CYBERSÉCURITÉ NIVEAU APPROFONDISSEMENT – Comprendre les vulnérabilités et protéger son application web

Durée
1 jour

L'intrusion sur les serveurs de l'entreprise représente un risque majeur.
Cette formation dresse un panorama concret des menaces du web. Elle détaille aussi bien les types d'attaques que peut subir une application que les failles les plus courantes des configurations serveurs ou des applications déployées.

Le cours se concentre également sur les technologies et méthodologies permettant de protéger son code, ainsi que sur les outils permettant de contrôler la sécurité des applications.

La formation s'attache enfin à vous communiquer les « bonnes pratiques » liées au développement sécurisé d'applications.

La formation se base sur des retours d'expérience, acquis à travers nos projets de développement et déploiement d'applications Web.
Elle se déroule en suivant un fil rouge et intègre des exercices pratiques et des labs.

Objectifs pédagogiques

A la fin de la formation, vous serez en mesure de :
- Présenter Identifier les principales attaques web OWASP
- Adopter les bonnes pratiques de sécurité
- Protéger son code
- Implémenter la sécurité d'un site web sur Azure

Programme

Matin :

Chapitre 1 – « Comprendre les menaces auxquelles sont confrontées les entreprises »
- Quizz introductif : pour évaluer les connaissances générales sur la Sécurité (format Kahoot)
- Qu'est-ce-que la donnée ?
- Quels sont les profils des hackers ?
- Que recherchent les hackers ?
- Quels sont les différents types d'attaque les plus fréquents ?

Chapitre 2 – « Comprendre et protéger son code contre les vulnérabilités décrites dans l'OWASP »
- Présentation des risques liés à des vulnérabilités OWASP (Labs/pptx)
- Comment protéger son code ? (Labs/pptx)
- Quelles sont les autres bonnes pratiques ? (pptx)

Après-midi :

Chapitre 3 – « L'automatisation de la détection des problèmes de sécurité »
- Présentation des bonnes pratiques de CI/CD (pptx)
  - Pre commit Hook / Sast / Dast / SCA / Vault / Signature des assemblys / Containeur / Pentest

Chapitre 4 – « Application de la sécurité au niveau infrastructure »
- Bonnes pratiques réseau (Labs)
  - Vnet, private Endpoint, bastion
- Contrôle flux et d'exécution (Labs)
  - Azure policy, application gateway
- Détection intrusion (pptx)
  - Log, sentinel

La formation se base sur des retours d'expérience, acquis à travers nos projets de développement et déploiement d'applications Web.
Elle se déroule en suivant un fil rouge et intègre des exercices pratiques et des labs.

Public cible

Public devant avoir une expérience en programmation, idéalement en développement web

Prérequis

Un ordinateur portable avec une bonne connexion, un éditeur de code pouvant compiler du .Net

Niveau

Avancé

Evaluation

Quiz

Modalités d'apprentissage

Stage pratique en présentiel, classe pratique à distance

Mode de délivrance

Intra et inter

Moyens

Slides
Labs

Certification associée

N/A

Session délivrée en

Français et Anglais

Langue(s) des supports

Anglais

Tarifs

Inter-entreprise : 1 100 €HT par participant
Intra-entreprise : sur demande