Privater Masterstudiengang
Pentesting und Red Team

tech technologische universität

tech technologische universität

Privater Masterstudiengang
Pentesting und Red Team

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

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

Index

01
Präsentation
Seite 4

02
Ziele
Seite 8

03
Kompetenzen
Seite 16

04
Kursleitung
Seite 20

05
Struktur und Inhalt
Seite 24

06
Methodik
Seite 34

07
Qualifizierung
Seite 42

01

Präsentation

Die Anzahl und Raffinesse von Cyberangriffen hat alarmierende Ausmaße angenommen. Angesichts der exponentiellen Zunahme der Bedrohungen, von *Ransomware*-Angriffen bis hin zu fortgeschrittenen Eindringlingen, ist der Bedarf an hochqualifizierten Cybersicherheitsexperten von entscheidender Bedeutung. Vor diesem Hintergrund bietet dieses Programm nicht nur eine umfassende Einführung in fortschrittliche Sicherheitstechniken, sondern berücksichtigt auch die Realität einer sich ständig weiterentwickelnden digitalen Umgebung. Auf diese Weise können die Studenten ihr Verständnis von Angriffs- und Verteidigungstechniken vertiefen und sich den anspruchsvollsten Sicherheitsherausforderungen stellen. Angetrieben von der Notwendigkeit, die Cyberverteidigung zu stärken, zeichnet sich dieser Studiengang durch seine 100%ige Online-Methodik und den effektiven Einsatz der *Relearning*-Methode zur Optimierung des Lernens aus.

Dank dieses bahnbrechenden Programms werden Sie unangreifbare Sicherheitsprotokolle mit der Garantie von TECH entwickeln"

Sich auf dem Laufenden zu halten ist unerlässlich, um sich gegen aktuelle und neue Bedrohungen wirksam zur Wehr setzen zu können. Die rasche Entwicklung von Technologien und Cyber-Taktiken macht eine ständige Aktualisierung unabdingbar. Die Ausbreitung der Bedrohungen unterstreicht die Dringlichkeit gut qualifizierter Fachleute.

In diesem Zusammenhang ist dieser Studiengang eine unverzichtbare Antwort, da er nicht nur ein tiefes Verständnis der fortschrittlichsten Techniken im Bereich der Cybersicherheit vermittelt, sondern auch sicherstellt, dass die Fachleute an der Spitze der neuesten Trends und Technologien stehen.

Der Lehrplan des Privaten Masterstudiengangs in Pentesting und Red Team wird die Studenten umfassend mit den Anforderungen der Cybersicherheit vertraut machen. Sie werden effektive Sicherheitsmaßnahmen in Netzwerken implementieren, einschließlich Firewalls, Intrusion Detection Systems (IDS) und Netzwerksegmentierung. Zu diesem Zweck wenden sie digitale forensische Untersuchungsmethoden an, um Fälle von der Identifizierung bis zur Dokumentation der Ergebnisse zu lösen.

Darüber hinaus entwickeln sie Fähigkeiten zur Simulation fortgeschrittener Bedrohungen, indem sie die von böswilligen Akteuren am häufigsten verwendeten Taktiken, Techniken und Verfahren nachbilden. Darüber hinaus gewährleistet der innovative Ansatz von TECH den Erwerb von Fähigkeiten, die im Arbeitsumfeld der Cybersicherheit anwendbar und wertvoll sind.

Die Methodik des akademischen Pfades unterstreicht den innovativen Charakter des Programms, da es eine 100%ige Online-Bildungsumgebung bietet. Das Programm ist auf die Bedürfnisse von vielbeschäftigten Fachleuten zugeschnitten, die ihre Karriere vorantreiben möchten. Es wird auch die Methode des *Relearning* anwenden, die auf der Wiederholung von zentralen Konzepten basiert, um das Wissen zu festigen und das Lernen zu erleichtern. Die Kombination aus Flexibilität und einem soliden didaktischen Ansatz macht das Programm nicht nur zugänglich, sondern bereitet IT-Fachkräfte auch sehr effektiv auf die dynamischen Herausforderungen der Cybersicherheit vor.

Dieser **Privater Masterstudiengang in Pentesting und Red Team** enthält das vollständigste und aktuellste Bildungsprogramm auf dem Markt. Seine herausragendsten Eigenschaften sind:

- Die Entwicklung praktischer Fälle, die von Experten in Pentesting und Red Team vorgestellt werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren Informationen
- Praktische Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens genutzt werden kann
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden
- Theoretische Vorträge, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- Die Verfügbarkeit des Zugriffs auf die Inhalte von jedem festen oder tragbaren Gerät mit Internetanschluss

In nur 12 Monaten geben Sie Ihrer Karriere den nötigen Schub. Schreiben Sie sich jetzt ein und erleben Sie sofortige Fortschritte!"

Wollen Sie einen Qualitätssprung in Ihrer Karriere erleben? Mit TECH werden Sie in der Umsetzung von Strategien für die effektive Durchführung von Cybersicherheitsprojekten weitergebildet"

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.

Dank der laut Forbes besten digitalen Universität der Welt werden Sie die Identifizierung und Bewertung von Schwachstellen in Webanwendungen gründlich erlernen.

Sie werden forensische Techniken in Pentesting-Umgebungen beherrschen. Positionieren Sie sich als der Cybersecurity-Experte, nach dem alle Unternehmen suchen!

02

Ziele

Das Hauptziel dieses akademischen Weges ist die Weiterbildung von Studenten in Penetrationstests und Red-Team-Simulationen. Während des gesamten Programms werden die Informatiker in einen praktischen und spezialisierten Ansatz eintauchen und Fähigkeiten entwickeln, um mit der Identifizierung und Ausnutzung von Schwachstellen in Systemen und Netzwerken umzugehen. Darüber hinaus soll dieser Lehrplan ein tiefgreifendes Verständnis für Taktiken und Strategien der Cybersicherheit vermitteln und die Studenten darauf vorbereiten, reale Herausforderungen zu meistern und bei der effektiven Umsetzung von Cybersicherheitsmaßnahmen führend zu sein.

Sie werden sich eingehend mit der Analyse und Entwicklung von Malware beschäftigen, um sich als führender Experte zu positionieren. 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
- Aufrechterhalten der Aktualität 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. Offensive Sicherheit

- Vertrautmachen des Studenten mit den 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 des theoretischen Wissens in praktischen Szenarien und Simulationen, wobei Sie sich realen Herausforderungen stellen, um Ihre Pentesting-Fähigkeiten zu verbessern
- 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. Management von Cybersecurity-Teams

- Entwickeln von Führungsqualitäten speziell für Cybersecurity-Teams, einschließlich der Fähigkeit, zu motivieren, zu inspirieren und die Bemühungen zu koordinieren, um gemeinsame Ziele zu erreichen
- Lernen, wie man Ressourcen innerhalb eines Cybersecurity-Teams effizient zuweist, wobei die individuellen Fähigkeiten berücksichtigt und die Projektproduktivität maximiert werden
- Verbessern der Kommunikationsfähigkeiten in einem technischen Umfeld, um das Verständnis und die Koordination zwischen den Teammitgliedern zu erleichtern
- Lernen von Strategien zur Erkennung und Bewältigung von Konflikten innerhalb des Cybersecurity-Teams, um eine kooperative und effiziente Arbeitsumgebung zu fördern

- Lernen, Metriken und Bewertungssysteme einzurichten, um die Leistung des Cybersecurity-Teams zu messen und bei Bedarf Anpassungen vorzunehmen
- Fördern der Integration ethischer Praktiken in das Management von Cybersecurity-Teams, um sicherzustellen, dass alle Aktivitäten auf ethische und rechtmäßige Weise durchgeführt werden
- Entwickeln von Kompetenzen für die Vorbereitung und das effiziente Management von Cybersicherheitsvorfällen, um eine schnelle und effektive Reaktion auf Bedrohungen zu gewährleisten

Modul 3. Sicherheits-Projektmanagement

- Entwickeln von Fähigkeiten zur Planung von Cybersicherheitsprojekten, zur Definition von Zielen, Umfang, Ressourcen und Zeitplänen für die Umsetzung
- Erlernen von Strategien für die effektive Durchführung von Sicherheitsprojekten, um die erfolgreiche Umsetzung geplanter Maßnahmen zu gewährleisten
- Entwickeln von Fähigkeiten zur effizienten Verwaltung von Budgets und Ressourcenzuweisung in Sicherheitsprojekten, um die Effektivität zu maximieren und die Kosten zu minimieren
- Verbessern der effektiven Kommunikation mit den *Stakeholders*, indem Berichte und Aktualisierungen auf klare und verständliche Weise präsentiert werden
- Erlernen von Techniken zur Überwachung und Steuerung von Projekten, zur Erkennung von Abweichungen und zur Ergreifung von Korrekturmaßnahmen bei Bedarf
- Vertrautmachen mit agilen Pentesting-Methoden
- Entwickeln von Fähigkeiten zur detaillierten Dokumentation und Berichterstattung, um einen klaren Überblick über den Projektfortschritt und die erzielten Ergebnisse zu erhalten
- Fördern einer effektiven Zusammenarbeit zwischen verschiedenen Teams und Disziplinen innerhalb von Sicherheitsprojekten, um einen ganzheitlichen und koordinierten Ansatz zu gewährleisten
- Erlernen von Strategien zur Bewertung und Messung der Effektivität von implementierten Maßnahmen, um eine kontinuierliche Verbesserung der Sicherheitslage des Unternehmens zu gewährleisten

Modul 4. 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
- Vertrautmachen des Studenten mit 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 5. Fortgeschrittenes Web-*Hacking*

- Entwickeln von Fähigkeiten zur Identifizierung und Bewertung von Schwachstellen in Webanwendungen, einschließlich SQL-Injektionen, Cross-Site Scripting (XSS) und anderen gängigen Angriffsvektoren
- Lernen, wie man Sicherheitstests für moderne Webanwendungen durchführt
- Erwerben von Kompetenzen in fortgeschrittenen Web-Hacking-Techniken, die Strategien zur Umgehung von Sicherheitsmaßnahmen und zur Ausnutzung raffinierter Schwachstellen erforsche
- Vertrautmachen des Studenten mit der Bewertung der Sicherheit von APIs und Webdiensten, Identifizierung potenzieller Schwachstellen und Stärkung der Sicherheit von Programmierschnittstellen
- Entwickeln von Fähigkeiten zur Implementierung effektiver Abhilfemaßnahmen in Webanwendungen, um die Anfälligkeit für Angriffe zu verringern und die Sicherheit zu erhöhen
- Teilnehmen an praktischen Simulationen, um die Sicherheit in komplexen Webumgebungen zu bewerten und das Wissen auf reale Szenarien anzuwenden
- Entwickeln von Kompetenzen bei der Formulierung effektiver Verteidigungsstrategien zum Schutz von Webanwendungen vor Cyber-Bedrohungen
- Lernen, fortgeschrittene Web-*Hacking*-Praktiken mit den relevanten Sicherheitsvorschriften und -standards in Einklang zu bringen, um die Einhaltung rechtlicher und ethischer Rahmenbedingungen zu gewährleisten
- Fördern einer effektiven Zusammenarbeit zwischen Entwicklungs- und Sicherheitsteams

Modul 6. Netzwerkarchitektur und Sicherheit

- Erwerben fortgeschrittener Kenntnisse der Netzwerkarchitektur, einschließlich Topologien, Protokollen und wichtigen Komponenten
- Entwickeln von Fähigkeiten zur Identifizierung und Bewertung spezifischer Schwachstellen in Netzwerkinfrastrukturen, unter Berücksichtigung
- Lernen, wie man effektive Netzwerksicherheitsmaßnahmen implementiert, einschließlich *Firewalls*, Intrusion Detection Systems (IDS) und Netzwerksegmentierung
- Vertrautmachen mit neuen Netzwerktechnologien wie Software-defined Networking (SDN) und Verstehen ihrer Auswirkungen auf die Sicherheit
- Entwickeln von Fähigkeiten zur Sicherung der Netzwerkkommunikation, einschließlich des Schutzes vor Bedrohungen wie *Sniffing* und *Man-in-the-Middle*-Angriffen
- Lernen, wie man Sicherheitskonfigurationen in Unternehmensnetzwerken bewertet und verbessert, um einen angemessenen Schutz zu gewährleisten
- Entwickeln von Fähigkeiten zur Implementierung effektiver Maßnahmen zur Abwehr von Bedrohungen in Unternehmensnetzwerken, von internen Angriffen bis hin zu externen Bedrohungen
- Fördern der effektiven Zusammenarbeit mit Sicherheitsteams, um Strategien und Bemühungen zum Schutz der Netzwerkinfrastruktur zu integrieren
- Fördern ethischer und rechtlicher Praktiken bei der Implementierung von Netzwerksicherheitsmaßnahmen und gewährleisten die Einhaltung ethischer Grundsätze bei allen Aktivitäten

Modul 7. 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
- Vertrautmachen mit 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 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 8. 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
- Vertrautmachen mit fortgeschrittenen 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
- Vertrautmachen mit 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 (IR)-Teams, um die Koordination bei der Untersuchung und Eindämmung von Bedrohungen zu optimieren
- Fördern ethischer und rechtlicher Praktiken bei der Untersuchung digitaler Forensik und gewährleisten die Einhaltung von Cybersicherheitsvorschriften und Verhaltensstandards

Modul 9. Erweiterte 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
- Vertrautmachen des Studenten mit 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
- Vertrautmachen mit 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 die Einhaltung von Cybersicherheitsvorschriften und ethischen Standards

Modul 10. Technische und ausführende Berichterstattung

- Entwickeln von Fähigkeiten zur Erstellung detaillierter technischer Berichte, in denen Ergebnisse, verwendete Methoden und Empfehlungen klar und umfassend dargestellt werden
- Lernen, effektiv mit technischen Zielgruppen zu kommunizieren und dabei eine präzise und angemessene Sprache zu verwenden, um komplexe technische Informationen zu vermitteln
- Entwickeln von Fähigkeiten, um umsetzbare und praktische Empfehlungen zu formulieren, die darauf abzielen, Schwachstellen zu entschärfen und die Sicherheitslage zu verbessern
- Lernen, die potenziellen Auswirkungen identifizierter Schwachstellen unter Berücksichtigung technischer, betrieblicher und strategischer Aspekte zu bewerten
- Vertrautmachen mit Best Practices für die Berichterstattung an Führungskräfte, um technische Informationen für ein nicht technisches Publikum aufzubereiten
- Entwickeln von Kompetenzen, um Ergebnisse und Empfehlungen mit den strategischen und operativen Zielen des Unternehmens in Einklang zu bringen
- Lernen, wie man Datenvisualisierungstools verwendet, um die in Berichten enthaltenen Informationen grafisch darzustellen und so das Verständnis zu erleichtern
- Fördern der Aufnahme relevanter Informationen über die Einhaltung von Vorschriften und Standards in Berichte, um die Einhaltung rechtlicher Anforderungen zu gewährleisten
- Fördern der effektiven Zusammenarbeit zwischen technischen und leitenden Teams, um Verständnis und Unterstützung für die im Bericht vorgeschlagenen Verbesserungsmaßnahmen sicherzustellen

03

Kompetenzen

Dank dieses Lehrplans werden die Studenten mit speziellen Fähigkeiten für die Umsetzung aktiver Verteidigungsmaßnahmen qualifiziert, die die Sicherheit von Systemen und Netzwerken auf der Grundlage von Best Practices im Bereich der Cybersicherheit stärken. Darüber hinaus erwerben die Studenten fortgeschrittene Kompetenzen in Penetrationstests und Red-Team-Simulationen und zeichnen sich durch eine proaktive Identifizierung und Eindämmung von Schwachstellen aus. Fachleute werden die technischen Fähigkeiten erwerben, die für den Umgang mit realen Bedrohungen erforderlich sind, und werden so darauf vorbereitet, in dynamischen Cyber-Umgebungen wirksame Strategien zur Bewertung und Stärkung der Sicherheit zu entwickeln. Darüber hinaus macht der 100%ige Online-Ansatz das Studium flexibel.

Werden Sie durch 1.500 Stunden der besten Multimedia-Inhalte mit dem Gütesiegel der TECH zu einem Experten für Cybersicherheit"

Allgemeine Kompetenzen

- Erwerben von Fähigkeiten in der Planung, Durchführung und Verwaltung von Cybersicherheitsprojekten, um effektive Ergebnisse und die Einhaltung von Zielen zu gewährleisten
- Erwerben fortgeschrittener Kenntnisse der Netzwerkarchitektur und ihrer Sicherheitsaspekte, Bewertung von Schwachstellen und Anwendung von Strategien zur Stärkung der Infrastruktur
- Entwickeln von Kompetenzen in der digitalen Forensik und der Reaktion auf Vorfälle, von der Sammlung von Beweisen bis zur Eindämmung von Bedrohungen und der Wiederherstellung des Betriebs
- Anwenden fortschrittlicher Taktiken bei der Planung und Durchführung von Red-Team-Übungen, bei denen reale Szenarien simuliert werden, um die Widerstandsfähigkeit der Infrastruktur zu bewerten, Schwachstellen zu erkennen und die Vorbereitung auf Cyber-Bedrohungen zu verbessern

Verbessern Sie Ihre Fähigkeiten im Prozess der Identifizierung, Bewertung und Abschwächung von Risiken, die für Cybersicherheitsprojekte spezifisch sind. Setzen Sie auf TECH!"

Spezifische Kompetenzen

- Erwerben von Coaching-Fähigkeiten für die berufliche Entwicklung von Teammitgliedern, um deren Wachstum und Verbesserung zu fördern
- Entwickeln strategischer Entscheidungsfähigkeiten in Cybersicherheitssituationen unter Berücksichtigung der kurz- und langfristigen Auswirkungen auf die organisatorische Sicherheit
- Erwerben von Kompetenzen zur Identifizierung, Bewertung und Abschwächung von Risiken, die für Cybersicherheitsprojekte spezifisch sind
- Entwickeln von Fähigkeiten zur Implementierung aktiver Verteidigungsmaßnahmen, die System- und Netzwerksicherheit stärken
- Erlernen von Techniken zur Analyse des Internetverkehrs, um Muster und anomales Verhalten zu identifizieren und so mögliche Bedrohungen zu erkennen
- Erwerben von Kompetenzen in der forensischen Analyse von Netzwerkumgebungen, die eine effektive Identifizierung von und Reaktion auf Cyber-Vorfälle ermöglichen
- Erlernen von Strategien zur effektiven Erkennung und Vorbeugung von Malware, einschließlich des Einsatzes von fortschrittlichen Sicherheitslösungen
- 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
- Erwerben von Fähigkeiten zur strategischen Planung von Red Team Übungen unter Berücksichtigung von Zielen, Umfang, Ressourcen und realistischen Szenarien
- Erwerben von Fähigkeiten zur Identifizierung und Priorisierung von Schwachstellen, Hervorheben derjenigen, die das größte Sicherheitsrisiko darstellen

04

Kursleitung

Für die Zusammenstellung des Dozententeams des privaten Masterstudiengangs in Pentesting und Red Team hat TECH die besten Spezialisten zusammengebracht, die über einen umfangreichen und anerkannten beruflichen Hintergrund in führenden Unternehmen der Branche verfügen. In diesem Sinne wird jedes Mitglied des Dozententeams seine praktische Erfahrung und sein Fachwissen einbringen, um sicherzustellen, dass die Studenten von der Lehre hochqualifizierter Fachleute profitieren. Darüber hinaus gewährleistet die sorgfältige Auswahl dieser Experten nicht nur die akademische Qualität, sondern auch die unmittelbare Relevanz und Anwendbarkeit der Inhalte in der dynamischen Cybersicherheitsumgebung.

Giganten der Cybersicherheitsbranche werden Sie mit diesem einzigartigen Universitätsprogramm von TECH in nur 12 Monaten zum Erfolg katapultieren"

Leitung

Hr. Gómez Pintado, Carlos

- Manager für Cybersicherheit und das Netzwerkteam Cipherbit bei Grupo Oesía
- Manager Advisor & Investor bei Wesson App
- Hochschulabschluss in Software Engineering und Technologien der Informationsgesellschaft an der Polytechnischen Universität von Madrid
- Arbeitet mit Bildungseinrichtungen bei der Vorbereitung von Ausbildungszyklen auf höherer Ebene im Bereich Cybersicherheit zusammen

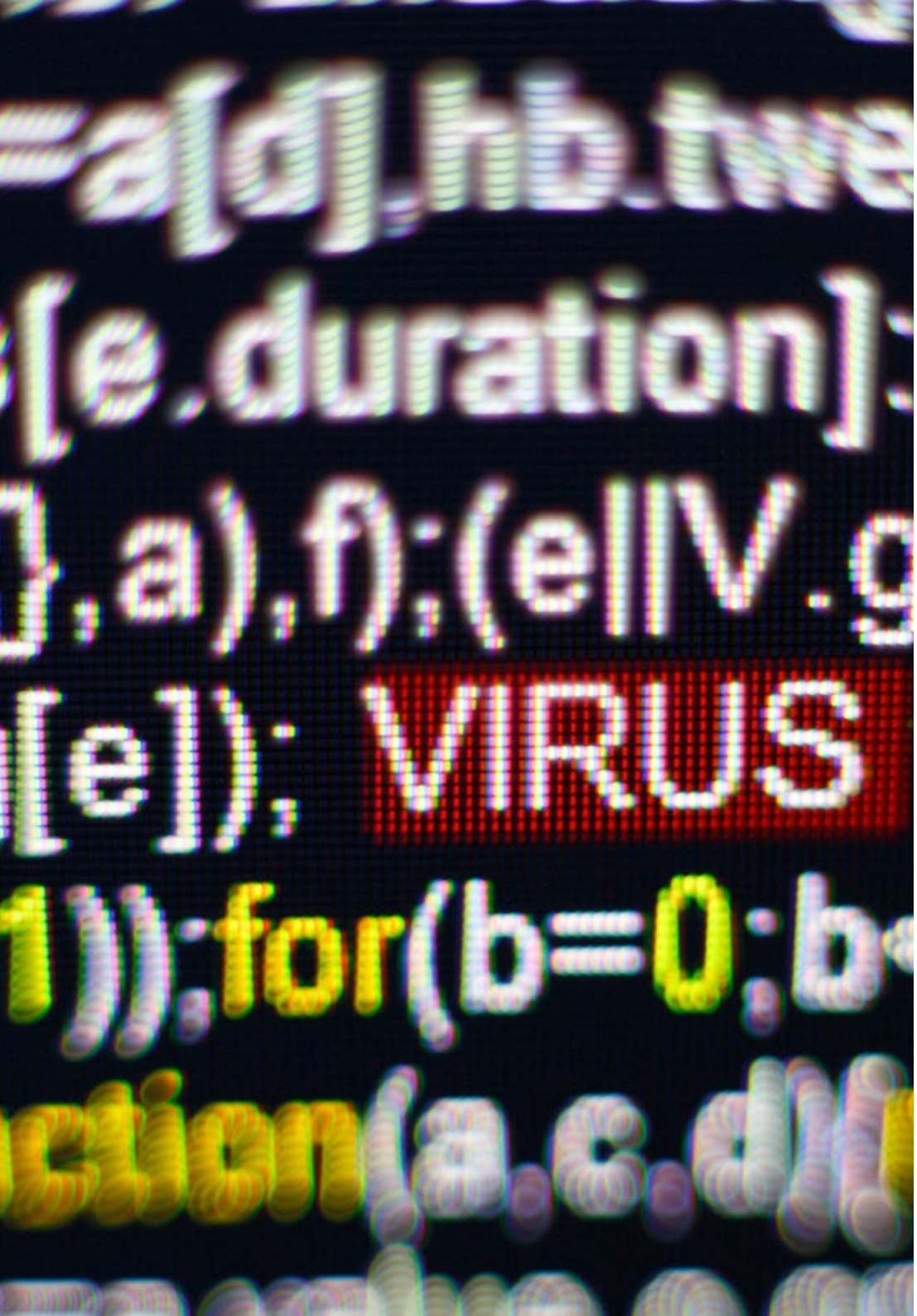
Professoren

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. 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

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

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. Mora Navas, Sergio

- Berater für Cybersicherheit bei der Oesía-Gruppe
- 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

05

Struktur und Inhalt

Dieses Universitätsprogramm bietet ein vollständiges Eintauchen in die entscheidenden Disziplinen der Penetrationstests und Red Team-Simulationen. Während des gesamten Lehrplans werden die Studenten erweiterte Fähigkeiten entwickeln, um Schwachstellen in Systemen und Netzwerken zu identifizieren und auszunutzen, indem sie moderne Techniken und Tools verwenden. Dieser praxisorientierte Studiengang rüstet Cybersecurity-Experten für die Herausforderungen der realen Welt. So profitieren die Studenten von einer einzigartigen Kombination aus Theorie und Praxis, die von Branchenexperten geleitet wird, um ihr Verständnis zu stärken und Sicherheitsbewertungsstrategien in Cyber-Umgebungen effektiv anzuwenden.

Sie werden sich mit den verschiedenen Rollen und Verantwortlichkeiten des Cybersecurity-Teams auseinandersetzen. Schreiben Sie sich jetzt ein!"

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. Zentrale Konzepte 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. OSINT-Grundlagen
- 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 der Wirtschaftsführung
- 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. Tools 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. *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. Eigenschaften
- 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 in drahtlosen Netzwerken
- 6.9.1. Einführung in drahtlose Netzwerke
- 6.9.2. Protokolle
- 6.9.3. Wichtige Elemente
- 6.9.4. Übliche 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 (*Portable Executable*) Dateiformat
- 7.3.2. Prozesse und *Threads*
- 7.3.3. Dateisystem und Registry
- 7.3.4. *Windows-Verteidiger*

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* con 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. Erweiterte Red Team-Übungen

9.1. Erweiterte Erkennungstechniken
- 9.1.1. Erweiterte Aufzählung von Subdomains
- 9.1.2. Erweitertes *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. Erweiterte 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. Wi-Fi-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. Technische und ausführende Berichterstattung

10.1. Berichtswesen
- 10.1.1. Aufbau eines Berichts
- 10.1.2. Prozess der Berichterstattung
- 10.1.3. Zentrale Konzepte
- 10.1.4. Exekutive vs. Technik

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. Vorgehensweise der Exekutive in der 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. Zentrale 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

06

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

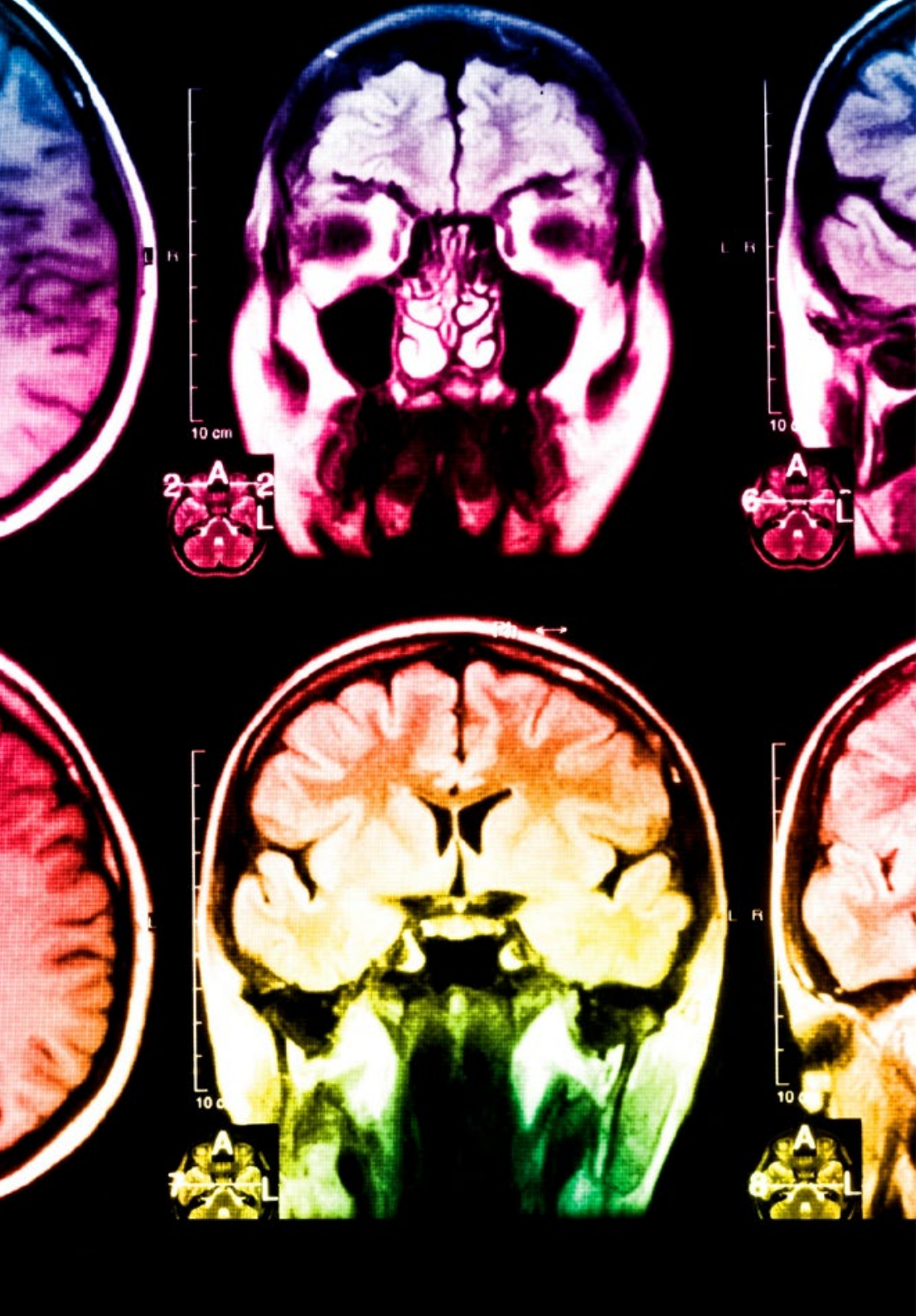
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

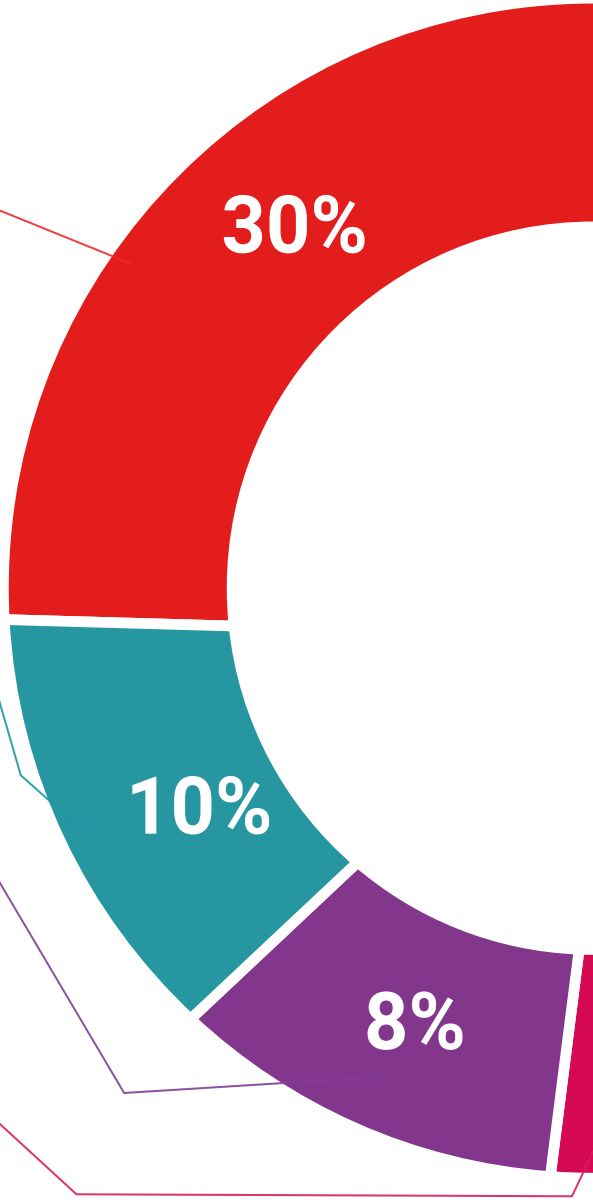
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

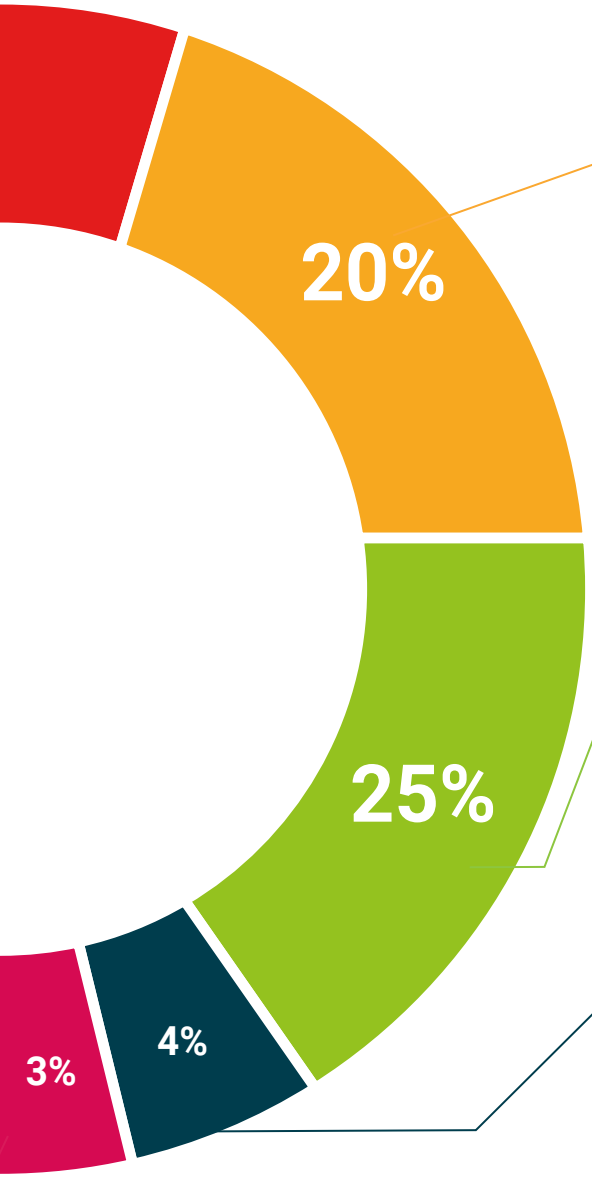
Übungen für Fertigkeiten und Kompetenzen

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.

07

Qualifizierung

Der Privater Masterstudiengang in Pentesting und Red Team garantiert neben der präzisesten und aktuellsten Fortbildung auch den Zugang zu einem von der TECH Technologischen Universität ausgestellten Diplom.

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

Dieser **Privater Masterstudiengang in Pentesting und Red Team** 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: **Privater Masterstudiengang in Pentesting und Red Team**

Anzahl der offiziellen Arbeitsstunden: **1.500 Std.**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

PRIVATER MASTERSTUDIENGANG

in

Pentesting und Red Team

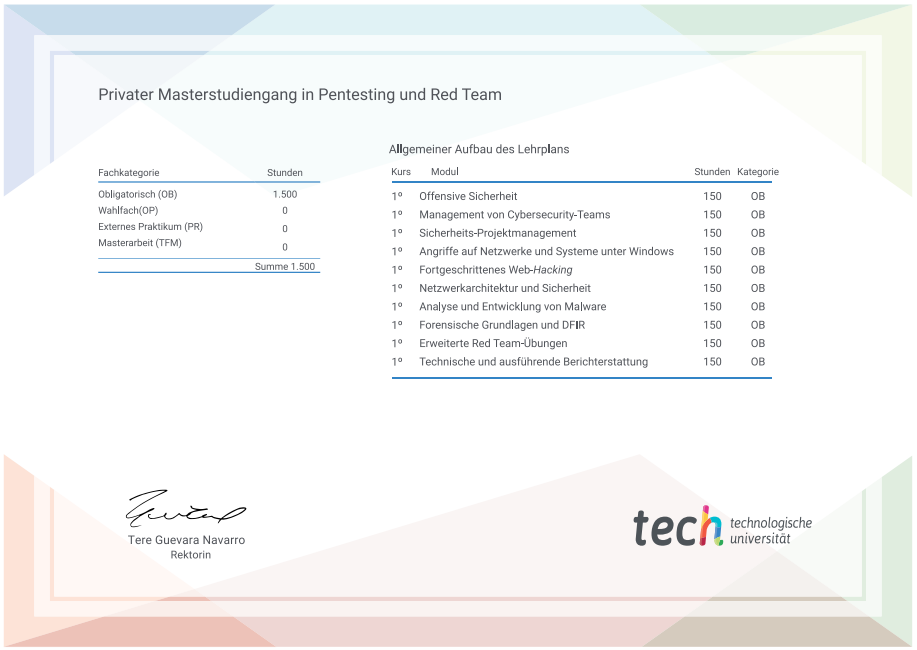
Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 1.500 Stunden, mit Anfangsdatum tt/mm/jjjj und Enddatum tt/mm/jjjj.

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


Privater Masterstudiengang in Pentesting und Red Team

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

Allgemeiner Aufbau des Lehrplans

Kurs	Modul	Stunden	Kategorie
1º	Offensive Sicherheit	150	OB
1º	Management von Cybersecurity-Teams	150	OB
1º	Sicherheits-Projektmanagement	150	OB
1º	Angriffe auf Netzwerke und Systeme unter Windows	150	OB
1º	Fortgeschrittenes Web-*Hacking*	150	OB
1º	Netzwerkarchitektur und Sicherheit	150	OB
1º	Analyse und Entwicklung von Malware	150	OB
1º	Forensische Grundlagen und DFIR	150	OB
1º	Erweiterte Red Team-Übungen	150	OB
1º	Technische und ausführende Berichterstattung	150	OB

Tere Guevara Navarro
Rektorin

tech technologische universität

*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

Privater Masterstudiengang
Pentesting und Red Team

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Privater Masterstudiengang
Pentesting und Red Team

tech technologische universität