PRADEEP KUMAR U

✉ pradeep4431k@gmail.com ☎ +91 9025858843 www.linkedin.com/in/pradeep-kumar-u-32b669224

https://pradeepkumaru-cyber.github.io/website/ https://github.com/Pradeepkumaru-cyber/portfolio

SUMMARY

DevSecOps and Cloud Security Engineer specializing in CI/CD security automation, Kubernetes hardening, and enterprise vulnerability management. CEH-certified security professional with hands-on expertise in building secure cloud-native infrastructures and SOC-based monitoring environments. Successfully reduced deployment failures by 35% and improved AI-based defect detection accuracy by 10% through automation, security orchestration, and intelligent system integration. Passionate about engineering scalable, secure-by-design cloud ecosystems.

EDUCATION

B.Tech in Electronics and Computer Engineering (AI & DS) | 2021 - 2025 | CGPA: 8.34 / 10

Karunya Institute of Technology and Sciences, Coimbatore, India

TECHNICAL SKILLS

- **Cybersecurity -** Threat Hunting, SIEM (Splunk, Elastic), Snort, Snyk, Qualys VMDR, OpenVAS, IDS/IPS, Vulnerability Assessment, Risk Mitigation
- **DevOps & Cloud -** Docker, Kubernetes, Jenkins, Git, Terraform, Ansible, Azure DevOps, AWS, Google Cloud, Azure Security Center, CI/CD, Infrastructure as Code
- **Programming & Scripting -** Python, Bash, PowerShell, C#, Java, KQL, SQL
- **Networking & System Security -** VPNs, Firewalls, Access Control, Incident Response, System Hardening

PROJECTS

DevSecOps CI/CD Pipeline Security Implementation

Tools: Jenkins, SonarQube, OWASP ZAP, Docker, Kubernetes, Git

- Built a secure CI/CD pipeline using Jenkins integrating SonarQube (SAST) and OWASP ZAP (DAST).
- Automated Docker image build and security validation, reducing deployment errors by 35%.
- Deployed applications to Kubernetes cluster with controlled rollout strategy.
- Embedded security checks within the development lifecycle to enhance release reliability and compliance.

Kubernetes Security Hardening Lab

Tools: Kubernetes, RBAC, Network Policies, Trivy, Falco, Kube-bench

- Configured RBAC policies and enforced least-privilege access control.
- Applied Network Policies to restrict unauthorized pod-to-pod communication.
- Performed container image scanning using Trivy to detect vulnerabilities.
- Deployed Falco for runtime threat detection, identifying anomalous behavior in container workloads.
- Conducted CIS benchmark assessments using Kube-bench to strengthen cluster security posture.

Automated Vulnerability Assessment Tool

Tools: Python, Nmap, OpenVAS, Linux, JSON Reporting

- Developed a Python-based tool integrating Nmap and OpenVAS for automated vulnerability scanning.
- Conducted port scanning, service enumeration, and vulnerability analysis.
- Implemented severity-based classification aligned with CVSS scoring standards.
- Generated structured security reports for risk prioritization and remediation tracking.

Zero Trust Architecture, SIEM & SOC Network Security Lab

Tools: Suricata, Wazuh, pfSense, Jenkins, Linux, Cloud IAM, TLS

- Implemented Zero Trust access controls with encrypted communication and strict identity verification.
- Deployed Suricata IDS and pfSense firewall for network monitoring, segmentation, and traffic control.
- Integrated Wazuh SIEM for centralized logging, File Integrity Monitoring (FIM), and real-time threat detection.
- Automated secure build workflows using Jenkins and established SOC-style alert monitoring procedures.

INDUSTRIAL PROJECT

- **AI-Powered Defect Detection System – MOHLER Machineries**
  - Enhanced an AI-driven system for real-time bobbin defect detection and automated classification.
  - Integrated AI, electronics, and mechanical systems to Improved defect detection accuracy by 10% through AI-driven classification.

EXPERIENCE

Shop Online New York | Remote

Cyber Security Specialist Intern | Jan 2025 – Apr 2025

- Identified and reported 20+ medium/high severity vulnerabilities.
- Supported static code analysis to identify security flaws in web applications.
- Performed vulnerability assessments using Qualys VMDR and OpenVAS on 50+ endpoints.

CERTIFICATIONS

• Certified Ethical Hacker v12 (CEH)	- ECCouncil
• Google Professional Cybersecurity Certification	- Coursera
• Google IT Certification	- Coursera
• Cisco Cybersecurity Essentials	- Cisco