Abhilash Pangutty Kumaran

Security Engineer

+44 7570184870
London, RM2 6GE
abhilashpkumars@gmail.com

Security Engineer with 9+ years of experience driving application, cloud, and DevSecOps security across large-scale environments. Proven record in building secure-by-design programs, embedding Shift-Left security into CI/CD pipelines, and automating vulnerability management and compliance controls. Skilled in threat modeling, GCP/AWS security, and enabling teams to deliver securely at speed. Recognised for a hands-on, automation-first approach that strengthens security maturity and aligns with business goals.

PROFESSIONAL EXPERIENCE

Sr Security Engineer at OXA (2023 - Present)

At Oxa, I lead initiatives to integrate and automate security practices across the organisation, ensuring all products meet modern security standards.

- Established and scaled Shift-Left security practices from scratch, embedding security into the development lifecycle through automated checks, developer tooling, and early-stage threat modeling.
- Implemented and maintained organization-wide SAST, Dependency Scanning, Secret Detection, and Container Scanning within GitLab CI pipelines.
- Defined and standardised architecture review and threat modeling processes to identify risks during early design stages.
- Established security maturity models to measure and enhance team-level security adoption.
- Developed and implemented an in house vulnerability management tool that synchronises findings from multiple sources — including GitLab security scans (SAST, DAST, Dependency Scanning) and Google Security Command Center (SCC) into Jira, automatically assigning issues to the right teams for remediation.
- Enforced Shift Security Left principles by introducing merge request-level vulnerability checks and automated pipeline gates.
- Implemented GCP organisation-wide constraint policies to prevent IAM misconfigurations and enforce least privilege, resulting in an 80% reduction in IAM misconfiguration vulnerabilities.
- Maintained GitLab and GCP configurations via Terraform, ensuring all security controls are codified and reproducible.
- Developed executive dashboards visualising the organisation’s security posture, SLA adherence, and vulnerability trends.
- Trained developers on building secure container images and delivered organisation-wide training on container security, resulting in a 40% reduction in vulnerability rate.
- Conducted targeted security training for platform and development teams, and presented key findings during internal “Show & Tell” sessions.
- Supported the Assurance team in implementing technical controls for ISO 27001:2022 certification.

Sr Security Engineer at Locus (2022 - 2023)

At Locus, I led security automation and secure-by-design initiatives across engineering teams, integrating security into development workflows and helping the organisation achieve SOC 2 compliance through robust technical control implementation.

- Implemented and maintained organisation-wide SAST, Dependency Scanning, Secret Detection, and Container Scanning within GitLab CI pipelines.
- Defined and standardised architecture review and threat modeling processes to identify risks during early design stages.
- Conducted security architecture reviews and created a Google Data Studio dashboard to visualize vulnerabilities.
- Automated secret scanning via GitHub organization webhooks.
- Deployed and customised Wazuh for infrastructure monitoring and security alerting.

Freshworks (2019 - 2022)

At Oxa, I lead initiatives to integrate and automate security practices across the organisation, ensuring all products meet modern security standards.

Lead Security Engineer

- Leading & mentoring a team of Security Engineers.
- Planning the security roadmap along with the product stakeholders.
- Implementation of Shift-left initiatives.
- Providing security solutions for various product requirements.
- Engaging in customer queries. Managing bug bounty programs.
- Performing vulnerability assessment & penetration testing on Freshworks suite of products.

Sr Security Engineer

- Implemented and maintained organization-wide SAST, Dependency Scanning, Secret
- Engaging developers and QA folks in training awareness programs.
- Working with developers on security bug fixes.
- Helping the QA folks in understanding and performing basic vulnerability assessments.
- Setting up a CI environment for customized SAST and SCA implementations.
- Performing vulnerability assessment & penetration testing on Freshworks suite of products.

Security Engineer

- Engaging developers and QA folks in training awareness programs.
- Working with developers on security bug fixes.
- Helping the QA folks in understanding and performing basic vulnerability assessments.
- Setting up a CI environment for customized SAST and SCA implementations.
- Performing vulnerability assessment & penetration testing on Freshworks suite of products.

Cyber Security Engineer at Tata Consultancy Services (2015 - 2019)

Within TCS's Cyber Security Practice I delivered assessments and automation for large enterprise clients, combining consulting, tool integrations, and incident response.

- Leading & mentoring a team of Security Engineers.
- Performed web application and vulnerability assessments for global clients.
- Integrated SAST tools into DevOps pipelines for continuous validation.
- Handled security incident management and response for Marks & Spencer UK.
- Conducted thematic security assessments to identify business-impact vulnerabilities.
- Recommended and implemented security tools aligned with client environments.

EXPLOIT TOOLS DEVELOPED

DNS Rebinder:

I have written a dns rebinder tool in golang. It is a light weight dns server which responds with alternate A records with ttl value 0. This tool can be used to exploit Server Side Request Forgery using DNS rebinding technique.
https://github.com/abhilash-pangutty/dns-rebinder

LOG 4J Exploit:

Automated the exploit process by writing the LDAP server and HTTP server to serve malicious class files for achieving Remote Code Execution in the target application using the vulnerable log4j
https://github.com/creativetoken/log4j-exploit

SKILLS

Tools & Platforms:
GitLab CI/CD, Google Cloud Platform (GCP), AWS, Terraform, Docker, Kubernetes

Security Scanning & Automation:
SAST, DAST, Dependency Scanning, Secret Detection, Container Scanning, Vulnerability Management Automation,Snyk, Semgrep

Programming & Scripting:
Go, Python, Java, Bash, Javascript

Governance & Compliance:
ISO 27001:2022, SOC 2, Security Maturity Models, Risk Management, Policy Enforcement

Monitoring & Reporting:
Google SCC, Security Dashboards, SIEM Integration, SLA-driven Metrics

CERTIFICATIONS

- **Professional Cloud Security Engineer Certification**
- **Associate Cloud Engineer Certification**
- **Certified Ethical Hacker (CEH v9) EC Council**
- **ITIL 2011 Foundation Certificate in ITSM Certification- AXELOS BP**

EDUCATION

M.Sc. Cyber Forensics and Information Security
University of Madras, Chennai, Tamil Nadu | 2018 – 2020

Bachelor of Engineering in Computer Science
Shri Shankaracharya Institute of Technology and Management (SSITM), Bhilai, Chhattisgarh | 2010 – 2014

HONORS & AWARDS

- **Hall of Fame - Intel - JUN 2018**
  Appreciated by Intel Security Team for reporting security bug
- **Hall of Fame - Sony - JAN 2019**
  Appreciated by Sony for reporting critical security issues related to their cloud infrastructure.
- **Hall of Fame – Telefonica (Bugcrowd) - JAN 2019**
  Listed in Hall of Fame for reporting security bug
- **Hall of Fame – Cloudsmith.io - Feb 2020**
  Reported an issue http://cloudsmith.ioin cloudsmith.io via responsible disclosure policy.
  Listed in Hall of Fame – https://help.cloudsmith.io/docs/exploits-all-of-fame