

Secure Software Development Lifecycle

Cursusduur: 3 Dagen Cursuscode: SSDLC

Beschrijving:

Global Knowledge is enthousiast om u een opleidingsprogramma aan te bieden dat gaat helpen het belang van informatiebeveiliging binnen softwareontwikkeling te leren begrijpen. Het programma helpt deelnemers basiskennis van informatiebeveiliging op te doen en vergroot het inzicht in het veilig ontwikkelen van software op basis van de Secure Software Development Life Cycle (SSDLC). Het maakt duidelijk wat er van elk teamlid verwacht wordt in elke fase van de SSDLC en brengt in kaart welke producten en processen ontwikkeld of verder uitgewerkt moeten worden, alsmede wie hier een bijdrage kan leveren.

Het vertrekpunt is een casus van een te ontwikkelen applicatie. Gedurende drie dagen zal deze casus gezamenlijk behandeld worden waarbij theorie met opdrachten afgewisseld worden.

De basis voor iedere groepssessie is in principe steeds gelijk. Daarnaast zal voor iedere groep op basis van het functieprofiel van de groep een deel maatwerk worden geleverd.

Doelgroep:

De training wordt verplicht voor een breed scala aan functies binnen de ontwikkelteams, waaronder: Projectmanagers (IV/IT) Product owners (IV) Scrum masters (IT) Business analisten (IV) Solution architecten (IT) Junior, Medior, Senior ontwikkelaars (IT) Testers (IT) Applicatiebeheerders (IT) Security officers (IV)

Doelstelling:

- | | |
|--|---|
| ■ Inhoudelijke wensen ten aanzien van de training: | ■ Inzicht vergroten in het veilig ontwikkelen van software op basis van de Secure Software Development Life Cycle (SSDLC). |
| ■ Belang van informatiebeveiliging begrijpen binnen softwareontwikkeling | ■ Helder krijgen wat er van elke teamlid verwacht wordt in elke fase van de SSDLC |
| ■ Basiskennis opdoen van informatiebeveiliging. | ■ In kaart brengen van welke producten en/of processen ontwikkeld en/of verder uitgewerkt moeten worden en wie hier een bijdrage kan leveren. |
-

Cursusinhoud:

Belang informatiebeveiliging

- Voorbeeld aanval
- Meest voorkomende kwetsbaarheden in software (bijvoorbeeld OWASP-top 10)
- Belang security door gehele software life-cycle (link naar BIO2 en NIS2)

Uitleg van de meest belangrijke termen en concepten in informatiebeveiliging, zoals:

- CIA
- Defense-in-Depth ; Breadth
- Identity ; Access Management
- Security principes zoals Least Privilege, Fail-Safe Defaults, Complete Mediation, Least Common Mechanism, Economy of Mechanism, Zero Trust
- Security en Privacy by Design
- OWASP secure code practices

SSDLC

- Fasen (Training, Requirements, Design, Implementation, Verification, Release, Response)

Mogelijk toepassen/inbedden van de SSDLC in een Agile/Scrum proces:

- Security user stories
- Risico analyse / Threat Modeling
- Het zichtbaar maken van een definition of done (DoD) voor security eisen
- Het omgaan met geautomatiseerde security checks
- Belang van hardening sprints
- Belang penetratie testen bij oplevering MVPs

Optionele onderwerpen:

- Belang van Architectural Runway om compliance en securityactiviteiten mee te plannen

De rol van Security Champion binnen het team

- Daar waar mogelijk aangeven welke hulpmiddelen zoals templates, checklists, etc. binnen de organisatie beschikbaar zijn.

Doel van de opdrachten is om ervaring op te doen met het doorlopen van de SSDLC en daarbij verbeteringen te identificeren. Zo zullen de volgende opdrachten uitgevoerd gaan worden:

- Verzamelen mogelijke stories en security user stories;

Op basis van de user stories en security user stories:

- Opstellen van een high-level ontwerp, om zo een beter beeld te krijgen van de samenhang van diverse componenten;

Uitvoeren van risicoanalyse die ondersteund wordt door een dreigingsanalyse op basis van de Microsoft STRIDE threat modeling methode op het eerder gemaakte high-level ontwerp;

- Bepalen van beveiligingsmaatregelen op basis van uitkomsten de risicoanalyse en deze vertalen naar aanvullende security user stories;
- Bepalen welke criteria er in de Definition of Done (DoD) moet worden opgenomen (denk aan: documentatie voor beheer en SOC-team, uitvoeren bepaalde testen, vastleggen van gevonden kwetsbaarheden, uitvoeren van bepaalde security testen, etc.)

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein