Omkar Hiremath

CYBER SECURITY ENGINEER

Phone: +91 8904874619

e-mail: omkarhiremath4619@gmail.com

Tools and Technologies

- Incident response & forensics
- Vulnerability scanning (Nessus, OpenVAS)
- Penetration testing (Burp Suite, Metasploit)
- SIEM management & alerts
- EDR (CrowdStrike, Carbon Black)
- Network security (firewalls, IDS, VPNs)
- MFA & access control
- Security automation (Python, PowerShell)
- DLP (Data Loss Prevention)
- Compliance (ISO, PCI, NIST)
- Usage of Wireshark and Zeek
- Log analysis & threat hunting
- Risk assessment & mitigation
- Security policy enforcement
- Usage of CanIphish
- Security awareness training
- Encryption (data at rest/in transit)
- Business continuity, DR planning
- Cloud security architecture
- Secure coding & app security
- Phishing campaign & user training
- IAM beyond AWS (AD, LDAP)
- Firewall & perimeter config
- Malware analysis & sandboxing
- Security governance & audit
- PAM (Privileged Access Management)

Professional Overview

Cyber Security Engineer with over **3 years** of experience helping businesses protect their web applications and AWS cloud environments. Focused on building and maintaining security systems, handling vulnerability assessments, and responding to incidents, I have hands-on experience with SIEM, EDR, and cloud-native security tools. I enjoy streamlining security operations through scripting, integrating compliance steps in deployment workflows, and working with Docker to keep environments stable. I'm comfortable collaborating across teams with Jira, and aim to deliver security solutions that are practical, reliable, and support how organizations work.

Work Experience

Senior Analyst III **25-Oct-2022 to Till Now**

DXC Technologies

Education Details

BE - Computer Science

Guru Nanak dev engineering college, VTU

2022-04 (60%)

Plus 2

Sri Chaitanya Jr College, Hyderabad

2015-06 (91.8%)

SSLC

Guru Nanak Public School, Bidar

2013-06 (70.3%)

Personal Details

Father	**Vaijinath**
Mother	**Saroja**
PAN	**ARRPH3341M**

Roles and Responsibilities

- Monitored and analysed security events through Splunk and Qradar to quickly detect and respond to potential threats.
- Actively investigated and resolved live security incidents, helping reduce breach risks by around 40%.
- Performed 200+ vulnerability scans each year using Nessus and OpenVAS to identify system weaknesses.
- Built automated alert workflows that helped cut average detection time by over one-third.
- Worked closely with IT teams to contain and remediate 20+ critical security incidents this year.

- Maintained detailed incident documentation to meet ISO 27001 and PCI DSS compliance standards.
- Supported malware investigations and forensic analysis for suspicious systems.
- Fine-tuned SIEM correlation rules to handle new phishing tactics, cutting down false positives.
- Designed and tested new SIEM use cases, improving overall threat detection by 25%.
- Analysed phishing campaigns, retrained staff, and improved detection success by 60%.
- Conducted root cause analysis after major incidents to close exploited vulnerabilities.
- Regularly updated playbooks to address new ransomware and DDoS attack methods.
- Led tabletop drills and red/blue team exercises to strengthen SOC response readiness.
- Gathered digital evidence for ongoing investigations and regulatory reviews.
- Prevented 95% of brute-force login attempts targeting Active Directory.
- Handled GDPR-related incident log analysis to support compliance reviews.
- Automated IOC hunts across endpoints using custom Python scripts.
- Built executive dashboards to track key security metrics and risk trends.
- Delivered security awareness training for over 200 employees, focusing on phishing and social engineering.
- Hardened both Windows and Linux servers following CIS security benchmarks.
- Reviewed firewall and WAF logs to identify signs of lateral movement.
- Deployed geo-blocking policies on network devices to limit external threats.
- Managed 24/7 alert queues to ensure continuous monitoring and fast response times.
- Integrated threat intelligence feeds into the SIEM for improved detection accuracy.
- Tuned IDS/IPS signatures to better protect critical business applications.
- Applied the MITRE ATT&CK framework to map and address detection gaps.
- Led response efforts for Business Email Compromise (BEC) incidents.
- Produced monthly reports highlighting key incident trends and SOC performance.
- Secured AWS and Azure workloads using built-in monitoring and compliance tools.
- Performed patch compliance checks on over 500 endpoints.
- Managed endpoint protection policies through EDR platforms.
- Maintained updated runbooks and incident response documentation.
- Oversaw log retention and archival to meet both regulatory and internal policy requirements.
- Spearheaded the deployment of Multi-Factor Authentication (MFA) across the organization.
- Ran phishing simulations and tracked employee improvement over time.
- Coordinated with IT and business teams to resolve escalations for critical incidents.
- Evaluated SIEM performance and recommended configuration improvements.
- Provided L1/L2 incident response support for escalated cases.
- Executed endpoint isolation during active compromise situations.
- Conducted privileged access audits to protect sensitive systems.
- Collaborated with purple teams and penetration testers to improve detection coverage.
- Managed patching and remediation for known vulnerabilities (CVEs) within SLAs.
- Tracked patch compliance and followed up on overdue vulnerabilities.
- Mentored junior analysts and interns on SOC monitoring and investigation skills.
- Stayed up to date with new threat indicators via intel feeds and security communities.
- Authored after-action reports summarizing incident learnings and prevention strategies