Divakar K

divakar.k2023@gmail.com | +91 93420 06729

SUMMARY

SOC and Cloud Security–focused Engineer experienced in SIEM monitoring, threat detection, and AWS security. Skilled in log analysis and incident response to protect hybrid infrastructure and improve security resilience.

EXPERIENCE

Internship
Aug 2025 - Sep 2025 | Elevate Labs

Conducted penetration testing and vulnerability assessments on web and mobile applications using OWASP Top 10 methodologies, identifying critical flaws including XSS, SQL injection, and authentication bypass vulnerabilities.

Applied networking and cybersecurity fundamentals in lab-based tasks, including network security monitoring, incident simulation, and building real-world security projects to demonstrate practical threat detection and mitigation skills.

Performed vulnerability scanning and service enumeration with Nmap and Burp Suite, followed by post-remediation validation to ensure security controls were effectively patched and critical vulnerabilities eliminated.

PROJECTS

WINDOWS SYSMON DETECTION LAB | SOC PROJECT

2025 – 2026 | Self Project

Built a Windows Sysmon detection lab to capture high-fidelity endpoint telemetry and security events. Ran controlled attack simulations to generate actionable log data and understand adversary behaviors.

Created custom detection rules and mapped events to MITRE ATTACK to enhance SOC-focused threat detection accuracy.

GitHub: WINDOWS ENDPOINT MONITORING AND DETECTION LAB

TOR DEANONYMIZATION FORENSICS SYSTEM | NETWORK FORENSICS PROJECT

2025 – 2026 | Team Project

Simulated a Tor network using Chutney for relay-level forensic traffic analysis, engineered features from captured data, and built an XGBoost–based detection model to identify deanonymization patterns, delivering a compact cybersecurity ML solution through team collaboration.

GitHub: TOR-DEANONYMIZATION-FORENSICS-SYSTEM

SQL INJECTION DETECTION | WEB SECURITY PROJECT

2025 - 2026 | Personal Project

Built a SQL Injection practice lab using Flask and PHP to demonstrate vulnerable vs. secure query handling, and developed a Python–based detection engine to identify malicious payloads and log real-time attack attempts for forensic analysis.

GitHub: SQL-INJECTION-DETECTION

EDUCATION

RAJALAKSHMI INSTITUTE OF TECHNOLOGY

Bachelor of Computer and Communication Engineering
Expected: Current | Chennai - 600010

SKILLS

PROGRAMMING

Python • Java • MySQL

SECURITY - TOOLS

Nmap • Burp Suite • Metasploit Framework • Wireshark • Splunk • OWASP ZAP • Gobuster • Hydra • Tenable Nessus • Git/GitHub • Zeek • ELK Stack

PLATFORMS | OS

Windows • Kali Linux • Docker

CONCEPTS

SIEM • IDS/IPS • Network Security Monitoring• Log Analysis • Threat Hunting • Incident Response • MITRE ATTACK

CERTIFICATIONS

CCEP – Red Team Leader

AWS Cloud Certification

AWS Security Encryption

Cisco Cybersecurity Essentials

GRC | Mindset, Methods, Skills

ISO/IEC 27001:2022 | Information Security Associate

LINKS

Github: **Divakar-K**
LinkedIn: **Divakar-K**
Portfolio: **Divakar-K-Portfolio**