Sunil Kumar

📱 +91-6376486690 — 📍 Jaipur, Rajasthan — in linkedin.com/in/tharvid — 🌐 tharvid.in — github.com/tharvid — ✉ stharvid@gmail.com

Professional Summary

A highly skilled Security Engineer with over **4 years** years of experience, currently working at Porch Group. Demonstrates a robust background in Cloud Security, DevSecOps, Incident Response, Security Tool Implementation and Administration, SOC Implementation, and Security Automation. Holds a B.Tech in Computer Science and Engineering, along with certifications such as CompTIA Security+, AWS Certified Security – Specialty, and Google Cloud Certified – Professional Cloud Security Engineer.

Experience

Porch Group, Remote June, 2024 – Present

Security Engineer

- Developed and maintained DevSecOps pipelines integrating SAST, IaC scanning, secret scanning, container scanning, DAST, API fuzzing, and dependency scanning. Automated vulnerability reporting to Jira using custom scripts for 500+ repositories spanning diverse technologies, and implemented ASPM for comprehensive application security monitoring.
- Implemented a SIEM solution integrating 50+ data sources, including custom integrations, parsers, correlation rules, and SOAR response workflows to enhance threat detection and automated incident response.
- Onboarded 30+ AWS, GCP, and Azure accounts into the CSPM solution, managing misconfigurations and indicators of attack in collaboration with account owner teams.
- Conducted gap assessments and supported the implementation of CIS Critical Security Controls across all 18 domains, ensuring PCI-DSS compliance and control alignment.
- Automated simple to complex security processes to enhance efficiency and reduce manual effort using Python, AWS Lambda, and Google Cloud Functions.
- Conducted penetration testing and vulnerability assessments to identify and remediate security weaknesses across applications, APIs, servers, and infrastructure.
- Managed and administered a wide range of security tools and platforms, including XDR, file integrity monitoring, DLP, network firewalls, WAFs, email security solutions, security awareness platforms, Okta, and Azure AD.

ACKO General Insurance, Bengaluru August, 2021 – June, 2024

Security Engineer

- Developed an advanced security system utilizing AWS CloudTrail, Config, Inspector, Detective, Macie, GuardDuty, and Security Hub for detailed logging and real-time monitoring, ensuring continuous security assessment and compliance.
- Seamlessly integrated DevSecOps stages into the DevOps pipeline, automating continuous security measures such as secret scanning, SAST, IaC security, container security, SCA, and DAST.
- Managed the triage of issues reported through bug bounty program, DevSecOps, and AWS/GCP security tools, ensuring timely resolution.
- Designed and implemented security policies for EDR, CASB, MDM solutions, and enforced RBAC, SSO, and Conditional Access across Google Workspace, AWS, and GCP IAM.
- Developed custom security tools, including TPRM, phishing simulations, DNS security tool, reporting solutions, and parsers, to streamline security processes.
- Actively engaged in incident detection and response, utilizing comprehensive strategies to identify and mitigate threats, enhancing the organization's defense mechanisms.
- Conducting in-depth infrastructure risk assessments to proactively identify and address potential security gaps.
- Conducted targeted penetration testing within microservices and API ecosystem to uncover and address security vulnerabilities.

Celebal Technologies, Jaipur February, 2021 – June, 2021

Associate - Cloud Infra and Security Intern

- Developed various proof of concepts (PoCs) focused on M365 Security and related technologies.
- Integrated Okta and Azure AD for streamlined authentication and access management.
- Developed advanced security monitoring dashboards in Azure Monitor and Dynatrace.
- Leveraged Microsoft Defender for Office 365 to enhance email security, delivering real-time protection against malware, viruses, and malicious links.

Netparam Technologies Pvt. Ltd., Remote May, 2020 - July, 2020

Cyber Security Trainee

- Developed strong networking and web application security understanding.
- Worked on different web security tools- Burp Suite, Nmap, Wireshark, Metasploit, Nikto.
- Gained understanding of Linux OS and general security methodologies.

Education

Government Engineering College, Ajmer July 2018 - July 2022

Bachelor of Technology - B.Tech (Computer Science & Engineering) *GPA: 7.94/10.0*

Aastha Academy Senior Secondary School, Sikar July 2016 - July 2017

Science- PCM *Percentage: 89.60/100.00*

Skills

Technologies: Cloud Security, DevSecOps, Security Automation, SOC, Incident Response, Threat Detection, SIEM, Vulnerability Assessment, Penetration Testing, IAM, Security Policy Management, SAST, DAST, IaC Security, SCA, ASPM, CSPM, SOAR, DLP, Security Infrastructure Development

Tools: AWS, GCP, Azure, Python, Google Apps Script, Burp Suite, Nmap, Wireshark, Metasploit, Docker, Jenkins, Git, Kubernetes, OWASP ZAP, Trend Micro, Sophos, CrowdStrike, NetSkope, Cloudflare, CheckPoint, Coralogix, Google Chronicle, Rapid7, Okta, Azure AD

Frameworks/Standards: CIS Critical Security Controls, PCI-DSS, ISO/IEC 27001

Personal Learning Projects

DevSecOps Pipeline with Open-Source Tools

- Implemented a open-source DevSecOps pipeline using Jenkins, integrating open-source tools like Semgrep, Checkov, Trivy, Gitleaks, OWASP ZAP, and AWS ECR scanning. This setup includes custom parsing and reporting of issues to JIRA and DefectDojo for streamlined security management.

Phishing Awareness Platform with Gophish

- Individually developed an phishing awareness platform using Gophish, hosted on AWS EC2 with secure hosting practices, stringent system hardening, and robust access controls. Integrated Amazon SES for email sending, managing large-scale, realistic phishing campaigns to educate employees and significantly enhance email security measures.

Publications

Fuzzing REST APIs for Bugs: An Empirical Analysis - FICTA 2022 Conference, 2023

- Publication Link

Artificial Intelligence in Indian Irrigation - IJSRCSEIT Journal, 2019

- Publication Link

Certifications

- CompTIA Security+
- AWS Certified Security - Specialty
- Professional Cloud Security Engineer Certification
- AWS Certified Cloud Practitioner
- Microsoft 365 Certified: Security Administrator Associate

Languages

English, Hindi