MedTech
Mediterranean
Institute of Technology

EXECUTIVE MASTER
DIGITAL HEALTH AND AI

• WWW.MEDTECH.TN •

Welcome

President's message

The strategic location of Tunisia in the heart of the Mediterranean combined with the diversity of its cultural heritage constitute major assets for the development of a regional hub of educational excellence.
It is in this framework that we have developed the South Mediterranean University (SMU).
On behalf of all members of our management team, we want to make your education at SMU a life changing experience and wish you success in your drive for professional excellence.

Mahmoud TRIKI,
Founder & President, SMU

Shape your **future** at MedTech

Our vision

MedTech aspires to be a regional hub of excellence in engineering education by fostering innovative learning and societal impact.

Our mission

MedTech is committed to train highly qualified engineers capable of contributing and leading innovative ventures in today's globalized world.

Our values

- Diversity
- Excellence
- Integrity
- Creativity
- Care

Major Achievements

- Internationally accredited Engineering programs by ABET
- Partnerships with top ranked universities (University of Michigan, HEC Montréal, Oakland University, etc.)
- State-of-the-art facilities

Our **learning strategy**

MedTech implements an adaptive learning strategy that offers students a life changing experience.

Digital

MedTech is facilitated with technology, information and instructions that are enhanced using various applications, tools and resources to improve the learning experience.

Active

Our active pedagogy allows our students to be continuously involved in the learning process through individual and group activities, bootcamps, simulation games enabling them to develop a variety of skill sets that differentiate our graduates on the job market.

Interdisciplinary

By combining our curricular objectives to different disciplines, we help our students acquire the knowledge and skills necessary for their personal and professional development.

The **Executive Master in Digital Health and AI** at a glance

In the dynamic healthcare landscape, the convergence of Digital Health and Artificial Intelligence (AI) is reshaping how we understand and deliver healthcare globally.Digital health technologies and AI emerge as transformative allies, offering innovative solutions to enhance patient outcomes, streamline workflows, and redefine the healthcare delivery. Notably, the importance of digital health extends universally, playing a pivotal role in overcoming disparities and improving access to quality healthcare worldwide.

The Program

The objective of the program is to train professionals from both the Healthcare and Engineering sectors and equip them with the necessary tools and competencies for leading Digital Health transformation projects while understanding the challenges in designing and developing AI-driven digital health solutions, with assurances of their ethical, safe, and effective deployments.

The program consists of modules and workshops aiming at:

- Develop artificial intelligence and Analytics techniques to integrate them into fast, optimal and low-cost digital health solutions.
- Overcome governance, interoperability, and data security challenges faced in health digitalization projects.
- Develop communication and change management skills.
- Operate and lead in a multidisciplinary environment.

The Format

The Executive Master in Digital Health and AI is a part-time program, designed to tailor the work and life commitments of participants. Classes meet four days a month (Thursday through Sunday from 9:00 AM to 6:00 PM) over a 17-month period, followed by three additional months dedicated to the final project.

Program at a glance

MESRS

Duration	Modules	Final project
17 months	**15**	**1**

Workshops	Course per month
5	**1 or 2**

The program key **differential values**

- **Strong methodological approach** facilitated with digital tools to achieve efficient coordination of processes, workflows, people, assets, and technology that Digital Health requires.
- **Tailored learning pathways** to meet the needs of professionals from different sectors of the digital transformation of Health, Health professionals, engineers, technicians, developers and managers.

Participant **profiles**

1.

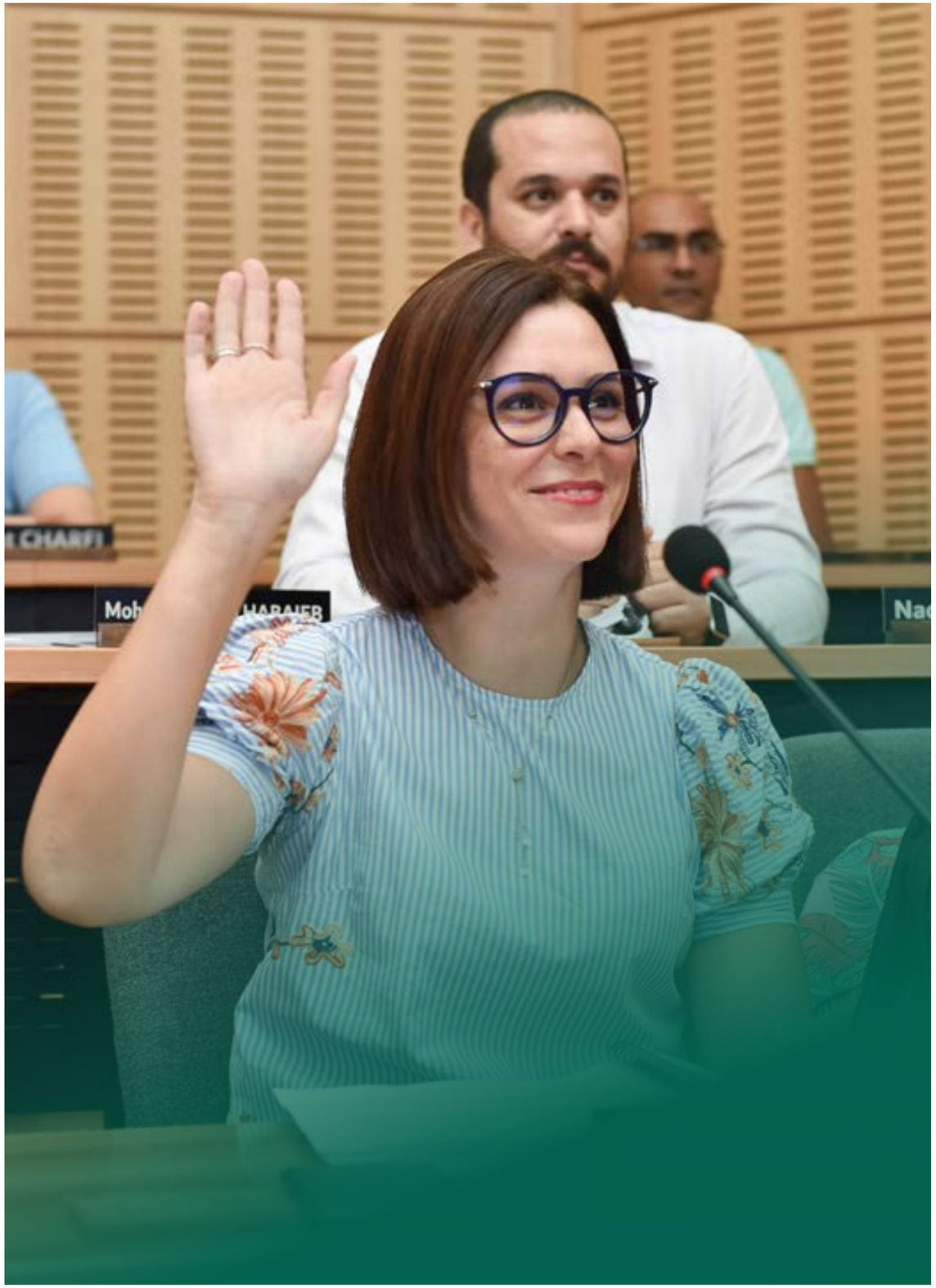
The program is aimed at experienced professionals who are expected to manage Digital Health and AI projects, including: Medical doctors, pharmacists, engineers, technicians, statisticians, computer scientist and health structures managers.

2.

Good English proficiency is required to enroll in the program. Applicants are interviewed to assess their motivation, potential and capacity to benefit from the program.

3.

Each class is composed of highly diversified participants (activity sector, age, gender, nationality, and educational background) to offer a unique learning experience and opportunities for networking.



Outline of the program

Term 01

HARMONIZATION PERIOD

For Engineers and participants without a biological background

INTRODUCTION TO PRINCIPLES OF MEDICINE AND HEALTHCARE SYSTEMS

Prepares engineers and non-medical students to understand the fundamentals of health care, to be able to communicate with health care professionals, and to become familiar with the health care jargon, environment as well as the healthcare system, and health economics.

For Health Professionals

ICT LITERACY AND MATH FUNDAMENTALS

Enables participants to become more comfortable with digital tools and simple quantitative methods depending on their needs. It Introduces numerical and computational tools necessary for problem solving skills in a digital environment.

MEDICAL SOFTWARE ENGINEERING AND AGILE METHODS

Introduces students to software development phases, stakeholder communication, and collaborative learning of best practices, emphasizing skills in addressing customer needs, using development tools, and incorporating non-technical aspects like project management and teamwork. The module offers practical application in healthcare software through simulated real-world projects.

INTRODUCTION TO DATA SCIENCE FOR HEALTH CARE

Establishes a statistical foundation for data science in healthcare, concentrating on key principles of data analysis and interpretation. With a specific focus on healthcare applications, students gain hands-on experience in statistical methods and visualization techniques. The emphasis is on utilizing statistical approaches to uncover insights and enhance decision-making within the healthcare domain.

DIGITAL PROJECT

Prepares future health digitalization leaders to work within a multidisciplinary team, to formulate project and to implement its functionalities with respect to the project requirements and deadlines.

Outline of the program

Term 02

DIGITAL HEALTH INFORMATION SYSTEM

Explores essential Information Systems (I.S.) concepts and their role in healthcare decision-making. It focuses on integrated healthcare solutions, project management skills, and addresses ethical, social, and security issues in Information Systems for healthcare. Participants gain insights into current I.S. trends relevant to the healthcare domain.

ADVANCED DATA ANALYTICS FOR HEALTHCARE

Prepares learners to be able to conduct a data analysis study in the field of healthcare, starting from defining a research question, gathering data, prepressing it, modelling and evaluating the quality of models. The course integrates hands-on experience with relevant tools and techniques, offering a comprehensive introduction to leveraging data science for insights and improvements in healthcare practices.

DIGITALIZATION MANAGEMENT

Combines Project Management and Change Management. Participants learn to plan and execute digital projects efficiently, exploring methodologies and collaboration tools. The Change Management component focuses on leading teams through digital transitions and fostering a transformation-ready culture. Together, these courses equip digital leaders to manage digital initiatives and navigate organizational change effectively.

HEALTH LAW & CSR

Explores the connection between legal frameworks, ethical considerations, and societal obligations in healthcare. Students examine key legal concepts, regulations, and the impact on patient care, privacy, and equitable access to healthcare. Through case studies, the course prepares students to navigate ethical challenges and understand their role in fulfilling social responsibilities within the healthcare system.

EFFECTIVE TECHNICAL COMMUNICATION

Develops participants' abilities in writing and presenting technical communication in a clear and professional manner. Likewise, participants will develop their ability to comprehend relevant technical communication, written and oral, within their fields.

Outline of the program

Term 03

COMPUTATIONAL EPIDEMIOLOGY AND SIMULATION

Equips students to proficiently study and develop computational techniques and tools. It focuses on modeling, simulating, predicting, forecasting, surveilling, mitigating, and visualizing the spread of diseases. Through this program, students will gain the skills necessary to contribute effectively to the field of epidemiology by leveraging computational methods for a comprehensive understanding and management of disease dynamics.

SENSING TECHNOLOGY FOR DIAGNOSTICS AND MONITORING

Provides a concise yet comprehensive overview of contemporary healthcare solutions including cutting-edge diagnostic tools, real-time monitoring, and the seamless integration of sensors into everyday environments. The module emphasizes cloud technology for efficient data storage and processing, enabling advanced analysis. Telemedicine concepts are included, highlighting the role of technology in remote diagnostics.

MEDICAL INFORMATION PROCESSING

Focuses on the crucial role of signal and image processing in healthcare. Students delve into advanced techniques for extracting meaningful information from medical signals and images. The course covers applications such as medical imaging, signal analysis for diagnostics, and the enhancement of medical data through processing methodologies.

INTELLIGENT SYSTEMS FOR HEALTHCARE

Equips students to proficiently apply specific mathematical techniques to solve problems in biomedical signals. Through hands-on applications and case studies, students gain a practical understanding of how AI and machine learning contribute to enhancing medical information processing in diverse healthcare settings while being aware of their limitations.

RESEARCH METHODS

Develops students' knowledge and understanding of the role and conduct of quantitative and qualitative research methods in healthcare. Through this module, students acquire necessary skills and practices to critically evaluate research and apply robust methods to address healthcare challenges.

Outline of the program

Term 04

FINAL PROJECT

Through immersive capstone projects, participants develop a hands-on understanding of how AI and machine learning methodologies can significantly elevate medical information processing across various facets of digital health. This exploration is enriched by an awareness of the nuanced limitations inherent in these advanced technologies, fostering a comprehensive and practical approach to their application in real-world healthcare scenarios.

South
Mediterranean
University

MSB . MedTech . LCI

dorra.louati@medtech.tn
Campus SMU : Les jardins du Lac 2, Tunis
(+216) 23 999 123
www.smu.tn

MedTech
Mediterranean
Institute of Technology

EXECUTIVE MASTER

BIM & ERP MANAGEMENT

• WWW.MEDTECH.TN •

Welcome

President's message

The strategic location of Tunisia in the heart of the Mediterranean combined with the diversity of its cultural heritage constitute major assets for the development of a regional hub of educational excellence.
It is in this framework that we have developed the South Mediterranean University (SMU).
On behalf of all members of our management team, we want to make your education at SMU a life changing experience and wish you success in your drive for professional excellence.

Mahmoud TRIKI,
Founder & President, SMU

Shape your **future** at MedTech

Our vision

MedTech aspires to be a regional hub of excellence in engineering education by fostering innovative learning and societal impact.

Our mission

MedTech is committed to train highly qualified engineers capable of contributing and leading innovative ventures in today's globalized world.

Our values

- Diversity
- Integrity
- Care
- Excellence
- Creativity

Major Achievements

- Internationally accredited Engineering programs by ABET
- Partnerships with top ranked universities (University of Michigan, HEC Montréal, Oakland University, etc.)
- State-of-the-art facilities

Our **learning strategy**

MedTech implements an adaptive learning strategy that offers students a life changing experience.

Digital

MedTech is facilitated with technology, information and instructions that are enhanced using various applications, tools and resources to improve the learning experience.

Active

Our active pedagogy allows our students to be continuously involved in the learning process through individual and group activities, bootcamps, simulation games enabling them to develop a variety of skill sets that differentiate our graduates on the job market.

Interdisciplinary

By combining our curricular objectives to different disciplines, we help our students acquire the knowledge and skills necessary for their personal and professional development.

The **Executive Master in BIM & ERP Management** at a glance

The Building Information Modeling (BIM) and Enterprise Resource Planning (ERP) methodologies have revolutionized the Architecture, Engineering, Construction, and Operation (AECO) industry. Yet there is a shortage of highly qualified practitioners to manage BIM projects. The Executive Master in BIM & ERP Management allows participants to acquire a high level of know-how in the management of processes, equipment, and workflows involved in the construction sector, throughout the entire lifecycle of a building project, from the planning and design phase, to procurement, construction and maintenance stage.

The Program

The objective of the program is to train professionals from the AECO industry, and equip them with the necessary tools and competencies for management roles in BIM projects.

The program consists of modules and workshops aiming at :

- Providing the knowledge and skills of how BIM and ERP methodologies can be applied across a construction/ infrastructure project from conception to demolition.
- Developing critical thinking, leadership, and decision-making skills, and the ability to apprehend strategic decisions dealing with both the technical administration and the execution of a project.
- Developing communication and collaboration skills.

The Format

The Executive Master in BIM & ERP Management is a part-time program, designed to tailor the work and life commitments of participants. Classes meet four days a month (Thursday through Sunday from 9:00 AM to 6:00 PM) over a 17-month period, followed by three additional months dedicated to the final project.

Program at a glance

MESRS

Duration	Courses	Final project
20 months	**13**	**1**

Workshops	Course per month
5	**1**

The program key **differential values**

- **Strong methodological approach** facilitated with digital tools to achieve efficient coordination of processes, workflows, people, assets and technology that BIM requires within the AECO sector.
- **openBIM collaborative process** as a sustainable information management approach of the building assets based on open standards and cloud workflows.
- **Tailored learning pathways** to meet the needs of professionals from different sectors of the AECO industry, such as architects, engineers, builders, developers, financiers, asset managers, and facilities managers.

Participant **profiles**

1.

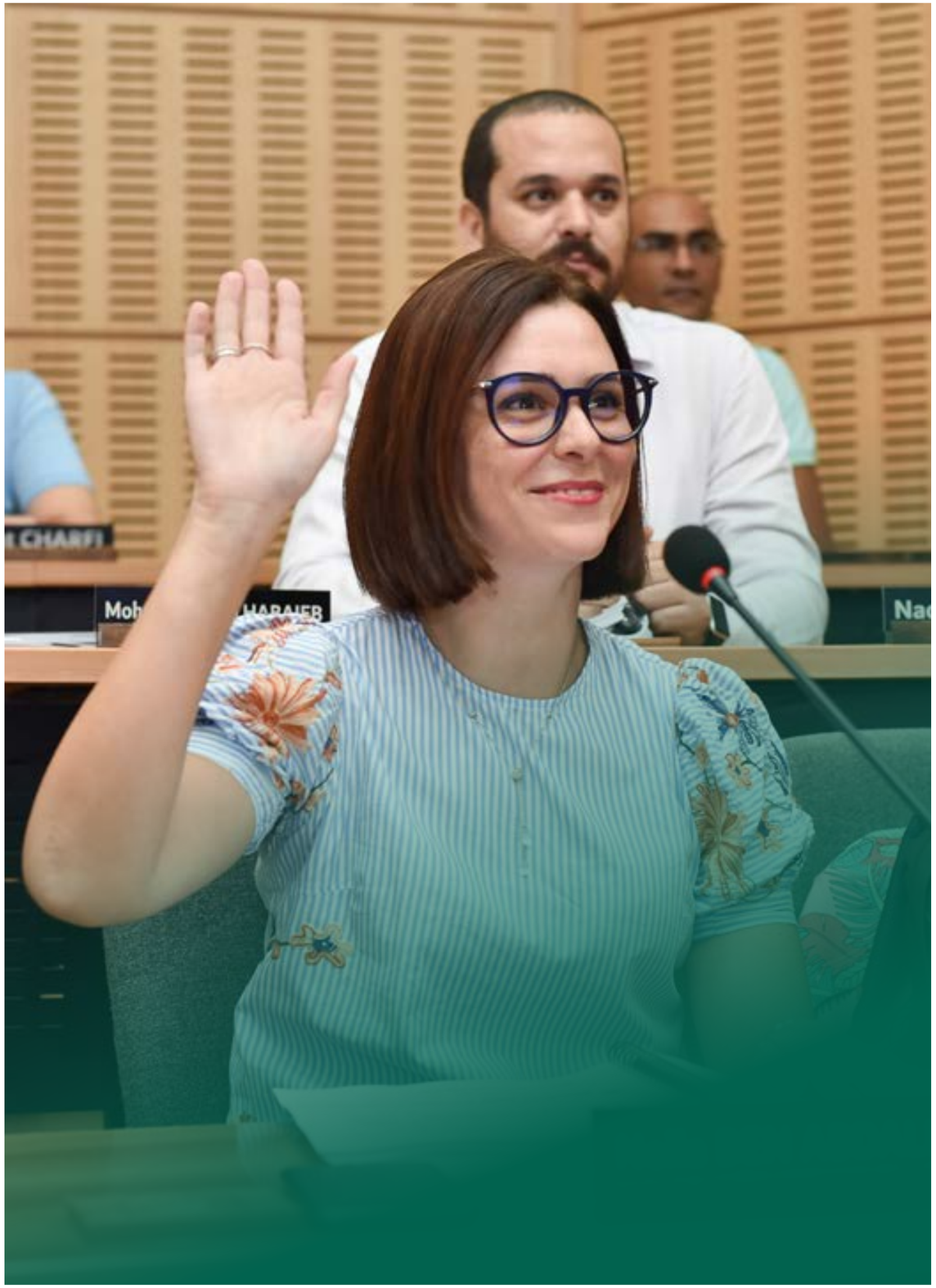
The program is aimed at experienced professionals from the AECO industry who are expected to manage BIM projects, including: architects, engineers, technicians, sub/contractors, manufacturers, and facilities and operations managers.

2.

Good English proficiency is required to enroll in the program. Applicants are interviewed to assess their motivation, potential and capacity to benefit from the program.

3.

Each class is composed of highly diversified participants (activity sector, age, gender, nationality, and educational background) to offer a unique learning experience and opportunities for networking.



Outline of the program

Term 01

BIM FUNDAMENTALS AND INFORMATION MANAGEMENT

Introduces participants to the basic concepts of BIM and the different information requirements based on the application of protocols and standards for control, feedback and analysis. These standards and protocols are developed at organizational, sector and project level and represent what stakeholders aim to achieve in the BIM project.

OPENBIM AND COLLABORATION PRACTICE

Introduces the Open BIM environment and the main steps of a full BIM workflow. Participants learn how to model, manage documentation and information inside the model, exchange BIM data between different software tools using open data standards, and recognize the importance of collaborative working between different disciplines.

AUTHORING IN DESIGN WITH AUTODESK REVIT

Provides a training for the design and integrated management of BIM models using Autodesk REVIT as an authoring modeling tool for architecture, structures, and mechanical electrical plumbing (MEP).

COORDINATION, COMMUNICATION & INTEROPERABILITY

Covers methodologies related to interoperability and the best practices for coordination and cloud-based communication within a BIM environment. It follows a working methodology based on learning-by-doing through practical case studies, teamwork assignments, and a real project to be carried out at the end of the training.

PROJECT MANAGEMENT

Provides a comprehensive view of Lean principles and tools, and how they can be applied to Project Management. The course includes Agile, Scrum, Critical Chain and Change Management methods, among other concepts, structured into sessions that are focused on a specific theme or methodology, using exercises, real-life case studies and simulations.

DIGITAL LITERACY

Enables participants to become more comfortable with digital tools and simple quantitative methods depending on their needs. Topics covered include data structure, digital workspaces, libraries and research tools, times series, variability, correlation, and simple and multiple regression models. The emphasis throughout the course is on concepts and reasoning, rather than technical details.

Outline of the program

Term 02

CORPORATE COMMUNICATION

Develops participants' abilities in writing and presenting technical communication in a clear and professional manner. Likewise, participants will develop their ability to comprehend relevant technical communication, written and oral, within their fields.

INFORMATION EXCHANGES THROUGH IFC

Highlights how the exchange of BIM content between different software programs is enabled with Industry Foundation Classes (IFC)-based model files, allowing for a better collaboration between different teams working on a BIM project throughout the entire project's lifecycle.

PRECONSTRUCTION, HANDOVER & 4D/5D STRATEGIES

Present the different aspects of preconstruction and handover using REVIT, including modeling, extraction of bills of quantities (BOQ), commissioning using BIM objects ID, delivery of as built model, and comparison of as built model with executed works. Emphasis is also placed on how to explore the pre-constructed models for interface management, extraction of quantities (5D), and planning management (4D) and synchronization.

PROJECTS TAKEOFF, PLANNING & BUDGET CONTROL

Provides participants with a foundational understanding of the importance of the 4D and 5D in the Construction Industry. Participants learn the process of preparing a strategic plan for the project, including creating a design, securing permits or entitlements, and gathering the labor and resources required for construction.

BIM QUALITY MANAGEMENT

Focuses on the effective use of the BIM Inspection Testing Plan and quality control workflow on a construction project across the project lifecycle. Topics include quality management processes, issue management, and clash detection.

GENERATIVE & PARAMETRIC DESIGN

Introduces the different aspects of Generative Design Using DYNAMO & GRASSHOPER, with a focus on parametric design, data extraction and classification from BIM model, workflow automation, and modelling of irregular shapes.

Outline of the program

Term 03

STANDARDS FOR ASSET MANAGEMENT

Provides insights on how to manage the progressive information flows, using different open standards throughout the project life cycle, and highlights the best practice for the integration of BIM into asset management processes.

COBIE EXCHANGE PROTOCOLS

Introduces the Construction Operations Building Information Exchange, known as COBie, which is a developing standard for the exchange of data to support facility management by owners and operators.

INTEGRATED BUSINESS PROCESSES

Highlights how the AEC processes can be integrated to the business process within a centralized and unique database to create a single source of information throughout the entire project's lifecycle, and provides a training on core business processes embedded in SAP S/4HANA.

ETHICS & CORPORATE SOCIAL RESPONSIBILITY

Covers the ethical and social issues related to the development and use of technology. It covers topics in ethical theory, and social, political, and legal considerations of modern technology systems and applications.

INTEGRATED PROJECT DELIVERY

Focuses on a project delivery approach that integrates people, systems, business structures and practices into a process that collaboratively harnesses the resources to optimize the project outcomes and make buildings more sustainable.

BIM IMPLEMENTATION PLAN

Explores the process for creating and managing information on a construction project across the project lifecycle, including the BIM Execution Plan (BEP) in different international contexts.

Outline of the program

Term 04

FINAL PROJECT

The final project is a real project simulation-based module integrating courses included in the program to be developed using openBIM approach. This allows the participants to make use of all the knowledge gained throughout the program and enables them to work collaboratively, with a client-oriented approach using different technologies and standardized methodologies, globally used.

Faculty

DAVID DELGADO VENDRELL

David Delgado Vendrell is architect, entrepreneur at DDV.cat and AECO consultant, specialized in openBIM and Agile frameworks. He is the Technical Coordinator and board member of buildingSMART Spain and an active member of the BIM User Group of Catalonia (GuBIMCat). He also collaborates with the “We Build the Future” Commission of ITEC in Catalonia, representing buildingSMART Spanish Chapter. He has co-authored the BIM classification system “GuBIMclass,” an initiative of GuBIMCat and Infraestructures de Catalunya.

DR. BILAL SUCCAR

Dr. Bilal Succar is a strategic advisor and independent researcher focusing on digital performance assessment and improvement in the Built Environment. He is the director of ChangeAgents AEC (ChangeAgents.com.au), a digital transformation consultancy operating out of Melbourne, Australia. Dr. Succar is the Founder of the not-for-profit BIMe Initiative (BIMexcellence.org), a community of 160+ researchers from 42 countries, and the Head Editor of the international BIM Dictionary (BIMdictionary.com) covering 27 languages (including Spanish). Bilal published highly cited academic journals, led prominent BIM education initiatives, and delivered keynote addresses and workshops across the world covering digital transformation and macro-BIM adoption. Dr. Succar’s stated mission is to encourage continuous performance improvement, international collaboration, and open knowledge sharing.

DR. KARAMA JERIBI

Dr. Karama Jeribi is an Assistant Professor at MedTech with over 10 years of experience teaching and researching in the field of Industrial Engineering. With a PhD in Optimization of Logistic Systems from Ecole Centrale de Lille, she is a certified Supply Chain expert and Green Belt Lean Six Sigma. Her expertise lies in continuous improvement, lean manufacturing, and management, supply chain and logistics. She has worked on numerous industrial projects in several fields. Her passion for teaching and commitment to excellence has earned her recognition from both students and colleagues.

PROF. DR. ZOUBEIR LAFHAJ

Prof. Dr. Zoubeir LAFHAJ is a Full Professor at Centrale Lille, France. He is holder of the “Construction 4.0” chair, an industrial research chair that deals with the challenges of odernizing the construction industry in France and Europe. Prof. Dr. Zoubeir LAFHAJ’s industrial research expertise focuses on (i) additive manufacturing (3D printing) for construction, industrialization and robotization of construction, (ii) applications of AI, blockchain and BIM in construction and finally (iii) value, productivity, quality, lean construction, logistics, and collaboration with all stakeholders in the construction industry.

DR. ONS NAJJAR

Dr. Ons Najjar is an architect, urban designer, BIM manager and academic researcher, with an international experience as a lecturer in the Middle East and Tunisia. Her industrial and research expertise focuses on the importance of digitalization on architecture, encouraged by creativity, innovation and Green Concepts. She is also responsible for developing a strategy for the digital Building concept for sustainable design and management.

DR. NÉJIB CHENNOUFI

Dr Néjib Chennoufi is associate professor of engineering at MedTech. He is dedicated to success with solid multi-disciplinary engineering background with proven managerial experience and abilities. Expert and certified in Agile methods and project management, he has led several teams and projects within a number of international fortune 500 companies for over 12 years. He has worked within the oil & gas context, developing analytical and numerical physics-based models and software solutions. Dr. Chennoufi has led successfully the efforts to obtain the ABET accreditation for the ongoing three engineering programs in MedTech.

DR. AIDA SIALA

Dr. Aida Siala is an Architect, Doctor of architectural sciences, BIM consultant and experienced educator in teaching BIM. She’s qualified as Lecturer of the Nationals Schools of Architecture in France and Certified Autodesk Instructor and associated researcher at the MAP-CRIA laboratory. Her research work focuses on digital design with great involvement in themes aiming to develop current BIM practices, through new approaches allowing models verification, optimization and control. Aida is passionate about helping students develop their skills in BIM and preparing them for successful careers in this field.

PATRICIA CERESANI

Patricia Ceresani joined SMU in 2014 and is the Director of the Language and Culture Institute. She is responsible for the Business English and Soft Skills programs for executive training, the Study Abroad Program, and the Communication department at MSB. Patricia has a BA in Modern Languages and a BA in Humanities and Social Sciences. She has a consolidated 30 years of experience in the field of teaching English, Business Communication, and Public Speaking for both the higher education and the corporate sectors. Patricia has worked in many countries worldwide and with several multinationals in Tunisia.

South
Mediterranean
University

MSB . MedTech . LCI

leila.costelle@medtech.tn
Campus SMU : Les jardins du Lac 2, Tunis
(+216) 20 428 665
www.smu.tn

MedTech Programs

MedTech Mediterranean Institute of Technology

Engineering Accreditation Commission

Certified Ethical Hacking

EC-COUNCIL | ACADEMIA PARTNER

I. Program overview & Benefit:

The Certified Ethical Hacker (C|EH) v12 program is a comprehensive certification designed to impart the latest ethical hacking skills and knowledge. Over the past 20 years, it has become a benchmark for cybersecurity expertise, equipping professionals to protect and secure IT infrastructures. This program combines theoretical learning with practical labs, offering a deep dive into ethical hacking phases like Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Covering Tracks.

Participants will benefit from hands-on experience with over 220 labs, access to 3500+ hacking tools, and preparation for real-world ethical hacking scenarios. The curriculum covers 20 refreshed modules, including the latest in MITRE ATTACK Framework, intrusion analysis, and cloud computing, ensuring learners are up-to-date with current cybersecurity challenges.

The C|EH v12 not only prepares you for the certification exam but also equips you with the skills necessary for various cybersecurity roles. It's recognized globally, enhancing career prospects and professional credibility. Through this program, learners can master ethical hacking techniques beyond the certification, engaging in continuous learning and global hacking competitions.

This structured approach to ethical hacking education ensures that participants are well-prepared to identify and tackle vulnerabilities, making it an essential certification for anyone looking to advance in the cybersecurity field.

II. Intended Participants:

The Certified Ethical Hacker (C|EH) v12 program is tailored for a diverse range of professionals involved in the cybersecurity domain. Intended participants include:

- Mid-Level Information Security Auditors
- Cybersecurity Auditors
- Security Administrators
- IT Security Administrators
- Cyber Defense Analysts
- Vulnerability Assessment Analysts
- SOC Security Analysts
- Warning Analysts
- Information Security Analysts
- Security Analysts
- Infosec Security Administrators
- Cybersecurity Analysts
- Network Security Engineers
- Network Engineers
- Senior Security Consultants
- Information Security Managers
- Senior SOC Analysts
- Solution Architects
- Cybersecurity Consultants

This program is designed for those already in the cybersecurity field looking to enhance their skills and knowledge in ethical hacking, as well as individuals seeking to enter the field with a comprehensive understanding of how to protect and secure IT infrastructures against potential threats.

III. Program Curriculum

The Certified Ethical Hacker (C|EH) v12 offers a blend of theoretical knowledge and practical labs across 20 modules, covering essential cybersecurity and ethical hacking topics. Participants engage in hands-on experiences in a state-of-the-art cyber range, mastering skills from system hacking to cloud computing and IoT hacking. This curriculum is designed to equip learners with in-demand cybersecurity capabilities, culminating in a globally recognized certification.

IV. Core program curriculum:

includes a comprehensive set of 20 refreshed modules, designed to cover the essentials of ethical hacking and cybersecurity. Here's a brief overview of the modules:

1. **Introduction to Ethical Hacking:** Fundamentals of ethical hacking, information security controls, laws, and standards.
2. **Footprinting and Reconnaissance:** Techniques and tools for footprinting and reconnaissance.
3. **Scanning Networks:** Network scanning techniques and countermeasures.
4. **Enumeration:** Enumeration techniques and countermeasures.
5. **Vulnerability Analysis:** Identifying security loopholes in networks, communication infrastructure, and end systems.
6. **System Hacking:** System hacking methodologies to discover vulnerabilities.
7. **Malware Threats:** Types of malware, malware analysis procedures, and countermeasures.
8. **Sniffing:** Packet sniffing techniques and countermeasures.
9. **Social Engineering:** Concepts, techniques, and countermeasures.
10. **Denial-of-Service:** DoS and DDoS attack techniques and tools.
11. **Session Hijacking:** Techniques, tools, and countermeasures.
11. **Evading IDS, Firewalls, and Honeypots:** Evasion techniques and countermeasures.
12. **Hacking Web Servers:** Attack methodologies and countermeasures.
14. **Hacking Web Applications:** Web application hacking methodologies and countermeasures.
15. **SQL Injection:** Attack techniques, evasion techniques, and countermeasures.
16. **Hacking Wireless Networks:** Wireless technologies, encryption threats, and countermeasures.
17. **Hacking Mobile Platforms:** Mobile platform attack vectors, security guidelines, and tools.
18. **IoT Hacking:** IoT and OT attacks, methodology, and countermeasures.
19. **Cloud Computing:** Cloud computing threats, attacks, security techniques, and tools.
20. **Cryptography:** Cryptographic techniques and their application in cybersecurity.

This curriculum is designed to provide participants with the knowledge and hands-on experience necessary to identify and exploit vulnerabilities in various systems and networks, making it an essential program for anyone looking to advance their career in cybersecurity.

V. Schedule:

The certificate program entails a commitment of 40 hours, with sessions lasting 4 hours each week. Candidates have the flexibility to select their preferred schedule from the following options:

Evening classes
From 6:30 PM to 8:30 PM
Monday and Tuesday or Thursday and Friday

Weekend classes
From 10:00 AM to 12:00 PM:
Saturday and Sunday

VI. Enrollment requirements:

Enrollment requirements are straightforward: there are no specific prerequisites. However, participants are expected to have a basic understanding of networking, operating systems, and coding principles.

VII. The Benefits of the program:

- **Career Advancement:** A majority report promotions post-certification.
- **Skill Enhancement:** 97% affirm the program's effectiveness in safeguarding organizations.
- **Practical Learning:** Labs mimic real-world cyber threats, enhancing practical skills.
- **Professional Recognition:** Highly valued by hiring managers for ethical hacking roles.
- **Confidence Boost:** Increases self-confidence in cybersecurity abilities.
- **Comprehensive Coverage:** Considered the most thorough ethical hacking program.
- **Community Contribution:** Enables participants to contribute effectively to the cybersecurity community.
- **Career Launchpad:** Often the starting point for many in their cybersecurity careers.

The C|EH v12 program not only equips participants with the latest ethical hacking techniques and knowledge but also significantly enhances their career prospects, professional recognition, and confidence in cybersecurity roles.

Contacts :

cybersecuritycontact@medtech.tn
Les jardins du LAC 2, 1053, Tunis - Tunisie

MedTech Programs

MedTech Mediterranean Institute of Technology

Certified Network Defender

EC-COUNCIL | ACADEMIA PARTNER

I. Program overview & Benefit:

In the evolving landscape of cybersecurity, the Certified Network Defender (CND) v2 program stands as a cornerstone for professionals aiming to master network defense in a post-pandemic world. This program, designed to address the challenges of remote work and expanded digital perimeters, equips participants with the skills necessary to protect, detect, respond to, and predict cybersecurity threats. By integrating the latest tools, technologies, and strategies, the CND v2 ensures that learners are prepared for the dynamic challenges of securing modern networks.

Key features of the program include a hands-on learning approach, covering essential topics such as network defense management, endpoint protection, and threat prediction. It is tailored for professionals in network administration and cybersecurity roles, aiming to enhance their capabilities in a comprehensive manner. Participants benefit from an immersive learning experience, guided by the latest industry practices and the NICE 2.0 Framework.

The CND v2 is more than just a training program; it is a pathway to becoming a proficient network defender capable of navigating the complexities of cybersecurity in today's interconnected world.

II. Intended Participants:

The intended participants for the Certified Network Defender (CND) v2 program are individuals working in the network administration/cybersecurity domain. This includes roles such as:

- Network Administrators/Engineers Network Security
- Administrators/Engineers/Analysts
- Cybersecurity Engineers
- Security Analysts
- Network Defense Technicians
- Security Operators

The program is designed for all cybersecurity operations roles, and anyone looking to build or advance their career in cybersecurity.

III. Program Curriculum

The Certified Network Defender (CND) v2 program curriculum is structured to provide a comprehensive understanding of network defense, covering a wide range of topics essential for cybersecurity professionals and, is designed to equip participants with the skills needed to protect, detect, respond to, and predict cybersecurity threats in a dynamic and evolving digital landscape. With a focus on hands-on learning, the program ensures that participants gain practical experience through EC-Council labs, covering a variety of domains crucial for effective network defense.

IV. Core program curriculum:

includes a comprehensive set of 20 refreshed modules, designed to cover the essentials of network defense. Here's a brief overview of the modules:

1. **Network Attacks and Defense Strategies:** Exploration of various network attacks and the strategies to defend against them, ensuring a strong foundation in network defense mechanisms.
2. **Administrative Network Security:** Focuses on the establishment of network security policies and procedures to manage and secure an organization's information.
3. **Technical Network Security:** Delve into the technical aspects of securing a network, including the implementation of security measures and technologies.
4. **Network Perimeter Security:** Techniques and tools for securing the network perimeter against unauthorized access and attacks.
5. **Endpoint Security-Windows Systems:** Specific strategies for securing Windows-based systems from vulnerabilities and threats.
6. **Endpoint Security-Linux Systems:** Tailored security measures for Linux systems, addressing the unique challenges they face.
7. **Endpoint Security- Mobile Devices:** Covers the security of mobile devices, emphasizing the growing need for protection in a mobile-first world.
8. **Endpoint Security-IoT Devices:** Focuses on the security concerns associated with IoT devices and strategies to mitigate them.
9. **Administrative Application Security:** Strategies for securing applications from an administrative perspective, ensuring application integrity.
10. **Data Security:** Methods and techniques for ensuring the confidentiality, integrity, and availability of data.
11. **Enterprise Virtual Network Security:** Security measures for virtual networks, critical in today's cloud-driven environment.
11. **Enterprise Cloud Network Security:** Focuses on securing cloud environments, addressing the unique challenges posed by cloud computing.
12. **Enterprise Wireless Network Security:** Strategies for securing wireless networks, an essential component of modern network infrastructures.
14. **Network Traffic Monitoring and Analysis:** Techniques for monitoring and analyzing network traffic to detect and respond to potential threats.
15. **Network Logs Monitoring and Analysis:** Utilizing log data for the detection and analysis of security incidents and trends.
16. **Incident Response and Forensic Investigation:** Procedures and techniques for responding to cybersecurity incidents and conducting forensic investigations.
17. **Business Continuity and Disaster Recovery:** Planning and implementing strategies to ensure business continuity and effective disaster recovery.
18. **Risk Anticipation with Risk Management:** Identifying and managing risks to minimize their impact on the organization.
19. **Threat Assessment with Attack Surface Analysis:** Techniques for assessing threats by analyzing the attack surface of an organization.
20. **Threat Prediction with Cyber Threat Intelligence:** Utilizing cyber threat intelligence to predict and prepare for potential future threats.

This detailed curriculum is designed to provide participants with a robust understanding of network defense principles, strategies, and practical applications, equipping them with the skills needed to protect, detect, respond to, and predict cybersecurity threats effectively.

V. Schedule:

The certificate program entails a commitment of 40 hours, with sessions lasting 4 hours each week. Candidates have the flexibility to select their preferred schedule from the following options:

Evening classes

From 6:30 PM to 8:30 PM

Monday and Tuesday or Thursday and Friday

Weekend classes

From 10:00 AM to 12:00 PM:

Saturday and Sunday

VI. Enrollment requirements:

Enrollment requirements are straightforward: there are no specific prerequisites. However, participants are expected to have a basic understanding of networking, operating systems, and coding principles.

VII. The Benefits of the program:

- **Comprehensive Skills:** Incorporates Protect, Detect, Respond, and Predict for network security.
- **NICE 2.0 Alignment:** Ensures skills meet industry standards.
- **Current Tools and Techniques:** Offers knowledge on the latest in cybersecurity.
- **Practical Learning:** Focuses on hands-on training for real-world application.
- **Strategic Preparedness:** Emphasizes on anticipating threats and ensuring business continuity.

These benefits make the CND v2 program a must-have for individuals and organizations aiming to equip themselves with the best possible defense against network breaches, emphasizing practical skills and up-to-date knowledge in network security.

Contacts :

cybersecuritycontact@medtech.tn
Les jardins du LAC 2, 1053, Tunis - Tunisie

MedTech Programs

MedTech Mediterranean Institute of Technology

Engineering Accreditation Commission

EC-COUNCIL | ACADEMIA PARTNER

Computer Hacking Forensic Invistigator

I. Program overview & Benefit:

The EC-Council's CHFI v10 (Computer Hacking Forensic Investigator version 10) is a cutting-edge program tailored for individuals keen on leading the digital forensics movement. Amid the rapid digital transformation and the escalating risk of cyberattacks, this program emerges as a critical solution for mastering digital forensics. CHFI v10 meticulously guides participants through the entire digital forensics process, from uncovering digital footprints left by cyber breaches to legally countering the perpetrators.

Structured with a blend of theory and practical sessions, the program is ideal for professionals aiming to excel as forensic analysts, cybercrime investigators, incident responders, IT auditors, among others. It boasts of an ANSI 17024 accreditation, aligning with the NICE 2.0 framework and recognized by the DoD under Directive 8570, ensuring its relevance and applicability in the real world.

Participants will delve into specialized modules like Dark Web and IoT Forensics, engage with over 50GB of crafted evidence files for hands-on investigation, and learn the latest in Malware Forensics, including handling contemporary malware threats like Emotet and EternalBlue. Furthermore, the curriculum covers forensic methodologies for cloud infrastructure, including Amazon AWS and Microsoft Azure, preparing students for challenges in today's cloud-centric operational environments.

CHFI v10 is not just a program but a gateway to becoming an indispensable part of the cybersecurity landscape, endorsed by top practitioners and trusted across the Fortune 500 companies globally.

II. Intended Participants:

The intended participants for the EC-Council's CHFI v10 (Computer Hacking Forensic Investigator version 10) program are professionals and aspiring professionals in various cybersecurity and digital forensics roles. This includes:

- Forensic analysts
- Cybercrime investigators
- Cyber defense analysts
- Incident responders
- Information technology auditors
- Malware analysts
- Security consultants
- Chief security officers

The program is engineered for individuals looking to deepen their expertise in digital forensics, aiming to address the growing need for skilled professionals capable of identifying, responding to, and investigating cyber breaches and cybercrimes.

III. Program Curriculum

The CHFI v10 program from EC-Council offers an in-depth journey into the world of digital forensics, tailored to the contemporary digital landscape. This comprehensive curriculum is designed to equip participants with the essential skills and knowledge required for excellence in digital forensics. Participants will engage in practical and theoretical learning, covering the critical aspects of digital forensics analysis and evaluation. From identifying digital footprints to collecting evidence for legal prosecution, the program walks students through every step of the forensic process with experiential learning. Crafted by industry veterans, this program is ideal for professionals aiming to navigate the complexities of cyber breaches and cybercrimes effectively.

IV. Core program curriculum:

The CHFI v10 curriculum includes a comprehensive set of 16 refreshed modules, designed to equip participants with advanced skills and knowledge in digital forensics. Here's a brief overview of the modules:

1. **Computer Forensics in Today's World:** An introduction to the field of digital forensics, highlighting its importance in the modern digital age.
2. **Computer Forensics Investigation Process:** Detailed processes involved in conducting forensic investigations from start to finish.
3. **Understanding Hard Disks and File Systems:** Fundamental knowledge of how data is stored and managed on digital devices.
4. **Data Acquisition and Duplication:** Techniques for securely collecting and duplicating data for analysis without tampering.
5. **Defeating Anti-Forensics Techniques:** Strategies to counteract methods used to obstruct forensic investigations.
6. **Windows Forensics:** Specialized techniques for investigating Windows operating systems.
7. **Linux and Mac Forensics:** Approaches for forensic investigations on Linux and Mac OS systems.
8. **Network Forensics:** Methods for analyzing network-related activities and uncovering digital evidence.
9. **Investigating Web Attacks:** Techniques for investigating attacks targeted at web applications and services.
10. **Dark Web Forensics:** Understanding and investigating activities on the dark web.
11. **Database Forensics:** Approaches for examining databases to extract and analyze evidence.
11. **Cloud Forensics:** Techniques for forensic investigations in cloud computing environments.
12. **Investigating Email Crimes:** Methods for analyzing emails to uncover evidence of crimes.
14. **Malware Forensics:** Techniques for analyzing and investigating malware.
15. **Mobile Forensics:** Strategies for extracting and analyzing data from mobile devices.
16. **IoT Forensics:** Approaches to investigate Internet of Things devices and gather digital evidence.

This curriculum is crafted to provide a thorough understanding of digital forensics, encompassing a wide range of topics essential for forensic analysts, cybercrime investigators, incident responders, and other cybersecurity professionals.

V. Schedule:

The certificate program entails a commitment of 40 hours, with sessions lasting 4 hours each week. Candidates have the flexibility to select their preferred schedule from the following options:

Evening classes

From 6:30 PM to 8:30 PM

Monday and Tuesday or Thursday and Friday

Weekend classes

From 10:00 AM to 12:00 PM:

Saturday and Sunday

VI. Enrollment requirements:

Enrollment requirements are straightforward: there are no specific prerequisites. However, participants are expected to have a basic understanding of networking, operating systems, and coding principles.

VII. The Benefits of the program:

- **Globally Recognized Certification:** ANSI 17024 accreditation and recognition by the DoD under Directive 8570.
- **Comprehensive Coverage:** Includes critical areas like Dark Web and IoT Forensics, and extensive labs in Malware Forensics.
- **Up-to-Date Content:** Massive updates across all modules to cover the latest forensic methodologies, especially for public cloud infrastructures like Amazon AWS and Microsoft Azure.
- **Practical Learning:** More than 50GB of evidence files for investigation purposes and exposure to the latest forensic tools including Splunk and DNSQuerySniffer.
- **Advanced Techniques:** In-depth focus on volatile and non-volatile data acquisition and examination, along with new techniques for defeating anti-forensic measures.
- **Industry Acceptance:** Trusted by cybersecurity practitioners across Fortune 500 companies globally.

These benefits collectively make the CHFI v10 program a valuable and comprehensive learning path for individuals aiming to excel in the field of digital forensics, offering the knowledge, skills, and credentials needed to advance in their careers.

Contacts :

cybersecuritycontact@medtech.tn
Les jardins du LAC 2, 1053, Tunis - Tunisie

MedTech Programs

MedTech Mediterranean Institute of Technology

Digital Forensics Essentials

EC-COUNCIL | ACADEMIA PARTNER

I. Program overview & Benefit:

Digital Forensics Essentials (DFE) is an essential course designed for individuals aiming to enhance their competency and expertise in digital forensics and information security. This comprehensive program introduces participants to the fundamentals of computer forensics, the computer forensics investigation process, and specialized areas such as Dark Web, Windows, Linux, and Malware forensics. The course incorporates interactive labs to ensure practical, hands-on experience, crucial for a successful career in digital forensics. Certification in DFE offers formal recognition of a learner's expertise and skills, significantly improving their employment prospects, opportunities for higher salaries, and job satisfaction.

II. Intended Participants:

This program is tailored for individuals seeking to start or advance their careers in digital forensics and information security. It is ideally suited for:

- Cybersecurity Technician
- IT Specialist
- Systems Specialist
- Computer support Specialist
- Network Technician
- And more

III. Program Curriculum

The curriculum focuses on imparting practical skills and knowledge in digital forensics, and is divided into 12 modules covering different aspects of the field:

1. Computer Forensic Fundamentals
2. Computer Forensic Investigation Process
3. Understanding Hard Disks and File Systems
4. Data Acquisition and Duplication
5. Defeating Anti-Forensic Techniques
6. Windows Forensics
6. Linux and Mac Forensics
7. Network Forensics
8. Investigating Web Attacks
9. Dark Web Forensics
10. Investigating Email Crimes
11. Malware Forensics

IV. Schedule:

The certificate program entails a commitment of 12 hours, with sessions lasting 4 hours each week. Candidates have the flexibility to select their preferred schedule from the following options:

Evening classes

From 6:30 PM to 8:30 PM

Monday and Tuesday or Thursday and Friday

Weekend classes

From 10:00 AM to 12:00 PM:

Saturday and Sunday

V. Enrollment requirements:

Enrollment requirements are straightforward: there are no specific prerequisites. However, participants are expected to have a basic understanding of networking, operating systems, and coding principles.

VII. The Benefits of the program:

- Mastery of digital forensics fundamentals and advanced topics, preparing participants for real-world challenges
- Practical, hands-on experience through interactive labs
- Enhanced career prospects with formal certification recognition, leading to potential for advancement.
- Increased job satisfaction through elevated skills and expertise

This program ensures participants are well-equipped with the necessary skills and knowledge to excel in the field of digital forensics, offering a pathway to career advancement and professional development in the rapidly evolving domain of information security.

Contacts :

cybersecuritycontact@medtech.tn
Les jardins du LAC 2, 1053, Tunis - Tunisie

MedTech Programs

MedTech Mediterranean Institute of Technology

Engineering Accreditation Commission

Ethical Hacking Essentials

EC-COUNCIL | ACADEMIA PARTNER

I. Program overview & Benefit:

Ethical Hacking Essentials (EHE) is a foundational course designed to equip learners with the essential skills and knowledge required for a successful career in cybersecurity. This comprehensive program introduces participants to the core concepts of computer and network security, ethical hacking, and penetration testing. Covering a wide range of topics from threats and vulnerabilities, password cracking, and web application attacks, to IoT and OT attacks, cloud computing, and pentesting fundamentals, the course provides a broad understanding of the cybersecurity landscape. Through hands-on practical experience, learners gain valuable skills that prepare them for real-world challenges in the cybersecurity domain. Certification in Ethical Hacking Essentials offers formal recognition of expertise and skills, enhancing employment prospects, opportunities for advancement, higher salaries, and greater job satisfaction.

II. Intended Participants:

This program is ideal for individuals seeking to start or advance their careers in cybersecurity. It is suitable for:

- Help Desk Technician
- Technical Support Specialist
- Systems Specialist
- Computer support Specialist
- Network Technician

III. Program Curriculum

The curriculum focuses on imparting practical skills and knowledge in ethical hacking, and is divided into 12 modules, each focusing on a different aspect of cybersecurity:

1. **Information Security Fundamentals:** Introduction to the basics of information security.
2. **Ethical Hacking Fundamentals:** Overview of ethical hacking principles and practices.
3. **Information Security Threats and Vulnerability Assessment:** Identifying and assessing vulnerabilities and threats.
4. **Password Cracking Techniques and Countermeasures:** Methods of password cracking and how to defend against them.
5. **Social Engineering Techniques and Countermeasures:** Understanding social engineering and its prevention.
6. **Network Level Attacks and Countermeasures:** Strategies for defending against network-level attacks.
7. **Web Application Attacks and Countermeasures:** Addressing webserver exploitation and attacks like SQL injection.
8. **Wireless Attacks and Countermeasures:** Securing wireless networks against attacks.
9. **Mobile Attacks and Countermeasures:** Protecting mobile devices from security threats.
10. **IOT & OT Attacks and Countermeasures:** Safeguarding IoT and OT devices.
11. **Cloud Computing Threats and Countermeasures:** Managing cloud computing security risks.
12. **Penetration Testing Fundamentals:** Fundamentals of conducting penetration tests.

IV. Schedule:

The certificate program entails a commitment of 12 hours, with sessions lasting 4 hours each week. Candidates have the flexibility to select their preferred schedule from the following options:

Evening classes

From 6:30 PM to 8:30 PM

Monday and Tuesday or Thursday and Friday

Weekend classes

From 10:00 AM to 12:00 PM:

Saturday and Sunday

V. Enrollment requirements:

Enrollment requirements are straightforward: there are no specific prerequisites. However, participants are expected to have a basic understanding of networking, operating systems, and coding principles.

VI. The Benefits of the program:

- **A strong foundation in the principles and practices of ethical hacking and cybersecurity.**
- **Hands-on experience with the latest tools and techniques in the field.**
- **The ability to identify, assess, and mitigate various cybersecurity threats and vulnerabilities.**
- **Enhanced career opportunities in the fast-growing field of cybersecurity.**
- **Formal recognition through certification, aiding in job advancement and satisfaction.**

These benefits clearly illustrate the dual impact of the EHE program: it not only propels individuals forward in their cybersecurity careers but also plays a crucial role in strengthening the security of our digital environment. By equipping participants with fundamental understanding of ethical hacking,

Contacts :

cybersecuritycontact@medtech.tn
Les jardins du LAC 2, 1053, Tunis - Tunisie

MedTech Programs

MedTech Mediterranean Institute of Technology

Network Defense Essentials

EC-COUNCIL | ACADEMIA PARTNER

I. Program overview & Benefit:

The Network Defense Essentials (NDE) course is a comprehensive introduction to the fundamental concepts of information security and network defense. This course is tailored for individuals looking to embark on a career in cybersecurity, providing an essential foundation for entry-level information security or cybersecurity roles. It encompasses a wide array of topics including Identification, Authentication, Authorization, Virtualization, Cloud Computing, Wireless Networks, Mobile and IoT Devices, and Data Security. A significant component of the course is its interactive labs, which offer hands-on, practical experience necessary for a successful future in the cybersecurity field. By earning the NDE certification, individuals gain formal recognition of their competency and expertise in network defense and information security skills, enhancing their resume and employability.

II. Intended Participants:

This course is designed for individuals aspiring to start a career in cybersecurity. It is ideal for those with a basic understanding of IT networking and cybersecurity concepts.

- Local Area Network Specialist
- Network Security Analysts
- Network Technician
- Network Administrator
- Network Coordinator

III. Program Curriculum

The curriculum of the Network Defense Essentials course is meticulously structured to cover the breadth and depth of information security and network defense. It is divided into twelve modules, each focusing on a key aspect of cybersecurity:

1. **Network Security Fundamentals**
2. **Identification, Authentication, and Authorization**
3. **Network Security Controls: Administrative Controls**
4. **Network Security Controls: Physical Controls**
5. **Network Security Controls: Technical Controls**
6. **Virtualization and Cloud Computing**
7. **Wireless Network Security**
8. **Mobile Device Security**
9. **IoT Device Security**
10. **Cryptography and the Public Key Infrastructure**
11. **Data Security**
12. **Network Traffic Monitoring**

This detailed curriculum is designed to provide participants with a robust understanding of network defense principles, strategies, and practical applications, equipping them with the skills needed to protect, detect, respond to, and predict cybersecurity threats effectively.

IV. Schedule:

The certificate program entails a commitment of 12 hours, with sessions lasting 4 hours each week. Candidates have the flexibility to select their preferred schedule from the following options:

Evening classes
From 6:30 PM to 8:30 PM
Monday and Tuesday or Thursday and Friday

Weekend classes
From 10:00 AM to 12:00 PM:
Saturday and Sunday

V. Enrollment requirements:

Enrollment requirements are straightforward: there are no specific prerequisites. However, participants are expected to have a basic understanding of networking, operating systems, and coding principles.

VI. The Benefits of the program:

- **Holistic Understanding:** Gain a comprehensive overview of key information security components and network defense strategies.
- **Practical Experience:** Benefit from interactive labs that provide the hands-on experience required for a career in cybersecurity.
- **Career Advancement:** The NDE certification serves as formal recognition of your expertise, enhancing your resume and employment prospects.
- **Foundational Knowledge:** Establish a solid foundation in cybersecurity, preparing you for more advanced studies and certifications in the field.

These benefits make the program a must-have for individuals and organizations aiming to equip themselves with the best possible defense against network breaches, emphasizing practical skills and up-to-date knowledge in network security.

Contacts :

cybersecuritycontact@medtech.tn
Les jardins du LAC 2, 1053, Tunis - Tunisie