AMDOR ANALYTICS

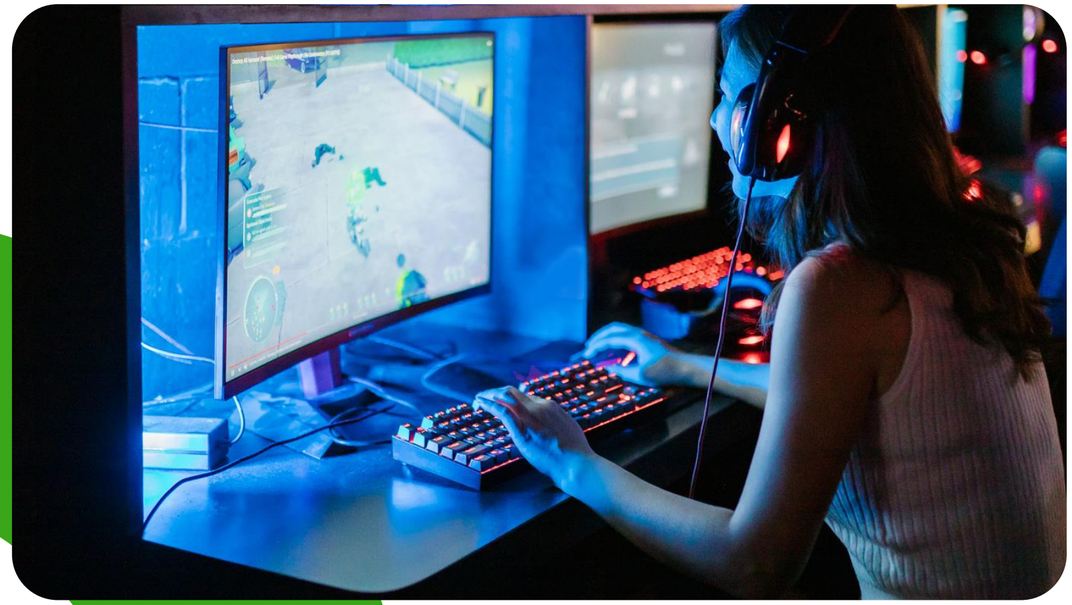
CYBER SECURITY BROCHURE

Become certified in Cyber security

PROGRAM OVERVIEW

- Saturday Live Classes for 5 months
- Weekly Drop-In Support Sessions
- Post-Training Support
- Linkedin Optimization
- Interview Preparatio Post-Training Support
- Building a Job-ready portfolio
- Navigating the Job Market Session
- Industry relevant certificate
- Two month internship
- CV Review
- • SOC Analyst mock interviews
- Building a personal cybersecurity brand

WHY CONSIDER CYBER SECURITY?



Cybersecurity gives you the ability to shield critical infrastructure and protect the digital identities that power our modern world. In today's interconnected economy, organizations face a constant barrage of evolving threats, making the protection of sensitive information a top priority. This has made cybersecurity one of the most essential and in-demand skills across every global industry.

Learning cybersecurity equips you with practical, hands-on skills to identify vulnerabilities, mitigate risks, and respond to digital attacks effectively. You'll learn how to think like an adversary to build stronger defenses, securing networks and systems against unauthorized access while ensuring data integrity.

Beyond career opportunities, cybersecurity empowers you to navigate the digital landscape with confidence and resilience. It is a mission-critical skill set that keeps you relevant and indispensable in a world where security is no longer just a technical requirement, but a fundamental pillar of business survival.

REQUIREMENTS

01

Duration
5 Months

02

Internship
8 Weeks

03

Skill Level
Beginner to Master

The future version of you depends on the effort you put in today

AMDOR ANALYTICS

OUR CURRICULUM

AMDOR ANALYTICS

Month 1- CYBERSECURITY FOUNDATIONS PLUS SYSTEM FUNDAMENTALS

Module 1

Introduction to Cybersecurity

- What is cybersecurity?
- CIA Triad (Confidentiality, Integrity, Availability)
- Types of cyber threats
- Cyber attack lifecycle
- Security domains (Network, Cloud, SOC, IAM, Blue-vs-Red Team)
- Overview of cyber roles and career paths

Hands-on Labs

- Explore live cyber-attack case studies
- Threat actor profiling
- Basic reconnaissance using OSINT tools

Month 1- CYBERSECURITY FOUNDATIONS PLUS SYSTEM FUNDAMENTALS

Module 2

Networking for Cybersecurity

- OSI Model
- TCP/IP
- Ports and protocols
- Firewalls, VPNs
- DNS, DHCP, ARP
- Network topology & architecture
- Network monitoring basics

Hands-on Labs

- Wireshark packet analysis
- Network traffic investigation
- Build a small virtual network

Month 1- CYBERSECURITY FOUNDATIONS PLUS SYSTEM FUNDAMENTALS

Module 3

Operating Systems (Windows & Linux)

- Windows architecture
- Linux architecture
- File systems & permissions
- System hardening
- CMD & PowerShell basics
- Bash scripting basics

Hands-on Labs

- Linux user/permission management
- Hardening a Windows machine
- Script for automating OS tasks

Month 1- CYBERSECURITY FOUNDATIONS PLUS SYSTEM FUNDAMENTALS

Module 4

Introduction to Virtualization & Lab Setup

- VirtualBox / VMware installation
- Creating isolated cyber labs
- Installing Linux distributions (Kali, Ubuntu)
- Installing Windows 10/11 test environment

Hands-on Labs

- Build a complete cybersecurity home lab
- Setup Kali Linux, Metasploitable, DVWA

END OF MONTH 1 PROJECT

Build Your Cybersecurity Virtual Lab + Conduct a Basic Threat Assessment

MONTH 2 — THREATS, VULNERABILITIES, AN SECURITY TOOLS

Module 5

Threats, Malware & Attack Vectors

- Malware types
- Ransomware behavior
- Social engineering
- MITRE ATT&CK framework
- Phishing lifecycle

Hands-on Labs

- Simulate phishing attacks (ethical)
- Malware sandbox observation

MONTH 2 — THREATS, VULNERABILITIES, AN SECURITY TOOLS

Module 6

Vulnerability Assessment & Scanning

- Vulnerability management lifecycle
- CVSS Scoring
- NVD database
- Tools: Nessus, OpenVAS, Nmap

Hands-on Labs

- Full vulnerability scan on Metasploitable
- Create vulnerability report

MONTH 2 — THREATS, VULNERABILITIES, AN SECURITY TOOLS

Module 7

Security Tools (SIEM, EDR, IDS/IPS)

- SIEM basics
- Log management
- Endpoint security concepts
- IDS/IPS overview
- Popular tools (Splunk, ELK, Wazuh, Defender, Suricata)

Hands-on Labs

- Setup Wazuh or Splunk
- Analyze logs
- Create custom security alerts

MONTH 2 — THREATS, VULNERABILITIES, AN SECURITY TOOLS

Module 8

SOC Fundamentals

- How Security Operations Centers work
- Incident lifecycle
- Threat hunting basics
- Alert triage levels
- SOC workflows

Hands-on Labs

- Investigate a brute-force alert
- Build a SOC playbook

END OF MONTH 2 PROJECT

Perform a vulnerability assessment and generate a professional remediation report.

MONTH 3 — PENETRATION TESTING & ETHICAL HACKING

Module 9

Ethical Hacking Foundations

- Penetration testing methodology
- Reconnaissance (active & passive)
- Scanning & enumeration
- Target profiling

Hands-on Labs

- Nmap deep scans
- Website footprinting

MONTH 3 — PENETRATION TESTING & ETHICA HACKING

Module 10

Exploitation Techniques

- Exploitation fundamentals
- Password attacks
- Man-in-the-Middle attacks
- Wireless hacking essentials
- Privilege escalation

Hands-on Labs

- Exploit vulnerabilities on DVWA
- Use Metasploit to gain access
- Conduct privilege escalation on Linux/Window

MONTH 3 — PENETRATION TESTING & ETHICAL HACKING

Module 11

Web Application Security (OWASP Top 10)

- SQL Injection
- XSS
- Broken Authentication
- Security Misconfigurations
- Insecure Direct Object References

Hands-on Labs

- Perform SQL Injection
- Capture cookies with XSS
- Exploit insecure authentication

MONTH 3 — PENETRATION TESTING & ETHICAL HACKING

Module 12

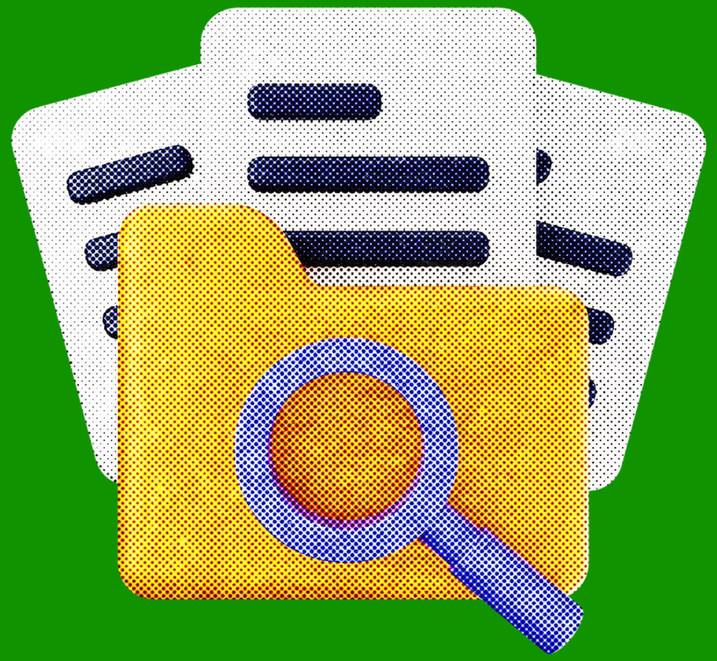
Red Team Tools

- Kali Linux
- Hydra
- Burp Suite
- John the Ripper
- Social Engineering Toolkit
- Hashcat

Hands-on Labs

- Crack passwords (ethical)
- Intercept requests with Burp Suite

END OF MONTH 3 PROJECT



Perform a Penetration Test on a vulnerable application and present an exploit report.

MONTH 4 — CLOUD SECURITY + DIGITAL FORENSICS + CYBER DEFENSE

Module 13

Cloud Security (AWS/Azure/GCP)

- Cloud fundamentals
- Identity & Access Management
- Shared responsibility model
- Cloud monitoring
- Cloud security misconfigurations

Hands-on Labs

- Secure S3 bucket
- IAM user privilege configuration
- Vulnerability scan on cloud environment

MONTH 4 — CLOUD SECURITY + DIGITAL FORENSICS + CYBER DEFENSE

Module 14

Digital Forensics (DFIR)

- Forensics process
- Chain-of-custody
- Memory forensics
- Disk forensics
- Log forensics

Hands-on Labs

- Memory capture & analysis (Volatility)
- Recover deleted files
- Investigate a security breach

MONTH 4 — CLOUD SECURITY + DIGITAL FORENSICS + CYBER DEFENSE

Module 15

Incident Response

- Incident Response Lifecycle
- Playbooks & runbooks
- Threat containment
- Memory, log & packet analysis
- Post-incident reporting

Hands-on Labs

- Build an IR plan
- Respond to a simulated ransomware attac

MONTH 4 — CLOUD SECURITY + DIGITAL FORENSICS + CYBER DEFENSE

Module 16

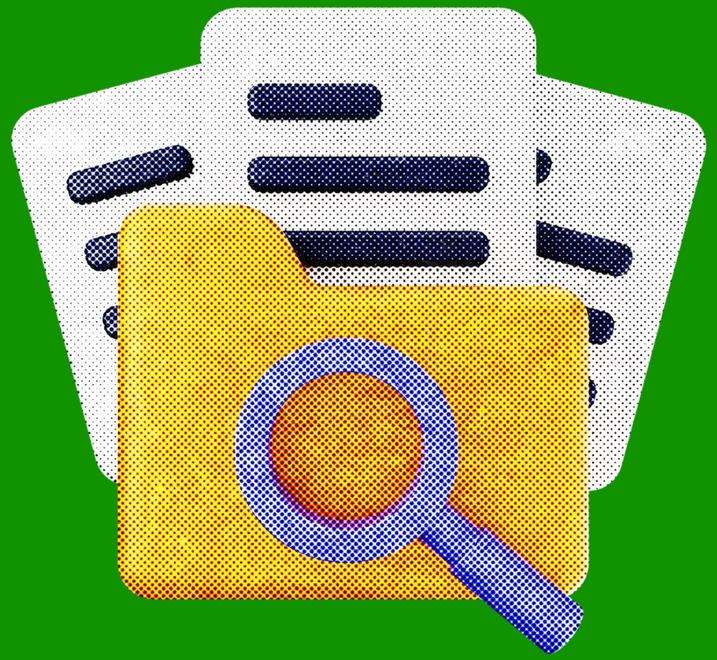
Cyber Defense & Threat Hunting

- Indicators of Compromise
- Behavioral analytics
- Threat hunting methods
- MITRE ATT&CK Deep Dive

Hands-on Labs

- Perform a real threat-hunting investigation
- Create custom detection rules

END OF MONTH 4 PROJECT



Investigate and respond to a simulated cyber attack. Produce a full forensics + incident response report.

MONTH 5 — ADVANCED SECURITY + AUTOMATION + CAPSTONE

Module 17

Security Governance, Risk & Compliance

- ISO 27001
- NIST CSF
- PCI DSS
- SOC 2
- GDPR
- Risk assessments
- Business continuity & disaster recovery

Hands-on Labs

- Build a risk assessment template
- Create a cybersecurity policy

MONTH 5 — ADVANCED SECURITY + AUTOMATION + CAPSTONE

Module 18

Python for Cybersecurity & Automation

- Python basics
- Automating log analysis
- Building scanning scripts
- Regex for security
- Automation for SOC tasks

Hands-on Labs

- Create a port scanning script
- Automate alert triage

MONTH 5 — ADVANCED SECURITY + AUTOMATION + CAPSTONE

Module 19

Python for Cybersecurity & Automation

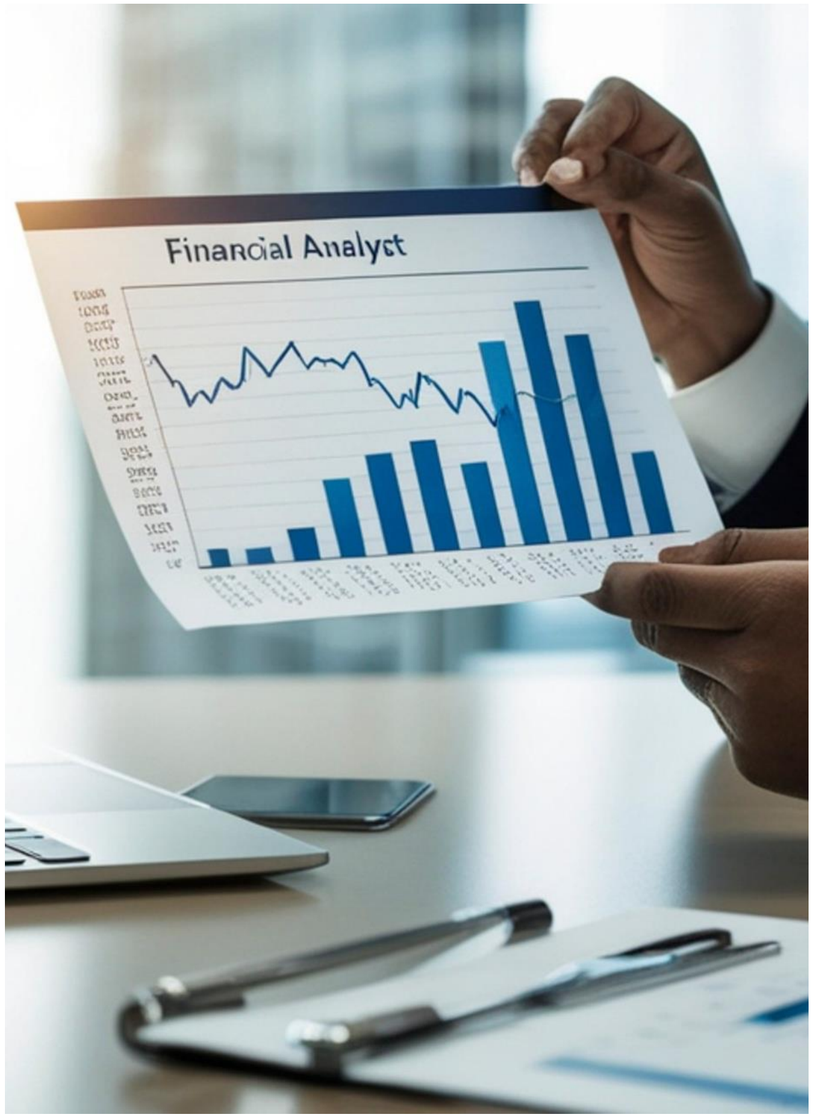
- Advanced SPL queries (Splunk)
- SIEM rule creation
- Threat intelligence integration
- Endpoint security tuning

Hands-on Labs

- Build a SOC dashboard
- Create custom detection rules

Industries That Employ Data Analysts

- Technology and Software Companies
- Manufacturing and Production
- Finance and Banking
- Energy and Utilities
- Healthcare and Pharmaceuticals
- Government and Public Sector
- E-commerce and Retail
- Education and EdTech
- Telecommunications
- Media & Entertainment



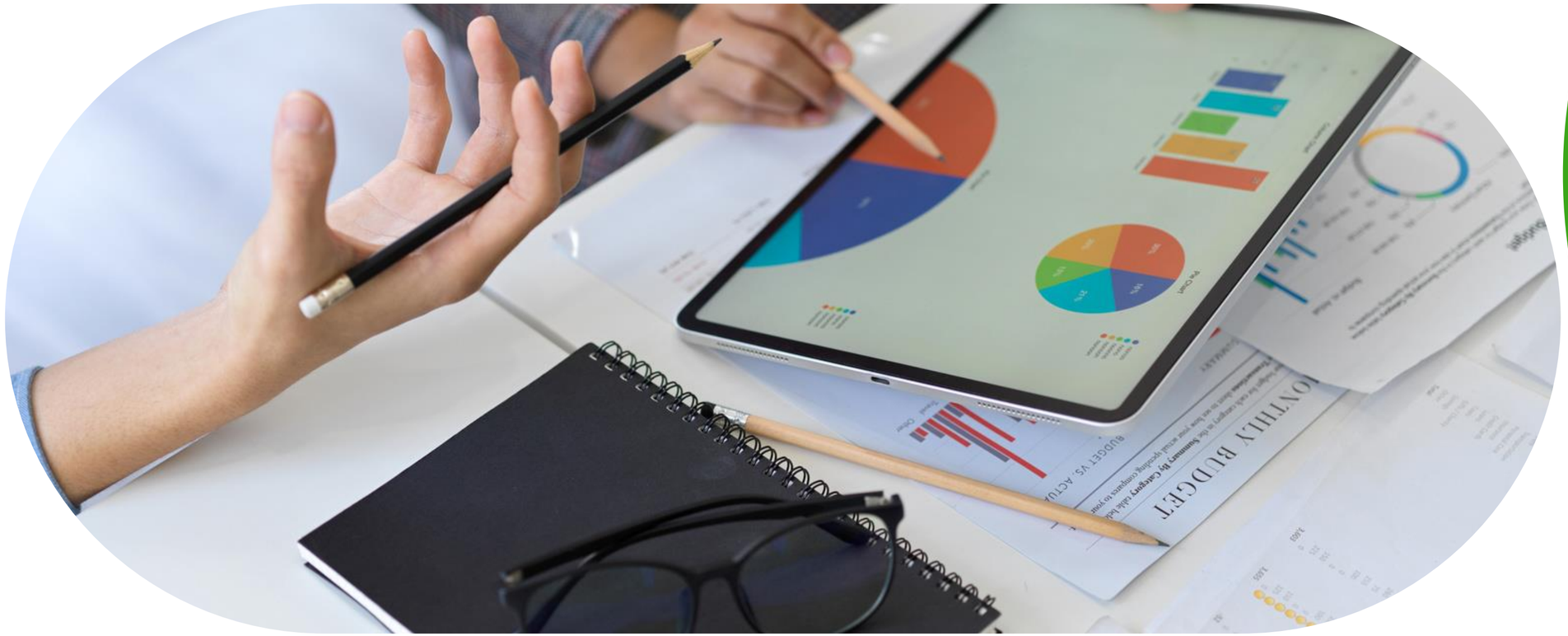
AMDOR ANALYTICS

WHY TRAIN WITH US?

- Practical, Job Ready Training
- Industry-Standard Tools & Technologies
- Expert Instructors With Real Experience
- Personalized Mentorship & Support
- Flexible and Beginner-Friendly
- Certification That Boosts Your CV
- Career Guidance & Portfolio Development
- Supportive Community
- Proven Success Stories
- Affordable Quality Training

Real world case studies

GROWTH INTERNSHIP PROGRAM



AMDOR ANALYTICS

JOIN OUR NEXT COHORT

AMDOR ANALYTICS

2026 TRAINING CALENDER

January 10 Saturday	**February** 14 Saturday	**March** 14 Saturday	**April** 11 Saturday
May 09 Saturday	**June** 13 Saturday	**July** 11 Saturday	**August** 08 Saturday
September 12 Saturday	**October** 10 Saturday	**November** 14 Saturday	**December** 12 Saturday

PROGRAM FEES

Testimonial

The following are genuine testimonials that we have received from our past students who have proven the benefits of the services we have provided to them.

Sodiq

★★★★★

I've attended other online classes before, but Amdor Analytics stands out for me. The facilitator is engaging, the sessions are practical, and the support team is responsive. I feel like I'm part of a real community that wants me to succeed. I'm happy I made this choice

Chinasa Fabian-Ijeruh

★★★★★

Before joining Amdor Analytics, I had no prior tech background. Now, I can confidently analyze data and build reports. The facilitator is very supportive and always encourages us to practice. The training has made me believe that anyone can learn tech if they're in the right environment.

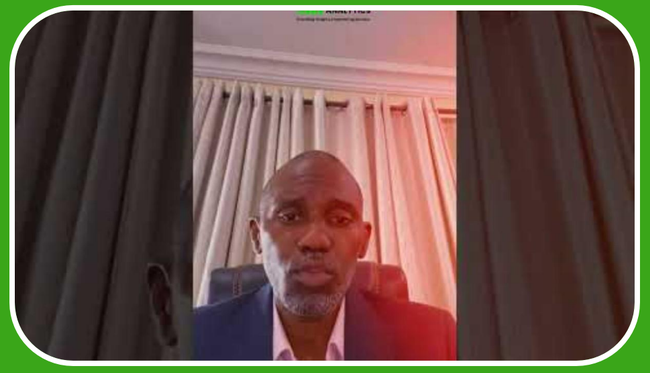
Chidimma Uzochukwu

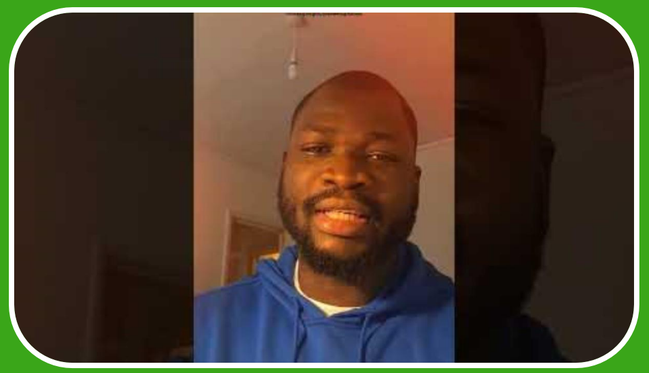
★★★★★

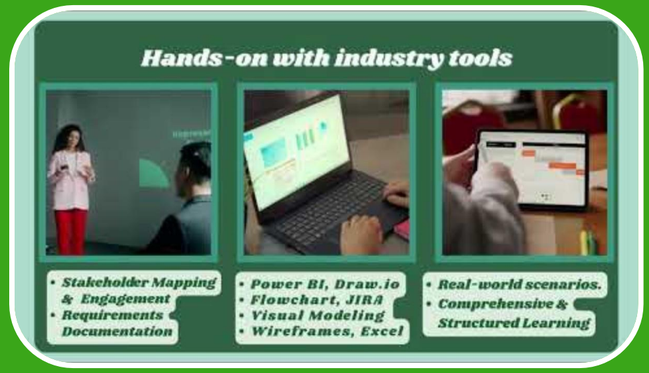
It's been an eye-opening experience learning at Amdor Analytics. The way the facilitator breaks down each lesson into relatable examples makes learning easy. Even though the pace is fast sometimes, the explanations are clear, and the resources provided are excellent. I'm really grateful for this opportunity.

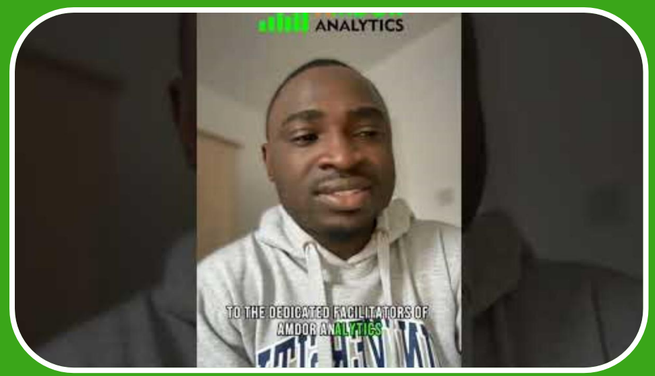
Testimonial

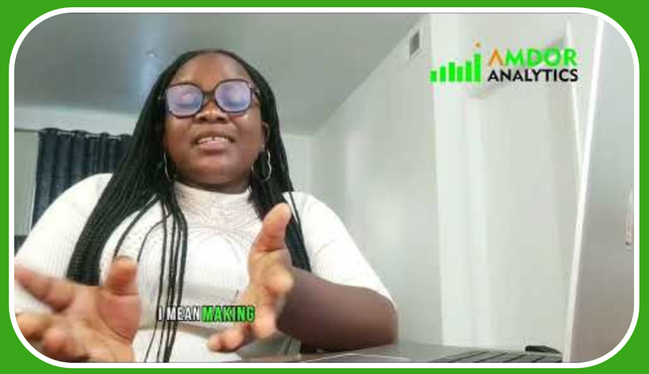
The following are genuine testimonials that we have received from our past students who have proven the benefits of the services we have provided to them.

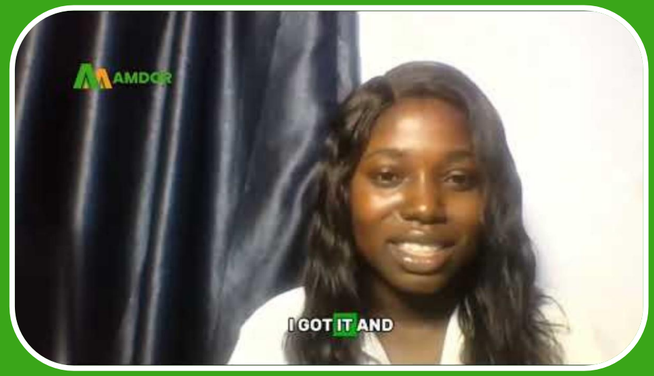






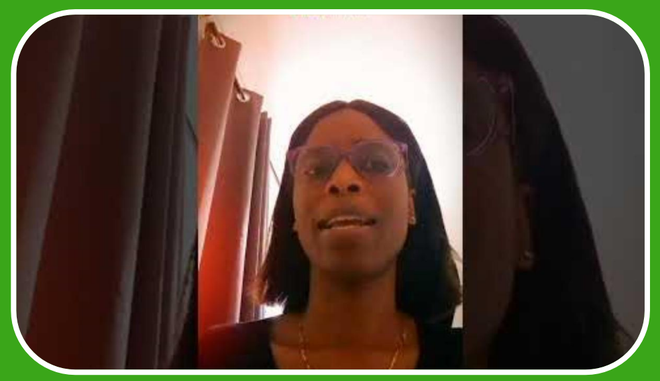


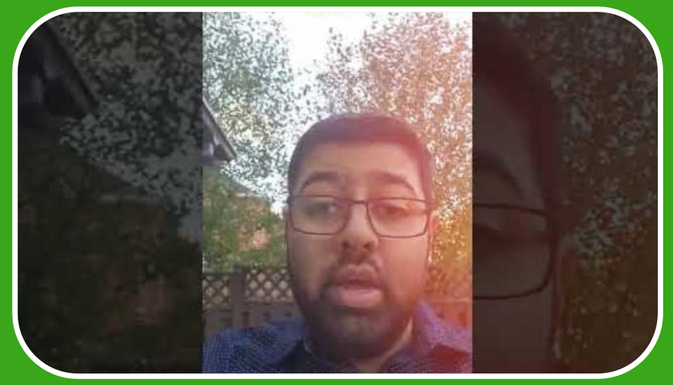


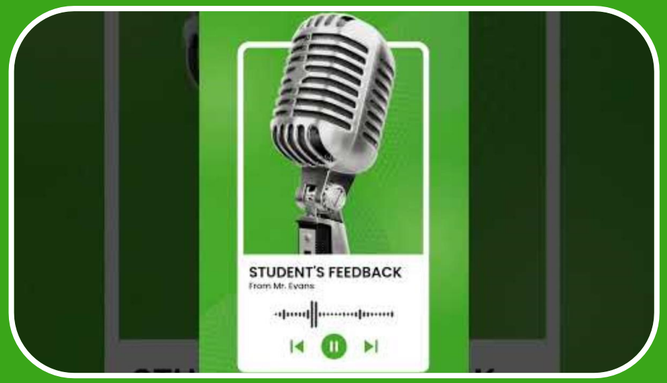


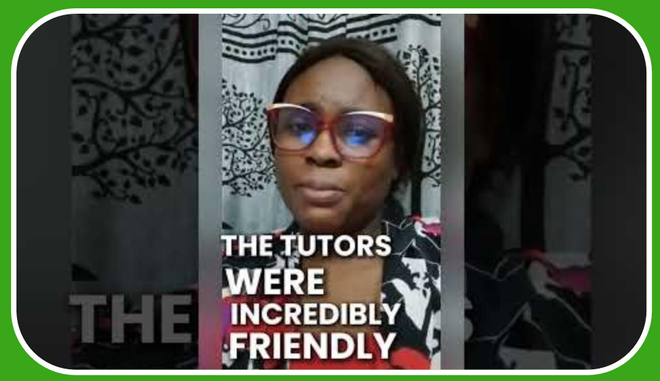
Testimonial

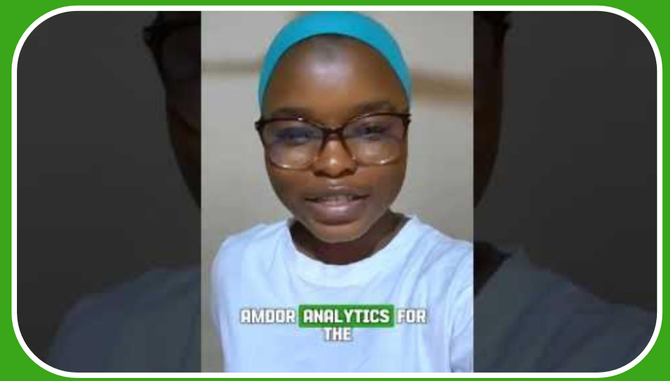
The following are genuine testimonials that we have received from our past students who have proven the benefits of the services we have provided to them.

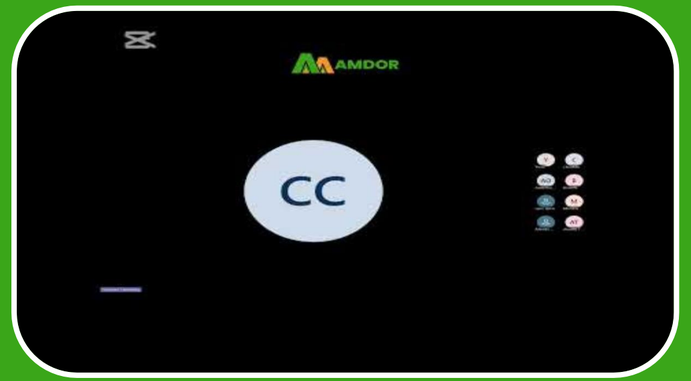












CONTACT US

+234 811 408 7403

@amdoranalytics

www.amdoranalytics.io