Glan Loyan Dsouza

Blue Teaming (Defensive Security)

+91 9535038728 • glanloyand@gmail.com • www.linkedin.com/in/glanloyandsouza
github.com/glanloyand ● www.realseclabs.com

Profile Summary

Cybersecurity professional with expertise in **SOC monitoring, threat detection, and incident response**. Proficient in **SIEM tools, log analysis, network security, and threat hunting**. CEH v12 certified with hands-on experience in **security operations, forensic analysis, and security event correlation**. Passionate about **protecting digital assets through proactive defense mechanisms**.

Core Skills

- **Hands-on SOC Analyst training via LetsDefend**, focusing on real-world threat analysis, SIEM investigations, and cybersecurity incident handling.
- **Gained hands-on experience in SOC monitoring** through one month of practical training on LetsDefend, analyzing security alerts and investigating incidents.
- **SOC Monitoring & Incident Response** – SIEM, Log Analysis, Threat Investigation
- **Threat Hunting & Malware Analysis**
- **Security Information & Event Management (SIEM)** – Splunk, QRadar, ELK
- **MITRE ATT&CK Framework & Cyber Kill Chain**
- **Python for Security Automation**: Skilled in scripting and automating offensive security tasks, including vulnerability detection and exploit development.
- **Proficient in Python and JavaScript**
- **Advanced Networking & Protocols**: Strong understanding of OSI and TCP/IP models, packet analysis, and secure network configurations.
- Network Security & Log Analysis – Intrusion detection, firewall monitoring, traffic analysis
- Forensic Investigations – Analyzing digital evidence for incident response
- Compliance & Risk Assessment – Understanding PCI DSS, ISO 27001, NIST frameworks

Work Experience

Cybersecurity Intern | Cybersapiens United LLP,India
October 2022 – October 2023

- Conducted **VAPT assessments** for clients like IISc, PharmEasy, and Tamara.com.
- Identified **clickjacking, subdomain takeovers, and web vulnerabilities**.
- Performed **SIEM investigations & incident response** using **Splunk & Wireshark**.
- Developed **VAPT reports** with **remediation strategies** for clients.

Education

MSc in Computer Science – Cybersecurity & Ethical Hacking
Yenepoya University, Mangaluru | 2024 – 2025 | CGPA: 9.0
Bachelor of Computer Applications (BCA)
St. Aloysius College, Mangaluru | 2019 – 2022 | CGPA: 7.3

Projects

Live SOC Monitoring (LetsDefend)

- Monitored real-time security alerts, performed triage, and investigated incidents in a simulated SOC environment.
- SIEM (Security Information and Event Management), Splunk, Wireshark, MITRE ATT&CK Framework, Log Analysis Tools.
- Improved incident response efficiency by accurately identifying threats, reducing false positives, and enhancing threat analysis skills in a real-world simulated environment.

Offensive Security Automation with Python

- Developed and automated penetration testing tools for reconnaissance, scanning, MITM attacks, exploitation, and web vulnerability testing.
- Python, Scapy, BeautifulSoup, Paramiko, ftplib, NetfilterQueue, PyInstaller.
- Streamlined security assessments by automating repetitive tasks, reducing manual effort, and improving accuracy in vulnerability detection.

Penetration Testing & Vulnerability Assessment Tool

- Developed a security testing tool featuring proxy, intruder, and automated scanning for enhanced security assessment using Javascript

Certifications

- EC-Council Certified Ethical Hacker (CEH v12)
- Microsoft Azure: Identity and Access Management
- LetsDefend SOC Analyst
- Certified Ethical Hacker from Cybersapiens United LLP
- Cyber Security And Threat Hunting Certificate from Cybersapiens United LLP

Achievements

- Performer of the Month – Cybersapiens United LLP
- VAPT Certificate of Appreciation for Outstanding Bug Detection
- Executive Board Member (Secretary) – OWASP Yenepoya Chapter