Advanced Executive Program In Cyber Security

TCEP Cyber Executive Program

6 Month Program	36 CPEs	Laptop Required

You Will Learn

- Understanding of ethical hacking's importance, legal aspects, and methodologies.
- Mastery in reconnaissance, network scanning, exploitation, and post-exploitation.
- Proficiency in assessing and securing web applications, addressing XSS and SQL injection.
- Ability to evaluate and secure wireless networks, including Wi-Fi encryption.
- Understanding of cryptography, encryption, and basic cryptanalysis techniques.
- Skill in identifying and prioritizing vulnerabilities, bolstering defense mechanisms.
- Hands-on experience with Metasploit Framework for vulnerability exploitation.
- Practical application in simulated red team engagements, from planning to reporting.
- Real-world scenario labs for skill practice in controlled environments.
- Proficiency in documenting findings and vulnerabilities for stakeholders.

TCEP Cyber Executive Program

TIAC Cyber Executive Program

The program stands out due to its practical approach, blending theoretical knowledge with hands-on experiences.

- This program boasts a faculty comprising industry experts and renowned professionals, ensuring participants receive the latest insights and practical experiences directly from those actively engaged in the cyber security field.
- Throughout the course, participants engage in live cyber security challenges, where they have the opportunity to respond to simulated real-time threats, enhancing their crisis management and incident response skills.
- Delving into ethical hacking intricacies, the program includes workshops that tackle real-world ethical dilemmas and gray areas in cyber security, helping participants develop a robust ethical compass.

The Advanced Executive Program in Cyber Security offered by Tutelr's TIAC (Tutelr Information Assurance Certification) is an intensive and comprehensive course meticulously designed to provide seasoned professionals with a thorough understanding of the complex and evolving landscape of cyber security. Covering a wide array of advanced topics, this program ensures that participants are equipped with the knowledge and skills necessary to effectively lead and manage cyber security initiatives within their organizations.

The syllabus encompasses critical modules that delve into the intricacies of cyber security, such as Network Security, System Security, Cloud Security, Cryptography, Incident Response, and more. Notably, the course places a strong emphasis on understanding the ever-evolving cyber threat landscape, legal and ethical aspects, and the nuances of risk management. Participants will also learn about the integration of privacy regulations, like GDPR, into the broader cyber security framework.

The program stands out due to its practical approach, blending theoretical knowledge with hands-on experiences. The four assignments provided as part of the curriculum require participants to apply their learning to real-world scenarios. These assignments cover areas such as risk assessment, network security implementation, application security analysis, and incident response simulation. Furthermore, the culminating project, centered around cyber security strategy development, provides participants the opportunity to synthesize their skills and devise comprehensive strategies for effectively safeguarding organizations against cyber threats.

As a testament to its comprehensive nature, the final examination evaluates participants on their ability to practically apply their knowledge across a range of scenarios. This includes understanding and responding to cyber threats, analyzing case studies, proposing solutions, and demonstrating their adeptness at critical cyber security thinking.

In summary, the Advanced Executive Program in Cyber Security offered by Tutelr's TIAC not only imparts cutting-edge knowledge but also hones participants' practical skills in addressing complex cyber security challenges. It prepares individuals to take on leadership roles in the cyber security domain, equipping them with the tools necessary to navigate the ever-changing cyber landscape and protect their organizations effectively.

"I could take this course five times more and get something new each time! So much valuable info to take back to my organization."

-Thowbik Ahmed - Security Engineer, **Freshworks Inc.**

"This course is terrific! Class discussion and relevant case studies are extremely helpful for better understanding the content."

-Charan Kumar - **SISA InfoSec**

Module Descriptions

Module 1: Foundations of Cyber Security

Unlocking Digital Fortresses: Embark on a Journey Through the Foundations of Cyber Security! Dive deep into the virtual realm where you'll uncover the secrets that safeguard the digital world. From deciphering the cyber threat landscape to mastering the art of risk management, this module sets the bedrock for your cyber security prowess. Join us to build a robust foundation that defends against the invisible forces lurking in the digital shadows.

TOPICS:

- **Introduction to Cyber Security**
- **Cyber Threat Landscape and Trends**
- **Information Security Principles**
- **Risk Management and Assessment**
- **Legal and Ethical Aspects of Cyber Security**

MODULE 3: System Security

Step into the heart of cyber fortifications with our 'System Security' module. Delve deep into the art of safeguarding digital citadels, learning to lock down operating systems, fortify endpoints, and wield the power of security configurations.

TOPICS:

- **Operating System Security**
- **Endpoint Protection and Antivirus**
- **Application Security**
- **Patch Management**
- **Security Configuration and Hardening**

MODULE 5: Cryptography and Data Protection

Discover the art of safeguarding information in the digital age with our immersive course on Cryptography and Data Protection. Delve into the world of encryption, where messages become codes and secrets are shielded from prying eyes. From unbreakable ciphers to the marvels of public-key infrastructure, join us in decoding the intricate dance between mathematics and security. In a realm where data is gold, learn the methods that keep it impenetrable, and unveil the shield that protects modern communication. Unleash the power of cryptography and become the guardian of digital secrets in an evolving cyber landscape.

TOPICS:

- **Encryption Algorithms and Protocols**
- **Public Key Infrastructure (PKI)**
- **Digital Signatures and Certificates**
- **Data Privacy and GDPR**
- **Cryptocurrency and Blockchain Security**

MODULE 7: Incident Response and Digital Forensics

Embark on a journey into the heart of cyber investigations with our module on "Incident Response and Digital Forensics." Decode digital evidence, trace threats, and craft precise response strategies. Unleash your inner digital detective and safeguard the virtual realm. Join us to master the art of cyber investigations!

TOPICS:

- **Incident Response Process**
- **Digital Evidence Collection and Preservation**
- **Forensic Analysis Techniques**
- **Incident Reporting and Documentation**
- **Post-Incident Recovery and Lessons Learned**

Module 2: Network Security

In the dynamic realm of cyber warfare, your organization's first line of defense is a robust network security infrastructure. Dive into the Network Security module of our Advanced Executive Program by Tutelr's TIAC, where you'll become the sentinel of the digital frontier. From dissecting cyber threats to fortifying digital perimeters, you'll wield cutting-edge tools and strategies to safeguard data highways. Unravel the mysteries of intrusion detection, firewall fortifications, and threat monitoring, as you become the architect of an impenetrable cyber citadel. Elevate your expertise and stand as the guardian of the network ramparts in an ever-evolving landscape of digital challenges.

TOPICS:

- **Network Architecture and Protocols**
- **Network Threats and Vulnerabilities**
- **Firewalls and Intrusion Detection Systems**
- **Virtual Private Networks (VPNs)**
- **Network Security Monitoring and Incident Response**

Module 4: Cyber Threats and Attacks

Explore the dark realms of the digital world in our captivating module on 'Cyber Threats and Attacks.' Discover the clandestine tactics employed by malicious actors as we unveil the methods behind malware, social engineering, and relentless Denial of Service assaults. Dive into the world of Advanced Persistent Threats (APTs) and spear phishing, arming yourself with insights to safeguard against cyber onslaughts.

TOPICS:

- **Malware Analysis and Reverse Engineering**
- **Social Engineering Attacks**
- **Phishing and Spear Phishing**
- **Denial of Service (DoS) Attacks**
- **Advanced Persistent Threats (APTs)**

MODULE 6: Cloud Security

Embark on a journey into the realm of cloud security where innovation meets protection. Our Cloud Security course isn't just about data in the cloud; it's about fortifying the future of digital landscapes. Discover how to wield the immense potential of cloud technologies while safeguarding your data with iron-clad defenses. From virtual fortresses to data encryption spells, join us in deciphering the secrets of cloud security. Elevate your expertise and soar high above the threat horizon with a skill set that ensures your data stays untouchable amidst the ever-changing cloudscape

TOPICS:

- **Cloud Computing Models**
- **Cloud Security Risks and Controls**
- **Identity and Access Management in Cloud**
- **Data Security in Cloud Environments**
- **Cloud Incident Response and Forensics**

Who Should Attend

- IT Professionals: Individuals working in IT roles who seek to specialize in cyber security and enhance their skills to effectively protect digital assets and networks.
- Security Analysts: Those currently in security roles looking to advance their knowledge in specific areas such as penetration testing, incident response, or digital forensics.
- Network Administrators: Professionals responsible for managing and securing networks who want to broaden their understanding of cyber threats and mitigation techniques.
- System Administrators: Individuals handling system configuration and management, interested in securing systems against potential cyber attacks.
- Software Developers: Developers aiming to create secure applications by understanding vulnerabilities and incorporating robust security measures into their coding practices.
- Risk Managers: Those tasked with assessing and mitigating risks, including cyber risks, who wish to incorporate advanced cyber security strategies into their risk management approach.
- Cybersecurity Enthusiasts: Individuals passionate about cyber security, even without prior experience, looking to kickstart their career in the field and develop practical skills.
- Recent Graduates and Students: Graduates and students studying computer science, IT, or related fields who want to specialize in cyber security to meet the growing industry demand.
- Security Consultants: Those consulting organizations on security matters, aiming to expand their expertise and provide more comprehensive solutions.
- Professionals Switching Careers: Individuals transitioning from other fields into cyber security, attracted by its dynamism and the increasing need for skilled professionals.

NICE Framework Work Roles

1. Security Analyst
2. Penetration Tester (Ethical Hacker)
3. Security Consultant
4. Incident Responder
5. Security Engineer
6. Cyber Threat Analyst
7. Digital Forensic Analyst
8. SOC Analyst (Security OperationsCenter)
9. Cybersecurity Architect
10. Security Compliance Officer
11. Cybersecurity Trainer/Educator
12. Security Operations Manager
13. Network Security Engineer
14. Malware Analyst
15. Security Risk Analyst