GAGAN YALAMURI

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

SUMMARY

Information Security Engineer with hands-on experience in SOAR engineering, detection automation, threat intelligence across multi-cloud environments. Skilled in Splunk, XSOAR, Terraform and Python automation to normalize and correlate threat data, reducing mean time to contain from 30 minutes to under 1 minute and saving 200+ annual manual hours. Adept at privileged access management, RBAC, maintaining real-time situational awareness for coordinated crisis response.

WORK EXPERIENCE

Cantor Fitzgerald | *Information Security* **Jun 2025 - Present**

- Orchestrated trusted-IP lifecycle across 6+ Azure tenants using XSOAR, GitHub Actions, and Terraform, reducing configuration drift to zero and cutting update time from hours to under 10 minutes.
- Built Splunk-to-XSOAR containment that publishes blocklists to EDLs and Cloudflare, reducing mean time to contain from ~30 minutes to under 1 minute.
- Implemented a progressive block policy with recurrence tracking using Splunk SOAR to harden threat containment and standardize decisions.
- Automated Email Quarantine Release using SOAR, AnyRun and OpenAI to deliver an automated, risk-scored triage path when user requests for release.
- Working on setting up internal MCP server catalogue by mitigating security risks.

NYU Tandon Cybersecurity | *Graduate Assistant, Cloud Security* **Sep 2025 - Present**

- Designed and taught a hands-on AWS GuardDuty lab for the Cloud Security course, with clear runbooks and teardown steps so students could detect and investigate threats end-to-end.
- Mentored students across AWS topics (IAM, S3, VPC, EKS, Vault), troubleshooting labs in office hours and online forums and helping them turn cloud-security concepts into working demos.
- Monitored cloud logs and guided students through incident response scenarios, reinforcing situational awareness and crisis management best practices.

Secure Systems Lab | *Open Source Contributor* **Aug 2024 - Nov 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.

Garrett - Advancing Motion | *Cybersecurity Intern* **Feb 2023 - Aug 2023**

- Unified MISP and OpenCTI for threat intelligence and hunting, automating enrichment and lifting investigation throughput ~30% across SOC workflows.
- Hardened Mercedes ECU cryptography, prototyped post-quantum X.509 migration using KEM and Dilithium.

PROJECTS

Securing Serverless Applications in AWS (Zero-Trust Framework)

- Architected Zero-Trust serverless on AWS (Lambda, API Gateway, WAF, Security Hub), enforcing least-privilege IAM and Secrets Manager-based credential protection.
- Delivered a hardened application with WAF threat mitigation, plus a risk assessment and cloud compliance guide for secure, auditable deployments.

Post-Quantum Cryptography Toolkit (PQCT)

- Built a Python cryptography toolkit implementing KEM and Dilithium signatures, achieving ~40% speedup via NumPy vectorization and optimized NTT routines.
- Released on PyPI with a hybrid X.509 prototype for post-quantum PKI, enabling staged migration to quantum-safe encryption and signatures.

Splunk SOAR - Adaptive MFA Enforcement

- Orchestrated Splunk SOAR playbooks to flag identities lacking multi-factor authentication, send three escalating notices, and auto-disable violators pending security review.
- Drove 2FA enforcement across 1,000+ profiles, reducing IAM administration overhead while strengthening access governance and overall risk posture.

Offensive Security - Exploit Solver Scripts

- Authored 30+ pwntools solvers (buffer overflow, ROP, shellcode) standardizing payload templates and helpers to cut time-to-exploit from hours to minutes.

RESEARCH PAPER

- Yalamuri, G., Honnavalli, P., & Eswaran, S..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

CERTIFICATIONS

- Certified Network Security Professional: The SecOps Group
- Academic Achievers Award: NYU

EDUCATION

New York University | *Master of Science, Cybersecurity* **(GPA: 4.0)** **New York Sep 2024 - May 2026**

PES University | *Bachelor of Technology, Computer Science and Engineering* **Bangalore Aug 2019 - Jul 2023**

SKILLS

- **Programming & Core:** Python, Go, C/C++, Java, Bash, PowerShell, PHP, SQL, JavaScript, Privileged Access Management, Cybersecurity Principles, Analytical Skills
- **Operating Systems & Cloud:** Windows, Kali Linux/Ubuntu, macOS, AWS, GCP, Azure, Kubernetes, Docker, OT/ICS, IoT
- **Red/Purple Team & Post-Exploitation:** Cobalt Strike, PowerShell Empire, Covenant, BloodHound, Mimikatz, Binary Ninja, Ghidra, Pwntools, GDB, Strace
- **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
- **Frameworks & Methodologies:** MITRE ATT&CK, PTES, OWASP Top 10, NIST SP 800-53, ISO 27001, Threat Modeling, Risk Assessments, Vendor Management
- **Security Operations & Incident Management:** Security Operations, Incident Management, Crisis Management