Darlin Diaz Muñoz

darli2819@gmail.com | 610-329-6667

Linkedin.com/in/darlin-diaz-munoz | github.com/darlin883

SUMMARY OF QUALIFICATIONS

Security+ certified cybersecurity candidate with hands-on experience using Splunk SIEM for alert triage, threat investigation, and log analysis in a SOC homelab. Experienced investigating authentication events, suspicious emails, DNS activity, and endpoint telemetry across Windows and Linux systems. Seeking Security Operations Center Intern role to contribute to incident response and threat detection efforts.

TECHNICAL SKILLS

SIEM: Splunk (SPL, dashboards, log ingestion, alert investigation)
Logs: Windows Event Logs, Sysmon, DNS, Authentication, Network
Systems/OS: Windows, Linux (Ubuntu, Kali)
Networking: TCP/IP, DNS, HTTP/HTTPS, OSI model
Security: MITRE ATT&CK, OWASP Top 10, Alert Triage, Incident Response (NIST)
Cloud/Endpoint: AWS fundamentals, CloudTrail awareness, IAM events, EDR
Tools: Burp Suite, Wireshark, Nmap, Metasploit, Git
Languages: Python, Java, SQL **| Virtualization:** Proxmox VE, VirtualBox **| SOAR:** Foundational

EDUCATION & CERTIFICATIONS

A.S. Software Engineering, Thaddeus Stevens College of Technology — Expected 2026
Certifications:

- CompTIA Security+ (Active)
- CompTIA CySA+ (In progress)

PROFESSIONAL EXPERIENCE

Mary's Daycare Center, LLC | Remote
Software Engineering Intern **2026 – Present**

- Configured and maintained Linux web server supporting deployment, uptime, and troubleshooting.
- Assisted with backend logic, application setup, and testing for internal web systems.

Thaddeus Stevens College of Technology | Lancaster, PA
Software Engineering Tutor **2025 – Present**

- Tutored students in Python, Java, and web development.
- Mentored peers in debugging, problem-solving, and foundational cybersecurity awareness.

TECHNICAL PROJECTS

SOC Homelab (Proxmox + Splunk SIEM + Windows/Linux Endpoints)

- Built multi-VM lab forwarding Windows and Linux logs into Splunk for centralized monitoring.
- Performed alert triage and root-cause investigations using SPL.
- Investigated authentication events, Sysmon process activity, DNS anomalies, and network behavior.
- Documented investigations in ticket-style reports with timelines, IOCs, actions taken, and follow-up recommendations.
- Analyzed suspicious email samples including header review, link inspection, and reputation checks to determine malicious intent.

Burp ClusterBomb Tools | Python 3.8+, Burp Suite, SQLi, SSRF, Automation

- Developed Python automation scripts integrated with Burp Suite for SQLi and SSRF testing.