

MATIAS MUSSO

Consultor de Ciberseguridad | SOC / Vulnerability Management | PCI-DSS

contacto@matiasmusso.com.ar • +54 343 416-5508

Resumen

Consultor de ciberseguridad especializado en despliegue, personalización y soporte de Wazuh y arquitecturas SIEM/EDR. Experiencia en creación de casos de uso, decoders y reglas de correlación, integración y normalización de fuentes, automatización/orquestación de detección y respuesta para reducir MTTD/MTTR, respuesta a incidentes y mentoría técnica a equipos N1/N2. Orientado a entrega de soluciones operativas y presentaciones técnicas para clientes.

Experiencia

Analista de ciberseguridad Sr

Credencial Payments

2024-10 - Presente

- Desplugué y administré Wazuh (manager y agentes) y módulos FIM, SCA y Vulnerability Detection para cumplimiento PCI-DSS 4.0, reduciendo MTTD/MTTR ~30–40%.
- Diseñé decoders, reglas de correlación y dashboards en Wazuh para monitoreo de controles PCI (logging, integridad y hardening), mejorando detección y trazabilidad operativa.
- Ejecuté hardening y evaluaciones con Wazuh SCA y FIM en más de 100 activos, reduciendo no conformidades críticas >60% entre ciclos de auditoría.
- Integré Wazuh con SIEM, EDR y múltiples fuentes de logs (aplicaciones, BD y servicios cloud), implementando parseo y normalización para mejorar correlación y búsquedas.
- Realicé Vulnerability Assessment y pentesting, priorizando hallazgos por CVSS/VPR y validando remediaciones; >85% de findings cerrados dentro de SLA.
- Lideré respuesta a incidentes y análisis forense apoyado en telemetría Wazuh, definiendo RCA y planes de remediación que redujeron recurrencia ~40%.

Analista de ciberseguridad Ssr

KPMG

2023-10 - 2024-09

- Asesoré técnicamente a clientes en seguridad informática, proponiendo casos de uso y reglas alineadas a controles regulatorios para mejorar detección y cumplimiento.
- Colaboré en análisis de riesgos y mapeo a MITRE ATT&CK para priorizar alertas y optimizar la eficacia de correlación y respuesta en operaciones SOC.
- Preparé documentación técnica y soporte para auditorías, facilitando evidencias y seguimiento de remediaciones para cumplimiento regulatorio y operativa.

Analista de ciberseguridad Jr

HDI Seguros Argentina

2022-10 - 2023-09

- Soporté operaciones de seguridad: monitoreo y triage de alertas, manejo de tickets y coordinación con equipos de TI para remediaciones dentro de SLA.

- Realicé análisis de vulnerabilidades y apoyé en implementación de controles de hardening en endpoints y servidores para reducir exposición.
- Participé en ejercicios de respuesta a incidentes y en la elaboración de procedimientos operativos del SOC para estandarizar procesos de escalamiento.

Gestor de Seguridad de la Información

DHL Global Forwarding

2022-04 - 2022-10

Educación

Técnico en Informatica

E.E.T. N. º 68 "Prof. Facundo Arce"

2014 - 2020

Ingeniería en Ingeniería Informática

UADE

2021 -

Tecnicatura en Ciberseguridad

Escuela Da Vinci

2025-08 -

Habilidades

Administración y resolución de problemas en Linux, redes (TCP/IP, DNS, HTTP/S, Syslog), programación en Python y Bash (automatización), implementación y ajuste de SIEM, integración de registros, reglas de análisis y correlación, operaciones de seguridad y respuesta a incidentes, configuración de cortafuegos y seguridad de redes, automatización y orquestación (API, flujos de trabajo), Docker, Kubernetes, Ansible, Elastic Stack / OpenSearch, presentaciones técnicas y asistencia al cliente, tutoría y documentación, análisis de registros, detección de amenazas, ingeniería SIEM, supervisión de seguridad, seguridad de endpoints.

Certificaciones

Enterprise Security Manager 11.0 Essentials

McAfee

ID: CLP7868

Kali Linux Fundamentals

Cybrary

ID: CC-1d78b8f7-a862-4011-ab24-de2e179545c8

Idiomas

Ingles - professional