

Jeevan Parajuli

Monroe, LA | jeevanparajuli856@gmail.com | [linkedin.com/in/jeevanparajuli856](https://www.linkedin.com/in/jeevanparajuli856) | github.com/jeevanparajuli856

Aspiring Security Engineer with a top 1% global rank on TryHackMe and a passion for defensive security and risk management. Combines hands-on experience in incident response, vulnerability assessment, and Secure SDLC with proven leadership skills. Eager to apply a proactive, analytical mindset to solve complex security challenges.

Education:

University of Louisiana Monroe

Bachelor of Science in Computer Science

Jan 2024 – Dec 2027

GPA: 4.0

Technical Skills:

- **Security Operation & Analysis:** Splunk, Wazuh, SIEM, EDR/XDR, Incident Response, Threat Detection, Log Analysis
 - **Scripting & Automation:** Python, Java, Bash, PowerShell
 - **Frameworks & Vulnerability Management:** MITRE ATT&CK, NIST CF, Threat Modeling, Risk Assessment, Cloud Security, Nessus, Nmap, SOC2, HIPAA
-

Relevant Experience:

Project Lead | University of Louisiana Monroe

Jun 2025 - Present

- Leading a team of four in a project funded by Louisiana Education Board, to develop a secure web platform for AI Ethics and Security training, utilizing Jira for agile project management to serve over 5000+ students.
- Overseeing the implementation of a Secure SDLC, which included an automated CI/CD pipeline and rigorous SAST/DAST analysis that has already identified and remediated 3+ critical authentication flaws using Burp Suite.
- Developing an engaging, 3D-based training game in Unity (C#) projected to increase student engagement by over 90%, while hardening the web platform's APIs to ensure secure integration.

IT Support Technician | University of Louisiana Monroe

Sep 2024 – Present

- Responded to 12+ endpoint security incidents flagged by CrowdStrike Falcon, performing initial triage, isolating compromised systems, escalating detailed host-based reports, contributing to a 97% remediation efficiency rate.
- Improved security and user satisfaction by 40% for over 8,000+ users by assisting IAM operations in Azure AD (RBAC, MFA) and resolving 50+ helpdesk tickets weekly ensuring all accounts and devices adhered to secure baselines.
- Increased helpdesk team efficiency by 90% by authoring clear technical documentation and standard operating procedures (SOPs) for a centralized knowledge base.

Vice-President | Google Developer Student Club ULM

Jul 2025 - Present

- Driving club growth and member participation by directing bi-weekly "CodeClash" competition and serving as a key liaison between students and professionals to plan a university-wide ULM TechExpo for Fall 2025.
-

Research and Projects:

JBEIL- ML Based Lateral Movement Detection | Python, Machine Learning, PyTorch

2025 - Present

- Architecting an enterprise-grade threat detection system from an inductive ML model (IEEE S&P 2024) in collaboration with Dr. Elias Harb(LSU), designed to identify lateral movement TTPs (MITRE ATT&CK T1021) with over 94% accuracy.
- Engineering a scalable Python data pipeline to ingest and process over 100,000 authentication logs per day and refactoring the ML model using PyTorch to improve computational efficiency by over 30% for real-world deployment.

Integrixa- Host-Based File Integrity Monitoring (FIM) Tool | Python, APIs

2025

- Developed a low-overhead, real-time FIM tool for Windows using Python and SHA-256 hashing, achieving a 98% true-positive rate while maintaining system performance with less than 1% CPU overhead.
- Engineered a self-healing watchdog service for continuous protection and integrated the Telegram API for instant alerting, reducing the mean time to detection (MTTD) to under 5 seconds.

Cybersecurity Home Lab & Threat Simulation

2024

- Designed and maintained a virtual lab environment to simulate enterprise attack scenarios, deploying Wazuh (SIEM/XDR) and Splunk to practice threat detection and incident response.
 - Utilized AWS Security Hub to conduct automated security checks, identifying and remediating misconfiguration in IAM and S3, improving overall security score by 60%.
-

Certifications:

- **CompTIA:** Security+, Cybersecurity Analyst (**CySA+**)
- **Coursera:** Penetration Testing and Threat Hunting (**IBM**), Object-Oriented Programming in Java (**UC San Diego**)