Divakar K

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

SUMMARY

SOC and SecOps-focused cybersecurity engineer with hands-on experience detecting endpoint and network-based attacks including suspicious PowerShell execution, brute-force authentication attempts, and web application attacks using Sysmon, SIEM, and log correlation techniques.

EXPERIENCE

Internship
Aug 2025 - Sep 2025 | Elevate Labs

Worked on practical cybersecurity tasks involving Windows Defender operations, network security fundamentals, VPN concepts, and browser security controls.

Performed phishing email analysis, web security assessments, password strength evaluation, and vulnerability analysis using tools such as Wireshark and Nessus as part of hands-on security labs.

PROJECTS

WINDOWS SYSMON DETECTION LAB | SOC PROJECT

2025 - 2026 | Self Project

Built a Sysmon-based detection lab to identify suspicious processes, PowerShell abuse, persistence activity, and anomalous network behavior.

GitHub: WINDOWS ENDPOINT MONITORING AND DETECTION LAB

TOR GUARD NODE PREDICTOR | NETWORK FORENSICS PROJECT

2025 - 2026 | Team Project

Analyzed synthetic Tor traffic and engineered features to study relay behavior and guard node prediction using machine learning.

GitHub: TOR-DEANONYMIZATION-FORENSICS-SYSTEM

SQL INJECTION DETECTION | WEB SECURITY PROJECT

2025 - 2026 | Personal Project

Developed a SQL injection detection lab to identify malicious queries and log attack payloads for forensic analysis.

GitHub: SQL-INJECTION-DETECTION

ACHIEVEMENTS

HACKATHON

Finalist at the TN Police Cyber Wings Hackathon, where the team presented a network forensics solution to analyze Tor exit node traffic for guard node prediction as part of onion routing research.

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

SECURITY CAPABILITIES

Endpoint attack detection using Sysmon telemetry.
Suspicious PowerShell activity detection and analysis.
Brute-force authentication attack detection.
Web application attack detection (SQL Injection, XSS)
SIEM-based log correlation and alert investigation.
MITRE ATT&CK-aligned threat analysis.

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**