INNOCENT JAMES ISSAT

Email: inocent.py@outlook.com , Linkedin: linkedin.com/in/issatx
GitHub: github.com/1024Cyber , Twitter: x.com/1024Cyber
Tel: +2349022096439

PROFESSIONAL SUMMARY

A Cybersecurity professional with strong knowledge of networking, operating systems, and security principles, seeking a hands-on security role.
Experienced with Linux and Windows, common attack vectors, the OWASP Top 10, vulnerability assessment, Threat Intelligence, SOC Analysis and Ethical Hacking, with a steady focus on learning new threats and defenses.

CORE COMPETENCE & TECHNICAL SKILLS

- Ethical Hacking
- Web Application Security
- OSINT
- Network Security
- Threat Intelligence
- Vulnerability Assessment
- Digital Forensics
- Linux & Windows Administration
- Firewalls
- SOC Analysis
- Secure Coding Concepts
- Python, Batch & Bash Scripting
- MITRE ATT&CK Framework

PROFESSIONAL EXPERIENCE

- **University of Uyo, Uyo** **June 2024 – Present**
  GRADUATE ASSISTANT
  Delivered Cybersecurity practical classes for both Undergraduate and Postgraduate students of the Department of Computer engineering (Faculty of Engineering) and Department of Cybersecurity (Faculty of Computing)

- **Ollic ICT, Uyo** **August 2025 – Present**
  CYBERSECURITY FACILITATOR
  Delivered hands-on practical classes for students for Ethical hacking,SOC analysis and Threat Intelligence

- **CloudBridge Technologies** **August 2024-April 2025**
  SECURITY ANALYST
  Conducted web application, network, and API penetration testing to identify and exploit security vulnerabilities, Performed reconnaissance and enumeration using OSINT techniques and tools to map attack surfaces

- **1024Technologies** **January 2022-Present**
  CYBERSECURITY PERSONNEL
  Performed Vulnerability assessment, Web application security, Patch management, Network security and firewall configuration settings, Threat intelligence and attack surfaces mapping

---

KEY PROJECTS

- **ATLAS** (Analyst Threat & Link Analysis System)

A self-hosted cyber threat intelligence workbench that I designed and built with FastAPI, SQLite and a single-file vanilla-JS frontend. It automates IOC collection from open sources (OTX, MISP feeds, OpenPhish, Emerging Threats, Feodo and others) and enriches indicators through VirusTotal, OTX and Shodan. It maps actors, campaigns and TTPs to MITRE ATT&CK, supports guided investigations and a correlation graph, and exports to STIX, MISP and PDF.

- **SOCBENCH**

SOC analyst training platform that allows user to generate realistic attack traffic in a control lab. Capture it, and analyse it using wireshark

- **DROIDSENTINEL**

An android Security framework that Scans, Enumerate and run intelligence analysis on android device connected via ADB, also check for CVE's by matching version against known android CVE from NVD

- **NEXABANK**

A Damn vulnerable banking application, suitable for learning web security

- **NEXAMART**

A Damn Vulnerable e-commerce application for learning and practicing web security relating to e-commerce platforms

- **SCAPYCRAFT**

A self-built, no-code web application for crafting and sending custom network packets using Scapy, designed for cybersecurity training environments.

- **TELEGRAM OSINT BOT**

A Bot that turns telegram into an investigation lab, User can run recon, gather intelligence and generate report

---

EDUCATION AND CERTIFICATE

(B.Eng.) Computer Engineering **2025**
University of Uyo, Uyo

MasterCard Phishing Email Simulation **2026**
theForage