Chris O. Agudosi

AI Security Engineer | OSCP | OSWE | AppSec | Applied AI Security
Remote (Los Angeles, CA) | 281 660 5217 | O.agudosi88@gmail.com | LinkedIn | GitHub

TECHNICAL SKILLS

Programming & Automation: Python, Bash, SQL, JavaScript, TypeScript, HTML/CSS, Web Scraping, Automation Scripting
Security Engineering: AI Security, Application Security (AppSec), Threat Hunting, Vulnerability Assessment, Penetration Testing, VAPT, Security Automation, Detection Engineering, Incident Response, DFIR, Digital Forensics, OSINT Investigation, Threat Intelligence, Malware Analysis, Reverse Engineering, OWASP Top 10, MITRE ATT&CK, NIST, Zero Trust, Threat Modeling, Vulnerability Management
Cloud & DevSecOps: AWS, Azure, GCP, Terraform, Docker, Kubernetes, OpenShift, GitHub Actions, Jenkins, Azure DevOps, CI/CD, Infrastructure Security, Container Security, Secure SDLC
Observability & Monitoring: Prometheus, Grafana, ELK Stack, New Relic, Logstash, AIOps, Infrastructure Monitoring, Alert Triage
AI Security & Testing: LLM Integration, OpenAI APIs, Pinecone, Prompt Injection Defense, AI Red Teaming, AI Governance, Adversarial Testing, AI Safety, Security Guardrails, Selenium, Pytest, Playwright, Regression Testing, Chaos Testing
Platforms & Tooling: Microsoft Sentinel, Splunk, Burp Suite, OWASP ZAP, Nessus, Metasploit, Nmap, Wireshark, CSI Linux, Git, Linux, IDA Pro Scripting, Elastic Stack, Jira, Confluence
Operating Systems: Kali Linux, CSI Linux, Ubuntu, Windows Server, Parrot OS, Android

PROFESSIONAL EXPERIENCE

Cyber Security Analyst **Aug 2024 – Present**
Manappuram Comptech & Consultants Ltd. *(Remote)*

- Conducted penetration testing across web, Android, API, and thick-client applications using OWASP Top 10, PTES, and CVSS methodologies, delivering remediation guidance for authentication, session, and input-validation vulnerabilities.
- Architected an AI-assisted VAPT platform integrating network vulnerability scanning, web security testing, Android analysis, and automated vulnerability classification, reducing repetitive assessment and reporting across multi-stage security reviews.
- Performed internal and external network VAPT operations involving host discovery, service enumeration, controlled exploitation, and attack-surface analysis using Nmap, Metasploit, Python, and Bash across enterprise infrastructure systems.
- Executed Android penetration testing involving APK decompilation, SSL pinning bypass, runtime method hooking, and dynamic analysis using MobSF, Frida, JADX, and ADB across multiple mobile application assessments.
- Led enterprise-wide phishing simulation campaigns supporting security awareness initiatives, generating post-assessment reporting covering click-through metrics, remediation priorities, and user-risk evaluation findings.
- Validated DAST and SAST findings, performed false-positive triage, and conducted secure code review procedures aligned with Secure SDLC and application security assessment standards.

AI Security & DevSecOps Engineer (Contract) **Jan 2023 – Present**
Global *(Remote)*

- Designed AI-assisted Secure SDLC orchestration frameworks using OpenAI APIs, GitHub Actions, and Azure DevOps across 12+ repositories, reducing manual QA preparation time by 15-18 hours per sprint.
- Implemented Prometheus, Grafana, ELK, and New Relic dashboards for Kubernetes environments supporting 40+ microservices and 300+ daily container events, cutting average incident recovery time from over 2 hours to nearly 75 minutes.
- Constructed an LLM-powered knowledge retrieval platform using OpenAI embeddings and Pinecone, centralizing 2,500+ engineering documents while supporting AI governance, prompt validation, and secure knowledge access controls.
- Orchestrated Jenkins, Selenium, and Pytest validation pipelines across AWS-hosted staging clusters, increasing regression coverage from 45% to 92% while reducing manual release testing by roughly 20 hours per cycle.
- Provisioned Terraform-based AWS and Azure infrastructure supporting multi-region deployments, reducing environment setup time from nearly 4 hours to under 45 minutes.
- Strengthened production alert triage across distributed systems processing 500K+ daily application events, reducing recurring alert escalations by nearly 25% during high-volume deployment periods.

Security Engineer | AI Defense & Threat Detection **Mar 2021 – Dec 2023**
Global Consulting Firm *– Dallas, TX (Remote)*

- Built LLM-assisted triage systems and Microsoft Sentinel SOAR automations that processed 1,200+ monthly security alerts, reducing average analyst response time from 45 minutes to under 10 minutes.
- Deployed Logic Apps playbooks for phishing analysis, endpoint investigations, and suspicious login threat response operations, reducing repetitive SOC workload by nearly 60 hours per month.
- Conducted threat detection, vulnerability investigation, and incident analysis across cloud environments using Microsoft Sentinel, Splunk, and MITRE ATT&CK-based investigation frameworks supporting 1,200+ monthly security alerts.
- Engineered Python-based security scripts for log parsing, IOC extraction, VAPT analysis, and security event correlation, reducing recurring alert investigation time from nearly 20 minutes to under 13 minutes.

Founder | AI Security, Reconnaissance & Automation Projects **Jan 2017 – Present**
NovusAegis AI | ReconPro | God's Eye, *Remote*

- Maintained 10+ GitHub repositories focused on OSINT investigation, DFIR tooling, malware analysis, VAPT research, and AI security experimentation initiatives.
- Supported AI systems and automation initiatives for government-sector environments, contributing to secure workflow orchestration, infrastructure automation, and operational security enhancements across multi-team deployment initiatives.
- Built a custom TAK (Tactical Assault Kit) server enabling secure situational awareness, real-time mapping, and unit-tracking capabilities across tactical communication environments.
- Developed custom IDA Pro plugins and static analysis utilities that accelerated malware triage and executable inspection procedures across security research labs.

SELECTED SECURITY PROJECTS

FLARE-ON Reverse Engineering Research

- Curated reverse engineering repositories covering 10+ years of FLARE-ON malware and binary analysis challenges, maintaining 80+ archived challenge write-ups and analysis resources using IDA Pro, Python, and static analysis tooling.
- Analyzed packed executables, obfuscated binaries, and malicious scripts across dozens of reverse engineering exercises focused on malware triage, executable inspection, and exploit-analysis operations.

Application Security & API Assessment

- Performed OWASP Top 10 and API penetration testing operations using Burp Suite, OWASP ZAP, and manual request analysis across authentication, session management, and input validation controls.
- Identified insecure configurations, exposed endpoints, and input-validation weaknesses during attack-surface assessments and API exploitation testing procedures.

Offensive Security & Reconnaissance Automation

- Engineered Python-based reconnaissance and web automation scripts using Requests, BeautifulSoup4, and CSV processing to support OSINT reconnaissance, attack-surface mapping, and VAPT assessment procedures.
- Processed hundreds of structured records through automated parsing and reconnaissance analysis operations focused on OSINT collection, attack-surface mapping, and vulnerability assessment efforts.

Threat Hunting & Detection Engineering

- Investigated suspicious authentication patterns, endpoint anomalies, and cloud-based security events using Microsoft Sentinel, Splunk, and MITRE ATT&CK-aligned threat-hunting methodologies.
- Tuned alert-correlation logic and threat triage procedures across environments processing 1,200+ monthly security alerts across hybrid infrastructure deployments.

AI Security & Adversarial Testing

- Evaluated prompt-handling behaviors, access controls, and AI safety validation processes across LLM-integrated security platforms and retrieval systems.
- Executed adversarial testing and prompt injection assessments supporting AI governance, model safety validation, and secure LLM interaction controls.

CERTIFICATIONS

- **Offensive Security Certified Professional (OSCP)**
- **Offensive Security Web Expert (OSWE)**
- **Certified Ethical Hacker (CEH)**
- **Certified Information Systems Auditor (CISA)**
- **Project Management Professional (PMP)**
- **CompTIA Security+**
- **Certified Kubernetes Administrator (CKA)**
- **AWS Certified Solutions Architect – Associate**
- **ISTQB Certified Tester – Advanced Level**
- **Google Cybersecurity Certificate**
- **Prompt Engineering Specialization (OpenAI)**

EDUCATION

Bachelor of Science in Engineering | ***Plymouth University*** **–** *United Kingdom* **May 2016**

- First Class Honours | Dean's List | EBS Scholarship | 70%+ Overall Average