Privater Masterstudiengang

Cybersecurity Management (CISO, Chief Information Security Officer)

tech technologische universität

tech technologische universität

Privater Masterstudiengang

Cybersecurity Management (CISO, Chief Information Security Officer)

- 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-cybersecurity-management-ciso-chief-information-security-officer

Index

01

Präsentation

Mit dem technologischen Fortschritt perfektionieren auch die Bedrohungen ihre Angriffstechniken. Mit anderen Worten, die Möglichkeiten und Wege für Cyberkriminelle, ihre Ziele zu erreichen, nehmen zu. In diesem Zusammenhang präsentiert TECH eine Qualifikation, mit der sich Fachleute auf den neuesten Stand bringen können und auf erschöpfende Weise lernen, verschiedene digitale Umgebungen zu schützen und zu sichern. All dies mit Hilfe einer revolutionären Methode, dem Relearning, und in einem bequemen und vollständig online zugänglichen Format, das es dem Studenten ermöglicht, Fähigkeiten und Fertigkeiten ohne einen vorgegebenen Zeitplan zu erwerben. Am Ende dieses Studiums verfügt die Fachkraft über die notwendigen Fähigkeiten und Kompetenzen, um mit großer Effizienz als Chief Information Security Officer zu arbeiten, eine Führungsposition mit großem Prestige sowie mit hohen Wachstums- und Expansionsaussichten.

Mit dem Fortschritt der Technologie und der Konnektivität steigt auch die Anzahl und die Form der potenziellen Bedrohungen. Deshalb ist es für künftige Chief Information Security Officers von entscheidender Bedeutung, ihr Wissen auf den neuesten Stand zu bringen, um Lösungen anbieten zu können, die besser an die Eigenheiten des Unternehmens angepasst sind"

Es ist kein Geheimnis, dass wir uns mitten im Informations- und Kommunikationszeitalter befinden, da wir alle sowohl zu Hause als auch in Unternehmen miteinander verbunden sind. So haben wir mit einem einzigen Klick, mit einer einzigen Suche in einer der uns zur Verfügung stehenden Suchmaschinen Zugang zu einer Vielzahl von Informationen, sei es von einem Smartphone, einem PC oder einem Arbeitscomputer aus. In diesem Zusammenhang gilt: "Zeit ist Geld", aber das gilt auch für Information.

In dem Maße, wie die Technologie für den Durchschnittsbürger und den Angestellten voranschreitet, wachsen auch die Bedrohungen und Angriffstechniken. Je mehr neue Funktionalitäten es gibt und je mehr wir miteinander kommunizieren, desto mehr vergrößert sich die Angriffsfläche. Mit anderen Worten, die Möglichkeiten und Wege für Cyberkriminelle, ihre Ziele zu erreichen, nehmen zu.

Vor diesem besorgniserregenden Hintergrund führt TECH dieses Programm für Cybersecurity Management (CISO, Chief Information Security Officer) ein, das von einem Team mit unterschiedlichen Berufsprofilen in verschiedenen Sektoren entwickelt wurde, das internationale Berufserfahrung in der Privatwirtschaft im Bereich FuEuI und umfangreiche Lehrerfahrung vereint. Daher sind sie nicht nur in jeder der Technologien auf dem neuesten Stand, sondern haben auch eine Perspektive für die zukünftigen Bedürfnisse des Sektors und präsentieren diese auf didaktische Weise.

Das Programm umfasst die verschiedenen Kernfächer im Bereich der Cybersicherheit, die sorgfältig ausgewählt wurden, um ein breites Spektrum von Technologien abzudecken, die in verschiedenen Arbeitsbereichen eingesetzt werden können. Aber es wird auch einen anderen Zweig von Themen abdecken, die normalerweise in den akademischen Katalogen anderer Institutionen selten zu finden sind und die den Studienplan der Fachkräfte zutiefst nähren werden. Auf diese Weise und dank des transversalen Wissens, das TECH mit diesem Programm anbietet, erwirbt der Student die Fähigkeiten, um als Manager im Bereich der Cybersicherheit (Chief Information Security Officer) zu arbeiten und so seine Aussichten auf persönliches und berufliches Wachstum zu verbessern.

Dieser **Privater Masterstudiengang in Cybersecurity Management (CISO, Chief Information Security Officer)** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung praktischer Fälle, die von Experten der Cybersicherheit vorgestellt werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt soll wissenschaftliche und praktische Informationen zu den für die berufliche Praxis wesentlichen Disziplinen vermitteln
- Die praktischen Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens durchgeführt werden kann
- Ein besonderer Schwerpunkt liegt auf innovativen Methoden
- Theoretische Vorträge, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- Die Verfügbarkeit des Zugangs zu Inhalten von jedem festen oder tragbaren Gerät mit Internetanschluss

Bereiten Sie sich auf die Arbeit als Chief Information Security Officer vor, ein Schlüsselprofil im Unternehmen aufgrund seiner Rolle als Schützer und Garant für die IT-Sicherheit"

Heben Sie sich in einem boomenden Sektor ab und werden Sie mit diesem TECH-Programm zu einem Experten für Cybersicherheit. Es ist die vollständigste Spezialisierung auf dem Markt"

Die Art und Weise, wie Menschen Informationen austauschen, entwickelt sich rasant weiter. Dies erfordert neue Formen des Cyberschutzes von Fachleuten.

Ein 100%iges Online-Programm mit einem äußerst praxisnahen Ansatz, der den Grundstein für Ihre berufliche Entwicklung legen wird.

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

Die multimedialen Inhalte, die mit der neuesten Bildungstechnologie entwickelt wurden, werden der Fachkraft ein situiertes und kontextbezogenes Lernen ermöglichen, d.h. eine simulierte Umgebung, die eine immersive Fortbildung bietet, die auf die Ausführung in 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 werden sie von einem innovativen interaktiven Videosystem unterstützt, das von renommierten Experten entwickelt wurde.

02

Ziele

TECH ist sich der Bedeutung der Cybersicherheit für Unternehmen bewusst und hat diesen privaten Masterstudiengang entwickelt, der darauf abzielt, die Kenntnisse von Fachleuten in der Erkennung, dem Schutz und der Prävention von Computerkriminalität zu fördern und zu aktualisieren. Auf diese Weise wird der künftige Student zu einem wichtigen Akteur bei der Pflege von Daten und Informationen und minimiert die Möglichkeit, dass Kriminelle mögliche bestehende Sicherheitslücken ausnutzen. Eine berufliche Kompetenz, die die Fachleute bei TECH in nur 12 Monaten erwerben können.

Dies ist eine einzigartige Gelegenheit, Ihre Träume und Ziele zu verwirklichen und ein Experte für Cybersicherheit zu werden"

Allgemeine Ziele

- Analysieren der Rolle des Cybersecurity-Analysten
- Erforschen des Social Engineering und seiner Methoden
- Untersuchen der Methoden OSINT, HUMINT, OWASP, PTEC, OSSTM, OWISAM
- Durchführen einer Risikoanalyse und Verstehen von Risikokennzahlen
- Bestimmen des angemessenen Einsatzes von Anonymität und der Nutzung von Netzwerken wie TOR, I2P und Freene
- Generieren von Fachwissen zur Durchführung eines Sicherheitsaudits
- Entwickeln geeigneter Nutzungsrichtlinien
- Prüfen von Erkennungs- und Präventionssystemen für wichtige Bedrohungen
- Bewerten von neuen Systemen zur Erkennung von Bedrohungen und deren Weiterentwicklung gegenüber herkömmlichen Lösungen
- Analysieren der wichtigsten aktuellen mobilen Plattformen, ihrer Funktionen und Nutzung
- Identifizieren, Analysieren und Bewerten der Sicherheitsrisiken von IoT-Projektteilen
- Auswerten der erhaltenen Informationen und Entwicklung von Präventions- und *Hacking*-Mechanismen
- Anwenden von Reverse Engineering auf die Cybersicherheitsumgebung
- Spezifizieren der Tests, die mit der entwickelten Software durchgeführt werden sollen
- Sammeln aller vorhandenen Beweise und Daten, um einen forensischen Bericht zu erstellen
- Präsentieren auf die richtige Weise des forensischen Berichts
- Analysieren des aktuellen und zukünftigen Stands der IT-Sicherheit
- Untersuchen der Risiken neu aufkommender Technologien
- Zusammenstellen der verschiedenen Technologien in Bezug auf die Computersicherheit

Spezifische Ziele

Modul 1. Cyberintelligenz und Cybersicherheit

- Entwickeln von Methoden für die Cybersicherheit
- Untersuchen des Informationszyklus und seine Anwendung auf Cyber Intelligence
- Bestimmen der Rolle des Geheimdienstanalysten und der Hindernisse für Evakuierungsmaßnahmen
- Analysieren von OSINT, OWISAM, OSSTM, PTES, OWASP-Methoden
- Ermitteln der gängigsten Tools für die Nachrichtenproduktion
- Durchführen einer Risikoanalyse und Verstehen der verwendeten Metriken
- Festlegen von Anonymisierungsoptionen und Verwendung von Netzwerken wie TOR, I2P, FreeNet
- Beschreiben im Detail der aktuellen Cybersicherheitsvorschriften

Modul 2. Host-Sicherheit

- Festlegen der *Backup*-Richtlinien für persönliche und berufliche Daten
- Bewerten der verschiedenen Tools, um Lösungen für bestimmte Sicherheitsprobleme zu finden
- Etablieren von Mechanismen, um das System auf dem neuesten Stand zu halten
- Analysieren der Ausrüstung zur Erkennung von Eindringlingen
- Festlegen der Regeln für den Zugriff auf das System
- Prüfen und Klassifizieren von Mails, um Betrug zu vermeiden
- Erstellen von Listen mit erlaubter Software

Modul 3. Netzwerksicherheit (Perimeter)

- Analysieren der aktuellen Netzwerkarchitekturen, um den zu schützenden Perimeter zu identifizieren
- Entwickeln von spezifischen *Firewall*- und Linux-Konfigurationen zur Entschärfung der häufigsten Angriffe
- Kompilieren der am häufigsten verwendeten Lösungen wie Snort und Suricata, sowie deren Konfiguration
- Untersuchen der verschiedenen zusätzlichen Schichten, die von *Firewalls* der neuen Generation und Netzwerkfunktionen in *Cloud*-Umgebungen bereitgestellt werden
- Bestimmen der Tools für den Netzwerkschutz und Aufzeigen, warum sie für eine mehrschichtige Verteidigung von grundlegender Bedeutung sind

Modul 4. Smartphone Sicherheit

- Untersuchen der verschiedenen Angriffsvektoren, um zu vermeiden, ein leichtes Ziel zu werden
- Bestimmen der wichtigsten Angriffe und Arten von *Malware*, denen Benutzer mobiler Geräte ausgesetzt sind
- Analysieren der aktuellsten Geräte, um eine sicherere Konfiguration zu erstellen
- Festlegen der wichtigsten Schritte zur Durchführung eines Penetrationstests auf iOS- und Android-Plattformen
- Entwickeln von Fachwissen über die verschiedenen Schutz- und Sicherheitstools
- Etablieren von Best Practices bei der Programmierung für mobile Geräte

Modul 5. IoT-Sicherheit

- Analysieren der wichtigsten IoT-Architekturen
- Untersuchen von Verbindungstechnologien
- Entwickeln der wichtigsten Anwendungsprotokolle
- Erkennen der verschiedenen Arten von vorhandenen Geräten
- Bewerten der Risikostufen und bekannten Schwachstellen
- Entwickeln von Richtlinien zur sicheren Nutzung
- Festlegen geeigneter Bedingungen für die Verwendung dieser Geräte

Modul 6. Ethisches Hacking

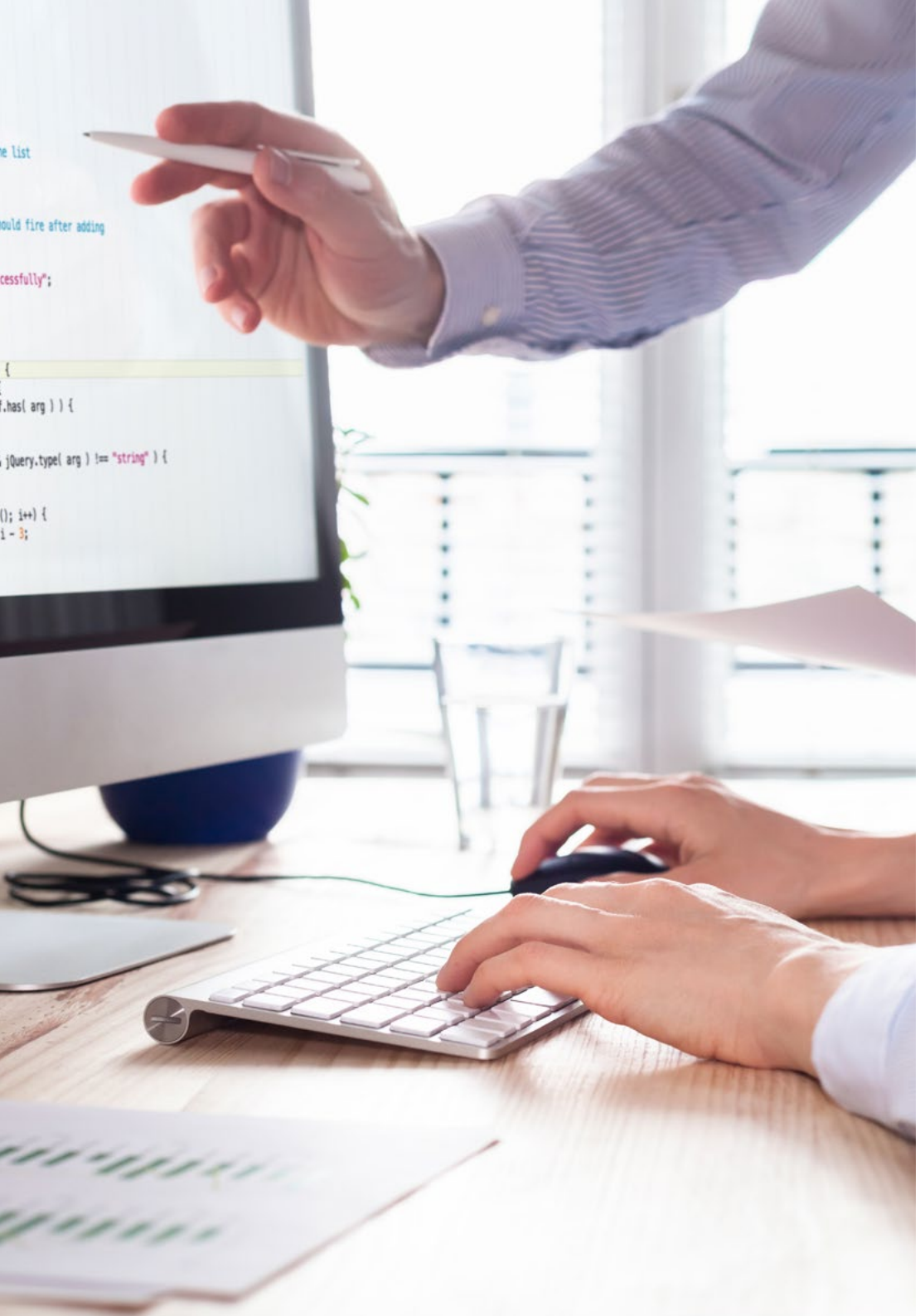
- Prüfen von OSINT-Methoden
- Sammeln von öffentlich zugänglichen Informationen
- Scannen von Netzwerken nach Informationen im aktiven Modus
- Entwickeln von Testlabors
- Analysieren von Tools für *Pentesting*-Leistungen
- Katalogisieren und Bewerten der verschiedenen Schwachstellen der Systeme
- Konkretisieren der verschiedenen *Hacking*-Methoden

Modul 7. Reverse Engineering

- Analysieren der Phasen eines Compilers
- Untersuchen der x86-Prozessorarchitektur und der ARM-Prozessorarchitektur
- Bestimmen der verschiedenen Arten von Analysen
- Anwenden von *Sandboxing* in verschiedenen Umgebungen
- Entwickeln verschiedener Techniken zur Analyse von *Malware*
- Entwickeln von Tools für die *Malware*-Analyse

Modul 8. Sichere Entwicklung

- Festlegen der Anforderungen, die für den korrekten Betrieb einer Anwendung auf sichere Weise erforderlich sind
- Untersuchen von *Logs*, um Fehlermeldungen zu verstehen
- Analysieren verschiedener Ereignisse und Entscheidung darüber, was dem Benutzer angezeigt und was in den *Logs* gespeichert werden soll
- Generieren von bereinigtem, leicht überprüfbarem, qualitativ hochwertigem Code
- Bewerten der geeigneten Dokumentation für jede Phase der Entwicklung
- Konkretisieren des Verhaltens des Servers, um das System zu optimieren
- Entwickeln von modularem, wiederverwendbarem und wartbarem Code



Modul 9. Forensische Analyse

- Identifizieren der verschiedenen Elemente, die ein Verbrechen beweisen
- Generieren von Spezialwissen, um Daten von verschiedenen Medien zu erhalten, bevor sie verloren gehen
- Wiederherstellen von Daten, die absichtlich gelöscht wurden
- Analysieren von System-*Logs* und Aufzeichnungen
- Bestimmen, wie die Daten dupliziert werden, ohne die Originale zu verändern
- Untermauern der Beweise für Konsistenz
- Erzeugen eines robusten und nahtlosen Berichts
- Präsentieren von Ergebnissen auf konsistente Weise
- Festlegen, wie der Bericht gegenüber der zuständigen Behörde verteidigt werden soll
- Festlegen von Strategien für sichere Telearbeit

Modul 10. Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit

- Untersuchen der Verwendung von Kryptowährungen, die Auswirkungen auf die Wirtschaft und die Sicherheit
- Analysieren der Situation der Nutzer und des Grades des digitalen Analphabetismus
- Bestimmen des Anwendungsbereichs von *Blockchain*
- Präsentieren von Alternativen zu IPv4 bei der Netzwerkadressierung
- Entwickeln von Strategien zur Schulung der Bevölkerung in der richtigen Nutzung von Technologien
- Erstellen von Fachwissen, um neue Sicherheitsherausforderungen zu bewältigen und Identitätsdiebstahl zu verhindern
- Entwickeln von Strategien für sichere Telearbeit

03

Kompetenzen

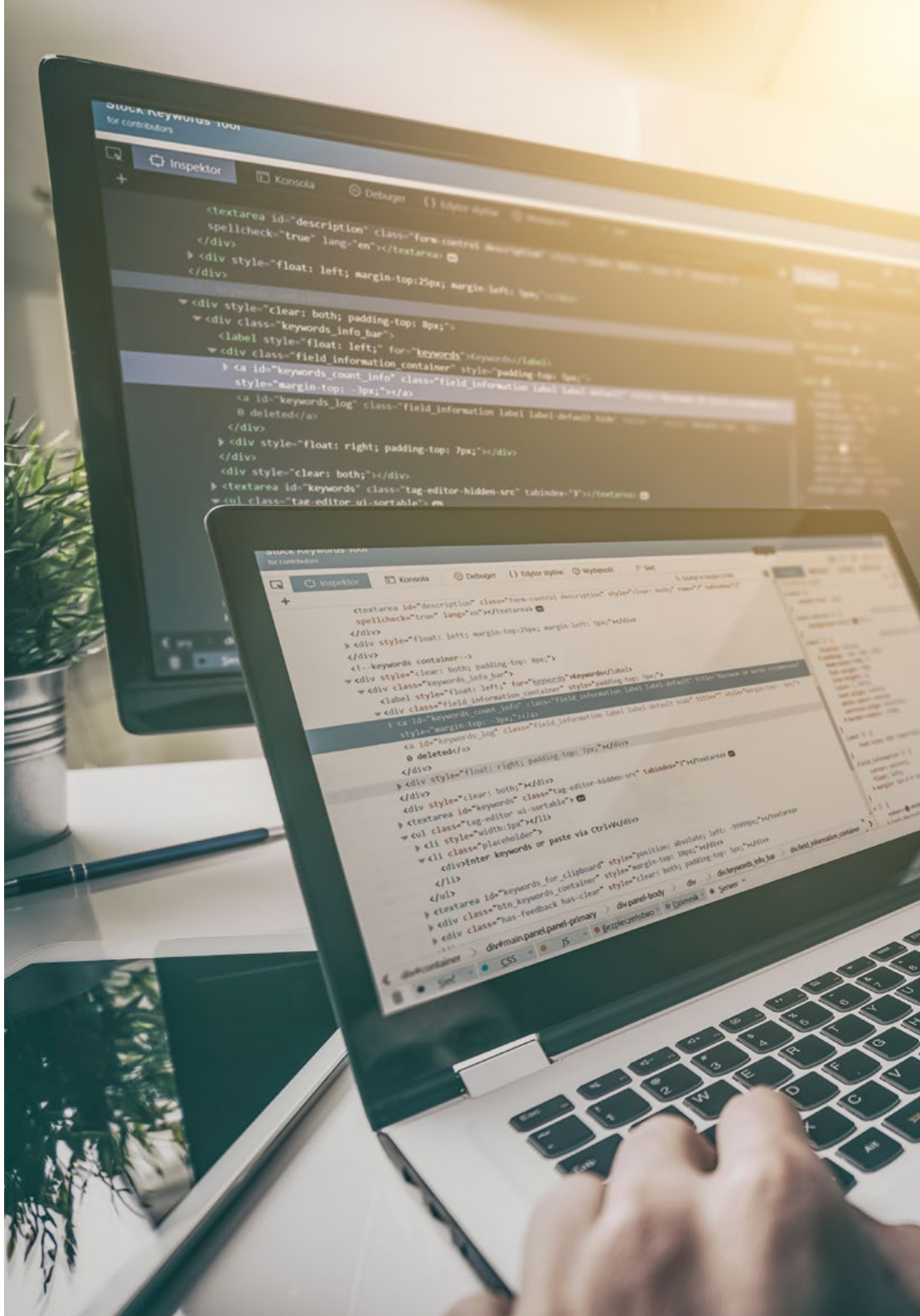
Nach Abschluss der Prüfung dieses privaten Masterstudiengangs wird die Fachkraft eine Reihe von Kenntnissen, Werkzeugen und Fähigkeiten erworben haben, die es ihr ermöglichen, mit größerer Erfolgsgarantie in diesem Sektor zu arbeiten. Auf diese Weise wird der Student nicht nur zu einem Experten für Cybersicherheit, sondern trägt auch positiv zur Reduzierung der Cyberkriminalität bei, indem er ein sichereres und stärkeres Netzwerk für alle schafft. So werden leitende Positionen wie die des Chief Information Security Officer erreicht.

Der Bereich der Cybersicherheit erfordert eine ständige Aktualisierung des Wissens. Mit Programmen wie diesem erreicht der Profi dies schnell und effektiv"

Allgemeine Kompetenzen

- Kennen der Methoden, die im Bereich der Cybersicherheit verwendet werden
- Wissen, wie man jede Art von Bedrohung bewertet, um in jedem Fall eine optimale Lösung anzubieten
- In der Lage sein, intelligente Komplettlösungen zu erstellen, um das Verhalten bei Zwischenfällen zu automatisieren
- Wissen, wie man die Risiken im Zusammenhang mit Schwachstellen innerhalb und außerhalb des Unternehmens einschätzen kann
- Verstehen der Entwicklung und der Auswirkungen des IoT im Laufe der Zeit
- Nachweisen, dass ein System verwundbar ist, es zu Präventionszwecken angreifen und solche Probleme lösen können
- Wissen, wie man *Sandboxing* in verschiedenen Umgebungen anwendet
- Kennen der Richtlinien, die ein guter Entwickler befolgen muss, um die notwendige Sicherheit zu gewährleisten

Die Verbesserung Ihrer Fähigkeiten in einem Dienst für alle wird Ihre berufliche und persönliche Karriere fördern"



Spezifische Kompetenzen

- Wissen, wie man defensive Sicherheitsmaßnahmen durchführt
- Verfügen über ein tiefgehendes und spezialisiertes Verständnis von Cybersicherheit
- Verfügen über spezielle Kenntnisse auf dem Gebiet der Cybersicherheit und Cyber Intelligence
- Verfügen über fundierte Kenntnisse grundlegender Aspekte, wie z.B. des Informationszyklus, der Informationsquellen, des Social Engineering, der OSINT-Methodik, des HUMINT, der Anonymisierung, der Risikoanalyse, der bestehenden Methoden (OWASP, OWISAM, OSSTM, PTES)
- Verstehen, wie wichtig es ist, eine mehrschichtige Verteidigung zu entwickeln, die auch als "Defence in Depth" bekannt ist und alle Aspekte eines Unternehmensnetzwerks abdeckt, wobei einige der besprochenen Konzepte und Systeme auch in einer häuslichen Umgebung genutzt und angewendet werden können
- Wissen, wie man Sicherheitsverfahren für Smartphones und tragbare Geräte anwende
- Kennen der Mittel, um das sogenannte ethische *Hacking* durchzuführen und ein Unternehmen vor einem Cyberangriff zu schützen
- In der Lage sein, einen Cybersicherheitsvorfall zu untersuchen
- Kennen der verschiedenen verfügbaren Angriffs- und Verteidigungstechniken
- Analysieren der Rolle des Cybersecurity Analysten
- Verstehen der Funktionsweise von Social Engineering und seiner Methoden

04

Kursleitung

Das Programm in Cybersecurity Management (CISO, Chief Information Security Officer) wurde von einem Team von Personen mit unterschiedlichen Berufsprofilen entwickelt, die auf verschiedene Sektoren spezialisiert sind und internationale Berufserfahrung in der Privatwirtschaft im Bereich FuEul sowie umfangreiche Lehrerfahrung kombinieren. Daher sind sie nicht nur in jeder der Technologien auf dem neuesten Stand, sondern haben auch eine Perspektive für die zukünftigen Bedürfnisse des Sektors und präsentieren diese auf didaktische Weise. Auf diese Weise haben Sie die Gewissheit, dass Sie von den Besten des Sektors lernen und über die aktuellsten Kenntnisse verfügen.

Während des Programms werden Sie von einer Reihe von Fachleuten begleitet, die Ihre Studienerfahrung einzigartig machen werden”

Internationale Gastdirektorin

Dr. Frederic Lemieux ist international als innovativer Experte und inspirierende Führungspersönlichkeit in den Bereichen der **Intelligenz, der nationalen Sicherheit, der inneren Sicherheit, der Cybersicherheit** und der **disruptiven Technologien** anerkannt. Sein ständiges Engagement und seine wichtigen Beiträge zu Forschung und Bildung machen ihn zu einer zentralen Figur bei der Förderung der Sicherheit und des Verständnisses der heutigen neuen Technologien. Während seiner beruflichen Laufbahn hat er an mehreren renommierten Institutionen wie der **Universität von Montreal,** der **George Washington Universität** und der Universität von Georgetown zukunftsweisende akademische Programme konzipiert und geleitet.

Im Laufe seiner umfangreichen Erfahrung hat er mehrere Bücher von großer Bedeutung veröffentlicht, die sich alle mit **kriminalistischer Aufklärung, Polizeiarbeit, Cyber-Bedrohungen und internationaler Sicherheit** befassen. Er hat auch einen wichtigen Beitrag zum Bereich der Cybersicherheit geleistet, indem er zahlreiche Artikel in akademischen Zeitschriften veröffentlicht hat, die sich mit der Verbrechensbekämpfung bei großen Katastrophen, der Terrorismusbekämpfung, den Nachrichtendiensten und der polizeilichen Zusammenarbeit beschäftigen. Darüber hinaus war er Podiumsteilnehmer und Hauptredner bei verschiedenen nationalen und internationalen Konferenzen und hat sich als führender Wissenschaftler und Praktiker etabliert.

Dr. Lemieux hatte redaktionelle und bewertende Funktionen in verschiedenen akademischen, privaten und staatlichen Organisationen inne, was seinen Einfluss und sein Engagement für Spitzenleistungen in seinem Fachgebiet widerspiegelt. Im Rahmen seiner angesehenen akademischen Laufbahn war er Professor für Praxis und Fakultätsleiter der MPS-Programme für **Angewandte Intelligenz, Risikomanagement für Cybersicherheit, Technologiemanagement und Informationstechnologiemanagement** an der **Universität von Georgetown.**

Dr. Lemieux, Frederic

- Forscher im Bereich Intelligenz, Cybersicherheit und Disruptive Technologien an der Universität von Georgetown
- Direktor des Masterstudiengangs in Information Technology Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Technology Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Cybersecurity Risk Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Applied Intelligence an der Universität von Georgetown
- Professor für Praktika an der Universität von Georgetown
- Promotion in Kriminologie an der School of Criminology der Universität von Montreal
- Hochschulabschluss in Soziologie, Nebenfach Psychologie, Universität von Laval
- Mitglied von:
- New Program Roundtable Committee, Universität von Georgetown

Dank TECH werden Sie mit den besten Fachleuten der Welt lernen können"

Leitung

Fr. Fernández Sapena, Sonia

- Ausbilderin für Computersicherheit und Ethical Hacking am Nationalen Referenzzentrum für Informatik und Telekommunikation
- Zertifizierte E-Council-Ausbilderin
- Kursleitung der folgenden Zertifizierungen: EXIN Ethical Hacking Foundation und EXIN Cyber & IT Security Foundation Madrid
- Von der CAM akkreditierte Fachausbilderin für die folgenden Berufszertifikate: IT-Sicherheit (IFCT0190), Verwaltung von Sprach- und Datennetzen (IFCM0310), Verwaltung von Abteilungsnetzen (IFCT0410), Alarmmanagement in Telekommunikationsnetzen (IFCM0410), Betreiber von Sprach- und Datennetzen (IFCM0110) und Verwaltung von Internetdiensten (IFCT0509)
- Externe Mitarbeit CSO/SSA (Chief Security Officer/Senior Security Architect)
- Computer- Ingenieurin an der von Alcalá de Henares Universität von Madrid
- Masterstudiengang in DevOps: Docker und Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies E-Council

Professoren

Hr. Redondo, Jesús Serrano

- Webentwickler und Cybersecurity-Techniker,
- Web-Entwickler, Roams, Palencia
- FrontEnd-Entwickler bei Telefónica, Madrid
- FrontEnd-Entwickler. Best Pro Consulting SL, Madrid
- Installateur von Telekommunikationsgeräten und -dienstleistungen. Zener Group, Castilla y León
- Installateur von Telekommunikationsgeräten und -dienstleistungen. Lican Comunicaciones SL, Castilla y León
- Zertifikat in Computersicherheit. CFTIC Getafe, Madrid
- Höherer Techniker: Telekommunikation und Computersysteme. IES Trinidad Arroyo, Palencia
- Höherer Techniker: Elektrotechnische MV- und LV-Installationen. IES Trinidad Arroyo, Palencia
- Ausbildung in Reverse Engineering, Stenographie, Verschlüsselung. Incibe Hacker Academy (Incibe Talents)

Hr. Jiménez Ramos, Álvaro

- Cybersecurity Analyst
- Senior Sicherheitsanalyst bei The Workshop
- L1 Cybersecurity Analyst bei Axians
- L2 Cybersecurity Analyst bei Axians
- Cybersecurity-Analyst bei SACYR S.A.
- Hochschulabschluss in Telematik-Ingenieurwesen an der Polytechnischen Universität von Madrid
- Masterstudiengang Cybersicherheit und ethisches Hacken von CICE
- Fortgeschrittenenkurs in Cybersicherheit von Deusto Formación

Fr. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Applikationsentwicklung bei B60. UK
- Analytikerin-Programmiererin für die Verwaltung, Koordination und Dokumentation einer virtualisierten Sicherheitsalarmumgebung
- Analytikerin-Programmiererin von Java-Anwendungen in Geldautomaten für Kunden
- Software Development Expertin für die Validierung von Unterschriften und die Anwendung zur Dokumentenverwaltung
- Systemtechnikerin für die Migration von Geräten und für die Verwaltung, Wartung und Schulung von PDA-Mobilgeräten vor Ort
- Technische Ingenieurwissenschaften für Computersysteme Universität Oberta de Katalonien (UOC)
- Masterstudiengang in Computersicherheit und Ethical Hacking Offizieller EC-Council und CompTIA von der Fachhochschule für neue Technologien CICE

Hr. Peralta Alonso, Jon

- Senior Consultant - Datenschutz und Cybersicherheit. Altia
- Rechtsanwalt / Rechtsbeistand Arriaga Asociados Rechtliche und wirtschaftliche Beratung, S.L. Rechtsberater / Trainee Professionelles Büro: Oscar Padura
- Hochschulabschluss in Jura Öffentliche Universität des Baskenlandes
- Masterstudiengang in Datenschutzbeauftragter. EIS Innovative School
- Masterstudiengang in Rechtswissenschaften. Öffentliche Universität des Baskenlandes
- Masterstudiengang in Zivilprozessrecht. Internationale Universität Isabel I de Castilla
- Dozent im Masterstudiengang für Datenschutz, Cybersicherheit und IKTRecht

Hr. Catalá Barba, José Francisco

- Elektroniker mit Erfahrung in Cybersicherheit
- Entwickler von Applikationen für mobile Geräte
- Elektronik-Techniker. Mittleres Management im spanischen Verteidigungsministerium
- Elektroniker im Ford-Werk in Almusafes, Valencia

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

05

Struktur und Inhalt

Um sicherzustellen, dass die Studenten die strengsten und modernsten Kenntnisse im Bereich der Cybersicherheit erwerben, hat TECH eine Reihe von Materialien entwickelt, die die neuesten Updates in diesem Bereich zusammenfassen. Diese Inhalte wurden von einer Gruppe von Fachleuten auf diesem Gebiet entworfen, so dass sie an die aktuellen Bedürfnisse der in der Branche angebotenen Stellen angepasst sind. Eine einzigartige und äußerst professionelle Gelegenheit, die die Studenten in ihrer beruflichen Entwicklung zum Erfolg führen wird.

Ein Studienplan auf hohem Niveau, entwickelt von und für Fachleute auf hohem Niveau. Werden Sie sich diese Gelegenheit entgehen lassen?"

Modul 1. Cyberintelligenz und Cybersicherheit

1.1. Cyberintelligenz
- 1.1.1. Cyberintelligenz
  - 1.1.1.1. Die Intelligenz
    - 1.1.1.1.1. Intelligenz-Zyklus
  - 1.1.1.2. Cyberintelligenz
  - 1.1.1.3. Cyberintelligenz und Cybersicherheit
- 1.1.2. Der Informationsanalyst
  - 1.1.2.1. Die Rolle des Informationsanalysten
  - 1.1.2.2. Voreingenommenheit des Informationsanalysten bei der Bewertung von Aktivitäten

1.2. Cybersicherheit
- 1.2.1. Schichten der Sicherheit
- 1.2.2. Identifizierung von Cyber-Bedrohungen
  - 1.2.2.1. Externe Bedrohungen
  - 1.2.2.2. Interne Bedrohungen
- 1.2.3. Nachteilige Maßnahmen
  - 1.2.3.1. Social Engineering
  - 1.2.3.2. Häufig verwendete Methoden

1.3. Intelligente Tools und Techniken
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. Humit
- 1.3.4. Linux-Distributionen und -Tools
- 1.3.5. OWISAM
- 1.3.6. OWASP
- 1.3.7. PTES
- 1.3.8. OSSTMM

1.4. Methoden der Bewertung
- 1.4.1. Informationsanalyse
- 1.4.2. Techniken zur Organisation der erworbenen Informationen
- 1.4.3. Verlässlichkeit und Glaubwürdigkeit von Informationsquellen
- 1.4.4. Methodologien der Analyse
- 1.4.5. Präsentation der Geheimdienstergebnisse

1.5. Audits und Dokumentation
- 1.5.1. Das IT-Sicherheitsaudit
- 1.5.2. Dokumentation und Berechtigungen für Audits
- 1.5.3. Arten von Audits
- 1.5.4. Liefergegenstände
  - 1.5.4.1. Technischer Bericht
  - 1.5.4.2. Bericht der Geschäftsführung

1.6. Anonymität im Netz
- 1.6.1. Nutzung der Anonymität
- 1.6.2. Anonymisierungstechniken (Proxy, VPN)
- 1.6.3. TOR, Freenet und IP2-Netzwerke

1.7. Bedrohungen und Arten von Sicherheit
- 1.7.1. Arten von Bedrohungen
- 1.7.2. Physische Sicherheit
- 1.7.3. Netzwerksicherheit
- 1.7.4. Logische Sicherheit
- 1.7.5. Sicherheit von Webanwendungen
- 1.7.6. Sicherheit für mobile Geräte

1.8. Regulierung und *Compliance*
- 1.8.1. Datenschutz-Grundverordnung
- 1.8.3. ISO 27000- Familie
- 1.8.4. NIST Cybersecurity Framework
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. *Cloud*-Standards
- 1.8.8. SOX
- 1.8.9. ICP

1.9. Risikoanalyse und Metriken
- 1.9.1. Umfang der Risiken
- 1.9.2. Vermögenswerte
- 1.9.3. Bedrohungen
- 1.9.4. Schwachstellen
- 1.9.5. Risikobewertung
- 1.9.6. Risikobehandlung

1.10. Einschlägige Stellen für Cybersicherheit
- 1.10.1. NIST
- 1.10.4. OEA
- 1.10.5. UNASUR PROSUR

Modul 2. Host-Sicherheit

2.1. Sicherungskopien
- 2.1.1. Strategien zur Datensicherung
- 2.1.2. Tools für Windows
- 2.1.3. Tools für Linux
- 2.1.4. Werkzeuge für MacOS

2.2. Benutzer Antivirus
- 2.2.1. Arten von Antivirenprogrammen
- 2.2.2. Antivirus für Windows
- 2.2.3. Antivirus für Linux
- 2.2.4. Antivirus für MacOS
- 2.2.5. Antivirus für Smartphones

2.3. HIDS Eindringlingsdetektoren
- 2.3.1. Methoden zur Erkennung von Eindringlingen
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. *Rkhunter*

2.4. Lokale *Firewall*
- 2.4.1. *Firewalls* für Windows
- 2.4.2. *Firewalls* für Linux
- 2.4.3. *Firewalls* für MacOS

2.5. Passwort-Manager
- 2.5.1. Password
- 2.5.2. *LastPass*
- 2.5.3. *KeePass*
- 2.5.4. *Sticky password*
- 2.5.5. RoboForm

2.6. *Phishing*-Detektoren
- 2.6.1. Manuelle *Phishing*-Erkennung
- 2.6.2. *Anti-Phishing*-Tools

2.7. *Spyware*
- 2.7.1. Vermeidungsmechanismen
- 2.7.2. *Anti-Spyware*-Tools

2.8. Tracker
- 2.8.1. Maßnahmen zum Schutz des Systems
- 2.8.2. Anti-Tracker-Tools

2.9. *EDR - Endpunkt-Erkennung und Reaktion*
- 2.9.1. Verhalten des EDR-Systems
- 2.9.2. Unterschiede zwischen EDR und Anti-Virus
- 2.9.3. Die Zukunft der EDR-Systeme

2.10. Kontrolle über die Software-Installation
- 2.10.1. Repositories und Software-Speicher
- 2.10.2. Listen mit erlaubter oder verbotener Software
- 2.10.3. Update-Kriterien
- 2.10.4. Berechtigungen für die Software-Installation

Modul 3. Netzwerksicherheit (Perimeter)

3.1. Systeme zur Erkennung und Abwehr von Bedrohungen
- 3.1.1. Allgemeiner Rahmen für Sicherheitsvorfälle
- 3.1.2. Aktuelle Verteidigungssysteme: *Defense in depth* und SOC
- 3.1.3. Aktuelle Netzwerkarchitekturen
- 3.1.4. Arten von Tools zur Erkennung und Verhinderung von Vorfällen
  - 3.1.4.1. Netzwerkbasierte Systeme
  - 3.1.4.2. *Host*-basierte Systeme
  - 3.1.4.3. Zentralisierte Systeme
- 3.1.5. Kommunikation und Erkennung von Instanzen/*Hosts*, Containern und *Serverless*

3.2. *Firewall*
- 3.2.1. Arten von *Firewalls*
- 3.2.2. Angriffe und Schadensbegrenzung

3.2.3. Gängige *Firewalls* in *Kernel* Linux
3.2.3.1. UFW
3.2.3.2. *Nftables* und *iptables*
3.2.3.3. *Firewalld*
3.2.4. Erkennungssysteme auf der Grundlage von System*logs*
3.2.4.1. TCP *wrappers*
3.2.4.2. *BlockHosts* und *DenyHosts*
3.2.4.3. Fail2Ban
3.3. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
3.3.1. Angriffe auf IDS/IPS
3.3.2. IDS/IPS-Systeme
3.3.2.1. *Snort*
3.3.2.2. Suricata
3.4. *Firewalls* der nächsten Generation (NGFW)
3.4.1. Unterschiede zwischen NGFW und traditionellen *Firewalls*
3.4.2. Kernkapazitäten
3.4.3. Business Lösungen
3.4.4. *Firewalls* für *Cloud*-Dienste
3.4.4.1. *Cloud* VPC Architektur
3.4.4.2. *Cloud* ACLs
3.4.4.3. *Security group*
3.5. *Proxy*
3.5.1. Arten von *Proxys*
3.5.2. *Proxy*-Nutzung. Vorteile und Nachteile
3.6. Antivirus-Engines
3.6.1. Allgemeiner Kontext von *Malware* und IOCs
3.6.2. Probleme mit Anti-Viren-Programmen
3.7. Mailschutzsysteme
3.7.1. Antispam
3.7.1.1. Whitelisting und Blacklisting
3.7.1.2. Bayes'sche Filter
3.7.2. *Mail Gateway* (MGW)
3.8. SIEM
3.8.1. Komponenten und Architektur
3.8.2. Korrelationsregeln und Anwendungsfälle
3.8.3. Aktuelle Herausforderungen von SIEM-Systemen
3.9. SOAR
3.9.1. SOAR und SIEM: Feinde oder Verbündete?
3.9.2. Die Zukunft der SOAR-Systeme
3.10. Andere netzwerkbasierte Systeme
3.10.1. WAF
3.10.2. NAC
3.10.3. *HoneyPots* und *HoneyNets*
3.10.4. CASB

Modul 4. Smartphone Sicherheit

4.1. Die Welt der mobilen Geräte
4.1.1. Arten von mobilen Plattformen
4.1.2. IOS-Geräte
4.1.3. Android-Geräte
4.2. Verwaltung der mobilen Sicherheit
4.2.1. OWASP Projekt für mobile Sicherheit
4.2.1.1. Top 10 Schwachstellen
4.2.2. Kommunikation, Netzwerke und Verbindungsarten
4.3. Das mobile Gerät in der Unternehmensumgebung
4.3.1. Risiken
4.3.3. Geräteüberwachung
4.3.4. Verwaltung mobiler Geräte (MDM)
4.4. Datenschutz und Datensicherheit
4.4.1. Informationen Staaten
4.4.3. Sichere Speicherung von Daten
4.4.3.1. Sicherer Speicher auf iOS
4.4.3.2. Sicherer Speicher auf Android
4.4.4. Bewährte Praktiken bei der Applikationsentwicklung

4.5. Schwachstellen und Angriffsvektoren
- 4.5.1. Schwachstellen
- 4.5.2. Angriffsvektoren
  - 4.5.2.1. *Malware*
  - 4.5.2.2. Exfiltration von Daten
  - 4.5.2.3. Datenmanipulation

4.6. Wichtigste Bedrohungen
- 4.6.1. Ungeschulter Benutzer
- 4.6.2. Malware
  - 4.6.2.1. Arten von Malware
- 4.6.3. Social Engineering
- 4.6.4. Datenleck
- 4.6.5. Datendiebstahl
- 4.6.6. Ungesicherte WiFi-Netzwerke
- 4.6.7. Veraltete Software
- 4.6.8. Bösartige Anwendungen
- 4.6.9. Unsichere Passwörter
- 4.6.10. Schwache oder nicht vorhandene Sicherheitseinstellungen
- 4.6.11. Physischer Zugang
- 4.6.12. Verlust oder Diebstahl des Geräts
- 4.6.13. Impersonation (Integrität)
- 4.6.14. Schwache oder defekte Kryptographie
- 4.6.15. Denial of Service (DoS)

4.7. Große Angriffe
- 4.7.1. Phishing-Angriffe
- 4.7.2. Angriffe im Zusammenhang mit Kommunikationsmodi
- 4.7.3. *Smishing*-Angriffe
- 4.7.4. *Criptojacking*-Angriffe
- 4.7.5. *Man in the Middle*

4.8. *Hacking*
- 4.8.1. *Rooting* und *jailbreaking*
- 4.8.2. Anatomie eines mobilen Angriffs
  - 4.8.2.1. Ausbreitung der Bedrohung
  - 4.8.2.2. Installation von *Malware* auf dem Gerät
  - 4.8.2.3. Persistenz
  - 4.8.2.4. Ausführung der *Payload* und Extraktion von Informationen
- 4.8.3. *Hacking* auf iOS-Geräten: Mechanismen und Tools
- 4.8.4. *Hacking* auf Android-Geräten: Mechanismen und Tools

4.9. Penetrationstests
- 4.9.1. iOS *Pentesting*
- 4.9.2. Android *Pentesting*
- 4.9.3. Tools

4.10. Schutz und Sicherheit
- 4.10.1. Sicherheitseinstellungen
  - 4.10.1.1. Auf iOS-Geräten
  - 4.10.1.2. Auf Android-Geräten
- 4.10.2. Sicherheitsmaßnahmen
- 4.10.3. Schutz-Tools

Modul 5. IoT-Sicherheit

5.1. Geräte
- 5.1.1. Arten von Geräten
- 5.1.2. Standardisierte Architekturen
  - 5.1.2.1. OneM2M
  - 5.1.2.2. IoTWF
- 5.1.3. Anwendungsprotokolle
- 5.1.4. Konnektivitätstechnologien

5.2. IoT-Geräte. Anwendungsbereiche
- 5.2.1. SmartHome
- 5.2.2. SmartCity
- 5.2.3. Transport
- 5.2.4. *Wearables*
- 5.2.5. Gesundheitssektor
- 5.2.6. IIoT

5.3. Kommunikationsprotokolle
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. SmartHome
- 5.4.1. Hausautomatisierung
- 5.4.2. Netzwerke
- 5.4.3. Haushaltsgeräte
- 5.4.4. Überwachung und Sicherheit

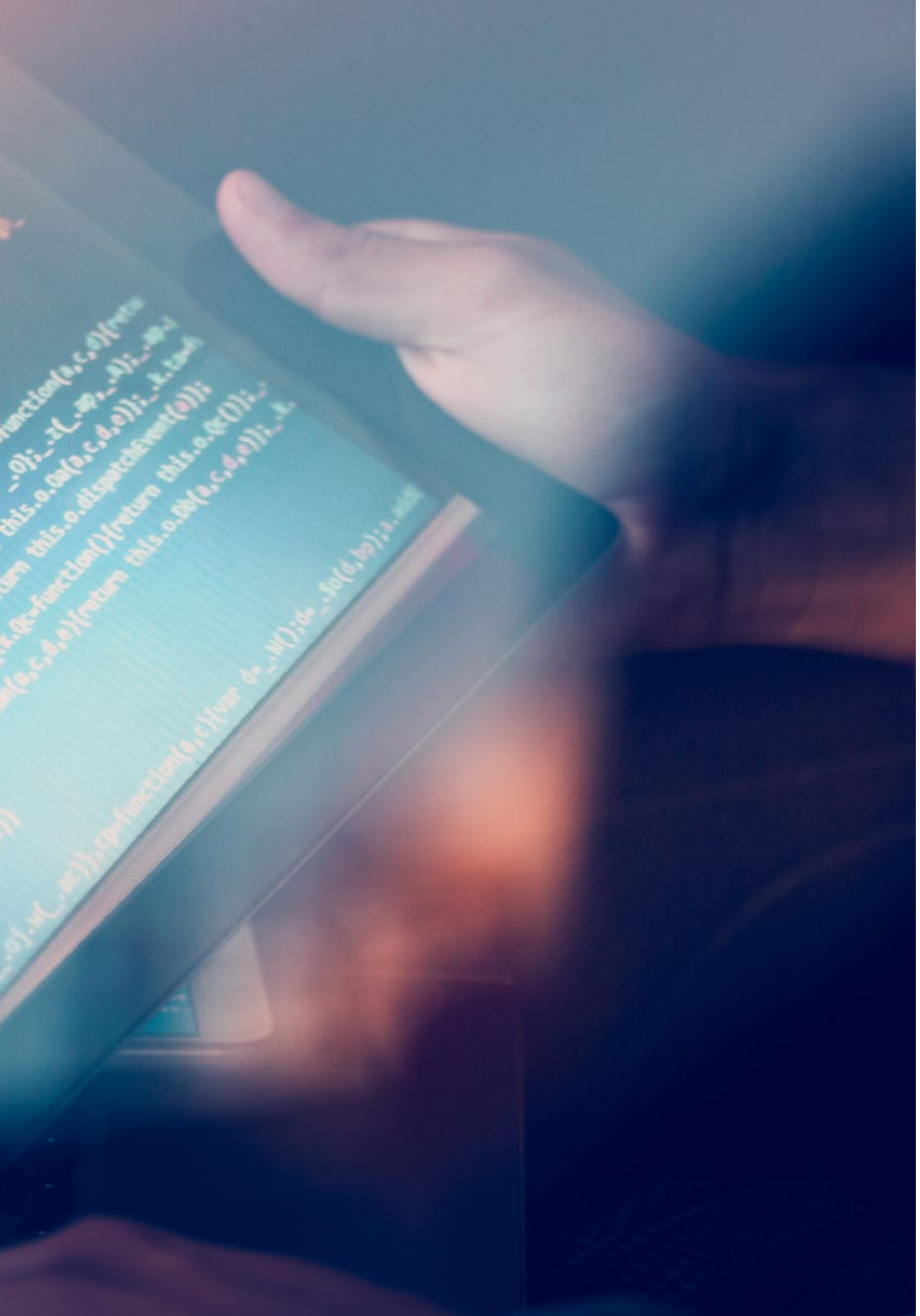
5.5. SmartCity
- 5.5.1. Beleuchtung
- 5.5.2. Meteorologie
- 5.5.3. Sicherheit

5.6. Transport
- 5.6.1. Lokalisation
- 5.6.2. Zahlungen leisten und Dienstleistungen in Anspruch nehmen
- 5.6.3. Konnektivität

5.7. *Wearables*
- 5.7.1. Intelligente Kleidung
- 5.7.2. Intelligenter Schmuck
- 5.7.3. Intelligente Uhren

5.8. Gesundheitssektor
- 5.8.1. Training/Herzfrequenzüberwachung
- 5.8.2. Überwachung von Patienten und älteren Menschen
- 5.8.3. Implantierbare Geräte
- 5.8.4. Chirurgische Roboter

5.9. Konnektivität
- 5.9.1. Wifi
- 5.9.2. Bluetooth
- 5.9.3. Eingebettete Konnektivität



5.10. Verbriefung
- 5.10.1. Dedizierte Netzwerke
- 5.10.2. Passwort Manager
- 5.10.3. Verwendung von verschlüsselten Protokollen
- 5.10.4. Tipps für die Verwendung

Modul 6. Ethisches Hacking

6.1. Arbeitsumgebung
- 6.1.1. Linux-Distributionen
  - 6.1.1.1. Kali Linux - Offensive Security
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Virtualisierungssysteme
- 6.1.3. Sandbox
- 6.1.4. Einsatz von Labors

6.2. Methoden
- 6.2.1. OSSTMM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. Footprinting
- 6.3.1. Open Source Intelligence (OSINT)
- 6.3.2. Suche nach Datenschutzverletzungen und Schwachstellen
- 6.3.3. Verwendung von passiven Tools

6.4. Netzwerk-Scans
- 6.4.1. Tools zum Scannen
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Andere Scan-Tools
- 6.4.2. Scanning-Techniken
- 6.4.3. Techniken zur Umgehung von *Firewalls* und IDS
- 6.4.4. Banner grabbing
- 6.4.5. Netzwerk-Diagramme

6.5. Aufzählung
- 6.5.1. SMTP Aufzählung
- 6.5.2. DNS Aufzählung
- 6.5.3. NetBIOS und Samba Aufzählung
- 6.5.4. LDAP Aufzählung
- 6.5.5. SNMP Aufzählung
- 6.5.6. Andere Aufzählungstechniken

6.6. Scannen auf Schwachstellen
- 6.6.1. Lösungen zum Scannen auf Schwachstellen
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2. Systeme zur Bewertung von Schwachstellen
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Angriffe auf drahtlose Netzwerke
- 6.7.1. Methodik zum *Hacken* drahtloser Netzwerke
  - 6.7.1.1. Wifi Discovery
  - 6.7.1.2. Verkehrsanalyse
  - 6.7.1.3. *Aircrack*-Angriffe
    - 6.7.1.3.1. WEP-Angriffe
    - 6.7.1.3.2. WPA/WPA2-Angriffe
  - 6.7.1.4. *Evil Twin*-Angriffe
  - 6.7.1.5. WPS-Angriffe
  - 6.7.1.6. *Jamming*
- 6.7.2. Tools für drahtlose Sicherheit

6.8. Hacking von Webservern
- 6.8.1. *Cross site Scripting*
- 6.8.2. CSRF
- 6.8.3. *Session Hijacking*
- 6.8.4. *SQL injection*

6.9. Ausnutzung von Schwachstellen
- 6.9.1. Verwendung von bekannten *Exploits*
- 6.9.2. Verwendung von *Metasploit*
- 6.9.3. Verwendung von *Malware*
  - 6.9.3.1. Definition und Umfang
  - 6.9.3.2. Generierung von *Malware*
  - 6.9.3.3. Umgehung von Anti-Viren-Lösungen

6.10. Persistenz
- 6.10.1. Installation von *Rootkits*
- 6.10.2. Ncat verwenden
- 6.10.3. Geplante Aufgaben für *Backdoors* verwenden
- 6.10.4. Benutzer erstellen
- 6.10.5. HIDS aufspüren

Modul 7. Reverse Engineering

7.1. Compiler
- 7.1.1. Arten von Code
- 7.1.2. Compiler-Phasen
- 7.1.3. Symboltabelle
- 7.1.4. Fehler-Handler
- 7.1.5. GCC Compiler

7.2. Arten der Compiler-Analyse
- 7.2.1. Lexikalische Analyse
  - 7.2.1.1. Terminologie
  - 7.2.1.2. Lexikalische Komponenten
  - 7.2.1.3. LEX Lexikalischer Analysator
- 7.2.2. Syntaktische Analyse
  - 7.2.2.1. Kontextfreie Grammatiken
  - 7.2.2.2. Arten des Parsing
    - 7.2.2.2.1. Top-down-Parsing
    - 7.2.2.2.2. Bottom-up-Parsing
  - 7.2.2.3. Syntaktische Bäume und Ableitungen
  - 7.2.2.4. Arten von Parsern
    - 7.2.2.4.1. LR-Parser (*Left to Right*)
    - 7.2.2.4.2. LALR-Parser

7.2.3. Semantische Analyse
7.2.3.1. Attribut-Grammatiken
7.2.3.2. S-Attribute
7.2.3.3. L-Attribute
7.3. Montage Datenstrukturen
7.3.1. Variablen
7.3.2. Arrays
7.3.3. Zeiger
7.3.4. Strukturen
7.3.5. Objekte
7.4. Assembly Code-Strukturen
7.4.1. Auswahl-Strukturen
7.4.1.1. If, else if, Else
7.4.1.2. *Switch*
7.4.2. Iterations-Strukturen
7.4.2.1. *For*
7.4.2.2. *While*
7.4.2.3. Verwendung des *Break*
7.4.3. Funktionen
7.5. x86-Hardware-Architektur
7.5.1. x86-Prozessorarchitektur
7.5.2. x86 Datenstrukturen
7.5.3. x86 Code-Strukturen
7.5.4. x86 Code-Strukturen
7.6. ARM Hardware-Architektur
7.6.1. ARM-Prozessorarchitektur
7.6.2. ARM-Daten-Strukturen
7.6.3. ARM-Code-Strukturen
7.7. Statische Code-Analyse
7.7.1. Disassembler
7.7.2. IDA
7.7.3. Code-Rekonstrukteure
7.8. Dynamische Code-Analyse
7.8.1. Verhaltensanalyse
7.8.1.1. Kommunikation
7.8.1.2. Überwachung
7.8.2. Linux Code-Debugger
7.8.3. Windows-Code-Debugger
7.9. Sandbox
7.9.1. Sandbox-Architektur
7.9.2. Sandbox-Umgehung
7.9.3. Erkennungstechniken
7.9.4. Ausweichtechniken
7.9.5. Gegenmaßnahmen
7.9.6. Sandbox in Linux
7.9.7. Sandbox in Windows
7.9.8. *Sandox* in MacOS
7.9.9. Sandbox in Android
7.10. *Malware*-Scans
7.10.1. Methoden zur Analyse des *Malware*
7.10.2. Techniken zur Verschleierung von *Malware*
7.10.2.1. Ausführbare Verschleierung
7.10.2.2. Einschränkung der Ausführungsumgebungen
7.10.3. Tools zur Analyse des *Malware*

Modul 8. Sichere Entwicklung

8.1. Sichere Entwicklung
8.1.1. Qualität, Funktionalität und Sicherheit
8.1.2. Vertraulichkeit, Integrität und Verfügbarkeit
8.1.3. Lebenszyklus der Softwareentwicklung
8.2. Phase der Anforderungen
8.2.1. Kontrolle der Authentifizierung
8.2.2. Kontrolle von Rollen und Privilegien
8.2.3. Risikoorientierte Anforderungen
8.2.4. Genehmigung von Privilegien

8.3. Analyse- und Entwurfsphasen
- 8.3.1. Komponentenzugriff und Systemverwaltung
- 8.3.2. Prüfpfade
- 8.3.3. Sitzungsmanagement
- 8.3.4. Historische Daten
- 8.3.5. Angemessene Fehlerbehandlung
- 8.3.6. Trennung der Funktionen

8.4. Phase der Implementierung und Kodierung
- 8.4.1. Absicherung der Entwicklungsumgebung
- 8.4.2. Ausarbeitung der technischen Dokumentation
- 8.4.3. Sichere Kodierung
- 8.4.4. Sicherheit des Kommunikation

8.5. Gute sichere Kodierungspraktiken
- 8.5.1. Validierung von Eingabedaten
- 8.5.2. Verschlüsselung der Ausgabedaten
- 8.5.3. Programmierstil
- 8.5.4. Handhabung des Änderungsprotokolls
- 8.5.5. Kryptographische Praktiken
- 8.5.6. Fehler- und Protokollverwaltung
- 8.5.7. Dateiverwaltung
- 8.5.8. Speicherverwaltung
- 8.5.9. Standardisierung und Wiederverwendung von Sicherheitsfunktionen

8.6. Vorbereitung und *Härtung* von Servern
- 8.6.1. Verwaltung von Benutzern, Gruppen und Rollen auf dem Server
- 8.6.2. Software-Installation
- 8.6.3. Server-*Härtung*
- 8.6.4. Robuste Konfiguration der Anwendungsumgebung

8.7. DB Vorbereitung und *Härtung*
- 8.7.1. Optimierung der DB-Engine
- 8.7.2. Erstellung eines eigenen Benutzers für die Anwendung
- 8.7.3. Zuweisung der erforderlichen Berechtigungen an den Benutzer
- 8.7.4. *Härtung* der DB

8.8. Testphase
- 8.8.1. Qualitätskontrolle bei Sicherheitskontrollen
- 8.8.2. Stufenweise Code Inspektion
- 8.8.3. Überprüfung der Konfigurationsverwaltung
- 8.8.4. Blackbox-Tests

8.9. Vorbereitungen für den Übergang zur Produktion
- 8.9.1. Änderungskontrolle durchführen
- 8.9.2. Führen Sie die Produktionsumstellung durch
- 8.9.3. *Rollback*-Prozedur durchführen
- 8.9.4. Tests in der Vorproduktionsphase

8.10. Erhaltungsphase
- 8.10.1. Risikobasierte Versicherung
- 8.10.2. White-Box-Tests zur Wartung der Sicherheit
- 8.10.3. Black Box Sicherheits-Wartungstests

Modul 9. Forensische Analyse

9.1. Datenerfassung und Replikation
- 9.1.1. Volatile Datenerfassung
  - 9.1.1.1. System-Informationen
  - 9.1.1.2. Netzwerk-Informationen
  - 9.1.1.3. Volatilität bestellen
- 9.1.2. Statische Datenerfassung
  - 9.1.2.1. Erstellung eines doppelten Bildes
  - 9.1.2.2. Erstellung eines Dokuments für die Überwachungskette
- 9.1.3. Methoden zur Validierung der erfassten Daten
  - 9.1.3.1. Methoden für Linux
  - 9.1.3.2. Methoden für Windows

9.2. Bewertung und Beseitigung von Anti-Forensik-Techniken
- 9.2.1. Ziele der forensischen Techniken
- 9.2.2. Löschung von Daten
  - 9.2.2.1. Löschung von Daten und Dateien
  - 9.2.2.2. Dateiwiederherstellung
  - 9.2.2.3. Wiederherstellung von gelöschten Partitionen

9.2.3. Passwortschutz
9.2.4. Steganographie
9.2.5. Sicheres Löschen von Geräten
9.2.6. Verschlüsselung
9.3. Betriebssystem-Forensik
9.3.1. Windows-Forensik
9.3.2. Linux-Forensik
9.3.3. Mac-Forensik
9.4. Netzwerk-Forensik
9.4.1. *Log*-Analyse
9.4.2. Korrelation der Daten
9.4.3. Netzwerk-Untersuchung
9.4.4. Schritte der forensischen Netzwerkanalyse
9.5. Web-Forensik
9.5.1. Untersuchung von Webangriffen
9.5.2. Angriffserkennung
9.5.3. Standort der IP-Adresse
9.6. Datenbank-Forensik
9.6.1. MSSQL-Forensik
9.6.2. MySQL-Forensik
9.6.3. PostgreSQL-Forensik
9.6.4. MongoDB-Forensik
9.7. *Cloud*-Forensik
9.7.1. Arten von *Cloud*-Verbrechen
9.7.1.1. Cloud als Thema
9.7.1.2. Die Wolke als Objekt
9.7.1.3. Die Cloud als Werkzeug
9.7.2. Herausforderungen der *Cloud*-Forensik
9.7.3. Untersuchung von *Cloud*-Speicherdiensten
9.7.4. Forensische Analyse-Tools für die *Cloud*
9.8. Untersuchung von E-Mail-Verbrechen
9.8.1. Mail-Systeme
9.8.1.1. Mail Clients
9.8.1.2. Mail-Server
9.8.1.3. SMTP-Server
9.8.1.4. POP3-Server
9.8.1.5. IMAP4-Server
9.8.2. Mail Verbrechen
9.8.3. Mail-Nachricht
9.8.3.1. Standard-Kopfzeilen
9.8.3.2. Erweiterte Kopfzeilen
9.8.4. Schritte bei der Untersuchung dieser Verbrechen
9.8.5. Tools für die E-Mail-Forensik
9.9. Mobile forensische Analyse
9.9.1. Zellulare Netzwerke
9.9.1.1. Arten von Netzwerken
9.9.1.2. CDR Inhalt
9.9.2. *Subscriber Identity Module* (SIM)
9.9.3. Logische Akquisition
9.9.4. Physische Akquisition
9.9.5. Dateisystem-Erfassung
9.10. Forensische Berichte schreiben und einreichen
9.10.1. Wichtige Aspekte eines forensischen Berichts
9.10.2. Klassifizierung und Arten von Berichten
9.10.3. Leitfaden zum Schreiben eines Berichts
9.10.4. Präsentation des Berichts
9.10.4.1. Vorbereitung auf die Zeugenaussage
9.10.4.2. Hinterlegung
9.10.4.3. Der Umgang mit den Medien

Modul 10. Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit

10.1. Blockchain Technologie
- 10.1.1. Anwendungsbereiche
- 10.1.2. Garantie der Vertraulichkeit
- 10.1.3. Garantie der Nicht-Abstreitbarkeit

10.2. Digitales Geld
- 10.2.1. Bitcoins
- 10.2.2. Kryptowährungen
- 10.2.3. Schürfen von Kryptowährungen
- 10.2.4. Schneeballsysteme
- 10.2.5. Andere mögliche Verbrechen und Probleme

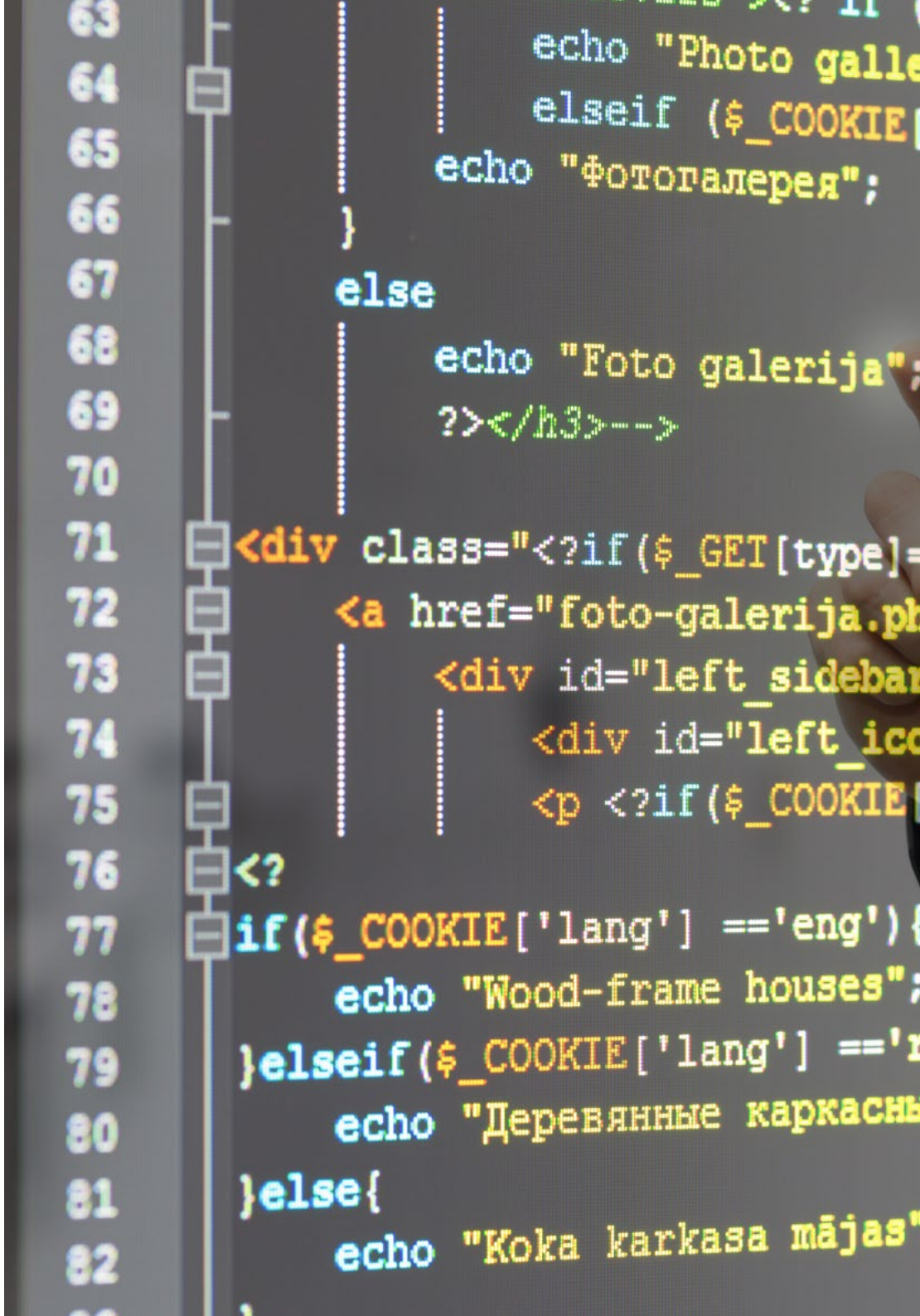
10.3. Deepfake
- 10.3.1. Auswirkungen auf die Medien
- 10.3.2. Gefahren für die Gesellschaft
- 10.3.3. Erkennungsmechanismen

10.4. Die Zukunft der künstlichen Intelligenz
- 10.4.1. Künstliche Intelligenz und kognitives Computing
- 10.4.2. Anwendungen zur Vereinfachung des Kundendienstes

10.5. Digitale Privatsphäre
- 10.5.1. Wert der Daten im Netzwerk
- 10.5.2. Verwendung von Daten im Netzwerk
- 10.5.3. Datenschutz und Verwaltung digitaler Identitäten

10.6. Cyber-Konflikte, Cyber-Kriminelle und Cyber-Angriffe
- 10.6.1. Auswirkungen der Cybersicherheit auf internationale Konflikte
- 10.6.2. Folgen von Cyberangriffen auf die allgemeine Bevölkerung
- 10.6.3. Arten von Cyber-Kriminellen. Schutzmaßnahmen

10.7. Telearbeit
- 10.7.1. Revolution der Telearbeit während und nach COVID-19
- 10.7.2. Engpässe beim Zugang
- 10.7.3. Variation der Angriffsfläche
- 10.7.4. Bedürfnisse der Arbeiter



10.8. Aufkommende *Wireless* Technologien
- 10.8.1. WPA3
- 10.8.2. 5G
- 10.8.3. Millimeter-Wellen
- 10.8.4. Trend zu "*Get Smart*" anstelle von "*Get more*"

10.9. Künftige Adressierung in Netzwerken
- 10.9.1. Aktuelle Probleme mit der IP-Adressierung
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. Vorteile von IPv4+ gegenüber IPv4
- 10.9.5. Vorteile von IPv6 gegenüber IPv4

10.10. Die Herausforderung, das Bewusstsein für eine frühzeitige und kontinuierliche Schulung der Bevölkerung zu schärfen
- 10.10.1. Aktuelle Strategien der Regierung
- 10.10.2. Der Widerstand der Menschen gegen das Lernen
- 10.10.3. Ausbildungspläne, die von den Unternehmen angenommen werden müssen

Ihre Zukunft beginnt hier. Schreiben Sie sich noch heute ein und werden Sie Chief Information Officer eines großen Unternehmens"

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

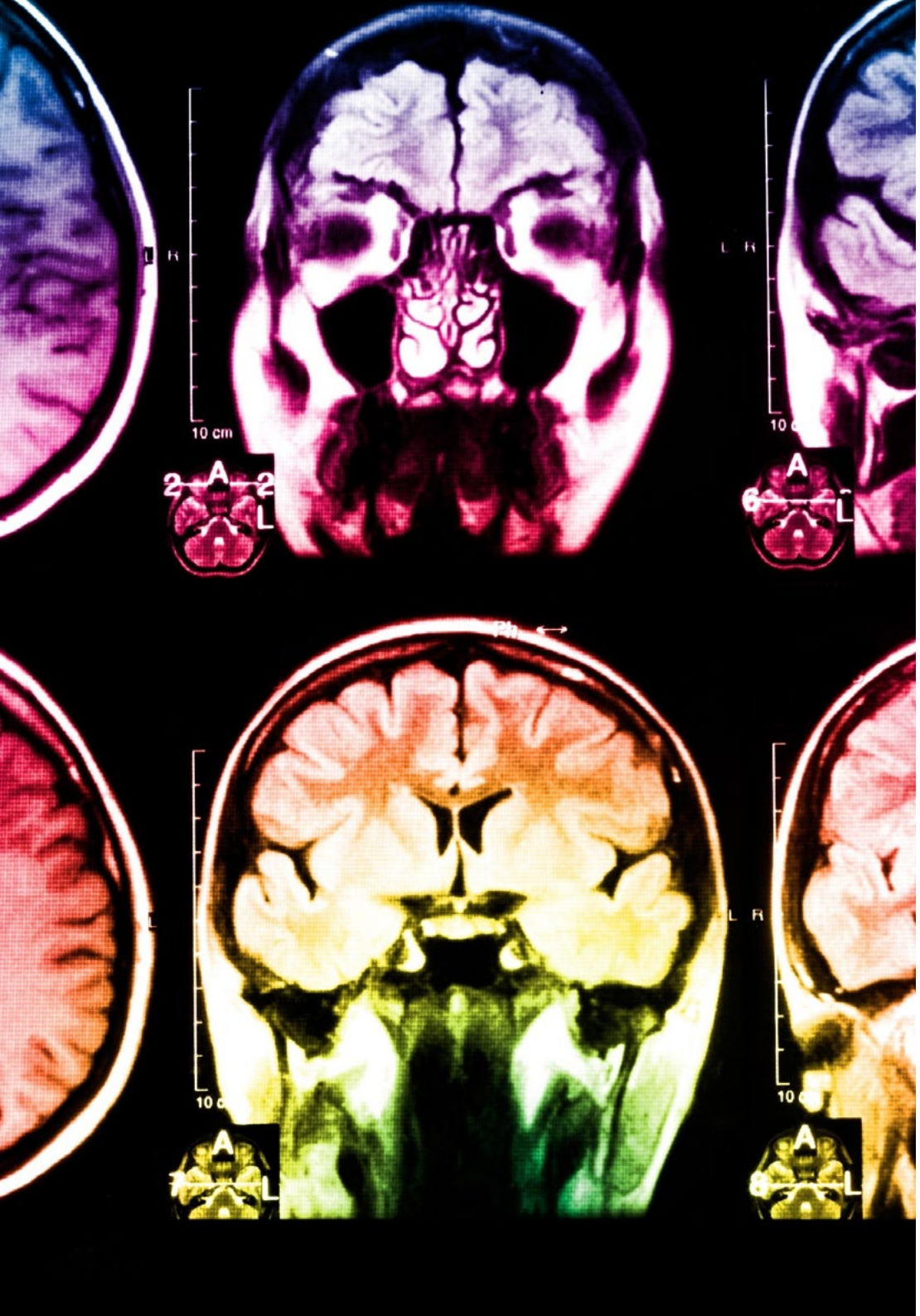
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

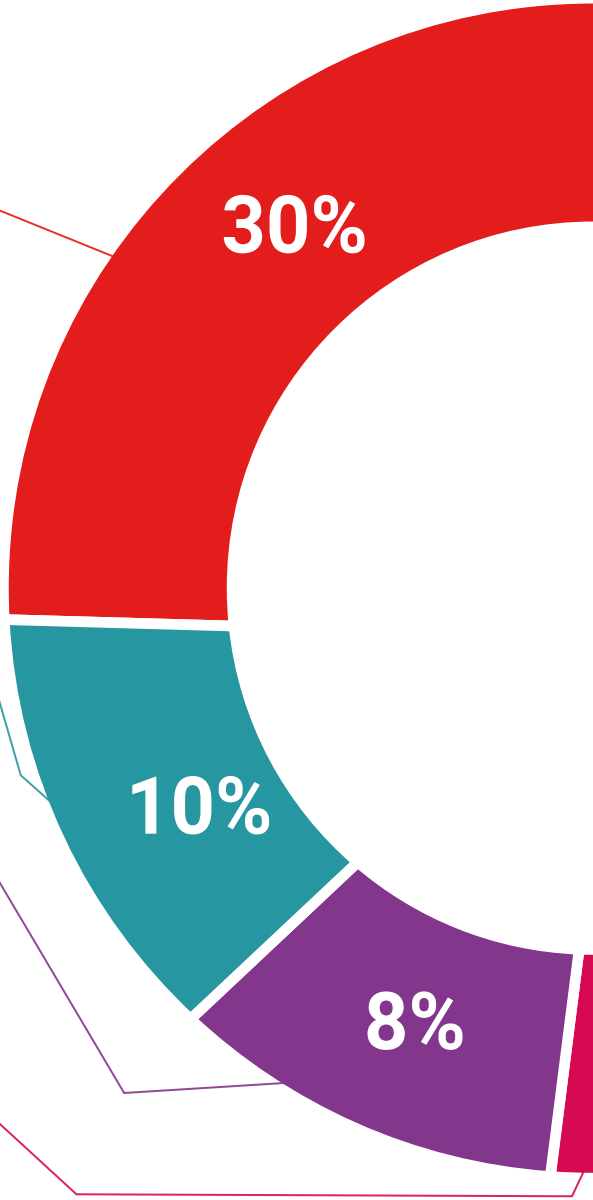
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

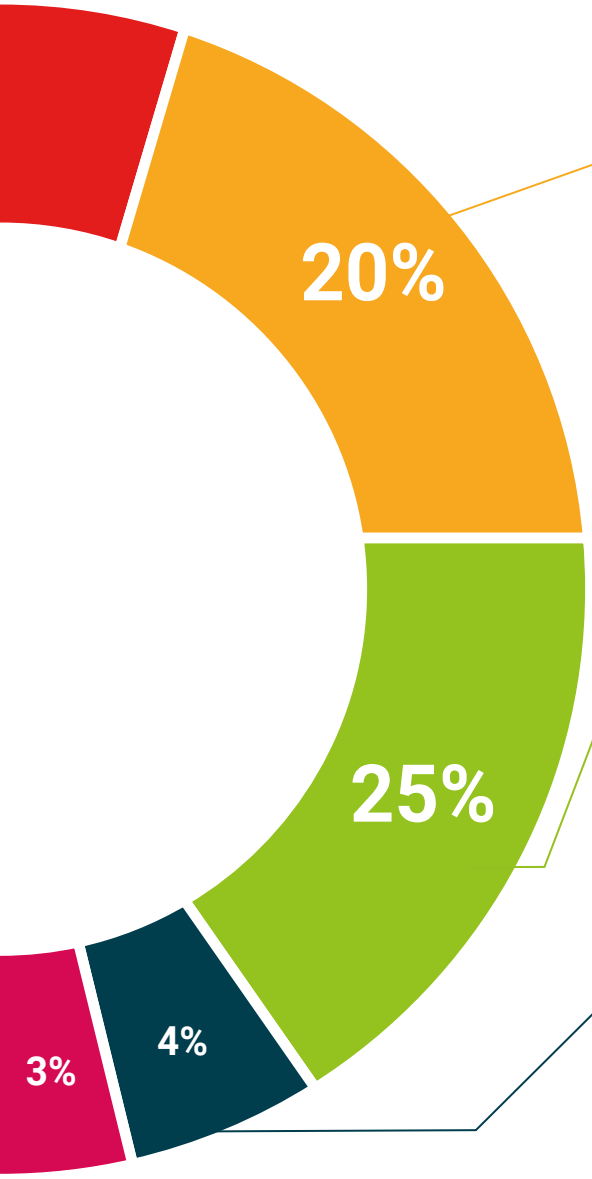
Übungen für Fertigkeiten und Kompetenzen

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 Cybersecurity Management (CISO, Chief Information Security Officer) 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 Cybersecurity Management (CISO, Chief Information Security Officer)** 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 Cybersecurity Management (CISO, Chief Information Security Officer)**

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

Cybersecurity Management (CISO, Chief Information Security Officer)

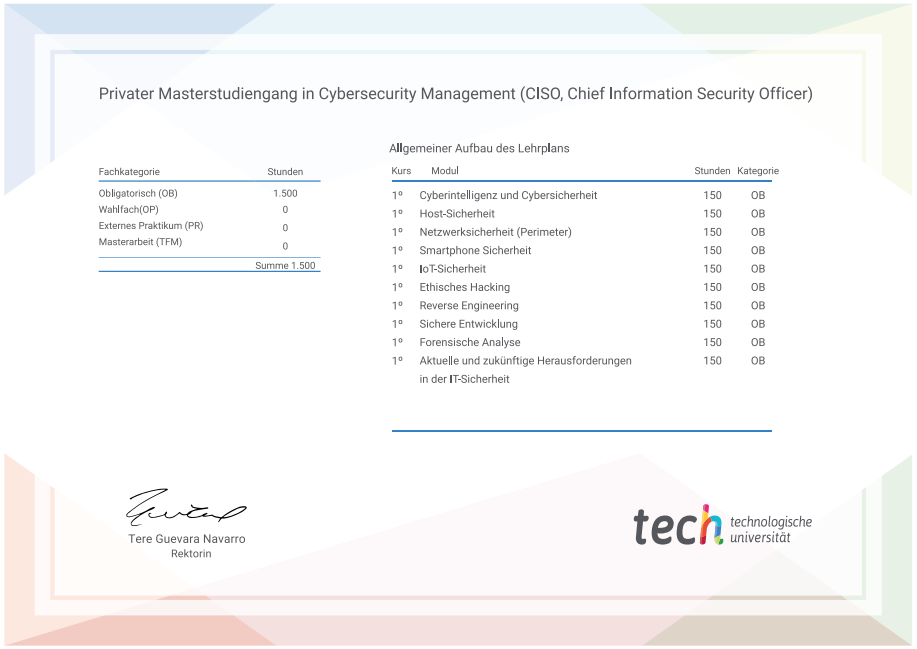
Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 1.500 Stunden, mit Anfangsdatum tt/mm/jjjj und Enddatum tt/mm/jjjj.

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 Cybersecurity Management (CISO, Chief Information Security Officer)

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
1°	Cyberintelligenz und Cybersicherheit	150	OB
1°	Host-Sicherheit	150	OB
1°	Netzwerksicherheit (Perimeter)	150	OB
1°	Smartphone Sicherheit	150	OB
1°	IoT-Sicherheit	150	OB
1°	Ethisches Hacking	150	OB
1°	Reverse Engineering	150	OB
1°	Sichere Entwicklung	150	OB
1°	Forensische Analyse	150	OB
1°	Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit	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

Cybersecurity Management (CISO, Chief Information Security Officer)

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

Privater Masterstudiengang

Cybersecurity Management (CISO, Chief Information Security Officer)

tech technologische universität