Steven Lang

www.linkedin.com/in/steven-lang-infosec | sjlang.805@gmail.com | 805-201-8440

Summary of Qualifications

Security Analyst with 2+ years in SOC and MDR-aligned roles within a university environment, working closely with the Security Operations Analyst and CISO. Experienced in SIEM design (ELK, Azure Sentinel), endpoint log analysis (Qualys, Duo), and automation of response workflows via playbooks and webhooks. Resolved 500+ security incidents involving phishing, malware, access issues, and endpoint compromise. Proficient in Bash and Python for scripting and automation. Familiar with MITRE ATT&CK techniques, threat hunting, and continuous detection tuning. Holds CompTIA Security+ and contributes to collaborative security initiatives across institutions by following CIS benchmarks and controls.

Technical Skills

Cloud & Infrastructure: Azure Cloud, Azure Arc, Azure Sentinel, Azure DevOps, Docker, SaaS Tools

Scripting: Bash, Python, PowerShell (basic), YAML, JSON, Rest API

Monitoring & SIEM: Elastic Stack (ELK), KQL, Custom Dashboards, Qualys, Duo Logs

Incident Response: Playbooks, SOPs, Threat Hunting, Ticket Triage, Risk Tabletops

EDR: Qualys, Blocklist management, Defender XDR, Log Analysis, Packet Analysis, Malware Analysis

Education

Bachelor of Science in Computer Science, Emphasis/Minors in Mathematics and Cybersecurity **May 2025**

California State University Channel Islands, Camarillo, CA

Employment Experience

California State University Channel Islands, Camarillo, CA **Mar 2023 - Present**

Information Security Student Assistant

- Promoted three times in under 18 months for consistent technical performance and leadership in securing university infrastructure and training junior analysts
- Resolved 500+ security tickets including phishing, password resets, malware detections, and endpoint compliance issues; triaged alerts and executed response actions per internal SOPs
- Built automated Azure Sentinel Playbooks for virus scanning, IP blacklisting, ticket creation, and email isolation using KQL, Logic Apps, and webhooks
- Created and maintained incident response documentation and detection use case playbooks; enforced SOPs for EOL asset decommissioning and agent integrity
- Conducted white box penetration testing in partnership with locksmiths and campus police on Mifare key-cards and locks via scanning/skimming tools and network assessments
- Conducted black box tests on newly created E-Sport lab's machines and network
- Collaborated with client-facing university teams and consulted CSU Sacramento's SIEM initiative on detection strategy and log ingestion
- Participated in risk review tabletops for ransomware and DR; contributed remediation recommendations and wrote post-event analysis docs