COURSE Catalog

The growing increase in cyberattacks by cybercriminals globally puts organizations and people in situations of risk and real threats, at **Capa8®**, aware of this reality, we have created a collection of courses whose main objective is to develop in people the talents necessary to apply skills that strengthen information security and cybersecurity in their organizations, through two objectives:

1. Support people who have the necessary cybersecurity knowledge and skills to carry out their duties; regardless of their profile, role or responsibility within technological environments.

2. Support organizations by enabling their employees as the organization's first firewall capable of protective behavior, with skills to identify abnormal activities within its range of operation and knowledge; and respond and communicate appropriately during and after the incident.

This is our catalog of courses, courses that can be adapted to the needs of each organization either remotely or on site and with flexible hours, among others.

Index

OWASP (TOP10)

Objective:

This course focuses on information technology professionals and aims to cover the following key points:
To be able to carry out vulnerability analysis processes on web platforms.
The participant will be able to perform static and dynamic code analysis tests.
The participant will have access to security testing methodologies based on the best practices established by the market.
Detect, test, and remediate security flaws based on automated and manual tests.
The participant will issue recommendations based on the mitigation and remediation of the findings resulting from vulnerability analysis or penetration testing.

COMPTIA A + 220-901

Objective:

This CompTIA A+ certification course will teach you the fundamentals. At the end of the course the user will be able to:

- Identify the types and characteristics of PC, laptop, and mobile device components, including motherboard, CPU, memory and storage, input and output devices.
- Install, configure and troubleshoot peripheral devices and system components; print device problems; wireless and wired LAN link problems and Internet access devices.

COMPTIA A + 220-902

Objective:

This CompTIA A+ certification course will teach you the fundamentals of installing, configuring and troubleshooting PCs, mobile devices, printers and network devices' hardware, helping you advance your career in PC support. Upon completion of this course, the student will be able to:

- Install, configure and troubleshoot Microsoft Windows, Linux and OS X PC operating systems plus iOS, Android, and Windows mobile devices.
- Configure and manage the network connectivity of PC, and mobile devices, in addition to users, groups and shared resources in a typical SOHO network.
- Use antivirus tools to prevent and recover from malware infections.
- Configure access control measures such as authentication, security policy, encryption, and firewalls.
- Perform essential PC maintenance while working safely and responsibly and communicating effectively with customers.

CCNA ROUTING AND SWITCHING

Objective:

The CCNA Routing & Switching course provides a global vision of the concepts, and knowledge on networks, from network applications to protocols, and services provided by these lower network layers' applications. Upon completion of this course, the student will be able to:

- Develop practical knowledge on routing, switching, network applications, protocols,
- Hands-on experience without complications.
- Organization of ICND1 and ICND2.
- Develop the skill to use Cisco networking devices.
- The students will have the knowledge and skills to take five certification exams: TestOut Routing Pro, TestOut Switching Pro, Cisco ICND1 (100-105), Cisco ICND2 (200-105), and the Cisco CCNA (200-125) exam.

CERTIFIED NETWORK DEFENDER

Objective:
This course focuses on information technology professionals and aims to cover the following key points:

- The student will learn about controls, protocols, devices, and network security. Participants will be able to prevent common network problems and improve the network-based attacks' detection.
- The student will be able to detect network threats promptly.
- The student will be able to design efficient network models using devices and their management.
- The student will become aware of the importance of physical security and establishing controls for the organization.
- Suitable and cost-benefit selection of network security devices.
- Successfully implementing a VPN solution.
- The student will identify various threats to wireless technology and learn how to mitigate them.

CERTIFIED ETHICAL HACKER V9

Objective:
This course focuses on information technology professionals and aims to cover the following key points:

- To be able to carry out vulnerability analysis processes.
- To be able to perform perimeter penetration tests.
- To have access to security testing methodologies based on the best practices established by the market.
- Detect, test, and remediate security flaws based on automated and manual tests' results.
- The participant will be able to issue recommendations based on the mitigation and remediation of the findings resulting from vulnerability analysis or penetration testing.

CERTIFIED HACKING FORENSIC INVESTIGATOR V9

Objective:

This course focuses on information technology professionals and aims to cover the following key points:

- The participant will be able to respond to technological incidents.
- Perform thorough examinations of hard disk drives and other electronic data storage devices.
- Recovering information and electronic data from hard disks and other data storage devices.
- Follow data structures and test handling procedures.
- Preserve the chain of custody and evidence integrity.
- Work on investigation-based technical review, analysis, and reporting of evidence.
- Use forensic tools and research methods to find electronic data, including Internet usage history, word processors' documents, images, and other files.
- Perform as first responders against incidents and assess a cybercrime scene, conduct preliminary interviews, document the crime scene, collect and preserve electronic evidence, pack and transport electronic evidence, and report the crime scene.
- Extract and analyze logs from various devices such as proxies, firewalls, IPSec, IDEas, desktops and laptops, servers, SIM tools, routers, AD servers, DHCP servers, access control systems, etc.
- Conduct a detailed evaluation of the data and any evidence of activity to analyze the full circumstances and consequences of the event.
- Ensure that reported incidents or suspected weaknesses, malfunctions, and deviations are handled with the expected level of confidentiality.
- Data collection using forensic technology methods in accordance with evidence handling procedures (including the collection of hard copy and electronic documents) as part of an investigation process.
- Archive temporary MAC data (dates and times modified, accessed, and created) as evidence of access and sequences of events.
- Crack (or attempted crack) of password-protected files.

STATIC AND DYNAMIC APPLICATION SECURITY TESTING

Objective:

This course focuses on cybersecurity professionals, is an analysis combining DAST and SAST, and aims to cover the following key points:

- Correlate and verify SAST analysis results and problems.
- Learn the different technologies designed to analyze the application source, byte, and binary codes.
- Identify coding and design conditions indicative of security vulnerabilities.
- Detect SAST and DAST solutions suitable for application analysis.
- Identify the appropriate tool for application analysis. When a tool is required, for it not to be run from the inside out in one state.
- Design safer software architectures that minimize vulnerabilities as much as possible.
- Define security checkpoints to ensure that systems going into operation meet the minimum thresholds.
- Create a philosophy to develop and maintain software under the scope of cybersecurity.

OFFENSIVE SECURITY CERTIFIED PROFESSIONAL

Objective:

This course focuses on information technology professionals and aims to cover the following key points:

- Use multiple information gathering techniques to identify and enumerate objectives running various operating systems and services.
- Create basic scripts and tools for the penetration testing process.
- Analyze, correct, modify, cross-compile, and carry the code for public exploitation.
- Successfully perform remote and client-side attacks.
- Identify and exploit XSS, SQL injection, and file attachment vulnerabilities in web applications.
- Implement tunneling techniques to bypass firewalls.
- Demonstrate creative problem solving and lateral thinking.

MOBILE FORENSICS FUNDAMENTALS

Objective:

The Course of Mobile Forensics Fundamentals (CMFF) is designed for researchers to identify mobile device hardware and understand the general forensic process. Students will learn how the four phases of the forensic analysis process are related and demonstrate how to handle devices while following best practices. Students will also perform basic analysis of data extracted from the device and generate reports using UFED Reader software.

Upon successful completion of this course, the student will be able to:

- Identify mobile devices' hardware.
- Talk about how devices communicate.
- Describe the four phases of the digital forensics process.
- Describe the importance of tests and documentation practice.
- Describe the tools and techniques for acquiring data from mobile devices.
- Define the types of data encryption used on mobile devices.

CERTIFIED PHYSICAL ANALYST

Objective:

The Certified Course of Physical Analyst (CCPA) is an advanced program designed for technically savvy researchers, digital evidence analysts, and forensic professionals. Since this course focuses on advanced analytics and search techniques using UFED Physical Analyzer, participants will perform extractions with the products. UFED Physical Analyzer software is widely used to explore recovered suppressed data, database content, advanced search and analysis techniques, verification and validation, and report generation.

Upon successful completion of this course, the student will be able to:

- Perform forensic analysis of advanced mobile devices using UFED Physical Analyzer.
- Employ techniques to authenticate and validate data analyzed and collected as
- Identify the physical analyzer software functions that may allow the examination of different types of data.
- Recognize the capabilities of the physical analyst to generate customized reports in an organized manner.
- Demonstrate mastery of the previously stated learning objectives by passing an evaluation on knowledge and practical skills with a score of 80% or higher.

CERTIFIED MOBILE EXAMINER

Objective:

Through the Certified Mobile Examiner, the candidate will improve the practical skills that will allow them to demonstrate their ability to analyze a known data set by applying the digital forensic best practices, concepts, and data analysis methodologies.
The CCME program is the final curriculum for the mobile forensic track. This program is designed to measure the knowledge, skills, and abilities of certification candidates based on the completion of time-limited practical exercises and knowledge-based supervision.

Upon successful completion of this course, the student will be able to:

- Achieve proficiency in the discipline of mobile device forensic investigation methodology.
- Achieve high-level proficiency while using Physical Analyzer software.
- Demonstrate basic knowledge, knowledge on tools, and hands-on experience using two popular mobile device operating systems, including Android and iOS.

COURSE REQUIREMENTS:

It's required that students present courses and demonstrate knowledge on the following:
- Mobile Forensics Fundamentals (CMFF).
- Operator Certificate (CCO).
- Certified Physical Analyst (CCPA).

ADVANCED PENETRATION TESTING

Objective:

The course will teach you how to perform a professional security test and produce the most crucial part of a test: the findings and the report. Upon successful completion of this course, the student will be able to:

- Analyze a variety of targets using a systematic process for professional safety testing.
- Identify the organization's risk level according to the systems and software found.

- Identify critical components susceptible to attack.
- Identify the defenses in place and bypass them.
- Create a professional safety report.
- Have a replicable and measurable approach to penetration tests.
- Perform advanced techniques and attack simulations to identify SQL injection, cross-site scripting (XSS), LFI, and RFI vulnerabilities in web applications.
- Obtain proprietary penetration testing methodologies.
- Exploit vulnerabilities in operating systems such as Windows or Linux.
- Rise the privileges to gain root access to a system.

ADVANCED MOBILE FORENSIC AND SECURITY

Objective:
This course provides students with the knowledge and practical skills to perform Mobile Forensic Investigations. The course is based on digital forensics principles, focusing heavily on Apple, Google, Android, and other mobile devices. Upon successful completion of this course, the student will be able to:

- Acquire digital forensics' fundamental processes, principles, and methodologies.
- To acquire the necessary knowledge to obtain evidence and final reports.
- Technical aspects of Mobile Forensics.
- Mobile OSX architecture.
- Evidence acquisition.
- Password circumvention.
- Weaknesses of iOS, Android, and Blackberry platforms' weaknesses.

WEB APPLICATION SECURITY

Objective:

This course is designed to encourage the programmer's security awareness. Upon successful completion of this course, the student will be able to:

- Learn practical coding.
- Increase your cyber awareness.
- Respond to any security breach.
- Keeping up to date with the latest security threats.
- Protection of the company's environment.
- Identify security flaws.

ADVANCED NETWORK DEFENSE

Objective:

This course builds an offensive mindset to arrange strong defenses skillfully and reinvent yourself. You will cover fundamental areas to strengthen your defenses by discovering methods to develop a secure baseline and how to fortify your enterprise architecture against the most advanced attacks. The course aims to cover the following key points:

- Learning to evaluate advanced hacking methods to strengthen your defense.
- Best practices and security methodologies.
- Apply practices in safe environments.
- Provide segmentation and isolation to reduce the effectiveness of advanced persistent threats.
- Obtain defenses against sophisticated malware.
- Memory analysis in real-time.
- Monitoring in real-time.

CERTIFIED INFORMATION SECURITY MANAGER

Objective:

The course provides tools to design, build, and manage company information security programs, offering effective security management and continuous assessment. Upon completion of this course, the student will be able to:

- Identify critical issues and customize specific practices to support IT governance.
- Obtain a comprehensive view of information systems security management and its connection to organizational success.
- Demonstrate commitment to compliance, safety, and integrity and attract and keep customers.
- Align the organization's information security programs with its objectives.
- Provide the organization with the fundamentals for international information security management certification.

CERTIFIED INFORMATION SECURITY AUDITOR

Objective:

Provide professionals with the skills needed to perform information systems audit, control, and security functions. They will obtain the experience and proven knowledge to identify and evaluate risks and provide advice to achieve solutions that minimize these systems' vulnerabilities. Upon completion of this course, the student will be able to:

- Assess vulnerabilities, generate compliance reports, and establish organizational controls. It confirms your knowledge and experience.
- Achieve high professional standards for continuing education and ethical conduct.
- Use technological controls to develop productivity indicators.
- Acquire skills in domains including standards and practices: organization, management, processes, integrity, confidentiality, availability, and software development, acquisition, and maintenance.
- Assess vulnerabilities, generate compliance reports, and establish controls within the organization. Confirm your knowledge and experience.
- Demonstrate a commitment to provide the company with the confidence and value of its information systems.

SOCIAL ENGINEERING

Objective:

Professionals will be able to identify illicit techniques to obtain confidential information; they will be able to prevent and carry out their treatment. This course focuses on information technology security. Upon completion of this course, the student will be able to:

- Prevent information and identity theft.
- Check for FALSE URLs or URLs with malicious code.
- Prevent and identify hacking attacks.
- Identify apocryphal e-mail messages.
- Preventing and identifying apocryphal telephone calls.
- Identify apocryphal cell phone messages.
- Treatment and identification of false advertising.
- Treatment and identification of false questionnaires
- Understand how phishing and phishing techniques work.

CISO, WHAT'S ITS SCOPE AND VALUE WITHIN THE ORGANIZATION?

Objective:

We aim to provide the key elements that Chief Information Security Officers, new or experienced, must address when inheriting an immature cyber security program or building a new cyber security program. We expect Chief Technology Officers (CTOs) and Chief Information Officers (CIOs), and their colleagues in the C-suite, to also benefit from these concepts and, as a result, become the CISO's best "partners."

Description:

CISO. The "Chief Information Security Officer" (CISO) position is relatively new to the industry, and there is a lack of institutionalized support. Nowadays, many organizations are still figuring out exactly what a CISO does and how to incorporate their functions within their organizations best. Currently, the demand for talented CISOs is much higher than the supply, and the turnover rate is high. As companies become more digitally interconnected, entire industries that in the past didn't think they would need a robust information security program are now forced to have one and catch up.

PARTICULARITIES OF SPEI, SPID, CODI, AND WIRE TRANSFER DATABASE

Description:

The main operational aspects of SPEI and SPID, as well as Banco de México's Transfer Database (BDT by its initials in Spanish) are described through a functional and applied perspective. Regarding SPEI, SPID and CoDi, the objective is to understand their background, the parties involved, and their operating procedures, flows, controls, modules, settlement, and synchronization. Regarding Banxico's Transfer Database (BDT), the objective is to know its purpose, its recent evolution, and the most recent operational and regulatory changes.

FUNDAMENTALS OF MONEY LAUNDERING PREVENTION

Description:

- KNOW the importance of preventing, detecting, and reporting money laundering and terrorist financing.
- IDENTIFY the origin of illicit resources.
- AVOID social, financial, and economic impacts of illicit resources.

FFINTECH – FUNDAMENTALS. HOW TO START AND OBTAIN THE AUTHORIZATION?

Description:

We will review the applications and implications of financial technology in today's financial sector operations. How do I initiate and obtain authorization, how does it affect the organization, how do I prepare for it, how do I take advantage of it?

PCI – DSS COMPLIANCE EVALUATION

Objective:

The student will learn about the Payment Card Industry Data Security Standard (PCI DSS) and the evaluation criteria that will allow them to determine the level of compliance with the standard in an entity involved in payment card processing.

PCI DSS was developed to promote and enhance the security of cardholder data and facilitate the adoption of uniform security measures globally. It provides a reference of technical and operational requirements developed to protect account data. It applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all entities that store, process, or transmit Cardholder Data (CHD) and/or Sensitive Authentication Data (SAD).

Upon completion of this course, the student will be able to:

1 . Know the requirements of the applicable standard.
2. Determine a PCI DSS evaluation's scope.
3. Conduct the PCI DSS evaluation in a live environment and in accordance with the testing procedures for each requirement.
4. Generate the appropriate evaluation report, including documentation of all compensating controls, in accordance with the applicable PCI guides and instructions.

COURSE REQUIREMENTS

The student should demonstrate previous knowledge on:

- Information systems and computing infrastructure.
- Communications' networks.
- Algoritmos de cifrado
- Encryption algorithm