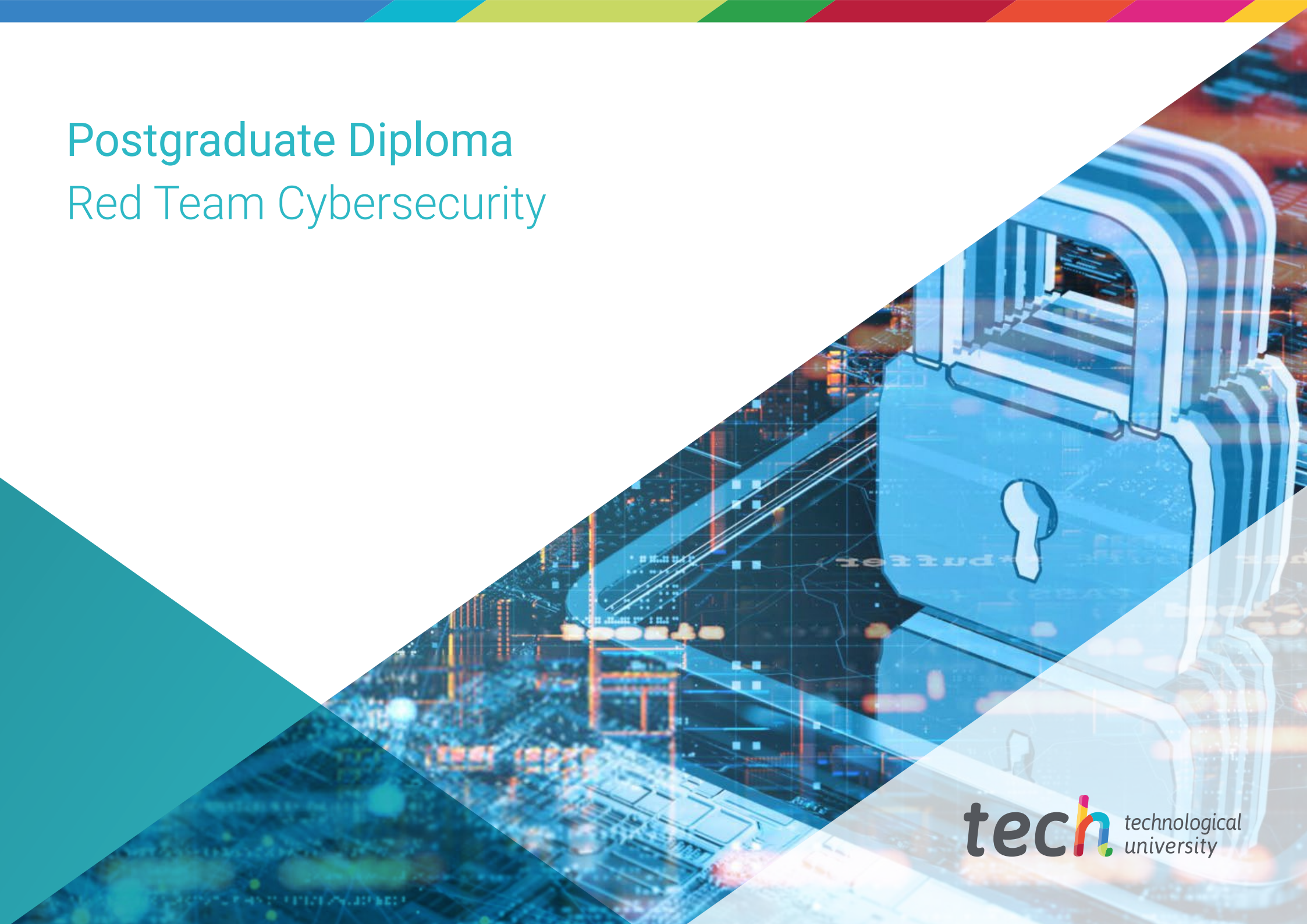
Postgraduate Diploma
Red Team Cybersecurity



tech technological university

tech technological university

Postgraduate Diploma
Red Team Cybersecurity

- Modality: **online**
- Duration: **6 months.**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Website: www.techtitute.com/in/infromation-technology/postgraduate-diploma/postgraduate-diploma-red-team-cybersecurity

Index

01

Introduction

Cybersecurity has become a fundamental pillar in the digital age, while the increasing interconnectedness of systems has intensified the threat of cyberattacks. The demand for highly specialized professionals in this field is more evident than ever, especially considering the exponential increase in cybercrime and sophisticated attacks. In this context, this program is presented as a strategic response to equip professionals with the necessary skills to face cyber threats. Throughout the curriculum, students will be immersed in the simulation of advanced threats. The methodology of the curriculum, 100% online, offers flexibility and accessibility, with a wide variety of multimedia content and the application of the Relearning method.

You will contribute to improving Cybersecurity and prevent major digital crimes from occurring. Don't miss this opportunity and enroll!"

In the complex scenario of Cybersecurity, having an expert in this field presents itself as an imperative need for organizations looking to strengthen their defenses against constantly evolving threats. This proactive approach, fundamental to continuously improving the security posture, highlights the critical need for experts.

Implementing proactive measures is essential and Red Team's specialized knowledge provides professionals with the ability to actively anticipate, identify and mitigate vulnerabilities in systems and networks. In this Postgraduate Diploma, the student will acquire skills in penetration testing and simulations, addressing the identification and exploitation of vulnerabilities. In this sense, they will not only develop advanced technical skills, but also foster effective collaboration with security teams, integrating strategies against malware threats.

In addition, the graduates will acquire a solid understanding of the fundamental principles of digital forensic investigation (DFIR), applicable in the resolution of cyber incidents. Furthermore, this comprehensive approach to the curriculum will ensure that professionals are equipped with cutting-edge skills in the field of Cybersecurity.

This academic pathway is distinguished not only by its content, but also by its advanced methodology. It will be available to students entirely online, giving them the flexibility they need to advance their careers without compromising their job responsibilities.

In addition, it will employ the Relearning methodology, consisting of the repetition of key concepts, is used to fix knowledge and facilitate effective learning. This combination of accessibility and robust pedagogical approach makes this Postgraduate Diploma not only an advanced educational option, but also a significant driver for those seeking to excel in the field of Cybersecurity.

This **Postgraduate Diploma in Red Team Cybersecurity** contains the most complete and up-to-date program on the market. The most important features include:

- The development of case studies presented by experts in Red Team Cybersecurity
- The graphic, schematic and practical contents with which it is conceived provide cutting- Therapeutics and practical information on those disciplines that are essential for professional practice
- Practical exercises where the self-assessment process can be carried out to improve learning
- Its special emphasis on innovative methodologies
- Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- Content that is accessible from any fixed or portable device with an Internet connection

You will stand out in a sector with great projection thanks to this exclusive university program at TECH"

You will delve into detailed forensic reporting at the world's top-rated university by its students, according to the Trustpilot platform (4.9/5)"

You will develop skills to evaluate and select anti-malware security tools.

Forget about memorizing! With the Relearning system you will integrate the concepts in a natural and progressive way.

The program's teaching staff includes professionals from the field who contribute their work experience to this educational program, as well as renowned specialists from leading societies and prestigious universities.

The multimedia content, developed with the latest educational technology, will provide the professional with situated and contextual learning, i.e., a simulated environment that will provide immersive education programmed to learn in real situations.

This program is designed around Problem-Based Learning, whereby the professional must try to solve the different professional practice situations that arise during the academic year For this purpose, the students will be assisted by an innovative interactive video system created by renowned and experienced experts.

02

Objectives

The main objective of the Postgraduate Diploma in Red Team Cybersecurity is to train students in the development of skills in advanced threat simulation. Throughout the program, graduates will be immersed in the replication of tactics, techniques and procedures (TTP) used by malicious actors. In this context, the specialized approach will not only strengthen the technical skills of the professionals, but will also train them to face real-world challenges in this field. In addition, the use of the Relearning methodology will facilitate the learning, fixing key concepts with little effort.

You will identify weak points and vulnerabilities in the cyber infrastructures of companies. Reach your goals with TECH!"

General Objectives

- Acquire advanced skills in penetration testing and *Red Team* simulations, addressing the identification and exploitation of vulnerabilities in systems and networks
- Develop leadership skills to coordinate teams specialized in offensive cybersecurity, optimizing the execution of *Pentesting* and *Red Team* projects
- Develop skills in the analysis and development of *malware*, understanding its functionality and applying defensive and educational strategies
- Refine communication skills by preparing detailed technical and executive reports, presenting findings effectively to technical and executive audiences
- Promote an ethical and responsible practice in the field of cybersecurity, considering ethical and legal principles in all activities
- Keep students up-to-date with emerging trends and technologies in cybersecurity

You will achieve your objectives thanks to TECH's didactic tools, including explanatory videos and interactive summaries"

Specific Objectives

Module 1. Malware Analysis and Development

- Acquire advanced knowledge of the nature, functionality and behavior of malware, understanding its various forms and targets
- Develop skills in forensic analysis applied to malware, enabling the identification of indicators of compromise (IoC) and attack patterns
- Learn strategies for effective malware detection and prevention, including the deployment of advanced security solutions
- Familiarize the student with the development of malware for educational and defensive purposes, allowing a deep understanding of the tactics used by attackers
- Promote ethical and legal practices in malware analysis and development, ensuring integrity and accountability in all activities
- Apply theoretical knowledge in simulated environments, participate in hands-on exercises to understand and counter malicious attacks
- Develop skills to evaluate and select anti-malware security tools, considering their effectiveness and adaptability to specific environments
- Learn how to implement effective mitigation against malicious threats, reducing the impact and spread of malware on systems and networks
- Foster effective collaboration with security teams, integrating strategies and efforts to protect against malware threats
- Keep the graduate up-to-date with the latest trends and techniques used in malware analysis and development, ensuring the continued relevance and effectiveness of the skills acquired

Module 2. Forensic Fundamentals and DFIR

- Acquire a solid understanding of the fundamental principles of digital forensic investigation (DFIR) and their application in the resolution of cyber incidents
- Develop skills in the secure and forensic acquisition of digital evidence, ensuring the preservation of the chain of custody
- Learn how to perform forensic analysis of file systems
- Familiarize the student with advanced techniques for log and log analysis, allowing the reconstruction of events in digital environments
- Learn how to apply digital forensic investigation methodologies in case resolution, from identification to documentation of findings
- Familiarize the student with the analysis of digital evidence and the application of forensic techniques in *Pentesting* environments
- Develop skills in the preparation of detailed and clear forensic reports, presenting findings and conclusions in an understandable manner
- Foster effective collaboration with incident response (IR) teams, optimizing coordination in threat investigation and mitigation
- Promote ethical and legal practices in digital forensics, ensuring adherence to cybersecurity regulations and standards of conduct

Module 3. Advanced Red Team Exercises

- Develop skills in advanced threat simulation, replicating tactics, techniques and procedures (TTP) used by attractive malicious actors
- Learn to identify weaknesses and vulnerabilities in the infrastructure through realistic *Red Team*exercises, strengthening the security posture
- Familiarize the graduate with advanced techniques for evasion of security measures, allowing to evaluate the resistance of the infrastructure against desirable attacks
- Develop effective coordination and collaboration skills among *Red Team* team members, optimizing the execution of tactics and strategies to comprehensively assess the security of the organization
- Learn how to simulate current threat scenarios, such as *ransomware* attacks or advanced *phishing* campaigns, to assess the organization's response capabilities
- Familiarize the student with post-exercise analysis techniques, evaluating the performance of the Red Team and extracting lessons learned for continuous improvement
- Develop skills to assess organizational resilience to simulated attacks, identifying areas for improvement in policies and procedures
- Learn to prepare detailed reports documenting findings, methodologies used and recommendations derived from advanced *Red Team* exercises
- Promote ethical and legal practices in the conduct of *Red Team* exercises, ensuring adherence to cybersecurity regulations and ethical standards

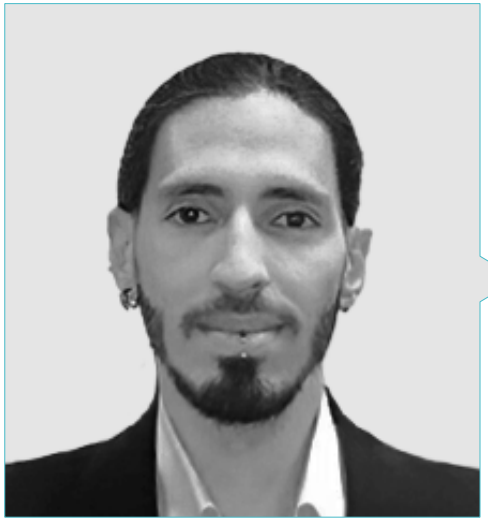
03

Course Management

For this university program, TECH has assembled a distinguished teaching staff, composed of the best specialists in the field. In this sense, each faculty member has an extensive and recognized professional background, forged in leading companies in the Cybersecurity sector. Carefully selected for their experience and expertise, these professionals will not only guarantee the academic quality of the curriculum, but will also provide a practical and up-to-date perspective, enriching the participants' training with valuable insights from their real-world experience in the Red Team environment.

Get up to date with the latest Shellcode (XQR) encryption techniques from the best experts in Cybersecurity. Launch your professional career with TECH!"

Management



Mr. Gómez Pintado, Carlos

- Manager of Cybersecurity and Network Team Cipherbit in Oesía Group
- Manager Advisor & Investor at Wesson App
- Graduate in Software Engineering and Information Society Technologies, Polytechnic University of Madrid
- Collaboration with educational institutions for the development of Higher Level Training Cycles in cybersecurity

04

Structure and Content

This curriculum will offer students a specialized immersion in forensic analysis applied to malware, highlighting the development of key skills for the identification of indicators of compromise (IoC) and attack patterns. Throughout the syllabus, graduates will be immersed in advanced methodologies, providing them with the necessary tools and knowledge to face sophisticated cyber threats. Likewise, this rigorously structured program will guarantee a comprehensive training in the Red Team field, preparing professionals to analyze and counteract the complex strategies used by malicious actors.

You will delve into advanced post-exploitation techniques and position yourself as an outstanding Red Teamer"

Module 1. *Malware* Analysis and Development

1.1. Malware Analysis and Development
- 1.1.1. History and Evolution of Malware
- 1.1.2. Classification and Types of Malware
- 1.1.3. Malware Analysis
- 1.1.4. Malware Development

1.2. Preparing the Environment
- 1.2.1. Configuration of Virtual Machines and Snapshots
- 1.2.2. Malware Analysis Tools
- 1.2.3. Malware Development Tools

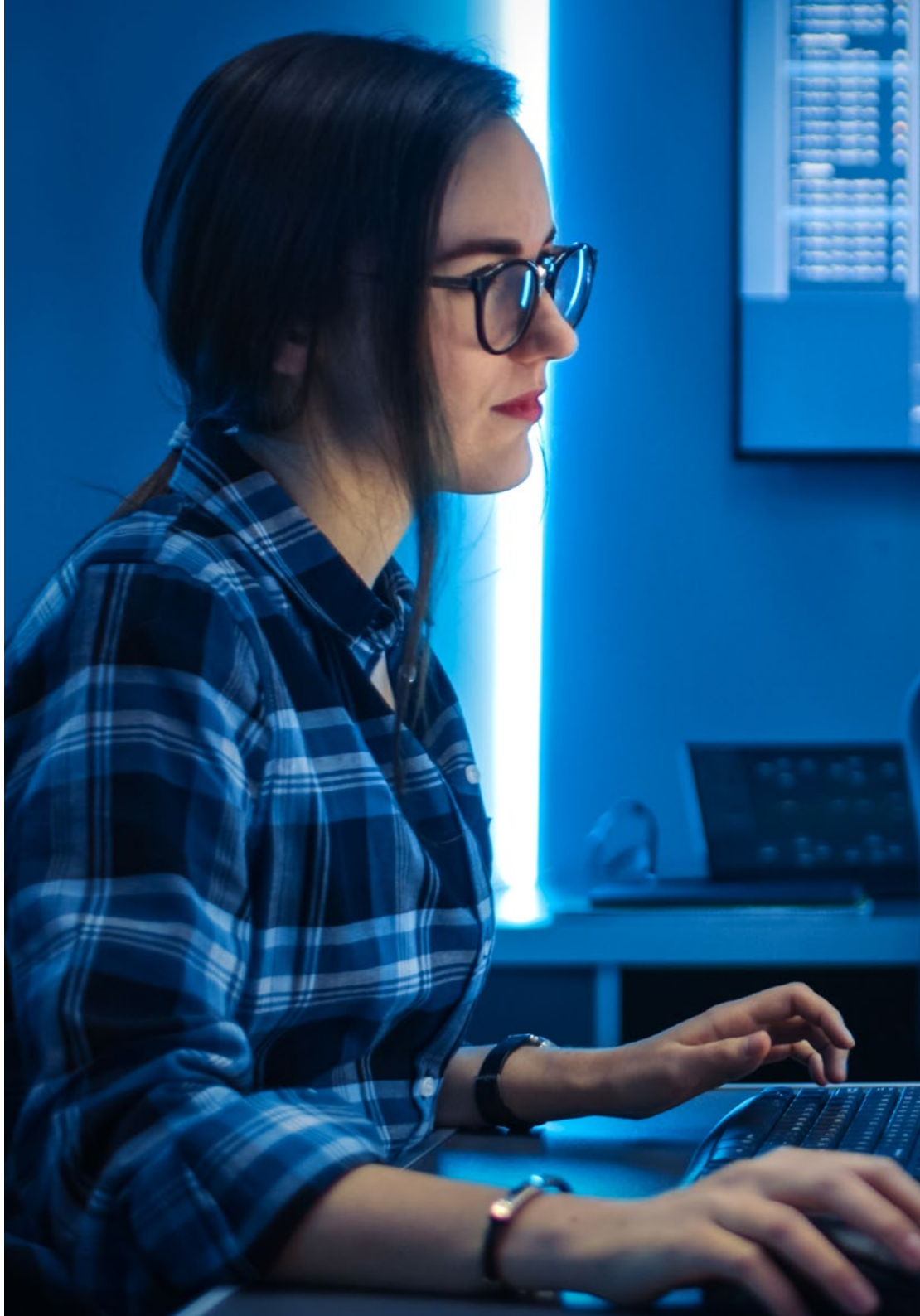
1.3. Windows Basics
- 1.3.1. PE file format (Portable Executable)
- 1.3.2. Processes and Threads
- 1.3.3. File System and Registry
- 1.3.4. Windows Defender

1.4. Basic Malware Techniques
- 1.4.1. Shellcode Generation
- 1.4.2. Execution of Shellcode on Disk
- 1.4.3. Disk vs Memory
- 1.4.4. Execution of Shellcode in Memory

1.5. Intermediate Malware Techniques
- 1.5.1. Persistence in Windows
- 1.5.2. Home Folder
- 1.5.3. Registration Keys
- 1.5.4. Screensaver

1.6. Advanced MalwareTechniques
- 1.6.1. Shellcode Encryption (XOR)
- 1.6.2. Shellcode Encryption (RSA)
- 1.6.3. String Obfuscation
- 1.6.4. Process Injection

1.7. Static Malware Analysis
- 1.7.1. Analyzing Packers with DIE (Detect It Easy)
- 1.7.2. Analyzing Sections with PE-Bear
- 1.7.3. Decompilation with Ghidra



1.8. Dynamic Malware Analysis
- 1.8.1. Observing Behavior with Process Hacker
- 1.8.2. Analyzing Calls with API Monitor
- 1.8.3. Analyzing Registry Changes with Regshot
- 1.8.4. Observing Network Requests with TCPView

1.9. Analysis in .NET
- 1.9.1. Introduction to .NET
- 1.9.2. Decompiling with dnSpy
- 1.9.3. Debugging with dnSpy

1.10. Analyzing Real Malware
- 1.10.1. Preparing the Environment
- 1.10.2. Static Malware Analysis
- 1.10.3. Dynamic Malware Analysis
- 1.10.4. YARA Rule Creation

Module 2. Forensic Fundamentals and DFIR

2.1. Digital Forensics
- 2.1.1. History and Evolution of Computer Forensics
- 2.1.2. Importance of Computer Forensics in Cybersecurity
- 2.1.3. History and Evolution of Computer Forensics

2.2. Fundamentals of Computer Forensics
- 2.2.1. Chain of Custody and Its Application
- 2.2.2. Types of Digital Evidence
- 2.2.3. Evidence Acquisition Processes

2.3. File Systems and Data Structure
- 2.3.1. Main File Systems
- 2.3.2. Data Hiding Methods
- 2.3.3. Analysis of File Metadata and Attributes

2.4. Operating Systems Analysis
- 2.4.1. Forensic Analysis of Windows Systems
- 2.4.2. Forensic Analysis of Linux Systems
- 2.4.3. Forensic Analysis of macOS Systems

2.5. Data Recovery and Disk Analysis
- 2.5.1. Data Recovery from Damaged Media
- 2.5.2. Disk Analysis Tools
- 2.5.3. Interpretation of File Allocation Tables

2.6. Network and Traffic Analysis
- 2.6.1. Network Packet Capture and Analysis
- 2.6.2. Firewall Log Analysis
- 2.6.3. Network Intrusion Detection

2.7. Malware and Malicious Code Analysis
- 2.7.1. Classification of Malware and Its Characteristics
- 2.7.2. Static and Dynamic Malware Analysis
- 2.7.3. Disassembly and Debugging Techniques

2.8. Log and Event Analysis
- 2.8.1. Types of Logs in Systems and Applications
- 2.8.2. Interpretation of Relevant Events
- 2.8.3. Log Analysis Tools

2.9. Respond to Security Incidents
- 2.9.1. Incident Response Process
- 2.9.2. Creating an Incident Response Plan
- 2.9.3. Coordination with Security Teams

2.10. Evidence and Legal Presentation
- 2.10.1. Rules of Digital Evidence in the Legal Field
- 2.10.2. Preparation of Forensic Reports
- 2.10.3. Appearance at Trial as an Expert Witness

Module 3. Advanced Red Team Exercises

3.1. Advanced Recognition Techniques
- 3.1.1. Advanced Subdomain Enumeration
- 3.1.2. Advanced Google Dorking
- 3.1.3. Social Networks and theHarvester

3.2. Advanced Phishing Campaigns
- 3.2.1. What is Reverse-Proxy Phishing?
- 3.2.2. 2FA Bypass with Evilginx
- 3.2.3. Data Exfiltration

3.3. Advanced Persistence Techniques
- 3.3.1. Golden Tickets
- 3.3.2. Silver Tickets
- 3.3.3. DCShadow Technique

3.4. Advanced Avoidance Techniques
- 3.4.1. AMSI Bypass
- 3.4.2. Modification of Existing Tools
- 3.4.3. Powershell Obfuscation

3.5. Advanced Lateral Movement Techniques
- 3.5.1. Pass-the-Ticket (PtT)
- 3.5.2. Overpass-the-Hash (Pass-the-Key)
- 3.5.3. NTLM Relay

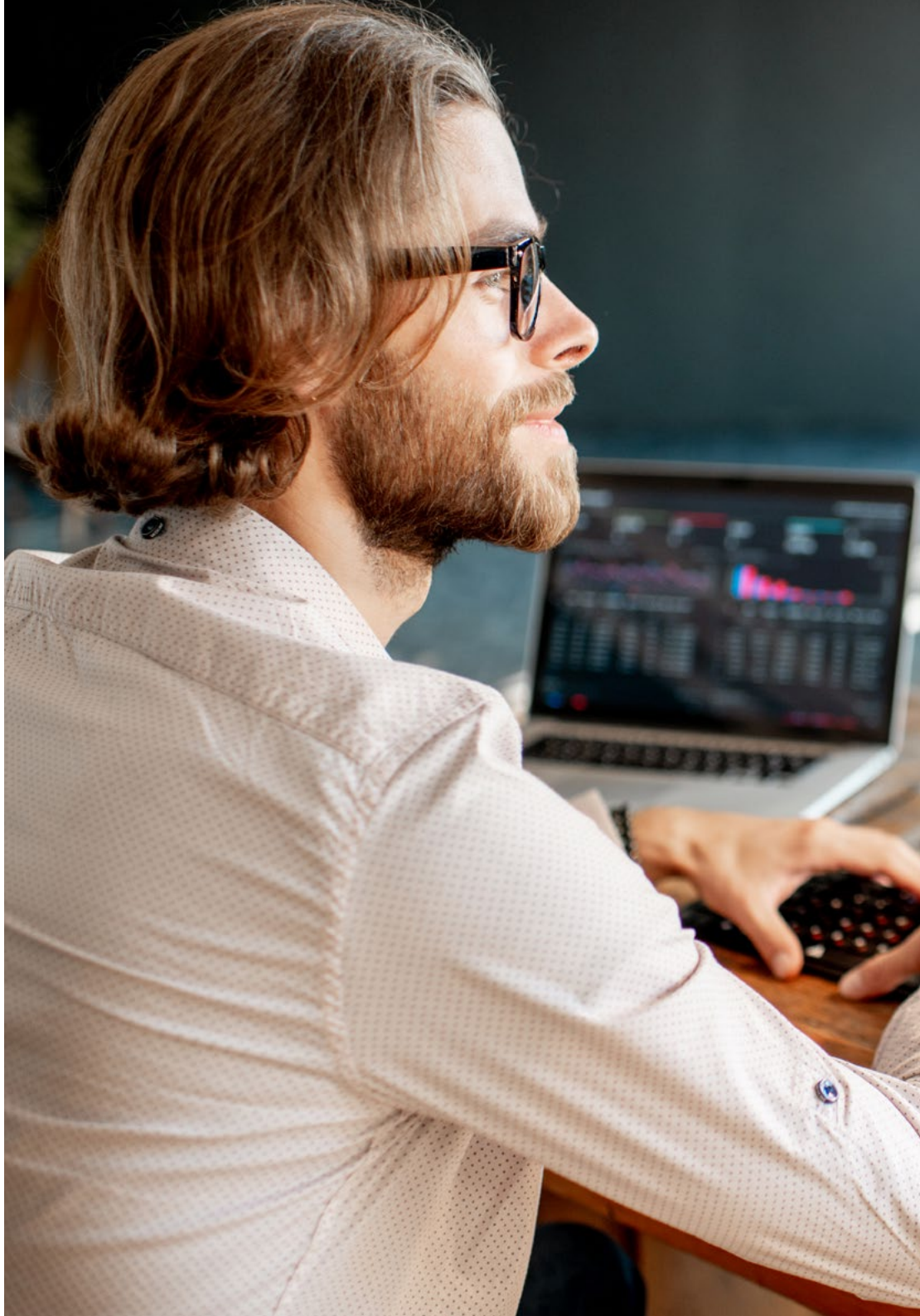
3.6. Advanced Post-Exploitation Techniques
- 3.6.1. LSASS Dump
- 3.6.2. SAM Dump
- 3.6.3. DCSync Attack

3.7. Advanced Pivoting Techniques
- 3.7.1. What Is Pivoting
- 3.7.2. Tunneling with SSH
- 3.7.3. Pivoting with Chisel

3.8. Physical Intrusions
- 3.8.1. Surveillance and Reconnaissance
- 3.8.2. Tailgating and Piggybacking
- 3.8.3. Lock-Picking

3.9. Wi-Fi Attacks
- 3.9.1. WPA/WPA2 PSK Attacks
- 3.9.2. AP Rogue Attacks
- 3.9.3. Attacks on WPA2 Enterprise

3.10. RFID Attacks
- 3.10.1. RFID Card Reading
- 3.10.2. RFID Card Manipulation
- 3.10.3. Creation of Cloned Cards



Don't miss the opportunity to boost your career through this innovative program. Become an expert in Cybersecurity!"

05

Methodology

This academic program offers students a different way of learning. Our methodology uses a cyclical learning approach: **Relearning.**

This teaching system is used, for example, in the most prestigious medical schools in the world, and major publications such as the **New England Journal of Medicine** have considered it to be one of the most effective.

Discover Relearning, a system that abandons conventional linear learning, to take you through cyclical teaching systems: a way of learning that has proven to be extremely effective, especially in subjects that require memorization"

Case Study to contextualize all content

Our program offers a revolutionary approach to developing skills and knowledge. Our goal is to strengthen skills in a changing, competitive, and highly demanding environment.

At TECH, you will experience a learning methodology that is shaking the foundations of traditional universities around the world"

You will have access to a learning system based on repetition, with natural and progressive teaching throughout the entire syllabus.

The student will learn to solve complex situations in real business environments through collaborative activities and real cases.

A learning method that is different and innovative

This TECH program is an intensive educational program, created from scratch, which presents the most demanding challenges and decisions in this field, both nationally and internationally. This methodology promotes personal and professional growth, representing a significant step towards success. The case method, a technique that lays the foundation for this content, ensures that the most current economic, social and professional reality is taken into account.

> *Our program prepares you to face new challenges in uncertain environments and achieve success in your career"*

The case method has been the most widely used learning system among the world's leading Information Technology schools for as long as they have existed. The case method was developed in 1912 so that law students would not only learn the law based on theoretical content. It consisted of presenting students with real-life, complex situations for them to make informed decisions and value judgments on how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

What should a professional do in a given situation? This is the question that you are presented with in the case method, an action-oriented learning method. Throughout the course, students will be presented with multiple real cases. They will have to combine all their knowledge and research, and argue and defend their ideas and decisions.

Relearning Methodology

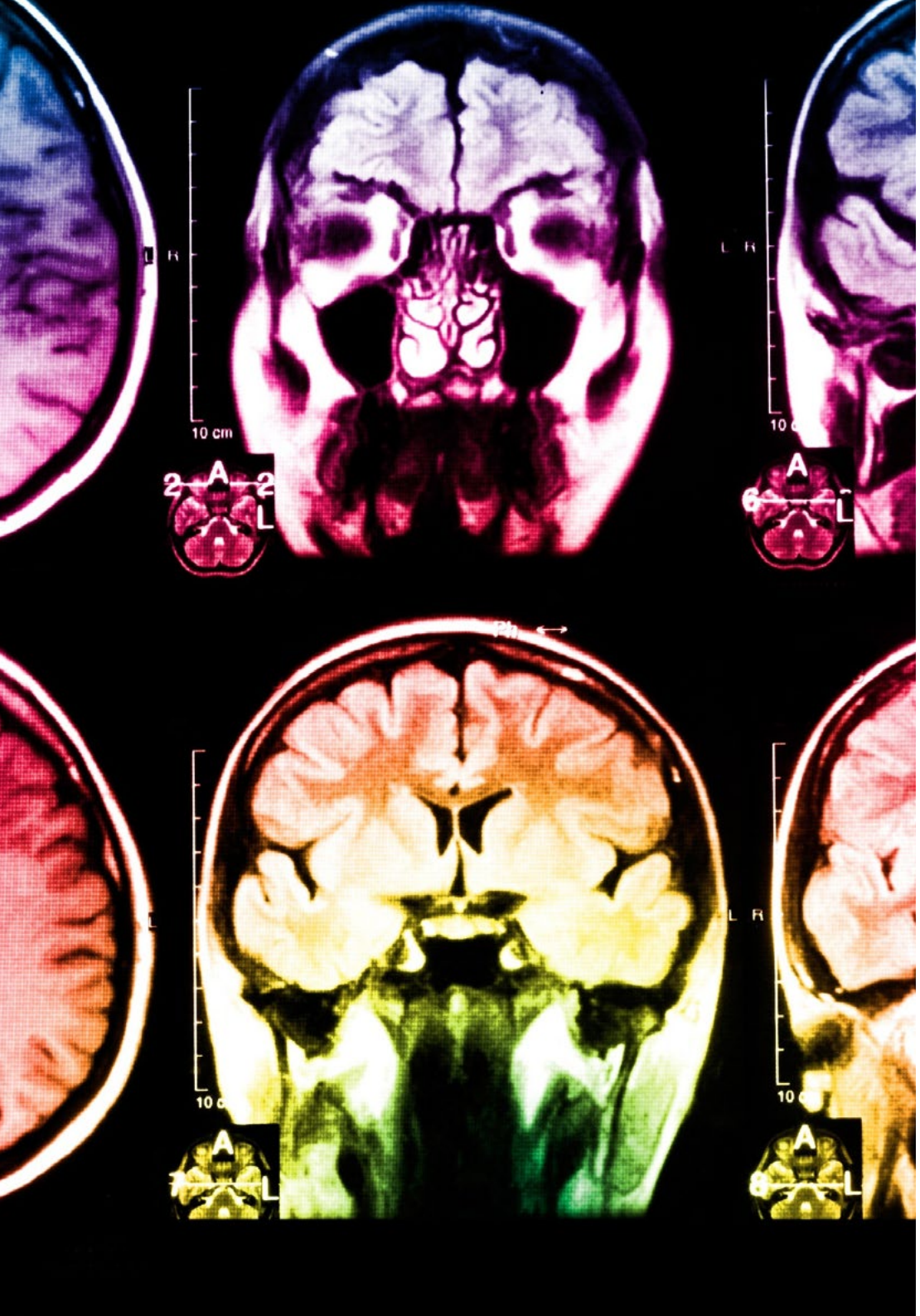
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

We enhance the Case Study with the best 100% online teaching method: Relearning.

In 2019, we obtained the best learning results of all online universities in the world.

At TECH you will learn using a cutting-edge methodology designed to train the executives of the future. This method, at the forefront of international teaching, is called Relearning.

Our university is the only one in the world authorized to employ this successful method. In 2019, we managed to improve our students' overall satisfaction levels (teaching quality, quality of materials, course structure, objectives...) based on the best online university indicators.



In our program, learning is not a linear process, but rather a spiral (learn, unlearn, forget, and re-learn). Therefore, we combine each of these elements concentrically. This methodology has trained more than 650,000 university graduates with unprecedented success in fields as diverse as biochemistry, genetics, surgery, international law, management skills, sports science, philosophy, law, engineering, journalism, history, and financial markets and instruments. All this in a highly demanding environment, where the students have a strong socio-economic profile and an average age of 43.5 years.

Relearning will allow you to learn with less effort and better performance, involving you more in your training, developing a critical mindset, defending arguments, and contrasting opinions: a direct equation for success.

From the latest scientific evidence in the field of neuroscience, not only do we know how to organize information, ideas, images and memories, but we know that the place and context where we have learned something is fundamental for us to be able to remember it and store it in the hippocampus, to retain it in our long-term memory.

In this way, and in what is called neurocognitive context-dependent e-learning, the different elements in our program are connected to the context where the individual carries out their professional activity.

This program offers the best educational material, prepared with professionals in mind:

Study Material

All teaching material is produced by the specialists who teach the course, specifically for the course, so that the teaching content is highly specific and precise.

These contents are then applied to the audiovisual format, to create the TECH online working method. All this, with the latest techniques that offer high quality pieces in each and every one of the materials that are made available to the student.

Classes

There is scientific evidence suggesting that observing third-party experts can be useful.

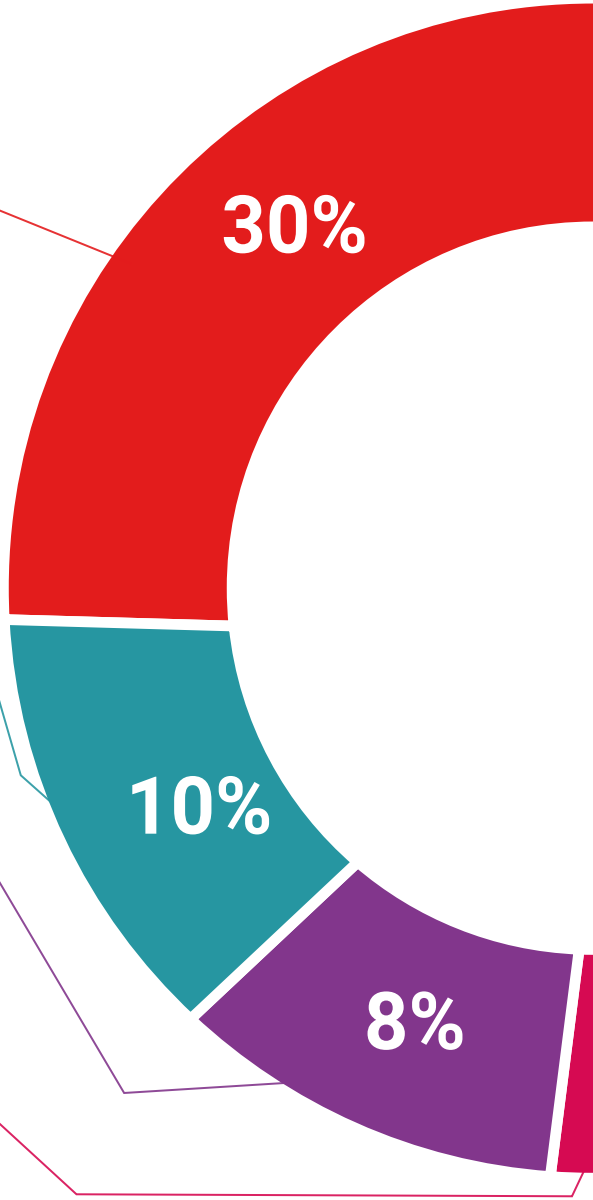
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

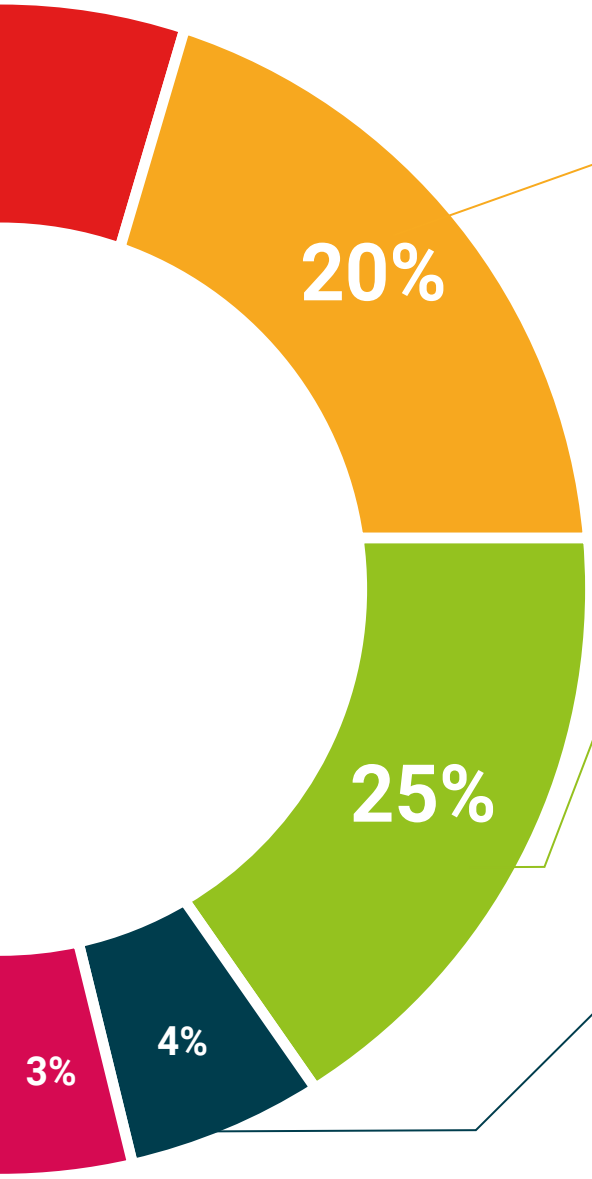
Practising Skills and Abilities

They will carry out activities to develop specific skills and abilities in each subject area. Exercises and activities to acquire and develop the skills and abilities that a specialist needs to develop in the context of the globalization that we are experiencing.

Additional Reading

Recent articles, consensus documents and international guidelines, among others. In TECH's virtual library, students will have access to everything they need to complete their course.





Case Studies

Students will complete a selection of the best case studies chosen specifically for this program. Cases that are presented, analyzed, and supervised by the best specialists in the world.

Interactive Summaries

The TECH team presents the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

This exclusive educational system for presenting multimedia content was awarded by Microsoft as a "European Success Story".

Testing & Retesting

We periodically evaluate and re-evaluate students' knowledge throughout the program, through assessment and self-assessment activities and exercises, so that they can see how they are achieving their goals.

06

Certificate

The Postgraduate Diploma in Red Team Cybersecurity guarantees students, in addition to the most rigorous and up-to-date education, access to a Postgraduate Diploma issued by TECH Technological University.

Successfully complete this program and receive your university qualification without having to travel or fill out laborious paperwork"

This**Postgraduate Diploma in Red Team Cybersecurity** contains the most complete and up-to-date program on the market.

After the student has passed the assessments, they will receive their corresponding **Postgraduate Diploma** issued by **TECH Technological University** via tracked delivery*.

The certificate issued by **TECH Technological University** will reflect the qualification obtained in the Postgraduate Diploma , and meets the requirements commonly demanded by labor exchanges, competitive examinations, and professional career evaluation committees.

Title: **Postgraduate Diploma in Red Team Cybersecurity**

Official Nº of Hours: **450 h.**


tech technological university

Awards the following

CERTIFICATE

to

Mr./Ms. _____, with identification number _____.

For having passed and accredited the following program

POSTGRADUATE DIPLOMA

in

Red Team Cybersecurity

This is a qualification awarded by this University, equivalent to 450 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

TECH is a Private Institution of Higher Education recognized by the Ministry of Public Education as of June 28, 2018.

June 17, 2020

Tere Guevara Navarro
Dean

Unique TECH Code: AFWORD23S techtitute.com/certificates

*Apostille Convention. In the event that the student wishes to have their paper certificate issued with an apostille, TECH EDUCATION will make the necessary arrangements to obtain it, at an additional cost.

tech technological university

Postgraduate Diploma
Red Team Cybersecurity

- Modality: **online**
- Duration: **6 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Postgraduate Diploma
Red Team Cybersecurity

tech technological university