KAMALESH JAYAPANDIARAJ ARUMUGAM

Cloud & Offensive Security | DevSecOps, VAPT, OSCP Track
Los Angeles, CA | karumuga@usc.edu | +1 (213)-691-4175 | LinkedIn | GitHub | Portfolio

EDUCATION

University of Southern California (USC) Los Angeles, CA, USA
Master of Science – Cybersecurity, GPA: 3.85/4 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

TECHNICAL SKILLS

Certifications: eJPT | OSCP (Expected Nov 2025) | CompTIA Security + | Azure SC – 900 | Oracle Cloud Infrastructure Architect Professional
Programming & Scripting: Python, Go, 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), Threat Modeling(STRIDE,MITRE ATT&CK)
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 Los Angeles, CA, USA
Cloud Security Intern 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%
- Built a **Go-based REST API** with **Azure AD auth, JWT validation, MySQL, and AWS S3 integration**, enabling secure, role-based workflow automation for institutional approval requests and streamlining internal operations.
- **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.
- **Implemented compliance automation** using **Terraform modules and AWS Config Rules**, aligning with **HIPAA** and **CMMC** to enable **policy-as-code** enforcement and continuous monitoring, cutting misconfigurations by **40%**.
- Collaborated with Azure and AWS teams to standardize IAM policies, federation setups and security baselines across **multi-cloud deployments**.

Oracle Corporation Bangalore, KA, India
Associate Cloud Solution Engineer – JAPAC 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.
- **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 Bangalore, KA, India
Cybersecurity Intern – Vulnerability Assessment & Penetration Testing 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

25th in NAMER - Amazon AppSec CTF: Placed 25/143 in a 48-hr invitational AppSec competition (Secure coding, Web, Cloud, AI) **(Writeup)**
Offensive Security Team Member, CPTC 2025 - Represented USC in a real-world enterprise penetration testing competition. **(Red-Teaming)**
Secured 2nd place in the Tenable × CRACCON 2025 Cloud & IAM CTF – Cloud exposure analysis, CNAPP security, IAM misconfigurations.
Blue Team Lead, WRCCDC 2025 - Defended enterprise systems in a live attack scenario; implemented **SIEM, IAM, and firewall policies.**
2nd Runner-Up: USC CTF Competition (Fall 2024) – Solved web security, forensics, reverse engineering & cryptography challenges. **(Writeup)**

PROJECTS

Secure SDLC & DevSecOps Pipeline (Github) August 2024 – October 2024

- Engineered a **CI/CD-integrated Secure SDLC** using GitHub Actions, Semgrep, SonarQube, ZAP, Burp Suite, and Trivy, automating SAST/DAST/container scanning, SBOM generation, and **policy-as-code gates** for continuous code integrity and software-supply-chain security.

SIEM Implementation with Suricata and Elastic Stack (Github) October 2024 – December 2024

- Deployed a **Suricata-driven SIEM** leveraging **Filebeat → Logstash → Elasticsearch → Kibana**, integrating **rule-based correlation, alert automation, and network telemetry visualisation** to detect and triage **adversarial traffic in real time.**

Active Directory Exploitation & Lateral Movement Lab May 2025 – July 2025

- Built a simulated Active Directory environment using Windows Server 2019 + Kali Linux, performing **Kerberoasting, pass-the-hash, BloodHound enumeration**, and **Privilege Escalation** → Lateral Movement chain mapping aligned with MITRE ATT&CK TTPs.