CCL | CÁMARA DE COMERCIO LIMA

Educación ejecutiva

CURSO DE ESPECIALIZACIÓN

Fundamentos de Ethical Hacking con ChatGTP

Certifica el Centro de Transformación Digital de la Cámara de Comercio de Lima

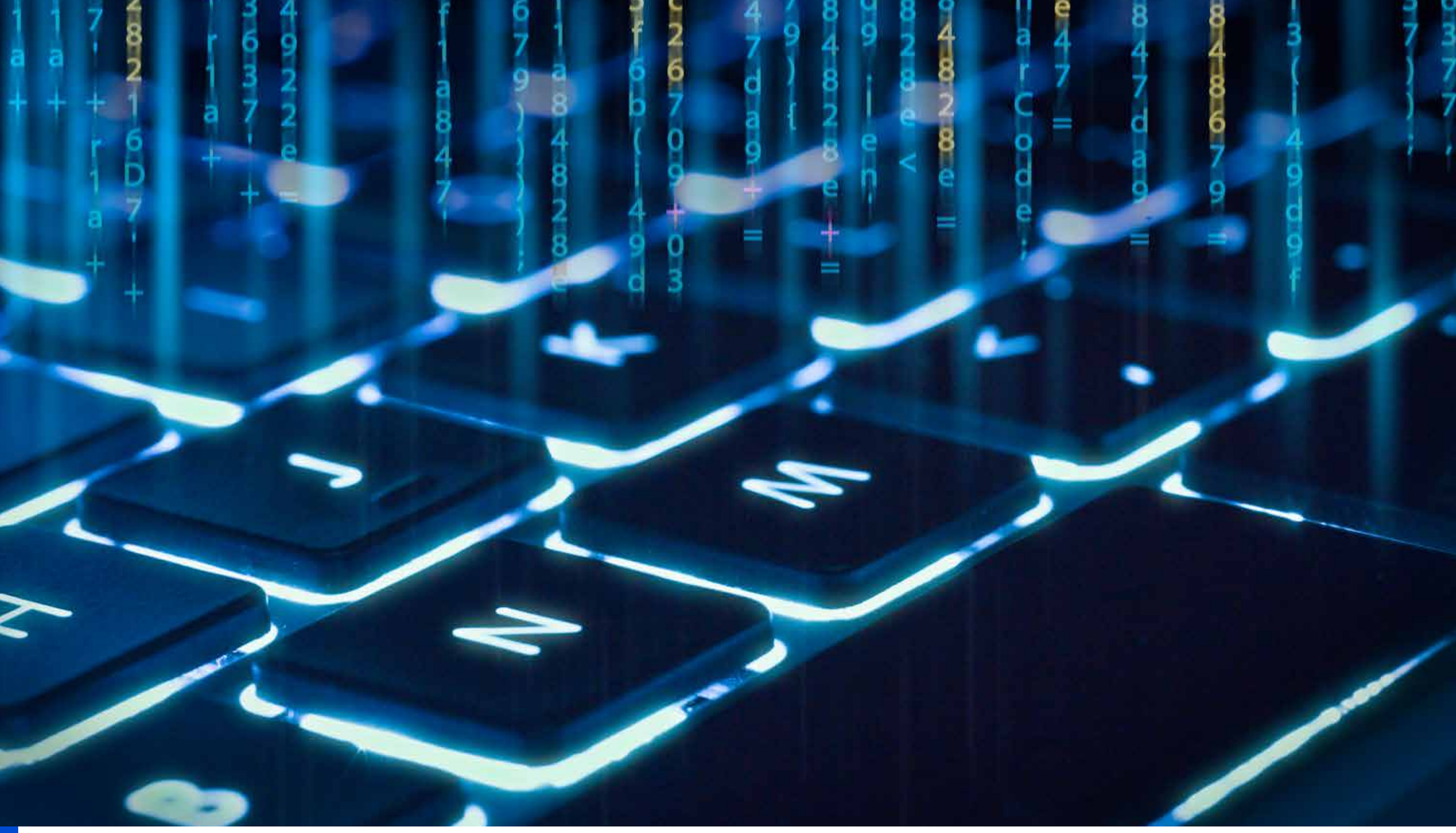
+30 AÑOS CAPACITANDO

INTRODUCCIÓN

La Cámara de Comercio de Lima presenta su nuevo Curso de Especialización en **Fundamentos de Ethical Hacking con Chatpt,** en Modalidad 100% Virtual.

El **Ethical Hacking** es una disciplina fundamental en el campo de la Ciberseguridad. Se centra en la identificación proactiva de vulnerabilidades y riesgos en sistemas informáticos, antes de que puedan ser explotados por actores maliciosos. Este curso te proporcionará las habilidades necesarias para realizar pruebas de penetración y simulacros de ataques bajo un marco legal y ético. Al dominar estas técnicas, desarrollarás la capacidad de detectar y remediar fallos de seguridad, protegiendo así la información crítica y los activos tecnológicos de tu organización.

Por otro lado, en este curso aprenderás a utilizar herramientas de Inteligencia Artificial como ChatGPT, para automatizar procesos, generar escenarios de ingeniería social, y apoyar en la exploración y explotación de vulnerabilidades. La integración de ChatGPT con Kali Linux, uno de los sistemas más robustos para pruebas de penetración, te permitirá ejecutar ataques simulados de manera más eficiente y sofisticada. Esta combinación de IA y herramientas de hacking ético le proporcionará un enfoque potente e innovador a tu formación en Ciberseguridad.



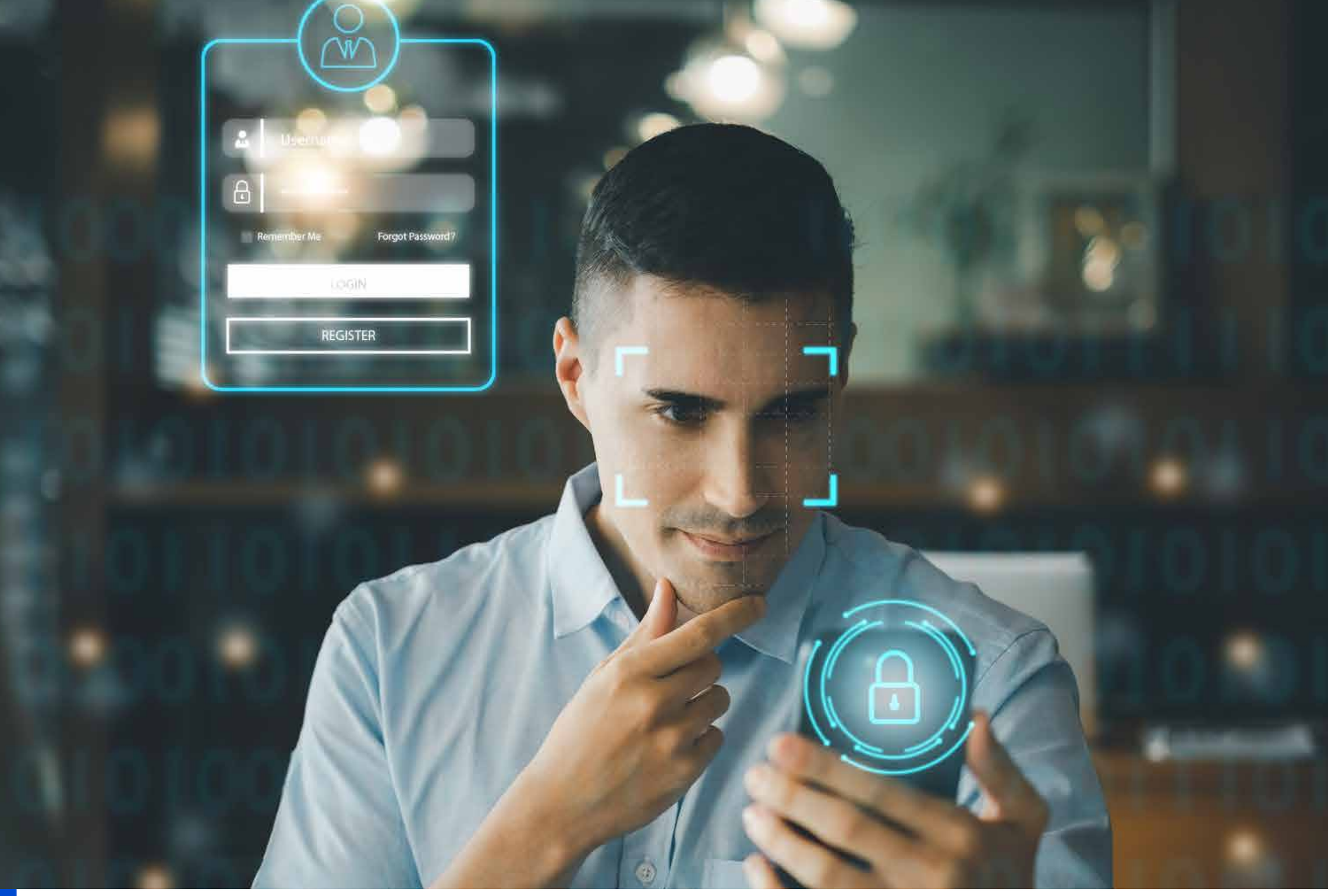
OBJETIVOS

- Dominar Metodologías de Hacking Ético: Aplicar marcos de trabajo reconocidos como MITRE ATT&CK para realizar análisis y pruebas de penetración estructuradas.

- Implementar IA en Ciberseguridad: Utilizar ChatGPT para automatizar tareas, ofrecer apoyo en ingeniería social, descubrimiento de contraseñas, y contramedidas contra ataques de inyección SQL y XSS.

- Integrar Herramientas Avanzadas: Aprender a combinar la funcionalidad de ChatGPT con Kali Linux, maximizando la eficiencia en simulaciones de ataques y evaluación de vulnerabilidades.

- Fortalecer la Ciberdefensa: Mejorar las estrategias y respuestas a incidentes, elevando la resiliencia de la organización frente a amenazas cibernéticas.



DIRIGIDO A

- Jefes y Gerentes de Sistemas y Tecnologías de la Información: Líderes que necesitan implementar y supervisar estrategias de seguridad robustas en sus organizaciones.

- Profesionales de TI y Gestores de Redes: Expertos que operan y mantienen la infraestructura de IT y requieren habilidades avanzadas para detectar y mitigar vulnerabilidades.

- Funcionarios de Cuerpos Policiales y del Ministerio Público: Personal dedicado a la investigación de delitos cibernéticos y computacionales que buscan actualizarse en las últimas técnicas de hacking ético y ciberseguridad.

TEMARIO

1. Metodología para Ethical Hacking

Revisión del Marco MITRE ATT&CK Este módulo introduce a los participantes en las metodologías fundamentales del ethical hacking, enfocándose en el marco de trabajo MITRE ATT&CK, una herramienta globalmente reconocida que describe las tácticas y técnicas utilizadas por los adversarios para infiltrarse en redes y sistemas. Los estudiantes aprenderán a mapear ataques, identificar posibles vulnerabilidades en sus sistemas, y desarrollar estrategias defensivas basadas en inteligencia de amenazas real y aplicable.

2. Beneficios y Limitaciones de ChatGPT

Integración de ChatGPT con Kali Linux En este módulo, se explorarán las capacidades y limitaciones de ChatGPT dentro del contexto de las pruebas de penetración. Se enseñará a los participantes cómo integrar ChatGPT con Kali Linux para optimizar las tareas de hacking ético. Los estudiantes experimentarán en tiempo real cómo la inteligencia artificial puede agilizar la recolección de datos, la generación de scripts y la automatización de ciertas tareas de hacking.

3. ChatGPT para Ingeniería Social

La ingeniería social sigue siendo una de las amenazas más significativas en seguridad informática. Este módulo se centra en cómo ChatGPT puede ser utilizado para simular ataques de ingeniería social, enseñando a los participantes a reconocer, replicar y responder a estas tácticas. Los ejercicios incluirán la creación de escenarios de phishing y otras formas de manipulación que los hackers podrían usar para explotar la confianza humana.

4. ChatGPT para Exploración de Contraseñas

Aquí, los estudiantes aprenderán cómo utilizar ChatGPT para apoyar en la exploración y cracking de contraseñas. El curso abordará técnicas de generación de listas de palabras clave, optimización de ataques de fuerza bruta y otros métodos asistidos por IA para descifrar contraseñas, destacando tanto la eficiencia como los desafíos éticos y legales relacionados.

5. ChatGPT para Realizar Inyección SQL, XSS

Este módulo enseña cómo ChatGPT puede ser usado para identificar y explotar vulnerabilidades de inyección SQL y XSS (Cross-Site Scripting). Los estudiantes aprenderán a construir consultas SQL maliciosas y scripts XSS con la ayuda de ChatGPT, mejorando su habilidad para probar y fortalecer la seguridad de las aplicaciones web.

6. ChatGPT como Mejora de la Ciberdefensa

El último módulo del curso enfatiza el uso de ChatGPT como una herramienta para mejorar la ciberdefensa. Los participantes explorarán cómo la IA puede asistir en el monitoreo continuo de sistemas, la detección de actividades sospechosas y la respuesta rápida a incidentes de seguridad. Se cubrirán temas como la automatización de respuestas a incidentes y la integración de ChatGPT en los flujos de trabajo de seguridad operacional.

EXPOSITOR

Mg. Ing. CIP Luis Gastulo Salazar

Sub Gerente de Seguridad Ofensiva en MiBanco

Ingeniero de Sistemas y cómputo de la Universidad Inca Garcilaso de la Vega, con grado de Magister en Ingeniería de Seguridad Informática de la Universidad Tecnológica del Perú. Así mismo, tiene el grado de Magister en Dirección de Tecnologías de información de la Universidad ESAN.

Se ha desempeñado anteriormente como, Jefe de Ciberseguridad, Aplicación y Datos en Banco Ripley Perú. Así mismo, como Jefe de Seguridad de la Información en el Ministerio de Educación.

DURACIÓN:

6 semanas

MODALIDAD:

100% virtual

INVERSIÓN:

Tarifa regular: S/ 720

Socio CCL: S/ 540

Importante: Cada participante debe asumir el costo USD 5 (costo referencial), utilizando su propia tarjeta de crédito/debito, para acceder a la Plataforma de OpenAI para los fines planteados en este curso.

CERTIFICA:

Centro de Transformación Digital de la Cámara de Comercio de Lima

MÉTODOS DE PAGO

- **Depósitos o transferencia** Cuenta corriente en soles banco

Banco o agente BCP
193-1943271-0-99

Banco o agente Interbank
005-0000007180

Banco BBVA
0011-0130-0100003020

Banco Scotiabank
000-2019361

Todas nuestras cuentas están a nombre de **CÁMARA DE COMERCIO DE LIMA – Ruc:** 20101266819

- **Tarjeta de crédito** Podrá realizar sus pagos con rapidez y total seguridad.

1. Ingresar a nuestra página web: **www.camaralima.org.pe**
2. Buscar: **Pagos online,** parte superior derecha.
3. Ingresar **datos de la empresa y/o persona** que solicito el servicio.
4. Ingresar **datos de la tarjeta de crédito y detalle del servicio.**
5. Procesar pago.

   Luego de realizar el pago, enviar el voucher de pago indicando el RUC y/o DNI del depositante al **asesor educativo.**

Hasta 3 cuotas sin intereses* con tus tarjetas de crédito
(*)Preguntar por términos y condiciones

- **Billetera electrónica** Escanea y paga

Considerar

Los horarios que están en la programación de todos los eventos que se realice están sometidos a cualquier cambio por cualquier inconveniente que se presente. ***Los cambios de los horarios serán notificados con anticipación.**

CCL | CÁMARA DE COMERCIO LIMA

CONTÁCTANOS

knunez@camaralima.org.pe

955 226 744