Universidad CENFOTEC
SOMOS LO QUE SABEMOS

LIDERÁ LA DEFENSA CON IA: PROGRAMÁ EL FUTURO DE LA CIBERSEGURIDAD INTELIGENTE

TÉCNICO EN **OPERACIONES DE SEGURIDAD INTELIGENTES** (AI-SOC)

CONVERTITE EN EL ESTRATEGA QUE LIDERA LA CIBERDEFENSA MODERNA

En un entorno donde las amenazas evolucionan con rapidez, no basta con reaccionar: tenés que anticipar. Con el programa **Técnico en Operaciones de Seguridad Inteligentes**, te formarás para operar y optimizar Centros de Operaciones de Seguridad (SOC) integrando **Inteligencia Artificial** en cada fase de detección y respuesta.

Vas a ser un experto capaz de dominar telemetría inteligente, automatización con SOAR y caza de amenazas proactiva.

¿POR QUÉ ELEGIR ESTE TÉCNICO?

- **Dominio de IA aplicada:** Aprendé a integrar inteligencia artificial en el ciclo completo del SOC para detectar ataques sofisticados.
- **Automatización Avanzada:** Maximizá la eficiencia operativa mediante la orquestación y automatización con herramientas **SOAR**.
- **Simulación Real:** Vas a terminar tu formación con un proyecto final de **Simulación de SOC Autónomo.**
- **Especialización en Detección:** Potenciá tus habilidades en ingeniería de detección utilizando marcos internacionales como **MITRE ATT&CK.**
- **Conectividad con el Mercado:** Vas a estar listo para los roles más demandados por las organizaciones de alta exigencia tecnológica en Costa Rica.

HERRAMIENTAS DE ÉLITE QUE VAS A DOMINAR

- **Frameworks de Explotación (Metasploit/Powershell Empire):** Aprendé a ejecutar pruebas de penetración profesionales y controladas.
- **Escáneres de Vulnerabilidades de Élite:** Dominá herramientas industriales para identificar brechas en sistemas y aplicaciones.
- **Proxies de Intercepción (Burp Suite):** Analizá y auditá la seguridad de aplicaciones web a nivel de protocolo.
- **Scripting Ofensivo con IA:** Potenciá tus habilidades con Python y Bash asistido por IA para crear herramientas de ataque personalizadas.

Metodología XperiencEdAI by Universidad CENFOTEC

¿QUÉ HACE ÚNICO NUESTRO PROGRAMA?

Este programa representa la evolución total hacia las operaciones inteligentes, donde vas a dominar la tecnología:

- **IA en el ADN de la Ciberdefensa:** Mientras otros programas se limitan a enseñarte a leer alertas, acá vas a aprender a entrenar y utilizar Inteligencia Artificial y Machine Learning para predecir ataques antes de que sucedan. No solo operás herramientas, las hacés más inteligentes.
- **Enfoque en Ingeniería de Detección:** Te formamos en Ingeniería de Detección, dándote la capacidad de crear tus propias reglas y modelos en entornos de SIEM y Data Lakes, utilizando lenguajes avanzados como KQL y SPL.
- **Dominio Total de la Automatización (SOAR):** En el mundo real, el tiempo es oro. Este programa es el único que profundiza en la orquestación y automatización (SOAR), enseñándote a diseñar flujos de trabajo que responden automáticamente a incidentes, reduciendo el error humano y acelerando la respuesta.
- **Simulación de SOC Autónomo:** Vas a terminar tu formación operando un SOC de simulación real, donde vas a gestionar incidentes complejos de principio a fin, utilizando un stack tecnológico de élite (EDR, XDR, Threat Intelligence).
- **Alineación con MITRE ATT&CK®:** Toda tu formación está estructurada bajo el marco de MITRE ATT&CK, asegurando que tus habilidades hablen el mismo idioma que las mejores organizaciones de ciberseguridad del mundo.

LAS HABILIDADES QUE TE DIFERENCIARÁN EN EL MERCADO LABORAL

- **Operación de SOC Moderno:** Capacidad para gestionar plataformas SIEM y Data Lakes con visión estratégica.
- **Threat Hunting Proactivo:** Dominio de técnicas asistidas por IA para encontrar amenazas antes de que causen daño.
- **Análisis de Malware:** Uso de herramientas inteligentes para la clasificación y desarticulación de software malicioso.
- **Respuesta Ágil:** Liderazgo en la gestión de incidentes críticos como ransomware y amenazas persistentes avanzadas (APT).

¿QUÉ VAS A APRENDER Y DESARROLLAR?

CURSO	HERRAMIENTAS CLAVE
Arquitectura SOC y Telemetría Inteligente	Wireshark, Sysmon, Zeek
Ingeniería de Detección en SIEM y Data Lakes	Splunk, Elastic Stack, KQL/SPL
Análisis de Amenazas y Clasificación con IA	Copilotos de seguridad, APIs de LLM
Análisis de Malware Asistido por IA	Flare-VM, Remnux, Sandboxes
Detección y Respuesta en el Endpoint (EDR/XDR)	Wazuh, SentinelOne, Crowdstrike
Inteligencia de Amenazas y Marco MITRE	MISP, OpenCTI, MITRE ATT&CK
Orquestación, Automatización y SOAR	Shuffle, n8n, Tines
Respuesta a Incidentes y Gestión Ágil	TheHive, Jira, Slack/Teams
Threat Hunting Proactivo con IA	Velociraptor, Jupyter Notebooks
Proyecto Final: Simulación de SOC Autónomo	Stack completo (SIEM, EDR, SOAR)

INFORMACIÓN DEL PROGRAMA

Cursos:	10
Créditos:	10
Duración:	1 año (12 meses)
Modalidad:	Virtual en vivo

PERSPECTIVA LABORAL Y EMPLEABILIDAD

- **Empleo: 97%.**
- **Desempleo: 3%.**
- **Tiempo promedio para emplearse: 2 meses.**
- **Demanda Global:** La ciberseguridad es una de las áreas con mayor escasez de talento y mejores salarios.
- **Crecimiento:** Las empresas priorizan profesionales que dominen IA para optimizar sus costos de defensa.
- **Proyección:** Accedé a oportunidades de teletrabajo para empresas multinacionales desde el primer año.

¿DÓNDE PODÉS TRABAJAR Y EN QUÉ ROLES?

Como egresado de este técnico, estarás listo para asumir posiciones estratégicas como:

- **Analista de SOC L2.**
- **Ingeniero de Detección.**
- **Threat Hunter Jr.**

NUESTROS EGRESADOS NO SON USUARIOS DE LA TECNOLOGÍA: LA CREAN, LA TRANSFORMAN Y LIDERAN SU EVOLUCIÓN

www.ucenfotec.ac.cr
info@ucenfotec.ac.cr
Teléfono: +506 4000 3950
+506 6000 8050
@UCenfotec