Introducción y objetivos generales

IMF Smart Education

I. Introducción y objetivos generales

1.1. Introducción general del módulo

En los últimos años se ha hablado mucho acerca de la ciberinteligencia. Esto es así porque los avances tecnológicos que se han venido dando en el campo de las comunicaciones han propiciado la obligación de plantear sistemas de protección orientados a que ese flujo constante de intercambio de información sea seguro.

¿Pero se sabe con certeza a qué se refiere uno cuando habla de ciberinteligencia?

La American Intelligence Group define la ciberinteligencia como: “La adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoye la toma de decisiones”.[1]

[1] American Intelligence Group. “Ciberseguridad”; s.f.

Para tomar consciencia de todo lo que abarca el estudio de la ciberseguridad hay que plantearse qué conocimiento es necesario tener para que el analista desarrolle su actividad, para salvaguardar la información y los canales de trasmisión. Para esto, también procede conocer en detalle cómo actúan los ciberdelincuentes y qué herramientas emplean para llevar a cabo sus ciberestafas.

Todo esto ha propiciado que dentro de cada SOC (o Centro de Operaciones de Seguridad) se hayan empezado a diversificar cada vez más las tareas de los equipos que están especializados en distintas funciones o amenazas. Ello convierte a los equipos de ciberinteligencia en un pilar clave para el resto de

áreas, puesto que es el encargado de conocer cada amenaza y proveer de toda la información posible al resto de analistas de ciberseguridad.

En este módulo, una vez se haya adquirido esta base de conocimientos, se avanzará en temas más técnicos dentro del mundo de la ciberinteligencia, como los diferentes tipos de fraude con vectores de entrada y las herramientas de difusión, además de la Deep Web entre otros temas.

CONTINUAR

1.2. Objetivos generales del módulo

1. Aprender a identificar los tipos de técnicas que usan los ciberatacantes para ejecutar sus ataques.

2. Conocer qué son los foros *underground* y qué tipo de información alojan, además de las funcionalidades de The Onion Router como red de comunicación.

3. Analizar en detalle los distintos tipos de ataques de *phishing* que existen.

4. Conocer el funcionamiento de un ataque de *phishing* a través de las evidencias, gracias al estudio del proceso completo y el análisis de la forma óptima con la que se pueden llevar a cabo este tipo de acciones.

5. Estudiar y comprender cómo se desarrolla una campaña *malware* a través de casos reales.