Universitätsexperte
Offensive Cybersicherheit

tech technologische universität

tech technologische universität

Universitätsexperte
Offensive 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-offensive-cybersicherheit

Index

01

Präsentation

Cybersicherheit ist für Institutionen unerlässlich, um ihr digitales Vermögen zu schützen, ihr gesellschaftliches Ansehen zu wahren und sich vor Spionage durch Konkurrenten zu schützen. Infolgedessen fragen immer mehr Unternehmen nach IT-Experten, um Konsequenzen zu vermeiden, die sich sogar auf ihre finanziellen Möglichkeiten auswirken könnten. In diesem Zusammenhang müssen diese Spezialisten ihre Kenntnisse und Fähigkeiten ständig aktualisieren, um mit den Techniken der Cyberkriminalität Schritt zu halten. Aus diesem Grund hat TECH einen innovativen Universitätsexperten entwickelt, in dem Bedrohungen identifiziert und entschärft werden sollen. Das gesamte Programm wird zu 100% online unterrichtet, um den Studenten mehr Komfort und Flexibilität zu bieten.

Sie werden Ihre Kenntnisse über das Kerberos-Protokoll vertiefen und Informationen in Netzwerkumgebungen schützen"

Jeden Tag wird in den Medien von Fällen berichtet, in denen Hacker Institutionen geschädigt haben, indem sie sich Zugang zu ihren Datenbanken verschafften. Die Folgen dieser Angriffe sind schwerwiegend, da sie den Betrieb stören und Unternehmen daran hindern, effektiv zu arbeiten. Sie können sich sogar direkt auf ihre Wirtschaft auswirken, indem sie zu Geldstrafen für die Nichteinhaltung von Vorschriften und zu Umsatzeinbußen führen.

Vor diesem Hintergrund hat TECH einen hochmodernen Studiengang zur Erkennung der am häufigsten verwendeten Eindringungstechniken sowie der optimalen Strategien zu deren Bekämpfung entwickelt. Unter der Leitung eines in diesem Bereich erfahrenen Lehrkörpers wird der Lehrplan die wesentlichen Grundlagen für das Verständnis der Denkweise von Hackern schaffen. Außerdem wird eine Reihe von Lösungen angeboten, die darauf abzielen, sichere Infrastrukturen für die Verwaltung digitaler Zertifikate in einem Unternehmensnetzwerk bereitzustellen.

Fachleute werden auch lernen, wie man virtuelle Umgebungen dank der Konfiguration von virtuellen Maschinen oder Snapshots optimal vorbereitet. Darüber hinaus wird Malware analysiert, indem Aufrufe mit API Monitor untersucht und Netzwerkanfragen mit TCPView beobachtet werden. Die Studenten lernen theoretische Konzepte in simulierten Umgebungen und werden so auf reale Herausforderungen im Bereich der offensiven Cybersicherheit vorbereitet. Schließlich wird der Schwerpunkt auf die Ethik und die soziale Verantwortung gelegt, die Experten in diesem Bereich auszeichnen sollten.

Um die Beherrschung all dieser Inhalte zu festigen, setzt der Universitätsexperte das innovative *Relearning*-System ein. TECH ist führend in der Anwendung dieses Lehrmodells, das die Aneignung komplexer Konzepte durch deren natürliche und schrittweise Wiederholung fördert. Das Programm verwendet auch Materialien in verschiedenen Formaten, wie z. B. erklärende Videos, interaktive Zusammenfassungen und Infografiken. All dies in einem bequemen 100%igen Online-Modus, der es ermöglicht, den Zeitplan jedes Einzelnen an seine Aufgaben und seine Verfügbarkeit anzupassen.

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

- Die Entwicklung von Fallstudien, die von Experten für offensive Cybersicherheit präsentiert werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren praktischen Informationen
- Praktische Übungen, anhand derer der Selbstbewertungsprozess zur Verbesserung des Lernens verwendet 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

Entwickeln Sie Ihre Fähigkeiten als offensiver Auditor und nehmen Sie eine neue berufliche Herausforderung in den renommiertesten digitalen Unternehmen an"

Sie werden Ihre Ziele mit Hilfe der didaktischen Werkzeuge von TECH erreichen, darunter erklärende Videos und interaktive Zusammenfassungen"

Möchten Sie ein Big Bounty Hunter werden? Mit diesem Programm werden Sie jede Sicherheitslücke im Internet finden.

In nur 6 Monaten werden Sie die Identitätsverwaltung in Azure AD beherrschen. Schreiben Sie sich jetzt ein!

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

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

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 Design dieses Programms bietet eine einzigartige Bildungserfahrung, die sich durch ihren praktischen und innovativen Ansatz zur Cybersicherheit auszeichnet. Auf diese Weise werden die Studenten alles von der Schwachstellenanalyse bis hin zu fortgeschrittenen Eindringungstechniken behandeln. In diesem Zusammenhang werden auch die optimalen Maßnahmen zur Bewertung und Stärkung der verschiedenen kybernetischen Systeme angeboten. Darüber hinaus wird der Schwerpunkt auf die rechtliche und ethische Verantwortung gelegt, die Experten in diesem Bereich übernehmen sollten.

Reduzieren Sie Malware-Bedrohungen mit Hilfe der laut Forbes besten digitalen Universität der Welt"

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

Spezifische Ziele

Modul 1. Offensive Sicherheit

- Vermitteln der Methoden der Penetrationstests, einschließlich der wichtigsten Phasen wie Informationsbeschaffung, Schwachstellenanalyse, Ausnutzung und Dokumentation
- Entwickeln praktischer Fähigkeiten im Umgang mit spezialisierten *Pentesting*-Tools, um Schwachstellen in Systemen und Netzwerken zu identifizieren und zu bewerten
- Studieren und Verstehen der Taktiken, Techniken und Verfahren, die von böswilligen Akteuren eingesetzt werden, um Bedrohungen zu identifizieren und zu simulieren
- Anwenden von theoretischen Kenntnissen in praktischen Szenarien und Simulationen, wobei echte Herausforderungen bewältigt werden, um die *Pentesting*-Fähigkeiten zu stärken
- Entwickeln von effektiven Dokumentationsfähigkeiten, Erstellen von detaillierten Berichten, die die Ergebnisse, die verwendeten Methoden und die Empfehlungen zur Verbesserung der Sicherheit wiedergeben
- Üben der effektiven Zusammenarbeit in offensiven Sicherheitsteams, um die Koordination und Durchführung von *Pentesting*-Aktivitäten zu optimieren

Modul 2. Angriffe auf Netzwerke und Systeme unter Windows

- Entwickeln von Fähigkeiten, um spezifische Schwachstellen in Windows-Betriebssystemen zu identifizieren und zu bewerten
- Erlernen fortgeschrittener Taktiken, die von Angreifern verwendet werden, um in Netzwerke, die auf Windows-Umgebungen basieren, einzudringen und dort zu bleiben
- Erwerben von Kenntnissen über Strategien und Tools zur Eindämmung spezifischer Bedrohungen, die auf Windows-Betriebssysteme abzielen
- Kennenlernen von forensischen Analysetechniken, die auf Windows-Systeme

angewandt werden und die Identifizierung und Reaktion auf Vorfälle erleichtern

- Anwenden des theoretischen Wissens in simulierten Umgebungen und Teilnahme an praktischen Übungen, um spezifische Angriffe auf Windows-Systeme zu verstehen und abzuwehren
- Erlernen spezifischer Strategien zur Sicherung von Unternehmensumgebungen mit Windows-Betriebssystemen unter Berücksichtigung der Komplexität von Unternehmensinfrastrukturen
- Entwickeln von Kompetenzen zur Bewertung und Verbesserung von Sicherheitskonfigurationen auf Windows-Systemen, um sicherzustellen, dass wirksame Maßnahmen ergriffen werden
- Fördern ethischer und rechtlicher Praktiken bei der Durchführung von Angriffen und Tests auf Windows-Systeme unter Berücksichtigung der ethischen Grundsätze der Cybersicherheit
- Aktualisieren der Studenten im Hinblick auf die neuesten Trends und Bedrohungen bei Angriffen auf Windows-Systeme, um die kontinuierliche Relevanz und Wirksamkeit der erworbenen Fähigkeiten zu gewährleisten

Modul 3. 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

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

03

Kursleitung

In ihrem Bestreben, eine hervorragende Fortbildung zu bieten, verfügt TECH über einen renommierten Lehrkörper. Diese Spezialisten verfügen über einen umfangreichen beruflichen Hintergrund, da sie in renommierten Unternehmen tätig waren, die sich mit offensiver Cybersicherheit beschäftigen. Aus diesem Grund wird der Studiengang die fortschrittlichsten Ressourcen und Technologien in diesem Bereich beinhalten. Darüber hinaus wird ein umfassender Ansatz angeboten, um die Erwartungen der Studenten zu erfüllen, die sich in einem Bereich spezialisieren wollen, der ihnen viele Möglichkeiten bietet.

Sie werden von einem Lehrkörper unterstützt, der sich aus angesehenen Fachleuten der offensiven Cybersicherheit zusammensetzt"

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

Professoren

Hr. González Parrilla, Yuba

- Linienkoordinator für offensive Sicherheit und Red Team
- Spezialist für *Predictive*-Projektmanagement am Project Management Institute
- *SmartDefense*-Spezialist
- Experte für *Web Application Penetration Tester* bei eLearnSecurity
- Junior Penetration Tester bei eLearnSecurity
- Hochschulabschluss in Computertechnik an der Polytechnischen Universität von Madrid

Hr. Gallego Sánchez, Alejandro

- Pentester bei Grupo Oesía
- Cybersecurity-Berater bei Integración Tecnológica Empresarial, SL
- Audiovisueller Techniker bei Ingeniería Audiovisual SA
- Hochschulabschluss in Cybersicherheitstechnik an der Universität Rey Juan Carlos

04

Struktur und Inhalt

Dieses Programm ist in 3 Module unterteilt: Offensive Sicherheit, Angriffe auf Netzwerke und Systeme unter Windows und Analyse und Entwicklung von *Malware*. Während des gesamten Lehrplans wird eine praktische Perspektive geboten, die darauf abzielt, Bedrohungen frühzeitig zu erkennen. In diesem Sinne wird die Kreativität der Studenten gefördert, um Herausforderungen durch innovative Lösungen zu bewältigen. Darüber hinaus wird die Kategorisierung von Schwachstellen, einschließlich CVE, eingehend erforscht. Es werden auch fortgeschrittene Techniken zur Analyse von *Malware* erforscht, um die Sicherheit in Cyber-Umgebungen zu stärken.

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

Modul 1. Offensive Sicherheit

1.1. Definition und Kontext
- 1.1.1. Grundlegende Konzepte der offensiven Sicherheit
- 1.1.2. Bedeutung der Cybersicherheit heute
- 1.1.3. Herausforderungen und Chancen der offensiven Sicherheit

1.2. Grundlagen der Cybersicherheit
- 1.2.1. Frühe Herausforderungen und sich entwickelnde Bedrohungen
- 1.2.2. Technologische Meilensteine und ihre Auswirkungen auf die Cybersicherheit
- 1.2.3. Cybersicherheit im modernen Zeitalter

1.3. Grundlagen der offensiven Sicherheit
- 1.3.1. Schlüsselkonzepte und Terminologie
- 1.3.2. *Think Outside the Box*
- 1.3.3. Unterschiede zwischen offensivem und defensivem Hacking

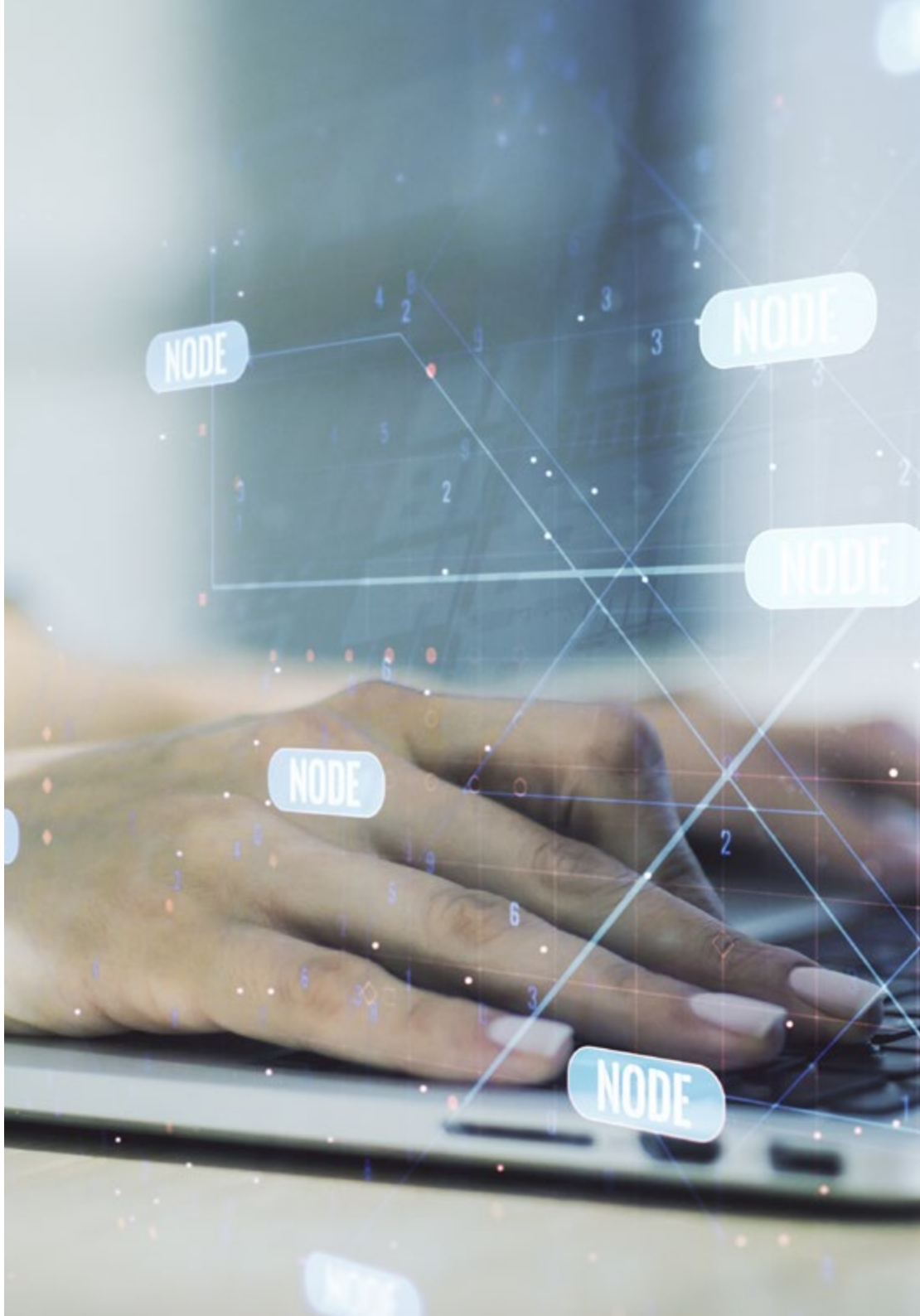
1.4. Offensive Sicherheitsmethoden
- 1.4.1. PTES (*Penetration Testing Execution Standard*)
- 1.4.2. OWASP (*Open Web Application Security Project*)
- 1.4.3. *Cyber Security Kill Chain*

1.5. Rollen und Verantwortlichkeiten bei der offensiven Sicherheit
- 1.5.1. Die wichtigsten Profile
- 1.5.2. *Bug Bounty Hunters*
- 1.5.3. *Researching:* Die Kunst des Recherchierens

1.6. Arsenal des Offensiv-Auditors
- 1.6.1. Betriebssysteme zum Hacking
- 1.6.2. Einführung in C2
- 1.6.3. *Metasploit:* Grundlagen und Verwendung
- 1.6.4. Nützliche Ressourcen

1.7. OSINT: Open-Source-Intelligenz
- 1.7.1. Grundlagen von OSINT
- 1.7.2. OSINT-Techniken und -Tools
- 1.7.3. OSINT-Anwendungen in der offensiven Sicherheit

1.8. Scripting: Einführung in die Automatisierung
- 1.8.1. Grundlagen des Scripting
- 1.8.2. *Scripting* in Bash
- 1.8.3. *Scripting* in Python



1.9. Schwachstellen-Kategorisierung
- 1.9.1. CVE (*Common Vulnerabilities and Exposure*)
- 1.9.2. CWE (*Common Weakness Enumeration*)
- 1.9.3. CAPEC (*Common Attack Pattern Enumeration and Classification*)
- 1.9.4. CVSS (*Common Vulnerability Scoring System*)
- 1.9.5. MITRE ATT & CK

1.10. Ethik und *Hacking*
- 1.10.1. Grundsätze der *Hacker*-Ethik
- 1.10.2. Die Grenze zwischen ethischem *Hacking* und bösartigem *Hacking*
- 1.10.3. Rechtliche Implikationen und Konsequenzen
- 1.10.4. Fallstudien: Ethische Situationen in der Cybersicherheit

Modul 2. Angriffe auf Netzwerke und Systeme unter Windows

2.1. Windows und Active Directory
- 2.1.1. Geschichte und Entwicklung von Windows
- 2.1.2. Active-Directory-Grundlagen
- 2.1.3. Funktionen und Dienste von Active Directory
- 2.1.4. Allgemeine Active-Directory-Architektur

2.2. Netzwerke in Active-Directory-Umgebungen
- 2.2.1. Netzwerkprotokolle in Windows
- 2.2.2. DNS und sein Betrieb in Active Directory
- 2.2.3. Netzwerk-Diagnosetools
- 2.2.4. Active-Directory-Netzwerke einrichten

2.3. Authentifizierung und Autorisierung in Active Directory
- 2.3.1. Authentifizierungsprozess und -ablauf
- 2.3.2. Berechtigungsnachweis-Typen
- 2.3.3. Speicherung und Verwaltung von Berechtigungsnachweisen
- 2.3.4. Sicherheit der Authentifizierung

2.4. Berechtigungen und Richtlinien in Active Directory
- 2.4.1. GPOs
- 2.4.2. Erzwingen und Verwalten von GPOs
- 2.4.3. Verwaltung von Berechtigungen in Active Directory
- 2.4.4. Schwachstellen bei Berechtigungen und Abhilfemaßnahmen

2.5. Kerberos-Grundlagen
- 2.5.1. Was ist Kerberos?
- 2.5.2. Komponenten und Funktionsweise
- 2.5.3. Tickets in Kerberos
- 2.5.4. Kerberos im Kontext von Active Directory

2.6. Erweiterte Kerberos-Techniken
- 2.6.1. Übliche Kerberos-Angriffe
- 2.6.2. Abhilfemaßnahmen und Schutzmaßnahmen
- 2.6.3. Überwachung des Kerberos-Verkehrs
- 2.6.4. Erweiterte Kerberos-Angriffe

2.7. *Active Directory Certificate Services* (ADCS)
- 2.7.1. Grundlegende Konzepte der PKI
- 2.7.2. ADCS-Rollen und -Komponenten
- 2.7.3. ADCS-Konfiguration und -Bereitstellung
- 2.7.4. ADCS-Sicherheit

2.8. Angriffe und Abwehrmaßnahmen in *Active Directory Certificate Services* (ADCS)
- 2.8.1. Häufige Schwachstellen in ADCS
- 2.8.2. Angriffe und Ausnutzungstechniken
- 2.8.3. Verteidigungsmaßnahmen und Abhilfemaßnahmen
- 2.8.4. ADCS-Überwachung und -Prüfung

2.9. Active-Directory-Überprüfung
- 2.9.1. Bedeutung von Audits im Active Directory
- 2.9.2. Audit-Tools
- 2.9.3. Erkennung von Anomalien und verdächtigen Verhaltensweisen
- 2.9.4. Reaktion auf Vorfälle und Wiederherstellung

2.10. Azure AD
- 2.10.1. Azure AD-Grundlagen
- 2.10.2. Synchronisierung mit dem lokalen Active Directory
- 2.10.3. Identitätsverwaltung in Azure AD
- 2.10.4. Integration mit Anwendungen und Diensten

Modul 3. Analyse und Entwicklung von *Malware*

3.1. Analyse und Entwicklung von *Malware*
- 3.1.1. Geschichte und Entwicklung von *Malware*
- 3.1.2. Klassifizierung und Arten von *Malware*
- 3.1.3. *Malware*-Scans
- 3.1.4. Entwicklung von *Malware*

3.2. Vorbereiten der Umgebung
- 3.2.1. Einrichten von virtuellen Maschinen und *Snapshots*
- 3.2.2. Tools zum Scannen von *Malware*
- 3.2.3. Tools zur Entwicklung von *Malware*

3.3. Windows-Grundlagen
- 3.3.1. PE (*Portable Executable*) Dateiformat
- 3.3.2. Prozesse und *Threads*
- 3.3.3. Dateisystem und Registry
- 3.3.4. *Windows Defender*

3.4. Grundlegende *Malware*-Techniken
- 3.4.1. *Shellcode*-Erzeugung
- 3.4.2. Ausführen von *Shellcode* auf der Festplatte
- 3.4.3. Festplatte vs. Speicher
- 3.4.4. Ausführen von *Shellcode* im Speicher

3.5. Zwischengeschaltete *Malware*-Techniken
- 3.5.1. Windows-Persistenz
- 3.5.2. Startup-Ordner
- 3.5.3. Registrierungsschlüssel
- 3.5.4. Bildschirmschoner

3.6. Erweiterte *Malware*-Techniken
- 3.6.1. *Shellcode*-Verschlüsselung (XOR)
- 3.6.2. *Shellcode*-Verschlüsselung (RSA)
- 3.6.3. *String*-Verschleierung
- 3.6.4. Prozess-Injektion

3.7. Statische *Malware*-Analyse
- 3.7.1. Analyse von *Packers* mit DIE (*Detect It Easy*)
- 3.7.2. Analyse von Sektionen mit PE-Bear
- 3.7.3. Dekompilieren mit Ghidra

3.8. Dynamische *Malware*-Analyse
- 3.8.1. Verhaltensbeobachtung mit Process Hacker
- 3.8.2. Analyse von Aufrufen mit API Monitor
- 3.8.3. Analyse von Änderungen in der Registrierung mit Regshot
- 3.8.4. Beobachtung von Netzwerkanfragen mit TCPView

3.9. Scannen in .NET
- 3.9.1. Einführung in .NET
- 3.9.2. Dekompilieren mit dnSpy
- 3.9.3. Fehlersuche mit dnSpy
- 3.10. Analyse von echter *Malware*

3.10.1. Vorbereiten der Umgebung
- 3.10.2. Statische Analyse der *Malware*
- 3.10.3. Dynamische Analyse der *Malware*
- 3.10.4. Erstellung von YARA-Regeln

Keine vorgegebenen Zeit- oder Bewertungspläne. Darum geht es bei dieser TECH-Fortbildung!“

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

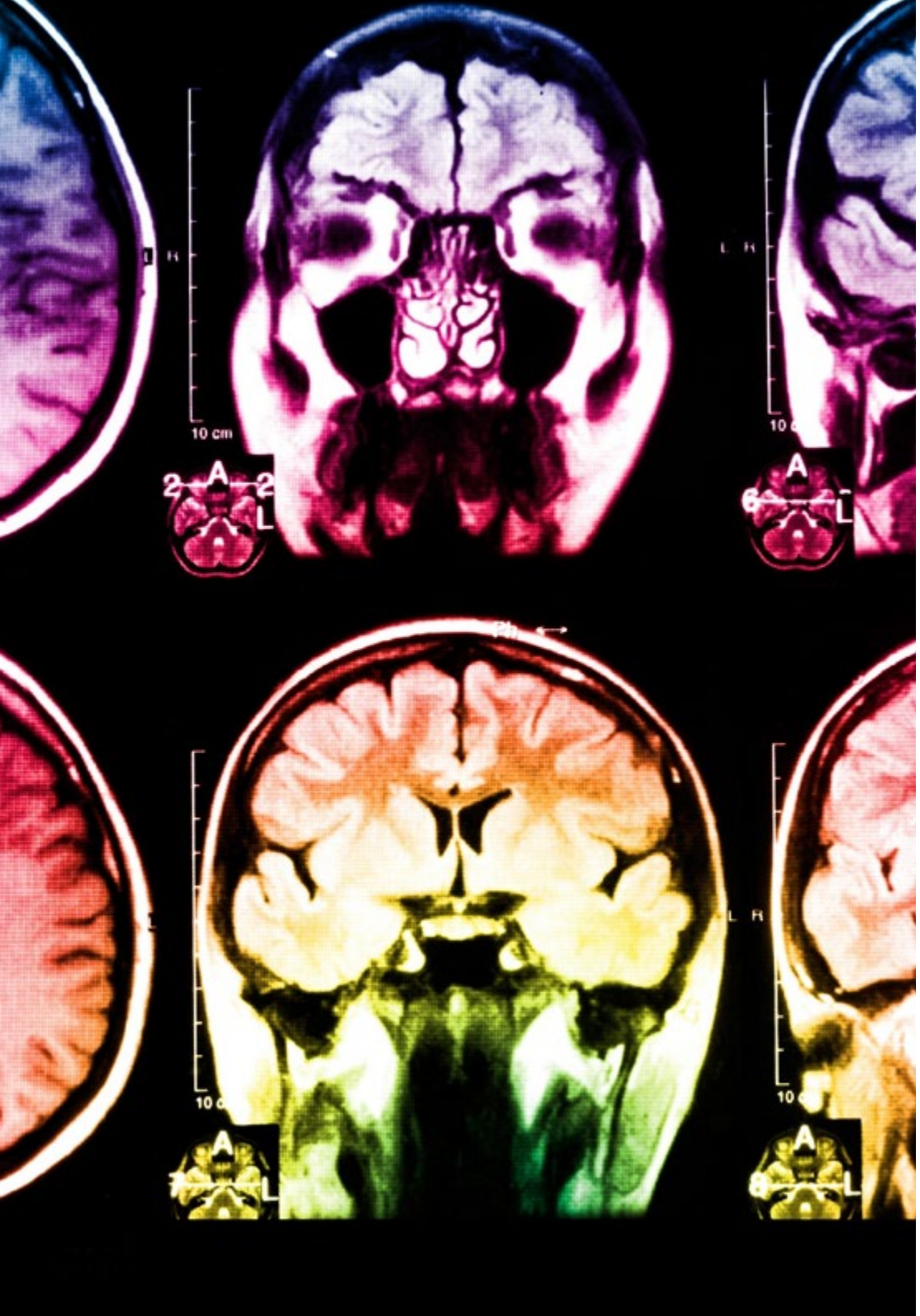
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

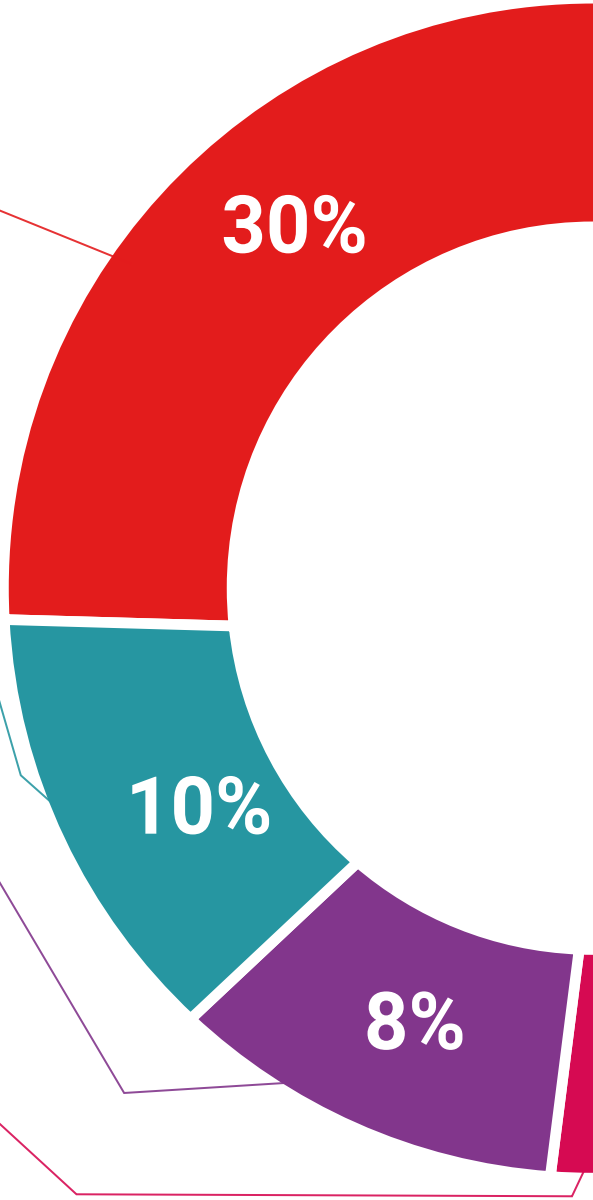
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

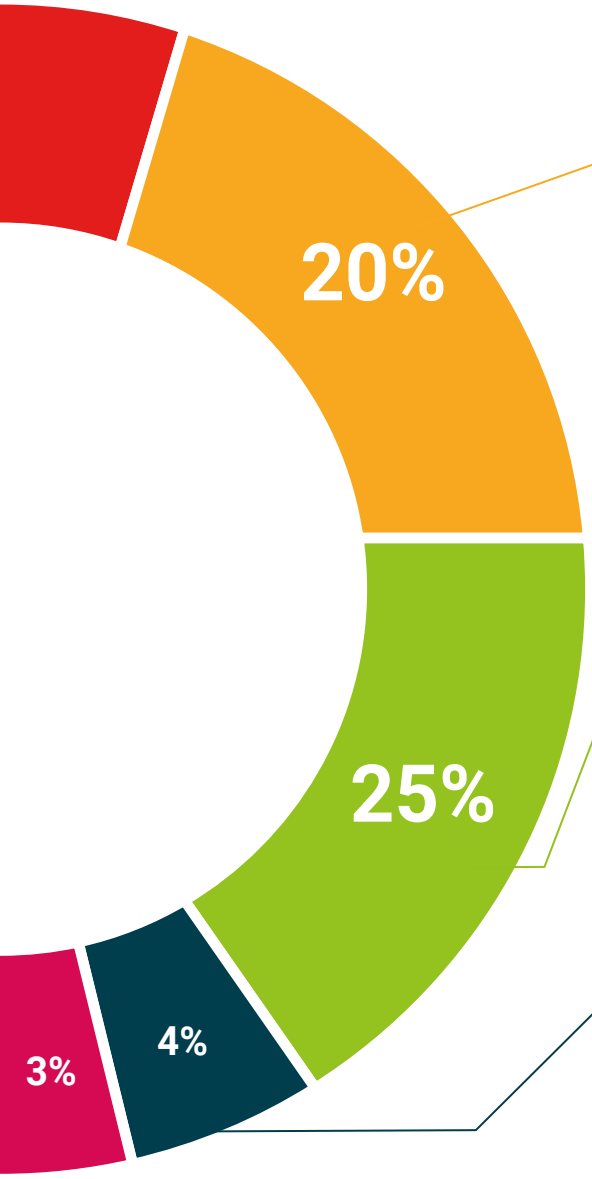
Übungen für Fertigkeiten und Kompetenzen

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 Offensive 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 Offensive 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 Offensive 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

Offensive 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
Offensive Cybersicherheit

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

Universitätsexperte
Offensive Cybersicherheit

tech technologische universität