Matthew Chin

781-697-4238 | matthwchin@proton.me | linkedin.com/in/matthewleechin | github.com/balnc9 | balnc9.github.io/

Education

University of Maryland College Park, MD
Bachelor of Science in Computer Science, Minor in Business *Jan. 2024 – May 2027*

Experience

Undergraduate Data Research Assistant Feb. 2025 – Present
Digital Media Lab, UMD *College Park, MD*

- Build Chrome Extension + Next.js frontend to scrape and visualize live news metadata, using Chart.js, TypeScript, and DOM parsing
- Designed interactive dashboards and visualizations plotting engagement metrics, enabling researchers and local news anchors to analyze user interaction patterns
- Applied secure coding practices in extension development, managing permissions, content scripts, and safe storage APIs.

Development Intern Jun. 2025 – Present
Colexia *New York, NY*

- Built scalable analytics platform processing 1000+ events/second using **Spring Boot**, **Kafka**, **PostgreSQL**, and **Docker**, reducing API latency by 85%
- Automated data workflows using Python scrapers and Google Drive API integration, accelerating data reports by 70% and supporting ML dataset standardization

Projects

Pseudo Random Number Generation Lab | *SEED Labs (Ubuntu VM)*

- Investigated weaknesses in Linux PRNGs (/dev/random and /dev/urandom) and conducted statistical randomness testing.
- Built a key-recovery attack on AES by exploiting poor entropy, demonstrating cryptographic vulnerabilities.
- Implemented secure key-generation in C for 128/256-bit encryption, applying entropy analysis from kernel-level sources.

SIEM Log Analysis & Threat Detection | *SQLite, Security, Docker*

- Developed Python SIEM solution with Flask/SQLite to automate threat detection for Windows/Linux logs, implementing 6 security rules detecting brute force, privilege escalation, and lateral movement with 800+ events/second throughput
- Built security analytics engine using Pandas behavioral analysis and sliding window algorithms, identifying 28 high-severity threats during testing while reducing false positives through threat intelligence integration
- Designed SOC-ready platform with real-time dashboard, Docker deployment, and incident response workflows, providing automated security reporting and forensic capabilities for compliance and vulnerability management

Colexia Event Ingestion Platform | *SpringBoot, Kafka, PostgreSQL, Next.js*

- Built scalable analytics platform processing 1000+ events/second using **Spring Boot** microservices, **Kafka**, **PostgreSQL**, and Redis caching, achieving 85% API latency reduction with **Docker containerization**
- Developed event-driven data pipeline with real-time aggregation, REST APIs, fault tolerance, and comprehensive monitoring using Prometheus and Spring Boot Actuator for production observability
- Created full-stack dashboard with Next.js, TypeScript, and React featuring responsive UI, real-time visualization, and analytics insights consuming optimized REST endpoints with sub-100ms response times

Technical Skills

Languages: Java, Python, C , (Rust, OCaml)
University Coursework: Cryptography, Computer Networks, Computer Systems, Algorithms, Organization of Programming Langauges, Discrete Structures, OOP I/II.
Certifications: CompTIA Sec+ (Expected Jan. 2026), Tata Cybersecurity Job Simulation, **Mastercard** Cybersecurity Job Simulation, AWS ML Solutions (Coursera)
Other: Seal of Bi-literacy (Spanish & English, 2022)