Executive Master

Pentesting und Red Team

MPRT

tech global university

tech global university

Executive Master
Pentesting und Red Team

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Global University**
- Akkreditierung: **60 ECTS**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**
- Gerichtet an: **Hochschulabsolventen, die zuvor einen der Studiengänge in den Bereichen Sozial- oder Rechtswissenschaften, Verwaltung oder Betriebswirtschaft abgeschlossen haben.**

Internetzugang: **www.techtitute.com/de/wirtschaftsschule/masterstudiengang/masterstudiengang-pentesting-red-team**

Index

01

Willkommen

Heutzutage haben Cyberangriffe erheblich an Bedeutung und Stärke gewonnen und beunruhigen die Bevölkerung und die Unternehmen selbst. Infolgedessen haben die Unternehmen exponentiell unter diesen Bedrohungen gelitten und müssen die Datenbanken und sensiblen Informationen ihrer Kunden maximal schützen. Daher ist dieser Sektor ständig auf der Suche nach hochqualifizierten Experten für Cybersicherheit. TECH hat daher dieses akademische Programm mit technologischen Ressourcen und anderen Entwicklungen rund um die von böswilligen Akteuren verwendeten Taktiken, Techniken und Verfahren entwickelt. All dies wird durch die *Relearning*-Methode und eine vollständige 100%ige Online-Plattform ermöglicht, die Flexibilität und Zeitersparnis bietet.

Executive Master in Pentesting und Red Team
TECH Global University

Dank dieses 100%igen Online-Programms werden Sie sich auf die Förderung ethischer und rechtlicher Praktiken bei der Durchführung von Angriffen und Tests auf Windows-Systeme spezialisieren"

02

Warum an der TECH studieren?

TECH ist die weltweit größte 100%ige Online Business School. Es handelt sich um eine Elite-Business School mit einem Modell, das höchsten akademischen Ansprüchen genügt. Ein leistungsstarkes internationales Zentrum für die intensive Fortbildung von Führungskräften.

TECH ist eine Universität an der Spitze der Technologie, die dem Studenten alle Ressourcen zur Verfügung stellt, um ihm zu helfen, geschäftlich erfolgreich zu sein"

Bei TECH Technologische Universität

Innovation

Die Universität bietet ein Online-Lernmodell an, das modernste Bildungstechnologie mit höchster pädagogischer Genauigkeit verbindet. Eine einzigartige Methode mit höchster internationaler Anerkennung, die dem Studenten die Schlüssel für seine Entwicklung in einer Welt des ständigen Wandels liefert, in der Innovation der wesentliche Einsatz eines jeden Unternehmers sein muss.

"Die Erfolgsgeschichte von Microsoft Europa" für die Einbeziehung des neuen interaktiven Multivideosystems in unsere Programme.

Maximalforderung

Das Zulassungskriterium von TECH ist nicht wirtschaftlich. Sie brauchen keine große Investitionen zu tätigen, um bei TECH zu studieren. Um jedoch einen Abschluss bei TECH zu erlangen, werden die Grenzen der Intelligenz und der Kapazität des Studenten getestet. Die akademischen Standards von TECH sind sehr hoch...

95% | **der Studenten von TECH schließen ihr Studium erfolgreich ab**

Networking

Fachleute aus der ganzen Welt nehmen an der TECH teil, so dass der Student ein großes Netzwerk von Kontakten knüpfen kann, die für seine Zukunft nützlich sein werden.

+100.000
jährlich spezialisierte Manager

+200
verschiedene Nationalitäten

Empowerment

Der Student wird Hand in Hand mit den besten Unternehmen und Fachleuten von großem Prestige und Einfluss wachsen. TECH hat strategische Allianzen und ein wertvolles Netz von Kontakten zu den wichtigsten Wirtschaftsakteuren auf den 7 Kontinenten aufgebaut.

+500 | **Partnerschaften mit den besten Unternehmen**

Talent

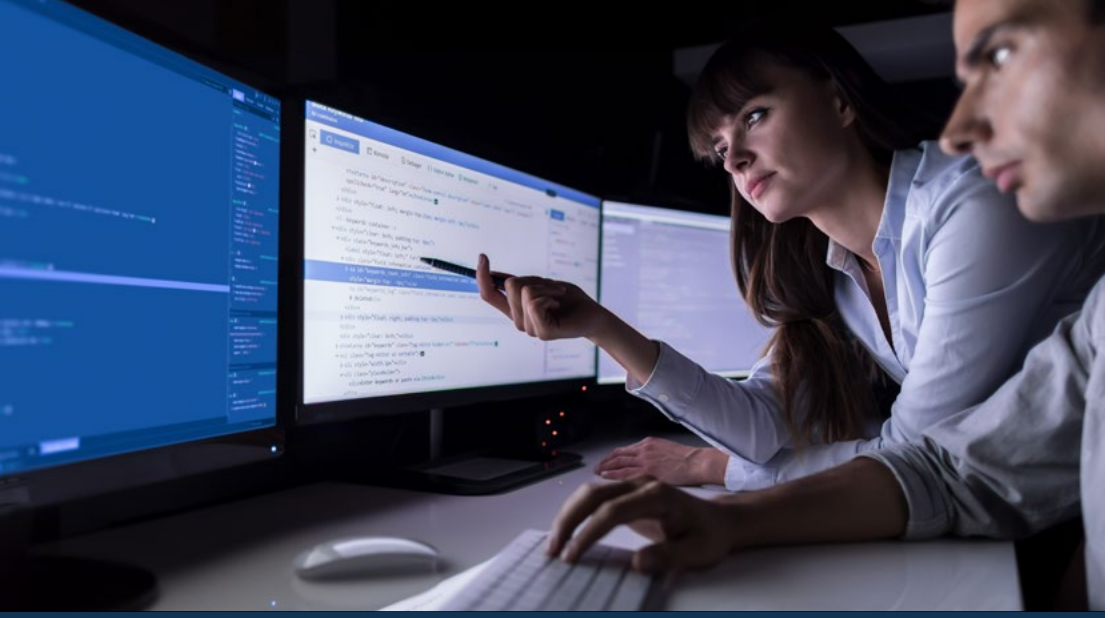
Dieses Programm ist ein einzigartiger Vorschlag, um die Talente des Studenten in der Geschäftswelt zu fördern. Eine Gelegenheit für ihn, seine Anliegen und seine Geschäftsvision vorzutragen.

TECH hilft dem Studenten, sein Talent am Ende dieses Programms der Welt zu zeigen.

Multikultureller Kontext

Ein Studium bei TECH bietet dem Studenten eine einzigartige Erfahrung. Er wird in einem multikulturellen Kontext studieren. In einem Programm mit einer globalen Vision, dank derer er die Arbeitsweise in verschiedenen Teilen der Welt kennenlernen und die neuesten Informationen sammeln kann, die am besten zu seiner Geschäftsidee passen.

Unsere Studenten kommen aus mehr als 200 Ländern.



Mit den Besten lernen

Das Lehrteam von TECH erklärt im Unterricht, was sie in ihren Unternehmen zum Erfolg geführt hat, und zwar in einem realen, lebendigen und dynamischen Kontext. Lehrkräfte, die sich voll und ganz dafür einsetzen, eine hochwertige Spezialisierung zu bieten, die es dem Studenten ermöglicht, in seiner Karriere voranzukommen und sich in der Geschäftswelt zu profilieren.

Lehrkräfte aus 20 verschiedenen Ländern.

Bei TECH werden Sie Zugang zu den präzisesten und aktuellsten Fallstudien im akademischen Bereich haben"

TECH strebt nach Exzellenz und hat zu diesem Zweck eine Reihe von Merkmalen, die sie zu einer einzigartigen Universität machen:

Analyse

TECH erforscht die kritische Seite des Studenten, seine Fähigkeit, Dinge zu hinterfragen, seine Problemlösungsfähigkeiten und seine zwischenmenschlichen Fähigkeiten.

Akademische Spitzenleistung

TECH bietet dem Studenten die beste Online-Lernmethodik. Die Universität kombiniert die *Relearning*-Methode (die international am besten bewertete Lernmethode für Aufbaustudien) mit der Fallstudie. Tradition und Avantgarde in einem schwierigen Gleichgewicht und im Rahmen einer anspruchsvollen akademischen Laufbahn.

Skaleneffekt

TECH ist die größte Online-Universität der Welt. Sie verfügt über ein Portfolio von mehr als 10.000 Hochschulabschlüssen. Und in der neuen Wirtschaft gilt: **Volumen + Technologie = disruptiver Preis**. Damit stellt TECH sicher, dass das Studium nicht so kostspielig ist wie an anderen Universitäten.

03

Warum unser Programm?

Die Teilnahme am TECH-Programm bedeutet eine Vervielfachung der Chancen auf beruflichen Erfolg im Bereich der höheren Unternehmensführung.

Es ist eine Herausforderung, die Anstrengung und Hingabe erfordert, aber die Tür zu einer vielversprechenden Zukunft öffnet. Der Student wird von den besten Lehrkräften und mit den flexibelsten und innovativsten Lehrmethoden unterrichtet.

Wir verfügen über das renommierteste Dozententeam und den umfassendsten Lehrplan auf dem Markt, so dass wir Ihnen eine Fortbildung auf höchstem akademischen Niveau bieten können"

Dieses Programm bietet eine Vielzahl von beruflichen und persönlichen Vorteilen, darunter die Folgenden:

01

Einen deutlichen Schub für die Karriere des Studenten

Mit einem Studium bei TECH wird der Student seine Zukunft selbst in die Hand nehmen und sein volles Potenzial entfalten können. Durch die Teilnahme an diesem Programm wird er die notwendigen Kompetenzen erwerben, um in kurzer Zeit eine positive Veränderung in seiner Karriere zu erreichen.

70% der Teilnehmer dieser Spezialisierung erreichen in weniger als 2 Jahren eine positive Veränderung in ihrer Karriere.

02

Entwicklung einer strategischen und globalen Vision des Unternehmens

TECH bietet einen detaillierten Überblick über das allgemeine Management, um zu verstehen, wie sich jede Entscheidung auf die verschiedenen Funktionsbereiche des Unternehmens auswirkt.

Die globale Vision des Unternehmens von TECH wird Ihre strategische Vision verbessern.

03

Konsolidierung des Studenten in der Unternehmensführung

Ein Studium an der TECH öffnet die Türen zu einem beruflichen Panorama von großer Bedeutung, so dass der Student sich als hochrangiger Manager mit einer umfassenden Vision des internationalen Umfelds positionieren kann.

Sie werden mehr als 100 reale Fälle aus dem Bereich der Unternehmensführung bearbeiten.

04

Übernahme neuer Verantwortung

Während des Programms werden die neuesten Trends, Entwicklungen und Strategien vorgestellt, damit der Student seine berufliche Tätigkeit in einem sich verändernden Umfeld ausüben kann.

45% der Studenten werden intern befördert.

05

Zugang zu einem leistungsfähigen Netzwerk von Kontakten

TECH vernetzt seine Studenten, um ihre Chancen zu maximieren. Studenten mit den gleichen Sorgen und dem Wunsch zu wachsen. So wird es möglich sein, Partner, Kunden oder Lieferanten zu teilen.

Sie werden ein Netz von Kontakten finden, das für Ihre berufliche Entwicklung unerlässlich ist.

06

Rigorose Entwicklung von Unternehmensprojekten

Der Student wird eine tiefgreifende strategische Vision erlangen, die ihm helfen wird, sein eigenes Projekt unter Berücksichtigung der verschiedenen Bereiche des Unternehmens zu entwickeln.

20% unserer Studenten entwickeln ihre eigene Geschäftsidee.

07

Verbesserung von *Soft Skills* und Führungsqualitäten

TECH hilft dem Studenten, sein erworbenes Wissen anzuwenden und weiterzuentwickeln und seine zwischenmenschlichen Fähigkeiten zu verbessern, um eine Führungspersönlichkeit zu werden, die etwas bewirkt.

Verbessern Sie Ihre Kommunikations- und Führungsfähigkeiten und geben Sie Ihrer Karriere einen neuen Impuls.

08

Teil einer exklusiven Gemeinschaft sein

Der Student wird Teil einer Gemeinschaft von Elite-Managern, großen Unternehmen, renommierten Institutionen und qualifizierten Professoren der renommiertesten Universitäten der Welt sein: die Gemeinschaft der TECH Technologischen Universität.

Wir bieten Ihnen die Möglichkeit, sich mit einem Team von international anerkannten Dozenten zu spezialisieren.

04

Ziele

Dieser Hochschulabschluss wird Studenten mit innovativen Updates in Bezug auf Vorschriften und Compliance bei Cybersicherheitsprojekten im Bereich *Pentesting* versorgen und so einen Mehrwert für ihre berufliche Laufbahn bieten. In diesem Sinne wird TECH während der gesamten Entwicklung des Programms didaktische Ressourcen zur Verfügung stellen, um die Kompetenzen im Zusammenhang mit der Erkennung von Anomalien und verdächtigem Verhalten zu verbessern. So wird der Absolvent am Ende dieses Programms sein Wissen über *Pentesting und Red Team* erweitert haben. Und das alles in einer 12-monatigen Online-Fortbildung.

Nach diesem Executive Master werden Sie auf dem neuesten Stand sein, was den Nutzen der digitalen Forensik (DFIR) bei der Aufklärung von Cyberkriminalität angeht"

TECH macht sich die Ziele ihrer Studenten zu eigen
Gemeinsam arbeiten sie daran, diese zu erreichen

Der **Executive Master in Pentesting und Red Team** wird den Studenten zu Folgendem befähigen:

01 Studieren und Verstehen der Taktiken, Techniken und Verfahren, die von böswilligen Akteuren eingesetzt werden, um Bedrohungen zu identifizieren und zu simulieren

02 Anwenden von theoretischen Kenntnissen in praktischen Szenarien und Simulationen, wobei echte Herausforderungen bewältigt werden, um die *Pentesting*-Fähigkeiten zu stärken

03 Lernen, wie man Ressourcen innerhalb eines *Cybersecurity*-Teams effizient zuweist, wobei die individuellen Fähigkeiten berücksichtigt und die Projektproduktivität maximiert werden

04 Verbessern der Kommunikationsfähigkeiten in einem technischen Umfeld, um das Verständnis und die Koordination zwischen den Teammitgliedern zu erleichtern

05 Erlernen von Techniken zur Überwachung und Steuerung von Projekten, zur Erkennung von Abweichungen und zur Ergreifung von Korrekturmaßnahmen bei Bedarf

06 Entwickeln von Kompetenzen zur Bewertung und Verbesserung von Sicherheitskonfigurationen auf Windows-Systemen, um sicherzustellen, dass wirksame Maßnahmen ergriffen werden

07 Fördern ethischer und rechtlicher Praktiken bei der Durchführung von Angriffen und Tests auf Windows-Systeme unter Berücksichtigung der ethischen Grundsätze der Cybersicherheit

08 Kennenlernen der Bewertung der Sicherheit von APIs und Webdiensten, Identifizierung potenzieller Schwachstellen und Stärkung der Sicherheit von Programmierschnittstellen

09 Fördern der effektiven Zusammenarbeit mit Sicherheitsteams, um Strategien und Bemühungen zum Schutz der Netzwerkinfrastruktur zu integrieren

10 Fördern ethischer und rechtlicher Praktiken bei der Analyse und Entwicklung von *Malware* und Gewährleisten von Integrität und Verantwortlichkeit bei allen Aktivitäten

11 Anwenden von theoretischem Wissen in simulierten Umgebungen, Durchführung von praktischen Übungen, um bösartige Angriffe zu verstehen und abzuwehren

12 Erwerben eines soliden Verständnisses der grundlegenden Prinzipien der digitalen forensischen Untersuchung (DFIR) und ihrer Anwendung bei der Lösung von Cybervorfällen

13 Lernen, detaillierte Berichte zu erstellen, in denen die Ergebnisse, die angewandten Methoden und die aus fortgeschrittenen *Red-Team*-Übungen abgeleiteten Empfehlungen dokumentiert werden

14 Entwickeln von Fähigkeiten, um umsetzbare und praktische Empfehlungen zu formulieren, die darauf abzielen, Schwachstellen zu entschärfen und die Sicherheitslage zu verbessern

15 Kennenlernen der Best Practices für die Berichterstattung an Führungskräfte, um technische Informationen für ein nicht technisches Publikum aufzubereiten

05

Kompetenzen

Dieser Abschluss wird dem Studenten einen aktuellen Überblick über *Pentesting* geben. Dies wird ihm die Möglichkeit geben, seine Fähigkeiten zu erweitern, indem er Führungsaufgaben übernimmt, sich herausfordernden und wechselnden Situationen stellt und sogar Hand in Hand und effektiv mit anderen Unternehmen im IT-Sektor zusammenarbeitet. Auf diese Weise stehen der Fachkraft mehrere Hilfsmittel zur Verfügung, wie z. B. Infografiken und Videos, die eine praktischere Perspektive auf dieses Fachgebiet bieten.

Verbessern Sie Ihre Fähigkeiten zur effektiven Erkennung und Vorbeugung von Malware und lösen Sie die schwierigsten Situationen im IT-Sektor"

01 Erwerben von *Coaching*-Fähigkeiten für die berufliche Entwicklung von Teammitgliedern, um deren Wachstum und Verbesserung zu fördern

02 Entwickeln strategischer Entscheidungsfähigkeiten in Cybersicherheitssituationen unter Berücksichtigung der kurz- und langfristigen Auswirkungen auf die organisatorische Sicherheit

03 Erwerben von Kompetenzen zur Identifizierung, Bewertung und Abschwächung von Risiken, die für Cybersicherheitsprojekte spezifisch sind

04 Entwickeln von Fähigkeiten zur Implementierung aktiver Verteidigungsmaßnahmen, die die System- und Netzwerksicherheit stärken

05 Erlernen von Techniken zur Analyse des Internetverkehrs, um Muster und anomales Verhalten zu identifizieren und so mögliche Bedrohungen zu erkennen

06 Erwerben von Kompetenzen in der forensischen Analyse von Netzwerkumgebungen, die eine effektive Identifizierung von und Reaktion auf Cyber-Vorfälle ermöglichen

07 Erlernen von Strategien zur effektiven Erkennung und Verhinderung von Malware, einschließlich des Einsatzes fortschrittlicher Sicherheitslösungen

08 Entwickeln von Fähigkeiten zur Identifizierung von Kompromissindikatoren (Indicators of Compromise, IoC) während der forensischen Untersuchung, um die Erkennung von Vorfällen und die Reaktion darauf zu erleichtern

09 Erwerben von Fähigkeiten zur strategischen Planung von *Red-Team*-Übungen unter Berücksichtigung von Zielen, Umfang, Ressourcen und realistischen Szenarien

10 Erwerben von Fähigkeiten zur Identifizierung und Priorisierung von Schwachstellen, Hervorheben derjenigen, die das größte Sicherheitsrisiko darstellen

06

Struktur und Inhalt

Der Studiengang Pentesting und Red Team ist ein Programm, das sich im Wesentlichen darauf konzentriert, dass der Student die Kompetenzen im Zusammenhang mit der Computerforensik in der Cybersicherheit erwirbt. Daher basiert diese Weiterbildung auf einer theoretisch-praktischen Struktur, die von der breiten Erfahrung und dem umfassenden Hintergrund eines hochspezialisierten Expertenteams begleitet wird.

Es gibt keine vordefinierten Zeitpläne oder kontinuierliche Prüfungen: TECH garantiert Ihnen auf diese Weise den schnellsten und flexibelsten Zugang zu den akademischen Inhalten"

Lehrplan

Dieser Hochschulabschluss besteht aus 1.500 Stunden kontinuierlichen Lernens durch Unterricht auf höchstem Niveau, dank dessen der Absolvent die besten Positionen im IT- und Wirtschaftssektor erreichen wird. Auf diese Weise werden die Studenten die verschiedenen Hindernisse überwinden, die ihnen das Arbeitsumfeld auferlegt. Dieser Abschluss vermittelt zahlreiche Fähigkeiten, die sich mit fortgeschrittenen Techniken in Kerberos, Abschwächungen und Schutzmaßnahmen befassen.

Andererseits hat das Dozententeam einen exklusiven Lehrplan entwickelt, der 10 Module umfasst, mit dem Ziel, dass der Student grundlegende Kompetenzen im Zusammenhang mit der Bewertung der Sicherheit von APIs und Webdiensten erwirbt und mögliche Schwachstellen identifiziert.

Ebenso wird sich die Fachkraft mit umsetzbaren und praktischen Empfehlungen befassen, die darauf abzielen, Schwachstellen zu entschärfen und die Sicherheitslage zu verbessern. In diesem Sinne wird sie zu einem wichtigen Spezialisten auf dem Gebiet der Konfliktprävention und der Messmethoden.

Bei diesem akademischen Programm werden die Unternehmer durch die einzigartige *Relearning*-Methode unterstützt, die es ihnen ermöglicht, komplexe Konzepte zu untersuchen und deren tägliche Anwendung nahtlos zu übernehmen. Gleichzeitig wird der Abschluss auf einer innovativen 100%igen Online-Lernplattform vermittelt, die nicht an feste Zeitpläne oder kontinuierliche Bewertungen gebunden ist.

Dieser Executive Master erstreckt sich über 12 Monate und ist in 10 Module unterteilt:

Modul 1	Offensive Sicherheit
Modul 2	Management von *Cybersecurity*-Teams
Modul 3	Sicherheits-Projektmanagement
Modul 4	Angriffe auf Netzwerke und Systeme unter Windows
Modul 5	Fortgeschrittenes Web-*Hacking*
Modul 6	Netzwerkarchitektur und -Sicherheit
Modul 7	Analyse und Entwicklung von *Malware*
Modul 8	Forensische Grundlagen und DFIR
Modul 9	Fortgeschrittene *Red-Team*-Übungen
Modul 10	Technischer Bericht und Executive Report

Wo, wann und wie wird unterrichtet?

TECH bietet die Möglichkeit, diesen Executive Master in Pentesting und Red Team vollständig online zu absolvieren. Während der 12-monatigen Spezialisierung wird der Student jederzeit auf alle Inhalte dieses Programms zugreifen können, was ihm die Möglichkeit gibt, seine Studienzeit selbst zu verwalten.

Eine einzigartige, wichtige und entscheidende Bildungserfahrung, um Ihre berufliche Entwicklung voranzutreiben und den endgültigen Sprung zu schaffen.

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. Management von *Cybersecurity*-Teams

2.1. Team-Management
2.1.1. Wer ist wer
2.1.2. Der Direktor
2.1.3. Schlussfolgerungen

2.2. Rollen und Verantwortlichkeiten
2.2.1. Identifizierung der Rollen
2.2.2. Effektive Delegation
2.2.3. Erwartungsmanagement

2.3. Bildung und Entwicklung von Teams
2.3.1. Etappen der Bildung von Teams
2.3.2. Gruppendynamiken
2.3.3. Bewertung und Feedback

2.4. Talentmanagement
2.4.1. Identifizierung von Talenten
2.4.2. Entwicklung von Fähigkeiten
2.4.3. Talentbindung

2.5. Teamführung und Motivation
2.5.1. Führungsstile
2.5.2. Theorien zur Motivation
2.5.3. Anerkennung von Leistungen

2.6. Kommunikation und Koordination
2.6.1. Kommunikationstools
2.6.2. Kommunikationsbarrieren
2.6.3. Strategien zur Koordinierung

2.7. Strategische Personalentwicklungsplanung
2.7.1. Identifizierung des Schulungsbedarfs
2.7.2. Individuelle Entwicklungspläne
2.7.3. Überwachung und Bewertung

2.8. Konfliktlösung
2.8.1. Identifizierung von Konflikten
2.8.2. Messmethoden
2.8.3. Konfliktvermeidung

2.9. Qualitätsmanagement und kontinuierliche Verbesserung
2.9.1. Grundsätze der Qualität
2.9.2. Techniken zur kontinuierlichen Verbesserung
2.9.3. *Feedback* und Rückmeldung

2.10. Werkzeuge und Technologien
2.10.1. Plattformen für die Zusammenarbeit
2.10.2. Projektmanagement
2.10.3. Schlussfolgerungen

Modul 3. Sicherheits-Projektmanagement

3.1. Sicherheitsprojektmanagement
3.1.1. Definition und Zweck des Cybersicherheits-Projektmanagements
3.1.2. Wichtigste Herausforderungen
3.1.3. Überlegungen

3.2. Lebenszyklus eines Sicherheitsprojekts
3.2.1. Anfangsphase und Definition der Ziele
3.2.2. Umsetzung und Durchführung
3.2.3. Bewertung und Überprüfung

3.3. Planung und Ressourcenabschätzung
3.3.1. Grundlegende Konzepte des wirtschaftlichen Managements
3.3.2. Bestimmung der menschlichen und technischen Ressourcen
3.3.3. Budgetierung und damit verbundene Kosten

3.4. Projektdurchführung und Kontrolle
3.4.1. Überwachung und Nachverfolgung
3.4.2. Anpassungen und Änderungen des Projekts
3.4.3. Halbzeitbewertung und Überprüfungen

3.5. Projektkommunikation und Berichterstattung
3.5.1. Wirksame Kommunikationsstrategien
3.5.2. Berichterstattung und Präsentation
3.5.3. Kommunikation mit Kunden und Management

3.6. Werkzeuge und Technologien
3.6.1. Planungs- und Organisationstools
3.6.2. Tools für Zusammenarbeit und Kommunikation
3.6.3. Tools für Dokumentation und Speicherung

3.7. Dokumentation und Protokolle
3.7.1. Strukturierung und Erstellung von Dokumentation
3.7.2. Protokolle für Maßnahmen
3.7.3. Leitfäden

3.8. Vorschriften und Compliance bei Cybersicherheitsprojekten
3.8.1. Internationale Gesetze und Vorschriften
3.8.2. Einhaltung der Vorschriften
3.8.3. Audits

3.9. Risikomanagement bei Sicherheitsprojekten
3.9.1. Identifizierung und Analyse von Risiken
3.9.2. Strategien zur Risikominderung
3.9.3. Risikoüberwachung und Überprüfung

3.10. Abschluss des Projekts
3.10.1. Überprüfung und Bewertung
3.10.2. Abschließende Dokumentation
3.10.3. *Feedback*

Modul 4. Angriffe auf Netzwerke und Systeme unter Windows

4.1. Windows und Active Directory
4.1.1. Geschichte und Entwicklung von Windows
4.1.2. Active-Directory-Grundlagen
4.1.3. Funktionen und Dienste von Active Directory
4.1.4. Allgemeine Active-Directory-Architektur

4.2. Netzwerke in Active-Directory-Umgebungen
4.2.1. Netzwerkprotokolle in Windows
4.2.2. DNS und sein Betrieb in Active Directory
4.2.3. Netzwerk-Diagnosetools
4.2.4. Active-Directory-Netzwerke einrichten

4.3. Authentifizierung und Autorisierung in Active Directory
4.3.1. Authentifizierungsprozess und -ablauf
4.3.2. Berechtigungsnachweis-Typen
4.3.3. Speicherung und Verwaltung von Berechtigungsnachweisen
4.3.4. Sicherheit der Authentifizierung

4.4. Berechtigungen und Richtlinien in Active Directory
4.4.1. GPOs
4.4.2. Erzwingen und Verwalten von GPOs
4.4.3. Verwaltung von Berechtigungen in Active Directory
4.4.4. Schwachstellen bei Berechtigungen und Abhilfemaßnahmen

4.5. Kerberos-Grundlagen
4.5.1. Was ist Kerberos?
4.5.2. Komponenten und Funktionsweise
4.5.3. Tickets in Kerberos
4.5.4. Kerberos im Kontext von Active Directory

4.6. Erweiterte Kerberos-Techniken
4.6.1. Übliche Kerberos-Angriffe
4.6.2. Abhilfemaßnahmen und Schutzmaßnahmen
4.6.3. Überwachung des Kerberos-Verkehrs
4.6.4. Erweiterte Kerberos-Angriffe

4.7. *Active Directory Certificate Services* (ADCS)
4.7.1. Grundlegende Konzepte der PKI
4.7.2. ADCS-Rollen und -Komponenten
4.7.3. ADCS-Konfiguration und -Bereitstellung
4.7.4. ADCS-Sicherheit

4.8. Angriffe und Abwehrmaßnahmen in *Active Directory Certificate Services* (ADCS)
4.8.1. Häufige Schwachstellen in ADCS
4.8.2. Angriffe und Ausnutzungstechniken
4.8.3. Verteidigungsmaßnahmen und Abhilfemaßnahmen
4.8.4. ADCS-Überwachung und -Prüfung

4.9. Active-Directory-Überprüfung
4.9.1. Bedeutung von Audits im Active Directory
4.9.2. Audit-Tools
4.9.3. Erkennung von Anomalien und verdächtigen Verhaltensweisen
4.9.4. Reaktion auf Vorfälle und Wiederherstellung

4.10. Azure AD
4.10.1. Azure AD-Grundlagen
4.10.2. Synchronisierung mit dem lokalen Active Directory
4.10.3. Identitätsverwaltung in Azure AD
4.10.4. Integration mit Anwendungen und Diensten

Modul 5. Fortgeschrittenes Web-*Hacking*

5.1. Wie eine Website funktioniert
5.1.1. Die URL und ihre Bestandteile
5.1.2. HTTP-Methoden
5.1.3. Die Kopfzeilen
5.1.4. Wie man Webanfragen mit Burp Suite betrachtet

5.2. Sitzungen
5.2.1. Die *Cookies*
5.2.2. *Tokens* JWT
5.2.3. *Session-Hijacking*-Angriffe
5.2.4. JWT-Angriffe

5.3. *Cross Site Scripting* (XSS)
5.3.1. Was ist ein XSS
5.3.2. Arten von XSS
5.3.3. Ausnutzen eines XSS
5.3.4. Einführung in *XSLeaks*

5.4. Datenbank-Injektionen
5.4.1. Was ist eine SQL-*Injection*?
5.4.2. Exfiltrieren von Informationen mit SQLi
5.4.3. SQLi Blind, Time-Based und Error-Based
5.4.4. NoSQLi-Injektionen

5.5. *Path Traversal und Local File Inclusion*
5.5.1. Was sie sind und ihre Unterschiede
5.5.2. Übliche Filter und wie man sie umgeht
5.5.3. *Log Poisoning*
5.5.4. LFIs in PHP

5.6. *Broken Authentication*
5.6.1. *User Enumeration*
5.6.2. *Password Bruteforce*
5.6.3. 2FA Bypass
5.6.4. *Cookies* mit sensiblen und änderbaren Informationen

5.7. *Remote Command Execution*
5.7.1. *Command Injection*
5.7.2. *Blind Command Injection*
5.7.3. *Insecure Deserialization* PHP
5.7.4. *Insecure Deserialization* Java

5.8. *File Uploads*
5.8.1. CERs über *Webshells*
5.8.2. XSS in Dateiuploads
5.8.3. XML *External Entity* (XXE) *Injection*
5.8.4. *Path traversal* bei Dateiuploads

5.9. *Broken Acess Control*
5.9.1. Uneingeschränkter Zugang zu den Panels
5.9.2. *Insecure Direct Object References* (IDOR)
5.9.3. Filter-*Bypass*
5.9.4. Unzureichende Autorisierungsmethoden

5.10. DOM-Schwachstellen und weitergehende Angriffe
5.10.1. *Regex Denial of Service*
5.10.2. DOM *Clobbering*
5.10.3. *Prototype Pollution*
5.10.4. HTTP *Request Smuggling*

Modul 6. Netzwerkarchitektur und -sicherheit

6.1. Computer-Netzwerke
6.1.1. Grundlegende Konzepte: LAN, WAN, CP, CC-Protokolle
6.1.2. OSI-Modell und TCP/IP
6.1.3. *Switching:* Grundlegende Konzepte
6.1.4. *Routing*: Grundlegende Konzepte

6.2. *Switching*
6.2.1. Einführung in VLANs
6.2.2. STP
6.2.3. *EtherChannel*
6.2.4. Angriffe auf Schicht 2

6.3. VLAN´s
6.3.1. Bedeutung von VLANs
6.3.2. Schwachstellen in VLANs
6.3.3. Häufige Angriffe auf VLANs
6.3.4. Abhilfemaßnahmen

6.4. *Routing*
6.4.1. IP-Adressierung - IPv4 und IPv6
6.4.2. Routing: Wichtige Konzepte
6.4.3. Statisches Routing
6.4.4. Dynamisches Routing: Einführung

6.5. IGP-Protokolle
6.5.1. RIP
6.5.2. OSPF
6.5.3. RIP vs OSPF
6.5.4. Analyse des Topologiebedarfs

6.6. Perimeter-Schutz
6.6.1. DMZs
6.6.2. *Firewalls*
6.6.3. Gemeinsame Architekturen
6.6.4. *Zero Trust Network Access*

6.7. IDS und IPS
6.7.1. Merkmale
6.7.2. Implementierung
6.7.3. SIEM und SIEM CLOUDS
6.7.4. Auf *HoneyPots* basierende Erkennung

6.8. TLS und VPNs
6.8.1. SSL/TLS
6.8.2. TLS: Häufige Angriffe
6.8.3. VPNs mit TLS
6.8.4. VPNs mit IPSEC

6.9. Sicherheit für drahtlose Netzwerke
6.9.1. Einführung in drahtlose Netzwerke
6.9.2. Protokolle
6.9.3. Wichtige Elemente
6.9.4. Häufige Angriffe

6.10. Unternehmensnetzwerke und der Umgang mit ihnen
6.10.1. Logische Segmentierung
6.10.2. Physische Segmentierung
6.10.3. Zugangskontrolle
6.10.4. Andere zu berücksichtigende Maßnahmen

Modul 7. Analyse und Entwicklung von *Malware*

7.1. Analyse und Entwicklung von *Malware*
7.1.1. Geschichte und Entwicklung von *Malware*
7.1.2. Klassifizierung und Arten von *Malware*
7.1.3. *Malware*-Scans
7.1.4. Entwicklung von *Malware*

7.2. Vorbereiten der Umgebung
7.2.1. Einrichten von virtuellen Maschinen und *Snapshots*
7.2.2. Tools zum Scannen von *Malware*
7.2.3. Tools zur Entwicklung von *Malware*

7.3. Windows-Grundlagen
7.3.1. PE-Dateiformat (*Portable Executable*)
7.3.2. Prozesse und *Threads*
7.3.3. Dateisystem und Registry
7.3.4. *Windows Defender*

7.4. Grundlegende *Malware*-Techniken
7.4.1. *Shellcode*-Erzeugung
7.4.2. Ausführen von *Shellcode* auf der Festplatte
7.4.3. Festplatte vs. Speicher
7.4.4. Ausführen von *Shellcode* im Speicher

7.5. Zwischengeschaltete *Malware*-Techniken
7.5.1. Windows-Persistenz
7.5.2. Startup-Ordner
7.5.3. Registrierungsschlüssel
7.5.4. Bildschirmschoner

7.6. Erweiterte *Malware*-Techniken
7.6.1. *Shellcode*-Verschlüsselung (XOR)
7.6.2. *Shellcode*-Verschlüsselung (RSA)
7.6.3. *String*-Verschleierung
7.6.4. Prozess-Injektion

7.7. Statische *Malware*-Analyse
7.7.1. Analyse von *Packers* mit DIE (*Detect It Easy*)
7.7.2. Analyse von Sektionen mit PE-Bear
7.7.3. Dekompilieren mit Ghidra

7.8. Dynamische *Malware*-Analyse
7.8.1. Verhaltensbeobachtung mit Process Hacker
7.8.2. Analyse von Aufrufen mit API Monitor
7.8.3. Analyse von Änderungen in der Registrierung mit Regshot
7.8.4. Beobachtung von Netzwerkanfragen mit TCPView

7.9. Scannen in .NET
7.9.1. Einführung in .NET
7.9.2. Dekompilieren mit dnSpy
7.9.3. Fehlersuche mit dnSpy

7.10. Analyse von echter *Malware*
7.10.1. Vorbereiten der Umgebung
7.10.2. Statische Analyse der *Malware*
7.10.3. Dynamische Analyse der *Malware*
7.10.4. Erstellung von YARA-Regeln

Modul 8. Forensische Grundlagen und DFIR

8.1. Digitale Forensik
8.1.1. Geschichte und Entwicklung der Computerforensik
8.1.2. Bedeutung der Computerforensik für die Cybersicherheit
8.1.3. Geschichte und Entwicklung der Computerforensik

8.2. Grundlagen der Computerforensik
8.2.1. Chain of Custody und ihre Anwendung
8.2.2. Arten von digitalen Beweisen
8.2.3. Prozesse zur Beschaffung von Beweisen

8.3. Dateisysteme und Datenstruktur
8.3.1. Die wichtigsten Ablagesysteme
8.3.2. Methoden zum Verstecken von Daten
8.3.3. Analyse von Datei-Metadaten und Attributen

8.4. Analyse von Betriebssystemen
8.4.1. Forensische Analyse von Windows-Systemen
8.4.2. Forensische Analyse von Linux-Systemen
8.4.3. Forensische Analyse von macOS-Systemen

8.5. Datenwiederherstellung und Festplattenanalyse
8.5.1. Datenrettung von beschädigten Datenträgern
8.5.2. Tools zur Festplattenanalyse
8.5.3. Interpretation von Dateizuordnungstabellen

8.6. Netzwerk- und Verkehrsanalyse
8.6.1. Erfassen und Analysieren von Netzwerkpaketen
8.6.2. Analyse der *Firewall*-Protokolle
8.6.3. Erkennung von Netzwerkeinbrüchen

8.7. Analyse von *Malware* und bösartigem Code
8.7.1. Klassifizierung von *Malware* und ihre Merkmale
8.7.2. Statische und dynamische Analyse von *Malware*
8.7.3. Disassemblierung und Fehlersuchtechniken

8.8. Protokoll- und Ereignisanalyse
8.8.1. Arten von Protokollen in Systemen und Anwendungen
8.8.2. Interpretation relevanter Ereignisse
8.8.3. Tools zur Protokollanalyse

8.9. Reagieren auf Sicherheitsvorfälle
8.9.1. Prozess der Reaktion auf Vorfälle
8.9.2. Erstellung eines Plans zur Reaktion auf Vorfälle
8.9.3. Koordinierung mit Sicherheitsteams

8.10. Vorlage von Beweisen und Rechtliches
8.10.1. Regeln für digitale Beweise im juristischen Bereich
8.10.2. Erstellung von forensischen Berichten
8.10.3. Erscheinen vor Gericht als Sachverständiger

Modul 9. Fortgeschrittene *Red-Team*-Übungen

9.1. Fortgeschrittene Erkennungstechniken
9.1.1. Fortgeschrittene Aufzählung von Subdomains
9.1.2. Fortgeschrittenes *Google Dorking*
9.1.3. Soziale Netzwerke und theHarvester

9.2. Fortgeschrittene *Phishing*-Kampagnen
9.2.1. Was ist *Reverse-Proxy-Phishing*?
9.2.2. *2FA Bypass* mit Evilginx
9.2.3. Exfiltration von Daten

9.3. Fortgeschrittene Persistenztechniken
9.3.1. *Golden Tickets*
9.3.2. *Silver Tickets*
9.3.3. *DCShadow*-Technik

9.4. Fortgeschrittene Ausweichtechniken
9.4.1. AMSI-Umgehung
9.4.2. Modifizierung bestehender Tools
9.4.3. *Powershell*-Verschleierung

9.5. Fortgeschrittene Lateral-Movement-Techniken
9.5.1. *Pass-the-Ticket* (PtT)
9.5.2. *Overpass-the-Hash* (Pass-the-Key)
9.5.3. NTLM Relay

9.6. Fortgeschrittene Post-Exploitation-Techniken
9.6.1. *Dump* von LSASS
9.6.2. *Dump* von SAM
9.6.3. *DCSync*-Angriff

9.7. Erweiterte *Pivoting*-Techniken
9.7.1. Was ist *Pivoting*?
9.7.2. Tunnel mit SSH
9.7.3. *Pivoting* mit Chisel

9.8. Physikalische Eindringlinge
9.8.1. Überwachung und Erkundung
9.8.2. *Tailgating und Piggybacking*
9.8.3. *Lock-Picking*

9.9. *WLAN*-Angriffe
9.9.1. WPA/WPA2 PSK-Angriffe
9.9.2. Rogue AP-Angriffe
9.9.3. WPA2 *Enterprise*-Angriffe

9.10. RFID-Angriffe
9.10.1. Lesen von RFID-Karten
9.10.2. RFID-Kartenmanipulation
9.10.3. Erstellung von geklonten Karten

Modul 10. Technischer Bericht und Executive Report

10.1. Prozess der Berichterstattung
10.1.1. Aufbau eines Berichts
10.1.2. Prozess der Berichterstattung
10.1.3. Wichtige Konzepte
10.1.4. Executive vs. technisch

10.2. Leitfäden
10.2.1. Einführung
10.2.2. Arten von Leitfäden
10.2.3. Nationale Leitfäden
10.2.4. Anwendungsbeispiele

10.3. Methoden
10.3.1. Bewertung
10.3.2. *Pentesting*
10.3.3. Überprüfung der gemeinsamen Methoden
10.3.4. Einführung in nationale Methodologien

10.4. Technischer Ansatz für die Berichtsphase
10.4.1. Die Grenzen von *Pentester* verstehen
10.4.2. Sprachgebrauch und Stichwörter
10.4.3. Präsentation von Informationen
10.4.4. Häufige Fehler

10.5. Executive-Ansatz für die Berichtsphase
10.5.1. Anpassen des Berichts an den Kontext
10.5.2. Sprachgebrauch und Stichwörter
10.5.3. Standardisierung
10.5.4. Häufige Fehler

10.6. OSSTMM
10.6.1. Verstehen der Methodik
10.6.2. Anerkennung
10.6.3. Dokumentation
10.6.4. Erstellen des Berichts

10.7. LINCE
10.7.1. Verstehen der Methodik
10.7.2. Anerkennung
10.7.3. Dokumentation
10.7.4. Erstellen des Berichts

10.8. Meldung von Schwachstellen
10.8.1. Wichtige Konzepte
10.8.2. Quantifizierung des Umfangs
10.8.3. Schwachstellen und Beweise
10.8.4. Häufige Fehler

10.9. Fokussierung des Berichts an den Kunden
10.9.1. Bedeutung von Arbeitstests
10.9.2. Lösungen und Abhilfemaßnahmen
10.9.3. Sensible und relevante Daten
10.9.4. Praktische Beispiele und Fälle

10.10. Berichterstattung über *Retakes*
10.10.1. Wichtige Konzepte
10.10.2. Verstehen von Altdaten
10.10.3. Fehlerprüfung
10.10.4. Hinzufügen von Informationen

07

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"

Die TECH Business School verwendet die Fallstudie, um alle Inhalte zu kontextualisieren.

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"

Dieses Programm bereitet Sie darauf vor, geschäftliche Herausforderungen in einem unsicheren Umfeld zu meistern und Ihr Unternehmen erfolgreich zu machen.

Unser Programm bereitet Sie darauf vor, sich neuen Herausforderungen in einem unsicheren Umfeld zu stellen und in Ihrer Karriere erfolgreich zu sein.

Eine innovative und andersartige Lernmethode

Dieses TECH-Programm ist eine intensive Spezialisierung, die von Grund auf neu geschaffen wurde, um Managern Herausforderungen und Geschäftsentscheidungen auf höchstem Niveau zu bieten, sowohl auf nationaler als auch auf internationaler Ebene. 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 geschäftliche Realität berücksichtigt wird.

> *Sie werden durch gemeinschaftliche Aktivitäten und reale Fälle lernen, komplexe Situationen in realen Geschäftsumgebungen zu lösen"*

Die Fallmethode ist das am weitesten verbreitete Lernsystem an den besten Business Schools 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 werden wir bei der Fallmethode konfrontiert, einer handlungsorientierten Lernmethode. Während des gesamten Programms werden die Studenten mit mehreren realen Fällen konfrontiert. Sie müssen ihr gesamtes Wissen integrieren, recherchieren, argumentieren und ihre Ideen und Entscheidungen verteidigen.

Relearning Methodology

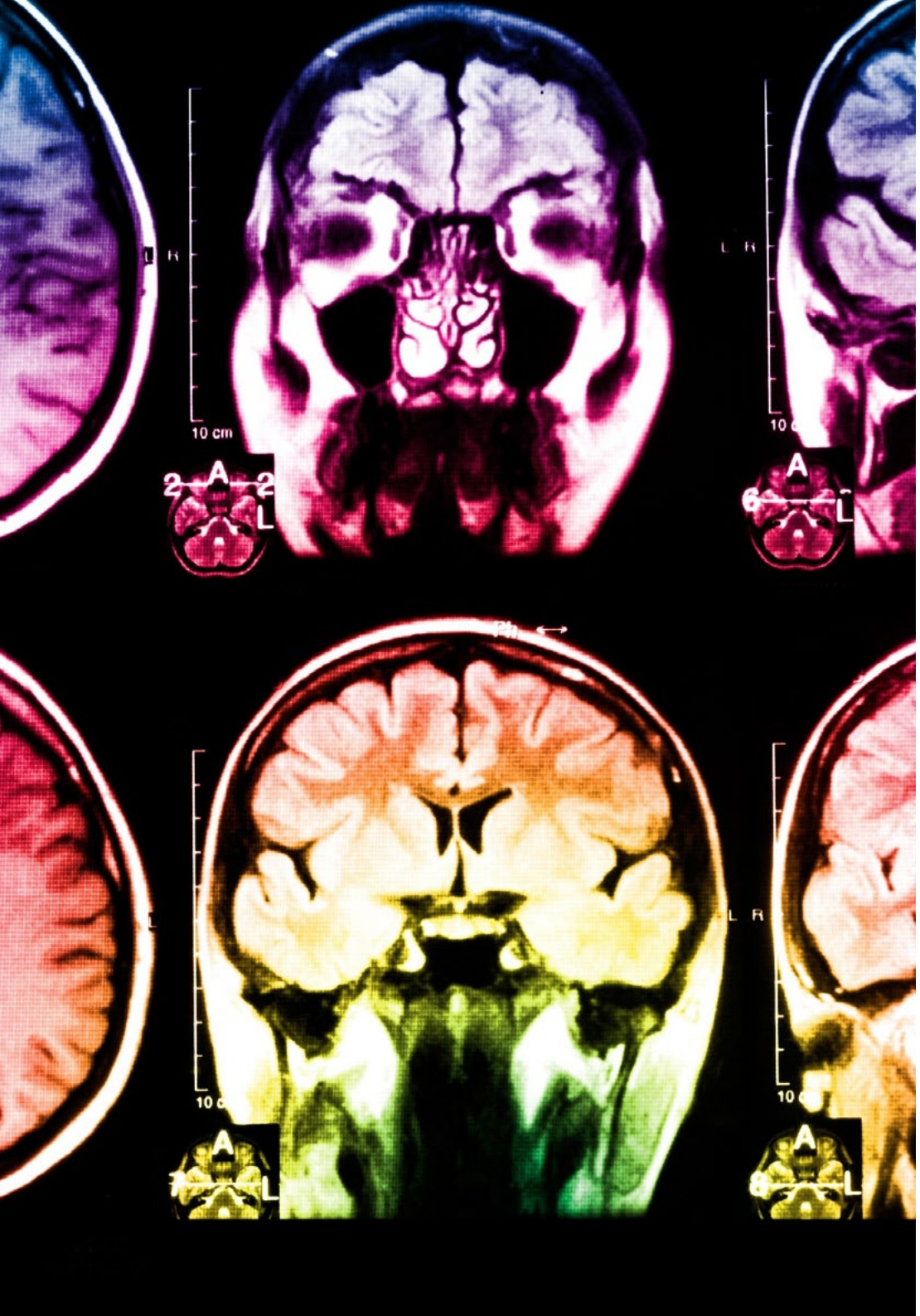
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

Wir ergänzen die Fallstudie mit der besten 100%igen Online-Lehrmethode: Relearning.

Unser Online-System ermöglicht es Ihnen, Ihre Zeit und Ihr Lerntempo zu organisieren und an Ihren Zeitplan anzupassen. Sie können die Inhalte von jedem festen oder mobilen Gerät mit Internetanschluss abrufen.

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 Wirtschaftshochschule ist die einzige spanischsprachige Schule, 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 kombinieren wir jedes dieser Elemente konzentrisch. 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.

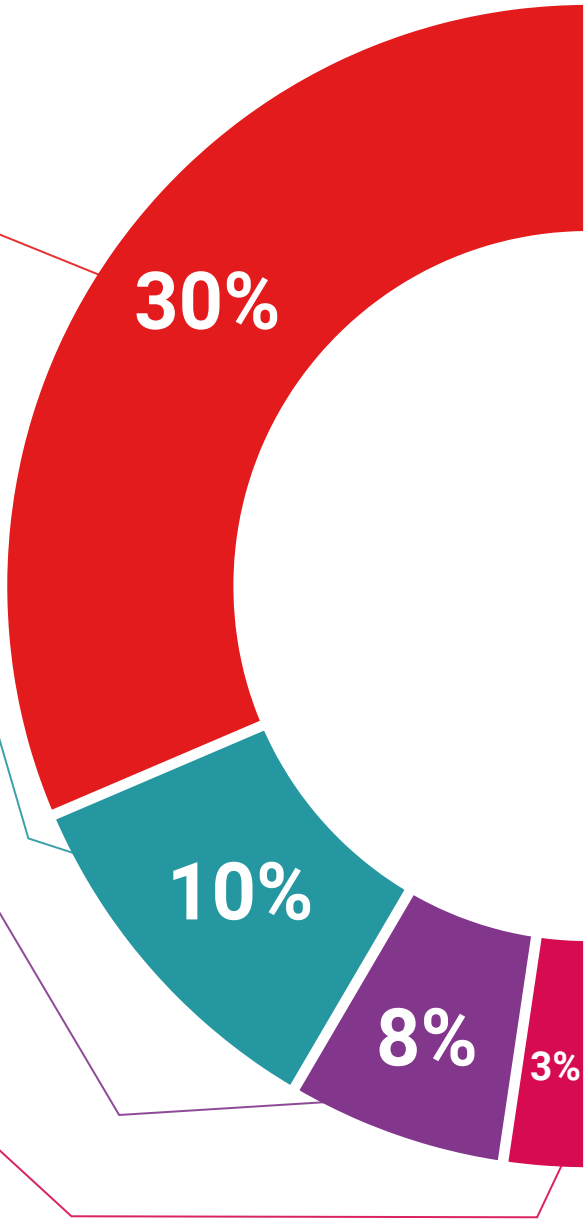
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

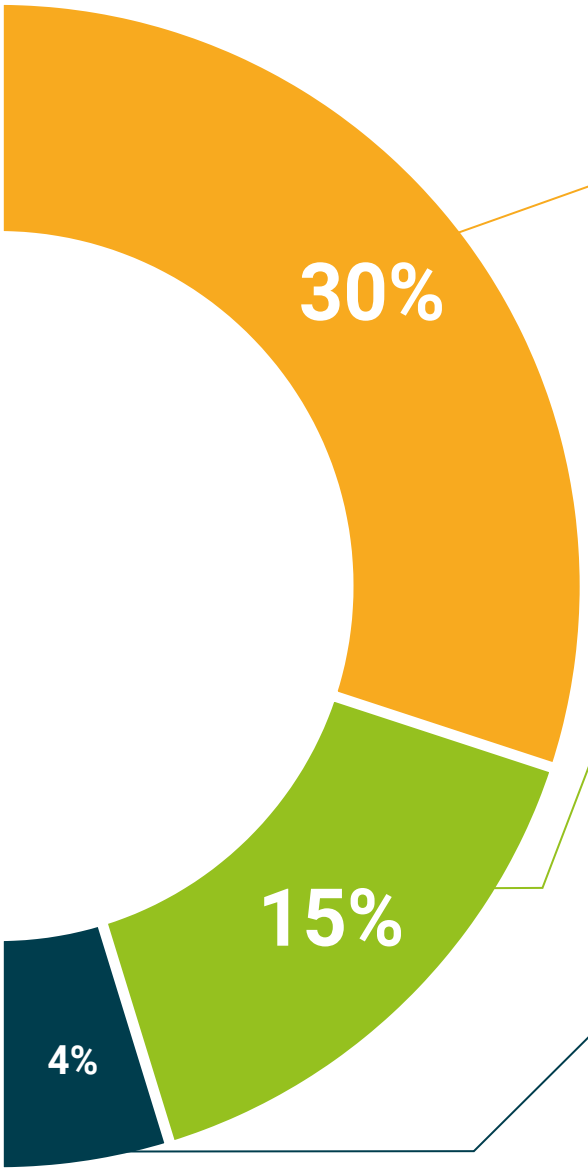
Übungen zu Managementfähigkeiten

Sie werden Aktivitäten durchführen, um spezifische Managementfähigkeiten in jedem Fachbereich zu entwickeln. Übungen und Aktivitäten zum Erwerb und zur Entwicklung der Fähigkeiten und Fertigkeiten, die ein leitender Angestellter 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. Fälle, die von den besten Experten in Senior Management der internationalen Szene präsentiert, analysiert und betreut werden.

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.

08

Profil unserer Studenten

Das Programm richtet sich an Hochschulabsolventen, die zuvor einen der Studiengänge in den Bereichen Sozial- und Rechtswissenschaften, Verwaltung oder Betriebswirtschaft abgeschlossen haben.

Die Vielfalt der Teilnehmer mit unterschiedlichen akademischen Profilen und mehreren Nationalitäten macht den multidisziplinären Ansatz dieses Programms aus.

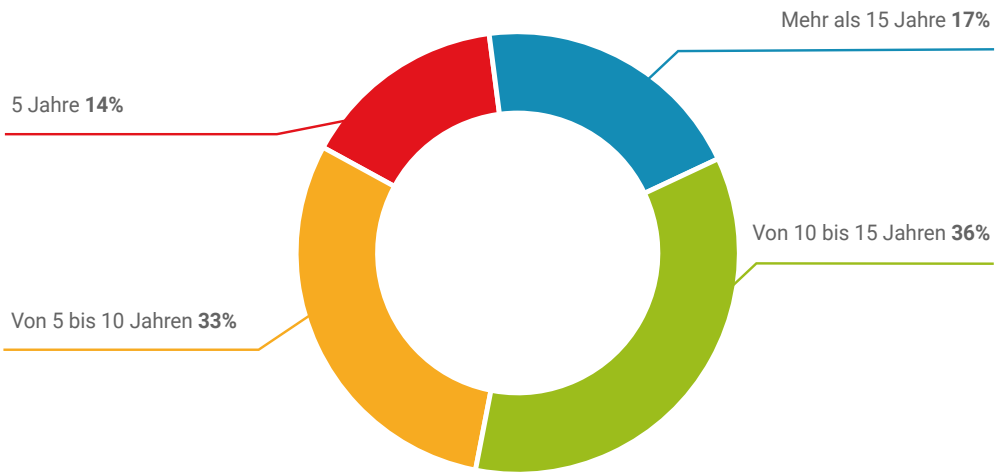
Der Universitätskurs kann auch von Berufstätigen belegt werden, die einen Hochschulabschluss in einem beliebigen Bereich haben und über zwei Jahre Berufserfahrung im IT-Bereich verfügen.

Wenn Sie Erfahrung im Bereich Pentesting und Red Team und haben und nach einer interessanten Verbesserung Ihrer Karriere suchen, während Sie weiterhin arbeiten, ist dies das richtige Programm für Sie“

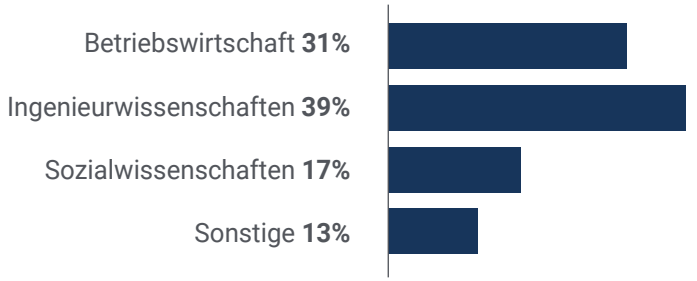
Durchschnittliches Alter

Zwischen **35** und **45** Jahren

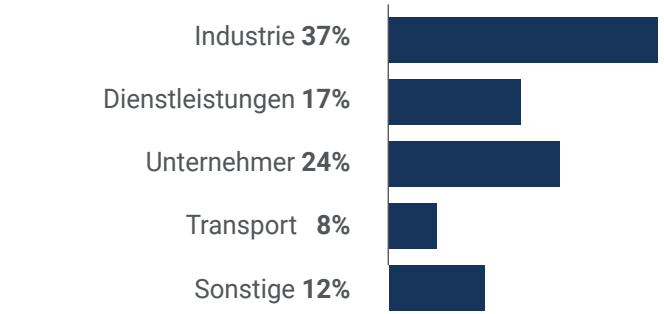
Jahre der Erfahrung



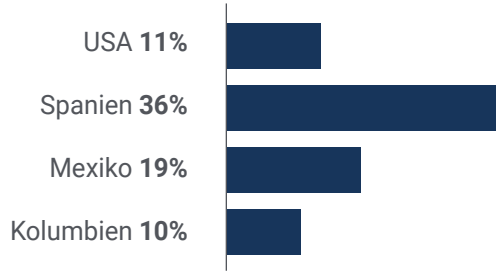
Ausbildung



Akademisches Profil



Geografische Verteilung



Salomón Galvis

Analyst für Informationssicherheit

"Aus diesem Studium möchte ich hervorheben, dass ich mein Verständnis für die Bedeutung regelmäßiger Bewertungen vertiefen konnte und wie wichtig es ist, Cybersicherheit zu messen. Eine großartige Investition, die sich dank der wichtigen Instrumente, die das Dozententeam bei der Entwicklung des Programms einsetzt, in der Zukunft widerspiegeln wird"

09

Kursleitung

Dieser Executive Master verfügt über ein international anerkanntes Dozententeam mit umfangreicher Expertise in den Bereichen Software und Technologien der Informationsgesellschaft sowie Cybersicherheit in der Integration von Unternehmenstechnologien. So spiegelt sich die erstklassige Ausbildung in einem dynamischen und innovativen Ansatz des Lehrplans wider, der die neuesten Trends in der Cybersicherheit umsetzt. Auf diese Weise werden simulierte Fälle und die Analyse realer Situationen kombiniert, um den Studenten eine erstklassige Praxis zu vermitteln, die es ihnen ermöglicht, verschiedene berufliche Herausforderungen am Arbeitsplatz zu meistern.

Große Experten für Pentesting und Red Team werden dieses innovative und fundierte Programm unterrichten"

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. Siles Rubia, Marcelino

- Cibersecurity Engineer
- Ingenieur für Cybersicherheit von der Universität Rey Juan Carlos
- Kenntnisse: Wettbewerbsorientierte Programmierung, *Web-Hacking, Active Directory und Malware Development*
- Gewinner des AdaByron-Wettbewerbs

Hr. González Sanz, Marcos

- Cybersecurity Consultant-Red Teamer Cipherbit bei Grupo Oesía
- Software-Ingenieur von der Polytechnischen Universität von Madrid
- Spezialist für *Cybersecurity Tutor* und *Core Dumped*

Hr. Redondo Castro, Pablo

- Pentester bei Grupo Oesía
- Ingenieur für Cybersicherheit von der Universität Rey Juan Carlos
- Umfangreiche Erfahrung als *Cybersecurity Evaluator Trainee*
- Er sammelt Lehrerfahrung, indem er Fortbildungen im Zusammenhang mit Capture The Flag-Turnieren gibt

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

Hr. Mora Navas, Sergio

- Berater für Cybersicherheit bei Grupo Oesía
- Ingenieur für Cybersicherheit von der Universität Rey Juan Carlos
- Computer-Ingenieur von der Universität von Burgos

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

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

10

Auswirkung auf Ihre Karriere

Dieses Hochschulprogramm wurde mit der Absicht entwickelt, den Studenten das Wissen zu vermitteln, mit dem sie sich jeder Situation im Bereich der Cybersicherheit stellen können. Auf diese Weise konzentriert sich TECH speziell auf die Lehre von höchster Qualität und strebt nach Effizienz in jedem ihrer Abschlüsse. So wird der Fachkraft eine spezialisierte Fortbildung in *Pentesting* und *Red Team* garantiert.

Red Team und andere IT-Aspekte der Cybersicherheit können durch diesen intensiven Abschluss in das Pentesting integriert werden"

Fortgeschrittene Pivotisierungstechniken sind einige der Fähigkeiten, die Sie nach diesem umfassenden 12-monatigen Executive Master beherrschen werden.

Sind Sie bereit, den Sprung zu wagen? Es erwartet Sie eine hervorragende berufliche Weiterentwicklung

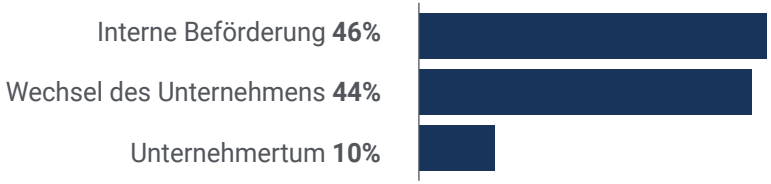
Der Executive Master in Pentesting und Red Team von TECH ist ein intensives Programm, das Sie auf die Herausforderungen und Geschäftsentscheidungen im Bereich der Informatik vorbereitet. Das Hauptziel ist es, Ihre persönliche und berufliche Entwicklung zu fördern. Wir helfen Ihnen, erfolgreich zu sein.

Wenn Sie sich verbessern, eine positive Veränderung auf beruflicher Ebene erreichen und mit den Besten zusammenarbeiten wollen, sind Sie hier genau richtig.

Nutzen Sie diese fundierte und umfassende Möglichkeit, Ihre Pentesting-Kenntnisse mit TECH, der laut Forbes besten Online-Universität der Welt, zu erweitern.

Zeitpunkt des Wandels

Art des Wandels



Gehaltsverbesserung

Der Abschluss dieses Programms bedeutet für unsere Studenten eine Gehaltserhöhung von mehr als **25,55%**

11

Vorteile für Ihr Unternehmen

Dieses Programm trägt dazu bei, die Talente des Unternehmens durch die Weiterbildung von hochrangigen Führungskräften auf ihr maximales Potenzial zu bringen.

Darüber hinaus ist die Teilnahme an dieser Weiterbildung eine einmalige Gelegenheit, ein leistungsfähiges Netzwerk von Kontakten zu knüpfen, um künftige Geschäftspartner, Kunden oder Lieferanten zu finden.

Im digitalen Zeitalter müssen Manager neue Prozesse und Strategien integrieren, die bedeutende Veränderungen und eine organisatorische Entwicklung mit sich bringen. Dies ist nur durch eine universitäre Fort- und Weiterbildung möglich“

Die Entwicklung und Bindung von Talenten in Unternehmen ist die beste langfristige Investition.

01

Wachsendes Talent und intellektuelles Kapital

Die Fachkraft wird neue Konzepte, Strategien und Perspektiven in das Unternehmen einbringen, die relevante Veränderungen bewirken können.

02

Bindung von Führungskräften mit hohem Potenzial und Vermeidung der Abwanderung von Fachkräften

Dieses Programm stärkt die Verbindung zwischen dem Unternehmen und der Fachkraft und eröffnet neue Wege für die berufliche Entwicklung innerhalb des Unternehmens.

03

Aufbau von Akteuren des Wandels

Die Fachkraft wird in der Lage sein, in unsicheren und krisenhaften Zeiten Entscheidungen zu treffen und der Organisation zu helfen, Hindernisse zu überwinden.

04

Verbesserte Möglichkeiten zur internationalen Expansion

Dank dieses Programms wird das Unternehmen mit den wichtigsten Märkten der Weltwirtschaft in Kontakt kommen.

05

Entwicklung eigener Projekte

Die Fachkraft kann an einem realen Projekt arbeiten oder neue Projekte im Bereich FuE oder *Business Development* ihres Unternehmens entwickeln.

06

Gesteigerte Wettbewerbsfähigkeit

Dieses Programm wird die Fachkräfte mit den Fähigkeiten ausstatten, neue Herausforderungen anzunehmen und so das Unternehmen voranzubringen.

12

Qualifizierung

Der Executive Master in Pentesting und Red Team garantiert neben der präzisesten und aktuellsten Fortbildung auch den Zugang zu einem von der TECH Global University ausgestellten Diplom.

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

Mit diesem Programm erwerben Sie den von **TECH Global University**, der größten digitalen Universität der Welt, bestätigten eigenen Titel **Executive Master in Pentesting und Red Team**.

TECH Global University ist eine offizielle europäische Universität, die von der Regierung von Andorra ***(Amtsblatt)*** öffentlich anerkannt ist. Andorra ist seit 2003 Teil des Europäischen Hochschulraums (EHR). Der EHR ist eine von der Europäischen Union geförderte Initiative, die darauf abzielt, den internationalen Ausbildungsrahmen zu organisieren und die Hochschulsysteme der Mitgliedsländer dieses Raums zu vereinheitlichen. Das Projekt fördert gemeinsame Werte, die Einführung gemeinsamer Instrumente und die Stärkung der Mechanismen zur Qualitätssicherung, um die Zusammenarbeit und Mobilität von Studenten, Forschern und Akademikern zu verbessern.

Dieser Abschluss der **TECH Global University** ist ein europäisches Programm zur kontinuierlichen Weiterbildung und beruflichen Fortbildung, das den Erwerb von Kompetenzen in seinem Wissensgebiet garantiert und dem Lebenslauf des Studenten, der das Programm absolviert, einen hohen Mehrwert verleiht.

Título: **Executive Master in Pentesting und Red Team**

Modalität: **online**

Dauer: **12 Monate**

Akkreditierung: **60 ECTS**


tech global university

Hr./Fr. _____, mit der Ausweis-Nr. _____ hat erfolgreich bestanden und den folgenden Abschluss erworben:

Executive Master in Pentesting und Red Team

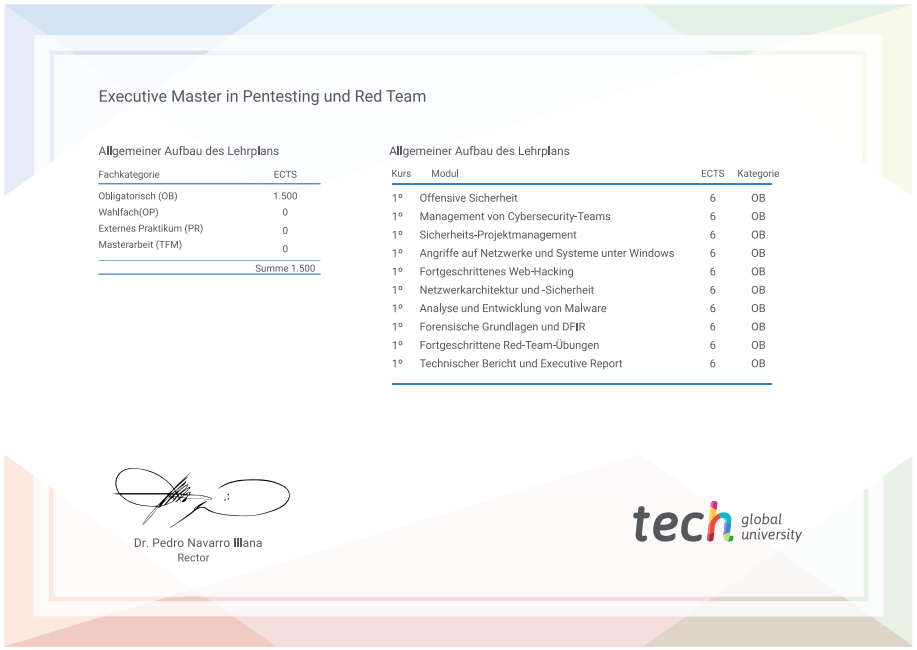
Es handelt sich um einen eigenen Abschluss mit einer Dauer von 1.500 Stunden, was 60 ECTS entspricht, mit Anfangsdatum am dd/mm/aaaa und Enddatum am dd/mm/aaaa.

TECH Global University ist eine von der Regierung Andorras am 31. Januar 2024 offiziell anerkannte Universität, die dem Europäischen Hochschulraum (EHR) angehört.

Andorra la Vella, den 28. Februar 2024

Dr. Pedro Navarro Illana
Rektor

einzigartiger Code TECH: AFWOR23S techtitute.com/titel


Executive Master in Pentesting und Red Team

Allgemeiner Aufbau des Lehrplans

Fachkategorie	ECTS
Obligatorisch (OB)	1.500
Wahlfach(OP)	0
Externes Praktikum (PR)	0
Masterarbeit (TFM)	0
	Summe 1.500

Allgemeiner Aufbau des Lehrplans

Kurs	Modul	ECTS	Kategorie
1°	Offensive Sicherheit	6	OB
1°	Management von Cybersecurity-Teams	6	OB
1°	Sicherheits-Projektmanagement	6	OB
1°	Angriffe auf Netzwerke und Systeme unter Windows	6	OB
1°	Fortgeschrittenes Web-Hacking	6	OB
1°	Netzwerkarchitektur und -Sicherheit	6	OB
1°	Analyse und Entwicklung von Malware	6	OB
1°	Forensische Grundlagen und DFIR	6	OB
1°	Fortgeschrittene Red-Team-Übungen	6	OB
1°	Technischer Bericht und Executive Report	6	OB

Dr. Pedro Navarro Illana
Rector

tech global university

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

tech global university

Executive Master
Pentesting und Red Team

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Global University**
- Akkreditierung: **60 ECTS**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Executive Master
Pentesting und Red Team

tech global university