Don Lopez

CYBERSECURITY ANALYST | SECURITY OPERATIONS

Indio, CA | frailtycraven@gmail.com
GitHub: github.com/IXI-2773 | LinkedIn: linkedin.com/in/ixi2773/

PROFESSIONAL SUMMARY

CompTIA Security+ and CySA+ certified professional with a B.S. in Information Systems & Technology (Cybersecurity). Hands-on cybersecurity lab experience in SIEM alert triage, SPL-based detection engineering, log correlation, and network traffic analysis. Brings six years of physical security experience in monitoring, incident documentation, and escalation.

CERTIFICATIONS

CompTIA CySA+ (Cybersecurity Analyst) | Earned October 2026
CompTIA Security+ | Certified
Splunk Certified Cybersecurity Defense Analyst (SCCDA) | Planned (Soon)

TECHNICAL SKILLS

Detection: Splunk (SPL), Sigma, Snort, MITRE ATT&CK
Security operations: Alert triage, log analysis and correlation, incident response, packet analysis
Security tools: Wireshark, Nessus, Nmap, Metasploit
Systems & cloud: Linux, Windows Server, VMware, Docker, AWS (basic)
Scripting & data: Python, Bash, PowerShell, SQL

CYBERSECURITY LAB PROJECTS

Detection Engineering & Rule Development 2026

- Developed and tested 5+ detection rules in Splunk SPL and Sigma for brute-force activity (T1110), Base64-encoded PowerShell, and lateral movement.
- Tuned rules and filters to reduce false positives by approximately 30% during lab validation.
- Simulated attack scenarios to validate alerts; mapped detections to MITRE ATT&CK and documented rule logic.

SIEM Threat Detection | Splunk 2025

- Built dashboards and alerts to identify authentication anomalies and rapid login attempts.
- Correlated authentication, network, and endpoint logs across 3+ sources to investigate security events.
- Triaged alerts, built event timelines, and documented investigations; optimized SPL queries to reduce false positives.

Network Intrusion Lab | Kali Linux, Wireshark, Snort 2025

- Simulated scanning, brute-force, and exploitation activity in a Kali Linux lab.
- Analyzed 5,000+ packets in Wireshark to identify suspicious network behavior.
- Implemented and tuned Snort intrusion detection rules to detect simulated attacks.

PROFESSIONAL EXPERIENCE

Security Officer | Allied Universal 2019 - Present

- Prepare and escalate 10+ incident reports monthly while monitoring a secure environment.
- Maintain detailed security logs and apply real-time threat recognition and response.

EDUCATION

B.S. Information Systems & Technology (Cybersecurity)
California State University, San Bernardino