Universitätskurs
Cybersicherheit im Netzwerk

tech technologische universität

tech technologische universität

Universitätskurs
Cybersicherheit im Netzwerk

- 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/cybersicherheit-netzwerk

Index

01

Präsentation

Mit dem technologischen Fortschritt nimmt unsere Vernetzung zu und damit auch die Bedrohungen und Angriffstechniken. Je mehr neue Funktionen es gibt und je mehr wir miteinander kommunizieren, desto größer wird unsere Angriffsfläche. Mit anderen Worten, die Möglichkeiten und Wege für Cyberkriminelle, ihre Ziele zu erreichen, nehmen zu. Aus diesem Grund wird in diesem Kurs diskutiert, wie wichtig es ist, eine mehrschichtige Verteidigung, auch „Defence in Depth" genannt, zu entwickeln, die alle Aspekte eines Unternehmensnetzwerks abdeckt. Mit der einzigartigen Qualität von TECH.

Erwerben Sie in nur wenigen Wochen die Fähigkeiten eines Netzwerk-Cybersecurity-Experten mit dem innovativsten Universitätskurs der Online-Bildung"

Wir befinden uns derzeit im Informationszeitalter, im Zeitalter der Konnektivität, in dem wir alle miteinander verbunden sind, sowohl im privaten als auch im geschäftlichen Umfeld.

Die Bandbreite der Bedrohungen ist sehr groß. Sie reicht von einem Trojaner mit eingebautem *Keylogger*, der es über eine E-Mail schafft, den Computer zu infizieren, um an sensible Daten zu gelangen, was sehr lukrativ sein kann, bis hin zu einem Trojaner, der den Computer oder jedes andere Gerät innerhalb des Netzwerks in einen Bot verwandelt, der mit einem *Command & Control*-Server kommuniziert, um einen groß angelegten *Denial-of-Service*-Angriff zu verüben.

Deshalb müssen sich die Sicherheitsüberwachungs- und Abwehrsysteme weiterentwickeln. Denn in einer Welt, in der Telearbeit und Cloud-Dienste immer mehr an Bedeutung gewinnen, reicht eine herkömmliche *Firewall* am Netzwerkrand nicht mehr aus.

Angesichts der riesigen Anzahl von Geräten, die Warnmeldungen generieren, ist außerdem ein Team erforderlich, das diese kontinuierlich überprüft, ein *Security Operations Centre* oder SOC, das dank der Korrelation aller Ereignisse in der Lage ist, von den einfachsten bis hin zu den komplexesten Bedrohungen zu erkennen und in vielen Fällen sogar automatisierte Reaktionen zu erstellen, um die Zeiten für die Eindämmung und Abschwächung von Angriffen zu verkürzen.

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

- Die Entwicklung praktischer Fälle, die von Experten der 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

Technologie und Konnektivität entwickeln sich gleichzeitig mit den Cyber-Bedrohungen weiter: Bleiben Sie auf dem Laufenden über die neuesten Entwicklungen in diesem Bereich"

Ein hochqualifizierter Prozess, der so gestaltet ist, dass er überschaubar und flexibel ist, mit der interessantesten Methodik des Online-Unterrichts”

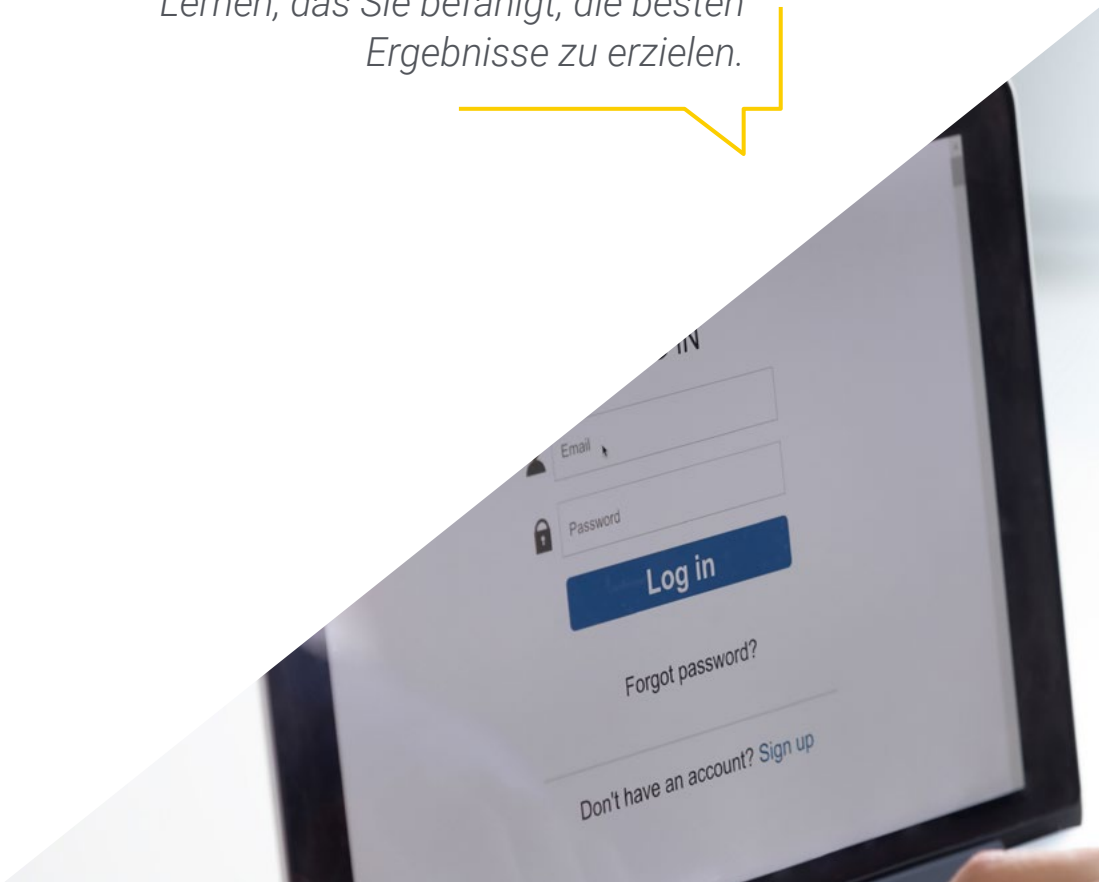
Dieser Universitätskurs ist ganz auf die Praxis ausgerichtet und steigert Ihre Fähigkeiten auf Spezialistenniveau.

Praktisches und kontextbezogenes Lernen, das Sie befähigt, die besten Ergebnisse zu erzielen.

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.

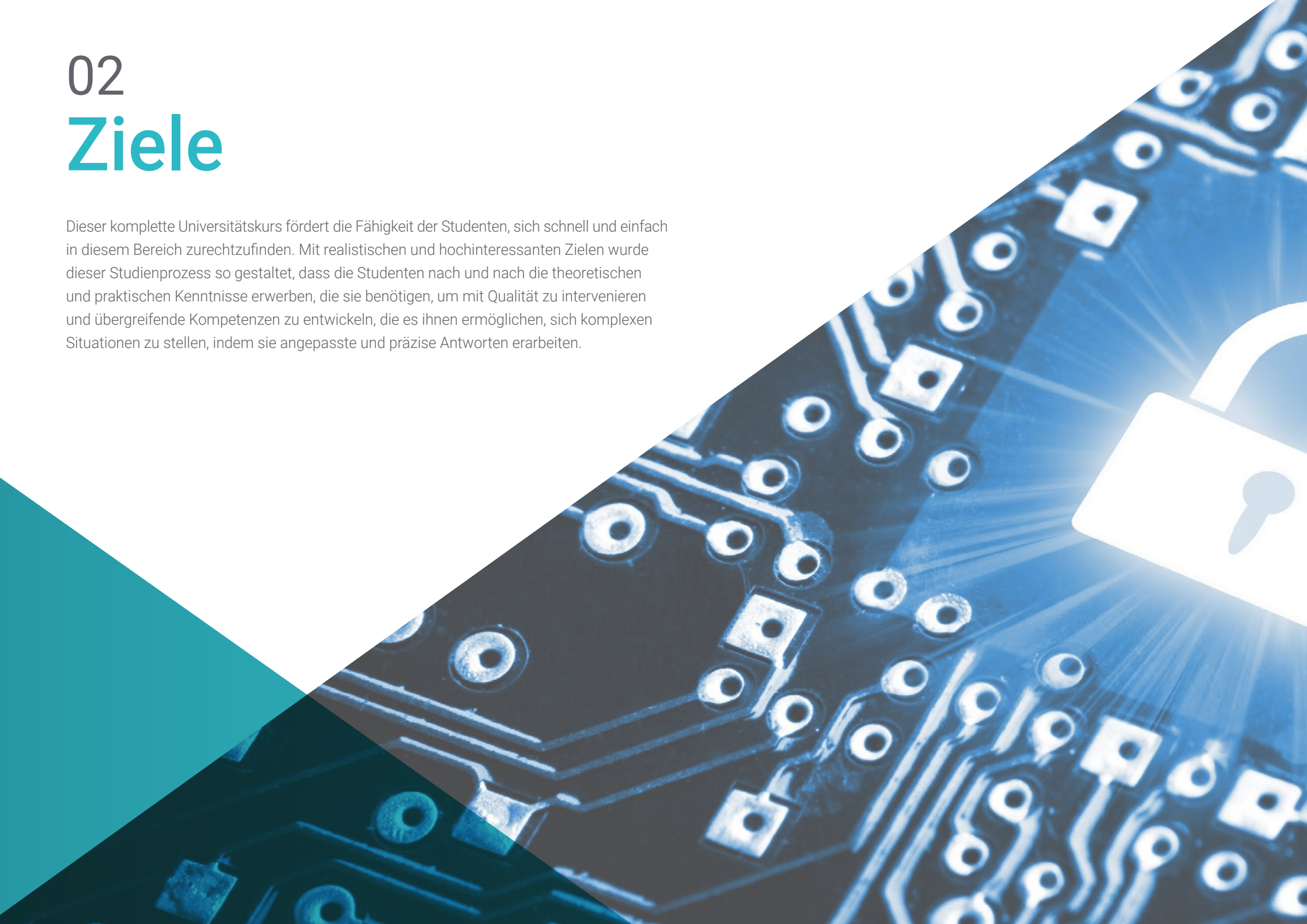
Die Gestaltung dieses Programms konzentriert sich auf problemorientiertes Lernen, bei dem die Fachkraft versuchen muss, die verschiedenen Situationen aus der beruflichen Praxis zu lösen, die während des gesamten Studiengangs gestellt werden. Zu diesem Zweck wird sie von einem innovativen interaktiven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



02

Ziele

Dieser komplette Universitätskurs fördert die Fähigkeit der Studenten, sich schnell und einfach in diesem Bereich zurechtzufinden. 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.

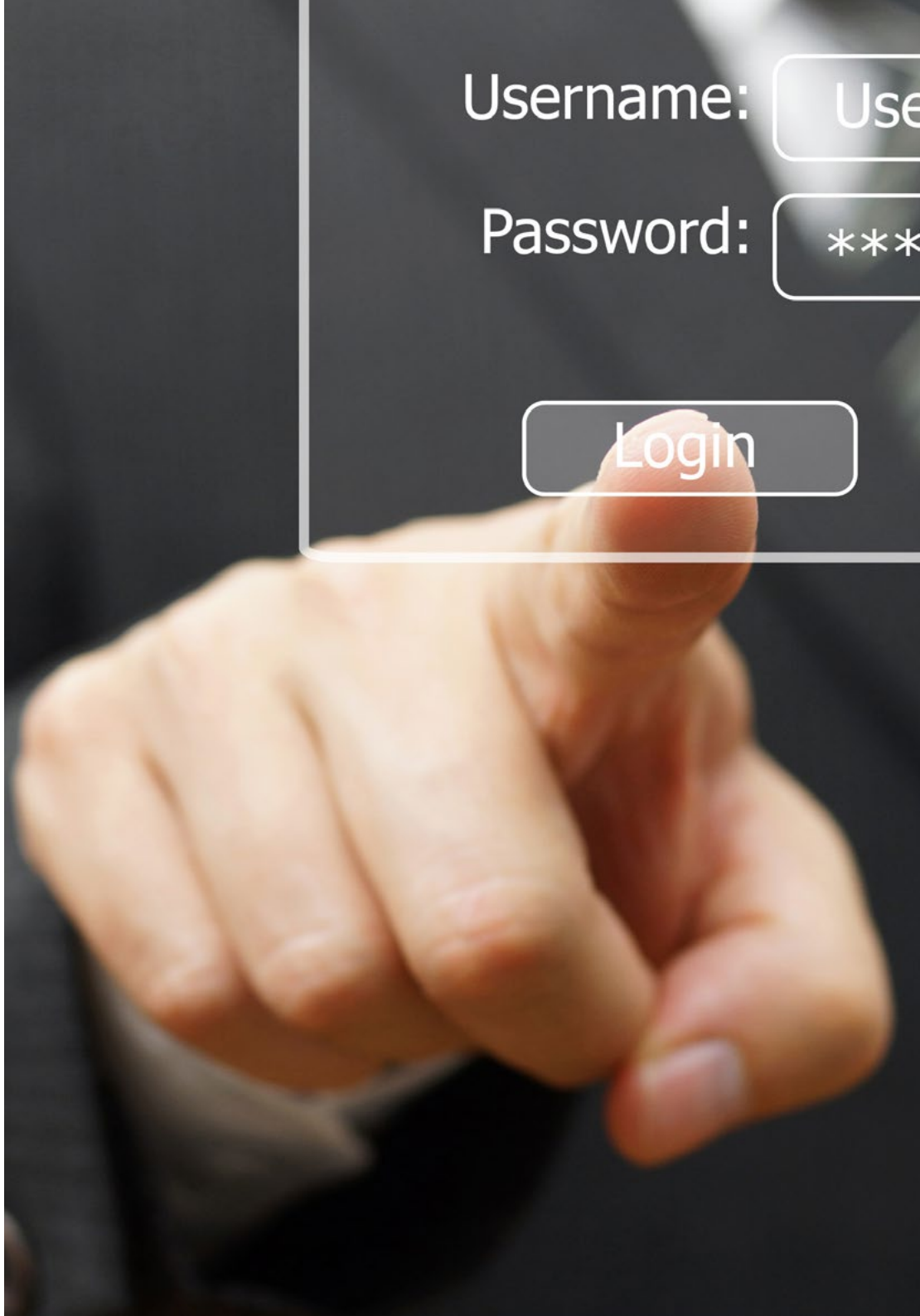


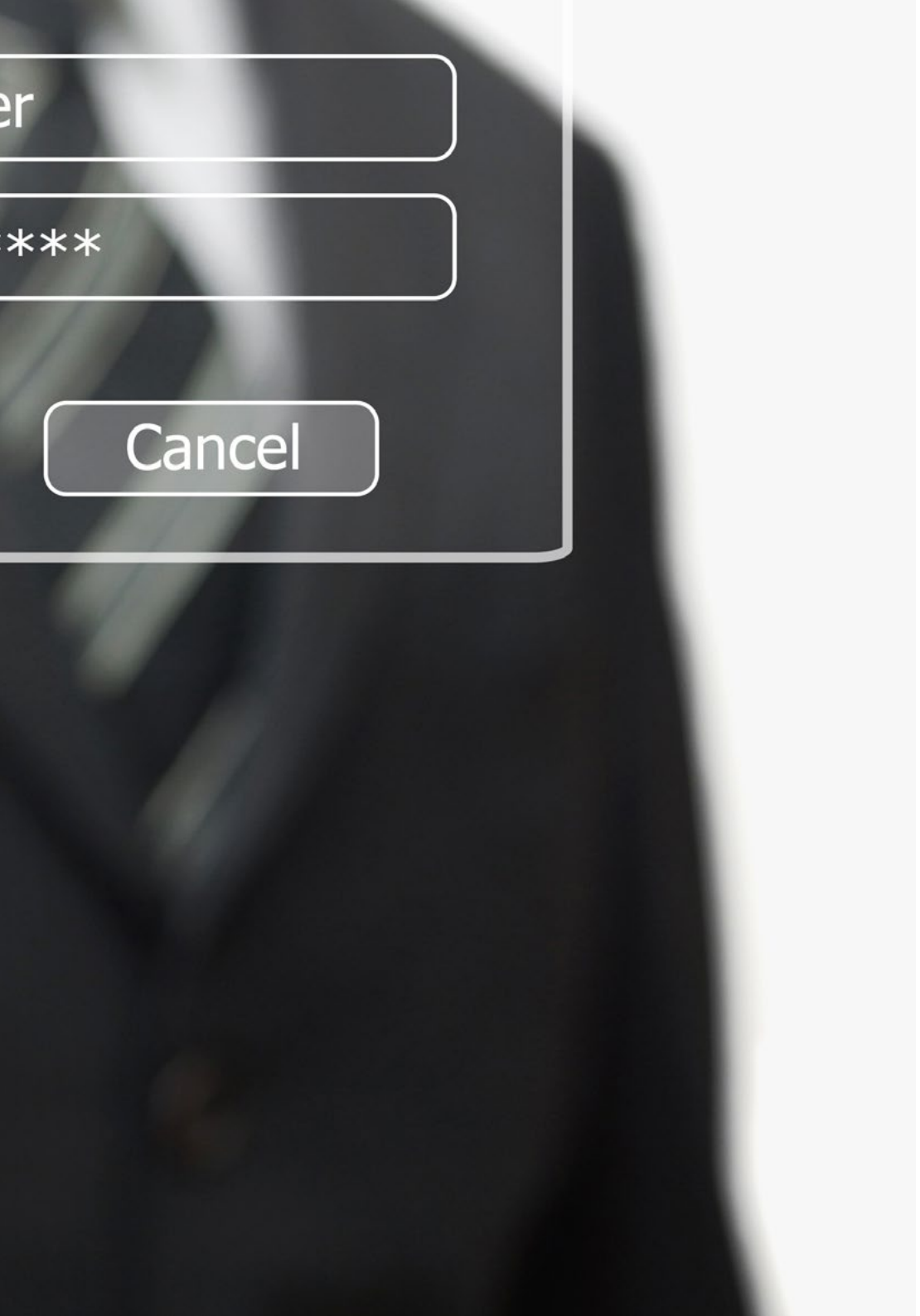
Alle Aspekte, die ein Cybersicherheitsprogramm beherrschen muss, mit einem hochqualifizierten Ziel, das Sie an die vorderste Front der Wettbewerbsfähigkeit bringt"

Allgemeine Ziele

- Analysieren des allgemeinen Rahmens und der Bedeutung von mehrschichtigen Verteidigungs- und Überwachungssystemen
- Entwickeln von *Firewall*-Lösungen auf Linux-Hosts und bei Cloud-Anbietern
- Bewerten neuer Systeme zur Erkennung von Bedrohungen und ihre Weiterentwicklung gegenüber traditionelleren Lösungen
- Bewerten von neuen Systemen zur Erkennung von Bedrohungen und deren Weiterentwicklung gegenüber herkömmlichen Lösungen
- Erstellen von intelligenten Komplettlösungen zur Automatisierung des Verhaltens bei Zwischenfällen

Ein perfektes Programm, das seinen intensiven Charakter meisterhaft mit Flexibilität verbindet"





Spezifische Ziele

- Analysieren der aktuellen Netzwerkarchitekturen, um den zu schützenden Perimeter zu identifizieren
- Entwickeln von spezifischen *Firewall*- und Linux-Konfigurationen zur Entschärfung der häufigsten Angriffe
- Kompilieren der am häufigsten verwendeten Lösungen wie Snort und Suricata, sowie deren Konfiguration
- Untersuchen der verschiedenen zusätzlichen Schichten, die von *Firewalls* der neuen Generation und Netzwerkfunktionen in Cloud-Umgebungen bereitgestellt werden
- Bestimmen der Tools für den Netzwerkschutz und Aufzeigen, warum sie für eine mehrschichtige Verteidigung von grundlegender Bedeutung sind

03

Kursleitung

Die Dozenten, die dieses Programm unterrichten, wurden aufgrund ihrer außergewöhnlichen Kompetenz in diesem Bereich ausgewählt. Sie verbinden technische und praktische Erfahrung mit Unterrichtserfahrung und bieten den Studenten erstklassige Unterstützung bei der Erreichung ihrer Ziele. Durch sie bietet das Programm 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 Cybersicherheit begleiten Sie in jeder Phase des Studiums und vermitteln Ihnen die realistischste Sicht auf diese Arbeit"

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

- Ausbilderin für Computersicherheit und *Ethical Hacking*, Nationales Referenzzentrum für IT und Telekommunikation in Getafe, Madrid
- Zertifizierte *E-Council*-Ausbilderin, Madrid
- Kursleitung der 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. Peralta Alonso, Jon

- Rechtsanwalt/DSB Altia Consultores S.A.
- Dozent im Masterstudiengang für Datenschutz, Cybersicherheit und IKT-Recht, Öffentliche Universität des Baskenlandes (UPV-EHU)
- Rechtsanwalt/Rechtsbeistand, Arriaga Asociados Asesoramiento Jurídico y Económico, SL
- Rechtsberater/Praktikant, Professionelles Büro: Oscar Padura
- Hochschulabschluss in Jura, Öffentliche Universität des Baskenlandes
- Masterstudiengang in Datenschutzbeauftragter, EIS *Innovative School*
- Masterstudiengang in Rechtswissenschaften, Öffentliche Universität des Baskenlandes
- Masterstudiengang in Zivilprozessrecht, Internationale Universität Isabel I de Castilla

Hr. Jiménez Ramos, Álvaro

- Senior Sicherheitsanalyst bei *The Workshop*
- L1 *Cybersecurity Analyst* bei Axians
- L2 *Cybersecurity Analyst* bei Axians
- Cybersecurity-Analyst bei SACYR S.A.
- Hochschulabschluss in Telematik-Ingenieurwesen an der Polytechnischen Universität von Madrid
- Masterstudiengang Cybersicherheit und ethisches Hacking von CICE
- Fortgeschrittenenkurs in Cybersicherheit von Deusto Formación

04

Struktur und Inhalt

Dieser Universitätskurs ist eine vollständige Analyse aller Wissensgebiete, die eine Fachkraft, die sich mit Cybersicherheit beschäftigt, auf dem Gebiet der Netzwerk-*Cybersecurity* kennen muss. Zu diesem Zweck wurde er mit Blick auf den effizienten Erwerb von summativem Wissen strukturiert, das es ermöglicht, das Gelernte zu vertiefen und zu festigen, so dass die Studenten in der Lage sind, so schnell wie möglich zu intervenieren. Ein hochintensiver und qualitativ hochwertiger Kurs, der die Besten des Sektors fortbilden soll.

Ein dynamisch entwickelter Universitätskurs durch einen auf Effizienz ausgerichteten Studienansatz"

Modul 1. Netzwerksicherheit (Perimeter)

1.1. Systeme zur Erkennung und Abwehr von Bedrohungen
- 1.1.1. Allgemeiner Rahmen für Sicherheitsvorfälle
- 1.1.2. Aktuelle Verteidigungssysteme: *Defense in Depth* und SOC
- 1.1.3. Aktuelle Netzwerkarchitekturen
- 1.1.4. Arten von Tools zur Erkennung und Verhinderung von Vorfällen
  - 1.1.4.1. Netzwerkbasierte Systeme
  - 1.1.4.2. Host-basierte Systeme
  - 1.1.4.3. Zentralisierte Systeme
- 1.1.5. Kommunikation und Erkennung von Instanzen/Hosts, Containern und *Serverless*

1.2. *Firewall*
- 1.2.1. Arten von *Firewalls*
- 1.2.2. Angriffe und Schadensbegrenzung
- 1.2.3. Gängige *Firewalls* in Kernel Linux
  - 1.2.3.1. UFW
  - 1.2.3.2. Nftables und iptables
  - 1.2.3.3. *Firewalld*
- 1.2.4. Erkennungssysteme auf der Grundlage von Systemlogs
  - 1.2.4.1. TCP *Wrappers*
  - 1.2.4.2. *BlockHosts* und *DenyHosts*
  - 1.2.4.3. Fail2Ban

1.3. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
- 1.3.1. Angriffe auf IDS/IPS
- 1.3.2. IDS/IPS-Systeme
  - 1.3.2.1. *Snort*
  - 1.3.2.2. Suricata

1.4. *Firewalls* der nächsten Generation (NGFW)
- 1.4.1. Unterschiede zwischen NGFW und traditionellen *Firewalls*
- 1.4.2. Kernkapazitäten
- 1.4.3. *Business*-Lösungen
- 1.4.4. *Firewalls* für Cloud-Dienste
  - 1.4.4.1. Cloud VPC Architektur
  - 1.4.4.2. Cloud ACLs
  - 1.4.4.3. *Security Group*

1.5. *Proxy*
  1.5.1. Arten von *Proxys*
  1.5.2. *Proxy*-Nutzung. Vorteile und Nachteile
1.6. Antivirus-Engines
  1.6.1. Allgemeiner Kontext von Malware und IOCs
  1.6.2. Probleme mit Anti-Viren-Programmen
1.7. Mailschutzsysteme
  1.7.1. Antispam
    1.7.1.1. Whitelisting und Blacklisting
    1.7.1.2. Bayessche Filter
  1.7.2. *Mail Gateway* (MGW)
1.8. SIEM
  1.8.1. Komponenten und Architektur
  1.8.2. Korrelationsregeln und Anwendungsfälle
  1.8.3. Aktuelle Herausforderungen von SIEM-Systemen
1.9. SOAR
  1.9.1. SOAR und SIEM: Feinde oder Verbündete?
  1.9.2. Die Zukunft der SOAR-Systeme
1.10. Andere netzwerkbasierte Systeme
  1.10.1. WAF
  1.10.2. NAC
  1.10.3. *HoneyPots* und *HoneyNets*
  1.10.4. CASB

Ein hochwirksamer Lehrplan, der Ihnen hilft, die heutigen Bedrohungen zu verstehen, damit Sie mit Agilität und spezialisierten Ressourcen handeln können"

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

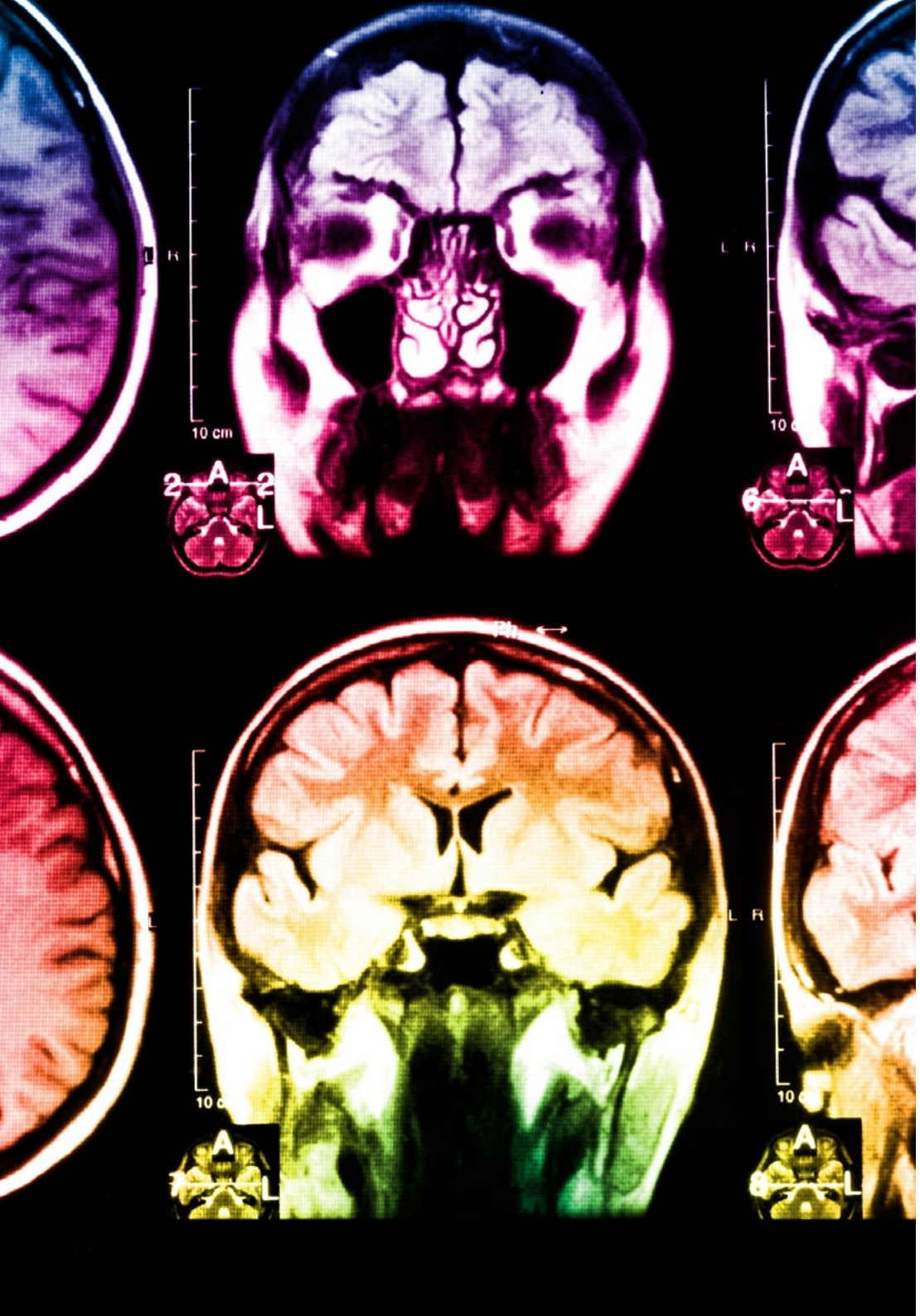
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

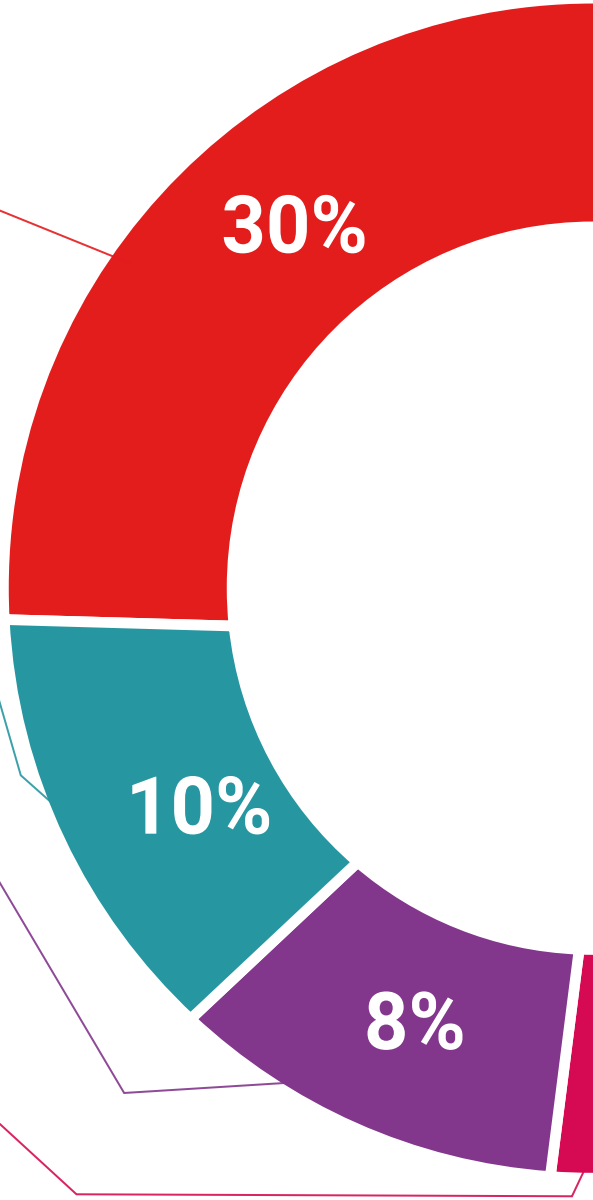
Das sogenannte Learning from an Expert baut Wissen und Gedächtnis auf und schafft Vertrauen für zukünftige schwierige Entscheidungen.

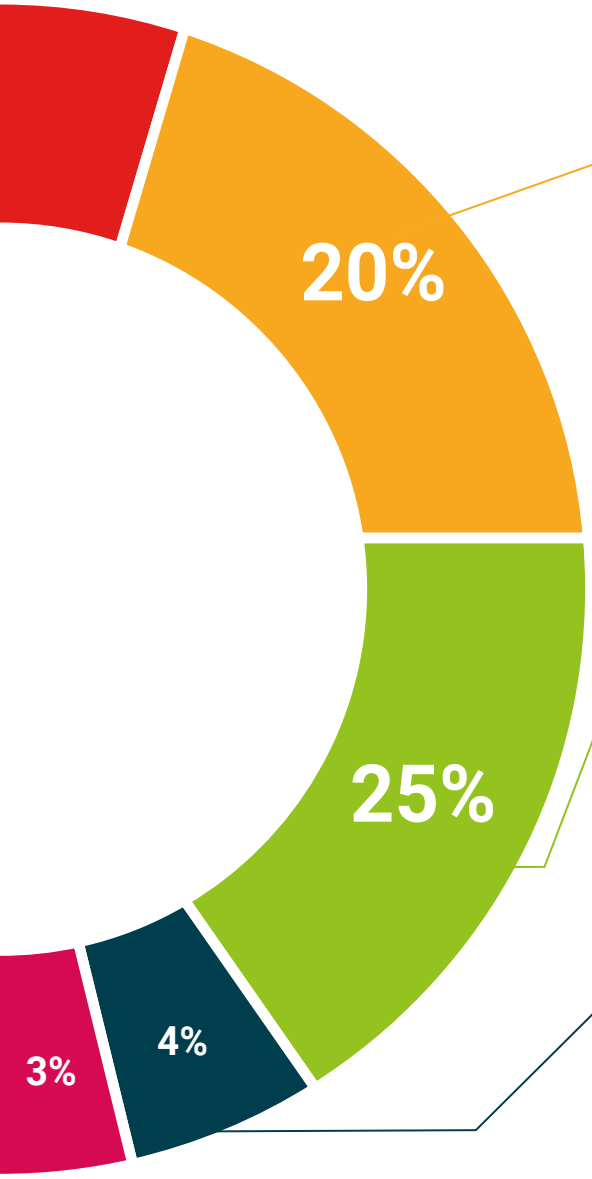
Fertigkeiten und Kompetenzen Praktiken

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 Cybersicherheit im Netzwerk 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 Cybersicherheit im Netzwerk** 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 Cybersicherheit im Netzwerk**

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

Cybersicherheit im Netzwerk

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.beschaffen.

tech technologische universität

Universitätskurs
Cybersicherheit im Netzwerk

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

Universitätskurs
Cybersicherheit im Netzwerk

tech technologische universität