

Uhkamallinnustyöpajan fasilitointiohje

Tämän ohjeen tarkoitus on auttaa sinua suunnittelemaan ja valmistelemaan ohjelmiston uhkamallinnustyöpajan. Ohje kokoaa yhteen keskeiset asiat, jotka fasilitaattorin kannattaa huomioida ennen työpajaa, sen aikana ja työpajan jälkeen.

Uhkamallinnus on yhteinen keskustelu, jossa tunnistetaan, mitä järjestelmässä voi mennä pieleen ja mitä asialle voidaan tehdä riskin pienentämiseksi. Parhaat tulokset syntyvät eri roolien ja näkökulmien yhteistyönä.

Varsinaisen työpajan läpivientiin käytetään tukena *Ohjelmiston uhkamallinnus – työpajan runko* -esitystä, joka sisältää työpajan vaiheet, fasilitointiohjeet, apukysymykset ja käytännön vinkit.

Uhkamallinnuksen tueksi on saatavilla myös erilisiä ohjeita, tukimateriaaleja ja täytettäviä pohjia. Niitä voi hyödyntää esimerkiksi ohjelmiston kontekstin kuvaamisessa, uhkien tunnistamisessa, riskien arvioinnissa sekä tulosten kirjaamisessa ja ylläpidossa.

Uhkamallinnus ei ole vaikeaa. Tavoitteena ei ole täydellinen analyysi, vaan riittävän hyvä yhteinen ymmärrys keskeisistä uhkista, riskeistä ja tarvittavista toimenpiteistä. Kun tämä toteutuu, työpaja on onnistunut.

Työpajan suunnittelu ja ennen työpajaa

Onnistunut uhkamallinnustyöpaja tehdään käytännössä ennen kuin työpaja edes alkaa. Hyvä valmistelu varmistaa, että työpajassa voidaan keskittyä olennaiseen eli uhkien tunnistamiseen, eikä aikaa kulu perusasioiden selvittelyyn.

Työpajalle on hyvä varata aikaa noin 2–3 tuntia. Tätä pidemmät sessiot harvoin säilyvät tehokkaina, koska osallistujien keskittyminen heikkenee. Usein parempi ratkaisu on jakaa kokonaisuus kahteen selkeästi rajattuun työpajaan yhden liian laajan sijaan. Käsittele esim. eri kokonaisuuksia erikseen (1. konteksti ja tietovirrat, 2. uhkamallinnus, 3. riskianalyysi ja toimenpiteet)

Kokonaisuus kannattaa myös jäsentää selkeisiin osiin ja käsitellä ne tarvittaessa erillisissä työpajoissa, esimerkiksi:

1. konteksti ja tietovirrat
2. uhkamallinnus
3. riskianalyysi ja toimenpiteet

Suunnittelun tukena voi hyödyntää esimerkiksi 7P-mallia, joka auttaa varmistamaan, että työpajan tavoitteet, osallistujat ja käytännön toteutus on mietitty etukäteen. Jokainen työpaja on hyvä suunnitella erikseen oman tavoitteensa mukaisesti. Lisäksi on tärkeää sopia, mitä työpajojen välillä tehdään, kuten työpajassa syntyneen materiaalin läpikäynti ja selkeyttäminen ennen seuraavaa vaihetta.

Näin onnistut käytännössä

- Älä aliarvioi valmistelua – se ratkaisee työpajan laadun
- Pidä tavoite konkreettisena ja rajattuna
- Varmista, että oikeat ihmiset ovat mukana
- Kerää vähintään perusmateriaalit etukäteen
- Suunnittele aikataulu realistisesti

Kun nämä ovat kunnossa, itse työpajan vetäminen on huomattavasti helpompaa.

7P malli työpajan suunnitteluun

Käy nämä kohdat läpi ennen työpajaa. Tavoitteenä on varmistaa, että työpaja pysyy fokuksitena ja tuottaa konkreettisia tuloksia. Käytä apuna dokumenttia *7P pohja työpajan suunnitteluun*.

1. Purpose – miksi työpaja järjestetään

Määrittele selkeä tavoite:

- Onko kyse uuden ohjelmiston uhkamallinnuksesta vai olemassa olevan päivityksestä
- Haetaanko laajaa kuvaa vai keskitytäänkö tiettyyn riskiin

Rajaa mitä tehdään ja mitä ei tehdä. Ilman rajausta keskustelu leviää helposti.

Hyvä tavoite on konkreettinen:

- "Tunnistetaan ohjelmiston X keskeiset tietoturvat ja sovitaan toimenpiteet"
- "Arvioidaan uuden integraation riskit ennen käyttöönottoa"

Lopputulos: kaikilla yhteinen ymmärrys tavoitteesta

2. Product – mitä työpajasta syntyy

Määrittele työpajan konkreettinen lopputulos:

- Syntykö lista tunnistetuista uhista tai riskeistä
- Arvioidaanko ja priorisoidaanko tunnistetut riskit
- Sovitaanko toimenpiteistä, vastuista ja jatkosta

Lopputuloksen tulee vastata suoraan tavoitteeseen.

Esimerkki:

- "Kattava lista tunnistetuista uhista."
- "Lista arvioiduista ja priorisoiduista riskeistä."

Määrittele myös, mihin ja missä muodossa tuotokset kirjataan, jotta ne eivät jää vain keskusteluksi.

Lopputulos: kaikilla yhteinen ymmärrys siitä, mitä työpajan päättyessä tulee olla valmiina.

3. Participants – ketkä osallistuvat

Kutsu mukaan oikeat ihmiset.

Tarvitset yleensä:

- tekninen ymmärrys (kehittäjä / arkkitehti)
- liiketoiminnan näkökulma

- tarvittaessa tietoturva-asiantuntija

Vältä liian suurta ryhmää. 4–6 henkilöä toimii hyvin.

Hyvä käytäntö:

- varmista että joku tuntee järjestelmän oikeasti
- varmista että joku ymmärtää vaikutukset liike-toimintaan

Lopputulos: ryhmä, joka pystyy tunnistamaan uhkia ja tekemään päätöksiä

4. Process – miten työpaja etenee

Suunnittele karkea eteneminen ja aikataulutus etukäteen. Voit käyttää apuna dokumenttia *Ohjelmiston uhkamallinnus – työpajan runko*.

Koko uhkamallinnus yhdessä työpajassa:

Sopii tilanteisiin, joissa:

- kohde on rajattu
- osallistujat tuntevat järjestelmän hyvin
- aikaa on riittävästi (esim. 3–4 h)

Eteneminen:

1. aloitus ja tavoite
2. ohjelmiston rakenne ja toiminta
3. uhkien tunnistus
4. riskien arviointi
5. toimenpiteiden määrittely
6. yhteenveto

Lopputulos:

- lista tunnistetuista uhista
- arvioidut riskit
- sovitut toimenpiteet

Uhkamallinnus useassa työpajassa:

Sopii tilanteisiin, joissa:

- järjestelmä on laaja tai monimutkainen
- osallistujia on useita rooleja
- halutaan parempi laatu ilman kiirettä

Työpajan 1 eteneminen:

1. aloitus ja tavoite
2. raja-
aus (scope)
3. ohjelmiston konteksti
4. tietovirrat
5. keskeiset komponentit / rajapinnat
6. uhkien tunnistus
7. lyhyt yhteenveto

Lopputulos:

- Yhteinen ymmärrys ohjelmiston rakenteesta ja toiminnasta
- lista tunnistetuista uhista (ilman riskiluokitusta)

Seuraavat työpajat:

- työpaja 2: riskien arviointi
- työpaja 3: toimenpiteiden määrittely ja priorisointi

5. Preparation – mitä pitää valmistella etukäteen

Tämä on yksi tärkeimmistä vaiheista. Hyvä valmistelu säästää aikaa ja helpottaa työpajan fasilitointia merkittävästi. Voit käyttää apuna dokumenttia *Ohjelmiston kontekstikuvaus*.

Kerää valmiiksi keskeinen taustatieto:

- arkkitehtuurikuva tai karkea hahmotelma
- keskeiset integraatiot
- käsiteltävä data (esim. henkilötiedot)
- mahdollinen aiempi uhkamalli

Selvitä myös:

- onko erityisiä vaatimuksia (sopimus, regulatio, tietosuojat)
- onko tiedossa aiempia tietoturvapoikkeamia

Jos tietoa ei ole:

- varaa työpajaan aikaa sen rakentamiseen
- älä oleta, että kaikki tiedetään valmiiksi

Valmistele osallistujat kevyesti:

- lähetä tavoite ja raja-
aus
- kerro mitä heiltä odotetaan

Esimerkki:

- "Tunnistetaan järjestelmän X keskeiset uhkat. Varaudu kuvaamaan oman alueesi toiminta ja riskit."

Lopputulos: riittävä lähtötieto ja osallistujat valmiina työpajaan.

6. Practical concerns – käytännön järjestelyt

Huolehdi perusasiat kuntoon etukäteen. Mieti työtavat sen mukaan, ovatko osallistujat paikalla vai etänä.

Varmista:

- tarvittavat tilat tai etäyhteydet
- kaikilla pääsy materiaaleihin
- työkalut (sähköiset tai esim. valkotaulut, tussit)
- käytettävät pohjat ovat valmiina

Suunnittele ajankäyttö:

- realistinen kesto
- tarvittaessa tauko
- aikaa lopun yhteenvedolle

Sovi kirjaamisesta:

- kuka kirjaa
- minne kirjataan

Hyvä käytäntö:

- avaa materiaalit valmiiksi ennen aloitusta
- testaa etäyhteys etukäteen

Lopputulos: työpaja etenee sujuvasti ilman turhaa säätöä

7. Pitfalls – mitä voi mennä pieleen

Tunnista yleisimmät ongelmat etukäteen.

Yleisiä haasteita:

- keskustelu lähtee rönstyilemään
- mennään liian syvälle teknisiin yksityiskohtiin

Varaudu haasteisiin:

- palaa tavoitteeseen, jos keskustelu karkaa
- rajaa tarvittaessa: "ei käsitellä tätä nyt"

Lopputulos: työpaja pysyy fokuksituna ja tuottaa tuloksia.

Työpajan vaiheet (tiivistetty)

Työpaja etenee selkeissä vaiheissa. Tarkoituksena ei ole tehdä täydellistä analyysiä, vaan tunnistaa keskeiset uhkat, arvioida niiden merkitys ja sopia tarvittavista toimenpiteistä. Voit käyttää dokumenttia *Ohjelmiston uhkamallinnus – työpajan runko* apuna työpajan läpijuoksuttamiseen.

1. Aloitus ja raja

Määritellään mitä tarkastellaan ja mikä on työpajan tavoite.

Lopputulos: yhteinen ymmärrys tavoitteesta ja rajauksesta.

2. Kontekstin läpikäynti

Käydään läpi järjestelmän rakenne, keskeiset komponentit ja tietovirrat.

Lopputulos: yhteinen kuva siitä, miten järjestelmä toimii.

3. Suojattavien asioiden tunnistaminen

Tunnistetaan, mikä järjestelmässä on arvokasta ja mitä pitää suojata.

Lopputulos: lista keskeisistä suojattavista asioista.

4. Uhkien tunnistaminen

Tunnistetaan, mitä järjestelmässä voi mennä pieleen eri näkökulmista.

Lopputulos: lista tunnistetuista uhkista.

5. Riskien arviointi

Arvioidaan uhkien todennäköisyys ja vaikutus, ja tunnistetaan tärkeimmät riskit.

Lopputulos: priorisoitu lista riskeistä.

6. Toimenpiteiden määrittely

Määritellään, miten merkittävimpiä riskejä pienennetään.

Lopputulos: lista konkreettisista toimenpiteistä.

7. Yhteenveto ja seuraavat askeleet

Kootaan keskeiset havainnot ja sovitaan jatkosta.

Lopputulos: selkeä käsitys siitä, mitä tehdään seuraavaksi.

Työpajan jälkeen

Työpaja tuottaa arvoa vasta, kun tulokset selkeytetään ja viedään käytäntöön. Tämä vaihe varmistaa, että tunnistetut riskit johtavat konkreettisiin toimenpiteisiin.

1. Selkeytä tulokset (1–2 päivän sisällä)

Siisti uhkat, riskit ja toimenpiteet ymmärrettävään muotoon. Yhdistä päällekkäisyydet ja varmista, että kuvaukset ovat selkeitä myös työpajan ulkopuolisille.

2. Priorisoi ja nimeä vastuut

Valitse tärkeimmät toimenpiteet ja nimeä niille vastuuhenkilöt. Sovi karkea aikataulu etenemiselle.

3. Vie tekemiseen

Liitä toimenpiteet osaksi jokapäiväistä kehitystyötä, esimerkiksi työjonoon tai projektiin. Vältä erillisiä listoja, jotka jäävät helposti seuraamatta.

4. Sovi seuranta ja päivitys

Tarkista toimenpiteiden eteneminen sovitusti. Päivitä uhkamallia, kun järjestelmä muuttuu tai uusia riskejä tunnistetaan.

Lopputulos

- Selkeä dokumentti uhkista, riskeistä ja toimenpiteistä
- Sovitut vastuut ja seuraavat askeleet
- Toimenpiteet osana normaalia tekemistä