Esperto Universitario
Cibersicurezza Offensiva

tech global university

tech global university

Esperto Universitario
Cibersicurezza Offensiva

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Global University**
- Accreditamento: **18 ECTS**
- Orario: **a scelta**
- Esami: **online**

Accesso al sito web: www.techtitute.com/it/informatica/specializzazione/specializzazione-cibersicurezza-offensiva

Indice

01

Presentazione

La cibersicurezza è essenziale per le istituzioni per proteggere i loro beni digitali, mantenere la loro reputazione sociale e salvaguardarsi dallo spionaggio da parte della concorrenza. Di conseguenza, un numero sempre maggiore di aziende richiede l'ingresso di esperti informatici nella propria organizzazione per evitare conseguenze che potrebbero persino compromettere le loro capacità finanziarie. In questo contesto, questi specialisti devono aggiornare costantemente le loro conoscenze e competenze per rimanere al passo con le tecniche di criminalità informatica. Per questo motivo, TECH ha sviluppato un innovativo programma di formazione universitaria, in cui le minacce saranno identificate e mitigate. Va notato che l'intero programma sarà insegnato in modalità 100% online, per garantire agli studenti una maggiore comodità e flessibilità.

Approfondirai la conoscenza del protocollo Kerberos e proteggerai le informazioni in ambienti di rete"

Ogni giorno i media riportano casi di hacker che danneggiano le istituzioni accedendo ai loro database. Le conseguenze di questi attacchi sono gravi, in quanto interrompono le operazioni e impediscono alle aziende di funzionare efficacemente. Possono infatti avere un impatto diretto sull'economia delle aziende, causando multe per la mancata conformità alle normative e limitando i ricavi.

A questo proposito, TECH ha creato un corso all'avanguardia per individuare le tecniche di intrusione più comunemente utilizzate, nonché le strategie più ottimali per affrontarle. Sotto la guida di un personale docente esperto del settore, il programma di studio getterà le basi essenziali per capire come pensano gli hacker. Fornirà inoltre una serie di soluzioni volte a fornire infrastrutture sicure per la gestione dei certificati digitali su una rete aziendale.

I professionisti impareranno anche a preparare in modo ottimale gli ambienti virtuali, grazie alla configurazione di macchine virtuali o di snapshot. Inoltre, verrà analizzato il malware, sondando le chiamate con API Monitor e osservando le richieste di rete con TCPView. Gli studenti apprenderanno i concetti teorici in ambienti simulati, preparandosi alle sfide del mondo reale nell'ambito della Cibersicurezza Offensiva. Infine, si porrà l'accento sull'etica e sulla responsabilità sociale che dovrebbero caratterizzare gli esperti di questo settore.

Per consolidare la padronanza di tutti questi contenuti, l'Esperto Universitario applica l'innovativo sistema Relearning. TECH è pioniere nell'utilizzo di questo modello didattico, che favorisce l'assimilazione di concetti complessi attraverso la loro naturale e progressiva reiterazione. Il programma utilizza anche materiali in vari formati, come video esplicativi, riassunti interattivi e infografiche. Tutto questo in una comoda modalità 100% online, che permette di adattare l'orario di ogni persona ai suoi impegni e disponibilità.

Questo **Esperto Universitario in Cibersicurezza Offensiva** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- Sviluppo di casi pratici presentati da esperti in Cibersicurezza Offensiva
- Contenuti grafici, schematici ed eminentemente pratici che forniscono informazioni complete e pratiche sulle discipline essenziali per l'esercizio della professione
- Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- Particolare enfasi sulle metodologie innovative
- Lezioni teoriche, domande all'esperto e/o al tutor, forum di discussione su questioni controverse e compiti di riflessione individuale
- Contenuti disponibili da qualsiasi dispositivo fisso o mobile dotato di connessione a internet

Sviluppa le tue competenze come auditor offensivo e intraprendi una nuova sfida professionale nelle più prestigiose aziende digitali"

Raggiungerai i tuoi obiettivi grazie agli strumenti didattici di TECH, tra cui video esplicativi e sintesi interattive"

Vuoi diventare un Big Bounty Hunter? Grazie a questo programma potrai individuare qualsiasi vulnerabilità su Internet.

In soli 6 mesi padroneggerai la gestione delle identità in Azure AD. Iscriviti subito!.

Il personale docente del programma comprende rinomati professionisti e riconosciuti specialisti appartenenti a prestigiose società e università, che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

I contenuti multimediali, sviluppati in base alle ultime tecnologie educative, forniranno al professionista un apprendimento coinvolgente e localizzato, ovvero inserito in un contesto reale.

La creazione di questo programma è incentrata sull'Apprendimento Basato su Problemi, mediante il quale il professionista deve cercare di risolvere le diverse situazioni che gli si presentano durante il corso. Lo studente potrà usufruire di un innovativo sistema di video interattivi creati da esperti di rinomata fama.

02

Obiettivi

Il progetto di questo programma offre un'esperienza formativa unica, che si distingue per l'approccio pratico e innovativo alla Cibersicurezza. In questo modo, gli studenti affronteranno dall'analisi delle vulnerabilità alle tecniche di intrusione avanzate. In questa linea, verranno offerte le misure ottimali per valutare e rafforzare i diversi sistemi cibernetici. Inoltre, si porrà l'accento sulle responsabilità legali ed etiche che gli esperti del settore dovrebbero adottare.

Riduci le minacce di malware con la migliore università digitale del mondo, secondo Forbes"

Obiettivi generali

- Acquisire competenze avanzate nei test di penetrazione e nelle simulazioni di *Red Team*, affrontando l'identificazione e lo sfruttamento delle vulnerabilità di sistemi e reti
- Sviluppare capacità di leadership per coordinare team specializzati nella cibersicurezza offensiva, ottimizzando l'esecuzione di progetti di *Pentesting*e *Red Team*
- Sviluppare competenze nell'analisi e nello sviluppo di malware, comprendendone le funzionalità e applicando misure difensive ed educative
- Affinare le capacità di comunicazione producendo relazioni tecniche ed esecutive dettagliate, presentando i risultati in modo efficace a un pubblico tecnico ed esecutivo
- Promuovere una pratica etica e responsabile nel campo della sicurezza informatica, tenendo conto dei principi etici e legali in tutte le attività
- Mantenere gli studenti aggiornati sulle tendenze e le tecnologie emergenti nel campo della cibersicurezza

Obiettivi specifici

Modulo 1. Sicurezza Offensiva

- Familiarizzare con le metodologie di penetration testing, comprese le fasi chiave quali la raccolta di informazioni, l'analisi delle vulnerabilità, lo sfruttamento e la documentazione
- Sviluppare competenze pratiche nell'uso di strumenti di *Pentesting* per identificare e valutare le vulnerabilità di sistemi e reti
- Studiare e comprendere le tattiche, le tecniche e le procedure utilizzate dagli attori malintenzionati, consentendo l'identificazione e la simulazione delle minacce
- Applicare le conoscenze teoriche in scenari pratici e simulazioni, affrontando sfide reali per rafforzare le competenze di *Pentesting*
- Sviluppare un'efficace capacità di documentazione, creando relazioni dettagliate che riflettano i risultati, le metodologie utilizzate e le raccomandazioni per il miglioramento della sicurezza
- Praticare una collaborazione efficace nei team di sicurezza offensiva, ottimizzando il coordinamento e l'esecuzione delle attività di *Pentesting*

Modulo 2. Attacchi alla Rete e al Sistema Windows

- Sviluppare le competenze per identificare e valutare le vulnerabilità specifiche dei sistemi operativi Windows
- Imparare le tattiche avanzate utilizzate dagli aggressori per infiltrarsi e persistere nelle reti basate su Windows
- Acquisire competenze sulle strategie e sugli strumenti per mitigare le minacce specifiche che colpiscono i sistemi operativi Windows
- Familiarizzare con le tecniche di analisi forense applicate ai sistemi Windows, facilitando l'identificazione e la risposta agli incidenti
- Applicare le conoscenze teoriche in ambienti simulati, partecipando a esercitazioni pratiche per comprendere e contrastare attacchi specifici ai sistemi Windows

- Apprendere strategie specifiche per la sicurezza degli ambienti aziendali utilizzando i sistemi operativi Windows, tenendo conto della complessità delle infrastrutture aziendali
- Sviluppare competenze per valutare e migliorare le configurazioni di sicurezza dei sistemi Windows, garantendo l'implementazione di misure efficaci
- Promuovere pratiche etiche e legali nell'esecuzione di attacchi e test su sistemi Windows, tenendo conto dei principi etici della cibersicurezza
- Mantenere lo studente aggiornato sulle ultime tendenze e minacce in materia di attacchi ai sistemi Windows, garantendo la continuità della sicurezza

Modulo 3. Analisi e Sviluppo di *Malware*

- Acquisire una conoscenza avanzata della natura, della funzionalità e del comportamento del *malware*, comprendendone le varie forme e gli obiettivi
- Sviluppare competenze nell'analisi forense applicata al *malware*, consentendo l'identificazione degli indicatori di compromissione (IoC) e dei modelli di attacco
- Apprendere strategie per il rilevamento e la prevenzione efficace di *malware*, compresa l'implementazione di soluzioni di sicurezza avanzate
- Familiarizzare con lo sviluppo di *malware* a scopo educativo e difensivo, consentendo una comprensione approfondita delle tattiche utilizzate dagli hacker
- Promuovere pratiche etiche e legali nell'analisi e nello sviluppo di malware, garantendo integrità e responsabilità in tutte le attività
- Promuovere pratiche etiche e legali nell'analisi e nello sviluppo di malware, garantendo integrità e responsabilità in tutte le attività
- Sviluppare le competenze per valutare e selezionare gli strumenti di sicurezza *anti-malware*, considerando la loro efficacia e adattabilità ad ambienti specifici
- Imparare a implementare una mitigazione efficace contro le minacce dannose, riducendo l'impatto e la diffusione del malware su sistemi e reti
- Promuovere una collaborazione efficace con i team di sicurezza, integrando strategie e sforzi per la protezione dalle minacce *malware*
- Aggiornarsi sulle ultime tendenze e tecniche utilizzate nell'analisi e nello sviluppo di *malware*, assicurando la continua rilevanza ed efficacia delle competenze acquisite

Dimenticati di memorizzare! Con il sistema Relearning integrerai i concetti in modo naturale e progressivo"

03

Direzione del corso

Nel suo impegno nell'offrire l'eccellenza didattica, TECH si avvale di un personale docente di prestigio. Va sottolineato che questi specialisti hanno un ampio background professionale, avendo fatto parte di rinomate aziende dedicate alla Cibersicurezza Offensiva. Per questo motivo, il percorso accademico includerà le risorse e le tecnologie più avanzate in questo campo. Inoltre, verrà offerto un approccio completo per soddisfare le aspettative degli studenti di specializzarsi in un campo che offrirà loro molte opportunità.

Avrai il supporto di un personale docente composto da illustri professionisti della Cibersicurezza Offensiva"

Direzione

Dott. Gómez Pintado, Carlos

- Responsabile di Cibersicurezza e Rete Cipherbit presso Grupo Oesía
- Responsabile *Advisor & Investor* presso Wesson App
- Laurea in Ingegneria del Software e Tecnologie della Società dell'Informazione, Università Politecnica di Madrid
- Collabora con istituzioni educative per la preparazione di cicli di formazione di livello superiore in materia di cibersicurezza

Personale docente

Dott. González Parrilla, Yuba

- Coordinatore della linea di sicurezza offensiva e del team di rete
- Specialista in Gestione di Progetti *Predictive* nel Project Management Institute
- Specialista in *SmartDefense*
- Esperto in *Web Application Penetration Tester* presso eLearnSecurity
- *Junior Penetration Tester* presso eLearnSecurity
- Laurea in Ingegneria Computazionale presso l'Università Politecnica di Madrid

Dott. Gallego Sánchez, Alejandro

- Pentester presso Grupo Oesía
- Consulente di Cibersicurezza presso Integración Tecnológica Empresarial, S.L.
- Tecnico audiovisivo presso Ingeniería Audiovisual S.A.
- Laurea in Ingegneria dei della Cibersicurezza presso l'Università Rey Juan Carlos

04

Struttura e contenuti

Questo programma è strutturato in 3 moduli: Sicurezza Offensiva, Attacco alle Reti o ai Sistemi Windows e Analisi e Sviluppo di *Malware*. Nel corso del programma di studi verrà fornita una prospettiva pratica, finalizzata all'individuazione di minacce precoci. In questo senso, la creatività degli studenti sarà incoraggiata a superare le sfide attraverso soluzioni innovative. Inoltre, verrà approfondita la categorizzazione delle vulnerabilità, compresa la CVE. Verranno anche esplorate tecniche avanzate di analisi del *malware*, per rafforzare la sicurezza negli ambienti informatici.

Avrai accesso ad un sistema di apprendimento basato sulla ripetizione, grazie ad un insegnamento semplice e graduale durante l'intero programma"

Modulo 1. Sicurezza Offensiva

1.1. Definizione e contesto
- 1.1.1. Concetti fondamentali della sicurezza offensiva
- 1.1.2. Importanza della cibersicurezza nell'attualità
- 1.1.3. Sfide e opportunità della sicurezza offensiva

1.2. Basi della cibersicurezza
- 1.2.1. Sfide iniziali e minacce in evoluzione
- 1.2.2. Pietre miliari della tecnologia e loro impatto sulla cibersicurezza
- 1.2.3. Cibersicurezza nell'era moderna

1.3. Basi della sicurezza offensiva
- 1.3.1. Concetti chiave e terminologia
- 1.3.2. *Think Outside the Box*
- 1.3.3. Differenze tra hacking offensivo e difensivo

1.4. Metodologie di sicurezza offensiva
- 1.4.1. PTES (*Penetration Testing Execution Standard*)
- 1.4.2. OWASP (*Open Web Application Security Project*)
- 1.4.3. *Cyber Security Kill Chain*

1.5. Ruoli e responsabilità nella sicurezza offensiva
- 1.5.1. Profili principali
- 1.5.2. *Bug Bounty Hunters*
- 1.5.3. *Researching:* L'arte della ricerca

1.6. Arsenale del revisore offensivo
- 1.6.1. Sistemi operativi di hacking
- 1.6.2. Introduzione al C2
- 1.6.3. *Metasploit:* Fondamenti e uso
- 1.6.4. Risorse utili

1.7. OSINT: Intelligenza open source
- 1.7.1. Fondamenti di OSINT
- 1.7.2. Tecniche e strumenti OSINT
- 1.7.3. Applicazioni OSINT nella sicurezza offensiva

1.8. Scripting: Introduzione all'automatizzazione
- 1.8.1. Fondamenti di scripting
- 1.8.2. *Scripting* in Bash
- 1.8.3. *Scripting* in Python

1.9. Categorizzazione delle vulnerabilità
- 1.9.1. CVE (*Common Vulnerabilities and Exposure*)
- 1.9.2. CWE (*Common Weakness Enumeration*)
- 1.9.3. CAPEC (*Common Attack Pattern Enumeration and Classification*)
- 1.9.4. CVSS (*Common Vulnerability Scoring System*)
- 1.9.5. MITRE ATT & CK

1.10. Etica e *hacking*
- 1.10.1. Principi di etica *hacker*
- 1.10.2. La linea tra *hacking* etico e malevolo
- 1.10.3. Implicazioni e conseguenze legali
- 1.10.4. Casi di studio: Situazioni etiche nella cibersicurezza

Modulo 2. Attacchi alla Rete e al Sistema Windows

2.1. Windows e Active Directory
- 2.1.1. Storia ed evoluzione di Windows
- 2.1.2. Nozioni di base di Active Directory
- 2.1.3. Ruoli e servizi di Active Directory
- 2.1.4. Architettura generale di Active Directory

2.2. Networking in ambienti Active Directory
- 2.2.1. Protocolli di rete in Windows
- 2.2.2. DNS e il suo funzionamento in Active Directory
- 2.2.3. Strumenti di siagnosi di rete
- 2.2.4. Implementazione della rete in Active Directory

2.3. Autenticazione e autorizzazione in Active Directory
- 2.3.1. Processo e flusso di autenticazione
- 2.3.2. Tipi di credenziali
- 2.3.3. Archiviazione e gestione dei credenziali
- 2.3.4. Sicurezza nell'autenticazione

2.4. Permessi e Politica in Active Directory
- 2.4.1. GPO
- 2.4.2. Applicazione e gestione delle GPO
- 2.4.3. Gestione dei permessi di Active Directory
- 2.4.4. Vulnerabilità e mitigazioni dei permessi

2.5. Fondamenti di Kerberos
- 2.5.1. Che cos'è Kerberos?
- 2.5.2. Componenti e funzionamento
- 2.5.3. Ticket in Kerberos
- 2.5.4. Kerberos nel contesto di Active Directory

2.6. Tecniche avanzate in Kerberos
- 2.6.1. Attacchi comuni a Kerberos
- 2.6.2. Mitigazioni e protezioni
- 2.6.3. Monitoraggio del traffico Kerberos
- 2.6.4. Attacchi avanzati a Kerberos

2.7. *Active Directory Certificate Services* (ADCS)
- 2.7.1. Nozioni di base sulla PKI
- 2.7.2. Ruoli e componenti di ADCS
- 2.7.3. Configurazione e distribuzione dell'ADCS
- 2.7.4. Sicurezza dell'ADCS

2.8. Attacchi e difese in *Active Directory Certificate Services* (ADCS)
- 2.8.1. Vulnerabilità comuni in ADCS
- 2.8.2. Attacchi e tecniche di utilizzo
- 2.8.3. Difese e mitigazioni
- 2.8.4. Monitoraggio e auditing dell'ADCS

2.9. Audit di Active Directory
- 2.9.1. Importanza dell'audit di Active Directory
- 2.9.2. Strumenti di audit
- 2.9.3. Rilevamento di anomalie e comportamenti sospetti
- 2.9.4. Risposta agli incidenti e recupero

2.10. Azure AD
- 2.10.1. Concetti base di Azure AD
- 2.10.2. Sincronizzazione con Active Directory locale
- 2.10.3. Gestione delle identità in Azure AD
- 2.10.4. Integrazione con applicazioni e servizi

Modulo 3. Analisi e Sviluppo di *Malware*

3.1. Analisi e sviluppo di *Malware*
- 3.1.1. Storia ed evoluzione di *malware*
- 3.1.2. Classificazione e tipi di *malware*
- 3.1.3. Analisi dei *malware*
- 3.1.4. Sviluppo di *malware*

3.2. Preparazione dell'ambiente
- 3.2.1. Configurazione di Macchine Virtuali e *Snapshots*
- 3.2.2. Strumenti di analisi del malware
- 3.2.3. Strumenti di sviluppo del malware

3.3. Fondamenti di Windows
- 3.3.1. Formato dei file PE (*Portable Executable*)
- 3.3.2. Processo e *Threads*
- 3.3.3. Sistemi di archivio e registro
- 3.3.4. *Windows Defender*

3.4. Tecniche di *malware* di base
- 3.4.1. Generazione di *shellcode*
- 3.4.2. Esecuzione di *shellcode* su disco
- 3.4.3. Disco vs memoria
- 3.4.4. Esecuzione di *shellcode* su memoria

3.5. Tecniche di *malware* intermedie
- 3.5.1. Persistenza di Windows
- 3.5.2. Cartella Home
- 3.5.3. Chiavi di registro
- 3.5.4. Screensaver

3.6. Tecniche di *malware* avanzate
- 3.6.1. Crittografia di *shellcode* (XOR)
- 3.6.2. Crittografia di *shellcode* (RSA)
- 3.6.3. Offuscamento di *strings*
- 3.6.4. Iniezione di processi

3.7. Analisi statica dei *malware*
- 3.7.1. Analisi dei *packers* con DIE (*Detect It Easy*)
- 3.7.2. Analisi delle sezioni con PE-Bear
- 3.7.3. Decompilazione con Ghidra

3.8. Analisi dinamica dei *malware*
- 3.8.1. Analisi del comportamento con Process Hacker
- 3.8.2. Analisi delle chiamate con API Monitor
- 3.8.3. Analisi delle modifiche al registro di sistema con Regshot
- 3.8.4. Analisi delle richieste di rete con TCPView

3.9. Analisi in .NET
- 3.9.1. Introduzione a .NET
- 3.9.2. Decompilazione con dnSpy
- 3.9.3. Debug con dnSpy
- 3.10. Analisi di malware reali

3.10.1. Preparazione dell'ambiente
- 3.10.2. Analisi statica dei *malware*
- 3.10.3. Analisi dinamica dei *malware*
- 3.10.4. Creazione di regole YARA

Nessun orario fisso o valutazioni rigide. Questo è il programma di TECH!"

05

Metodologia

Questo programma ti offre un modo differente di imparare. La nostra metodologia si sviluppa in una modalità di apprendimento ciclico: ***il Relearning***.

Questo sistema di insegnamento viene applicato nelle più prestigiose facoltà di medicina del mondo ed è considerato uno dei più efficaci da importanti pubblicazioni come il ***New England Journal of Medicine.***

Scopri il Relearning, un sistema che abbandona l'apprendimento lineare convenzionale, per guidarti attraverso dei sistemi di insegnamento ciclici: una modalità di apprendimento che ha dimostrato la sua enorme efficacia, soprattutto nelle materie che richiedono la memorizzazione"

Caso di Studio per contestualizzare tutti i contenuti

Il nostro programma offre un metodo rivoluzionario per sviluppare le abilità e le conoscenze. Il nostro obiettivo è quello di rafforzare le competenze in un contesto mutevole, competitivo e altamente esigente.

Con TECH potrai sperimentare un modo di imparare che sta scuotendo le fondamenta delle università tradizionali in tutto il mondo"

Avrai accesso a un sistema di apprendimento basato sulla ripetizione, con un insegnamento naturale e progressivo durante tutto il programma.

Imparerai, attraverso attività collaborative e casi reali, la risoluzione di situazioni complesse in ambienti aziendali reali.

Un metodo di apprendimento innovativo e differente

Questo programma di TECH consiste in un insegnamento intensivo, creato ex novo, che propone le sfide e le decisioni più impegnative in questo campo, sia a livello nazionale che internazionale. Grazie a questa metodologia, la crescita personale e professionale viene potenziata, effettuando un passo decisivo verso il successo. Il metodo casistico, la tecnica che sta alla base di questi contenuti, garantisce il rispetto della realtà economica, sociale e professionale più attuali.

> *Il nostro programma ti prepara ad affrontare nuove sfide in ambienti incerti e a raggiungere il successo nella tua carriera"*

Il Metodo Casistico è stato il sistema di apprendimento più usato nelle migliori Scuole di Informatica del mondo da quando esistono. Sviluppato nel 1912 affinché gli studenti di Diritto non imparassero la legge solo sulla base del contenuto teorico, il metodo casistico consisteva nel presentare loro situazioni reali e complesse per prendere decisioni informate e giudizi di valore su come risolverle. Nel 1924 fu stabilito come metodo di insegnamento standard ad Harvard.

Cosa dovrebbe fare un professionista per affrontare una determinata situazione? Questa è la domanda con cui ti confrontiamo nel metodo dei casi, un metodo di apprendimento orientato all'azione. Durante il corso, gli studenti si confronteranno con diversi casi di vita reale. Dovranno integrare tutte le loro conoscenze, effettuare ricerche, argomentare e difendere le proprie idee e decisioni.

Metodologia Relearning

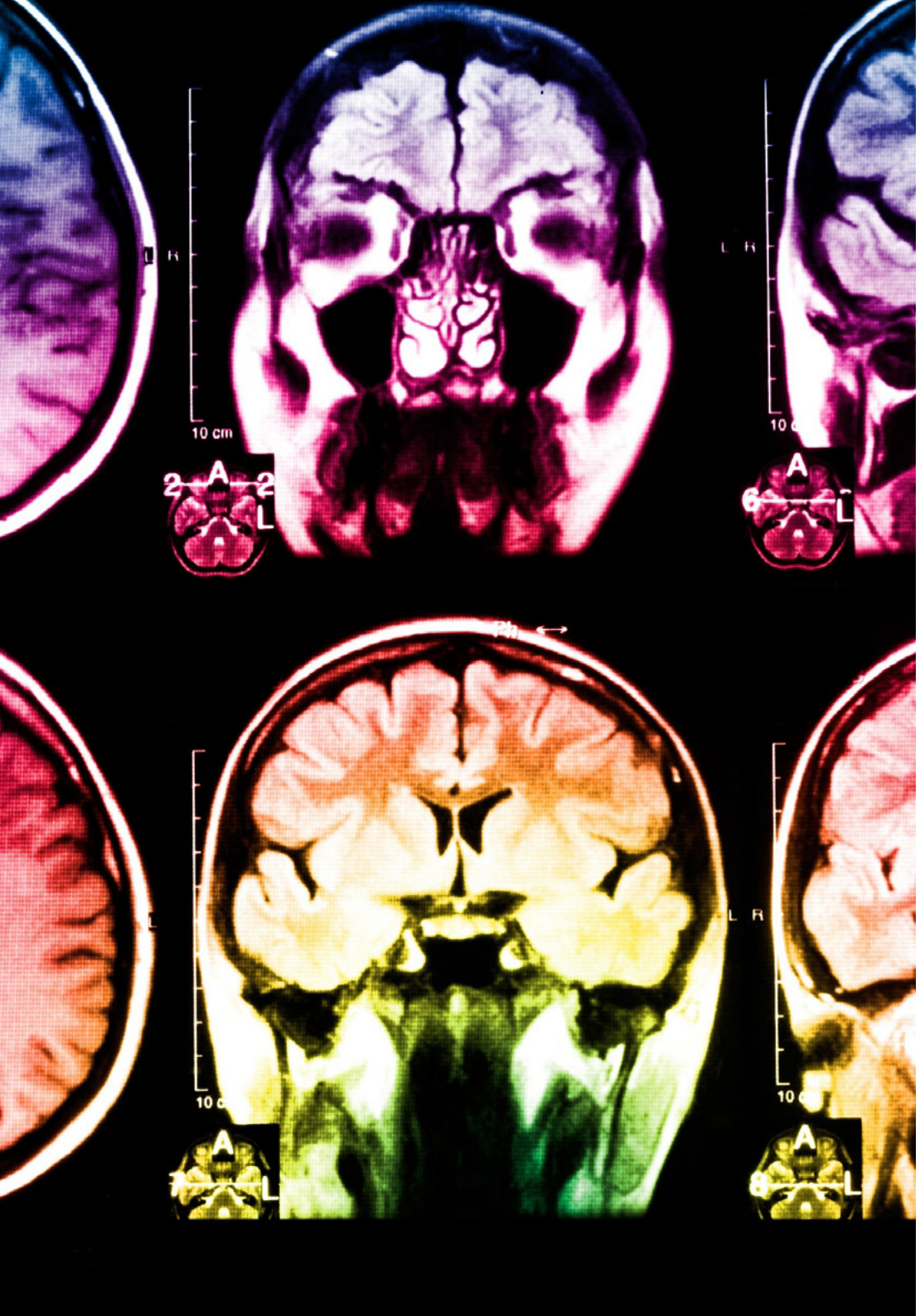
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

Potenziamo il Caso di Studio con il miglior metodo di insegnamento 100% online: il Relearning.

Nel 2019 abbiamo ottenuto i migliori risultati di apprendimento di tutte le università online del mondo.

In TECH imparerai con una metodologia all'avanguardia progettata per formare i manager del futuro. Questo metodo, all'avanguardia della pedagogia mondiale, si chiama Relearning.

La nostra università è l'unica autorizzata a utilizzare questo metodo di successo. Nel 2019, siamo riusciti a migliorare il livello di soddisfazione generale dei nostri studenti (qualità dell'insegnamento, qualità dei materiali, struttura del corso, obiettivi...) rispetto agli indicatori della migliore università online.



Nel nostro programma, l'apprendimento non è un processo lineare, ma avviene in una spirale (impariamo, disimpariamo, dimentichiamo e re-impariamo). Pertanto, combiniamo ciascuno di questi elementi in modo concentrico. Questa metodologia ha formato più di 650.000 laureati con un successo senza precedenti in campi diversi come la biochimica, la genetica, la chirurgia, il diritto internazionale, le competenze manageriali, le scienze sportive, la filosofia, il diritto, l'ingegneria, il giornalismo, la storia, i mercati e gli strumenti finanziari. Tutto questo in un ambiente molto esigente, con un corpo di studenti universitari con un alto profilo socio-economico e un'età media di 43,5 anni.

Il Relearning ti permetterà di apprendere con meno sforzo e più performance, impegnandoti maggiormente nella tua specializzazione, sviluppando uno spirito critico, difendendo gli argomenti e contrastando le opinioni: un'equazione diretta al successo.

Dalle ultime evidenze scientifiche nel campo delle neuroscienze, non solo sappiamo come organizzare le informazioni, le idee, le immagini e i ricordi, ma sappiamo che il luogo e il contesto in cui abbiamo imparato qualcosa è fondamentale per la nostra capacità di ricordarlo e immagazzinarlo nell'ippocampo, per conservarlo nella nostra memoria a lungo termine.

In questo modo, e in quello che si chiama Neurocognitive Context-dependent E-learning, i diversi elementi del nostro programma sono collegati al contesto in cui il partecipante sviluppa la sua pratica professionale.

Questo programma offre i migliori materiali didattici, preparati appositamente per i professionisti:

Materiale di studio

Tutti i contenuti didattici sono creati appositamente per il corso dagli specialisti che lo impartiranno, per fare in modo che lo sviluppo didattico sia davvero specifico e concreto.

Questi contenuti sono poi applicati al formato audiovisivo che supporterà la modalità di lavoro online di TECH. Tutto questo, con le ultime tecniche che offrono componenti di alta qualità in ognuno dei materiali che vengono messi a disposizione dello studente.

Master class

Esistono evidenze scientifiche sull'utilità dell'osservazione di esperti terzi.

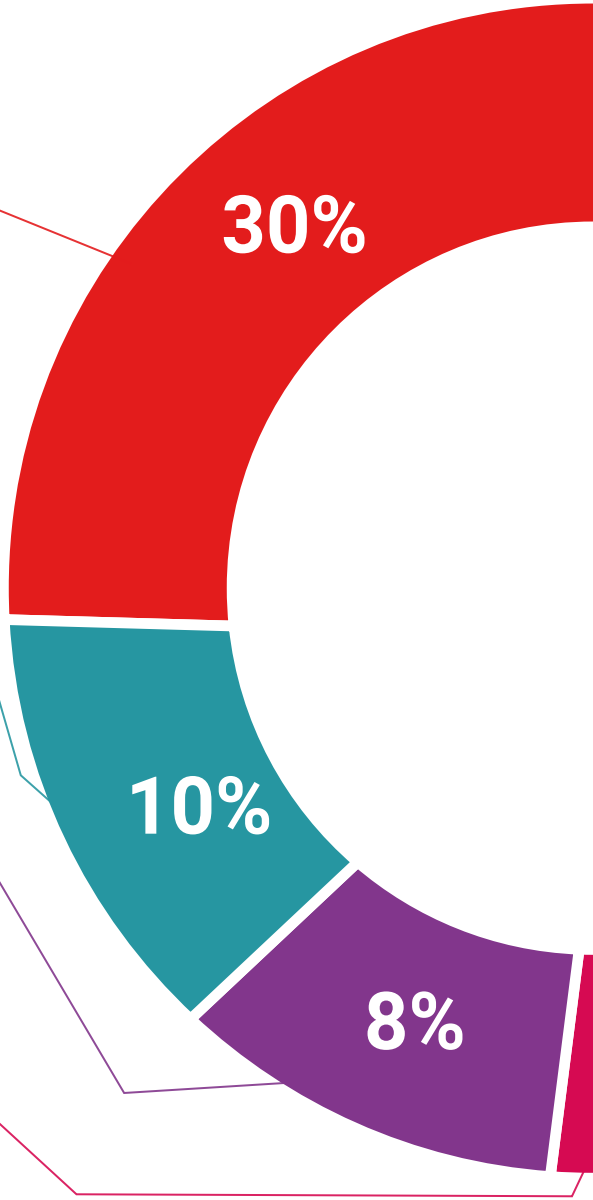
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

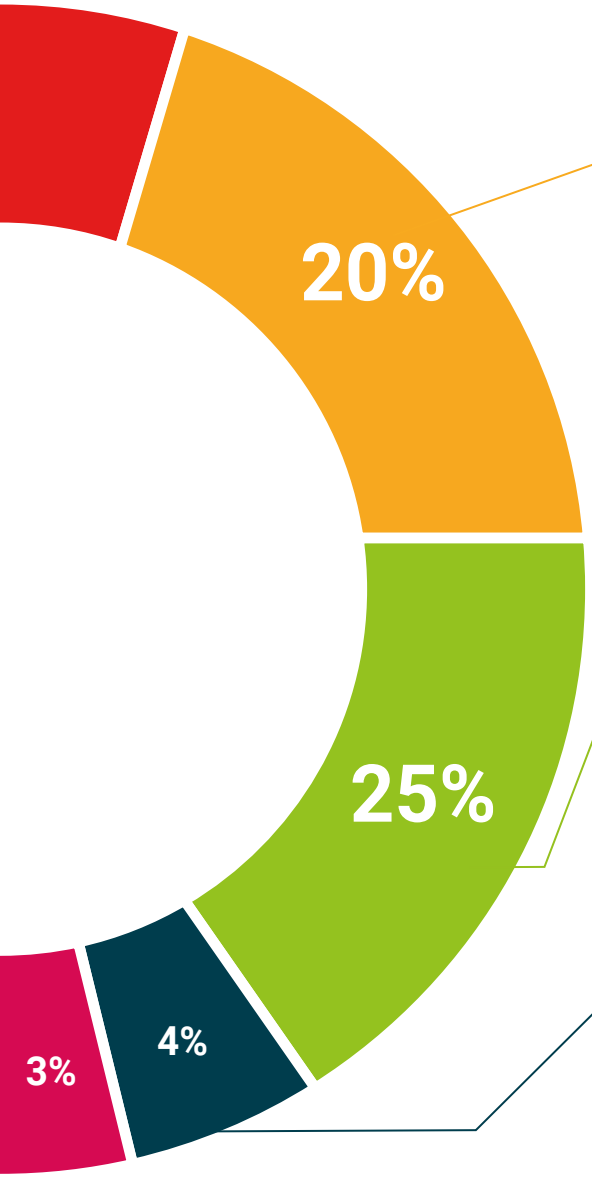
Pratiche di competenze e competenze

Svolgerai attività per sviluppare competenze e capacità specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che uno specialista deve sviluppare nel quadro della globalizzazione in cui viviamo.

Letture complementari

Articoli recenti, documenti di consenso e linee guida internazionali, tra gli altri. Nella biblioteca virtuale di TECH potrai accedere a tutto il materiale necessario per completare la tua specializzazione.





Casi di Studio

Completerai una selezione dei migliori casi di studio scelti appositamente per questo corso. Casi presentati, analizzati e monitorati dai migliori specialisti del panorama internazionale.

Riepiloghi interattivi

Il team di TECH presenta i contenuti in modo accattivante e dinamico in pillole multimediali che includono audio, video, immagini, diagrammi e mappe concettuali per consolidare la conoscenza.

Questo esclusivo sistema di specializzazione per la presentazione di contenuti multimediali è stato premiato da Microsoft come "Caso di successo in Europa".

Testing & Retesting

Valutiamo e rivalutiamo periodicamente le tue conoscenze durante tutto il programma con attività ed esercizi di valutazione e autovalutazione, affinché tu possa verificare come raggiungi progressivamente i tuoi obiettivi.

06

Titolo

Questo programma ti consentirà di ottenere il titolo di studio di Esperto Universitario in Cibersicurezza Offensiva rilasciato da TECH Global University, la più grande università digitale del mondo.

Porta a termine questo programma e ricevi la tua qualifica universitaria senza spostamenti o fastidiose formalità”

Questo programma ti consentirà di ottenere il titolo di studio di **Esperto Universitario in Cibersicurezza Offensiva** rilasciato da **TECH Global University**, la più grande università digitale del mondo.

TECH Global University è un'Università Ufficiale Europea riconosciuta pubblicamente dal Governo di Andorra ***(bollettino ufficiale)***. Andorra fa parte dello Spazio Europeo dell'Istruzione Superiore (EHEA) dal 2003. L'EHEA è un'iniziativa promossa dall'Unione Europea che mira a organizzare il quadro formativo internazionale e ad armonizzare i sistemi di istruzione superiore dei Paesi membri di questo spazio. Il progetto promuove valori comuni, l'implementazione di strumenti congiunti e il rafforzamento dei meccanismi di garanzia della qualità per migliorare la collaborazione e la mobilità tra studenti, ricercatori e accademici.

Questo titolo privato di **TECH Global Universtity** è un programma europeo di formazione continua e aggiornamento professionale che garantisce l'acquisizione di competenze nella propria area di conoscenza, conferendo allo studente che supera il programma un elevato valore curriculare.

Titolo: **Esperto Universitario in Cibersicurezza Offensiva**

ECTS: **18**

Nº Ore Ufficiali: **450 o.**


tech global university

Dott _____, con documento d'identità _____ ha superat o con successo e ottenuto il titolo di:

Esperto Universitario in Cibersicurezza Offensiva

Si tratta di un titolo di studio privato corrispondente a 450 horas di durata equivalente a 18 ECTS, con data di inizio dd/mm/aaaa e data di fine dd/mm/aaaa.

TECH Global University è un'università riconosciuta ufficialmente dal Governo di Andorra il 31 de gennaio 2024, appartenente allo Spazio Europeo dell'Istruzione Superiore (EHEA).

In Andorra la Vella, 28 febbraio 2024

Dott. Pedro Navarro Illa na
Rettore

código único TECH: AFWOR23S techtitute.com/titulos

Apostille dell'Aia. Se lo studente dovesse richiedere che il suo diploma cartaceo sia provvisto di Apostille dell'Aia, TECH Global University effettuerà le gestioni opportune per ottenerla pagando un costo aggiuntivo.

tech global university

Esperto Universitario
Cibersicurezza Offensiva

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Global University**
- Accreditamento: **18 ECTS**
- Orario: **a scelta**
- Esami: **online**

Esperto Universitario
Cibersicurezza Offensiva

tech global university