# KASHINATH R

Thrissur, Kerala, India | +91 9746376243 | kashinath.rajesh11@gmail.com
LinkedIn: linkedin.com/in/kashinath-r/ | GitHub: github.com/KashinathRajesh

## PROFESSIONAL SUMMARY

**Security Engineering aspirant** with a strong foundation in **Security Automation** and **Tool Development**. Proven experience in engineering **SOAR pipelines**, building Python-based security tools, and hardening infrastructure. Passionate about integrating **DevSecOps** principles and elevating organizational security posture through data-driven threat management.

## TECHNICAL SKILLS

| | |
|---|---|
| **Security Engineering:** | Python (Advanced), Bash Scripting, SOAR (Shuffle), SIEM (Wazuh, Splunk) |
| **Vulnerability Mgmt:** | Malware Analysis, PE File Analysis, Snort, Wireshark, Nmap, Nessus, Burp Suite |
| **Infrastructure & Cloud:** | AWS (EC2, S3), Linux Admin, Network Protocol Analysis (TCP/IP) |
| **DevSecOps:** | Java, Spring Boot, Node.js (Secure Coding & API Security) |

## PROJECTS

**Automated Security Operations Center (SOAR Pipeline) |** *Tools: Wazuh, TheHive, Shuffle*

- **Security Engineering:** Engineered a complete SOC environment by integrating Wazuh (SIEM) with TheHive (Case Management) using Shuffle for orchestration.
- **Automation:** Developed automated **detection mechanisms and playbooks** to handle security alerts, significantly reducing Mean Time to Respond (MTTR).
- **Threat Management:** Configured active response scripts to automatically block malicious IPs and isolate compromised endpoints without human intervention.

**Python-Based Malware Detection Engine |** *Tools: Python, XGBoost, Streamlit*

- **Tool Development:** Built an end-to-end security tool to detect malicious Windows executables, aligning with **security engineering** best practices.
- **Static Analysis:** Automated the extraction of Static PE (Portable Executable) file headers to identify indicators of compromise (IoCs).
- **Performance:** Achieved 99.2% detection accuracy using machine learning, demonstrating strong ability in **scripting for task development**.

**Network Intrusion Detection System (NIDS) |** *Tools: Python, Scapy, Pandas*

- **Infrastructure Security:** Developed a lightweight NIDS to monitor network traffic in real-time, identifying potential vulnerabilities and unauthorized access attempts.
- **Traffic Analysis:** Implemented packet sniffing and protocol analysis to flag anomalies in TCP/UDP traffic, contributing to **infrastructure hardening** efforts.
- **Reporting:** Automated the generation of log reports for traffic analysis, facilitating easier vulnerability remediation and audit trails.

## EDUCATION

**B.Tech in Computer Science & Engineering (Cybersecurity and Digital Forensics)**

Vellore Institute of Technology, Bhopal **|** *2022 - 2026*

CGPA: 8.28 / 10.0

## CERTIFICATIONS

- **Cybersecurity Analyst** – IBM Career Education Program
- **Python Essentials I & II** – Cisco Networking Academy
- **Networking Basics** – Cisco Networking Academy