

Pallavi Srinivasappa

Boston, MA | +1 (617) 412-6383 | pallavii@bu.edu

LinkedIn: [linkedin.com/in/pallavi-dev](https://www.linkedin.com/in/pallavi-dev) | **GitHub:** github.com/pallavi-dev | **Portfolio:** pallaviis.com

Professional Experience

Security & Backend Engineer — FlixVerse (Early-Stage Web3 Startup)

Dec 2021 – Apr 2022

- Configured and maintained security controls and monitoring infrastructure across systems and APIs, assessing risk and implementing best practices that cut exploitable endpoints by an estimated 60%.
- Conducted risk assessments and threat/vulnerability analyses, recommending and validating controls that reduced organizational risk and blocked ~95% of automated abuse traffic.
- Applied governance controls to an AI/automation system, including data redaction and access boundaries to prevent unauthorized access and data exposure through automated workflows.
- Developed incident-response procedures and security documentation, and communicated technical risk clearly to both technical and non-technical stakeholders across 4 core services.

Java Full Stack Developer Intern — Sonata Software

Jan 2024 – May 2024

- Conducted vulnerability assessments and implemented security controls across enterprise systems and data-access layers, remediating all 8 findings from a security review.
- Collaborated with engineering and product teams to integrate security requirements throughout the development lifecycle, supporting secure, on-time releases.
- Supported audits and risk assessments by documenting controls and remediation, communicating findings clearly to technical and non-technical stakeholders across a team of 6.
- Developed and maintained enterprise services serving 5,000+ daily requests, applying secure configuration that reduced average response latency by 30%.

Technical Projects

Azure SOC Home Lab — SIEM/EDR Monitoring, Threat Hunting & Incident Response

- Built a SOC lab monitoring endpoint, cloud, and network telemetry in Microsoft Sentinel (SIEM) across 10+ sources, detecting, analyzing, and responding to potential threats.
- Authored KQL detections mapped to MITRE ATT&CK and ran log/IOC-based threat hunting, surfacing 1,000+ malicious logon attempts and driving incident response.
- Documented detection logic and response procedures on GitHub, aligned to NIST and security best practices.

Enterprise IDS/IPS & Firewall Lab — Network Security, Vuln Scanning & Controls

- Deployed a firewall, Suricata IDS/IPS, and Wazuh SIEM across a segmented network, implementing and configuring network security controls across zones.
- Ran vulnerability scans and endpoint monitoring across VLAN-segmented zones, analyzing risk and remediating findings against MITRE ATT&CK scenarios.
- Documented architecture and hardening standards as reproducible references, reducing false positives by an estimated 50% through tuning.

RuleRecoil — AI/Automation Security & Control Validation — Python

- Built a platform that validates security controls and detections against replayable attack telemetry, classifying each as verified, gap, or false positive to identify and close weaknesses.
- Applied data-exposure and access controls to an AI/automation system, including PII redaction on ingested data and access boundaries, directly relevant to securing LLM integrations and data connectors.
- Documented per-control findings and remediation recommendations across ~125 tests, producing defensible evidence for control validation and reporting.

Technical Skills

Security Infrastructure: SIEM, DLP, Anti-Malware, Intrusion Detection/Response, EDR, Endpoint & Network Security, Security Tool Configuration & Maintenance

Frameworks & Compliance: NIST CSF, PCI-DSS, ISO 27001, Security Controls Alignment, Data Privacy Awareness, Policy & Standards, Audit Support

Risk & Vulnerability: Risk Assessment, Threat & Vulnerability Analysis, Vulnerability Management, Control Validation, Continuous Monitoring, Remediation

AI & Cloud Security: AI/LLM Integration Risk, Third-Party & Data-Connector Security, AWS/Azure Cloud Security, IAM & Access Control, Data Exposure Prevention

IR & Communication: Incident Response Planning, Post-Incident Review, Mac & Windows, Python, PowerShell, Risk Communication to Technical & Executive Audiences

Education

Boston University

Jan 2025 – May 2026

M.S. in Computer Information Systems (Cybersecurity Concentration) | Relevant Coursework: Cybersecurity, Enterprise Cybersecurity Management, Business Network Communications, Database Security, Systems Analysis & Design