Aswin Suresh

U.S. Citizen | West Lafayette, IN | Sicklerville, NJ | aswinsureshche@gmail.com | github.com/aswinsureshche

EDUCATION

Purdue University, Polytechnic Institute – *West Lafayette, IN* **August 2025 - May 2028 (Expected)**

B.S. in Cybersecurity | Minor in Artificial Intelligence & Machine Learning

CERTIFICATIONS

CompTIA Security+ | Cisco Certified Network Associate (CCNA) – *(Scheduled for December 2026)*

PROJECTS

Home SOC / SIEM Lab | *Wazuh, Suricata, Sysmon, Python, Metasploit* **September 2026**

- Built a multi-VM home SOC with a Dockerized Wazuh SIEM and a Suricata network sensor, collecting Sysmon, Windows event, firewall, and Nutanix AHV logs on an isolated virtual network with Windows Server and Metasploitable targets
- Wrote 11 custom Wazuh detection rules and a Windows Firewall log decoder covering 8 MITRE ATT&CK techniques, including a multi-stage rule that flags recon, brute force, and exploitation from one source IP within a 15-minute window
- Created a Python correlation engine that pulls alerts from the Wazuh Indexer API, groups them into incidents by source IP, time window, and attack stage (recon, brute force, exploitation), and auto-generates Markdown or PDF incident reports

Cloud Misconfiguration Lab | *AWS, Terraform, Prowler, ScoutSuite, Python* **September 2026 – Present**

- Built an AWS lab in Terraform with four deliberate misconfigurations (a public S3 bucket, wildcard IAM policy, SSH open to 0.0.0.0/0, and a public EBS snapshot) that a single Terraform variable switches between vulnerable and hardened states
- Mapped each misconfiguration to its CIS AWS Foundations Benchmark controls and MITRE ATT&CK techniques (T1530, T1078.004, T1133), documenting how a real attacker could exploit each one and how hardening closes the gap
- Wrote Bash scripts to run Prowler and ScoutSuite scans, comparing the before and after reports to confirm which findings were fixed and which remain, plus a teardown verification script and an AWS Budgets alert for runaway costs

ASL Gesture Recognition App | *YOLOv8, Roboflow* **November 2024**

- Built an American Sign Language (ASL) recognition app for the Congressional App Challenge (District NJ-01) around a custom YOLOv8 object detection model, handling all dataset preparation, image annotation, and training in Roboflow
- Partnered with members of the Deaf community to test and refine the model, ensuring it met real-world accessibility needs
- Deployed the model in a web app that detects signs in a live video feed and displays the matching letter or word on screen

COMPETITIONS

National Cyber League (NCL) – Team Lead **November 2025**

- Led team to a top 3% national finish among 4,500+ teams in a timed, Jeopardy-style capture-the-flag (CTF) competition
- Solved 80+ hands-on challenges in network traffic analysis, cryptography, web exploitation, and forensics, using Wireshark to analyze packet captures, Burp Suite to exploit web apps, Nmap to map hosts, and Hashcat to crack password hashes

WORK EXPERIENCE

Network Solutions Intern – Stealth Marketing (*Verizon Fios)* **June 2026 – August 2026**

- Closed 300+ new Verizon Fios residential accounts by canvassing 1,000+ households as a brand ambassador
- Assessed homeowners' existing networks for coverage gaps and bandwidth needs, then recommended fiber and Wi-Fi plans
- Translated fiber, Wi-Fi, and home network security concepts into clear, plain language for 1,750+ non-technical residents

SKILLS

Security Tools: Wazuh, Suricata, Sysmon, Wireshark, Nmap, Metasploit, Burp Suite, Hashcat, Prowler, ScoutSuite

Cloud & Infrastructure: AWS (IAM, S3, EC2/EBS, VPC), Terraform, Docker, Linux, Windows Server, Active Directory, DNS, Nutanix AHV, VM Provisioning & Hardening, RBAC/ABAC, Linux ACLs

Frameworks & Concepts: MITRE ATT&CK, CIS Benchmarks, SIEM Detection Rules, Network Traffic Analysis, Web Exploitation, Cryptography, Digital Forensics

Languages: Python, Bash, PowerShell, SQL, C, HTML/CSS

AI & Machine Learning: YOLOv8, Computer Vision, Neural Networks, Model Training, Roboflow