LIVE CLASS

CON APLICACIÓN DE IA

Workshop en Ciberseguridad

Defensa híbrida con IA

Anticipar la amenaza.
Automatizar la respuesta.
Garantizar la continuidad.

Lográ el aval de nuestros expertos

En Kinetic Training se unen tus ganas de crecer con nuestra experiencia y conocimientos para que puedas desarrollar todo tu potencial.

Nuestras formaciones están respaldadas por la excelencia académica y la experiencia profesional y empresarial de un equipo de trainers altamente calificados.

Al completar la formación, recibirás esta insignia que reconoce tu aprendizaje, dedicación y esfuerzo.

Esto es Kinetic Training, donde la experiencia de aprendizaje es transformadora desde el primer clic.

¡CONOCENOS!

¿Por qué tomar esta formación?

Este programa marca la evolución definitiva de la seguridad estática hacia la Ciberresiliencia Activa. No se trata solo de bloquear amenazas, sino de garantizar la supervivencia operativa.

Utilizando la Inteligencia Artificial como motor estratégico, transformamos la postura defensiva: de reactiva a predictiva.

Abordamos desde la priorización inteligente de riesgos hasta la automatización de respuestas (SOAR), asegurando que cuando el perímetro falle, la continuidad del negocio (BCP/DRP) prevalezca.

¿A quién está dirigida?

- Profesionales y estudiantes del ámbito tecnológico, personal de áreas de TI y ciberseguridad, analistas o técnicos que trabajan con sistemas de información.
- Miembros de áreas legales, comunicaciones y cumplimiento.
- Cualquier persona interesada en comprender y aplicar la Inteligencia Artificial de manera estratégica en la seguridad de la información y la ciber-resiliencia.

Objetivo de la formación

Romper el paradigma de la seguridad estática tradicional para adoptar una postura de defensa híbrida y ciberresiliente, demostrando el valor estratégico de la Inteligencia Artificial en la optimización de la prevención, detección y respuesta ante amenazas cibernéticas modernas.

¿Qué vas a aprender?

- A identificar cómo la Inteligencia Artificial ha industrializado los ciberataques, permitiendo campañas de phishing hiperrealistas y la creación de malware polimórfico.
- A distinguir y priorizar los Activos Críticos de tu organización basándote en el impacto a la Confidencialidad, Integridad y Disponibilidad (tríada C-I-D).
- A aplicar un modelo de Scoring Híbrido que utiliza IA para ponderar la gravedad técnica de una vulnerabilidad junto con el contexto real del negocio y la inteligencia de amenazas.
- A diferenciar entre la seguridad tradicional basada en "firmas" y la detección moderna de anomalías comportamentales para identificar amenazas de día cero.
- A estructurar un Playbook de respuesta a incidentes que transforme el caos en un procedimiento de contención ordenado y efectivo.
- A comprender el rol de la orquestación (SOAR) para automatizar acciones de defensa en segundos y la diferencia crítica entre un Plan de Continuidad (BCP) y un Plan de Recuperación (DRP).

Metodología de trabajo

Duración de la cursada

4 horas

- 2 encuentros de 2 horas.

Condiciones para obtener el certificado

- 70% de asistencia.

Cantidad de kines que acumula

4 Kines (crédito virtual para ser utilizado en futuras formaciones)

Inicio de la formación

La apertura de nuestras formaciones depende de la disponibilidad y el cupo. En situaciones excepcionales que impidan el inicio de una formación, ofrecemos devolver el importe abonado o utilizarlo como pago parcial o total de alguna otra formación.

Modalidad

LIVE CLASS

- Encuentros virtuales sincrónicos, en vivo, y actividades grupales interactivas.
- Participación en foros, acceso a los materiales y ejercicios prácticos dentro de nuestra plataforma de formación Kinetic Training.
- El objetivo es que la interacción entre el instructor y los participantes asegure el intercambio del aprendizaje grupal y una comunicación fluida entre ellos

Requisitos técnicos

- Computadora / Notebook con *Zoom* instalado.
- Buena velocidad de internet: bajada 10 mbps y subida 2 mbps (mínimo).

Conocimientos previos requeridos:

- El contenido está estructurado para nivelar conocimientos, por lo que **no se requieren habilidades técnicas avanzadas de programación o hacking**, pero sí un conocimiento operativo del entorno corporativo:
    - **Conocimiento del contexto de su organización:** se requiere que los asistentes conozcan la estructura de su empresa para realizar ejercicios prácticos, como definir sus propios Activos Críticos de Confidencialidad, Integridad y Disponibilidad.
    - **Familiaridad básica con infraestructura TI:** es útil que los asistentes entiendan conceptos generales como qué es un servidor, una base de datos, un firewall o un endpoint (antivirus), ya que se utilizan analogías como la "defensa en profundidad" basada en estas capas.
    - **Nociones de gestión:** no se requiere experiencia previa en IA, ya que el curso explica desde cero cómo la IA cambia el panorama de ataques (ej. phishing y malware) y define conceptos básicos como la triada de seguridad (C-I-D) al inicio.

Programa

1 MÓDULO 1: Fundamentos del nuevo riesgo

Este módulo establece la base conceptual, contrastando la seguridad tradicional con la nueva realidad de amenazas impulsadas por IA.

- **1. La ciberseguridad y la escalada de la amenaza**
  - **Definición Fundamental (C-I-D):** se repasa que la ciberseguridad protege la Confidencialidad, Integridad y Disponibilidad de los datos. Si se falla en uno, se falla en todo.
  - **La industrialización del ataque:**
    - *Antes de la IA*: los ataques de *phishing* masivos eran fáciles de detectar por errores y requerían programadores expertos.
    - *Con IA Generativa*: los atacantes usan LLMs para crear *phishing* hiperrealista y sin errores, y generan código de *malware* polimórfico que evade antivirus.

- **2. Principios de ciberresiliencia y defensa en profundidad**
  - **Concepto de ciberresiliencia:** cambiar la pregunta de "si seremos atacados" a "cuándo", enfocándose en la capacidad de volver a operar tras el golpe.
  - **Defensa en profundidad (Analogía de la cebolla):** comprender la seguridad en capas: Perímetro/Firewall (Capa 1), Endpoints/Antivirus (Capa 2) y Datos/Cifrado (Capa 3).
  - **Interacción de capas:** como se integran las capas: si el Firewall falla, el Antivirus debe detectar; si ambos fallan, se activa el Plan de Continuidad, cuando iniciar el proceso es vital.

- **3. Ejercicios prácticos / Casos de uso.**

2 MÓDULO 2: Aplicación IA: Scoring y vulnerabilidades

- **1. Metodología de identificación crítica de activos**
  - **Priorización:** no se puede proteger todo igual. Se enseña a definir Activos Críticos (AC) según el impacto:
    - *AC-C (Confidencialidad):* genera multas si se fuga (ej. PII).
    - *AC-I (Integridad)*: mata el negocio si se corrompe (ej. registros contables).
    - *AC-D (Disponibilidad):* detiene la operación si cae (ej. servidor web).

- **2. El poder del scoring de riesgo con IA**
  - **Problema:** el exceso de alertas en los escáneres de vulnerabilidades.
  - **Modelo híbrido:** la IA pondera la gravedad técnica (CVSS) junto con el contexto del negocio (si es un activo crítico) y la inteligencia de amenazas (si hay explotación activa).
  - **Resultado:** permite enfocarse en arreglar lo más peligroso en lugar de sólo "lo más afectado".

- **3. Detección de anomalías**
  - **Limitación de firmas:** los antivirus tradicionales fallan ante amenazas nuevas sin firma conocida.
  - **Machine Learning:** el sistema aprende el comportamiento normal (*baseline*) de cada usuario (ej. horarios, IPs, volumen de descarga).
  - **Detección:** identifica desviaciones (ej. accesos en horarios inusuales o descargas masivas) como anomalías de alta probabilidad, detectando amenazas de día cero.

- **4. Ejercicios prácticos / Casos de uso.**

3 MÓDULO 3: Aceleración: Respuesta e incidentes

- **1. El Playbook como primer auxilio**
  - **Concepto:** un "guión de supervivencia" para evitar el pánico y seguir procedimientos ciegamente.
  - **Estructura:** debe incluir nombre del incidente, equipo de respuesta, prioridad y pasos de contención para los primeros 30 minutos (ej. desconectar red, alertar usuarios, no apagar máquina para el forense).

- **2. Integración IA para respuesta automatizada (SOAR)**
  - **Necesidad:** la defensa humana es lenta contra ataques de IA; se requiere automatización.
  - **Funcionamiento:** el SOAR ejecuta el *Playbook* automáticamente. Ante una alerta de ataque de credenciales, puede suspender la cuenta y aislar el *endpoint* en menos de 5 segundos.

- **3. BCP y DRP**
  - **Diferenciación:**
    - *BCP (Continuidad)*: cómo operar manualmente o por vías alternativas si TI cae (ej. papel y WhatsApp).
    - *DRP (Recuperación)*: enfoque técnico, centrado en backups inmutables que no puedan ser cifrados por ransomware.

- **4. Ejercicios prácticos / Casos de uso.**

Medios de pago

- Tarjetas de crédito

  Si el pago con tarjeta de crédito se realiza mediante PayPal, puede existir algún cargo extra según el país de emisión de cada tarjeta.
- Contado o transferencia bancaria

  Si la transferencia se realiza vía Payoneer, puede existir algún cargo extra según el país desde donde se realiza la transferencia.
- Billeteras virtuales
- PayPal
- Consultar otros medios de pago vigentes al momento de la compra

Descuentos y promociones:

Descuentos por tiempo limitado. Consultá con nuestros asesores la vigencia de cada uno de ellos.

- Hasta **40% OFF** por inscripción temprana
- Uso de **KINES** como parte de pago
- **12 cuotas sin interés** con tarjetas bancarizadas
  Solo válido en Argentina.
- **20% OFF extra** por compra de formaciones *Live Class + On Demand*
- Descuento para grupos de **3 o más personas**

¡QUIERO CONOCER COSTOS!

kinetic
TRAINING