Siris St.Victor

Security Engineer Intern

sst.victor05@gmail.com • 347-993-5645 • Github • LinkedIn • Medium

Education

Computer Science 05/2027
Farmingdale State College
- **Coursework:** Computer Networking, Computer Arch & Organization, Software Engineering, Data Management
- **Academic Recognition**: Dean's List
- **Clubs**: Computer Security (participating in CTFs & security workshops)

Projects

AWS Detection as Code Pipeline
- Streamlined a threat detection pipeline from Visual Studio Code using *Sumo Logic, Terraform, Git, Github*
- Acquired expertise building threat detections for modern cloud native attack techniques and SaaS environments
- Analyzed AWS Cloud Trail logs for malicious behavior and mapped them to MITRE ATT&CK's Cloud Matrix

Windows Detection as Code Pipeline
- Used Terraform to manage and deploy Windows detection content as code following defensive TTPs
- Leveraged Atomic Red Team and Threat Reports to simulate a realistic enterprise attack paths to craft detections
- Analyzed Windows Sysmon logs to detect lateral movement, credential dumping, and persistence mechanisms

Linux Detection as Code Pipeline
- Implemented Linux host telemetry with auditd and laurel to support syscall and process execution detections
- Researched Linux internals and runtime threats to build threat detections and inform detection logic
- Used threat reports and adversary tradecraft to simulate offensive TTPs and validate Linux detections

Certifications

ACRTP - Amazon Cloud Red Team Professional
(Expected March 2026)

TCM Security PSAA - Practical SOC Analyst Associate

Community Engagement

BSides NYC 10/2025 | NY
Pros v Joes Player
- Competed in the *Pros v. Joes* blue team challenge with a team of 12 by defending an environment containing over 25 endpoints ranging from Linux, Windows, Firewalls and productions Servers against red team attacks
- Exercised technical skills in Incident Response, Threat hunting, and System Hardening in a collaborative team setting to help eridicate perisentce mechanism and remediate the infected endpoints