GAGAN YALAMURI

gagan.y@nyu.edu | +1 (917) 261-1568 | LinkedIn | GitHub | Medium

WORK EXPERIENCE

Information Security Intern, Cantor Fitzgerald *| New York, USA | June 2025 - Present*

- Orchestrated trusted-IP lifecycle across 6+ Azure tenants using XSOAR, GitHub, and Terraform, reducing configuration drift to zero and cutting update time from hours to under 10 minutes.
- Built Splunk-to-XSOAR containment that publishes blocks to EDLs and Cloudflare, reducing mean time to contain from ~30 minutes to under 1 minute.
- Implemented a progressive block policy (15 days then 30 days) with recurrence tracking to harden threat containment and standardize decisions.
- Delivered 15+ Python utilities and 5+ SOAR playbooks, eliminating ~200 hours per year of manual work (about 4 hours per week).
- Streamlined SSL certificate renewals on F5 BIG-IP via AppViewX APIs, avoiding more than 200 hours per year of manual effort.

Open-Source Contributor, Secure Systems Lab *| Brooklyn, USA | August 2024 – November 2024*

- Standardized release signing with CI checks for projects protecting ~$5M in assets; prevented 2048-bit fallbacks and unsigned artifacts.
- Fixed Git and build issues (key-size downgrades, signer trust, merge/submodule drift), shortening release cycles and cutting manual triage time.

Cybersecurity Intern, Garrett - Advancing Motion *| Bengaluru, India | February 2023 – August 2023*

- Integrated MISP and OpenCTI for threat hunting; increased investigation throughput by approximately 30%.
- Hardened cryptographic communications for Mercedes ECU units to resist tampering.
- Prototyped a migration path to post-quantum X.509 for quantum-safe PKI.
- Scripted management for 40+ servers, reinforcing SOC operations and reducing manual interventions.

Summer Intern, HCL Technologies Ltd. *| Remote(India) | June 2022 – August 2022*

- Developed ML-based DDoS prototype (SVM, Logistic Regression), achieving 94% detection accuracy at the SDN layer.
- Utilized classifiers like SVM to accurately classify over 100,000 simulated IPs, segregating fake addresses with high precision.

PROJECTS

Securing Serverless Applications in AWS (Zero-Trust Framework)

- Built a secure serverless environment in AWS (Lambda, API Gateway, WAF, Security Hub) applying Zero-Trust principles.
- Configured IAM least privilege, Secrets Manager for key protection, and WAF rules to block malicious traffic.
- Delivered a working serverless app, risk assessment report, and compliance guide for AWS deployments.

Post-Quantum Cryptography Toolkit (PQCT)

- Developed a Python toolkit implementing Kyber (KEM) and Dilithium (digital signatures) with 40% performance gain via NumPy vectorization.
- Published on PyPI for community use, supporting secure encryption/signatures against future quantum threats.
- Extended toolkit with a hybrid X.509 prototype, enabling gradual migration to quantum-safe PKI.

Splunk SOAR – Adaptive MFA Enforcement

- Automated identity security workflow in Splunk SOAR to detect users without MFA.
- Issued 3 automated warnings, then locked non-compliant accounts pending InfoSec approval for reactivation.
- Reduced manual IAM admin effort and enforced MFA adoption across 1,000+ accounts.

Offensive Security - Exploit Solver Scripts

- Authored 30+ solver scripts for exploit challenges (stack overflows, ROP, shellcode); standardized payload templates and reusable helpers that cut solve time from hours to minutes.

RESEARCH PAPER

➢ Yalamuri, G., Honnavalli, P., & Eswaran, S. (2022). A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats. Procedia Computer Science, 215, pp.834–845. **Cited 50+ times** (https://doi.org/10.1016/j.procs.2022.12.086)

EDUCATION

Master of Science - Cybersecurity (GPA: 4.0/4.0) | New York University | Sept 2024 - May 2026 (Expected)

Bachelor of Technology - Computer Science and Engineering | PES University | Aug 2019 - July 2023

SKILLS

Programming & Scripting: Python, Go, C/C++, Java, Bash, PowerShell, PHP , SQL, JavaScript

Operating Systems & Cloud: Windows, Kali Linux/Ubuntu, macOS, AWS (EC2, S3, GuardDuty, Lambda), GCP , Azure, Kubernetes (GKE), Docker, OT/ICS, IoT

Red/Purple Team & Post-Exploitation: Cobalt Strike, PowerShell Empire, Covenant, BloodHound, Mimikatz, Binary Ninja, Ghidra, Pwntools, GDB, Strace

Recon & Vulnerability Assessment: Nmap, Nessus, OpenVAS, Burp Suite, OWASP ZAP , SQLMap, AppScan, Metasploit, Wireshark, IDS/IPS

Detection Engineering & SIEM: Splunk, Wazuh, AWS GuardDuty/CloudWatch, EDR, custom log pipelines, XSOAR, Xpanse Cloud Suite, Sentinel

DevSecOps & Automation: Terraform, Ansible, GitHub Actions, SAST / DAST pipelines, CloudFox, Azure (IAM, API integrations, App registrations)

Frameworks & Methodologies: MITRE ATT&CK, PTES, OWASP Top 10, NIST SP 800-53, Cyber Kill Chain, Threat Modeling, Risk Assessments