Stephen Stasaitis

Arlington, VA • +1-508-808-3931 • stephen.stasaitis@gmail.com
GitHub Portfolio • LinkedIn

PROFESSIONAL SUMMARY

Entry-level IT Support and Cybersecurity Specialist with hands-on experience in technical support, SIEM deployment, threat detection, and red team simulation. CompTIA Security+ and Network+ certified, with a proven record of discovering and reporting 12 critical vulnerabilities in a production AI system, all of which were later patched by the vendor. Former startup operations lead who thrived in high-pressure environments, independently managing crisis events, resolving technical issues, and coordinating multi-team operations in real time. Committed to security-focused support, technical self-study, and continuous hands-on lab development.

TECHNICAL SKILLS

- Security Tools: Wazuh, Security Onion, Sysmon, Event Viewer
- Detection & Analysis: MITRE ATT&CK Mapping, CVSS Scoring, YAML/JSON Injection, Log Correlation, Triage, Alert Tuning
- Offensive Tools: Kali Linux, Nmap, Evil-WinRM, Hydra, NetExec, SecLists
- Systems & Networking: Windows Server, Ubuntu, Active Directory, DNS, DHCP, SMB, VLANs, NAT, Firewalls, VirtualBox, Postfix
- Cloud & Scripting: Azure (learning), Splunk (learning), PowerShell, Bash, Flask, GitHub Actions, Render

CYBERSECURITY PROJECT EXPERIENCE

- **AI Assistant Red Team Simulation**
  Simulated adversarial prompt injection and logic mapping attacks on a production AI assistant deployed by a high-growth, early-stage startup. Identified 12 critical and 6 high-risk vulnerabilities, 100% vendor-patched. Delivered CVSS-scored reports and proof-of-concept payloads using custom Python fuzzers.
- **Enterprise Security Lab**
  Deployed a virtual enterprise network using Windows Server and Ubuntu with Wazuh and Security Onion. Simulated brute force attacks, monitored SIEM alerts, and hardened a Postfix mail server.
- **Cloud SIEM Honeypot & Geolocation Dashboard (Azure Sentinel)**
  Developed a honeypot for RDP brute-force attacks using Azure Sentinel. Used PowerShell to extract Windows event metadata and send it to a geolocation API. Parsed location data in Log Analytics and built a Sentinel workbook to map global attacks.
- **Offensive Security Lab**
  Built a test environment with vulnerable machines to practice privilege escalation and lateral movement. Used Hydra and Evil-WinRM for access and validated detection capabilities with MITRE mapping.
- **Fantasy Baseball AI Assistant** *(In Progress)*
  Python Flask chatbot that tracks fantasy stats using ESPN and StatsAPI; responds to user queries and updates via GitHub Actions.

WORK EXPERIENCE

Head of Dispatch Operations – Courial | San Francisco, CA *Feb 2021 – Jul 2024*

- Drove $4MM+ in revenue from market launch, leading to investment from Elemental Excelerator and Techstars.
- Raised $80K in seed capital through direct networking to help launch the startup.
- Directed nationwide dispatch operations for a network of 100,000+ Courials, spearheading automation initiatives that streamlined workflows and overseeing task execution across multiple teams to ensure 24/7 business continuity.
- Led crisis operations during DDoS attacks and infrastructure failures, coordinating real-time emergency response, driver logistics, and incident resolution to protect revenue-generating activity.

EDUCATION

The Pennsylvania State University, University Park, PA *Graduation Date: December 2019*

- Bachelor of Science in Finance
- GPA 3.65/4.00

CERTIFICATIONS

- CompTIA Network+ and Security+ | Issued Feb 2025 - Expires Feb 2028

ADDITIONAL DETAILS

- Raised $85,000+ for pediatric cancer research through Penn State THON.
- Transitioned into cybersecurity in 2024; built homelabs, deployed SIEMs, simulated attacks, and earned Security+ and Network+.
- Interests include threat hunting, AI prompt testing, homelab engineering, and fantasy baseball analytics.