

# Certification DevSecOps Engineer (ECDE)

## OBJECTIFS

- Comprendre la chaîne d'outils DevSecOps et les contrôles de sécurité dans le pipeline automatisé DevOps.
- Adoptez des pratiques de sécurité telles que la collecte des exigences de sécurité, la modélisation des menaces et la sécurisation des révisions de code dans le flux de travail de développement.
- Découvrez les outils AWS et Azure DevSecOps pour sécuriser les applications.
- Intégrez des outils et des pratiques pour générer des commentaires continus dans le pipeline DevSecOps à l'aide des notifications par e-mail de Jenkins et Microsoft Teams.
- Auditez les poussées, les pipelines et la conformité du code à l'aide de divers outils de journalisation et journaux de surveillance tels que Sumo Logic, Datadog, Splunk, ELK et Nagios.

## Prérequis

Les participants doivent avoir une compréhension des concepts de sécurité

## PROGRAMME

Ce cours EC-Council couvre l'intégration et l'automatisation de tous les outils, processus et méthodologies DevSecOps largement utilisés qui aident les organisations à créer rapidement des applications sécurisées. ECDE forme les étudiants au DevSecOps pour les réseaux basés sur le cloud, notamment Amazon Web Services et Microsoft Azure. Notre programme compte plus de 80 laboratoires de compétences qui enseignent la sécurité et l'intégration d'outils aux huit étapes DevOps.

- **MODULE 01** | Comprendre la culture DevOps
- **MODULE 02** | Introduction à DevSecOps
- **MODULE 03** | Pipeline DevSecOps – Étape de planification
- **MODULE 04** | Pipeline DevSecOps – Étape de code
- **MODULE 05** | Pipeline DevSecOps – étape de création et de test
- **MODULE 06** | Pipeline DevSecOps – étape de publication et de déploiement
- **MODULE 07** | Pipeline DevSecOps : étape d'exploitation et de surveillance