Universitätsexperte
Maßnahmen zur Cyberabwehr

tech technologische universität

tech technologische universität

Universitätsexperte

Maßnahmen zur Cyberabwehr

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

Internetzugang: **www.techtitute.com/de/informatik/spezialisierung/spezialisierung-massnahmen-cyberabwehr**

Index

01

Präsentation

Im Finanz-, Handels- und Tourismussektor ist eine Zunahme von Social-Engineering-Angriffen zu verzeichnen, die sensible und wertvolle Informationen der Organisationen selbst und ihrer Kunden gefährden. Cyberangriffe bereiten den Unternehmen nach wie vor Kopfzerbrechen, weshalb in den letzten Jahren immer mehr Arbeitsplätze im Bereich der IT-Sicherheit geschaffen wurden. Als Antwort auf diesen Bedarf bietet dieses Programm IT-Fachkräften eine Spezialisierung im Bereich der Maßnahmen zur Cyberabwehr. Ein fachkundiges Dozententeam unterrichtet diesen Studiengang in einem 100%igen Online-Modus, so dass Sie dank der umfangreichen Multimedia-Inhalte ein aktuelles und umfassendes Wissen erwerben können.

Geben Sie mit diesem Universitätsexperten die beste Antwort in Sachen Computersicherheit und verhindern Sie, dass Unternehmen auf Social Engineering hereinfallen”

Die Umsetzung von Computersicherheitsrichtlinien ist für Unternehmen mit Kosten verbunden, die sie jedoch aufgrund der hohen Verluste, die das Hacken ihrer Systeme mit sich bringt und deren ordnungsgemäße Funktionsweise sowie die Bereitstellung von Dienstleistungen für ihre Kunden gefährdet, bereit sind, dafür zu zahlen. IT-Experten spielen in diesem Szenario eine Schlüsselrolle.

Dieser Universitätsexperte bietet den Studenten eine gründliche Weiterbildung im Bereich der Verteidigungsmaßnahmen im Bereich der Computersicherheit, die auf einer Analyse der Bedrohungen und ihrer korrekten Klassifizierung beruhen, um herauszufinden, wo ein Unternehmen mehr oder weniger verwundbar ist. Ebenso vermittelt das auf dieses Thema spezialisierte Dozententeam die wesentlichen Werkzeuge zur Durchführung einer forensischen Computeranalyse. Auf diese Weise wird die Erkennung von Vorfällen durch IDS/IPS-Systeme und deren Behandlung in SIEM bis hin zum Benachrichtigungs- und Eskalationsprozess demonstriert.

Um bei der Sicherheitsverteidigung an vorderster Front zu stehen, werden IT-Profis in diesem Kurs Techniken entwickeln, um *Denial of Service, Session Hacking* und Angriffe auf Webanwendungen zu entschärfen. All dies wird zu 100% online gelehrt, so dass die Studenten ihre berufliche Tätigkeit mit einem Programm verbinden können, das innovative Multimedia-Inhalte bietet. Sie benötigen nur ein Gerät mit Internetanschluss, um auf einen Lehrplan zuzugreifen, den sie in ihrem eigenen Tempo absolvieren können.

Dieser **Universitätsexperte in Maßnahmen zur Cyberabwehr** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten für Computersicherheit präsentiert werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren technischen und praktischen Informationen
- 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 Zugriffs auf die Inhalte von jedem beliebigen Gerät ob stationär oder tragbar mit einer Internetverbindung

Implementieren Sie mit diesem Universitätsexperten effiziente Sicherheitsrichtlinien gegen Session Hijacking, Hacking von Webservern oder mobilen Plattformen"

Beherrschen Sie die ISO-Norm 27035 und erfüllen Sie die Anforderungen an ein korrektes Incident Management. Schreiben Sie sich für diesen Universitätsexperten ein”

Steigern Sie Ihre Karrierechancen mit einem Programm, das Sie tiefer in die Analyse und Bekämpfung von Computerbedrohungen eintauchen lässt.

Sie sind nur einen Klick davon entfernt, sich für einen Universitätsexperten einzuschreiben, der Ihnen neue Karrieremöglichkeiten eröffnet.

Zu den Dozenten des Programms gehören Fachleute aus der Branche, die ihre Erfahrungen aus ihrer Arbeit in diese Weiterbildung einbringen, sowie anerkannte Spezialisten aus führenden Unternehmen und renommierten Universitäten.

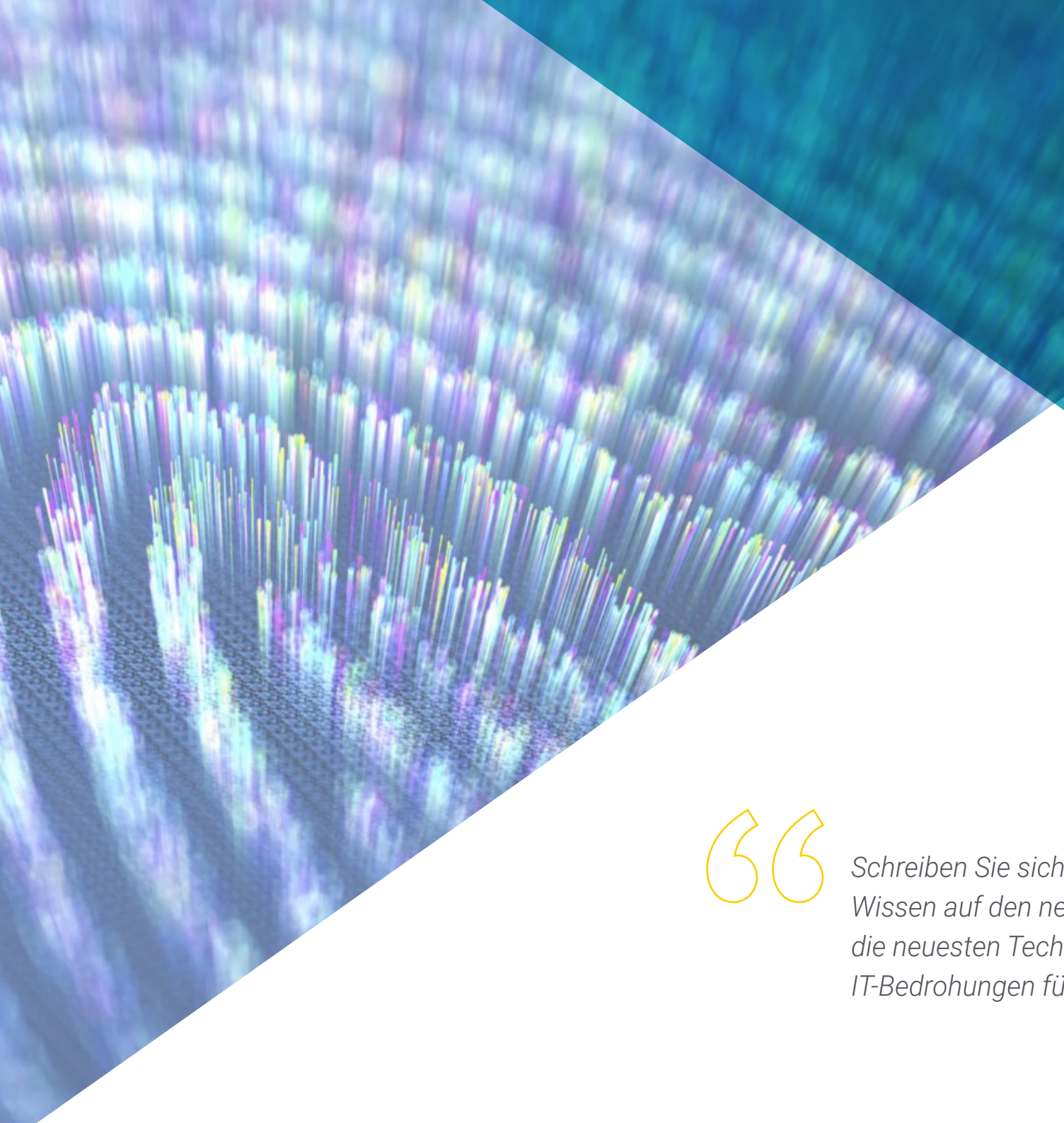
Die multimedialen Inhalte, die mit der neuesten Bildungstechnologie entwickelt wurden, werden der Fachkraft ein situiertes und kontextbezogenes Lernen ermöglichen, d. h. eine simulierte Umgebung, die eine immersive Fortbildung bietet, die auf die Ausführung von realen Situationen ausgerichtet ist.

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

02

Ziele

Der Universitätsexperte bietet eine Weiterbildung, die darauf abzielt, IT-Fachkräften eine spezialisierte Qualifikation im Bereich der Sicherheit zu vermitteln. Während des Programms verbessern Sie Ihre Fähigkeiten in der Bedrohungsanalyse und vergleichen verschiedene Managementmethoden, um die für den jeweiligen Vorfall am besten geeignete auszuwählen. Sie werden auch in der technischen Umsetzung von Maßnahmen fortgebildet, um die wichtigsten Bedrohungen für das Unternehmen zu entschärfen. Auf diese Weise erhalten IT-Fachkräfte eine Qualifikation, die ihnen einen beruflichen Aufstieg ermöglicht.



Schreiben Sie sich jetzt ein. Bringen Sie Ihr Wissen auf den neuesten Stand und lernen Sie die neuesten Techniken kennen, um den größten IT-Bedrohungen für Unternehmen vorzubeugen"

Allgemeine Ziele

- Vertiefen der wichtigsten Konzepte der Informationssicherheit
- Entwickeln der notwendigen Maßnahmen zur Gewährleistung guter Informationssicherheitspraktiken
- Entwickeln der verschiedenen Methoden zur Durchführung einer umfassenden Bedrohungsanalyse
- Installieren und Erlernen der verschiedenen Tools, die bei der Behandlung und Vorbeugung von Vorfällen eingesetzt werden

Erweren Sie eine Hochschulqualifikation, die Ihnen die innovativsten und effizientesten Strategien zur Bewältigung von IT-Angriffen vermittelt"

Spezifische Ziele

Modul 1. Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen

- Analysieren der Bedeutung von Bedrohungen
- Bestimmen der Phasen des präventiven Bedrohungsmanagements
- Vergleichen verschiedener Methoden des Bedrohungsmanagements

Modul 2. Richtlinien für das Management von Sicherheitsvorfällen

- Entwickeln von Fachwissen über den Umgang mit Vorfällen, die durch Computersicherheitsereignisse verursacht werden
- Festlegen der Arbeitsweise eines Teams zur Bearbeitung von Sicherheitsvorfällen
- Analysieren der verschiedenen Phasen des Managements von IT-Sicherheitsvorfällen
- Untersuchen der standardisierten Protokolle für den Umgang mit Sicherheitsvorfällen

Modul 3. Praktische Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen

- Bestimmen der verschiedenen realen Angriffe auf unser Informationssystem
- Bewerten der verschiedenen Sicherheitsmaßnahmen zur Eindämmung von Angriffen
- Implementieren der technischen Maßnahmen zur Abschwächung der wichtigsten Bedrohungen

03

Kursleitung

TECH wählt alle Dozenten, die die Studiengänge unterrichten, sorgfältig aus. Der Universitätsexperte verfügt über ein hochqualifiziertes Dozententeam im Bereich der IT-Sicherheit. Ihre Erfahrungen als Sicherheitsverantwortliche in diesem Bereich in öffentlichen und privaten Einrichtungen garantieren den Studenten ein fundiertes Wissen, das für Fachleute, die aus erster Hand die wichtigsten Maßnahmen in diesem Bereich angesichts der größten Bedrohungen kennenlernen möchten, von großem Wert ist. Auf diese Weise ähneln die vorgestellten praktischen Fälle den realen Situationen, mit denen die Studenten in ihrem Arbeitsumfeld konfrontiert werden, und werden sie in ihrer beruflichen Entwicklung unterstützen.

Ein auf Computersicherheit spezialisiertes Dozententeam stellt Ihnen sein gesamtes Wissen zur Verfügung, damit Sie in Ihrer beruflichen Laufbahn vorankommen"

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)
- Computer- Ingenieurin an der Universität von Alcalá de Henares von Madrid
- Masterstudiengang in DevOps: Docker und Kubernetes, Cas-Training
- Microsoft Azure Security Techonologies, E-Council

Professoren

Fr. López García, Rosa María

- Spezialistin für Management-Informationen
- Dozentin am Linux Professional Institute
- Mitarbeiterin der Hackerkademie Incibe
- Cybersecurity Talent Captain bei Teamciberhack
- Verwaltungs-, Buchhaltungs- und Finanzmanagerin bei Integra2Transportes
- Verwaltungsassistentin für den Einkauf von Ressourcen im Bildungszentrum Cardenal Marcelo Espínola
- Höhere Technikerin in Cybersicherheit und ethischem Hacking
- Mitglied von Ciberpatrulla

Hr. Oropesiano Carrizosa, Francisco

- Computer-Ingenieur
- Mikroinformatiker, Netzwerktechniker und Sicherheitstechniker bei Cas-Training
- Entwickler für Webdienste, CMS, e-Commerce, UI und UX bei Fersa Reparaciones
- Manager für Webdienste, Inhalte, Mail und DNS bei Oropesia Web & Network
- Grafiker und Designer für Webanwendungen bei Xarxa Sakai Projectes
- Universitätskurs in Computersystemen an der Universität von Alcalá de Henares
- Masterstudiengang in DevOps: Docker and Kubernetes von Cyber Business Center
- Techniker für Netzwerke und Computersicherheit von der Universität der Balearischen Inseln
- Experte in Grafikdesign von der Polytechnischen Universität von Madrid

04

Struktur und Inhalt

Die Dozenten dieses Universitätsexperten haben einen Lehrplan entwickelt, der jede Phase der Entwicklung eines Sicherheitsplans für den Umgang mit Bedrohungen für Computersysteme eingehend behandelt. So werden die Analyse der Bedrohung, ihre Klassifizierung, das Vorfallmanagement und die neuesten Tools zu ihrer Erkennung ausführlich behandelt. Auch die Probleme, die durch Social Engineering in den betroffenen Unternehmen entstehen, werden behandelt. All dies wird durch aktuelles Multimedia-Material unterstützt, das das Verständnis des Inhalts erleichtert, und durch das *Relearning*-System, das den Erwerb solider Kenntnisse ermöglicht.

Sie erhalten Zugang zu einem 100%igen Online-Studium, das flexibel ist und es Ihnen ermöglicht, Ihrem eigenen Rhythmus zu folgen. Sie können Ihr Privatleben mit einer qualitativ hochwertigen Weiterbildung verbinden. Schreiben Sie sich ein"

Modul 1. Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen

1.1. Bedrohungsmanagement in Sicherheitsrichtlinien
- 1.1.1. Das Risikomanagement
- 1.1.2. Das Sicherheitsrisiko
- 1.1.3. Methodologien im Bedrohungsmanagement
- 1.1.4. Implementierung von Methoden

1.2. Phasen des Managements von Bedrohungen
- 1.2.1. Identifizierung
- 1.2.2. Analyse
- 1.2.3. Standort
- 1.2.4. Schutzmaßnahmen

1.3. Auditsysteme zur Lokalisierung von Bedrohungen
- 1.3.1. Klassifizierung und Informationsfluss
- 1.3.2. Analyse der anfälligen Prozesse

1.4. Risikoklassifizierung
- 1.4.1. Arten von Risiko
- 1.4.2. Berechnung der Gefahrenwahrscheinlichkeit
- 1.4.3. Residuales Risiko

1.5. Risikobehandlung
- 1.5.1. Umsetzung von Schutzmaßnahmen
- 1.5.2. Übertragung oder Übernahme

1.6. Risikokontrolle
- 1.6.1. Kontinuierlicher Risikomanagementprozess
- 1.6.2. Implementierung von Sicherheitsmetriken
- 1.6.3. Strategisches Modell der Metriken für die Informationssicherheit

1.7. Praktische Methoden für die Analyse und Kontrolle von Bedrohungen
- 1.7.1. Katalog der Bedrohungen
- 1.7.2. Katalog der Kontrollmaßnahmen
- 1.7.3. Katalog der Sicherheitsvorkehrungen

1.8. ISO 27005-Norm
- 1.8.1. Identifizierung von Risiken
- 1.8.2. Risikoanalyse
- 1.8.3. Risikobewertung

1.9. Matrix der Risiken, Auswirkungen und Bedrohungen
  1.9.1. Daten, Systeme und Personal
  1.9.2. Wahrscheinlichkeit der Bedrohung
  1.9.3. Ausmaß des Schadens
1.10. Gestaltung von Phasen und Prozessen in der Gefahrenanalyse
  1.10.1. Identifizierung der kritischen Elemente der Organisation
  1.10.2. Bestimmung der Bedrohungen und Auswirkungen
  1.10.3. Analyse der Auswirkungen und Risiken
  1.10.4. Methoden

Modul 2. Richtlinien für das Management von Sicherheitsvorfällen

2.1. Richtlinien und Verbesserungen für das Management von Sicherheitsvorfällen in der Informationssicherheit
  2.1.1. Management von Zwischenfällen
  2.1.2. Verantwortlichkeiten und Verfahren
  2.1.3. Event-Benachrichtigung
2.2. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
  2.2.1. Daten zur Systemleistung
  2.2.2. Arten von Intrusion Detection Systemen
  2.2.3. Kriterien für den Standort von IDS/IPS
2.3. Reaktion auf Sicherheitsvorfälle
  2.3.1. Verfahren zum Sammeln von Informationen
  2.3.2. Verfahren zur Überprüfung der Intrusion
  2.3.3. CERT-Gremien
2.4. Benachrichtigung über einen Einbruchsversuch und Managementprozess
  2.4.1. Verantwortlichkeiten im Benachrichtigungsprozess
  2.4.2. Klassifizierung von Vorfällen
  2.4.3. Lösung und Wiederherstellungsprozess
2.5. Forensische Analyse als Sicherheitspolitik
  2.5.1. Volatile und nichtvolatile Beweise
  2.5.2. Analyse und Sammlung von elektronischen Beweismitteln
    2.5.2.1. Analyse von elektronischen Beweismitteln
    2.5.2.2. Sammlung von elektronischen Beweismitteln

2.6. Werkzeuge für Intrusion Detection und Prevention Systeme (IDS/IPS)
- 2.6.1. Snort
- 2.6.2. Suricata
- 2.6.3. SolarWinds

2.7. Tools zur Zentralisierung von Ereignissen
- 2.7.1. SIM
- 2.7.2. SEM
- 2.7.3. SIEM

2.8. CCN-STIC Sicherheitsleitfaden 817
- 2.8.1. Management von Cybervorfällen
- 2.8.2. Metriken und Indikatoren

2.9. NIST SP800-61
- 2.9.1. Fähigkeit zur Reaktion auf Computer-Sicherheitsvorfälle
- 2.9.2. Umgang mit einem Vorfall
- 2.9.3. Koordinierung und Informationsaustausch

2.10. ISO 27035-Norm
- 2.10.1. ISO 27035-Norm. Grundsätze des Vorfallsmanagements
- 2.10.2. Richtlinien für die Entwicklung eines Vorfallsmanagementplans
- 2.10.3. Richtlinien für die Reaktion auf Vorfälle

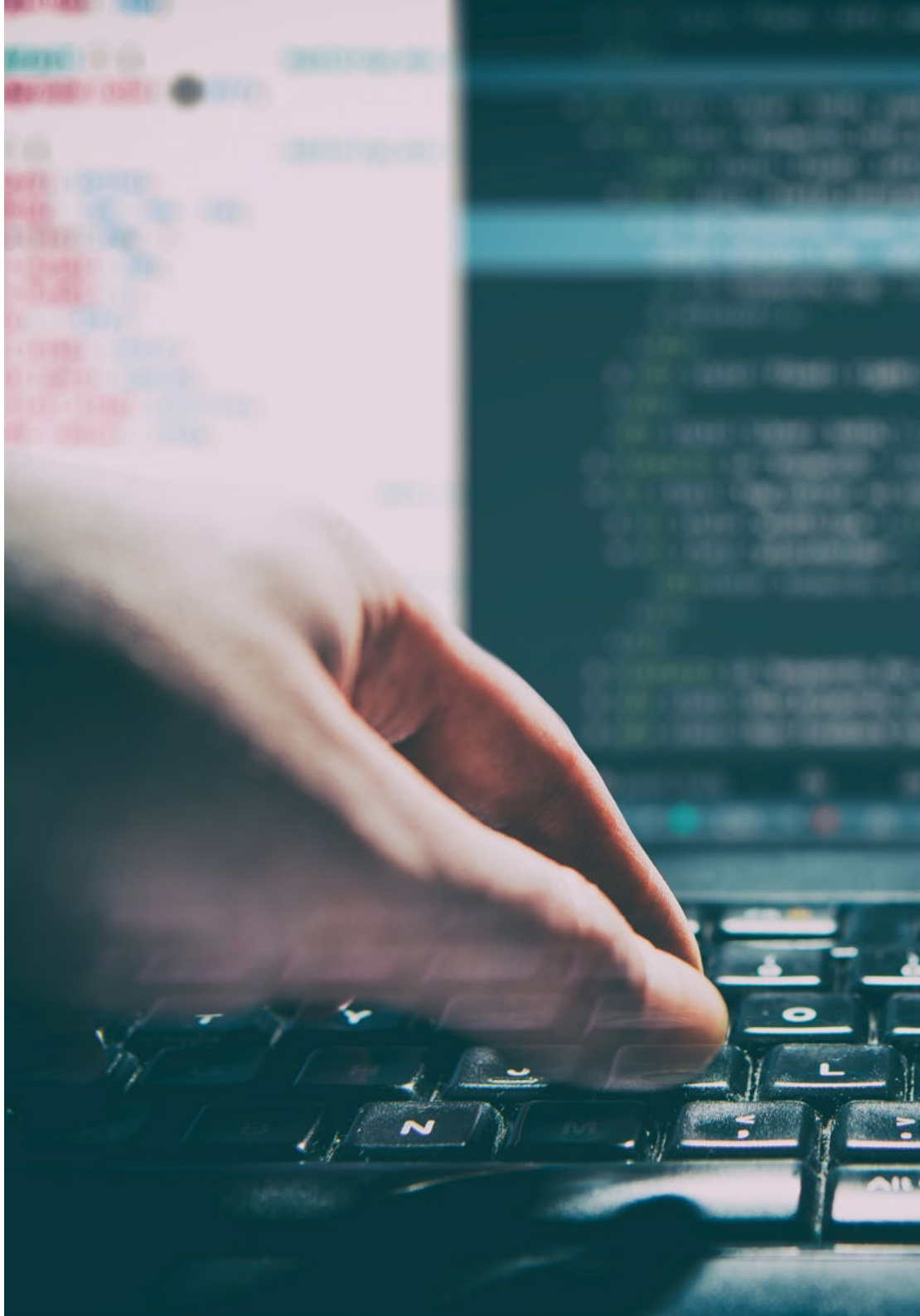
Modul 3. Praktische Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen

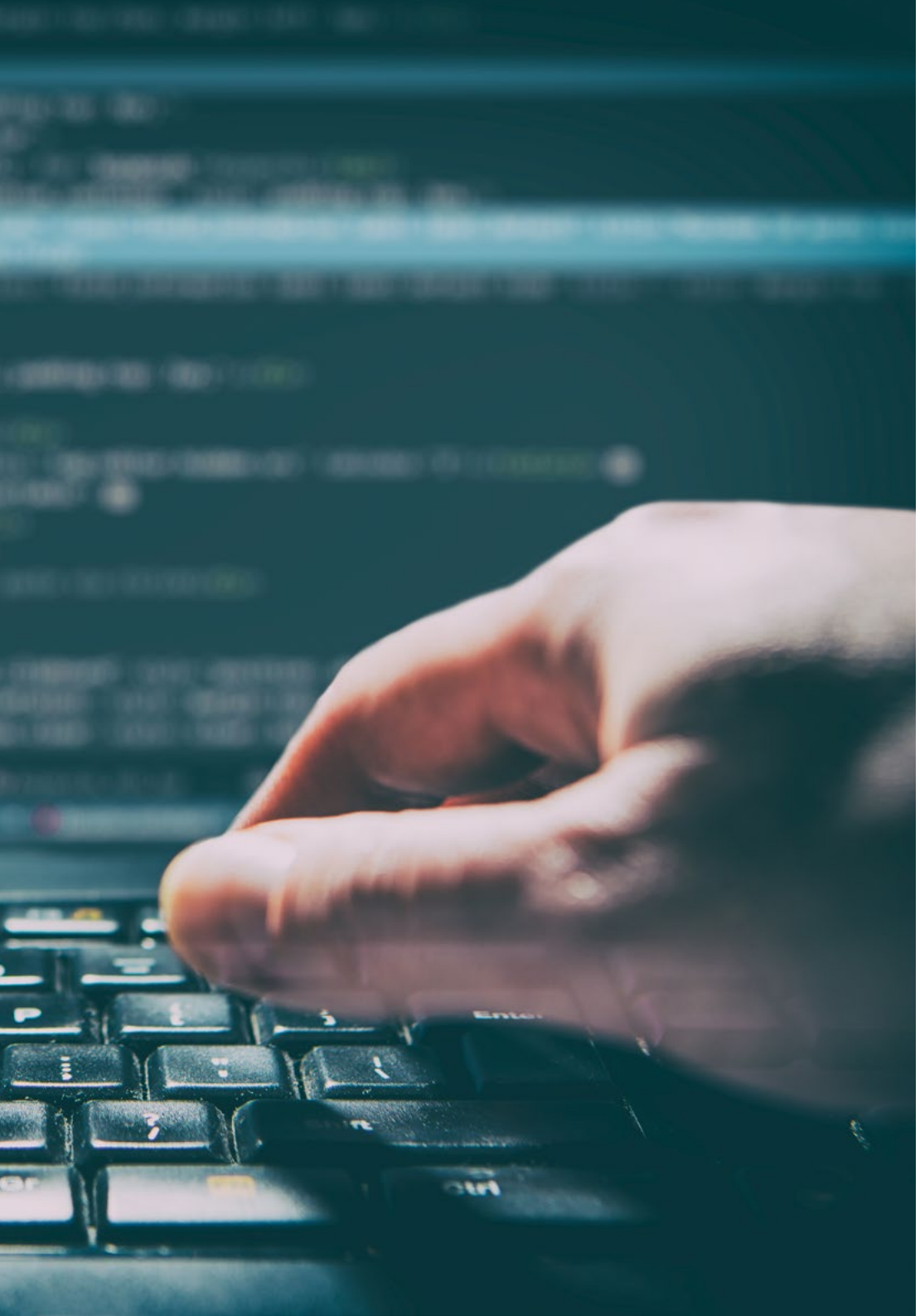
3.1. *System Hacking*
- 3.1.1. Risiken und Schwachstellen
- 3.1.2. Gegenmaßnahmen

3.2. DoS in Dienstleistungen
- 3.2.1. Risiken und Schwachstellen
- 3.2.2. Gegenmaßnahmen

3.3. *Session Hijacking*
- 3.3.1. Der *Hijacking*-Prozess
- 3.3.2. Gegenmaßnahmen zum *Hijacking*

3.4. Umgehung von IDS, *Firewalls and Honeypots*
- 3.4.1. Ausweichtechniken
- 3.4.2. Implementierung von Gegenmaßnahmen





3.5. *Hacking Web Servers*
- 3.5.1. Angriffe auf Webserver
- 3.5.2. Implementierung von Abwehrmaßnahmen

3.6. *Hacking Web Applications*
- 3.6.1. Angriffe auf Webanwendungen
- 3.6.2. Implementierung von Abwehrmaßnahmen

3.7. *Hacking Wireless Networks*
- 3.7.1. Schwachstellen im Wifi-Netzwerk
- 3.7.2. Implementierung von Abwehrmaßnahmen

3.8. *Hacking Mobile Platforms*
- 3.8.1. Schwachstellen von mobilen Plattformen
- 3.8.2. Implementierung von Gegenmaßnahmen

3.9. *Ransomware*
- 3.9.1. Schwachstellen, die *Ransomware* erlauben
- 3.9.2. Implementierung von Gegenmaßnahmen

3.10. *Social Engineering*
- 3.10.1. Arten von *Social Engineering*
- 3.10.2. Gegenmaßnahmen für *Social Engineering*

Fallstudien und Multimedia-Inhalte sind die wichtigsten Werkzeuge dieses Universitätsexperten. Laden Sie sie vom ersten Tag an herunter und bringen Sie Ihre Karriere in Schwung”

05

Methodik

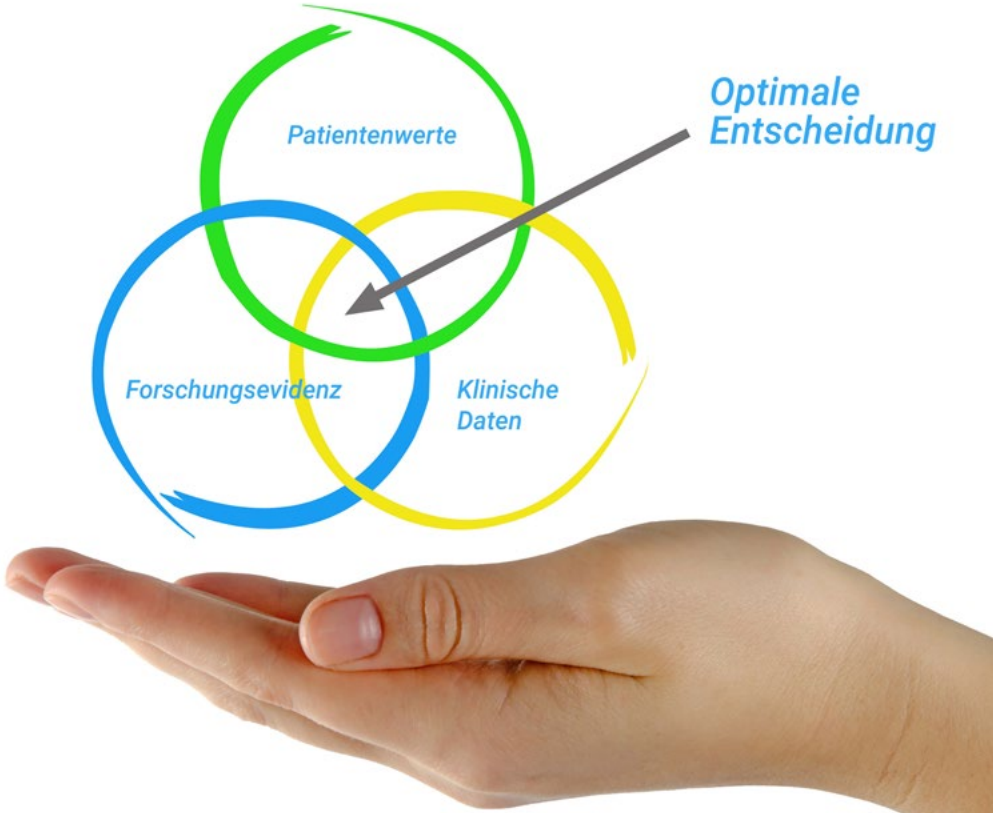
Dieses Fortbildungsprogramm bietet eine andere Art des Lernens. Unsere Methodik wird durch eine zyklische Lernmethode entwickelt: ***das Relearning***. Dieses Lehrsystem wird z. B. an den renommiertesten medizinischen Fakultäten der Welt angewandt und wird von wichtigen Publikationen wie dem ***New England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

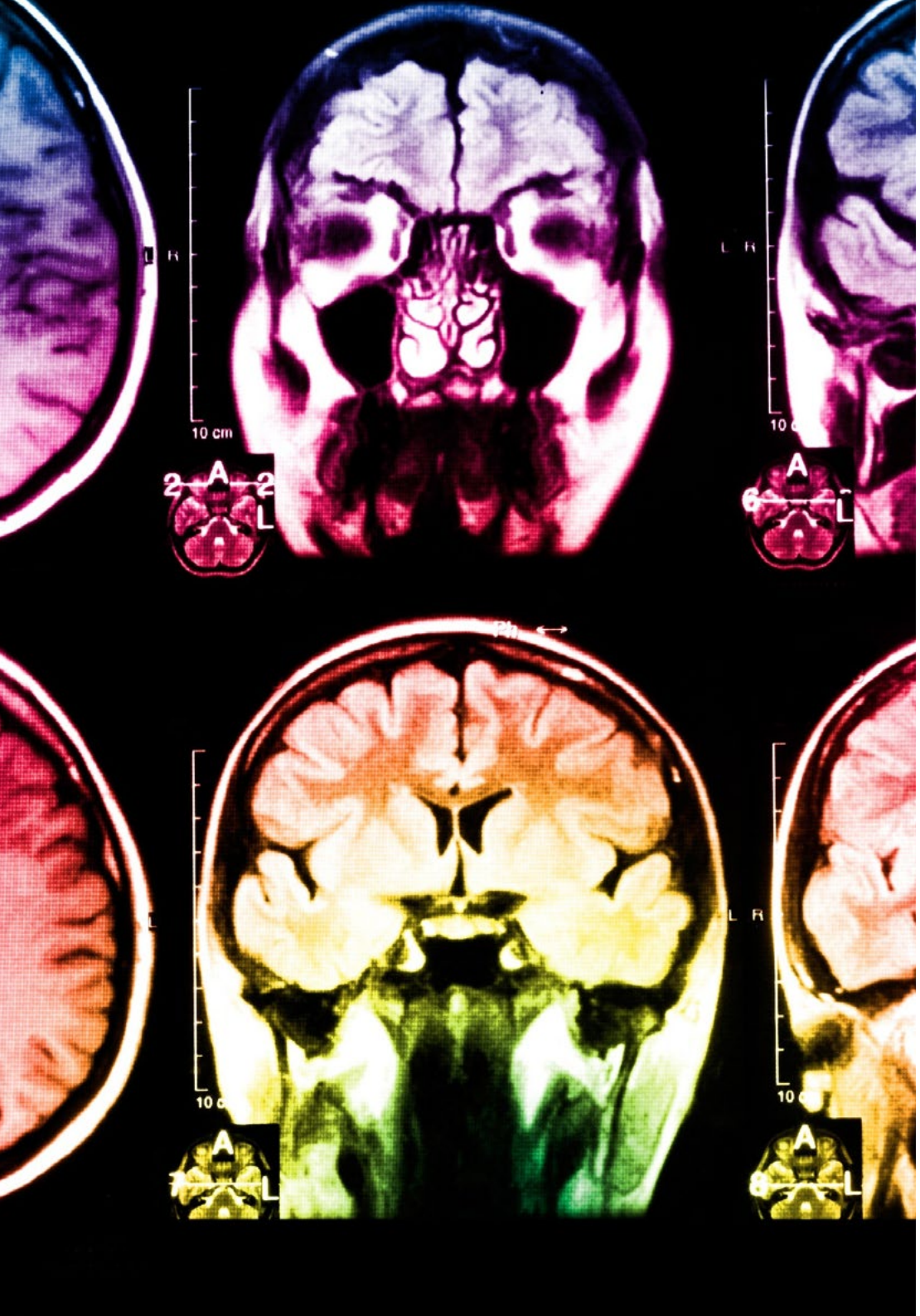
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

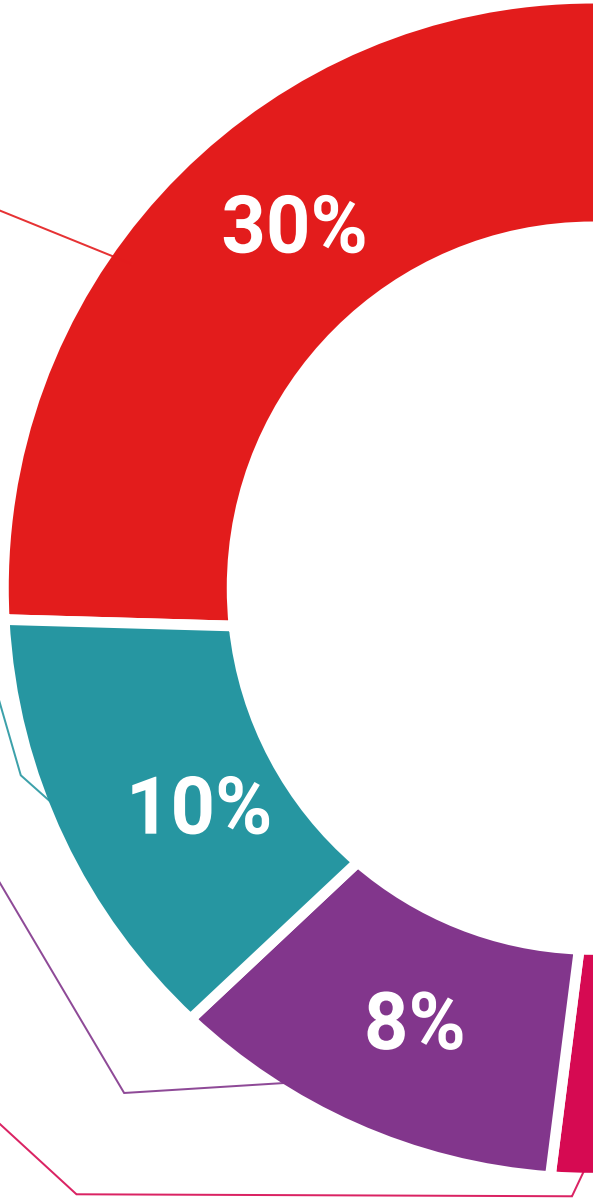
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

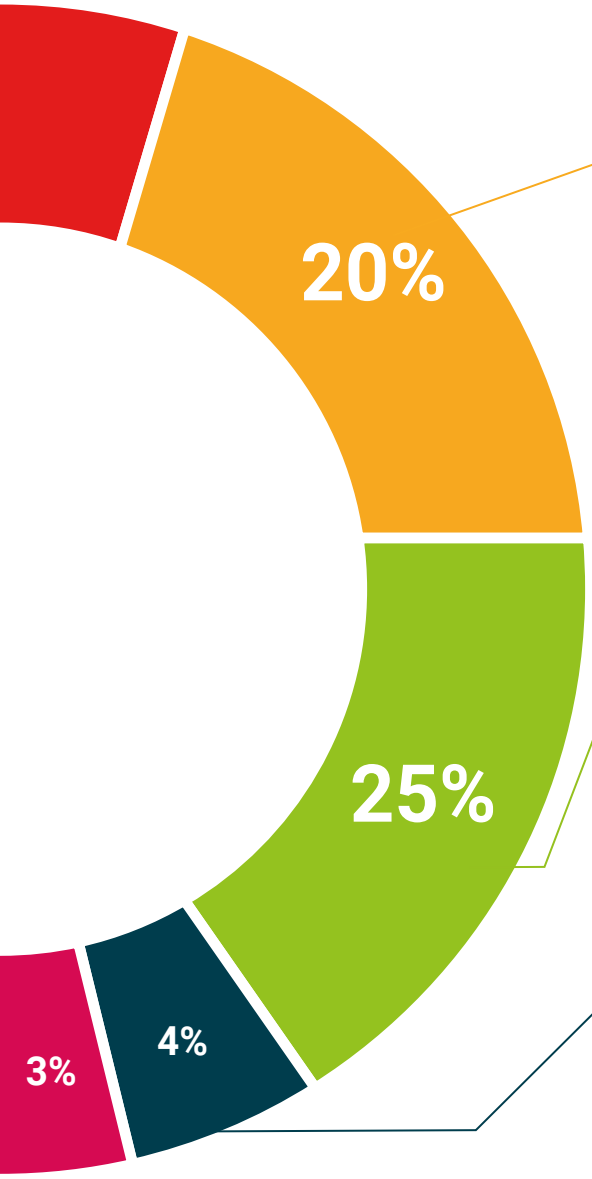
Übungen für Fertigkeiten und Kompetenzen

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 Maßnahmen zur Cyberabwehr 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 Maßnahmen zur Cyberabwehr** 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: **Universitätsexperte in Maßnahmen zur Cyberabwehr**

Anzahl der offiziellen Arbeitsstunden: **450 Std.**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

UNIVERSITÄTSEXPERTE

in

Maßnahmen zur Cyberabwehr

Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 450 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

Universitätsexperte

Maßnahmen zur Cyberabwehr

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

Universitätsexperte
Maßnahmen zur Cyberabwehr

tech technologische universität