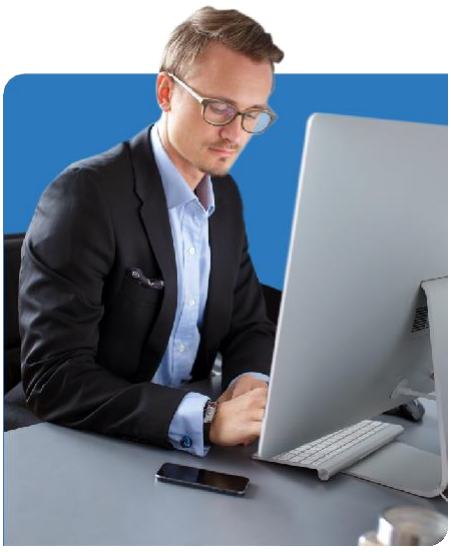
ThriveDX

ThriveDX Fundamentals of Cybersecurity for Executives

TDXCS-19



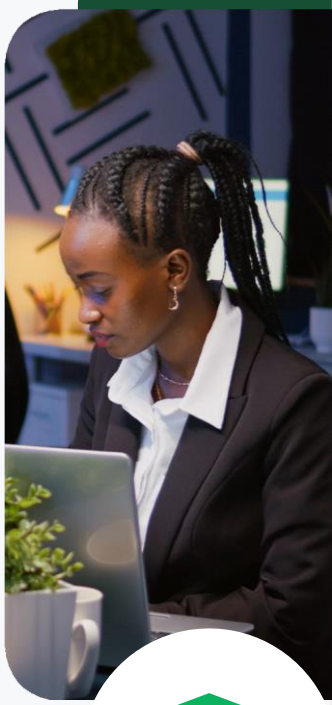
ThriveDX Fundamentals of Cybersecurity for Executives Course

Time Commitment	Skill Level	Format	Course Category
16 hours total (2 days, 8 hours/day)	Basic Level: Cybersecurity Essentials	Online (Live), Instructor-Led, On-Demand	Cyber Defense

This course equips professionals with the essential knowledge and skills to navigate the complex world of cybersecurity. Participants will delve into three key modules, each focusing on critical aspects of cybersecurity, ensuring that participants are equipped with the practical skills to protect their organization's digital assets and mitigate cyber risks effectively.

Who Should Attend:

- **Business Leaders and Executives** Individuals responsible for overseeing cybersecurity strategies and policies within their organizations.
- **Managers and Team Leaders** Those managing teams responsible for cybersecurity or involved in cybersecurity operations.
- **IT Professionals** IT professionals seeking to expand their knowledge of cybersecurity
- **Business Analysts and Consultants**: Professionals involved in advising on business processes and strategies can benefit from understanding cybersecurity risks and implications for business operations.
- **Anyone Interested in Cybersecurity** Individuals with a general interest in cybersecurity who want to gain foundational knowledge and skills in the field.



Prerequisites:

- Basic computer literacy and familiarity with using the internet.
- Interest in cybersecurity and a desire to learn about cybersecurity principles and practices. (No prior cybersecurity knowledge or experience is required, as the course will cover foundational concepts).

Upon Completion, Participants will Emerge with:

1

Introduction to cybersecurity, including the need for cybersecurity, fundamental procedures, prevalent security threats, and their impact on businesses.

2

Box 2

Understanding attackers, their motivations, and how they launch attacks, as well as advanced persistent threats (APTs) and the cyber kill chain.

3

Mitigating risks through ethical hacking, employee education, and risk management processes and standards (e.g., PCI, PHI, PII).

4

Introduction to malware types, analysis approaches (static and dynamic), and their impact on cybersecurity.

5

Overview of cybersecurity policies, procedures, and guidelines, including password policies and the CIA triad (confidentiality, integrity, availability).

Program Structure

Module 1

The Cybersecurity World and Crime

The learner will begin by gaining an understanding of the need for cybersecurity in every organization, the fundamental procedures that must be followed by cybersecurity professionals, the most prevalent security threats, and how they are carried out and affect various industries.

Topics Covered

- The need for cybersecurity
- The impact of cyber threats on business
- Ensuring cybersecurity
- Recent cyber attacks with critical consequences on businesses
- How AI Changes the game of cybersecurity
- Common Cyber Security Threats: DoS/DDoS, brute force, MITM, social engineering, phishing, and spear phishing
- Malware types: ransomware, trojan, virus, worm, adware
- Blue and Red Teams

Module 2

Attackers and APTs

The learner will gain an understanding of the hacking aspect of cyber by studying the various kinds of attackers, their motivations, and how they launch and distribute their objectives. The learner will gain insight into advanced persistent threats and the most well-known groups over the past few years. The learner will understand the cyber kill chain and all the processes that attackers follow, from initiating an attack to achieving their goals.

Topics Covered

- Attacker types: Cyber terrorists, industrial spies, insiders, hacktivists, cybercriminals
- Exploits, vulnerabilities, zero-day attack, payload, and RAT
- Advanced Persistent Threats: APT goals, stages, famous groups, case studies, and warning signs
- The cyber kill chain stages
- Types of hackers
- Ethical hacking (Red Team and Bug Bounty)

Module 3

Mitigating The Risk & Taking Control

The learner will delve into the significance of ethical hacking and discover how employee education, such as enforcing password policies, can prevent cyberattacks. The learner will then explore the risk management processes, the most well-known policies, procedures, standards, and guidelines, including PCI, PHI, and PII, as well as practice managing a risk process.

Topics Covered

- Business Impact Analysis and Risk Assessment
- NIST and MITRE Frameworks
- Valuable data types and data protection standards: PII, PCI, PHI
- Enforcement of strong passwords
- Risk management processes
- CIA triad
- Practicing risk management—real-world examples

Certification Readiness

All participants completing the course will receive a **ThriveDX Course Completion Certification.**

Embedded Labs and Challenges

The course includes our state-of-the-art proprietary cloud-based digital education platform, **TDX Arena**, in which real-life scenarios and advanced tech teaching meet in a gamified environment.