT&CK –viitekehys sisältää laajasti tietoja tietomurroissa käytetyistä tekniikoista ja taktiikoista
- ❑ Median ja sosiaalisen median kanavat
- ❑ Tiedonvaihtoverkostot

Esimerkkejä tyypillisistä tietoturvauhkista

- ❑ Tietojen kalastelu
- ❑ Palvelunestohyökkäykset
- ❑ Kiristyshaittaohjelmat
- ❑ Sisäiset ja ulkoiset väärinkäytökset
- ❑ Tietovuodot, tietojen varastaminen ja tuhoamien
- ❑ Haavoittuvuudet päivittämättömissä järjestelmissä
- ❑ Haittaohjelmat
- ❑ Tietomurrot
- ❑ Fyysiset uhkat, kuten murtautuminen, tulipalo, sabotaasi

5 Valvottavien kohteiden tunnistaminen

Mitä kohteita tietoturvavalvomon tulisi valvoa?

Valvottavat kohteet ja lokilähteet voivat olla tyypillisesti:

- ❑ Identiteetin- ja pääsynhallinnan ratkaisut ja niiden tuottama tieto
- ❑ Tietoliikenneinfrastruktuuri, kuten palomuurit, reitittimet ja VPN-yhteydet
- ❑ Tietokannat
- ❑ Sovellukset ja niiden rajapinnat
- ❑ Käyttäjien päätelaitteet
- ❑ Virtualisointialustat ja palvelimet
- ❑ Pilvipalvelut
- ❑ Konfiguraatiotietojen muutokset
- ❑ Hallintayhteydet
- ❑ Etätyöpöytien ja etäyhteyksien käyttö
- ❑ Käyttäjien tekemät poikkeamailmoitukset

Valvottavat kohteet kannattaa luokitella kriittisiin ja ei-kriittisiin kohteisiin.

Apuna voi käyttää esimerkiksi kriittisyysluokittelun VAHTI-työkalua. Kriittisiä kohteita voivat olla esimerkiksi:

- ❑ Toiminnan kannalta välttämättömät järjestelmät ja palvelut
- ❑ Luottamuksellista tietoa sisältävät järjestelmät ja palvelut
- ❑ Keskitetyt toiminnot, kuten esimerkiksi identiteetin- ja pääsynhallinta
- ❑ Johtamiskanavat, kuten sähköposti ja pikaviestintäkanavat
- ❑ Tietoliikenteen reitityspisteet ja palomuurit

6 Tietoturvavalvomon kilpailutus ja hankinta

Mitä hankinnassa kannattaa huomioida palveluntarjoajan ja teknologiavalinnan osalta?

Palveluntarjoajan valinnassa huomioitavia tekijöitä:

- ❑ Hankittavan palvelun budjetti
- ❑ Palveluntarjoajan referenssit
- ❑ Käytettävät teknologiat
- ❑ Palvelun sisältö ja palvelutaso
- ❑ Maantieteellinen sijainti
- ❑ Palvelun laatu ja yhteistyö
- ❑ Palveluntarjoajan kokoluokka ja taustat
- ❑ Turvallisuusvaatimukset
- ❑ Osaaminen

Teknologiavalintaan vaikuttavia tekijöitä:

- ❑ Olemassa oleva infrastruktuuri, kuten:
  - kapasiteetti,
  - palvelininfrastruktuuri ja
  - tietoliikenneinfrastruktuuri
- ❑ Pilvipalvelualustat
- ❑ Kehittämisen tiekartat ja suunnitelmat
- ❑ Turvallisuusvaatimukset
- ❑ Tuotantotavalle asetetut vaatimukset
- ❑ Vaadittavat ohjelmistolisenssit ja lisensointitapa
- ❑ Valvontaohjelmiston päivityskäytännöt

7 Vastuiden ja toimivaltuuksien määrittely

Määritellään roolit ja vastuut tilaajan, toimittajan ja muiden sidosryhmien välillä

Roolit ja vastuut määritellään asiakkaan ja palvelutoimittajan välisin sopimuksin. Vastuiden jakautumiseen asiakkaan ja palveluntoimittajan välillä vaikuttaa muun muassa palvelun laajuus sekä palveluntoimittajan ja asiakkaan omat kyvykkyydet. Alla olevassa taulukossa on kuvattu tyypillistä vastuunjakoa asiakkaan ja palveluntoimittajan välillä:

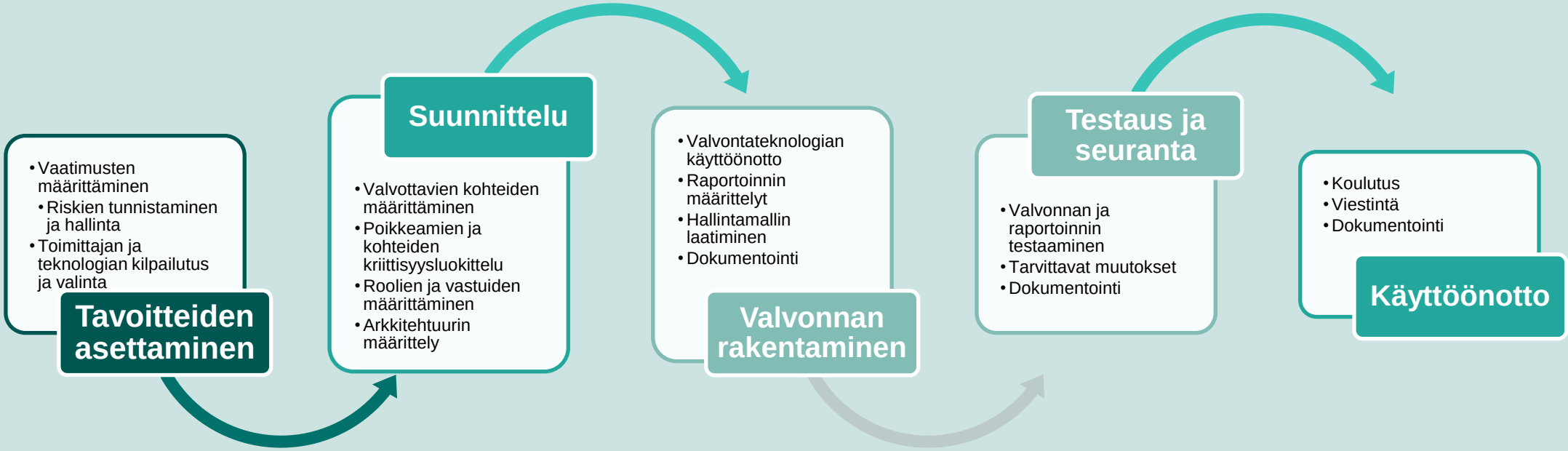
Toimittajan vastuulla	Yhteisesti vastuutettu	Asiakkaan vastuulla
Valvonta, ▪ poikkeamien tunnistaminen ja arviointi	Toimintaohjeiden ja pelikirjojen laatiminen	Valvottavien kohteiden luokittelu ja tunnistaminen
Reagointi, ▪ poikkeamien rajoittaminen ja ratkaisu	Laajavaikutteisten poikkeamien selvittäminen ja ratkaisu	Palvelun vaatimusten määrittely
Palvelun ylläpito, kehittäminen	Ulkoinen viestintä poikkeamatilanteissa	Sisäinen tiedotus ja viestintä poikkeamatilanteissa
Palvelutason saavuttaminen ja säännöllinen raportointi	Yhteiset kehitys- ja laatupalaverit	Sidosryhmien koordinointi
Teknologian ylläpito ja käyttö		Eri palveluntarjoajien välinen yhteistyö

8 Käyttöönottoprojekti

Mitä tietoturvavalvomon käyttöönottoprojekti pitää sisällään?

Tietoturvavalvomon käyttöönottoprojektin päävaiheet ovat samat kuin missä tahansa muussa ICT-projektissa. Alla on kuvattu esimerkinomaisesti tietoturvavalvomon käyttöönottoprojektin tyypillisiä vaiheita ja sisältöä. Valvottavasta ympäristöstä riippuen käyttöönotossa tulee huomioida myös esimerkiksi IT- ja OT-ympäristöjen valvonnan erityispiirteet.

Tyypillisesti käyttöönottoprojekti kestää 6-12 kuukautta, mutta kesto saattaa vaihdella toteutuksen laajuuden perusteella paljonkin.

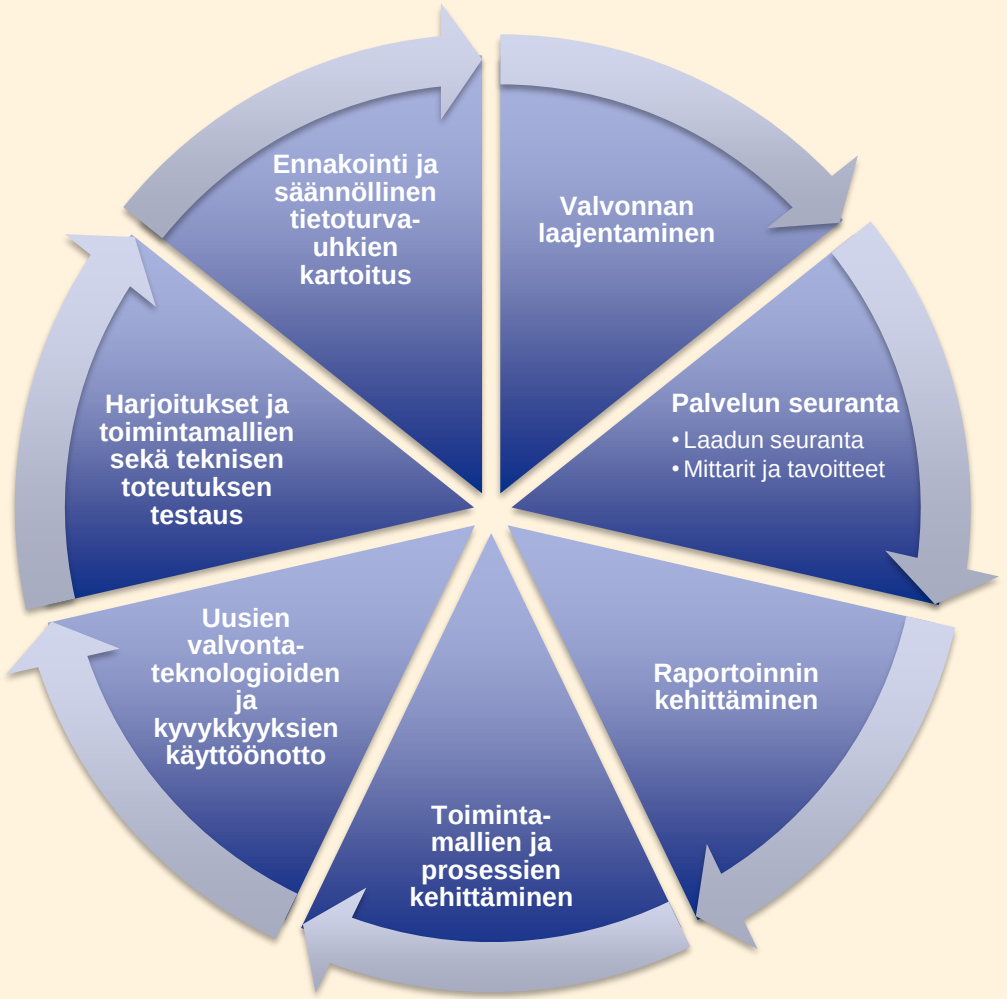


9 Jatkuva kehittäminen

Miten tietoturvavalvomon jatkuva kehittäminen voidaan varmistaa?

Kuten jokainen palvelu, prosessi ja toiminto, myös tietoturvavalvomo vaatii kokemuksiin ja tietoon pohjautuvaa jatkuvaa kehittämistä toimiakseen mahdollisimman tehokkaasti.

Oheisessa kuviossa on esitetty 7 teemaa, jotka tulee huomioida tietoturvavalvomon jatkuvassa kehittämisessä.



Linkit

- Digitaalisen turvallisuuden havainnoinnin kehittäminen (Digi- ja väestötietovirasto, 2023)
- Digitaalisen turvallisuuden arkkitehtuuri (Digi- ja väestötietovirasto, 2022)
- Turvaa digitaalinen toiminta häiriötilanteissa (eOppiva, 2020)
- Tietoturvapoikkeamatilanteiden hallinta (VAHTI, 2017)
- Kyberturvallisuuskeskuksen tilannekuvatuotteet (Liikenne- ja viestintävirasto Traficom)
- Euroopan Unionin kyberturvallisuusvirasto ENISA:n tilannekuvaraportit (ENISA)
- MITRE ATT&CK –viitekehys (MITRE)
- Kriittisten kohteiden luokittelu (VAHTI, 2022)

DIGI- JA VÄESTÖTIETOVIRASTO

dvv.fi