Cybersecurity Specialization: DevSecOps

Durée: 3 Jours **Réf de cours: GK840102** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

Apprenez à intégrer la sécurité dans DevOps

Cette formation de 3 jours est conçue pour vous donner les connaissances et les compétences nécessaires pour intégrer la sécurité dans votre pipeline DevOps.

Vous comprendrez en profondeur les principes et pratiques de DevSecOps, garantissant que la sécurité fait partie intégrante de votre cycle de vie de développement logiciel (SDLC). En maîtrisant les méthodes et outils de tests de sécurité continus, vous serez en mesure d'identifier et de résoudre tôt les vulnérabilités, améliorant ainsi la sécurité globale de vos applications.

Vous acquérerez les connaissances et les outils pour assurer une sécurité et une conformité continues, protégeant vos solutions logicielles contre les menaces potentielles.

Nos cours de spécialisation en cybersécurité suivent les 9 piliers de la cybersécurité, fournissant les compétences clés nécessaires pour réussir en tant que professionnel de la cybersécurité.

Mise à jour : 10/12/2024

Public visé:

Ce cours de niveau intermédiaire à avancé est conçu pour :
° les professionnels de l'informatique,
° les développeurs de logiciels,
° les ingénieurs en sécurité,
° les praticiens DevOps et les administrateurs système qui ont de l'expérience avec DevOps et souhaitent intégrer la sécurité dans leurs processus de développement et d'exploitation.

Ce cours est idéal pour ceux qui cherchent à améliorer leurs compétences en pratiques de codage sécurisé, en modélisation des menaces, en tests de sécurité continus et en mise en œuvre de la sécurité dans les pipelines CI/CD.

Les participants doivent avoir une compréhension de base des principes DevOps et des concepts de sécurité fondamentaux.

Objectifs pédagogiques:

- Comprendre les principes et pratiques de DevSecOps pour intégrer la sécurité dans le pipeline DevOps
- Maîtriser les techniques du cycle de vie de développement logiciel sécurisé (SDLC)
- Connaître les méthodes et outils de tests de sécurité continus pour identifier tôt les vulnérabilités
- Améliorer les pratiques de codage sécurisé en comprenant les vulnérabilités courantes et comment les atténuer
- Comprendre les sttratégies avancées de modélisation des menaces et d'évaluation des risques
- Mettre en œuvre les meilleures pratiques pour la sécurité des conteneurs en utilisant des outils d'orchestration de conteneurs
- Exploiter la sécurité de l'Infrastructure as Code (IaC) pour sécuriser l'infrastructure dès le départ
- Utiliser les outils de gestion des informations et des événements de sécurité (SIEM) pour l'analyse en temps réel des alertes de sécurité
- Développer des stratégies pour une réponse aux incidents efficace et la criminalistique numérique
- Comprendre les exigences de conformité et de réglementation
- Améliorations des chaînes d'outils DevOps sécurisées
- Intégrer les services de sécurité spécifiques au cloud fournis par les principaux fournisseurs de cloud pour protéger les applications et l'infrastructure basées sur le cloud
- Interagir avec les outils de sécurité réseau pour protéger les communications réseau
- Concevoir des scripts professionnels pour automatiser les tâches de sécurité et améliorer l'efficacité
- Interroger les bases de données en toute sécurité, en garantissant

- Maîtriser les principes de gestion des identités et des accès (IAM) pour gérer les identités et les permissions des utilisateurs en toute sécurité
- Acquérir une expérience pratique avec les outils de test de sécurité des applications (AST) pour découvrir et remédier aux failles de sécurité
- l'intégrité des données et la protection contre les vulnérabilités liées aux bases de données
- Traiter et protéger les données sensibles en utilisant des mesures de sécurité pour assurer la conformité aux lois et aux meilleures pratiques en matière de protection des données

Pré-requis:

Pour assister à cette formation, il est recommandé pour les candidats de:

- **Connaissances de base en DevOps :** Les participants doivent avoir une compréhension de base des principes et des pratiques DevOps.
- **Concepts de sécurité de base :** Etre familié avec les concepts fondamentaux de la cybersécurité est requis.
- **Expérience avec les pipelines CI/CD :** Une expérience préalable dans la configuration et l'utilisation des pipelines d'intégration continue et de déploiement continu (CI/CD) est nécessaire.
- **Connaissances en scripting :** Expérience dans l'écriture de scripts dans des langages tels que Python, Bash ou PowerShell.
- **Maîtrise des systèmes d'exploitation :** Une connaissance pratique des systèmes Unix/Linux, Mac ou Windows au niveau utilisateur

Suivre la formation https://www.globalknowledge.com/fr-fr/formation/security/cybersecurity_foundation_and_awareness/9701 est recommandé

Afin de vous assurer que vous possédez toutes les connaissances requises pour participer à la formation, notre équipe commerciale vous proposera un QCM.

- 9701 - Cybersecurity Foundations

Contenu:

Jour 1

Aperçu de DevSecOps

- Principes de DevSecOps
- Le cycle de vie DevOps et l'intégration de la sécurité
- Principaux défis de la mise en œuvre de DevSecOps

Sécurité par conception

- Cycle de vie de développement logiciel sécurisé (SSDLC)
- Modélisation des menaces et évaluation des risques
- Meilleures pratiques pour un codage sécurisé
- Ressources : OWASP Top Ten, NIST Cybersecurity Framework

Sécurité de l'infrastructure en tant que code (IaC)

- Introduction à IaC et ses avantages
- Considérations de sécurité pour IaC
- Outils à utiliser : Terraform, Azure Resource Manager (ARM)

Ressources à utiliser : Terraform : HashiCorp Terraform, Azure ARM : Documentation Azure

Jour 2

Intégration continue et sécurité continue

- Conception de pipeline CI/CD sécurisé
- Mise en œuvre de Zero Trust dans les pipelines CI/CD
- Réponse aux incidents et récupération dans les pipelines CI/CD
- Intégration des outils de sécurité dans les pipelines CI/CD
- Mise en œuvre de portes de sécurité dans les pipelines CI/CD
- Outils à couvrir : Jenkins, GitHub Actions, Azure DevOps
- Ressources à utiliser : Jenkins : Documentation Jenkins, GitHub Actions : GitHub Actions

Tests de sécurité des applications

- Tests de sécurité des applications statiques (SAST)
- Tests de sécurité des applications dynamiques (DAST)
- Outils : SonarQube, OWASP ZAP, autres outils SAST (Checkmarx, Veracode), autres outils DAST (Burp Suite, Acunetix)
- Ressources : SonarQube : Documentation SonarQube, OWASP ZAP : Documentation OWASP ZAP

Sécurité des conteneurs

- Sécurisation des images et des conteneurs Docker
- Meilleures pratiques pour la sécurité des conteneurs
- Outils : Docker, Aqua Security, Kubernetes Security
- Ressources : Docker : Documentation Docker, Trivy : Documentation Aqua Trivy

Surveillance et journalisation

- Importance de la surveillance et de la journalisation en matière de sécurité
- Outils pour la surveillance et la journalisation : ELK Stack, Prometheus, Grafana, SIEM (Security Information and Event Management), Grafana pour la visualisation des métriques de sécurité
- Ressources : ELK Stack : Documentation Elastic, Prometheus : Prometheus

Jour 3

Réponse aux incidents et Forensic

- Planification et exécution de la réponse aux incidents
- Forensic et revue post-incident
- Outils : Splunk, Wireshark, SOAR (Security Orchestration, Automation, and Response), Volatility
- Ressources : Splunk : Documentation Splunk, Wireshark : Documentation Wireshark

Conformité et gouvernance

- Comprendre les exigences de conformité en matière de sécurité
- Mise en œuvre des politiques de sécurité et de gouvernance
- Normes : GDPR, HIPAA, PCI-DSS, CCPA (California Consumer Privacy Act)
- Ressources : GDPR : Informations sur le GDPR de l'UE, HIPAA : Journal HIPAA, PCI-DSS : Conseil des normes de sécurité PCI

Sécurité et confidentialité des données

- Protection des données sensibles
- Techniques de chiffrement et gestion des clés
- Outils : Vault par HashiCorp, Azure Key Vault, Google Cloud Key Management Service (KMS), AWS Key Management Service (KMS)
- Ressources : Vault : Documentation HashiCorp Vault, Azure Key Vault : Azure

Projet de fin de formation

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.

Un support de cours électronique sera remis aux participants.

Pour profiter pleinement du support électronique dès le 1er jour, nous invitons les participants à se munir d'un PC ou d'une tablette, qu'ils pourront connecter en WiFi dans nos locaux de Rueil, Lyon ou nos agences en régions.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement