شهادة الخبرة الجامعية
الأمن السيبراني للفريق الأحمر (Red Team)

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

شهادة الخبرة الجامعية
الأمن السيبراني للفريق الأحمر (Red Team)

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **6 أشهر**
- المؤهل العلمي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

رابط الدخول إلى الموقع الإلكتروني: www.techtitute.com/ae/infromation-technology/postgraduate-diploma/postgraduate-diploma-red-team-cybersecurity

الفهرس

01

المقدمة

لقد أصبح الأمن السيبراني ركيزة أساسية في العصر الرقمي، في حين أن الترابط المتزايد بين الأنظمة زاد من خطر الهجمات االسيبرانية. وقد أصبح الطلب على المتخصصين ذوي المهارات العالية في هذا المجال أكثر وضوحاً من أي وقت مضى، خاصةً في ظل الزيادة الهائلة في الجرائم االسيبرانية والهجمات المتطورة. في هذا السياق، يتم تقديم هذا البرنامج كاستجابة استراتيجية لتزويد المهنيين بالمهارات اللازمة للتعامل مع التهديدات السيبرانية. سيخضع الطلاب خلال الدورة التدريبية لمحاكاة التهديدات المتقدمة. توفر منهجية المنهج، وهي متاحة 100% عبر الإنترنت، المرونة وسهولة الوصول، مع مجموعة متنوعة من محتوى الوسائط المتعددة وتطبيق طريقة إعادة التعلمRelearning.

سوف تساهم في تحسين الأمن السيبراني ومنع وقوع الجرائم الرقمية الكبرى. لا تفوّت هذه الفرصة واشترك الآن!"

في السيناريو المعقد للأمن السيبراني، يعد وجود خبير في هذا المجال ضرورة مطلقة للمؤسسات التي تسعى إلى تعزيز دفاعاتها ضد التهديدات المتطورة باستمرار. يسلط هذا النهج الاستباقي، وهو أساسي لتحسين الوضع الأمني باستمرار، الضوء على الحاجة الماسة إلى الخبرة.

يعد تنفيذ التدابير الاستباقية أمرًا ضروريًا، ويوفر التدريب المتخصص الذي يقدمه الفريق الأحمر للمهنيين القدرة على توقع وتحديد نقاط الضعف في الأنظمة والشبكات والتخفيف من حدتها. في شهادة الخبرة الجامعية، سيكتسب الطالب مهارات في اختبار الاختراق والمحاكاة، ويتناول تحديد نقاط الضعف واستغلالها. في هذا الصدد، لن يقتصر الأمر على تطوير المهارات التقنية المتقدمة فحسب، بل سيعزز أيضاً التعاون الفعال مع فرق الأمن، ودمج الاستراتيجيات ضد تهديدات البرمجيات الخبيثة malware.

بالإضافة إلى ذلك، سيكتسب الخريجون فهماً راسخاً للمبادئ الأساسية للتحقيق الجنائي الرقمي (DFIR)، والتي تنطبق على حل الحوادث السيبرانية. علاوة على ذلك، سيضمن هذا النهج الشامل للمناهج الدراسية تزويد المهنيين بأحدث المهارات في مجال الأمن السيبراني.

يتميز هذا المسار الأكاديمي ليس فقط بمحتواه، ولكن أيضًا بمنهجيته المتقدمة. سيكون متاحًا للطلاب عبر الإنترنت بالكامل، مما يمنحهم المرونة التي يحتاجونها للتقدم في حياتهم المهنية دون المساس بمسؤوليات عملهم.

بالمثل، سيتم استخدام تطبيق أجهزة إعادة التعلم (Relearning)، القائمة على تكرار المفاهيم الرئيسية، لترسيخ المعرفة وتسهيل التعلم الفعال. إن هذا المزيج من سهولة الوصول والنهج التربوي القوي يجعل من شهادة الخبرة الجامعية ليس فقط خياراً تعليمياً متقدماً، بل أيضاً محركاً مهماً للراغبين في التفوق في مجال الأمن السيبراني.

تحتوي **شهادة الخبرة الجامعية في الأمن السيبراني للفريق الأحمر (Red Team)** على البرنامج التعليمي الأكثر اكتمالاً وحداثة في السوق. أبرز خصائصها هي:

- تطوير الحالات العملية التي يقدمها خبراء الأمن السيبراني للفريق الأحمر (Red Team)
- 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
- تركيزها على المنهجيات المبتكرة
- كل هذا سيتم استكماله بدروس نظرية وأسئلة للخبراء ومنتديات مناقشة حول القضايا المثيرة للجدل وأعمال التفكير الفردية
- توفير المحتوى من أي جهاز ثابت أو محمول متصل بالإنترنت

> ستكتسب فهماً متعمقاً للتشريعات واللوائح الدولية التي ستساهم في نجاح عمليات التدقيق الخاصة بك"

سوف تتعمق في إعداد تقارير الطب الشرعي التفصيلية في الجامعة الأعلى تقييمًا في العالم من قبل طلابها، وفقًا لمنصة Trustpilot (4.9/5)"

سوف تقوم بتطوير مهارات تقييم واختيار أدوات الأمان المضادة للبرمجيات الخبيثة anti-malware.

انسى حفظ المناهج الدراسية!" مع منهج إعادة التعلم (Relearning)، ستدمج المفاهيم بطريقة طبيعية وتقدمية.

البرنامج يضم في أعضاء هيئة تدريسه محترفين في مجال الطاقات المتجددة يصبون في هذا التدريب خبرة عملهم، بالإضافة إلى متخصصين معترف بهم من الشركات الرائدة والجامعات المرموقة.

وسيتيح محتوى البرنامج المتعدد الوسائط، والذي صيغ بأحدث التقنيات التعليمية، للمهني التعلم السياقي والموقعي، أي في بيئة محاكاة توفر تدريبا غامرا مبرمجا 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.

02

الأهداف

إن الهدف الرئيسي شهادة الخبرة الجامعية في الأمن السيبراني للفريق الأحمر (Red Team) هو تدريب الطلاب على تطوير مهاراتهم في محاكاة التهديدات المتقدمة. طوال فترة البرنامج، سينغمس الخريجون في محاكاة التكتيكات والتقنيات والإجراءات التي تستخدمها الجهات الخبيثة. في هذا السياق، لن يؤدي النهج المتخصص في هذا السياق إلى تعزيز المهارات التقنية للمهنيين فحسب، بل سيمكنهم أيضًا من مواجهة التحديات الواقعية في هذا المجال. بالإضافة إلى ذلك، فإن استخدام منهجية إعادة التعلم Relearning سيسهل التعلم، وتثبيت المفاهيم الأساسية بأقل جهد ممكن.

سوف تحدد نقاط الضعف والثغرات في البنى التحتية السيبرانية للشركات. حقق أهدافك مع TECH!"

الأهداف العامة

- اكتساب مهارات متقدمة في اختبار الاختراق ومحاكاة Red Team، ومعالجة وتحديد واستغلال نقاط الضعف في الأنظمة والشبكات
- تطوير القدرات القيادية لتنسيق الفرق المتخصصة في الأمن السيبراني الهجومي، وتحسين تنفيذ مشاريع Pentesting Red Teamg
- تطوير المهارات في تحليل وتطوير البرمجيات الخبيثة وفهم وظائفها وتطبيق الاستراتيجيات الدفاعية والتعليمية
- صقل مهارات التواصل من خلال إنتاج تقارير تقنية وتنفيذية مفصلة، وعرض النتائج بفعالية على الجمهور التقني والتنفيذي
- تعزيز الممارسة الأخلاقية والمسؤولة في مجال الأمن السيبراني، مع مراعاة المبادئ الأخلاقية والقانونية في جميع الأنشطة
- إبقاء الطلاب على اطلاع دائم بالاتجاهات والتقنيات الناشئة في مجال الأمن السيبراني

الأهداف المحددة

الوحدة 1. تحليل البرمجيات الخبيثة Malware وتطويرها

- 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 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 anti-malware، 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 malware
- إبقاء الخريج على اطلاع دائم بأحدث الاتجاهات والتقنيات المستخدمة في تحليل البرمجيات الخبيثة malwareوتطويرها، مما يضمن استمرار أهمية وفعالية المهارات المكتسبة

الوحدة 2. أساسيات الطب الشرعي و DFIR

- اكتساب فهم قوي للمبادئ الأساسية للتحقيق الجنائي الرقمي (DFIR) وتطبيقها في حل الحوادث السيبرانية
- تطوير المهارات في الحصول الآمن والجنائي على الأدلة الرقمية، بما يضمن الحفاظ على سلسلة الحفظ
- تعلّم كيفية إجراء تحليل الطب الشرعي لأنظمة الملفات
- تعريف الطالب بالتقنيات المتقدمة لتحليل السجلات والسجلات، مما يتيح إعادة بناء الأحداث في البيئات الرقمية
- تعرّف على كيفية تطبيق منهجيات التحقيق الجنائي الرقمي في حل القضايا، بدءاً من تحديد الهوية وحتى توثيق النتائج
- تعريف الطالب بتحليل الأدلة الرقمية وتطبيق تقنيات الطب الشرعي في بيئات الاختبار الخماسي Pentesting
- تطوير المهارات في إعداد تقارير الطب الشرعي المفصلة والواضحة، وعرض النتائج والاستنتاجات بطريقة مفهومة
- تعزيز التعاون الفعال مع فرق الاستجابة للحوادث، وتحسين التنسيق في التحقيق في التهديدات والتخفيف من حدتها
- تعزيز الممارسات الأخلاقية والقانونية في مجال التحليل الجنائي الرقمي، وضمان الالتزام بلوائح الأمن السيبراني ومعايير السلوك

الوحدة 3. تمارين الفريق الأحمرRed Team المتقدمة

- تطوير المهارات في محاكاة التهديدات المتقدمة، ومحاكاة التكتيكات والتقنيات والإجراءات (TTPs) التي تستخدمها الجهات الخبيثة الجذابة
- تعلم كيفية تحديد نقاط الضعف ونقاط الضعف في البنية التحتية من خلال تمارين الفريق الأحمرRed Team الواقعية، وتعزيز الوضع الأمني
- إلمام الخريج بتقنيات التهرب الأمني المتقدمة، مما يتيح تقييم مرونة البنية التحتية في مواجهة الهجمات المرغوبة
- تطوير مهارات التنسيق والتعاون الفعال بين أعضاء الفريق الأحمر Red Team، وتحسين تنفيذ التكتيكات والاستراتيجيات لتقييم أمن المؤسسة بشكل شامل
- تعرّف على كيفية محاكاة سيناريوهات التهديدات الحالية، مثل هجمات ransomwareبرامج الفدية الخبيثة أو حملات phishingالتصيد الاحتيالي المتقدمة، لتقييم قدرة المؤسسة على الاستجابة
- تعريف الطالب بتقنيات التحليل اللاحق للتمرين وتقييم أداء الفريق الأحمر Red Team واستخلاص الدروس المستفادة للتحسين المستمر
- تطوير مهارات تقييم المرونة التنظيمية في مواجهة هجمات المحاكاة وتحديد مجالات التحسين في السياسات والإجراءات
- تعلم كيفية إنتاج تقارير مفصلة توثق النتائج والمنهجيات المستخدمة والتوصيات المستمدة من تمارين الفريق الأحمرRed Team المتقدمة
- تعزيز الممارسات الأخلاقية والقانونية في إجراء تمارين الفريق الأحمرRed Team، وضمان الالتزام بلوائح الأمن السيبراني والمعايير الأخلاقية

03

هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

بالنسبة لهذا البرنامج الجامعي، جمعت TECH هيئة تدريس متميزة تضم أفضل المتخصصين في هذا المجال. من هذا المنطلق، يتمتع كل عضو من أعضاء هيئة التدريس بخلفية مهنية واسعة ومعترف بها، وقد تم تكوينها في شركات رائدة في قطاع الأمن السيبراني. لن يضمن هؤلاء المحترفون الذين تم اختيارهم بعناية لخبراتهم وتجاربهم جودة المنهج الأكاديمي فحسب، بل سيقدمون أيضًا منظورًا عمليًا وحديثًا، مما يثري تدريب المشاركين برؤى قيمة من خبراتهم الواقعية في بيئة الفريق الأحمرRed Team..

اطّلع على أحدث تقنيات تشفير Shellcode (XQR) من كبار خبراء الأمن السيبراني. ابدأ مسيرتك المهنية مع TECH!"

هيكل الإدارة

أ. Gómez Pintado, Carlos

- مدير فريق الأمن السيبراني والشبكات Cipherbit في Grupo Oesía
- مستشار إداري Advisor ومستثمر Investor في تطبيق Wesson App
- بكالوريوس 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

04

الهيكل والمحتوى

سيزود هذا المنهج الطلاب بمهارات متخصصة في التحليل الجنائي المطبق على البرمجيات الخبيثةmalware، مع التركيز على تطوير المهارات الأساسية لتحديد مؤشرات الاختراق وأنماط الهجوم. سيتعلم الخريجون خلال الدورة التدريبية المنهجيات المتقدمة، مما يوفر لهم الأدوات والمعرفة اللازمة للتعامل مع التهديدات السيبرانية المتطورة. بالإضافة إلى ذلك، سيضمن هذا البرنامج المنظم بدقة تدريباً شاملاً في مجال الفريق الأحمرRed Team، وإعداد المهنيين لتحليل الاستراتيجيات المعقدة التي تستخدمها الجهات الفاعلة الخبيثة ومواجهتها.

سوف تعمق معرفتك بتقنيات ما بعد
الاستغلال المتقدمة وتضع نفسك
في مكانة متميزة في "Red Teamer

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 البرمجيات الخبيثة وأنواعها Malware
3.1.1. تحليل البرامج الضارة
4.1.1. تطوير البرمجيات الخبيثة Malware
2.1. تهيئة البيئة
1.2.1. تهيئة الأجهزة الافتراضية Snapshotsg
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(Portable Executable)
2.3.1. العمليات والمسارات Threads
3.3.1. نظام الملفات والسجل
4.3.1. Windows Defender
4.1. تقنيات البرمجيات الخبيثة Malware الأساسية
1.4.1. توليد الرموز البرمجية Shellcode
2.4.1. تنفيذ الرمز الصوري Shellcode على القرص
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. المجلد الرئيسي
3.5.1. مفاتيح التسجيل
4.5.1. شاشات التوقف
6.1. تقنيات البرمجيات الخبيثةmalware المتقدمة
1.6.1. تشفير من shellcode (XOR)
2.6.1. تشفير من shellcode (RSA)
3.6.1. تشويش Strings
4.6.1. حقن العملية

7.1. التحليل الثابت من Malware
1.7.1. تحليل Packers مع DIE (Detect It Easy)
2.7.1. تحليل المقاطع باستخدام PE-Bear
3.7.1. فك التجميع مع Ghidra
8.1. التحليل الديناميكي من malware
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. تهيئة البيئة
2.10.1. التحليل الثابت للبرمجيات الخبيثة Malware
3.10.1. التحليل الديناميكي من malware
4.10.1. إنشاء قواعد YARA

الوحدة 2. أساسيات الطب الشرعي و DFIR

1.2. فورينس ديجيتال
1.1.2. تاريخ الطب الشرعي الحاسوبي وتطوره
2.1.2. أهمية الأدلة الجنائية الحاسوبية في الأمن السيبراني
3.1.2. تاريخ الطب الشرعي الحاسوبي وتطوره
2.2. أساسيات الأدلة الجنائية الحاسوبية
1.2.2. سلسلة العهدة وتنفيذها
2.2.2. أنواع الأدلة الرقمية
3.2.2. عمليات الحصول على الأدلة
3.2. أنظمة الملفات وهيكل البيانات
1.3.2. أنظمة الملفات الرئيسية
2.3.2. طرق إخفاء البيانات
3.3.2. تحليل البيانات الوصفية للملف وسماته

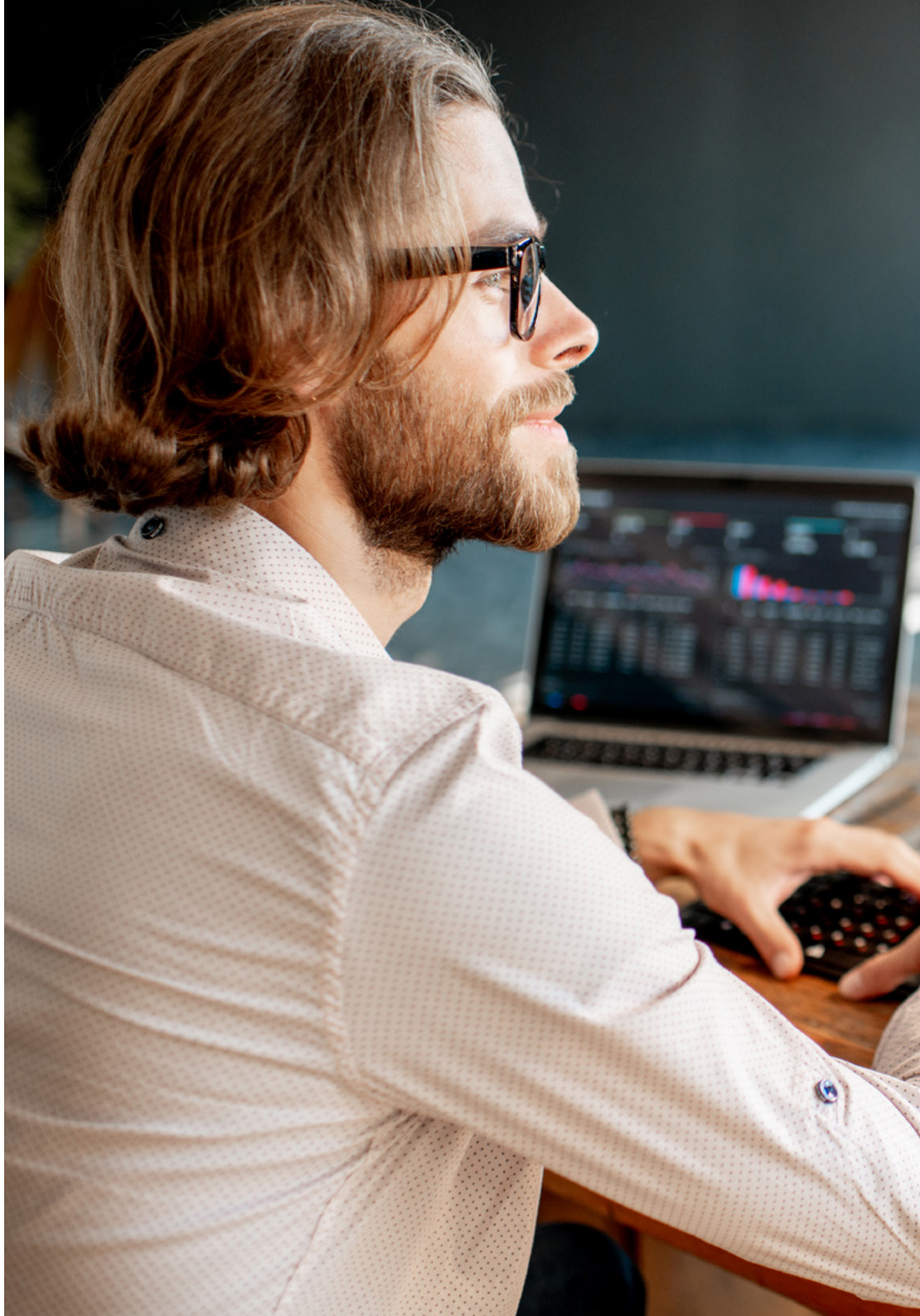
4.2. تحليل أنظمة التشغيل
1.4.2. تحليل الطب الشرعي لأنظمة ويندوزWindows
2.4.2. تحليل الطب الشرعي لأنظمة لينكس Linux
3.4.2. تحليل الطب الشرعي لأنظمة macOS
5.2. استعادة البيانات وتحليل الأقراص
1.5.2. استعادة البيانات من الوسائط التالفة
2.5.2. أدوات تحليل الأقراص
3.5.2. تفسير جداول تخصيص الملفات
6.2. تحليل الشبكة وحركة المرور
1.6.2. التقاط حزم الشبكة وتحليلها
2.6.2. تحليل سجلات جدار الحماية firewall
3.6.2. كشف التسلل إلى الشبكة
7.2. تحليل البرامج الضارة والشفرات البرمجية الخبيثة Malware
1.7.2. التصنيف البرمجيات الخبيثة malware وخصائصها
2.7.2. تحليل البرمجيات الخبيثة الثابتة والديناميكية malware
3.7.2. تقنيات التفكيك وتصحيح الأخطاء
8.2. تحليل السجلات والأحداث
1.8.2. أنواع السجلات في الأنظمة والتطبيقات
2.8.2. تفسير الأحداث ذات الصلة
3.8.2. أدوات تحليل السجل
9.2. الاستجابة للحوادث الأمنية
1.9.2. عملية الاستجابة للحوادث
2.9.2. إنشاء خطة الاستجابة للحوادث
3.9.2. التنسيق مع فرق الأمن
10.2. تقديم الأدلة والبراهين القانونية
1.10.2. قواعد الأدلة الرقمية في المجال القانوني
2.10.2. إعداد تقارير الطب الشرعي
3.10.2. المثول أمام المحكمة كشاهد خبير

الوحدة 3. تمارين الفريق الأحمرRed Team المتقدمة

1.3. تقنيات التعرف المتقدمة
1.1.3. تعداد النطاقات الفرعية المتقدمة
2.1.3. Google Dorking متقدم
3.1.3. وسائل التواصل الاجتماعي و theHarvester
2.3. حملاتphishing المتقدمة
1.2.3. ما هو التصيد الاحتيالي بالوكيل العكسي؟ Reverse-Proxy Phishing
2.2.3. FA Bypass con Evilginx2
3.2.3. استخراج البيانات
3.3. تقنيات المثابرة المتقدمة
1.3.3. Golden Tickets
2.3.3. Silver Tickets
3.3.3. تقنية DCShadow
4.3. تقنيات التجنب المتقدمة
1.4.3. Bypass de AMSI
2.4.3. تعديل الأدوات الموجودة
3.4.3. تشويش Powershell
5.3. تقنيات الحركة الجانبية المتقدمة
1.5.3. (Pass-the-Ticket (PtT
2.5.3. (Overpass-the-Hash (Pass-the-Key
3.5.3. NTLM Relay
6.3. تقنيات ما بعد الاستغلال المتقدمة
1.6.3. Dump de LSASS
2.6.3. Dump de SAM
3.6.3. هجوم DCSync
7.3. تقنيات التمحور المتقدمة pivoting
1.7.3. ما هو التمحورpivoting
2.7.3. الربط مع SSH
3.7.3. Pivotingإزميل مخروطي محوري

8.3. الاقتحامات الجسدية
1.8.3. المراقبة والاستطلاع
2.8.3. التخييم في الخلفية Tailgating و التحميل على الظهرPiggybacking
3.8.3. فتح الأقفال Lock-Picking
9.3. هجمات Wi-Fi
1.9.3. الهجمات على PSK 2WPA/WPA
2.9.3. هجمات Rogue AP
3.9.3. الهجمات على Enterprise 2WPA
10.3. هجمات الترددات اللاسلكية RFID
1.10.3. قراءة بطاقة RFID
2.10.3. التلاعب بطاقة RFID
3.10.3. إنشاء بطاقات مستنسخة

لا تفوّت هذه الفرصة لتعزيز حياتك المهنية من خلال هذا البرنامج المبتكر. كن خبيراً في الأمن السيبراني!"



05

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.

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

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 يرسي 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 سنواجهك 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.

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 طليعة التعليم العالمي، يسمى *Relearning* أو إعادة التعلم.

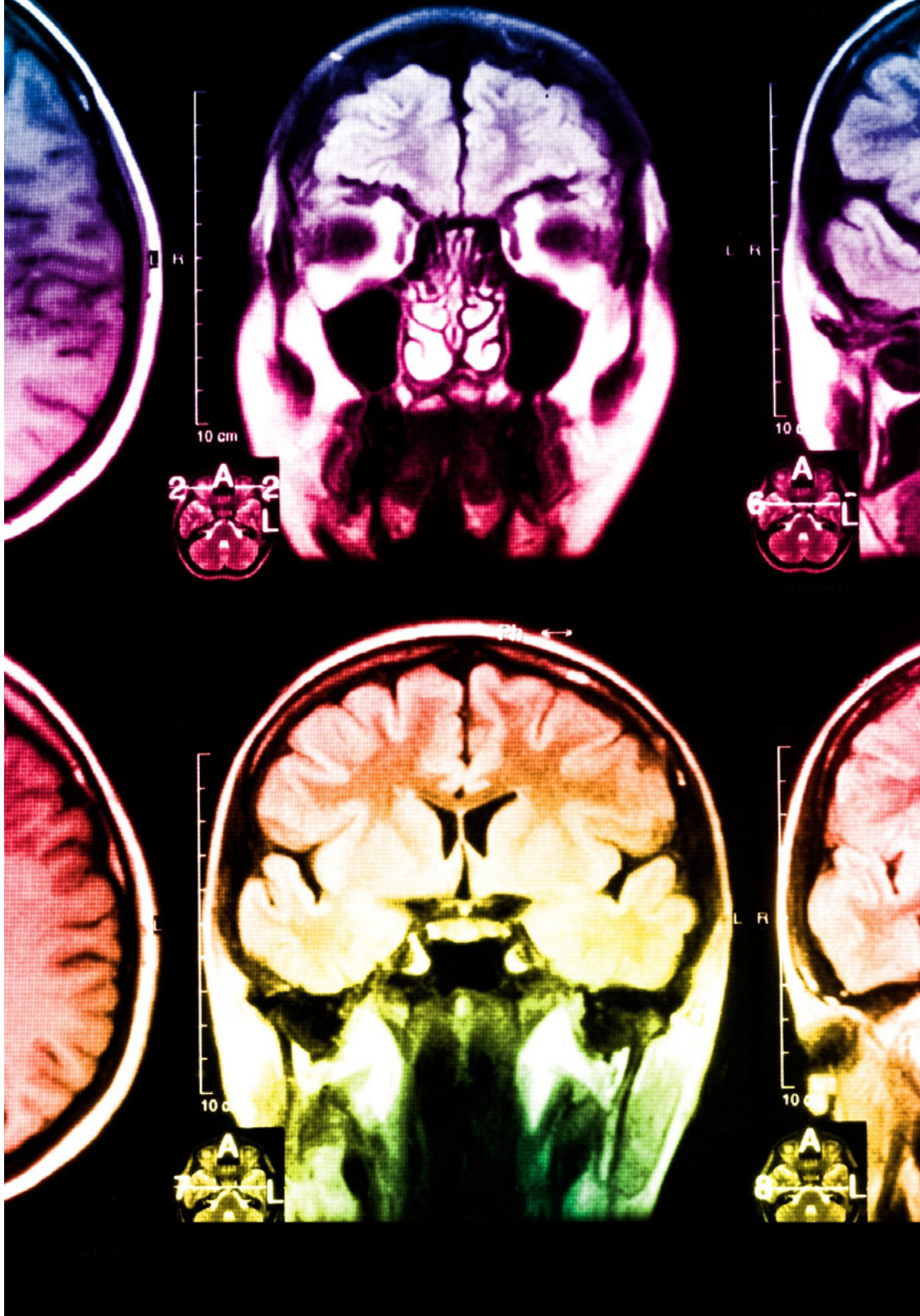
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

في برنامجنا، التعلم ليس عملية خطية، ولكنه يحدث في شكل لولبي (نتعلّم ثم نطرح ماتعلمناه جانبًا فننساه 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 الحُصين بالمخ، لكي نحتفظ بها في ذاكرتنا طويلة المدى.

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



يقدم هذا البرنامج أفضل المواد التعليمية المُعَدَّة بعناية للمهنيين:

المواد الدراسية

يتم إنشاء جميع محتويات التدريس من قبل المتخصصين الذين سيقومون بتدريس البرنامج الجامعي، وتحديداً من أجله، بحيث يكون التطوير التعليمي محددًا وملموسًا حقًا.

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.

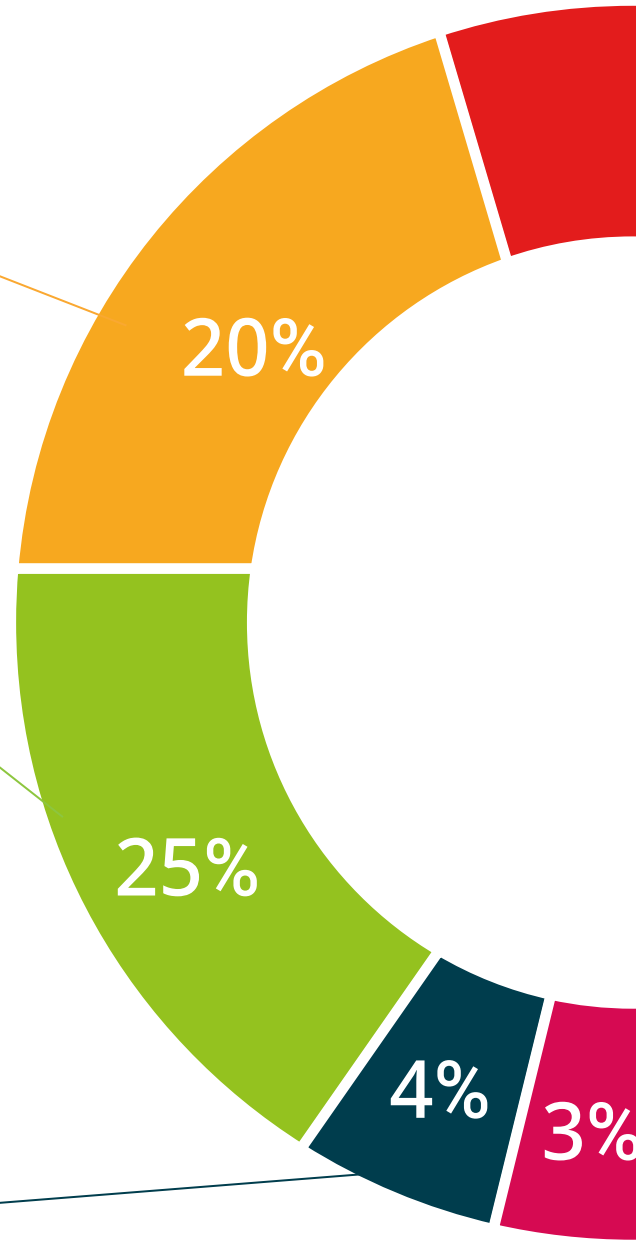
ملخصات تفاعلية

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 مايكروسوف 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.



06

المؤهل العلمي

تضمن شهادة الخبرة الجامعية هذه فى الأمن السيبراني للفريق الأحمر (Red Team), بالإضافة إلى التدريب الأكثر دقة وحداثة الحصول على مؤهل شهادة الخبرة الجامعية الصادر عن TECH الجامعة التكنولوجية.

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

تحتوي **شهادة الخبرة الجامعية في الأمن السيبراني للفريق الأحمر (Red Team)** على البرنامج الأكثر اكتمالا وحداثة في السوق.

بعد اجتياز التقييم، سيحصل الطالب عن طريق البريد العادي* مصحوب بعلم وصول مؤهل **شهادة الخبرة الجامعية** الصادرعن **TECH الجامعة التكنولوجية**.

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

المؤهل العلمي: **شهادة الخبرة الجامعية في الأمن السيبراني للفريق الأحمر (Red Team)**

طريقة الدراسة: **عبر الإنترنت**

مدة الدراسة: **6 أشهر**


tech الجامعة التكنولوجية

شهادة تخرج

هذه الشهادة ممنوحة إلى

لـ

المواطن/المواطنة ..... مع وثيقة تحقيق شخصية رقم .....

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

شهادة الخبرة الجامعية

في

الأمن السيبراني للفريق الأحمر (Red Team)

وهي شهادة خاصة من هذه الجامعة موافقة لـ 450
ساعة، مع تاريخ بدء يوم/شهر/ سنة وتاريخ انتهاء يوم/شهر/سنة

تيك مؤسسة خاصة للتعليم العالي معتمدة من وزارة التعليم العام منذ 28 يونيو 2018

في تاريخ 17 يونيو 2020

أ. د./ Tere Guevara Navarro
رئيس الجامعة

الكود الفريد الخاص بجامعة TECH: AFWOR23S techtitute.com/certificates

*تصديق لاهاي أبوستيل. في حالة قيام الطالب بالتقدم للحصول على درجته العلمية الورقية وبتصديق لاهاي أبوستيل، ستتخذ مؤسسة TECH EDUCATION الإجراءات المناسبة لكي يحصل عليها وذلك بتكلفة إضافية.

الجامعة التيكنولوجية

شهادة الخبرة الجامعية
الأمن السيبراني للفريق الأحمر (Red Team)

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **6 أشهر**
- المؤهل العلمي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

شهادة الخبرة الجامعية
الأمن السيبراني للفريق الأحمر (Red Team)

tech الجامعة التيكنولوجية