KAMALESH JAYAPANDIARAJ ARUMUGAM

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

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

SSN College of Engineering (SSN), Anna University — Chennai, TN, India
Bachelor of Engineering (B.E) – Electronics & Communication, GPA: 8.81/10 (Silver Medalist) — August 2018 – July 2022
Relevant Coursework: Data Structures & Algorithms, Operating Systems, OOPS, Computer Architecture, Cryptography, Network Security

PROFESSIONAL EXPERIENCE

Keck Medicine of USC — Los Angeles, CA, USA
Information Security Intern (Cloud Security) — October 2024 – Present

- **Designed and deployed scalable AWS security architecture** using GuardDuty, CloudWatch, and Security Hub for centralized threat intelligence, anomaly detection, and **automated incident response**, reducing response time by 60% and cutting security ops cost by 25%.
- **Automated** security remediation workflows using **Python-based AWS Lambda functions**, reducing manual threat triage and response by 80%, enhancing real-time security response and system resilience.
- Developed reusable **Terraform modules and AWS Config Rules** to implement security baselines (policy-as-code), enabling **Cloud Security Posture Management (CSPM)** and minimizing cloud misconfigurations.
- Engineered **compliance automation pipelines** aligned with HIPAA, HITRUST, FedRAMP, and CMMC, ensuring end-to-end data protection across **multi-cloud environments (AWS + Azure).**

Oracle Corporation — Bangalore, KA, India
Associate Cloud Solution Engineer – JAPAC — September 2022 – July 2024

- Led **cloud security and adoption strategy for enterprise clients** across JAPAC, contributing to $5M+ revenue by driving **secure cloud migrations**, implementing identity controls, and advising on **risk mitigation**, governance, and cost optimization.
- 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%.
- Conducted **code reviews** and built secure applications using Oracle APEX, applying secure coding standards, **input validation techniques**, and protection against SQL injection, XSS, and authentication bypasses to **strengthen application security posture.**
- 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.

Standardization Testing and Quality Certification (STQC) Directorate w/ IISC Bangalore — Bangalore, KA, India
Cybersecurity Intern – Vulnerability Assessment & Penetration Testing — July 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.
- Performed **OSINT research** to collect Indicators of Compromise (IOCs) and delivered threat briefings on emerging attack vectors, correlating data from public repositories, dark web sources, and vulnerability feeds to inform security analysts and **enhance real-time incident response**.

TECHNICAL SKILLS

Certs: eJPT | OSCP (in progress) | CompTIA Security + | Azure SC – 900 | OCI Architect Professional | Oracle APEX Cloud Developer
Technology stack: Python, SQL, Java, C++, PHP, AWS (EC2, Lambda, S3, DynamoDB, SQS), Azure AD, GCP, Kubernetes, Docker, Cryptographic Protocols, Zero Trust Architecture (ZTA), Identity and Access Management (IAM), Infrastructure as Code (IaC) and Linux Bash
Tools: Security tools (Wireshark, Snort, Nmap, Metasploit, Nessus, Burp Suite, Postman, Ghidra), Cloud IAM tools, SIEM tools (Suricata, Elastic Stack, Microsoft Sentinel), Terraform, Ansible, PowerShell, Vulnerability Scanners, Infrastructure Automation, and Threat Detection Frameworks

PROJECTS

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

- Designed and deployed a **custom SIEM pipeline using Suricata IDS** and the Elastic Stack (Filebeat, Logstash, Elasticsearch, Kibana), enabling **real-time detection, log correlation, and threat triaging** across simulated enterprise networks.
- Reduced alert noise by creating **high-fidelity Suricata rules** mapped to MITRE ATT&CK techniques, enhancing detection of reconnaissance, brute-force, and exploitation attempts while **improving signal-to-noise ratio** in security monitoring.
- Automated **secure log forwarding and alert workflows** using **X-Pack** and custom enrichment to support cloud-based detection and triage.

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.

AWARDS & LEADERSHIP

2nd Runner-Up: USC CTF Competition (Fall 2024) – Solved web security, forensics, reverse engineering & cryptography challenges. **(Github)**
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 modelling of adversarial space-ground cyber operations. (ongoing)