The DevSecOps Company

Microsoft Partner

GH-500T00
GitHub Advanced Security

Información general.

GitHub Advanced Security (GHAS) desempeña un papel crucial en el fortalecimiento de la postura de seguridad de proyectos de desarrollo de software en GitHub. Proporciona un conjunto completo de herramientas y funcionalidades diseñadas para identificar y abordar la seguridad vulnerabilidades a lo largo del ciclo de vida del desarrollo. Integrando Directamente en el proceso de desarrollo con GHAS, tu equipo puede Construye un software más seguro y fiable. El curso explorará cómo utilizar GHAS para maximizar el impacto en seguridad y comprender GHAS y su función en el ecosistema de seguridad.

Duración.

1 Día.

Perfil del público.

Este curso está dirigido a estudiantes que deseen comprender e implementar prácticas avanzadas de seguridad con la ayuda de GitHub Advanced Security (GHAS). Aprenderán a hacerlo de manera significativa mejorar los procesos de desarrollo de software y crear una estructura más resiliente y Ecosistema de desarrollo seguro utilizando soluciones centradas en el desarrollo para desbloquear la capacidad de mantener el código, la cadena de suministro y los secretos seguros ante ti Empuja a producción. Aprenderán cómo GHAS ofrece a los equipos de seguridad Visibilidad sobre la postura de seguridad y el suministro interorganizacional acceso en cadena e inigualable a inteligencia de seguridad curada desde millones de desarrolladores e investigadores en seguridad en todo el mundo.

Examen.

GH-500: GitHub Advanced Security.

Temario.

Ruta de aprendizaje: GitHub Advanced Security Parte 1.

Aprende cómo proteger tu código con funciones avanzadas de seguridad en cada etapa de tu ciclo de desarrollo. GitHub Advanced Security es un complemento de GitHub Enterprise que te permite utilizar funciones de seguridad, como escaneo de secretos, escaneo de código y gestión de dependencias en tus repositorios privados.

Módulo 1: Introducción a la seguridad avanzada de GitHub.

Este módulo te ayudará a familiarizarte con las funciones avanzadas de seguridad (GHAS) y las mejores prácticas de GitHub. A medida que aprendas sobre estas características, identificarás áreas críticas para eliminar brechas de seguridad.

- Define GHAS y la importancia de sus características integrales.
- Cómo utilizar GHAS para obtener el mayor impacto posible.
- Entiende GHAS y su papel en el ecosistema de seguridad.

Módulo 2: Configura las actualizaciones de seguridad de Dependabot en tu repositorio de GitHub.

Gestiona tus dependencias con GitHub Dependabot.

- Gestiona tus dependencias en GitHub.
- Alertas de dependabot.
- Actualizaciones de seguridad de Dependabot.
- Gestionar notificaciones e informes de Dependabot.
- Revisión de dependencias.

Ejercicio: Configurar actualizaciones de seguridad de Dependabot.

Módulo 3: Configura y usa el escaneo de secretos en tu repositorio de GitHub.

Entiende cómo funciona el escaneo secreto para configurarlo y usarlo de forma eficiente.

- ¿Qué es el escaneo secreto?
- Configurar el escaneo secreto.
- Utiliza escaneo secreto.

Módulo 4: Configurar el escaneo de código en GitHub.

Este módulo te introduce en el escaneo de código y sus funciones. Aprenderás a implementar el escaneo de código usando CodeQL, herramientas de terceros y GitHub Actions.

- ¿Qué es el escaneo de código?
- Habilitar el escaneo de código con herramientas de terceros.
- Configurar el escaneo de código.
- Configurar el ejercicio de escaneo de código.

Ruta de aprendizaje: GitHub Advanced Security Parte 2.

Aprende cómo proteger tu código con funciones avanzadas de seguridad en cada etapa de tu ciclo de desarrollo. GitHub Advanced Security es un complemento de GitHub Enterprise que te permite utilizar funciones de seguridad, como escaneo de secretos, escaneo de código y gestión de dependencias en tus repositorios privados.

Módulo 5: Identifica vulnerabilidades de seguridad en tu base de código usando CodeQL.

En este módulo, aprendes sobre CodeQL y cómo puedes usarlo para analizar el código de tu repositorio de GitHub e identificar vulnerabilidades de seguridad.

- Preparar una base de datos para CodeQL.
- Ejecutar CodeQL en una base de datos.
- Entender los resultados de CodeQL.
- Resolución de problemas de los resultados de CodeQL.

Módulo 6: Escaneo de código con GitHub CodeQL.

Aprende a usar CodeQL, una potente herramienta de análisis estático, para implementar el escaneo de código en GitHub.

- ¿Qué es CodeQL?
- ¿Cómo analiza CodeQL el código?
- ¿Qué es QL?
- Escaneo de código y CodeQL.
- Personaliza tu flujo de trabajo de escaneo de código con CodeQL.
- Utiliza la CLI de CodeQL.
- Personalizar lenguajes y compilaciones para escanear código.

Ejercicios:

- Referencia a una consulta CodeQL.
- Configurar una matriz de lenguaje CodeQL.

Módulo 7: Administración de GitHub para GitHub Advanced Security.

Entiende dónde encaja GitHub Advanced Security en tu ciclo de vida del desarrollo de software y cómo habilitarlo y desplegarlo en tu organización.

- ¿Qué es la Seguridad Avanzada de GitHub?
- Habilitar la seguridad avanzada de GitHub
- Gestionar el acceso a GitHub Advanced Security.
- Gestionar las funciones y alertas avanzadas de seguridad de GitHub.

Módulo 8: Gestionar datos sensibles y políticas de seguridad dentro de GitHub.

Familiarízate con las herramientas básicas de seguridad de GitHub, que preparan repositorios para un desarrollo seguro y una respuesta estándar del sector ante amenazas.

- Establecimiento de políticas de seguridad.
- Crear y gestionar conjuntos de reglas de repositorios.
- Informes y registro.