

ECDE – Certified DevSecOps Engineer

EC-Council – E|CDE v2. Hands On.

ECDE - DEVSECOPS ENGINEER

SOBRE O CURSO:

Durante muito tempo a segurança foi a última etapa antes de colocar um sistema em produção, e, por isso mesmo, a mais cara e a mais ignorada. O DevSecOps muda esta lógica: a segurança passa a fazer parte de cada etapa do pipeline, desde o planejamento até a operação. É o famoso "shift left".

A certificação EC-Council Certified DevSecOps Engineer (E|CDE) é um programa prático, com mais de 70% do tempo dedicado a laboratórios, que cobre a segurança de aplicações e de infraestrutura em ambientes on-premises e nas principais nuvens (AWS, Microsoft Azure e Google Cloud), integrando ferramentas de segurança nas oito etapas do ciclo DevOps. A versão 2 incorpora o uso de Inteligência Artificial no pipeline DevSecOps.

O treinamento foi desenvolvido com base no conteúdo oficial do E|CDE, organizado em sete módulos: Cultura DevOps, Introdução ao DevSecOps e as etapas Plan, Code, Build and Test, Release and Deploy, e Operate and Monitor do pipeline DevSecOps.

O Grupo Utah criou este treinamento utilizando uma metodologia onde o aluno não apenas irá adquirir conhecimento técnico, mas também competências comportamentais que irão apoiá-lo em todo o seu processo de desenvolvimento de carreira. A metodologia DILDIP proporciona isso porque é baseada no modelo 70/20/10. É a continuação natural da nossa Carreira DevOps (Administrador Linux, Engenheiro Linux e Engenheiro DevOps).

SOBRE A CERTIFICAÇÃO:

- ✓ **Exame:** EC-Council Certified DevSecOps Engineer (E|CDE) – código 312-97
- ✓ **Formato:** 100 questões de múltipla escolha
- ✓ **Duração:** 4 horas
- ✓ **Aprovação:** 70%
- ✓ **Aplicação:** EC-Council Exam Portal

CARGA HORÁRIA:

- ✓ 40 Horas

APÓS ESTE CURSO VOCÊ ESTARÁ APTO A:

- ✓ Compreender a cultura DevOps e a evolução para o DevSecOps.
- ✓ Integrar segurança em todas as etapas do pipeline: planejar, codificar, construir, testar, liberar, implantar, operar e monitorar.
- ✓ Realizar modelagem de ameaças e definir requisitos de segurança desde o planejamento.
- ✓ Proteger repositórios de código, evitar vazamento de segredos e aplicar práticas de codificação segura.
- ✓ Integrar testes SAST, DAST, IAST e SCA em pipelines de CI/CD.
- ✓ Proteger imagens de contêiner, Kubernetes e infraestrutura como código.
- ✓ Gerenciar segredos com ferramentas como HashiCorp Vault e serviços nativos de nuvem.
- ✓ Aplicar DevSecOps em AWS, Microsoft Azure e Google Cloud.

- ✓ Implementar monitoramento contínuo, logs, alertas e resposta a incidentes.
- ✓ Usar ferramentas de IA para acelerar a detecção e correção de vulnerabilidades.
- ✓ Prestar o exame de certificação EC-Council E|CDE (312-97).

PRÉ-REQUISITOS:

- ✓ Conhecimento em Linux, Serviços e Redes de Computadores.
- ✓ Conhecimento básico de Git, Docker e pipelines de CI/CD.
- ✓ Desejável conhecimento em desenvolvimento de aplicações e segurança de aplicações (por exemplo, C|ASE).

POR QUE A UTAH:

- ✓ Aulas gravadas e disponibilizadas para acesso na central do aluno durante 3 meses após o treinamento.
- ✓ Simulados baseados na prova oficial EC-Council 312-97.
- ✓ Descontos e parcelamentos na prova de certificação.
- ✓ Laboratórios práticos (Hands On) em ambiente real, com cenários do dia a dia corporativo.
- ✓ Aqui você terá o desenvolvimento de uma carreira, não apenas um treinamento.
- ✓ Pioneira em Treinamentos Linux / Software Livre no Brasil, com 26 anos de mercado.
- ✓ Material Didático Impresso.
- ✓ Técnicas de Coaching utilizadas para desenvolvimento de comportamentos (metodologia DILDIP, modelo 70/20/10).
- ✓ Grupos exclusivos no WhatsApp / Telegram para tirar dúvidas.
- ✓ Encaminhamento de Profissionais para empresas parceiras.
- ✓ Certificado Utah reconhecido pelo mercado de trabalho.
- ✓ Possibilidade de reposição de aula presencial.
- ✓ E muito mais.

EMENTA:

EC-COUNCIL CERTIFIED DEVSECOPS ENGINEER – E|CDE (312-97)

- **Módulo 01 – Entendendo a Cultura DevOps.**
  - Introdução ao DevOps: histórico, princípios e benefícios.
  - Cultura DevOps: colaboração entre desenvolvimento e operações, CALMS e as Três Maneiras.
  - Pipeline DevOps e suas etapas: plan, code, build, test, release, deploy, operate e monitor.
  - Ferramentas DevOps: gerenciamento de código-fonte, integração contínua, entrega contínua e gerenciamento de configuração.
  - Integração contínua (CI), entrega contínua e implantação contínua (CD).
  - DevOps em ambientes on-premises e em nuvem.
- **Módulo 02 – Introdução ao DevSecOps.**
  - O que é DevSecOps e por que a segurança deve começar cedo (shift left).

- Desafios de segurança em ambientes DevOps e na cadeia de suprimentos de software.
- Pipeline DevSecOps e a integração de segurança em cada etapa.
- Funções e responsabilidades do Engenheiro DevSecOps.
- Frameworks e boas práticas: OWASP SAMM, OWASP DSOMM, NIST SSDF e BSIMM.
- Ferramentas DevSecOps nativas de nuvem: AWS, Microsoft Azure e Google Cloud.
- Uso de Inteligência Artificial no DevSecOps.

- **Módulo 03 – Pipeline DevSecOps: Etapa Plan.**
  - Requisitos de segurança, histórias de usuário de abuso e critérios de aceitação de segurança.
  - Modelagem de ameaças: STRIDE, DREAD, PASTA e ferramentas (Microsoft Threat Modeling Tool, OWASP Threat Dragon, IriusRisk, ThreatModeler).
  - Integração da modelagem de ameaças com ferramentas de gestão de projetos (Jira, Azure Boards).
  - Comunicação e colaboração entre equipes de segurança, desenvolvimento e operações (Slack, Microsoft Teams).
  - Treinamento e conscientização de segurança para desenvolvedores.

- **Módulo 04 – Pipeline DevSecOps: Etapa Code.**
  - Práticas de codificação segura e OWASP Top 10.
  - Segurança em repositórios Git: branch protection, commits assinados e controle de acesso.
  - Ferramentas de segurança na IDE: SonarLint, Snyk e assistentes de código com IA.
  - Prevenção de vazamento de segredos: git-secrets, Talisman, GitGuardian, TruffleHog e pre-commit hooks.
  - Revisão de código segura e pull requests com verificações automáticas.

- **Módulo 05 – Pipeline DevSecOps: Etapa Build and Test.**
  - Segurança no servidor de CI: Jenkins, GitHub Actions, GitLab CI/CD, Azure Pipelines e AWS CodeBuild.
  - Testes estáticos de segurança (SAST): SonarQube, Checkmarx, Semgrep e Snyk Code.
  - Análise de composição de software (SCA) e SBOM: OWASP Dependency-Check, Snyk Open Source, Mend.
  - Testes dinâmicos (DAST): OWASP ZAP, Burp Suite e Arachni.
  - Testes interativos (IAST) e testes de segurança de APIs.
  - Quebra de build (security gates) por severidade de vulnerabilidades.
  - Correção de vulnerabilidades assistida por IA.

- **Módulo 06 – Pipeline DevSecOps: Etapa Release and Deploy.**
  - Segurança de artefatos e repositórios de artefatos; assinatura e verificação de imagens.
  - Segurança de contêineres: Docker, varredura de imagens com Trivy, Anchore, Clair e Grype.
  - Segurança no Kubernetes: RBAC, Pod Security Standards, Network Policies e admission controllers (OPA Gatekeeper, Kyverno).
  - Segurança de Infraestrutura como Código: Terraform, CloudFormation e Ansible com Checkov, tfsec, KICS e Terrascan.

- Gerenciamento de segredos: HashiCorp Vault, AWS Secrets Manager, Azure Key Vault e Google Secret Manager.
- Proteção em tempo de execução (RASP) e estratégias de implantação seguras (blue/green, canary).

- **Módulo 07 – Pipeline DevSecOps: Etapa Operate and Monitor.**
  - Monitoramento contínuo de segurança e conformidade.
  - Gerenciamento de logs e observabilidade: ELK Stack, Splunk, Prometheus, Grafana e Datadog.
  - Detecção de ameaças em tempo de execução com Falco e serviços nativos de nuvem.
  - Alertas e resposta a incidentes: Opsgenie, PagerDuty, Incident.io e Splunk.
  - Gestão de vulnerabilidades em produção e aplicação de patches.
  - Conformidade como código (Compliance as Code) e auditoria contínua.
  - Melhoria contínua e feedback de segurança para o ciclo de desenvolvimento.

FORMAS DE PAGAMENTO:

CARTÃO DE CRÉDITO: Em até **12X** sem juros.

BOLETO: Em até **12X** sem juros ou **24X** com juros de **1.8% a.m.**

Atenciosamente,

PALOMA MORAES
Sales Trainning – Grupo Utah
55 11 96931-1515
paloma@utah.com.br
www.utah.com.br