Universitätskurs
Offensive Sicherheit

tech technologische universität

tech technologische universität

Universitätskurs
Offensive Sicherheit

- Modalität: **online**
- Dauer: **6 Wochen**
- Qualifizierung: **TECH Technologische Universität**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Internetzugang: **www.techtitute.com/de/informatik/universitatskurs/offensive-sicherheit**

Index

01

Präsentation

In der schnelllebigen Welt der Cybersicherheit erfordert die ständige Weiterentwicklung von Cyberbedrohungen eine kontinuierliche Vorbereitung, um bösartigen Akteuren einen Schritt voraus zu sein. In diesem Zusammenhang ist es von unschätzbarem Wert, sich auf dem Laufenden zu halten, um die Sicherheit von Organisationen und den Schutz vor immer raffinierteren Cyberangriffen zu gewährleisten. In diesem Sinne bietet dieses Programm einen tiefen Einblick in offensive Sicherheitstaktiken, die es den Teilnehmern ermöglichen, komplexe Bedrohungen zu antizipieren und effektiv auf sie zu reagieren. Mit einem 100%igen Online-Format bietet der Lehrplan die nötige Flexibilität, um den Zeitplan vielbeschäftigter Berufstätiger zu berücksichtigen. Er enthält eine Vielzahl von Multimedia-Inhalten und wendet die *Relearning*-Methode an, um die Wissensspeicherung zu optimieren.

In diesem einzigartigen 100%igen Online-Hochschulprogramm werden Sie reale Herausforderungen durch fortgeschrittene Simulationen von Cyberbedrohungen angehen"

In der heutigen Cybersicherheitslandschaft, in der sich die Bedrohungen ständig weiterentwickeln, ist ein effektives Management der Teamarbeit unerlässlich geworden. Daher ist eine effektive Zusammenarbeit zwischen Sicherheitsteams nicht nur eine Notwendigkeit, sondern ein Muss, um komplexe Cyber-Bedrohungen vorherzusehen und zu entschärfen. Hier entsteht der entscheidende Bedarf für dieses Programm, das die Bedeutung eines guten Teammanagements bei der Erkennung von und dem Schutz vor Malware-Bedrohungen nicht nur erkennt, sondern auch behandelt. Dieser Lehrplan bietet die notwendigen Werkzeuge und Strategien, um Sicherheitsteams zu integrieren, Rollen effektiv zuzuweisen und die Koordination bei der Reaktion auf digitale Bedrohungen zu optimieren.

Während des gesamten Verlaufs dieses Universitätskurses in Offensive Sicherheit erlangen die Studenten ein tiefgehendes Verständnis der Methoden von Penetrationstests, die ein umfassendes Verständnis der wichtigsten Phasen wie Informationsbeschaffung, Schwachstellenanalyse, Ausnutzung und Dokumentation vermitteln. Die Studenten werden nicht nur theoretisches Wissen erwerben, sondern auch praktische Fähigkeiten durch den Einsatz spezieller *Pentesting*-Tools entwickeln. Dieses Eintauchen in die Praxis ermöglicht die effektive Identifizierung und Bewertung von Schwachstellen in Systemen und Netzwerken. Darüber hinaus wird besonderer Wert auf die Praxis der effektiven Zusammenarbeit in offensiven Sicherheitsteams gelegt, wodurch die Zuweisung von Rollen, die Koordination und die Durchführung von *Pentesting*-Aktivitäten optimiert werden. Diese praktische Ausrichtung stellt sicher, dass die Teilnehmer nicht nur die theoretischen Konzepte verstehen, sondern auch darauf vorbereitet sind, sie in realen Situationen effektiv anzuwenden.

Dieses Programm zeichnet sich durch seine innovative Methodik aus. Da es zu 100% online durchgeführt wird, kann es flexibel an die Zeitpläne von Berufstätigen angepasst werden, so dass geografische und zeitliche Barrieren entfallen. Darüber hinaus wird *Relearning* angewandt, das auf der Wiederholung der wichtigsten Konzepte basiert, um das Einprägen des Wissens zu verstärken und das effektive Lernen zu erleichtern.

Dieser **Universitätskurs in Offensive Sicherheit** enthält das vollständigste und aktuellste Programm auf dem Markt. Seine herausragendsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten für offensive Sicherheit vorgestellt werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren Informationen
- Die praktischen Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens durchgeführt werden kann
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden
- Theoretische Vorträge, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- Die Verfügbarkeit des Zugriffs auf die Inhalte von jedem festen oder tragbaren Gerät mit Internetanschluss

Sie werden in die innovativsten Betriebssysteme für Hacking eintauchen, ohne starre Zeit- oder Bewertungspläne: darum geht es in diesem TECH-Programm"

Informieren Sie sich über die neuesten Methoden der offensiven Sicherheit an der laut Forbes besten digitalen Universität der Welt"

Vergessen Sie das Auswendiglernen! Mit dem Relearning-System werden Sie die Konzepte auf natürliche und progressive Weise integrieren.

Mit diesem innovativen Lehrplan werden Sie die Grundlagen der offensiven Sicherheit beherrschen und Ihre Karriere vorantreiben.

Das Dozententeam des Programms besteht aus Experten des Sektors, die ihre Berufserfahrung in diese Fortbildung einbringen, sowie aus renommierten Fachleuten von führenden Unternehmen und angesehenen Universitäten.

Die multimedialen Inhalte, die mit der neuesten Bildungstechnologie entwickelt wurden, werden der Fachkraft ein situiertes und kontextbezogenes Lernen ermöglichen, d. h. eine simulierte Umgebung, die eine immersive Fortbildung bietet, die auf die Ausführung von realen Situationen ausgerichtet ist.

Das Konzept dieses Programms konzentriert sich auf problemorientiertes Lernen, bei dem die Fachkraft versuchen muss, die verschiedenen Situationen aus der beruflichen Praxis zu lösen, die während des gesamten Studiengangs gestellt werden. Zu diesem Zweck wird sie von einem innovativen interaktiven Videosystem unterstützt, das von renommierten Experten entwickelt wurde.

02

Ziele

Das Hauptziel dieses Universitätsprogramms ist es, die Taktiken, Techniken und Verfahren zu studieren und zu verstehen, die von bösartigen Akteuren im Bereich der Cybersicherheit eingesetzt werden. Während des gesamten Lehrplans werden die Studenten in die detaillierte Analyse dieser Praktiken eintauchen, was sie nicht nur in die Lage versetzt, Bedrohungen zu erkennen, sondern auch effektiv zu simulieren. In diesem Sinne stellt dieser spezialisierte Ansatz sicher, dass die Studenten fortgeschrittene Kenntnisse und anwendbare Fähigkeiten erwerben, um den realen Herausforderungen im Bereich der offensiven Sicherheit zu begegnen und sie auf eine führende Rolle beim Schutz vor Cyberbedrohungen vorzubereiten.

Sie werden das Arsenal des offensiven Auditors ergründen. Holen Sie das Beste aus Ihren Ressourcen heraus und erreichen Sie Ihre Ziele mit TECH!"

Allgemeine Ziele

- Erwerben fortgeschrittener Fähigkeiten in Penetrationstests und *Red-Team*-Simulationen, die sich mit der Identifizierung und Ausnutzung von Schwachstellen in Systemen und Netzwerken befassen
- Entwickeln von Führungsqualitäten, um auf offensive Cybersicherheit spezialisierte Teams zu koordinieren und die Durchführung von *Pentesting*- und *Red-Team*-Projekten zu optimieren
- Entwickeln von Fähigkeiten zur Analyse und Entwicklung von Malware, zum Verständnis ihrer Funktionsweise und zur Anwendung von Verteidigungs- und Aufklärungsstrategien
- Verbessern der Kommunikationsfähigkeiten durch die Erstellung von detaillierten technischen Berichten und Berichten für die Geschäftsleitung, wobei die Ergebnisse einem technischen Publikum und der Geschäftsleitung effektiv präsentiert werden

In nur 6 Wochen geben Sie Ihrer Karriere den nötigen Schub dank dieses Hochschulprogramms mit dem TECH-Gütesiegel"

Spezifische Ziele

- Vermitteln der Methoden der Penetrationstests, einschließlich der wichtigsten Phasen wie Informationsbeschaffung, Schwachstellenanalyse, Ausnutzung und Dokumentation
- Entwickeln praktischer Fähigkeiten im Umgang mit spezialisierten *Pentesting*-Tools, um Schwachstellen in Systemen und Netzwerken zu identifizieren und zu bewerten
- Studieren und Verstehen der Taktiken, Techniken und Verfahren, die von böswilligen Akteuren eingesetzt werden, um Bedrohungen zu identifizieren und zu simulieren
- Anwenden von theoretischen Kenntnissen in praktischen Szenarien und Simulationen, wobei echte Herausforderungen bewältigt werden, um die *Pentesting*-Fähigkeiten zu stärken
- Entwickeln von effektiven Dokumentationsfähigkeiten, Erstellen von detaillierten Berichten, die die Ergebnisse, die verwendeten Methoden und die Empfehlungen zur Verbesserung der Sicherheit wiedergeben
- Üben der effektiven Zusammenarbeit in offensiven Sicherheitsteams, um die Koordination und Durchführung von *Pentesting*-Aktivitäten zu optimieren

03

Kursleitung

TECH hat sorgfältig die besten Spezialisten auf diesem Gebiet ausgewählt, um das Dozententeam für diesen Studiengang zusammenzustellen. In diesem Sinne bringt jedes Mitglied dieses Lehrkörpers einen umfangreichen beruflichen Hintergrund mit, der in führenden Unternehmen im Bereich der Cybersicherheit erworben wurde. Darüber hinaus gewährleistet diese sorgfältige Auswahl, dass die Studenten von der direkten und aktuellen Erfahrung von Fachleuten profitieren, die sich den Herausforderungen der offensiven Sicherheit gestellt und sie gelöst haben. Zudem erleichtert die Anwendung der *Relearning*-Methode das Lernen und verankert das Wissen durch die Wiederholung der wichtigsten Konzepte im gesamten Lehrplan.

Sie werden von einem Lehrkörper unterstützt, der sich aus angesehenen Gurus der offensiven Sicherheit zusammensetzt. Worauf warten Sie noch, um Ihre Karriere voranzutreiben?"

Leitung

Hr. Gómez Pintado, Carlos

- Manager für Cybersicherheit und Red Team Cipherbit bei Grupo Oesía
- Geschäftsführender *Advisor & Investor* bei Wesson App
- Hochschulabschluss in Software Engineering und Technologien der Informationsgesellschaft an der Polytechnischen Universität von Madrid
- Zusammenarbeit mit Bildungseinrichtungen bei der Entwicklung von höherstufigen Ausbildungszyklen im Bereich Cybersicherheit

Professoren

Hr. González Parrilla, Yuba

- Linienkoordinator für offensive Sicherheit und Red Team
- Spezialist für *Predictive*-Projektmanagement am Project Management Institute
- *SmartDefense*-Spezialist
- Experte für *Web Application Penetration Tester* bei eLearnSecurity
- *Junior Penetration Tester* bei eLearnSecurity
- Hochschulabschluss in Computertechnik an der Polytechnischen Universität von Madrid

04

Struktur und Inhalt

Dieser Lehrplan vermittelt den Studenten praktische Fähigkeiten durch den Einsatz von speziellen *Pentesting*-Tools. Während des gesamten Lehrplans liegt der Schwerpunkt auf der Entwicklung fortgeschrittener technischer Fähigkeiten, die es den Studenten ermöglichen, Schwachstellen in Systemen und Netzwerken zu identifizieren und zu bewerten. Darüber hinaus stellt dieser praktische Ansatz, der durch einen strukturierten Lehrplan unterstützt wird, sicher, dass Fachleute grundlegende Fähigkeiten in offensiver Sicherheit erwerben. Mit einem besonderen Schwerpunkt auf der direkten Anwendung von Wissen ist dieses Programm eine unverzichtbare Plattform für diejenigen, die sich im dynamischen Bereich der Cybersicherheit profilieren wollen.

In diesem 100%igen Online-Universitätskurs werden Sie in innovative Methoden der offensiven Sicherheit eingeführt. Und das in nur 6 Monaten!“

Modul 1. Offensive Sicherheit

1.1. Definition und Kontext
- 1.1.1. Grundlegende Konzepte der offensiven Sicherheit
- 1.1.2. Bedeutung der Cybersicherheit heute
- 1.1.3. Herausforderungen und Chancen der offensiven Sicherheit

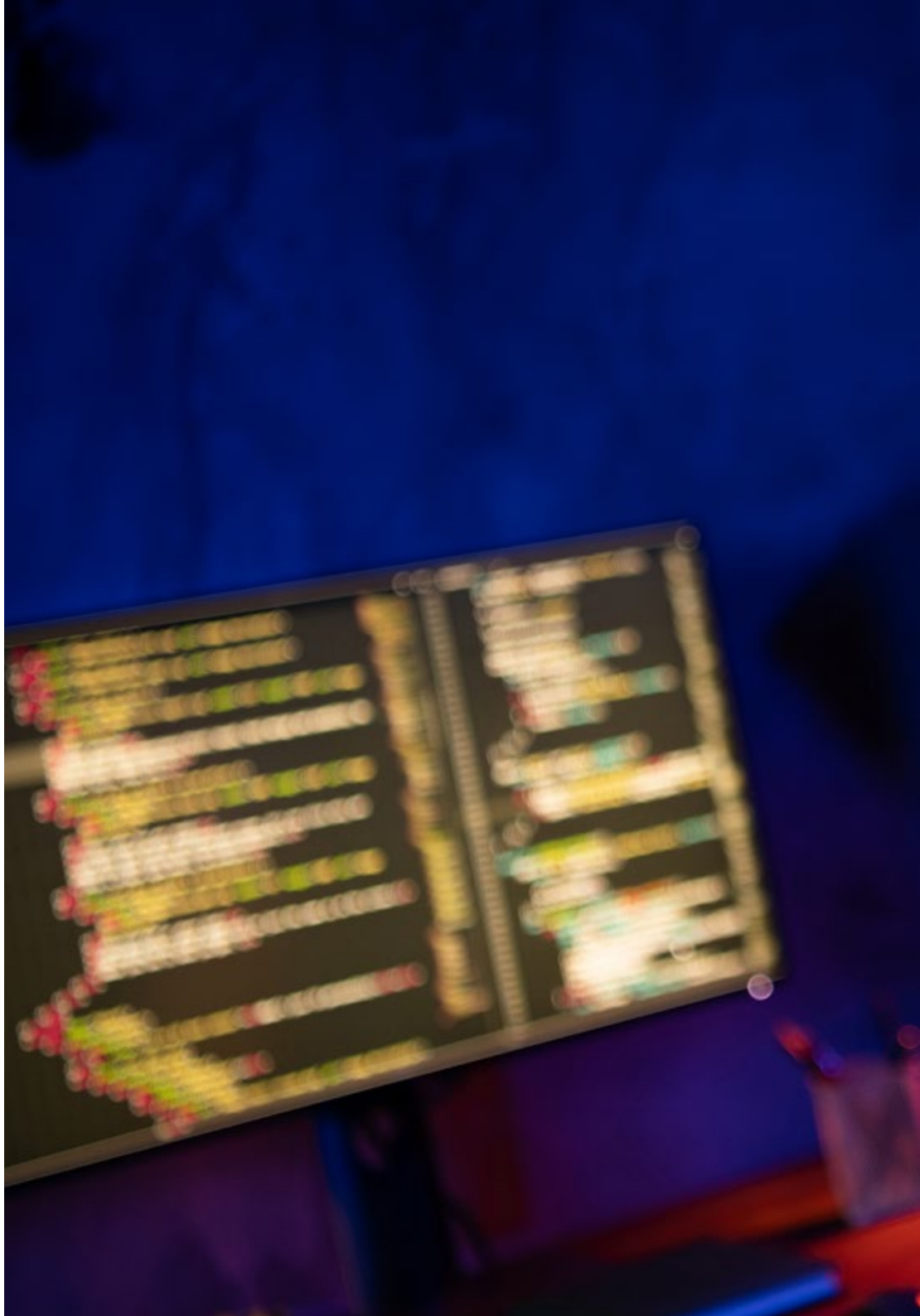
1.2. Grundlagen der Cybersicherheit
- 1.2.1. Frühe Herausforderungen und sich entwickelnde Bedrohungen
- 1.2.2. Technologische Meilensteine und ihre Auswirkungen auf die Cybersicherheit
- 1.2.3. Cybersicherheit im modernen Zeitalter

1.3. Grundlagen der offensiven Sicherheit
- 1.3.1. Schlüsselkonzepte und Terminologie
- 1.3.2. *Think Outside the Box*
- 1.3.3. Unterschiede zwischen offensivem und defensivem Hacking

1.4. Offensive Sicherheitsmethoden
- 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. Rollen und Verantwortlichkeiten bei der offensiven Sicherheit
- 1.5.1. Die wichtigsten Profile
- 1.5.2. *Bug Bounty Hunters*
- 1.5.3. *Researching*. Die Kunst des Recherchierens

1.6. Arsenal des Offensiv-Auditors
- 1.6.1. Betriebssysteme zum Hacking
- 1.6.2. Einführung in C2
- 1.6.3. *Metasploit*: Grundlagen und Verwendung
- 1.6.4. Nützliche Ressourcen



1.7. OSINT: Open-Source-Intelligenz
  1.7.1. Grundlagen von OSINT
  1.7.2. OSINT-Techniken und -Tools
  1.7.3. OSINT-Anwendungen in der offensiven Sicherheit
1.8. *Scripting*: Einführung in die Automatisierung
  1.8.1. Grundlagen des *Scripting*
  1.8.2. *Scripting* in Bash
  1.8.3. *Scripting* in Python
1.9. Schwachstellen-Kategorisierung
  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. Ethik und Hacking
  1.10.1. Grundsätze der Hacker-Ethik
  1.10.2. Die Grenze zwischen ethischem Hacking und bösartigem Hacking
  1.10.3. Rechtliche Implikationen und Konsequenzen
  1.10.4. Fallstudien: Ethische Situationen in der Cybersicherheit

Verpassen Sie nicht die Gelegenheit, Ihre Karriere in der Cybersicherheit durch dieses innovative Programm zu fördern"

05

Methodik

Dieses Fortbildungsprogramm bietet eine andere Art des Lernens. Unsere Methodik wird durch eine zyklische Lernmethode entwickelt: ***das Relearning***.
Dieses Lehrsystem wird z. B. an den renommiertesten medizinischen Fakultäten der Welt angewandt und wird von wichtigen Publikationen wie dem ***New England Journal of Medicine*** als eines der effektivsten angesehen.

Entdecken Sie Relearning, ein System, das das herkömmliche lineare Lernen hinter sich lässt und Sie durch zyklische Lehrsysteme führt: eine Art des Lernens, die sich als äußerst effektiv erwiesen hat, insbesondere in Fächern, die Auswendiglernen erfordern"

Fallstudie zur Kontextualisierung aller Inhalte

Unser Programm bietet eine revolutionäre Methode zur Entwicklung von Fähigkeiten und Kenntnissen. Unser Ziel ist es, Kompetenzen in einem sich wandelnden, wettbewerbsorientierten und sehr anspruchsvollen Umfeld zu stärken.

Mit TECH werden Sie eine Art des Lernens erleben, die an den Grundlagen der traditionellen Universitäten auf der ganzen Welt rüttelt"

Sie werden Zugang zu einem Lernsystem haben, das auf Wiederholung basiert, mit natürlichem und progressivem Unterricht während des gesamten Lehrplans.

Der Student wird durch gemeinschaftliche Aktivitäten und reale Fälle lernen, wie man komplexe Situationen in realen Geschäftsumgebungen löst.

Eine innovative und andersartige Lernmethode

Dieses TECH-Programm ist ein von Grund auf neu entwickeltes, intensives Lehrprogramm, das die anspruchsvollsten Herausforderungen und Entscheidungen in diesem Bereich sowohl auf nationaler als auch auf internationaler Ebene vorsieht. Dank dieser Methodik wird das persönliche und berufliche Wachstum gefördert und ein entscheidender Schritt in Richtung Erfolg gemacht. Die Fallmethode, die Technik, die diesem Inhalt zugrunde liegt, gewährleistet, dass die aktuellste wirtschaftliche, soziale und berufliche Realität berücksichtigt wird.

> *Unser Programm bereitet Sie darauf vor, sich neuen Herausforderungen in einem unsicheren Umfeld zu stellen und in Ihrer Karriere erfolgreich zu sein"*

Die Fallmethode ist das am weitesten verbreitete Lernsystem an den besten Informatikschulen der Welt, seit es sie gibt. Die Fallmethode wurde 1912 entwickelt, damit Jurastudenten das Recht nicht nur auf der Grundlage theoretischer Inhalte erlernen. Sie bestand darin, ihnen reale komplexe Situationen zu präsentieren, damit sie fundierte Entscheidungen treffen und Werturteile darüber fällen konnten, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard etabliert.

Was sollte eine Fachkraft in einer bestimmten Situation tun? Mit dieser Frage konfrontieren wir Sie in der Fallmethode, einer handlungsorientierten Lernmethode. Während des gesamten Kurses werden die Studenten mit mehreren realen Fällen konfrontiert. Sie müssen ihr gesamtes Wissen integrieren, recherchieren, argumentieren und ihre Ideen und Entscheidungen verteidigen.

Relearning Methodology

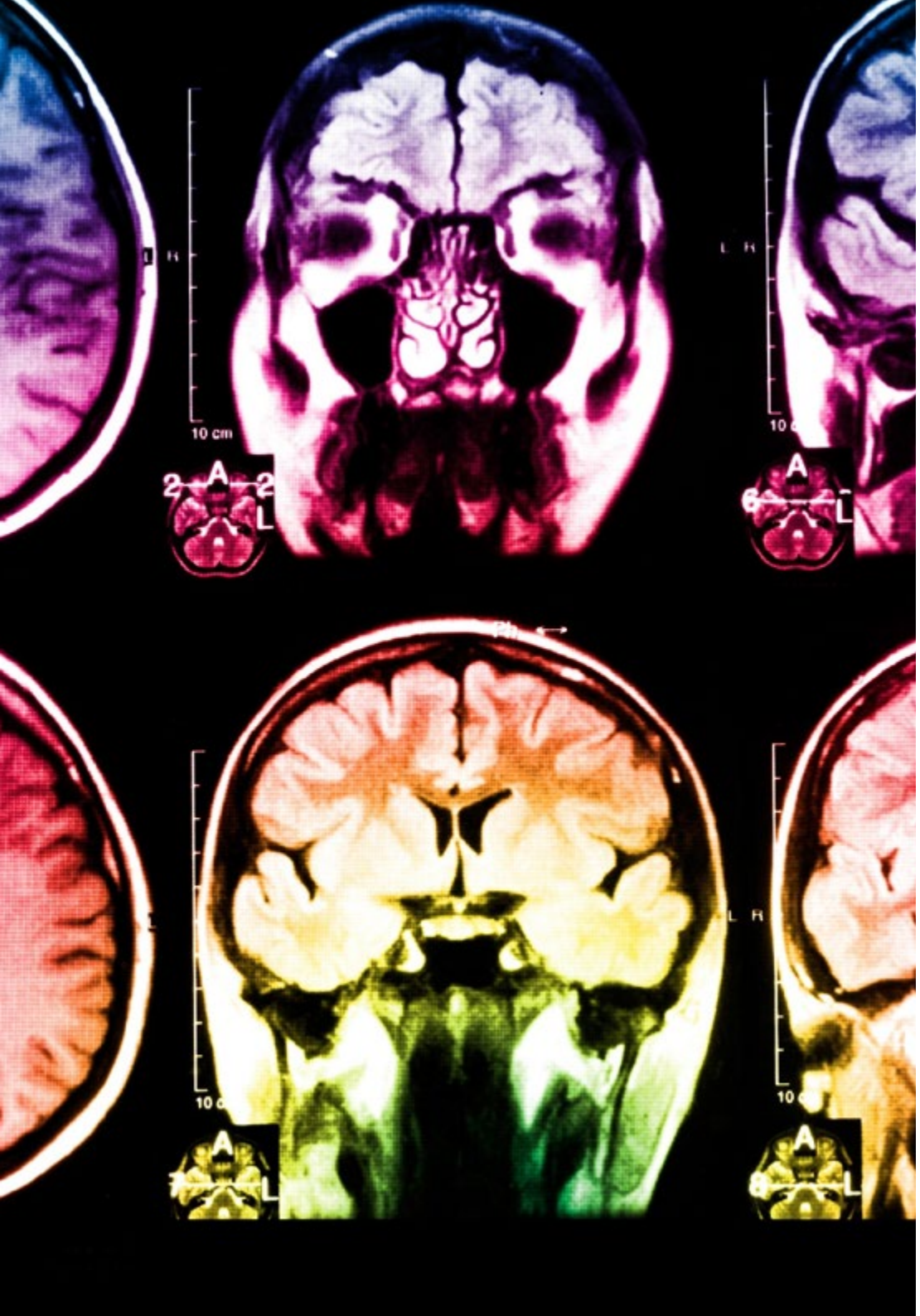
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

Wir ergänzen die Fallstudie mit der besten 100%igen Online-Lehrmethode: Relearning.

Im Jahr 2019 erzielten wir die besten Lernergebnisse aller spanischsprachigen Online-Universitäten der Welt.

Bei TECH lernen Sie mit einer hochmodernen Methodik, die darauf ausgerichtet ist, die Führungskräfte der Zukunft zu spezialisieren. Diese Methode, die an der Spitze der weltweiten Pädagogik steht, wird Relearning genannt.

Unsere Universität ist die einzige in der spanischsprachigen Welt, die für die Anwendung dieser erfolgreichen Methode zugelassen ist. Im Jahr 2019 ist es uns gelungen, die Gesamtzufriedenheit unserer Studenten (Qualität der Lehre, Qualität der Materialien, Kursstruktur, Ziele...) in Bezug auf die Indikatoren der besten spanischsprachigen Online-Universität zu verbessern.



In unserem Programm ist das Lernen kein linearer Prozess, sondern erfolgt in einer Spirale (lernen, verlernen, vergessen und neu lernen). Daher wird jedes dieser Elemente konzentrisch kombiniert. Mit dieser Methode wurden mehr als 650.000 Hochschulabsolventen mit beispiellosem Erfolg in so unterschiedlichen Bereichen wie Biochemie, Genetik, Chirurgie, internationales Recht, Managementfähigkeiten, Sportwissenschaft, Philosophie, Recht, Ingenieurwesen, Journalismus, Geschichte, Finanzmärkte und -instrumente fortgebildet. Dies alles in einem sehr anspruchsvollen Umfeld mit einer Studentenschaft mit hohem sozioökonomischem Profil und einem Durchschnittsalter von 43,5 Jahren.

Das Relearning ermöglicht es Ihnen, mit weniger Aufwand und mehr Leistung zu lernen, sich mehr auf Ihre Spezialisierung einzulassen, einen kritischen Geist zu entwickeln, Argumente zu verteidigen und Meinungen zu kontrastieren: eine direkte Gleichung zum Erfolg.

Nach den neuesten wissenschaftlichen Erkenntnissen der Neurowissenschaften wissen wir nicht nur, wie wir Informationen, Ideen, Bilder und Erinnerungen organisieren, sondern auch, dass der Ort und der Kontext, in dem wir etwas gelernt haben, von grundlegender Bedeutung dafür sind, dass wir uns daran erinnern und es im Hippocampus speichern können, um es in unserem Langzeitgedächtnis zu behalten.

Auf diese Weise sind die verschiedenen Elemente unseres Programms im Rahmen des so genannten Neurocognitive Context-Dependent E-Learning mit dem Kontext verbunden, in dem der Teilnehmer seine berufliche Praxis entwickelt.

Dieses Programm bietet die besten Lehrmaterialien, die sorgfältig für Fachleute aufbereitet sind:

Studienmaterial

Alle didaktischen Inhalte werden von den Fachleuten, die den Kurs unterrichten werden, speziell für den Kurs erstellt, so dass die didaktische Entwicklung wirklich spezifisch und konkret ist.

Diese Inhalte werden dann auf das audiovisuelle Format angewendet, um die Online-Arbeitsmethode von TECH zu schaffen. All dies mit den neuesten Techniken, die in jedem einzelnen der Materialien, die dem Studenten zur Verfügung gestellt werden, qualitativ hochwertige Elemente bieten.

Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

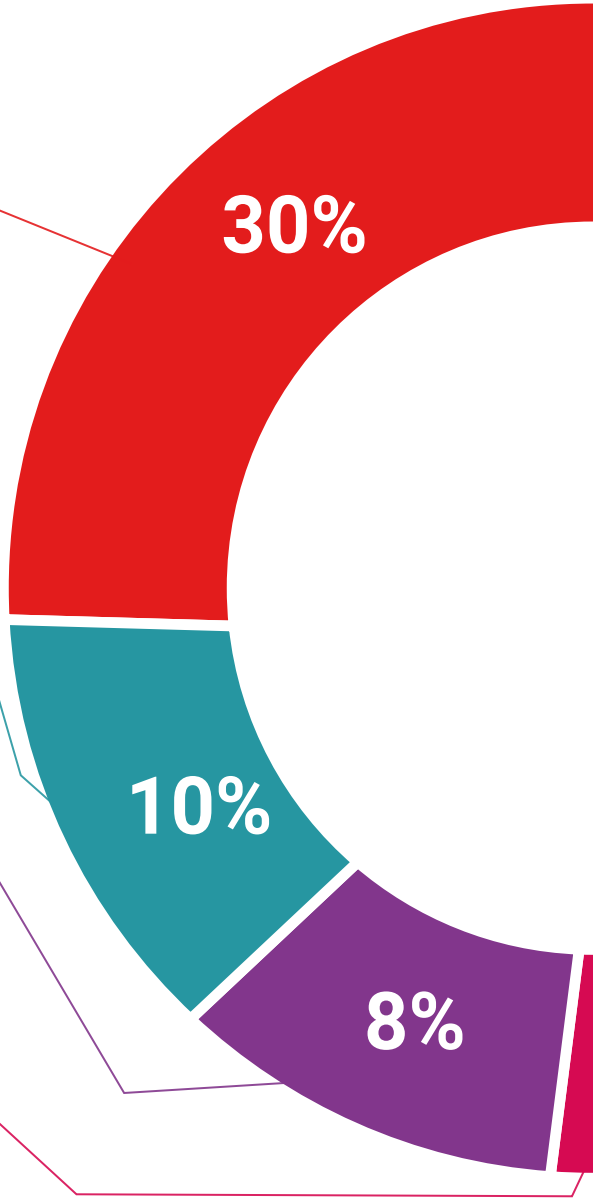
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

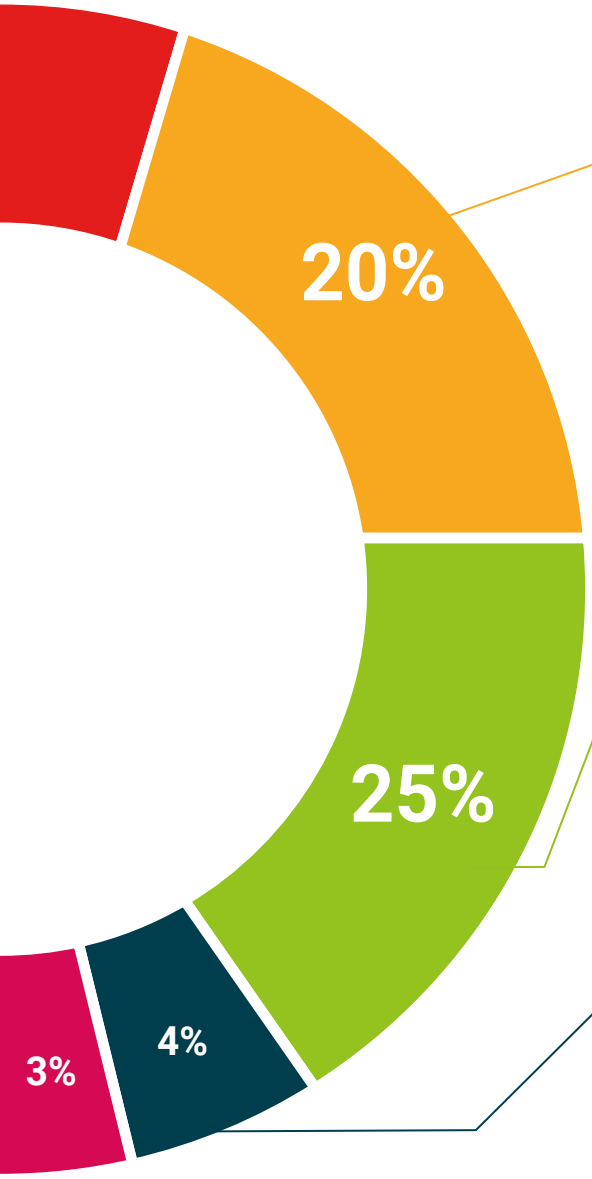
Übungen für Fertigkeiten und Kompetenzen

Sie werden Aktivitäten durchführen, um spezifische Kompetenzen und Fertigkeiten in jedem Fachbereich zu entwickeln. Übungen und Aktivitäten zum Erwerb und zur Entwicklung der Fähigkeiten und Fertigkeiten, die ein Spezialist im Rahmen der Globalisierung, in der wir leben, entwickeln muss.

Weitere Lektüren

Aktuelle Artikel, Konsensdokumente und internationale Leitfäden, u. a. In der virtuellen Bibliothek von TECH hat der Student Zugang zu allem, was er für seine Fortbildung benötigt.





Case Studies

Sie werden eine Auswahl der besten Fallstudien vervollständigen, die speziell für diese Qualifizierung ausgewählt wurden. Die Fälle werden von den besten Spezialisten der internationalen Szene präsentiert, analysiert und betreut.

Interaktive Zusammenfassungen

Das TECH-Team präsentiert die Inhalte auf attraktive und dynamische Weise in multimedialen Pillen, die Audios, Videos, Bilder, Diagramme und konzeptionelle Karten enthalten, um das Wissen zu vertiefen.

Dieses einzigartige Bildungssystem für die Präsentation multimedialer Inhalte wurde von Microsoft als "Europäische Erfolgsgeschichte" ausgezeichnet.

Testing & Retesting

Die Kenntnisse des Studenten werden während des gesamten Programms regelmäßig durch Bewertungs- und Selbsteinschätzungsaktivitäten und -übungen beurteilt und neu bewertet, so dass der Student überprüfen kann, wie er seine Ziele erreicht.

06

Qualifizierung

Der Universitätskurs in Offensive Sicherheit garantiert neben der präzisesten und aktuellsten Fortbildung auch den Zugang zu einem von der TECH Technologische Universität ausgestellten Diplom.

Schließen Sie dieses Programm erfolgreich ab und erhalten Sie Ihren Universitätsabschluss ohne lästige Reisen oder Formalitäten”

Dieser **Universitätskurs in Offensive Sicherheit** enthält das vollständigste und aktuellste Programm auf dem Markt.

Sobald der Student die Prüfungen bestanden hat, erhält er/sie per Post* mit Empfangsbestätigung das entsprechende Diplom, ausgestellt von der **TECH Technologischen Universität.**

Das von **TECH Technologische Universität** ausgestellte Diplom drückt die erworbene Qualifikation aus und entspricht den Anforderungen, die in der Regel von Stellenbörsen, Auswahlprüfungen und Berufsbildungsausschüssen verlangt werden.

Titel: **Universitätskurs in Offensive Sicherheit**

Modalität: **online**

Dauer: **6 Wochen**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

UNIVERSITÄTSKURS

in

Offensive Sicherheit

Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 150 Stunden, mit Anfangsdatum tt/mm/jjjj und Enddatum tt/mm/jjjj.

TECH ist eine private Hochschuleinrichtung, die seit dem 28. Juni 2018 vom Ministerium für öffentliche Bildung anerkannt ist.

Zum 17. Juni 2020

Tere Guevara Navarro
Rektorin

einzigartiger Code TECH: AFWOR23S techtitute.com/titel

*Haager Apostille. Für den Fall, dass der Student die Haager Apostille für sein Papierdiplom beantragt, wird TECH EDUCATION die notwendigen Vorkehrungen treffen, um diese gegen eine zusätzliche Gebühr zu beschaffen.

tech technologische universität

Universitätskurs
Offensive Sicherheit

- Modalität: **online**
- Dauer: **6 Wochen**
- Qualifizierung: **TECH Technologische Universität**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Universitätskurs
Offensive Sicherheit

tech technologische universität