

CHINMAY VAIBHAV MEVEKARI

9595458910 | chinmaymevekari@gmail.com | <https://www.linkedin.com/in/chinmay-mevekari-054329229>

PROFESSIONAL SUMMARY

SOC Analyst with 6+ months of industry experience, skilled in threat detection, incident response, and vulnerability assessment. Certified Ethical Hacker (CEH v13 – Practical) with hands-on expertise in SIEM (Wazuh, QRadar, Splunk), XDR, and cloud security (AWS, Prisma Cloud). Strong foundation in network security, ethical hacking, and VAPT.

EDUCATION

B.Tech CSIT (Cyber Security), Symbiosis Skills And Professional University, Pune – 2025
CGPA: 8.1

CERTIFICATIONS

- Certified Ethical Hacker (Practical) v13

EXPERIENCE

SOC Analyst Intern | Lentra AI Pvt Ltd, Pune (May 2025 – Present)

- Worked in the Security Operations Center focusing on real-time threat detection and incident analysis.
- Monitored logs and alerts using Wazuh SIEM integrated with AWS services.
- Fine-tuned detection rules to reduce false positives and improve alert accuracy.
- Performed incident analysis and reporting using Cortex XDR.
- Assisted in securing cloud environments using Palo Alto Prisma Cloud.
- Contributed to internal Vulnerability Assessment and Penetration Testing (VAPT) and prepared detailed reports.

SOC Analyst L1 | SPK Infrahack Cyber Forensic Pvt Ltd, Pune (Jan 2025 – May 25)

- Conducted proactive monitoring, investigation, and mitigation of security incidents.
- Performed log analysis using IBM QRadar.
- Investigated firewall, email, web, and DNS logs to identify and mitigate intrusion attempts.

Penetration Tester Intern | Cyber Secured India (Jun 2023 – Aug 2023)

- Conducted penetration testing on web applications using Burp Suite.
- Performed attacks using tools such as Nmap, Metasploit, Wireshark, and Hydra.
- Prepared detailed reports on findings from penetration testing activities.

PROJECTS

1. **AWS SIEM for Security Monitoring** | AWS CloudWatch, CloudTrail, GuardDuty, Security Hub
 - Designed and implemented a SIEM solution using AWS services for centralized log management.
 - Configured AWS CloudWatch alarms for suspicious activity detection.
 - Enhanced threat visibility by integrating AWS Security Hub and GuardDuty.
2. **Automated Penetration Testing Tool** | HTML, CSS, JavaScript, Python
 - Developed a web application for automated penetration testing based on OWASP Top 10 vulnerabilities.
 - Implemented features to auto-generate reports with severity-based classifications.
 - Enabled real-time penetration testing on target web applications using integrated libraries and APIs.

TECHNICAL SKILLS

- SIEM & EDR/XDR: Wazuh, QRadar, Splunk, Cortex XDR
- Cloud Security: AWS (CloudWatch, CloudTrail, GuardDuty, Security Hub), Palo Alto Prisma Cloud
- Penetration Testing Tools: Burp Suite, Metasploit, Wireshark, OWASP ZAP, Nmap, SQLmap
- Network Security: Firewall & IDS/IPS Management, ACLs, Network Penetration Testing
- Scripting Languages: Python, PowerShell, JavaScript
- Compliance & Governance: NIST CSF, ISO 27001, PCI-DSS, GDPR
- Operating Systems: Linux, Windows 10

ACHIEVEMENTS

- Certified Ethical Hacker (CEH v13 Practical).
- Captain of University Football Team.
- Actively participated in technical events including CTFs, poster-making, and cybersecurity competitions.