Indicar la REFERENCIA del perfil para el que se opta:

OFERTA DE EMPLEO: INCIDENT HANDLER - Detection and Response Dept.
COMPAÑÍA: INCIDE
LUGAR: Barcelona / Teletrabajo
FECHA OFERTA: 01/09/2022
NÚMERO DE PUESTOS: 1

PUESTO: Incident Handler (**Referencia**: 220901IHJS)

Interesados, contactad a través de **rrhh@incide.es**

PERFIL BUSCADO

- Grado en ingeniería o campo similar o experiencia profesional equivalente demostrable.
- 1 año de experiencia mínima demostrable en respuesta a incidentes o análisis forense.
- Conocimientos técnicos demostrables de los principales artefactos forenses.
- Conocimientos demostrables de los procedimientos de gestión y respuesta a incidentes y mejores prácticas.
- Capacidad de scripting demostrable: bash/python/PowerShell.
- Conocimientos en administración de sistemas en entornos Windows y UNIX.
- Conocimientos de red y de los principales protocolos de comunicación.
- Dotes de liderazgo y coordinación con equipo.
- Capacidad de priorización y gestión del tiempo.
- Capacidad de trabajo en equipo.
- Altas habilidades comunicativas y de reporting.
- Capacidad de toma de decisiones.
- Capacidad de gestionar situaciones de crisis.
- Saber transmitir a la organización afectada la información necesaria en el momento adecuado para mantener informada a la dirección o comité de crisis.
- Se valorará Máster o certificación en el ámbito de la ciberseguridad, especialmente en DFIR o Red Team (IRCP, CHFI, ECIH, GIAC, GCFA o similares).

QUÉ OFRECEMOS

- Formación continuada, interna y externa.
- Participar directamente en la gestión y respuesta a incidentes reales de distintas tipologías y en organizaciones heterogéneas.
- Creación y mantenimiento de herramientas.
- Formar parte de un equipo joven y dinámico en un excelente ambiente de trabajo.
- Plan de carrera profesional personalizado con el que, en función de tus inquietudes y evolución personal, podrás especializarte en alguna de las siguientes áreas: respuesta a incidentes, análisis forense, threat hunting, detection engineering, pentesting o red team; igualmente, se dispondrá de la opción de profundizar en tus conocimientos técnicos u orientarte en áreas de gestión o preventa.
- Facilidades para la conciliación laboral y personal.

- Teletrabajo o cómodas oficinas en zona céntrica de Barcelona.
- Horario flexible.

RESUMEN

INCIDE es una compañía proveedora de servicios de seguridad defensiva y ofensiva (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, defensiva y ofensiva, ayudándolos mediante soporte a la detección y mitigación de amenazas mediante servicios de Detección y Respuesta (MDR), Threat Intelligence, Detection Engineering, 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 de protección.

Los **Incident Handler** del equipo de DFIR de INCIDE **lideran** la respuesta a incidentes, estableciendo las **estrategias de respuesta y contención,** y **definen las líneas de investigación** de un incidente basadas en hipótesis. A nivel interno, los Incident Handler **coordinan y guían** a los analistas DFIR y trabajan conjuntamente con ellos con el objetivo principal de determinar el vector de entrada, las acciones realizadas por el atacante, identificar IOCs y proponer acciones de contención y recomendaciones.
Por otro lado, los Incident Handler interactúan con los clientes afectados por un incidente con el objetivo de **entender la situación, asesorar al cliente** en la contención, estrategia de adquisición de datos y en la recuperación. En ocasiones se enfrentarán a situaciones de crisis y darán **soporte en las decisiones** legales y de negocio de la organización.
Durante la respuesta a incidentes y análisis forense, los miembros del equipo de DFIR de INCIDE trabajan en estrecha colaboración con los miembros del Red Team, los Detection Engineers y los Threat Hunters de INCIDE con el objetivo de entender, detectar e identificar las acciones del atacante, así como de formular y validar nuevas hipótesis.