

INICIO EN CIBERSEGURIDAD

ENTRA AL MUNDO H4CK3R SIN MORIR EN EL INTENTO



¿Quiénes somos?



ereina-I (Elena)

Formación en
Forense



frnavarr (Javi)

Formación en
Blue Team

Índice

- ¿Qué es la ciberseguridad?
- La actualidad en el sector
- Ruta de aprendizaje
- Áreas de la ciberseguridad
- Blue Team
- Red Team
- Forense
- Certificaciones
- Networking





¿Qué es la ciberseguridad?

Proteger todo lo que está conectado a Internet.

Datos personales, sistemas, redes y dispositivos.



Ejemplos de datos sensibles:

- DNI / NIF
- Tarjetas de crédito
- Contraseñas
- Historial médico



Ámbitos que abarca:

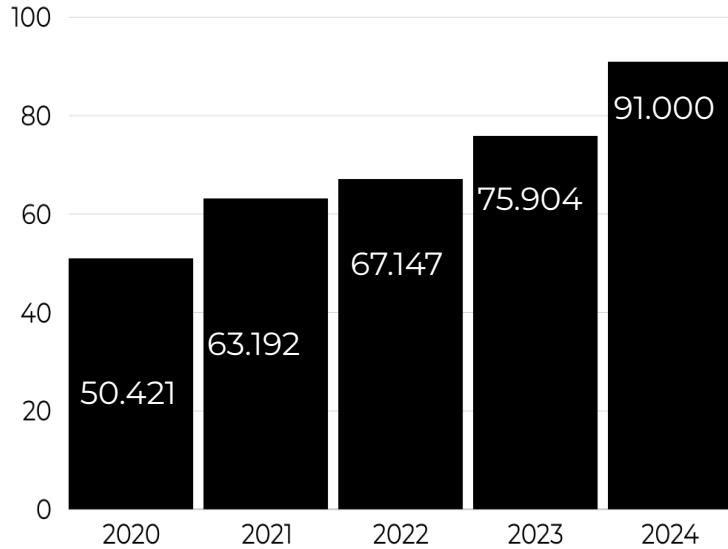
- Código y aplicaciones
- Bases de datos
- Infraestructura de red (WiFi, LAN corporativa)
- Dispositivos conectados

Ataques recientes en España

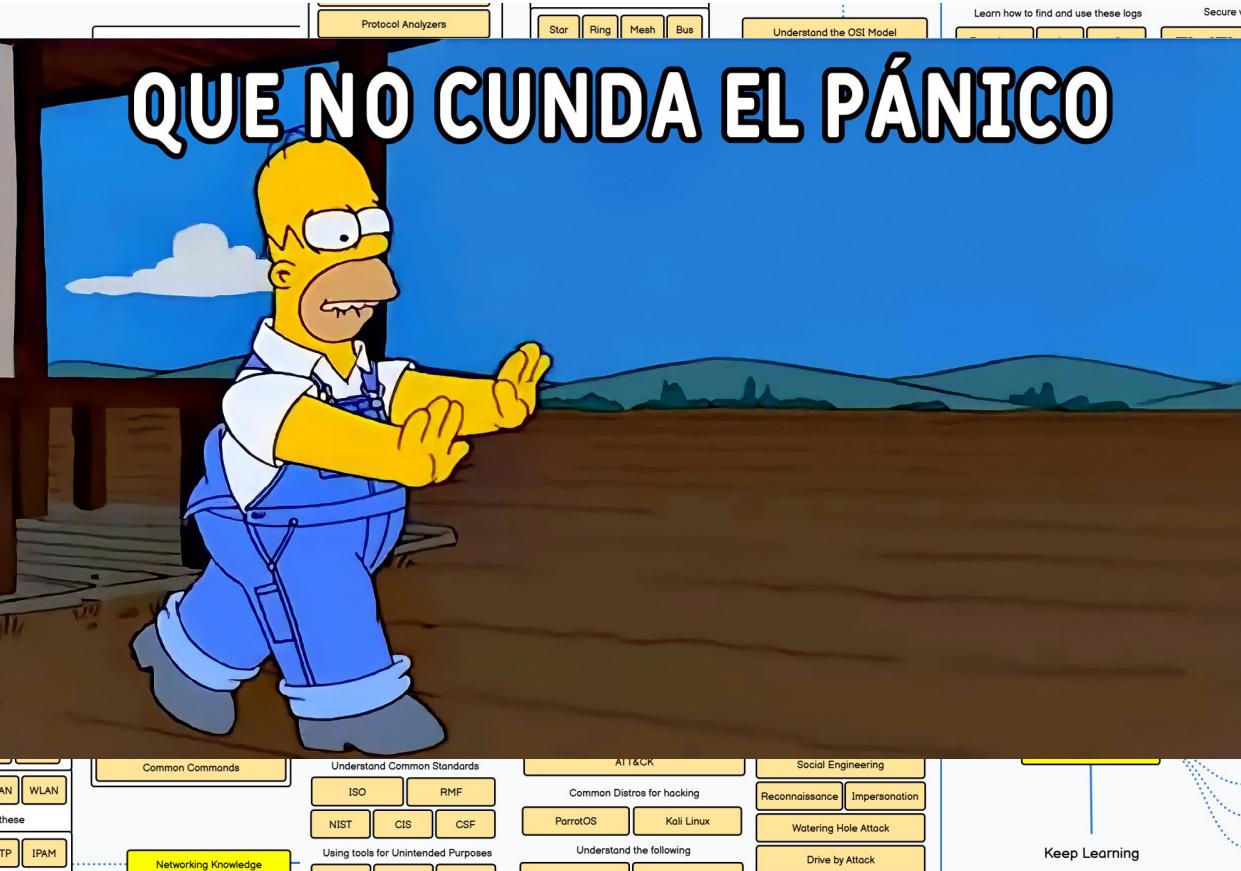


Mercado Laboral

Dentro de las grandes empresas, hay mucha demanda de talento. Además es el sector con más crecimiento dentro de la programación.



Cyber Roadmap



Fundamentos antes de empezar

Asegúrate de entender la base de:

Redes

- TCP/IP: Comunicación entre dispositivos
- DNS: Traducción de nombres de dominio
- HTTP/HTTPS: Protocolo web (seguro vs. no seguro)
- Firewall: Protección de redes



Sistemas Operativos

- Linux: Usado en servidores y ciberseguridad
- Windows: Plataforma más atacada



Programación Básica

- Python: Automatización y herramientas de seguridad
- Bash: Scripting en entornos Linux



Plataformas de estudio

Cursos de fundamentos teóricos:

Coursera, Udemy (cursos de Google, CISCO, AWS, Microsoft)



Academias online:

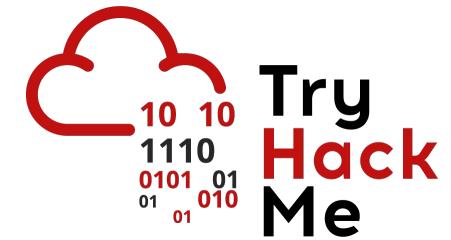
Mastermind, Hack4u

Canales de Youtube:

S4vitar, El Pingüino de Mario, Contando Bits, Hackavis

Laboratorios de aprendizaje práctico:

TryHackMe, HackTheBox, DockerLabs, Vulnhub



Áreas de la ciberseguridad

Red Team

- "Los atacantes éticos" (Pentesters, Red Teamer)
- Simulan ataques reales para encontrar vulnerabilidades.

Blue Team

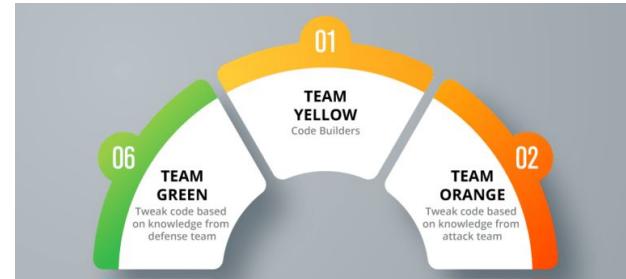
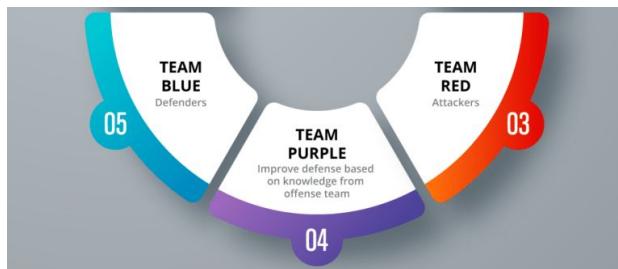
- "Los defensores" (SOC Analyst, Incident Responder, Threat Hunter)
- Detectan, responden y mitigan amenazas.

Forense Digital

- Análisis post-ataque.
- Recuperación de evidencia y reconstrucción de eventos.

Purple Team

- Colaboración entre Red y Blue
- Rol más estratégico y de comunicación.



Yellow Team

- "El arquitecto"
- Diseña y construye infraestructuras seguras.
- Roles: Security Engineer, Security Architect, DevSecOps.

GRC (Governance, Risk & Compliance)

- Enfocados en políticas, normativas y gestión de riesgos.
- Importante para empresas grandes y entornos regulados.

¿Qué es el Blue Team?



Defensores del sistema

Protegen la infraestructura frente a amenazas reales y simuladas.



Detectores de intrusos

Monitorean redes, sistemas y registros para identificar comportamientos anómalos.



Fortalecedores

Implementan medidas defensivas para prevenir, detectar y responder a ataques.



Ejemplo de actuación del Blue Team

Caso real

Un sistema SIEM* lanza una alerta por múltiples intentos de conexión SSH fallidos desde una IP externa (192.168.3.42) hacia un servidor Linux.

Análisis del evento

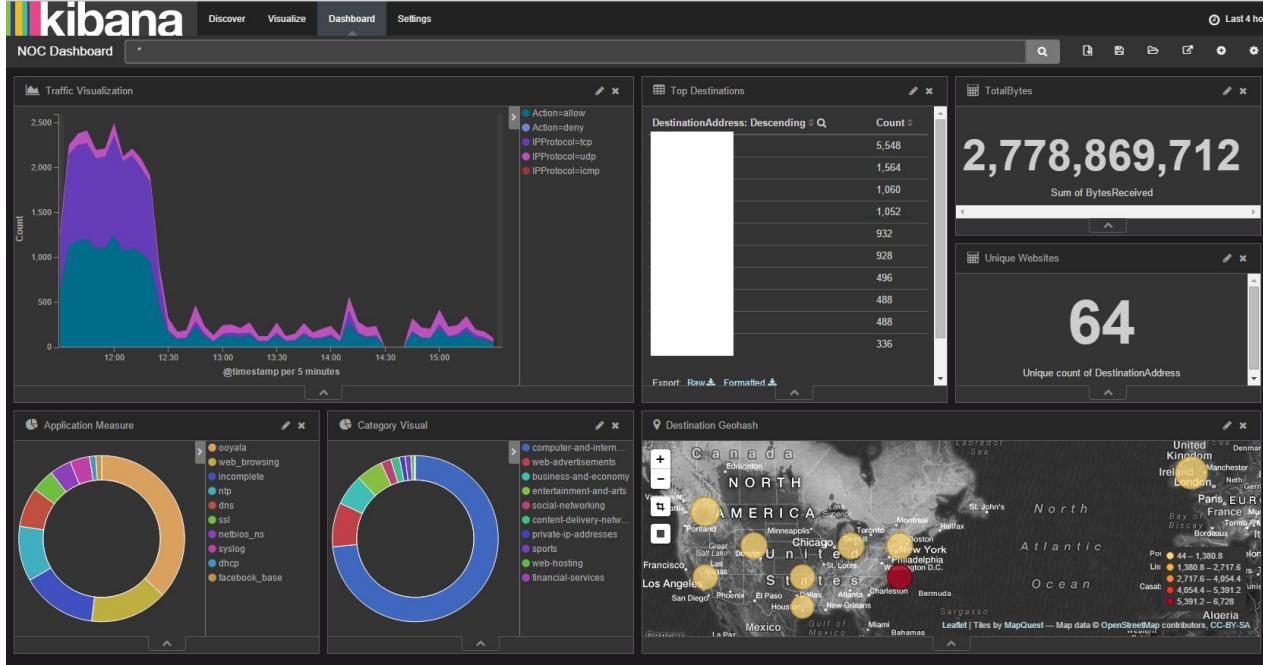
- Herramienta: Kibana (SIEM)
- El log muestra 15 intentos en menos de 2 min con usuarios inexistentes.
- Regla activada: *Brute-Force SSH* (*ID 5710*)

Respuesta del equipo Blue

- Bloqueo de la IP mediante Firewall
- Verificar la integridad del equipo afectado.
- Notificar al Red Team para simular ataques parecidos.

*SIEM (Security Information and Event Management) es el vigilante de seguridad digital de una empresa.

Herramientas del Blue Team



Esta imagen muestra un **dashboard de Kibana**, una herramienta clave para equipos Blue Team en monitoreo y análisis de seguridad. Se puede visualizar el tráfico de red en tiempo real.



Sirve para analizar el **tráfico de red**; captura y examina los paquetes de red.



La usan los de Threat Intelligence, sirve para crear **reglas** para detectar malware.

¿Qué es el **Red Team**?



Simuladores de ataques

Equipos ofensivos que emulan tácticas de hackers reales para descubrir vulnerabilidades.



Cazadores de fallos

Buscan debilidades en sistemas, redes y procesos antes que los atacantes.



Securizadores

Su objetivo es mejorar la seguridad identificando brechas explotables.



¿Qué hace el **Red Team**?



Reconocimiento

Identifican puntos débiles mediante técnicas avanzadas de escaneo.

Ingeniería social

Manipulan personal para obtener acceso no autorizado.

Explotación

Aprovechan vulnerabilidades para demostrar posibles compromisos.

Documentación

Reportan hallazgos detallados con recomendaciones.



Red Team

Roles y Herramientas

Roles Profesionales

- Ethical Hacker
- Pentester
- Red Teamer especializado en APTs
- Analista de malware



Herramientas más conocidas

- Kali Linux
- Metasploit Framework
- Cobalt Strike
- Nmap y Burp Suite
- BloodHound



Red Team

Empresas y Referentes del Sector

Empresas Líderes

- Offensive Security
- TrustedSec
- SpecterOps
- FireEye

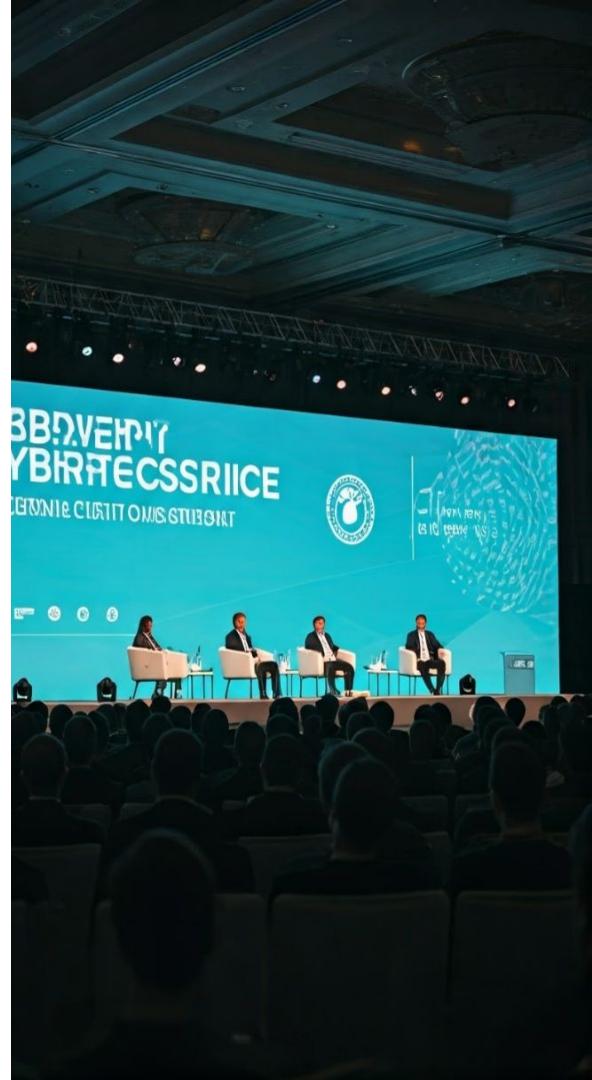
Figuras Destacadas

- Raphael Mudge (Cobalt Strike)
- Kevin Mitnick (Leyenda del hacking)
- Georgia Weidman (Autora experta)

En España, y que visitan 42 Málaga

 **DEKRA**

Hispasec]



Forense

¿Qué es la Informática Forense?

Disciplina que analiza dispositivos digitales (discos, USB, RAM, etc.) en busca de **evidencias** tras un incidente o delito.

Objetivo: **Preservar, analizar y reportar datos** sin alterar su integridad.

¿Qué son los Artefactos Forenses?

Elementos del sistema que registran actividad de usuarios y procesos.

Permiten:

- Reconstruir eventos (fechas, conexiones, ejecutables)
- Identificar usuarios/atacantes
- Detectar malware y persistencia
- Servir como prueba legal



Forense

¿Qué es DFIR?

DFIR = Forense Digital + Respuesta a Incidentes (Trabajan juntos para actuar rápido y preservar evidencias).

- **Forense Digital:** Recopila y analiza evidencias digitales.
- **Respuesta a Incidentes:** Detecta, contiene y mitiga ataques activos.

Proceso Forense Digital (NIST)

1. **Recopilación** (sin alterar datos)
2. **Examen** (búsqueda de indicios maliciosos)
3. **Análisis** (correlación de pruebas)
4. **Informe** (reporte técnico y legal)

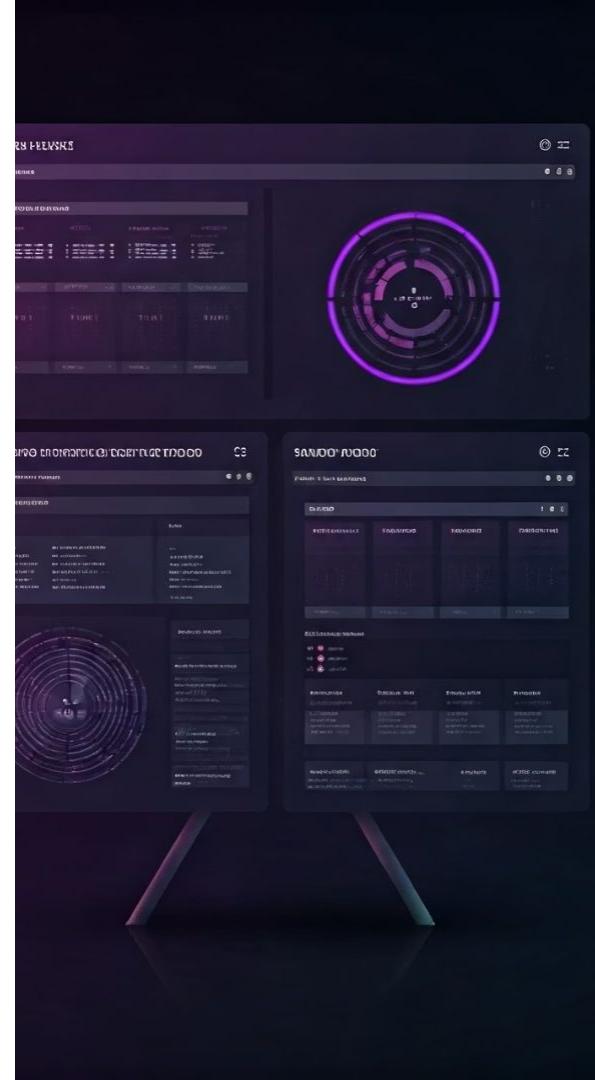
Proceso de Respuesta a Incidentes

1. Preparación
2. Detección y análisis
3. Contención
4. Erradicación
5. Recuperación
6. Revisión post-incidente

Forense

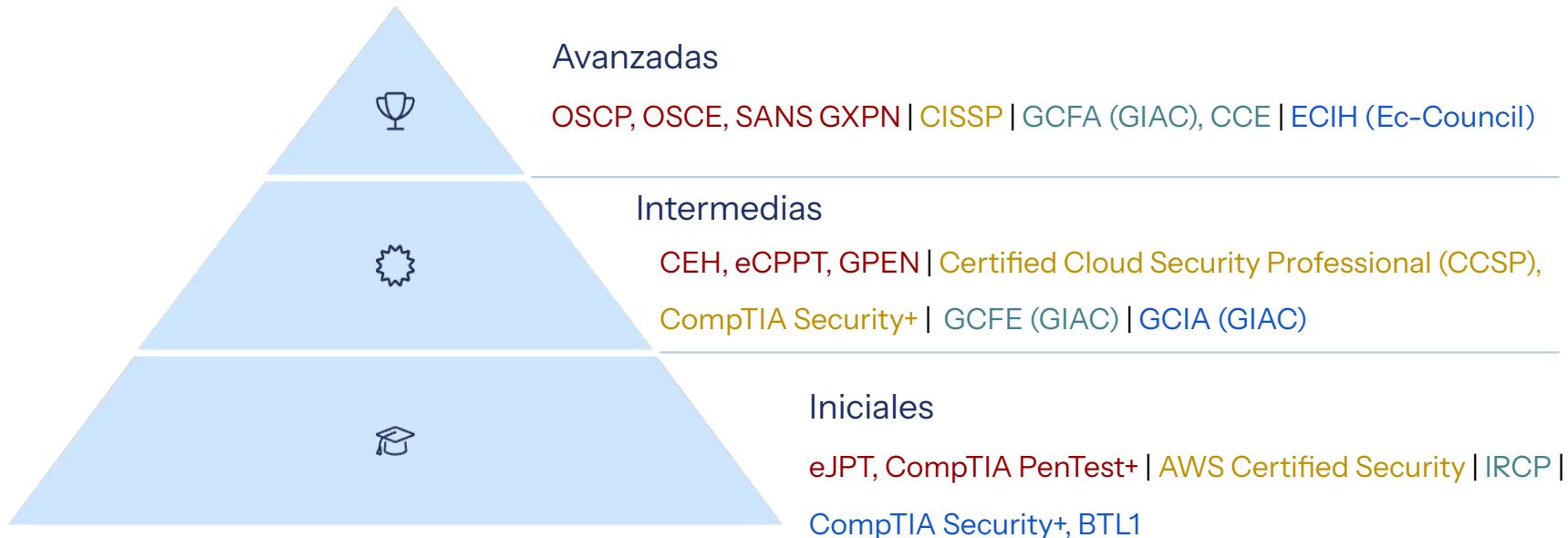
Herramientas clave para DFIR

- **Autopsy** analiza discos y archivos
- **Velociraptor** analiza datos en tiempo real en endpoints
- **Volatility** analiza la memoria RAM



¿Qué pide el mercado?

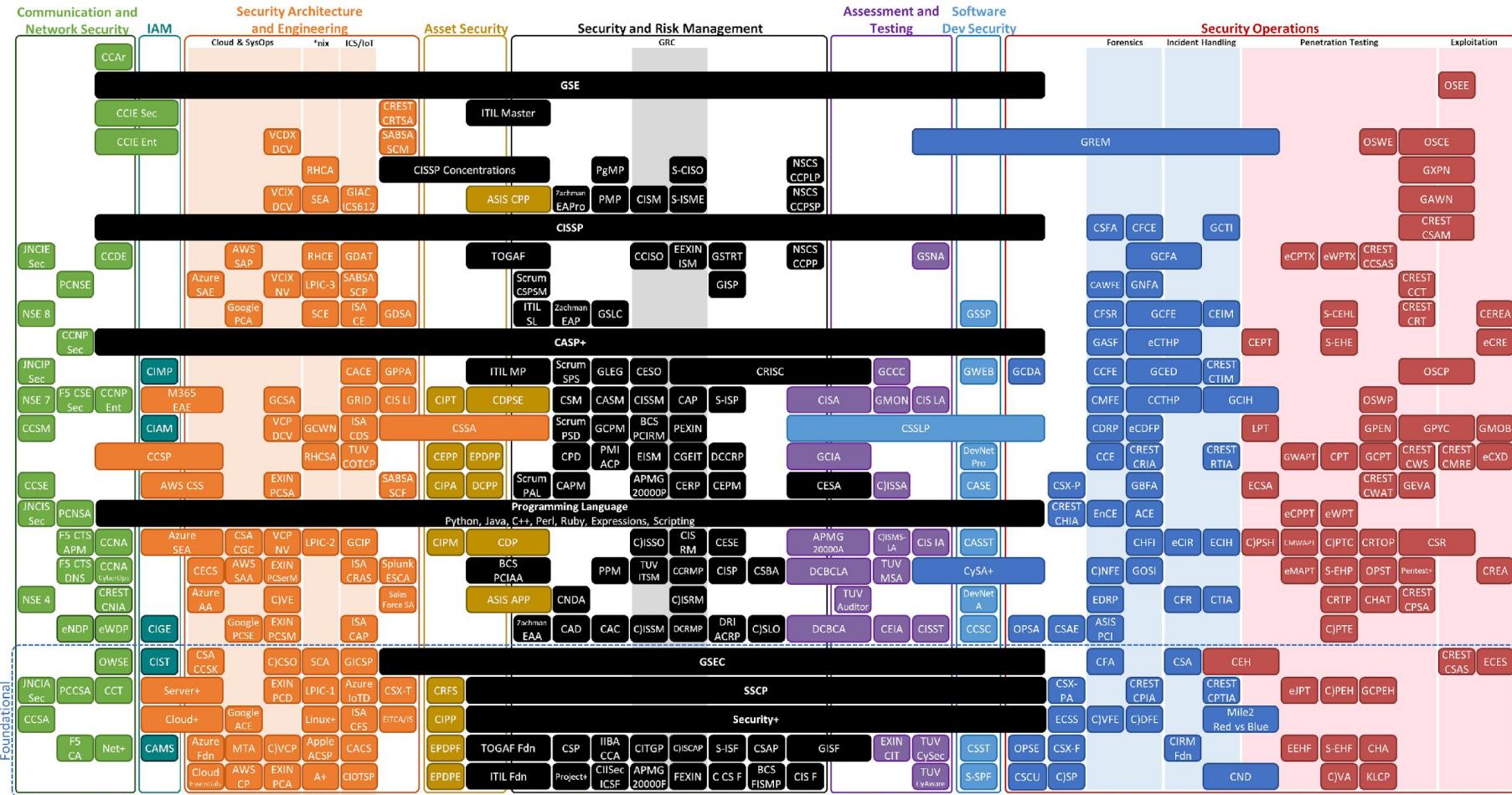
Formación y Certificaciones



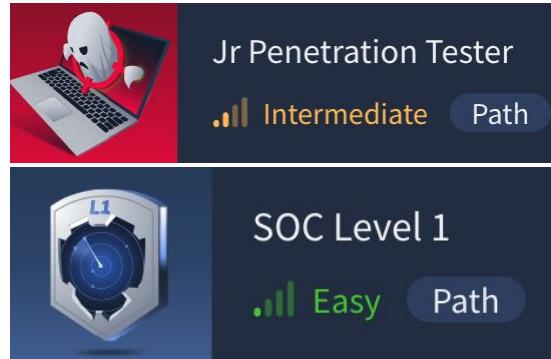
Security Certification Progression Chart 7.0

(ISC)² CBK Security Domain Alignment

More info @ www.pauljeremy.com/security-certification-roadmap | 356 certs listed | October 2020



Ruta de certificaciones que recomendamos



Networking

Participa en eventos (presenciales o virtuales)

Comparte lo aprendido (Linkedin, Blog, Notion ...)

Únete a conferencias (Empresas del PTA, Google GSEC, Incibe)

Asiste a congresos

Participa en Hackathons

Google Safety Engineering Center
Málaga



/Rooted®CON

Kahoot!

Q&A, os escuchamos

MUCHAS GRACIAS