Patrick Selby

Security & Detection Engineering Intern · Threat Detection · MITRE ATT&CK · Log Analysis · Python

Grambling, LA | (614) 332-6860 | patrickselby256@gmail.com | linkedin.com/in/patrick-ennin-selby | github.com/pat-selby | patrickselby.vercel.app

Education

Grambling State University Expected Dec 2028

*B.S. Cybersecurity, Minor in Computer Information Systems | GPA: **3.88/4.00***

Relevant Coursework: Attacks, Threats & Vulnerabilities, Networking, Data Structures & Algorithms, Probability & Statistics

Experience

Grambling State University AIoT Lab, Security Research Assistant Mar 2026 – May 2026

- Stopped scan data from leaving the phone, as measured by **0 URLs sent** and **0 images saved**, by running 22 checks on the device in **under 5 ms**.
- Set the project's first accuracy score, as measured by **85% of 28 known bad links caught**, by building the test set and measuring each run.
- Moved the plan toward machine learning, as measured by its place in the lab's NSF report, by showing the **15%** the rules kept missing.

CodePath, Threat Detection Analyst Feb 2026 – May 2026

- Traced how an attacker gained admin rights, as measured by **4 linked log events**, by following the steps from stolen token to new service.
- Made the alert far less noisy, as measured by logic that tells real attacks from normal admin work, by matching **MITRE ATT&CK T1134.001** within a time window.
- Wrote a response guide others can reuse, as measured by steps a responder can follow on the next case, by turning the investigation into clear instructions.

Hydroficient, IoT Security Extern Feb 2026 – Mar 2026

- Stopped attackers replaying old device messages, as measured by **0 messages** that could be sent twice, by adding timestamps, counters, and **HMAC** checks.
- Made every device prove who it is, as measured by **100% of connections verified**, by adding per-device certificates through TLS/mTLS.
- Fixed the biggest risks first, as measured by the **2 top risks** from a full **STRIDE** review, by ranking each one on how likely and how damaging it was.

AI4ALL Ignite, AI/ML Fellow Jun 2026 – Aug 2026

- Built a fraud model on **568K transactions**, as measured by precision, recall, and F1 on a rare fraud class, by building the training and scoring pipeline.
- Caught a model that looked good but missed fraud, as measured by high accuracy with almost no fraud caught, by scoring on precision and recall instead.
- Got the team onto one process, as measured by everyone using the same data split, by writing the train and test rules.

Projects

Breach Investigation Toolkit | *Linux, auditd, ausearch, Bash* GitHub

- Found which program changed protected files, as measured by a full evidence trail, by turning on **auditd** rules and searching the log with `ausearch`.
- Closed the gaps that allowed it, as measured by **3 ranked fixes**, by tying each finding to the weakness behind it.

QR Phishing Scanner | *Python, OpenCV, NumPy, Tkinter*

- Stopped unsafe QR codes from opening, as measured by **only http(s) links allowed**, by reading codes from any window and checking them first.
- Fixed codes that would not scan, as measured by **28 passing tests**, by correcting angle, contrast, and inverted images.

Certifications, Leadership & Affiliations

Certifications: AWS Academy Cloud Foundations | CodePath CYB102 (Honors) | Google Cybersecurity | IBM SkillsBuild

Leadership: S.E.C.U.R.E. Cybersecurity Club, GSU — run CTF and hackathon prep for a chapter grown **40%** in membership | TMCF DevCon Zone 2 Scholar (2026)

Affiliations: Cloud Security Alliance | ColorStack | NSBE | IEEE | IOBSE 2026

Technical Skills

Detection: Threat Detection, MITRE ATT&CK, Windows Event Analysis, Log Analysis, Incident Response, STRIDE

Tools & Code: Linux CLI, auditd, Nmap, Wireshark, OpenVAS, Git, AWS; Python, Bash, SQL, Swift, Kotlin; TLS/mTLS, HMAC, MQTT