ماجستير خاص

إدارة الأمن السيبراني

(كبير مسؤولي أمن المعلومات ،CISO)

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

ماجستير خاص

إدارة الأمن السيبراني

(كبير مسؤولي أمن المعلومات، CISO)

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **12 شهر**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- عدد الساعات المخصصة للدراسة: **16 ساعات أسبوعيًا**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

رابط الدخول إلى الموقع الإلكتروني: **www.techtitute.com/ae/information-technology/professional-master-degree/master-cybersecurity-management-ciso-chief-information-security-officer**

الفهرس

01
المقدمة

مع تقدم التكنولوجيا تتطور التهديدات وتتقن تقنيات الهجوم الخاصة بها. بعبارة أخرى تتزايد الإمكانيات والطرق التي يتعين على مجرمي الإنترنت تحقيق أهدافهم بها. في هذا السياق تقدم TECH درجة يمكن للمهنيين من خلالها اللحاق بالركب والتعلم بشكل شامل لحماية وتأمين البيئات الرقمية المختلفة. كل هذا من خلال منهجية ثورية وإعادة التعلم وبصيغة مريحة تمامًا عبر الإنترنت مما سيسمح للخريج باكتساب المهارات والقدرات دون توقيت محدد مسبقًا. وبالتالي عند الانتهاء من هذه الدرجة سيكتسب الطالب المختص المهارات والكفاءات اللازمة لأداء رئيس أمن المعلومات بكفاءة عالية ومنصب إداري رفيع يتمتع بمكانة كبيرة فضلاً عن آفاق عالية للنمو والتوسع.

مع تقدم التكنولوجيا والاتصال يزداد عدد وشكل التهديدات المحتملة. لهذا السبب من الأهمية بمكان أن يقوم كبار مسؤولي أمن المعلومات المستقبليين بتحديث معارفهم لتقديم حلول أكثر تكيفًا مع خصوصيات الشركة "

لا يخفى على أحد أننا في خضم عصر المعلومات والاتصالات لأننا جميعًا متصلون في المنزل وفي بيئات الشركة. وبالتالي يمكننا الوصول إلى العديد من المعلومات بنقرة واحدة مع بحث واحد في أي من المحركات التي لدينا تحت تصرفنا سواء من هاتف ذكي أو كمبيوتر شخصي أو كمبيوتر عمل. في هذا السياق»الوقت هو المال" وكذلك المعلومات.

مع تقدم التكنولوجيا بالنسبة للمواطن العادي والموظف تزداد أيضًا تقنيات التهديدات والهجوم. كلما وجدت وظائف جديدة وكلما زاد تواصلنا زاد سطح الهجوم. بعبارة أخرى تتزايد الإمكانيات والطرق التي يتعين على مجرمي الإنترنت تحقيق أهدافهم بها.

بالنظر إلى هذا السياق المقلق تطلق TECH هذا البرنامج في إدارة الأمن السيبراني (CISO، كبير مسؤولي أمن المعلومات) والذي تم تطويره من قبل فريق مع ملفات مهنية مختلفة متخصصة في قطاعات مختلفة تجمع بين الخبرة المهنية الدولية في القطاع الخاص في I+D+i وخبرة تعليمية واسعة. لذلك فهي ليست محدثة فقط في كل من التقنيات ولكن لديها أيضًا منظور حول الاحتياجات المستقبلية للقطاع وتقديمها بطريقة تعليمية.

يشمل البرنامج الموضوعات الأساسية المختلفة في مجال الأمن السيبراني والتي تم اختيارها بعناية لتغطية مجموعة واسعة من التقنيات المطبقة في بيئات العمل المختلفة. لكنه سيتعامل أيضًا مع فرع آخر من الموضوعات التي عادة ما تكون نادرة في الفهرس الأكاديمي للمؤسسات الأخرى والتي ستغذي بعمق المناهج المهنية. بهذه الطريقة وبفضل المعرفة المستعرضة التي تقدمها TECH مع هذا البرنامج سيكتسب الخريج المهارات اللازمة للعمل كمدير في مجال الأمن السيبراني (كبير مسؤولي أمن المعلومات) وبالتالي زيادة آفاقهم الشخصية والمهنية نمو.

تحتوي درجة **ماجستير خاص في إدارة الأمن السيبراني (CISO، كبير مسؤولي أمن المعلومات)** على البرنامج العلمي الأكثر اكتمالا وحداثة في السوق.

ومن أبرز الميزات:

- تطوير الحالات العملية التي يقدمها الخبراء في الأمن السيبراني
- محتوياتها الرسومية والتخطيطية والعملية البارزة التي يتم تصورها تجمع المعلومات العلمية للممارسة الصحية حول تلك التخصصات الأساسية للممارسة المهنية
- التدريبات العملية حيث يتم إجراء عملية التقييم الذاتي لتحسين التعليم
- تركيزها الخاص على المنهجيات المبتكرة
- دروس نظرية وأسئلة للخبراء ومنتديات مناقشة حول القضايا الخلافية وأعمال التفكير الفردي
- توفر الوصول إلى المحتوى من أي جهاز ثابت أو محمول متصل إلى الإنترنت

> استعد للعمل كرئيس تنفيذي لأمن المعلومات وهو ملف تعريف رئيسي في الشركة نظرًا لدورها كحامي وضامن لأمن الكمبيوتر"

تميز في قطاع مزدهر وكن شهادة الخبرة الجامعيةً
حقيقيًا في الأمن السيبراني مع برنامج *TECH* هذا.
إنه الأكثر اكتمالا في السوق"

تتطور الطرق التي يتبادل بها الناس المعلومات بسرعة. وهذا يتطلب أشكالًا جديدة من الحماية الإلكترونية للمهنيين.

برنامج عبر الإنترنت بنسبة *100*٪ بنهج عملي بارز من شأنه أن يضع الأسس لنموك المهني

البرنامج يضم في هيئة التدريس متخصصين في المجال والذين يصبون خبراتهم العملية في هذا التدريب بالإضافة إلى متخصصين معترف بهم من مجتمعات رائدة وجامعات مرموقة.

سيسمح محتوى الوسائط المتعددة المُعد بأحدث التقنيات التعليمية إلى التعلم المهني والسياقي أي في بيئة محاكاة التي ستوفرها هذه الشهادة الجامعية من تدريب ضمن مواقف حقيقية.

يركز تصميم هذا البرنامج على التعلم القائم على المشكلات والذي يجب على المهني من خلاله محاولة حل الحالات المختلفة للممارسة المهنية التي تُطرَح على مدار هذا البرنامج. للقيام بذلك سيحصل على مساعدة من نظام جديد من مقاطع الفيديو التفاعلية التي أعدها خبراء معترف بهم.

02

الأهداف

نظرًا لكون الجامعة مدركةً تمامًا لأهمية الأمن السيبراني للشركات فقد طورت TECH درجة الماجستير الخاص هذه التي تهدف إلى رعاية وتحديث معرفة المهنيين في مجال الكشف عن جرائم الكمبيوتر وحمايتها ومنعها. بهذه الطريقة سيصبح الخريج المستقبلي عضواً رئيسياً في رعاية البيانات والمعلومات مما يقلل من إمكانية استفادة المجرمين من الانتهاكات الأمنية الحالية المحتملة. الكفاءة المهنية التي سيتمكن الطالب المختص من اكتسابها في TECH في غضون 12 شهرًا فقط.

أنت تواجه فرصة فريدة لتحقيق أحلامك وأهدافك وتصبح شهادة الخبرة الجامعيةً في الأمن السيبراني"

الأهداف العامة

- تحليل دور محلل الأمن السيبراني
- التعمق في الهندسة الاجتماعية وطرقها
- فحص منهجيات OSINT، HUMINT، OWASP، PTEC، OSSTM، OWISAM
- إجراء تحليل للمخاطر وتعلم مقاييس المخاطر
- تحديد الاستخدام المناسب لإخفاء الهوية واستخدام الشبكات مثل TOR و I2P و Freenet
- توليد المعرفة المتخصصة لأداء تدقيق الأمن
- تطوير سياسات الاستخدام المناسبة
- فحص أنظمة الكشف والوقاية لأهم التهديدات
- تقييم أنظمة الكشف عن التهديدات الجديدة بالإضافة إلى تطورها فيما يتعلق بالحلول الأكثر تقليدية
- تحليل منصات المحمول الرئيسية الحالية وخصائصها واستخداماتها
- تحديد وتحليل وتقييم المخاطر الأمنية لأجزاء مشروع الإنترنت IoT
- تقييم المعلومات التي تم الحصول عليها وتطوير آليات الوقاية والاختراق
- تطبيق الهندسة العكسية على بيئة الأمن السيبراني
- تحديد الاختبارات التي يجب إجراؤها على البرنامج المطور
- جمع كل الأدلة والبيانات الموجودة لتنفيذ تقرير المعلومات الشرعية
- تقديم تقرير المعلومات الشرعية بشكل صحيح
- تحليل الحالة الحالية والمستقبلية لأمن الكمبيوتر
- فحص مخاطر التقنيات الناشئة الجديدة
- تجميع التقنيات المختلفة فيما يتعلق بأمن الكمبيوتر

الأهداف المحددة

الوحدة 1. الذكاء السيبراني والأمن السيبراني

- تطوير المنهجيات المستخدمة في الأمن السيبراني
- فحص دورة الذكاء وتأسيس تطبيقه في الذكاء السيبراني
- تحديد دور محلل المخابرات ومعوقات نشاط الإخلاء
- تحليل منهجيات OSINT، OWISAM، OSSTM، PTES، OWASP
- إنشاء الأدوات الأكثر شيوعًا لإنتاج المعلومات الاستخبارية
- إجراء تحليل للمخاطر ومعرفة المقاييس المستخدمة
- تحديد خيارات إخفاء الهوية واستخدام الشبكات مثل TOR و I2P و FreeNet
- تفصيل اللوائح الحالية بشأن الأمن السيبراني

الوحدة 2. أمن المضيف

- تحديد سياسات النسخ الاحتياطي للبيانات الشخصية والمهنية
- تقييم الأدوات المختلفة لتقديم حلول لمشاكل أمنية محددة
- إنشاء آليات للحصول على نظام محدث
- فحص جهاز الكمبيوتر الخاص بك لاكتشاف الدخلاء
- تحديد قواعد الوصول إلى النظام
- فحص وتصنيف رسائل البريد الإلكتروني لتجنب الاحتيال
- إنشاء قوائم بالبرامج المسموح بها

الوحدة 3. أمان الشبكة (المحيطية)

- تحليل هياكل الشبكة الحالية لتحديد المحيط الذي يجب علينا حمايته
- تطوير جدار حماية وتكوينات Linux المحددة للتخفيف من الهجمات الأكثر شيوعًا
- القيام بتجميع الحلول الأكثر استخدامًا مثل Snort و Suricata بالإضافة إلى تكوينها
- فحص الطبقات الإضافية المختلفة التي يوفرها الجيل التالي من جدران الحماية وإمكانيات الشبكات في بيئات السحابة
- تحديد أدوات حماية الشبكة واشرح سبب أهميتها للدفاع متعدد الطبقات

الوحدة 4. أمان الهاتف الذكي

- فحص نواقل الهجوم المختلفة لتجنب أن تصبح هدفًا سهلاً
- تحديد الهجمات الرئيسية وأنواع البرامج الضارة التي يتعرض لها مستخدمو الأجهزة المحمولة
- تحليل أحدث الأجهزة لإنشاء أمان أكبر في التكوين
- تحديد الخطوات الرئيسية لإجراء اختبار الاختراق على كل من أنظمة iOS ومنصات Android
- تطوير المعرفة المتخصصة حول أدوات الحماية والأمن المختلفة
- إنشاء الممارسات الجيدة في البرمجة الموجهة للأجهزة المحمولة

الوحدة 5. أمن إنترنت الأشياء IoT

- تحليل البنى الأساسية لإنترنت الأشياء IoT
- تصفح تقنيات الاتصال
- تطوير بروتوكولات التطبيق الأساسية
- تحديد الأنواع المختلفة للأجهزة الموجودة
- تقييم مستويات المخاطر ونقاط الضعف المعروفة
- تطوير سياسات الاستخدام الآمن
- تحديد شروط الاستخدام المناسبة لهذه الأجهزة

الوحدة 6. القرصنة الأخلاقية

- تصفح أساليب OSINT
- جمع المعلومات المتاحة في وسائل الإعلام العامة
- فحص الشبكات للحصول على معلومات الوضع النشط
- تطوير معامل الاختبار
- تحليل أدوات أداء *Pentesting*
- فهرسة وتقييم نقاط الضعف المختلفة للأنظمة
- تحديد المنهجيات المختلفة للقرصنة

الوحدة 7. الهندسة العكسية

- تحليل مراحل المترجم
- تصفح بنية معالج x86 وبنية معالج ARM
- تحديد أنواع التحليل المختلفة
- وضع الحماية *Sandboxing* في بيئات مختلفة
- تطوير تقنيات تحليل البرامج الضارة المختلفة
- إنشاء الأدوات الموجهة لتحليل البرامج الضارة

الوحدة 8. التنمية الآمنة

- تحديد المتطلبات اللازمة للتشغيل الصحيح للتطبيق بطريقة آمنة
- فحص ملفات السجل لفهم رسائل الخطأ
- تحليل الأحداث المختلفة وحدد ما يجب إظهاره للمستخدم وما يجب حفظه في السجلات
- إنشاء كود خالٍ من التعقيدات يمكن التحقق منه بسهولة
- تقييم الوثائق المناسبة لكل مرحلة من مراحل التطوير
- تحديد سلوك الخادم لتحسين النظام
- تطوير كود معياري وقابل لإعادة الاستخدام وقابل للصيانة

الوحدة 9. التحليل الجنائي

- تحديد العناصر المختلفة التي تثبت الجريمة
- توليد المعرفة المتخصصة للحصول على البيانات من الوسائط المختلفة قبل ضياعها
- استعادة البيانات التي تم حذفها عمدًا
- تحليل التسجيلات و السجلات للأنظمة
- تحديد كيفية تكرار البيانات حتى لا تغير الأصول
- اختبارات تحقق من أجل الاتساق
- إنشاء تقرير قوي وسلس
- تقديم الاستنتاجات بشكل متماسك
- تحديد كيفية الدفاع عن التقرير أمام السلطة المختصة
- تحديد استراتيجيات لجعل العمل عن بعد آمنًا

الوحدة 10. التحديات الحالية والمستقبلية في أمن الكمبيوتر

- فحص استخدام العملات المشفرة وتأثيرها على الاقتصاد والأمن
- تحليل أوضاع المستخدمين ودرجة الأمية الرقمية
- تحديد نطاق استخدام *Blockchain*
- تقديم بدائل لـ IPv4 في عنونة الشبكة
- تطوير استراتيجيات لتدريب السكان على الاستخدام الصحيح للتقنيات
- توليد المعرفة المتخصصة لمواجهة التحديات الأمنية الجديدة ومنع سرقة الهوية
- تحديد استراتيجيات لجعل العمل عن بعد آمنًا

برنامج فريد ومثالي إذا كنت تتطلع إلى زيادة معرفتك بالأمن السيبراني "

03

الكفاءات

بعد الانتهاء من عملية التقييم لدرجة الماجستير هذه سيكتسب الطالب المختص سلسلة من المعرفة والأدوات والمهارات التي ستسمح له بالممارسة في هذا القطاع مع ضمانات أكبر للنجاح. بهذه الطريقة لن يصبح الطالب شهادة الخبرة الجامعيةًا في الأمن السيبراني فحسب بل سيساهم أيضًا بشكل إيجابي في الحد من جرائم الكمبيوتر من خلال إقامة شبكة أكثر أمانًا وأقوى للجميع. الوصول إلى مناصب إدارية عليا مثل رئيس أمن المعلومات.

يتطلب قطاع الأمن السيبراني تحديثًا مستمرًا للمعرفة. مع برامج مثل هذه سيحقق الطالب المختص كل ذلك بسرعة وفعالية"

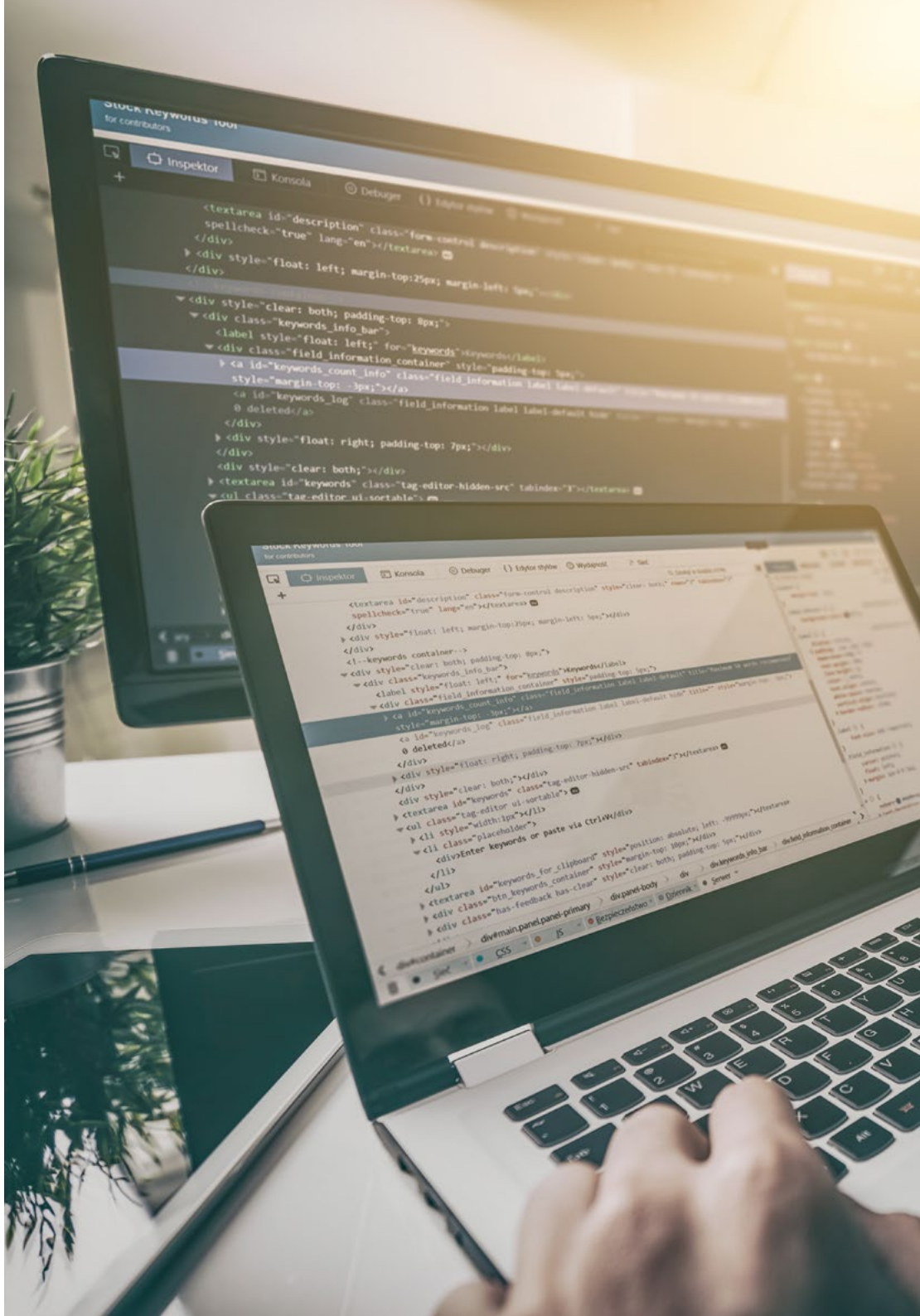
لكفاءات العامة

- التعرف على المنهجيات المستخدمة في الأمن السيبراني
- كيفية تقييم كل نوع من أنواع التهديد لتقديم الحل الأمثل في كل حالة
- القدرة على إنشاء حلول ذكية كاملة لأتمتة السلوك في حالة وقوع حوادث
- التعرف على كيفية تقييم المخاطر المرتبطة بنقاط الضعف خارج الشركة وداخلها
- التعرف على تطور وتأثير إنترنت الأشياء بمرور الوقت
- القدرة على إثبات ضعف النظام ومهاجمته لأغراض وقائية وحل هذه المشكلات
- كيفية وضع الحماية *Sandboxing* في بيئات مختلفة
- التعرف على الإرشادات التي يجب على المطور الجيد اتباعها للامتثال للأمان اللازم

> حسِّن مهاراتك في الخدمات مما سيعزز حياتك المهنية وحياتك الشخصية"

الكفاءات المحددة

- التعرف على كيفية تنفيذ عمليات الأمن الدفاعية
- امتلاك تصور عميق ومتخصص لأمن الكمبيوتر
- امتلاك معرفة متخصصة في مجال الأمن السيبراني والذكاء السيبراني
- فهم أهمية ابتكار دفاع متعدد الطبقات يُعرف أيضًا باسم"الدفاع في العمق" والذي يغطي جميع جوانب شبكة الشركة حيث يمكن أيضًا استخدام بعض المفاهيم والأنظمة التي سنراها وتطبيقها في بيئة محلية
- التعرف على كيفية تطبيق عمليات الأمان على الهواتف الذكية والأجهزة المحمولة
- التعرف على وسائل تنفيذ ما يسمى بالقرصنة الأخلاقية وحماية الشركة من هجوم إلكتروني
- القدرة على التحقيق في حادث الأمن السيبراني
- التعرف على تقنيات الهجوم والدفاع المختلفة الموجودة
- تحليل دور محلل الأمن السيبراني
- التعرف على عمل الهندسة الاجتماعية وطرقها



04

هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

تم تطوير برنامج إدارة الأمن السيبراني (CISO، كبير مسؤولي أمن المعلومات) من قبل فريق من الأشخاص ذوي التشكيلات المهنية المختلفة والمتخصصين في قطاعات مختلفة والذين يجمعون بين الخبرة المهنية الدولية في المجال الخاص في I+D+i وخبرة تعليمية واسعة النطاق. لذلك فهي ليست محدثة فقط في كل من التقنيات ولكن لديها أيضًا منظور حول الاحتياجات المستقبلية للقطاع وتقديمها بطريقة تعليمية. وبالتالي يضمن الطالب المختص أنه يتعلم من أوائل المعلمين في هذا القطاع مع ضمان الحصول على أحدث المعارف.

"أثناء البرنامج سترافقك سلسلة من المختصين الخبراء الذين سيجعلون تجربتك التعليمية حدثًا فريدًا"

المدير الدولي المُستضاف

الدكتور Frederic Lemieux مشهور دوليًا كخبير مبتكر وقائد ملهم في مجالات الاستخبارات والأمن القومي والأمن الداخلي والأمن السيبراني والتقنيات الإبتكارية. إن تفانيه المستمر ومساهماته ذات الصلة في البحث والتعليم تضعه كشخصية رئيسية في تعزيز سلامة وفهم التقنيات الناشئة اليوم. خلال حياته المهنية، وضع تصورات وأدار برامج أكاديمية متطورة في العديد من المؤسسات الشهيرة، مثل جامعة مونتريال وجامعة جورج واشنطن وجامعة جورج تاون.

خلال خلفيته الواسعة، نشر العديد من الكتب ذات الصلة للغاية، وكلها تتعلق بالاستخبارات الجنائية وعمل الشرطة والتهديدات الإلكترونية والأمن الدولي. كما ساهم بشكل كبير في مجال الأمن السيبراني من خلال نشر العديد من المقالات في المجلات الأكاديمية، التي تدرس السيطرة على الجريمة أثناء الكوارث الكبرى، ومكافحة الإرهاب، ووكالات الاستخبارات وتعاون الشرطة. وبالإضافة إلى ذلك، كان عضوا في حلقة النقاش ومتحدثا رئيسيا في مختلف المؤتمرات الوطنية والدولية، وعزز نفسه كمرجع في المجالين الأكاديمي والمهني.

قام الدكتور Lemieux بأدوار التحرير والتقييم في مختلف المنظمات الأكاديمية والخاصة والحكومية، مما يعكس تأثيره والتزامه بالتميز في مجال تخصصه. وبهذه الطريقة، قادته مسيرته الأكاديمية المرموقة إلى العمل كأستاذ للممارسات ومدير كلية لبرامج MPS في الذكاء التطبيقي وإدارة المخاطر في الأمن السيبراني وإدارة التكنولوجيا وإدارة تكنولوجيا المعلومات، في جامعة جورج تاون.

د. Lemieux, Frederic

- باحث في مجال الاستخبارات والأمن السيبراني والتقنيات الابتكارية
- باحث في الاستخبارات والأمن السيبراني والتقنيات الابتكارية في جامعة جورج تاون
- مدير الماجستير في Information Technology Management بجامعة جورج تاون
- مدير الماجستير في Technology Management بجامعة جورج تاون
- مدير الماجستير في Cybersecurity Risk Management بجامعة جورج تاون
- مدير الماجستير في Applied Intelligence بجامعة جورج تاون
- أستاذ التدريب في بجامعة جورج تاون
- دكتوراه في علم الجريمة، كلية علم الجريمة، جامعة مونتريال
- بكالوريوس في علم الاجتماع، درجة ثانوية في علم النفس، من جامعة لافال
- عضو في New Program Roundtable Committee, من جامعة جورج تاون

بفضل *TECH* ستتمكن من التعلم مع أفضل المحترفين في العالم"

هيكل الإدارة

أ. Fernández Sapena, Sonia

- مدربة أمن الكمبيوتر والقرصنة الأخلاقية في المركز المرجعي الوطني لعلوم الكمبيوتر والاتصالات السلكية واللاسلكية
- مدربة معتمد من المجلس الإلكتروني
- مدربة في الشهادات التالية: مؤسسة EXIN Ethical Hacking Foundation و EXIN Cyber & IT Security Foundation. مدريد
- مدربة شهادة الخبرة الجامعية معتمد من قبل CAM من الشهادات المهنية التالية: أمن الكمبيوتر (IFCT0190)، إدارة شبكات الصوت والبيانات (IFCM0310)، إدارة شبكات الإدارات (IFCT0410)، إدارة الإنذارات في شبكات الاتصالات (IFCM0410)، مشغل شبكات الصوت والبيانات (IFCM0110)، وإدارة خدمات الإنترنت (IFCT0509)
- متعاونة خارجية CSO / SSA (كبير مسؤولي الأمن / كبير مهندسي الأمن) في جامعة Islas Baleares
- مهندسة كمبيوتر من جامعة Alcalá de Henares في مدريد
- ماجستير في DevOps: Docker and Kubernetes. Cas-Training
- تقنيات أمان Microsoft Azure. E-Council

الأساتذة

أ. Redondo, Jesús Serrano

- مطور ويب وفني الأمن السيبراني
- مطور مواقع الويب. Roams, Palencia
- مطور الواجهة الأمامية في Telefónica بمدريد
- مطور FrontEnd. أفضل شركة استشارات احترافية SL بمدريد
- تركيب معدات وخدمات الاتصالات السلكية واللاسلكية. مجموعة Zener في Castilla و León
- تركيب معدات وخدمات الاتصالات السلكية واللاسلكية. شركة Lican للاتصالات في Castilla و León
- شهادة في أمن الحاسوب. CFTIC خيتافي، مدريد
- فني متقدم: الاتصالات السلكية واللاسلكية وأنظمة الكمبيوتر. IES Trinidad Arroyo, Palencia
- فني متقدم: التركيبات الكهروتقنية MT و BT. IES Trinidad Arroyo, Palencia
- التدريب في الهندسة العكسية والاختزال والتشفير. أكاديمية (Hacker Incibe (Talentos Incibe

أ. Jiménez Ramos, Álvaro

- محلل الأمن السيبراني
- كبير محللي الأمن في The Workshop
- محلل الأمن السيبراني L1 في Axians
- محلل الأمن السيبراني L2 في Axians
- محلل الأمن السيبراني في SACYR S.A
- شهادة في هندسة الاتصالات عن بعد من جامعة Politécnica بمدريد
- ماجستير في الأمن السيبراني و القرصنة الأخلاقية في CICE
- دورة عليا في الأمن السيبراني من قبل Deusto Formación

أ. Marcos Sbarbaro, Victoria Alicia

- مطورة تطبيقات Android Mobile الأصلي في B60. المملكة المتحدة
- محللة ومبرمجة لإدارة وتنسيق وتوثيق البيئة الافتراضية لأجهزة الإنذار الأمنية
- محللة مبرمجة لتطبيقات Java لأجهزة الصراف الآلي
- مختصة تطوير البرمجيات لتطبيق التحقق من صحة التوقيع وإدارة الوثائق
- فنية أنظمة لترحيل المعدات ولإدارة وصيانة وتدريب أجهزة المساعد الرقمي الشخصي الخاصة بالأجهزة المحمولة
- الهندسة التقنية لأنظمة الكمبيوتر بجامعة Oberta في كاتالونيا
- ماجستير في أمن الكمبيوتر والقرصنة الأخلاقية الرسمية EC-Council و CompTIA من المدرسة المهنية للتكنولوجيات الجديدة CICE

أ. Peralta Alonso, Jon

- مستشار أول - حماية البيانات والأمن السيبراني. Altia
- محامي / مستشار قانوني. شركة Arriaga Associates للاستشارات القانونية والاقتصادية S.L. مستشار قانوني / متدرب. المكتب المهني: Oscar Padura
- شهادة بكالوريوس في القانون. الجامعة الحكومية في إقليم Vasco
- درجة ماجستير في حماية البيانات. المدرسة المبتكرة EIS
- ماجستير في القانون. الجامعة الحكومية في إقليم Vasco
- ماجستير متخصص في الإجراءات المدنية. الجامعة الدولية Isabel I de Castilla
- مدرس ماجستير في حماية البيانات الشخصية والأمن السيبراني وقانون تكنولوجيا المعلومات والاتصالات

أ. Catalá Barba, José Francisco

- شهادة الخبرة الجامعية فني الكتروني في الأمن السيبراني
- مطور لتطبيقات الجوال
- فني الكتروني. قيادي وسيط في وزارة الدفاع الإسبانية
- فني الكتروني في مصنع فورد الكائن في منطقة Almusafes بفالنسيا

05

الهيكل والمحتوى

لضمان حصول الطالب على المعرفة الأكثر دقة وابتكارًا في مجال الأمن السيبراني صممت TECH سلسلة من المواد التي تجمع بين آخر التحديثات في المهنة. تم تصميم هذه المحتويات من قبل مجموعة من الخبراء في هذا المجال بحيث يتم تكييفها مع الاحتياجات الحالية للوظائف المعروضة في هذا القطاع. مناسبة احترافية فريدة من نوعها من شأنها أن تقطع الطالب إلى النجاح في تطوره المهني.

منهج دراسي على مستوى تم تصميمه من قبل محترفين
ومن أجلهم. هل ستفوت هذه الفرصة؟"

الوحدة 1. الذكاء السيبراني والأمن السيبراني

1.1. الذكاء السيبراني
1.1.1. الذكاء السيبراني
1.1.1.1. الذكاء
1.1.1.1.1. دورة الذكاء
2.1.1.1. الذكاء السيبراني
3.1.1.1. الذكاء السيبراني والأمن السيبراني
2.1.1. محلل الذكاء
1.2.1.1. دور محلل الذكاء
2.2.1.1. تحيزات محلل الذكاء في النشاط التقييمي
2.1. الأمن السيبراني
1.2.1. طبقات الأمان
2.2.1. تحديد التهديدات السيبرانية
1.2.2.1. التهديدات الخارجية
2.2.2.1. التهديدات الداخلية
3.2.1. الإجراءات السلبية
1.3.2.1. الهندسة الاجتماعية
2.3.2.1. الطرق الشائعة الاستخدام
3.1. تقنيات وأدوات الذكاء
1.3.1. OSINT
2.3.1. SOCMINT
3.3.1. HUMIT
4.3.1. توزيعات وأدوات Linux
5.3.1. OWISAM
6.3.1. OWASP
7.3.1. PTES
8.3.1. OSSTMM
4.1. منهجيات التقييم
1.4.1. تحليل الذكاء
2.4.1. تقنيات تنظيم المعلومات المكتسبة
3.4.1. الموثوقية والمصداقية في مصادر المعلومات
4.4.1. منهجيات التحليل
5.4.1. عرض نتائج الاستخبارات
5.1. التدقيق والتوثيق
1.5.1. تدقيق أمن تكنولوجيا المعلومات
2.5.1. تصاريح التوثيق والتدقيق
3.5.1. أنواع التدقيق
4.5.1. التسليمات
1.4.5.1. التقرير الفني
2.4.5.1. التقرير التنفيذي
6.1. عدم الكشف عن الهوية في الشبكة
1.6.1. استخدام المجهولية
2.6.1. تقنيات إخفاء الهوية (Proxy و VPN)
3.6.1. شبكات IP2 و Freenet و TOR
7.1. التهديدات وأنواع الأمن
1.7.1. أنواع التهديدات
2.7.1. الأمن المادي
3.7.1. أمن الشبكات
4.7.1. الأمن المنطقي
5.7.1. أمن تطبيقات الويب
6.7.1. أمن الجهاز المحمول
8.1. اللوائح والامتثال
1.8.1. RGPD
2.8.1. شهادة ISO 27000
3.8.1. إطار عمل الأمن السيبراني NIST
4.8.1. PIC
5.8.1. ISO 27032
6.8.1. أنظمة السحابة
7.8.1. SOX
8.8.1. PCI
9.1. تحليل المخاطر والمقاييس
1.9.1. نطاق المخاطر
2.9.1. النشطة
3.9.1. التهديدات
4.9.1. نقاط الضعف
5.9.1. تقييم المخاطر
6.9.1. علاج المخاطر

10.1. منظمات مهمة في مجال الأمن السيبراني

1.10.1. NIST

2.10.1. ENISA

3.10.1. OEA

4.10.1. UNASUR PROSUR

الوحدة 2. أمن المضيف

1.2. النسخ الاحتياطية

1.1.2. استراتيجيات النسخ الاحتياطي

2.1.2. أدوات لنظام التشغيل Windows

3.1.2. أدوات Linux

4.1.2. أدوات لنظام MacOS

2.2. مضاد فيروسات المستخدم

1.2.2. أنواع مضادات الفيروسات

2.2.2. مضاد فيروسات Windows

3.2.2. مضاد فيروسات Linux

4.2.2. مضاد فيروسات MacOS

5.2.2. مضاد فيروسات للهواتف الذكية

3.2. أجهزة كشف التسلل HIDS

1.3.2. طرق كشف التطفل

2.3.2. Sagan

3.3.2. Aide

4.3.2. *Rkhunter*

4.2. جدار الحماية المحلي

1.4.2. جدار حماية Windows

2.4.2. جدار حماية Linux

3.4.2. جدار حماية MacOS

5.2. مديري كلمات المرور

1.5.2. كلمة المرور

2.5.2. *LastPass*

3.5.2. *KeePass*

4.5.2. *Sticky Password*

5.5.2. RoboForm

6.2. أجهزة كشف التصيدالاحتيالي

1.6.2. كشف التصيد الاحتيالي يدويا

2.6.2. أدوات مكافحة التصيد الاحتيالي

7.2. برامج التجسس

1.7.2. آليات التجنب

2.7.2. أدوات مكافحة برامج التجسس

8.2. البرامج التتبعية

1.8.2. تدابير لحماية النظام

2.8.2. أدوات مكافحة التعقب

9.2. *EDR*- اكتشاف نقطة النهاية والاستجابة لها

1.9.2. سلوك نظام EDR

2.9.2. الاختلافات بين EDR ومكافحة الفيروسات

3.9.2. مستقبل أنظمة EDR

10.2. السيطرة على تثبيت البرنامج

1.10.2. مستودعات ومخازن البرمجيات

2.10.2. قوائم البرامج المسموح بها أو المحظورة

3.10.2. معايير الترقية

4.10.2. امتيازات لتثبيت البرنامج

الوحدة 3. أمان الشبكة (المحيطية)

1.3. أنظمة الكشف عن التهديدات والوقاية منها

1.1.3. الإطار العام للحوادث الأمنية

2.1.3. أنظمة الدفاع الحالية: دفاع في العمق SOC

3.1.3. أبنية الشبكة الحالية

4.1.3. أنواع أدوات الكشف والوقاية من الحوادث

1.4.1.3. الأنظمة القائمة على الشبكة

2.4.1.3. الأنظمة المستندة إلى المضيف

3.4.1.3. النظم المركزية

5.1.3. الاتصال واكتشاف الحالات/المضيفينوالحاويات وبدون خادم

2.3. جدار الحماية

1.2.3. أنواع جدران الحماية

2.2.3. الهجمات والتخفيف منها

3.2.3. جدران الحماية الشائعة في *kernel* Linux

3.2.3.1. *UFW*

3.2.3.2. *iptables* و *Nftables*

3.2.3.3. جدار الحماية

3.2.3.4. أنظمة الكشف على أساس سجلات النظام

3.2.4.1. مغلفات TCP

3.2.4.2. *DenyHosts* و *BlockHosts*

3.2.4.3. Ban2Fail

3.3. أنظمة كشف ومنع التسلل (IDS / IPS)

3.3.1. الهجمات على IDS / IPS

3.3.2. أنظمة IDS / IPS

3.3.2.1. *Snort*

3.3.2.2. السرقاط

3.4. جدران الحماية للجيل القادم (NGFW)

3.4.1. الاختلافات بين NGFW و جدار الحماية التقليدي

3.4.2. القدرات الرئيسية

3.4.3. حلول الأعمال

3.4.4. جدران الحماية للخدمات السحابية

3.4.4.1. هندسة سحابة VPC

3.4.4.2. سحابة ACLs

3.4.4.3. مجموعة الأمان

3.5. البروكسي

3.5.1. أنواع البروكسي

3.5.2. استخدام البروكسي. المميزات والعيوب

3.6. محركات مكافحة الفيروسات

3.6.1. السياق العام للبرامج الضارة وبطاقات IOCs

3.6.2. مشاكل محرك مكافحة الفيروسات

3.7. أنظمة حماية البريد

3.7.1. مكافحة البريد المزعج

3.7.1.1. القوائم السوداء والبيضاء

3.7.1.2. فلاتر Bayesianos

3.7.2. بوابة البريد (MGW)

3.8. SIEM

3.8.1. المكونات والعمارة

3.8.2. قواعد الارتباط وحالات الاستخدام

3.8.3. التحديات الحالية لأنظمة SIEM

3.9. SOAR

3.9.1. SOAR و SIEM: أعداء أو حلفاء

3.9.2. مستقبل أنظمة SOAR

3.10. أنظمة أخرى قائمة على الشبكة

3.10.1. WAF

3.10.2. NAC

3.10.3. *HoneyNets* و *HoneyPots*

3.10.4. CASB

الوحدة 4. أمان الهاتف الذكي

4.1. عالم الهواتف المحمولة

4.1.1. أنواع المنصات المتنقلة

4.1.2. أجهزة iOS

4.1.3. أجهزة Android

4.2. إدارة أمن الأجهزة المحمولة

4.2.1. مشروع OWASP للأمان على الأجهزة المحمولة

4.2.1.1. أهم 10 نقاط ضعف

4.2.2. الاتصالات والشبكات وأنماط الاتصال

4.3. الجهاز المحمول في بيئة الأعمال

4.3.1. المخاطر

4.3.3. مراقبة الجهاز

4.3.4. إدارة الأجهزة المحمولة (MDM)

4.4. خصوصية المستخدم وأمن البيانات

4.4.1. حالة المعلومات

4.4.2. تخزين آمن للبيانات

4.4.2.1. تخزين آمن في iOS

4.4.2.2. تخزين آمن في Android

4.4.4. الممارسات الجيدة في تطوير التطبيقات

5.4. نقاط الضعف ونواقل الهجوم
1.5.4. نقاط الضعف
2.5.4. نواقل الهجوم
1.2.5.4. البرمجيات الضارة
2.2.5.4. استخراج البيانات
3.2.5.4. التلاعب بالبيانات
6.4. التهديدات الرئيسية
1.6.4. مستخدم غير أشكال
2.6.4. البرمجيات الضارة
1.2.6.4. أنواع البرمجيات الضارة
3.6.4. الهندسة الاجتماعية
4.6.4. تسرب البيانات
5.6.4. سرقة المعلومات
6.6.4. شبكات Wi-Fi غير آمنة
7.6.4. البرمجيات الغير مُحَدَثة
8.6.4. التطبيقات الضارة
9.6.4. كلمات السر الضعيفة
10.6.4. إعدادات الأمان ضعيفة أو غير موجودة
11.6.4. الوصول المادي
12.6.4. جهاز مفقود أو مسروق
13.6.4. انتحال الهوية (النزاهة)
14.6.4. تشفير ضعيف أو معطل
15.6.4. رفض الخدمة (DoS)
7.4. الهجمات الرئيسية
1.7.4. هجمات التصيد الاحتيالي
2.7.4. الهجمات المتعلقة بأساليب الاتصال
3.7.4. هجمات الرسائل القصيرة الاحتيالية
4.7.4. هجمات التعدين السري
5.7.4. *Man in The Middle*
8.4. القرصنة
1.8.4. التجذير و كسر الحماية
2.8.4. تشريح الهجوم المحمول
1.2.8.4. انتشار التهديد
2.2.8.4. تثبيت البرمجيات الضارة على الجهاز
3.2.8.4. المثابرة
4.2.8.4. تنفيذ الحمولة واستخراج المعلومات
3.8.4. القرصنة على أجهزة iOS: الآليات والأدوات
4.8.4. القرصنة على أجهزة Android: الآليات والأدوات
9.4. اختبارات الاختراق
1.9.4. اختبار المكافحة على iOS
2.9.4. اختبار المكافحة على Android
3.9.4. أدوات
10.4. الحماية والأمن
1.10.4. اعدادات الامان
1.1.10.4. على أجهزة iOS
2.1.10.4. على أجهزة Android
2.10.4. تدابير أمنية
3.10.4. أدوات الحماية

الوحدة 5. أمن إنترنت الأشياء IoT

1.5. الأجهزة
1.1.5. أنواع الأجهزة
2.1.5. أبنية موحدة
1.2.1.5. OneM2M
2.2.1.5. IoTWF
3.1.5. بروتوكولات التطبيق
4.1.5. تقنيات الاتصال
2.5. أجهزة IoT. مجالات التطبيق
1.2.5. المنزل الذكي
2.2.5. المدينة الذكية
3.2.5. وسائل النقل
4.2.5. الأجهزة القابلة للارتداء
5.2.5. القطاع الصحي
6.2.5. IIoT

3.5. بروتوكولات الاتصال
1.3.5. MQTT
2.3.5. LWM2M
3.3.5. OMA-DM
4.3.5. TR - 069
4.5. المنزل الذكي
1.4.5. التشغيل الآلي للمنزل
2.4.5. شبكات التواصل
3.4.5. الأجهزة المنزلية
4.4.5. اليقظة والأمن
5.5. المدينة الذكية
1.5.5. الإضاءة
2.5.5. علم الارصاد الجوية
3.5.5. السلامة
6.5. وسائل النقل
1.6.5. موقع
2.6.5. سداد المدفوعات والحصول على الخدمات
3.6.5. الاتصال
7.5. الأجهزة القابلة للارتداء
1.7.5. الملابس الذكية
2.7.5. المجوهرات الذكية
3.7.5. الساعات الذكية
8.5. القطاع الصحي
1.8.5. التمرين / مراقبة معدل ضربات القلب
2.8.5. مراقبة المرضى وكبار السن
3.8.5. الزرع
4.8.5. الروبوتات الجراحية
9.5. الاتصال
1.9.5. شبكة ال Wifi
2.9.5. Bluetooth
3.9.5. اتصال مدمج
10.5. التوريق
1.10.5. شبكات مخصصة
2.10.5. مسئول كلمات المرور
3.10.5. استخدام البروتوكولات المشفرة
4.10.5. استخدم النصائح

الوحدة 6. القرصنة الأخلاقية

1.6. بيئة العمل
1.1.6. توزيعات Linux
1.1.1.6. Kali Linux - الحماية الهجومية
2.1.1.6. نظام تشغيل Parrot
3.1.1.6. Ubuntu
2.1.6. أنظمة المحاكاة الافتراضية
3.1.6. Sandbox
4.1.6. انتشار المعامل
2.6. المنهجيات
1.2.6. OSSTMM
2.2.6. OWASP
3.2.6. NIST
4.2.6. PTES
5.2.6. ISSAF
3.6. البصمات
1.3.6. استخبارات مفتوحة المصدر (OSINT)
2.3.6. البحث عن خرق البيانات ونقاط الضعف
3.3.6. استخدام الأدوات الخاملة
4.6. فحص الشبكة
1.4.6. أدوات المسح
1.1.4.6. Nmap
2.1.4.6. Hping3
3.1.4.6. أدوات المسح الأخرى
2.4.6. تقنيات المسح
3.4.6. تقنيات التهرب من جدار الحماية و IDS
4.4.6. لافتة الاستيلاء
5.4.6. مخططات الشبكة

5.6. ترقيم
1.5.6. ترقيم SMTP
2.5.6. ترقيم DNS
3.5.6. ترقيم NetBIOS و Samba
4.5.6. ترقيم LDAP
5.5.6. ترقيم SNMP
6.5.6. تقنيات الترقيم الأخرى
6.6. فحص الثغرات الأمنية
1.6.6. حلول لفحص الثغرات الأمنية
1.1.6.6. Qualys
2.1.6.6. Nessus
3.1.6.6. CFI LanGuard
2.6.6. أنظمة تسجيل الثغرات الأمنية
1.2.6.6. CVSS
2.2.6.6. CVE
3.2.6.6. NVD
7.6. الهجمات على الشبكات اللاسلكية
1.7.6. منهجية القرصنة في الشبكات اللاسلكية
1.1.7.6. مستكشف شبكة ال Wifi
2.1.7.6. تحليل الحركة
3.1.7.6. هجمات *Aircrack*
1.3.1.7.6. هجمات الويب
2.3.1.7.6. هجمات WPA / WPA2
4.1.7.6. هجمات *Evil Twin*
5.1.7.6. هجمات WPS
6.1.7.6. *Jamming*
2.7.6. أدوات الأمن اللاسلكية
8.6. قرصنة خادم الويب
1.8.6. البرمجة عبر الموقع
2.8.6. CSRF
3.8.6. قرصنة الجلسة
4.8.6. إدخال لغة الاستعلامات النصية SQL
9.6. استغلال الثغرات الأمنية
1.9.6. استخدام الثغرات المعروفة
2.9.6. استخدام *Metasploit*
3.9.6. استخدام البرمجيات الضارة
1.3.9.6. التعريف والنطاق
2.3.9.6. إنشاء البرمجيات الضارة
3.3.9.6. تجاوز حلول الحماية من الفيروسات
10.6. المثابرة
1.10.6. تركيب الجذور الخفية
2.10.6. استخدام Ncat
3.10.6. استخدام المهام المجدولة ل *Backdoors*
4.10.6. إنشاء المستخدمين
5.10.6. الكشف عن HIDS

الوحدة 7. الهندسة العكسية

1.7. المُجَمِعين
1.1.7. أنواع الأكواد أو الرموز
2.1.7. أطوار المترجم
3.1.7. جداول الرموز
4.1.7. معالج الأخطاء
5.1.7. مترجم GCC
2.7. أنواع التحليل في المجمعين
1.2.7. التحليل المعجمي
1.1.2.7. المصطلحات
2.1.2.7. المكونات المعجمية
3.1.2.7. محلل LEX المعجمي
2.2.7. التحليل النحوي
1.2.2.7. القواعد النحوية الخالية من السياق
2.2.2.7. أنواع التحليل
1.2.2.2.7. التحليل التنازلي
2.2.2.2.7. التحليل التصاعدي
3.2.2.7. أشجار النحو والاشتقاقات

4.2.2.7. أنواع المحللات

1.4.2.2.7. أجهزة التحليل LR (من اليسار إلى اليمين)

2.4.2.2.7. محللات LALR

3.2.7. التحليل الدلالي

1.3.2.7. السمة النحوية

2.3.2.7. المنسوبات-S

3.3.2.7. المنسوبات-L

3.7. هياكل البيانات في المُجمّع

1.3.7. المتغيرات

2.3.7. المصفوفات

3.3.7. المؤشرات

4.3.7. الهياكل

5.3.7. العناصر

4.7. هياكل كود التجميع

1.4.7. هياكل الاختيار

If, else if, Else .1.1.4.7

Switch .2.1.4.7

2.4.7. هياكل التكرار

For .1.2.4.7

While .2.2.4.7

3.2.4.7. استخدام كسر التكرار البرمجي *break*

3.4.7. المهام

5.7. هندسة الأجهزة في x86

1.5.7. هندسة المعالجات في x86

2.5.7. هياكل البيانات في x86

3.5.7. هياكل الكود في x86

4.5.7. هياكل الكود في x86

6.7. هندسة الأجهزة في ARM

1.6.7. هندسة المعالجات في ARM

2.6.7. هياكل البيانات في ARM

3.6.7. هياكل الكود في ARM

7.7. تحليل الكود الثابت

1.7.7. المفككات

2.7.7. IDA

3.7.7. مصممي الكود

8.7. تحليل الكود الديناميكي

1.8.7. تحليل السلوك

1.1.8.7. الاتصالات

2.1.8.7. المتابعة

2.8.7. مصححات التعليمات البرمجية على Linux

3.8.7. مصححات التعليمات البرمجية على Windows

9.7. Sandbox

1.9.7. هندسة تصميم Sandbox

2.9.7. التهرب من Sandbox

3.9.7. تقنيات الكشف

4.9.7. تقنيات التهرب

5.9.7. التدابير المضادة

6.9.7. Sandbox في Linux

7.9.7. Sandbox في Windows

8.9.7. Sandox في MacOS

9.9.7. Sandbox في Android

10.7. تحليل البرمجيات الخبيثة

1.10.7. تحليل البرمجيات الضارة

2.10.7. تقنيات التعتيم على البرمجيات الضارة

1.2.10.7. التعتيم على الملفات التنفيذية

2.2.10.7. تقييد بيئات التنفيذ

3.10.7. أدوات تحليل البرمجيات الضارة

الوحدة 8. التنمية الآمنة

1.8. التنمية الآمنة
1.1.8. الجودة والأداء والسلامة
2.1.8. السرية والنزاهة والتوافر
3.1.8. دورة حياة تطوير البرمجيات
2.8. مرحلة المتطلبات
1.2.8. مراقبة المصادقة
2.2.8. السيطرة على الأدوار والامتيازات
3.2.8. المتطلبات الموجهة نحو المخاطر
4.2.8. الموافقة على الامتياز
3.8. مراحل التصميم والتحليل
1.3.8. الوصول إلى المكونات وإدارة النظام
2.3.8. مسارات مراجعة الحسابات
3.3.8. إدارة الجلسة
4.3.8. الحقائق التاريخية
5.3.8. المعالجة المناسبة للخطأ
6.3.8. فصل المهمات
4.8. مرحلة التنفيذ والترميز
1.4.8. ضمان بيئة التطوير
2.4.8. إعداد الوثائق الفنية
3.4.8. التشفير الآمن
4.4.8. أمن الإتصالات
5.8. ممارسات الترميز الآمنة الجيدة
1.5.8. التحقق من صحة البيانات المدخلة
2.5.8. ترميز بيانات الإخراج
3.5.8. أسلوب البرمجة
4.5.8. تغيير معالجة السجل
5.5.8. التدرب على التشفير
6.5.8. الخطأ وإدارة السجل
7.5.8. إدارة الملفات
8.5.8. إدارة الذاكرة
9.5.8. توحيد وإعادة استخدام وظائف الأمن
6.8. إعداد الخادم و التقوية
1.6.8. إدارة المستخدمين والمجموعات والأدوار على الخادم
2.6.8. تنصيب البرامج
3.6.8. تقوية الخادم
4.6.8. التكوين المتين لبيئة التطبيق
7.8. اعداد قاعدة البيانات و تقوية
1.7.8. تحسين محرك قاعدة البيانات
2.7.8. إنشاء المستخدم الخاص للتطبيق
3.7.8. تعيين الامتيازات الدقيقة للمستخدم
4.7.8. تقوية قاعدة البيانات
8.8. مرحلة الإختبار
1.8.8. مراقبة الجودة في الضوابط الأمنية
2.8.8. فحص الكود المرحلي
3.8.8. فحص إدارة التكوين
4.8.8. اختبار الصندوق الأسود
9.8. التحضير للانتقال إلى الإنتاج
1.9.8. قم بمراقبة التغيير
2.9.8. قم بتنفيذ إجراءات خطوة الإنتاج
3.9.8. تنفيذ إجراء العودة إلى الحالة السابقة
4.9.8. الاختبارات في مرحلة ما قبل الإنتاج
10.8. مرحلة الصيانة
1.10.8. التأكيد على أساس المخاطر
2.10.8. اختبار صيانة الصندوق الأبيض
3.10.8. اختبار صيانة الصندوق الأسود

الوحدة 9. التحليل الجنائي

1.9. الحصول على البيانات والازدواجية
1.1.9. الحصول على بيانات المتغير
1.1.1.9. معلومات النظام
2.1.1.9. معلومات الشبكة
3.1.1.9. ترتيب التقلب
2.1.9. الحصول على بيانات ثابتة
1.2.1.9. عمل نسخة طبق الأصل
2.2.1.9. إعداد وثيقة لسلسلة الحراسة

3.1.9. طرق التحقق من صحة البيانات المكتسبة
1.3.1.9. طرق Linux
2.3.1.9. طرق Windows
2.9. تقييم وهزيمة تقنيات مكافحة الأدلة الجنائية
1.2.9. أهداف تقنيات مكافحة الأدلة الجنائية
2.2.9. حذف البيانات
1.2.2.9. حذف البيانات والملفات
2.2.2.9. استعادة الملف
3.2.2.9. استعادة الأجزاء المحذوفة
3.2.9. حماية كلمة المرور
4.2.9. إخفاء المعلومات
5.2.9. محو بيانات الجهاز الآمن
6.2.9. التشفير
3.9. التحليل الجنائي لنظام التشغيل
1.3.9. التحليل الجنائي لنظام Windows
2.3.9. التحليل الجنائي لنظام Linux
3.3.9. التحليل الجنائي لنظام Mac
4.9. التحليل الجنائي للشبكة
1.4.9. تحليل السجلات
2.4.9. ارتباط البيانات
3.4.9. التحقيق ضمن الشبكة
4.4.9. خطوات لمتابعة التحليل الجنائي للشبكة
5.9. التحليل الجنائي للويب
1.5.9. التحقيق في الهجمات على الويب
2.5.9. الكشف عن الهجوم
3.5.9. موقع عناوين بروتوكول الإنترنت IPs
6.9. قاعدة بيانات التحليل الجنائي
1.6.9. التحليل الجنائي في MSSQL
2.6.9. التحليل الجنائي في MySQL
3.6.9. التحليل الجنائي في PostgreSQL
4.6.9. التحليل الجنائي في MongoDB

7.9. التحليل الجنائي في السحابية
1.7.9. أنواع الجرائم السحابية
1.1.7.9. السحابة كعنصر
2.1.7.9. السحابة ككائن
3.1.7.9. السحابة كأداة
2.7.9. تحديثات التحليل الجنائي للسحابة
3.7.9. التحقيق في خدمات التخزين للسحابية
4.7.9. أدوات التحليل الجنائي للسحابة
8.9. التحقيق في الجرائم عبر البريد الإلكتروني
1.8.9. أنظمة البريد
1.1.8.9. عملاء البريد
2.1.8.9. خادم البريد
3.1.8.9. خادم SMTP
4.1.8.9. خادم POP3
5.1.8.9. خادم IMAP4
2.8.9. جرائم البريد
3.8.9. رسائل البريد الإلكتروني
1.3.8.9. الرؤوس القياسية
2.3.8.9. الرؤوس الموسعة
4.8.9. خطوات التحقيق في هذه الجرائم
5.8.9. أدوات جنائية للبريد الإلكتروني
9.9. التحليل الجنائي لنظام المحمول
1.9.9. الشبكات الخلوية
1.1.9.9. أنواع الشبكات
2.1.9.9. محتويات CDR
2.9.9. وحدة تعريف المشترك (SIM)
3.9.9. الاستحواذ المنطقي
4.9.9. الاستحواذ المادي
5.9.9. الحصول على نظام الملفات

10.9. صياغة وتقديم التقارير للتحاليل الجنائية
1.10.9. جوانب مهمة من تقرير للتحاليل الجنائية
2.10.9. تصنيف وأنواع التقارير
3.10.9. دليل لكتابة التقرير
4.10.9. عرض التقرير
1.4.10.9. التحضير السابق للشهادة
2.4.10.9. الإيداع
3.4.10.9. التعامل مع وسائل الإعلام

الوحدة 10. التحديات الحالية والمستقبلية في أمن الكمبيوتر

1.10. تقنية Blockchain
1.1.10. مجالات التطبيق
2.1.10. ضمان السرية
3.1.10. ضمان عدم الرفض
2.10. النقود الرقمية
1.2.10. بيتكوين
2.2.10. العملات الرقمية
3.2.10. تعدين العملات المشفرة
4.2.10. مخططات بونزي
5.2.10. الجرائم والمشاكل المحتملة الأخرى
3.10. التزييف العميق
1.3.10. تأثير وسائل الإعلام
2.3.10. الأخطار على المجتمع
3.3.10. آليات الكشف
4.10. مستقبل الذكاء الاصطناعي
1.4.10. الذكاء الاصطناعي والحوسبة المعرفية
2.4.10. الاستخدامات لتبسيط خدمة العملاء
5.10. الخصوصية الرقمية
1.5.10. قيمة البيانات في الشبكة
2.5.10. استخدام البيانات على الشبكة
3.5.10. إدارة الخصوصية والهوية الرقمية
6.10. النزاعات السيبرانية ومجرمو الإنترنت والهجمات الإلكترونية
1.6.10. تأثير الأمن السيبراني في النزاعات الدولية
2.6.10. عواقب الهجمات الإلكترونية على عموم السكان
3.6.10. أنواع مجرمي الإنترنت. تدابير الحماية
7.10. العمل إلكترونيا
1.7.10. ثورة العمل عن بعد أثناء وبعد COVID-19
2.7.10. اختناقات الوصول
3.7.10. تباين سطح الهجوم
4.7.10. احتياجات العامل
8.10. التقنيات اللاسلكية الناشئة
1.8.10. WPA3
2.8.10. 5G
3.8.10. موجات ملليمتر
4.8.10. الاتجاه في "*Get Smart*" بدلاً من "*Get more*"
9.10. عنونة المستقبل في الشبكات
1.9.10. المشكلات الحالية مع معالجة IP
2.9.10. IPv6
3.9.10. IPv4+
4.9.10. مزايا IPv4+ عبر IPv4
5.9.10. مزايا IPv6 عبر IPv4
10.10. التحدي المتمثل في زيادة الوعي بالتدريب المبكر والمستمر للسكان
1.10.10. الاستراتيجيات الحكومية الحالية
2.10.10. المقاومة السكانية للتعلم
3.10.10. خطط التدريب التي يجب أن تتبناها الشركات

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

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.

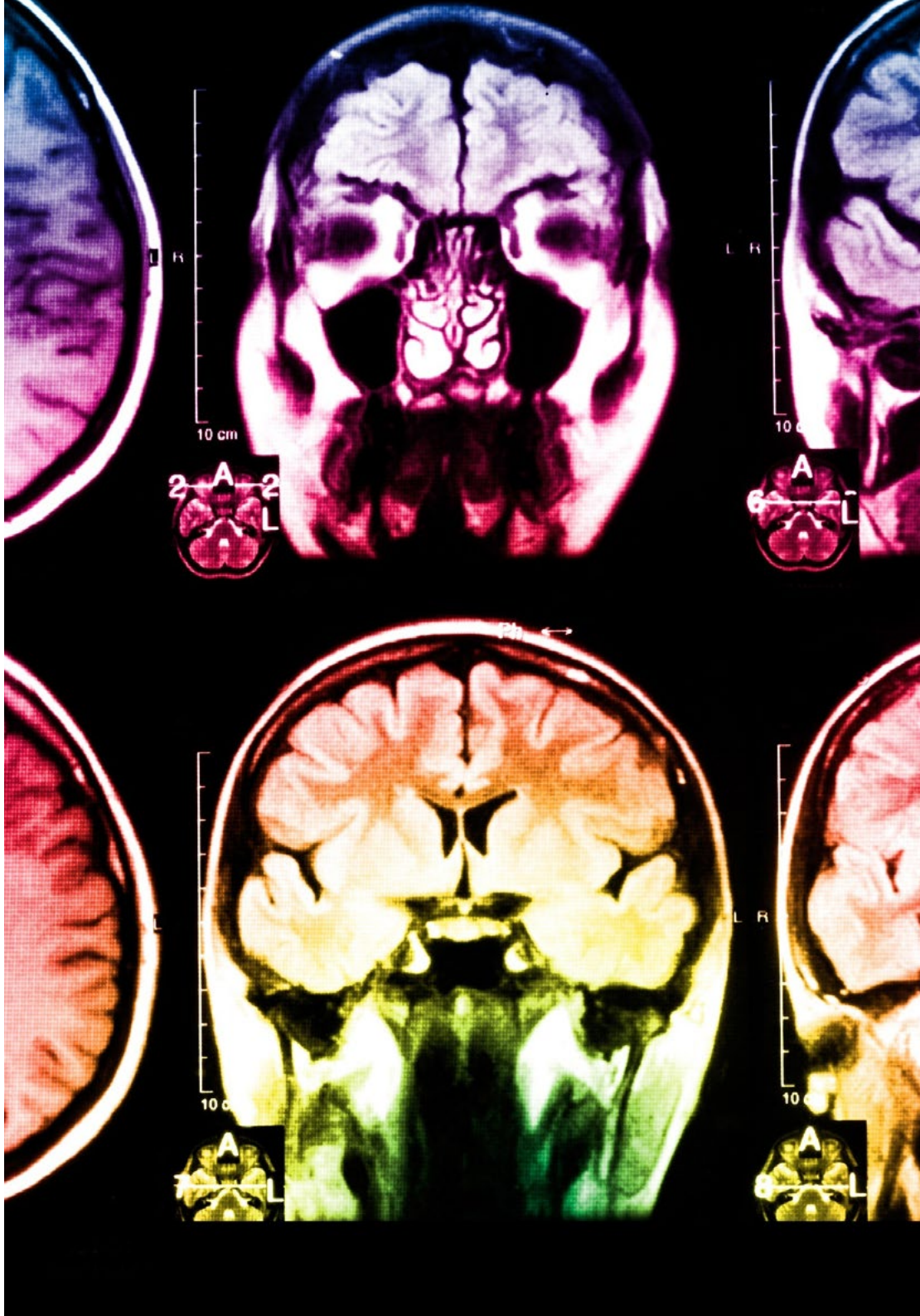
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

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.

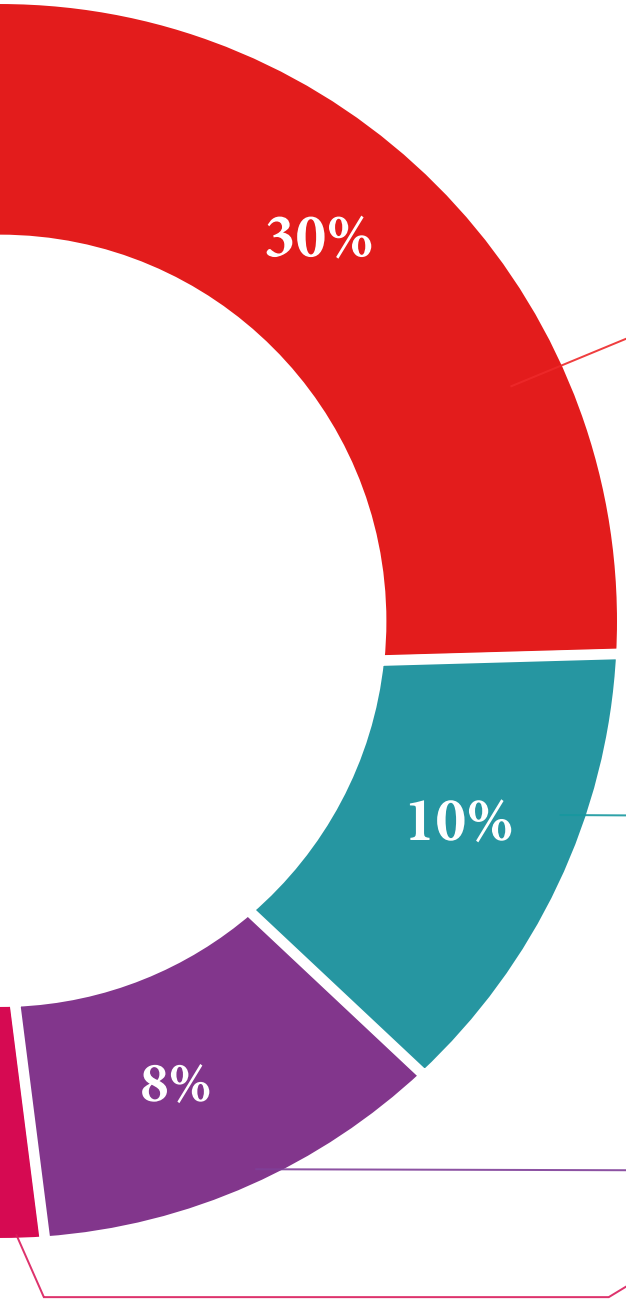
ستتيح لك منهجية إعادة التعلم والمعروفة بـ *Relearning*، التعلم بجهد أقل ومزيد من الأداء، وإشراكك بشكل أكبر في تدريبك، وتنمية الروح النقدية لديك، وكذلك قدرتك على الدفاع عن الحجج والآراء المتباينة: إنها معادلة واضحة للنجاح.

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

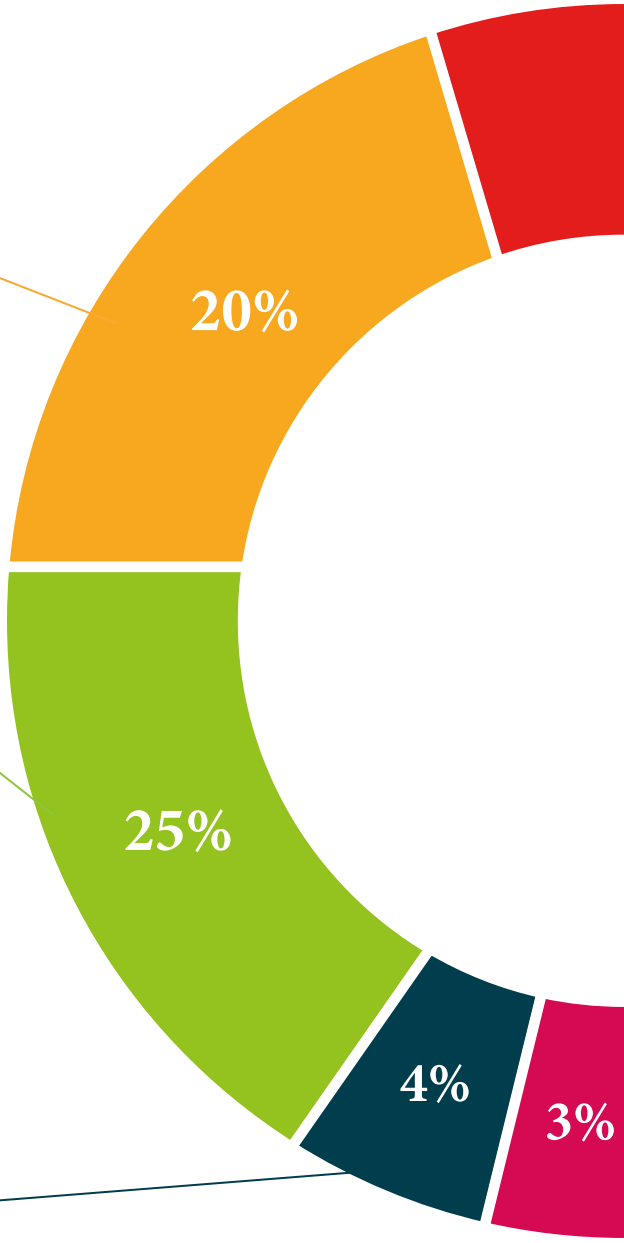
ملخصات تفاعلية

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



07

المؤهل العلمي

تضمن درجة الماجستير الخاص في إدارة الأمن السيبراني (CISO، كبير مسؤولي أمن المعلومات) بالإضافة إلى التدريب الأكثر دقة وتحديثًا، الحصول على شهادة اجتياز الماجستير الخاص الصادرة عن TECH الجامعة التكنولوجية.

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

تحتوي درجة **ماجستير خاص في إدارة الأمن السيبراني (CISO، كبير مسؤولي أمن المعلومات)** على البرنامج العلمي الأكثر اكتمالا وحداثة في السوق.

بعد اجتياز الطالب للتقييمات، سوف يتلقى عن طريق البريد العادي* مصحوب بعلم وصول مؤهل **ماجستير خاص** ذا الصلة الصادر عن **TECH الجامعة التكنولوجية.**

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

المؤهل العلمي: **ماجستير خاص في إدارة الأمن السيبراني (CISO، كبير مسؤولي أمن المعلومات)**

عدد الساعات الدراسية المعتمدة: **1500 ساعة**


الجامعة التكنولوجية

تمنح هذا

الدبلوم

لـ

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

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

ماجستير خاص

في

إدارة الأمن السيبراني

(كبير مسؤولي أمن المعلومات، CISO)

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 إدارة الأمن السيبراني

(كبير مسؤولي أمن المعلومات، CISO)

التوزيع العام للخطة الدراسية

نوع المادة	عدد الساعات
(OB) إجباري	1.500
(OP) إختياري	0
(PR) الممارسات الخارجية	0
(TFM) مشروع تخرج الماجيستير	0
الإجمالي 1500	

التوزيع العام للخطة الدراسية

الدورة	المادة	الطريقة	عدد الساعات
1°	الذكاء السيبراني والأمن السيبراني	إجباري	150
1°	أمن المضيف	إجباري	150
1°	أمان الشبكة (المحيطية)	إجباري	150
1°	أمان الهاتف الذكي	إجباري	150
1°	أمن إنترنت الأشياء IoT	إجباري	150
1°	القرصنة الأخلاقية	إجباري	150
1°	الهندسة العكسية	إجباري	150
1°	التنمية الآمنة	إجباري	150
1°	التحليل الجنائي	إجباري	150
1°	التحديات الحالية والمستقبلية في أمن الكمبيوتر	إجباري	150

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.

ماجستير خاص
إدارة الأمن السيبراني
(كبير مسؤولي أمن المعلومات، CISO)

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **12 شهر**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- عدد الساعات المخصصة للدراسة: **16 ساعات أسبوعيًا**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

ماجستير خاص

إدارة الأمن السيبراني

(كبير مسؤولي أمن المعلومات، CISO)

tech الجامعة التيكنولوجية