CYBRON

CYBRON PROFESIONAL CERTIFIED CYBER SECURITY ARCHITECT PROFESSIONAL

Cybron Professional Certifications

CYBER SECURITY RAPID OFFENSIVE NATIVE FORUM

Published by:

Cyber Security Rapid Offensive Native Forum

Cybron

404 Old Bedford Road, Luton, England LU2 7BP SIC codes – 62012 United Kingdom

contactus@cybroninternational.com

(+44) 7783 530138

,

Contents

INTRODUCTION

We help you to establish your career in Cyber Security

Many students aspire to build their careers in the field of cybersecurity, but due to the lack of proper guidance and structured pathways, they often struggle to progress in line with market demands. Research shows that while some schools have introduced cybersecurity-related content, the curriculum is limited, outdated, and insufficient to meet the evolving needs of both students and society.

However, emerging technologies are reshaping the landscape, and new methodologies and systems associated with Industry 4.0 and 5.0 play a vital role in building Society 5.0. To remain competitive in both local and international markets, students and professionals must develop a deep understanding of these latest technologies and acquire the skills to work effectively with them.

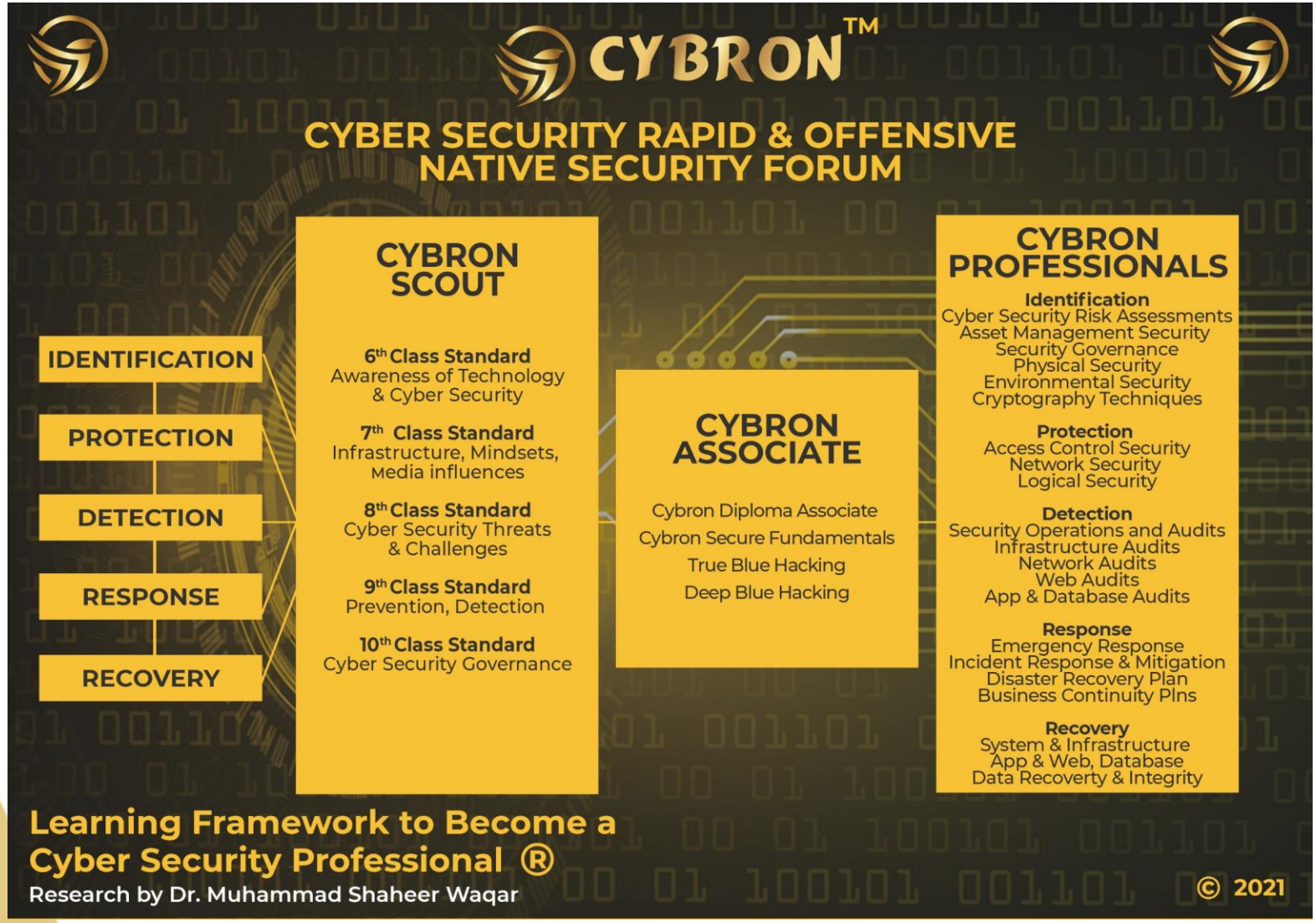
With reference to the above discussion, a significant gap between industry and academia has been identified. This gap continues to widen daily as technology evolves rapidly, while academic institutions often struggle to update and deliver the latest knowledge in a timely manner.

In this context, it is evident that our daily lives, whether at home, in the office, or in business are increasingly connected through digital technologies and the Internet. Today, most services and products are delivered via Information Technology**,** bringing immense convenience and efficiency. However, alongside these advantages comes the growing challenge of cybersecurity. To address this, I have developed a new framework that introduces cybersecurity education from the secondary school level and progressively advances to the professional level**.**

The Cybron Certified Cyber Security Architect program is for Professionals and has been designed after detailed research to identify the essential requirement for professional. The course integrates industry frameworks (NIST, ISO 27001, TOGAF, SABSA, Zero Trust, Cloud Security Alliance) with practical design labs, preparing participants to design secure systems, align with business objectives, and manage risks effectively**.**

CYBRON FRAMEWORK

One of the Leading Learning Framework of Cyber Security



CYBRON FRAMEWORK DESCRIPTION

The CYBRON framework, influenced by the international standard NIST (USA) and further expanded through research, addresses critical gaps in cybersecurity practices. While organizations and industries invest heavily in advanced security tools and monitoring systems to safeguard their data, processes, and technologies from unauthorized access, absolute security remains uncertain. Despite substantial investment, no organization can confidently claim complete protection against internal or external threats, attacks, or risks.

In this context, Dr. Muhammad Shaheer Waqar has introduced a new dimension in cybersecurity through the development of CYBRON - the Cyber Security Rapid Offensive Native Forum. According to his research, cybersecurity is not solely about tools and systems but fundamentally a matter of mindset. As children grow and learn about the world, they must also understand technology, its benefits, and its role in making life easier and more efficient. At the same time, they should recognize the importance of using these technologies responsibly rather than misusing them to harm others.

The first pillar of the CYBRON framework focuses on cultivating a positive mindset from an early age. Students are guided to view digital technologies as valuable, beneficial, and supportive tools in their daily routines. They are encouraged to use technology constructively and avoid negative or harmful practices.

Another key aspect of the framework is awareness of threats. Children and young learners are taught that malicious actors exist in the digital environment and may attempt to sabotage, harm, or disrupt their lives. Therefore, the "good users" must be equipped with knowledge of cybersecurity threats, risks, and challenges - both current and emerging, so they can protect themselves and, ultimately, contribute to safeguarding society and humanity at large.

Through this mindset-driven approach, the CYBRON framework seeks to create a generation of responsible digital citizens who are both aware of cybersecurity dangers and empowered to defend themselves and others in the digital age.

PROGRAM BENEFITS TO & PRE-REQUISITE

REQUIRED QUALIFICATIONS

- Bachelor's Degree or 14 years of Education or equivalent is required with cyber security background
- 2 years of Working Experience in the field of cyber security

CREDENTIALS

- Cyber Security Architect Certification from Cybron International - UK
- International Recognized Certificate from Cybron UK

BENEFITS

- After this course you can able to design Enterprise level security understanding
- It covers major frameworks (NIST, ISO 27001, TOGAF, SABSA, Zero Trust, Cloud Security Alliance)
- You can design and implement resilient and scalable security architectures for on-premises, cloud, and hybrid environments.
- Conduct threat modeling, risk assessment, and security gap analysis
- Architect identity and access management (IAM), network security, cloud security, and application security solutions.
- Design incident response, business continuity, and disaster recovery (BC/DR) strategies.
- Develop governance, policies, and compliance roadmaps for enterprises.

WHO CAN DO THIS CERTIFICATION

- Senior IT Managers & System Engineers
- Information Security Professionals
- Solution Architects / Enterprise Architects
- Cybersecurity Consultants
- SOC Managers & Incident Responders
- IT Risk & Compliance Officers
- IT Auditors
- Management Consultants of Information Security

PROGRAM STRUCTURE

Total Lectures	30
Online Lectures	Available on LMS
Accredited Trainers	Can Deliver the lectures
Each Lecture Duration	2 hours
One Credit Hour	60 Learning Hours
Total Credits Required	6 Credit Hours
Assessment	Online / Paper based
Passing Criteria	70 percent

OTHER LEARNING ACTIVITIES

- Design Enterprise level security architect
- Use any one of major frameworks (NIST, ISO 27001, TOGAF, SABSA, Zero Trust, Cloud Security Alliance) and incorporate as use case in the organization
- Design and implement resilient and scalable security architectures for on-premises, cloud, and hybrid environments.
- Learn and conduct threat modeling, risk assessment, and security gap analysis
- Architect identity and access management (IAM), network security, cloud security, and application security solutions**.**
- Design incident response, business continuity, and disaster recovery (BC/DR) strategies**.**
- Develop governance, policies, and compliance roadmaps for enterprises.

PROGRESSION OF THE PROGRAM

Total Credentials	=	6 Credit Hours
One Credit Hours	=	60 Learning hours
Final Assessment	=	Online or physical assessment can be taken

Awarding of Cybron Certified Cyber Security Architect

Once the candidate has completed the content, then candidate can apply through partners/trainers or directly to Cybron UK for assessment.

DOMAINS AND TASKS

In this document you will find an updated structure for the CYBON Certification Examination Content Outline. We have devised and simplifying the format so that the CYBRON CERTIFICATION is easier to understand and interpret.

The domain and task are well defined on the following pages:

Domain: Defined as the high-level knowledge area that is essential to the practice of Cyber Security.

Tasks: The underlying responsibilities of the cyber security team member within each domain area.

CYBRON CERTIFICATION Course examination will include all tasks of each domain, and CYBRON will adhere to the percentage of coverage at the domain level as outlined in the further pages.

KNOWLEDGE AREAS

Domain 1: Foundations of Cyber Security Architecture	
Task 1	Role of a Cyber Security Architect Core principles of security architecture (Confidentiality, Integrity, Availability, Resilience)
Task 2	Overview of SABSA, NIST, TOGAF, and Zero Trust frameworks Business-IT alignment in security architecture
Task 3	Case study: Mapping business drivers to security controls

Domain 2: Security Governance & Frameworks	
Task 1	Security policies, standards, and procedures Risk management methodologies (ISO 27005, NIST RMF, OCTAVE) Legal, regulatory, and compliance requirements (GDPR, HIPAA, PCI-DSS, etc.)
Task 2	Designing a Governance, Risk & Compliance (GRC) architecture
Task 3	Practical Lab: Developing a governance blueprint for an enterprise

Domain 3: Threat Modeling & Risk Assessment	
Task 1	Understanding threat actors and threat vectors STRIDE, DREAD, and MITRE ATT&CK frameworks
Task 2	Attack surface analysis and architecture resilience Security by Design principles
Task 3	Lab: Building a threat model for a real-world system

Domain 4: Enterprise Security Architecture Design	
Task 1	Architectural layers: Business, Information, Application, Technology, Security Security patterns and design principles
Task 2	Secure network design (segmentation, firewalls, IDS/IPS, Zero Trust Network Access) Integration of cloud and hybrid infrastructures
Task 3	Lab: Designing a secure enterprise architecture

Domain 5: Identity, Access & Data Security	
Task 1	Identity and Access Management (IAM) architecture Role-based access control (RBAC), Attribute-based access control (ABAC), and Privileged Access Management (PAM)
Task 2	Data security architecture (encryption, tokenization, DLP, database security) Federation and Single Sign-On (SSO) architectures
Task 3	Lab: Designing IAM for a multi-cloud environment

Domain 6: Cloud & Emerging Technology Security	
Task 1	Learn Cloud security frameworks (CSA CCM, NIST Cloud)
Task 2	How to Secure multi-cloud architecture (AWS, Azure, GCP)
Task 3	Securing containers, microservices, and DevSecOps pipelines
Task 4	Security in Industry 4.0 / 5.0 (IoT, AI, Blockchain, 5G)
Task 5	Lab: Architecting a secure multi-cloud infrastructure

Domain 7: Security Operations & Monitoring Architecture	
Task 1	Security Information and Event Management (SIEM) design
Task 2	Security Orchestration, Automation, and Response (SOAR)
Task 3	Designing a Security Operations Center (SOC)
Task 4	Threat intelligence and hunting in architectural design
Task 5	Lab: Building a SOC architecture for an enterprise

Domain 8: Incident Response, Business Continuity & Disaster Recovery	
Task 1	Incident Response (IR) planning and frameworks
Task 2	Crisis management and forensics readiness
Task 3	Business continuity planning (BCP) and Disaster Recovery (DR) architecture
Task 4	Lab: Designing an IR and BCP/DR strategy for a critical infrastructure

CYBRON PROFESSIONAL REGISTRATION AND PAYMENT

REQUIRED QUALIFICATIONS

- Bachelor's Degree or 14 years of Education or equivalent is required with cyber security background
- 2 years of Working Experience in the field of cyber security

CREDENTIALS

- Cyber Security Architect Certification from Cybron International - UK
- International Recognized Certificate from Cybron UK

REGISTRATION PROCESS

Registration can be done through our registered partners/trainer or if you do not any registered partners at your vicinity then you can directly approach to Cybron International UK office through email registration@cybroninternational.com for admission and registration.

PROGRAM BIFURCATION

The program is bifurcated into 60 learning hours where different tasks can be given to learn and understand and give the examination accordingly. The preparatory material is available through our partners/ trainers/ institutes and our LMS directly.

ASSESSMENT OF PROGRAM (ONLINE/PHYSICAL)

- The paper will be an open book and students can give the answers according to scenarios
- The paper will be online/physical including practical and theory.
- The weightage of examination will be practical, and theoretical.
- Practical assessment will be taken in labs assessors by internal examiners, where theory paper will be taken through online or paper based (if online facility not available)
- Those candidate who cannot be able to give the online test and they do not have a facility, Therefore, their papers will be taken a paper based examination. Otherwise, center must have the facility to provide online test mechanism to students and facilitate for the final assessment.
- Assessment will be done according to domain and tasks defined above through our online methodology

CYBRON CERTIFIED CYBER SECURITY ARCHITECT
FEE STRUCTURE

S. No	Description	Fees
1	Program Fee For Members	595 British Sterling Pound
2.	Program Fee Non-Members	795 British Sterling Pound For

CYBRON PROFESSIONAL EXAMINATION SYSTEM

Partner Institute Internal Examination System

- The concerned partner / institute / trainer or Cybron examination will take the online examinations and if the concerned partners/students would not have the facility to give the online examinations then it physical examination can be taken on request and partner will submit to the Cybron International Examination Department through email at examinations@cybroninternational.com

Cybron UK Online Exam System

Cybron International UK will provide access to all partners/trainers to schedule the exams of any course of any registered individual candidate. According to the availability of schedule, the partner institutes can schedule the exam of any individual subject or course/certification.

CONTINUING EDUCATIONAL REQUIREMENTS (CER) PROGRAM

CER—Continuing Educational Requirements Program is important and supports the ongoing educational and professional development of any candidate. Therefore, Cybron International insists on keep learning according to current market requirements. You have to prepare to meet the demands of the market each today due to the most complex and competitive environment of businesses, you have to develop yourself.

The main purpose of CER is:

- Continuously develop yourself and enhance your learning capability
- Keep yourself updated about the latest trends in technologies and vulnerabilities
- We encourage and recognize individualized learning opportunities
- 60 hours of learning CER is mandatory to make your diploma/certification active
- Submit your membership and certification/diploma fee £ 50 every year
- Global Recognition to sustain the valuable diploma of Cybron International (CI)

Note: If you any issue to submit your CER and its, so you may contact to our local partner, who help you in this regard. Further, if you have any issue, then you can directly email us examinations@cybroninternational.com

CONTACT DETAILS

CONTACTUS@CYBRONINTERNATIONAL.COM

ADDRESS 404 Old Bedford Road, Luton, England LU2 7BP SIC codes – 62012 United Kingdom

TELEPHONE (+44) 7783 530138

Web https://www.cybroninternational.com

EMAIL info@cybroninternational.com

SOCIAL MEDIA ACCOUNT

Facebook https://www.facebook.com/cybroninternational

Twitter https://x.com/cybronintl

LinkedIn https://www.linkedin.com/company/cybron-international

YouTube https://www.youtube.com/@cybroninternational

CYBRON INTERNATIONAL LIMITED

COMPANY REGISTRATION 14686268

UNITED KINGDOM