◦ Curso de preparación para certificación

Curso de preparación intensiva para certificación en Ciclo de Vida de Software Seguro (CSSLP)

Duración
5 encuentros de
8 horas c/u (total 40hs)

Plataforma:
Cisco Webex

POWERED BY BDO Academy

Objetivo

Preparar a aquellos que quieran acceder a la Certificación de Profesional en Ciclo de Vida de software seguro (CSSP). El curso repasa el amplio, actualizado y global cuerpo común de conocimientos (CBK) que presenta el CSSP, garantizando que los líderes de seguridad tengan una profunda comprensión de las nuevas amenazas, tecnologías, regulaciones, estándares y prácticas.

Módulos

1. Conceptos de software seguro:

Implicaciones y metodologías de seguridad dentro de sistemas centralizados y descentralizados, entornos a través de los sistemas informáticos de la empresa en desarrollo de software.

- Conceptos básicos
- Principios de diseño de seguridad
- Intimidad
- Gobernanza, Riesgo y Cumplimiento
- Metodologías de desarrollo de software

2. Requisitos de software seguro:

Captura de controles de seguridad utilizado durante la fase de requisitos para integrar la seguridad dentro el proceso, para identificar los objetivos clave de seguridad y para maximizar la seguridad del software y minimizar la interrupción de los planes y horarios.

- Descomposición de políticas
- Clasificación y categorización de datos
- Requerimientos funcionales
- Requerimientos operacionales

3. Diseño de software seguro:

Traducción de los requisitos de seguridad en elementos de diseño de aplicaciones, incluida la documentación de los elementos de las superficies de ataque de software, la realización de amenazas modelado y definición de cualquier criterio de seguridad específico

- Procesos de diseño

Dirigido a:

Profesionales que se desempeñen en el rol de Consultor de seguridad, Gerente de seguridad, Director/Gerente de TI, Auditor de seguridad, Arquitecto de seguridad, analista de seguridad, Ingeniero de Sistemas de Seguridad, Director de seguridad de la información, Director de seguridad y Arquitecto de red.

Alianza educativa:

Fast Lane

• Consideraciones de diseño
• Protección de la arquitectura de uso común
• Tecnologías

4. Implementación/codificación de software seguro:
Implica la aplicación de estándares de codificación y prueba, aplicación de seguridad
herramientas de prueba que incluyen "fuzzing", escaneo de código de análisis estático
herramientas y realizar revisiones de código.
• Seguridad declarativa versus imperativa (programática)
• Base de datos de vulnerabilidades / Listas
• Prácticas y controles de codificación defensiva
• Código fuente y control de versiones
• Entorno de desarrollo y construcción
• Código / Revisión por pares
• Análisis de código
• Técnicas anti-manipulación

5. Pruebas de software seguras:
Pruebas de control de calidad integradas para la seguridad funcionalidad y resistencia al ataque.
• Prueba de artefactos
• Pruebas de seguridad y control de calidad
• Tipos de pruebas
• Evaluación de impacto y acción correctiva
• Gestión del ciclo de vida de los datos de prueba

6. Aceptación del software:
Implicaciones de seguridad en el software fase de aceptación, incluidos los criterios de finalización, el riesgo, aceptación y documentación, Common Criteria y métodos de pruebas independientes.
• Pre-lanzamiento o pre-implementación
• Posteriores a la liberación

7. Implementación de software, operaciones, mantenimiento y Eliminación:
Cuestiones de seguridad en torno a las operaciones en estado estacionario y gestión de software. Medidas de seguridad que deben ser tomada cuando un producto llega al final de su vida útil.
• Instalación y Despliegue
• Operaciones y mantenimiento
• Eliminación de software

8. Cadena de suministro y adquisición de software:
Proporciona una descripción general de los conocimientos y las tareas necesarias para gestionar el riesgo para el desarrollo subcontratado, la adquisición y la adquisición de software y servicios relacionados.
• Evaluación de riesgos de proveedores
• Abastecimiento de proveedores
• Prueba de desarrollo de software
• Entrega de software, operaciones y mantenimiento
• Transición de proveedores

Equipo docente
Docentes de Fast Lane con certificación AWS

Sobre la certificación:

La certificación CSSP independiente es la credencial ideal para aquellos con profundos conocimientos técnicos y de gestión comprobada competencia, habilidades, experiencia y credibilidad para diseñar, diseñar, implementar y administrar información general programa de seguridad para proteger a las organizaciones del crecimiento ataques sofisticados.

El CSSLP le ayuda a:
• Valide su experiencia en seguridad de aplicaciones.
• Conquiste las vulnerabilidades de las aplicaciones ofreciendo más valor
• A su empleador.
• Demostrar un conocimiento práctico de la aplicación.
• Seguridad.
• Diferencie y mejore su credibilidad y
• Comerciabilidad a escala mundial.
• Afirme su compromiso con la competencia continua en el
• Mejores prácticas más actuales a través de (ISC)
• Requisitos de Educación Profesional (CPE).

El CSSLP ayuda a los empleadores:
• Rompe el enfoque de prueba de penetración y parche.
• Reduzca los costos de producción, las vulnerabilidades, la entrega y retrasos
• Mejorar la credibilidad de su organización y su equipo de desarrollo.
• Reducir la pérdida de ingresos y reputación debido a una infracción resultado de un software inseguro.
• Garantizar el cumplimiento con el gobierno o la industria regulaciones.

Metodología de evaluación:

Al final del taller, recibirán un cupón para realizar un examen de práctica en línea adicional sin costo alguno.