ماجيستير خاص
اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

ماجيستير خاص
اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **12 شهر**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

رابط الدخول إلى الموقع الإلكتروني: www.techtitute.com/ae/information-technology/proffesional-master-degree/master-pentesting-red-team

الفهرس

01

المقدمة

لقد وصل عدد الهجمات السيبرانية وتطورها إلى أبعاد تنذر بالخطر. مع الزيادة الهائلة في التهديدات، بدءاً من هجمات ransomwareإلى الاختراقات المتقدمة، فإن الحاجة إلى متخصصين مدربين تدريباً عالياً في مجال الأمن السيبراني أمر بالغ الأهمية. في هذا السياق ينشأ البرنامج الحالي، الذي لن يوفر فقط الانغماس الكامل في التقنيات الأمنية المتقدمة، بل سيتناول أيضًا واقع البيئة الرقمية المتطورة باستمرار. بهذه الطريقة، سيعمق الطلاب معرفتهم بتقنيات الهجوم والدفاع، ومواجهة التحديات الأمنية الأكثر تطوراً. انطلاقاً من الحاجة إلى تعزيز الدفاعات السيبرانية، يتميز هذا المنهج بمنهجيته التي تعتمد 100% عبر الإنترنت والاستخدام الفعال لمنهج إعادة التعلم (المعروف بـ Relearning) لتحسين التعلم.

سوف تقوم بتصميم بروتوكولات أمنية منيعة
بفضل هذا البرنامج الرائد، مع ضمانة من TECH"

إن مواكبة آخر المستجدات أمر حيوي للحفاظ على الفعالية في الدفاع ضد التهديدات الحالية والناشئة. في هذا الصدد، جعل التطور السريع للتكنولوجيا والتكتيكات السيبرانية من التحديث المستمر ضرورة حتمية. يؤكد انتشار التهديدات على الحاجة الملحة لوجود مهنيين مدربين تدريباً عالياً.

في هذا السياق، يُعتبر هذا البرنامج الجامعي استجابة ضرورية، حيث أنه لن يوفر فقط فهماً متعمقاً لأحدث التقنيات في مجال الأمن السيبراني، بل سيضمن أيضاً أن يكون المهنيون في طليعة من يواكبون أحدث الاتجاهات والتقنيات.

سيتناول الخريج في منهج درجة الماجستير في اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team) بشكل شامل المتطلبات في مجال الأمن السيبراني. ستنفذ تدابير أمنية فعالة للشبكة، بما في ذلك جدران الحماية وأنظمة كشف التسلل (IDS) وتجزئة الشبكة. تحقيقًا لهذه الغاية، سيطبق المتخصصون منهجيات التحقيق الجنائي الرقمي لحل القضايا، بدءًا من تحديد الهوية وحتى توثيق النتائج.

بالإضافة إلى ذلك، سيقومون بتطوير مهاراتهم في محاكاة التهديدات المتقدمة، ومحاكاة التكتيكات والتقنيات والإجراءات الأكثر استخداماً من قبل الجهات الخبيثة. علاوةً على ذلك، سيضمن النهج المبتكر الذي يتبعه مركز التكنولوجيا التكنولوجية اكتساب المهارات القابلة للتطبيق والقيمة في بيئة العمل في مجال الأمن السيبراني.

تعزز منهجية المسار الأكاديمي من طابعه المبتكر، حيث سيوفر بيئة تعليمية 100% عبر الإنترنت. سيكون هذا البرنامج مصمماً خصيصاً لتلبية احتياجات المهنيين المشغولين الذين يتطلعون إلى التقدم في حياتهم المهنية. بالمثل يستند منهج إعادة التعلم (المعروف بـ Relearning) إلى تكرار المفاهيم الرئيسية لإرساء المعرفة وتيسير التعلم. بهذه الطريقة، فإن الجمع بين المرونة والنهج التربوي القوي لن يجعلها سهلة المنال فحسب، بل سيجعلها فعالة للغاية في إعداد علماء الحاسوب لمواجهة التحديات الديناميكية للأمن السيبراني.

يحتوي هذا **الماجستير الخاص في اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)** على البرنامج التعليمي الأكثر اكتمالاً وحداثة في السوق أبرز خصائصها هي:

- تطوير الحالات العملية التي يقدمها خبراء اختبارات الاختراق (pentesting) والفريق 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
- توفر المحتوى من أي جهاز ثابت أو محمول متصل بالإنترنت

في غضون 12 شهرًا فقط ستعطي
حياتك المهنية الدفعة التي تحتاجها.
قم بالتسجيل الآن واختبر التقدم الفوري!"

هل ترغب في تحقيق قفزة نوعية في حياتك المهنية؟ مع TECH سيتم تدريبك على تنفيذ استراتيجيات التنفيذ الفعال لمشاريع الأمن السيبراني"

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.

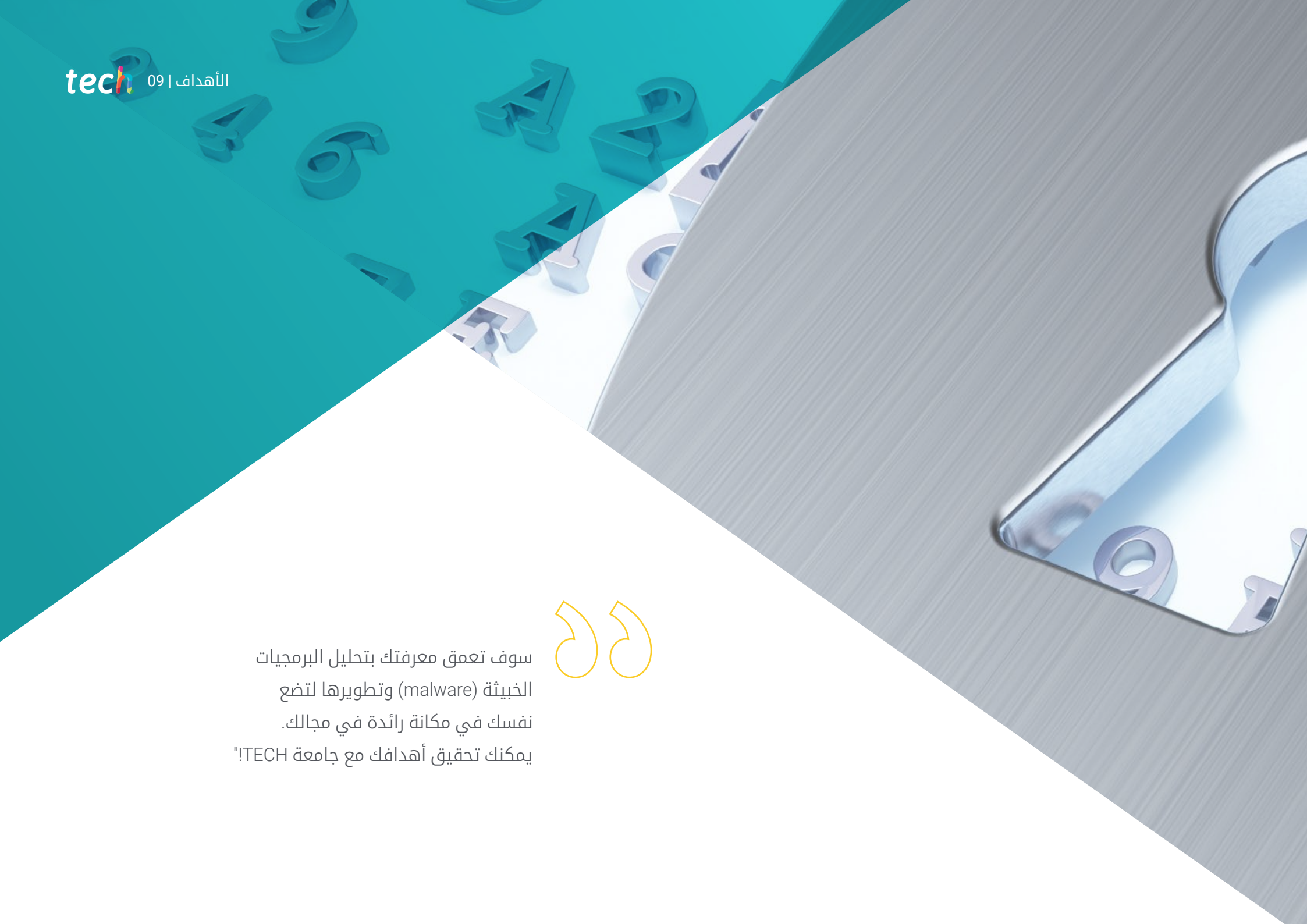
سوف تتعلم المزيد عن تحديد وتقييم الثغرات الأمنية في تطبيقات الويب، وذلك بفضل أفضل جامعة رقمية في العالم وفقاً لمجلة Forbes.

سوف تتقن تقنيات الطب الشرعي في بيئات اختبارات الاختراق (pentesting). ضع نفسك كخبير الأمن السيبراني الذي تبحث عنه كل شركة.

02

الأهداف

الهدف الرئيسي لهذا المسار الأكاديمي هو تدريب الخريجين على اختبار الاختراق ومحاكاة الفريق الأحمر (Red Team). طوال فترة البرنامج، سينغمس علماء الحاسوب في نهج عملي ومتخصص، حيث سيتم تطوير مهارات التعامل مع تحديد واستغلال نقاط الضعف في الأنظمة والشبكات. بالإضافة إلى ذلك، صُمم هذا المنهج الدراسي لتوفير فهم متعمق لتكتيكات واستراتيجيات الأمن السيبراني، وإعداد الطلاب لمواجهة تحديات العالم الحقيقي والريادة في التنفيذ الفعال لتدابير الأمن السيبراني.



سوف تعمق معرفتك بتحليل البرمجيات الخبيثة (malware) وتطويرها لتضع نفسك في مكانة رائدة في مجالك.
يمكنك تحقيق أهدافك مع جامعة TECH!"

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 اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)
- 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

ستحقق أهدافك بفضل أدوات TECH التعليمية، بما في ذلك مقاطع الفيديو التوضيحية والملخصات التفاعلية"

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 متخصصة في اختبارات الاختراق (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 اختبارات الاختراق (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 اختبارات الاختراق (pentesting)

الوحدة 2. إدارة فريق الأمن السيبراني

- تطوير مهارات القيادة الخاصة بفرق الأمن السيبراني، بما في ذلك القدرة على التحفيز والإلهام وتنسيق الجهود لتحقيق الأهداف المشتركة
- تعلّم كيفية تخصيص الموارد بكفاءة داخل فريق الأمن السيبراني مع مراعاة المهارات الفردية وزيادة إنتاجية المشروع إلى أقصى حد ممكن
- تحسين مهارات التواصل الخاصة بالبيئات التقنية، وتسهيل التفاهم والتنسيق بين أعضاء الفريق
- تعلم استراتيجيات تحديد النزاعات وإدارتها داخل فريق الأمن السيبراني، وتعزيز بيئة عمل تعاونية وفعالة
- تعلم كيفية إنشاء مقاييس وأنظمة تقييم لقياس أداء فريق الأمن السيبراني وإجراء التعديلات حسب الحاجة
- تعزيز إدماج الممارسات الأخلاقية في إدارة فرق الأمن السيبراني، وضمان إجراء جميع الأنشطة بطريقة أخلاقية وقانونية
- تطوير الكفاءات اللازمة للتحضير والإدارة الفعالة لحوادث الأمن السيبراني، بما يضمن الاستجابة السريعة والفعالة للتهديدات

الوحدة 3. إدارة المشاريع الأمنية

- تطوير مهارات تخطيط مشاريع الأمن السيبراني وتحديد الأهداف والنطاق والموارد والجداول الزمنية للتنفيذ
- تعلم استراتيجيات التنفيذ الفعال للمشاريع الأمنية، وضمان التنفيذ الناجح للتدابير المخطط لها
- تطوير مهارات الإدارة الفعالة للميزانيات وتخصيص الموارد في المشاريع الأمنية، وتعظيم الفعالية وتقليل التكاليف
- تحسين التواصل الفعال مع أصحاب المصلحة (stakeholders)، وتقديم التقارير والتحديثات بطريقة واضحة ومفهومة
- تعلم تقنيات مراقبة المشروع والتحكم فيه، وتحديد الانحرافات واتخاذ الإجراءات التصحيحية حسب الضرورة
- تعريف الطلاب بمنهجيات اختبارات الاختراق (pentesting) الرشيقة
- تطوير المهارات في التوثيق التفصيلي وإعداد التقارير، وتقديم صورة واضحة عن تقدم المشروع والنتائج المحققة
- تعزيز التعاون الفعال بين مختلف الفرق والتخصصات داخل المشاريع الأمنية، بما يضمن اتباع نهج شامل ومنسق
- تعلّم استراتيجيات لتقييم وقياس فعالية التدابير المنفذة وضمان التحسين المستمر للوضع الأمني للمؤسسة

الوحدة 4. الهجمات على أنظمة وشبكات Windows

- تطوير مهارات تحديد وتقييم نقاط الضعف المحددة في أنظمة تشغيل 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 الويندوز، مما يضمن استمرار أهمية وفعالية المهارات المكتسبة

الوحدة 5. قرصنة الويب المتقدمة

- تطوير مهارات تحديد وتقييم نقاط الضعف في تطبيقات الويب، بما في ذلك حقن SQL، وXSSs (Cross-Site Scripting)، وغيرها من نواقل الهجوم الشائعة
- تعلّم كيفية إجراء اختبارات الأمان على تطبيقات الويب الحديثة
- اكتساب مهارات في تقنيات اختراق الويب المتقدمة، واستكشاف استراتيجيات التحايل على التدابير الأمنية واستغلال الثغرات الأمنية المتطورة
- تعريف الخريج بتقييم الأمن في واجهات برمجة التطبيقات وخدمات الويب، وتحديد نقاط الضعف المحتملة وتعزيز الأمن في واجهات البرمجة
- تطوير المهارات اللازمة لتنفيذ تدابير التخفيف الفعّالة في تطبيقات الويب، والحد من التعرض للهجمات وتعزيز الأمن
- المشاركة في المحاكاة العملية لتقييم الأمن في بيئات الويب المعقدة، وتطبيق المعرفة في مواقف العالم الحقيقي
- تطوير الكفاءات في صياغة استراتيجيات دفاعية فعالة لحماية تطبيقات الويب من التهديدات الإلكترونية
- تعلّم كيفية مواءمة ممارسات اختراق الويب hacking web المتقدمة مع اللوائح والمعايير الأمنية ذات الصلة، بما يضمن الالتزام بالأطر القانونية والأخلاقية
- تعزيز التعاون الفعال بين فرق التطوير وفرق الأمن

الوحدة 6. بنية الشبكات وأمنها

- اكتساب معرفة متقدمة ببنية الشبكة، بما في ذلك الطوبولوجيات والبروتوكولات والمكونات الرئيسية
- تطوير المهارات اللازمة لتحديد وتقييم نقاط الضعف المحددة في البنى التحتية للشبكة، مع مراعاة التهديدات المحتملة.
- تعلّم كيفية تنفيذ تدابير أمنية فعّالة للشبكة، بما في ذلك firewalls الحماية وأنظمة كشف التسلل (IDS) وتجزئة الشبكة
- تعريف الطالب بتقنيات الشبكات الناشئة، مثل الشبكات المعرفة بالبرمجيات (SDN)، وفهم تأثيرها على الأمن
- تطوير المهارات في تأمين اتصالات الشبكة، بما في ذلك الحماية من التهديدات مثل sniffing وهجمات الوسطاء
- التعرف على كيفية تقييم تكوينات الأمان وتحسينها في بيئات شبكات المؤسسات، بما يضمن توفير الحماية الكافية
- تطوير المهارات اللازمة لتنفيذ تدابير التخفيف الفعالة ضد التهديدات التي تتعرض لها شبكات المؤسسات، بدءاً من الهجمات الداخلية وحتى التهديدات الخارجية
- تعزيز التعاون الفعال مع فرق الأمن، ودمج الاستراتيجيات والجهود المبذولة لحماية البنية التحتية للشبكة
- تعزيز الممارسات الأخلاقية والقانونية في تنفيذ تدابير أمن الشبكة، وضمان الالتزام بالمبادئ الأخلاقية في جميع الأنشطة

الوحدة 7. تحليل Malware وتطويرها

- اكتساب معرفة متقدمة بطبيعة البرمجيات الخبيثة ووظائفها وسلوكها، وفهم أشكالها وأهدافها المختلفة
- تطوير المهارات في التحليل الجنائي المطبق على malware، 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 malware لأغراض تعليمية ودفاعية، مما يتيح فهماً شاملاً للتكتيكات التي يستخدمها المهاجمون
- تعزيز الممارسات الأخلاقية والقانونية في تحليل 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 anti-malware، مع مراعاة فعاليتها وقدرتها على التكيف مع بيئات محددة
- التعرّف على كيفية تنفيذ إجراءات فعّالة للتخفيف من حدةmalware، والحد من تأثير وانتشار البرمجيات الخبيثة على الأنظمة والشبكات
- تعزيز التعاون الفعال مع فرق الأمن، وتكامل الاستراتيجيات والجهود للحماية من تهديدات البرمجيات malware
- إبقاء الخريج على اطلاع دائم بأحدث الاتجاهات والتقنيات المستخدمة في تحليل البرمجيات الخبيثة malwareوتطويرها، مما يضمن استمرار أهمية وفعالية المهارات المكتسبة

الوحدة 8. 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 اختبارات الاختراق (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 9. 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

الوحدة 10. التقرير التقني والتنفيذي

- تطوير المهارات اللازمة لإعداد تقارير تقنية مفصلة، وعرض النتائج والمنهجيات المستخدمة والتوصيات بشكل واضح وشامل
- تعلم كيفية التواصل الفعال مع الجمهور التقني باستخدام لغة دقيقة ومناسبة لنقل المعلومات التقنية المعقدة
- تطوير المهارات اللازمة لصياغة توصيات عملية وقابلة للتنفيذ تهدف إلى التخفيف من نقاط الضعف وتحسين الوضع الأمني
- تعلم كيفية تقييم التأثير المحتمل لنقاط الضعف التي تم تحديدها، مع مراعاة الجوانب التقنية والتشغيلية والاستراتيجية
- إطلاع المتعلم على أفضل الممارسات لإعداد التقارير التنفيذية، وتكييف المعلومات التقنية للجمهور غير التقني
- تطوير الكفاءات لمواءمة النتائج والتوصيات مع الأهداف الاستراتيجية والتشغيلية للمؤسسة
- تعلّم كيفية استخدام أدوات عرض البيانات لتمثيل المعلومات الواردة في التقارير بيانياً، مما يسهل فهمها
- الترويج لإدراج المعلومات ذات الصلة بالامتثال للوائح والمعايير في التقارير، وضمان الالتزام بالمتطلبات القانونية
- تعزيز التعاون الفعال بين الفرق التقنية والتنفيذية، بما يضمن فهم ودعم إجراءات التحسين المقترحة في التقرير

03

الكفاءات

بفضل هذا المنهج، سيتم تدريب الخريجين بمهارات متخصصة لتنفيذ تدابير دفاعية فعالة، وتعزيز أمن الأنظمة والشبكات بناءً على أفضل ممارسات الأمن السيبراني. بالإضافة إلى ذلك، سيكتسب الطلاب مهارات متقدمة في اختبار الاختراق ومحاكاة الفريق الأحمر Red Team، وسيتفوقون في تحديد الثغرات الاستباقية والتخفيف من حدتها. من هذا المنطلق، سيتقن المحترفون المهارات التقنية اللازمة للتعامل مع التهديدات في العالم الحقيقي، مما يؤهلهم لقيادة استراتيجيات تقييم وتحصين أمنية فعالة في البيئات السيبرانية الديناميكية. بالإضافة إلى ذلك، فإن النهج المتبع 100% عبر الإنترنت يجعل التعلم أكثر مرونة.

كن خبيراً في الأمن السيبراني من خلال 1800 ساعة من
أفضل محتوى الوسائط المتعددة، مع ختم الجودة من TECH"

الكفاءات العامة

- اكتساب الكفاءات في تخطيط وتنفيذ وإدارة مشاريع الأمن السيبراني، بما يضمن تحقيق نتائج فعالة وتحقيق الأهداف
- اكتساب معرفة متقدمة ببنية الشبكة وجوانبها الأمنية، وتقييم نقاط الضعف وتنفيذ استراتيجيات لتعزيز البنية التحتية
- تطوير الكفاءات في مجال الأدلة الجنائية الرقمية والاستجابة للحوادث، بدءاً من جمع الأدلة إلى التخفيف من حدة التهديدات واستعادة العمليات
- تطبيق التكتيكات المتقدمة في تخطيط وتنفيذ تمارين الفريق الأحمر Red Team، ومحاكاة سيناريوهات العالم الحقيقي لتقييم مرونة البنية التحتية واكتشاف نقاط الضعف وتحسين التأهب للتهديدات السيبرانية

"تعرّف على عملية تحديد وتقييم وتخفيف المخاطر الخاصة بمشاريع الأمن السيبراني. راهن على TECH!"

الكفاءات المحددة

- اكتساب مهارات التدريب من أجل التطوير المهني لأعضاء الفريق، وتعزيز النمو والتحسين
- تطوير مهارات اتخاذ القرارات الاستراتيجية في مواقف الأمن السيبراني، مع مراعاة التأثير قصير وطويل الأجل على الأمن المؤسسي
- اكتساب الكفاءات في تحديد وتقييم وتخفيف المخاطر الخاصة بمشاريع الأمن السيبراني
- تطوير المهارات اللازمة لتنفيذ تدابير الدفاع النشطة، وتعزيز أمن الأنظمة والشبكات القائمة
- تعلّم تقنيات تحليل حركة المرور على الويب لتحديد الأنماط والسلوكيات الشاذة، مما يسهل اكتشاف التهديدات المحتملة
- اكتساب المهارات في التحليل الجنائي المطبق على بيئات الشبكات، مما يتيح التعرف الفعال على الحوادث السيبرانية والاستجابة لها
- تعلّم استراتيجيات الكشف الفعّال عن البرمجيات الخبيثة والوقاية منها، بما في ذلك نشر حلول الأمان المتقدمة
- تطوير المهارات في تحديد مؤشرات الاختراق (IoC) أثناء التحقيق الجنائي، مما يسهل اكتشاف الحوادث والاستجابة لها
- اكتساب مهارات التخطيط الاستراتيجي لتمارين الفريق الأحمرRed Team، مع مراعاة الأهداف والنطاق والموارد والسيناريوهات الواقعية
- اكتساب المهارات في تحديد نقاط الضعف وترتيبها حسب الأولوية، وتسليط الضوء على تلك التي تشكل أكبر المخاطر الأمنية

04

هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

من أجل إنشاء هيئة تدريس الماجيستير الخاص في اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team) قامت TECH بجمع أفضل المتخصصين الذين يتمتعون بخلفية مهنية واسعة ومعترف بها في الشركات الرائدة في هذا القطاع.
في هذا الصدد، سيساهم كل عضو من أعضاء هيئة التدريس بخبرته العملية وخبرته في هذا المجال، مما يضمن استفادة الطلاب من تدريس متخصصين مؤهلين تأهيلاً عالياً. علاوة على ذلك، فإن الاختيار الدقيق لهؤلاء الخبراء لن يضمن فقط الجودة الأكاديمية، بل سيضمن أيضًا ملاءمة المحتوى وقابليته للتطبيق الفوري في بيئة الأمن السيبراني الديناميكية.

سيقودك عمالقة صناعة الأمن السيبراني
إلى النجاح في 12 شهراً فقط من خلال
هذا البرنامج الجامعي الحصري "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 في هندسة البرمجيات وتقنيات مجتمع المعلومات، جامعة مدريد التقنية السياسية
- التعاون مع المؤسسات التعليمية لتطوير دورات تدريبية عالية المستوى في مجال الأمن السيبراني

الأساتذة

أ. Siles Rubia, Marcelino

- Cibersecurity Engineer
- هندسة الأمن السيبراني في جامعة Rey Juan Carlos
- المعارف البرمجة التنافسية Web, Active Directory Hacking و Malware Development
- فائز في مسابقة AdaByron

أ. Redondo Castro, Pablo

- خبير اختراقات Pentester في مجموعة Oesía
- مهندس الأمن السيبراني من جامعة Rey Juan Carlos
- خبرة واسعة في Cibersecurity Evaluator Traineev
- مكتسب خبرة في التدريس، حيث يقدم دورات تدريبية متعلقة ببطولات Capture The Flag

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
- بكالوريوس في هندسة الحاسوب من جامعة البوليتكنيك في مدريد

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

أ. Villaverde, David

- مستشار الأمن السيبراني في Cipherbit
- خبير منصات تحدي القرصنة HackTheBox
- أخصائي اختبارات الاختراق
- خبير البرمجيات الخبيثة
- مهندس برمجيات متخصص في الأمن السيبراني من المركز الجامعي للتكنولوجيا والفنون الرقمية في Las Rozas

أ. Castillo, Carlos

- Red Teamer en Cipherbit و Cybersecurity Consultant
- Offensive Security Wireless Professional
- eLearnSecurity Web Application Penetration Tester
- eLearnSecurity Certified Professional Penetration Tester v2
- eLearnSecurity Junior Penetration Tester
- استشاري الأمن السيبراني
- مهندس برمجيات 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. Mora Navas, Sergio

- استشاري الأمن السيبراني في مجموعة Oesía
- مهندس في الأمن السيبراني من جامعة Rey Juan Carlos
- مهندس كمبيوتر من جامعة بورغوس

05

الهيكل والمحتوى

يقدم هذا البرنامج الجامعي انغماساً كاملاً في التخصصات الهامة لاختبار الاختراق ومحاكاة الفريق الأحمر (Red Team). سيطور الخريجون خلال الدورة مهارات متقدمة لتحديد واستغلال نقاط الضعف في الأنظمة والشبكات باستخدام التقنيات والأدوات الحديثة. صُمم هذا المؤهل العلمي بتركيز عملي لتجهيز المتخصصين في مجال الأمن السيبراني لمواجهة تحديات العالم الحقيقي. من هذا المنطلق، سيستفيد الطلاب من مزيج فريد من النظرية والتطبيق، بتوجيه من خبراء الصناعة، لتعزيز فهمهم وتنفيذ استراتيجيات التقييم الأمني في البيئات السيبرانية بفعالية.

سوف تكتسب فهماً متعمقاً للأدوار والمسؤوليات المختلفة لفريق الأمن السيبراني. سجل الآن!"

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. Penetration Testing Execution Standard (PTES)
2.4.1. Open Web Application Security Project (OWASP)
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 للقرصنة hacking
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. التقنيات والأدوات 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. Common Vulnerabilities and Exposure (CVE)
2.9.1. Common Weakness Enumeration (CWE)
3.9.1. Common Attack Pattern Enumeration and Classification (CAPEC)
4.9.1. Common Vulnerability Scoring System (CVSS)
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. إدارة فريق الأمن السيبراني

1.2. إدارة الفريق
1.1.2. من هو من
2.1.2. المدير
3.1.2. الاستنتاجات
2.2. الادوار والمسؤوليات
1.2.2. تحديد الدور
2.2.2. التفويض الفعال
3.2.2. إدارة التوقعات
3.2. بناء الفريق وتطويره
1.3.2. مراحل بناء الفريق
2.3.2. ديناميكيات المجموعة
3.3.2. التقييم والتغذية الراجعة

الوحدة 3. إدارة المشاريع الأمنية

1.3. إدارة المشاريع الأمنية
1.1.3. تعريف إدارة مشاريع الأمن السيبراني والغرض منها
2.1.3. التحديات الرئيسية
3.1.3. الاعتبارات
2.3. دورة حياة المشروع الأمني
1.2.3. المراحل الأولية وتحديد الأهداف
2.2.3. التطبيق والتنفيذ
3.2.3. التقييم والمراجعة
3.3. تخطيط الموارد وتقديرها
1.3.3. المفاهيم الأساسية للإدارة الاقتصادية
2.3.3. تحديد الموارد البشرية والتقنية
3.3.3. الميزانية والتكاليف المرتبطة بها
4.3. تنفيذ المشروع ورصده
1.4.3. المراقبة والمتابعة
2.4.3. التكيف والتغييرات في المشروع
3.4.3. تقييم منتصف المدة والمراجعات
5.3. الاتصال بالمشروع وإعداد التقارير
1.5.3. استراتيجيات الاتصال الفعال
2.5.3. إعداد التقارير والعروض التقديمية
3.5.3. التواصل مع العميل والإدارة
6.3. الأدوات والتقنيات
1.6.3. أدوات التخطيط والتنظيم
2.6.3. أدوات التعاون والتواصل
3.6.3. أدوات التوثيق والتخزين
7.3. الوثائق والبروتوكولات
1.7.3. هيكلة الوثائق وإنشاءها
2.7.3. بروتوكولات العمل
3.7.3. الدليل

4.2. إدارة الموهبة
1.4.2. تحديد المواهب
2.4.2. بناء القدرات
3.4.2. الاحتفاظ بالمواهب
5.2. قيادة الفريق والتحفيز
1.5.2. أساليب القيادة
2.5.2. نظريات التحفيز
3.5.2. الاعتراف بالإنجازات
6.2. التواصل والتنسيق
1.6.2. أدوات الاتصال
2.6.2. حواجز التواصل
3.6.2. استراتيجيات التنسيق
7.2. التخطيط الاستراتيجي لتطوير الموظفين
1.7.2. تحديد احتياجات التدريب
2.7.2. خطط التنمية الفردية
3.7.2. الرصد والتقييم
8.2. تسوية المنازعات
1.8.2. تحديد التعارضات
2.8.2. طرق القياس
3.8.2. منع نشوب النزاعات
9.2. إدارة الجودة والتحسين المستمر
1.9.2. مبادئ الجودة
2.9.2. تقنيات التحسين المستمر
3.9.2. الملاحظات والتعليقات Feedback
10.2. الأدوات والتقنيات
1.10.2. المنصات التعاونية
2.10.2. إدارة المشاريع
3.10.2. الاستنتاجات

8.3. اللوائح التنظيمية والامتثال في مشاريع الأمن السيبراني
1.8.3. القوانين واللوائح الدولية
2.8.3. الامتثال
3.8.3. عمليات التدقيق
9.3. إدارة المخاطر في المشاريع الأمنية
1.9.3. تحديد المخاطر وتحليلها
2.9.3. استراتيجيات التخفيف من المخاطر
3.9.3. مراقبة المخاطر ومراجعتها
10.3. إغلاق المشروع
1.10.3. المراجعة والتقييم
2.10.3. الوثائق النهائية
3.10.3. Feedback

الوحدة 4. الهجمات على أنظمة وشبكات Windows

1.4. الويندوز Windows والدليل النشط (Active Directory)
1.1.4. تاريخ وتطور الويندوز Windows
2.1.4. أساسيات الدليل النشط
3.1.4. وظائف وخدمات الدليل النشط
4.1.4. البنية العامة للدليل النشط
2.4. الشبكات في بيئات الدليل النشط
1.2.4. بروتوكولات الشبكة في الويندوز
2.2.4. نظام أسماء النطاقات (DNS) وعمله في الدليل النشط
3.2.4. أدوات تشخيص الشبكة
4.2.4. توزيع الشبكة في الدليل النشط
3.4. المصادقة والتخويل في الدليل النشط
1.3.4. عملية وتدفق التوثيق
2.3.4. أنواع الاعتمادات
3.3.4. تخزين وإدارة الاعتمادات
4.3.4. أمن المصادقة
4.4. الأذونات والسياسات في الدليل النشط
1.4.4. عناصر سياسة المجموعة (GPOs)
2.4.4. تنفيذ وإدارة عناصر سياسة المجموعة
3.4.4. ادارة ألتراخيص في الدليل النشط
4.4.4. نقاط الضعف والتخفيف من حدتها في التراخيص
5.4. أساسيات Kerberos
1.5.4. ما هو Kerberos؟
2.5.4. المكونات والتشغيل
3.5.4. التذاكر في Kerberos
4.5.4. Kerberos في سياق الدليل النشط
6.4. التقنيات المتقدمة في Kerberos
1.6.4. الهجمات الشائعة في Kerberos
2.6.4. إجراءات التخفيف والحماية
3.6.4. مراقبة حركة مرور Kerberos
4.6.4. الهجمات المتقدمة في Kerberos
7.4. Active Directory Certificate Services ADCS
1.7.4. أساسيات PKI
2.7.4. أدوار خدمات شهادات الدليل النشط ومكوناته
3.7.4. تهيئة خدمات شهادات الدليل النشط ADCS ونشرها
4.7.4. الأمان في ADCS
8.4. الهجمات و الدفاعات في خدمات شهادات الدليل النشط (ADCS)
1.8.4. نقاط الضعف الشائعة في ADCS
2.8.4. الهجمات وتقنيات الاستغلال
3.8.4. الدفاعات والتخفيف
4.8.4. مراقبة ADCS ومراجعتها
9.4. تدقيق الدليل النشط
1.9.4. أهمية التدقيق في الدليل النشط
2.9.4. أدوات التدقيق
3.9.4. الكشف عن الحالات الشاذة والسلوكيات المشبوهة
4.9.4. الاستجابة للحوادث والتعافي من آثارها
10.4. Azure AD
1.10.4. مفاهيم أساسيات Azure AD
2.10.4. المزامنة مع الدليل النشط المحلي
3.10.4. إدارة الهوية في Azure AD
4.10.4. التكامل مع التطبيقات والخدمات

الوحدة 5. قرصنة Hacking الويب Web المتقدمة

1.5. طريقة عمل الموقع الإلكتروني
1.1.5. URL وأجزاؤه
2.1.5. طرق HTTP
3.1.5. رؤوس الصفحات
4.1.5. كيفية عرض طلبات الويب باستخدام حزمة Burp Suite
2.5. الحلقات
1.2.5. ملفات تعريف الارتباط
2.2.5. رموز JWT Tokens
3.2.5. هجمات سرقة الحسابات
4.2.5. هجمات JWT
3.5. Cross Site Scripting XSS
1.3.5. ما هو ال XSS؟
2.3.5. أنواع XSS
3.3.5. استغلال XSS
4.3.5. مقدمة في XSLeaks
4.5. الضخ إلى قاعدة البيانات
1.4.5. ما هو حقن SQL
2.4.5. استخراج المعلومات باستخدام SQLi
3.4.5. Error-Basedg SQLi Blind, Time-Based
4.4.5. حقن NoSQLi
5.5. Local File Inclusion و Path Traversal
1.5.5. ماهيتهما واختلافاتهما
2.5.5. المرشحات الشائعة وكيفية تجاوزها
3.5.5. Log poisoning
4.5.5. LFIs في PHP
6.5. Broken Authentication
1.6.5. User Enumeration
2.6.5. Password Bruteforce
3.6.5. FA Bypass2
4.6.5. ملفات تعريف Cookies الارتباط التي تحتوي على معلومات حساسة وقابلة للتعديل
7.5. Remote Command Execution
1.7.5. Command Injection
2.7.5. Blind Command Injection
3.7.5. إلغاء التسلسل غير الآمن PHP
4.7.5. إلغاء التسلسل غير الآمن جافا Java
8.5. File Uploads
1.8.5. webshells عبر Remote Code Execution
2.8.5. XSS في تحميل الملفات
3.8.5. XML External Entity (XXE) Injection
4.8.5. اجتياز المسار في تحميل الملفات Path traversal
9.5. Broken Acess Control
1.9.5. الوصول غير المقيد إلى اللوحات
2.9.5. Insecure direct object references IDOR
3.9.5. تجاوز المرشح
4.9.5. طرق التفويض غير كافية
10.5. نقاط ضعف DOM والهجمات الأكثر تقدمًا
1.10.5. Regex Denial of Service
2.10.5. DOM Clobbering
3.10.5. Prototype Pollution
4.10.5. HTTP Request Smuggling

الوحدة 6. بنية الشبكات وأمنها

1.6. شبكات الحاسوب
1.1.6. مفاهيم أساسية: بروتوكولات LAN, WAN, CP, CC
2.1.6. نموذج OSI TCP / IP
3.1.6. Switching. مفاهيم أساسية
4.1.6. Routing. مفاهيم أساسية
2.6. Switching.
1.2.6. مقدمة في VLAN's
2.2.6. بروتوكول الشجرة المتفرعة STP
3.2.6. EtherChannel
4.2.6. الهجمات على الطبقة 2

3.6. الشبكات المحلية الافتراضية VLAN´s
1.3.6. أهمية الشبكات المحلية الافتراضية VLAN
2.3.6. ثغرات الشبكات المحلية الافتراضية VLAN's
3.3.6. الهجومات الشائعة في VLAN
4.3.6. تخفيف الآثار
4.6. Routing
1.4.6. عنونة IPv - 4IP و 6IPv
2.4.6. التوجيه: المفاهيم الرئيسية
3.4.6. التوجيه الثابت
4.4.6. التوجيه الديناميكي: المقدمة
5.6. بروتوكول IGP
1.5.6. Routing Information Protocol RIP
2.5.6. Open Shortest Path First OSPF
3.5.6. RIP مقابل OSPF
4.5.6. تحليل احتياجات الطوبولوجيا
6.6. الحماية المحيطية
1.6.6. المناطق العازلة DMZs
2.6.6. جدران الحماية
3.6.6. البنى الشائعة
4.6.6. Zero Trust Network Access
7.6. IPS Intrusion Prevention System و IDS Intrusion Detection System
1.7.6. الخصائص
2.7.6. التنفيذ
3.7.6. SIEM و SIEM CLOUDS
4.7.6. الكشف المستند إلى HoneyPots
8.6. TLS وشبكات VPN
1.8.6. SSL/TLS
2.8.6. TLS: الهجمات الشائعة
3.8.6. شبكات VPN مع TLS
4.8.6. شبكات VPN مع IPSEC

9.6. أمان الشبكة اللاسلكية
1.9.6. مقدمة إلى الشبكات اللاسلكية
2.9.6. بروتوكولات
3.9.6. العناصر الرئيسية
4.9.6. الهجمات الشائعة
10.6. شبكات الأعمال وكيفية التعامل معها
1.10.6. التقسيم المنطقي
2.10.6. التقسيم المادي
3.10.6. التحكم في الوصول
4.10.6. التدابير الأخرى التي يجب أخذها في الاعتبار

الوحدة 7. تحليل البرمجيات الخبيثة Malware وتطويرها

1.7. تحليل البرمجيات الخبيثة Malware وتطويرها
1.1.7. تاريخ وتطور البرمجيات الخبيثة Malware
2.1.7. تصنيف البرمجيات الخبيثة وأنواعها Malware
3.1.7. تحليل البرامج الضارة
4.1.7. تطوير البرمجيات الخبيثة Malware
2.7. تهيئة البيئة
1.2.7. تهيئة الأجهزة الافتراضية Snapshotsg
2.2.7. أدوات تحليل البرمجيات الخبيثة Malware
3.2.7. أدوات تطوير البرمجيات الخبيثة Malware
3.7. أساسيات الويندوز
1.3.7. تنسيق ملف Portable Executable
2.3.7. العمليات والمسارات Threads
3.3.7. نظام الملفات والسجل
4.3.7. Windows Defender
4.7. تقنيات البرمجيات الخبيثة Malware الأساسية
1.4.7. توليد الرموز البرمجية Shellcode
2.4.7. تنفيذ الرمز الصوري Shellcode على القرص
3.4.7. القرص مقابل الذاكرة
4.4.7. تنفيذ الرمز shellcode الصوري داخل الذاكرة

7.5. تقنيات البرمجيات الخبيثة Malware الوسيطة
7.5.1. الثبات على الويندوز
7.5.2. المجلد الرئيسي
7.5.3. مفاتيح التسجيل
7.5.4. شاشات التوقف
7.6. تقنيات البرمجيات الخبيثةmalware المتقدمة
7.6.1. تشفير من shellcode XOR
7.6.2. تشفير من shellcode RSA
7.6.3. تشويش Strings
7.6.4. حقن العملية
7.7. التحليل الثابت من Malware
7.7.1. تحليل Packers مع DIE Detect It Easy
7.7.2. تحليل المقاطع باستخدام PE-Bear
7.7.3. فك التجميع مع Ghidra
7.8. التحليل الديناميكي من malware
7.8.1. مراقبة السلوك مع Process Hacker
7.8.2. تحليل المكالمات API Monitor
7.8.3. تحليل تغييرات السجل Regshot
7.8.4. مراقبة طلبات الشبكة باستخدام TCPView
7.9. التحليل في.NET
7.9.1. مقدمة في.NET
7.9.2. فك التجميع باستخدام dnSpy
7.9.3. تصحيح الأخطاء باستخدام dnSpy
7.10. تحليل البرمجيات الخبيثة Malware الحقيقية
7.10.1. تهيئة البيئة
7.10.2. التحليل الثابت للبرمجيات الخبيثة Malware
7.10.3. التحليل الديناميكي من malware
7.10.4. إنشاء قواعد YARA

الوحدة 8. أساسيات الطب الشرعي و DFIR

1.8. فورينس ديجيتال
1.1.8. تاريخ الطب الشرعي الحاسوبي وتطوره
2.1.8. أهمية الأدلة الجنائية الحاسوبية في الأمن السيبراني
3.1.8. تاريخ الطب الشرعي الحاسوبي وتطوره
2.8. أساسيات الأدلة الجنائية الحاسوبية
1.2.8. سلسلة العهدة وتنفيذها
2.2.8. أنواع الأدلة الرقمية
3.2.8. عمليات الحصول على الأدلة
3.8. أنظمة الملفات وهيكل البيانات
1.3.8. أنظمة الملفات الرئيسية
2.3.8. طرق إخفاء البيانات
3.3.8. تحليل البيانات الوصفية للملف وسماته
4.8. تحليل أنظمة التشغيل
1.4.8. تحليل الطب الشرعي لأنظمة ويندوز Windows
2.4.8. تحليل الطب الشرعي لأنظمة لينكس Linux
3.4.8. تحليل الطب الشرعي لأنظمة macOS
5.8. استعادة البيانات وتحليل الأقراص
1.5.8. استعادة البيانات من الوسائط التالفة
2.5.8. أدوات تحليل الأقراص
3.5.8. تفسير جداول تخصيص الملفات
6.8. تحليل الشبكة وحركة المرور
1.6.8. التقاط حزم الشبكة وتحليلها
2.6.8. تحليل سجلات جدار الحماية firewall
3.6.8. كشف التسلل إلى الشبكة
7.8. تحليل البرامج الضارة والشفرات البرمجية الخبيثة Malware
1.7.8. التصنيف البرمجيات الخبيثة malware وخصائصها
2.7.8. تحليل البرمجيات الخبيثة الثابتة والديناميكية malware
3.7.8. تقنيات التفكيك وتصحيح الأخطاء
8.8. تحليل السجلات والأحداث
1.8.8. أنواع السجلات في الأنظمة والتطبيقات
2.8.8. تفسير الأحداث ذات الصلة
3.8.8. أدوات تحليل السجل
9.8. الاستجابة للحوادث الأمنية
1.9.8. عملية الاستجابة للحوادث
2.9.8. إنشاء خطة الاستجابة للحوادث
3.9.8. التنسيق مع فرق الأمن
10.8. تقديم الأدلة والبراهين القانونية
1.10.8 . قواعد الأدلة الرقمية في المجال القانوني
2.10.8. إعداد تقارير الطب الشرعي
3.10.8. المثول أمام المحكمة كشاهد خبير

الوحدة 9. تمارين الفريق الأحمرRed Team المتقدمة

1.9. تقنيات التعرف المتقدمة
1.1.9. تعداد النطاقات الفرعية المتقدمة
2.1.9. Google Dorking متقدم
3.1.9. وسائل التواصل الاجتماعي و theHarvester
2.9. حملاتphishing المتقدمة
1.2.9. ما هو التصيد الاحتيالي بالوكيل العكسي؟ Reverse-Proxy Phishing
2.2.9. FA Bypass con Evilginx2
3.2.9. استخراج البيانات
3.9. تقنيات المثابرة المتقدمة
1.3.9. Golden Tickets
2.3.9. Silver Tickets
3.3.9. تقنية DCShadow
4.9. تقنيات التجنب المتقدمة
1.4.9. Bypass de AMSI
2.4.9. تعديل الأدوات الموجودة
3.4.9. تشويش Powershell
5.9. تقنيات الحركة الجانبية المتقدمة
1.5.9. Pass-the-Ticket PtT
2.5.9. Overpass-the-Hash Pass-the-Key
3.5.9. NTLM Relay
6.9. تقنيات ما بعد الاستغلال المتقدمة
1.6.9. Dump de LSASS
2.6.9. Dump de SAM
3.6.9. هجوم DCSync

7.9. تقنيات التمحور المتقدمة pivoting
1.7.9. ما هو التمحور pivoting
2.7.9. الربط مع SSH
3.7.9. إزميل مخروطي محوريPivoting con Chisel
8.9. الاقتحامات الجسدية
1.8.9. المراقبة والاستطلاع
2.8.9. التخييم في الخلفية Tailgating و التحميل على الظهرPiggybacking
3.8.9. فتح الأقفال Lock-Picking
9.9. هجمات Wi-Fi
1.9.9. الهجمات على PSK 2WPA/WPA
2.9.9. هجمات Rogue AP
3.9.9. الهجمات على Enterprise 2WPA
10.9. هجمات الترددات اللاسلكية RFID
1.10.9. قراءة بطاقة RFID
2.10.9. التلاعب بطاقة RFID
3.10.9. إنشاء بطاقات مستنسخة

الوحدة 10. التقرير التقني والتنفيذي

1.10. عملية إعداد التقارير
1.1.10. هيكل التقرير
2.1.10. عملية إعداد التقارير
3.1.10. المفاهيم الرئيسية
4.1.10. التنفيذي مقابل التقني
2.10. الدليل
1.2.10. المقدمة
2.2.10. أنواع الدلائل
3.2.10. الدلائل الإرشادية الوطنية
4.2.10. حالات الاستخدام
3.10. المنهجيات
1.3.10. التقييم
2.3.10. أختبارات الاختراق
3.3.10. مراجعة المنهجيات الشائعة
4.3.10. مقدمة في المنهجيات الوطنية
4.10. النهج التقني لمرحلة إعداد التقارير
1.4.10. فهم حدود اختبارات الاختراق (pentesting)
2.4.10. استخدام اللغة والإشارات
3.4.10. عرض المعلومة
4.4.10. الأخطاء الشائعة
5.10. النهج التنفيذي لمرحلة إعداد التقارير
1.5.10. تكييف التقرير مع السياق
2.5.10. استخدام اللغة والإشارات
3.5.10. التوحيد القياسي
4.5.10. الأخطاء الشائعة
6.10. Open Source Security Testing Methodology Manual, OSSTMM
1.6.10. فهم المنهجية
2.6.10. الاعتراف
3.6.10. الوثائق
4.6.10. صياغة التقرير
7.10. شهادة LINCE
1.7.10. فهم المنهجية
2.7.10. الاعتراف
3.7.10. الوثائق
4.7.10. صياغة التقرير
8.10. الإبلاغ عن الثغرات الأمنية
1.8.10. المفاهيم الرئيسية
2.8.10. تحديد النطاق الكمي
3.8.10. نقاط الضعف والأدلة
4.8.10. الأخطاء الشائعة
9.10. تركيز التقرير على العميل
1.9.10. أهمية اختبارات العمل
2.9.10. الحلول والتخفيف
3.9.10. البيانات الحساسة و المهمة
4.9.10. أمثلة عملية وحالات
10.10. إعادة الإبلاغ عن التقارير Retakes
1.10.10. المفاهيم الرئيسية
2.10.10. فهم المعلومات الموروثة
3.10.10. التحقق من الأخطاء
4.10.10. إضافة المعلومات

06

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.

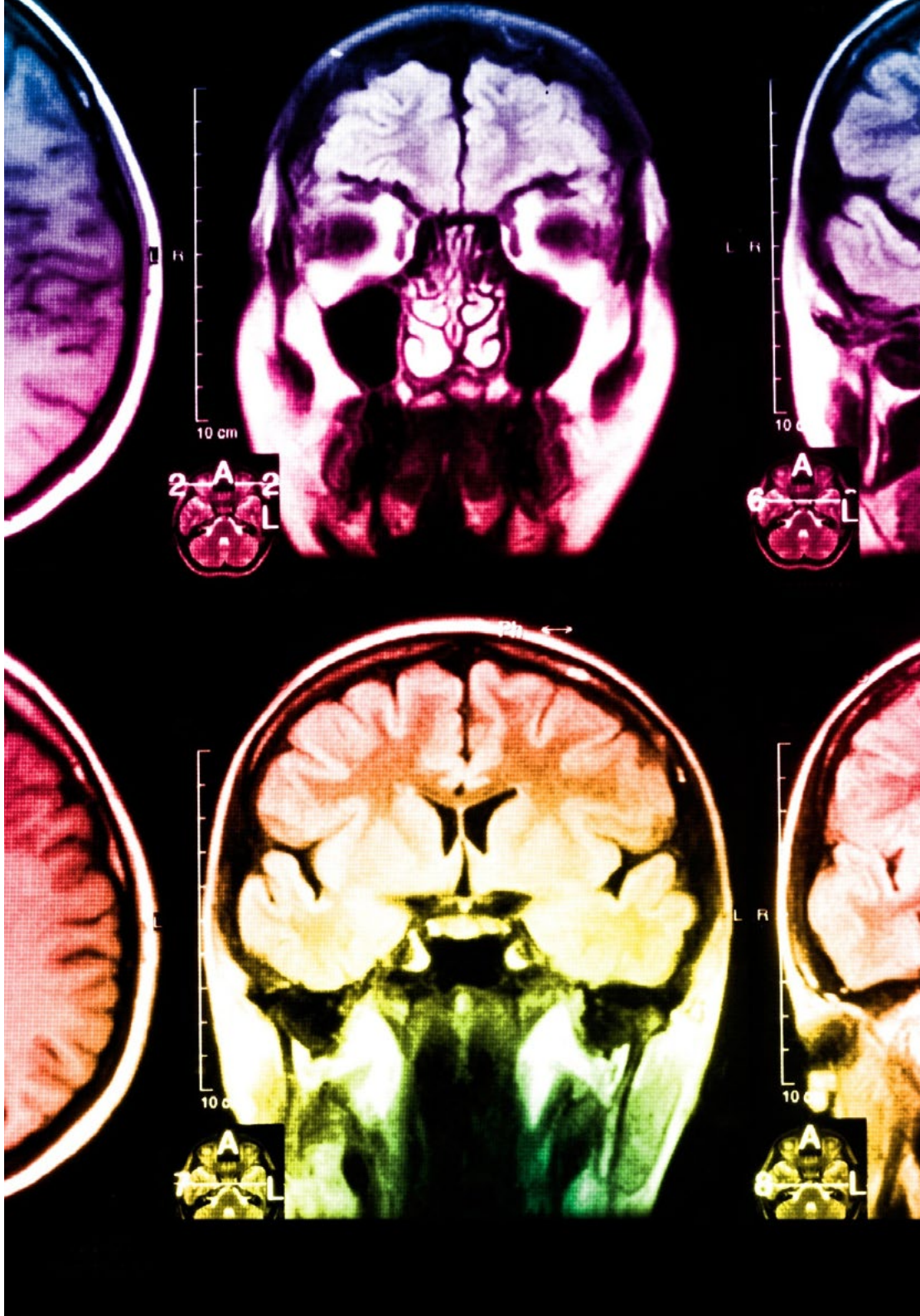
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

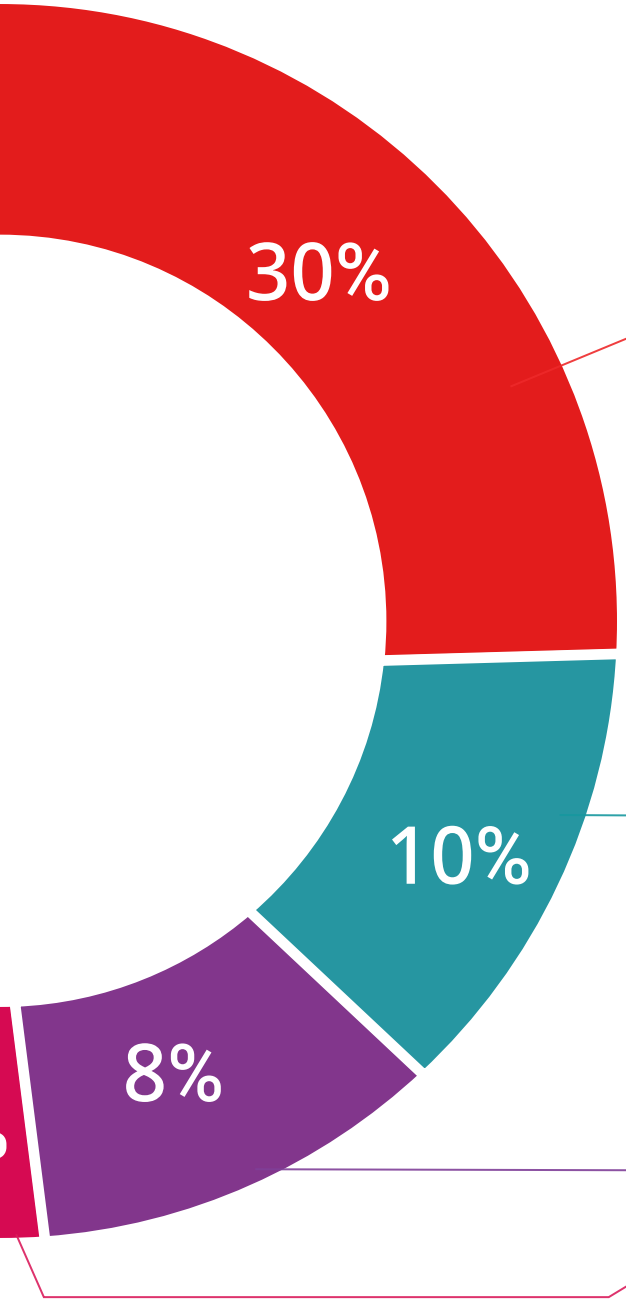
في برنامجنا، التعلم ليس عملية خطية، ولكنه يحدث في شكل لولبي (نتعلّم ثم نطرح ماتعلمناه جانبًا فننساه ثم نعيد تعلمه). لذلك، نقوم بدمج كل عنصر من هذه العناصر بشكل مركزي. باستخدام هذه المنهجية، تم تدريب أكثر من 650000 خريج جامعي بنجاح غير مسبوق في مجالات متنوعة مثل الكيمياء الحيوية، وعلم الوراثة، والجراحة،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

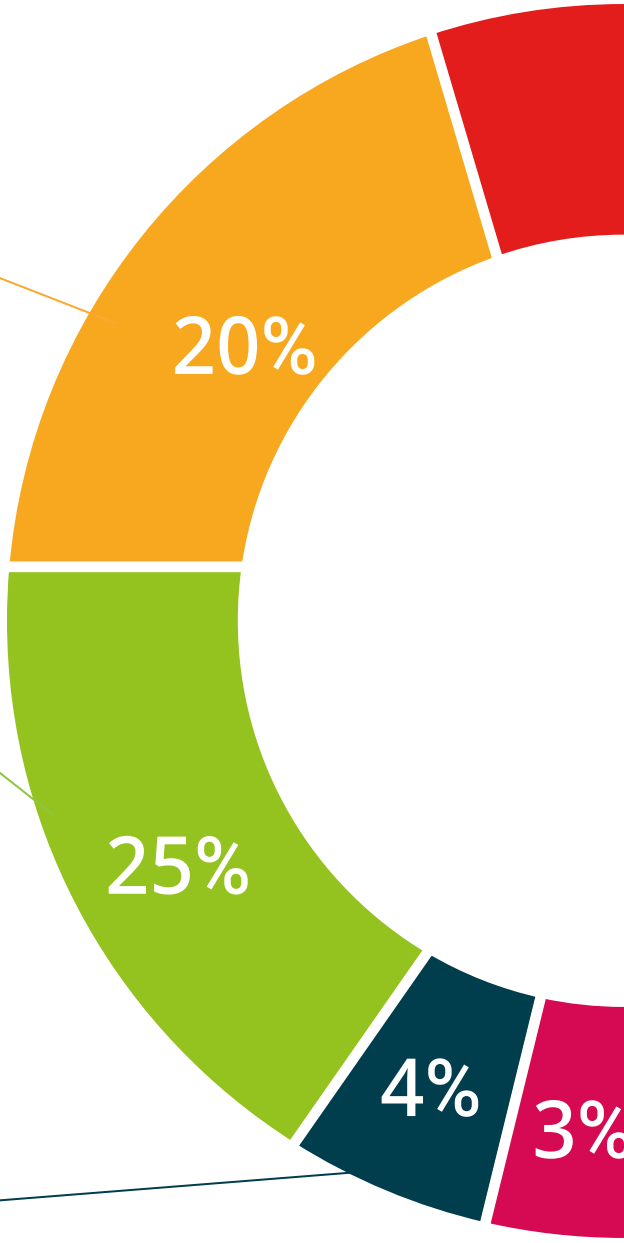
ملخصات تفاعلية

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.



07

المؤهل العلمي

يضمن الماجستير الخاص في فن اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)، الحصول على مؤهل الماجستير الخاص الصادر عن TECH الجامعة التكنولوجية.

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

تحتوي درجة **الماجستير الخاص في اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)** على البرنامج العلمي الأكثر اكتمالا وحداثة في السوق.

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

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

المؤهل العلمي: **ماجيستير خاص في اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)**

طريقة الدراسة: **عبر الإنترنت**

مدة الدراسة: **12 شهر**


tech الجامعة التكنولوجية

شهادة تخرج

هذه الشهادة ممنوحة إلى

لـ

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

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

ماجستير خاص

في

اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)

وهي شهادة خاصة من هذه الجامعة موافقة لـ 1500
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


ماجستير خاص في اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)

التوزيع العام للخطة الدراسية

نوع المادة	عدد الساعات
(OB) إجباري	1500
(OP) إختياري	0
(PR) الممارسات الخارجية	0
(TFM) مشروع تخرج الماجيستير	0
الإجمالي	1500

التوزيع العام للخطة الدراسية

الدورة	المادة	الطريقة	عدد الساعات
1°	الأمن الهجومي	إجباري	150
1°	إدارة فريق الأمن السيبراني	إجباري	150
1°	إدارة المشاريع الأمنية	إجباري	150
1°	الهجمات على الأنظمة وشبكات Windows	إجباري	150
1°	فرصنة الويب المتقدمة	إجباري	150
1°	بنية الشبكات وأمنها	إجباري	150
1°	تحليل Malware وتطويرها	إجباري	150
1°	أساسيات الطب الشرعي و DFIR	إجباري	150
1°	تمارين الفريق الأحمر Red Team المتقدمة	إجباري	150
1°	التقرير الفني والتنفيذي	إجباري	150

tech الجامعة التكنولوجية

أ. د./ Tere Guevara Navarro
رئيس الجامعة

*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

ماجيستير خاص
اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **12 شهر**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

ماجيستير خاص
اختبارات الاختراق (pentesting) والفريق الأحمر (Red Team)

tech الجامعة التيكنولوجية