NUEVO

AUDITORÍAS AVANZADAS DE CIBERSEGURIDAD *RED TEAMING*

INSCRIPCIÓN

13 DE JUNIO | HORAS CPE: 8 | TARIFA*: 760 € · SOCIO: 645 € · SOCIO CORPORATIVO: 530 € | NIVEL: TODOS

La Ciberseguridad, su marco de control y los modelos de auditorías de seguridad requieren una revisión en un formato continuo y con nuevos enfoques para asegurar que estén siempre alineados a los ataques cada vez más sofisticados y en constante evolución. La aparición de 0-days, las vulnerabilidades críticas, los límites en las tecnologías de protección y la falta de concienciación de los usuarios implican en más capacidades de detección, respuesta y remediación, y la necesidad de nuevos modelos y organización de auditorías de Seguridad.

En este curso se propone un enfoque *Red Teaming* que permite evaluar nuestras capacidades corporativas de detección, mitigación y respuesta frente a Ciberamenazas de una manera eficaz y eficiente. Un *Red Team* es un equipo de profesionales especializados en ámbitos de la Seguridad Lógica y Física que utilizan sus conocimientos avanzados para crear escenarios que ponen a prueba la seguridad de una organización. Su misión es ejecutar las acciones de un atacante mediante un equipo gestionado desde una Dirección de Control Interno para realizar actividades no autorizadas en los sistemas corporativos.

Si un punto de control crítico en el mundo de la Ciberseguridad es dar respuesta a la pregunta "¿Qué pasa si…?". Un *Red Team* da esta respuesta.

OBJETIVO

Proporcionar a los asistentes, mediante un enfoque práctico y operativo, conocimiento para implantar esquemas de auditorías internas bajo un enfoque *Red Teaming,* lo que incluye:

- Conocer todos los conceptos básicos de Red Teaming.
- Diseñar un proceso y equipo para realizar la función interna de *Red Teaming.*

TEMARIO

Conceptos de Red Team.
- Necesidad, objeto y finalidad.
- Diferencias y similitudes con *pentesting.*
- El *Red Team* versus *Blue Team* y *Green Team.*

Modelo organizativo.
- Principales procesos (Inteligencia, Operaciones, Remediación, Medición).
- El equipo humano.
- La externalización de la *workforce.*

Inteligencia de Amenazas, Vulnerabilidades y Ataques.
- Mapa de Amenazas y Vulnerabilidades.
- Gestión del *know-how* de escenarios internos.
- Catálogo *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK).*
- Gestión y mantenimiento del arsenal.

Categorización y Selección de Targets.
- Mapa de Servicios y Arquitecturas corporativas.
- Criterios de selección de targets para órdenes de operación.

Operaciones.
- Diseño y Planificación de Operaciones.
- CTF. *Capture The Flag.*
- BTD. *Break The Defense.*
- UTP. *(Un)Trusted Third Parties.*
- IO. *Intelligence Operations.*

Gestión de resultados y medición.
- *KPIs* de la función, las operaciones y sus resultados.
- *SLAs* con proveedores.

DESTINATARIOS

- Directores de Sistemas.
- Responsables de la Seguridad de la Información.
- Auditores y profesionales de TI que tengan responsabilidad en materia de cumplimiento, organización y gestión de aspectos relacionados con Seguridad de la Información.

DIRECCIÓN TÉCNICA

Manuel Mendiola Antona, CIA, CRMA, CISA, CISM, CGEIT, CRISC
Auditor Informático.
Diplomado en Informática de Gestión. Director de Auditoría en KPMG.

PONENTE

Damián Ruiz Soriano, CISA, CISSP, Lead auditor 27001
Auditor de Sistemas en Bankia (Seguridad Física y Ciberseguridad).
Informática de Sistemas (Universidad Politécnica de Madrid).
Formación Superior en Dirección de Seguridad Privada.
Técnico Avanzado en Fundamentos de Inteligencia y Contrainteligencia.

HORARIO

De 9,00 h. a 18,00 h.

LUGAR DE CELEBRACIÓN

MADRID · Sede social del IAI (Santa Cruz de Marcenado, 33 - 1º).

* 21% de IVA no incluido