LOGESHWARAN S

Cybersecurity Analyst

☎ +91 7418549258 ✉ logesh.spy@gmail.com github.com/logesh-GIT001 Tamilnadu,India.

PROFESSIONAL SUMMARY

SOC-Focused Cybersecurity Analyst proficient in real-time alert monitoring, multi-source log analysis, and incident investigation. Deep technical foundation in computer networking and Linux-based security forensics. Skilled in navigating SOC workflows–from initial alert validation and root cause analysis to critical escalation. Proven ability to analyze web application behavior to identify and mitigate emerging threats.

SKILLS

- **SOC Operations:** Security Event Monitoring , Alert Triage & Prioritization , Log Analysis , Incident Investigation.
- **Network & Infrastructure:** Network Traffic Analysis , Computer Networks , Firewall & IDS/IPS Basics.
- **Tools & Platforms:** SIEM (Splunk, Microsoft Sentinel) , Endpoint Security Tools , Documentation.
- **Programming & Automation**: Python Scripting for Security, Bash Scripting.

TECHNICAL EXPERIENCE

Signal-Flare | Python, Security Automation | GitHub **Dec 2025 - Jan 2026**

- Automated post-exploitation breach detection by planting honey credentials.
- Provides real-time alerts on stolen credential use, minimizing false positives and alert fatigue.

SOC & Blue Team Simulations | TryHackMe, LetsDefend **Dec 2025 - Present**

- Performed real-world SOC simulations, handling incident triage, alert investigation, and log analysis.
- Investigated phishing, malware, brute-force, and lateral movement scenarios using SIEM-style workflows.

Bug Bounty & Security Research **Dec 2025 - Present**

- High-Impact VRPs: Secured validated security reports for Google Android VRP, NVIDIA PSIRT, and CERT-In (Government platforms).
- Technical Skills: Utilized Burp Suite, Linux, and Python scripting for manual exploitation and VPAT.

EDUCATION

Erode Sengunthar Engineering college **Jun 2022 - May 2027**

M.TECH-COMPUTER SCIENCE ENGINEERING(5 YEARS INTEGRATED)

Advanced Cybersecurity Architecture, Threat Hunting, and Python Security Automation; hands-on focus on SOC operations, vulnerability management, system hardening, log forensics, incident triage, and malware analysis in Linux environments.

CERTIFICATIONS

- Cisco Networking Basics – Completed
- Cybersecurity Fundamentals – Completed
- Cisco Endpoint Security - Progress
- Python for Security Automation – Self-learning / Lab-based