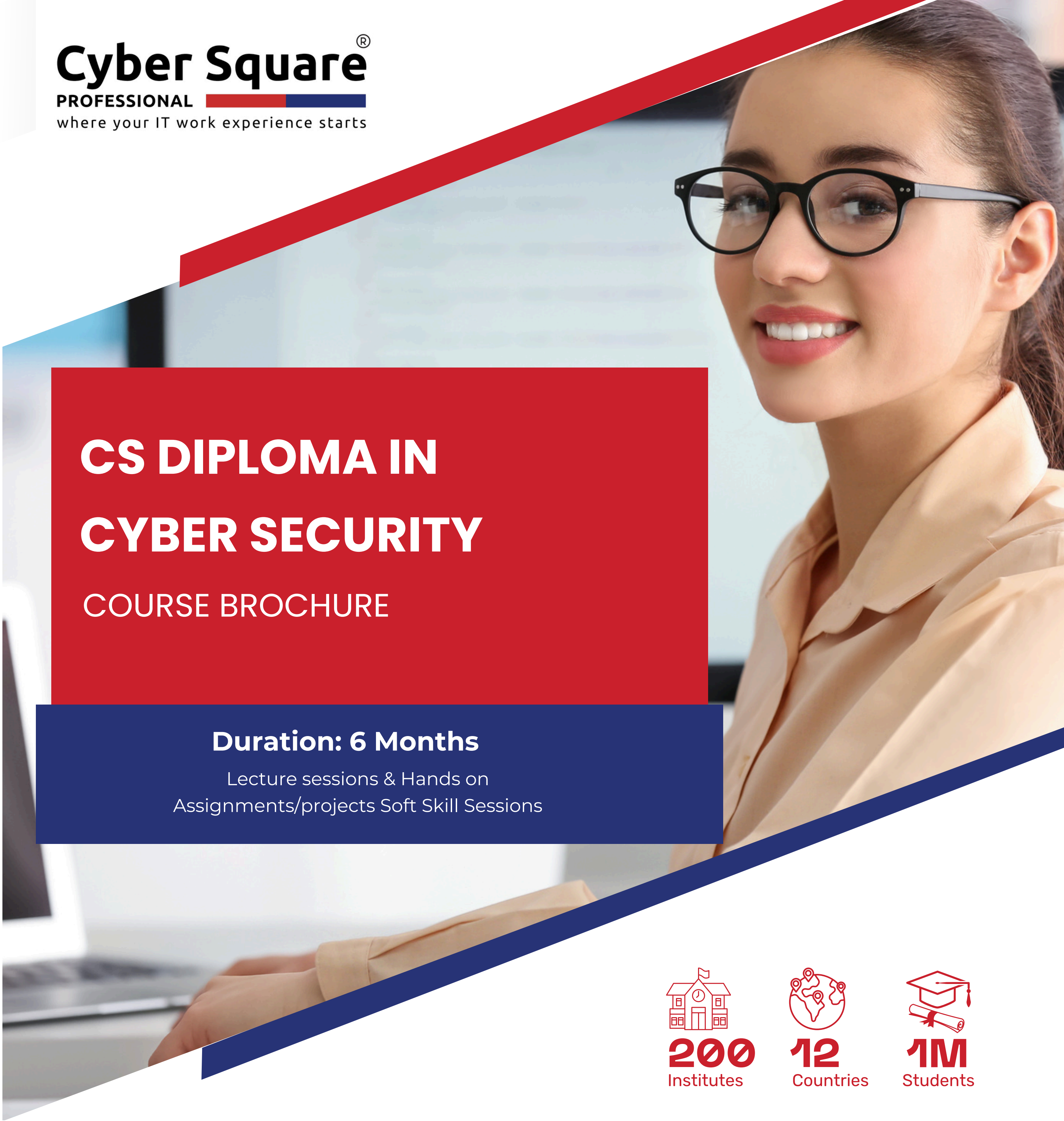
Cyber Square®
PROFESSIONAL
where your IT work experience starts



CS DIPLOMA IN CYBER SECURITY

COURSE BROCHURE

Duration: 6 Months

Lecture sessions & Hands on
Assignments/projects Soft Skill Sessions

200	12	1M
Institutes	Countries	Students

Empowering Tomorrow's High-Paying workforce
with Internship-Driven Industry Experience

STEM.ORG ACCREDITED™
EDUCATIONAL EXPERIENCE

ORAY
EDUCATION

https://cybersquare.pro/

About Cyber Square Professional

Immerse yourself in a unique learning experience where the virtual meets the real-world. Our courses go beyond conventional training, simulating a dynamic working environment that mirrors a global software company. Interns, dispersed worldwide, collaborate seamlessly on real projects, bringing the virtual workspace to life.

This international exposure not only sharpens the technical skills but also instills the collaborative spirit needed in today's interconnected software development landscape. Soft skills sessions are also seamlessly integrated, ensuring a holistic learning experience. Get ready to thrive in a virtual company setting, acquiring invaluable experience that transcends geographical boundaries.

About the Course

Embark on a transformative journey into the world of cybersecurity with our comprehensive internship program. Designed for both beginners and experienced individuals, this internship provides a robust foundation in both offensive and defensive cybersecurity practices. Through hands-on experience and expert guidance, you'll develop the skills necessary to excel in various cybersecurity roles.

Next, you'll dive into the role of a SOC Analyst, where you'll gain expertise in monitoring, detecting, and responding to security incidents. Learn to utilize advanced tools like SIEM (Splunk) and SOAR (Cortex XSOAR) to analyze logs, generate alerts, and automate security operations. You'll also explore the MITRE ATT &CK framework, malware analysis, and threat hunting techniques to enhance your incident response capabilities.

For those interested in penetration testing, our internship offers an in-depth exploration of ethical hacking methodologies. You'll start with the basics of cybersecurity and networking, progressing through advanced topics such as exploiting system vulnerabilities, cryptography, and social engineering. Practical labs and projects will give you hands-on experience with tools like Kali Linux, Metasploit, and Burp Suite.

Throughout the internship, you'll engage in real-world projects that provide practical experience and enhance your problem-solving skills. Benefit from the guidance of experienced cybersecurity professionals who will mentor you through complex topics and career paths. Additionally, connect with peers and industry experts, building a network that can support your career growth.

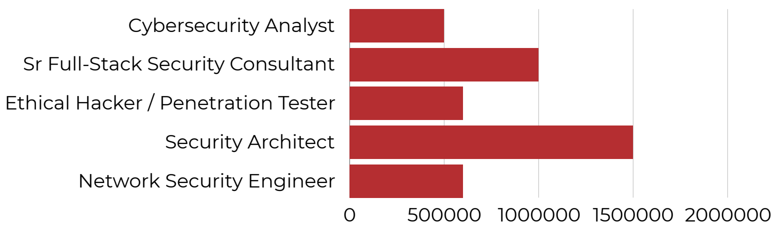
By the end of this internship, you'll have the skills and confidence to tackle real-world cybersecurity challenges. Whether you aim to become a SOC Analyst, Penetration Tester, or Bug Bounty Hunter, this program will equip you with the necessary knowledge and experience.

Reasons to learn Cyber Security

High Package

Cybersecurity professionals command competitive salaries due to the high demand for their expertise. Entry-level positions often offer above-average starting salaries, with significant growth potential as you gain experience and certifications.

Average Annual Salary



Growing Job Opportunities

- **High Demand Across Industries:** Virtually every sector requires cybersecurity expertise to protect sensitive data and infrastructure. This includes finance, healthcare, government, and tech industries.

- **Job Security:** With the rise in cyber threats, the demand for cybersecurity professionals is expected to grow. According to the Bureau of Labor Statistics, the employment of information security analysts is projected to grow much faster than the average for all occupations.

Impact and Importance

- **Protecting Critical Infrastructure:** Cybersecurity professionals play a vital role in safeguarding essential services like power grids, financial systems, and healthcare facilities from cyber-attacks.

- **Contribution to National Security:** By defending against cyber threats, cybersecurity experts help maintain national security and protect sensitive government data from hostile entities.

Diverse Career Paths

- **Variety of Roles:** The cybersecurity field offers a range of specializations such as ethical hacking, threat analysis, risk management, and compliance, allowing professionals to find their niche.
- **Interdisciplinary Opportunities:** Cybersecurity intersects with other fields like forensics, legal studies, and business, providing opportunities for roles in cyber law, digital forensics, and information assurance.

Continuous Learning and Development

- **Rapidly Evolving Field:** The cybersecurity landscape is dynamic, requiring professionals to continuously update their knowledge and skills. This offers opportunities for lifelong learning and staying intellectually engaged.

- **Access to Certifications and Training**: Numerous certifications (e.g., CISSP, CEH, CISM) and training programs are available to help professionals enhance their expertise and career prospects.

Remote Work Flexibility

- **Telecommuting Opportunities:** Many cybersecurity roles offer the possibility to work remotely, providing flexibility and a better work-life balance. This has become more prevalent due to advancements in secure remote access technologies.

- **Global Job Market:** Cybersecurity skills are in demand worldwide, allowing professionals to work for companies across the globe without the need to relocate.

Positive Job Satisfaction

- **Sense of Accomplishment:** Cybersecurity professionals often find their work rewarding as they play a crucial role in protecting organizations from significant threats and breaches.

- **Problem-Solving Engagement:** The field involves constant problem-solving and critical thinking, which can be highly satisfying for those who enjoy tackling complex challenges.

Who should take this course?

Cyber Security for whom?

This course is ideal for anyone with an interest in technology, problem-solving, and safeguarding digital information, as well as those seeking a high-demand career with excellent salary potential and job security.

□ Those with no prior knowledge of Cyber Security

□ Individuals Preparing for Cybersecurity Certifications

□ Those interested in roles such as Information Security Analyst, Ethical Hacker, Cybersecurity Consultant, or Chief Information Security Officer (CISO)

□ Students and Recent Graduates

□ Security Enthusiasts, Business and Risk Management Professionals

□ Entrepreneurs and Start-Up Founders

Student Intern Status - International Point System

Embark on a structured learning journey with our International Point System, an essential aspect of our internship placement process. Here's a snapshot of the process:

This system not only establishes a standardized evaluation process but also motivates students to excel in their internship, enhancing their preparedness for future professional endeavors. Embrace the International Point System and set yourself on the path to a rewarding placement experience.

Point Accumulation

Students earn points by successfully fulfilling the required tasks and objectives.

Mandatory Requirements

To be eligible for the placement process, students must complete a set of mandatory items outlined in our International Point System.

Minimum Required Points

Meeting the minimum required points is essential for students to qualify for the placement process. This ensures a fair and competitive environment.

Offensive Security - Penetration Testing

Course content

Module 1: Introduction to Cybersecurity

Objective: The module covers cybersecurity fundamentals, threats, vulnerabilities, risks, the CIA triad, and cybersecurity policies and procedures.

- Cybersecurity Fundamentals
- 4o Threats, Vulnerabilities, and Risks
- Security Principles (CIA Triad)
- Cybersecurity Policies and Procedures

Module 2: Introduction to Networking

Objective: Introduces network fundamentals, including TCP/IP and the OSI model, network devices and topologies, protocols and services, and essential network security concepts.

- Network Fundamentals (TCP/IP, OSI Model)
- Network Devices and Topologies
- Network Protocols and Services
- Network Security Concepts

Module 3: Introducing Kali Linux

Objective: Equip learners with the skills to set up, customize, and utilize Kali Linux for advanced cybersecurity tasks.

- Introduction to Kali Linux
- Setting Up Kali Linux Environment
- Essential Tools and Commands
- Customizing and Updating Kali Linux

Module 4: Ethical Hacking & Pen-testing Methodologies

Objective: Explores ethical hacking concepts, phases of penetration testing, legal and ethical issues, and standards such as PTES and OSSTMM.

- Ethical Hacking Concepts
- Phases of Penetration Testing
- Legal and Ethical Issues in Penetration Testing
- Penetration Testing Standards (PTES, OSSTMM)

Module 5: Data Intelligence

Objective: Focuses on open source intelligence (OSINT), including data collection and analysis, tools like Maltego and Recon-ng, and methods for analyzing and reporting data.

- Open Source Intelligence (OSINT)
- Data Collection and Analysis
- Tools for Data Intelligence (Maltego, Recon-ng)
- Analyzing and Reporting Data

Module 6: Scanning

Objective: Understand network scanning techniques, including port and vulnerability scanning, and the use of tools such as Nmap, Nessus, and OpenVAS, along with methods for analyzing scan results.

- Network Scanning Techniques
- Port and Vulnerability Scanning
- Tools: Nmap, Nessus, OpenVAS
- Analyzing Scan Results

Module 7: Machine Exploitation(30+ Machines)

Objective: Learn about exploiting system vulnerabilities, privilege escalation techniques, post-exploitation strategies, and the use of exploit frameworks.

- Exploiting System Vulnerabilities
- Privilege Escalation Techniques
- Post-Exploitation Strategies
- Using Exploit Frameworks

Module 8: Cryptography (Project 1)

Objective: Learn cryptographic concepts and algorithms, including symmetric and asymmetric encryption, digital signatures and certificates, and cryptographic tools and techniques.

- Cryptographic Concepts and Algorithms
- Symmetric and Asymmetric Encryption
- Digital Signatures and Certificates
- Cryptographic Tools and Techniques

Module 9: Steganography

Objective: Exploring steganography principles, methods, tools, and detection techniques.

- Principles of Steganography
- Methods of Steganography (Image, Audio, Video)
- Tools for Steganography (Steghide, OpenPuff)
- Detecting Steganography

Module 10: Metasploit

Objective: Introducing Metasploit Framework, including its use for exploitation, creating and customizing exploits, and post-exploitation modules.

- Introduction to Metasploit Framework
- Using Metasploit for Exploitation
- Creating and Customizing Exploits
- Post-Exploitation Modules

Module 11: Wireshark

Objective: Master network traffic analysis with Wireshark: capture, filter, and analyze packets to troubleshoot issues.

- Network Traffic Analysis with Wireshark
- Capturing and Filtering Packets
- Analyzing Network Protocols
- Troubleshooting Network Issues

Module 12: Social Engineering

Objective: Learn uncover phishing, pretexting, and psychological manipulation, and learn defenses against attacks.

- Social Engineering Techniques
- Phishing and Pretexting
- Psychological Manipulation
- Defense Against Social Engineering Attacks

Module 13: Shell Scripting (Project 2)

Objective: Learn shell scripting basics: write, execute, and automate tasks, with a focus on security automation.

- Basics of Shell Scripting
- Writing and Executing Scripts
- Automating Tasks with Scripts
- Scripting for Security Automation

Module 14: Introduction to Web Application Pen-testing (Project 3)

Objective: Explore web application architecture, common vulnerabilities, and penetration testing tools and methodologies.

- Web Application Architecture
- Common Web Vulnerabilities
- Penetration Testing Tools (Burp Suite, OWASP ZAP)
- Testing Methodologies

Module 15: Burp Suite

Objective: Get started with Burp Suite: configure, intercept, and analyze traffic, and perform automated and manual testing.

- Introduction to Burp Suite
- Configuring Burp Suite
- Intercepting and Analyzing Traffic
- Automated and Manual Testing with Burp Suite

Module 16: OWASP Top-10 (Project 4)

Objective: Explore the OWASP Top-10: analyze vulnerabilities, review case studies, and learn mitigation strategies.

- Overview of OWASP Top-10
- In-depth Analysis of Each Vulnerability
- Real-world Examples and Case Studies
- Mitigation Strategies

Module 17: Sniffing and Spoofing

Objective: Dive into network sniffing: ARP and DNS spoofing techniques, using Wireshark and Ettercap, with detection and prevention methods

- Network Sniffing Techniques
- ARP Spoofing and DNS Spoofing
- Tools: Wireshark, Ettercap
- Detection and Prevention Methods

Module 18: Bug Report Preparation

Objective: Write effective bug reports, detail findings, provide reproducible steps, and recommend mitigations.

- Writing Effective Bug Reports
- Detailing Findings and Impacts
- Providing Reproducible Steps
- Recommendations and Mitigations

Module 19: Final Project

Objective: Plan and execute a comprehensive penetration test

- Planning and Executing a Comprehensive Penetration Test
- Documenting Findings
- Presenting the Final Report
- Peer Review and Feedback

SOC Analyst

Duration: 3 Months

Sprint 7 (Project 6)

Objective: Introduction to SOC, network security, endpoint protection, threat intelligence, vulnerability assessment, and log analysis.

- Introudction to SOC
- Network and security concepts
- Network security
- endpoint security
- Threat Intelligence
- Vulnerability Assessment
- CIS Critical Controls
- Raw Log Analysis

Sprint 8 (Project 7)

Objective: Build your own SOC, case studies, labs, SIEM (Splunk), alert analysis, playbooks, incident response, and MITRE ATT&CK.

- Build your own SOC
- IR-Case studies
- Labs
- SIEM(Splunk)
- Alert Analysis
- Playbooks
- Incident Response
- MITRE ATT&CK

Sprint 9 (Project 8)

Objective: Master SOAR with Cortex XSOAR, threat hunting, compliance, playbook creation, and report generation.

- SOAR(Cortex XSOAR)
- Threat Hunting
- Compliance
- Playbook Creation
- Report Creation

Sprint 10 (Project 9)

Objective: Master the nuances of MSS RFPs.

- Malware Analysis
- Understanding MSS RFPs

Sprint 11 (Project 10)

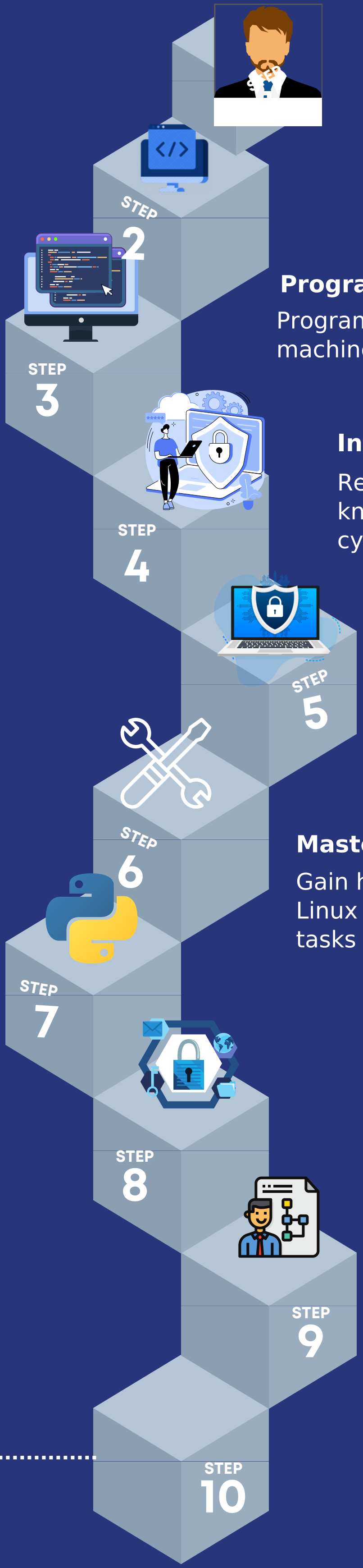
- CV Preparation
- Mock Interviews
- Project Disussion
- New Tool Evaluation

Sprint 12 (Project 11)

- SOC project
- Final Presentation of SOC Project and Findings

Learning Path

Cyber Square®
PROFESSIONAL
where your IT work experience starts



Basics of computer science

Computer architecture and organization Programming Computer networking

Programing Concepts

Programming concepts & machine language

Introduction to Cybersecurity

Recognize the core skills and knowledge needed for cybersecurity careers

Network Security Fundamentals

Define network types, components, data transmission, and network security principles.

Mastering the Tools

Gain hands-on experience with Linux and SQL for security tasks

Automating with Python

Leverage Python for cybersecurity tasks

Launching Your Cybersecurity Career

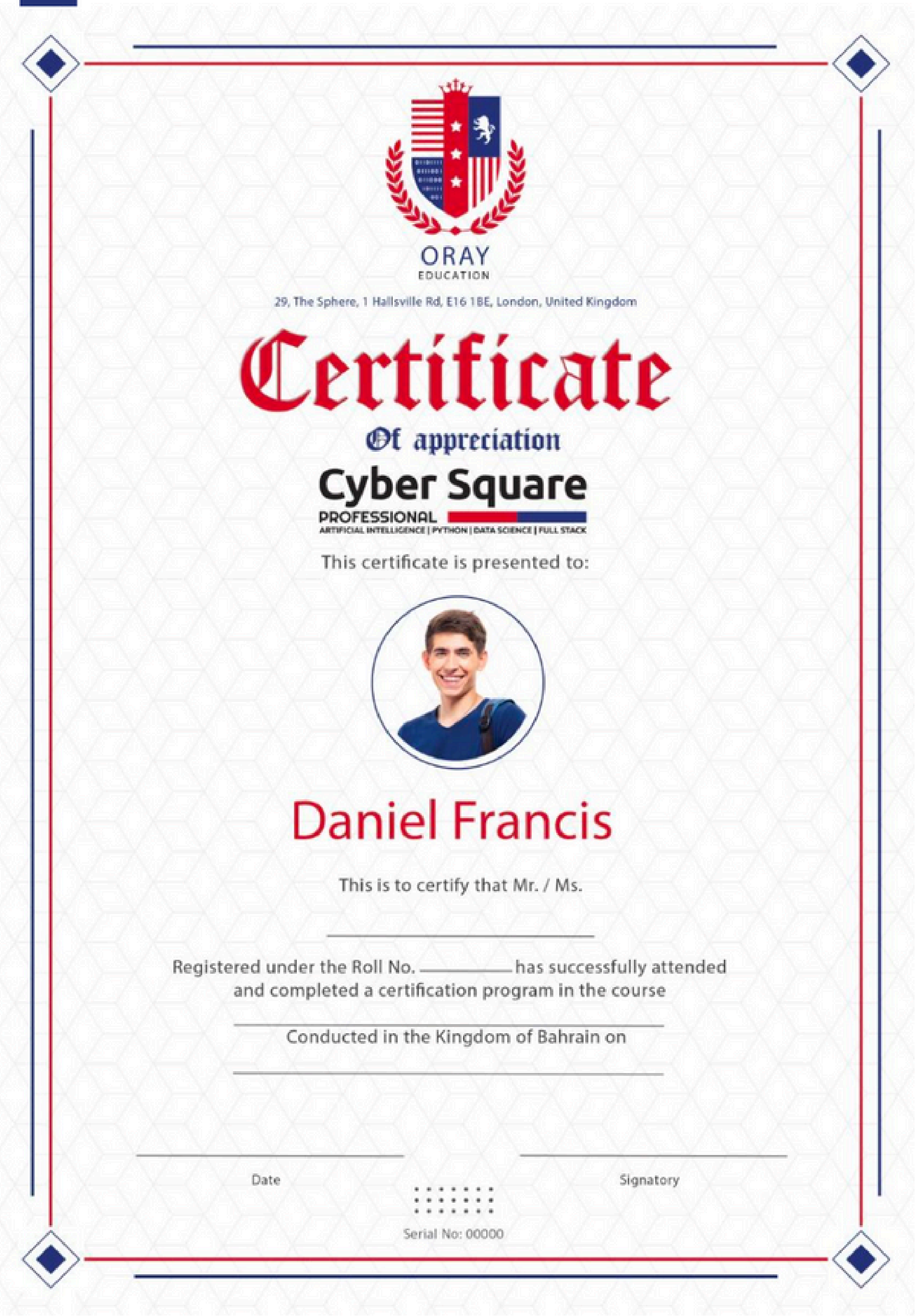
Develop strategies for job search, applications, and interviews

Project

Through practical experience with the project, interns go beyond theoretical knowledge, gaining hands-on experience and applying these technologies to enhance an existing project.

Completion Certificate

CERTIFICATE



ORAY
EDUCATION

29, The Sphere, 1 Hallsville Rd, E16 1BE, London, United Kingdom

Certificate

Of appreciation

Cyber Square
PROFESSIONAL
ARTIFICIAL INTELLIGENCE | PYTHON | DATA SCIENCE | FULL STACK

This certificate is presented to:

Daniel Francis

This is to certify that Mr. / Ms.

____

Registered under the Roll No. ________ has successfully attended
and completed a certification program in the course

____
Conducted in the Kingdom of Bahrain on
____

________________________ Date

________________________ Signatory

Serial No: 00000

Classroom-Level Immersion: Delivered Digitally

- Any Where, Anytime access
- Online Self learning
- Courses designed by alumni of IIT, NIT & IIM.
- CS Certificate Internship Certificate & UK Certificate
- CS Talent Show

Cyber Square Pro

Our Branch All Around World

ORAY EDUCATION

Cyber Square®
PROFESSIONAL
where your IT work experience starts

UK (Headquarters)

29, The Sphere,
1 Hallsville Rd, London E16 BE, UK Ph-
+44 7448 241977

CANADA

299 Senator street, Pickering,
ON L1V6N2, Canada
+1 647 3722376

INDIA

Cafit Square,
5th FLoor,
Hilite Business Park, Calicut, India
+91 9739954676

UAE

Suit No 51, Oasis Centre,
Sheikh Zayed Road, Dubai, UAE
+971 508881947

Cyber Square Pro

More Information About us?

Contact Us!

Cyber Square Pro is a learning platform and resource hub for professionals looking to learn cutting-edge digital skills, whether they're coding novices or programming pros.

Phone :

+91 859 205 8444

Address :

5th Floor, HiLite Business
Park, Thondayad Bye-Pass,
Kozhikode

Website :

https://cybersquare.pro/

Thank You!