Kalyan Gopalam

Boston, MA | +1 (857) 339-9252 | gopalam.k@northeastern.edu
LinkedIn: linkedin.com/in/gk-eh | **GitHub:** github.com/Kalyan-Deva | **Portfolio:** kalyangopalam.com

Education

Northeastern University **Boston, MA**

M.S. in Cybersecurity | Expected May 2027 | GPA: [Add] | Relevant Coursework: Network Security, Systems Administration, Critical Infrastructure Protection, Database Security

Technical Skills

Offensive Security & Exploitation: CVE Research & Exploitation, PCAP Analysis, Reverse Shell Detection & Crafting, SQL Injection (Offense & Defense), ECDSA/EdDSA Lattice Attacks (Nonce-Reuse), OSINT & Domain Reconnaissance, Network Protocol Fuzzing & DoS, CTF Competition (MetaCTF, MITRE eCTF)

Defensive Security & Monitoring: Snort IDS/IPS (Rule Authoring, NFQUEUE Inline Mode), Wireshark, PCAP Forensics, Intrusion Detection Tuning, Access Control Auditing, Incident Triage & Documentation

Embedded & Firmware Security: ARM Cortex-M0+ (Bare-Metal C), AES-CBC-256 (AESADV Hardware Peripheral), HMAC-SHA256, HKDF Key Hierarchy, DMA-Driven Crypto, HSM Firmware Design, Flash Filesystem Security, PIN Rate Limiting, Fail-Closed Permission Modeling, Raspberry Pi 4

Networking & Protocols: TCP/IP, DNS, DHCP, MQTT, HTTP/S, VLANs, VPN, Firewalls, Wi-Fi Security, Nmap, Port Scanning & Enumeration

Database Security: Oracle DB (DBMS_FGA, DBMS_CRYPTO, VPD, Unified Audit Policies, TDE), PostgreSQL, Fine-Grained Auditing, RBAC, SQL Injection Defense, Privacy-Preserving Databases, Data Dictionary Views

Identity, Cloud & Access Management: SSO, MFA, User Provisioning/Deprovisioning, Zero Trust Architecture, Cloud IAM, Google Workspace, Active Directory/Microsoft Entra, Okta

Web & Full-Stack Development: Next.js 14, React, TypeScript, Node.js, PostgreSQL, BullMQ, Server-Sent Events (SSE), REST APIs, MapLibre GL JS, Zustand, SheetJS, PptxGenJS, SVG Engineering

Languages & Scripting: Python, C (Embedded/Bare-Metal), Java, TypeScript/JavaScript, SQL, Bash/Shell, LaTeX

Tools & Platforms: Git/GitHub, Linux (Ubuntu, Kali), Docker, VMware, Wireshark, Snort, Oracle DB, VS Code

Frameworks & Standards: MITRE ATT&CK, CVE/CWE Taxonomy, OWASP, NIST CSF 2.0, SP 800-53/171, ISO 27001, CIS Controls, Zero Trust Architecture, Threat Modeling (DFD), Supply Chain Risk Management

Experience

NUIoTConnect — Northeastern University **Boston, MA**

Technical Director *Sep 2024 – Present*

- Inherited a technically unfocused 100+ member club with no structured curriculum; redesigned the lab program from scratch to center on hands-on IoT security, network hardening, and offensive security fundamentals, raising member engagement and technical depth across skill levels.
- Designed and delivered end-to-end labs covering MQTT protocol attacks, Snort IDS/IPS configuration, CVE analysis, and network troubleshooting, giving members direct exposure to tools and scenarios mirroring real security operations workflows.
- Secured university funding and coordinated logistics for a five-student delegation to DEF CON 34 (August 2026), managing sponsorship proposals, travel planning, and cross-team coordination from initial proposal through approval.
- Managed equipment inventory, lab infrastructure, and cross-team collaboration across 100+ members, maintaining operational continuity while running concurrent research and competition workstreams.

Sonata Software **Bengaluru, India**

Java Full-Stack Developer Intern *Jan 2024 – May 2024*

- Tasked with reducing deployment friction across development and staging environments where manual validation steps were causing recurring pre-release delays; automated environment validation and configuration checks using Python and Bash, cutting manual errors by ∼25% and standardizing deployment consistency across the team.
- Identified recurring defects in enterprise software behavior that were consuming repeated engineer hours; triaged root causes end-to-end, resolved issues within defined release timelines, and documented resolution steps in structured records so teammates could handle recurrences independently without escalation.
- Owned configuration, deployment, and validation workflows across multiple service environments, ensuring system behavior matched expected specifications before each release milestone.

Flixverse — Early-Stage Startup **Bengaluru, India**

Application Security Analyst *July 2020 – April 2022*

- Served as primary triage point for application-layer security incidents spanning web interfaces, authentication systems, and session management; consistently resolved incidents within turnaround windows and escalated unresolved cases with full technical context to minimize handoff loss.

- Identified provisioning errors and access-control gaps during quarterly user access reviews by auditing account assignments against current role definitions, remediating misconfigurations before they could be exploited.
- Recognized that inconsistent incident records were causing repeated escalations of already-solved problems; authored structured internal technical notes covering incident status, resolution steps, and verification outcomes, improving handoff clarity and enabling consistent, repeatable triage across the team.

Academic Projects & Research

MITRE eCTF 2026 — Team Lead, HSM Firmware on ARM Cortex-M0+ | C, AES-CBC-256, HMAC-SHA256, HKDF, DMA, ARM Cortex-M0+ **Spring 2026**

- Led Team NEU-1 (NeuSense) as Team Lead in MITRE's national embedded security competition; architected the full cryptographic stack for a Hardware Security Module (HSM) running on ARM Cortex-M0+, including AES-CBC-256 via the AESADV hardware peripheral with DMA-driven crypto offload for timing-safe operation.
- Designed a three-tier HKDF key hierarchy (ROOT_SEED → DEVICE_SEED → ENC_SEED/SESSION_SEED), HMAC-SHA256 authentication, PIN rate limiting, and a fail-closed permission model, hardening firmware against physical extraction, side-channel attacks, and fault injection.

Critical Infrastructure Security: Boston Metro Electric Power Grid | Python, Network Analysis, MBRA, Fault Tree Analysis **Apr 2026**

- Modeled the Boston Metropolitan Electric Power Distribution Network as an 8-node graph with an adjacency matrix, computing degree, betweenness, and eigenvector centrality alongside spectral radius to quantify structural vulnerabilities under targeted and random failure scenarios.
- Applied Multi-Criteria Betweenness-based Risk Assessment (MBRA) to rank critical nodes, conducted fault tree analysis on the Downtown Distribution Substation, and framed findings within the DHS Energy Sector cybersecurity framework; submitted to Prof. Themis A. Papageorge, April 2026.

MQTT Broker DoS: Infrastructure Attack & Resilience Analysis | Python, Mosquitto, Raspberry Pi 4, Linux **Fall 2025**

- Deployed a full MQTT broker environment on Raspberry Pi 4 (authentication, ACLs, rate limiting, client topology) to establish a controlled baseline, then executed three attack vectors — retained message flood, wildcard topic storm, and session exhaustion — using custom Python scripts to test broker resilience under adversarial load.
- Drove RAM from 600 MB to 8 GB and traffic from under 1 to 600–700 Mbit/s, achieving complete broker outage (≈49 minutes); isolated root causes per vector, applied targeted mitigations, and documented the full attack-to-remediation cycle as a reproducible runbook.

Snort IDS/IPS Lab: CVE Detection, Rule Engineering & Reverse Shell Detection | Snort, Wireshark, NFQUEUE, Linux **Fall 2025**

- Configured Snort in both passive IDS and inline IPS (NFQUEUE) modes, then authored custom detection rules targeting SQL injection, three high-severity CVEs (CVE-2021-26855 Exchange ProxyLogon, CVE-2022-1388 F5 BIG-IP, CVE-2018-7600 Drupalgeddon), and active reverse shell payloads.
- Validated each signature against live PCAP captures in Wireshark, iteratively tuned rules to eliminate false positives, and produced a structured analysis documenting detection logic, evasion gaps, and recommended IPS policy changes.

BD Alaris 8015 Medical Device Security Analysis | CVE Research, Threat Modeling, DFD **Fall 2025**

- Investigated CVE-2016-9355 (sensitive data exposure) and a newly identified CWE-798 (hardcoded credentials) vulnerability in the BD Alaris 8015 PC Unit infusion pump to understand the full attack surface of a deployed clinical device.
- Produced a complete research deliverable package — term paper, threat model, Data Flow Diagram (DFD), credential XML samples, and presentation deck — translating raw vulnerability data into structured findings with remediation recommendations.

Bounty Hawk: Automated Recon & Reporting Pipeline | Python, Bash, Modular CLI Design **Apr 2024 – Aug 2024**

- Built a modular Python and Bash pipeline to automate service detection, system validation, and configuration checks across networked targets, producing consistent structured output and reducing manual verification effort for repeated recon workflows.
- Wrote full internal documentation covering setup, usage, and output interpretation, enabling independent onboarding by team members with no prior context and reflecting knowledge-base practices central to repeatable security operations.

Leadership & Additional

Author — *Beneath the Shell*: Published book by Kalyan Gopalam; established presence as a technical author alongside academic and security research work.

MetaCTF Competitor: Competed in challenges covering OSINT, lattice-based cryptographic exploitation (ECDSA/EdDSA nonce-reuse attacks), and domain reconnaissance; active participant in university and open CTF circuits.