

SWETHA DEVI SAI PRIYA BONU

Telangana, India | P: +91-7670872188 | swethadevi1125@gmail.com | [Linkedin.com](#) | [Github.com](#)

PROFESSIONAL SUMMARY

Cybersecurity Analyst with proven experience across blue and red team operations, combining threat detection, automation, and offensive security tactics. Delivered impactful results in phishing analysis, SIEM rule tuning, and exploit research—backed by CAP, and 100+ hands-on labs. Known for engineering real-world attack simulations and aligning security outcomes with global standards like MITRE, NIST, and ISO 27001

WORK EXPERIENCE

TriArmour AI Private Limited – India(Startup) Hyderabad, India
Cybersecurity Analyst Internship: Aug 2023 – Feb 2024 | Full-Time: Mar 2024 – Mar 2025

- Performed phishing analysis by examining email headers, attachments, and malicious URLs, reducing false positives by 32% through triage automation in Python.
- Implemented SPF, DKIM, and DMARC validations, improving email security posture across 2 business units.
- Contributed to SIEM log correlation efforts and detection rule testing using simulated attacks in a lab Splunk instance, enhancing detection coverage of brute-force and phishing attacks (MITRE T1110, T1566).
- Investigated real-time threats using EDR platforms (Bitdefender GravityZone, Sophos MDR) and isolated endpoints during simulated malware outbreaks
- Created weekly threat reports and supported GRC tasks by aligning findings with NIST CSF and ISO 27001 controls during internal audits.

Gradespot IT Solutions Hyderabad, India
Cybersecurity Intern Sep 2023 – Mar 2024

- Conducted in-depth research on critical vulnerabilities, including Log4Shell (CVE-2021-44228) and MOVEit (CVE-2023-34362), delivering risk summaries to senior analysts.
- Created Python scripts to automate CVE scraping and mapping to MITRE ATT&CK techniques
- Assisted in evidence collection and chain-of-custody documentation for simulated security incidents, enhancing forensic integrity workflows.

CERTIFICATIONS

- **Certified AppSec Practitioner (CAP) – SeCops Group**
- Python – V Tech Solutions , C Language – Geeni Institutions
- Junior PenTester Path – TryHackMe
- Cisco Networking Academy & ICT Academy (Honeywell) – Cybersecurity Training
- Penetration Testing and Ethical Hacking – Cybrary
- Open Source Intelligence – Basel Institute on Governance

PROJECTS

CyberPulse Telegram Bot

- Aggregates real-time threat intelligence from CVE, CISA, GitHub, and more, with update intervals and spam-control logic.

Evil Twin Attack using NodeMCU

- Rogue AP with Aircrack-ng tools to demonstrate Wi-Fi credential harvesting.

Wanna Hack CLI Tool DoS:

- Python tool for detecting DoS attacks with response pattern analysis.

Phishing Campaign Analysis

- Used GoPhish and SpamAssassin for simulation, analysis, and mitigation strategy documentation

TECHNICAL SKILLS

Blue Team: Log Analysis, Incident Response, Detection Rule Tuning, Alert Triage, Threat Hunting (MITRE ATT&CK Mapping), SIEM Analysis (Splunk – lab-based via TryHackMe), IDS/IPS (Suricata, Snort), Packet Analysis (Wireshark, Zeek, Tshark, Brim), Endpoint Security (Bitdefender GravityZone, Sophos MDR, ThreatLocker), Email Header Analysis

Red Team: Web App Exploitation (XSS, SQLi, IDOR, SSRF, Command Injection), Privilege Escalation (Linux/Windows), OSINT & Recon, Payload Crafting (Metasploit), Password Attacks (Hydra, Hashcat, John the Ripper), Burp Suite (Repeater, Intruder, Extensions), Wireless Attacks (Aircrack-ng)

Security Engineering & GRC: Vulnerability Management, Firewall Rules & DLP Basics, IAM Principles, SDLC Security, Cloud Security (AWS Fundamentals), Risk Mapping (ISO 27001, NIST CSF), Internal Policy Alignment

Scripting & Automation: Python (Automation, Parsing Logs, Custom Tools), Bash (Basic Scripting)

Frameworks & Models: MITRE ATT&CK, Cyber Kill Chain, OWASP Top 10, Diamond Model

EDUCATION

Sri Indu College of Engineering and Technology
Bachelor of Technology in Cyber Security

Hyderabad, India
Nov 2021- May 2025

Cumulative GPA: 8.12/10.0

Relevant Coursework: Network Security • Web Application Security • Operating Systems • Ethical Hacking • Security Information & Event Management (SIEM) • Incident Response & Digital Forensics • Malware Analysis • Secure Software Development Life Cycle (SSDLC)

Key Academic Projects:

Threat Actor Profiling Using OSINT & Splunk:

Investigated real-world threat actors using open-source intelligence tools (Shodan, SpiderFoot) and threat intel feeds. Built a Splunk dashboard to correlate IOCs, analyse patterns, and map TTPs to MITRE ATT&CK.

XSS Detection & Mitigation Framework:

Designed and tested a vulnerable web app to demonstrate stored and reflected XSS attacks. Implemented input sanitisation, output encoding, and CSP (Content Security Policy) to mitigate exploits.

Telangana State Residential Junior College,
Intermediate Public Education

Hyderabad, India
2019 – 2021 | 87%