Universitätskurs
Reverse Engineering in Cybersicherheit

tech technologische universität

tech technologische universität

Universitätskurs
Reverse Engineering in Cybersicherheit

- Modalität: **online**
- Dauer: **6 Wochen**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Internetzugang: www.techtitute.com/de/informatik/universitatskurs/reverse-engineering-cybersicherheit

Index

01

Präsentation

In der IT-Umgebung gibt es verschiedene Motivationen, die uns dazu bringen, verschiedene *Reverse Engineering*-Techniken anzuwenden, um eine Software, ein Kommunikationsprotokoll oder einen Algorithmus zu verstehen und genug darüber zu wissen. Dieses tiefe Verständnis ist die Grundlage, die es der Fachkraft ermöglicht, an diese Prozesse angepasste Programme zu entwickeln, die die Anwendung eines spezifischen Schutzes von höherer Qualität und mit einer größeren Kapazität zur Reaktion auf Cyberangriffe ermöglichen. Dieses Programm ermöglicht es Ihnen, diese Fähigkeiten mit der Sicherheit und Garantie von TECH in einem hochqualifizierten, intensiven und schnellen Kurs zu erwerben.

Lernen Sie in wenigen Wochen, wie und in welchem Kontext Sie die verschiedenen Techniken des Reverse Engineering in der Cybersicherheit anwenden können”

Reverse Engineering-Techniken wie die statische Codeanalyse und die dynamische Analyse zur Entschlüsselung von Kommunikationsprotokollen führen zu einem ausreichenden Verständnis des Protokolls, das es uns ermöglicht, eigene Programme zu entwickeln, die uns sagen, wie das Protokoll zu verwenden ist.

Es ist üblich, die in der Entwicklung befindliche Software zu prüfen, um Schwachstellen zu entdecken: Manchmal befindet sich die Schwachstelle nicht im Quellcode, sondern wird durch den *Compiler* eingeführt, der den Maschinencode erzeugt.

Mit dem Wissen über *Reverse Engineering* und somit darüber, wie wir den Maschinencode erhalten, können wir solche Schwachstellen aufspüren.

Eine der bekanntesten Anwendungen des *Reverse Engineering* ist die Analyse von Malware, die es uns mit Hilfe verschiedener Techniken wie *Sandboxing* ermöglicht, die untersuchte Schadsoftware zu verstehen und zu kennen und damit die Entwicklung von Software zu ermöglichen, die in der Lage ist, sie zu erkennen und ihr entgegenzuwirken, wie im Fall von Antiviren-Software, die mit Signaturen arbeitet.

Dieser **Universitätskurs in Reverse Engineering in Cybersicherheit** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung praktischer Fälle, die von Experten in Cybersicherheit vorgestellt werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt soll wissenschaftliche und praktische Informationen zu den für die berufliche Praxis wesentlichen Disziplinen vermitteln
- Er enthält praktische Übungen, in denen der Selbstbewertungsprozess durchgeführt werden kann, um das Lernen zu verbessern
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden
- Theoretische Vorträge, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- Die Verfügbarkeit des Zugangs zu Inhalten von jedem festen oder tragbaren Gerät mit Internetanschluss

Lernen Sie, wie Sie die x86-Prozessorarchitektur und die ARM-Prozessorarchitektur mit Präzision und Genauigkeit untersuchen können"

Analysieren Sie Reverse Engineering-Techniken in einem Prozess der beruflichen Weiterentwicklung, der es Ihnen ermöglicht, das Sicherheitsniveau Ihrer Codes zu erhöhen"

Ein hochqualifizierter Prozess, der so gestaltet ist, dass er überschaubar und flexibel ist, mit der interessantesten Methodik der Online-Bildung.

Studieren Sie in einem praxisorientierten Universitätskurs, der Ihre Fähigkeiten auf das Niveau eines Spezialisten hebt.

Zu den Dozenten des Programms gehören Fachleute aus der Branche, die ihre Erfahrungen in diese Fortbildung einbringen, sowie anerkannte Spezialisten von führenden Gesellschaften und renommierten 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.

Die Gestaltung 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

Dieser Universitätskurs ermöglicht es, die Fähigkeit der Studenten, in diesem Bereich zu arbeiten, schnell und einfach zu verbessern. Mit realistischen und hochinteressanten Zielen wurde dieser Studienprozess so gestaltet, dass die Studenten nach und nach die theoretischen und praktischen Kenntnisse erwerben, die sie benötigen, um mit Qualität zu intervenieren und übergreifende Kompetenzen zu entwickeln, die es ihnen ermöglichen, sich komplexen Situationen zu stellen, indem sie angepasste und präzise Antworten erarbeiten.

Setzen Sie sich mit Qualität in einem Arbeitsfeld voller Beschäftigungsmöglichkeiten durch einen Prozess von außergewöhnlicher Qualität durch”

Allgemeine Ziele

- Analysieren von *Reverse Engineering* und verschiedenen Techniken
- Untersuchen der unterschiedlichen Architekturen und wie diese das *Reverse Engineering* beeinflussen
- Bestimmen, unter welchen Bedingungen verschiedene *Reverse Engineering*-Techniken eingesetzt werden sollen
- Anwenden von *Reverse Engineering* auf die Cybersicherheitsumgebung

Die komfortabelsten und effizientesten Studienunterstützungssysteme, die es gibt, in einem Programm von außergewöhnlicher Qualität”

Spezifische Ziele

- Analysieren der Phasen eines *Compilers*
- Untersuchen der x86-Prozessorarchitektur und der ARM-Prozessorarchitektur
- Bestimmen der verschiedenen Arten von Analysen
- Anwenden von *Sandboxing* in verschiedenen Umgebungen
- Entwickeln verschiedener Techniken zur Analyse von Malware
- Entwickeln von Tools für die Malware-Analyse

03

Kursleitung

Die Professoren des Programms wurden aufgrund ihrer außergewöhnlichen Kompetenz auf diesem Gebiet ausgewählt. Sie verbinden technische und praktische Erfahrung mit Unterrichtserfahrung und bieten den Studenten erstklassige Unterstützung bei der Erreichung ihrer Ziele. Durch sie bietet der Universitätskurs die direkteste und unmittelbarste Sicht auf die realen Merkmale der Intervention in diesem Bereich und erreicht eine kontextuelle Vision von maximalem Interesse.

Fachkundige Dozenten für Reverse Engineering in Cybersicherheit werden Sie in jeder Phase des Studiums begleiten und Ihnen einen möglichst realistischen Einblick in diese Arbeit geben"

Internationale Gastdirektorin

Dr. Frederic Lemieux ist international als innovativer Experte und inspirierende Führungspersönlichkeit in den Bereichen der **Intelligenz, der nationalen Sicherheit, der inneren Sicherheit, der Cybersicherheit** und der **disruptiven Technologien** anerkannt. Sein ständiges Engagement und seine wichtigen Beiträge zu Forschung und Bildung machen ihn zu einer zentralen Figur bei der Förderung der Sicherheit und des Verständnisses der heutigen neuen Technologien. Während seiner beruflichen Laufbahn hat er an mehreren renommierten Institutionen wie der **Universität von Montreal,** der **George Washington Universität** und der Universität von Georgetown zukunftsweisende akademische Programme konzipiert und geleitet.

Im Laufe seiner umfangreichen Erfahrung hat er mehrere Bücher von großer Bedeutung veröffentlicht, die sich alle mit **kriminalistischer Aufklärung, Polizeiarbeit, Cyber-Bedrohungen und internationaler Sicherheit** befassen. Er hat auch einen wichtigen Beitrag zum Bereich der Cybersicherheit geleistet, indem er zahlreiche Artikel in akademischen Zeitschriften veröffentlicht hat, die sich mit der Verbrechensbekämpfung bei großen Katastrophen, der Terrorismusbekämpfung, den Nachrichtendiensten und der polizeilichen Zusammenarbeit beschäftigen. Darüber hinaus war er Podiumsteilnehmer und Hauptredner bei verschiedenen nationalen und internationalen Konferenzen und hat sich als führender Wissenschaftler und Praktiker etabliert.

Dr. Lemieux hatte redaktionelle und bewertende Funktionen in verschiedenen akademischen, privaten und staatlichen Organisationen inne, was seinen Einfluss und sein Engagement für Spitzenleistungen in seinem Fachgebiet widerspiegelt. Im Rahmen seiner angesehenen akademischen Laufbahn war er Professor für Praxis und Fakultätsleiter der MPS-Programme für **Angewandte Intelligenz, Risikomanagement für Cybersicherheit, Technologiemanagement und Informationstechnologiemanagement** an der **Universität von Georgetown.**

Dr. Lemieux, Frederic

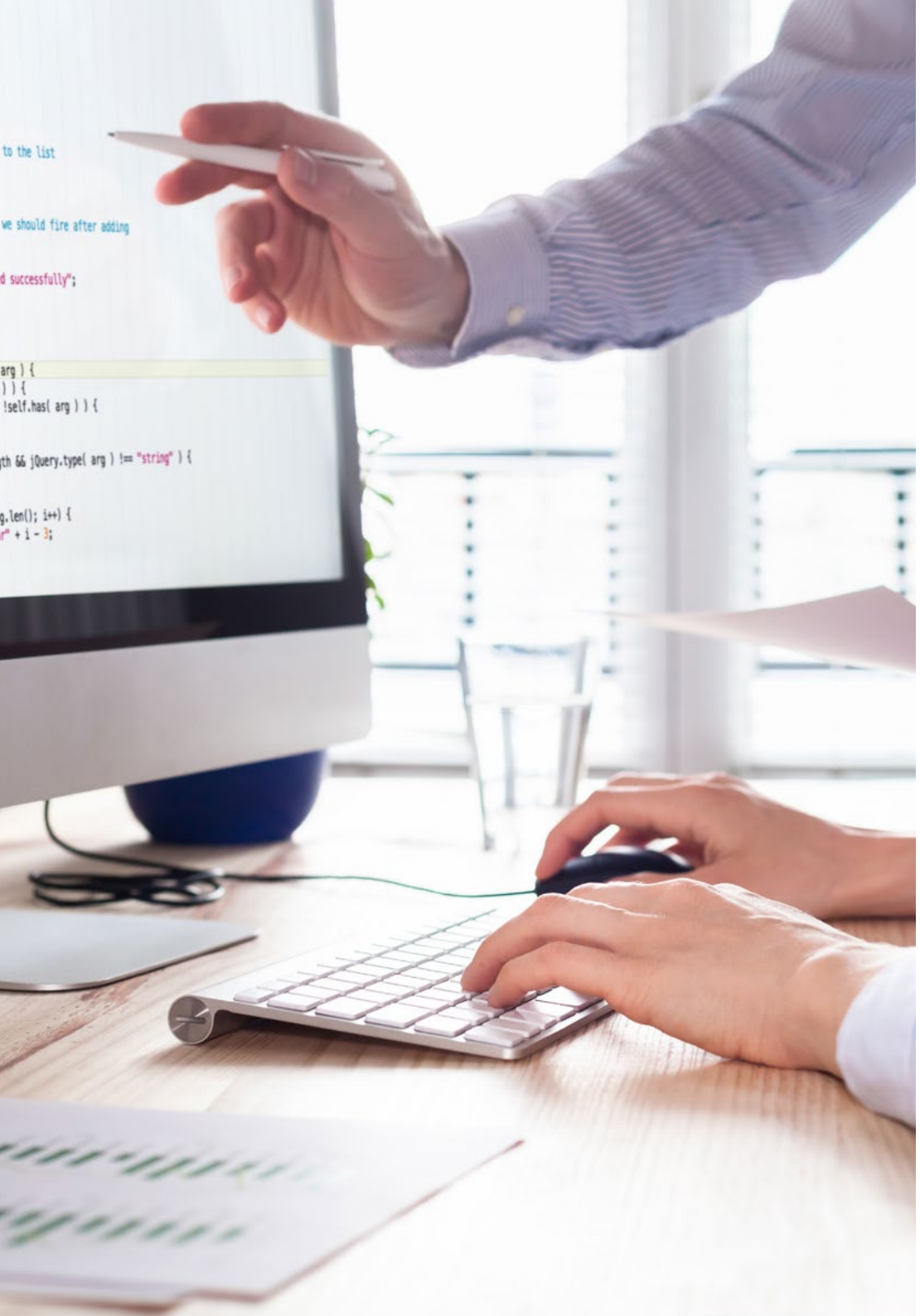
- Forscher im Bereich Intelligenz, Cybersicherheit und Disruptive Technologien an der Universität von Georgetown
- Direktor des Masterstudiengangs in Information Technology Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Technology Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Cybersecurity Risk Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Applied Intelligence an der Universität von Georgetown
- Professor für Praktika an der Universität von Georgetown
- Promotion in Kriminologie an der School of Criminology der Universität von Montreal
- Hochschulabschluss in Soziologie, Nebenfach Psychologie, Universität von Laval
- Mitglied von:
- New Program Roundtable Committee, Universität von Georgetown

Dank TECH werden Sie mit den besten Fachleuten der Welt lernen können"

Leitung

Fr. Fernández Sapena, Sonia

- AAusbilderin für Computersicherheit und *Ethical Hacking*, Nationales Referenzzentrum für IT und Telekommunikation in Getafe, Madrid
- Zertifizierte *E-Council*-Ausbilderin, Madrid
- Ausbilderin für die folgenden Zertifizierungen: EXIN *Ethical Hacking Foundation* und EXIN *Cyber & IT Security Foundation*, Madrid
- Von der CAM akkreditierte Fachausbilderin für die folgenden Berufszertifikate: IT-Sicherheit (IFCT0190), Verwaltung von Sprach- und Datennetzen (IFCM0310), Verwaltung von Abteilungsnetzen (IFCT0410), Alarmmanagement in Telekommunikationsnetzen (IFCM0410), Betreiber von Sprach- und Datennetzen (IFCM0110) und Verwaltung von Internetdiensten (IFCT0509)
- Externe Mitarbeit CSO/SSA (*Chief Security Officer/Senior Security Architect*), Universität der Balearischen Inseln
- Informatik-Ingenieurin, Universität von Alcalá de Henares, Madrid
- Masterstudiengang in DevOps: Docker und Kubernetes, Cas-Training, Madrid
- *Microsoft Azure Security Techonologies, E-Council,* Madrid



Professoren

Hr. Redondo, Jesús Serrano

- Junior *FrontEnd*-Entwickler und Junior *Cybersecurity*-Techniker
- *FrontEnd*-Entwickler bei Telefónica, Madrid
- *FrontEnd*-Entwickler, *Best Pro Consulting SL*, Madrid
- Installateur von Telekommunikationsgeräten und -dienstleistungen, Zener Group, Castilla y León
- Installateur von Telekommunikationsgeräten und -dienstleistungen, Lican Comunicaciones SL, Castilla y León
- Zertifikat in Computersicherheit, CFTIC Getafe, Madrid
- Höherer Techniker: Telekommunikation und Computersysteme, IES Trinidad Arroyo, Palencia
- Höherer Techniker: Elektrotechnische MV- und LV-Installationen, IES Trinidad Arroyo, Palencia
- Ausbildung in *Reverse Engineering*, Stenographie, Verschlüsselung, *Incibe Hacker Academy* (Incibe Talente)

Eine anregende Reise zur beruflichen Weiterentwicklung, die Ihr Interesse und Ihre Motivation während der gesamten Fortbildung aufrechterhält"

04

Struktur und Inhalt

Dank des praktischen Ansatzes dieses Universitätskurses ist es einfach, sich genaue und aktuelle Kenntnisse auf dem Gebiet des *Reverse Engineering* in Cybersicherheit anzueignen. Der Kurs wurde mit Blick auf den effizienten Erwerb von ergänzenden Lerninhalten strukturiert, die die Vertiefung und die Konsolidierung des Gelernten ermöglichen und die Studenten in die Lage versetzen, so schnell wie möglich zu intervenieren. Ein hochintensiver und qualitativ hochwertiger Kurs, der die Besten des Sektors fortbilden soll.

Lernen Sie in nur wenigen Wochen, wie die Anwendung von Reverse Engineering unschätzbare Daten für Cybersicherheitsmaßnahmen liefert"

Modul 1. *Reverse Engineering*

1.1. *Compiler*
- 1.1.1. Arten von Code
- 1.1.2. *Compiler*-Phasen
- 1.1.3. Symboltabelle
- 1.1.4. Fehler-Handler
- 1.1.5. GCC Compiler

1.2. Arten der *Compiler*-Analyse
- 1.2.1. Lexikalische Analyse
  - 1.2.1.1. Terminologie
  - 1.2.1.2. Lexikalische Komponenten
  - 1.2.1.3. LEX Lexikalischer Analysator
- 1.2.2. Syntaktische Analyse
  - 1.2.2.1. Kontextfreie Grammatiken
  - 1.2.2.2. Arten des *Parsing*
    - 1.2.2.2.1. *Top-down-Parsing*
    - 1.2.2.2.2. *Bottom-up-Parsing*
  - 1.2.2.3. Syntaktische Bäume und Ableitungen
  - 1.2.2.4. Arten von Parsern
    - 1.2.2.4.1. LR-Parser (*Left to Right*)
    - 1.2.2.4.2. LALR-Parser
- 1.2.3. Semantische Analyse
  - 1.2.3.1. Attribut-Grammatiken
  - 1.2.3.2. S-Attribute
  - 1.2.3.3. L-Attribute

1.3. Montage Datenstrukturen
- 1.3.1. Variablen
- 1.3.2. *Arrays*
- 1.3.3. Zeiger
- 1.3.4. Strukturen
- 1.3.5. Objekte

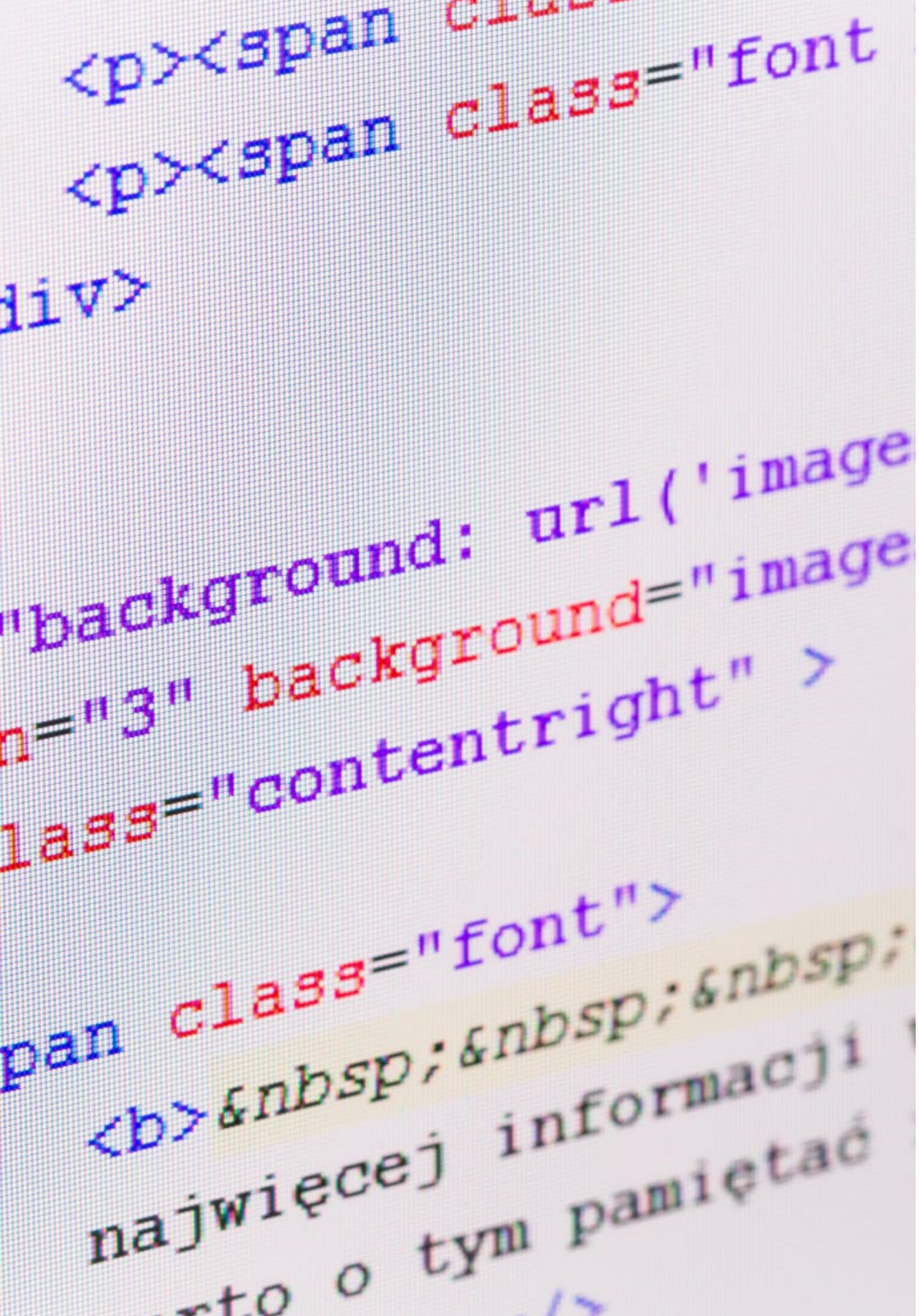
1.4. *Assembly* Code-Strukturen
- 1.4.1. Auswahl-Strukturen
  - 1.4.1.1. *If, else if, Else*
  - 1.4.1.2. *Switch*
- 1.4.2. Iterations-Strukturen
  - 1.4.2.1. *For*
  - 1.4.2.2. *While*
  - 1.4.2.3. Verwendung des *Break*
- 1.4.3. Funktionen

1.5. x86-Hardware-Architektur
- 1.5.1. x86-Prozessorarchitektur
- 1.5.2. x86 Datenstrukturen
- 1.5.3. x86 Code-Strukturen
- 1.5.4. x86 Code-Strukturen

1.6. ARM Hardware-Architektur
- 1.6.1. ARM-Prozessorarchitektur
- 1.6.2. ARM-Daten-Strukturen
- 1.6.3. ARM-Code-Strukturen

1.7. Statische Code-Analyse
- 1.7.1. *Disassembler*
- 1.7.2. IDA
- 1.7.3. Code-Rekonstrukteure

1.8. Dynamische Code-Analyse
- 1.8.1. Verhaltensanalyse
  - 1.8.1.1. Kommunikation
  - 1.8.1.2. Überwachung
- 1.8.2. *Linux Code-Debugger*
- 1.8.3. *Windows-Code-Debugger*



1.9. *Sandbox*
- 1.9.1. *Sandbox*-Architektur
- 1.9.2. *Sandbox*-Umgehung
- 1.9.3. Erkennungstechniken
- 1.9.4. Ausweichtechniken
- 1.9.5. Gegenmaßnahmen
- 1.9.6. *Sandbox* in Linux
- 1.9.7. *Sandbox* in Windows
- 1.9.8. *Sandbox* in MacOS
- 1.9.9. *Sandbox* in Android

1.10. Malware-Scans
- 1.10.1. Methoden zur Analyse der Malware
- 1.10.2. Techniken zur Verschleierung von Malware
  - 1.10.2.1. Ausführbare Verschleierung
  - 1.10.2.2. Einschränkung der Ausführungsumgebungen
- 1.10.3. Tools zur Analyse der Malware

Ein Prozess von höchstem Interesse für Fachleute, die im Bereich der Cybersicherheit arbeiten, der Sie auf den neuesten Stand bringt und Sie auf dem Arbeitsmarkt voranbringt"

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 aufgibt 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 die Grundlagen der traditionellen Universitäten in der ganzen Welt verschiebt”

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

Die Studenten lernen durch gemeinschaftliche Aktivitäten und reale Fälle die Lösung komplexer Situationen in realen Geschäftsumgebungen.

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 die Jurastudenten das Recht nicht nur anhand theoretischer Inhalte erlernen, sondern ihnen reale, komplexe Situationen vorlegen, damit sie fundierte Entscheidungen treffen und Werturteile darüber fällen können, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard eingeführt.

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 Studierenden mit mehreren realen Fällen konfrontiert. Sie müssen Ihr gesamtes Wissen integrieren, recherchieren, argumentieren und Ihre Ideen und Entscheidungen verteidigen.

Relearning Methodik

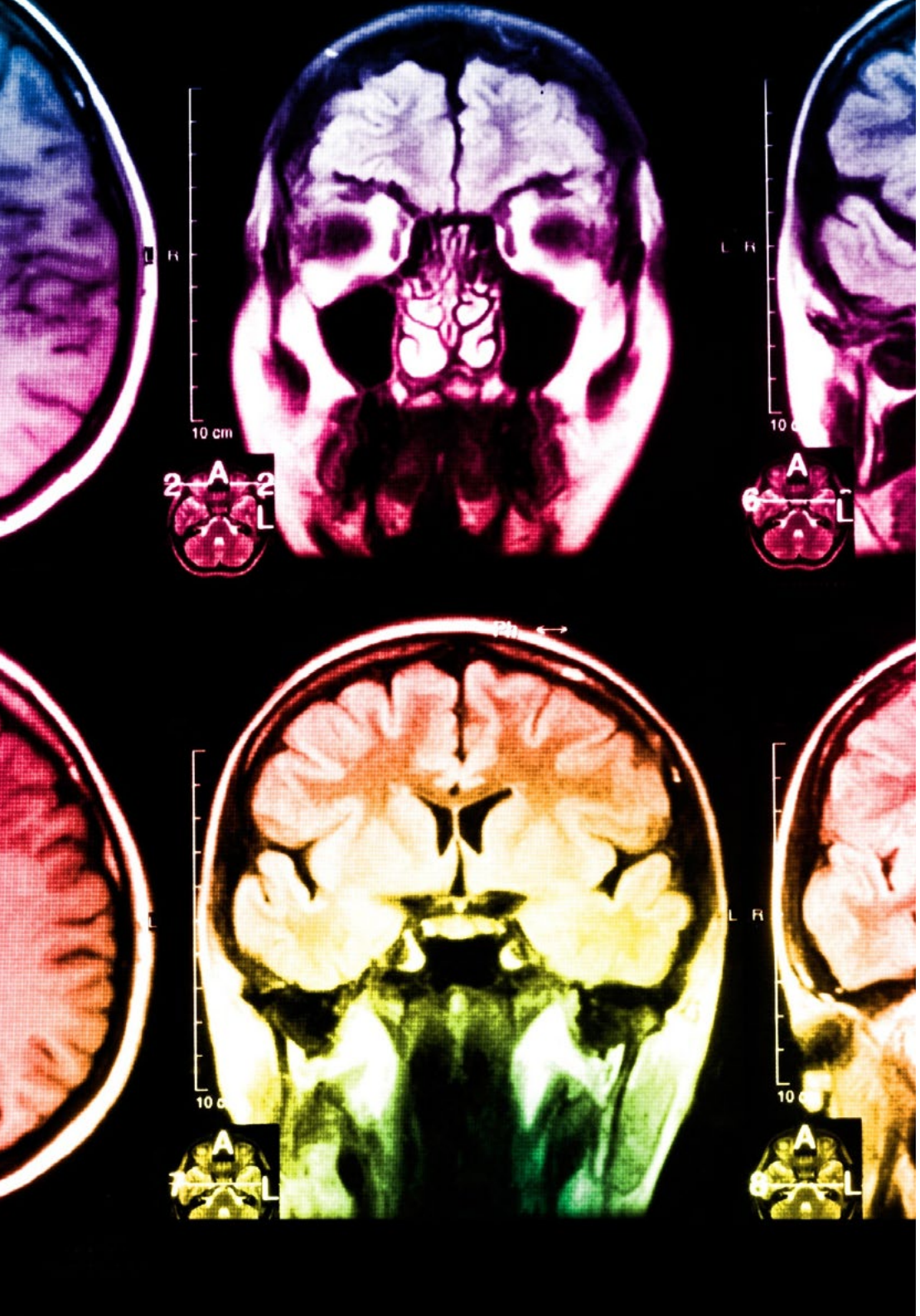
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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 auszubilden. 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 Online-Universität in Spanisch 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 ausgebildet. 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 Ihr Fachgebiet 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 neurokognitiven kontextabhängigen E-Learnings 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 TECH-Online-Arbeitsmethode zu schaffen. Und das alles mit den neuesten Techniken, die dem Studenten qualitativ hochwertige Stücke aus jedem einzelnen Material zur Verfügung stellen.

Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

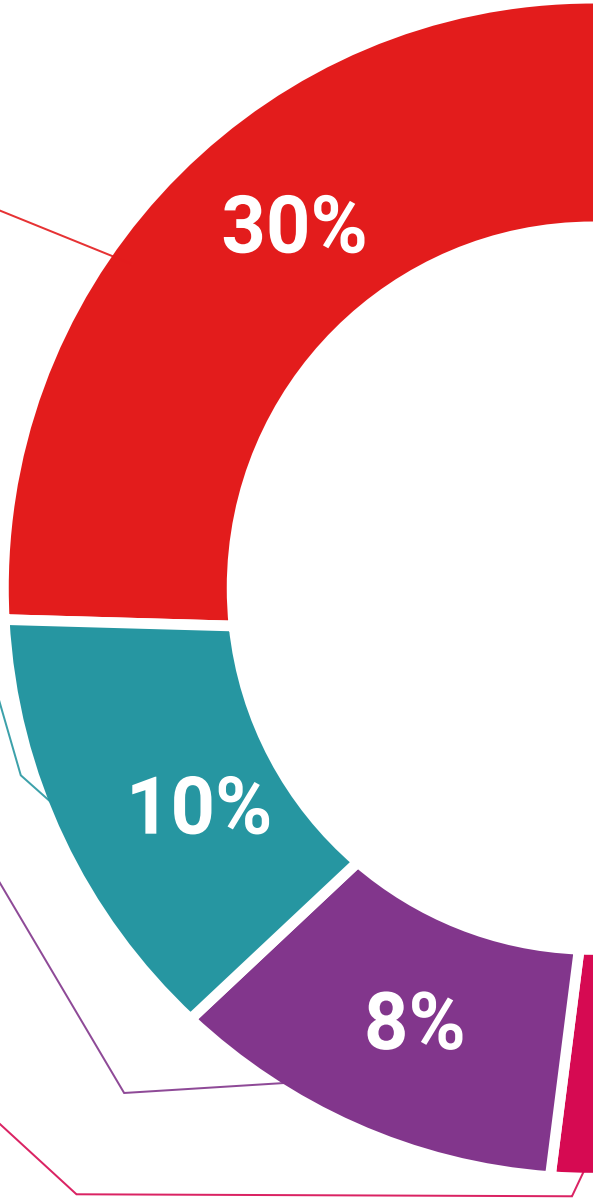
Das sogenannte Learning from an Expert baut Wissen und Gedächtnis auf und schafft Vertrauen für zukünftige schwierige Entscheidungen.

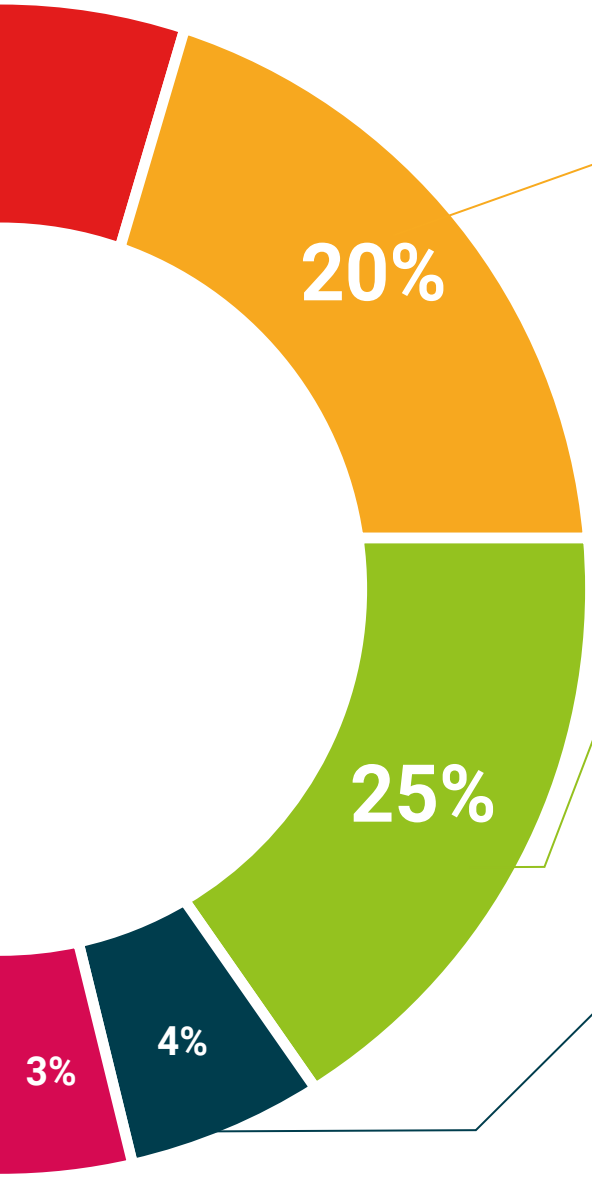
Fertigkeiten und Kompetenzen Praktiken

Sie werden Aktivitäten durchführen, um spezifische Kompetenzen und Fertigkeiten in jedem Fachbereich zu entwickeln. Praktiken und Dynamiken 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 haben die Studenten Zugang zu allem, was sie für ihre Ausbildung benötigen.





Fallstudien

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.

Prüfung und Nachprüfung

Die Kenntnisse der Studenten werden während des gesamten Programms regelmäßig durch Bewertungs- und Selbsteinschätzungsaktivitäten und -übungen beurteilt und neu bewertet, so dass die Studenten überprüfen können, wie sie ihre Ziele erreichen.

06

Qualifizierung

Der Universitätskurs in Reverse Engineering in Cybersicherheit garantiert neben der präzisesten und aktuellsten Fortbildung auch den Zugang zu einem von der TECH Technologischen Universität ausgestellten Diplom.

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

Dieser **Universitätskurs in Reverse Engineering in Cybersicherheit** 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 Reverse Engineering in Cybersicherheit**

Anzahl der offiziellen Arbeitsstunden: **150 Std.**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

UNIVERSITÄTSKURS

in

Reverse Engineering in Cybersicherheit

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
Reverse Engineering in Cybersicherheit

- Modalität: **online**
- Dauer: **6 Wochen**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Universitätskurs
Reverse Engineering in Cybersicherheit

tech technologische universität