online
EN DIRECTO

Máster en
Cyber Threat Intelligence

- 2ª ED. CLASES ONLINE EN DIRECTO -

9 meses	Clases online en directo	Bolsa de empleo

KSCHOOL

www.kschool.com

online
EN DIRECTO

Máster en

Cyber Threat Intelligence

- 2ª ED. CLASES ONLINE EN DIRECTO -

Descubre el Máster en Cyber Threat Intelligence

En un mundo donde el peligro de las ciberamenazas avanza de manera vertiginosa y los atacantes adaptan sus tácticas, técnicas y procedimientos a los avances de las nuevas tecnologías, es vital contar con perfiles profesionales que sepan tratar y gestionar dichas amenazas de manera proactiva antes de que puedan suponer un riesgo para la empresa.

El valor que ofrece el analista de Cyber Threat Intelligence a cualquier empresa, es la seguridad de que se cuenta con un perfil capaz de detectar y analizar, a tiempo y de la forma adecuada, cualquier ciberataque. Además, este tipo de perfiles se encargan también de elaborar informes de Inteligencia enfocados a la toma de decisiones frente a ciberamenazas concretas en base a las necesidades de un cliente, proveedor o de la propia empresa.

Para que diferentes perfiles profesionales puedan adquirir las competencias necesarias para hacer frente a todo tipo de ciberamenazas, desde KSchool hemos desarrollado esta formación con una doble perspectiva:

· **Cyber Threat Intelligence técnico**, que capacita al alumno para aplicar distintas técnicas de detección y análisis de amenazas utilizando diversas fuentes de Inteligencia a bajo nivel técnico. También se aprenderá a desarrollar pequeñas automatizaciones en Python que ayuden en la recolección y tratamiento de la información.

· **Cyber Threat Intelligence analítico**, que capacita para la comprensión de las ciberamenazas desde todos los ángulos, lo que permitirá disponer de una visión 360 grados sobre cómo pueden afectar éstas dentro de un ecosistema empresarial concreto.

Objetivos

1. Adquirir los fundamentos del Cyber Threat Intelligence (incluyendo el Ciclo de Inteligencia, categorización de las fuentes de información en función de su fiabilidad y credibilidad, disciplinas de Inteligencia, TOP 10 de ciberamenazas, riesgos asociados a las ciberamenazas, etc).

2. Planificar y elaborar un producto de Cyber Threat Intelligence apoyándose en el Ciclo de Inteligencia.

3. Aplicación de metodologías reconocidas del mundo de la Inteligencia (Modelo diamante, Cyber Kill Chain, OPSEC, entre otros).

4. Tratamiento y análisis de amenazas usando estándares más utilizados para la compartición de información (STIX, TAXII, etc) y construcción de un modelado de amenazas.

5. Análisis profundo de los adversarios, sus TTPs y sus motivaciones.

6. Utilización de diferentes técnicas para la recolección y análisis de distintos tipos de datos asociados a amenazas nutriéndose de distintas disciplinas de Inteligencia (OSINT, SOCMINT, HUMINT), Deep Web y Dark Web.

7. Uso de técnicas de análisis de Inteligencia (generación de escenarios, ACH, mapas mentales, generación de hipótesis, SNA, análisis de campañas de desinformación).

8. Detectar, analizar y mitigar ciberamenazas desde la perspectiva defensiva y desde los distintos niveles de Inteligencia (estratégico, táctico y operacional).

9. Creación de un informe de Cyber Threat Intelligence adaptado a las necesidades reales del decisor y enfocado al interlocutor idóneo.

10. Creación de pequeñas automatizaciones en Python para el eliminar tareas repetitivas y generación de Playbooks más avanzados mediante SOAR.

Requisitos técnicos

Para poder seguir este máster solo necesitarás un ordenador, puede ser Windows o Mac, y conexión a Internet. No es necesario contar con requisitos técnicos específicos en el ordenador ya que durante el desarrollo del máster te proporcionaremos una máquina virtual en la nube.

Ten en cuenta que para poder seguir el curso y realizar los ejercicios prácticos es necesario disponer de un ordenador en el que cuentes con todos los permisos de administración que te permitan instalar los programas que se utilizarán durante las clases.

Perfil del alumno

Nuestro máster de CTI está dirigido a perfiles que quieran adquirir un conocimiento 100% práctico y enfocado al entorno laboral. No es necesario disponer de una titulación previa, pero sí que te interese el mundo de los ciber ataques, ya sea desde un punto de vista estratégico o más técnico. Para esta formación se recomienda tener nociones básicas de programación y muchas ganas de aprender.

Salidas profesionales

Al finalizar el máster, estarás preparado para trabajar como:

- Consultor de Ciberseguridad.
- Consultor de Ciberinteligencia.
- Analista de Blue Team.
- Analista de Cyber Threat Intelligence.
- Analista de SOC.
- Análista de Inteligencia.

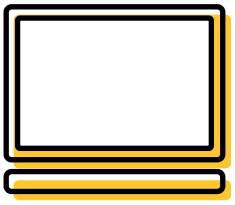
Modalidad Online

Lo mejor de nuestro presencial, ahora desde casa

El formato Online te permitirá vivir la experiencia presencial, desde tu casa: un profesor/a se conectará en directo para impartir su clase y responder preguntas y proponer ejercicios prácticos. Será como estar en KSchool pero desde la silla de tu escritorio.

CLASES EN DIRECTO en horario entre semana
+
¡GRABAMOS TODAS LAS SESIONES! Para que no te pierdas nada

ACCESO AL **CAMPUS VIRTUAL** para ver las clases y consultar material adicional, grabaciones y ejercicios.



ACCESO VITALICIO A LA **BOLSA DE EMPLEO** de KSchool.
+
INVITACIÓN A **EVENTOS EXCLUSIVOS** solo para alumnos.

Te esperamos en clase para que puedas aprender de la mano de los mejores profesores.

¿Estás preparado para convertirte en el mejor hacker ético? Elige tu futuro, ¡qué nosotros te ayudamos a llegar a él!

Temario

01. Introducción al Cyber Threat Intelligence:

- Introducción a la Inteligencia
- Amenazas, vulnerabilidades y riesgos
- Metodologías de trabajo sobre amenazas
- Securización de las operaciones (OPSEC)
- Elementos clave en Cyber Threat Intelligence
- Estándares de compartición de información sobre amenazas
- Generación de avatares para la investigación
- Preparación de la máquina virtual

02. Recolección y obtención de información:

- Técnicas de obtención mediante buscadores
- Técnicas de obtención de información de fuentes abiertas: Infraestructuras tecnológicas
- Técnicas de obtención de información de fuentes abiertas: Sociedades
- Técnicas de obtención de información de fuentes abiertas: Individuos
- Técnicas de obtención de información de redes sociales
- técnicas de obtención de información de la Dark Web
- Tratamiento de evidencias

03. Tratamiento y extracción automatizada de información:

- Tratamiento de información mediante Linux
- Scripting con Python
- Introducción a Docker
- Integración de Bases de Datos mediante Docker y tratamiento automatizado mediante Python: MongoDB y ELK
- Tratamiento de información y automatización de Tor, Slack y Discord
- Tratamiento de información y automatización de Telegram
- Jupyter Notebook

04. Perfilado de actores y análisis de TTPs:

- Identificación y perfilado de actores de amenaza - Cibercrimen y Ciberterrorismo
- Identificación y perfilado de actores de amenaza - Hacktivismo y Ciberespionaje
- Inteligencia Artificial (IA) adaptada al reconocimiento de adversarios
- Introducción al análisis de TTPs con MITRE ATT&CK
- Análisis avanzado de TTPs con MITRE ATT&CK
- [Master Class] Perfilado de actores desde el punto de visto de la criminología
- Modelado de amenazas
- Framework TIBER

05. Técnicas de análisis de Inteligencia:

- Introducción a las técnicas de análisis de Inteligencia clásicas
- Introducción al Social Network Analysis (SNA)
- Social Network Analysis (SNA) mediante herramientas técnicas
- Introducción a la desinformación
- Casos prácticos sobre desinformación
- Verificación y atribución de contenidos
- [Master Class] Análisis de campañas de desinformación y geopolitica

06. Técnicas de detección y análisis de amenazas:

- Reglas de detección: SIGMA
- Reglas de detección: YARA
- Análisis defensivo
- Detección y análisis de botnets y C&C
- Análisis estático de malware
- Análisis dinámico de malware
- Introducción al Threat Hunting
- Plataformas sobre Threat Hunting: CALDERA
- Plataformas sobre Threat Hunting: HELK

07. Plataformas para el enriquecimiento de la información:

- Plataforma ATT&CK Workbench
- Plataformas de Threat Intelligence: MISP
- Plataformas de Threat Intelligence: OpenCTI
- Plataformas de malware
- Ecosistema TheHive
- Introducción a los playbooks con SOAR
- Generación de playbooks avanzados con SOAR

08. Elaboración del informe y difusión del producto de Inteligencia:

- Elaboración del informe.
- Difusión del producto de inteligencia.
- Threat Landscape.

09. Prácticas en Empresa (Optativas)

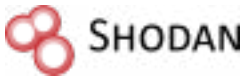
Trabajo de Fin de Máster

El TFM será en grupo y abordará una investigación de una amenaza a elegir por los alumnos o facilitada por el tutor que incluirá una sección que refleje un resumen de lo más importante de cada módulo. El TFM podrá ir realizándose poco a poco a medida que se avance por el programa.

Herramientas

En el Máster de Cyber Threat Intelligence aprenderás a utilizar con soltura las herramientas más demandadas en las ofertas de empleo:

STIX



Shodan

Censys

ZoomEye

Tor

Jupyter Notebook

Python

Herramientas del ecosistema MITRE

...¡y muchas más!

Profesores

Director del Máster en Cyber Threat Intelligence

Iván Portillo

Cyber Threat Intelligence Leader en beDisruptive e instructor de ciberinteligencia

Ángel Luis Veloy

Senior SOC Cyber-Security & Cyber-Intelligence Analyst en SIX

Nounou Mbeiri

Senior Cyber Threat Intelligence Analyst and MITRE ATT&CK Defender (MAD)

Francisco Carcaño

Cybersecurity - Threat Intelligence Team Lead at BABEL | CCII

Jezer Ferreira

OSINT Instructor de las FFCCS (Spain/LATAM/USA) e INTERPOL | OSINTOMÁTICO co-founder

Carlos Caballero

Threat Hunting en BBVA

Ainoa Guillén

Global Head of Cybercrime and Threat Intelligence Research en Cipher

Elena Casado

Cyber Threat Intelligence Operations Lead

Tabatha Torres

Analista de Inteligencia

Gonzalo Terciado

Analista de Inteligencia

Pino Penilla Marquínez

Cyber Threat Intelligence Analyst at BABEL Group

Jorge Testa

Global Cybersecurity Technology Researcher Lead en Cipher by Prosegur | Autor de “Killing The Bear”

Lórien Doménech

Principal Security Engineer

Carlos Galán

Associate Professor en Universidad Carlos III de Madrid

Pablo Bentanachs

EMEA Threat Intelligence Consultant at Recorded Future

José Luís Sánchez Martínez

Threat Researcher en VirusTotal

* El claustro de profesores puede sufrir modificaciones.

Inscripción y precio

1º. RESERVA DE PLAZA

500 €

2º. OPCIONES DE PAGO

Pago único
-5% de descuento

Ponemos a tu disposición las mejores alternativas para **financiar** el importe total de la formación. ¡Tú eliges!

Desde KSchool te ofrecemos dos opciones de financiación

KSCHOOL

Hasta 12 cuotas
sin intereses*

¿Necesitas más tiempo? Estudiaremos tu situación de forma **personalizada** para encontrar la solución más adecuada.

*Hasta 12 cuotas sin intereses: financiación a medida según el perfil crediticio del alumno. El 100% de las cuotas deberán de estar abonadas 30 días antes de la finalización del máster. El numero de cuota se adapta a 30 días antes de la finalización, al perfil crediticio y según la fecha de contratación.

Bonificable con FUNDAE

Todos nuestros cursos son bonificables a través de la **Fundación Estatal para la Formación en el Empleo** (FUNDAE, antigua FUNDACIÓN TRIPARTITA).

Si estás interesado coméntanoslo al hacer tu inscripción. Desde KSchool nos encargamos de la gestión para cursos o másteres de más de 60 horas.

Si nuestros planes de financiación o becas no se ajustan a tu situación, ¡escríbenos!

En KSchool **tratamos cada caso de forma personalizada**. Queremos que te formes con nosotros.

Bolsa de Empleo

En KSchool contamos con una Bolsa de Empleo propia donde las mejores empresas buscan talento.

Nos enorgullece decir que el 96% de nuestros alumnos están trabajando y que muchos de ellos consiguieron su primer empleo en el sector digital o lograron cambiar su puesto gracias a la Bolsa de Empleo.

Pero, ¿**cómo funciona** esta Bolsa de Empleo?

1. Tienes que ser alumno de KSchool
2. Entra a la plataforma y consulta las nuevas ofertas. Solo recibirás las que vayan dirigidas a tu área de formación. ¡Todo bien filtrado para que solo te lleguen las ofertas de empleo que de verdad te interesan!
3. Aplicas a la oferta y si todo va bien...
4. La empresa te contactará para que hagas una entrevista y puedas formar parte de su proceso de selección.
5. Este es el punto que más nos gusta: cuando os eligen para cubrir su vacante y nos escribís para contarnoslo :) ¡Es genial cada vez que un/a KSchoolero/a nos dice que tiene un nuevo trabajo gracias a la Bolsa de Empleo!

Eventos y networking

Además de poder aprender mucho en clase, desde KSchool os invitamos a eventos, masterclass, talleres y conferencias que os servirán para ampliar vuestros conocimientos y para contactar con grandes profesionales.

Síguenos a través de las redes sociales para estar al tanto de estas acciones y revisa tu mail. ¡Algunos de nuestros eventos son exclusivos para alumnos!

Preguntas frecuentes

Para resolver cualquier duda podéis escribirnos a **admisiones@kschool.com** o llamarnos al **91 910 09 54**, pero a continuación recogemos algunas de las preguntas que más nos hacéis. ¡Esperamos que os sean de ayuda!

¿Qué diferencias hay entre la modalidad presencial y Online?

La principal, el formato presencial requiere que acudas a clase, por lo que solo podrás cursarla si estás en Madrid o Barcelona, y siempre que tengas disponibilidad los viernes por la tarde y sábados por la mañana.

El formato Online es para todos aquellos que tengan una buena conexión a internet, ya sea desde Granada, Teruel o Cuenca. Las clases se imparten entre semana a partir de las 18:30 horas.

¿Qué pasa si no puedo acudir a una clase?

En la modalidad Online las clases quedan grabadas, ¡así que podrás verla en cualquier otro momento!

¿Para qué sirve el Campus Virtual?

Desde Campus Virtual podrás acceder a las clases en directo y volver a ver las grabaciones. Encontrarás ejercicios y materiales complementarios para que puedas mejorar tus habilidades y conocimientos. Además, también tendrás acceso a las presentaciones que los profesores utilizarán en sus clases y podrás comunicarte con tus compañeros y profesores para resolver dudas a través de los foros que se incluyen en él.

¿Hay exámenes?

¡No! Durante las clases realizaréis ejercicios prácticos y en la plataforma virtual podréis seguir practicando para adquirir los conocimientos necesarios para superar el máster.

¿Necesito un título universitario para cursar un máster en KSchool?

No, no necesitas ningún título previo. Existen formaciones donde si es necesario contar con unos conocimientos básicos, pero no te preocupes por esto ya que antes de realizar la reserva te preguntaremos por tu preparación previa y si fuese necesario te solicitaríamos el CV. ¡Queremos que aproveches al máximo tu paso por KSchool!

Los números de KSchool

Nacimos en 2011 con una idea en la cabeza: formar a los nuevos perfiles profesionales que la red demanda de forma constante y hacerlo de la mejor forma posible. Por ello, nos definimos como “La escuela de los profesionales de Internet”.

La experiencia y los grandes profesionales con los que contamos como profesores nos avalan. Como siempre decimos, en ciertos sectores a día de hoy, el valor no lo aporta un título si no lo que el profesional sabe hacer.

DESDE 2011
FORMANDO PERFILES

+6.000
ALUMNOS
HAN PASADO POR NUESTRAS AULAS

3
MODALIDADES
DE FORMACIÓN: PRESENCIAL, ONLINE E HÍBRIDA

+60
EDICIONES
EN ALGUNOS DE NUESTROS PROGRAMAS

+20
PROGRAMAS
¡PARA QUE ELIJAS TU FUTURO!

+ 1.600
EMPRESAS
HAN BUSCADO TALENTO EN NUESTRA BOLSA DE EMPLEO

Tenemos **experiencia**, los mejores y más actualizados **programas de formación**, y a los **profesionales** más reconocidos del sector impartiendo clases en nuestras aulas.

Manifiesto

- Si el sistema no está preparado para darnos el conocimiento que necesitamos lo vamos a conseguir por nuestra cuenta.
- Hoy, en ciertos sectores el valor no lo aporta un título. Lo aporta lo que cada profesional sabe hacer.
- Si dependemos de nosotros mismos, vamos a pensar por nosotros mismos.
- No queremos, ni podemos sentarnos a esperar a que alguien se fije en nosotros.
- No hay ningún mapa. Debemos hacer nuestro camino, y es un camino que muchas veces no ha sido explorado, pavimentado, ni señalizado.
- Nuestro conocimiento es la clave de nuestro desarrollo personal y profesional.
- Todo el mundo tiene algo que enseñar. Queremos aprender todos de todos.
- En el mundo del conocimiento, cuanto más se comparte más se tiene.
- Lo que aprendemos es lo que practicamos.
- Especializarse es ponerle un apellido a nuestra profesión. Es echarle especias a nuestro ingrediente principal.
- Queremos construirnos un futuro fuera del rebaño. Para eso vamos a pensar y hacer las cosas de forma diferente.
- No vamos a seguir instrucciones a ciegas, no vamos a ser pelotas, no vamos a mantener la cabeza agachada. Esas formas no van con nosotros.
- Vamos a estar siempre en movimiento. No vamos a parar de movernos. Somos inquietos, y nos gusta ser así.
- Como queremos resultados diferentes, vamos a hacer las cosas de forma diferente.
- Las pirámides son monumentos funerarios. Nos divierte verlas en los libros de historia, no sufrirlas en nuestro trabajo.
- Nuestro mercado no es el de los empleos. Es el de las oportunidades.
- Queremos colaborar con nuestras empresas a generar ingresos, no queremos tener un simple empleo.
- Queremos avanzar elaborando mejores recetas, no cocinando más.
- Queremos poner vida a los años, no solo años a la vida.
- Somos mucho más que un perfil y unas competencias. Somos algo más que las hojas de nuestro CV.
- Queremos levantarnos con ilusión los próximos 40 años. Queremos hacer las cosas con pasión, cariño y humanidad.

Contacto

No te quedes con ninguna duda, estamos aquí para ayudarte. Llámanos o escríbenos y tendremos una conversación personalizada contigo, ¡nos encanta conoceros!

INFORMACIÓN KSCHOOL

admisiones@kschool.com
91 910 09 54