FABIAN ALEJANDRO SANTANA BORQUEZ

SOC ANALYST JUNIOR

Analista de Seguridad en formación con experiencia práctica en monitoreo de eventos de seguridad, correlación de logs y análisis de incidentes utilizando SIEMs. Conocimiento en redes, sistemas Windows/Linux y herramientas de detección de amenazas. Orientado a roles de SOC Analyst L1, con interés en fortalecer procesos de detección temprana y gestión de alertas.

Experiencia de trabajo

Novofish

Asistente Informática

- Instalación, configuración y soporte técnico de equipos de cómputo (hardware y software).
- Implementación y mantenimiento de sistemas de videovigilancia (CCTV).
- Gestión de cuentas de usuario y permisos en entornos corporativos.
- Resolución de incidencias técnicas, asegurando la continuidad operativa.

Análisis y Correlación de Eventos de Autenticación con Splunk Enterprise

Proyecto Personal

- Configuración de ingesta y normalización de eventos de seguridad de Windows en Splunk mediante Universal Forwarder.
- Desarrollo de reglas de correlación en SPL para identificar patrones de autenticación fallida vinculados a ataques de fuerza bruta RDP.
- Implementación de alertas automatizadas con umbrales definidos, incluyendo envío de notificaciones por correo electrónico.
- Documentación del flujo de detección y alineación con el marco MITRE ATT&CK.

Implementación de Reglas Personalizadas de Detección con Wazuh

Proyecto personal

- Implementación de agente Wazuh en endpoints Windows para la recolección y análisis centralizado de eventos de seguridad.
- Diseño y despliegue de reglas de correlación para detectar múltiples intentos de autenticación fallida en servicios RDP.
- Creación de regla personalizada en local_rules.xml para identificar patrones de fuerza bruta, elevando la criticidad al nivel 12.
- Validación de la detección en escenarios simulados, optimizando la visibilidad de ataques y fortaleciendo la respuesta SOC.

Contactos

linkedin.com/in/fsantanab

fabiansantana@outlook.cl

github.com/ne1n0

+56 9 99107066

https://ne1nsec.com

Educación

Ingeniería en Ciberseguridad - AIEP 2022 - Actualidad

Certificaciones

- Google Cybersecurity 2025 (Coursera)
- CompTIA Security + (preparación en curso)

Habilidades

- SIEM: Splunk, Wazuh
- IDS/IPS: Suricata, Snort
- Firewalls: pfSense, Fortinet
- Lenguajes/Scripting: Python, Javascript, SQL, Bash, Powershell
- Excel: Intermerdio