Cybersecurity Essentials 1.0
Alcance y secuencia

Última actualización: 22 mayo 2017

Público al que está destinado

El curso *Cybersecurity Essentials 1.0* está diseñado para estudiantes que están interesados en obtener estudios más avanzados en el campo de la ciberseguridad. Este curso preparatorio brinda una descripción general del campo de la ciberseguridad. El currículo analiza las características y las tácticas utilizadas por los delincuentes cibernéticos. Luego profundiza en las tecnologías, los productos y los procedimientos que el profesional de la ciberseguridad usa para combatir el delito cibernético. El currículo es apropiado para estudiantes de muchos niveles de educación y tipos de instituciones, como escuelas secundarias, institutos de enseñanza superior, universidades, escuelas técnicas y de formación profesional, y centros comunitarios.

Requisitos previos

Para el desarrollo correcto de las habilidades, los estudiantes deben estar familiarizados con el contenido y las habilidades que se describen en el curso de requisitos previos:

- Introduction to Cybersecurity 2.0

Certificaciones a las que se aspira

No existen certificaciones objetivo para este curso.

Descripción del currículo

El curso tiene muchas funciones para ayudar a los estudiantes a comprender estos conceptos:

- Contenido multimedia enriquecedor, que incluye actividades interactivas, videos, juegos y pruebas que abordan una variedad de estilos de aprendizaje y ayudan a estimular el aprendizaje y a aumentar la retención del conocimiento.
- Las prácticas de laboratorio y las actividades de aprendizaje basadas en la simulación de Packet Tracer ayudan a los estudiantes a desarrollar el pensamiento crítico y las aptitudes para la resolución de problemas complejos
- Los exámenes innovadores proporcionan un panorama inmediato que sirve de apoyo a la evaluación del conocimiento y las habilidades adquiridas
- Los conceptos técnicos se explican en el idioma adecuado para los estudiantes de todos los niveles y las actividades interactivas integradas dividen la lectura del contenido y ayudan a reforzar la comprensión
- El currículo incentiva a los estudiantes a considerar la formación adicional en TI y también enfatiza las habilidades y la experiencia práctica aplicadas

Las actividades de Cisco Packet Tracer están diseñadas para usarse con Packet Tracer 6.3 o superior.

© 2017 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Objetivos del currículo

Cybersecurity Essentials 1.0 abarca las habilidades de conocimiento y principios básicos en todos los dominios de seguridad del mundo cibernético: seguridad de la información, seguridad de sistemas, seguridad de la red, seguridad móvil, seguridad física, ética y leyes, tecnologías relacionadas, técnicas de defensa y mitigación utilizadas en la protección de los negocios.

Cuando los estudiantes finalicen el curso *Cybersecurity Essentials 1.0*, serán capaces de realizar las siguientes tareas:

- Describir las características de los delincuentes y héroes del ámbito de la ciberseguridad.
- Describir los principios de confidencialidad, integridad y disponibilidad que se relacionan con los estados de datos y las contramedidas de ciberseguridad.
- Describir las tácticas, las técnicas y los procedimientos utilizados por los delincuentes cibernéticos.
- Describir cómo las tecnologías, los productos y los procedimientos se utilizan para proteger la confidencialidad.
- Describir cómo las tecnologías, los productos y los procedimientos se utilizan para garantizar la integridad.
- Describir cómo las tecnologías, los productos y los procedimientos proporcionan alta disponibilidad.
- Explicar la forma en que los profesionales de la ciberseguridad utilizan las tecnologías, los procesos y los procedimientos para defender todos los componentes de la red.
- Explicar el propósito de las leyes relacionadas con la ciberseguridad.

Requerimientos mínimos del sistema

Para proporcionarle una mejor experiencia de aprendizaje, se recomienda contar con un tamaño típico de clase para 12 a 15 estudiantes, con una relación de una computadora de laboratorio por estudiante. A lo sumo, dos estudiantes pueden compartir una computadora de laboratorio para las actividades prácticas. Para algunas actividades, es necesario que las PC del laboratorio que utilizan los alumnos estén conectadas a una red local.

Requisitos de hardware de las PC de laboratorio

- Computadora con un mínimo de 2 Gb de RAM y 8 Gb de espacio libre en disco
- Acceso a Internet de alta velocidad para descargar Oracle VirtualBox y el archivo de imagen de máquina virtual

Descripción general del currículo

El curso *Cybersecurity Essentials 1.0* ayuda a los estudiantes:

- A comprender los participantes del mundo de la ciberseguridad y la motivación de los delincuentes cibernéticos y los especialistas en ciberseguridad.
- A aprender a identificar los ataques a la seguridad, los síntomas, los procesos y las contramedidas.
- A adquirir los conocimientos básicos en varios dominios de seguridad.
- A desarrollar habilidades de administración de seguridad, controles, protección y tecnologías de mitigación.
- A conocer las leyes de seguridad, ética y cómo desarrollar políticas de seguridad.
- A conocer las funciones de diferentes profesionales de la ciberseguridad y las opciones profesionales.

© 2013 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Esquema del curso

Tabla 1. Esquema del curso Cybersecurity Essentials 1.0

Capítulo o sección	Metas u objetivos
Capítulo 1. Ciberseguridad: un mundo de paladines, delincuentes y héroes	**Describa las características de los delincuentes y héroes del ámbito de la ciberseguridad.**
1.1 El mundo de la ciberseguridad	Describa las características comunes que componen el mundo de la ciberseguridad
1.2 Los delincuentes cibernéticos frente a los héroes cibernéticos	Distinga las características de los delincuentes cibernéticos y de los héroes cibernéticos
1.3 Amenazas al reino	Compare la manera en que las amenazas a la ciberseguridad afectan a las personas, las empresas y las organizaciones
1.4 El lado oscuro de la ciberseguridad	Describa los factores que conducen a la propagación y al crecimiento de los delitos cibernéticos.
1.5 Creación de más héroes	Describa las organizaciones y los esfuerzos comprometidos a expandir la fuerza laboral de ciberseguridad
tulo 2. El cubo de destrezas de ciberseguridad	**Describa los principios de confidencialidad, integridad y disponibilidad que se relacionan con los estados de datos y las contramedidas de ciberseguridad.**
2.1 El cubo de destrezas de ciberseguridad	Describa las tres dimensiones del cubo de McCumber.
2.2 Tríada de CIA	Describa los principios de confidencialidad, integridad y disponibilidad.
2.3 Estados de los datos	Diferencie los tres estados de los datos.
2.4 Contramedidas de la ciberseguridad	Compare los tipos de contramedidas de la ciberseguridad.
2.5 Marco de trabajo para la administración de la seguridad de TI	Describa el modelo de ciberseguridad de ISO
Capítulo 3. Amenazas, vulnerabilidades y ataques a la ciberseguridad	**Describa las tácticas, las técnicas y los procedimientos utilizados por los delincuentes cibernéticos.**
3.1 Malware y código malicioso	Diferencie los tipos de malware y de código malicioso.
3.2 Uso de trucos	Compare los diferentes métodos utilizados en ingeniería social.
3.3 Ataques	Compare los diferentes tipos de ciberataques.
Capítulo 4. El arte de los secretos de protección	**Describa cómo las tecnologías, los productos y los procedimientos se utilizan para proteger la confidencialidad.**
4.1 Criptografía	Explique cómo las técnicas de encriptación protegen la confidencialidad.
4.2 Controles de acceso	Describir cómo las técnicas de control de acceso protegen la confidencialidad.
4.3 Ocultamiento de datos	Describa el concepto de ocultamiento de datos.

© 2013 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Capítulo 5. El arte de garantizar la integridad	Describa cómo las tecnologías, los productos y los procedimientos se utilizan para garantizar la integridad.
5.1 Tipos de controles de integridad de datos	Explique los procesos utilizados para garantizar la integridad.
5.2 Firmas digitales	Explique el propósito de las firmas digitales.
5.3 Certificados	Explique el propósito de los certificados digitales.
5.4 Aplicación de la integridad de la base de datos	Explique la necesidad de la aplicación de la integridad de la base de datos.
Capítulo 6. El universo de los cinco nueves	**Describa cómo las tecnologías, los productos y los procedimientos proporcionan alta disponibilidad.**
6.1 Alta disponibilidad	Explique el concepto de alta disponibilidad.
6.2 Medidas para mejorar la disponibilidad	Explique cómo se utilizan las medidas de alta disponibilidad para mejorar la disponibilidad.
6.3 Respuesta ante los incidentes	Describa cómo un plan de respuesta ante los incidentes mejora la alta disponibilidad.
6.4 Recuperación tras un desastre	Describa cómo la planificación de recuperación tras un desastre juega un papel fundamental en la implementación de la alta disponibilidad.
Capítulo 7. Fortalecimiento del reino	**Explique la forma en que los profesionales de la ciberseguridad utilizan las tecnologías, los procesos y los procedimientos para defender todos los componentes de la red.**
7.1 Defensa de sistemas y dispositivos	Explique la forma en que los procesos y procedimientos protegen los sistemas.
7.2 Fortalecimiento de los servidores	Explique cómo proteger los servidores en una red.
7.3 Fortalecimiento de las redes	Explique cómo implementar las medidas de seguridad para proteger los dispositivos de red
7.4 Seguridad física y medioambiental	Explique cómo se implementan las medidas de seguridad físicas para proteger el equipo de red.
Capítulo 8. Unirse al pedido de los héroes cibernéticos	**Explique el propósito de las leyes relacionadas con la ciberseguridad.**
8.1 Dominios de la ciberseguridad	Describa cómo los dominios de la ciberseguridad se utilizan en la tríada de CIA.
8.2 Comprensión del juramento de pertenencia	Explique cómo la ética proporciona orientación.
8.3 Siguiente paso	Explique cómo dar el siguiente paso para convertirse en un profesional del área de la ciberseguridad

Sede central en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia-Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV Amsterdam,
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono y fax se encuentran en la Web de Cisco en www.cisco.com/go/offices.

Cisco y el logotipo de Cisco son marcas comerciales o marcas registradas de Cisco o de sus filiales en EE. UU. y en otros países. Si desea consultar una lista de las marcas comerciales de Cisco, visite www.cisco.com/go/trademarks. Las marcas registradas de terceros que se mencionan aquí son de propiedad exclusiva de sus respectivos propietarios. El uso de la palabra "partner" no implica la existencia de una asociación entre Cisco y cualquier otra empresa. (1110R)

© 2017 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.