Luis Mamani

Lima, Chorrillos 15057 | 990641247 | herrera1930@hotmail.com | https://www.linkedin.com/in/luis-jesus-reynaldo-mamani-herrera-9762aa125/

Profile

Cybersecurity Analyst specialized in Security Operations Center (SOC) operations, with hands-on experience in threat detection, analysis, and incident response. Proficient in SIEM platforms (Wazuh, Splunk, ELK), EDR/XDR solutions, and proactive monitoring methodologies. Skilled in alert triage, threat investigation, log analysis, event correlation, and incident handling following MITRE ATT&CK and NIST frameworks.

Adept at working under pressure and prioritizing critical incidents to ensure infrastructure security and business continuity. Knowledgeable in Windows, Linux, and TCP/IP networks, as well as basic penetration testing for vulnerability validation. Committed to continuous improvement, process automation, and accurate incident documentation.

Experience

August 12, 2024 - August 12, 2025

Security Operation Center | Stefanini Group |

- Cybersecurity professional with advanced skills in vulnerability analysis, penetration testing (pentesting), and critical infrastructure defense. Expert in identifying and mitigating threats by implementing proactive and reactive security measures.
- Familiar with Red Team methodologies and tools, as well as standards such as FORTINET, PALO ALTO, and WAF.
- Collaborate with security engineers and SOC administrators to provide situational awareness through detection, containment, and remediation of attacks on networks, web applications, and systems.
- Coordinate the SIEM development plan in collaboration with enterprise systems.
- Able to develop detailed reports and propose effective solutions to strengthen security posture. Currently focused on obtaining OSCP certification to consolidate skills in system exploitation and privilege escalation.
- Use of SIEM, tools such as QRADAR, SENTINEL, GRAFANA, AXUR

October 24, 2023 - July 31, 2024

Network Operation Center | YOFC |

- Network operations management and integration
- Management of Fiber Optic and Radio Link Projects at a national level
- Technical support for different problems.
- Maintenance and Operation of optical nodes (security, energy, networking, fiber optics)
- Coordination with PMO on correct implementation of the network
- LAN/WAN, TCP/IP Networking
- FortiManager/Fortigate
- Amazon EC2/Direct Connect
- Routing Protocols – BGP, OSPF, ECMP, MPLS

October 6, 2022 - October 21, 2023

Network Operation Center | GILAT |

- Network operations management and integration
- Management and monitoring of network and infrastructure operations, ensuring high quality of service to the end user (PRONATEL, Claro, Bitel, among others)
- Fiber Optic and Radio Link Projects at National Level
- Maintenance and Operation of optical nodes (security, energy, networking, fiber optics)

Education

MARCH 2011 – DECEMBER 2018

Electronic Engineering | National University of Altiplano - Puno - Peru
MARCH 2011 – DECEMBER 2018

Skills

- **Security and Monitoring**
  - Python – Intermediate Level
  - SIEM: **Wazuh, Splunk, ELK/Elastic Stack,QRadar, ArcSight**
  - EDR/XDR: **CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint, Sophos Intercept X**
  - IDS/IPS: **Snort, Suricata, Zeek**
  - Traffic and log analysis: **Wireshark, tcpdump**
- **Gestión de Vulnerabilidades**
  - Escaneo con **Nessus, OpenVAS, Qualys**
  - Evaluación y priorización según **CVSS**
  - Coordinación de parches y remediaciones
- **Redes y Protocolos**
  - Modelos **OSI** y **TCP/IP**
  - Protocolos: HTTP/S, DNS, SMTP, FTP, SSH
  - Segmentación de redes y VLANs
  - Firewalls y VPNs (Fortinet, Palo Alto, Cisco ASA)

Certifications

- FORTINET
- CCNA
- QRADAR
- Ability to work under pressure
- Experience in most restaurant positions

Interests

Theater, environmental conservation, traveling.