



PUESTO: Analista Pentest - DFIR (Junior) (Referencia: 200129PTDF)

COMPAÑÍA: INCIDE

LUGAR: Barcelona (puesto presencial)

RANGO SALARIAL : 23k-27k (en función de experiencia y skills)

FECHA OFERTA: 29/01/2020

VACANTES: 1

Interesados, contactad a través de rrhh@incide.es

RESUMEN

INCIDE es una compañía proveedora de servicios DFIR y Red Team con base en Barcelona y más de 15 años de experiencia. Utilizamos esta experiencia y conocimiento acumulado para prestar a nuestros clientes servicios en las áreas de seguridad preventiva y ofensiva. Ayudándolos mediante la validación de sus configuraciones de seguridad, soporte a la detección y mitigación de amenazas mediante servicios de Threat Hunting y, en su caso, Respuesta a Incidentes de Seguridad. En el área ofensiva prestamos servicios de Pentest y Red Team para la validación de las configuraciones, procedimientos y adecuado uso de las tecnologías protección.

Los miembros del equipo de Red Team llevan a cabo ejercicios de ataque utilizando las mismas técnicas que los atacantes reales más avanzados con el objetivo principal de simulación de un ataque, lo más real posible, sin ser detectados por los equipos y sistemas de monitorización del cliente. Al mismo tiempo, los integrantes del grupo de DFIR realizan tanto pruebas atómicas dentro del ciclo de Threat Hunting que les permitan definir los IOCs adecuados para cada cliente desde un punto de vista forense como participarán en la atención de Respuesta a Incidentes.

Para poder llevar a cabo con éxito estas tareas es necesario tener una base de conocimientos técnicos de diferentes áreas, como redes, sistemas operativos, sistemas de detección perimetral y EndPoint, eventos y sistemas de monitorización, etc.

PERFIL BUSCADO

- Grado en ingeniería o campo similar o experiencia profesional equivalente demostrable
- Capacidad de scripting demostrable: bash/python/PS
- Experiencia con frameworks de explotación/post-explotación (metasploit, empire o similares)
- Conocimientos en administración de sistemas en entornos Windows y UNIX
- Experiencia con SIEM, IDS y otras soluciones de seguridad perimetrales
- Destacable habilidad analítica y de investigación
- Se valorará conocimiento de Sleuth Kit y/o otras tools forenses open-source en entorno linux
- Se valorará Máster o certificación en el ámbito de la ciberseguridad, especialmente en el campo DFIR o pentesting (CEH, OSCP, IRCP, RTCP, o similares)

QUE OFRECEMOS

- Formación continuada, interna y externa
- Creación y mantenimiento de herramientas
- Formar parte de un equipo joven y dinámico en un excelente ambiente de trabajo
- Tenemos muy presente la conciliación laboral y personal
- Oficinas cómodas y agradables en zona céntrica de Barcelona
- Horario flexible