CYBER SECURITY FOUNDATION
PROFESSIONAL CERTIFICATE

CSFPC™ Versión 062022

CertiProf®

Cyber Security Foundation Professional Certificate CSFPC™

Syllabus V062022

Introducción

Entienda los fundamentos de las técnicas de protección de la información personal, incluyendo comunicaciones, aplicaciones, e inferencias de las bases de datos y procesamiento de datos. También conozca otros sistemas que soportan los derechos en línea que se refieren a censura y circunvención, secrecía, elecciones electrónicas, y privacidad en pagos y sistemas de identidad.

La fuente de esta certificación es el Cuerpo de Conocimiento de Ciber Seguridad (Cyber Security Body of Knowledge - CyBok) versión 1.0.

Objetivos de Aprendizaje

- Entender la importancia de la Ciberseguridad
- Comprender los conceptos clave relacionados con la seguridad cibernética
- Comprender los conceptos relacionados con los aspectos humanos, organizativos y normativos.
- Comprender los conceptos relacionados con Ataques y Defensas

Formato y Duración del Examen

Este programa de estudio tiene un examen el cual el candidato debe alcanzar un puntaje para obtener la certificacion en Cyber Security Foundation Professional Certificate™

- Formato: Opción múltiple
- Preguntas: 40
- Puntaje de Aprobación: - 80%
- Idioma: Inglés / Español
- Duración: 60 minutos
- Entrega: Este examen está disponible en línea
- Supervisado: Auto-supervisado
- A libro cerrado

Elegibilidad para la Certificación

Esta certificación está dirigida a todas las personas que quieran orientar su futura carrera profesional en el área de Ciberseguridad y a profesionales tales como:

- Todos
- Usuarios Finales
- Gerentes

Contenido

Recuperar
Muestra de Actividades de Recuperación
Marco de Trabajo
Tips Cotidianos
Recursos

Módulo 1: CyBOK – Fundamentos de Ciberseguridad

Definición de Ciberseguridad
Áreas de Conocimiento CyBOK
Cómo Desplegar Conocimiento CyBOK para Resolver Problemas de Protección (Security)
Funciones Dentro de un Sistema de Gestión de Protección (Security)
Principios
Tema Interdisciplinario
Ciberespacio

Módulo 2: Gestión de Riesgos

Temas a Tratar en esta Lección
¿Qué es el riesgo?
¿Por qué la evaluación y la gestión del riesgo son importantes?
¿Qué es la evaluación y gestión del riesgo cibernético?
Gobernanza de Riesgo
El Factor Humano y Comunicación del Riesgo
Cultura de Seguridad y Conciencia
Promulgación de la Política de Seguridad
Principios de Evaluación y Gestión de Riesgos
Elementos de Riesgo
Métodos de Evaluación y Gestión de Riesgos
Marcos de Gestión de Riesgos Cibernéticos Basados en Componentes
Métodos de Gestión de Riesgos Cibernéticos Impulsados por el Sistema
Evaluación y Gestión de Riesgos en Sistemas Ciberfísicos y Tecnología Operativa
Métricas de Seguridad
¿Qué constituye las métricas buenas y malas?
Continuidad del Negocio
ISO/IEC 27035-1:2016
NCSC- ISO/IEC 27035
Directrices para Mapear el Problema de Gestión de Riesgo
Conclusión

Módulo 3: Ley y Regulación

Introducción
Desafíos
Respuesta

Fuera del Alcance
Principios Introductorios de la Ley e Investigación Legal
"Para Probar" Algo
"Niveles" de Pruebas
Aplicando el Derecho al Ciberespacio y las Tecnologías de la Información
Distinguiendo el Derecho Penal y Civil
Jurisdicción
Una Taxonomía de Jurisdicción
Jurisdicción Legislativa (Prescriptiva)
Jurisdicción de Ejecución
El Problema de la Soberanía de los Datos
Leyes de Privacidad en General e Interceptación Electrónica
Interceptación Estatal (Acceso Legal)
Interceptación No Estatal
Protección de Datos
Los "Jugadores"
¿Qué se regula?
"Datos Personales" vs "PII"
Puntos Destacados de la Protección de Datos
Delitos Informáticos
Crímenes en Contra de los Sistemas de Información
Desafíos Recurrentes
Contrato
Contrato como un Medio para Incentivar Conductas de Protección (Security)
Límites de Influencia
Influencia Relacionada con el Contrato Sobre Comportamiento de Protección (Security)
Incumplimiento de Contrato y Recursos
Delito
Ejemplos de Delito
Negligencia (Responsabilidad Culposa)
Responsabilidad del Producto (Responsabilidad Rigurosa)
Cuantía de Pérdida (Q)
Asignación e Imputación de Responsabilidad
Propiedad Intelectual
Ingeniería Inversa
Blindaje de los Intermediarios de Internet de los Procedimientos de Responsabilidad y Remoción (Bajar el Contenido)
Desmaterialización de los Documentos y de los Servicios Fiduciarios Electrónicos
Emergen Cambios Legales

Otras Cuestiones Normativas
Ley Pública Internacional
Atribución Estatal
Operaciones de un Único Lugar
Ética
Códigos de Conducta
Pruebas de Vulnerabilidad y Divulgación
Gestión del Riesgo Legal

Módulo 4: Factores Humanos

Introducción
Factores Humanos
La Protección (Security) Debe Ser Utilizable
Adaptar la Tarea al Ser Humano
Capacidades y Limitaciones Humanas
STM Y One-time password (OTPs)
Capacidades y Limitaciones Humanas Generales
CAPTCHA
Metas y Tareas
Capacidades y Limitaciones del Dispositivo
Error Humano
Condiciones de Diseño Latentes
Conciencia y Educación
Sensibilización y Educación
¿Qué problemas de utilización enfrentan los desarrolladores?
¡Los Desarrolladores no son el Enemigo! La Necesidad de APIs de Protección (Security) Utilizables
La Utilización Huele: Un Análisis de la Lucha de los Desarrolladores con las Bibliotecas Criptográficas

Módulo 5: Privacidad y Derechos en Línea

Introducción
Visión General
Privacidad como Confidencialidad
¿Cuál es el problema?
¿Qué es la privacidad?
Definiendo la Privacidad
Privacidad como…
Privacidad como Transparencia
Privacidad como Control
Límites del Control y Transparencia

Privacidad como Confidencialidad
Panorama de Amenazas a la Privacidad
Enfoque Formal para el Control de Inferencia
Privacidad como Confidencialidad
Confidencialidad de Datos
Confidencialidad de Metadatos
Privacidad como Control
Privacidad como Transparencia
Tecnologías de Privacidad
Ingeniería de la Privacidad
Evaluación de la Privacidad
Conclusiones

Módulo 6: Malware y Tecnologías de Ataque

Introducción
Malware
Taxonomía del Malware
Taxonomía del Malware: Dimensiones
Taxonomía: Ejemplos
Programas Potencialmente No Deseados (PUPs)
Actividades Maliciosas del Malware
El Modelo Cyber Kill Chain
Ecosistema Clandestino
Objetivos de Acción
¿Por qué analizar el Malware?
Adquiriendo la Información del Malware
Análisis Estático
Análisis Dinámico
Otras Técnicas de Análisis
Entorno de Análisis
Entornos Comunes
Seguridad y Entornos Vivos
Técnicas de Anti-Análisis y Evasión
Objetivo de la Detección de Malware
Evasión y Contramedidas
Detección de Ataque de Malware
Análisis de Seguridad Basado en ML
Detección de Malware Basada en ML
Evasión de la Detección de Malware Basada en ML
Deriva Conceptual

Respuesta del Malware
Interrupción de las Operaciones de Malware
Atribución
Evasión y Contramedidas
Conclusión

Módulo 7: Comportamiento Adverso

Introducción
Una Caracterización de Adversarios
Agresores Interpersonales
Delincuentes Organizados Cibernéticos
Hacktivistas
Actores Estatales
Los Elementos de una Operación Maliciosa
Servicios Especializados
Servicios Humanos
Métodos de Pago
Modelos para Entender las Operaciones Maliciosas
Árboles de Ataque: Ejemplo de un Ataque
Cyber Kill Chain
Criminología Ambiental
Atribución de Ataque

Módulo 8 : Operaciones de Seguridad y Gestión de Incidentes

Introducción
¿De qué se trata?
Cronología y Alcance
Blucle MAPE-K General
Componentes de MAPE-K Supervisar-Analizar-Planificar-Ejecutar
Despliegues de las Tecnologías SOIM
Principios de Arquitectura - Arquitectura Típica
Detección de Intrusos y Sistemas de Prevención
MONITOR: Fuentes de Datos
Fuentes de Datos de Red: Posibles Detecciones
Fuentes de Datos de Aplicación
Fuentes de Datos del Sistema
Syslog
Problemas Frecuentes de Fuentes de Datos
Análisis de Rastros
Del Evento al Incidente
Detección de Uso Indebido

Detección de Anomalías
Problemas Generales en la Detección de Intrusos
Arquitectura Típica Información de Seguridad y Gestión de Eventos
Recolección de Datos en SIEM
Correlación de Alerta
Mitigación y Contramedidas Herramientas y Técnicas
Inteligencia y Análisis
Ciclo de Vida de la Gestión de Incidentes
Conclusión

Módulo 9: Examen de Certificación

Insignia
Condiciones del Examen