

# Quentin Mayo, Ph.D.

Prosper, TX | 256-525-3199 | quentinmayo@hotmail.com | quentinmayo.com

---

## Senior Cybersecurity Engineer

**GWAPT, GWEB, GCSA, AWS Certified Cloud Practitioner, CompTIA Security+ with deep Application Security expertise**

**Languages and Frameworks:** Python, SQL, PHP, HTML, SQL, Perl, PowerShell, JavaScript, Java, SciKit Learn

**Platforms & Environments:** Linux, iOS, Android, Windows, OS X, AWS, GCP

**Knowledge Areas:** CI/CD, Vulnerability Management, Machine Learning & Data Mining, Web & Native App Security, STRIDE Threat Modeling, SAML, OAuth, OWASP, DAST, SAST, & IAST Analysis, DevSecOps

**Tech & Tools:** Burp Suite, Snyk, Semgrep, Okta, Kubernetes, Wiz, Nessus, Checkmarks, AppScan, Gauntlet, Recorded Future, Splunk, Databricks, AirFlow, Jira, Confluence, Jenkins, GitHub, Circle CI, Lacework, Fossa, HackerOne, BugCrowd

---

## Experience

### Pinterest

March 2024 - Present

#### Sr. Security Engineer

- Lead the enterprise Application & Product Security Vulnerability Management Program, owning end-to-end lifecycle management including automated triage, ownership routing, remediation governance, and executive reporting.
- Increased contractual SLA compliance for vulnerability remediation to **80%+**, designing and operationalizing risk-based SLAs aligned to severity, exploitability, and business impact.
- Expanded secure code and product scanning coverage(SCA, SAST) from **<20% to ~80% of the codebase** by centralizing scanning logic and standardizing onboarding across engineering teams.
- Built automation to analyze and scan Bazel-managed dependencies, integrating SCA workflows directly into Bazel build pipelines to improve dependency visibility and reduce blind spots in monorepo environments.
- Designed and implemented a **rule-based ownership and confidence scoring system** to automate vulnerability routing and triage, significantly reducing manual review overhead and improving assignment accuracy.
- Built automation pipelines to ingest, normalize, deduplicate, and prioritize findings across multiple security tools (SAST, DAST, dependency, container, internal services), enabling scalable triage of high-volume security signals.
- Centralized vulnerability scanning actions and remediation workflows across the organization, creating a consistent vulnerability lifecycle for product teams.
- Designed and implemented a **secure bastion host solution** to enable controlled interaction with production resources during incident response, strengthening PROD access governance following environment separation initiatives.
- Triage and validated **hundreds of bug bounty submissions**, improving signal quality, reducing false positives, and accelerating confirmed vulnerability remediation.
- Supported PCI compliance initiatives, including control validation and audit readiness; built automation to generate **quarterly security metrics and attestation reporting** for internal leadership and external stakeholders.
- Conducted threat modeling and security design reviews for internal services and product features, influencing secure-by-design architecture decisions across engineering teams.

### Nextdoor

Aug 2020 - Dec 2023

#### Sr. Security Engineer

- Owned the design and development of Application Security from scratch for the cloud-native, engineering-focused, social networking platform operating in 11 countries with 40M+ WAU, advancing security maturity and reducing risk in preparation for the company's planned IPO and 2X company growth.
- Developed and executed the application security roadmap including process, tooling, reporting, and visibility; partnering closely with the CISO to develop a security vision by taking a data-centric approach, assessing current state, identifying blind spots, and establishing security priorities.
- Led the technical strategy and execution for a major vulnerability risk reduction campaign, writing python scripts to correlate data values from Wiz, Checkmarks, GitHub, Fossa, and Open-Source tools that reduced 14k alerts into 5 solution patterns, eliminating 97% of critical vulnerabilities in one quarter.
- Switched SAST from Checkmarks to GitHub Advanced Security (GHAS) with a centralized repository and Jira ticketing, enabling immediate engineering notification for Pull request alerts; results included shortened time to remediate by removing security as a bottleneck and saving \$300k/year in SaaS costs.
- Spearheaded the Nextdoor bug bounty program, leading to the identification and remediation of in-production x-site scripting issues, IDOR, privacy model issues, and more.
- Developed and implemented automation scripts to perform continuous checks for vulnerabilities, secret leaks, and poor coding practices, integrating these checks into engineers' pull requests to enable early detection and resolution of issues which fostered a culture of security awareness and rapid issue resolution.
- Conducted assessments and enhancements of AWS security posture, contributed to Kubernetes security initiatives, reinforcing the security of containerized applications, and worked closely with dev and cloud engineering teams.

## **Federal Reserve Bank of New York**

### **Application Security Engineer**

Aug 2017 - Aug 2020

- Developed and implemented scripts to automate the creation of detailed vulnerability reports, streamlining the reporting process and enhancing efficiency in communication with key stakeholders.
- Shared vulnerability reports with key entities, including the Treasury, Board of Governors, and various Federal Reserve Banks, ensuring timely communication and coordinated efforts in addressing security concerns.
- Played a crucial role in managing and resolving security incidents, particularly during the TLS Heartbleed and critical COT vulnerabilities, demonstrating a rapid and effective response to mitigate potential risks.
- Conducted thorough threat modeling exercises, identifying potential security risks and proposing proactive measures to enhance application security.

### **Federal Reserve, Application Security Engineer, Continued**

- Worked collaboratively with cross-functional teams to resolve security incidents promptly, minimizing the impact on critical systems and maintaining the integrity of sensitive information.
- Utilized security tools to conduct comprehensive security assessments, vulnerability scans, and risk analyses on critical applications and systems.
- Provided expertise and insights in the form of security advisories related to emerging threats, vulnerabilities, and best practices to strengthen the overall security posture of the organization.

## **University of North Texas**

### **PhD Researcher, Open SSL Security Pattern-Based Vulnerability Detection using Static Analysis**

2015 – 2018

- Developed an ML-based predictive engine to identify probable recurrences of vulnerabilities in Open SSL using scikit-learn to analyze Git commit history using SAMATE to benchmark algorithms

### **Masters Researcher, Test Suite Prioritization Techniques**

2012 - 2015

## **Education**

### **Ph.D., Computer Science and Computer Engineering, University of North Texas, Winter 2018**

Dissertation: Security Pattern-Based Vulnerability Detection using Static Analysis

### **Masters, Computer Science and Computer Engineering, University of North Texas, Fall 2015**

### **Bachelor of Science (B.S) in Computer Science, Jacksonville State University, Spring 2012**

Area of Concentration: Security (Information Security & Assurance), Minor: Math

## **Skills and Knowledge Areas**

- |                                      |                               |   |
|--------------------------------------|-------------------------------|---|
| • Application Security               | • Applied Network Security    | • Vulnerability Analysis                  |
| • AWS & K8s Security                 | • Linux System Administration | • Intrusion Detection                     |
| • Security Related Context-Awareness | • Network Visualization       | • Technical Writing                       |
|                                      | • Honeypot Testing            |   |
| • Machine Learning                   | • Object-Orientated Design    | • Data Mining and Machine Learning Theory |
| • Full Stack Web Development         | • Rapid Prototyping           | • Algorithms                              |
| • Version Control                    | • Usability Testing           | • Programming Languages Theory            |
| • Script Programming                 |                               |   |

## **Professional Societies**

- IEEE Society, 2015- Present
- ACM Society, 2015- Present
- Dev/Color, 2020- Present
- NSBE, 2020- Present

