

محاضرة جامعية
تحليل البرمجيات الخبيثة
Malware وتطويرها



الجامعة
التكنولوجية
tech

محاضرة جامعية تحليل البرمجيات الخبيثة Malware وتطويرها

- « طريقة التدريس: أونلاين
- « مدة الدراسة: 6 اسابيع
- « المؤهل الجامعي من: TECH الجامعة التكنولوجية
- « مواعيد الدراسة: وفقاً لوتيرتك الخاصة
- « الامتحانات: أونلاين

رابط الدخول إلى الموقع الإلكتروني: www.techtute.com/ae/information-technology/postgraduate-certificate/malware-analysis-development

الفهرس

01

المقدمة

صفحة 4

02

الأهداف

صفحة 8

03

هكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

صفحة 12

04

الهكل والمحتوى

صفحة 16

05

المنهجية

صفحة 20

06

المؤهل العلمي

صفحة 28

المقدمة

في بيئة رقمية تعتمد فيها أصول الأعمال بشكل حاسم على الأمن الإلكتروني، يمثل التهديد المستمر للبرمجيات الخبيثة تحدياً كبيراً. في هذا الصدد، يؤكد انتشار الهجمات الخبيثة على الحاجة الملحة لوجود متخصصين مدربين تدريباً عالياً في هذا المجال. وفي هذا الصدد، يتناول المنهج الدراسي الحاجة الملحة إلى خبراء لا يفهمون تعقيدات التهديدات الرقمية فحسب، بل يمكنهم أيضاً تصميم استراتيجيات استباقية للكشف عنها والتخفيف من حدتها. سيتعلم الخريجون الأدوات الأساسية لحماية سلامة الأنظمة في بيئة الأعمال التي تتزايد فيها الرقمنة. بفضل مرونة وضع 100% عبر الإنترنت، تضمن هذه المحاضرة الجامعية إمكانية الوصول والتحديث المستمر اللازمين لمواجهة التحديات المتغيرة للفضاء الإلكتروني.

كن خبيرًا في مجال البرمجيات الخبيثة Malware باستخدام تقنيات التحليل الديناميكي المبتكرة بفضل هذا البرنامج الحصري 100% عبر الإنترنت"



هذه المحاضرة الجامعية في تحليل البرمجيات الخبيثة Malware وتطويرها تحتوي على البرنامج العلمي الأكثر اكتمالا وحدثا في السوق. أبرز خصائصها هي:

- ♦ تطوير دراسات الحالة التي يقدمها خبراء في تحليل البرمجيات الخبيثة Malware وتطويرها.
- ♦ جمع المعلومات المحدثة والتطبيقية المتعلقة بالتخصصات الضرورية من أجل الممارسة المهنية، والتي تشكل جزءا من المحتويات الرسومية والتخطيطية والعملية البارزة التي صمم بها
- ♦ التمارين العملية حيث يمكن إجراء عملية التقييم الذاتي لتحسين التعلم
- ♦ تركيزه على المنهجيات المبتكرة
- ♦ كل هذا سيتم استكماله بدروس نظرية وأسئلة للخبراء ومنتديات مناقشة حول القضايا المثيرة للجدل وأعمال التفكير الفردية
- ♦ توفر المحتوى من أي جهاز ثابت أو محمول متصل بالإنترنت

في مشهد الأمن السيبراني اليوم، وصل تعقيد التهديدات الإلكترونية إلى مستويات غير مسبوقة، مما أدى إلى تزايد الطلب على المتخصصين في تحليل البرمجيات الخبيثة Malware وتطويرها. إن التطور المستمر للتكتيكات الخبيثة يتطلب استجابة ديناميكية مماثلة من خبراء الأمن السيبراني. وفي هذا السياق، يبرز برنامج TECH الحالي كحل شامل لتلبية هذه الاحتياجات. صُمم المنهج لتزويد الطلاب بالمعرفة المتقدمة، ويتراوح المنهج بين الفهم الشامل لطبيعة البرمجيات الخبيثة وتقييم أدوات مكافحة البرمجيات الخبيثة. يعمل هذا النهج الشامل على إعداد المهنيين للتعامل مع التهديدات الحالية والمستقبلية.

إن برنامج تحليل البرمجيات الخبيثة Malware وتطويرها الذي تقدمه TECH هو خلاصة معرفية قوية تغطي مختلف أبعاد عالم البرمجيات الخبيثة. سوف يستكشف الخريجون بعمق مختلف أشكال البرمجيات الخبيثة وأهدافها، ويكتسبون معرفة متقدمة بطبيعتها ووظائفها وسلوكها. يتعمق البرنامج في تحليل الطب الشرعي المطبق على البرمجيات الخبيثة، ويزود الطلاب بالمهارات اللازمة لتحديد مؤشرات الاختراق (IoC) وأنماط الهجوم، وهو أمر بالغ الأهمية للكشف المبكر والاستجابة الفعالة للحوادث الأمنية. بالإضافة إلى ذلك، يركز المسار على تطوير مهارات محددة لتقييم واختيار أدوات مكافحة البرمجيات الخبيثة. سيتعلم الطلاب كيفية تمييز فعالية هذه الأدوات وقابليتها للتكيف مع بيئات معينة، وهو أمر ضروري في تنفيذ استراتيجيات الدفاع الفعالة.

بعد هذا البرنامج الجامعي مقترحاً تدريباً فريداً من نوعه بفضل نهجه المبتكر والقابل للتكيف. يضمن نمط التعليم عبر 100% عبر الإنترنت ومنهجية إعادة التعلم Relearning عبر الإنترنت تجربة تعليمية مرنة وفعالة، مما يسمح للمهنيين بالتقدم في حياتهم المهنية دون انقطاع والتكيف باستمرار مع المتطلبات المتغيرة لمجال الأمن السيبراني.



سوف تتقن تحليل المكالمات باستخدام API monitor في 6 أسابيع فقط من أفضل تدريب عبر الإنترنت"

ستصل إلى نظام تعليمي يعتمد على التكرار،
مع التدريس الطبيعي والتقدمي في جميع
أنحاء المنهج الدراسي بأكمله"

سوف تتعمق أكثر في التعقيم على Strings
امنح حياتك المهنية الدفعة التي تحتاجها!

”
سوف تتعلم كيفية إنشاء رموز Shellcode في
الجامعة الأفضل تقييماً في العالم من قبل طلابها
وفقاً لمنصة 5/4.9 Trustpilot"

يضم البرنامج في هيئة التدريس متخصصين في هذا القطاع الذين يجلبون خبراتهم العملية إلى هذا التدريب، بالإضافة إلى متخصصين معترف بهم من المجتمعات الرائدة والجامعات المرموقة.

سيتيح محتوى البرنامج المتعدد الوسائط، والذي صيغ بأحدث التقنيات التعليمية، للمهني التعلم السياقي والموقعي، أي في بيئة محاكاة توفر تدريباً غامراً مبرمجاً للتدريب في حالات حقيقية.

يركز تصميم هذا البرنامج على التعلّم القائم على حل المشكلات، والذي يجب على المهني من خلاله محاولة حل مختلف مواقف الممارسة المهنية التي تنشأ على مدار العام الدراسي. للقيام بذلك، سيحصل على مساعدة من نظام فيديو تفاعلي مبتكر من قبل خبراء مشهورين.

الأهداف

الهدف الرئيسي من هذا المنهج هو تمكين الخريجين من إتقان المعرفة المتقدمة بطبيعة البرمجيات الخبيثة ووظائفها وسلوكها. سيتعرف الطلاب خلال البرنامج على الأشكال المختلفة للبرمجيات الخبيثة وأهدافها، مما يمكنهم من تحليل وتطوير استراتيجيات دفاعية فعالة في مجال الأمن السيبراني. يسعى هذا النهج الشامل أيضًا إلى تدريب المهنيين القادرين على مواجهة التحديات الناشئة في الكشف عن تهديدات البرمجيات الخبيثة في البيئات الرقمية المعقدة وتحليلها والتخفيف من حدتها. وبالإضافة إلى ذلك، فإن استخدام منهجية التعلم عبر 100% عبر الإنترنت يجعل التعلم أكثر مرونة، مما يتيح إمكانية الوصول إلى أي وقت ومكان.

ستحقق أهدافك بفضل أدوات التدريس الخاصة
بـ TECH، بما في ذلك مقاطع الفيديو التفسيرية
والملخصات التفاعلية"



الأهداف العامة



- ♦ اكتساب مهارات متقدمة في اختبار الاختراق ومحاكاة فريق الشبكة، ومعالجة وتحديد واستغلال نقاط الضعف في الأنظمة والشبكات
- ♦ تطوير المهارات القيادية لتنسيق الفرق المتخصصة في الأمن السيبراني الهجومي، وتحسين تنفيذ مشاريع فريق الاختبار الخامس وفريق الشبكة
- ♦ تطوير المهارات في تحليل البرمجيات الخبيثة Malware وتطويرها وفهم وظائفها وتطبيق الاستراتيجيات الدفاعية والتعليمية
- ♦ نقل مهارات التواصل من خلال إنتاج تقارير تقنية وتنفيذية مفصلة، وعرض النتائج بفعالية على الجمهور التقني والتنفيذي
- ♦ تعزيز الممارسة الأخلاقية والمسؤولية في مجال الأمن السيبراني، مع مراعاة المبادئ الأخلاقية والقانونية في جميع الأنشطة



هل ترغب في تحقيق قفزة نوعية في حياتك المهنية؟ مع TECH ستكتسب مهارات في التحليل الجنائي المطبق على البرمجيات الخبيثة "malware"

الأهداف المحددة



- ♦ اكتساب معرفة متقدمة بطبيعة البرمجيات الخبيثة ووظائفها وسلوكها، وفهم أشكالها وأهدافها المختلفة.
- ♦ تطوير المهارات في التحليل الجنائي المطبق على البرمجيات الخبيثة، مما يتيح تحديد مؤشرات الاختراق (IoC) وأنماط الهجوم
- ♦ تعلّم استراتيجيات الكشف الفعّال عن البرمجيات الخبيثة والوقاية منها، بما في ذلك نشر حلول الأمان المتقدمة
- ♦ تعريف المتعلم بتطوير البرمجيات الخبيثة لأغراض تعليمية ودفاعية، مما يتيح فهماً شاملاً للتكتيكات التي يستخدمها المهاجمون
- ♦ تعزيز الممارسات الأخلاقية والقانونية في تحليل البرمجيات الخبيثة Malware وتطويرها، وضمان النزاهة والمسؤولية في جميع الأنشطة
- ♦ تطبيق المعرفة النظرية في بيئات المحاكاة، والمشاركة في التدريبات العملية لفهم الهجمات الخبيثة والتصدي لها
- ♦ تطوير المهارات اللازمة لتقييم واختيار الأدوات الأمنية لمكافحة البرمجيات الخبيثة، مع مراعاة فعاليتها وقدرتها على التكيف مع بيئات محددة
- ♦ تعرّف على كيفية تنفيذ إجراءات فعّالة للتخفيف من حدة التهديدات الخبيثة، والحد من تأثير وانتشار البرمجيات الخبيثة على الأنظمة والشبكات
- ♦ تعزيز التعاون الفعال مع فرق الأمن، وتكامل الاستراتيجيات والجهود للحماية من تهديدات البرمجيات الخبيثة



هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

يضم برنامج تحليل البرمجيات الخبيثة Malware وتطويرها هيئة تدريس مؤهلة بشكل استثنائي. ولهذا الغرض، اختارت TECH خبراء ذوي الخبرة والمكانة المعترف بها في الشركات الرائدة في قطاع الأمن السيبراني. لا يقتصر دور هيئة التدريس التي تتألف من كبار المتخصصين على تقديم خبراتهم العملية في تحليل البرمجيات الخبيثة Malware وتطويرها فحسب، بل أيضًا التزامهم بتدريب المتخصصين في المستقبل، مما يضمن تعليماً حديثاً يتماشى مع المتطلبات والتحديات الحالية في مجال الأمن السيبراني.



احصل على تحديث في تكوين الأجهزة الافتراضية
snapshotsg من أفضل الخبراء في هذا المجال.
ابدأ مسيرتك المهنية مع TECH!"



هيكـل الإدارة

أ. Gómez Pintado, Carlos

- ♦ مدير فريق الأمن السيبراني والشبكات Cipherbit في Grupo Oesfa
- ♦ مستشار *Advisor* إداري *Investorg* في تطبيق Wesson App
- ♦ خريج هندسة البرمجيات وتقنيات مجتمع المعلومات، جامعة مدريد التقنية السياسية
- ♦ التعاون مع المؤسسات التعليمية لتطوير دورات تدريبية عالية المستوى في مجال الأمن السيبراني



الأساتذة

أ. González Sanz, Marco

- ♦ مستشار الأمن السيبراني في Cipherbit
- ♦ eLearnSecurity Certified eXploit Developer
- ♦ Offensive Security Certified Professional
- ♦ Offensive Security Wireless Professional
- ♦ Virtual Hacking Labs Plus
- ♦ بكالوريوس هندسة البرمجيات من جامعة بوليتكنيك مدريد



الهيكل والمحتوى

سيوفر هذا البرنامج الجامعي للطلاب فرصة التعمق في عالم البرمجيات الخبيثة، مع التركيز على تطويرها لأغراض تعليمية ودفاعية. سيتناول الخريجون خلال المساق تعقيدات البرمجيات الخبيثة، مما يتيح فهمًا تفصيليًا للتكتيكات التي يستخدمها المهاجمون. في هذا الصدد، لا يعزز النهج المتوازن للمناهج الدراسية اكتساب المعرفة المتقدمة في تحليل البرمجيات الخبيثة فحسب، بل يمكّن الطلاب أيضاً من تطوير استراتيجيات دفاعية أساسية في مجال الأمن السيبراني.



ستحصل على منهج دراسي صممه هيئة تدريس مشهورة، مما سيضمن التعلم الناجح"

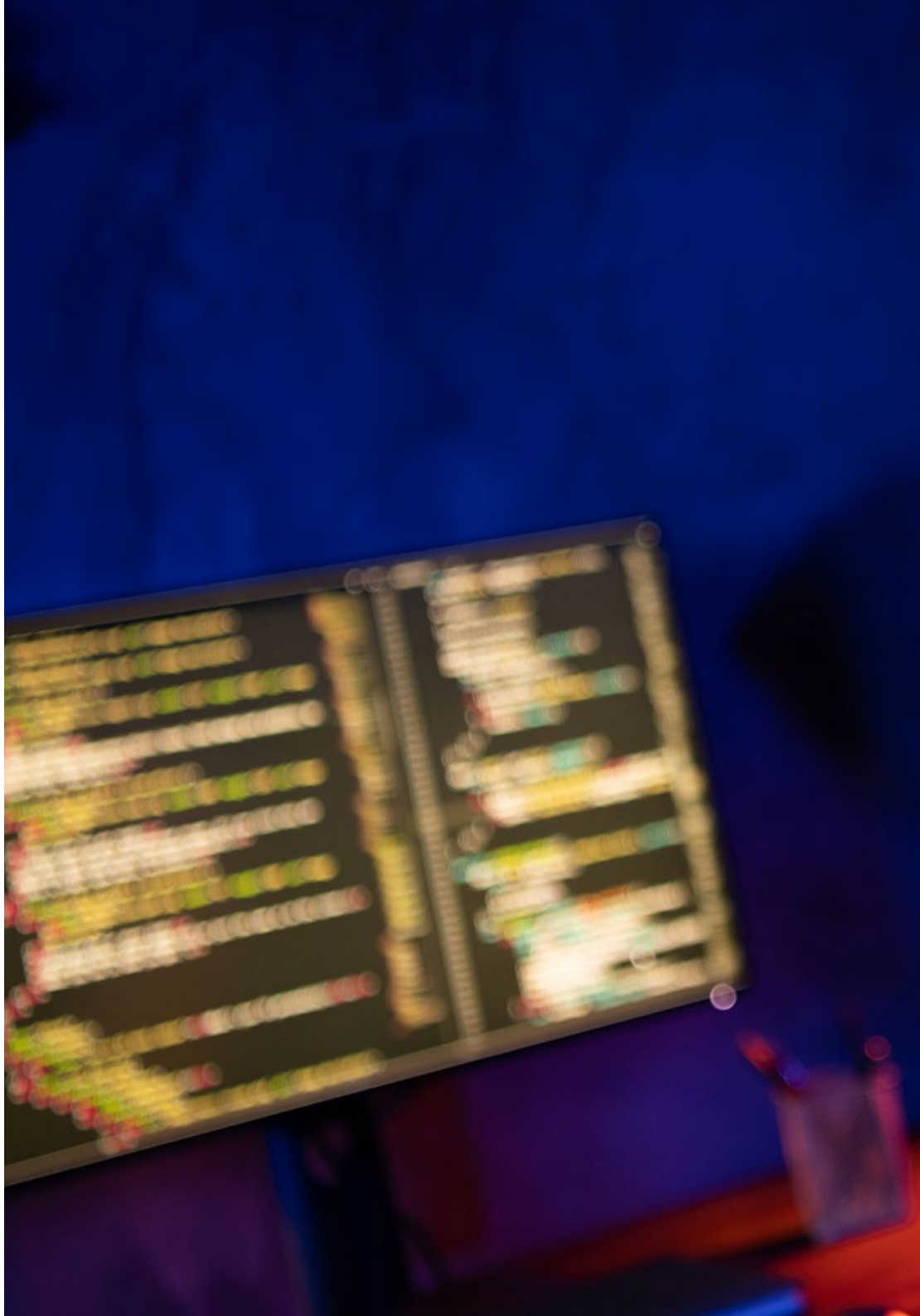


الوحدة 1. تحليل البرمجيات الخبيثة Malware وتطويرها

- 1.1 تحليل البرمجيات الخبيثة Malware وتطويرها
 - 1.1.1 تاريخ وتطور البرمجيات الخبيثة Malware
 - 2.1.1 تصنيف وأنواع البرمجيات الخبيثة Malware
 - 3.1.1 تحليل البرامج الخبيثة Malware
 - 4.1.1 تطوير البرمجيات الخبيثة Malware
- 2.1 تجهيز المحيط
 - 1.2.1 تهيئة الأجهزة الافتراضية و Snapshots
 - 2.2.1 أدوات تحليل البرمجيات الخبيثة Malware
 - 3.2.1 أدوات تطوير البرمجيات الخبيثة Malware
- 3.1 أساسيات الويندوز
 - 1.3.1 تنسيق ملف PE (محمول قابل للتفيد)
 - 2.3.1 العمليات والمسارات
 - 3.3.1 نظام الملفات والسجل
 - 4.3.1 Windows Defender
- 4.1 تقنيات البرمجيات الخبيثة Malware الأساسية
 - 1.4.1 خلق أكواد Shellcode
 - 2.4.1 تشغيل Shellcode في القرص الصلب
 - 3.4.1 القرص مقابل الذاكرة
 - 4.4.1 تشغيل Shellcode في الذاكرة
- 5.1 تقنيات البرمجيات الخبيثة Malware الوسيطة
 - 1.5.1 الثبات على الويندوز
 - 2.5.1 مجلد البدء
 - 3.5.1 مفاتيح السجل
 - 4.5.1 شاشات التوقف
- 6.1 تقنيات البرمجيات الخبيثة Malware لمتقدمة
 - 1.6.1 تشفير (XOR) Shellcode
 - 2.6.1 تشفير (RSA) Shellcode
 - 3.6.1 تشويش Strings
 - 4.6.1 حقن المعالجة

- 7.1 التحليل الثابت للبرمجيات الخبيثة
 - 1.7.1.1 تحليل Packers مع (Detect It Easy) DIE
 - 2.7.1 تحليل المقاطع باستخدام PE-Bear
 - 3.7.1 فك التجميع مع Ghidra
- 8.1 التحليل الديناميكي للبرمجيات الخبيثة
 - 1.8.1 مراقبة السلوك مع Process Hacker
 - 2.8.1 تحليل المكالمات API Monitor
 - 3.8.1 تحليل تغييرات السجل Regshot
 - 4.8.1 مراقبة طلبات الشبكة باستخدام TCPView
- 9.1 التحليل في .NET
 - 1.9.1 مقدمة في .NET
 - 2.9.1 فك التجميع باستخدام dnSpy
 - 3.9.1 تصحيح الأخطاء باستخدام dnSpy
- 10.1 تحليل البرمجيات الخبيثة Malware الحقيقية
 - 1.10.1 تجهيز المحيط
 - 2.10.1 التحليل الثابت للبرمجيات الخبيثة Malware
 - 3.10.1 التحليل الديناميكي للبرمجيات الخبيثة
 - 4.10.1 إنشاء قواعد YARA

لا تفوت فرصة تعزيز حياتك المهنية
من خلال هذا البرنامج المبتكر



المنهجية

يقدم هذا البرنامج التدريبي طريقة مختلفة للتعلم. فقد تم تطوير منهجيتنا من خلال أسلوب التعليم المرتكز على التكرار: **el Relearning** أو ما يعرف بمنهجية إعادة التعلم. يتم استخدام نظام التدريس هذا، على سبيل المثال، في أكثر كليات الطب شهرة في العالم، وقد تم اعتباره أحد أكثر المناهج فعالية في المنشورات ذات الصلة مثل مجلة نيو إنجلند الطبية *New England Journal of Medicine*.





اكتشف منهجية Relearning (منهجية إعادة التعلم)، وهي نظام يتخلى عن التعلم الخطي التقليدي ليأخذك عبر أنظمة التدريس التعليم المرتكزة على التكرار: إنها طريقة تعلم أثبتت فعاليتها بشكل كبير، لا سيما في المواد الدراسية التي تتطلب الحفظ"

منهج دراسة الحالة لوضع جميع محتويات المنهج في سياقها المناسب

يقدم برنامجنا منهج ثوري لتطوير المهارات والمعرفة. هدفنا هو تعزيز المهارات في سياق متغير وتنافسي ومتطلب للغاية.



مع جامعة TECH يمكنك تجربة طريقة تعلم تهز
أسس الجامعات التقليدية في جميع أنحاء العالم"

سيتم توجيهك من خلال نظام التعلم القائم على إعادة التأكيد على ما تم تعلمه، مع منهج تدريس طبيعي وتقدمي على طول المنهج الدراسي بأكمله.

منهج تعلم مبتكرة ومختلفة

إن هذا البرنامج المُقدم من خلال TECH هو برنامج تدريس مكثف، تم خلقه من الصفر، والذي يقدم التحديات والقرارات الأكثر تطلبًا في هذا المجال، سواء على المستوى المحلي أو الدولي. تعزز هذه المنهجية النمو الشخصي والمهني، متخذة بذلك خطوة حاسمة نحو تحقيق النجاح. ومنهج دراسة الحالة، وهو أسلوب يرسّي الأسس لهذا المحتوى، يكفل اتباع أحدث الحقائق الاقتصادية والاجتماعية والمهنية.

يعدك برنامجنا هذا لمواجهة تحديات جديدة
في بيئات غير مستقرة ولتحقيق النجاح في
حياتك المهنية"

كان منهج دراسة الحالة هو نظام التعلم الأكثر استخدامًا من قبل أفضل كليات الحاسبات في العالم منذ نشأتها. تم تطويره في عام 1912 بحيث لا يتعلم طلاب القانون القوانين بناءً على المحتويات النظرية فحسب، بل اعتمد منهج دراسة الحالة على تقديم مواقف معقدة حقيقية لهم لاتخاذ قرارات مستنيرة وتقدير الأحكام حول كيفية حلها. في عام 1924 تم تحديد هذه المنهجية كمنهج قياسي للتدريس في جامعة هارفارد.

أمام حالة معينة، ما الذي يجب أن يفعله المهني؟ هذا هو السؤال الذي سنواجهه بها في منهج دراسة الحالة، وهو منهج تعلم موجه نحو الإجراءات المتخذة لحل الحالات. طوال المحاضرة الجامعية، سيواجه الطلاب عدة حالات حقيقية. يجب عليهم دمج كل معارفهم والتحقيق والجدال والدفاع عن أفكارهم وقراراتهم.



سيتعلم الطالب، من خلال الأنشطة التعاونية
والحالات الحقيقية، حل المواقف المعقدة في
بيئات الأعمال الحقيقية.



منهجية إعادة التعلم (Relearning)

تجمع جامعة TECH بين منهج دراسة الحالة ونظام التعلم عن بعد، 100% عبر الانترنت والقائم على التكرار، حيث تجمع بين عناصر مختلفة في كل درس.

نحن نعزز منهج دراسة الحالة بأفضل منهجية تدريس 100% عبر الانترنت في الوقت الحالي وهي: منهجية إعادة التعلم والمعروفة بـ *Relearning*.

في عام 2019، حصلنا على أفضل نتائج تعليمية متفوقين بذلك على جميع الجامعات الافتراضية الناطقة باللغة الإسبانية في العالم.

في TECH ستتعلم بمنهجية رائدة مصممة لتدريب مدراء المستقبل. وهذا المنهج، في طبيعة التعليم العالمي، يسمى *Relearning* أو إعادة التعلم.

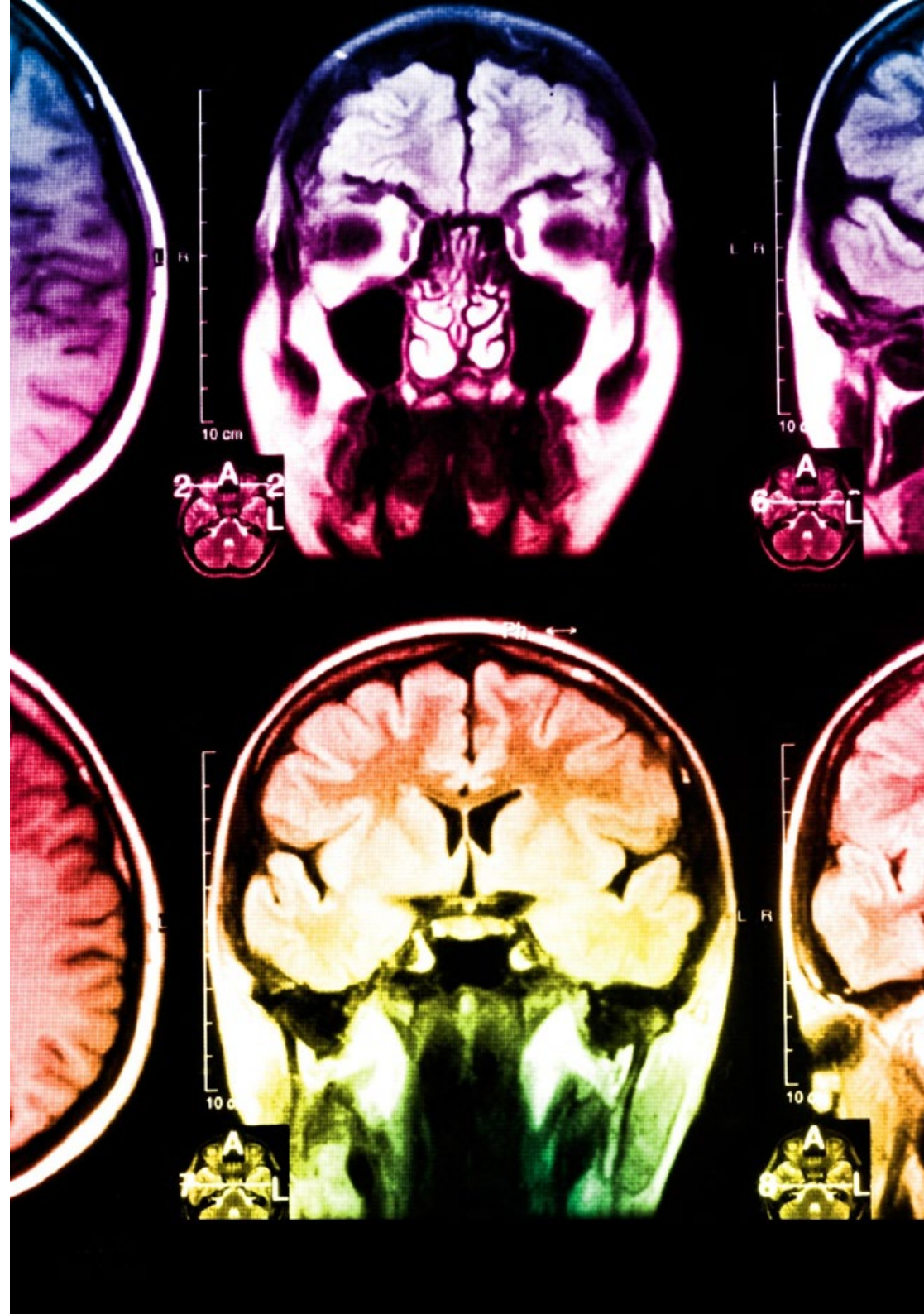
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصريح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

في برنامجنا، التعلم ليس عملية خطية، ولكنه يحدث في شكل لولبي (نتعلم ثم نطرح ماتعلمناه جانبًا فننساها ثم نعيد تعلمه). لذلك، نقوم بدمج كل عنصر من هذه العناصر بشكل مركزي. باستخدام هذه المنهجية، تم تدريب أكثر من 650000 خريج جامعي بنجاح غير مسبوق في مجالات متنوعة مثل الكيمياء الحيوية، وعلم الوراثة، والجراحة، والقانون الدولي، والمهارات الإدارية، وعلوم الرياضة، والفلسفة، والقانون، والهندسة، والصحافة، والتاريخ، والأسواق والأدوات المالية. كل ذلك في بيئة شديدة المتطلبات، مع طلاب جامعيين يتمتعون بمظهر اجتماعي واقتصادي مرتفع ومتوسط عمر يبلغ 43.5 عاماً.

ستتيح لك منهجية إعادة التعلم والمعروفة بـ *Relearning*،
التعلم بجهد أقل ومزيد من الأداء، وإشراكك بشكل أكبر في
تدريبك، وتنمية الروح النقدية لديك، وكذلك قدرتك على
الدفاع عن الحجج والآراء المتباينة: إنها معادلة واضحة للنجاح.

استنادًا إلى أحدث الأدلة العلمية في مجال علم الأعصاب، لا نعرف فقط كيفية تنظيم المعلومات والأفكار والصور والذكريات، ولكننا نعلم أيضًا أن المكان والسياق الذي تعلمنا فيه شيئًا هو ضروريًا لكي نكون قادرين على تذكرها وتخزينها في الحصين بالبحر، لكي نحفظ بها في ذاكرتنا طويلة المدى.

بهذه الطريقة، وفيما يسمى التعلم الإلكتروني المعتمد على السياق العصبي، ترتبط العناصر المختلفة لبرنامجنا بالسياق الذي تطور فيه المشارك ممارسته المهنية.



يقدم هذا البرنامج أفضل المواد التعليمية المُعدَّة بعناية للمهنيين:

المواد الدراسية



يتم إنشاء جميع محتويات التدريس من قبل المتخصصين الذين سيقومون بتدريس البرنامج الجامعي، وتحديداً من أجله، بحيث يكون التطوير التعليمي محدداً وملموحاً حقاً.

ثم يتم تطبيق هذه المحتويات على التنسيق السمعي البصري الذي سيخلق منهج جامعة TECH في العمل عبر الإنترنت. كل هذا بأحدث التقنيات التي تقدم أجزاء عالية الجودة في كل مادة من المواد التي يتم توفيرها للطالب.

المحاضرات الرئيسية



هناك أدلة علمية على فائدة المراقبة بواسطة الخبراء كطرف ثالث في عملية التعلم.

إن مفهوم ما يسمى *Learning from an Expert* أو التعلم من خبير يقوي المعرفة والذاكرة، ويولد الثقة في القرارات الصعبة في المستقبل.

التدريب العملي على المهارات والكفاءات

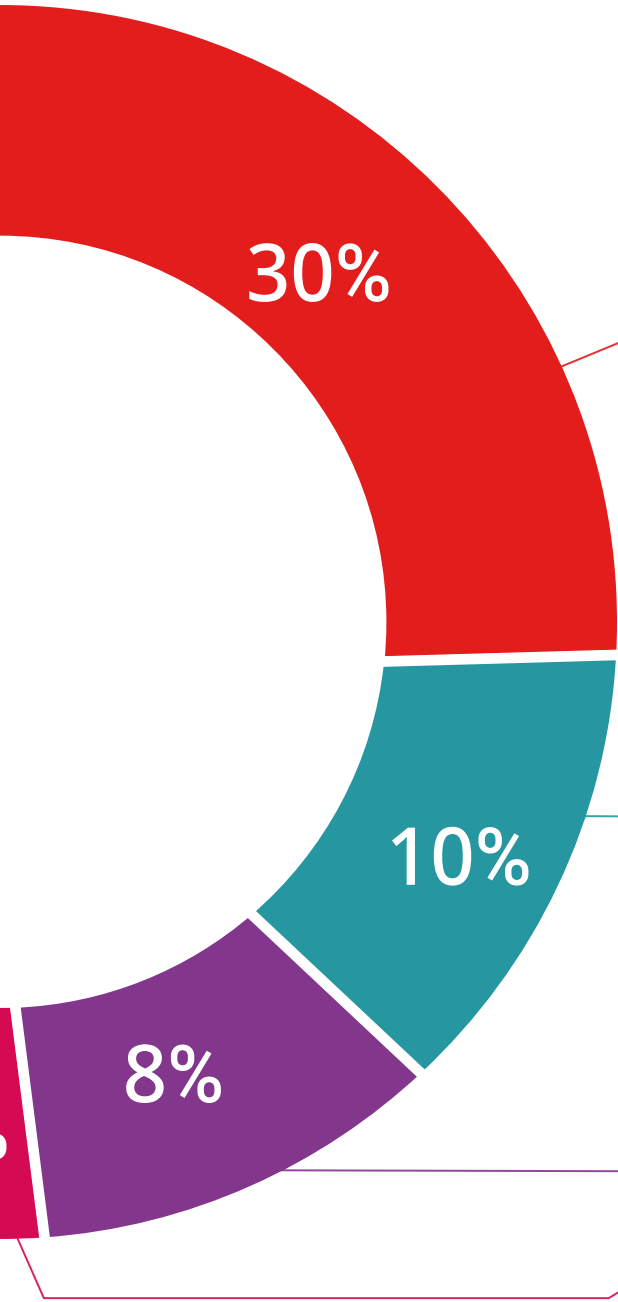


سيقومون بتنفيذ أنشطة لتطوير مهارات وقدرات محددة في كل مجال مواضيعي. التدريب العملي والديناميكيات لاكتساب وتطوير المهارات والقدرات التي يحتاجها المتخصص لنموه في إطار العولمة التي نعيشها.

قراءات تكميلية



المقالات الحديثة، ووثائق اعتمدت بتوافق الآراء، والأدلة الدولية. من بين آخرين. في مكتبة جامعة TECH الافتراضية، سيتمكن الطالب من الوصول إلى كل ما يحتاجه لإكمال تدريبه.





دراسات الحالة (Case studies)

سيقومون بإكمال مجموعة مختارة من أفضل دراسات الحالة المختارة خصيصًا لهذا المؤهل. حالات معروضة ومحللة ومدروسة من قبل أفضل المتخصصين على الساحة الدولية.



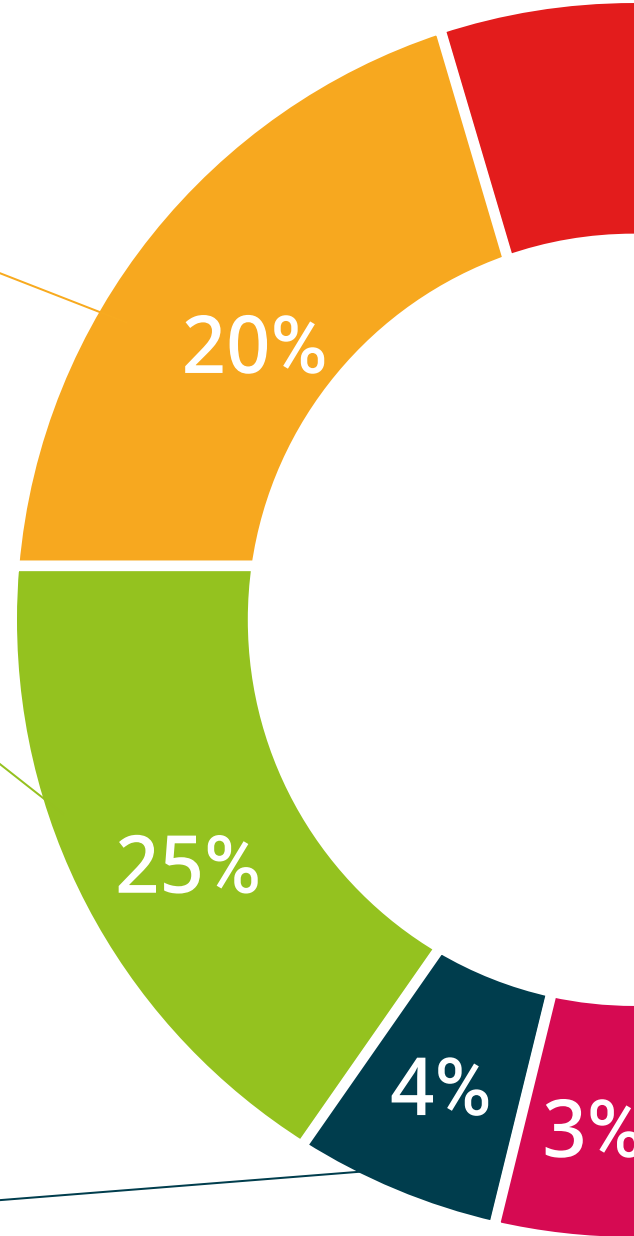
ملخصات تفاعلية

يقدم فريق جامعة TECH المحتويات بطريقة جذابة وديناميكية في أقراص الوسائط المتعددة التي تشمل الملفات الصوتية والفيديوهات والصور والرسوم البيانية والخرائط المفاهيمية من أجل تعزيز المعرفة. اعترفت شركة مايكروسوفت بهذا النظام التعليمي الفريد لتقديم محتوى الوسائط المتعددة على أنه "قصة نجاح أوروبية"



الاختبار وإعادة الاختبار

يتم بشكل دوري تقييم وإعادة تقييم معرفة الطالب في جميع مراحل البرنامج، من خلال الأنشطة والتدريبات التقييمية وذاتية التقييم؛ حتى يتمكن من التحقق من كيفية تحقيق أهدافه.



المؤهل العلمي

تضمن محاضرة جامعية في تحليل البرمجيات الخبيثة Malware وتطويرها، بالإضافة إلى التدريب الأكثر دقة وتحديثاً، الوصول إلى درجة الماجستير الصادرة عن TECH الجامعة التكنولوجية.



اجتاز هذا البرنامج بنجاح واحصل على شهادتك الجامعية
دون الحاجة إلى السفر أو القيام بأية إجراءات مرهقة"



تحتوي ال محاضرة جامعية في تحليل البرمجيات الخبيثة Malware وتطويرها على البرنامج العلمية الأكثر اكتمالا و حداثة في السوق.

بعد اجتياز التقييم، سيحصل الطالب عن طريق البريد العادي* مصحوب بعلم وصول مؤهل ال محاضرة الجامعية الصادر عن TECH الجامعة التكنولوجية.

إن المؤهل الصادر عن TECH الجامعة التكنولوجية سوف يشير إلى التقدير الذي تم الحصول عليه في برنامج المحاضرة الجامعية وسوف يفي بالمتطلبات التي عادة ما تُطلب من قبل مكاتب التوظيف ومسابقات التعيين ولجان التقييم الوظيفي والمهني.

المؤهل العلمي: محاضرة جامعية في تحليل البرمجيات الخبيثة Malware وتطويرها

طريقة: عبر الإنترنت

مدة: 6 أسابيع



المستقبل

الأشخاص

الصحة

الثقة

التعليم

المرشدون الأكاديميون المعلومات

الضمان

التدريس

الاعتماد الأكاديمي

المؤسسات

التعلم

المجتمع

الالتزام

التقنية

tech الجامعة
التكنولوجية

الحاضر

الابتكار

الحاضر

الجودة

محاضرة جامعية
تحليل البرمجيات الخبيثة
Malware وتطويرها

المعرفة

التدريب الافتراضي

المؤسسات

- « طريقة التدريس: أونلاين
- « مدة الدراسة: 6 اسابيع
- « المؤهل الحاملي من: TECH الجامعة التكنولوجية
- « مواعيد الدراسة: وفقاً لوتيرتك الخاصة
- « الامتحانات: أونلاين

الفصول الافتراضية

اللغات

محاضرة جامعية
تحليل البرمجيات الخبيثة
Malware وتطويرها