Universidad Zaragoza

Curso Académico: 2024/25

61087 - Ciberseguridad

Información del Plan Docente

Año académico: 2024/25
Asignatura: 61087 - Ciberseguridad
Centro académico: 110 - Escuela de Ingeniería y Arquitectura
Titulación: 658 - Máster Universitario en Ingeniería de Telecomunicación
Créditos: 3.0
Curso: 2
Periodo de impartición: Primer semestre
Clase de asignatura: Optativa
Materia:

1. Información básica de la asignatura

El objetivo principal de la asignatura es brindar al alumno una visión clara y detallada del ámbito de la ciberseguridad, haciendo especial hincapié en la detección de intrusos y en la construcción de un Centro de Operaciones de Ciberseguridad (SOC). La primera etapa de este enfoque consiste en la recogida y procesamiento de información, que abarca la recopilación de datos relevantes tanto de equipos como de tráfico de red y su análisis para identificar posibles amenazas. Estos datos pueden incluir flujs de red y logs de diferentes sistemas operativos, entre otros. Para gestionar eficazmente esta información, es fundamental contar con una infraestructura adecuada para un SOC, que centraliza el almacenamiento y la monitorización de la información. Dentro del SOC, la detección de intrusos y el Threat Hunting son actividades esenciales que permiten identificar comportamientos anómalos y amenazas activas mediante técnicas avanzadas de análisis, como la detección por Indicadores de Compromiso y la detección de anomalías con Machine Learning. Finalmente, la generación de alertas y la respuesta ante incidentes son componentes clave para mitigar rápidamente los efectos de un ataque, proporcionando notificaciones oportunas y acciones correctivas para asegurar la continuidad y seguridad de las operaciones.

2. Resultados de aprendizaje

HA_01: Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería de telecomunicación.
HA_07: Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos electrónicos y de telecomunicaciones, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
HA_13: Capacidad para diseñar y dimensionar redes de transporte, difusión y distribución de señales multimedia.
HA_15: Capacidad para modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.
HA_16: Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.
HA_17: Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de Internet de nueva generación, los modelos de componentes, software intermediario y servicios.
HA_18: Capacidad para resolver la convergencia, interoperabilidad y diseño de redes heterogéneas con redes locales, de acceso y troncales, así como la integración de servicios de telefonía, datos, televisión e interactivos.
CP_06: Autoaprendizaje permanente
CP_07: Capacidad para saber comunicar (de forma oral y escrita) las conclusiones- y los conocimientos y razones últimas que las sustentan- a públicos especializados y no especializados de un modo claro y sin ambigüedades.

3. Programa de la asignatura

1. Introducción a la Ciberseguridad: Cobertura de conceptos fundamentales, importancia, principales amenazas, vulnerabilidades y mecanismos básicos de protección. Se estudian ciberataques históricos y marcos legales.

2. Recogida y Procesamiento de Información: Técnicas y herramientas como Zeek, Sysmon y Osquery para monitorizar flujos de red y recolectar datos de sistemas operativos, identificando amenazas.

3. Infraestructura para un SOC: Construcción y configuración de un SOC con Elastic Stack, incluyendo Elasticsearch, Logstash, Kibana y Beats.

4. Detección de Intrusos y Threat Hunting: Técnicas avanzadas para la detección de intrusos y caza de amenazas en tiempo real con Elastic Stack.

5. Generación de Alertas y Respuesta ante Incidentes: Configuración de alertas y desarrollo de planes de respuesta para gestionar incidentes de seguridad.

4. Actividades académicas

Clase magistral participativa (10 horas). Exposición por parte del profesor de los principales contenidos de la asignatura, combinada con la participación del alumnado.
Prácticas de laboratorio (20 horas). Los alumnos realizarán sesiones de prácticas de 2 horas de duración durante 10 sesiones.
Evaluación (3 horas). Conjunto de pruebas escritas teórico - prácticas y presentación de informes y/o trabajos utilizados en la evaluación del progreso del estudiante. El detalle se encuentra en la sección correspondiente a las actividades de evaluación.

5. Sistema de evaluación

El alumno podrá superar la asignatura mediante evaluación continua, consistente en la realización y entrega prácticas y la realización de una prueba de evaluación.
1. Las prácticas representarán el 70% de la nota final.
2. La prueba de evaluación representará el 30% de la nota final.

Para superar la asignatura por evaluación continua es necesario que la calificación de cada una de las partes sea superior a 3 puntos sobre 10, y que la media de todas las partes sea superior a 5.
El alumno que no haya superado la asignatura por evaluación continua dispondrá de una prueba global en cada una de las convocatorias establecidas a lo largo del curso. Las fechas y horarios de las pruebas vendrán determinadas por la Escuela. La calificación de dicha prueba se obtendrá de la siguiente forma:
E1: Examen final (100%). Puntuación de 0 a 10 puntos. Se trata de una prueba escrita que puede incluir tanto la resolución de problemas, pruebas prácticas en el laboratorio así como preguntas teóricas y prácticas formuladas en modo test u otro modo. Mediante esta prueba se evalúan todos los resultados de aprendizaje definidos para la asignatura.
Para superar la asignatura es necesaria una puntuación mínima de 5 puntos sobre 10 en E1.

6. Objetivos de Desarrollo Sostenible

9 - Industria, Innovación e Infraestructura