Atharva Sardesai

Cybersecurity Consultant

☎ +91 94235 21051 atharvapsardesai@gmail.com
🏠 Pune, Maharashtra, India in [LinkedIn](#) 🌐 [Cyber With Atharva](#)

Summary

Cybersecurity enthusiast dedicated to safeguarding digital assets through effective Security Information and Event Management (SIEM). Specializing in log analysis, threat detection, vulnerability management, and incident response strategies, I proactively monitor and secure digital environments. Experienced in cloud security, malware analysis, and automation with strong problem-solving skills.

Areas of Expertise

SIEM Solutions - Log Analysis & Threat Detection - Vulnerability Management - Cloud Security Monitoring - Malware Analysis

Online Courses & Certifications

- Blue Team Junior Analyst - Security Blue Team

- Google Cybersecurity Certificate - Google

- Architecting Solutions on AWS - Amazon Web Services

- AWS Security Fundamentals - AWS Skill Builder

Skills

SIEM & Log Analysis
- Analyzed and correlated logs from servers, firewalls, and IDSIPS to detect security incidents.

- Automated log analysis using Splunk, ELK Stack for faster incident detection and response.

Threat Detection & Malware Analysis
- Investigated and reverse-engineered malware using tools such as Wireshark, Fiddler, Process Hacker, and Anyrun.

- Configured sandbox environments (Cuckoo Sandbox) for safe malware analysis and reporting.

Vulnerability Management & Web Security
- Identified and mitigated OWASP Top 10 vulnerabilities using Burp Suite, OWASP ZAP.

- Conducted penetration testing and security assessments for cloud-based applications.

Cloud Security
- Implemented security controls for AWS & Azure, utilizing CloudTrail, CloudWatch, and Azure Monitor.

- Conducted CSPM scans using Prowler and generated actionable reports.

Automation & Scripting
- Developed Python/Bash scripts to automate security tasks, log parsing, and report generation.

- Created SIEM automation rules for efficient threat correlation and incident response.

Experience

Cybersecurity Consultant (Intern) *06/2024 - Present*
SecComply

- Perform in-depth security assessments of cloud environments, identifying configuration issues, mismanagement risks, and potential vulnerabilities.

- Utilized tools like Prowler, Cloud Custodian, and CSPM platforms to evaluate cloud security against industry best practices and compliance standards.

- Perform manual and automated testing to identify hidden risks and analyze potential threats and exploitation scenarios.

- Compile detailed vulnerability reports, providing clear risk analysis, root cause identification, and actionable mitigation recommendations.

Education

B.Tech Information Technology *Vishwakarma Institute of Information Technology* **Pune** *(2021-2025)*
12th HSC *Arihant Junior College of Arts, Commerce and Science* **Pune** *(2021)*
10th CBSE *Sainik School Satara* **Satara** *(2019)*

Projects

Security Operations Center (SOC) Lab using ELK Stack
- Designed and implemented a SOC lab on Oracle Cloud using Elasticsearch, Logstash, and Kibana (ELK).

- Developed custom log parsers and alert rules to detect security misconfigurations and attacks.

Portfolio Website :
- Designed and deployed a responsive portfolio website using AWS Amplify.

- Integrated an AWS Lambda function to dynamically update blog posts from Medium.

- Configured AWS API Gateway for efficient API request handling.

Position of Responsibility

President *09/2023 - 09/2024*
Information Technocrats Students Forum, VIIT
Human Resource Manager *08/2022 - 09/2023*
Information Technocrats Students Forum, VIIT
Social Media and Publicity Team *08/2022 - 09/2023*
Office of International Relations, VIIT