شهادة الخبرة الجامعية
الأمن السيبراني الهجومي

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

شهادة الخبرة الجامعية
الأمن السيبراني الهجومي

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

رابط الدخول إلى الموقع الإلكتروني: www.techtitute.com/ae/information-technology/postgraduate-diploma/postgraduate-diploma-offensive-cibersecurity

الفهرس

01

المقدمة

يُعد الأمن السيبراني جانبًا أساسيًا للمؤسسات لحماية أصولها الرقمية، والحفاظ على سمعتها الاجتماعية وحمايتها من التجسس من قبل المنافسين. من ثم، فإن المزيد والمزيد من الشركات تطلب دمج خبراء تكنولوجيا المعلومات في مخططاتها التنظيمية، وذلك لتجنب العواقب التي قد تؤثر حتى على قدراتها المالية. في هذا السياق، يحتاج هؤلاء الأخصائيون إلى تحديث معارفهم ومهاراتهم باستمرار لمواكبة تقنيات الجريمة الإلكترونية. لهذا السبب، طورت جامعة TECH خبيرًا جامعيًا مبتكرًا يتم من خلاله تحديد التهديدات والتخفيف من حدتها. تجدر الإشارة إلى أن البرنامج بأكمله سيتم تدريسه 100% عبر الإنترنت، لضمان حصول الطلاب على قدر أكبر من الراحة والمرونة.

سوف تتعلم المزيد عن بروتوكول Kerberos
وحماية المعلومات في بيئات الشبكة"

تتناقل وسائل الإعلام كل يوم حالات اختراق قراصنة يلحقون الضرر بالمؤسسات من خلال الوصول إلى قواعد بياناتها. إن العواقب المترتبة على هذه الهجمات وخيمة، حيث تعطل العمليات وتمنع الشركات من العمل بفعالية. في الواقع، يمكن أن يؤثر ذلك بشكل مباشر على اقتصادك من خلال فرض غرامات على عدم الامتثال للوائح وقيود الإيرادات.

من هذا المنطلق، أنشأت جامعة TECH مؤهلاً متطورًا للكشف عن تقنيات الاختراق الأكثر استخدامًا، بالإضافة إلى أفضل الاستراتيجيات للتعامل معها. تحت إشراف أعضاء هيئة تدريس متمرسين، سيضع المنهج الدراسي الأسس الأساسية لفهم كيفية تفكير القراصنة. كما ستوفر مجموعة متنوعة من الحلول التي تهدف إلى توفير بنية تحتية آمنة لإدارة الشهادات الرقمية في شبكة المؤسسة.

بالمثل، سيتناول المتخصصون الإعداد الأمثل للبيئات الافتراضية، وذلك بفضل تكوين الأجهزة الافتراضية أو اللقطات. snapshots بالإضافة إلى ذلك، سيتم تحليل البرمجيات الخبيثة، وسبر المكالمات باستخدام أداة مراقبة واجهة برمجة التطبيقات ومراقبة طلبات الشبكة باستخدام TCPView. سيتعلم الخريجون المفاهيم النظرية في بيئات المحاكاة، مما يعدهم لمواجهة تحديات العالم الحقيقي في مجال الأمن السيبراني الهجومي. أخيراً، سيتم التركيز على الأخلاقيات والمسؤولية الاجتماعية التي يجب أن يتحلى بها الخبراء في هذا المجال.

من أجل تعزيز إتقان جميع هذه المحتويات، يطبق الخبير الجامعي نظام إعادة التعلم المبتكرRelearning. تعد TECH رائدتًا في استخدام هذا النموذج التعليمي الذي يعزز استيعاب المفاهيم المعقدة من خلال التكرار الطبيعي والتدريجي لها. يعتمد البرنامج أيضاً على مواد في أشكال متنوعة، مثل مقاطع الفيديو التوضيحية والملخصات التفاعلية والرسوم البيانية. كل هذا في وضع مناسب 100% عبر الإنترنت، مما يسمح لكل شخص بتعديل الجدول الزمني لكل شخص وفقًا لمسؤولياته وتوافره.

يحتوي هذا البرنامج **شهادة الخبرة الجامعية هذه في الأمن السيبراني الهجومي** على البرنامج العلمي الأكثر اكتمالا وحداثة في السوق. أبرز خصائصها هي:

- تطوير دراسات الحالة التي يقدمها خبراء في الأمن السيبراني الهجومي
- يجمع المحتوى الرسومي والتخطيطي والعملي البارز الذي تم تصميمه به معلومات كاملة وعملية عن تلك التخصصات الأساسية للممارسة المهنية
- 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
- توفر المحتوى من أي جهاز ثابت أو محمول متصل بالإنترنت

> طوِّر مهاراتك كمدقق حسابات هجومي وانطلق في تحدٍ مهني جديد في أكثر الشركات الرقمية المرموقة"

ستحقق أهدافك من خلال أدوات التدريس الخاصة بـ TECH، بما في ذلك مقاطع الفيديو التوضيحية والملخصات التفاعلية"

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

سيتيح 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 التعلم القائم على حل المشكلات، والذي يجب على المهني من خلاله محاولة حل مواقف الممارسة المهنية المختلفة التي تنشأ طوال العام الدراسي. للقيام بذلك، سيحصل على مساعدة من نظام فيديو تفاعلي مبتكر من قبل خبراء مشهورين.

هل تريد أن تصبح Big Bounty Hunter؟ سوف تلتقط أي ثغرة على الإنترنت بفضل هذا البرنامج.

في غضون 6 أشهر فقط ستتقن إدارة الهوية في Azure AD. سجل الآن!

02

الأهداف

يقدم تصميم هذا البرنامج تجربة تعليمية فريدة من نوعها، والتي تتميز بنهجها العملي والمبتكر في مجال الأمن السيبراني. بهذه الطريقة، سيتعرف الطلاب على كل شيء بدءاً من تحليل الثغرات الأمنية وصولاً إلى تقنيات الاختراق المتقدمة. في هذا الخط، سيتم توفير التدابير المثلى لتقييم وتعزيز الأنظمة السيبرانية المختلفة. بالإضافة إلى ذلك، سيتم التركيز على كل من المسؤوليات القانونية والأخلاقية التي يجب على الخبراء في هذا المجال تبنيها.

قلل من تهديدات البرنامج الخبيث مع أفضل
جامعة رقمية في العالم، وفقًا لمجلة Forbes"

الأهداف العامة

- اكتساب مهارات متقدمة في اختبار الاختراق ومحاكاة فريق الشبكة Red Team، ومعالجة وتحديد واستغلال نقاط الضعف في الأنظمة والشبكات
- تطوير المهارات القيادية لتنسيق الفرق المتخصصة في الأمن السيبراني الهجومي، وتحسين تنفيذ مشاريع فريق الاختبار الخماسي وفريق الشبكة
- تطوير المهارات في تحليل وتطوير البرمجيات الخبيثة وفهم وظائفها وتطبيق الاستراتيجيات الدفاعية والتعليمية
- صقل مهارات التواصل من خلال إنتاج تقارير فنية وتنفيذية مفصلة، وعرض النتائج بفعالية على الجمهور الفني 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. الأمن الهجومي

- تعريف الخريج بمنهجيات اختبار الاختراق، بما في ذلك المراحل الرئيسية مثل جمع المعلومات وتحليل الثغرات الأمنية والاستغلال والتوثيق
- تطوير مهارات عملية في استخدام أدوات الاختبار الخماسي المتخصصة Pentesting لتحديد وتقييم نقاط الضعف في الأنظمة والشبكات
- دراسة وفهم التكتيكات والتقنيات والإجراءات التي تستخدمها الجهات الفاعلة الخبيثة، مما يتيح تحديد التهديدات ومحاكاتها
- تطبيق المعرفة النظرية في سيناريوهات عملية ومحاكاة، ومواجهة تحديات حقيقية لتعزيز مهارات الاختبار الخماسي Pentesting
- تطوير مهارات التوثيق الفعالة، وإنشاء تقارير مفصلة تعكس النتائج والمنهجيات المستخدمة والتوصيات لتحسين الأمن
- ممارسة التعاون الفعال في فرق الأمن الهجومي، وتحسين تنسيق وتنفيذ أنشطة الاختبار الخماسي Pentesting

الوحدة 2. الهجمات على أنظمة Windows

- تطوير مهارات تحديد وتقييم نقاط الضعف المحددة في أنظمة التشغيل Windows
- التعرف على التكتيكات المتقدمة التي يستخدمها المهاجمون للتسلل إلى الشبكات المستندة إلى Windows والاستمرار فيها
- اكتساب المهارات في الاستراتيجيات والأدوات اللازمة للتخفيف من التهديدات المحددة التي تستهدف أنظمة تشغيل الويندوز Windows
- إلمام الخريج بتقنيات التحليل الجنائي المطبقة على أنظمة الويندوز، مما يسهل التعرف على الحوادث والاستجابة لها
- تطبيق المعرفة النظرية في بيئات المحاكاة، والمشاركة في تمارين عملية لفهم ومواجهة هجمات محددة على أنظمة الويندوز Windows
- تعلم استراتيجيات محددة لتأمين بيئات المؤسسات باستخدام أنظمة تشغيل Windows، مع مراعاة تعقيدات البنى التحتية للمؤسسات
- تطوير الكفاءات لتقييم وتحسين التكوينات الأمنية على أنظمة الويندوز، وضمان تنفيذ تدابير فعالة
- تعزيز الممارسات الأخلاقية والقانونية في تنفيذ الهجمات والاختبارات على أنظمة الويندوز Windows، مع مراعاة المبادئ الأخلاقية للأمن السيبراني
- إبقاء المتعلم على اطلاع دائم بأحدث الاتجاهات والتهديدات في الهجمات على أنظمة Windows، مما يضمن استمرار أهمية وفعالية المهارات المكتسبة

الوحدة 3. تحليل البرمجيات الخبيثة وتطويرها Malware

- اكتساب معرفة متقدمة بطبيعة البرمجيات الخبيثة ووظائفها وسلوكها، وفهم أشكالها وأهدافها المختلفة
- تطوير المهارات في التحليل الجنائي المطبق على البرمجيات الخبيثة malware، مما يتيح تحديد مؤشرات الاختراق (IoC) وأنماط الهجوم
- تعلّم استراتيجيات الكشف الفعّال عن البرمجيات الخبيثة malware والوقاية منها، بما في ذلك نشر حلول الأمان المتقدمة
- تعريف المتعلم بتطوير البرمجيات الخبيثة malware 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 anti-malware، مع مراعاة فعاليتها وقدرتها على التكيف مع بيئات محددة
- التعرّف 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

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

03

هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

في إطار التزامها بتقديم التميز التعليمي، تضم TECH التطبيقية هيئة تدريس مرموقة. تجدر الإشارة إلى أن هؤلاء المتخصصين يتمتعون بخلفية مهنية واسعة، حيث كانوا جزءًا من شركات شهيرة متخصصة في الأمن السيبراني الهجومي. لهذا السبب، سيتضمن خط سير الرحلة الأكاديمية أكثر الموارد والتقنيات تقدماً في هذا المجال. بالإضافة إلى ذلك، سيتم تقديم منهج شامل لتلبية تطلعات الخريجين للتخصص في مجال سيوفر لهم العديد من الفرص.

سيتم دعمك من قبل هيئة تدريس من المتخصصين المتميزين في مجال الأمن السيبراني الهجومي"

هيكل الإدارة

أ. Gómez Pintado, Carlos

- مدير فريق الأمن السيبراني والشبكات Cipherbit في Grupo Oesía
- مستشار إداري Advisor ومستثمر Investor 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 Parrilla, Yuba

- الخط الأمني الهجومي ومنسق فريق الأمن الهجومي والشبكة
- أخصائي في إدارة المشاريع التنبؤية في معهد إدارة المشاريع Predictive Project Management Institute
- أخصائي SmartDefense
- أخصائي Web Application Penetration Tester في eLearnSecurity
- Junior Penetration Tester في eLearnSecurity
- خريج هندسة الحاسوب من جامعة البوليتكنيك في مدريد

أ. Gallego Sánchez, Alejandro

- خبير اختراقات Pentester في مجموعة Oesía
- مستشار الأمن السيبراني في Integración Tecnológica Empresarial, S.L
- تقني سمعي بصري في شركة Ingeniería Audiovisual S.A
- بكالوريوس هندسة الأمن السيبراني من جامعة Rey Juan Carlos

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

ينقسم هذا البرنامج إلى 3 وحدات: الأمن الهجومي، ومهاجمة الشبكات أو أنظمة Windows، وتحليل البرمجيات الخبيثة وتطويرهاMalware. خلال المنهج، سيتم تقديم منظور عملي حول الكشف المبكر عن التهديدات في وقت مبكر. في هذا الصدد، سيتم تشجيع الطلاب على الإبداع للتغلب على التحديات من خلال حلول مبتكرة. بالإضافة إلى ذلك، فإن تصنيف نقاط الضعف، والتي من أهمها مكافحة التطرف العنيف CVE. كما سيتم استكشاف تقنيات تحليل البرمجيات الخبيثة malwareالمتقدمة من أجل تعزيز الأمن في البيئات السيبرانية.

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

الوحدة 1. الأمن الهجومي

1.1. التعريف والسياق
1.1.1. المفاهيم الأساسية للأمن الهجومي
2.1.1. أهمية الأمن السيبراني في الوقت الحاضر
3.1.1. التحديات والفرص في الأمن الهجومي
2.1. أساسيات الأمن السيبراني
1.2.1. التحديات المبكرة والتهديدات المتطورة
2.2.1. المعالم التكنولوجية وتأثيرها على الأمن السيبراني
3.2.1. الأمن السيبراني في العصر الحديث
3.1. أساس الأمن الهجومي
1.3.1. المفاهيم والمصطلحات الرئيسية
2.3.1. Think Outside the Box
3.3.1. الاختلافات بين القرصنة الهجومية والدفاعية
4.1. منهجيات الأمن الهجومي
1.4.1. PTES Penetration Testing Execution Standard
2.4.1. OWASP Open Web Application Security Project
3.4.1. Cyber Security Kill Chain
5.1. الأدوار والمسؤوليات الأمنية الهجومية
1.5.1. الملامح الرئيسية
2.5.1. Bug Bounty Hunters
3.5.1. Researching: فن البحث
6.1. ترسانة المدقق الهجومي
1.6.1. أنظمة التشغيل للقرصنةHacking
2.6.1. مقدمة في مراكز القيادة والتحكم 2
3.6.1. Metasploit: الأساسيات والاستخدام
4.6.1. موارد مفيدة
7.1. OSINT ذكاء مفتوح المصدر
1.7.1. أساسيات استخبارات نظام التشغيل OSINT
2.7.1. تقنيات وأدوات OSINT
3.7.1. تطبيقات استخبارات العمليات OSINT في الأمن الهجومي

8.1. Scripting: مقدمة في الأتمتة
1.8.1. أساسيات البرمجة النصية scripting
2.8.1. Scripting en Bash
3.8.1. Scripting en Python
9.1. تصنيف نقاط الضعف
1.9.1. CVE Common Vulnerabilities and Exposure
2.9.1. CWE Common Weakness Enumeration
3.9.1. CAPEC Common Attack Pattern Enumeration and Classification
4.9.1. CVSS Common Vulnerability Scoring System
5.9.1. MITRE ATT & CK
10.1. الأخلاقيات و hacking
1.10.1. مبادئ أخلاقيات القراصنة hacker
2.10.1. الخط الفاصل بين القرصنة الأخلاقية hacking القرصنة الخبيثة
3.10.1. الآثار والعواقب القانونية
4.10.1. دراسات حالة: المواقف الأخلاقية في الأمن السيبراني

الوحدة 2. الهجمات على أنظمة وشبكات Windows

1.2. الويندوز Windows والدليل النشط (Active Directory)
1.1.2. تاريخ وتطور الويندوز Windows
2.1.2. أساسيات الدليل النشط
3.1.2. وظائف وخدمات الدليل النشط
4.1.2. البنية العامة للدليل النشط
2.2. الشبكات في بيئات الدليل النشط
1.2.2. بروتوكولات الشبكة في الويندوز
2.2.2. نظام أسماء النطاقات (DNS) وعمله في الدليل النشط
3.2.2. أدوات تشخيص الشبكة
4.2.2. توزيع الشبكة في الدليل النشط
3.2. المصادقة والتخويل في الدليل النشط
1.3.2. عملية وتدفق التوثيق
2.3.2. أنواع الاعتمادات
3.3.2. تخزين وإدارة الاعتمادات
4.3.2. أمن المصادقة

4.2. الأذونات والسياسات في الدليل النشط
1.4.2. عناصر سياسة المجموعة (GPOs)
2.4.2. تنفيذ وإدارة عناصر سياسة المجموعة
3.4.2. ادارة ألتراخيص في الدليل النشط
4.4.2. نقاط الضعف والتخفيف من حدتها في التراخيص
5.2. أساسيات Kerberos
1.5.2. ما هو Kerberos؟
2.5.2. المكونات والتشغيل
3.5.2. التذاكر في Kerberos
4.5.2. Kerberos في سياق الدليل النشط
6.2. التقنيات المتقدمة في Kerberos
1.6.2. الهجمات الشائعة في Kerberos
2.6.2. إجراءات التخفيف والحماية
3.6.2. مراقبة حركة مرور Kerberos
4.6.2. الهجمات المتقدمة في Kerberos
7.2. Active Directory Certificate Services
1.7.2. أساسيات PKI
2.7.2. أدوار خدمات شهادات الدليل النشط ومكوناته
3.7.2. تهيئة خدمات شهادات الدليل النشط ADCS ونشرها
4.7.2. الأمان في ADCS
8.2. الهجمات والدفاعات في خدمات شهادات الدليل النشط Active Directory Certificate Services ADCS
1.8.2. نقاط الضعف الشائعة في ADCS
2.8.2. الهجمات وتقنيات الاستغلال
3.8.2. الدفاعات والتخفيف
4.8.2. مراقبة ADCS ومراجعتها
9.2. تدقيق الدليل النشط
1.9.2. أهمية التدقيق في الدليل النشط
2.9.2. أدوات التدقيق
3.9.2. الكشف عن الحالات الشاذة والسلوكيات المشبوهة
4.9.2. الاستجابة للحوادث والتعافي من آثارها

10.2. Azure AD

1.10.2. مفاهيم أساسيات Azure AD

2.10.2. المزامنة مع الدليل النشط المحلي

3.10.2. إدارة الهوية في Azure AD

4.10.2. التكامل مع التطبيقات والخدمات

الوحدة 3. تحليل البرمجيات الخبيثة Malware وتطويرها

1.3. تحليل البرمجيات الخبيثة Malware وتطويرها

1.1.3. تاريخ وتطور البرمجيات الخبيثة Malware

2.1.3. تصنيف البرمجيات الخبيثة وأنواعها Malware

3.1.3. تحليل البرامج الضارة

4.1.3. تطوير البرمجيات الخبيثة Malware

2.3. تهيئة البيئة

1.2.3. تهيئة الأجهزة الافتراضية Snapshotsg

2.2.3. أدوات تحليل البرمجيات الخبيثة Malware

3.2.3. أدوات تطوير البرمجيات الخبيثة Malware

3.3. أساسيات الويندوز

1.3.3. تنسيق ملف PE Portable Executable

2.3.3. العمليات والمسارات Threads

3.3.3. نظام الملفات والسجل

4.3.3. Windows Defender

4.3. تقنيات البرمجيات الخبيثة Malware الأساسية

1.4.3. توليد الرموز البرمجية Shellcode

2.4.3. تنفيذ الرمز الصوري Shellcode على القرص

3.4.3. القرص مقابل الذاكرة

4.4.3. تشغيل Shellcode في الذاكرة

5.3. تقنيات البرمجيات الخبيثة Malware الوسيطة

1.5.3. الثبات على الويندوز

2.5.3. المجلد الرئيسي

3.5.3. مفاتيح التسجيل

4.5.3. شاشات التوقف

6.3. تقنيات البرمجيات الخبيثةmalware المتقدمة

1.6.3. تشفير من shellcode XOR

2.6.3. تشفير من shellcode RSA

3.6.3. تشويش Strings

4.6.3. حقن العملية

7.3. تحليل البرامج الضارة الثابتة

1.7.3. تحليل Packers مع DIE Detect It Easy

2.7.3. تحليل المقاطع باستخدام PE-Bear

3.7.3. فك التجميع مع Ghidra

8.3. التحليل الديناميكي من malware

1.8.3. مراقبة السلوك مع Process Hacker

2.8.3. تحليل المكالمات API Monitor

3.8.3. تحليل تغييرات السجل Regshot

4.8.3. مراقبة طلبات الشبكة باستخدام TCPView

9.3. التحليل في .NET

1.9.3. مقدمة في .NET

2.9.3. فك التجميع باستخدام dnSpy

3.9.3. تصحيح الأخطاء باستخدام dnSpy

10.3. تحليل البرمجيات الخبيثة Malware الحقيقية

1.10.3. تهيئة البيئة

2.10.3. التحليل الثابت للبرمجيات الخبيثة Malware

3.10.3. التحليل الديناميكي من malware

4.10.3. إنشاء قواعد YARA

لا توجد جداول زمنية محددة مسبقاً أو جداول زمنية للتقييم. هذا ما يبدو عليه هذا التدريب التقني في TECH!"

05

المنهجية

يقدم هذا البرنامج التدريبي طريقة مختلفة للتعلم. فقد تم تطوير منهجيتنا من خلال أسلوب التعليم المرتكز على التكرار: ***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 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.

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

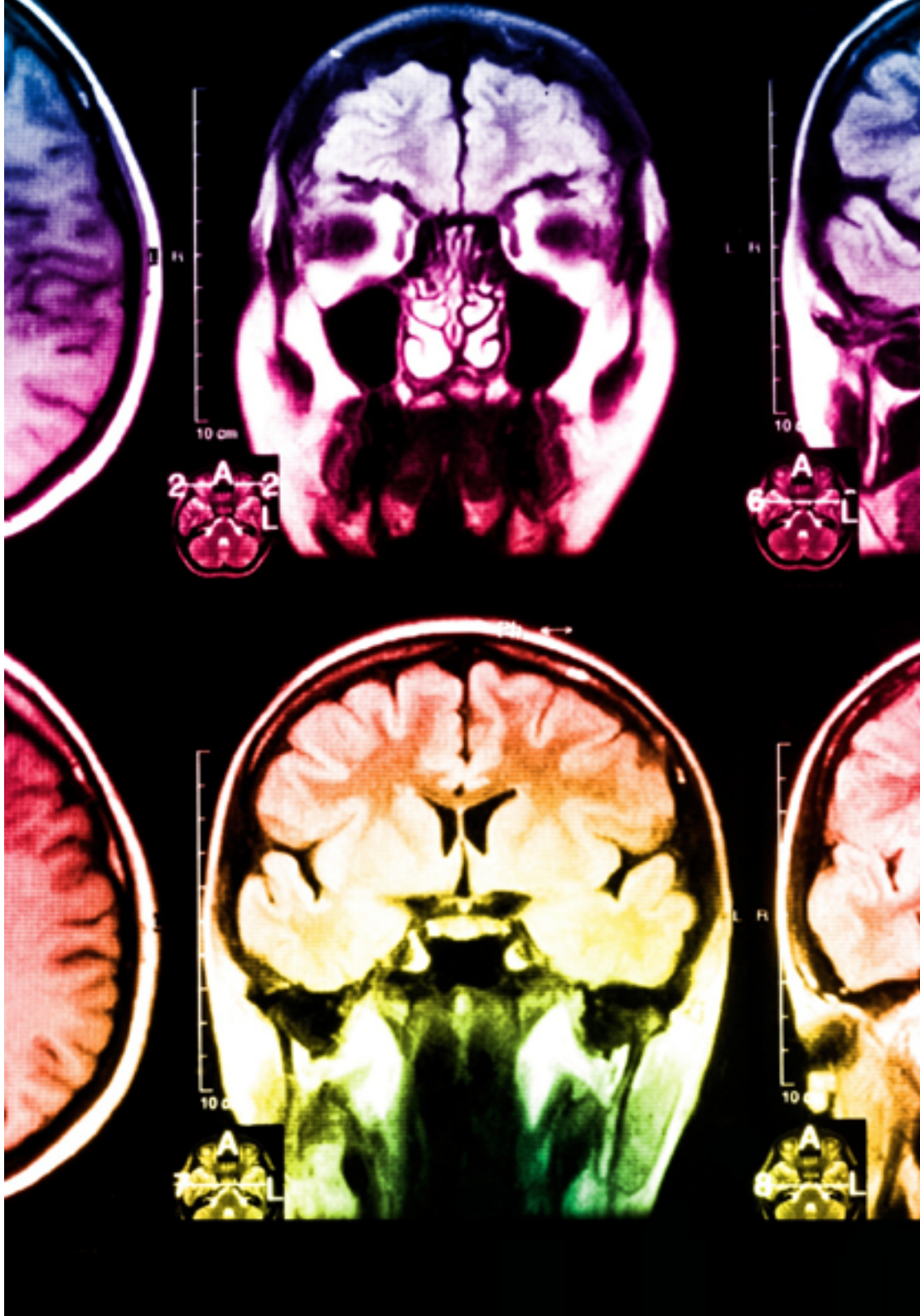
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

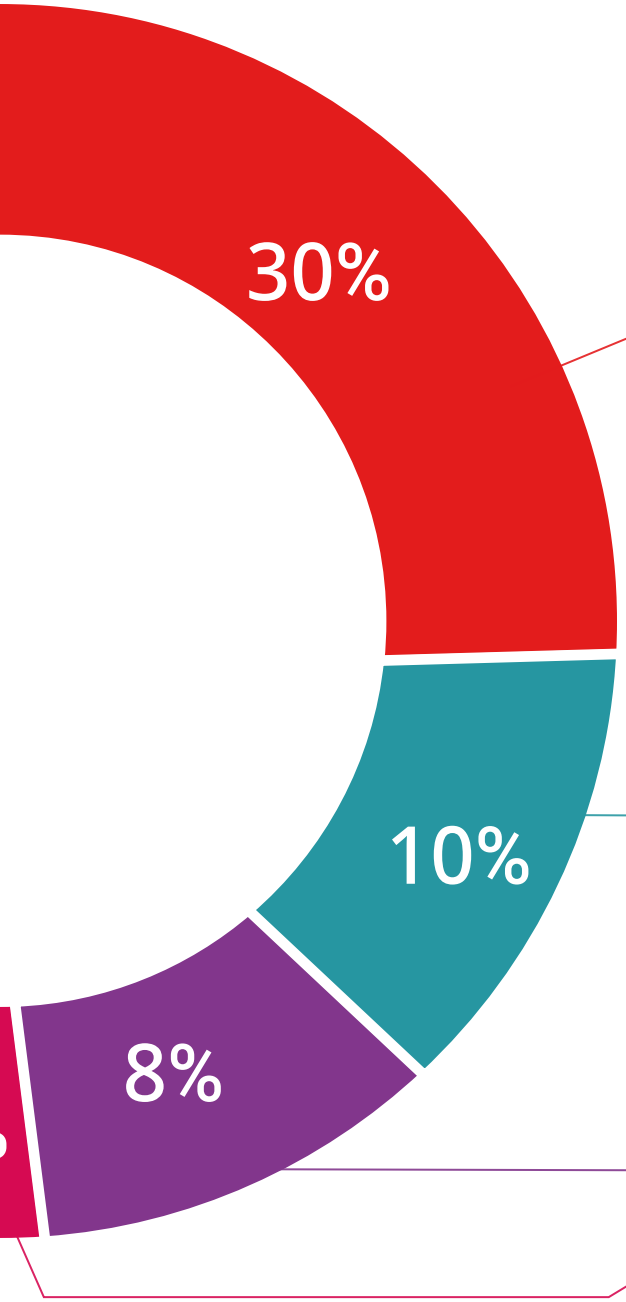
في برنامجنا، التعلم ليس عملية خطية، ولكنه يحدث في شكل لولبي (نتعلّم ثم نطرح ماتعلمناه جانبًا فننساه ثم نعيد تعلمه). لذلك، نقوم بدمج كل عنصر من هذه العناصر بشكل مركزي. باستخدام هذه المنهجية، تم تدريب أكثر من 650000 خريج جامعي بنجاح غير مسبوق في مجالات متنوعة مثل الكيمياء الحيوية، وعلم الوراثة، والجراحة، 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.

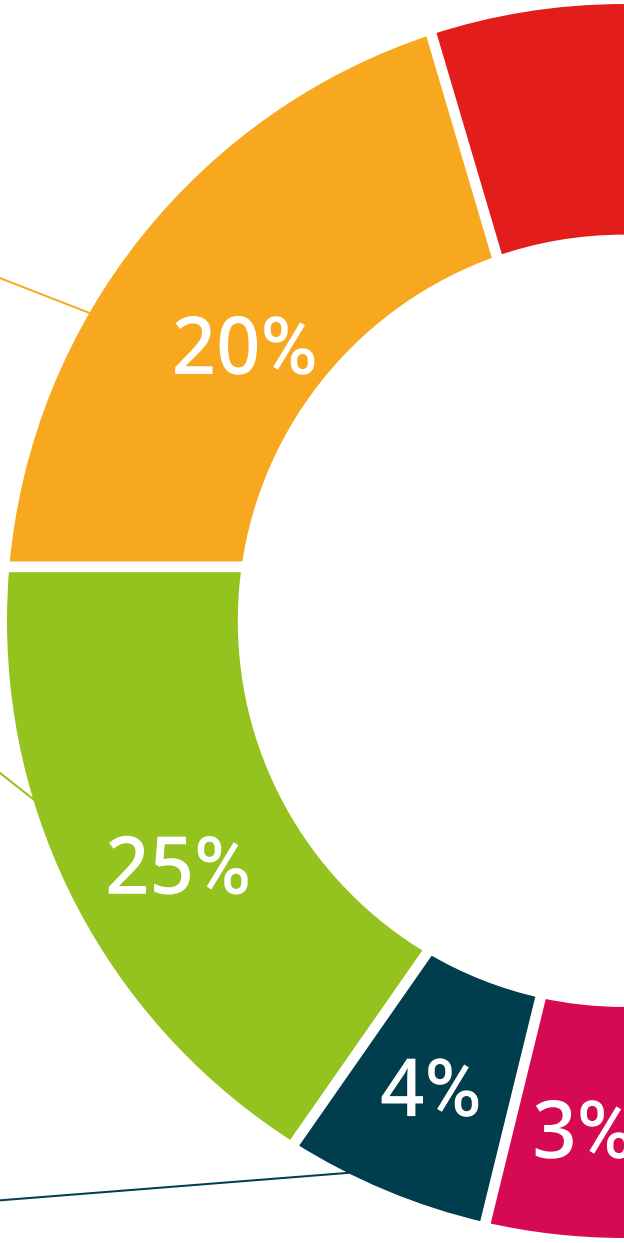
ملخصات تفاعلية

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 فى الأمن السيبراني الهجومي بالإضافة إلى التدريب الأكثر دقة وحداثة الحصول على مؤهل شهادة الخبرة الجامعية الصادر عن TECH الجامعة التكنولوجية.

اجتز هذا البرنامج بنجاح واحصل على مؤهلك العلمي الجامعى
دون الحاجة إلى السفر أو القيام بأية إجراءات مرهقة"

تحتوي **شهادة الخبرة الجامعية في الأمن السيبراني الهجومي** 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 الهجومي**

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 الهجومي

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 الهجومي

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

شهادة الخبرة الجامعية
الأمن السيبراني الهجومي

tech الجامعة التيكنولوجية