Sunil Kumar

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

Professional Summary

A highly skilled Senior Security Engineer with over 4 years of professional experience, currently working at Porch Group. Demonstrates a strong 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 Professional Cloud Security Engineer.

Experience

Porch Group, Remote — June 2024 – Present

Senior Security Engineer (Nov 2025 – Present)

Security Engineer (Jun 2024 – Nov 2025)

- 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.
- Managed and deployed 10+ Kubernetes clusters into a KSPM platform with runtime protection to monitor and secure workloads in real time.
- Conducted gap assessments and supported the implementation of CIS Critical Security Controls across all 18 domains, ensuring PCI-DSS compliance and control alignment.
- Automated security processes using Python, AWS Lambda, and Google Cloud Functions to enhance efficiency and reduce manual effort.
- Collaborated with global business units, stakeholders, and leadership teams across subsidiaries to close vulnerabilities and enforce security policies enterprise-wide.

ACKO General Insurance, Bengaluru — Aug 2021 – Jun 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.
- Integrated DevSecOps stages into DevOps pipelines, automating security measures such as secret scanning, SAST, IaC security, container security, SCA, and DAST.
- Managed the triage of issues from bug bounty programs, DevSecOps, and cloud security tools, ensuring timely resolution.
- Designed and implemented security policies for EDR, CASB, and 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, and reporting solutions to streamline processes.
- Actively engaged in incident detection and response, enhancing defense mechanisms through deep log analysis and coordinated response.
- Conducted risk assessments and penetration tests to identify and mitigate vulnerabilities.

Celebal Technologies, Jaipur — Feb 2021 – Jun 2021

Associate - Cloud Infra and Security Intern

- Developed proof-of-concepts (PoCs) focused on M365 Security and related technologies, demonstrating early interest in cloud security.
- Integrated Okta and Azure AD for centralized identity management and streamlined authentication.
- Built Azure Monitor and Dynatrace dashboards for proactive threat monitoring and alerting.
- Leveraged Microsoft Defender for Office 365 to enhance real-time email threat protection.

Education

Government Engineering College, Ajmer Jul 2018 – Jul 2022
Bachelor of Technology - B.Tech (Computer Science & Engineering) *GPA: 7.94/10.0*

Skills

Technologies: Cloud Security, DevSecOps, Security Automation, SOC Implementation, 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, Cisco Meraki, DNSFilter, Mimecast, Qualys, Rapid7, Google Chronicle, Okta, Azure AD

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

Personal Learning Projects

Enterprise SOAR Workflow Automation

- Built an enterprise SOAR workflow integrating CheckPoint, Entra ID, Okta, Mimecast, Jira, ServiceDesk, PagerDuty, CrowdStrike XDR, Exchange Online, Google Workspace, AWS, and GenAI-based analysis and enrichment to automate incident response actions triggered from SIEM detections across multiple subsidiaries, reducing MTTR.

DevSecOps Pipeline with Open-Source Tools

- Implemented an open-source DevSecOps pipeline using Jenkins, integrating tools like Semgrep, Checkov, Trivy, Gitleaks, OWASP ZAP, and AWS ECR scanning with automated parsing and reporting to Jira and DefectDojo for streamlined security management.

Phishing Awareness Platform with Gophish

- Developed a phishing awareness platform using Gophish, hosted securely on AWS EC2 with Amazon SES integration to run large-scale phishing simulations and improve employee security awareness.

Certifications

CompTIA Security+

AWS Certified Security - Specialty

Google Cloud Professional Cloud Security Engineer

Docker Foundations Professional Certificate

AWS Certified Cloud Practitioner

Microsoft 365 Certified: Security Administrator Associate

Languages

English

Hindi