Joseph Posas

Charlotte, North Carolina | joseph.posasm@gmail.com | 980 899 3207 | josephposas.com | josephposas.com/linkedin

Summary

Cybersecurity graduate student with hands-on experience in threat intelligence, SIEM analysis, and security research. Recently deployed SSH honeypot analyzing 475+ attack events using Splunk, mapping attacker behavior to MITRE ATT&CK framework. Experienced in secure web development (140+ students taught), IoT security research (50+ papers reviewed), and network security. Seeking SOC analyst or security analyst internship to apply threat detection and incident response skills in production environment.

Education

University of North Carolina at Charlotte, Charlotte, NC

Accelerated Master of Science in Cybersecurity May 2027

Bachelor of Science in Computer Science, Cybersecurity Concentration May 2026

Central Piedmont Community College , Charlotte, NC

Associate's Degree in Computer Science May 2024

Experience

University of North Carolina at Charlotte, Charlotte, NC

Web Development Teaching Assistant Dec 2024 – Present

- Facilitated learning for 140+ students in web security topics such as input validation, XSS prevention, and authentication.
- Guided students in debugging code, troubleshooting errors, and reinforcing accessibility and clean coding practices.
- Collaborated with the instructor to enhance course materials on secure coding and web application security.

IoT Security Research Assistant Sep 2024 – Dec 2024

- Reviewed 50+ academic papers on exploit automation and IoT security.
- Examined vulnerability patterns and exploit techniques to contribute to research on AI-driven cybersecurity threats.
- Engaged in a research project focused on exploring exploit automation and emerging security risks in IoT systems.

Linxy, Charlotte, NC

Software Development Intern May 2024 – Aug 2024

- Built customer and admin dashboards in React, adding role-based access controls to strengthen security.
- Resolved 15+ issues during QA testing, including security vulnerabilities, to improve reliability.

Technical Projects

SSH Honeypot Deployment and Threat Intelligence Analysis with Splunk SIEM GitHub

- Deployed Cowrie SSH honeypot and configured Splunk Universal Forwarder to analyze 475+ security events across 44 attack sessions, identifying brute-force patterns and post-compromise reconnaissance activity.
- Built 3 Splunk dashboards mapping attacker behavior to MITRE ATT&CK framework, detecting T1087 (Account Discovery), T1105 (Ingress Tool Transfer), and T1548 (Privilege Escalation) across 72 executed commands.
- Developed 15+ SPL detection rules and correlation searches for automated attack identification, malicious command detection, and credential theft attempts.
- Created comprehensive GitHub repository with setup guides, Splunk queries, and threat intelligence findings demonstrating complete security research lifecycle.

Enterprise Network Security Infrastructure Design GitHub

- Designed and implemented a multi-site enterprise network in Cisco Packet Tracer simulating business environments.
- Configured routers, switches, and VLANs to segment traffic, enforce access control, and prevent data leaks.
- Applied ACLs and static routes to control interdepartmental traffic and strengthen internal network security.
- Tested connectivity and redundancy through simulated packet transfers, verifying failover performance and routing accuracy.

Network Analysis and Packet Inspection using Wireshark

- Captured and analyzed packet data using Wireshark to study HTTP, DNS, and TCP communications.
- Applied display filters (http, dns, tcp.srcport != 80, frame.len == 1514) to isolate and interpret network traffic patterns.
- Examined protocol layers and frame details to identify communication types, ports, and hosts in live network captures.

Technical Skills

Cybersecurity: Threat Intelligence, SIEM Configuration & Management (Splunk), Security Monitoring & Detection, Log Analysis, MITRE ATT&CK Framework, Network Security, Secure Web Development, IoT Security, Incident Investigation, Behavioral Analysis, Vulnerability Assessment, Exploit Automation Research, Incident Response Documentation

Programming & Development: Java, Python, JavaScript, HTML/CSS, Swift, React, Secure Coding Practices

Security Tools & Technologies: Splunk Enterprise (SIEM), Cowrie Honeypot, Wireshark, Nmap, Burp Suite, Cisco Packet Tracer, Kali Linux (Basic), GitHub, Splunk Universal Forwarder, Linux System Administration

Additional Tools: Microsoft Office Suite, Windows Server, Xcode, Photoshop, Active Directory (Basic), Figma