ADITYA KUMAR GOSWAMI

Vadodara, Gujarat | +91 9726279007 | akgoswami185@gmail.com

LinkedIn | GitHub | Portfolio

PROFESSIONAL SUMMARY

Cybersecurity Analyst with 1.5+ years of hands-on experience in **SOC Operations, Vulnerability Assessment, and Cloud Security**. Adept at automating monitoring workflows, detecting and mitigating threats, and optimizing cloud and enterprise security. Demonstrated expertise in **incident management**, SIEM correlation, and VAPT with strong analytical, collaborative, and problem- solving skills. Passionate about **security automation** and continuous improvement in blue/red team environments.

CORE COMPETENCIES

SOC Operations: Threat Detection, Incident Management, SIEM Dashboard, WAF Monitoring, Log Analysis, Alert Triage
VAPT: Web s Network Scanning, OWASP Testing, Exploitation Simulation, Risk Mitigation
Cloud Security: AWS WAF, Cloudflare, Azure, IAM, Infrastructure Hardening, CloudWatch
Tools: Kibana, Wazuh, Suricata, Cloudflare, Splunk, Sumo Logic, Log360, Burp Suite, Nessus, ZAP, SQLMap, Wireshark
Soft Skills: Analytical Thinking, Communication, Team Collaboration, Leadership

PROFESSIONAL EXPERIENCE

Associate SOC Engineer

Investis Digital Pvt Ltd (IDX) | May 2024 - Present

Impact Summary: Improved incident detection efficiency and reduced alert noise by **25%** through SIEM tuning and automation.

- Monitored and analyzed WAF/CDN traffic via Cloudflare and Symantec, **mitigating DDoS and bot anomalies**.
- Investigated alerts using Kibana and AWS CloudWatch, **improving false positive reduction by 30%.**
- Conducted vulnerability assessments using **Nmap, Burp Suite, and Nessus;** prioritized remediation based on CVSS.
- Automated SSL expiry alerts integrated with Jira, **cutting incident response time by 20%.**
- Managed AWS IAM configurations, **enhancing access control and visibility.**
- **Resolved 10,000+ security alerts** ensuring quick escalation and proactive response.

PROJECTS

SOC Lab Setup: Built open-source SOC using **Wazuh, Suricata, and Kibana** for real-time detection.
Recon Veritas (Tool): Developed automated recon tool combining multiple **OSINT** utilities for red teaming.
Red Team WAF Bypass Lab: Designed lab for testing **WAF detection and bypass** using payload manipulation.
Kibana SIEM Dashboard: Created dashboards to visualize **brute-force patterns** in Linux logs.

CERTIFICATIONS

SOC s Blue Team: Blue Team Junior Analyst, SOC Level 1 & 2 (Try Hack Me), Multi-Cloud Blue Team Analyst & Cybersecurity Analyst (CWL)
VAPT s Red Team: Multi-Cloud Red Team Analyst (CWL), CEH (Cisco), Cyber Threat Management (Cisco), EHE (EC-Council)
Cloud Security: AWS Cloud Practitioner, AWS Security Fundamentals, SC-900 (Microsoft)

EDUCATION

B.Sc. Forensic Science **(Cyber Forensics Specialization)** - Parul University (2021-2024)
CGPA: **9.47 - Gold Medalist**

LEADERSHIP s EXTRACURRICULAR

Led SOC knowledge sessions on SIEM tuning and alert investigation.
Mentored interns in vulnerability analysis and triage workflows.
Active participant in **Hack the Box, Try Hack Me, and security CTFs.**