

## **Analista SOC ARG**

### **¿Qué buscamos?**

Estamos en la búsqueda de nuevos talentos para la posición de **Analista SOC Sr o Semi Sr**, en modalidad full time, horario flexible en modalidad remota. Con base en Argentina.

### **¿Qué conocimientos debes tener?**

Estudiante avanzado de TI / Seguridad, egresado de carreras universitarias o técnicas de TI / Seguridad.

Experiencia mínima de 2 años en roles similares.

- Conocimientos y Experiencia en Microsoft Sentinel.
  - Administración y operación de la plataforma tecnológica.
  - Armado y optimización de reglas.
  - Integración de fuentes
  - Generación de dashboards
  - Triage de Incidentes.
  - Contención de Incidentes e implementación de playbooks
  - Conocimientos de AWS, Containers y EKS.

Valoraremos también certificación técnicas aplicables al rol.

- Certificaciones técnicas aplicables al rol, ya sea del roadmap de seguridad de Microsoft como también de la industria y agnósticas a marcas.

Ser proactivo, analítico sin perder la creatividad y con buena capacidad de comunicación con el cliente y equipo.

Capacidad de entender requerimientos funcionales y no funcionales, y a partir de ellos colaborar en la definición de soluciones técnicas / funcionales.

Conocimientos de Inglés para participar en videoconferencias con angloparlantes.

### **¿Cuáles serán tus responsabilidades y actividades?**

Administrar y mantener de forma óptima la plataforma SIEM, MS Sentinel. Integrar nuevas fuentes de datos y ampliar los casos de uso de detección. Creación y tuning de playbooks.

Dar apoyo al SOC, colaborando en la Gestión de Incidentes de ciberseguridad.

### **¿Qué te proponemos?**

Integrarte a un equipo de profesionales de alto perfil técnico y calidad humana en una empresa dedicada a tecnología de seguridad informática

y servicios de Cyberseguridad.

Que te sumes a una empresa regional, con posibilidades de crecimiento y desarrollo, tanto profesional como personal.

Que seas parte de un equipo de trabajo dinámico, activo, descontracturado y en constante movimiento que se mantiene en el estado del arte.

Que sumes, aportes y contribuyas para que Security Advisor sea una mejor empresa.

### **Modalidad de trabajo**

Remoto, con la posibilidad de alguna jornada presencial para actividades de Team Building internas o con el cliente.

Disponibilidad para viajar por periodos cortos (semana a modo de ejemplo)

Full time ; horario flexible.

Tipo de contrato permanente.

País Argentina

### **¿Te sentís identificad@?**

Envíanos tu CV a [talentos\\_ar@sadvisor.com](mailto:talentos_ar@sadvisor.com) con la referencia: **Analista SOC - Argentina**