Universitätsexperte
Red-Team-Cybersicherheit

tech technologische universität

tech technologische universität

Universitätsexperte
Red-Team-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-red-team-cybersicherheit

Index

01

Präsentation

Die Cybersicherheit ist zu einem Grundpfeiler des digitalen Zeitalters geworden, während die zunehmende Vernetzung der Systeme die Bedrohung durch Cyberangriffe verschärft hat. Die Nachfrage nach gut fortgebildeten Fachleuten in diesem Bereich ist offensichtlicher denn je, insbesondere angesichts der exponentiellen Zunahme von Cyberkriminalität und ausgeklügelten Angriffen. In diesem Zusammenhang wird dieses Programm als strategische Antwort präsentiert, um Fachleute mit den notwendigen Fähigkeiten für den Umgang mit Cyberbedrohungen auszustatten. Während des gesamten Lehrplans werden die Studenten in die Simulation von fortgeschrittenen Bedrohungen eintauchen. Die Methodik des Lehrplans, der zu 100% online durchgeführt wird, bietet Flexibilität und Zugänglichkeit, mit einer großen Vielfalt an Multimedia-Inhalten und der Anwendung der *Relearning*-Methode.

Sie werden dazu beitragen, die Cybersicherheit zu verbessern und großen digitalen Verbrechen vorzubeugen. Lassen Sie sich diese Gelegenheit nicht entgehen und schreiben Sie sich jetzt ein!"

In der komplexen Landschaft der Cybersicherheit ist ein Experte auf diesem Gebiet für Unternehmen, die ihre Abwehr gegen die sich ständig weiterentwickelnden Bedrohungen stärken wollen, zwingend erforderlich. Dieser proaktive Ansatz, der für die kontinuierliche Verbesserung der Sicherheitslage von grundlegender Bedeutung ist, unterstreicht den entscheidenden Bedarf an Experten.

Die Umsetzung proaktiver Maßnahmen ist von entscheidender Bedeutung, und die spezialisierte Ausbildung in Red Team vermittelt Fachleuten die Fähigkeit, Schwachstellen in Systemen und Netzwerken aktiv zu antizipieren, zu identifizieren und zu entschärfen. In diesem Universitätsexperten werden die Teilnehmer Fähigkeiten in Penetrationstests und Simulationen erwerben, die sich mit der Identifizierung und Ausnutzung von Schwachstellen befassen. In diesem Sinne werden sie nicht nur fortgeschrittene technische Kompetenzen entwickeln, sondern auch die effektive Zusammenarbeit mit Sicherheitsteams fördern, um Strategien gegen *Malware*-Bedrohungen zu integrieren.

Darüber hinaus erwerben die Studenten ein solides Verständnis der grundlegenden Prinzipien der digitalen forensischen Untersuchung (DFIR), die bei der Aufklärung von Cybervorfällen Anwendung finden. Zudem stellt dieser ganzheitliche Ansatz des Lehrplans sicher, dass die Fachleute mit den modernsten Fähigkeiten auf dem Gebiet der Cybersicherheit ausgestattet sind.

Dieser Studiengang zeichnet sich nicht nur durch seinen Inhalt, sondern auch durch seine fortschrittliche Methodik aus. Er wird den Studenten vollständig online zur Verfügung stehen, so dass sie die nötige Flexibilität haben, um ihre Karriere voranzutreiben, ohne ihre beruflichen Pflichten zu vernachlässigen.

Darüber hinaus wird die Anwendung von *Relearning*, bestehend aus der Wiederholung der wichtigsten Konzepte, eingesetzt, um das Wissen zu festigen und das effektive Lernen zu erleichtern. Diese Kombination aus Zugänglichkeit und robustem pädagogischen Ansatz macht diesen Universitätsexperten nicht nur zu einer fortschrittlichen Bildungsoption, sondern auch zu einem wichtigen Impulsgeber für diejenigen, die sich im Bereich der Cybersicherheit profilieren möchten.

Dieser **Universitätsexperte in Red-Team-Cybersicherheit** enthält das vollständigste und aktuellste Programm auf dem Markt. Seine herausragendsten Merkmale sind:

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

Dank dieses exklusiven Hochschulprogramms der TECH werden Sie in einem Sektor mit großem Vorsprung hervorstechen"

Sie werden sich mit der detaillierten forensischen Berichterstattung an der laut der Plattform Trustpilot (4.9/5) von ihren Studenten am besten bewerteten Universität der Welt beschäftigen"

Entwickeln Sie Fähigkeiten zur Bewertung und Auswahl von Anti-Malware-Sicherheitstools.

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

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

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

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

02

Ziele

Das Hauptziel des Universitätsexperten in Red-Team-Cybersicherheit ist die Fortbildung von Studenten in der Entwicklung von Fähigkeiten zur Simulation von fortgeschrittenen Bedrohungen. Während des gesamten Programms werden die Studenten in die Replikation von Taktiken, Techniken und Prozeduren (TTP), die von bösartigen Akteuren eingesetzt werden, eintauchen. In diesem Zusammenhang wird der spezialisierte Ansatz nicht nur die technischen Fähigkeiten der Fachleute stärken, sondern sie auch in die Lage versetzen, sich den Herausforderungen der realen Welt in diesem Bereich zu stellen. Darüber hinaus wird der Einsatz der *Relearning*-Methode das Lernen erleichtern, indem Schlüsselkonzepte mit wenig Aufwand fixiert werden.

Sie werden Schwachstellen und Sicherheitslücken in den Cyber-Infrastrukturen von Unternehmen erkennen. Erreichen Sie Ihre Ziele mit TECH!“

Allgemeine Ziele

- Erwerben fortgeschrittener Fähigkeiten in Penetrationstests und *Red-Team*-Simulationen, die sich mit der Identifizierung und Ausnutzung von Schwachstellen in Systemen und Netzwerken befassen
- Entwickeln von Führungsqualitäten, um auf offensive Cybersicherheit spezialisierte Teams zu koordinieren und die Durchführung von *Pentesting*- und *Red-Team*-Projekten zu optimieren
- Entwickeln von Fähigkeiten zur Analyse und Entwicklung von *Malware*, zum Verständnis ihrer Funktionsweise und zur Anwendung von Verteidigungs- und Aufklärungsstrategien
- Verbessern der Kommunikationsfähigkeiten durch die Erstellung von detaillierten technischen Berichten und Berichten für die Geschäftsleitung, wobei die Ergebnisse einem technischen Publikum und der Geschäftsleitung effektiv präsentiert werden
- Fördern der ethischen und verantwortungsbewussten Praxis im Bereich der Cybersicherheit, wobei ethische und rechtliche Grundsätze bei allen Aktivitäten berücksichtigt werden
- Aktualisieren der Studenten in Bezug auf neue Trends und Technologien im Bereich der Cybersicherheit

Dank der didaktischen Hilfsmittel von TECH, darunter erklärende Videos und interaktive Zusammenfassungen, werden Sie Ihre Ziele erreichen"

Spezifische Ziele

Modul 1. Analyse und Entwicklung von *Malware*

- Erwerben erweiterter Kenntnisse über das Wesen, die Funktionsweise und das Verhalten von *Malware* und Verstehen ihrer verschiedenen Formen und Ziele
- Entwickeln von Fähigkeiten in der forensischen Analyse von *Malware*, die die Identifizierung von Kompromissindikatoren (IoC) und Angriffsmustern ermöglichen
- Erlernen von Strategien zur effektiven Erkennung und Verhinderung von *Malware*, einschließlich des Einsatzes fortschrittlicher Sicherheitslösungen
- Kennenlernen der Entwicklung von *Malware* zu Aufklärungs- und Verteidigungszwecken, um die Taktiken der Angreifer besser zu verstehen
- Fördern ethischer und rechtlicher Praktiken bei der Analyse und Entwicklung von *Malware* und Gewährleisten von Integrität und Verantwortlichkeit bei allen Aktivitäten
- Anwenden von theoretischem Wissen in simulierten Umgebungen, Durchführung von praktischen Übungen, um bösartige Angriffe zu verstehen und abzuwehren
- Entwickeln von Fähigkeiten zur Bewertung und Auswahl von *Anti-Malware*-Sicherheitstools unter Berücksichtigung ihrer Wirksamkeit und Anpassungsfähigkeit an spezifische Umgebungen
- Lernen, wie man effektive Schutzmaßnahmen gegen bösartige Bedrohungen implementiert, um die Auswirkungen und die Verbreitung von Malware auf Systeme und Netzwerke zu reduzieren
- Fördern einer effektiven Zusammenarbeit mit Sicherheitsteams, um Strategien und Bemühungen zum Schutz vor *Malware*-Bedrohungen zu integrieren
- Aktualisieren der neuesten Trends und Techniken in der *Malware*-Analyse und -Entwicklung, um die Relevanz und Wirksamkeit der erworbenen Fähigkeiten zu gewährleisten

Modul 2. Forensische Grundlagen und DFIR

- Erwerben eines soliden Verständnisses der grundlegenden Prinzipien der digitalen forensischen Untersuchung (DFIR) und ihrer Anwendung bei der Lösung von Cyber-Vorfällen
- Entwickeln von Fähigkeiten zur sicheren und forensischen Beschaffung digitaler Beweise, die die Wahrung der Beweiskette gewährleisten
- Lernen, wie man eine forensische Analyse von Dateisystemen durchführt
- Kennenlernen fortgeschrittener Techniken zur Analyse von Aufzeichnungen und Protokollen, die die Rekonstruktion von Ereignissen in digitalen Umgebungen ermöglichen
- Lernen, digitale forensische Untersuchungsmethoden bei der Lösung von Fällen anzuwenden, von der Identifizierung bis zur Dokumentation der Ergebnisse
- Kennenlernen der Analyse von digitalem Beweismaterial und der Anwendung forensischer Techniken in *Pentesting*-Umgebungen
- Entwickeln von Fähigkeiten zur Erstellung detaillierter und klarer forensischer Berichte, in denen die Ergebnisse und Schlussfolgerungen auf verständliche Art und Weise dargestellt werden
- Fördern einer effektiven Zusammenarbeit mit *Incident-Response*-Teams (IR), um die Koordination bei der Untersuchung und Eindämmung von Bedrohungen zu optimieren
- Fördern ethischer und rechtlicher Praktiken bei der Untersuchung digitaler Forensik und Gewährleisten der Einhaltung von Cybersicherheitsvorschriften und Verhaltensstandards

Modul 3. Fortgeschrittene *Red-Team*-Übungen

- Entwickeln von Fähigkeiten in der Simulation fortgeschrittener Bedrohungen, indem Taktiken, Techniken und Verfahren (TTP) nachgebildet werden, die von attraktiven bösartigen Akteuren verwendet werden
- Lernen, Schwachstellen und Verwundbarkeiten in der Infrastruktur durch realistische *Red-Team*-Übungen zu identifizieren und so die Sicherheitslage zu verbessern
- Kennenlernen von fortgeschrittenen Sicherheitsumgehungstechniken, um die Widerstandsfähigkeit der Infrastruktur gegenüber gewünschten Angriffen zu bewerten
- Entwickeln effektiver Koordinations- und Kollaborationsfähigkeiten zwischen den Mitgliedern des *Red Teams*, um die Ausführung von Taktiken und Strategien zu optimieren und die Sicherheit der Organisation umfassend zu bewerten
- Lernen, wie man aktuelle Bedrohungsszenarien simuliert, wie z. B. *Ransomware*-Angriffe oder fortgeschrittene *Phishing*-Kampagnen, um die Reaktionsfähigkeit der Organisation zu bewerten
- Kennenlernen von Analysetechniken für die Zeit nach der Übung, um die Leistung des *Red Teams* zu bewerten und Lehren für die kontinuierliche Verbesserung zu ziehen
- Entwickeln von Fähigkeiten, um die Widerstandsfähigkeit der Organisation gegenüber simulierten Angriffen zu bewerten und Bereiche zu identifizieren, in denen die Richtlinien und Verfahren verbessert werden können
- Lernen, detaillierte Berichte zu erstellen, in denen die Ergebnisse, die angewandten Methoden und die aus fortgeschrittenen *Red-Team*-Übungen abgeleiteten Empfehlungen dokumentiert werden
- Fördern der ethischen und rechtlichen Praktiken bei der Durchführung von *Red-Team*-Übungen und Gewährleisten der Einhaltung von Cybersicherheitsvorschriften und ethischen Standards

03

Kursleitung

Für dieses Hochschulprogramm hat TECH einen hervorragenden Lehrkörper zusammengestellt, der sich aus den besten Spezialisten auf diesem Gebiet zusammensetzt. In diesem Sinne verfügt jedes Mitglied des Lehrkörpers über einen umfassenden und anerkannten beruflichen Hintergrund, der in führenden Unternehmen im Bereich der Cybersicherheit erworben wurde. Diese Fachleute, die aufgrund ihrer Erfahrung und ihres Fachwissens sorgfältig ausgewählt wurden, garantieren nicht nur die akademische Qualität des Lehrplans, sondern bieten auch eine praktische und aktuelle Perspektive und bereichern die Fortbildung der Teilnehmer mit wertvollen Einblicken aus ihrer realen Erfahrung im Bereich *Red Team*.

Informieren Sie sich über die neuesten Verschlüsselungstechniken mit Shellcode (XQR) von führenden Experten für Cybersicherheit. Starten Sie Ihre berufliche Laufbahn mit TECH!“

Leitung

Hr. Gómez Pintado, Carlos

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

04

Struktur und Inhalt

Dieser Lehrplan bietet den Studenten ein spezialisiertes Eintauchen in die forensische Analyse von *Malware*, wobei die Entwicklung von Schlüsselkompetenzen für die Identifizierung von Kompromissindikatoren (IoC) und Angriffsmustern im Vordergrund steht. Während des gesamten Lehrplans werden die Studenten mit fortschrittlichen Methoden vertraut gemacht, die sie mit den notwendigen Werkzeugen und Kenntnissen ausstatten, um mit anspruchsvollen Cyberbedrohungen umzugehen. Darüber hinaus garantiert dieses streng strukturierte Programm eine umfassende Fortbildung im Bereich *Red Team* und bereitet Fachleute darauf vor, die komplexen Strategien böswilliger Akteure zu analysieren und zu bekämpfen.

Sie werden sich mit fortgeschrittenen Post-Exploitation-Techniken befassen und sich als hervorragender Red Teamer positionieren"

Modul 1. Analyse und Entwicklung von *Malware*

1.1. Analyse und Entwicklung von *Malware*
- 1.1.1. Geschichte und Entwicklung von *Malware*
- 1.1.2. Klassifizierung und Arten von *Malware*
- 1.1.3. *Malware*-Scans
- 1.1.4. Entwicklung von *Malware*

1.2. Vorbereiten der Umgebung
- 1.2.1. Einrichten von virtuellen Maschinen und *Snapshots*
- 1.2.2. Tools zum Scannen von *Malware*
- 1.2.3. Tools zur Entwicklung von *Malware*

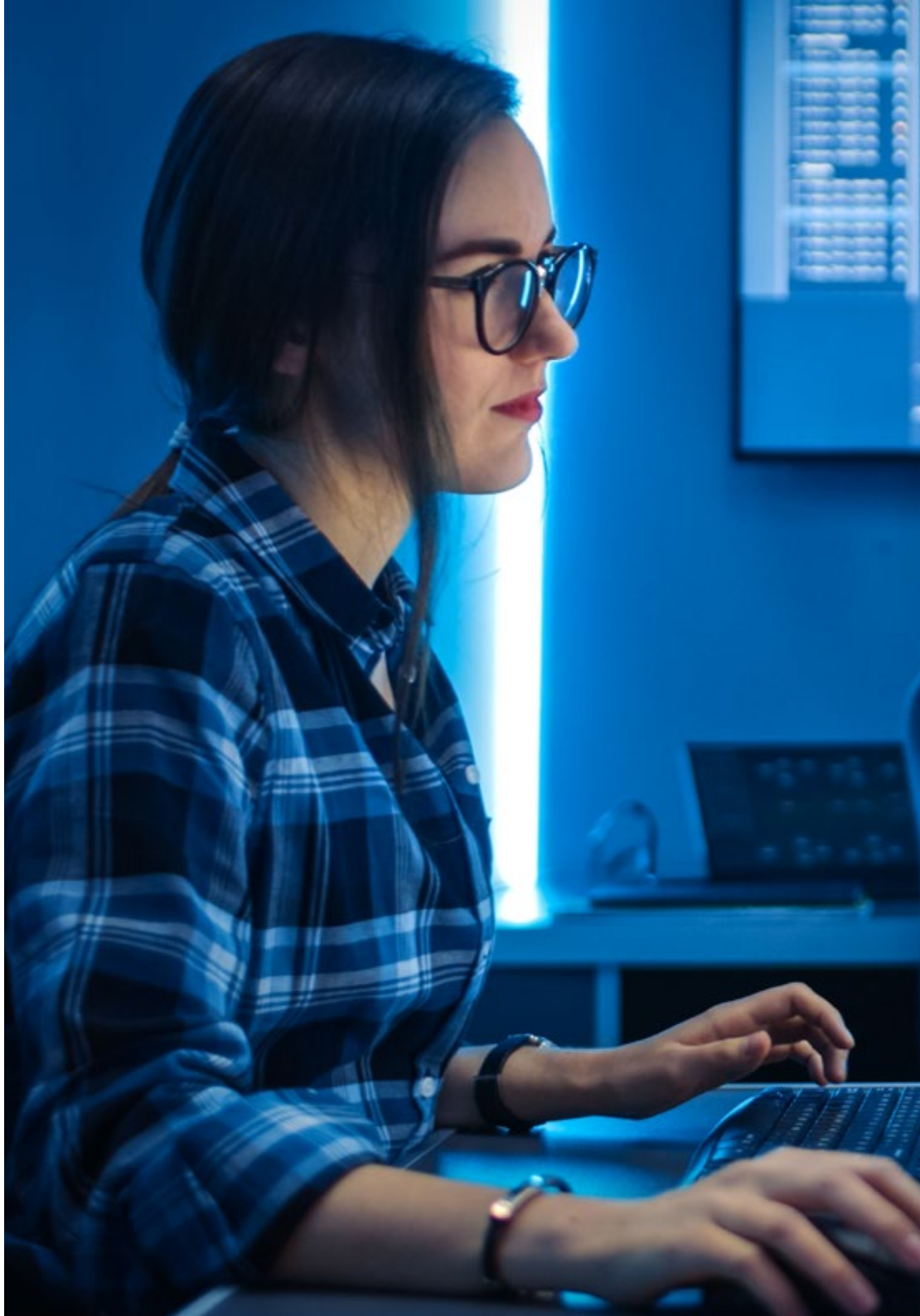
1.3. Windows-Grundlagen
- 1.3.1. PE (*Portable Executable*) Dateiformat
- 1.3.2. Prozesse und *Threads*
- 1.3.3. Dateisystem und Registry
- 1.3.4. *Windows Defender*

1.4. Grundlegende *Malware*-Techniken
- 1.4.1. *Shellcode*-Erzeugung
- 1.4.2. Ausführen von *Shellcode* auf der Festplatte
- 1.4.3. Festplatte vs. Speicher
- 1.4.4. Ausführen von *Shellcode* im Speicher

1.5. Zwischengeschaltete *Malware*-Techniken
- 1.5.1. Windows-Persistenz
- 1.5.2. Startup-Ordner
- 1.5.3. Registrierungsschlüssel
- 1.5.4. Bildschirmschoner

1.6. Erweiterte *Malware*-Techniken
- 1.6.1. *Shellcode*-Verschlüsselung (XOR)
- 1.6.2. *Shellcode*-Verschlüsselung (RSA)
- 1.6.3. *String*-Verschleierung
- 1.6.4. Prozess-Injektion

1.7. Statische *Malware*-Analyse
- 1.7.1. Analyse von *Packers* mit DIE (*Detect It Easy*)
- 1.7.2. Analyse von Sektionen mit PE-Bear
- 1.7.3. Dekompilieren mit Ghidra



1.8. Dynamische *Malware*-Analyse
- 1.8.1. Verhaltensbeobachtung mit Process Hacker
- 1.8.2. Analyse von Aufrufen mit API Monitor
- 1.8.3. Analyse von Änderungen in der Registrierung mit Regshot
- 1.8.4. Beobachtung von Netzwerkanfragen mit TCPView

1.9. Scannen in .NET
- 1.9.1. Einführung in .NET
- 1.9.2. Dekompilieren mit dnSpy
- 1.9.3. Fehlersuche mit dnSpy

1.10. Analyse von echter *Malware*
- 1.10.1. Vorbereiten der Umgebung
- 1.10.2. Statische Analyse der *Malware*
- 1.10.3. Dynamische Analyse der *Malware*
- 1.10.4. Erstellung von YARA-Regeln

Modul 2. Forensische Grundlagen und DFIR

2.1. Digitale Forensik
- 2.1.1. Geschichte und Entwicklung der Computerforensik
- 2.1.2. Bedeutung der Computerforensik für die Cybersicherheit
- 2.1.3. Geschichte und Entwicklung der Computerforensik

2.2. Grundlagen der Computerforensik
- 2.2.1. *Chain of Custody* und ihre Anwendung
- 2.2.2. Arten von digitalen Beweisen
- 2.2.3. Prozesse zur Beschaffung von Beweisen

2.3. Dateisysteme und Datenstruktur
- 2.3.1. Die wichtigsten Ablagesysteme
- 2.3.2. Methoden zum Verstecken von Daten
- 2.3.3. Analyse von Datei-Metadaten und Attributen

2.4. Analyse von Betriebssystemen
- 2.4.1. Forensische Analyse von Windows-Systemen
- 2.4.2. Forensische Analyse von Linux-Systemen
- 2.4.3. Forensische Analyse von macOS-Systemen

2.5. Datenwiederherstellung und Festplattenanalyse
- 2.5.1. Datenrettung von beschädigten Datenträgern
- 2.5.2. Tools zur Festplattenanalyse
- 2.5.3. Interpretation von Dateizuordnungstabellen

2.6. Netzwerk- und Verkehrsanalyse
- 2.6.1. Erfassen und Analysieren von Netzwerkpaketen
- 2.6.2. Analyse der *Firewall*-Protokolle
- 2.6.3. Erkennung von Netzwerkeinbrüchen

2.7. Analyse von *Malware* und bösartigem Code
- 2.7.1. Klassifizierung von *Malware* und ihre Merkmale
- 2.7.2. Statische und dynamische Analyse von *Malware*
- 2.7.3. Disassemblierung und Fehlersuchtechniken

2.8. Protokoll- und Ereignisanalyse
- 2.8.1. Arten von Protokollen in Systemen und Anwendungen
- 2.8.2. Interpretation relevanter Ereignisse
- 2.8.3. Tools zur Protokollanalyse

2.9. Reagieren auf Sicherheitsvorfälle
- 2.9.1. Prozess der Reaktion auf Vorfälle
- 2.9.2. Erstellung eines Plans zur Reaktion auf Vorfälle
- 2.9.3. Koordinierung mit Sicherheitsteams

2.10. Vorlage von Beweisen und Rechtliches
- 2.10.1. Regeln für digitale Beweise im juristischen Bereich
- 2.10.2. Erstellung von forensischen Berichten
- 2.10.3. Erscheinen vor Gericht als Sachverständiger

Modul 3. Fortgeschrittene *Red-Team*-Übungen

3.1. Fortgeschrittene Erkennungstechniken
- 3.1.1. Fortgeschrittene Aufzählung von Subdomains
- 3.1.2. Fortgeschrittenes *Google Dorking*
- 3.1.3. Soziale Netzwerke und theHarvester

3.2. Fortgeschrittene *Phishing*-Kampagnen
- 3.2.1. Was ist *Reverse-Proxy-Phishing*?
- 3.2.2. *2FA Bypass* mit Evilginx
- 3.2.3. Exfiltration von Daten

3.3. Fortgeschrittene Persistenztechniken
- 3.3.1. *Golden Tickets*
- 3.3.2. *Silver Tickets*
- 3.3.3. *DCShadow*-Technik

3.4. Fortgeschrittene Ausweichtechniken
- 3.4.1. AMSI-Umgehung
- 3.4.2. Modifizierung bestehender Tools
- 3.4.3. *Powershell*-Verschleierung

3.5. Fortgeschrittene *Lateral-Movement*-Techniken
- 3.5.1. *Pass-the-Ticket* (PtT)
- 3.5.2. *Overpass-the-Hash (Pass-the-Key)*
- 3.5.3. NTLM Relay

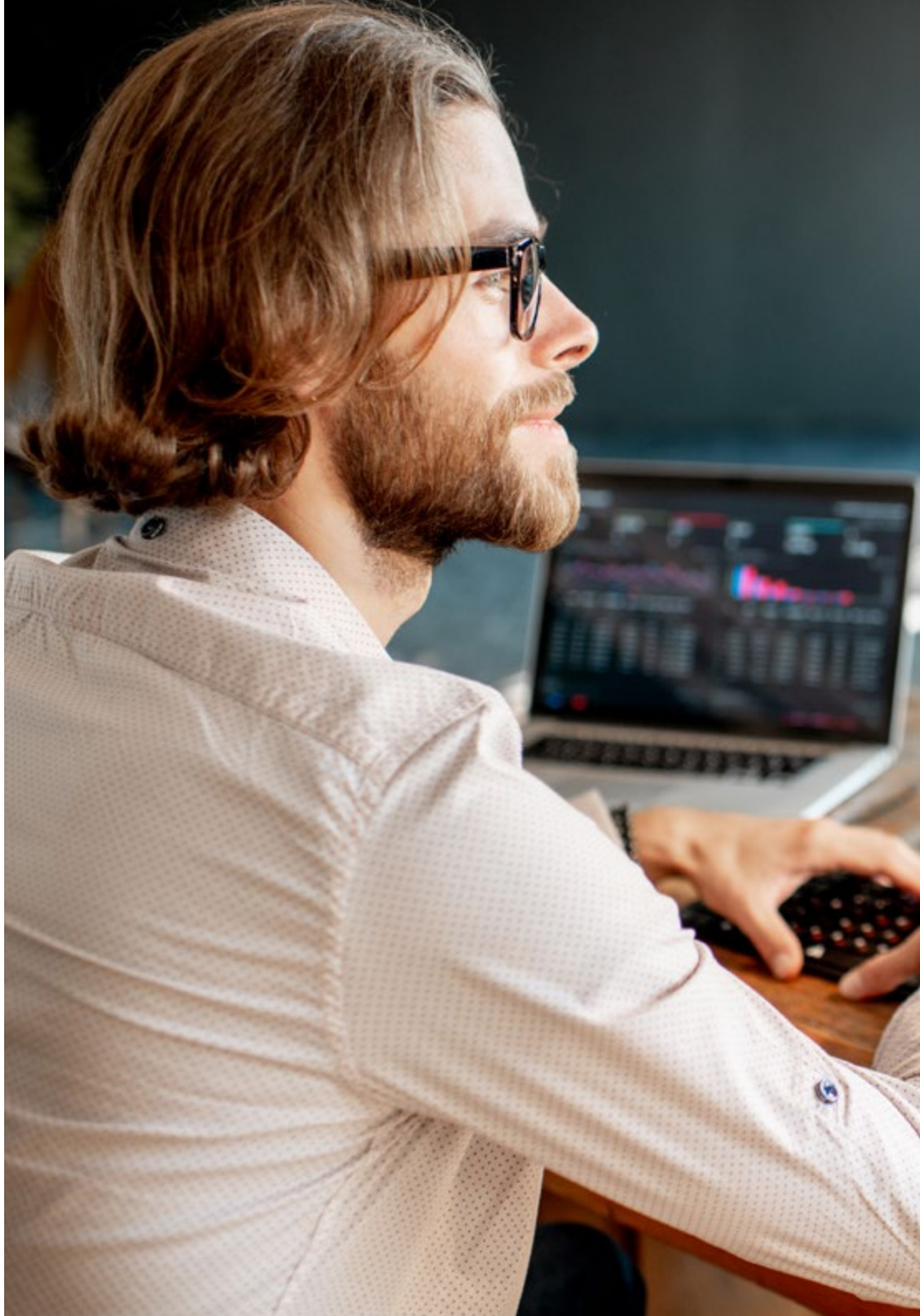
3.6. Fortgeschrittene *Post-Exploitation*-Techniken
- 3.6.1. *Dump* von LSASS
- 3.6.2. *Dump* von SAM
- 3.6.3. *DCSync*-Angriff

3.7. Erweiterte *Pivoting*-Techniken
- 3.7.1. Was ist *Pivoting*?
- 3.7.2. Tunnel mit SSH
- 3.7.3. *Pivoting* mit Chisel

3.8. Physikalische Eindringlinge
- 3.8.1. Überwachung und Erkundung
- 3.8.2. *Tailgating* und *Piggybacking*
- 3.8.3. *Lock-Picking*

3.9. WLAN-Angriffe
- 3.9.1. WPA/WPA2 PSK-Angriffe
- 3.9.2. Rogue AP-Angriffe
- 3.9.3. WPA2 *Enterprise*-Angriffe

3.10. RFID-Angriffe
- 3.10.1. Lesen von RFID-Karten
- 3.10.2. RFID-Kartenmanipulation
- 3.10.3. Erstellung von geklonten Karten



Verpassen Sie nicht die Gelegenheit, Ihre Karriere durch dieses innovative Programm anzukurbeln" Werden Sie ein Experte für Cybersicherheit!"

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

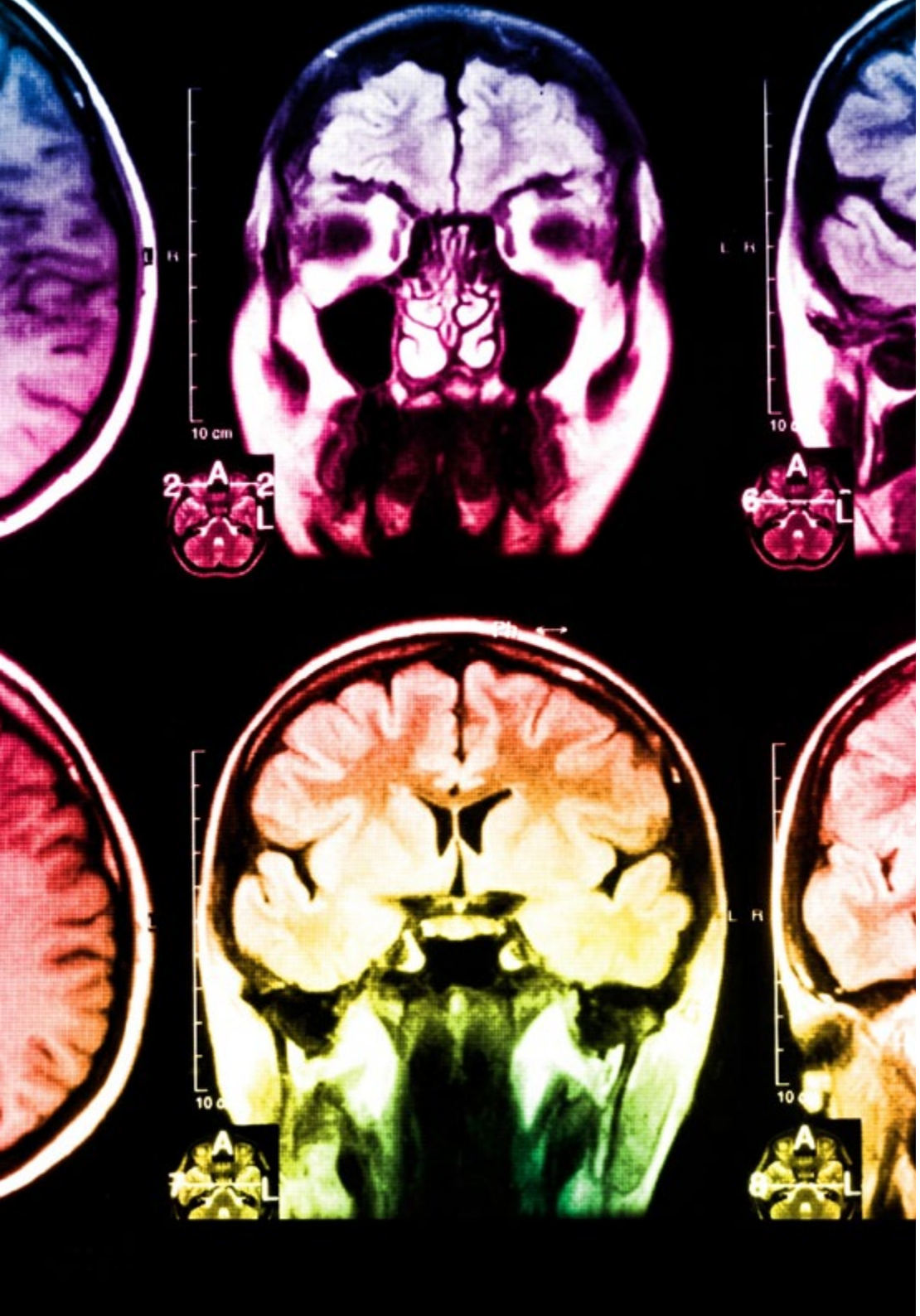
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

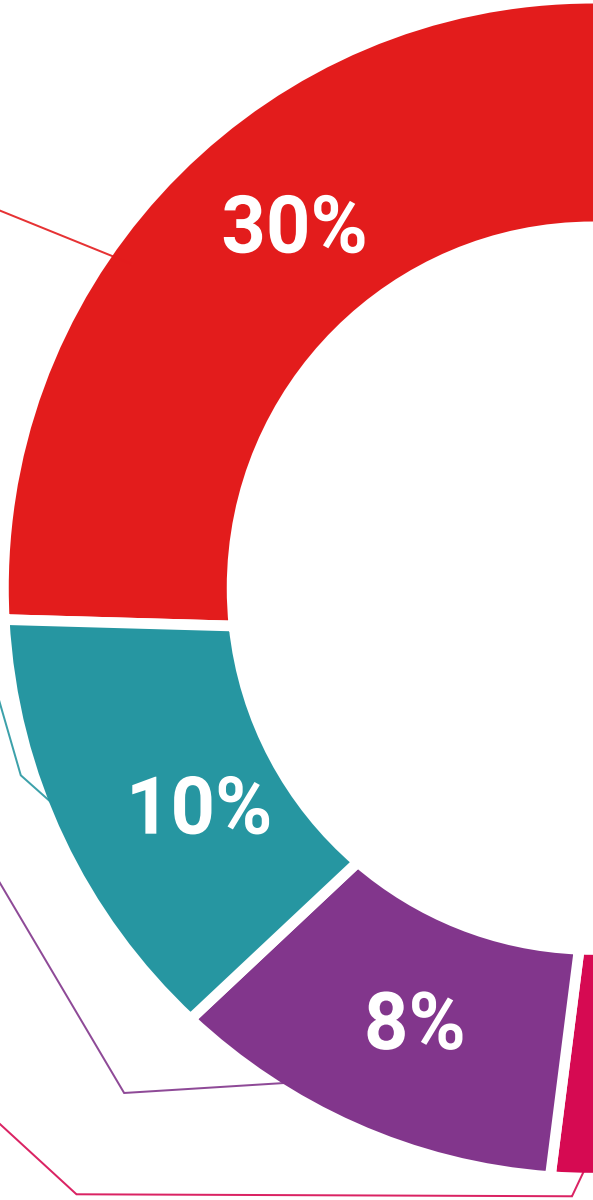
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

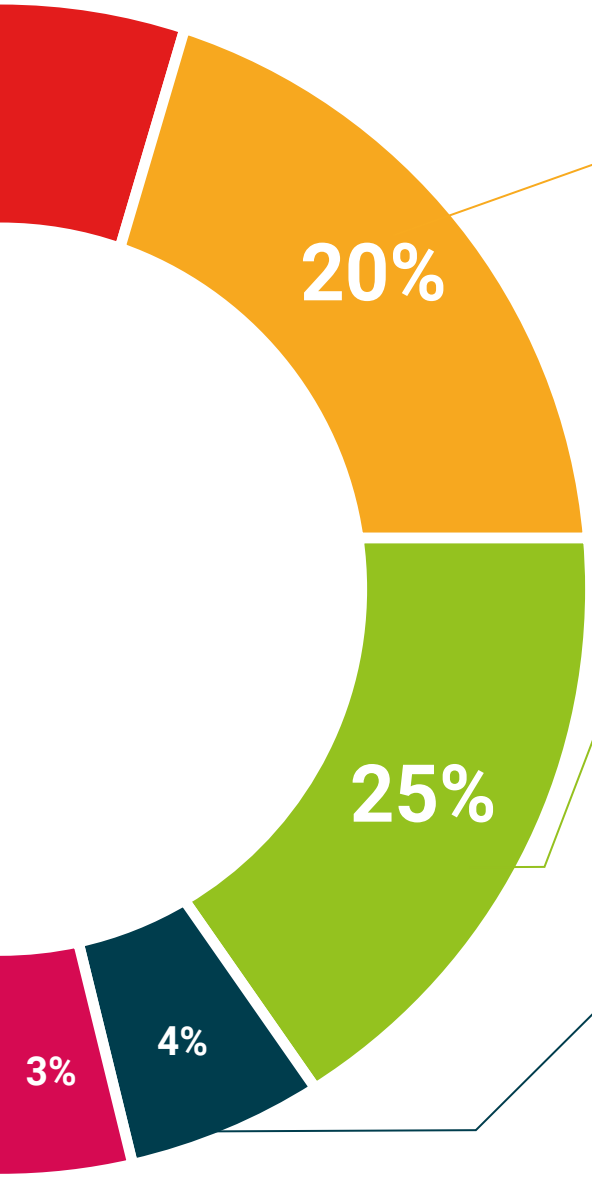
Übungen für Fertigkeiten und Kompetenzen

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 Red-Team-Cybersicherheit garantiert neben der präzisesten und aktuellsten Fortbildung auch den Zugang zu einem von der TECH Technologische Universität ausgestellten Diplom.

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

Dieser **Universitätsexperte in Red-Team-Cybersicherheit** enthält das vollständigste und aktuellste Programm auf dem Markt.

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

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

Titel: **Universitätsexperte in Red-Team-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

Red-Team-Cybersicherheit

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
Red-Team-Cybersicherheit

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

Universitätsexperte
Red-Team-Cybersicherheit

tech technologische universität