ISACA
San Salvador Chapter

Fundamentos Informática Forense
(Nivel Básico)

En el curso Fundamentos de la Informática Forense aprenderá los principios y metodologías utilizadas en la investigación de delitos informáticos. Aprenderá sobre la importancia de la prevención y presentación de evidencias digitales, así como la normativa y regulaciones a nivel internacional. También explorará los diferentes tipos de evidencia digital y los delitos más comunes en el ámbito informático.

Dirigido a:
Profesionales IT y ciberseguridad, agentes de aplicación de la ley, profesionales legales y de cumplimiento, auditores y consultores de seguridad informática.

Inversión:

- Miembros ISACA: **$130.00 + IVA**
- Público general: **$160.00 + IVA**

Detalles del curso:

- **Fechas y horarios:**
  - Lunes 10 de agosto: De 5:00 pm a 9:00pm.
  - Martes 11, miércoles 12, jueves 13 y viernes 14 de agosto: De 5:00 pm a 8:00pm.
- **Modalidad:** Virtual (Plataforma de ZOOM)
- Incluye diploma de participación y 16 CPE

Importante: Cada participante debe usar su equipo personal, si es empresarial debe tener el usuario “administrador” para poder instalar el software que se utilizará.

Inscripción:

Para registrar tu cupo debes enviarnos la ficha de inscripción completa y comprobante de pago a:

- administracion@isaca.org.sv o al
- (503) 6844-5653

Cupo limitado

Más información

@chapter_sv_isaca
@ISACAElSalvador
+503 6844-5653
@ISACAElSalvador
capitulosansalvador@isaca.org.sv

Instructor

Edwin Henríquez
(CSXF, EH, CAPC, CFCA, CPPT)

Consultor de Tecnología con más de 25 años de experiencia con certificaciones vigentes, en el área de informática, en Capacitaciones, Desarrollo de aplicaciones Web y Móviles, Administración bases de datos (Tradicionales y NoSQL), Inteligencia Artificial, Seguridad de la información, Ciberseguridad, Pentesting y Forense Informático.
Speaker ISACA Regional y Latinoamérica, Conferencista de eventos Informáticos, Líder Técnico OWASP El Salvador, Miembro comunidad Hackers DragonJAR. ISO 42001 AI Governance Funamentals Professional Certification.

Contenido del curso

Día 1: Metodología, Normativa y Preservación de Evidencia (Teoría y práctica de laboratorio)

- Principios del análisis forense digital y el rol del perito.
- Ciclo de vida de la evidencia: Identificación, Preservación, Análisis y Presentación.
- Estándar **ISO/IEC 27037** (Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital).
- Cadena de Custodia: Importancia legal, formatos físicos y control de cambios.
- Orden de volatilidad de los datos (RFC 3227).

Día 2: Triaje y Análisis de Memoria RAM (Teoría y práctica de laboratorio)

- Por qué la memoria RAM es el "santo grial" en incidentes modernos (malware sin archivos, cifrado activo, sesiones abiertas).
- Técnicas de captura de memoria sin contaminar la escena.
- Introducción al motor de análisis de Volatility.

Día 3: Análisis de Artefactos y Sistemas de Archivos (Windows Forensics) (Teoría y práctica de laboratorio)

- Sistemas de archivos NTFS y FAT32 (conceptos básicos, metadatos y borrado lógico).
- Artefactos de ejecución y persistencia en Windows: *Prefetch, Shimcache, Amcache, y Registros de Windows*.
- Evidencia de acceso a archivos: archivos de acceso directo (*LNK files*) y *Jump Lists*.

Día 4: Forense en Correo Electrónico y Ataques de Suplantación (Teoría y práctica de laboratorio)

- Estructura técnica de un correo electrónico (MIME y protocolo SMTP).
- Anatomía detallada de los encabezados (*Headers*) de correo.
- Protocolos de validación perimetral: SPF, DKIM y DMARC (cómo interpretar fallos de alineación).

Día 5: Correlación de Eventos (Logs) e Informe Pericial (Teoría y práctica de laboratorio)

- Fuentes de registros en la empresa: Eventos de Windows (*Security, System*), Syslog, logs de servidores web (Apache/IIS).
- Creación de líneas de tiempo (*Timelines*) y normalización horaria (UTC vs. hora local).
- Estructura, redacción y defensa de un Informe Pericial Técnico-Forense (buenas prácticas para audiencias técnicas y ejecutivas).
- Práctica en Laboratorio: *Escenario de Defacement/Intrusión Web.*

Más información

@chapter_sv_isaca
+503 6844-5653
capitulosansalvador@isaca.org.sv
@ISACAElSalvador
@ISACAElSalvador