

Tietoturvallinen ohjelmistokehitys (2 pv)

Kysymys tietoturvallisuudesta ohjelmistokehityksessä on alati muuttuvassa toimintaympäristösämme yhä keskeisempi.

Tässä koulutuksessa opit tietoturvallisen ohjelmistokehityksen periaatteet ja käytännöt tunnettujen viitekehysten avulla, saat ohjeita niiden jalkauttamiseksi omaan organisaatioosi sekä tutustut tietoturvallisen ohjelmistokehityksen haasteisiin ja mahdollisuuksiin. Opit myös tunnistamaan tietoturvan luoman lisäarvon erikokoisissa ja -tyyppisissä ohjelmistokehitysprojekteissa. Koulutus sisältää oppimistasi edistäviä harjoituksia.

Koulutuksen keskiössä on tietoturvallisuuden integroiminen osaksi yrityskulttuuria ja ohjelmistokehitystä hyvien käytänteiden mukaisesti. Käymme läpi hallinnollisen tietoturvallisuuden perusteet ja vaatimusmäärittelyn ohjelmistokehityksen suunnannäyttäjänä. Koulutuksessa käydään läpi turvallisen ohjelmistokehityksen elinkaarimallin (secure development lifecycle, SDL) kaikki vaiheet ja syvennytään niiden tärkeimpiin aktiviteetteihin. Tutustumme erilaisiin työkaluihin ja prosesseihin, jotka tukevat turvallisuuteen liittyvien aktiviteettien toteuttamista.

Tule mukaan oppimaan ohjelmistoturvallisuuden tilannekuvasta ja tietoturvaosaamisen lisäämisestä sovelluskehityksen näkökulmasta! Käymme läpi myös erilaiset SDL-viitekehykset (Microsoft SDL, OWASP SAMM, NIST SP 800-218, BSIMM), sekä niiden heikkoudet ja vahvuudet.

Päivä 1

Tietoturvan ja kyberturvallisuuden perusteet

- Tietoturvan perusteet
- Kyberturvallisuuden erilaiset toimijat
- Kyberturvallisuuden nykytila

Ohjelmistoturvallisuuden perusteet

- Yleiset ohjelmistoturvallisuuden uhat
- Turvallisen ohjelmistokehityksen elinkaarimalli (SDL)
- Ohjelmistoturvallisuuden kypsyys

Hallinnollinen tietoturva ja tavoitteet

- Riskienhallinta
- Tietoturva-vaatimukset
- Tietoturvaosaamisen kehittäminen

Uhkamallinnus

- Uhkamallinnuksen tavoitteet
- Uhkamallinnus osana riskienhallintaa ja vaatimusmäärittelyä
- Uhkamallinnusharjoitus

Päivä 2

Turvallinen ympäristö

- Verkkoturvallisuus
- Turvalliset asetukset
- Turvalliset kehitysympäristöt

Tietoturvallinen suunnittelu

- Turvallisen suunnittelun periaatteet
- Monitasoinen suojaus
- Hyökkäyspinta-alan minimointi

Tietoturvallinen ohjelmointi

- Turvallisen ohjelmoinnin periaatteet
- Turvallisen ohjelmoinnin työkalut
- Kolmannen osapuolen komponentit

Tietoturvatestaus

- Tietoturvatestaamisen tavoitteet
- Tietoturvatestauksen työkalut
- Tietoturvatestauksen eri tyypit

Poikkeamanhallinta

- Poikkeamanhallinta
- Haavoittuvuuksienhallinta

Kurssin tavoitteet

Koulutuksen jälkeen osallistuja:

- tietää miten erilaiset viitekehykset näkevät tietoturvallisen ohjelmistokehityksen
- ymmärtää miksi ja miten tietoturva integroidaan osaksi yrityksen kulttuuria ja ohjelmistokehitysprosesseja
- osaa huomioida eri kokoisten ja erilaisten ohjelmistokehitysprojektien tietoturvatarpeet
- tietää millaisia tietoturvavaatimuksia ohjelmistokehityksessä on huomioitava tulevaisuudessa

Kohderyhmä

Koulutus on suunnattu ohjelmistokehityksestä vastaaville henkilöille, kuten tuotepäälliköille, arkitehdeille, projektipäälliköille ja tiiminvetäjille. Koulutus sopii myös erinomaisesti ohjelmistokehittäjille. Koulutuksesta on myös hyötyä jo tietoturvan parissa työskenteleville henkilöille, jotka haluavat syventää osaamistaan ohjelmistoturvallisuuden parissa.

Esitiedot

Koulutukselle ei ole tiukkoja esitietovaatimuksia. Kuitenkin tietoturvallisuuden perusteiden ja ohjelmistokehitysprosessien perusasioiden ymmärtäminen auttaa osallistujia saamaan parhaan mahdollisen hyödyn koulutuksesta.