

Bhargava Reddy Kikkuru

312-989-9914 / bhargavakikkuru@gmail.com / <https://www.linkedin.com/in/kbreddy>

Professional Summary

Security Analyst with practical experience in vulnerability management, endpoint security, and cloud infrastructure protection. I focus on identifying and remediating security risks across macOS, Linux, and multi-cloud environments while automating security processes to improve efficiency. My background includes threat modeling, compliance implementation, and working with engineering teams to build security into products from the ground up. I hold certifications in Security+, CEH, and AWS Security Specialty, with a Master's degree in Cybersecurity.

Previous Experience

B.I.R. Solutions

Reno, Nevada

Cyber Security Analyst

Jun 2024 - Present

- Identify and remediate vulnerabilities across macOS and multi-cloud environments using Nessus, AWS Inspector, and Akamai WAF, reducing high-severity security risks by 40% through systematic scanning and prioritized remediation
- Write security assessments, deployment guides, and technical documentation that help teams implement secure system builds
- Automate patching, compliance enforcement, and endpoint onboarding using Python, Bash, and PowerShell scripts, cutting manual workload by approximately 30%
- Conduct STRIDE threat modeling for CDN and cloud-native solutions, identifying design vulnerabilities early in the development cycle and reducing critical design flaws by 30%
- Collaborate with engineering teams to align security practices with NIST CSF, OWASP Top 10, and MITRE ATT&CK frameworks, improving audit readiness and threat detection coverage
- Build internal tools for cache purging, system diagnostics, and alerting that reduce downtime and improve performance reliability
- Communicate security findings and remediation guidance to technical teams and senior leadership

Chotu - Share Cart Technologies

Hyderabad, India

Cyber Security Analyst

Dec 2020 - Sep 2022

- Implemented and secured high-traffic CDN environments on Akamai and AWS CloudFront, supporting both web and API workloads
- Audited and optimized system and application logs using ELK stack, Prometheus, and CloudWatch to detect anomalies and performance issues
- Developed Python and AWS Lambda scripts for automated log analysis and incident escalation, significantly improving response times
- Partnered with cross-functional teams to strengthen the reliability and security posture of distributed applications

Madiee Games

Chennai, India

Cyber Security Analyst Intern

Jan 2019 - Dec 2020

- Supported SIEM tuning and forensic analysis using tools like Splunk, QRadar, Wireshark, and Autopsy
- Assisted with code and system audits, identifying vulnerabilities and recommending mitigations to improve compliance and system resilience
- Participated in disaster recovery planning and infrastructure hardening efforts

Technical Skills

- **Programming & Scripting:** Python, PowerShell, Bash, Java, React
- **Operating Systems:** Linux, Unix, Kali Linux, Windows, macOS
- **Virtualization & Containers:** Docker, Kubernetes, Proxmox, VirtualBox, VMware
- **CI/CD & Infrastructure as Code:** Jenkins, Terraform, Ansible, GitHub
- **AWS Services:** CloudTrail, GuardDuty, Security Hub, CloudWatch, Lambda, Inspector
- **Cloud Security:** Cloud Infrastructure Security, API Security, Threat Modeling, Cloud Governance
- **SIEM & Monitoring:** Splunk ES, Azure Sentinel, QRadar, MITRE ATT&CK, UEBA, ElasticSearch
- **CDN Platforms:** Akamai (SiteShield, WAF, Cache Control, CP Codes), CloudFront, Cloudflare
- **Monitoring & Observability:** Dynatrace, ELK Stack, Grafana, Splunk, Azure Sentinel
- **Network Security:** Suricata, Snort, Wireshark
- **Forensic Tools:** Wireshark, AWS Athena, Autopsy, FTK Imager
- **Vulnerability Management:** Nessus, AWS Inspector
- **Endpoint Security:** SentinelOne, CrowdStrike
- **Penetration Testing:** Burp Suite, OWASP ZAP, SQLMap, IDA Pro, Metasploit

Education

Illinois Institute of Technology

Master's in Cyber Security

Chicago, IL, USA

Jan 2023 – Dec 2024

Relevant Coursework: Database Security, Cloud Security, Network Security, Incident Response, Threat Modeling

Keshav Memorial Institute of Technology

Bachelor of Technology, Computer Science & Engineering

Hyderabad, India

Jul 2018 – Jul 2022

Relevant Coursework: Data structures, Design and Analysis of Algorithms, Software Engineering

Projects

Interview Proxy Detection System

Python(Flask, sys), Tailwind, mysql

- Objective: Prevent cheating and impersonation in remote interviews by identifying the use of unauthorized remote access tools.
- Outcome: Developed a Python web app that triggers alerts when suspicious software like TeamViewer or AnyDesk is detected during interviews.
- Impact: Increased hiring process integrity by 98% and reduced policy violations using custom threat detection and real-time alerting, aligned with threat intelligence best practices.

OSINT Application for Ethical Data Collection

Python(Tkinter), API(Facebook, Instagram, Twitter)

- Objective: Create a secure GUI application to collect and visualize public social media data for research and analysis.
- Outcome: Built a Tkinter-based app with secure API integration and privacy-focused design, preventing unauthorized data retention or misuse.
- Impact: Delivered ethical OSINT capability aligned with data governance policies, improving research speed and compliance adherence.

Digital Signage Security Platform – Raspberry Pi & Flask

Python(Flask), Tailwind, mysql, linux

- Objective: Design a secure IoT-based digital signage system enabling remote content management with cybersecurity safeguards.
- Outcome: Delivered a Flask-based dashboard with encrypted communications and authentication controls; hardened the system against tampering.
- Impact: Improved remote management efficiency by 40%, mitigated unauthorized access risks, and aligned with NIST and data integrity standards.

Secure Serial Data Monitoring & Visualization System

Python(Flask), Aws, Tailwind, mysql

- Objective: Build a secure data acquisition and monitoring system for industrial RS-485 devices with real-time data visualization.
- Outcome: Used Raspberry Pi, public-key encryption, and secure APIs to protect data in transit; created a real-time dashboard for monitoring.
- Impact: Enhanced industrial cybersecurity posture; improved incident response and observability while meeting GRC and confidentiality requirements.

Certifications

- CompTIA Security+ (SY0-701)
- Certified Ethical Hacker (CEH) – EC-Council
- Certified Cyber Security Technician (CCT) – EC-Council
- AWS Certified Security – Specialty
- TestOut CyberDefense Pro – TestOut Corporation
- Pursuing Microsoft Intune Specialist certification