Sunil Kumar

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

Professional Summary

A skilled Security Engineer with over 2.7 years of experience, currently working at ACKO General Insurance in Gurugram. Possesses a strong background in Cloud Security, DevSecOps, Incident Response, and Security Automation. Holds a B.Tech in Computer Science and Engineering, along with certifications such as CompTIA Security+ and AWS Security Specialty.

Experience

ACKO General Insurance, Bengaluru August, 2021 – Present

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 - September 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

Hard Skills: Cloud Security, DevSecOps, Security Automation, Data Security and Compliance, SOC, Incident Response, AWS Security, Threat Detection, SIEM, Vulnerability Assessment, Penetration Testing, Security Tool Implementation, IAM, Security Policy Management, SAST, DAST, IaC, SCA

Tools: AWS, GCP, Python, Google Apps Script, Burp Suite, NMAP, Wireshark, Metasploit, Docker, Jenkins, GIT, Coralogix, Trendmicro, Sophos Firewall and Antivirus, Cloudflare, Kubernetes, NetSkope, OWASP ZAP

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.

Internal Phishing Awareness Platform with Gophish

- Individually developed an internal 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

AWS Certified Cloud Practitioner

Microsoft 365 Certified: Security Administrator Associate

Languages

English, Hindi