THE BRIDGE

Junta de Andalucía | Consejería de Empleo, Empresa y Trabajo Autónomo | Servicio Andaluz de Empleo

Defensa **Ataque**

Bootcamp de Ciberseguridad

- Aprendes
- Creas
- Te transformas

Formación **100% práctica** en ciberseguridad para dominar **Red Team y Blue Team** y desarrollar una visión completa de la protección digital. Se adquieren competencias en hacking ético, análisis forense y defensa frente a amenazas, construyendo una mentalidad crítica para trabajar en **protección digital de las empresas**

Visión general

En el Bootcamp en Ciberseguridad de The Bridge aprenderás todo lo necesario sobre **seguridad ofensiva y defensiva**, preparándote para proteger los activos más valiosos de cualquier organización.

Simularás ataques reales, aprenderás a responder ante incidentes, crearás campañas de phishing, analizarás malware y trabajarás como parte de un equipo Red Team o Blue Team.

Es el único bootcamp que te prepara para actuar como un profesional de ciberseguridad desde el primer día, con un **enfoque práctico, técnico y conectado** con la realidad del sector.

Serás capaz de detectar, prevenir y responder ante amenazas reales en entornos digitales.

Sea cual sea la dirección que más encaje contigo, este recorrido te permitirá avanzar con seguridad en el sector tecnológico.

En The Bridge creemos que aprender tecnología no tiene por qué ser frío ni solitario. Por eso este bootcamp combina exigencia técnica, claridad metodológica con **conexiones reales humanas y profesionales** auténticas que se construyen dentro y fuera del aula.

Estructura académica del programa

1 Introducción sistemas y lenguajes

En este bloque introductorio se verán las bases sobre los distintos sistemas operativos y lenguajes básicos, así como conocimientos iniciales de seguridad.

- Gestión y desarrollo de scripts en Bash para la automatización de tareas.
- Adquisición de conocimientos básicos sobre lenguaje JavaScript y HTML.
- Análisis de paquetes de red.
- Conocimiento sobre el modelo OSI, protocolos de comunicación típicos y su funcionamiento.
- Implementación de protocolos criptográficos y herramientas de seguridad.
- Conocimiento sobre los fundamentos de la seguridad informática, el pentesting y conceptos de análisis de vulnerabilidades.

2 Seguridad ofensiva

Desarrollarás las principales técnicas utilizadas en ejercicios de Pentesting y Red Team mediante la simulación de ataques. Este módulo incluye técnicas de descubrimiento, explotación y escalada de privilegios hasta movimientos laterales en entornos de Active Directory.

- Reconocimiento OSINT y análisis de objetivos para identificar vectores de ataque
- Ejecución de ataques y explotación de vulnerabilidades en sistemas, redes y aplicaciones
- Post-explotación, escalada de privilegios y evasión de defensas
- Análisis de riesgos, cumplimiento normativo y elaboración de informes técnicos
- Simulación de entornos reales con metodologías OWASP y MITRE ATT&CK

3 Seguridad defensiva

En este tercer bloque se introducirán las herramientas defensivas más utilizadas en equipos de Blue Team, incluyendo la protección activa de infraestructuras, detección temprana de amenazas y respuesta eficaz ante incidentes de ciberseguridad.

- Configuración de sistemas de protección de infraestructuras y segmentación de redes mediante herramientas Firewall.
- Despliegue de protección de aplicaciones web mediante herramientas WAF.
- Implementación de sistemas de detección de intrusiones (IDS/IPS) y protección en tiempo real a nivel de estación de trabajo (Antivirus y EDR).
- Gestión y correlación de eventos de seguridad mediante herramientas SIEM.
- Definición de equipos DFIR y elaboración del procedimiento de respuesta ante incidentes y análisis forense digital.

4 BridgeLab

El eje central de este módulo es el **Desafío de Tripulaciones**, un proyecto en el que se afronta un reto real planteado por una empresa real.

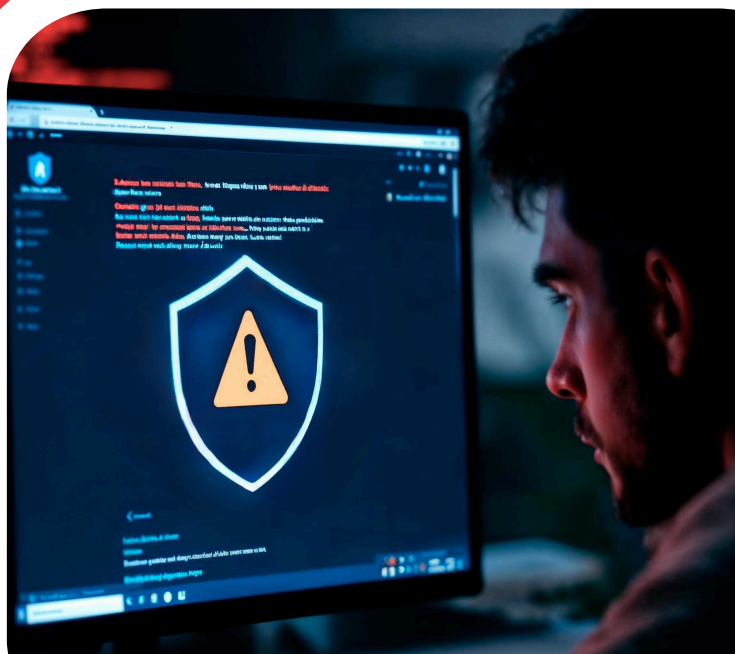
El trabajo se desarrolla en equipo, aplicando metodologías ágiles para construir un MVP a partir del briefing inicial, gestionando tiempos, prioridades y toma de decisiones en un contexto que reproduce dinámicas profesionales auténticas.

El producto digital se construye de forma colaborativa, integrando perfiles diversos y asumiendo responsabilidades reales dentro del equipo de trabajo.

El proyecto finaliza con la presentación y defensa de la solución, convirtiéndose en una evidencia tangible del trabajo realizado y en una pieza sólida para mostrar como parte de tu presentación profesional.

MÓDULO

Ciberseguridad ofensiva



Módulo: Ciberseguridad ofensiva

En este módulo te adentrarás en el mundo del hacking ético y las pruebas de penetración. Aprenderás a simular ataques reales para identificar vulnerabilidades en sistemas, redes y aplicaciones, así como a evaluar riesgos y proponer mejoras. Dominarás técnicas como el phishing, la creación de troyanos, análisis de redes inalámbricas y auditorías de apps Android.

Con este módulo aprenderás a:

- Realizar auditorías internas o externas para comprobar la seguridad de todo tipo de aplicaciones.
- Realizar informes técnicos y ejecutivos.
- Identificar riesgos potenciales a la seguridad y sus posibles mitigaciones o erradicaciones.
- Crear y desarrollar proyectos de seguridad informática y de las comunicaciones.
- Supervisar regularmente la seguridad de la red para estar informado de toda la actividad que se produce.
- Realizar pruebas de vulnerabilidad y análisis de riesgos para valorar y evaluar la seguridad actual y ver dónde hay que mejorar las normas.
- Realizar auditorías y evaluaciones de seguridad internas y externas, así como informar de los resultados y desarrollar planes.
- Desarrollar y aplicar las mejores prácticas de ciberseguridad.
- Discutir los puntos débiles y las mejoras del sistema con la dirección y el personal informático.
- Informar sobre las causas y recomendaciones de las violaciones de seguridad.
- Analizar la seguridad de aplicaciones Android y redes wireless.
- Crear troyanos y campañas de phishing para la evasión de defensas

MÓDULO

Ciberseguridad defensiva

Módulo: Ciberseguridad defensiva

En este módulo aprenderás a proteger sistemas y redes frente a ciberataques. Adquirirás las habilidades necesarias para detectar amenazas, responder a incidentes y mantener la seguridad operativa de una organización. Dominarás herramientas como firewalls, sistemas SIEM y técnicas de análisis forense.

Con este módulo desarrollarás la capacidad de: (1/2)

- Atender emergencias en materia de seguridad informática.
- Identificar riesgos potenciales a la seguridad, supervisar el uso de archivos de datos.
- Proteger activos de todo tipo.
- Realizar informes de análisis forense.
- Integrarse en cualquier equipo de respuesta ante incidentes.
- Regular el acceso para salvaguardar la información en archivos informáticos.
- Detectar y prevenir posibles amenazas o ciberataques.
- Conocer e interpretar las normativas de centros de respuesta a incidentes de seguridad.
- Supervisar regularmente la seguridad de la red para estar informado de toda la actividad que se produce.

Con este módulo desarrollarás la capacidad de: (2/2)

- Instalar, gestionar y actualizar el software de seguridad, como cortafuegos y encriptaciones.
- Asegurar que todo el software tiene implementadas las medidas de seguridad adecuadas.
- Realizar pruebas de vulnerabilidad y análisis de riesgos para valorar y evaluar la seguridad actual y ver dónde hay que mejorar las normas.
- Evaluar el cumplimiento de la organización con los requisitos reglamentarios y las normas del sector.
- Informar de los resultados y desarrollar planes.
- Actualizar el plan de recuperación de desastres de la organización.
- Garantizar que la organización tiene copias de seguridad en caso de ciberataque.
- Desarrollar y aplicar las mejores prácticas de ciberseguridad.
- Mantenerse al día sobre las tendencias, los avances y las mejores prácticas en materia de ciberseguridad.
- Analizar malware y cualquier tipo de objeto sospechoso o potencialmente peligroso.
- Conocer los fundamentos de los sistemas SIEM y trabajar en ellos.

SALIDAS PROFESIONALES

Roles a los que puedes aspirar

Al finalizar el programa de Ciberseguridad podrás proyectar tu desarrollo hacia perfiles especializados en seguridad ofensiva y defensiva, con una base sólida en sistemas, redes, análisis forense y gestión de la seguridad.

Seguridad Ofensiva (Red Team y Pentesting)

Perfiles orientados a identificar vulnerabilidades, simular ataques y evaluar la seguridad de sistemas y aplicaciones.

- Pentester
- Auditor/a de Seguridad Ofensiva
- Consultor/a de Seguridad de Aplicaciones Móviles
- Analista de Malware

Seguridad Defensiva y Operaciones (Blue Team / SOC)

Perfiles centrados en la monitorización, detección y respuesta ante incidentes de seguridad.

- Analista de Ciberseguridad
- Operador/a de Seguridad
- Técnico de incidentes SIEM
- Incident Response Lead
- Técnico de Ciberinteligencia

Análisis Forense y Respuesta a Incidentes (DFIR)

- Analista Forense Informático

Gobierno, Riesgo y Cumplimiento (GRC)

- Consultor/a Compliance de Seguridad

Arquitectura y Diseño de Seguridad

- Arquitecto/a de Ciberseguridad


THE
BRIDGE