

# BALAMURUGAN P

9626457885 | bala369936@gmail.com

---

Final-year **B.Tech Computer Science and Engineering (Cyber Security)** student with hands-on academic and lab-based experience in **SOC fundamentals, SIEM log analysis, malware analysis, and network security**. Actively seeking a **Cybersecurity Intern / SOC L1 Trainee / Entry-Level Security Analyst** role to apply practical skills in monitoring, analysis, and incident detection.

---

## EDUCATION

**Hindustan Institute Of Technology & Science**

B.TECH CSE CYBER SECURITY  
2022-2026

**Velammal Vidyalaya Viraganoor**

CLASS 12 CBSE  
2022

CLASS 10 CBSE  
2020

---

## PROJECTS

### **SECURE ENHANCE FILE STORAGE SYSTEM**

Jan 2024 - May 2025

It effectively covers:

- **Problem Addressed:** Combatting theft and scams related to sensitive information usage.
- **Key Security Features Implemented:** Biometric authentication, dynamic security codes, embedded chip technology for encryption, text steganography for digital certificates, SHA-256 for OTP verification, and real-time fraud detection.

**Impact:** Mitigating data theft and fraud, instilling user confidence

---

## Vulnerability Analysis of Android Applications

**Tool:** MobSF

- Performed static analysis of Android APKs to identify security vulnerabilities.
  - Detected insecure data storage, hardcoded credentials, and permission misuse.
  - Generated automated reports and documented remediation recommendations.
- 

## Splunk Log Analysis & Monitoring (SOC-Oriented Labs)

- Collected and analyzed system and network logs using **Splunk**.
  - Created dashboards to monitor security events and system behavior.
  - Configured alerts for suspicious activities and basic threat indicators.
  - Performed introductory log correlation to identify anomalies.
- 

## Malware Analysis – TryHackMe Labs

- Conducted static and dynamic analysis of Windows malware samples in sandboxed environments.
  - Extracted hashes, metadata, strings, and imports using **PeStudio**.
  - Identified registry changes using **Regshot**.
  - Monitored process and file activity using **Process Monitor (ProcMon)**.
- 

## HANDS-ON CYBERSECURITY LABS (CTF PRACTICE)

### TryHackMe – SOC & Security Labs

- Completed guided labs focused on **SOC Level 1 fundamentals**.
- Practiced **log analysis, alert understanding, and basic incident triage**.
- Performed **malware analysis, network traffic analysis, and vulnerability identification** in controlled lab environments.
- Gained exposure to **endpoint behavior, phishing concepts**, and attacker techniques.

### Tools Used:

Splunk (labs), Wireshark, Nmap, PeStudio, ProcMon, Regshot, Windows Event Logs

---

## SKILLS

**Programming:** C, C++, Java, Python

**Web Basics:** HTML, CSS

**Databases:** MySQL

**Networking:**

TCP/IP, Subnetting, Basic Network Security Concepts

**Operating Systems:**

Windows, Linux (Basic)

**Security Tools:**

Splunk, Wireshark, Nmap, MobSF, VMware, PeStudio, ProcMon, Regshot, nslookup

**Security Fundamentals:**

SOC Basics, Log Analysis, Malware Analysis (Beginner), Vulnerability Concepts, Incident Detection (L1)

---

## Licenses & certifications

- ❖ Cisco Networking Foundations: Fundamentals of Cisco Networking
  - ❖ Networking Foundations: Protocols and CLI Tools
  - ❖ Kali Linux Essential Training
  - ❖ Networking Foundations: Wide Area Networks (WANs)
  - ❖ Learning PC Maintenance and Performance (2021)
  - ❖ Python Essential Training
- Cisco Certified Network Associate Routing and Switching (CCNA)
-