Patrick Selby

pselby@gsumail.gram.edu | +1 (614) 332-6860 |**LinkedIn**| **Github** | **Portfolio**

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, Calculus I

TECHNICAL SKILLS

Cybersecurity & IT: Linux CLI, Network Fundamentals, Nmap, Wireshark, Basic Incident Response, Vulnerability Assessment, Threat modelling

Cloud & Systems: AWS (EC2, S3, IAM) | **Programming & Data:** Python, SQL | **Version Control:** Git, GitHub

EXPERIENCE

IoT Cyber Defense Extern (Simulated) | Extern / Hydroficient — Remote

Jan 2026 – Mar 2026

- **Mapped an end-to-end IoT water monitoring system** by analyzing simulated sensor telemetry, control commands, and cloud data flows, **identifying trust boundaries and potential attack surfaces.**
- **Evaluated IoT security risks** by reviewing encryption in transit, device authentication, and access-control mechanisms, **highlighting how replay, interception, and spoofing attacks could impact system integrity.**
- **Documented mitigation strategies** for simulated IoT threat scenarios, **demonstrating how baseline defensive controls reduce unauthorized device communication risk.**

PROJECTS

IT Risk Assessment & Data Classification Lab

- **Conducted an IT risk assessment** by inventorying organizational assets, classifying sensitive data, and scoring risks using likelihood and impact analysis, **resulting in prioritized, audit-aligned mitigation recommendations.**
- **Developed a formal data classification standard** to define handling requirements for restricted and confidential information, **reducing ambiguity in data usage and access decisions.**
- **Translated technical risk findings into leadership-ready documentation, supporting clearer decision-making for non-technical stakeholders.**

Incident Response & Evidence Documentation Lab (Linux)

- **Simulated an incident response workflow** by detecting failed authentication attempts, preserving authentication log evidence, and documenting response actions**, resulting in a complete and audit-ready incident record.**
- **Analyzed Linux authentication logs** by extracting and curating relevant failed login events, **improving signal-to-noise while maintaining evidence integrity.**
- **Performed a post-incident review** to identify root causes and preventative controls, **demonstrating a prevention-focused and documentation-driven security approach.**

CERTIFICATIONS

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