Bowman Williams

LEONARD BELL

NOC Analyst | SOC Analyst | Security+ | AZ-900 | Cybersecurity Analyst | Endpoint & Email Security

PROFESSIONAL SUMMARY

Security+ and AZ-900 certified IT professional with 4+ years of enterprise experience supporting endpoint, identity, and email security environments. Hands-on experience investigating phishing incidents, analyzing suspicious activity, and performing initial incident triage using tools such as Microsoft Defender and enterprise email security platforms. Currently building a home SOC lab and developing real-world cybersecurity projects, including a custom SOC Toolkit Lab designed to simulate investigation workflows using tools like Wireshark, Nmap, and Splunk. Actively transitioning into a SOC Analyst role with a focus on threat detection, incident response, and security operations.

EDUCATION

Security+ Training Program | College of Southern Maryland **Jan 2021 – Jun 2021**
Cybersecurity Workforce Training program

AAS Cybersecurity | Allegany College of Maryland **Aug 2015 – Aug 2017**
Cybersecuruty Studies (Coursework completed)

EXPERIENCE

Network Administrator | Community IT Innovators (MSP) **May 2023 – Feb 2026**

- Investigated phishing incidents and performed message trace analysis in Microsoft 365, identifying suspicious emails and supporting initial incident triage
- Performed IP blocking and basic containment actions for identified threats in coordination with the security team
- Monitored and troubleshot network and system issues involving DNS, TCP/IP, and endpoint con nectivity, supporting uptime and operational stability
- Collaborated with the security team by escalating suspicious activity and providing findings for further investigation
- Gained exposure to security operations workflows including phishing analysis, incident triage, and basic containment actions
- Monitored network and system performance using SolarWinds, identifying connectivity issues and supporting incident response

IT Support / Helpdesk Administrator | Transcendent IT (MSP) **Nov 2021 – May 2023**

- Enforced least privilege access across SharePoint and enterprise collaboration platforms
- Investigated phishing incidents and conducted message trace analysis in Microsoft Defender, supporting initial threat identification and response

PROJECTS

SOCPilot – AI SOC Triage Dashboard | GitHub | Live Demo

- Built AI-powered SOC triage tool using Next.js, TypeScript, and OpenAI API to analyze security alerts in real time
- Classified alert severity, mapped threats to MITRE ATT&CK, and generated investigation and remediation steps
- Extracted IOCs (IPs, domains, hashes) from raw security data for analyst use
- Deployed production application using Vercel with GitHub integration

Cyber Toolkit Lab | GitHub

- Built a custom SOC investigation toolkit integrating tools such as Wireshark, Nmap, Process Explorer, Autoruns, and CyberChef
- Designed a structured workflow for network analysis, endpoint investigation, and incident response

SKILLS

Security Tools: Microsoft Defender, CrowdStrike Falcon EDR, Splunk (SIEM)

Networking: TCP/IP, DNS, DHCP, SolarWinds

Analysis: Windows Event Logs, Threat Analysis, Incident Response