GH-500: GitHub Advanced Security

Microsoft - Cloud

- **Nível:** Intermédio
- **Duração:** 7h

Sobre o curso

O curso irá explorar como utilizar o GitHub Advanced Security (GHAS) para maximizar o impacto na segurança e compreender o GHAS e o seu papel no ecossistema de segurança.

O GitHub Advanced Security (GHAS) desempenha um papel crucial no reforço da postura de segurança dos projetos de desenvolvimento de software no GitHub. Fornece um conjunto abrangente de ferramentas e funcionalidades concebidas para identificar e resolver vulnerabilidades de segurança ao longo de todo o ciclo de vida do desenvolvimento.

Ao integrar a segurança diretamente no processo de desenvolvimento com o GHAS, a tua equipa pode criar software mais seguro e fiável.

Aprende a proteger o teu código com funcionalidades de segurança avançadas em todas as fases do ciclo de vida do desenvolvimento. O GitHub Advanced Security é um complemento do GitHub Enterprise que permite utilizar funcionalidades de segurança, como a análise de segredos, a análise de código e a gestão de dependências, nos teus repositórios privados.

Destinatários

Este curso destina-se a profissionais que queiram compreender e implementar práticas avançadas de segurança com o apoio do GitHub Advanced Security (GHAS).

Vão aprender a melhorar significativamente os processos de desenvolvimento de software e a criar um ecossistema de desenvolvimento mais resiliente e seguro, utilizando soluções orientadas para programadores que permitem proteger o código, a cadeia de fornecimento e os segredos antes da passagem para produção.

Vão aprender como o GHAS proporciona às equipas de segurança visibilidade sobre a postura de segurança transversal à organização e à cadeia de fornecimento, bem como acesso incomparável a inteligência de segurança verificada, proveniente de milhões de programadores e investigadores de segurança em todo o mundo.

Objetivos

- Adquirir uma compreensão das funcionalidades do GitHub Advanced Security
- Obter as competências para reconhecer, aplicar e avaliar estas funcionalidades no teu próprio ambiente GitHub

---

Pré-requisitos

Compreensão básica dos fundamentos do GitHub.

Programa

- Introdução ao GitHub Advanced Security
- Configurar atualizações de segurança do Dependabot em repositório GitHub
- Configurar e utilizar a análise de segredos em repositório GitHub
- Configurar a análise de código no GitHub
- Identificar vulnerabilidades de segurança em código com o CodeQL
- Análise de código com o GitHub CodeQL
- Administração GitHub para o GitHub Advanced Security
- Gerir dados sensíveis e políticas de segurança no GitHub

Introdução ao GitHub Advanced Security
Este módulo vai ajudar-te a familiarizar-te com as funcionalidades do GitHub Advanced Security (GHAS) e com as boas práticas. À medida que aprendes sobre estas funcionalidades, vais identificar áreas críticas para eliminar lacunas de segurança.

- Definir o GHAS e a importância das suas funcionalidades essenciais
- Como utilizar o GHAS para obter o maior impacto
- Compreender o GHAS e o seu papel no ecossistema de segurança

Configurar atualizações de segurança do Dependabot em repositório GitHub
Neste módulo gere as tuas dependências com o GitHub Dependabot.

- Gerir as tuas dependências no GitHub
- Alertas do Dependabot
- Atualizações de segurança do Dependabot
- Gerir notificações e relatórios do Dependabot
- Revisão de dependências
  Exercício – Configurar atualizações de segurança do Dependabot

Configurar e utilizar a análise de segredos em repositório GitHub
Compreende como funciona a análise de segredos para a configurar e utilizar de forma eficiente.

- O que é a análise de segredos?
- Configurar a análise de segredos
- Utilizar a análise de segredos

Configurar a análise de código no GitHub
Este módulo introduz-te à análise de código e às suas funcionalidades. Vais aprender a implementar a análise de código usando CodeQL, ferramentas de terceiros e GitHub Actions.

- O que é a análise de código?
- Ativar a análise de código com ferramentas de terceiros
- Configurar a análise de código
- Exercício de configuração da análise de código

Identificar vulnerabilidades de segurança em código com o CodeQL
Neste módulo, vais aprender sobre o CodeQL e como o podes usar para analisar o código no teu repositório GitHub e identificar vulnerabilidades de segurança.

- Preparar uma base de dados para o CodeQL
- Executar o CodeQL numa base de dados
- Compreender os resultados do CodeQL
- Resolver problemas com os resultados do CodeQL

Análise de código com o GitHub CodeQL
Aprende a utilizar o CodeQL, uma poderosa ferramenta de análise estática, para implementar a análise de código no GitHub.

- O que é o CodeQL?
- Como o CodeQL analisa o código?
- O que é o QL?
- Análise de código e CodeQL
- Personalizar o teu fluxo de trabalho de análise de código com o CodeQL – Parte 1
- Exercício – Referenciar uma consulta CodeQL
- Personalizar o teu fluxo de trabalho de análise de código com o CodeQL – Parte 2
- Utilizar a CLI do CodeQL
- Personalizar linguagens e builds para análise de código
- Exercício – Configurar uma matriz de linguagens CodeQL

Administração GitHub para o GitHub Advanced Security
Compreende onde o GitHub Advanced Security se insere no ciclo de vida do desenvolvimento de software e como o ativar e implementar na tua organização.

- O que é o GitHub Advanced Security?
- Ativar o GitHub Advanced Security
- Gerir o acesso ao GitHub Advanced Security
- Gerir as funcionalidades e alertas do GitHub Advanced Security

Gerir dados sensíveis e políticas de segurança no GitHub

Familiariza-te com as ferramentas básicas de segurança do GitHub, que preparam os repositórios para um desenvolvimento seguro e para uma resposta a ameaças de acordo com os padrões da indústria.

- Definir políticas de segurança
- Criar e gerir conjuntos de regras de repositório
- Relatórios e registos