ADITYA KUMAR GOSWAMI

Vadodara, Gujarat | +91 9726279007 | akgoswami185@gmail.com
LinkedIn: linkedin.com/in/aditya-kumar-goswami | GitHub: github.com/Aditya-Sec

PROFESSIONAL SUMMARY

Cybersecurity professional with 1.5+ years of experience in SOC operations, incident response, and vulnerability management. Skilled in SIEM tools (Kibana, Wazuh, Suricata), threat analysis, and automation. Focused on enhancing detection accuracy, minimizing false positives, and strengthening enterprise security posture.

CORE COMPETENCIES

SOC Monitoring & Threat Detection | Incident Response | Log Analysis | VAPT | Cloud Security (AWS, Azure) | SIEM & SOAR | DFIR | ISO 27001 Compliance | Automation & Dashboarding

PROFESSIONAL EXPERIENCE

Associate SOC Engineer | Investis Digital Pvt. Ltd. (IDX)
May 2024 – Present | Vadodara, Gujarat

- Monitored and analyzed threats using Cloudflare WAF, Symantec, and AWS CloudWatch for 24x7 infrastructure security.
- Performed log correlation and incident triage in Kibana and Wazuh, escalating high-severity alerts promptly.
- Conducted vulnerability assessments using Nmap, Nessus, Burp Suite, and ZAP to identify exploitable weaknesses.
- Collaborated with DevOps for AWS WAF tuning, SSL automation, and audit readiness documentation.
- Managed and triaged 10,000+ security alerts across cloud and on-prem environments; received the *Rising Star Award* for exceptional performance.

EDUCATION

Bachelor of Science (Forensic Science) – Specialization: Cyber Forensics
Parul University, Vadodara, Gujarat | 2021 – 2024
CGPA: 9.47 | **Gold Medalist**

CERTIFICATIONS

Cybersecurity & Blue Team

- (ISC)^2 Certified in Cybersecurity – (ISC)^2
- Blue Team Junior Analyst – Security Blue Team
- SOC Level 1 & 2 – TryHackMe
- SC-900: Microsoft Security, Compliance & Identity Fundamentals – Microsoft

Governance, Risk & Compliance (GRC)

- ISO/IEC 27001:2022 Lead Auditor – Mastermind
- ISO/IEC 27001:2022 Internal Auditor – Quality Asia

Cloud & Infrastructure Security

- AWS Cloud Practitioner Essentials – AWS
- AWS Security Fundamentals – AWS

Red Team / VAPT

- Certified Ethical Hacker (CEH) – Cisco
- Multi-Cloud Red Team Analyst – CyberWarFare Labs

Digital Forensics & DFIR

- Digital Forensic Essentials (DFE) – EC-Council
- Network Defense Essentials (NDE) – EC-Council
- OS Forensics V10 Triage Certification – PassMark Software

PROJECTS

SOC Lab – Open Source Threat Detection Setup
Built a full-stack SOC using Kibana, Wazuh, Suricata, TheHive, and Cortex for real-time log monitoring, alerting, and automated incident enrichment.

ReconVeritas – Automated Recon Tool
Developed a Python-based automated reconnaissance framework integrating tools like Nmap, Subfinder, and Whois for asset discovery and vulnerability mapping.

RedTeam WAF Detection & Bypass Lab
Designed a simulated WAF environment to perform detection, bypass, and payload evasion testing for web application security validation.