ماجستير متقدم

إدارة المعلومات الآمنة

(Secure Information Management)

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

ماجستير متقدم
إدارة المعلومات الآمنة
(Secure Information Management)

- طريقة الدراسة: **عبر الإنترنت**
- مدة الدراسة: **2 سنتين**
- المؤهل العلمي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **عبر الإنترنت**

رابط الدخول إلى الموقع الإلكتروني: www.techtitute.com/ae/information-technology/advanced-master-degree/advanced-master-degree-secure-information-management

الفهرس

01 تقديم البرنامج ص. 4

02 لماذا تدرس في TECH؟ ص. 8

03 خطة الدراسة ص. 12

04 أهداف التدريس ص. 32

05 الفرص المهنية ص. 38

06 منهجية الدراسة ص. 42

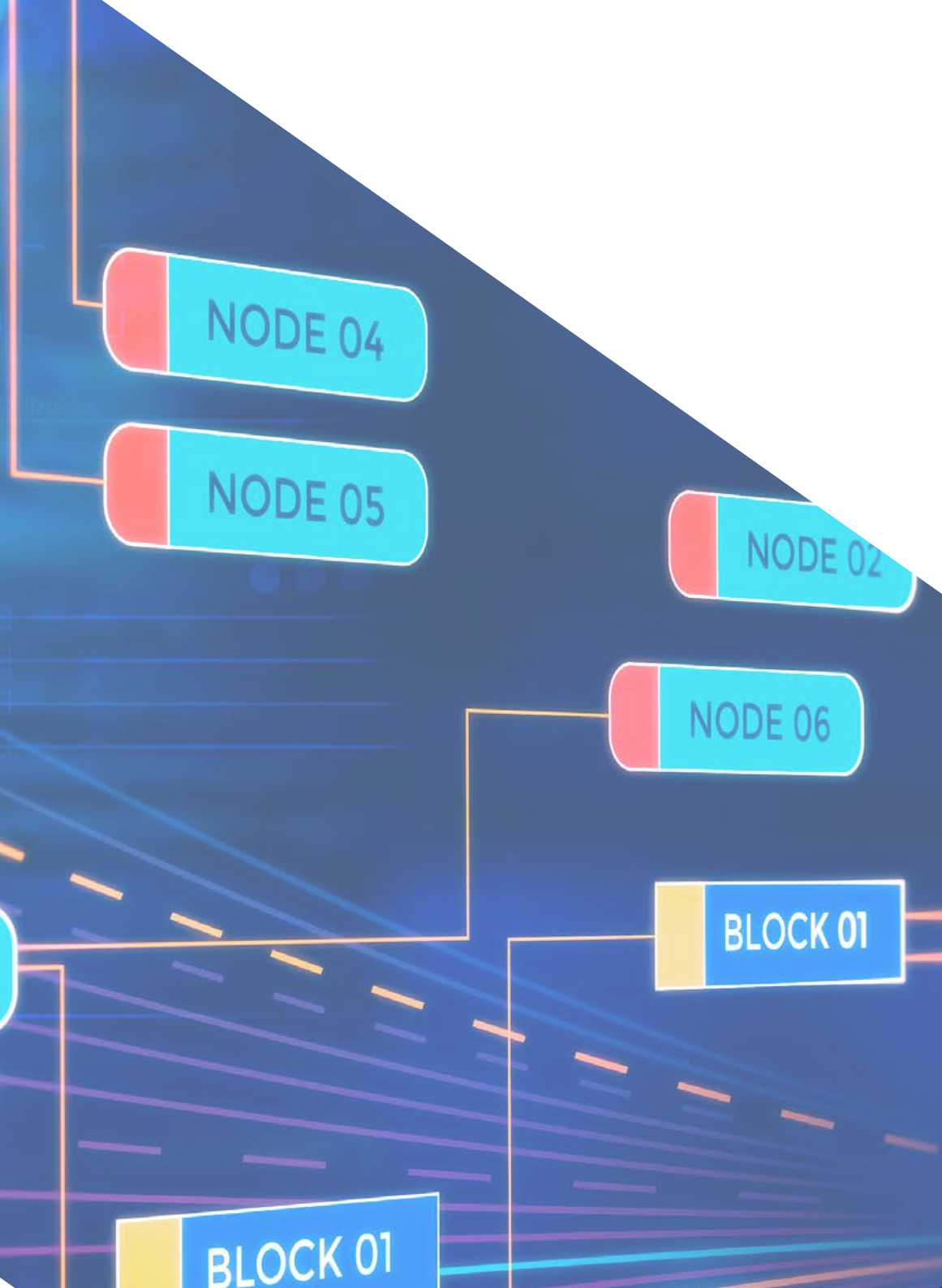
07 أعضاء هيئة التدريس ص. 52

08 المؤهل العلمي ص. 62

01

تقديم البرنامج

في العصر الرقمي الحالي، يتم تسيير الأنشطة في مختلف المجالات بشكل متكامل عبر الإنترنت. يعتمد الترفيه والعمل والتواصل مع الأصدقاء والعائلة بشكل متزايد على الأدوات والموارد المتاحة عبر الإنترنت. يتم يوميًا نقل كميات هائلة من المعلومات، بدءًا من البيانات البسيطة في المحادثات عبر شبكات التواصل الاجتماعي وتطبيقات المراسلة، وصولًا إلى المعلومات الحساسة ذات الطابع الشخصي والمهني المخزنة على المنصات المصرفية أو المؤسساتية. يتطلب هذا المشهد وجود متخصصين قادرين على إدارة المعلومات وحمايتها في سياقات متنوعة، مع إعطاء الأولوية لأمنها. ولهذا السبب، قامت TECH الجامعة التكنولوجية بتصميم هذا البرنامج في هندسة البرمجيات، والذي يركز على تأهيل المهنيين بالمهارات اللازمة لتسيير وحماية المعلومات بفعالية، ومواجهة التحديات الرقمية الحالية، والمساهمة في إنشاء بيئات تكنولوجية أكثر أمانًا وموثوقية.



"حماية البيانات أمر أساسي في مواجهة التهديدات المستمرة. يمكنك أن تكون الحارس لهذه المعلومات القيّمة"

في كل ثانية، يتم إنشاء آلاف البيانات ومشاركتها وتخزينها في البيئة الرقمية. بدءًا من إجراء المدفوعات عبر الإنترنت والوصول إلى الخدمات التعليمية، وصولًا إلى تنسيق الأنشطة المؤسساتية أو حماية الهويات الرقمية، أصبحت التكنولوجيا ركيزة أساسية تُحوِّل باستمرار طريقة عيشنا وعملنا. تنتج هذه التفاعلات وتنقل كميات هائلة من البيانات في كل لحظة، بدءًا من المعلومات الشخصية إلى الملفات الحساسة المتعلقة بالشركات والمؤسسات. يُبرز هذا التدفق المستمر للبيانات الحاجة إلى تسييرها بشكل مناسب لضمان أمنها وخصوصيتها.

تسيير وحماية هذه البيانات ليست مهمة سهلة، حيث تتطلب مزيجًا من المعرفة المتخصصة للغاية في مجالات مثل الأمن السيبراني وتسيير المعلومات. ورغم اختلاف هذه التخصصات، إلا أنه يجب دمجها لمواجهة التحديات المعقدة التي يفرضها العالم الرقمي اليوم. في هذا السياق، يمثل الماجيستير المتقدم في إدارة المعلومات الآمنة ((Secure Information Management)) فرصة فريدة للمهندسين والمهنيين في مجال المعلوماتية الذين يسعون إلى اكتساب رؤية شاملة تمكنهم من إتقان كلا المجالين والتميز كقادة في قطاع يشهد نموًا مستمرًا.

تواجه العديد من الشركات والمؤسسات الحاجة إلى حماية بياناتها الحساسة والحرجة، لكنها تفتقر إلى الخبراء القادرين على ضمان إدارة فعالة لمعلوماتها الرقمية وصيانتها ومراقبتها. وللإجابة على هذا الطلب، صممت TECH الجامعة التكنولوجية UNIVERSITY برنامجًا يجمع بين أفضل المحتويات وأعضاء هيئة تدريس يتمتعون بخبرة مهنية مرموقة. يضمن هذا النهج تزويد الطلاب بالأدوات والمعرفة اللازمة للتميز في سوق العمل والوصول إلى مناصب استراتيجية في المؤسسات التي تسعى إلى تعزيز أمن معلوماتها.

هذا **الماجستير المتقدم في إدارة المعلومات الآمنة** (**Secure Information Management**) يحتوي على البرنامج التعليم الأكثر اكتمالا وحداثة في السوق. أبرز خصائصه هي:

- تطوير حالات عملية يقدمها خبراء في إدارة المعلومات الآمنة
- المحتويات الرسومية والتخطيطية والعملية البارزة التي يتم تصورها بها، تجمع المعلومات العلمية والعملية حول تلك التخصصات الأساسية للممارسة المهنية.
- التمارين العملية حيث يمكن إجراء عملية التقييم الذاتي لتحسين التعلم
- تركيزه الخاص على المنهجيات المبتكرة في تسيير إدارة المعلومات الآمنة (Secure Information Management)
- دروس نظرية وأسئلة للخبراء ومنتديات مناقشة حول القضايا المثيرة للجدل وأعمال التفكير الفردية
- توفر المحتوى من أي جهاز ثابت أو محمول متصل بالإنترنت

"اكتسب المهارات اللازمة لضمان الأمن وتسيير البيانات بفعالية في بيئة رقمية تنافسية"

اكتشف المنهجية التعليمية الأكثر ابتكارًا التي صممتها TECH لضمان تعلم غامر ومترابط بالسياق.

استفد من برنامج 100% عبر الإنترنت يتيح لك الدراسة وفقًا لوتيرتك الخاصة، في أي وقت ومن أي مكان في العالم.

"عزز معارفك النظرية من خلال الموارد العملية العديدة المتضمنة في هذا ماجيستير متقدم في إدارة المعلومات الآمنة (Secure Information Management)"

يضم فريقه الأكاديمي مهنيين من مجال المالية، ينقلون إلى هذا البرنامج خبرتهم العملية، إلى جانب متخصصين بارزين من مؤسسات مرجعية وجامعات مرموقة

إن محتوى الوسائط المتعددة الذي تم تطويره باستخدام أحدث التقنيات التعليمية، والذين سيتيح للمهني فرصة للتعلم الموضوعي والسياقي، أي في بيئة محاكاة ستوفر تعليماً غامرًا مبرمجًا للتدريب في مواقف حقيقية.

يركز تصميم هذا البرنامج على التعلم القائم على المشكلات، والذي يجب على الطالب من خلاله محاولة حل الحالات المختلفة للممارسة المهنية التي تُطرَح على مدار هذه الدورة الأكاديمية. للقيام بذلك، المهني سيحصل على مساعدة من نظام فيديو تفاعلي مبتكر من قبل خبراء مشهورين.

02

لماذا تدرس في TECH؟

جامعة TECH هي أكبر جامعة رقمية في العالم. بفضل كتالوجه المذهل الذي يضم أكثر من 14000 برنامج جامعي متاح بـ 11 لغة، تحتل TECH موقع الريادة في قابلية التوظيف، مع معدل إدماج مهني يبلغ 99%. بالإضافة إلى ذلك، تضم هيئة تدريسية واسعة تضم أكثر من 6000 أستاذ من أعلى مستويات التقدير الدولي.

"ادرس في أكبر جامعة رقمية في العالم واضمن نجاحك المهني. المستقبل يبدأ في TECH"

أفضل جامعة عبر الإنترنت في العالم وفقًا لمجلة FORBES

أشادت مجلة فوربس المرموقة، المتخصصة في الأعمال والتمويل، بـ TECH ووصفتها بأنها «أفضل جامعة عبر الإنترنت في العالم». وقد أكدت ذلك مؤخرًا في مقال نُشر في نسختها الرقمية، حيث سلطت الضوء على نجاح هذه المؤسسة «بفضل عرضها الأكاديمي، واختيارها لفريقها التدريسي، ومنهجها التعليمي المبتكر الذي يهدف إلى تأهيل مهنيي المستقبل»

أفضل هيئة تدريس دولية من النخبة

تضم هيئة التدريس في TECH أكثر من 000, أستاذ من أعلى مستويات التقدير الدولي. أساتذة وباحثون وكبار المديرين التنفيذيين من شركات متعددة الجنسيات، من بينهم Isaiah Covington، مدرب الأداء في فريق Boston Celtics، Magda Romanskag، الباحثة الرئيسية في Harvard MetaLAB، Egacio Wistumbag، رئيس قسم علم الأمراض الجزيئية الانتقالية في مركز MD Anderson لعلاج السرطان، و D.W. Pine، المدير الإبداعي لمجلة TIME، وغيرهم.

أكبر جامعة رقمية في العالم

جامعة TECH أكبر جامعة رقمية في العالم. نحن أكبر نطاق تعليمية، بأفضل وأوسع قائمة برامج تعليمية رقمية، مائة في المئة عبرالانترنت وتغطي الغالبية العظمى من شتى مجالات المعرفة. نحن نقدم أكبر عدد من المؤهلات العلمية الجامعية الخاصة والمعتمدة في الدراسات العليا عبرالأنترنت وكذلك في البكالوريوس الجامعي. أجمالا، أكثر من 14000 مؤهل جامعي، بإحدى عشر لغة مختلفة، تجعلنا أكبر نطاق تعليمية في العالم.

Forbes
Mejor universidad online del mundo

Plan
de estudios
más completo

Profesorado
TOP
Internacional

La metodología
más eficaz

nº1
Mundial
Mayor universidad online del mundo

أكثر الخطط الدراسية شمولاً في المشهد الجامعي

توفر TECH أكثر الخطط الدراسية تكاملاً في المشهد الجامعي، مع مناهج تشمل المفاهيم الأساسية وأحدث التطورات العلمية في مجالاتها التخصصية. بالإضافة إلى ذلك، يتم تحديث هذه البرامج باستمرار لضمان تزويد الطلاب بأحدث المعارف الأكاديمية والمهارات المهنية الأكثر طلبًا. وبذلك، تمنح شهادات الجامعة لخريجيها ميزة كبيرة لدفع مسيرتهم المهنية نحو النجاح.

أسلوب تعليمي فريد

تعد TECH أول جامعة تطبق منهجية Relearning في جميع برامجها الأكاديمية.. ويُعتبر هذا النهج أفضل أسلوب تعليمي عبر الإنترنت، حيث حصل على شهادات جودة أكاديمية دولية معتمدة من وكالات تعليمية مرموقة. علاوة على ذلك، يُكمل هذا النموذج الأكاديمي المتطور بـ"منهجية الحالة"، مما يشكل استراتيجية تعليمية رقمية فريدة من نوعها. كما تعتمد الجامعة موارد تعليمية مبتكرة تشمل مقاطع فيديو تفصيلية، وإنفوجرافيك، وملخصات تفاعلية.

الجامعة الافتراضية الرسمية للرابطة الوطنية لكرة السلة NBA

جامعة TECH هي الجامعة الرسمية عبر الإنترنت للـNBA وبفضل شراكتها مع أكبر دوري لكرة السلة في العالم، تقدم برامج جامعية حصرية لطلابها، بالإضافة إلى مجموعة واسعة من الموارد التعليمية التي تركز على قطاع أعمال الرابطة ومجالات أخرى في صناعة الرياضة. كل برنامج مصمم بمحتوى أكاديمي فريد، ويشمل محاضرات يقدمها متحدثون متميزون، وهم خبراء رياضيون بارزون يشاركون خبراتهم حول الموضوعات الأكثر أهمية.

الريادة في التوظيف

نجحت TECH في أن تصبح الجامعة الرائدة في توظيف الخريجين، حيث يحصل 99% من طلابها على وظيفة في مجالهم الأكاديمي خلال أقل من عام من التخرج. كما يتمكن عدد كبير منهم من تحسين مسارهم المهني فور الانتهاء من برامجهم الدراسية. ويعود هذا النجاح إلى منهجية تعليمية تركز على اكتساب المهارات العملية، وهي عنصر أساسي لضمان التفوق المهني في سوق العمل.

99%
Garantía de máxima empleabilidad

4.9/5
★★★★★
★ global score

NBA
Universidad online oficial de la NBA

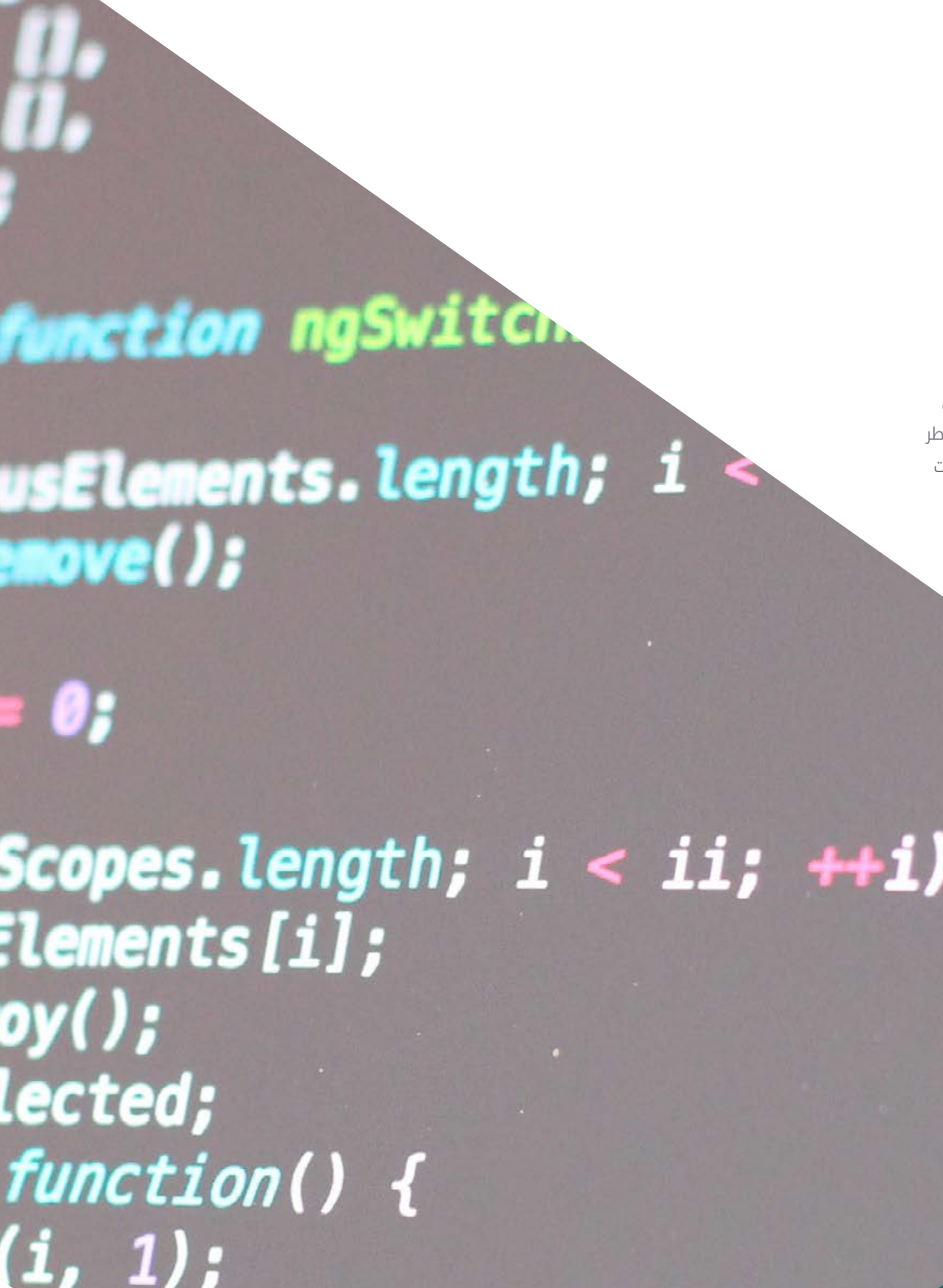
Google Partner
PREMIER 2023

الجامعة الأعلى تصنيفاً على مستوى العالم قبل طلابها

حصلت TECH على لقب الجامعة الأعلى تقييمًا عالميًا وفقًا لأبرز منصات التقييم، حيث حققت تصنيفًا متميزًا بلغ 4.9 من 5، بناءً على أكثر من 1,000 مراجعة. تعكس هذه النتائج مكانة TECH كمرجع أكاديمي دولي، مما يعزز جودة نموذجها التعليمي وأثره الإيجابي على طلابها.

Google Partner Premier

حصلت TECH على شارة Google Partner Premier المرموقة من عملاق التكنولوجيا الأمريكي. هذا التقدير، الذي لا تحصل عليه سوى 3% من الشركات في العالم، يبرز تجربة التعلم الفعالة والمرنة والمبتكرة التي توفرها الجامعة لطلابها. ولا يقتصر هذا الاعتراف على تأكيد أعلى معايير الجودة الأكاديمية، بل يعزز مكانة TECH كإحدى أبرز المؤسسات التكنولوجية في العالم.



03

خطة الدراسة

تم إعداد المواد التعليمية التي يتضمنها هذا الماجيستير المتقدم في إدارة المعلومات الآمنة (Secure Information Management) من قبل فريق من الخبراء في الأمن السيبراني وتسيير البيانات. بهذه الطريقة، يتعمق المنهج الدراسي في التهديدات الرقمية الرئيسية وأحدث المنهجيات لحماية المعلومات وإدارتها. سيمكن ذلك الخريجين من تحديد المخاطر المحددة وتطوير حلول فعالة لضمان أمان البيانات في مختلف البيئات المهنية. علاوة على ذلك، يتناول المحتوى الأدوات الأكثر ابتكارًا في هذا المجال، مما يعزز الاستراتيجيات الموجهة لحماية الأصول الرقمية للمؤسسات.

"ستساهم في حماية البيانات الحساسة وإنشاء أنظمة آمنة تضمن استمرارية العمليات في الشركات والمؤسسات"

الوحدة 1. تحليلات البيانات في المؤسسة التجارية

1.1. تحليل الأعمال
1.1.1. تحليل الأعمال
2.1.1. هيكل البيانات
3.1.1. المراحل والعناصر
2.1. تحليلات البيانات في المؤسسة التجارية
1.2.1. لوحات المعلومات ومؤشرات الأداء الرئيسية حسب القسم
2.2.1. التقارير التشغيلية والتكتيكية والاستراتيجية
3.2.1. تطبيق تحليلات البيانات على كل قسم
1.3.2.1. التسويق والاتصال
2.3.2.1. تجاري
3.3.2.1. خدمة العملاء
4.3.2.1. المشتريات
5.3.2.1. الإدارة
6.3.2.1. الموارد البشرية
7.3.2.1. الإنتاج
8.3.2.1. IT
3.1. التسويق والاتصال
1.3.1. مؤشرات الأداء الرئيسية للقياس والتطبيقات والفوائد
2.3.1. أنظمة التسويق ومستودعات البيانات
3.3.1. تنفيذ هيكل تحليل البيانات في التسويق
4.3.1. خطة التسويق والاتصال
5.3.1. الإستراتيجيات والتنبؤ وإدارة الحملات
4.1. التجارة والمبيعات
1.4.1. مساهمات تحليلات البيانات في المجال التجاري
2.4.1. احتياجات قسم المبيعات
3.4.1. دراسات السوق
5.1. خدمة العملاء
1.5.1. الولاء
2.5.1. الجودة الشخصية والذكاء العاطفي
3.5.1. رضا العملاء
6.1. المشتريات
1.6.1. تحليلات البيانات لأبحاث السوق
2.6.1. تحليلات البيانات لدراسات المنافسة
3.6.1. التطبيقات الأخرى
7.1. الإدارة
1.7.1. الاحتياجات في قسم الإدارة
2.7.1. مستودع البيانات وتحليل المخاطر المالية
3.7.1. مستودع البيانات وتحليل المخاطر الائتمانية
8.1. الموارد البشرية
1.8.1. الموارد البشرية وفوائد تحليلات البيانات
2.8.1. أدوات تحليل البيانات في قسم الموارد البشرية.
3.8.1. تطبيق تحليلات البيانات في الموارد البشرية.
9.1. الإنتاج
1.9.1. تحليل البيانات في قسم الإنتاج
2.9.1. التطبيقات
3.9.1. الفوائد
10.1. IT
1.10.1.قسم تكنولوجيا المعلومات
2.10.1.تحليلات البيانات والتحول الرقمي
3.10.1.الابتكار والإنتاجية

الوحدة 2. إدارة ومعالجة البيانات والمعلومات لعلوم البيانات

1.2. إحصائيات. المتغيرات والمؤشرات والنسب
1.1.2. الإحصاءات.
2.1.2. الأبعاد الإحصائية
3.1.2. المتغيرات والمؤشرات والنسب
2.2. نوع البيانات
1.2.2. نوعية
2.2.2. كمية
3.2.2. التوصيف والفئات
3.2. معرفة البيانات من القياسات
1.3.2. المقاييس المركزية
2.3.2. مقاييس التشتت
3.3.2. الارتباطات
4.2. رؤى حول البيانات من الرسوم البيانية
1.4.2. التصور حسب نوع البيانات
2.4.2. تفسير المعلومات الرسومية
3.4.2. تخصيص الرسومات باستخدام برنامج آر.

5.2. الاحتمال
1.5.2. الاحتمال
2.5.2. وظيفة الاحتمال
3.5.2. التوزيعات
6.2. جمع البيانات
1.6.2. منهجية التحصيل
2.6.2. أدوات التحصيل
3.6.2. قنوات التحصيل
7.2. تنظيف البيانات
1.7.2. مراحل تطهير البيانات
2.7.2. جودة البيانات
3.7.2. معالجة البيانات (مع لغة R)
8.2. تحليل البيانات وتفسيرها وتقييم النتائج
1.8.2. المقاييس الإحصائية
2.8.2. مؤشرات العلاقة
3.8.2. استخراج البيانات
9.2. مستودع البيانات (Datawarehouse)
1.9.2. العوامل
2.9.2. التصميم
10.2. توافر البيانات
1.10.2.الدخول
2.10.2.الوصول
3.10.2.الأمان

الوحدة 3. أجهزة ومنصات IoT كأساس لعلوم البيانات

1.3. انترنت الأشياء
1.1.3. إنترنت المستقبل، Internet of Things
2.1.3. اتحاد الإنترنت الصناعي
2.3. الهندسة المعمارية المرجعية
1.2.3. العمارة المرجعية
2.2.3. الطبقات
3.2.3. المكونات
3.3. المجسّات وأجهزة IoT
1.3.3. المكونات الرئيسية
2.3.3. المستشعرات والمشغلات الميكانيكية
4.3. الاتصالات والبروتوكولات
1.4.3. بروتوكولات. نموذج اللوحة القماشية
2.4.3. تكنولوجيات الاتصال
5.3. المنصات السحابية لإنترنت الأشياء وإنترنت الأشياء الصناعية
1.5.3. منصات الأغراض العامة
2.5.3. منصات صناعية
3.5.3. منصات مفتوحة المصدر
6.3. إدارة البيانات في منصات إنترنت الأشياء IoT
1.6.3. آليات إدارة البيانات. البيانات المفتوحة
2.6.3. تبادل البيانات والتصور
7.3. الأمن في إنترنت الأشياء IoT
1.7.3. المتطلبات ومجالات الأمان
2.7.3. استراتيجيات أمان الإنترنت الصناعي للأشياء IIoT
8.3. تطبيقات إنترنت الأشياء IoT
1.8.3. المدن الذكية
2.8.3. الصحة و اللياقة
3.8.3. المنزل الذكي
4.8.3. التطبيقات الأخرى
9.3. تطبيقات إنترنت الصناعي للأشياء IIoT
1.9.3. التصنيع
2.9.3. النقل
3.9.3. طاقة
4.9.3. الزراعة وتربية المواشي
5.9.3. قطاعات أخرى
10.3. الصناعة 0.4
1.10.3.IoRT (إنترنت الأشياء الروبوتية)
2.10.3.تصنيع المواد المضافة ثلاثية الأبعاد
3.10.3.Big Data Analytics

الوحدة 4. العرض البياني لتحليل البيانات

1.4. التحليل الاستكشافي
1.1.4. العرض من أجل تحليل المعلومات
2.1.4. قيمة التمثيل البياني
3.1.4. نماذج جديدة للتمثيل البياني

2.4. تحسين علوم البيانات
1.2.4. نطاق اللون والتصميم
2.2.4. نظرية الغَشتَلت في التمثيل البياني
3.2.4. تجنب الأخطاء والنصائح
3.4. مصادر البيانات الأساسية
1.3.4. من أجل عرض الجودة
2.3.4. من أجل عرض الكمية
3.3.4. من أجل عرض الوقت
4.4. مصادر البيانات المعقدة
1.4.4. الملفات والقوائم وقواعد بيانات
2.4.4. البيانات المفتوحة
3.4.4. إنشاء البيانات المستمرة
5.4. أنواع المخططات
1.5.4. العروض الأساسية
2.5.4. العروض الكتلية
3.5.4. العروض لتحليل التشتت
4.5.4. العروض الدائرية
5.5.4. عروض الفقاعة
6.5.4. العروض الجغرافية
6.4. أنواع العرض
1.6.4. المقارنة والعلائقية
2.6.4. التوزيع
3.6.4. الهرمية
7.4. تصميم التقارير مع العرض البياني
1.7.4. تطبيق الرسوم البيانية في تقارير التسويق
2.7.4. تطبيق الرسوم البيانية في لوحات المعلومات ومؤشرات الأداء الرئيسية
3.7.4. تطبيق الرسوم البيانية في الخطط الاستراتيجية
4.7.4. استخدامات أخرى: علم، صحة، أعمال
8.4. السرد التصويري
1.8.4. السرد التصويري
2.8.4. التطور
3.8.4. الوصول
9.4. أدوات موجهة للتصور
1.9.4. ادوات متطورة
2.9.4. برامج عبر الإنترنت
3.9.4. Open Source
10.4. التقنيات الجديدة في تصور البيانات
1.10.4. أنظمة لافتراضية الواقع
2.10.4. أنظمة تكبير وتقوية الواقع
3.10.4. أنظمة ذكية

الوحدة 5. أدوات علوم البيانات

1.5. علم البيانات
1.1.5. علم البيانات
2.1.5. أدوات متقدمة لعالم البيانات
2.5. البيانات والمعلومات والمعرفة
1.2.5. البيانات والمعلومات والمعرفة
2.2.5. أنواع البيانات
3.2.5. مصادر البيانات
3.5. من البيانات إلى المعلومات
1.3.5. تحليل البيانات
2.3.5. أنواع التحليل
3.3.5. استخراج المعلومات من مجموعة البيانات Dataset
4.5. استخراج المعلومات من خلال التصور
1.4.5. التصور كأداة تحليل
2.4.5. طرق العرض
3.4.5. عرض مجموعة البيانات
5.5. جودة البيانات
1.5.5. بيانات الجودة
2.5.5. تطهير البيانات
3.5.5. معالجة البيانات الأساسية
6.5. Dataset
1.6.5. تخصيب مجموعة البيانات
2.6.5. لعنة الأبعاد
3.6.5. تعديل مجموعة البيانات الخاصة بنا

7.5. اختلال التوازن
1.7.5. عدم التوازن الطبقي
2.7.5. تقنيات تخفيف الاختلال
3.7.5. موازنة مجموعة البيانات
8.5. نماذج غير خاضعة للرقابة
1.8.5. نموذج غير خاضع للرقابة
2.8.5. مناهج
3.8.5. التصنيف بنماذج غير خاضعة للرقابة
9.5. النماذج الخاضعة للإشراف
1.9.5. نموذج خاضع للإشراف
2.9.5. مناهج
3.9.5. التصنيف مع النماذج الخاضعة للإشراف
10.5. الأدوات والممارسات الجيدة
1.10.5. أفضل الممارسات لعالم البيانات
2.10.5. أفضل نموذج
3.10.5. أدوات مفيدة

الوحدة 6. تنقيب البيانات والاختيار والمعالجة المسبقة والتحويل

1.6. الاستدلال الإحصائي
1.1.6. الإحصاء الوصفي مقابل. الاستدلال الإحصائي
2.1.6. إجراءات حدودية
3.1.6. الإجراءات اللامعلمية
2.6. التحليل الاستكشافي
1.2.6. التحليل الوصفي
2.2.6. العرض
3.2.6. إعداد البيانات
3.6. إعداد البيانات
1.3.6. تكامل البيانات وتنقيتها
2.3.6. تطبيع البيانات
3.3.6. سمات التحويل
4.6. القيم المفقودة
1.4.6. معالجة القيم الناقصة
2.4.6. طرق التضمين القصوى
3.4.6. احتساب القيم المفقودة باستخدام التعلم الآلي
5.6. الضجيج في البيانات
1.5.6. فئات وسمات الضجيج
2.5.6. ترشيح الضجيج
3.5.6. تأثير الضجيج
6.6. لعنة الأبعاد
1.6.6. الإفراط في أخذ العينات
2.6.6. Undersampling
3.6.6. تقليل البيانات متعددة الأبعاد
7.6. من الصفات المستمرة إلى المنفصلة
1.7.6. البيانات المستمرة مقابل البيانات المنفصلة
2.7.6. عملية التكتم
8.6. البيانات
1.8.6. اختيار البيانات
2.8.6. وجهات النظر ومعايير الاختيار
3.8.6. مناهج الاختيار
9.6. تحديد المثيل
1.9.6. مناهج اختيار الحالات
2.9.6. اختيار النماذج
3.9.6. مناهج متقدمة لاختيار المثيل
10.6. المعالجة التمهيدية للبيانات في بيئات البيانات الضخمة Big Data
1.10.6. Big Data
2.10.6. المعالجة"الكلاسيكية" مقابل المعالجة المسبقة السائبة
3.10.6. Smart Data

الوحدة 7. القدرة على التنبؤ وتحليل الظواهر العشوائية

1.7. السلاسل الزمنية
1.1.7. السلاسل الزمنية
2.1.7. المنفعة والتطبيق
3.1.7. الحالات ذات الصلة
2.7. السلسلة الزمنية
1.2.7. اتجاه الموسمية ST
2.2.7. الاختلافات النموذجية
3.2.7. تحليل المخلفات

3.7. الأنماط
1.3.7. الثابتة
2.3.7. الغير ثابتة
3.3.7. التحولات والتعديلات
4.7. مخططات السلاسل الزمنية
1.4.7. مخطط (نموذج) مضاف
2.4.7. مخطط مضاعف (نموذج)
3.4.7. إجراءات تحديد نوع النموذج
5.7. طرق التنبؤ الأساسية forecast
1.5.7. إعلام
2.5.7. Naïve
3.5.7. Naïve موسمية
4.5.7. مقارنة المناهج
6.7. تحليل المخلفات
1.6.7. الارتباط التلقائي
2.6.7. النفايات ACF
3.6.7. اختبار الارتباط
7.7. الانحدار في سياق السلاسل الزمنية
1.7.7. ANOVA
2.7.7. الأساسيات
3.7.7. تطبيقات عملية
8.7. النماذج التنبؤية للسلاسل الزمنية
1.8.7. ARIMA
2.8.7. تجانس الأسي
9.7. معالجة وتحليل السلاسل الزمنية باستخدام R.
1.9.7. إعداد البيانات
2.9.7. تحديد النمط
3.9.7. تحليل النموذج
4.9.7. التنبؤ
10.7. الجمع بين التحليل البياني مع R
1.10.7. المواقف الإعتيادية
2.10.7. تطبيق عملي لحل المشاكل البسيطة
3.10.7. تطبيق عملي لحل المشاكل المتقدمة

الوحدة 8. تصميم وتطوير الأنظمة الذكية

1.8. المعالجة المسبقة للبيانات
1.1.8. المعالجة المسبقة للبيانات
2.1.8. تحويل البيانات
3.1.8. استخراج البيانات
2.8. التعلم الالي
1.2.8. التعلم الخاضع للإشراف وغير الخاضع للإشراف
2.2.8. التعليم المعزز
3.2.8. نماذج أخرى للتعلم
3.8. خوارزميات التصنيف
1.3.8. التعلم الآلي الاستقرائي
2.3.8. SVM و KNN
3.3.8. مقاييس ودرجات الترتيب
4.8. خوارزميات الانحدار
1.4.8. الانحدارالخطي والانحدار اللوجستي والنماذج غير الخطية
2.4.8. التسلسل الزمني
3.4.8. مقاييس ودرجات الانحدار
5.8. خوارزميات التجميع
1.5.8. تقنيات التجميع الهرمي
2.5.8. تقنيات التجميع الجزئي
3.5.8. المقاييس والنتائج للتجميع (clustering)
6.8. تقنيات قواعد الجمعية
1.6.8. مناهج استخراج القواعد
2.6.8. المقاييس والنتائج لخوارزميات قاعدة الارتباط
7.8. تقنيات التصنيف المتقدمة. المصنفات المتعددة
1.7.8. خوارزميات التعبئة (Bagging)
2.7.8. غابات الفارس العشوائية
3.7.8. التعزيز من أجل أشجار القرار
8.8. النماذج الرسومية الاحتمالية
1.8.8. النماذج الاحتمالية
2.8.8. شبكة بايزية. الخصائص والتمثيل والمعلمات
3.8.8. نماذج بيانية احتمالية أخرى

9.8. الشبكات العصبية
1.9.8. التعلم الآلي باستخدام الشبكات العصبية الاصطناعية
2.9.8. شبكات التغذية (feedforward)
10.8. التعلم العميق
1.10.8. شبكات التغذية feedforward العميقة
2.10.8. الشبكات العصبونية التلافيفية ونماذج التسلسل
3.10.8. أدوات لتنفيذ الشبكات العصبية العميقة

الوحدة 9. معماريات وأنظمة للاستخدام المكثف للبيانات

1.9. المتطلبات الغير التشغيلية ركائز تطبيقات البيانات الضخمة
1.1.9. المصداقية
2.1.9. القدرة على التكيف
3.1.9. قابلية الصيانة
2.9. نماذج البيانات
1.2.9. نموذج العلائقية
2.2.9. نموذج وثائقي
3.2.9. نموذج بيانات الرسم البياني
3.9. قواعد بيانات. تخزين البيانات وإدارة استرجاعها
1.3.9. مؤشرات التجزئة
2.3.9. تخزين السجل المنظم
3.3.9. الأشجار ب
4.9. تنسيقات ترميز البيانات
1.4.9. تنسيقات خاصة باللغة
2.4.9. تنسيقات موحدة
3.4.9. تنسيقات الترميز الثنائي
4.4.9. تدفق البيانات بين العمليات
5.9. النسخ
1.5.9. أهداف النسخ المتماثل
2.5.9. نماذج النسخ المتماثل
3.5.9. قضايا النسخ المتماثل
6.9. المعاملات الموزعة
1.6.9. العملية
2.6.9. بروتوكولات المعاملات الموزعة
3.6.9. المعاملات القابلة للتسلسل
7.9. التقسيم
1.7.9. أشكال التقسيم
2.7.9. تفاعل الفهارس الثانوية والتقسيم
3.7.9. إعادة موازنة الأقسام
8.9. معالجة البيانات دون اتصال بالإنترنت
1.8.9. تجهيز الدفعات
2.8.9. أنظمة الملفات الموزعة
3.8.9. MapReduce
9.9. معالجة البيانات في الوقت الحقيقي
1.9.9. أنواع وسيط الرسائل
2.9.9. تمثيل قواعد البيانات كتدفقات البيانات
3.9.9. معالجة دفق البيانات
10.9. تطبيقات عملية في المؤسسة التجارية
1.10.9. الاتساق في القراءات
2.10.9. نهج شامل للبيانات
3.10.9. توسيع نطاق الخدمة الموزعة

الوحدة 10. التطبيق العملي لعلوم البيانات في قطاعات النشاط التجاري

1.10. قطاع الصحة
1.1.10. تداعيات الذكاء الاصطناعي وتحليلات البيانات في قطاع الرعاية الصحية
2.1.10. الفرص والتحديات
2.10. المخاطر والاتجاهات في قطاع الصحة
1.2.10. الاستخدام في قطاع الرعاية الصحية
2.2.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
3.10. الخدمات المالية
1.3.10. تداعيات الذكاء الاصطناعي وتحليلات البيانات في صناعة الخدمات المالية
2.3.10. الاستخدام في الخدمات المالية
3.3.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
4.10. البيع بالتجزئة Retail
1.4.10. تداعيات الذكاء الاصطناعي وتحليلات البيانات في قطاع البيع بالتجزئة
2.4.10. استخدام البيع بالتجزئة
3.4.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي

5.10. الصناعة 0.4
1.5.10.تداعيات الذكاء الاصطناعي وتحليلات البيانات في الصناعة 0.4.
2.5.10.الاستخدام في الصناعة 0.4.
6.10. المخاطر والاتجاهات في الصناعة 0.4.
1.6.10.المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
7.10. الإدارة العامة
1.7.10.تداعيات الذكاء الاصطناعي وتحليلات البيانات فيفي الإدارة العامة.
2.7.10.استخدامها في الإدارة العامة
3.7.10.المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
8.10. التعليم
1.8.10.تداعيات الذكاء الاصطناعي وتحليلات البيانات في التعليم
2.8.10.المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
9.10. الغابات والزراعة
1.9.10.الآثار المترتبة على الذكاء الاصطناعي وتحليلات البيانات في قطاع الغابات والزراعة
2.9.10.الاستخدم في الغابات والزراعة
3.9.10.المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
10.10. الموارد البشرية
1.10.10. آثار الذكاء الاصطناعي وتحليلات البيانات في إدارة الموارد البشرية
2.10.10. تطبيقات عملية في عالم الأعمال
3.10.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي

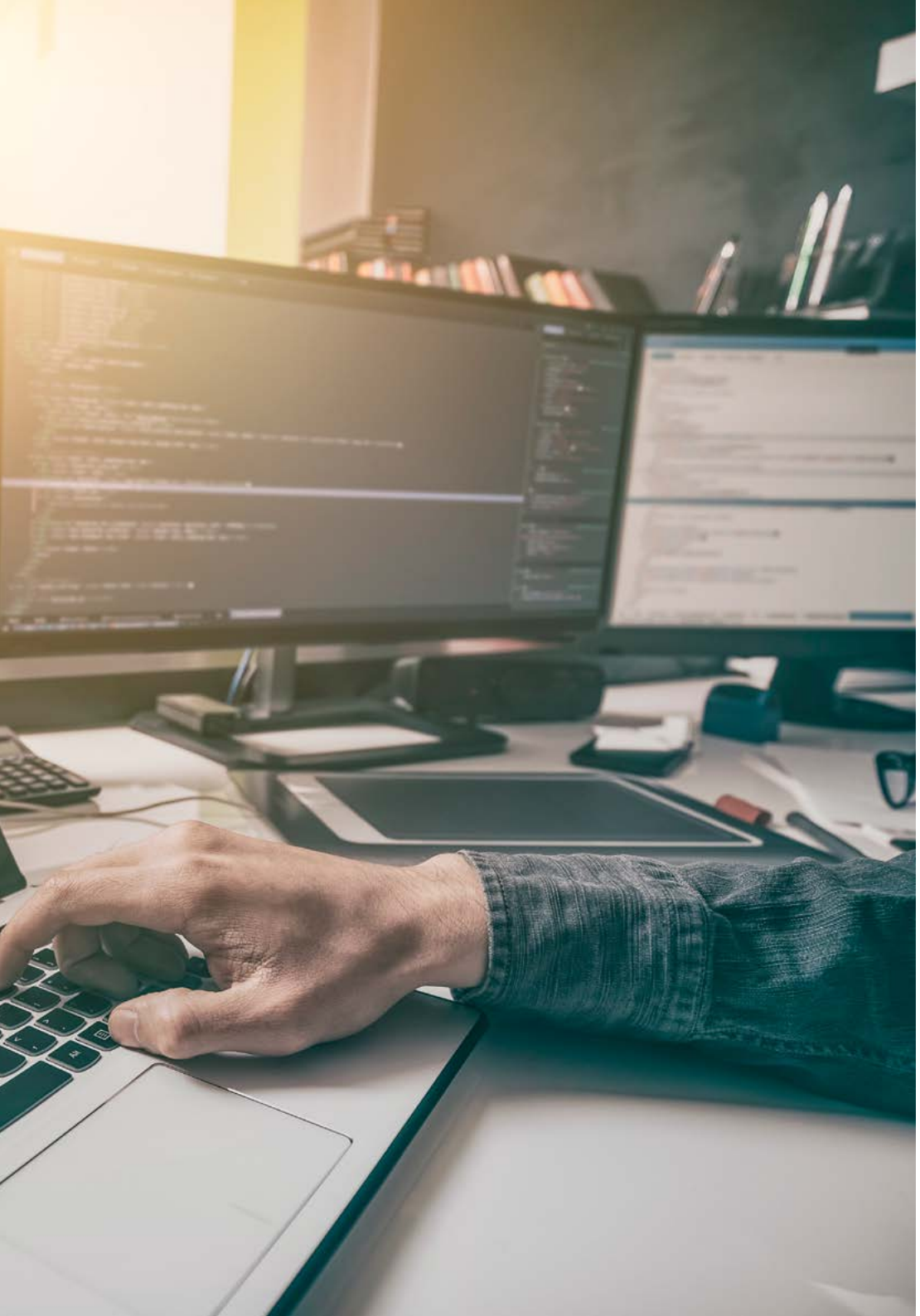
الوحدة 11. الذكاء والأمن السيبراني

1.11. الذكاء السيبراني
1.1.11.الذكاء السيبراني
1.1.1.11. الذكاء
1.1.1.1.11. دورة ذكاء
2.1.1.11. الذكاء السيبراني
3.1.1.11. الذكاء والأمن السيبراني
2.1.11.محلل الاستخبارات
1.2.1.11. دور المحلل الاستخباراتي
2.2.1.11. تحيز محلل الاستخبارات في النشاط التقييمي
2.11. الأمن السيبراني
1.2.11.طبقات الأمان
2.2.11.التعرف على التهديدات السيبراني
1.2.2.11. التهديدات الخارجية
2.2.2.11. التهديدات الداخلية
3.2.11.الإجراءات العكسية
1.3.2.11. الهندسة الاجتماعية
2.3.2.11. الطرق الشائعة الاستخدام
3.11. تقنيات وأدوات الذكاء
1.3.11.استخبارات المصادر المفتوحة
2.3.11.ذكاء وسائل التواصل الاجتماعي
3.3.11.الاستخبارات البشرية
4.3.11.توزيعات وأدوات لينكس
5.3.11.منهجية تقييم الأمن اللاسلكى المفتوح
6.3.11.مشروع أمان تطبيق الويب المفتوح
7.3.11.معيار أداء اختبار الاختراق PTES
8.3.11.دليل منهجية اختبار الأمان مفتوح المصدر OSSTM
4.11. منهجيات التقييم
1.4.11.تحليل الذكاء
2.4.11.تقنيات تنظيم المعلومات المكتسبة
3.4.11.الموثوقية والمصداقية في مصادر المعلومات
4.4.11.منهجيات التحليل
5.4.11.عرض نتائج الذكاء
5.11. التدقيق والتوثيق
1.5.11.التدقيق فى أمن تكنولوجيا المعلومات
2.5.11.التوثيق والتصاريح للمراجعة
3.5.11.أنواع التدقيق
4.5.11.الإنجازات
1.4.5.11. تقرير تقني
2.4.5.11. البيان التنفيذي

6.11. عدم الكشف عن الهوية على الشبكة
1.6.11.استخدام عدم الكشف عن الهوية
2.6.11.تقنيات إخفاء الهوية (Proxy، VPN)، الشبكة الخصوصية الافتراضية)
3.6.11.شبكات TOR، مشروع الانترنت المخفية 2IP وFreenet
7.11. التهديدات وأنواع الأمن
1.7.11.أنواع التهديدات
2.7.11.الأمن المادي
3.7.11.الامن في الشبكات
4.7.11.الأمن المنطقي
5.7.11.الأمان في تطبيقات الويب
6.7.11.الأمن على الأجهزة المحمولة
8.11. اللوائح والامتثال compliance
1.8.11.النظام الأوروبي العام لحماية البيانات
2.8.11.الإستراتيجية الوطنية للأمن الإلكترونى 1920
3.8.11.مجموعة من المعايير الدولية لأمن المعلومات ISO 00072
4.8.11.إطار عمل الأمن الإلكترونى من المعهد الوطني للمعايير والتكنولوجيا
5.8.11.بك (متحكم دقيق)
6.8.11.CUGBP Elav-like family member 23072
7.8.11.اللوائح cloud
8.8.11.SOX
9.8.11.PCI
9.11. تحليل المخاطر والمعايير
1.9.11.مدى المخاطر
2.9.11.الأصول
3.9.11.التهديدات
4.9.11.نقاط الضعف
5.9.11.تقييم المخاطر
6.9.11.علاج المخاطر
10.11. منظمات مهمة في مجال الأمن السيبراني
1.10.11. إطار الأمن السيبرانيNIST
2.10.11. وكالة الاتحاد الأوروبي للأمن السيبراني
3.10.11. المعهد الوطني للأمن الإلكترونى
4.10.11. منظمة الدول الأمريكية
5.10.11. UNASUR - PROSUR

الوحدة 12. أمن host

1.12. نسخ احتياطية
1.1.12.استراتيجيات النسخ الاحتياطية
2.1.12.أدوات ويندوز
3.1.12.أدوات لنظام Linux
4.1.12.أدوات لنظام MacOS
2.12. برنامج مكافحة الفيروسات للمستخدم
1.2.12.أنواع مضادات الفيروسات
2.2.12.مضاد فيروسات Windows
3.2.12.مضاد فيروسات Linux
4.2.12.مضاد فيروسات لنظام MacOS
5.2.12.مضاد فيروسات للهواتف الذكية smartphones
3.12. أجهزة كشف التسلل - HIDS
1.3.12.طرق كشف التسلل
2.3.12.Sagan
3.3.12.Aide
4.3.12.Rkhunter
4.12. المحلى Firewall
1.4.12.جدار الحماية لنظام التشغيل Windows
2.4.12.جدران الحماية لنظام Linux
3.4.12.جدران الحماية لنظام macOS
5.12. مديرى كلمات المرور
1.5.12.Password
2.5.12.LastPass
3.5.12.KeePass
4.5.12.StickyPassword
5.5.12.RoboForm
6.12. أجهزة كشف التصيد phishing
1.6.12.الكشف اليدوي عن التصيد 1
2.6.12.أدوات antiphishing
7.12. Spyware
1.7.12.آليات التجنب
2.7.12.أدوات مكافحة برامج التجسس antispyware

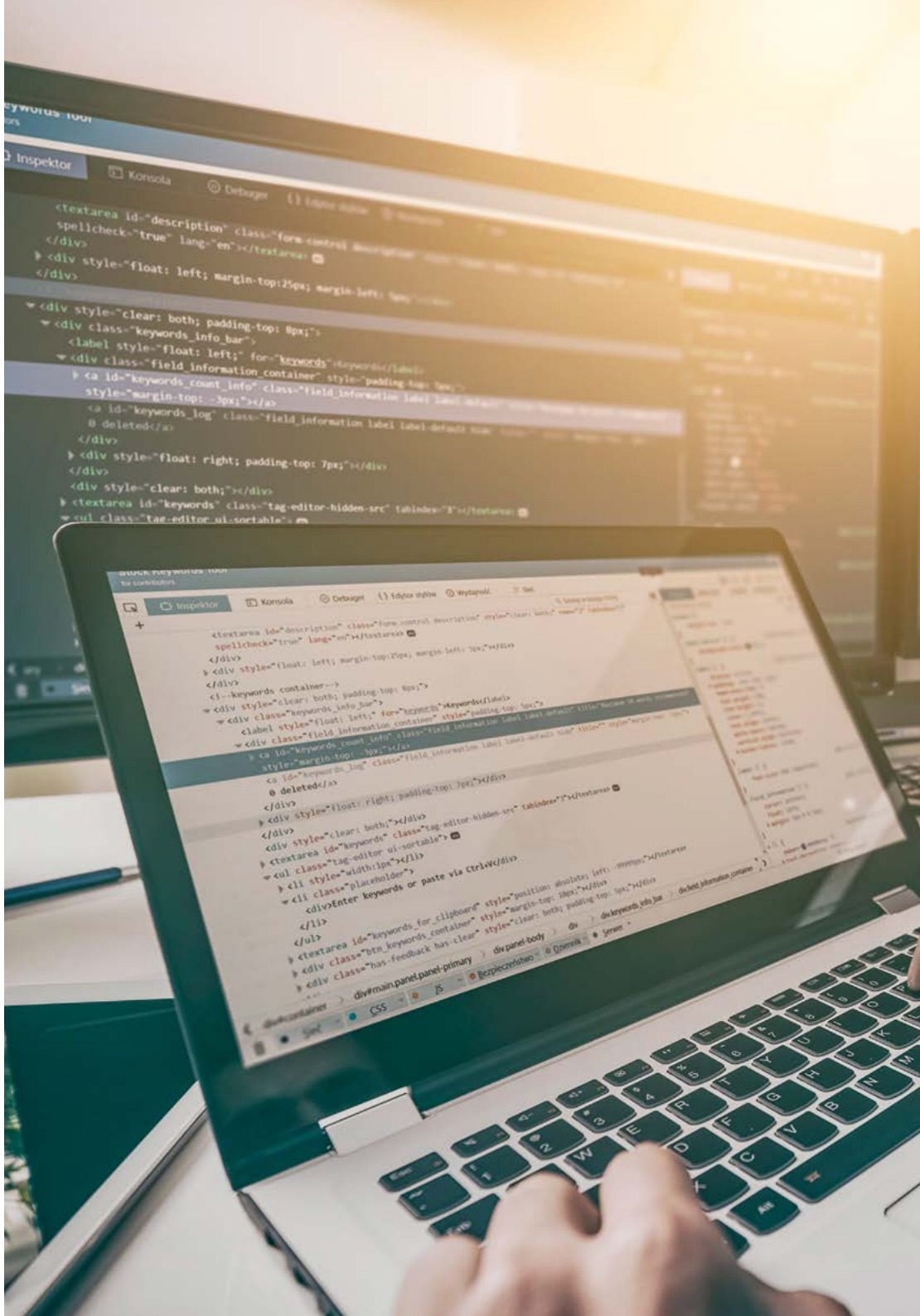


8.12. أجهزة التتبع
1.8.12.تدابير لحماية النظام
2.8.12.أدوات مكافحة التتبع
9.12. EDR- End Point Detection and Response
1.9.12.سلوك نظام EDR
2.9.12.الاختلافات بين كشف نقطة النهاية والاستجابة لها ومكافحة الفيروسات
3.9.12.مستقبل أنظمة كشف نقطة النهاية والاستجابة لها
10.12. السيطرة على تثبيت البرنامج
1.10.12. المستودعات ومحلات البرمجيات
2.10.12. قوائم البرامج المسموح بها أو المحظورة
3.10.12. معايير التحديث
4.10.12. امتيازات تثبيت البرامج

الوحدة 13. أمان الشبكة (المحيط)

1.13. أنظمة الكشف عن التهديدات والوقاية منها
1.1.13.الإطار العام للحوادث الأمنية
2.1.13.أنظمة الدفاع الحالية: Defense in Depthومركز العمليات الأمنية
3.1.13.معماريات الشبكات الحالية
4.1.13.أنواع أدوات الكشف والوقاية من الحوادث
1.4.1.13. أنظمة قائمة على شبكات
2.4.1.13. أنظمة قائمة على المضيف
3.4.1.13. أنظمة مركزية
5.1.13.الاتصال واكتشاف الحالات/المضيفين والحاويات واللاسيرفرات serverless
2.13. Firewall
1.2.13.أنواع firewalls
2.2.13.الهجمات والتخفيف من آثارها
3.2.13.Firewalls الشائعة فى kernel Linux
1.3.2.13. UFW
2.3.2.13. iptables و Nftables
3.3.2.13. Firewalld
4.2.13.أنظمة الكشف على أساس سجلات النظام
1.4.2.13. أغلفة بروتوكول التحكم بالنقل TCP Wrappers
2.4.2.13. BlockHosts وdenyHosts
3.4.2.13. ban2Fai

3.13. أنظمة كشف التسلل والوقاية منه
1.3.13.الهجمات على أنظمة كشف التسلل وأنظمة الوقاية منه
2.3.13.أنظمة كشف التسلل وأنظمة الوقاية منه
1.2.3.13. نظام كشف التسلل الأكثر شعبية
2.2.3.13. موتور كشف ومنع التسلل
4.13. الجيل القادم من جدران الحماية (NGFW)
1.4.13.الاختلافات بين NGFW وجدار الحماية التقليدي
2.4.13.القدرات الأساسية
3.4.13.حلول الأعمال
4.4.13.Firewalls للخدمات Cloud
1.4.4.13. Arquitectura Cloud سحابة أمازون الافتراضية الخاصة
2.4.4.13. سحابة ACLs
3.4.4.13. Security Group
5.13. Proxy
1.5.13.أنواع Proxy
2.5.13.استخدام Proxy. المميزات والعيوب
6.13. محركات مكافحة الفيروسات
1.6.13.السياق العام للبرامج الضارة وبطاقات e
2.6.13.مشاكل محرك مكافحة الفيروسات
7.13. أنظمة حماية البريد
1.7.13.مكافحة البريد الغير مرغوب فيه Antispam
1.1.7.13. القوائم السوداء والبيضاء
2.1.7.13. مرشحات بايزي
2.7.13.(Mail Gateway (MGW
8.13. المعلومات الأمنية وإدارة الأحداث
1.8.13.المكونات والعمارة
2.8.13.قواعد الارتباط وحالات الاستخدام
3.8.13.التحديات الحالية للمعلومات الأمنية وإدارة الأحداث
9.13. التنسيق الأمني والأتمتة والاستجابة
1.9.13.SOAR و SIEM: أعداء أو حلفاء
2.9.13.مستقبل أنظمة التنسيق الأمني والأتمتة والاستجابة



10.13. نظم أخرى قائمة في الشبكات
1.10.13. جدار الحماية لتطبيقات الويب
2.10.13. التحكم في الوصول إلى الشبكة
3.10.13. HoneyPots و HoneyNets
4.10.13. وسيط أمان الوصول إلى السحابة

الوحدة 14. أمن الهواتف الذكية smartphones

1.14. عالم الأجهزة النقالة
1.1.14. أنواع المنصات المحمولة
2.1.14. أجهزة iOS
3.1.14. أجهزة Android
2.14. إدارة أمن الأجهزة المحمولة
1.2.14. مشروع OWASP للأمان على الأجهزة المحمولة
1.1.2.14. أهم 10 نقاط ضعف
2.2.14. الاتصالات والشبكات وأنماط الاتصال
3.14. الجهاز المحمول في بيئة الأعمال
1.3.14. المخاطر
2.3.14. سياسات الأمن
3.3.14. مراقبة الاجهزة
4.3.14. إدارة البيانات الرئيسية (MDM)
4.14. خصوصية المستخدم وأمن البيانات
1.4.14. حالة المعلومات
2.4.14. حماية البيانات والسرية
1.2.4.14. أذونات
2.2.4.14. التشفير
3.4.14. تخزين البيانات بشكل آمن
1.3.4.14. تخزين آمن في iOS
2.3.4.14. تخزين آمن في Android
4.4.14. الممارسات الجيدة في تطوير التطبيقات
5.14. نقاط الضعف ونواقل الهجوم
1.5.14. نقاط الضعف
2.5.14. نواقل الهجوم
1.2.5.14. البرمجيات الخبيثة
2.2.5.14. استخراج البيانات
3.2.5.14. التلاعب بالبيانات

6.14. التهديدات الرئيسية
1.6.14. مستخدم غير مجبر
2.6.14. البرمجيات الخبيثة
1.2.6.14. أنواع البرمجيات الخبيثة
3.6.14. الهندسة الاجتماعية
4.6.14. تسرب البيانات
5.6.14. سرقة المعلومات
6.6.14. شبكات لاسلكية wi-fi غير آمنة
7.6.14. برامج غير محدثة
8.6.14. تطبيقات خبيثة
9.6.14. كلمات مرور ضعيفة
10.6.14. إعدادات أمان ضعيفة أو غير موجودة
11.6.14. الوصول المادي
12.6.14. فقدان أو سرقة الجهاز
13.6.14. انتحال الهوية (النزاهة)
14.6.14. تشفير ضعيف أو مكسور
15.6.14. رفض الخدمة
7.14. الهجمات الرئيسية
1.7.14. هجمات phishing
2.7.14. الهجمات المتعلقة بأساليب الاتصال
3.7.14. هجمات تحطيم Smishing
4.7.14. هجمات Criptojacking
5.7.14. Man in The Middle
8.14. القرصنة Hacking
1.8.14. Rooting و Jailbreaking
2.8.14. تشريح هجوم محمول
1.2.8.14. انتشار التهديد
2.2.8.14. تركيب البرمجيات الخبيثة على الجهاز
3.2.8.14. المثابرة
4.2.8.14. تنفيذ الحمولة واستخراج المعلومات
3.8.14. Hacking على أجهزة iOS: الآليات والأدوات
4.8.14. Hacking على أجهزة Android: الآليات والأدوات

9.14. اختبارات الاختراق
1.9.14. iOS PenTesting
2.9.14. Android pentesting
3.9.14. الأدوات
10.14. الحماية والأمن
1.10.14. اعدادات الامان
1.1.10.14. في أجهزة iOS
2.1.10.14. في أجهزة أندرويد
2.10.14. إجراءات السلامة
3.10.14. أدوات الحماية

الوحدة 15. الأمن في إنترنت الأشياء IoT

1.15. الأجهزة
1.1.15. أنواع الأجهزة
2.1.15. هياكل قياسية
1.2.1.15. مشروع الشراكة العالمية
2.2.1.15. المنتدى العالمي لإنترنت الأشياء IoTWF
3.1.15. بروتوكولات التطبيق
4.1.15. تقنيات الاتصال
2.15. أجهزة إنترنت الأشياء. مجالات التطبيق
1.2.15. SmartHome
2.2.15. SmartCity
3.2.15. وسائل النقل
4.2.15. الأجهزة القابلة للارتداء Wearables
5.2.15. قطاع الصحة
6.2.15. إنترنت الأشياء
3.15. بروتوكولات الاتصال
1.3.15. برتوكول MQTT
2.3.15. فتح بروتوكول تحالف المحمول
3.3.15. بروتوكول إدارة أجهزة تحالف الجوال المفتوح OMA-DM
4.3.15. التقرير الفني 960
4.15. SmartHome
1.4.15. أتمتة المنزل
2.4.15. شبكات التواصل
3.4.15. الأجهزة المنزلية
4.4.15. المراقبة والأمن
5.15. SmartCity
1.5.15. الإضاءة
2.5.15. علم الارصاد الجوية
3.5.15. الأمان
6.15. وسائل النقل
1.6.15. موقع
2.6.15. سداد المدفوعات والحصول على الخدمات
3.6.15. الاتصال
7.15. الأجهزة القابلة للارتداء Wearables
1.7.15. ملابس ذكية
2.7.15. مجوهرات ذكية
3.7.15. الساعات الذكية
8.15. قطاع الصحة
1.8.15. مراقبة التمرين/معدل ضربات القلب
2.8.15. مراقبة المرضى وكبار السن
3.8.15. قابل للزرع
4.8.15. الروبوتات الجراحية
9.15. الاتصال
1.9.15. Wi-Fi/Gateway
2.9.15. بلوتوث
3.9.15. الاتصال المدمج
10.15. التأمين
1.10.15. الشبكات المعنية
2.10.15. مدير كلمات المرور
3.10.15. استخدام البروتوكولات المشفرة
4.10.15. نصائح الاستخدام

الوحدة 16. القرصنة الأخلاقية

1.16. بيئة العمل
1.1.16. توزيعات Linux
1.1.1.16. كالي لينكس Kali Linux - Offensive Security
2.1.1.16. Parrot OS
3.1.1.16. نظام تشغيل متعدد الاستخدامات Ubuntu

2.1.16. أنظمة المحاكاة الافتراضية
3.1.16. صندوق الحماية
4.1.16. نشر المختبرات
2.16. المنهجيات
1.2.16. دليل منهجية اختبار الأمان مفتوح المصدر OSSTM
2.2.16. مشروع أمان تطبيقات الويب المفتوحة OWASP
3.2.16. إطار الأمن السيبراني NIST
4.2.16. معيار أداء اختبار الاختراق PTES
5.2.16. إطار عمل مفتوح المصدر للتحليل والاختبار الأمني ISSAF
3.16. بصمات الأقدام Footprinting
1.3.16. الاستخبارات مفتوحة المصدر (OSINT)
2.3.16. البحث عن الخروقات ونقاط الضعف في البيانات
3.3.16. استخدام الأدوات السلبية
4.16. مسح الشبكات
1.4.16. أدوات المسح
1.1.4.16. اختصار مخطط الشبكة
2.1.4.16. مولد حزم مفتوح المصدر
3.1.4.16. أدوات المسح الأخرى
2.4.16. تقنيات المسح
3.4.16. تقنيات النهرب من firewall ونظام كشف التسلل
4.4.16. Banner Grabbing
5.4.16. مخططات الشبكة
5.16. تعداد
1.5.16. تعداد SMTP
2.5.16. تعداد نظام اسم المجال
3.5.16. تعداد بروتوكول إنترنت وسامبا (برنامج)
4.5.16. تعداد بروتوكول الوصول الى الدليل خفيف الوزن
5.5.16. تعداد بروتوكول إدارة الشبكات البسيطة
6.5.16. تقنيات التعداد الأخرى
6.16. فحص الثغرات الأمنية
1.6.16. حلول فحص الثغرات الأمنية
1.1.6.16. Qualys
2.1.6.16. نيساس Nessus
3.1.6.16. إدارة التصحيح وفحص الثغرات الأمنية وتدقيق الشبكة
2.6.16. أنظمة تسجيل نقاط الضعف
1.2.6.16. نظام تسجيل نقاط الضعف المشتركة
2.2.6.16. نقاط الضعف والتعرضات الشائعة
3.2.6.16. قاعدة بيانات الضعف الوطنية
7.16. هجمات الشبكات اللاسلكية
1.7.16. منهجية القرصنة في الشبكات اللاسلكية
1.1.7.16. Wi-Fi Discovery
2.1.7.16. تحليل حركة المرور
3.1.7.16. هجمات aircrack
1.3.1.7.16. هجمات الشبكة العنكبوتية العالمية
2.3.1.7.16. هجمات وصول محمي للشبكات اللاسلكية / الوصول المحمي بتقنية Wi-Fi 2
4.1.7.16. هجمات Evil Twin
5.1.7.16. هجمات إعداد واي فاي المحمي
6.1.7.16. التشويش
2.7.16. أدوات الأمن اللاسلكية
8.16. القرصنة على خوادم الويب
1.8.16. عبر موقع البرمجة
2.8.16. تزوير الطلب عبر المواقع
3.8.16. Session Hijacking
4.8.16. SQLinjection
9.16. استغلال نقاط الضعف
1.9.16. استخدام exploits المعروفة
2.9.16. استخدام metasploit
3.9.16. استخدام malware
1.3.9.16. التعريف والنطاق
2.3.9.16. توليد البرامج الضارة malware
3.3.9.16. تجاوز حلول مكافحة الفيروسات
10.16. المثابرة
1.10.16. تثبيت rootkits
2.10.16. استخدام ncat
3.10.16. استخدام المهام المجدولة للأبواب الخلفية backdoors
4.10.16. إنشاء المستخدم

5.10.16. نظام كشف التسلل القائم على المضيف

الوحدة 17. الهندسة العكسية

1.17. المجمعين
1.1.17.أنواع الأكواد
2.1.17.مراحل مجمع البيانات
3.1.17.جدول الرموز
4.1.17.مدير الأخطاء
5.1.17.مجموعة مترجمات جنو
2.17. أنواع التحليل في المجمعين
1.2.17.تحليل معجمي
1.1.2.17. المصطلحات
2.1.2.17. المكونات المعجمية
3.1.2.17. محلل معجمي القانون الكنسي LEX
2.2.17.التحليل النحوي
1.2.2.17. قواعد نحوية خالية من السياق
2.2.2.17. أنواع التحليل النحوي
1.2.2.2.17. التحليل التنازلي
2.2.2.2.17. التحليل التصاعدي
3.2.2.17. أشجار النحو والاشتقاقات
4.2.2.17. أنواع المحللين النحويين
1.4.2.2.17. محللين مجزئ يسار يمين (Left To Right)
2.4.2.2.17. محللين مجزئ يسار يمين
3.2.17.التحليل الدلالي
1.3.2.17. قواعد السمات
2.3.2.17. القواعد المنسوبة التي تحتوي على السمات المركبة S-atribuidas
3.3.2.17. القواعد المنسوبة التي تحتوي على السمات المركبة L-Atribuidas
3.17. هياكل بيانات المجمّع
1.3.17.المتغيرات
2.3.17.Arrays
3.3.17.المؤشرات
4.3.17.الهياكل
5.3.17.العناصر
4.17. هياكل الكود في المجمع
1.4.17.هياكل الاختيار
1.1.4.17. If، else if، Else
2.1.4.17. Switch
2.4.17.هياكل التكرار
1.2.4.17. For
2.2.4.17. While
3.2.4.17. استخدام break
3.4.17.الدوال
5.17. بنية الأجهزة 68x
1.5.17.بنية المعالج 68x
2.5.17.بنية البيانات في 68x
3.5.17.بنية الكود فى 68x
6.17. بنية الأجهزة ARM
1.6.17.بنية معالج معمارية ARM
2.6.17.بنية بيانات معمارية ARM
3.6.17.بنية الكود في معمارية ARM
7.17. تحليل الشفرة الثابتة
1.7.17.المفككات
2.7.17.المفكك التفاعلي IDA
3.7.17.معيدي بناء الكود
8.17. تحليل الشفرة الديناميكية
1.8.17.تحليل السلوك
1.1.8.17. الاتصالات
2.1.8.17. المراقبة

2.8.17. مصححات كود Linux
3.8.17. مصححات كود Windows
9.17. صندوق الحماية
1.9.17. هندسة صندوق الحماية
2.9.17. التهرب من Sandbox
3.9.17. تقنيات الكشف
4.9.17. تقنيات التهرب
5.9.17. التدابير المضادة
6.9.17. صندوق الحماية في لينكس
7.9.17. صندوق الحماية في ويندوز
8.9.17. صندوق الحماية في MacOS
9.9.17. Sandbox في Android
10.17. تحليل البرامج الضارة
1.10.17. مناهج تحاليل malware
2.10.17. تقنيات تشويش البرمجيات الخبيثة malware
1.2.10.17. التعتيم على الملفات التنفيذية
2.2.10.17. تقييد بيئات التنفيذ
3.10.17. أدوات تحليل البرمجيات الخبيثة

الوحدة 18. التطوير الآمن

1.18. التطوير الآمن
1.1.18. الجودة والوظيفة والسلامة
2.1.18. السرية والنزاهة والتوافر
3.1.18. دورة حياة تطوير البرمجيات
2.18. مرحلة المتطلبات
1.2.18. التحكم في المصادقة
2.2.18. السيطرة على الأدوار والامتيازات
3.2.18. المتطلبات الموجهة للمخاطر
4.2.18. اعتماد الامتيازات
3.18. مرحلة التحليل والتصميم
1.3.18. الوصول إلى المكونات وإدارة النظام
2.3.18. مسارات التدقيق
3.3.18. إدارة الجلسات
4.3.18. بيانات تاريخية
5.3.18. التعامل السليم مع الأخطاء
6.3.18. الفصل بين الوظائف
4.18. مرحلة التنفيذ والتشفير
1.4.18. ضمان البيئة التطويرية
2.4.18. إعداد الوثائق الفنية
3.4.18. تشفير آمن
4.4.18. أمن الاتصالات
5.18. الممارسات الجيدة للتشفير الآمن
1.5.18. التحقق من صحة البيانات المدخلة
2.5.18. تشفير بيانات الإخراج
3.5.18. أسلوب البرمجة
4.5.18. إدارة سجل التغيير
5.5.18. ممارسات التشفير
6.5.18. إدارة الأخطاء والسجلات
7.5.18. إدارة السجلات
8.5.18. إدارة الذاكرة
9.5.18. توحيد وإعادة استخدام وظائف الأمن
6.18. إعداد الخادم وتقويته Hardening
1.6.18. إدارة المستخدمين والمجموعات والأدوار على الخادم
2.6.18. تثبيت البرامج
3.6.18. Hardening الخادم
4.6.18. اعداد قوي لبيئة التطبيق
7.18. إعداد قاعدة البيانات وتقويتها
1.7.18. تحسين محرك قاعدة البيانات
2.7.18. إنشاء مستخدم خاص للتطبيق
3.7.18. تعيين الامتيازات الدقيقة للمستخدم
4.7.18. Hardening قاعدة البيانات
8.18. مرحلة الإختبار
1.8.18. مراقبة الجودة في الضوابط الأمنية

2.8.18. فحص الرمز على مراحل
3.8.18. التحقق من إدارة التهيئة
4.8.18. اختبار الصندوق الأسود
9.18. تحضير خطوة الإنتاج
1.9.18. مراقبة التغيير
2.9.18. تنفيذ إجراء خطوة إلى الإنتاج
3.9.18. تنفيذ إجراء rollback
4.9.18. الاختبارات في مرحلة ما قبل الإنتاج
10.18. مرحلة الصيانة
1.10.18. التأمين على أساس المخاطر
2.10.18. اختبارات صيانة سلامة الصندوق الأبيض
3.10.18. اختبارات صيانة سلامة الصندوق الاسود

الوحدة 19. التحليل الجنائي

1.19. الحصول على البيانات ونسخها
1.1.19. الحصول على البيانات المتقلبة
1.1.1.19. معلومات النظام
2.1.1.19. معلومات الشبكة
3.1.1.19. ترتيب التقلب
2.1.19. الحصول على البيانات الثابتة
1.2.1.19. إنشاء صورة منسوخة
2.2.1.19. إعداد وثيقة لسلسلة الحيازة
3.1.19. طرق التحقق من صحة البيانات المكتسبة
1.3.1.19. منهجيات Linux
2.3.1.19. منهجيات Windows
2.19. تقييم وهزيمة تقنيات مكافحة الأدلة الجنائية
1.2.19. أهداف التقنيات امكافحة الأدلة الجنائية
2.2.19. مسح البيانات
1.2.2.19. حذف البيانات والملفات
2.2.2.19. استرجاع الملفات
3.2.2.19. استرجاع الأقسام المحذوفة
3.2.19. الحماية بكلمة مرور
4.2.19. إخفاء المعلومات
5.2.19. الحذف الآمن للأجهزة
6.2.19. التشفير
3.19. التحليل الجنائي لنظام التشغيل
1.3.19. التحليل الجنائي لنظام Windows
2.3.19. التحليل الجنائي لنظام Windows
3.3.19. التحليل الجنائي لنظام Mac
4.19. التحليل الجنائي للشبكة
1.4.19. تحليل السجلات
2.4.19. ترابط البيانات
3.4.19. بحث الشبكة
4.4.19. الخطوات الواجب اتباعها في التحليل الجنائي للشبكة
5.19. التحليل الجنائي للويب
1.5.19. التحقيق في هجمات الويب
2.5.19. كشف الهجمات
3.5.19. تعقب عناوين نظام منع الاختراق IPs
6.19. التحليل الجنائي لقواعد البيانات
1.6.19. التحليل الجنائي لبرنامج قواعد البيانات العلائقية MSSQL
2.6.19. التحليل الجنائي نظام إدارة قواعد البيانات MySQL
3.6.19. التحليل الجنائي في نظام إدارة قواعد البيانات PostgreSQL
4.6.19. التحليل الجنائي في نظام قاعدة بيانات مفتوحة المصدر MongoDB
7.19. التحليل الجنائي في Cloud
1.7.19. أنواع الجرائم فى Cloud
1.1.7.19. السحابة كمشتبه
2.1.7.19. السحابة كغرض
3.1.7.19. السحابة كأداة
2.7.19. تحديات التحليل الجنائى فى Cloud
3.7.19. التحقيق فى خدمات التخزين Cloud
4.7.19. أدوات الادلة الجنائية Cloud
8.19. التحقيق في جرائم البريد الإلكتروني
1.8.19. أنظمة البريد
1.1.8.19. عملاء البريد

2.1.8.19. خادم البريد
3.1.8.19. خادم البريد الصادر SMTP
4.1.8.19. خادم روتوكول الوصول إلى رسائل الإنترنت
5.1.8.19. خادم روتوكول الوصول إلى رسائل الإنترنت
2.8.19.جرائم البريد
3.8.19.رسالة بريدية
1.3.8.19. رؤوس قياسية
2.3.8.19. رؤوس ممتدة
4.8.19.خطوات التحقيق في هذه الجرائم
5.8.19.أدوات جنائية للبريد الإلكتروني
9.19. التحليل الجنائي للهواتف المحمولة
1.9.19.شبكات خلوية
1.1.9.19. أنواع الشبكات
2.1.9.19. محتويات إثبات الاستلام CDR
2.9.19.وحدة تعريف المشترك (SIM)
3.9.19.الاستحواذ المنطقي
4.9.19.الاستحواذ المادي
5.9.19.اكتساب نظام الملفات
10.19. صياغة تقارير التحليل الجنائي وتقديمها
1.10.19. الجوانب الهامة لتقرير التحليل الجنائي
2.10.19. تصنيف وأنواع التقارير
3.10.19. دليل لكتابة التقرير
4.10.19. عرض التقرير
1.4.10.19. التحضير المسبق للإدلاء بشهادة
2.4.10.19. شهادة
3.4.10.19. التعامل مع الوسائط

الوحدة 20. التحديات الحالية والمستقبلية في أمن الحاسوب

1.20. تكنولوجيا بلوكشين blockchain
1.1.20.مجالات التطبيق
2.1.20.ضمان السرية
3.1.20.ضمان عدم التنصل
2.20. النقود الرقمية
1.2.20.عملات البيتكوين
2.2.20.العملات الرقمية
3.2.20.تعدين العملات المشفرة
4.2.20.عمليات احتيال الهرمي
5.2.20.الجرائم والمشاكل المحتملة الأخرى
3.20. Deepfake
1.3.20.تأثير الوسائط
2.3.20.مخاطر على المجتمع
3.3.20.آليات الكشف
4.20. مستقبل الذكاء الاصطناعي
1.4.20.الذكاء الاصطناعي والحوسبة المعرفية
2.4.20.استخدامات لتبسيط خدمة العملاء
5.20. الخصوصية الرقمية
1.5.20.قيمة البيانات على الشبكة
2.5.20.استخدام البيانات على الشبكة
3.5.20.إدارة الخصوصية والهوية الرقمية
6.20. النزاعات السيبرانية ومجرمين الإنترنت والهجمات الإلكترونية
1.6.20.تأثير الأمن السيبراني في النزاعات الدولية
2.6.20.عواقب الهجمات السيبراني على عموم السكان
3.6.20.أنواع مجرمي الإنترنت. إجراءات الحماية

7.20. العمل عن بعد
1.7.20.ثورة العمل عن بعد أثناء وبعد كوفيد-19
2.7.20.اختناقات الوصول
3.7.20.تباين سطح الهجوم
4.7.20.احتياجات العمال
8.20. التقنيات اللاسلكية الناشئة
1.8.20.الوصول إلى شبكة Wi-Fi المحمية 3
2.8.20.شبكة الجيل الخامس
3.8.20.موجات مليمترية
4.8.20.الاتجاه إلى Get Smart بدلا من Get more
9.20. عنونة المستقبل في الشبكات
1.9.20.المشاكل الحالية مع عنونة نظام منع الاختراق
2.9.20.الإصدار السادس من بروتوكول الإنترنت
3.9.20.الإصدار الرابع من بروتوكول الإنترنت IPv4+
4.9.20.مميزات الإصدار السادس من بروتوكول الإنترنت + الإصدار الرابع من بروتوكول الإنترنت
5.9.20.مميزات الإصدار السادس من بروتوكول الإنترنت IPv6 عن الإصدار الرابع من بروتوكول الإنترنت
10.20. التحدي المتمثل في زيادة الوعي بالتعليم المبكر والمستمر للسكان
1.10.20. الاستراتيجيات الحالية للحكومات
2.10.20. مقاومة السكان للتعلم
3.10.20. خطط التدريب التي يجب أن تتبناها الشركات

"سوف تتعلم من خلال حالات واقعية مصممة في بيئات محاكاة تعليمية تعكس التحديات الحالية في تسيير البيانات والأمن السيبراني"

04

أهداف التدريس

الهدف الرئيسي من الماجيستير المتقدم في إدارة المعلومات الآمنة (Secure Information Management) هو تزويد الطلاب بمعرفة متقدمة في مجالين أساسيين ومتكاملين في علوم الكمبيوتر والهندسة: إدارة البيانات في البيئات الرقمية والأمن السيبراني. يجمع هذا البرنامج بين التخصصين لتمكين المهنيين من تنفيذ حلول متقدمة، مما يسمح لهم بمواجهة التحديات الوظيفية بالأدوات اللازمة لإدارة وحماية المعلومات الحساسة في مؤسساتهم.

"حوّل مسارك المهني مع هذا الماجيستير المتقدم المبتكر، المصمم ليكون نقطة تحول في تخصصك في إدارة البيانات والأمن السيبراني"

الأهداف العامة

- تطوير معرفة متقدمة في تحليل البيانات والأمن السيبراني لتحسين العمليات التجارية باستخدام أدوات وتقنيات مبتكرة
- تنفيذ استراتيجيات أمان فعالة لمنع التهديدات الرقمية في الأنظمة والشبكات والأجهزة المحمولة
- حل التحديات في الأمن السيبراني من خلال عمليات التدقيق والهندسة العكسية والتحليل الجنائي المستند إلى الأدلة
- التنبؤ بالاتجاهات التكنولوجية وتطبيق حلول مبتكرة لحماية الأصول الرقمية والأنظمة المتقدمة

"قم بقيادة إدارة البيانات والأمن السيبراني في البيئة الرقمية من خلال هذا البرنامج المتخصص"

الأهداف المحددة

الوحدة 1. تحليل البيانات في المؤسسة

- تطوير المهارات في استخدام تقنيات تحليل البيانات
- إنتاج معلومات قيّمة لتعزيز اتخاذ القرارات الاستراتيجية داخل المؤسسات، مما يحسن الكفاءة والقدرة التنافسية

الوحدة 2. إدارة البيانات ومعالجتها لعلوم البيانات

- تمكين الطلاب من إدارة كميات كبيرة من البيانات بكفاءة
- تطبيق منهجيات وأدوات لتنظيم وتنظيف وتحويل البيانات إلى معلومات مفيدة لمشاريع علوم البيانات

الوحدة 3. الأجهزة والمنصات الذكية IoT كأساس لعلوم البيانات

- تقديم المعرفة اللازمة حول المنصات والأجهزة الذكية وتكاملها في علوم البيانات
- التعمق في التقاط البيانات ومعالجتها وتحليلها في الوقت الفعلي

الوحدة 4. التمثيل البياني لتحليل البيانات

- استخدام الأدوات والتقنيات المتقدمة لعرض البيانات بشكل مرئي
- تسهيل فهم الأنماط والاتجاهات والعلاقات داخل مجموعات البيانات الكبيرة

الوحدة 5. أدوات علوم البيانات

- تمكين الطلاب من استخدام الأدوات والبرامج المتخصصة في علوم البيانات، مثل Python
- التعمق في جمع البيانات وتحليلها وعرضها في سياقات مهنية متنوعة

الوحدة 6. استخراج البيانات الاختيار والمعالجة الأولية والتحويل

- تزويد الطلاب بالمعرفة والمهارات اللازمة لتطبيق تقنيات التنقيب عن البيانات
- تحليل الاختيار والمعالجة الأولية وتحويل البيانات لاستخراج الأنماط والاتجاهات المهمة

الوحدة 7. التنبؤ وتحليل الظواهر العشوائية

- تطوير مهارات في نمذجة وتحليل الظواهر العشوائية
- استخدام طرق إحصائية متقدمة للتنبؤ بالسلوكيات والاتجاهات في بيئات غير مؤكدة وديناميكية

الوحدة 8. تصميم وتطوير الأنظمة الذكية

- تدريب الطلاب على تصميم وتطوير الأنظمة الذكية باستخدام تقنيات التعلم الآلي والذكاء الاصطناعي
- إنشاء حلول تلقائية لحل المشكلات المعقدة بكفاءة

الوحدة 9. البنى وأنظمة الاستخدام المكثف للمعلومات في علوم البيانات

- تقديم المعرفة حول إنشاء بنى تحتية للأنظمة القادرة على معالجة كميات هائلة من البيانات بكفاءة
- استخدام تقنيات متقدمة مثل قواعد البيانات الموزعة والمعالجة المتوازية

الوحدة 10. التطبيق العملي لعلوم البيانات في قطاعات النشاط التجاري

- تطوير القدرة على تطبيق ممارسات علوم البيانات في قطاعات الأعمال المختلفة
- دمج المعرفة المكتسبة لتحسين اتخاذ القرار، وتحسين العمليات، وتعزيز الابتكار داخل المؤسسة

الوحدة 11. الاستخبارات السيبرانية والأمن السيبراني

- تزويد الطلاب بالمعرفة والمهارات اللازمة لتطبيق تقنيات الاستخبارات السيبرانية والأمن السيبراني
- حماية الأنظمة والشبكات من التهديدات السيبرانية وضمان سلامة البيانات

الوحدة 12. أمان Host

- تدريب الطلاب على تنفيذ تدابير أمان فعالة في أنظمة المضيف
- ضمان حماية الخوادم والتطبيقات الحساسة من خلال استخدام الأدوات وأفضل ممارسات الأمن المعلوماتي

الوحدة 13. أمن الشبكات (الحماية الطرفية)

- تقديم المعرفة حول حماية الشبكات وأنظمة المعلومات على المستوى الطرفي
- إدارة الجدران النارية (Firewalls) والشبكات الخاصة الافتراضية (VPNs) وأدوات أخرى لضمان أمن البنية التحتية للشبكة

الوحدة 14. أمن الهواتف الذكية smartphones

- تطوير المهارات اللازمة لضمان أمان الأجهزة المحمولة
- فهم الثغرات الأمنية الشائعة وتطبيق التدابير الوقائية لحماية المعلومات والتطبيقات على الهواتف الذكية

الوحدة 15. الأمن في إنترنت الأشياء IoT

- تقديم المعرفة اللازمة لتنفيذ حلول أمان للأجهزة الذكية المتصلة بالإنترنت
- حماية الشبكات والأنظمة التي تربط بين الأجهزة وضمان سرية البيانات وسلامتها

الوحدة 16. أخلاقيات Hacking

- تدريب الطلاب على ممارسات الاختراق الأخلاقي وإجراء اختبارات الاختراق (Penetration Testing)
- تحديد الثغرات الأمنية في الأنظمة لتحسين الأمن قبل أن يستغلها المهاجمون

الوحدة 17. الهندسة العكسية

- تقديم المعرفة حول تقنيات الهندسة العكسية، مما يسمح بتحليل وفهم تشغيل البرمجيات والأجهزة
- اكتشاف العيوب الأمنية أو تحسين وظائف الأنظمة القائمة

الوحدة 18. التطوير الآمن

- تدريب الطلاب على تطوير البرمجيات الآمنة من خلال أفضل ممارسات التشفير والأمن خلال دورة حياة البرمجيات
- القدرة على منع الثغرات الأمنية وحماية الأنظمة من الهجمات

الوحدة 19. التحليل الجنائي

- تطوير المهارات اللازمة لإجراء التحقيقات الجنائية الرقمية
- استخدام أدوات وتقنيات متقدمة لاستعادة وتحليل وحفظ الأدلة الإلكترونية في حوادث الأمن المعلوماتي

الوحدة 20. التحديات الحالية والمستقبلية في أمن الحاسوب

- استكشاف التحديات الحالية والمستقبلية في مجال الأمن السيبراني من خلال تحليل التهديدات الناشئة والتقنيات الجديدة للحماية
- التعمق في استراتيجيات تقليل المخاطر في بيئة تقنية دائمة التغير

05

الآفاق المهنية

بعد إكمال برنامج الماجيستير المتقدم في إدارة المعلومات الآمنة (Secure Information Management)، سيكتسب المتخصصون فهماً راسخًا لأحدث الاستراتيجيات في الأمن السيبراني وإدارة البيانات الرقمية. سيكون الخريجون مستعدين لتصميم وتنفيذ حلول تضمن حماية المعلومات الحساسة وتحسن عمليات التحليل واتخاذ القرار في البيئات التجارية. وبذلك، سيعززون آفاقهم المهنية ويتقلدون أدوارًا متخصصة مثل محللي الأمن السيبراني، ومستشاري الاستخبارات، ومديري البيانات الحرجة.

"ستضمن أمان الأصول الرقمية وستكون عنصرًا أساسيًا في التحول الرقمي للمؤسسات"

ملامح الخريج

سيكون خريج برنامج الماجيستير المتقدم في إدارة المعلومات الآمنة (Secure Information Management) محترفًا عالي الكفاءة في إدارة وحماية المعلومات في البيئات الرقمية.

سيتمتع بمعرفة متقدمة في مجالات مثل الأمن السيبراني، والاستخبارات الرقمية، وتحليل البيانات، إلى جانب مهارات عملية في تصميم وتنفيذ استراتيجيات الدفاع ضد التهديدات.

يجمع ملفه الشخصي بين فهم تقني عميق وكفاءات استراتيجية تمكّنه من قيادة المشاريع في القطاعات التجارية الرئيسية.

> ستصبح قائدًا في مجال حماية البيانات والأمن السيبراني، حيث ستتعاون مع الشركات لمواجهة تحديات البيئة الرقمية.

- **إدارة الأمن:** تنمية القدرة على تحديد المخاطر وتنفيذ استراتيجيات دفاع متعددة الطبقات وضمان سرية البيانات وسلامتها وتوافرها.
- **التحليل النقدي وحل المشكلات:** تطبيق تقنيات متقدمة لتقييم الأنظمة، واكتشاف الثغرات الأمنية، وتصميم حلول تتكيف مع البيئات التكنولوجية المختلفة.
- **الكفاءة التقنية والرقمية:** إتقان الأدوات المتقدمة في تحليل البيانات والأمن السيبراني وأنظمة الاستخبارات، مما يتيح لك قيادة مشاريع الابتكار التكنولوجي.
- **التفكير الاستراتيجي:** تصميم سياسات أمنية واستراتيجيات تجارية تتماشى مع متطلبات البيئة الرقمية الحالية والمستقبلية.
- **التعاون بين التخصصات:** العمل مع فرق متعددة التخصصات لمواجهة التحديات المعقدة وضمان الأمن في الشبكات ومنصات إنترنت الأشياء والأجهزة المحمولة.

بعد إكمال هذا البرنامج، ستكون مؤهلًا لشغل الوظائف التالية:

1. **مدير الأمن السيبراني:** قيادة فرق الأمن السيبراني وتصميم استراتيجيات لحماية الأصول الرقمية في المؤسسات الكبرى.
2. **محلل بيانات:** تصميم تحليلات تنبؤية وأنظمة تصور البيانات لتعزيز اتخاذ القرارات الاستراتيجية.
3. **مستشار استخبارات رقمية:** خبير استشاري يقدم حلولاً متقدمة تعتمد على الذكاء الاصطناعي وتحليل المخاطر.
4. **متخصص في إنترنت الأشياء والأمن:** تصميم تدابير حماية للأجهزة المتصلة والبيئات الصناعية.
5. **هاكر أخلاقي:** تقييم الثغرات الأمنية في الأنظمة وتصحيحها لمنع الهجمات السيبرانية.
6. **مدقق أمن المعلومات:** إجراء عمليات التدقيق والتحليل الجنائي لضمان الامتثال للمعايير الأمنية.
7. **مدير بيانات الأعمال:** مسؤول عن تصميم وإدارة أنظمة تخزين وتحليل البيانات لتعزيز الكفاءة التشغيلية.

"أكمل هذا البرنامج وكن متخصصًا في أكثر المجالات طلبًا في البيئة الرقمية"

00

منهجية الدراسة

TECH هي أول جامعة في العالم تجمع بين منهجيةدراسات الحالة مع التعلم المتجدد، وهو نظام تعلم 100% عبر الإنترنت قائم، قائم على التكرار الموجهتم تصميم هذه الاستراتيجية التربوية المبتكرة لتوفير الفرصة للمهنيين لتحديث معارفهم وتطوير مهاراتهم بطريقة مكثفة ودقيقة. نموذج تعلُّم يضع الطالب في مركز العملية الأكاديمية ويمنحه كل الأهمية، متكيّفًا مع احتياجاته ومتخليًا عن المناهج الأكثر تقليدية

"TECH تُعدُّك لمواجهة تحديات جديدة في بيئات غير مؤكدة
وتحقيق النجاح في مسيرتك المهنية"

الطالب: الأولوية في جميع برامج TECH

في منهجية الدراسة في TECH، يعتبر الطالب البطل المطلق.

تم اختيار الأدوات التربوية لكل برنامج مع مراعاة متطلبات الوقت والتوافر والدقة الأكاديمية التي، في الوقت الحاضر، لا يطلبها الطلاب فحسب، بل أيضًا أكثر المناصب تنافسية في السوق

مع نموذج TECH التعليمي غير المتزامن، يكون الطالب هو من يختار الوقت الذي يخصصه للدراسة، وكيف يقرر تنظيم روتينه، و كل ذلك من الجهاز الإلكتروني المفضّل لديه. لن يحتاج الطالب إلى حضور دروس مباشرة، والتي غالبًا ما لا يستطيع حضورها. سيقوم بأنشطة التعلم عندما يناسبه ذلك سيستطيع دائمًا تحديد متى وأين يدرس

"في TECH لن تكون لديك دروس مباشرة (والتي لا يمكنك حضورها أبدًا لاحقًا)"

المناهج الدراسية الأكثر شمولاً على مستوى العالم

تتميز TECH بتقديم أكثر المسارات الأكاديمية اكتمالاً في المحيط الجامعي. يتم تحقيق هذه الشمولية من خلال إنشاء مناهج لا تغطي فقط المعارف الأساسية، بل تشمل أيضًا أحدث الابتكارات في كل مجال.

من خلال التحديث المستمر، تتيح هذه البرامج للطلاب البقاء على اطلاع دائم على تغييرات السوق واكتساب المهارات الأكثر قيمة لدى أصحاب العمل. وبهذه الطريقة، يحصل الذين ينهون دراساتهم في TECH الجامعة التكنولوجية على إعداد شامل يمنحهم ميزة تنافسية ملحوظة للتقدم في مساراتهم المهنية.

وبالإضافة إلى ذلك، سيتمكنون من القيام بذلك من أي جهاز، سواء كان حاسوبًا شخصيًا، أو جهازًا لوحيًا، أو هاتفًا ذكيًا.

"نموذج TECH الجامعة التكنولوجية غير متزامن، مما يسمح لك بالدراسة باستخدام حاسوبك الشخصي، أو جهازك اللوحي، أو هاتفك الذكي أينما شئت، ومتى شئت، وللمدة التي تريدها"

Case studies أو دراسات الحالة

كانت طريقة الحالة هي نظام التعلم الأكثر استخداماً من قبل أفضل الكليات في العالم. قد كان منهج الحالة النظام التعليمي الأكثر استخدامًا من قبل أفضل كليات الأعمال في العالم. تم تطويره في عام 1219 لكي لا يتعلم طلاب القانون القوانين فقط على أساس المحتوى النظري، بل كان دوره أيضًا تقديم مواقف حقيقية معقدة لهم. وهكذا، يمكنهم اتخاذ قرارات وإصدار أحكام قيمة مبنية على أسس حول كيفية حلها. في عام 1924 تم تحديد هذه المنهجية كمنهج قياسي للتدريس في جامعة Harvard.

مع هذا النموذج التعليمي، يكون الطالب نفسه هو الذي يبني كفاءته المهنية من خلال استراتيجيات مثل **التعلم بالممارسة** أو التفكير التصميمي، والتي تستخدمها مؤسسات مرموقة أخرى مثل جامعة ييل أو ستانفورد. سيتم تطبيق هذه الطريقة، الموجهة نحو العمل، طوال المسار الأكاديمي الذي سيخوضه الطالب مع TECH الجامعة التكنولوجية.

سيتم تطبيق هذه الطريقة الموجهة نحو العمل على طول المسار الأكاديمي الكامل الذي سيخوضه الطالب مع TECH. وبهذه الطريقة سيواجه مواقف حقيقية متعددة، وعليه دمج المعارف والبحث والمجادلة والدفاع عن أفكاره وقراراته. كل ذلك مع فرضية الإجابة على التساؤل حول كيفية تصرفه عند مواجهته لأحداث معقدة محددة في عمله اليومي.

طريقة Relearning

في TECH، يتم تعزيز دراسات الحالة بأفضل طريقة تدريس عبر الإنترنت بنسبة 100%: **إعادة** التعلم.

هذه الطريقة تكسر الأساليب التقليدية للتدريس لوضع الطالب في مركز المعادلة، وتزويده بأفضل المحتويات في صيغ مختلفة. بهذه الطريقة، يتمكن من مراجعة وتكرار المفاهيم الأساسية لكل مادة وتعلم كيفية تطبيقها في بيئة حقيقية.

وفي هذا السياق، وبناءً على العديد من الأبحاث العلمية، يعتبر التكرار أفضل وسيلة للتعلم. لهذا السبب، تقدم TECH بين 8 و16 تكرارًا لكل مفهوم أساسي داخل نفس الدرس، مقدمة بطرق مختلفة، بهدف ضمان ترسيخ المعرفة تمامًا خلال عملية الدراسة.

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

حرم جامعي افتراضي 100% عبر الإنترنت مع أفضل الموارد التعليمية.

من أجل تطبيق منهجيته بفعالية، يركز برنامج TECH على تزويد الخريجين بمواد تعليمية بأشكال مختلفة: نصوص، وفيديوهات تفاعلية، ورسوم توضيحية وخرائط معرفية وغيرها.
تم تصميمها جميعًا من قبل مدرسين مؤهلين يركزون في عملهم على الجمع بين الحالات الحقيقية وحل المواقف المعقدة من خلال المحاكاة، ودراسة السياقات المطبقة على كل مهنة مهنية والتعلم القائم على التّكرار من خلال الصوتيات والعروض التقديمية والرسوم المتحركة والصور وغيرها.

تشير أحدث الأدلة العلمية في مجال علم الأعصاب إلى أهمية مراعاة المكان والسياق الذي يتم فيه الوصول إلى المحتوى قبل البدء في عملية تعلم جديدة.
إن القدرة على ضبط هذه المتغيرات بطريقة مخصصة تساعد الأشخاص على تذكر المعرفة وتخزينها في الحُصين من أجل الاحتفاظ بها على المدى الطويل.
هذا هو نموذج يسمى التعلم الإلكتروني المعتمد على السياق العصبي المعرفي العصبي، والذي يتم تطبيقه بوعي في هذه الدرجة الجامعية.

من ناحية أخرى، ومن أجل تفضيل الاتصال بين المرشد والمتدرب قدر الإمكان، يتم توفير مجموعة واسعة من إمكانيات الاتصال، سواء في الوقت الحقيقي أو المؤجل (الرسائل الداخلية، ومنتديات المناقشة، وخدمة الهاتف، والاتصال عبر البريد الإلكتروني مع مكتب السكرتير الفني، والدردشة ومؤتمرات الفيديو)

وبالمثل، سيسمح هذا الحرم الجامعي الافتراضي المتكامل للغاية لطلاب TECH بتنظيم جداولهم الدراسية وفقًا لتوافرهم الشخصي أو التزامات العمل.
وبهذه الطريقة، سيتمكنون من التحكم الشامل في المحتويات الأكاديمية وأدواتهم التعليمية، وفقًا لتحديثهم المهني المتسارع.

> ستسمح لك طريقة الدراسة عبر الإنترنت لهذا البرنامج بتنظيم وقتك ووتيرة تعلمك، وتكييفها مع جدولك الزمني"

تُبرر فعالية المنهج بأربعة إنجازات أساسية:

1. الطلاب الذين يتبعون هذا المنهج لا يحققون فقط استيعاب المفاهيم، ولكن أيضاً تنمية قدراتهم العقلية من خلال التمارين التي تقيم المواقف الحقيقية وتقوم بتطبيق المعرفة المكتسبة.

2. يركزمنهج التعلم بقوة على المهارات العملية التي تسمح للطالب بالاندماج بشكل أفضل في العالم الحقيقي.

3. يتم تحقيق استيعاب أبسط وأكثر كفاءة للأفكار والمفاهيم، وذلك بفضل منهج المواقف التي نشأت من الواقع.

4. يصبح الشعور بكفاءة الجهد المستثمر حافزًا مهمًا للغاية للطلاب، مما يترجم إلى اهتمام أكبر بالتعلم وزيادة في الوقت المخصص للعمل في المحاضرة الجامعية.

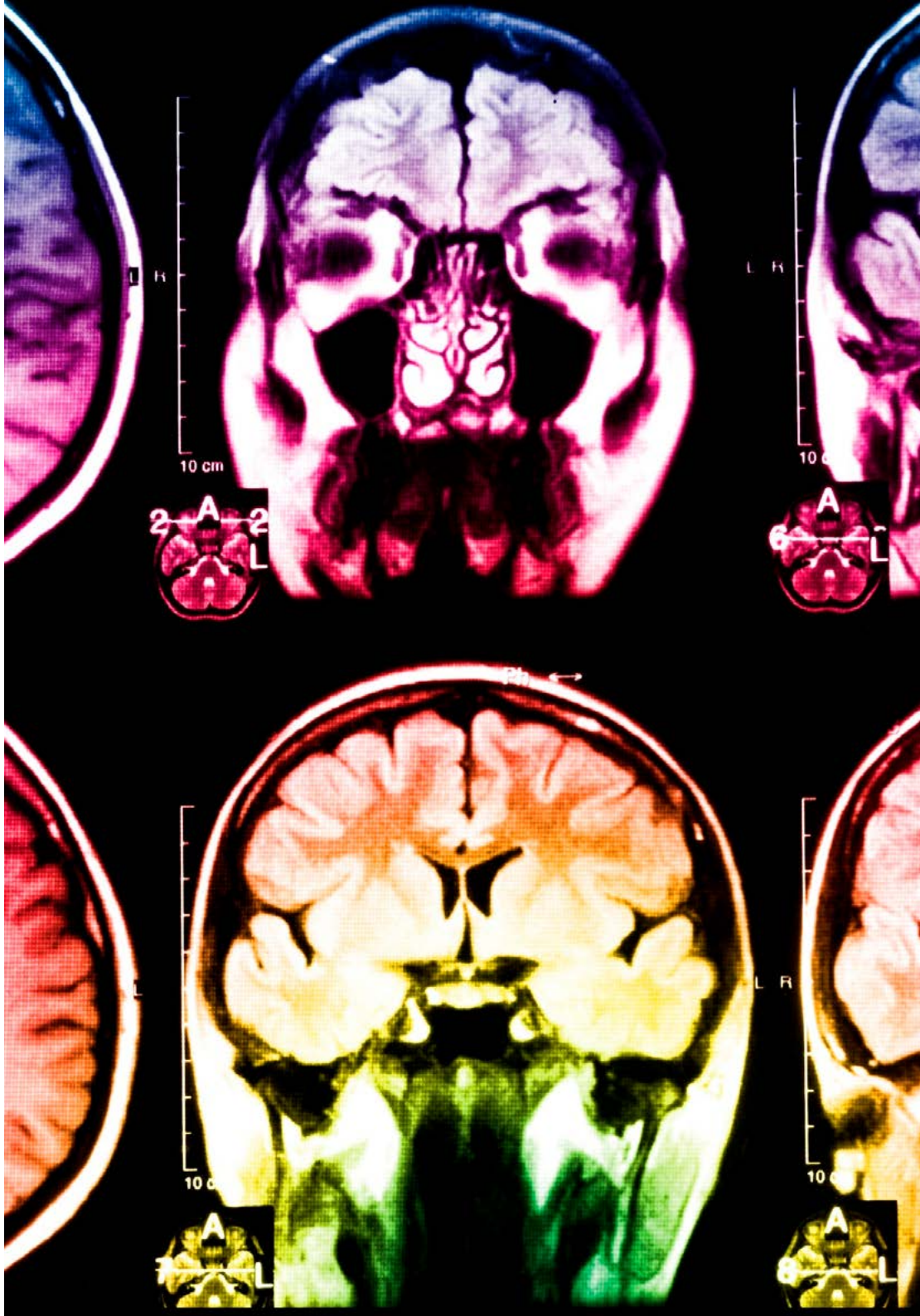
المنهجية الجامعية الأفضل تصنيفاً من قبل طلابها

نتائج هذا النموذج الأكاديمي المبتكريمكن ملاحضته في مستويات الرضا العام لخريجي TECH.

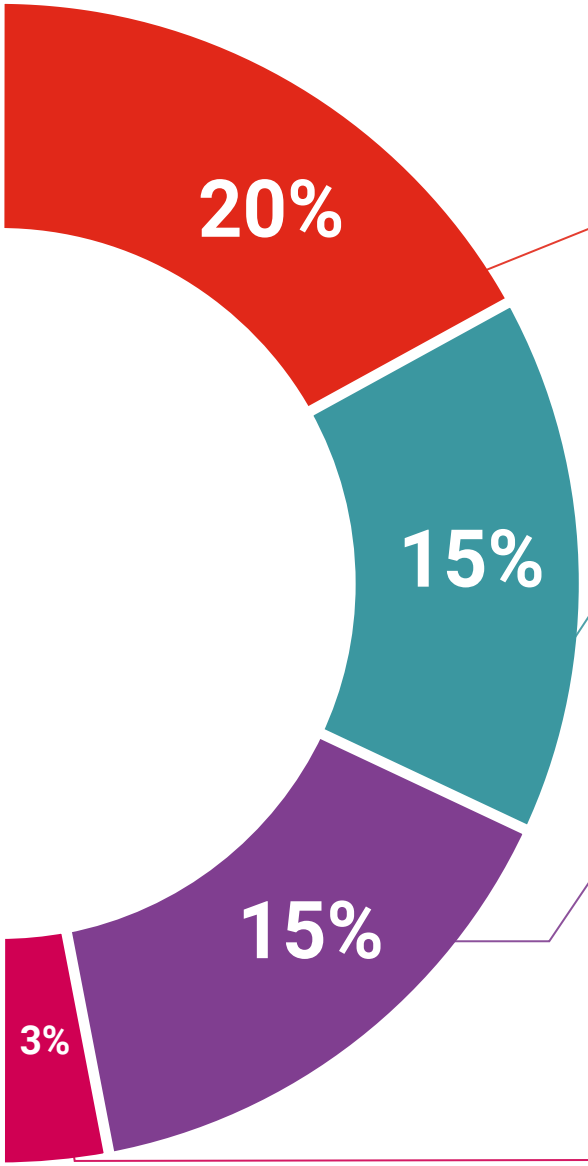
تقييم الطلاب لجودة التدريس، جودة المواد، هيكل الدورة وأهدافها ممتاز. وليس من قبيل الصدفة أن تصبح المؤسسة الجامعة الأعلى تقييماً من قبل طلابها وفقاً لمؤشر global score، حيث حصلت على 4.9 من 5.

يمكنك الوصول إلى محتويات الدراسة من أي جهاز متصل بالإنترنت (كمبيوتر، جهاز لوحي، هاتف ذكي) بفضل كون TECH على اطلاع بأحدث التطورات التكنولوجية والتربوية.

"التعلم من خبير"ستتمكن من التعلم مع مزايا الوصول إلى بيئات تعليمية محاكاة ونهج التعلم بالملاحظة، أي "التعلم من خبير"



وهكذا، ستكون أفضل المواد التعليمية، المُعدّة بعناية فائقة، متاحة في هذا البرنامج:



المواد الدراسية

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

يتم بعد ذلك تطبيق هذه المحتويات على التنسيق السمعي البصري الذي سيخلق طريقتنا في العمل عبر الإنترنت، مع التقنيات الأكثر ابتكارًا التي تتيح لنا أن نقدم لك جودة عالية، في كل قطعة سنضعها في خدمتك.

التدريب العملي على المهارات والكفاءات

ستنفذ أنشطة لتطوير كفاءات ومهارات محددة في كل مجال من مجالات المواد الدراسية. التدريب العملي والديناميكيات لاكتساب وتطوير المهارات والقدرات التي يحتاجها المتخصص لنموه في إطار العولمة التي نعيشها.

ملخصات تفاعلية

نقدم 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 من نوعه لتقديم محتوى الوسائط المتعددة على أنه"قصة نجاح أوروبية".

قراءات تكميلية

المقالات الحديثة والوثائق التوافقية والمبادئ التوجيهية الدولية... في مكتبة TECH الافتراضية، سيكون لديك وصول إلى كل ما تحتاجه لإكمال تدريبك.

دراسات الحالة (Case studies)

ستكمل مجموعة مختارة من أفضل دراسات الحالة في المادة التي يتم توظيفها. حالات تم عرضها وتحليلها وتدريسها من قبل أفضل المتخصصين على الساحة الدولية.

الاختبار وإعادة الاختبار

نقوم بتقييم وإعادة تقييم معرفتك بشكل دوري طوال فترة البرنامج. نقوم بذلك على 3 من 4 مستويات من هرم ميلر.

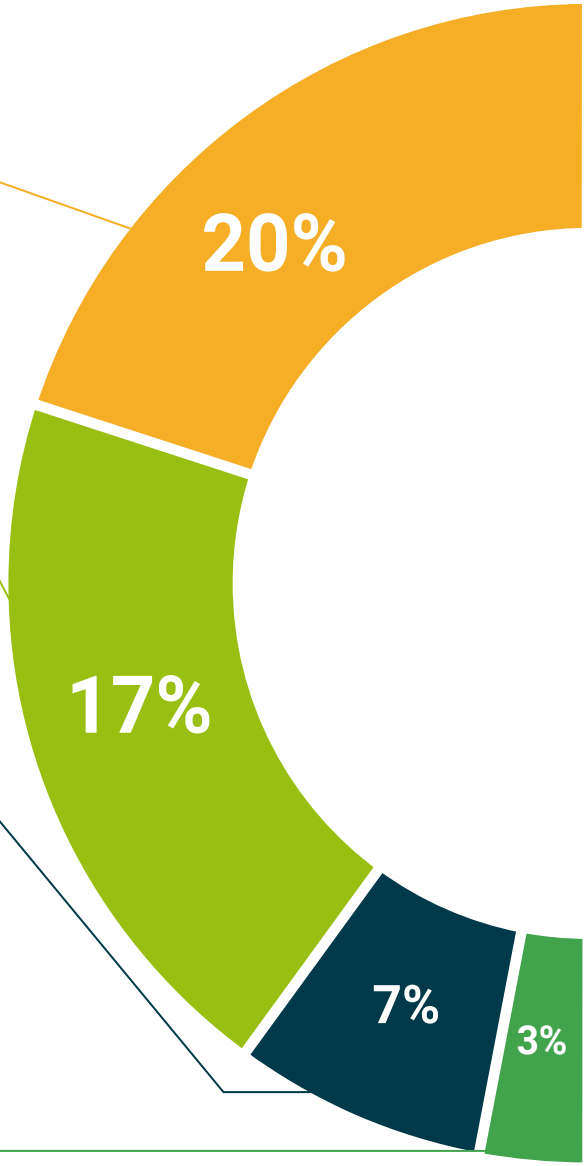
المحاضرات الرئيسية

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

إن ما يسمى **التعلم من خبير** يقوي المعرفة والذاكرة ، ويولد الأمان في قراراتنا الصعبة في المستقبل.

إرشادات توجيهية سريعة للعمل

تقدم TECH المحتويات الأكثر صلة بالدورة التدريبية في شكل أوراق عمل أو إرشادات توجيهية سريعة للعمل. إنها طريقة موجزة وعملية وفعالة لمساعدة الطلاب على التقدم في تعلمهم.



07

أعضاء هيئة التدريس

هذه الشهادة تُقدَّم من قبل خبراء بارزين في الأمن السيبراني وإدارة البيانات الرقمية يضمن خبراؤنا أن يحصل الطلاب على محتوى شامل ومُحدَّث، يمكن تطبيقه مباشرة في حياتهم المهنية. وبفضل ذلك، يشارك الأساتذة في الماجيستير المتقدم في إدارة المعلومات الآمنة (Secure Information Management) معارفهم لتكوين متخصصين مؤهلين تأهيلاً عاليًا ومطلوبين من قِبَل كبرى الشركات على المستوى الدولي.

"انطلق نحو النجاح برفقة الأفضل، واكتسب المعرفة والمهارات الأساسية للريادة في إدارة البيانات والأمن السيبراني في البيئة الرقمية"

المدير الدولي المستضاف

الدكتورFrederic Lemieux **هو خبير دولي بارز وقائد مُلهم في مجالات الاستخبارات والأمن الوطني , والأمن الداخلي, والأمن السيبراني والتقنيات الحديثة.** كما أن تفانيه المستمر ومساهماته ذات الصلة في البحث والتعليم يضعه كشخصية رئيسية فى تعزيز الأمنووفهم التقنيات فى الوضع الحالى. خلال حياته المهنية، قام بوضع تصور وإدارة البرامج الأكاديمية المتطورة في العديد من المؤسسات الشهيرة، مثل جامعة مونتريال، وجامعة جورج واشنطن،**جامعة مونتريال**، وجامعة **جورج واشنطن** و **جامعة جورج تاون**..

طوال خلفيته الواسعة، نشر العديد من الكتب ذات الصلة للغاية، وجميعها تتعلقبالاستخبارات الجنائية والعمل السياسى والتهديدات الإلكترونية و **الأمن الدولى.** بالإضافة إلى ذلك، ساهم بشكل كبير في مجالالأمن الإلكترونى من خلال نشر العديد من المقالات في المجلات الأكاديمية، التي تتناول مكافحة الجريمة أثناء الكوارث الكبرى ومكافحة الإرهاب ووكالات الاستخبارات، والتعاون مع الشرطة. بالإضافة إلى ذلك، كان عضوًا في اللجنة ومتحدثًا رئيسيًا في العديد من المؤتمرات الوطنية والدولية، مما جعله مرجعًا في المجال الأكاديمي والمهني.

شغل الدكتور Doctor Lemieux أدوارًا تحريرية وتقييمية في مختلف المؤسسات الأكاديمية والخاصة والحكومية، مما يعكس تأثيره والتزامه بالتميز في مجال تخصصه. **وبهذه الطريقة، قادته مسيرته الأكاديمية المرموقة إلى العمل كأستاذ ممارس ومدير هيئة التدريس لبرامج جدول الإنتاج الرئيسيفي الذكاء التطبيقي وإدارة مخاطر الأمن الإلكترونى وإدارة التكنولوجيا** و **إدارة تكنولوجيا المعلومات فى جامعة Georgetown.**

د. Lemieux, Frederic

- مدير برنامج الماجستير في Cybersecurity Risk Managementt في Georgetown، واشنطن، الولايات المتحدة الأمريكية
- مدير برنامج الماجستير في Technology Managementt في جامعة Georgetown
- مدير برنامج الماجستير في Applied Intelligence بجامعة Georgetown
- أستاذ التدريب العملى في جامعة Georgetown
- دكتوراه في علم الجريمة من la School of Criminology جامعة Montreal
- ليسانس في علم الاجتماع وحاصل على درجة Minor Degree في علم النفس من جامعة Laval
- عضو في: New Program Roundtable Committee، جامعة Georgetown

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

هيكل الإدارة

د. Peralta Martín-Palomino, Arturo

- الرئيس التنفيذي CEO ومدير قسم التكنولوجيا CTO في Prometeus Global Solutions
- مدير قسم التكنولوجيا في Korporate Technologies
- مدير قسم التكنولوجيا في AI Shepherds GmbH
- مرشد ومستشار الأعمال الاستراتيجية في Alliance Medical
- مدير التصميم والتطوير في DocPath
- دكتور في هندسة الحاسوب من جامعة Castilla-La Mancha
- دكتور في الاقتصاد والأعمال والماليات من جامعة Camilo José Cela
- دكتور في علم النفس من جامعة Castilla-La Mancha
- الماجستير التنفيذي MBA من جامعة Isabel I
- ماجستير في الإدارة التجارية والتسويق من جامعة Isabel I
- ماجستير خبير في البيانات الضخمة Big Data من تدريب Hadoop
- ماجستير في تقنيات الكمبيوتر المتقدمة من جامعة Castilla-La Mancha
- عضو في مجموعة الأبحاث التخصصات SMILE

أ. Fernández Sapena, Sonia

- مدربة أمن الحاسوب والقرصنة الأخلاقية في مركز Getafe الوطني المرجعي للحوسبة والاتصالات بمدريد
- مدربة معتمدة من المجلس الإلكتروني
- مدربة في الشهادات التالية: شركة الصناعات الحصرية العامة المحدودة Ethical Hacking Foundation وشركة الصناعات الحصرية العامة المحدودة سايبروتكنولوجيا المعلومات Security Foundation. مدريد
- مدربة خبيرة معتمدة من قبل التصنيع بمساعدة الحاسوب للشهادات 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 كبير ضباط الأمن / مهندس أمني أول (Chief Security Officer/Senior Security Architect. فى جامعة las Islas Baleares
- مهندسة حاسوب من جامعة Alcalá de Henares في مدريد
- ماجستير في DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

الأساتذة

أ. Montoro Montarroso, Andrés

- باحث في مجموعة SMILe بجامعة Castilla-La Mancha
- باحث في جامعة غرناطة
- عالم بيانات في Prometeus Global Solutions
- نائب الرئيس ومطور البرمجيات في CireBits
- دكتوراه في تقنيات الكمبيوتر المتقدمة من جامعة كاستيا لا مانشا
- بكالوريوس في هندسة الكمبيوتر من جامعة Castilla-La Mancha
- ماجستير في علوم البيانات وهندسة الكمبيوتر من جامعة غرناطة
- أستاذ ضيف في موضوع النظم القائمة على المعرفة في المدرسة العليا للمعلوماتية في سيوداد ريال، يلقي مؤتمر: تقنيات الذكاء الاصطناعي المتقدمة: بحث وتحليل الإمكانات الجذرية في وسائل التواصل الاجتماعي
- أستاذ ضيف في موضوع التنقيب عن البيانات في المدرسة العليا للمعلوماتية في سيوداد ريال، يلقي مؤتمر: تطبيقات معالجة اللغات الطبيعية: المنطق الضبابي في تحليل الرسائل على شبكات التواصل الاجتماعي
- متحدث في ندوة حول الوقاية من الفساد في الإدارات العامة والذكاء الاصطناعي في كلية العلوم القانونية والاجتماعية في توليدو، حيث ألقى المحاضرة: تقنيات الذكاء الاصطناعي
- متحدث في الندوة الدولية الأولى حول القانون الإداري والذكاء الاصطناعي (DAIA). ينظمه مركز Luis Ortega Álvarez للدراسات الأوروبية ومعهد TransJus للأبحاث. مؤتمر بعنوان تحليل المشاعر للوقاية من رسائل الكراهية على شبكات التواصل الاجتماعي

أ. Peris Morillo، Luis Javier

- قائد تقني أول في مجال الدعم الفني ودعم التسليم الرئيسي في شركة HCL Technologiesمحرر تقني في Baeldung
- Agile Coach ومدير العمليات في Mirai Advisory
- مطور، Agile Coach، Scrum Master، Team Lead و Product Manager في DocPathتقني في ARCO
- بكالوريوس في هندسة متفوق في الكمبيوتر من جامعة Castilla-La Mancha
- دراسات عليا في إدارة المشاريع من قبل CEOE

أ. Fernández Meléndez، Galina

- متخصصة في Big Data
- محللة بيانات في شركة آريسي لإدارة الأموال
- محللة بيانات في ADN Mobile Solution
- شهادة في إدارة الأعمال من جامعة بيسينتيناريا دي أراغوا. كاراكاس، فنزويلا
- محاضرة جامعية في التخطيط والمالية العامة من المدرسة الفنزويلية للتخطيط
- ماجستير في تحليل البيانات وذكاء الأعمال من جامعة أوفييدو
- MBA في إدارة الأعمال والإدارة لكلية الأعمال الأوروبية في برشلونة
- ماجستير في البيانات الضخمة وذكاء الأعمال من كلية الأعمال الأوروبية في برشلونة

أ. Pedrajas Parabá, María Elena

- New Technologies and Digital Transformation Consultant في Managementt Solutions
- باحث في قسم علوم الحاسوب والتحليل العددي بجامعة قرطبة
- باحثة في مركز Centro Singular de Investigación en Tecnologías Inteligentes في سانتياغو دي كومبوستيلا
- بكالوريوس في هندسة الكمبيوتر من جامعة قرطبة
- ماجستير في علوم البيانات وهندسة الكمبيوتر من جامعة غرناطة
- ماجستير في استشارات الاعمال من جامعة Comillas البابوية

أ. Martínez Cerrato, Yésica

- رئيسة التدريبات التقنية في Securitas Seguridad España
- متخصصة في التعليم والأعمال والتسويق
- Product Manager مديرة المنتجات في الأمن الإلكتروني في Securitas Seguridad España
- محللة ذكاء الأعمال في Ricopia Technologies
- تقنية كمبيوتر ورئيسة فصول OTEC الحاسوبية في جامعة Alcalá de Henares
- متعاونة في جمعية ASALUMA
- إجازة في هندسة الاتصالات الإلكترونية من مدرسة الفنون التطبيقية العليا، جامعة Alcalá de Henares

أ. Fondón Alcalde،Rubén

- محلل أمازون Amazon Web Services أوروبا والشرق الأوسط وأفريقيا
- محلل أعمال في إدارة قيمة العملاء في Vodafone إسبانيا
- رئيس تكامل الخدمات في Entelgy for Telefónica Global Solutions
- مدير الحساب عبر الإنترنت لخوادم Clone في EDM Electronics
- مدير تنفيذ الخدمات الدولية في شركة Vodafone Global Enterprise
- استشاري حلول لإسبانيا والبرتغال، Telvent Global Services
- محلل أعمال لجنوب أوروبا في Vodafone Global Enterprise
- مهندس اتصالات من الجامعة الأوروبية بمدريد
- ماجستير في البيانات الضخمة Big Data والتحليلات Analytics من جامعة فالنسيا الدولية

أ. Díaz Díaz-Chirón, Tobías

- باحث في مجموعة SMILe بجامعة Castilla-La Mancha
- مستشار في شركة Blue Telecom
- يعمل مستقل متخصص بشكل أساسي لقطاع الاتصالات السلكية واللاسلكية، متخصص في شبكات 4G / 5G
- OpenStack: النشر والإدارة
- مهندس علوم كمبيوتر من جامعة كاستيلا لامانشا
- التخصص في هندسة الحاسوب والشبكات
- أستاذ مشارك في جامعة Cádiz
- المتحدث في دورة Sepecam على إدارة الشبكة

أ. Tato Sánchez، Rafael

- المدير الفني في Indra Sistemas SA
- مهندس النظم في ENA Traffic SAU
- ماجستير في الصناعة 4.0. من الجامعة على الإنترنت
- ماجستير في الهندسة الصناعية من جامعة الأوروبية
- شهادة في هندسة الإلكترونيات الصناعية والأتمتة من الجامعة الأوروبية
- مهندس التقنيات صناعي من جامعة البوليتكنيك في مدريد

أ. Marcos Sbarbaro, Victoria Alicia

- مطورة تطبيقات موبايل أندرويد الأصلية B60. المملكة المتحدة
- محللة برمجة لإدارة وتنسيق وتوثيق البيئة الافتراضية للإنذارات الأمنية
- محللة ومبرمجة تطبيقات جافا لأجهزة الصراف الآلي للعميل
- محترفة تطوير Software للتحقق من صحة توقيع العميل وتطبيق إدارة المستندات
- تقنية أنظمة لترحيل المعدات وإدارة وصيانة وتدريب أجهزة المساعد الرقمي الشخصي المحمولة
- مهندسة تقنية في أنظمة الكمبيوتر من جامعة Oberta في كاتالونيا
- ماجستير في أمن الكمبيوتر والقرصنة الأخلاقية الرسمية من EC- Council و CompTIA من قبل المدرسة المهنية للتكنولوجيات الجديدة CICE

أ. Catalá Barba, José Francisco

- تقني إلكترونيات خبير في الأمن السيبراني
- مطور تطبيقات الأجهزة المحمولة
- تقني إلكترونيات في القيادة المتوسطة بوزارة الدفاع الإسبانية
- تقني إلكترونيات في Factoría Ford Sita في Valencia

أ. Armero Fernández, Rafael

- Business Intelligence Consultant في مجموعة SDG
- Digital Engineer في MI-GSO
- Logistic Engineer في Torrecid SA
- Quality Intern في INDRA
- تخرج في هندسة الطيران من جامعة البوليتكنيك في فالنسيا
- ماجستير في التطوير المهني 4.0 من جامعة Alcalá

أ. Peralta Alonso, Jon

- مستشار أول لحماية البيانات والأمن السيبراني في Altia
- محامي ومستشار قانوني في Arriaga Asociados مؤسسة ذات مسؤلية محدودة للاستشارات القانونية والاقتصادية
- المستشار القانوني / المتدرب في شركة مهنية: Óscar Padura
- إجازة في القانون من جامعة Pública del País Vasco
- ماجستير في حماية البيانات من مدرسة نظام المعلومات التنفيذي Innovative School
- ماجستير في القانون من جامعة Pública del País Vasco
- ماجستير في ممارسة الإجراءات المدنية من جامعة Isabel 1 الدولية de Castilla
- مدرس في درجة الماجستير في حماية البيانات الشخصية والأمن السيبراني وقانون تكنولوجيا المعلومات والاتصالات

أ. Redondo, Jesús Serrano

- مطور ويب وفني الأمن السيبراني
- مطور ويب في Roams،Palencia
- مطور FrontEnd في تليفونيكا، مدريد
- مطور FrontEnd في أفضل شركة استشارات احترافية Best Pro Consulting، مدريد
- مُركِّب معدات وخدمات الاتصالات في Grupo Zener، Castilla،León
- مُركِّب معدات وخدمات الاتصالات في Lican Comunicaciones SL، Castilla،León
- شهادة في أمن معلومات الحاسوب من المركز المرجعي الوطني لتطوير الحاسوب والاتصالات Getafe، مدريد
- فني عالي في الاتصالات وأنظمة الحاسوب من مؤسسات التعليم العالي IES Trinidad Arroyo، Palencia
- فني عالي في التركيبات الكهروتقنية ناقل الحركة اليدوي والجهد المنخفض من مؤسسات التعليم العالى IES Trinidad Arroyo، Palencia
- تدريب في الهندسة العكسية والاختزال والتشفير من أكاديمية Hacker 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
- إجازة في هندسة الاتصالات عن بعد من جامعة Politécnica بمدريد
- ماجستير في الأمن السيبراني والقرصنة الأخلاقية من المدرسة المهنية للتقنيات الجديدة CICE
- دورة عليا في الأمن السيبراني من قبل Deusto Formación

"اغتنم الفرصة للتعرف على أحدث التطورات في هذا الشأن لتطبيقها في ممارستك اليومية"

08

المؤهل العلمي

يضمن الماجستير المتقدم في إدارة المعلومات الآمنة (Secure Information Management) بالإضافة إلى التدريب الأكثر دقة وحداثة، الحصول على مؤهل الماجستير المتقدم الصادر عن TECH الجامعة التكنولوجية.

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

تحتوي درجة **الماجستير المتقدم في إدارة المعلومات الآمنة (Secure Information Management)** على البرنامج الأكثر اكتمالا وحداثة في السوق.

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

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

المؤهل العلمي: **ماجستير متقدم في إدارة المعلومات الآمنة (Secure Information Management)**

طريقة الدراسة: **عبر الإنترنت**

مدة الدراسة: **2 سنتين**

tech الجامعة التكنولوجية

شهادة تخرج

هذه الشهادة ممنوحة إلى

لـ

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

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

ماجستير متقدم

في

إدارة المعلومات الآمنة (Secure Information Management)

وهي شهادة خاصة من هذه الجامعة موافقة لـ 3000 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 متقدم في (Secure Information Management) إدارة المعلومات الآمنة

التوزيع العام للخطة الدراسية

الدورة	المادة	الطريقة	عدد الساعات
1º	تحليل البيانات في المؤسسة	إجباري	150
1º	إدارة البيانات ومعالجتها لعلوم البيانات	إجباري	150
1º	الأجهزة والمنصات الذكية IoT كأساس لعلوم البيانات	إجباري	150
1º	التمثيل البياني لتحليل البيانات	إجباري	150
1º	أدوات علوم البيانات	إجباري	150
1º	استخراج البيانات للاختيار والمعالجة الأولية والتحويل	إجباري	150
1º	التنبؤ وتحليل الظواهر العشوائية	إجباري	150
1º	تصميم وتطوير الأنظمة الذكية	إجباري	150
1º	البنى وأنظمة الاستخدام المكثف للمعلومات في علوم البيانات	إجباري	150
1º	التطبيق العملي لعلوم البيانات في قطاعات النشاط التجاري	إجباري	150

الدورة	المادة	الطريقة	عدد الساعات
2º	الاستخبارات السيبرانية والأمن السيبراني	إجباري	150
2º	أمان Host	إجباري	150
2º	أمن الشبكات (الحماية الطرفية)	إجباري	150
2º	أمن الهواتف الذكية smartphones	إجباري	150
2º	الأمن في إنترنت الأشياء IoT	إجباري	150
2º	تكتيكات Hacking	إجباري	150
2º	الهندسة العكسية	إجباري	150
2º	التطوير الآمن	إجباري	150
2º	التحليل الجنائي	إجباري	150
2º	التحديات الحالية والمستقبلية في أمن الحاسوب	إجباري	150

أ. د./ Tere Guevara Navarro
رئيس الجامعة

tech الجامعة التكنولوجية

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

الجامعة التيكنولوجية

ماجستير متقدم
إدارة المعلومات الآمنة
(Secure Information Management)

- طريقة الدراسة: **عبر الإنترنت**
- مدة الدراسة: **2 سنتين**
- المؤهل العلمي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **عبر الإنترنت**

ماجستير متقدم

إدارة المعلومات الآمنة

(Secure Information Management)

tech الجامعة التيكنولوجية