Date de publication : 24/07/2024

Formation : DevSecOps, état de l'art et bonnes pratiques

comment franchir un nouveau palier dans la qualité de votre développement

Séminaire - 1j - 07h - Réf. DSF

Prix : 1100 CHF H.T.

DevOps multiplie les déploiements du code, souvent décomposé en microservices containerisés dans différents clouds. Rechercher l'origine d'une faille de sécurité dans cette multiplicité de "boîtes blanches" changeantes relève de la gageure. DevSecOps consiste à tenir compte de la sécurité le plus tôt possible.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Comprendre le cycle de développement DevSecOps dans le cadre d'architectures à base de conteneurs déployés on cloud
- Connaître les types de test et les outils associés que l'on peut intégrer dans un cycle DevSecOps
- Être capable de planifier le passage d'une organisation DevOps à une organisation DevSecOps

Public concerné

Responsables RH, DSI, RSSI, responsables sécurité, chefs de projets, consultants, administrateurs.

Prérequis

Connaissances de base sur le cycle de développement DevOps.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

PARTICIPANTS

Responsables RH, DSI, RSSI, responsables sécurité, chefs de projets, consultants, administrateurs.

PRÉREQUIS

Connaissances de base sur le cycle de développement DevOps.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

1 Qu'est-ce que DevSecOps ?

- Le cycle de développement DevOps. Les différents environnements (développement, test, production).
- DevOps avec prise en compte de la sécurité en fin de cycle de développement.
- Faire glisser les tests de sécurité vers la gauche.
- Le cycle de développement DevSecOps.

2 DevSecOps et les architectures distribuées à base de conteneurs

- Principes des conteneurs. Leur intérêt dans le cadre du déploiement continu.
- La souplesse d'utilisation des conteneurs. Avantages et inconvénients du point de vue de la sécurité.
- Intégrer l'analyse de code dans le pipeline de développement. Tester la sécurité d'un conteneur.
- Tester la sécurité de l'environnement de production. Outils d'analyse de logs, SIEM. Feedback vers les développeurs.

3 Les défis réels de la prise en compte de la sécurité

- Le fossé des compétences. Les membres de l'équipe DevOps ne sont pas des experts en sécurité.
- L'équipe sécurité est séparée de l'équipe DevOps.
- Utiliser correctement les fonctionnalités de sécurité proposées par le fournisseur.
- Les conteneurs et microservices transitoires sont difficiles à surveiller. La plateforme de sécurité Aqua.
- Risques de déploiement dans le cloud. Configuration des ressources.
- Les applications legacy et leur prise en compte dans le cycle de développement.

4 Bonnes pratiques pour un passage à DevSecOps

- Gérer le changement. Rôles concernés, enjeux organisationnels, plan de formation, plan d'action.
- Tenir compte des bonnes pratiques de sécurité cloud. Les référentiels de la CSA. Les risques selon l'ENISA.
- Évaluer la sécurité de vos fournisseurs cloud. Tenir compte des SLA sécurité de votre fournisseur.
- Intégrer des verrouillages de sécurité rendant impossible le déploiement d'un environnement non sécurisé.
- Pousser l'automatisation jusqu'à l'Infrastructure as code (IaC). Intégrer les équipes système et sécurité.
- Automatiser la surveillance continue.
- Intégrer la veille des annonces de vulnérabilités (notamment pour les logiciels open source).

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.