L'AKADÉMIE DU DIGITAL · PROGRAMA DE FORMAÇÃO Certificação Qualiopi em preparação

DevSecOps

FOR-DEV-M4-A · Desenvolvimento, DevOps e Dados

Integrar a segurança ao longo de toda a cadeia de desenvolvimento e de implementação

DURAÇÃO
28 horas — 4 dias

PREÇO
1?960 € s/ IVA

PÚBLICO
Escolas e centros de formação

PRAZO DE ACESSO
Acesso em 2 dias úteis após validação da necessidade e dos pré-requisitos.

Preço estabelecido com base em 28 h a 70 € s/ IVA por hora. Percurso dedicado a escolas e centros de formação, estabelecido por orçamento; preço indicativo e negociável consoante o volume e o contexto.

O módulo alterna sequências teóricas e oficinas práticas ao longo de cada dia. Prolonga a cadeia DevOps integrando nela a segurança («shift left»): cultura DevSecOps, vulnerabilidades aplicacionais, segurança do código e das dependências, segurança do pipeline e dos contentores, testes dinâmicos e gestão de vulnerabilidades. O fio condutor das oficinas é o GitLab CI.

Objetivos pedagógicos

- Compreender a filosofia DevSecOps: «shift left», a segurança como responsabilidade de todos
- Identificar as principais vulnerabilidades aplicacionais (sensibilização OWASP Top 10)
- Integrar controlos de segurança automatizados num pipeline CI/CD (SAST, DAST, SCA)
- Gerir os segredos, as dependências e a segurança dos contentores e das imagens
- Implementar uma abordagem de testes de segurança e de gestão de vulnerabilidades
- Conhecer as bases da conformidade, da rastreabilidade e da resposta a incidentes

Público-alvo

- Estudantes e formandos das escolas e centros de formação parceiros
- Programadores e perfis DevOps que queiram integrar a segurança na sua prática
- Perfis técnicos que visam funções DevSecOps / segurança aplicacional

Pré-requisitos

É exigido o domínio das bases DevOps e CI/CD (módulo «DevOps e CI/CD» fortemente recomendado), bem como à-vontade com Git, Docker e um pipeline. Noções de desenvolvimento web facilitam a compreensão das vulnerabilidades. Estes elementos são validados por um formulário online e / ou por uma entrevista prévia.

- Dominar as bases DevOps e CI/CD (módulo DevOps e CI/CD aconselhado).

- Sentir-se à vontade com Git, Docker e um pipeline de integração.
- Ter noções de desenvolvimento web (uma mais-valia para as vulnerabilidades).
- Ter autonomia técnica e sensibilidade para os desafios de segurança.

Programa

Dia 1 — Cultura DevSecOps e ameaças aplicacionais

Do DevOps ao DevSecOps	1h15	«Shift left», segurança partilhada, o que o DevSecOps muda; quadro defensivo e ético. Exposição interativa, esquema da cadeia segura, lembrete do quadro ético.	Perguntas orais; questionário de escolha múltipla sobre a cultura DevSecOps.
Superfície de ataque	2h15	Mapear a superfície de ataque de uma aplicação. Trabalho prático guiado, aplicação de teste, grelha de análise.	Mapeamento da superfície de ataque validado.
Panorama das vulnerabilidades (OWASP)	1h00	Sensibilização para o OWASP Top 10 e para as vulnerabilidades comuns. Exposição, exemplos ilustrados, referências OWASP.	Questionário de escolha múltipla sobre o OWASP Top 10.
Identificar vulnerabilidades	2h30	Identificar vulnerabilidades numa aplicação propositadamente vulnerável. Trabalho prático em ambiente de teste dedicado, identificação enquadrada, debriefing.	Vulnerabilidades identificadas validadas.

Dia 2 — Segurança do código e das dependências

Análise estática (SAST)	1h15	Princípios do SAST, revisão de código orientada para a segurança. Exposição, exemplos de findings, boas práticas.	Perguntas orais; questionário de escolha múltipla.
Integrar uma ferramenta SAST	2h15	Implementar um SAST e interpretar os resultados. Trabalho prático guiado, ferramenta SAST, análise dos relatórios.	Análise SAST validada.
Dependências (SCA) e segredos	1h00	Segurança das dependências e gestão de segredos. Exposição, exemplos de CVE, boas práticas de gestão de segredos.	Questionário de escolha múltipla sobre SCA e segredos.
Dependências e segredos	2h30	Detetar dependências vulneráveis e proteger segredos. Trabalho prático, scanner de dependências, cofre de segredos.	Deteção e proteção validadas.

Dia 3 — Segurança no pipeline e nos contentores

Segurança na CI/CD	1h15	Security gates, automatização dos controlos de segurança. Exposição, esquema de pipeline seguro, exemplos.	Perguntas orais; questionário de escolha múltipla.
Proteger o pipeline (GitLab CI)	2h15	Adicionar controlos de segurança automatizados ao pipeline. Trabalho prático guiado em GitLab CI, etapas de segurança, acompanhamento.	Controlos de segurança integrados validados.
Segurança dos contentores e imagens	1h00	Análise de imagens, endurecimento, boas práticas. Exposição, exemplos de vulnerabilidades de imagens.	Questionário de escolha múltipla sobre a segurança dos contentores.
Analisar e endurecer uma imagem	2h30	Analisar e endurecer uma imagem de contentor. Trabalho prático, scanner de imagens, correção, revisão coletiva.	Imagem endurecida validada.

Dia 4 — Testes dinâmicos, conformidade, resposta e projeto

Testes dinâmicos (DAST) e vulnerabilidades	1h00	Princípios do DAST, gestão e priorização das vulnerabilidades. Exposição, exemplos de análises, método de priorização.	Questionário de escolha múltipla sobre o DAST.
Análise DAST e priorização	2h00	Lançar uma análise DAST e priorizar as correções. Trabalho prático, ferramenta DAST em ambiente de teste, plano de correção.	Análise DAST e priorização validadas.
Conformidade e resposta a incidentes	1h00	Conformidade, rastreabilidade, logs de segurança, bases da resposta a incidentes. Exposição, exemplos, boas práticas de rastreabilidade.	Questionário de escolha múltipla sobre conformidade e resposta.
Cadeia CI/CD segura e apresentação de resultados	2h30	Proteger uma cadeia CI/CD de ponta a ponta e apresentar. Trabalho prático de síntese, apresentações, revisão coletiva, questionário final de escolha múltipla, inquérito de satisfação.	Avaliação sumativa: pipeline seguro + questionário final de escolha múltipla.

Modalidades e meios pedagógicos

Formação presencial nas nossas instalações ou nas suas, em grupo reduzido. Alternância de contributos teóricos, oficinas práticas e simulações.

Material necessário :

16 GB de RAM recomendados

- Os formandos devem dispor de um PC com Wi-Fi e 16 GB de RAM recomendados.
- Efetivo adaptado ao formato escola / centro de formação.
- Percurso dedicado a escolas e centros de formação, estabelecido por orçamento.

Modalidades de avaliação

Avaliação das aprendizagens durante e no final da formação; certificado de conclusão entregue a cada formando.

Acessibilidade

Formação acessível a pessoas com deficiência. Contacte-nos antes da inscrição para estudarmos as adaptações necessárias.

Financiamento

Orçamento ou convenção de formação a pedido. A certificação Qualiopi está em preparação: a elegibilidade para financiamentos OPCO será aberta após a sua obtenção.

Auditoria de certificação prevista para T1 2027. Sem elegibilidade OPCO antes da sua obtenção.