Harrish Raj *Senior Information Security Engineer*

raj@harrishleth.in +91 8838767615 Portfolio Website Credly badges Harrish Raj aharrishraj1@gmail.com
Bengaluru, KA

Profile

Senior Information Security Engineer with 5+ years of experience in **GRC, Cyber Security, Application Security, Cloud Security, and Information Security** across AWS and GCP environments. Proven track record of uncovering real-world vulnerabilities, leading penetration testing engagements, and **securing cloud-native architectures through risk-driven, attacker-mindset approaches**. Skilled in strengthening **access controls, driving end-to-end remediation, and building scalable security processes that improve organizational resilience**. Experienced in **security control mapping, policy development, and Cloud Activity Monitoring (CAM) initiatives**. Adept at supporting audit readiness and implementing controls aligned with **NIST CSF, CIS Controls, ISO 27001, GDPR, PCI DSS, and HIPAA, + 40 regulations, standards, and framework.** Collaborative cross-functional partner to engineering and product teams, consistently delivering practical, business-aligned security solutions.

Core Competencies

- **Core Skills:** (Cyber Security, Cloud Security, Product Security, Information Security, Risk Management, Governance, Risk & Compliance (GRC), AI Security & Governance, VAPT, AI-Assisted Security Tooling Development)
- **AI:** (LLM-integrated detection pipelines (UEBA + LLM triage), RAG and vector database architecture, LLM context and token optimisation, prompt-injection and AI threat modelling, OWASP Top 10 for LLM & Agentic Applications, MITRE ATLAS)
- **Controls, Frameworks & Benchmarking:** (NIST CSF, NIST 800-53, NIST 800-171, NIST Privacy Framework, CIS Controls v8, CIS AWS & GCP Benchmarks, OWASP Top 10 (Web, API, LLM).)
- **Governance & Compliance:** (ISO 27001/27002/27701, SOC 2, PCI DSS, HIPAA, GDPR, EU DORA, DPDPA, and 40+ global regulations and frameworks)
- **Security Practices:** (Security Control Mapping, Cloud Activity Monitoring (CAM) Policy Design & Implementation, Risk Assessment, Vulnerability Management, Audit Readiness, Policy Creation & Implementation, Security Awareness & Training)
- **Cloud Platforms:** (Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP))
- **Security & Detection:** (SIEM, IDS/IPS, MITRE ATT&CK, Threat Detection & Modelling for On-Prem and Clouds)
- **Tools:** (AWS Pacu, Burp Suite, OWASP ZAP, Nmap, Nikto, Metasploit, Kali Linux, Parrot OS, Nessus, Wazuh, Claude, Vulnerability Management Tool kit etc., (Open-Source Tools))
- **Programming:** (Python, JSON, C++)

Work Experience

Senior Information Security Engineer, Banyan Cloud Inc. May 2024 – Present
Bengaluru, India

- Working on the AI related Project for a product feature and working in RWP project.
- Involved in Auditing Process along with team, with respective regulation and built a custom based GRC PLATFORM for customer.
- Acted as **Technical SPOC** for Client (via MSSP), managing product onboarding and **lead VAPT** engagement simultaneously; previously **delivered VAPT** for an enterprise client across 27 external IPs and Azure cloud infrastructure.
- Designed and implemented an attack-path–driven **Cloud Detection & Response (CDR)** system for **AWS**, mapping attacker navigation across 30+ services using a structured cloud kill chain model, with **risk-scoring logic** to prioritize high-impact attack paths.
- Built hybrid detection combining signature-based guardrails with ML-driven UEBA, enriched via CloudTrail, identity/session correlation, and CSPM posture — improving detection accuracy and reducing false positives.
- Currently, extending the **detection and monitoring capabilities and UEBA Functionalities** and posture management across **Azure, GCP and OCI** Environments.
- Authored **Cloud Activity Monitoring policies** for threat identification/detection and delivered end-to-end attack narratives, improving investigation efficiency and threat visibility.
- Engineered a **Full-stack CWP Vulnerability Prioritisation Dashboard** integrating 13 threat intelligence feeds **(CISA KEV, EPSS, NVD, MITRE ATT&CK STIX, OSV.dev, GHSA, ThreatFox, VulnCheck, Shodan, CIRCL, Red Hat, Ubuntu)** with a composite CVE scoring engine (0–100) weighting **CVSS, EPSS, KEV presence, ATT&CK** correlation, patch availability, and internet exposure with time-decay.
- Designed a three-tier CVE coverage model and a two-tier concurrent patch pipeline (ThreadPoolExecutor with smart-routed fallbacks), reducing patch lookup latency from 36s to under 8s, and resolved NVD's Cloudflare bot-blocking via a browser-direct fetch pattern with OSV.dev fallback.

Information Security Engineer, Banyan Cloud Inc. August 2021 – April 2024
Bangalore, India

- Embedded India BFSI regulatory requirements (RBI, IRDAI, SEBI) into **product architecture, IAM policies, and audit-ready documentation**, enabling compliance for enterprise customers.
- Led security operations and compliance across **multi-cloud and hybrid environments**, driving **control testing, GRC mapping, audit readiness, and risk management**.
- Delivered global regulatory compliance across **GDPR, HIPAA, PCI DSS, ISO/IEC 27001, NIST CSF, and EU DORA**, including **US, UK, and Middle East** frameworks.
- Strengthened cloud security posture by improving **IAM, permission boundaries, RBAC, and security testing** across **AWS, Azure, and OCI**.

- Enhanced product and detection security by applying **CIS Benchmarks** and mapping **MITRE ATT&CK** to cloud services, improving **configuration hygiene and detection coverage**.

Data Security Consultant, Banyan Cloud Inc. May 2021 – August 2021
Bangalore, India

- **Performed security testing across internal environments** to identify vulnerabilities, assess exposure risk, and support remediation efforts, strengthening overall **data protection and security posture**.
- **Partnered with infrastructure teams to implement Data Loss Prevention (DLP)** controls, reducing the risk of **unauthorized data access** and ensuring protection of sensitive information.

Cyber Security Intern - Remote, Virtually Testing Foundation January 2021 – March 2021
California, USA,

Projects

Cloud Detection & Response (CDR) Platform, Attack Path–Driven Threat Detection (Organization Project)

- Designed an attack-path–driven Cloud Detection & Response (CDR) system for AWS to detect advanced threats across multi-service environments.
- Mapped realistic attacker navigation paths across 30+ AWS services using a structured cloud kill chain model.
- Improved threat visibility and investigation efficiency by presenting end-to-end attack narratives.
- Created and Implemented the Cloud Activity Monitoring Policies for threat identification and threat detection based on cloud events...

Shayera AI - A Virtual Assistant for PC, (University Project)

- As a Team of Three Members, We had Create an Actual Virtual Assistant to all supported Computers.
- I'm the Team Lead of this Project, Helping Team-Mates to develop the code in our own way of exposure.
- This Virtual Assistant can be controlled by voice. As this Assistant using Artificial Intelligence to Recognize the user's Voice and Respond.
- This Project is an initial Start to provide an example of my futuristic Model of Shayera - AI.

Threat & Vulnerability Prioritization Platform, CWP vulnerability Dashboard, (Organization Project)

- Engineered a full-stack CWP Vulnerability Prioritisation Dashboard integrating 13 threat intelligence feeds with a composite CVE scoring engine (0–100) weighting CVSS, EPSS, KEV presence, ATT&CK correlation, patch availability, and internet exposure with time-decay.
- Designed a three-tier CVE coverage model and a two-tier concurrent patch pipeline (ThreadPoolExecutor with smart-routed fallbacks), reducing patch lookup latency from 36s to under 8s.

Education

Bachelor of Engineering / Computer Science & Engineering, August 2017 – June 2021
Dhanalakshmi Srinivasan Engineering College / 8.2 CGPA / 3.32-4 GPA Perambalur, India

Higher Secondary Certificate / Computer Science, 2016 – 2017
St. James Matriculation Higher Secondary School / 80.3% / 3.21-4 GPA Trichy, India

Secondary School Leaving Certificate, St. James Matriculation Higher Secondary School / 87% 2014 – 2015
Trichy, India

Certifications

Professional Cloud Security Engineer
Google Cloud - Certified

Cloud Cybersecurity Certificate
Google Cloud - Certified

Certified Cyber Threat Intelligence Analyst
CCTIA - Cyber Training 365

SASE Expert -
CATO Network - Level 1 & 2

Cyber security Specialist Professional Certificate
IBM, ISC2 & Coursera

IBM Cyber Security Analyst
IT fundamentals for Cyber Security
Security Analyst fundamentals

Google IT Support Specialist
Google & Coursera - Specialist

Blue Team Junior Analyst
BTJA - SecurityBlue Team

Ethical Hacking Essentials
Codered by Eccouncil

Certified Red Team Operations Management (CRTOM)
Red Team Leaders

Google Cyber Security Specialization
Google & Coursera - Specialist

Palo Alto Cyber Security Networks Professional
Palo Alto & Coursera - Professional

ISO/ IEC 27001 INFORMATION SECURITY ASSOCIATE
SkillFront - Associate

Cyber Samurai Program in Cyber Defence
IIT Jodhpur (TISC) - Entry-Level

Workshops, In-plant training, Conference & Virtual Internships

Software Engineering Virtual Experience,
JPMorgan Chase & Co

Securing the Digital Frontier - Quaterly Meet-up
Bsides Bangalore

Engineering: Undergraduate & Masters Virtual Internship Platform,
Microsoft

Annual Cybersecurity Conference 2024
Bsides Bangalore

Technology Consulting Virtual Internship,
Deloitte

VulCon CyberSecurity Conference 2026
VulCon

Cyber Security Conference, IOT-Village 2020
CIACON2020