

# Patrick Selby

pselby@gsumail.gram.edu | +1 (614) 332-6860 | [LinkedIn](#) | [Github](#)

## CAREER OBJECTIVE

Sophomore Cybersecurity student seeking hands-on exposure to security operations, risk analysis, and defensive security practices through industry-aligned programs and professional development opportunities.

---

## EDUCATION

### Grambling State University – Grambling, LA

**B.S. Cybersecurity** (Minor: Computer Information Systems (CIS) | **GPA: 3.9/4.0**

Jan 2025 – Dec 2028

#### Relevant Coursework:

Attacks, Threats, and Vulnerabilities (CompTIA Security+ SY0-701 aligned), Discrete Structures, Data Structures & Algorithms (In Progress), Probability & Statistics I (In Progress), Calculus I

---

## TECHNICAL SKILLS

**Cybersecurity & Systems:** Linux CLI, Network Fundamentals, Nmap, Wireshark, Basic Incident Response, Vulnerability Assessment (Foundational)

**Cloud & Platforms:** AWS (EC2, S3, IAM)

**Programming & Data:** Python, SQL

**Version Control:** Git, GitHub

---

## EXPERIENCE

### IoT Cyber Defense Extern (Simulated) – Extern / Hydroficient (Remote)

- Mapped an **end-to-end IoT system** by analyzing **10+** simulated data flows (sensor telemetry, control commands, and cloud ingestion paths) to identify **multiple potential attack surfaces** in a water-monitoring environment.
  - Evaluated security risks across **3 core control areas** (encryption in transit, device authentication, and access control) under guided adversarial scenarios, identifying weaknesses tied to replay and interception attacks.
  - Documented mitigation strategies for **5+ identified risk scenarios**, aligning recommendations with critical-infrastructure and IoT security best practices.
- 

## PROJECT

### AWS Incident Response Lab

- Investigated a simulated cloud security incident by reviewing **100+ CloudTrail log events** using JQ, leading to the identification of a publicly exposed **S3 bucket** and misused **IAM credentials**.
  - Reduced incident investigation time by correlating **API activity, source IPs, and affected resources** to isolate indicators of compromise within a single analysis workflow.
  - Improved cloud security posture by implementing **3 remediation actions** (restricting bucket access, rotating credentials, and enforcing least privilege) aligned with incident response best practices
- 

## CERTIFICATIONS

**AWS Academy Cloud Foundations** (AWS, Apr 2025) | **Google Cybersecurity Specialization** (Foundations of Cybersecurity, Play It Safe: Manage Security Risks) – 2025 | **IBM SkillsBuild** (AI, Data, Cybersecurity), 2025

---

## AFFILIATIONS

ColorStack | NSBE | IEEE | Honor Society® | S.E.C.U.R.E. Cybersecurity Club (GSU) | The Lantern Network (Career & Mentorship) | National Society of Leadership and Success (NSLS) | National Association of Black Accountants (NABA)