

# Postgraduate Certificate

## Computer Security

### Incident Management



## Postgraduate Certificate Computer Security Incident Management

- » Modality: online
- » Duration: 6 weeks
- » Certificate: TECH Global University
- » Accreditation: 6 ECTS
- » Schedule: at your own pace
- » Exams: online

Website: [www.techtitude.com/us/information-technology/postgraduate-certificate/computer-security-incident-management](http://www.techtitude.com/us/information-technology/postgraduate-certificate/computer-security-incident-management)

# Index

01

Introduction

---

p. 4

02

Objectives

---

p. 8

03

Course Management

---

p. 12

04

Structure and Content

---

p. 16

05

Study Methodology

---

p. 20

06

Certificate

---

p. 30

# 01 Introduction

Proper management of computer security breaches allows affected companies and organizations to find out how the attack occurred and who was responsible, to respond to it and to prevent it from happening again. This is a task performed by IT professionals through computer forensics. In this Postgraduate Certificate, students, guided by expert cybersecurity professionals, will delve into an area that constantly requires staff with up-to-date knowledge. The 100% online format of this program also allows access to the entire syllabus at any time of the day and with just an internet-connected device.





“

*Improve your knowledge of  
cybersecurity and advance in your  
professional career. Enroll now”*

The practical implementation policy of all technological devices allows for the detection and response to computer security incidents. This is one of the main weapons that companies have to avoid suffering cyberattacks, the other is to have computer professionals on their teams capable of doing an excellent job that guarantees them a management that provides security to all their systems.

This Postgraduate Certificate provides students with all the information necessary to respond to incidents and detect their level of importance. Management is broad and covers operations that allow the detection of incidents through IDS/IPS systems and their subsequent processing in SIEM, notification and escalation to the corresponding department. An exhaustive analysis that will be possible thanks to the knowledge provided in this program by a team of professional experts in this branch of IT.

The 100% online format of this Postgraduate Certificate, which is offered by TECH, makes it easier for students to learn by being able to balance their personal responsibilities with an education that will allow them to advance in their professional career. In this way, students only need a device with an Internet connection to access the entire syllabus, which can also be downloaded from day one.

This **Postgraduate Certificate in Computer Security Incident Management** 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 information security policies
- ♦ The graphic, schematic and practical contents of the book provide technical and practical information on those disciplines that are essential for professional practice
- ♦ Practical exercises where self-assessment can be used 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



*Become a computer security professional. Manage any incident with optimal results. Enroll now"*



*Learn how CERT organizations work to detect incidents and improve your skills. Enroll now”*

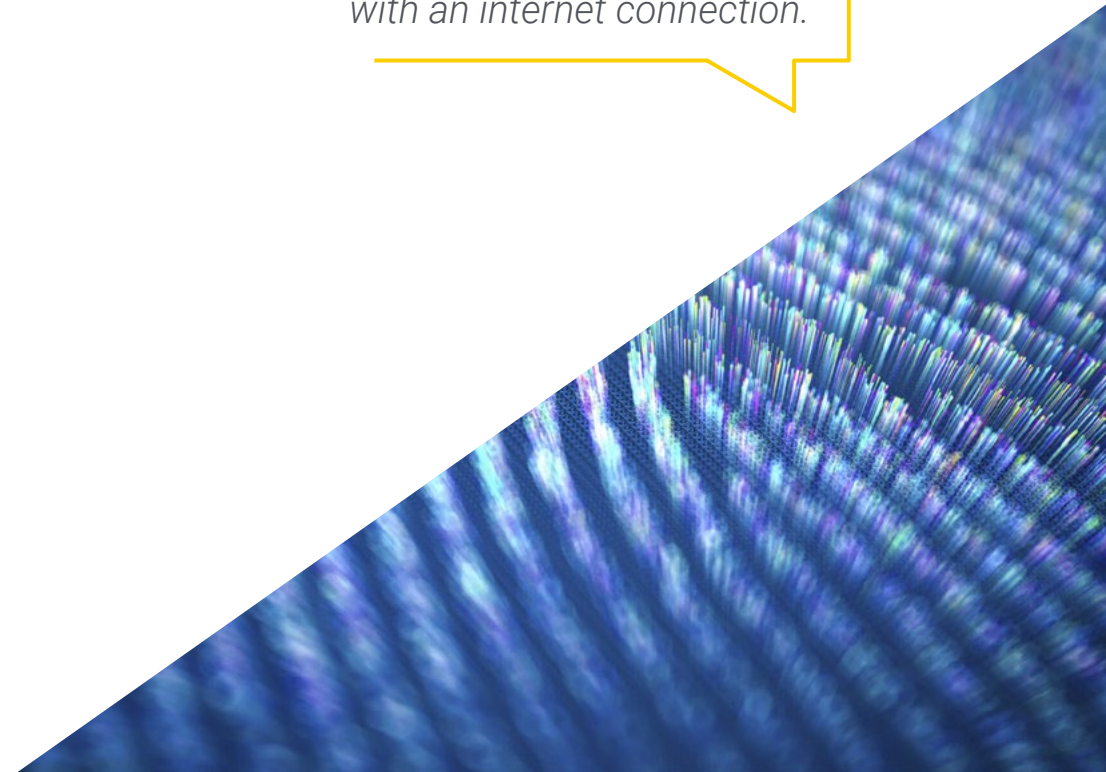
The program's teaching staff includes professionals from the sector who contribute their work experience to this educational program, as well as renowned specialists from leading societies and prestigious universities.

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 prepare for 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 course. For this purpose, students will be assisted by an innovative interactive video system created by renowned and experienced experts.

*Master ISO standards and safety regulations applied to different fields with this Postgraduate Certificate. Click and enroll.*

*This 100% online Postgraduate Certificate gives you total freedom of access, with no fixed schedules and from any device with an internet connection.*





# 02 Objectives

On completing this Postgraduate Certificate, IT professionals will have acquired in-depth knowledge of computer security incident management. Students will be able to analyze the different phases involved in the detection and resolution of incidents, carry out a correct computer forensic analysis, as well as apply current legal regulations and ISO standards. The teaching team specialized in this area will be in charge of accompanying the students so that they reach all their goals and progress in their professional careers.





“

*Improve your knowledge in a field that requires professionals who know how to effectively manage any cyberattack”*





## General Objectives

- Develop specialized knowledge on how to manage incidents caused by IT security events
- Determine the operation of a security incident handling team
- Analyze the different phases of an IT security event management
- Install and learn about the different tools used in the treatment and prevention of incidents
- Review standardized protocols for handling security incidents



*Master all the necessary stages for dealing with incidents caused by security breaches. Enroll now"*





## Specific Objectives

---

- ♦ Analyze the importance of a correct treatment of security incidents
- ♦ Determine the necessary phases for the treatment of incidents caused by computer security failures
- ♦ Implement the various tools for incident prevention
- ♦ Determine what is a team of preventive and reactive treatment of security incidents
- ♦ Assess the need for a computer forensic analysis for the in-depth study of recorded incidents
- ♦ Implement CCN-STIC 817 and Implement ISO 27035



03

# Course Management

This Postgraduate Certificate has a teaching staff with expertise in the field of computer security in public and private organizations, which provides students with teaching that is very close to the reality of the IT industry. Likewise, the high qualifications of the professional who teaches this Postgraduate Certificate means that the learning experience that students acquire during the six weeks of this course is of the highest quality. The closeness of the lecturer will allow professionals to progress and achieve their objectives.



“

*A teaching staff with experience in the public and private sectors will guide students through this Postgraduate Certificate”*

## Management



### Ms. Fernández Sapena, Sonia

- Trainer in Computer Security and Ethical Hacking at the National Reference Center of Getafe in Computer Science and Telecommunications in Madrid
- Certified E-Council instructor
- Trainer in the following certifications: EXIN Ethical Hacking Foundation and EXIN Cyber & IT Security Foundation. Madrid
- Accredited expert trainer by the CAM of the following certificates of professionalism: Computer Security (IFCT0190), Voice and Data Network Management (IFCM0310), Departmental Network Administration (IFCT0410), Alarm Management in Telecommunications Networks (IFCM0410), Voice and Data Network Operator (IFCM0110), and Internet Services Administration (IFCT0509)
- External collaborator CSO/SSA (*Chief Security Officer/Senior Security Architect*) at the University of the Balearic Islands
- Degree in Computer Engineering from the University of Alcalá de Henares, Madrid.
- Master's Degree in DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Technologies. E-Council





## Professors

### Mr. Solana Villarias, Fabián

- ♦ Information Technology Consultant
- ♦ Creator and Administrator of Survey Services in Research, Planning and Development SA
- ♦ Financial Markets and IT Systems Maintenance Specialist at Iberia Financial Software
- ♦ Web Developer and Accessibility Specialist at Indra
- ♦ Degree in Systems Engineering from the University of Wales/CESINE
- ♦ Diploma in Technical Engineering in Computer Systems Engineering from the University of Wales/ CESINE

“

*A unique, key and decisive learning experience to boost your professional development”*

# 04

## Structure and Content

The syllabus for this Postgraduate Certificate covers each of the critical points for the application of information security policies in companies. The syllabus, drawn up by professionals in the field, covers incident management, intrusion detection and prevention systems, the tools used and the regulations to be applied in the public and private sectors. Video summaries and additional reading will provide students with a foundation of knowledge in a program that provides them with specialization in an area with a wide range of job opportunities.



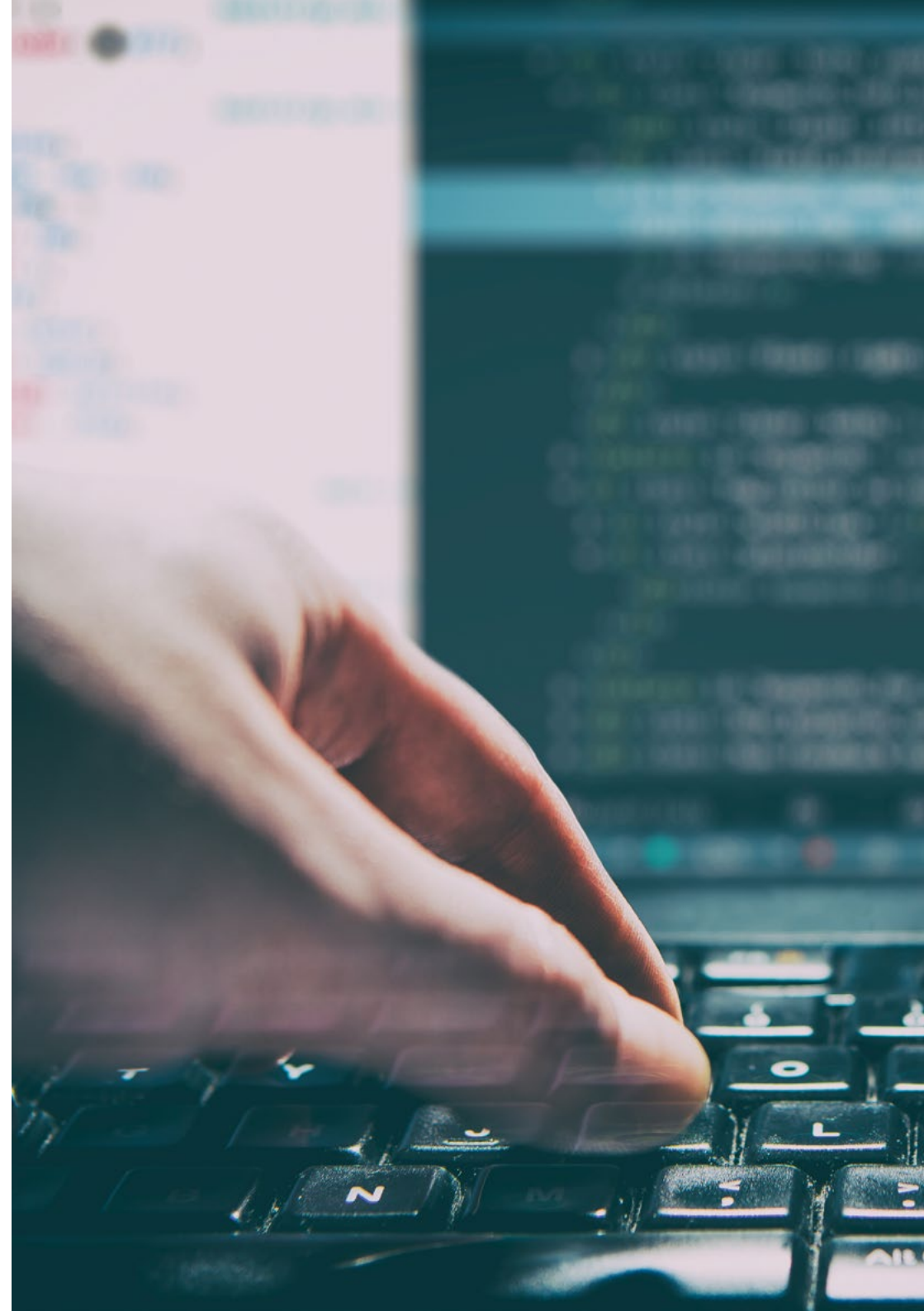
“

*A syllabus with up-to-date content and completely available from the very beginning of this Postgraduate Certificate. Learn at your own pace”*



## Module 1. Security Incident Management Policies

- 1.1. Information Security Incident Management Policies and Enhancements
  - 1.1.1. Incident Management
  - 1.1.2. Responsibilities and Procedures
  - 1.1.3. Event Notification
- 1.2. Intrusion Detection and Prevention Systems (IDS/IPS)
  - 1.2.1. System Operating Data
  - 1.2.2. Types of Intrusion Detection Systems
  - 1.2.3. Criteria for IDS/IPS Placement
- 1.3. Security Incident Response
  - 1.3.1. Data Collection Procedure
  - 1.3.2. Intrusion Verification Process
  - 1.3.3. CERT Organizations
- 1.4. Intrusion Attempt Notification and Management Process
  - 1.4.1. Responsibilities in the Notification Process
  - 1.4.2. Classification of Incidents
  - 1.4.3. Resolution and Recovery Process
- 1.5. Forensic Analysis as a Security Policy
  - 1.5.1. Volatile and Non-Volatile Evidence
  - 1.5.2. Analysis and Collection of Electronic Evidence
    - 1.5.2.1. Analysis of Electronic Evidence
    - 1.5.2.2. Collection of Electronic Evidence
- 1.6. Intrusion Detection and Prevention Systems (IDS/IPS) Tools
  - 1.6.1. Snort
  - 1.6.2. Suricata
  - 1.6.3. Solar-Winds
- 1.7. Event Centralizing Tools
  - 1.7.1. SIM
  - 1.7.2. SEM
  - 1.7.3. SIEM



- 1.8. CCN-STIC Security Guide 817
  - 1.8.1. Cyber Incident Management
  - 1.8.2. Metrics and Indicators
- 1.9. NIST SP800-61
  - 1.9.1. Computer Security Incident Response Capability
  - 1.9.2. Handling an Incident
  - 1.9.3. Coordination and Information Sharing
- 1.10. ISO 27035
  - 1.10.1. ISO 27035 Standard. Incident Management Principles
  - 1.10.2. Incident Management Plan Preparation Guidelines
  - 1.10.3. Incident Response Operations Guides

“A unique study plan designed for you. Without fixed schedules or on-site attendance. Distribute the teaching load according to your needs. Enroll now”



# 05 Study Methodology

TECH is the world's first university to combine the **case study** methodology with **Relearning**, a 100% online learning system based on guided repetition.

This disruptive pedagogical strategy has been conceived to offer professionals the opportunity to update their knowledge and develop their skills in an intensive and rigorous way. A learning model that places students at the center of the educational process giving them the leading role, adapting to their needs and leaving aside more conventional methodologies.





“

*TECH will prepare you to face new challenges in uncertain environments and achieve success in your career”*

## The student: the priority of all TECH programs

In TECH's study methodology, the student is the main protagonist.

The teaching tools of each program have been selected taking into account the demands of time, availability and academic rigor that, today, not only students demand but also the most competitive positions in the market.

With TECH's asynchronous educational model, it is students who choose the time they dedicate to study, how they decide to establish their routines, and all this from the comfort of the electronic device of their choice. The student will not have to participate in live classes, which in many cases they will not be able to attend. The learning activities will be done when it is convenient for them. They can always decide when and from where they want to study.

“

*At TECH you will NOT have live classes  
(which you might not be able to attend)”*



### The most comprehensive study plans at the international level

TECH is distinguished by offering the most complete academic itineraries on the university scene. This comprehensiveness is achieved through the creation of syllabi that not only cover the essential knowledge, but also the most recent innovations in each area.

By being constantly up to date, these programs allow students to keep up with market changes and acquire the skills most valued by employers. In this way, those who complete their studies at TECH receive a comprehensive education that provides them with a notable competitive advantage to further their careers.

And what's more, they will be able to do so from any device, pc, tablet or smartphone.

“*TECH's model is asynchronous, so it allows you to study with your pc, tablet or your smartphone wherever you want, whenever you want and for as long as you want*”



## Case Studies and Case Method

The case method has been the learning system most used by the world's best business schools. Developed in 1912 so that law students would not only learn the law based on theoretical content, its function was also to present them with real complex situations. In this way, they could make informed decisions and value judgments about how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

With this teaching model, it is students themselves who build their professional competence through strategies such as Learning by Doing or Design Thinking, used by other renowned institutions such as Yale or Stanford.

This action-oriented method will be applied throughout the entire academic itinerary that the student undertakes with TECH. Students will be confronted with multiple real-life situations and will have to integrate knowledge, research, discuss and defend their ideas and decisions. All this with the premise of answering the question of how they would act when facing specific events of complexity in their daily work.



## Relearning Methodology

At TECH, case studies are enhanced with the best 100% online teaching method: Relearning.

This method breaks with traditional teaching techniques to put the student at the center of the equation, providing the best content in different formats. In this way, it manages to review and reiterate the key concepts of each subject and learn to apply them in a real context.

In the same line, and according to multiple scientific researches, reiteration is the best way to learn. For this reason, TECH offers between 8 and 16 repetitions of each key concept within the same lesson, presented in a different way, with the objective of ensuring that the knowledge is completely consolidated during the study process.

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



## A 100% online Virtual Campus with the best teaching resources

In order to apply its methodology effectively, TECH focuses on providing graduates with teaching materials in different formats: texts, interactive videos, illustrations and knowledge maps, among others. All of them are designed by qualified teachers who focus their work on combining real cases with the resolution of complex situations through simulation, the study of contexts applied to each professional career and learning based on repetition, through audios, presentations, animations, images, etc.

The latest scientific evidence in the field of Neuroscience points to the importance of taking into account the place and context where the content is accessed before starting a new learning process. Being able to adjust these variables in a personalized way helps people to remember and store knowledge in the hippocampus to retain it in the long term. This is a model called Neurocognitive context-dependent e-learning that is consciously applied in this university qualification.

In order to facilitate tutor-student contact as much as possible, you will have a wide range of communication possibilities, both in real time and delayed (internal messaging, telephone answering service, email contact with the technical secretary, chat and videoconferences).

Likewise, this very complete Virtual Campus will allow TECH students to organize their study schedules according to their personal availability or work obligations. In this way, they will have global control of the academic content and teaching tools, based on their fast-paced professional update.



*The online study mode of this program will allow you to organize your time and learning pace, adapting it to your schedule"*

### The effectiveness of the method is justified by four fundamental achievements:

1. Students who follow this method not only achieve the assimilation of concepts, but also a development of their mental capacity, through exercises that assess real situations and the application of knowledge.
2. Learning is solidly translated into practical skills that allow the student to better integrate into the real world.
3. Ideas and concepts are understood more efficiently, given that the example situations are based on real-life.
4. Students like to feel that the effort they put into their studies is worthwhile. This then translates into a greater interest in learning and more time dedicated to working on the course.



### The university methodology top-rated by its students

The results of this innovative teaching model can be seen in the overall satisfaction levels of TECH graduates.

The students' assessment of the teaching quality, the quality of the materials, the structure of the program and its objectives is excellent. Not surprisingly, the institution became the top-rated university by its students according to the global score index, obtaining a 4.9 out of 5.

*Access the study contents from any device with an Internet connection (computer, tablet, smartphone) thanks to the fact that TECH is at the forefront of technology and teaching.*

*You will be able to learn with the advantages that come with having access to simulated learning environments and the learning by observation approach, that is, Learning from an expert.*



As such, the best educational materials, thoroughly prepared, will be available in this program:



#### 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.

This content is then adapted in an audiovisual format that will create our way of working online, with the latest techniques that allow us to offer you high quality in all of the material that we provide you with.



#### Practicing Skills and Abilities

You will carry out activities to develop specific competencies and skills in each thematic field. Exercises and activities to acquire and develop the skills and abilities that a specialist needs to develop within the framework of the globalization we live in.



#### Interactive Summaries

We present the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

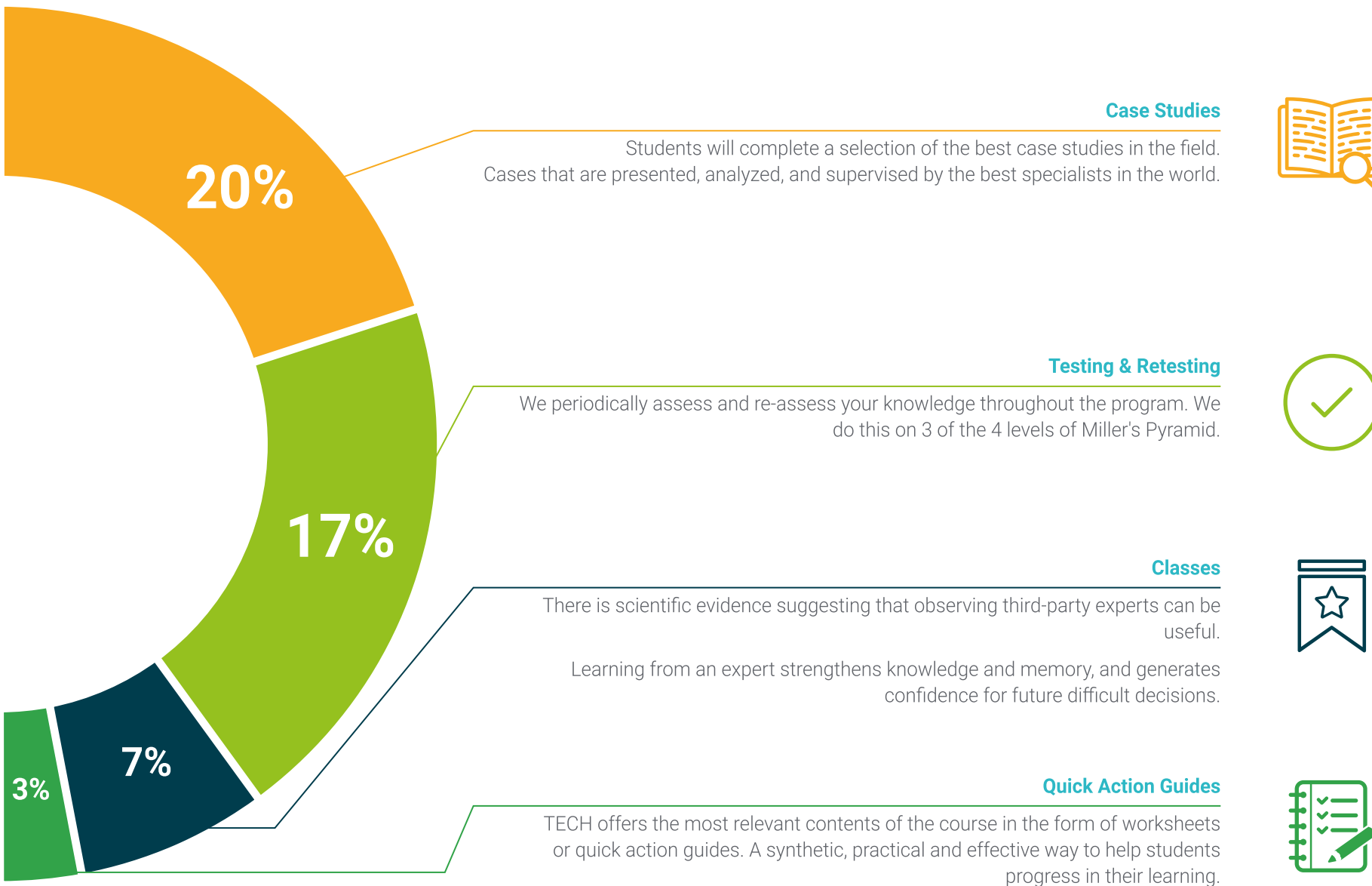
This exclusive educational system for presenting multimedia content was awarded by Microsoft as a "European Success Story".



#### Additional Reading

Recent articles, consensus documents, international guides... In our virtual library you will have access to everything you need to complete your education.







# 06 Certificate

The Postgraduate Certificate in Computer Security Incident Management guarantees students, in addition to the most rigorous and up-to-date education, access to a diploma for the Postgraduate Certificate issued by TECH Global University.



“

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

This private qualification will allow you to obtain a diploma for the **Postgraduate Certificate in Computer Security Incident Management** endorsed by **TECH Global University**, the world's largest online university.

**TECH Global University**, is an official European University publicly recognized by the Government of Andorra ([official bulletin](#)). Andorra is part of the European Higher Education Area (EHEA) since 2003. The EHEA is an initiative promoted by the European Union that aims to organize the international training framework and harmonize the higher education systems of the member countries of this space. The project promotes common values, the implementation of collaborative tools and strengthening its quality assurance mechanisms to enhance collaboration and mobility among students, researchers and academics.

This **TECH Global University private qualification**, is a European program of continuing education and professional updating that guarantees the acquisition of competencies in its area of knowledge, providing a high curricular value to the student who completes the program.

Title: **Postgraduate Certificate in Computer Security Incident Management**

Modality: **online**

Duration: **6 weeks**

Accreditation: **6 ECTS**







## Postgraduate Certificate Computer Security Incident Management

- » Modality: online
- » Duration: 6 weeks
- » Certificate: TECH Global University
- » Accreditation: 6 ECTS
- » Schedule: at your own pace
- » Exams: online

# Postgraduate Certificate Computer Security Incident Management