

Universitätsexperte Korrektive Cybersicherheit und Forensische Analyse





Universitätsexperte Korrektive Cybersicherheit und Forensische Analyse

- » Modalität: online
- » Dauer: 6 Monate
- » Qualifizierung: TECH Technologische Universität
- » Aufwand: 16 Std./Woche
- » Zeitplan: in Ihrem eigenen Tempo
- » Prüfungen: online

Internetzugang: www.techtitude.com/de/informatik/spezialisierung/spezialisierung-korrektive-cybersicherheit-forensische-analyse

Index

01

Präsentation

Seite 4

02

Ziele

Seite 8

03

Kursleitung

Seite 12

04

Struktur und Inhalt

Seite 18

05

Methodik

Seite 24

06

Qualifizierung

Seite 32

01

Präsentation

In einer Welt, die sich täglich verändert und weiterentwickelt, mit Technologien, die schnell auftauchen und übernommen werden, ohne ausgereift zu sein, müssen wir auf viele Herausforderungen vorbereitet sein und die Auswirkungen, die sie auf die Gesellschaft haben werden, vorhersehen können. Dieses Programm spezialisiert IT-Ingenieure darauf, einen Cybersicherheitsvorfall zu untersuchen, sobald er auftritt, und vermittelt ihnen das Wissen und die Mechanismen, um alle Informationen zu sammeln, zu analysieren und zu melden. Von dem Moment an, in dem ein Forensiker ein Szenario entdeckt und beschließt, auf nichtdestruktive Weise Beweise zu sammeln, benötigt er Richtlinien, um die aus verschiedenen Quellen gewonnenen Daten miteinander in Beziehung zu setzen und unwiderlegbare Schlussfolgerungen zu ziehen.





“

*Erlangen Sie die Fähigkeit,
die Schlüssel zu einem
Cybersicherheitsvorfall mit dem
neuesten Wissen über forensische
Expertise in diesem Bereich zu liefern"*

Im IT-Umfeld gibt es unterschiedliche Motivationen, die zur Anwendung verschiedener *Reverse Engineering*-Techniken führen, um eine Software, ein Kommunikationsprotokoll oder einen Algorithmus zu verstehen und genug darüber zu wissen.

Eine der bekanntesten Anwendungen des *Reverse Engineering* ist die Analyse von Malware, bei der verschiedene Techniken wie das *Sandboxing* eingesetzt werden, um die untersuchte Malware zu verstehen und kennenzulernen und so die Entwicklung von Software zu ermöglichen, die in der Lage ist, sie zu erkennen und ihr entgegenzuwirken, wie im Fall von Antivirensoftware, die mit Signaturen arbeitet.

Manchmal befindet sich die Schwachstelle nicht im Quellcode, sondern wird durch den *Compiler* eingeführt, der den Maschinencode erzeugt. Die Kenntnis des *Reverse Engineering* und damit der Art und Weise, wie wir den Maschinencode erhalten, ermöglicht es uns, diese Schwachstellen zu entdecken.

Es ist wichtig, die verschiedenen Szenarien zu kennen, die verschiedenen Technologien zu verstehen und in der Lage zu sein, sie in verschiedenen Sprachen zu erklären, je nachdem, an wen sich der Bericht richtet. Die Anzahl der verschiedenen Straftaten, mit denen sich ein forensischer Experte auseinandersetzen muss, bedeutet, dass er Fachwissen, Einsicht und Gelassenheit benötigt, um diese äußerst wichtige Aufgabe zu erfüllen, da das Urteil eines Prozesses von seiner korrekten Leistung abhängen kann.

Der Experte auf diesem Gebiet muss einen weiten und peripheren Blick haben, um nicht nur den Nutzen dieser Technologien zu erkennen, sondern auch den möglichen Schaden, den sie anrichten können. Dieses Programm bereitet die Studenten darauf vor, zu verstehen, was auf sie zukommt, wie es sich auf die heutigen Berufe auswirken kann, wie sie ausgeübt werden und was in der manchmal ungewissen Zukunft passieren kann.

Dieser **Universitätsexperte in Korrektive Cybersicherheit und Forensische Analyse** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- ♦ Die Entwicklung von Fallstudien, die von Experten präsentiert 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
- ♦ Sein 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



Verstehen Sie die Grundlagen und die Funktionsweise von Malware als Basis für die Entwicklung hocheffektiver Bewältigungsstrategien"

“

Dieser Universitätsexperte ist ganz auf die Praxis ausgerichtet und wird Ihre Fähigkeiten auf das Niveau eines Spezialisten bringen“

Zu den Dozenten des Programms gehören Experten aus der Branche, die ihre Berufserfahrung in diese Fortbildung einbringen, sowie renommierte Fachleute von Referenzgesellschaften und angesehenen Universitäten.

Die multimedialen Inhalte, die mit der neuesten Bildungstechnologie entwickelt wurden, werden der Fachkraft ein situierendes 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 Studiengangs konzentriert sich auf problemorientiertes Lernen, bei dem die Fachkraft versuchen muss, die verschiedenen Situationen aus der beruflichen Praxis zu lösen, die während des akademischen Programms auftreten. Zu diesem Zweck wird sie von einem innovativen interaktiven Videosystem unterstützt, das von renommierten Experten entwickelt wurde.

Eine Weiterbildung, die es Ihnen ermöglicht, als forensischer Experte für Cybersicherheit im juristischen Bereich tätig zu werden.

Ein hochqualifizierter Prozess, der so gestaltet ist, dass er überschaubar und flexibel ist, mit der interessantesten Methodik der Online-Bildung.



02 Ziele

Dieser Universitats­experte fordert die Fahigkeit der Studenten, sich schnell und einfach in diesem Bereich zurechtzufinden. Mit realistischen und hochinteressanten Zielen soll dieser Studienprozess die Studenten schrittweise zum Erwerb der theoretischen und praktischen Kenntnisse fuhren, die fur eine qualitativ hochwertige Intervention erforderlich sind. Auerdem werden transversale Kompetenzen entwickelt, die es ihnen ermoglichen, sich komplexen Situationen zu stellen, indem sie angepasste und prazise Antworten erarbeiten.



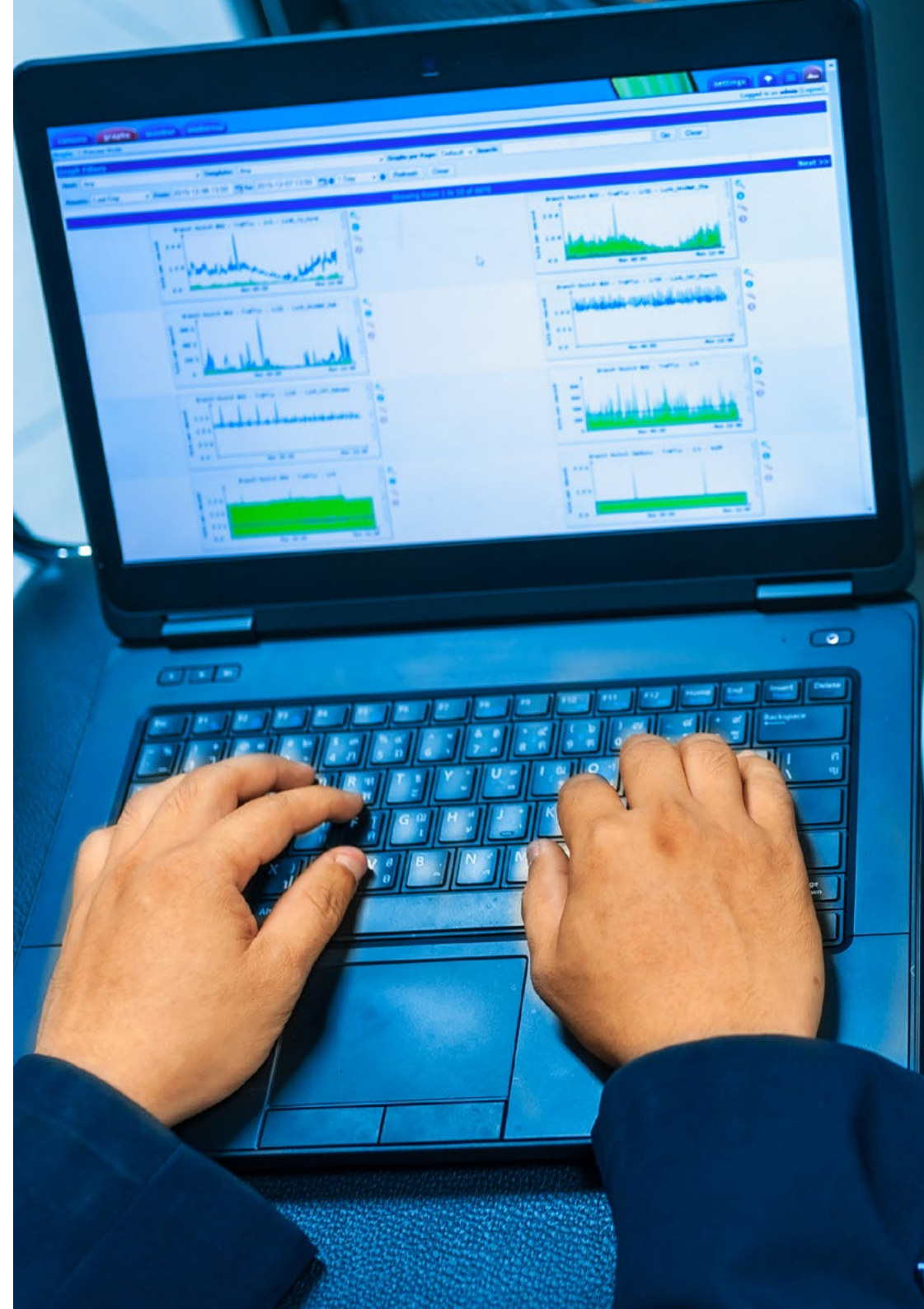
“

*Intensives Lernen in Korrektiver
Cybersicherheit und Forensischer
Analyse, das es Ihnen ermöglicht, Ihr
Arbeitsfeld in einem Bereich voller
Beschäftigungsmöglichkeiten zu erweitern”*



Allgemeine Ziele

- ◆ Analysieren von *Reverse Engineering* und verschiedenen Techniken
- ◆ Untersuchen der unterschiedlichen Architekturen und wie diese das *Reverse Engineering* beeinflussen
- ◆ Bestimmen, unter welchen Bedingungen verschiedene *Reverse Engineering*-Techniken eingesetzt werden sollen
- ◆ Anwenden von *Reverse Engineering* auf die Cybersicherheitsumgebung
- ◆ Sammeln aller vorhandenen Beweise und Daten, um einen forensischen Bericht zu erstellen
- ◆ Analysieren und Korrelieren der Daten in geeigneter Weise
- ◆ Aufbewahren der Beweise für einen forensischen Bericht
- ◆ Präsentieren des forensischen Berichts in angemessener Form
- ◆ 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. 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
- ◆ Entwicklung von Tools für die Malware-Analyse

Modul 2. 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 Systemlogs 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
- ◆ Entwickeln von Strategien für sichere Telearbeit

Modul 3. Aktuelle und zukünftige Herausforderungen in der IT-Sicherheit

- ◆ Untersuchen der Verwendung von Kryptowährungen, der Auswirkungen auf die Wirtschaft und der 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 Aufklärung der Bevölkerung über die richtige Nutzung von Technologien
- ◆ Erstellen von Fachwissen, um neue Sicherheitsherausforderungen zu bewältigen und Identitätsdiebstahl zu verhindern
- ◆ Entwickeln von Strategien für sichere Telearbeit



Erwerben Sie die Kompetenz, einen umfassenden und qualitativ hochwertigen Bericht zu erstellen und der zuständigen Behörde vorzulegen"

03

Kursleitung

Die Dozenten, die dieses Programm unterrichten, wurden aufgrund ihrer außergewöhnlichen Kompetenz in diesem Bereich ausgewählt. Sie verbinden technische und praktische Erfahrung mit Unterrichtserfahrung und bieten den Studenten erstklassige Unterstützung bei der Erreichung ihrer Ziele. Durch sie bietet das Programm die direkteste und unmittelbarste Sicht auf die realen Merkmale der Intervention in diesem Bereich und erreicht eine kontextuelle Vision von maximalem Interesse.



“

*Fachkundige Dozenten für
Cybersicherheit begleiten Sie in jeder
Phase des Studiums und vermitteln Ihnen
die realistischste Sicht auf diese Arbeit”*

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*, Nationales Referenzzentrum für IT und Telekommunikation in Getafe, Madrid
- ◆ Zertifizierte *E-Council*-Ausbilderin, Madrid
- ◆ Ausbilderin für die 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*), Universität der Balearischen Inseln
- ◆ Informatik-Ingenieurin, Universität von Alcalá de Henares, Madrid
- ◆ Masterstudiengang in DevOps: Docker und Kubernetes, Cas-Training, Madrid
- ◆ *Microsoft Azure Security Technologies*, *E-Council*, Madrid

Professoren

Hr. Redondo, Jesús Serrano

- ♦ Junior *FrontEnd*-Entwickler und Junior *Cybersecurity*-Techniker
- ♦ *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 Talente)


“

Eine anregende Reise zur beruflichen Weiterentwicklung, die Ihr Interesse und Ihre Motivation während der gesamten Fortbildung aufrechterhält”

04

Struktur und Inhalt

Dieser Universitätsexperte ist eine vollständige Analyse aller Wissensgebiete, die ein Profi, der sich mit Cybersicherheit beschäftigt, im Bereich der korrigierenden Cybersicherheit und der forensischen Expertise kennen muss. Zu diesem Zweck wurde er mit Blick auf den effizienten Erwerb von summativem Wissen strukturiert, das es ermöglicht, das Gelernte zu durchdringen und zu festigen, so dass die Studenten in der Lage sind, so schnell wie möglich zu intervenieren. Ein hochintensiver und qualitativ hochwertiger Kurs, der die Besten des Sektors fortbilden soll.



```
arg ) {  
    arg ) {  
        unique || !self.has( arg ) {  
            .push( arg );  
        }  
    }  
    else if ( arg && arg.length && jQuery.type( arg ) !== "string" ) {  
        // Inspect recursively  
        for ( var i = 0; i < arg.len(); i++ ) {  
            arg += "loading var" + i - 3;  
            add( arg );  
        }  
    }  
}
```

“

*Alle Konzepte der korrektiven
Cybersicherheit und der forensischen
Expertise werden auf strukturierte Weise
in einem auf Effizienz ausgerichteten
Studienansatz entwickelt”*

Modul 1. Reverse Engineering

- 1.1. *Compiler*
 - 1.1.1. Arten von Code
 - 1.1.2. *Compiler*-Phasen
 - 1.1.3. Symboltabelle
 - 1.1.4. Fehler-Handler
 - 1.1.5. GCC Compiler
- 1.2. Arten der *Compiler*-Analyse
 - 1.2.1. Lexikalische Analyse
 - 1.2.1.1. Terminologie
 - 1.2.1.2. Lexikalische Komponenten
 - 1.2.1.3. LEX Lexikalischer Analysator
 - 1.2.2. Syntaktische Analyse
 - 1.2.2.1. Kontextfreie Grammatiken
 - 1.2.2.2. Arten des *Parsing*
 - 1.2.2.2.1. *Top-down-Parsing*
 - 1.2.2.2.2. *Bottom-up-Parsing*
 - 1.2.2.3. Syntaktische Bäume und Ableitungen
 - 1.2.2.4. Arten von Parsern
 - 1.2.2.4.1. LR-Parser (*Left to Right*)
 - 1.2.2.4.2. LALR-Parser
 - 1.2.3. Semantische Analyse
 - 1.2.3.1. Attribut-Grammatiken
 - 1.2.3.2. S-Attribute
 - 1.2.3.3. L-Attribute
- 1.3. Montage Datenstrukturen
 - 1.3.1. Variablen
 - 1.3.2. Arrays
 - 1.3.3. Zeiger
 - 1.3.4. Strukturen
 - 1.3.5. Objekte
- 1.4. *Assembly Code*-Strukturen
 - 1.4.1. Auswahl-Strukturen
 - 1.4.1.1. *If, else if, Else*
 - 1.4.1.2. *Switch*
 - 1.4.2. Iterations-Strukturen
 - 1.4.2.1. *For*
 - 1.4.2.2. *While*
 - 1.4.2.3. Verwendung des *Break*
 - 1.4.3. Funktionen
- 1.5. x86-Hardware-Architektur
 - 1.5.1. x86-Prozessorarchitektur
 - 1.5.2. x86 Datenstrukturen
 - 1.5.3. x86 Code-Strukturen
- 1.6. ARM Hardware-Architektur
 - 1.6.1. ARM-Prozessorarchitektur
 - 1.6.2. ARM-Daten-Strukturen
 - 1.6.3. ARM-Code-Strukturen
- 1.7. Statische Code-Analyse
 - 1.7.1. Disassembler
 - 1.7.2. IDA
 - 1.7.3. Code-Rekonstrukteure
- 1.8. Dynamische Code-Analyse
 - 1.8.1. Verhaltensanalyse
 - 1.8.1.1. Kommunikation
 - 1.8.1.2. Überwachung
 - 1.8.2. Linux Code-*Debugger*
 - 1.8.3. Windows-Code-*Debugger*



- 1.9. *Sandbox*
 - 1.9.1. *Sandbox*-Architektur
 - 1.9.2. *Sandbox*-Umgehung
 - 1.9.3. Erkennungstechniken
 - 1.9.4. Ausweichtechniken
 - 1.9.5. Gegenmaßnahmen
 - 1.9.6. *Sandbox* in Linux
 - 1.9.7. *Sandbox* in Windows
 - 1.9.8. *Sandbox* in MacOS
 - 1.9.9. *Sandbox* in Android
- 1.10. Malware-Scans
 - 1.10.1. Methoden zur Analyse des Malware
 - 1.10.2. Techniken zur Verschleierung von Malware
 - 1.10.2.1. Ausführbare Verschleierung
 - 1.10.2.2. Einschränkung der Ausführungsumgebungen
 - 1.10.3. Tools zur Analyse des Malware

Modul 2. Forensische Analyse

- 2.1. Datenerfassung und Replikation
 - 2.1.1. Volatile Datenerfassung
 - 2.1.1.1. System-Informationen
 - 2.1.1.2. Netzwerk-Informationen
 - 2.1.1.3. Volatilität bestellen
 - 2.1.2. Statische Datenerfassung
 - 2.1.2.1. Erstellung eines doppelten Bildes
 - 2.1.2.2. Erstellung eines Dokuments für die Überwachungskette
 - 2.1.3. Methoden zur Validierung der erfassten Daten
 - 2.1.3.1. Methoden für Linux
 - 2.1.3.2. Methoden für Windows

- 2.2. Bewertung und Beseitigung von Anti-Forensik-Techniken
 - 2.2.1. Ziele der forensischen Techniken
 - 2.2.2. Löschung von Daten
 - 2.2.2.1. Löschung von Daten und Dateien
 - 2.2.2.2. Dateiwiederherstellung
 - 2.2.2.3. Wiederherstellung von gelöschten Partitionen
 - 2.2.3. Passwortschutz
 - 2.2.4. Steganographie
 - 2.2.5. Sicheres Löschen von Geräten
 - 2.2.6. Verschlüsselung
- 2.3. Betriebssystem-Forensik
 - 2.3.1. Windows-Forensik
 - 2.3.2. Linux-Forensik
 - 2.3.3. Mac-Forensik
- 2.4. Netzwerk-Forensik
 - 2.4.1. Log-Analyse
 - 2.4.2. Korrelation der Daten
 - 2.4.3. Netzwerk-Untersuchung
 - 2.4.4. Schritte der forensischen Netzwerkanalyse
- 2.5. Web-Forensik
 - 2.5.1. Untersuchung von Webangriffen
 - 2.5.2. Angriffserkennung
 - 2.5.3. Standort der IP-Adresse
- 2.6. Datenbank-Forensik
 - 2.6.1. MSSQL-Forensik
 - 2.6.2. MySQL-Forensik
 - 2.6.3. PostgreSQL-Forensik
 - 2.6.4. MongoDB-Forensik
- 2.7. Cloud-Forensik
 - 2.7.1. Arten von Cloud-Verbrechen
 - 2.7.1.1. Cloud als Thema
 - 2.7.1.2. Cloud als Objekt
 - 2.7.1.3. Cloud als Werkzeug
 - 2.7.2. Herausforderungen der Cloud-Forensik
 - 2.7.3. Untersuchung von Cloud-Speicherdiensten
 - 2.7.4. Forensische Analyse-Tools für die Cloud
- 2.8. Untersuchung von E-Mail-Verbrechen
 - 2.8.1. Mail-Systeme
 - 2.8.1.1. Mail Clients
 - 2.8.1.2. Mail-Server
 - 2.8.1.3. SMTP-Server
 - 2.8.1.4. POP3-Server
 - 2.8.1.5. IMAP4-Server
 - 2.8.2. Mail-Verbrechen
 - 2.8.3. Mail-Nachricht
 - 2.8.3.1. Standard-Kopfzeilen
 - 2.8.3.2. Erweiterte Kopfzeilen
 - 2.8.4. Schritte bei der Untersuchung dieser Verbrechen
 - 2.8.5. Tools für die E-Mail-Forensik
- 2.9. Mobile forensische Analyse
 - 2.9.1. Zellulare Netzwerke
 - 2.9.1.1. Arten von Netzwerken
 - 2.9.1.2. CDR Inhalt
 - 2.9.2. Subscriber Identity Module (SIM)
 - 2.9.3. Logische Akquisition
 - 2.9.4. Physische Akquisition
 - 2.9.5. Dateisystem-Erfassung
- 2.10. Forensische Berichte schreiben und einreichen
 - 2.10.1. Wichtige Aspekte eines forensischen Berichts
 - 2.10.2. Klassifizierung und Arten von Berichten
 - 2.10.3. Leitfaden zum Schreiben eines Berichts
 - 2.10.4. Präsentation des Berichts
 - 2.10.4.1. Vorbereitung auf die Zeugenaussage
 - 2.10.4.2. Hinterlegung
 - 2.10.4.3. Der Umgang mit den Medien

Modul 3. Aktuelle und zukünftige Herausforderungen in der Informationssicherheit

- 3.1. *Blockchain*-Technologie
 - 3.1.1. Anwendungsbereiche
 - 3.1.2. Garantie der Vertraulichkeit
 - 3.1.3. Garantie der Nichtabstreitbarkeit
- 3.2. Digitales Geld
 - 3.2.1. Bitcoins
 - 3.2.2. Kryptowährungen
 - 3.2.3. Schürfen von Kryptowährungen
 - 3.2.4. Schneeballsysteme
 - 3.2.5. Andere mögliche Verbrechen und Probleme
- 3.3. *Deepfake*
 - 3.3.1. Auswirkungen auf die Medien
 - 3.3.2. Gefahren für die Gesellschaft
 - 3.3.3. Erkennungsmechanismen
- 3.4. Die Zukunft der künstlichen Intelligenz
 - 3.4.1. Künstliche Intelligenz und kognitives *Computing*
 - 3.4.2. Anwendungen zur Vereinfachung des Kundendienstes
- 3.5. Digitale Privatsphäre
 - 3.5.1. Wert der Daten im Netzwerk
 - 3.5.2. Verwendung von Daten im Netzwerk
 - 3.5.3. Datenschutz und Verwaltung digitaler Identitäten
- 3.6. Cyber-Konflikte, Cyber-Kriminelle und Cyber-Angriffe
 - 3.6.1. Auswirkungen der Cybersicherheit auf internationale Konflikte
 - 3.6.2. Folgen von Cyberangriffen auf die allgemeine Bevölkerung
 - 3.6.3. Arten von Cyber-Kriminellen. Schutzmaßnahmen
- 3.7. Telearbeit
 - 3.7.1. Revolution der Telearbeit während und nach COVID-19
 - 3.7.2. Engpässe beim Zugang
 - 3.7.3. Variation der Angriffsfläche
 - 3.7.4. Bedürfnisse der Arbeiter
- 3.8. Aufkommende *Wireless*-Technologien
 - 3.8.1. WPA3
 - 3.8.2. 5G
 - 3.8.3. Millimeter-Wellen
 - 3.8.4. Trend zu "*Get Smart*" anstelle von "*Get More*"
- 3.9. Künftige Adressierung in Netzwerken
 - 3.9.1. Aktuelle Probleme mit der IP-Adressierung
 - 3.9.2. IPv6
 - 3.9.3. IPv4+
 - 3.9.4. Vorteile von IPv4+ gegenüber IPv4
 - 3.9.5. Vorteile von IPv6 gegenüber IPv4
- 3.10. Die Herausforderung, das Bewusstsein für eine frühzeitige und kontinuierliche Schulung der Bevölkerung zu schärfen
 - 3.10.1. Aktuelle Strategien der Regierung
 - 3.10.2. Der Widerstand der Menschen gegen das Lernen
 - 3.10.3. Ausbildungspläne, die von den Unternehmen angenommen werden müssen



Ein hochwirksamer Lehrplan für Ihre Fähigkeiten, der es Ihnen ermöglicht, mit modernsten Mitteln effizient in die Bereiche korrigierende Cybersicherheit und forensische Analyse einzugreifen"

05 Methodik

Dieses Fortbildungsprogramm bietet eine andere Art des Lernens. Unsere Methodik wird durch eine zyklische Lernmethode entwickelt: **das Relearning**.

Dieses Lehrsystem wird z. B. an den renommiertesten medizinischen Fakultäten der Welt angewandt und wird von wichtigen Publikationen wie dem **New England Journal of Medicine** als eines der effektivsten angesehen.



“

Entdecken Sie Relearning, ein System, das das herkömmliche lineare Lernen aufgibt 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 die Grundlagen der traditionellen Universitäten in der ganzen Welt verschiebt”



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



Die Studenten lernen durch gemeinschaftliche Aktivitäten und reale Fälle die Lösung komplexer Situationen in realen Geschäftsumgebungen.

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 die Jurastudenten das Recht nicht nur anhand theoretischer Inhalte erlernen, sondern ihnen reale, komplexe Situationen vorlegen, damit sie fundierte Entscheidungen treffen und Werturteile darüber fällen können, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard eingeführt.

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 Studierenden mit mehreren realen Fällen konfrontiert. Sie müssen Ihr gesamtes Wissen integrieren, recherchieren, argumentieren und Ihre Ideen und Entscheidungen verteidigen.

Relearning Methodik

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 auszubilden. 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 Online-Universität in Spanisch 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 ausgebildet. 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 Ihr Fachgebiet 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 neurokognitiven kontextabhängigen E-Learnings 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 TECH-Online-Arbeitsmethode zu schaffen. Und das alles mit den neuesten Techniken, die dem Studenten qualitativ hochwertige Stücke aus jedem einzelnen Material zur Verfügung stellen.



Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

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



Fertigkeiten und Kompetenzen Praktiken

Sie werden Aktivitäten durchführen, um spezifische Kompetenzen und Fertigkeiten in jedem Fachbereich zu entwickeln. Praktiken und Dynamiken 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 haben die Studenten Zugang zu allem, was sie für ihre Ausbildung benötigen.





Fallstudien

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.



Prüfung und Nachprüfung

Die Kenntnisse der Studenten werden während des gesamten Programms regelmäßig durch Bewertungs- und Selbsteinschätzungsaktivitäten und -übungen beurteilt und neu bewertet, so dass die Studenten überprüfen können, wie sie ihre Ziele erreichen.



06

Qualifizierung

Der Universitätsexperte in Korrektive Cybersicherheit und Forensische Analyse 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 **Universitätsexperte in Korrektive Cybersicherheit und Forensische Analyse** enthält das vollständigste und aktuellste Programm auf dem Markt.

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

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

Titel: **Universitätsexperte in Korrektive Cybersicherheit und Forensische Analyse**

Anzahl der offiziellen Arbeitsstunden: **450 Std.**



*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.

zukunft

gesundheit vertrauen menschen
erziehung information tutoeren
garantie akkreditierung unterricht
institutionen technologie lernen
gemeinschaft verpflichtung
persönliche betreuung innovation
wissen gegenwart qualität
online-Ausbildung
entwicklung institut
virtuelles Klassenzimmer

tech technologische
universität

Universitätsexperte
Korrektive Cybersicherheit
und Forensische Analyse

- » Modalität: online
- » Dauer: 6 Monate
- » Qualifizierung: TECH Technologische Universität
- » Aufwand: 16 Std./Woche
- » Zeitplan: in Ihrem eigenen Tempo
- » Prüfungen: online

Universitätsexperte

Korrektive Cybersicherheit und Forensische Analyse