Jai Padhiar

Cloud Security Engineer | Ethical Hacker | Cybersecurity Analyst

jaiipadhiar@gmail.com | 8000545506 | Ahmedabad, Gujarat | LinkedIn | Portfolio

Summary

Cloud Security Engineer specializing in EDR/XDR (CrowdStrike, TrendMicro Vision One), Penetration Testing and AWS security. Reduced incidents by 47% and secured 500+ endpoints at Operisoft. Completed 25+ penetration tests and red team projects. Hold 45+ certifications including ISC2 CC, Microsoft SC-200, and TrendMicro Vision One Advanced.

Skills

- **Cloud Security:** AWS WAF, VPC Security, AWS CloudTrail, AWS SNS, Network ACLs
- **Endpoint Security:** CrowdStrike EDR, Qualys VMDR, Bitdefender, Trend Micro
- **Security Tools:** Nmap, Metasploit, Burp Suite, Prompt Engineering
- **Vulnerability Management:** Penetration Testing, VA/PT, SQL Injection, XSS Mitigation, OWASP Top 10
- **Languages & Scripting:** Python (Scripting), PowerShell
- **Operating Systems:** Linux, Windows
- **Professional Skills:** Incident Response, Security Documentation, Stakeholder Management

Professional Experience

Cyber Security Engineer, *Operisoft Technologies Pvt. Ltd.* 12/2024 – Present
Ahmedabad, India

- Deployed CrowdStrike EDR across 500+ endpoints with custom firewall rules and detection policies, reducing security incidents by 47%
- Implemented Qualys Cloud Agent for continuous vulnerability management, achieving 100% attack surface visibility and automating compliance reporting (saving 80% manual effort)
- Conducted security requirement gathering with enterprise clients and developed comprehensive security documentation, improving implementation efficiency by 30%

Penetration Tester (Apprenticeship), *Cyber Octet Pvt. Ltd.* 07/2021 – 05/2022
Ahmedabad, India

- Executed 25+ comprehensive penetration tests on web applications, identifying and remediating critical vulnerabilities including SQL injection, XSS, and authentication bypass flaws
- Secured high-traffic platforms for Lok-Patrika and AllEvents by discovering and mitigating 15+ critical OWASP Top 10 vulnerabilities, preventing potential data breaches
- Automated security testing workflows using custom Python scripts, increasing assessment efficiency by 40% and standardizing reporting processes

Education

Master of Computer Application(MCA), *Institute of Technology, Nirma University* 08/2023 – 04/2025
Grade: 8.51

Bachelor's of Computer Application (BCA), *Kadi Sarva Vishwavidyalaya* 03/2020 – 04/2023
Grade: 8.48

Projects

Real-Time Browser Log Tracker, TabTrail, *Ethical Hacking*

- Built Flask-based browser activity tracker monitoring Chrome/Edge/Brave with 100% tab visit coverage for security auditing
- Implemented role-based authentication and session management, preventing unauthorized access to sensitive browsing logs
- Deployed real-time dashboard for incident investigation, reducing log analysis time by 60%

Internal Threat Monitoring & Alert System, *Ethical Hacking*

- Built real-time monitoring system detecting suspicious internal activities including privilege escalation and data exfiltration attempts
- Integrated AWS SNS for instant alert dispatch to security team, reducing mean time to detect (MTTD) by 70%
- Monitored critical file access, unauthorized command execution, and abnormal network connections across endpoints

Anti DDoS/DDoS Protection Script, BlackHole, *Web Application Security*

- Designed Python-based DDoS detection engine achieving 95-98% accuracy using traffic pattern analysis and rate limiting
- Automated threat mitigation by dynamically updating AWS Network ACLs, blocking 1000+ malicious IPs in real-time
- Integrated AWS SNS alerts and CloudWatch metrics, reducing incident response time from 15 minutes to under 2 minutes

Ransomware Simulation Tool for IR Training, *Red Teaming*

- Developed PowerShell-based ransomware simulator for controlled red team exercises in isolated lab environments
- Simulated file encryption, ransom note delivery, and C2 communication to validate incident response procedures
- Provided actionable insights improving backup recovery time by 40% and enhancing endpoint detection capabilities

Certificates

- Certified in Cybersecurity (CC) - **ISC2**
- Trend Vision One Security Operations (Advanced) - **TrendMicro**
- SC-200: Microsoft Defender XDR - **Microsoft**
- Network Defense Essentials (NDE) - **EC-Council**
- Advanced Diploma in Ethical Hacking - **Cyber Octet**
- Azure Fundamentals - **Microsoft**
- Ethical Hacker: Hacking Techniques - **Infosys**
- Cybersecurity Professional - **Google**
- Certified Zero Trust Cyber Associate (ZTCA) - **Zscaler**