Raghavendra Kari

314-333-9609 | raghavendrakari@outlook.com | linkedin.com/in/raghavendra-kari | github.com/raghavendrakari

SUMMARY

- Cybersecurity Engineer with 4+ years of experience in application security, SOC operations, vulnerability management, threat detection, and incident response across enterprise cloud and on-premises environments.
- Proven track record of identifying and remediating 150+ vulnerabilities through SAST, DAST, penetration testing, and manual security assessments, reducing critical findings by 45% prior to production releases.
- Experienced in building and automating scalable security tooling, detection pipelines, and compliance workflows using Python and PowerShell, reducing manual effort by 60% and improving threat detection efficiency.
- Hands-on expertise with SIEM platforms, AWS (IAM, CloudTrail, Access Analyzer), threat modeling, secure SDLC, identity and access management, and cross-functional collaboration with engineering and legal teams.
- Holds an MS in Cybersecurity backed by CCNP, CCNA, ISC2, AZ-900, and DHS certifications, with a strong foundation in network security, cloud security, and secure software development.

SKILLS

Security Operations & SOC: SIEM, Threat Detection, Anomaly Detection, Insider Risk Analysis, Security Event Monitoring, Incident Response, Alert Triage, Escalation Management, Threat Hunting

Application Security: SAST, DAST, Penetration Testing, Threat Modeling, Secure Code Review, Vulnerability Management, OWASP Top 10, CI/CD Security, Web Application Security, API Security

Identity & Access Management: IAM, RBAC, TACACS, SSO (SAML, OAuth, OIDC), User Provisioning, Access Reviews, Privileged Access Management, Zero Trust, Directory Services (LDAP, Active Directory), Identity Providers (Okta, Microsoft Entra ID, Ping Identity), Federation, Claims Mapping, Certificate Management, Token Validation

Cloud Security: AWS (IAM, CloudTrail, Access Analyzer, STS, GuardDuty), Microsoft Azure, Cloud Security Posture Management, IaC Security

Network Security: Firewall Management, IDS/IPS, VPN, IPSec, BGP, OSPF, TCP/IP, DNS, HTTP, Wireshark, NetFlow, Packet Analysis

Programming & Scripting: Python, PowerShell, SQL, JavaScript, Java, C, C++, Ansible, Bash, Terraform

SIEM & Log Analysis: Splunk (log analysis, dashboards, alerts, SPL queries), IBM QRadar, Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft Defender for Endpoint, SIEM, Wireshark (packet analysis), NetFlow, Tanium (Comply, Deploy, Patch, Discover, Enforce, Threat Response, Integrity Monitor, Performance, Core Platform), Threat Hunting, Anomaly Detection, Security Event Monitoring

Forensics & Endpoint Security: CrowdStrike Falcon, Autopsy, FTK Imager, Endpoint Detection & Response (EDR), Malware Analysis, Digital Forensics

Frameworks & Compliance: NIST CSF, MITRE ATT&CK, OWASP, ISO 27001, SOC 2, SDLC, Agile, Zero Trust Architecture, CIS Benchmarks

Developer Tools: GitHub, Docker, VS Code, Postman, Jupyter Notebook, Jira, Terraform

EXPERIENCE

Hewlett-Packard (HP) | Senior Security Engineer **October 2023 - Present**

- Identified and remediated 150+ application vulnerabilities through SAST, DAST, and manual security assessments, reducing critical security findings by 45% prior to production releases.
- Performed deep-dive analysis of security datasets, logs, and telemetry to detect anomalies, insider risk indicators, and emerging threats across cloud and application environments.
- Conducted threat modeling for 20+ software projects using MITRE ATT&CK and STRIDE frameworks, enabling early identification of attack vectors and reducing post-release security defects by 35%.
- Integrated automated SAST/DAST security scanning into CI/CD pipelines for 50+ repositories, reducing vulnerability detection time from days to under 1 hour.
- Performed secure code reviews and security assessments for 30+ web applications and APIs, resulting in a 40% reduction in OWASP Top 10 vulnerabilities across development teams.
- Implemented secure authentication, authorization, and IAM controls across 25+ applications following Zero Trust principles, reducing unauthorized access incidents by 50%.
- Led vulnerability management program by triaging and tracking 500+ security findings annually using a risk-based approach, achieving a 95% closure rate within SLA targets.
- Conducted penetration testing and security validation activities uncovering 75+ high-risk vulnerabilities, preventing potential exploitation in production environments.
- Collaborated with engineering and legal teams to develop preventative security controls and remediate critical vulnerabilities, decreasing average remediation time by 60%.

- Designed and automated security reporting and compliance workflows using Python, reducing manual effort by 20 hours/month and improving audit readiness.
- Monitored and investigated security events across cloud and application environments using Splunk and AWS CloudTrail, reducing incident response times by 40%.

Hexaware Technologies, India | Security Engineer I **June 2022 – July 2023**

- Monitored and analyzed 500+ daily security events using SIEM platforms, performing threat hunting and identifying insider and external threat indicators for escalation and remediation.
- Performed vulnerability assessments on 100+ servers, network devices, and applications, reducing critical and high-risk findings by 30% through timely prioritized remediation.
- Supported end-to-end incident response activities including investigation of security alerts, malware infections, and suspicious network traffic, reducing average resolution time by 35%.
- Configured and maintained endpoint security solutions (EDR) across 1,000+ endpoints, improving malware detection and prevention capabilities across the enterprise.
- Supported IAM processes including user provisioning, RBAC enforcement, privileged access management, and periodic access reviews for 2,000+ user accounts.
- Conducted security audits and compliance reviews aligned with NIST CSF and ISO 27001 frameworks, achieving 100% adherence to internal policies and regulatory requirements.
- Performed packet analysis using Wireshark and firewall log analysis to investigate security incidents, reducing investigation time by 40%.
- Automated routine security and compliance checks using Python and PowerShell, reducing manual effort by 15 hours per month and improving detection consistency.
- Assisted in deployment and management of VPN and secure remote access solutions, supporting 500+ remote users while enforcing network access control policies.
- Participated in phishing simulation exercises and security awareness programs, contributing to a 20% reduction in successful phishing attempts across the organization.
- Developed and maintained incident response playbooks and security SOPs, improving operational efficiency and knowledge transfer across the security team.

EDUCATION

Master of Science in Cybersecurity | Saint Louis University, St. Louis, MO **May 2025**

Bachelor's in computer science and applications | KL Deemed To Be University, India **May 2023**

CERTIFICATIONS

- ISC2 Candidate | Certificate 2024
- Cisco Certified Network Professional (CCNP) 2024
- Cisco Certified Network Associate (CCNA) 2024
- Microsoft Certified (AZ-900): Azure Fundamentals 2022
- U.S. Department of Homeland Security: Cybersecurity for ICS 2021
- Oracle Certified: Cloud Associate 2021
- Early Achiever | Microsoft Future Ready Talent Virtual Internship 2022