

MATIAS MUSSO

Cybersecurity Consultant | SOC / Vulnerability Management | PCI-DSS

contacto@matiasmusso.com.ar • +54 343 416-5508 • [LinkedIn](#) • Argentina

Summary

Cybersecurity consultant specializing in the deployment, customization, and support of Wazuh and SIEM/EDR architecture. Experience in creating use cases, decoders, and correlation rules; integrating and normalizing sources; and automating/orchestrating detection and response to reduce MTTD/MTTR, incident response, and technical mentoring for N1/N2 teams. Focused on delivering operational solutions and technical presentations to clients. Experience

Experience

PCI-DSS Security Consultant

Credencial Payments

2024-10 - Present

- I deployed and managed Wazuh (manager and agents) along with FIM, SCA, and Vulnerability Detection modules for PCI-DSS 4.0 compliance, reducing MTTD/MTTR by approximately 30–40%.
- I designed decoders, correlation rules, and dashboards in Wazuh for continuous monitoring of PCI controls (logging, file integrity, and hardening), improving detection and traceability.
- I performed hardening and assessments using Wazuh SCA and FIM on over 100 assets, reducing critical non-compliances by >60% between audit cycles.
- I integrated Wazuh with SIEM, EDR, and log sources (applications, databases, and cloud services), implementing parsing and normalization to improve correlation and search capabilities.
- I performed vulnerability assessments and penetration testing, prioritizing findings by CVSS/VPR and validating remediation; >85% of findings closed within SLA.
- I led incident response and forensic analysis supported by Wazuh telemetry, defining root cause analysis (RCA) and remediation plans that reduced recurrence by ~40%.

Senior Security Consultant

KPMG

2023-10 - 2024-09

- I provided technical consulting to clients on IT security, proposing use cases and policies aligned with regulatory requirements.
- I contributed to risk analysis and MITRE ATT&CK mapping to improve alert detection and prioritization.
- I prepared technical documentation and support for audits, providing evidence and tracking corrective actions.

Junior Cybersecurity Analyst

HDI Seguros Argentina

2022-10 - 2023-09

- I supported security operations, including monitoring and triaging alerts, managing tickets, and coordinating with IT teams to resolve issues within the SLA.
- I conducted vulnerability assessments and assisted with the implementation of hardening controls on endpoints and servers.
- I participated in incident response drills and in the development of SOC operating procedures.

Information Security Manager

DHL Global Forwarding

2022-04 - 2022-10

- I managed information security policies and operational controls to protect assets.
- I coordinated awareness campaigns and access controls with regional teams, thereby improving the implementation of these controls.
- I monitored policy compliance and assisted with incident reports and internal audits.

Education

Technician in Computer Science

E.E.T. N. ° 68 "Prof. Facundo Arce"

2014 - 2020

Engineering in Computer Science

UADE

2021 - 2027

Technician in Associate Degree in Cybersecurity

Escuela Da Vinci

2025-08 - 2028

Skills

Linux administration & troubleshooting, Networking (TCP/IP, DNS, HTTP/S, Syslog), Python & Bash scripting (automation), SIEM deployment & tuning (Wazuh, FortiSIEM), Log integration, parsing & correlation rules, Security operations & incident response, Firewall configuration & network security, Automation & orchestration (APIs, workflows), Docker, Kubernetes, Ansible, Elastic Stack / OpenSearch, Git version control, Technical presentations & client support, Mentoring & documentation, log análisis, threat detection, SIEM engineering, security monitoring, endpoint security.

Certifications

Enterprise Security Manager 11.0 Essentials

McAfee

ID: CLP7868

Kali Linux Fundamentals

Cybrary

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

Languages

English - Intermediate