MARIA PAULA CARREÑO FERNANDEZ

maria.paufer14@gmail.com
https://mpcarreno.github.io/

SUMMARY

Electronics Engineer with over 2 years of experience in IT environments, with expertise in Cloud Services, Cybersecurity, Digital Forensics, and Incident Response. AZ-900 and BTL1 Certified. Skilled in cloud environments, network monitoring, and threat detection, with strong foundations in Windows and Linux systems.

EXPERIENCE

CyberSOC Analyst **Aug 2023 - Aug 2025**
SLB (Fortune 500 Company) *Bogotá, Colombia*

Responsible for monitoring and triaging security alerts, documenting findings, and following established procedures and playbooks. Performed necessary mitigation actions and identified incidents requiring escalation. Operated in an environment with over 250 alert types from more than 80 integrated data sources, supporting over 40,000 endpoints and 100,000+ users. Collaborated closely with international teams across both Western and Eastern Hemispheres, serving as the primary point of contact for messaging-related security incident escalations. Some of my contributions and recognitions:

- **Azure Pipelines – Software Supply Chain Security:** Designed and implemented a CI/CD pipeline using Azure Pipelines, Docker, and Swagger for a cybersecurity application at SLB. Managed the Software Bill of Materials (SBOM) lifecycle as part of the company's Software Supply Chain Security strategy, aligned with U.S. Executive Order 14028 (May 2021) to enhance national cybersecurity.
- **Proofpoint Data Integration ETL:** Collaborated with the automation team to extract data from Proofpoint Threat Response via API and integrate it into XSIAM (Palo Alto Networks). Enriched alerts, optimized detection rules, and reduced false positives, streamlining messaging investigations for analysts.
- **Cybersecurity Visibility Across Teams:** Delivered multiple internal training sessions and contributed to planning and organizing international cybersecurity events.
- **Outstanding Performance Recognition:** Awarded highest performance rating within the team.

IT Student Intern **Jan 2023 - Jun 2023**
SLB (Fortune 500 Company) *Bogotá, Colombia*

Focused on daily Security Operations Center (SOC) activities, including email analysis, SIEM, and EDR monitoring. Supported cloud projects as a back-end developer and managed APIs for an internal security application.

EDUCATION

Bachelor of Science in Electronics Engineering Sept 2023
Pontificia Universidad Javeriana
GPA: 4.2/5.0
Acknowledgments: Granted a full scholarship, Thesis Honorable Mention

PERSONAL PROJECTS

EAD3 Expo App implementation
Cross-platform application to optimize the clinical administration of the Abbreviated Development Scale (EAD-3). Designed to accelerate assessments, reduce manual scoring errors, enable reliable standardized developmental screening and support scalable longitudinal analysis of pediatric development.

CERTIFICATES

BTL1 - Blue Team Level 1 December 2024
SC-900 - Security, Compliance, and Identity Fundamentals May 2024
AZ-900 - Azure Fundamentals February 2024

COURSES

SANS FOR508 - Advanced Incident Response, Threat Hunting, and Digital Forensics May 2025

SKILLS

Knowledge: Cloud Platforms (AWS, GCP, Azure), Cloud Security, Infrastructure as Code (Terraform), Incident Response, Threat Intelligence, Digital Forensics, Network Protocols, Email Security, SIEM/SOAR, IDS/IPS, Threat Hunting, MITRE ATT&CK.

Tools: Terraform, Microsoft Sentinel, Splunk, Cortex XSIAM/XDR/XSOAR, Wireshark, Nmap, Microsoft Defender, Carbon Black, Proofpoint, Autopsy, Volatility, MISP, Qualys, CASB, Visual Studio, Git.

Programming Languages: Python, Bash, PowerShell, TypeScript.

LANGUAGES

English - C1 (CEPT)
Spanish - Native