

Results-oriented IT specialist with more than a year of practical experience in cybersecurity and cloud security. Demonstrated proficiency with Microsoft Sentinel (SIEM), Microsoft Defender for Endpoint (MDE), and Microsoft Defender for Cloud (MDC). 300+ devices were successfully onboarded and configured across SIEM and EDR platforms. Effective configuration and policy tuning have been shown to reduce security incidents by 30% and increase threat detection and mitigation efficiency by 20%. competent in threat analysis, incident management support, and improving security posture through system hardening and practical technical recommendations.

CERTIFICATIONS

- ISC² - Certified Cybersecurity
- [IBM - Cybersecurity Fundamentals](#)
- FCSS - Public Cloud Security 7.6 Architect
- Google Cloud SecOps Technical Credentials
- Virtual Internship in Cyber-Security – Palo Alto

EDUCATION

B. Tech Computer Science & Engg

8.8 CGPA

2020 - 2024

Kolhapur Institute of Technology, Kolhapur

PROFESSIONAL EXPERIENCE

Cloud4c Services | Hyderabad

November 2024 - Present

Associate Cloud Security Analyst

Configured, deployed, and administered Microsoft Sentinel for advanced threat detection and incident response across 30+ client environments. Onboarded new customers end-to-end, integrating 300+ devices with proper workspace configuration and security baseline alignment. Supervised daily operations including health checks, AMA agent troubleshooting, device offboarding, DCR creation/editing, asset validation, and capping analysis with threshold tuning. Built custom KQL-based analytical rules, automated incident workflows via SOAR playbooks, and configured CEF log forwarding. Generated and actioned Microsoft Defender for Cloud (MDC) recommendation reports, implementing remediation to close vulnerabilities and improve compliance

Cloud4c Services | Hyderabad

July 2024 - November 2024

Associate Engineer

Executed disaster recovery procedures and maintained VM host snapshot backups to safeguard data integrity. Monitored cloud infrastructure performance and resource utilization to ensure high availability. Escalated critical incidents, performed root cause analysis, and troubleshot network to minimize downtime.

Cloud4c Services | Hyderabad

February 2024 - May 2024

Associate Engineer Trainee

Acquired in-depth knowledge of cloud computing, data center operations, operating systems, and networking. Gained foundational expertise in cloud architecture, virtualization, security principles, and infrastructure management.

Spiderweb Technologies | Ahmedabad (Remote)

May 2024 - October 2024

PHP Developer & Database Intern

Contributed to the development of Beyond Space, an e-commerce furniture platform for a Dubai-based client during an internship at Spiderweb Technologies. Designed and implemented the database architecture, integrated backend connections in PHP, and improved UI/UX design to enhance user engagement and ensure a seamless shopping experience.

SKILLS

- Microsoft Sentinel
- Microsoft Defender for Cloud (MDC)
- Microsoft Defender for Endpoint (MDE)
- SIEM, SOAR, CSPM, EDR, XDR
- Python (80%)
- KQL (Basic)
- PHP, SQL, Database
- HBSS, CyberArk
- Windows, Linux
- Computer Networking
- Logic Apps
- Azure WAF