Universitätsexperte
Defensive Cybersicherheit

tech technologische universität

tech technologische universität

Universitätsexperte
Defensive Cybersicherheit

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

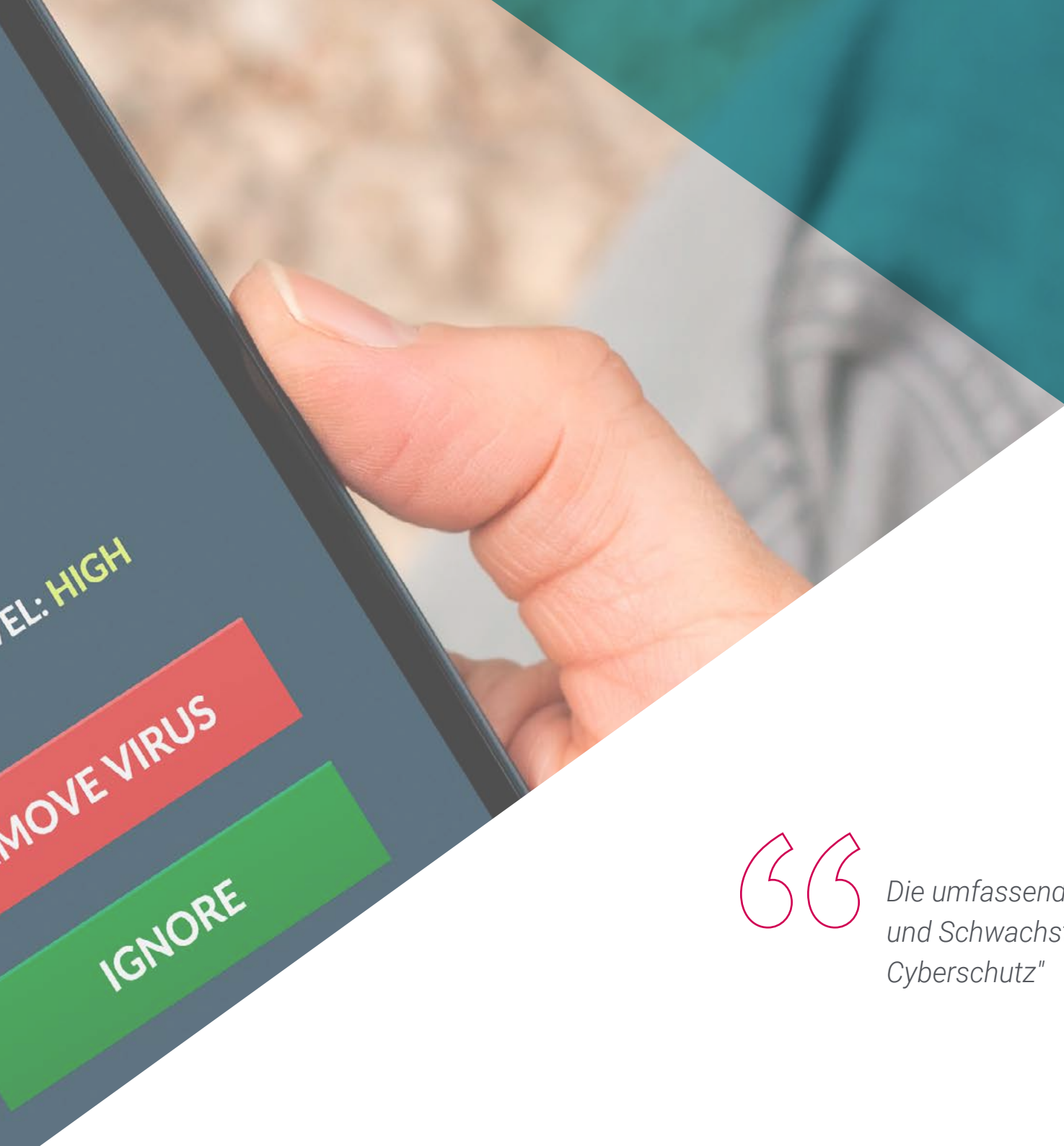
Internetzugang: www.techtitute.com/de/informatik/spezialisierung/spezialisierung-defensive-cybersicherheit

Index

01

Präsentation

In der heutigen Zeit, in der das tägliche Leben direkt mit der Nutzung mobiler Geräte verbunden ist, ist das Wissen um die möglichen Formen der Verwundbarkeit, die mit ihrer Nutzung einhergehen, ein zwingendes Bedürfnis für Fachleute in den technologischen Branchen. Die Raffinesse der Modelle hat ihnen eine noch nie dagewesene Arbeitsfähigkeit verliehen, die sie zu unersetzlichen Werkzeugen gemacht hat, die sogar auf sensible persönliche und geschäftliche Daten zugreifen. In diesem Programm werden alle Aspekte, die zu Cyberangriffen führen können, eingehend untersucht und die derzeit innovativsten und effektivsten Verteidigungsstrategien für die Cybersicherheit entwickelt. Ein hochqualifizierender Kurs, der Sie in die Lage versetzt, als Spezialist auf diesem Gebiet zu agieren.



Die umfassendste Tour durch die Gefahren und Schwachstellen mobiler Geräte und deren Cyberschutz"

Die Sicherheit von Privathaushalten und Unternehmen muss schichtweise aufgebaut sein. Sie ist wie eine Kette und nur so stark wie das schwächste Glied in der Kette. In diesem Universitätsexperten werden die wichtigsten Bedrohungen für die Computer der Benutzer und die Server vorgestellt, so dass wir in der Lage sind, die entsprechenden Maßnahmen zu ergreifen und in jeder Situation wachsam zu sein.

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. Deshalb müssen sich auch 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. Aus diesem Grund wird dieser Experte auch auf die Bedeutung einer mehrschichtigen Verteidigung eingehen, die auch als *Defence in Depth* bekannt ist und alle Aspekte eines Unternehmensnetzwerks abdeckt, wobei einige der vorgestellten Konzepte und Systeme auch in einer häuslichen Umgebung genutzt und angewendet werden können.

Als großartige Ergänzung zum Lehrplan bietet das Programm den Studenten auch zusätzliche Lektionen in Cybersicherheit. Dabei handelt es sich um *Masterclasses*, die von einem international renommierten Dozenten, einem Spezialisten für Intelligenz, Cybersicherheit und disruptive Technologien, vorbereitet wurden. So wird der IT-Profi in die grundlegenden Aspekte der defensiven Cybersicherheit eintauchen, wie z. B. Antivirus, Firewalls oder Eindringlingsdetektoren (HIDS).

Hundertprozentige Sicherheit gibt es nicht, aber wenn wir uns der Arten von Angriffen bewusst sind, denen wir ausgesetzt sind, und wenn wir über die notwendigen Informationen verfügen, um damit umzugehen, haben wir einen wichtigen Schritt getan und eine weitere Sicherheitsschicht für unsere Daten hinzugefügt.

Dieser **Universitätsexperte in Defensive Cybersicherheit** enthält das vollständigste und aktuellste wissenschaftliche Programm auf dem Markt. Die wichtigsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten präsentiert werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren wissenschaftlichen und praktischen Informationen
- Die praktischen Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens durchgeführt werden kann
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden
- Theoretische Lektionen, 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

Möchten Sie sich auf die defensive Cybersicherheit spezialisieren? Dank der Masterclasses, die von einem Spezialisten für Intelligenz, Cybersicherheit und disruptive Technologien entwickelt wurden, werden Sie dies erreichen“

Ein kompletter Rundgang, der es Ihnen ermöglicht, zu wissen, worum es sich bei den aktuellen Cyberbedrohungen handelt und wie sie funktionieren, um eine Grundlage für die Entwicklung von Verteidigungsstrategien zu schaffen"

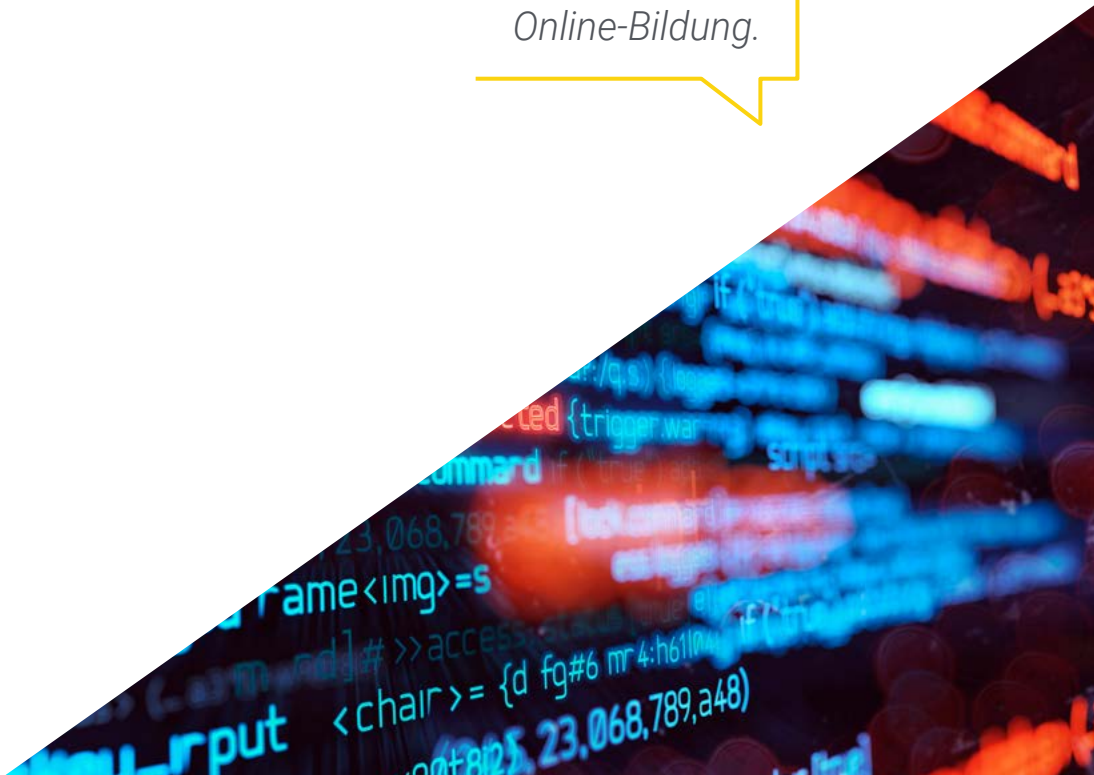
Dieser Universitätsexperte ist ganz auf die Praxis ausgerichtet und wird Ihre Fähigkeiten auf das Niveau eines Spezialisten bringen.

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

Zu den Dozenten des Programms gehören Experten aus der Branche, die ihre Erfahrungen in diese Fortbildung einbringen, sowie anerkannte Spezialisten aus 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

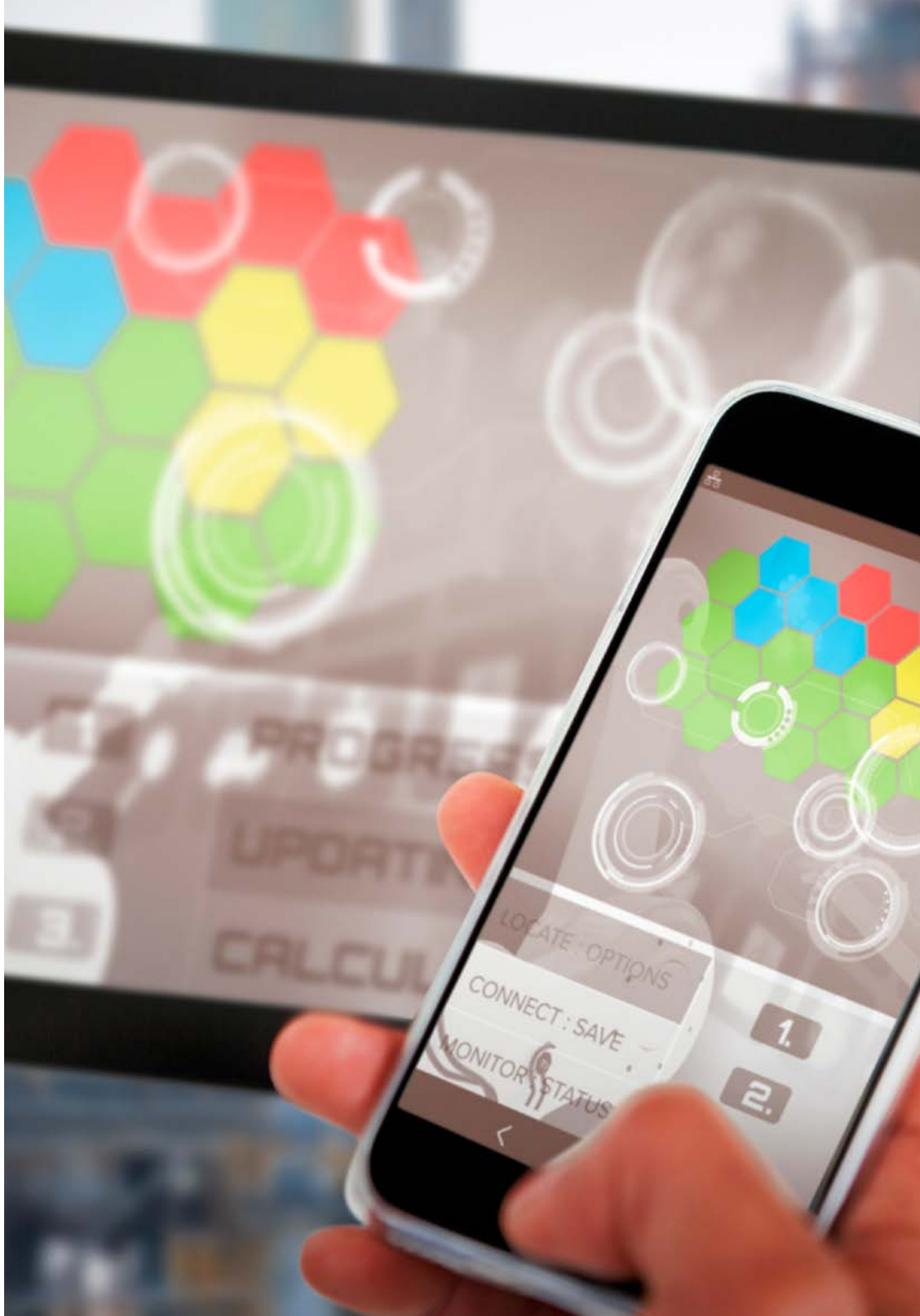
Ziele

Die Teilnahme an diesem Universitätsexperten ermöglicht es, sich in der Fähigkeit, in diesem Bereich zu intervenieren, exponentiell zu verbessern. Mit realistischen und hochinteressanten Zielen wurde dieser Studiengang so konzipiert, dass die Studenten nach und nach die theoretischen und praktischen Kenntnisse erwerben, die für ein qualitativ hochwertiges Eingreifen erforderlich sind, und gleichzeitig bereichsübergreifende Kompetenzen entwickeln, die es ihnen ermöglichen, komplexe Situationen zu meistern, indem sie angemessene und präzise Antworten entwickeln.

Eine vollständige Aktualisierung aller Aspekte, die die defensive Cybersicherheit in letzter Zeit hervorgebracht hat"

Allgemeine Ziele

- Bewerten der Sicherheit der Computer der Benutzer und der Server
- Untersuchen potenzieller Bedrohungen basierend auf der Nutzungsumgebung
- Analysieren der Lösungen für jede Bedrohung
- Entwickeln geeigneter Nutzungsrichtlinien
- Analysieren des allgemeinen Rahmens, der Bedeutung von mehrschichtigen Verteidigungs- und Überwachungssystemen
- Prüfen von Erkennungs- und Präventionssystemen für wichtige Bedrohungen
- Entwickeln von *Firewall*-Lösungen für *Linux-Hosts* und *Cloud*-Anbieter
- Bewerten von neuen Systemen zur Erkennung von Bedrohungen und deren Weiterentwicklung gegenüber herkömmlichen Lösungen
- Erstellen von intelligenten Komplettlösungen zur Automatisierung des Verhaltens bei Zwischenfällen
- Analysieren der wichtigsten aktuellen mobilen Plattformen, ihrer Funktionen und Nutzung
- Untersuchen der vorhandenen Schwachstellen und Bedrohungen sowie der wichtigsten Angriffsvektoren
- Bewerten der Risiken im Zusammenhang mit Schwachstellen außerhalb innerhalb des Unternehmens
- Ermitteln von Tools und Best-Practice-Richtlinien für die Sicherung mobiler Geräte
- Analysieren des IoT in verschiedenen Bereichen von heute
- Untersuchen der Entwicklung und der Auswirkungen des IoT
- Bestimmen der Bestandteile eines IoT-Projekts
- Identifizieren, Analysieren und Bewerten der Sicherheitsrisiken von IoT-Projektteilen



Spezifische Ziele

Modul 1. Host-Sicherheit

- Festlegen der *Backup*-Richtlinien für persönliche und berufliche Daten
- Bewerten der verschiedenen Tools, um Lösungen für bestimmte Sicherheitsprobleme zu finden
- Etablieren von Mechanismen, um das System auf dem neuesten Stand zu halten
- Analysieren der Ausrüstung zur Erkennung von Eindringlingen
- Festlegen der Regeln für den Zugriff auf das System
- Prüfen und Klassifizieren von Mails, um Betrug zu vermeiden
- Erstellen von Listen mit erlaubter Software

Modul 2. Netzwerksicherheit (Perimeter)

- 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

Modul 3. Smartphone-Sicherheit

- Untersuchen der verschiedenen Angriffsvektoren, um zu vermeiden, ein leichtes Ziel zu werden
- Bestimmen der wichtigsten Angriffe und Arten von *Malware*, denen Benutzer mobiler Geräte ausgesetzt sind
- Analysieren der aktuellsten Geräte, um eine sicherere Konfiguration zu erstellen
- Festlegen der wichtigsten Schritte zur Durchführung eines Penetrationstests auf iOS- und Android-Plattformen
- Entwickeln von Fachwissen über die verschiedenen Schutz und Sicherheitstools
- Etablieren von *Best Practices* bei der Programmierung für mobile Geräte

Modul 4. IoT-Sicherheit

- Analysieren der wichtigsten IoT-Architekturen
- Untersuchen von Verbindungstechnologien
- Entwickeln der wichtigsten Anwendungsprotokolle
- Erkennen der verschiedenen Arten von vorhandenen Geräten
- Bewerten der Risikostufen und bekannten Schwachstellen
- Entwickeln von Richtlinien zur sicheren Nutzung
- Festlegen geeigneter Bedingungen für die Verwendung dieser Geräte

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 der Universitätskurs die direkteste und unmittelbarste Sicht auf die realen Merkmale der Intervention in diesem Bereich und erreicht eine kontextuelle Vision von maximalem Interesse.

Der direkte Blick auf einen Beruf, der ständig in Bewegung ist, durch erfahrene Fachleute, die Ihnen einen möglichst realistischen Einblick in diese Arbeit geben"

Internationaler Gastdirektor

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**, **Cyberbedrohungen** 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

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

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

Leitung

Fr. Fernández Sapena, Sonia

- Ausbilderin für Computersicherheit und Ethical Hacking am Nationalen Referenzzentrum von Getafe für Informatik und Telekommunikation von Madrid
- Zertifizierte E-Council-Ausbilderin
- 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*) an der Universität der Balearischen Inseln
- Computer- Ingenieurin von der Universität von Alcalá de Henares in Madrid
- Masterstudiengang in DevOps: Docker und Kubernetes, Cas-Training
- Microsoft Azure Security Techonologies, E-Council

Professoren

Fr. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Applikationsentwicklung bei B60, UK
- Analytikerin-Programmiererin für die Verwaltung, Koordination und Dokumentation einer virtualisierten Sicherheitsalarmumgebung
- Analytikerin-Programmiererin von Java-Anwendungen in Geldautomaten für Kunden
- Software Development-Expertin für die Validierung von Unterschriften und die Anwendung zur Dokumentenverwaltung
- Systemtechnikerin für die Migration von Geräten und für die Verwaltung, Wartung und Schulung von PDA-Mobilgeräten vor Ort
- Technische Ingenieurin für Computersysteme von der Offenen Universität von Katalonien (UOC)
- Masterstudiengang in Computersicherheit und Ethical Hacking Offizieller EC-Council und CompTIA von der Fachhochschule für neue Technologien CICE

Hr. Peralta Alonso, Jon

- Senior Consultant - Datenschutz und Cybersicherheit
- Jurist / Rechtsberater bei Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Rechtsberater / Praktikant in einer professionellen Kanzlei: Óscar Padura
- Hochschulabschluss in Jura an der Öffentlichen Universität des Baskenlandes
- Masterstudiengang in Datenschutzbeauftragter an der EIS Innovative School
- Masterstudiengang in Anwaltschaft an der Öffentlichen Universität des Baskenlandes
- Masterstudiengang in Zivilprozessrecht an der Internationalen Universität Isabel I. von Kastilien
- Dozent im Masterstudiengang für Datenschutz, Cybersicherheit und IKT-Recht

Hr. Catalá Barba, José Francisco

- Elektroniker mit Erfahrung in Cybersicherheit
- Entwickler von mobilen Anwendungen
- Elektroniker im mittleren Führungsstab des spanischen Verteidigungsministeriums
- Elektroniker im Ford-Werk in Valencia

Hr. Jiménez Ramos, Álvaro

- Cybersecurity Analyst
- 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 in Cybersicherheit und ethisches Hacken von CICE
- Fortgeschrittenenkurs in Cybersicherheit von Deusto Formación

Eine einzigartige, wichtige und entscheidende Fortbildungserfahrung, die Ihre berufliche Entwicklung fördert"

04

Struktur und Inhalt

Der Lehrplan dieses Programms deckt alle Wissensbereiche ab, die eine Fachkraft, die sich mit Cybersicherheit beschäftigt, im Bereich der Abwehrmaßnahmen kennen muss. Zu diesem Zweck wurde er mit Blick auf den effizienten Erwerb von summativem Wissen strukturiert, das es ermöglicht, das Gelernte zu durchdringen 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.

Alle Aspekte, die für eine defensive Cybersicherheitsanalyse und -intervention erforderlich sind, werden auf strukturierte Weise in einem auf Effizienz ausgerichteten Studienansatz entwickelt“

Modul 1. *Host*-Sicherheit

1.1. Sicherungskopien
- 1.1.1. Strategien zur Datensicherung
- 1.1.2. Tools für Windows
- 1.1.3. Tools für Linux
- 1.1.4. Tools für MacOS

1.2. Benutzer-Antivirus
- 1.2.1. Arten von Antivirenprogrammen
- 1.2.2. Antivirus für Windows
- 1.2.3. Antivirus für Linux
- 1.2.4. Antivirus für MacOS
- 1.2.5. Antivirus für Smartphones

1.3. HIDS Eindringlingsdetektoren
- 1.3.1. Methoden zur Erkennung von Eindringlingen
- 1.3.2. Sagan
- 1.3.3. Aide
- 1.3.4. *Rkhunter*

1.4. Lokale *Firewall*
- 1.4.1. *Firewalls* für Windows
- 1.4.2. *Firewalls* für Linux
- 1.4.3. *Firewalls* für MacOS

1.5. Passwortmanager
- 1.5.1. Password
- 1.5.2. *LastPass*
- 1.5.3. *KeePass*
- 1.5.4. *Sticky Password*
- 1.5.5. RoboForm

1.6. *Phishing*-Detektoren
- 1.6.1. Manuelle *Phishing*-Erkennung
- 1.6.2. *Anti-Phishing*-Tools

1.7. *Spyware*
- 1.7.1. Vermeidungsmechanismen
- 1.7.2. *Anti-Spyware*-Tools

1.8. Tracker
- 1.8.1. Maßnahmen zum Schutz des Systems
- 1.8.2. Anti-Tracker-Tools

1.9. *EDR - End Point Detection and Response*
- 1.9.1. Verhalten des EDR-Systems
- 1.9.2. Unterschiede zwischen EDR und Anti-Virus
- 1.9.3. Die Zukunft der EDR-Systeme

1.10. Kontrolle über die Software-Installation
- 1.10.1. Repositories und Software-Speicher
- 1.10.2. Listen mit erlaubter oder verbotener Software
- 1.10.3. Update-Kriterien
- 1.10.4. Berechtigungen für die Software-Installation

Modul 2. Netzwerksicherheit (Perimeter)

2.1. Systeme zur Erkennung und Abwehr von Bedrohungen
- 2.1.1. Allgemeiner Rahmen für Sicherheitsvorfälle
- 2.1.2. Aktuelle Verteidigungssysteme: *Defense in Depth* und SOC
- 2.1.3. Aktuelle Netzwerkarchitekturen
- 2.1.4. Arten von Tools zur Erkennung und Verhinderung von Vorfällen
  - 2.1.4.1. Netzwerkbasierte Systeme
  - 2.1.4.2. *Host*-basierte Systeme
  - 2.1.4.3. Zentralisierte Systeme
- 2.1.5. Kommunikation und Erkennung von Instanzen/*Hosts*, Containern und *Serverless*

2.2. *Firewall*
- 2.2.1. Arten von *Firewalls*
- 2.2.2. Angriffe und Schadensbegrenzung
- 2.2.3. Gängige *Firewalls* in *Kernel* Linux
  - 2.2.3.1. UFW
  - 2.2.3.2. Nftables und iptables
  - 2.2.3.3. *Firewalld*

2.2.4. Erkennungssysteme auf der Grundlage von *Systemlogs*
2.2.4.1. TCP *Wrappers*
2.2.4.2. *BlockHosts* und *DenyHosts*
2.2.4.3. Fail2Ban
2.3. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
2.3.1. Angriffe auf IDS/IPS
2.3.2. IDS/IPS-Systeme
2.3.2.1. *Snort*
2.3.2.2. Suricata
2.4. *Firewalls* der nächsten Generation (NGFW)
2.4.1. Unterschiede zwischen NGFW und traditionellen *Firewalls*
2.4.2. Kernkapazitäten
2.4.3. Business-Lösungen
2.4.4. *Firewalls* für *Cloud*-Dienste
2.4.4.1. Cloud-VPC-Architektur
2.4.4.2. *Cloud* ACLs
2.4.4.3. *Security Group*
2.5. *Proxy*
2.5.1. Arten von *Proxys*
2.5.2. *Proxy*-Nutzung. Vor- und Nachteile
2.6. Antivirus-Engines
2.6.1. Allgemeiner Kontext von *Malware* und IOCs
2.6.2. Probleme mit Anti-Viren-Programmen
2.7. Mailschutzsysteme
2.7.1. Antispam
2.7.1.1. Whitelisting und Blacklisting
2.7.1.2. Bayessche Filter
2.7.2. *Mail Gateway* (MGW)
2.8. SIEM
2.8.1. Komponenten und Architektur
2.8.2. Korrelationsregeln und Anwendungsfälle
2.8.3. Aktuelle Herausforderungen von SIEM-Systemen
2.9. SOAR
2.9.1. SOAR und SIEM: Feinde oder Verbündete?
2.9.2. Die Zukunft der SOAR-Systeme
2.10. Andere netzwerkbasierte Systeme
2.10.1. WAF
2.10.2. NAC
2.10.3. *HoneyPots* und *HoneyNets*
2.10.4. CASB

Modul 3. Smartphone-Sicherheit

3.1. Die Welt der mobilen Geräte
3.1.1. Arten von mobilen Plattformen
3.1.2. IOS-Geräte
3.1.3. Android-Geräte
3.2. Verwaltung der mobilen Sicherheit
3.2.1. OWASP-Projekt für mobile Sicherheit
3.2.1.1. Top 10 Schwachstellen
3.2.2. Kommunikation, Netzwerke und Verbindungsarten
3.3. Das mobile Gerät in der Unternehmensumgebung
3.3.1. Risiken
3.3.3. Geräteüberwachung
3.3.4. Verwaltung mobiler Geräte (MDM)
3.4. Datenschutz und Datensicherheit
3.4.1. Informationsstände
3.4.3. Sichere Speicherung von Daten
3.4.3.1. Sichere Speicherung auf iOS
3.4.3.2. Sicherer Speicher auf Android
3.4.4. Bewährte Praktiken bei der Applikationsentwicklung
3.5. Schwachstellen und Angriffsvektoren
3.5.1. Schwachstellen
3.5.2. Angriffsvektoren
3.5.2.1. *Malware*
3.5.2.2. Exfiltration von Daten
3.5.2.3. Datenmanipulation

3.6. Wichtigste Bedrohungen
- 3.6.1. Ungezwungener Benutzer
- 3.6.2. *Malware*
  - 3.6.2.1. Arten von *Malware*
- 3.6.3. Social Engineering
- 3.6.4. Datenleck
- 3.6.5. Datendiebstahl
- 3.6.6. Ungesicherte WiFi-Netzwerke
- 3.6.7. Veraltete Software
- 3.6.8. Bösartige Anwendungen
- 3.6.9. Unsichere Passwörter
- 3.6.10. Schwache oder nicht vorhandene Sicherheitseinstellungen
- 3.6.11. Physischer Zugang
- 3.6.12. Verlust oder Diebstahl des Geräts
- 3.6.13. Impersonation (Integrität)
- 3.6.14. Schwache oder defekte Kryptographie
- 3.6.15. Denial of Service (DoS)

3.7. Große Angriffe
- 3.7.1. *Phishing*-Angriffe
- 3.7.2. Angriffe im Zusammenhang mit Kommunikationsmodi
- 3.7.3. *Smishing*-Angriffe
- 3.7.4. *Criptojacking*-Angriffe
- 3.7.5. *Man in The Middle*

3.8. *Hacking*
- 3.8.1. *Rooting* und *Jailbreaking*
- 3.8.2. Anatomie eines mobilen Angriffs
  - 3.8.2.1. Ausbreitung der Bedrohung
  - 3.8.2.2. Installation von *Malware* auf dem Gerät
  - 3.8.2.3. Persistenz
  - 3.8.2.4. Ausführen der *Payload* und Extrahieren der Informationen
- 3.8.3. *Hacking* auf IOS-Geräten: Mechanismen und Tools
- 3.8.4. *Hacking* auf Android-Geräten: Mechanismen und Tools

3.9. Penetrationstests
- 3.9.1. iOS *Pentesting*
- 3.9.2. Android *Pentesting*
- 3.9.3. Hilfsmittel

3.10. Schutz und Sicherheit
- 3.10.1. Sicherheitseinstellungen
  - 3.10.1.1. Auf iOS-Geräten
  - 3.10.1.2. Auf Android-Geräten
- 3.10.2. Sicherheitsmaßnahmen
- 3.10.3. Schutz-Tools

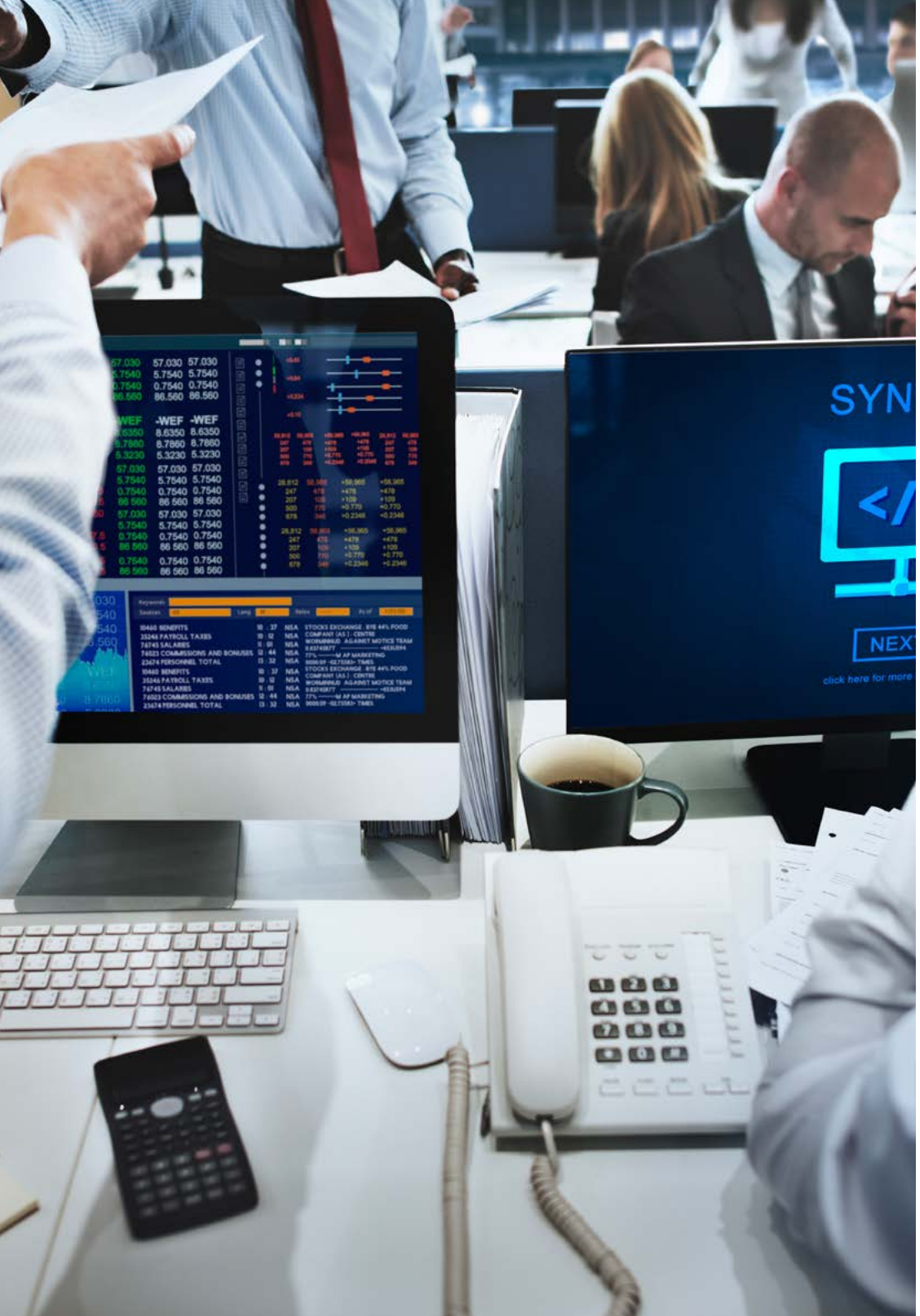
Modul 4. IoT-Sicherheit

4.1. Geräte
- 4.1.1. Arten von Geräten
- 4.1.2. Standardisierte Architekturen
  - 4.1.2.1. OneM2M
  - 4.1.2.2. IoTWF
- 4.1.3. Anwendungsprotokolle
- 4.1.4. Konnektivitätstechnologien

4.2. IoT-Geräte. Anwendungsbereiche
- 4.2.1. SmartHome
- 4.2.2. SmartCity
- 4.2.3. Transport
- 4.2.4. *Wearables*
- 4.2.5. Gesundheitssektor
- 4.2.6. IIoT

4.3. Kommunikationsprotokolle
- 4.3.1. MQTT
- 4.3.2. LWM2M
- 4.3.3. OMA-DM
- 4.3.4. TR-069

4.4. SmartHome
- 4.4.1. Hausautomatisierung
- 4.4.2. Netzwerke
- 4.4.3. Haushaltsgeräte
- 4.4.4. Überwachung und Sicherheit



4.5. SmartCity
- 4.5.1. Beleuchtung
- 4.5.2. Meteorologie
- 4.5.3. Sicherheit

4.6. Transport
- 4.6.1. Standort
- 4.6.2. Zahlungen leisten und Dienstleistungen in Anspruch nehmen
- 4.6.3. Konnektivität

4.7. Wearables
- 4.7.1. Intelligente Kleidung
- 4.7.2. Intelligenter Schmuck
- 4.7.3. Intelligente Uhren

4.8. Gesundheitssektor
- 4.8.1. Training/Herzfrequenzüberwachung
- 4.8.2. Überwachung von Patienten und älteren Menschen
- 4.8.3. Implantierbare Geräte
- 4.8.4. Chirurgische Roboter

4.9. Konnektivität
- 4.9.1. WiFi
- 4.9.2. Bluetooth
- 4.9.3. Eingebettete Konnektivität

4.10. Sicherung
- 4.10.1. Dedizierte Netzwerke
- 4.10.2. Passwortmanager
- 4.10.3. Verwendung von verschlüsselten Protokollen
- 4.10.4. Tipps für die Verwendung

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.

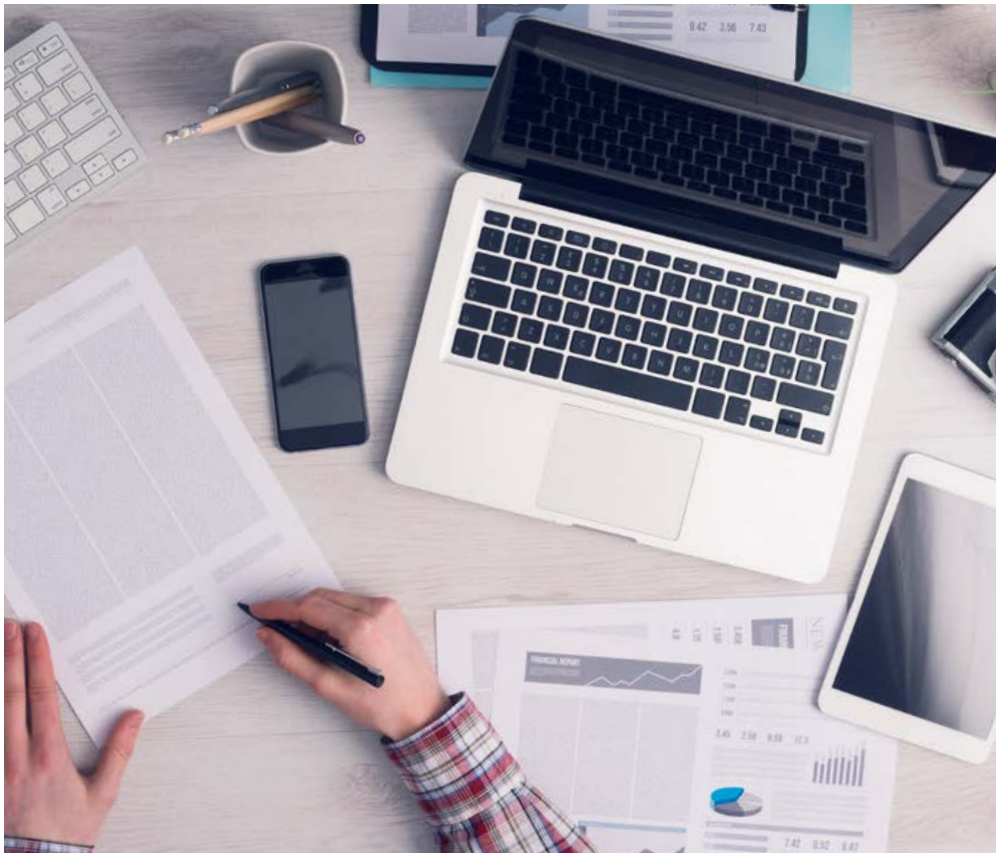
Entdecken Sie Relearning, ein System, das das herkömmliche lineare Lernen hinter sich lässt und Sie durch zyklische Lehrsysteme führt: eine Art des Lernens, die sich als äußerst effektiv erwiesen hat, insbesondere in Fächern, die Auswendiglernen erfordern"

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

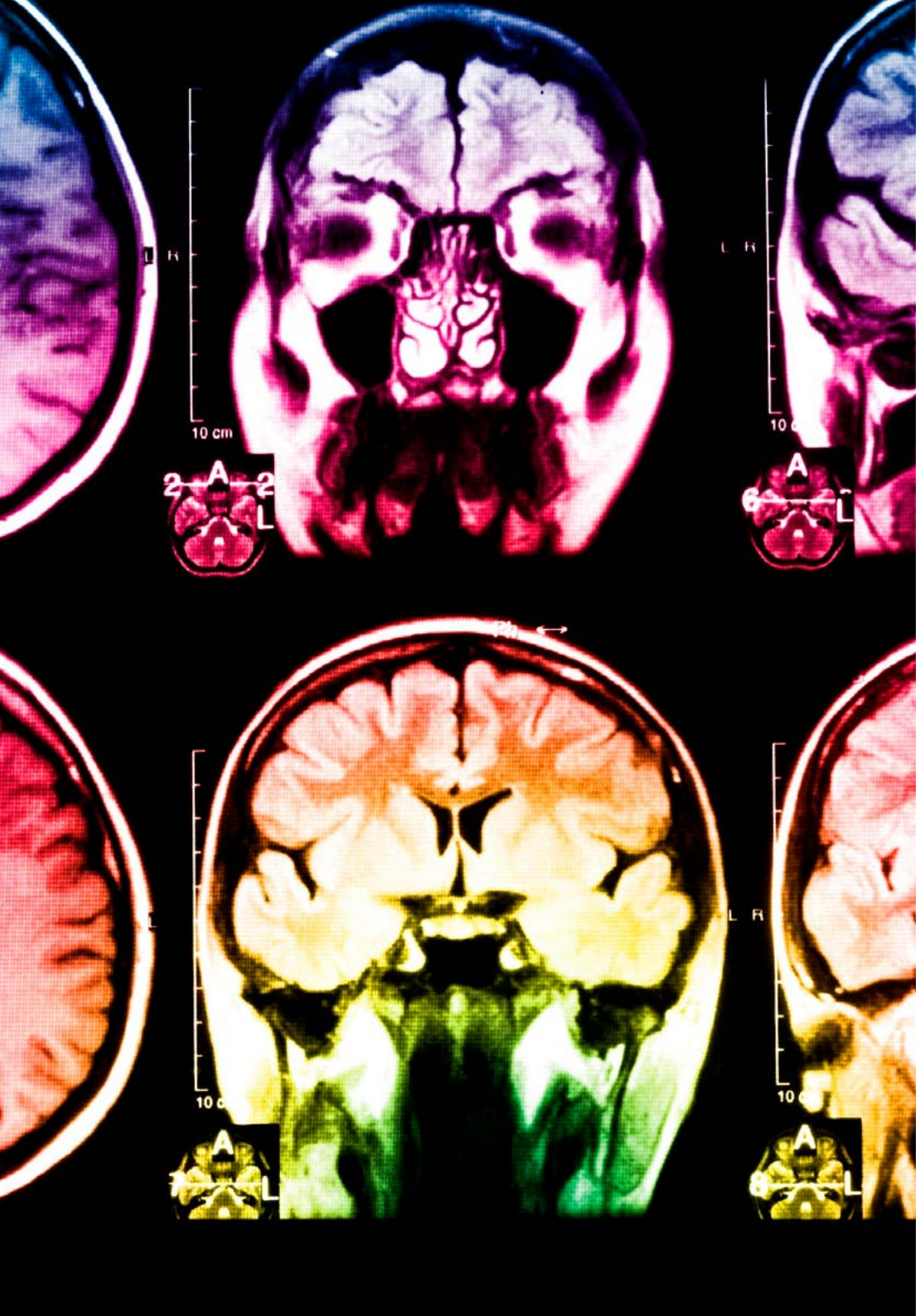
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

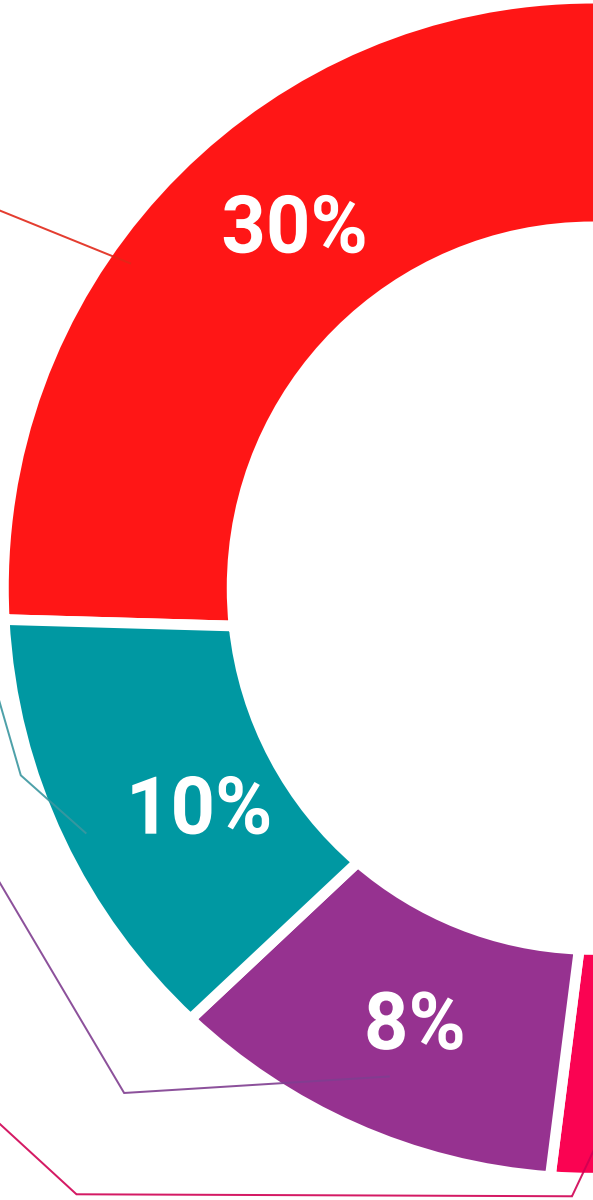
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

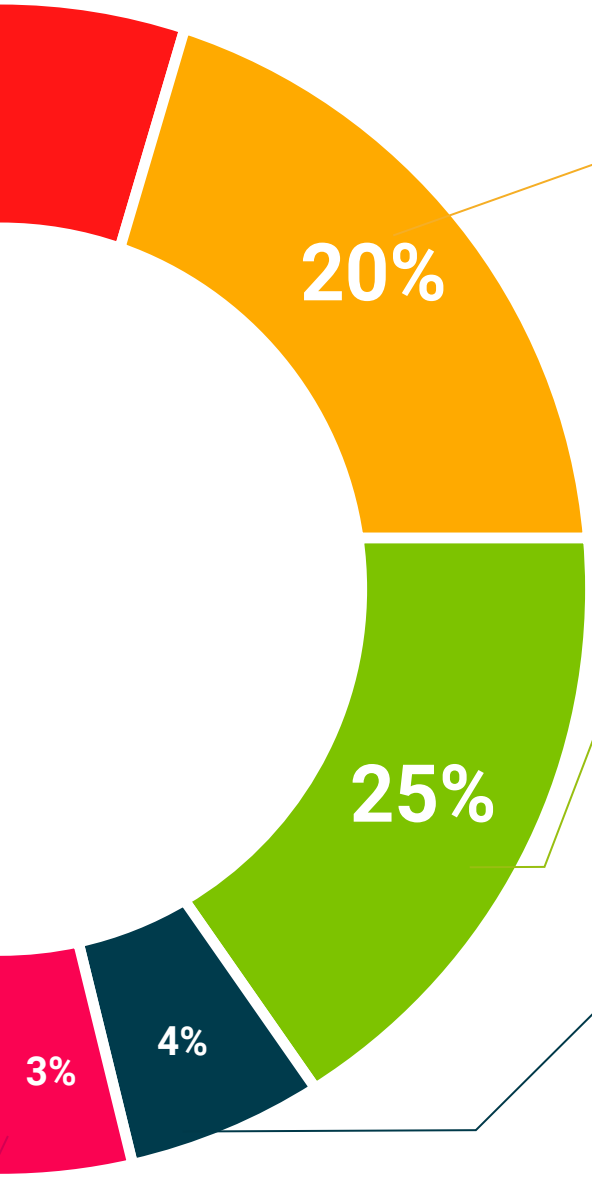
Übungen für Fertigkeiten und Kompetenzen

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 Universitätsexperte in Defensive 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 **Universitätsexperte in Defensive 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.

Títel: **Universitätsexperte in Defensive Cybersicherheit**

Modalität: **online**

Dauer: **6 Monate**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

UNIVERSITÄTSEXPERTE

in

Defensive Cybersicherheit

Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 600 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

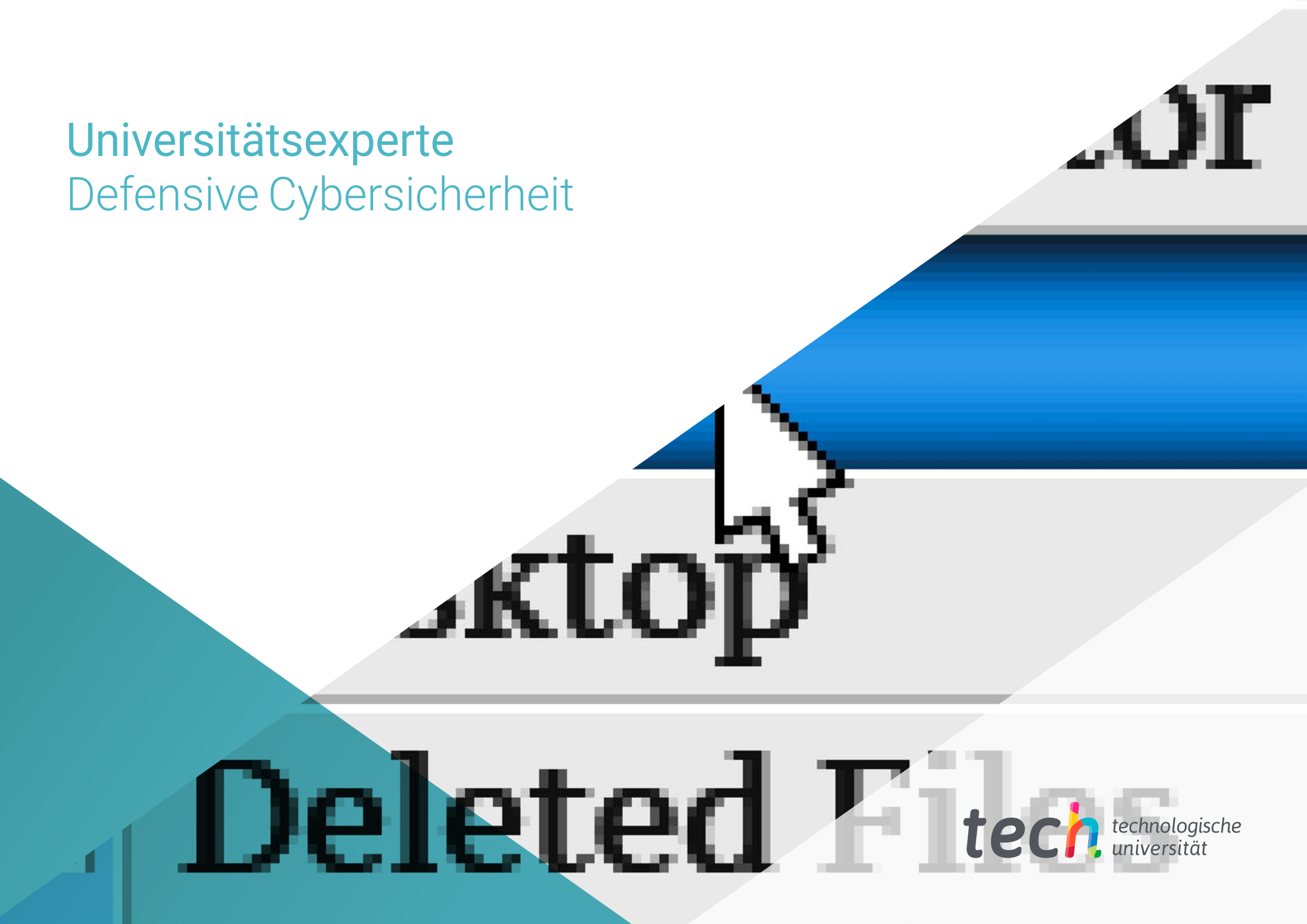
*Haager Apostille. Für den Fall, dass der Student die Haager Apostille für sein Papierdiplom beantragt, wird TECH EDUCATION die notwendigen Vorkehrungen treffen, um diese gegen eine zusätzliche Gebühr zu beschaffen.

tech global university

Universitätsexperte
Defensive Cybersicherheit

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

Universitätsexperte
Defensive Cybersicherheit



tech technologische universität