# SWAPNIL VELHAL

SOC Analyst

91-7507316206 swapnilvelhal006@gmail.com Pune,India

## SUMMARY

Results-driven SOC Analyst with a 3 years of hands on experience in monitoring, triage, analysis, and swift response to security incidents. Proficient in leveraging industry-leading tools like SIEM, IDS/IPS, Firewall, AV/EDR, Email Gateway, and Web Proxy for effective cyber threat detection and mitigation.Notable expertise in conducting in-depth investigations, implementing robust security measures, and collaborating with cross- functional teams to fortify organizational defenses. Known for fostering collaboration, I excel in working with fellow security professionals to elevate the overall security posture of organizations. Adept at preserving the integrity of networks and systems, I am committed to staying abreast of emerging security trends Seeking to apply my skills and experience in a challenging SOC Analyst role within a dynamic cybersecurity team.

## EXPERIENCE

### SOC Analyst

**AARNA Technologies Pvt. Ltd.**

Jan 2022 - Present Pune

Technology company specializing in cybersecurity solutions.

- Conduct proactive monitoring and efficient triage of security events.
- Investigate all security alerts, utilizing tools and log files to differentiate whether the event is a false positive or a security incident.
- Recognize potential, successful, and unsuccessful intrusion attempts through reviews and analyses of relevant event details.
- Monitor diverse security events and logs for situational awareness.
- Investigate reported suspicious emails, categorize them, and respond to users.
- Collect and analyze threat intelligence feeds, investigating potential Indicators of Compromise (IOCs).
- Develop SOC monitoring use cases to proactively detect emerging threats.
- Fine-tune SIEM rules to minimize false positives and eliminate false negatives.
- Monitor the health of security sensors and SIEM infrastructure.
- Deliver concise SOC reports to senior management,outlining the current security status and recent incidents,threat trends and control effectiveness.

## EDUCATION

### B.E Mechanical

**Shivaji University**

## KEY HIGHLIGHTS

Proactively detected threats through continuous event monitoring and Triage.

Investigated and classified security alerts for rapid response.

Mitigated intrusion attempts, ensuring a secure environment.

Monitored events from various sources for comprehensive threat analysis.

Responded swiftly to suspicious emails, enhancing security measures.

Collected and reviewed threat intelligence for proactive defense.

Optimized SIEM rules for accurate threat identification.

Contributed to maintaining a 24x7 security operations center for continuous vigilance

## SKILLS

SIEM-Splunk

EDR- Crowdstrike

Firewall- Palo alto

Email Gateway- Proofpoint, Symantec

Web Proxy- BlueCoat, Zscaler

Web Application Firewall- Imperva

Anti-Malware - Symantec Endpoint, McAfee

IDS/IPS- Tipping point, McAfee

Ticfieting Tools-Remedy Smart IT, ServiceNow

Malware Analysis-Wireshark, McAfee ATD, Anyrun, Hybrid Analysis