

# KAMALESH JAYAPANDIARAJ ARUMUGAM

Cloud & Offensive Security | DevSecOps, VAPT, OSCP Track

Los Angeles, CA | [karumuga@usc.edu](mailto:karumuga@usc.edu) | +1 (213)-691-4175 | [LinkedIn](#) | [GitHub](#) | [Portfolio](#)

## EDUCATION

### University of Southern California (USC)

Master of Science – Cybersecurity, GPA: 3.85/4

Los Angeles, CA, USA

August 2024 – May 2026

**Relevant Coursework:** INF 519 Foundations & Policy for Information Security, CSCI 530 Security Systems, INF 523 Computer Systems Assurance, ITP 425 Web Application Security, INF 529 Security and Privacy in Informatics, INF 528 Computer and Digital Forensics

### SSN College of Engineering (SSN), Anna University

Bachelor of Engineering (B.E) – Electronics & Communication, GPA: 8.81/10 (Silver Medalist)

Chennai, TN, India

August 2018 – July 2022

**Relevant Coursework:** Data Structures & Algorithms, Operating Systems, OOPS, Computer Architecture, Cryptography, Network Security

## TECHNICAL SKILLS

**Certifications:** eJPT | OSCP (Expected Nov 2025) | CompTIA Security+ | Azure SC – 900 | Oracle Cloud Infrastructure Architect Professional

**Programming & Scripting:** Python, Bash, PowerShell, SQL, Java, C/C++, PHP, JavaScript, YAML, JSON

**Cloud & Infrastructure:** AWS (EC2, Lambda, S3, DynamoDB, SQS, IAM, GuardDuty, Security Hub, Config), Azure AD & Entra ID, GCP, Kubernetes, Docker, Terraform, Ansible, Infrastructure as Code (IaC), Zero Trust Architecture (ZTA), Cloud Security Posture Management (CSPM)

**Security Domains:** Identity & Access Management (IAM, SSO, MFA, Federation, RBAC), SDLC (SAST, DAST, Container Security, Threat Detection & Response (EDR/XDR, Incident Response), Cloud Workload Protection (CWPP, CNAPP), Zero Trust Architecture (ZTA)

**Tools & Frameworks:** Burp Suite, OWASP ZAP, Metasploit, Nessus, Nmap, Wireshark, Postman, Ghidra, Trivy, Semgrep, SonarQube, GitHub Actions, Jenkins, SBOM, MITRE ATT&CK, OWASP Top 10, OWASP ASVS, CWE Top 25, Cloud Security Benchmarks (CIS, NIST 800-53)

## PROFESSIONAL EXPERIENCE

### Keck Medicine of USC

Cloud Security Intern

Los Angeles, CA, USA

October 2024 – Present

- Co-developed the “Keck Cloud Portal,” an **internal tool for secure cloud workload deployments**, integrating Terraform modules, AWS Lambda automations, and policy-as-code controls to streamline provisioning and enforce security by default, reducing deployment time by 40%
- Designed and deployed scalable AWS security architecture** using GuardDuty, CloudWatch, and Security Hub to centralize threat detection anomaly monitoring, and **automated incident response**, reducing mean response time by 60% and cutting security ops cost by 25%.
- Automated security remediation workflows with **Python Lambda functions**, cutting 80% of manual triage tasks to enhance system resilience.
- Developed reusable **Terraform modules and AWS Config Rules** to implement security baseline compliance (policy-as-code), enabling **Cloud Security Posture Management (CSPM)** and reducing misconfigurations across cloud workloads by 40%.
- Built compliance automation pipelines aligned with **HIPAA and CMMC frameworks**, ensuring continuous monitoring and data protection.
- Collaborated with Azure and AWS teams to standardize IAM policies, federation setups and security baselines across **multi-cloud deployments**.

### Oracle Corporation

Associate Cloud Solution Engineer – JAPAC

Bangalore, KA, India

September 2022 – July 2024

- Migrated 20+ workloads on OCI, Kubernetes, and Docker, implementing **Data Loss Prevention (DLP), granular network segmentation, and real-time threat monitoring** to secure production deployments and reduce misconfigurations by 90%.
- Integrated **DevSecOps into CI/CD pipelines** using OCI DevOps and Terraform, enabling automated vulnerability scanning, SAST integration, IaC validation, and secure deployment workflows, cutting release risk by 30%.
- Performed **cloud security assessments and configured IAM policies, Cloud Guard rules, and identity federation setups** to enhance access control, enforce least privilege, and **reduce security misconfigurations** across multi-tenant environments.
- Designed secure IaaS and PaaS architectures** with disaster recovery planning, autoscaling, encrypted backups, and high availability zones to ensure infrastructure resilience, business continuity, and platform security under high load.
- Created proof-of-concepts and demos** (OCI DevOps pipelines, AVDF, Zero Data Loss Recovery Service) to showcase security capabilities to enterprise clients, influencing \$5M+ revenue impact across JAPAC.

### Standardization Testing and Quality Certification (STQC) Directorate w/ IISC Bangalore

Cybersecurity Intern – Vulnerability Assessment & Penetration Testing

Bangalore, KA, India

May 2021 – August 2021

- Conducted **penetration testing and vulnerability assessment** of the ‘Indian Urban Data Exchange’ application (Govt. of India) using **Burp Suite, OWASP ZAP, Postman, and Nmap**, enhancing **application security** and ensuring compliance with national standards.
- Applied **OWASP ASVS Levels 1–3** and aligned findings with **CWE Top 25, OWASP Top 10, MITRE ATT&CK, and NIST SP 800-63**, conducting systematic **threat analysis**, and documenting mitigation strategies for high-risk vulnerabilities across APIs and user flows.
- Conducted **code reviews** on application modules and APIs, identifying insecure input handling and logic flaws; recommended remediations aligned with **secure coding standards** to address risks such as SQL injection, XSS, broken access control, IDOR and session fixation.

## AWARDS & LEADERSHIP

**25<sup>th</sup> in NAMER - Amazon AppSec CTF:** Placed 25/143 in a 48-hr invitational AppSec competition (Secure coding, Web, Cloud, AI) (**Writeup**)  
**Secured 2nd place in the Tenable × CRACCON 2025 Cloud & IAM CTF** – Cloud exposure analysis, CNAPP security, IAM misconfigurations.  
**2nd Runner-Up: USC CTF Competition (Fall 2024)** – Solved web security, forensics, reverse engineering & cryptography challenges. (**Writeup**)  
**Blue Team Lead, WRCCDC 2025** - Defended enterprise systems in a live attack scenario; implemented **SIEM, IAM, and firewall policies**.  
**Satellite Cybersecurity Research @ USC** - SPARTA-based threat modeling of adversarial space-ground cyber operations. (ongoing)

## PROJECTS

### Secure SDLC & DevSecOps Pipeline ([Github](#))

August 2024 – October 2024

- Integrated SAST (Semgrep, SonarQube) and DAST (OWASP ZAP, Burp Suite) into GitHub Actions CI/CD for automated secure code reviews.
- Secured containerized workloads with **Trivy**, implemented **SBOM generation and SLSA compliance** for software supply chain integrity.
- Implemented **contextual alert enrichment and developer feedback loops**, tagging findings with CWE IDs, severity, and remediation guidance, and routing results to GitHub PRs for immediate triage and developer actionability.
- Enhanced CI/CD pipeline efficiency by automating security gates and policy checks**, reducing insecure code deploys by 30% while maintaining rapid release cycles.