GIRONA NOTICIES.COM
+ Periodisme

QuantiKa14 publica el curso de OSINT 2025

Actualidad Empresarial | 19/07/2025 | 00:00

La tercera edición del curso “Investigación OSINT Avanzada”, dirigido por Jorge Coronado, está consolidándose como una de las formaciones más completas y especializadas en el ámbito de la inteligencia de fuentes abiertas en el entorno hispanohablante. Coronado, perito judicial en informática, docente universitario y CEO de QuantiKa14, ha diseñado un programa que aúna metodología, tecnología propia y casos reales, ofreciendo una experiencia formativa de alta aplicabilidad tanto para el sector público como para el privado.

Con un enfoque eminentemente práctico, más del 70% los contenidos están basados en ejercicios, simulaciones y escenarios reales. Este enfoque ha atraído en sus tres ediciones a profesionales de élite de distintos ámbitos: miembros del Grupo de Acción Rápida (GAO), la Unidad Central Operativa (UCO), el Centro Nacional de Inteligencia (CNI), el Centro Criptológico Nacional (CCN-CERT), así como más de 120 detectives privados, periodistas y analistas de inteligencia. La diversidad y el perfil profesional del alumnado enriquecen el curso y generan un entorno de aprendizaje colaborativo y transversal.

Uno de los aspectos diferenciales de esta formación es la incorporación de herramientas desarrolladas por el propio Jorge Coronado, como el bot de Telegram Dante’s Gates o la herramienta Guasap Forensic, utilizadas activamente en investigaciones reales. Los participantes tienen acceso a estas plataformas durante el curso, lo que les permite no solo conocer su funcionamiento técnico, sino también aplicarlas en contextos operativos. Además, el curso proporciona licencias de uso para otras soluciones OSINT como IntelRTV, y acceso a contenidos exclusivos que incluyen informes, casos de estudio y materiales complementarios.

El programa está estructurado en varios módulos progresivos. El primero de ellos introduce los fundamentos del OSINT y las bases del anonimato digital, incluyendo la configuración de entornos virtualizados y el uso de alias seguros para el correo electrónico. Le siguen sesiones dedicadas a la seguridad en redes sociales, donde se analizan plataformas como LinkedIn, Facebook, Telegram, WhatsApp, Twitter e Instagram, abordando aspectos de privacidad, configuración segura y detección de amenazas.

En la segunda parte del curso, se profundiza en el uso de herramientas de búsqueda y análisis de información, incluyendo motores especializados como DeDigger, WorldCat, OCCRP Aleph, PublicWWW o SearchCode, entre otros. También se trabaja con herramientas de forense digital como Maltego y Spiderfoot, y se realizan ejercicios prácticos para detectar vulnerabilidades, filtrar información crítica y estructurar hallazgos de forma efectiva.

Una de las secciones más valoradas por los alumnos es la que se centra en la ciberinvestigación aplicada a casos reales. A lo largo de estas lecciones, se estudian técnicas de identificación de

perfiles falsos, patrones de fraude digital como las estafas del amor o el fraude del CEO, y estrategias de documentación y seguimiento utilizando herramientas como PowerToys, PhantomBuster u Obsidian. También se aborda el análisis de huellas digitales mediante Dante's Gates, permitiendo a los alumnos trazar vínculos y comportamientos en distintos entornos online.

Otro bloque clave del curso es el dedicado al uso de NINT, Big Data y Data Science en el contexto de la inteligencia de fuentes abiertas. Se exploran herramientas como ChatGPT, Perplexity, ChatPDF y plataformas de reconocimiento visual como Carnet.ia. En esta fase, los alumnos aprenden a automatizar consultas, analizar grandes volúmenes de datos procedentes de canales y grupos de Telegram, y a visualizar sus resultados mediante herramientas como JupyterLab y Tableau. Esta parte del programa refuerza las capacidades analíticas del alumnado y les introduce en procesos de inteligencia apoyados en ciencia de datos.

También se incluye un módulo dedicado al ransomware y su análisis desde una perspectiva OSINT. Se revisan las principales familias de ransomware, se estudian sus patrones de comportamiento, y se presentan herramientas para el seguimiento de transacciones de criptomonedas asociadas a incidentes de secuestro de datos. Los alumnos acceden a informes sobre grupos como CONTI o LAPSUS$, y realizan ejercicios centrados en la trazabilidad de fondos y la comprensión del ecosistema cibercriminal.

La formación se completa con un módulo dedicado a la investigación de empresas. En este apartado, se trabaja sobre proyectos vinculados a criptomonedas, reputación de dominios, análisis de datos financieros y mercantiles, y detección de tipografías sospechosas (typosquatting). También se revisan indicadores bancarios como el SWIFT o el IBAN, y códigos BIN/IIN de tarjetas de crédito. Se utilizan fuentes abiertas y bases de datos públicas para realizar perfiles reputacionales de empresas e identificar vínculos de interés.

Uno de los grandes valores añadidos de este curso es el acompañamiento directo por parte de Jorge Coronado, quien mantiene una relación cercana con los alumnos y resuelve dudas de manera personalizada. Su experiencia como perito judicial y su participación en investigaciones mediáticas, como el reciente análisis forense de los audios del caso Koldo en el programa «Horizonte» de Cuatro, aportan una perspectiva realista y actualizada a todos los contenidos.

El curso está disponible en modalidad online y presencial, con una duración aproximada de dos meses. La superación del curso está condicionada a la realización de tres ejercicios prácticos y un test final. Los alumnos que lo completen obtienen una certificación avalada por QuantiKa14 y acceso a una bolsa de empleo exclusiva. Además, se ofrece la posibilidad de asistir a una comida de networking en Sevilla, valorada en 80 euros, con otros profesionales del sector y antiguos alumnos del curso.

Las plazas para cada edición están limitadas a entre 20 y 40 alumnos, precisamente para asegurar la atención personalizada y el aprovechamiento práctico de todos los contenidos. Actualmente, ya se está preparando la cuarta edición del curso, que incluirá nuevas herramientas, casos de investigación actualizados y mejoras en la plataforma educativa.

Las personas interesadas en participar pueden consultar toda la información actualizada en la web oficial del curso, www.cursodeosint.com, donde también se puede solicitar información sobre opciones de matrícula gratuita o financiada. Se trata de una oportunidad para adquirir competencias altamente demandadas en un entorno profesional cada vez más digitalizado y expuesto a riesgos cibernéticos.

En un contexto en el que la inteligencia de fuentes abiertas se ha convertido en una herramienta esencial para la seguridad, el periodismo de investigación, la detección de fraudes y la protección de derechos, el curso dirigido por Jorge Coronado ofrece una formación rigurosa, ágil y completamente alineada con las necesidades reales del mercado.

Autor: Redacció

https://gironanoticies.com/empresarial/274802-quantika14-publica-el-curso-de-osint-2025.htm