ماجستير متقدم
الإدارة العليا للأمن السيبراني
(كبير مسؤولي أمن المعلومات CISO)

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

ماجستير متقدم
الإدارة العليا للأمن السيبراني
(كبير مسؤولي أمن المعلومات CISO)

- طريقة الدراسة: **عبر الإنترنت**
- مدة الدراسة: **سنتين**
- المؤهل الجامعي 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-senior-cibersecurity-management

الفهرس

01

المقدمة

في عالم اليوم، يعد الأمن السيبراني عنصراً بالغ الأهمية للأفراد والشركات، التي أصبحت أكثر عرضة للهجمات من أي وقت مضى. يرجع ذلك إلى التطور المستمر للتقنيات الجديدة وعملية الرقمنة التي أحدثت تحولات في جميع أنواع الشركات، مما أدى إلى تبسيط العديد من الأنشطة ولكن أدى أيضًا إلى ظهور نقاط ضعف جديدة. لهذا السبب، فإن إحدى أكثر الوظائف المطلوبة اليوم هي وظيفة مدير الأمن السيبراني، وهي شخصية متنامية مع العديد من الفرص الوظيفية.

يتعمق هذا البرنامج في هذا المجال، ويؤهل عالم الحاسوب للتعامل بفعالية وشمولية مع جميع التحديات الحالية في هذا المجال، حيث يتطلب الأمر أيضاً مهارات إدارية ومنظور تجاري. بالإضافة إلى ذلك، تم تطوير الشهادة بصيغة 100% عبر الإنترنت، مما يجعلها مثالية للجمع بينها وبين العمل، مما يسمح للمحترف بالدراسة وقتما يشاء.

سيُعدك هذا البرنامج لمواجهة جميع تحديات الحاضر والمستقبل في مجال الأمن السيبراني، مما يتيح لك التخصص في القيادة في هذا المجال الهام من مجالات تكنولوجيا المعلومات"

العمليات المصرفية، والتسوق عبر الإنترنت، والاتصالات الداخلية في المؤسسات المختلفة، والإجراءات الإدارية، وما إلى ذلك. في الوقت الحاضر، أدت الرقمنة إلى تغيير الطريقة التي يعمل بها الأفراد والشركات بشكل يومي. لقد سرّعت العديد من الأنشطة، وجعلت من غير الضروري القيام برحلات معينة، مما أدى إلى تحسين نوعية حياة السكان وتوفير التكاليف على الشركات. مع ذلك، فقد جلبت هذه المزايا، بالتوازي، مساوئ أخرى للأمن السيبراني.

يتم تطوير العديد من التقنيات والأدوات الرقمية المستخدمة اليوم باستمرار، وبالتالي فهي عرضة للهجوم. مع انتشار استخدام التطبيقات والأجهزة الرقمية على نطاق واسع، فإن أي فشل في هذه التطبيقات والأجهزة يعد أمرًا بالغ الأهمية، حيث يمكن أن يؤثر على تطور المؤسسة، ليس فقط من حيث التسويق والمبيعات، ولكن في عملها الداخلي الذي يعتمد أيضًا على هذه المرافق.

لهذا السبب، تحتاج الشركات إلى خبراء في الأمن السيبراني يمكنهم الاستجابة للمشاكل المختلفة التي قد تنشأ في هذا المجال. من أكثر المناصب المطلوبة هي منصب مدير الأمن السيبراني، وهو منصب يستلزم رؤية عالمية لهذا المجال، ويوفر هذا الماجستير المتقدم إعداداً كاملاً له. بالتالي، يعد هذا البرنامج فرصة عظيمة لعالم الحاسوب لأنه سيجعله على مقربة من كل ما هو جديد في هذا المجال، ويهيئه، في الوقت نفسه، لمواجهة القرارات الإدارية التي تتطلب أفضل المعارف والمهارات القيادية.

كل هذا، استنادًا إلى منهجية التعلم عبر الإنترنت التي تتكيف مع الظروف المهنية للطالب، مع مرافقة طاقم تدريس ذو مكانة مرموقة في هذا المجال من علوم الحاسب الآلي. سيكون لديك أيضًا تحت تصرفك أفضل التقنيات التعليمية وأحدث الموارد التعليمية: الملخصات التفاعلية ومقاطع الفيديو والدروس الرئيسية ودراسات الحالة والقراءات التكميلية.

دون أن ننسى المواد المكملة للمنهج الدراسي، مثل الصفوف الدراسية المتقدمةMasterclasses العشر التي يقدمها خبير مشهور عالمياً في مجال الذكاء والأمن السيبراني والتقنيات الثورية. بفضل هذا المحتوى الإضافي سيتمكن الخريج من إثراء تعلمهم في مجال الإدارة العليا للأمن السيبراني (كبير مسؤولي أمن المعلومات CISO)، وسيتمكنون من تعميق معرفتهم بالمفاهيم المتعلقة بالذكاء السيبراني وأمن المعلومات

يحتوي هذا **الماجستير المتقدم في الإدارة العليا للأمن السيبراني (كبير مسؤولي أمن المعلومات CISO)** على البرنامج التعليمي الأكثر اكتمالاً وحداثة في السوق. أبرز خصائصه هي:

- تطوير الحالات العملية التي يقدمها الخبراء في تكنولوجيا المعلومات الأمن السيبراني
- يوفر المحتوى البياني والتخطيطي والعملي البارز للكتاب معلومات علمية وعملية عن تلك التخصصات الضرورية للممارسة المهنية
- التمارين العملية حيث يمكن إجراء عملية التقييم الذاتي لتحسين التعلم
- تركيزه الخاص على المنهجيات المبتكرة في إدارة الأمن السيبراني
- محاضرات نظرية، وأسئلة للخبير، ومنتديات نقاشية حول القضايا المثيرة للجدل وأعمال التفكير الفردي
- توفر المحتوى من أي جهاز ثابت أو محمول متصل بالإنترنت

> تخصّص في الإدارة العليا للأمن السيبراني (كبير مسؤولي أمن المعلومات CISO)، وعزّز معرفتك بفضل 10 صفوف دراسية متقدمة يقدمها محترف ذو مكانة دولية مرموقة"

مع هذا الماجستير المتقدم ستتمكن من التعمق أكثر في أمن إنترنت الأشياء، والحوسبة السحابية، والبلوك تشين، وستتعلم كيفية إجراء عمليات تدقيق عالية المستوى لجميع أنواع الشركات والمؤسسات"

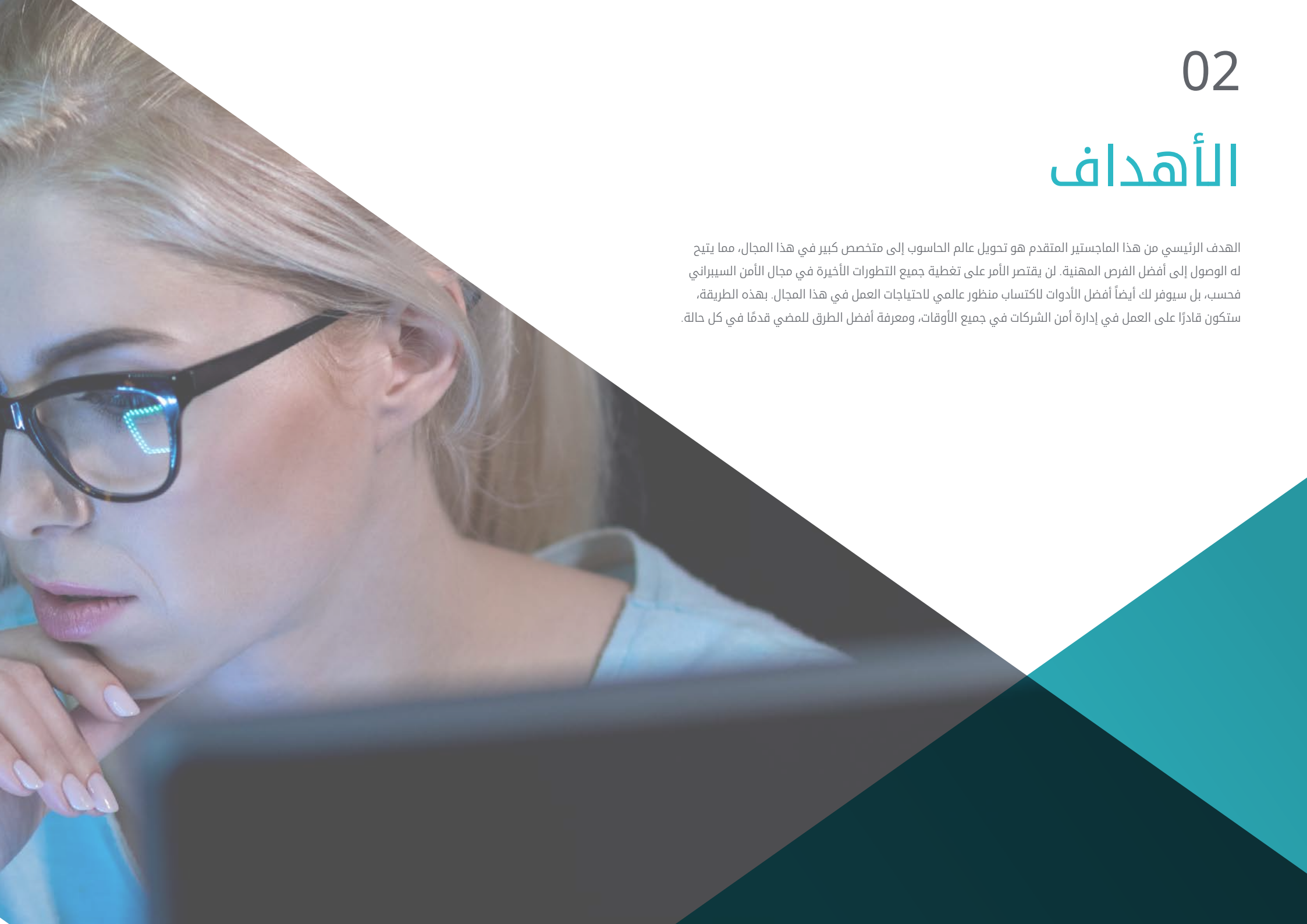
ستستمتع بدعم هيئة تدريس محترمة للغاية، والتي ستضمن حصولك على جميع المفاتيح في مجال إدارة الأمن السيبراني

سيكون لديك تحت تصرفك أحدث الموارد التعليمية لضمان عملية تعلم سريعة وفعالة.

يضم أعضاء هيئة التدريس المتخصصين في مجال ألأمن السيبراني، الذين يصبون خبراتهم العملية في هذا البرنامج، بالإضافة إلى متخصصين معترف بهم من المجتمعات الرائدة والجامعات المرموقة.

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

الأهداف

الهدف الرئيسي من هذا الماجستير المتقدم هو تحويل عالم الحاسوب إلى متخصص كبير في هذا المجال، مما يتيح له الوصول إلى أفضل الفرص المهنية. لن يقتصر الأمر على تغطية جميع التطورات الأخيرة في مجال الأمن السيبراني فحسب، بل سيوفر لك أيضاً أفضل الأدوات لاكتساب منظور عالمي لاحتياجات العمل في هذا المجال. بهذه الطريقة، ستكون قادرًا على العمل في إدارة أمن الشركات في جميع الأوقات، ومعرفة أفضل الطرق للمضي قدمًا في كل حالة.

سيساعدك هذا الماجستير المتقدم على تحقيق التقدم المهني الذي تتطلع إليه، وذلك بفضل محتواه الشامل والمحدث، وطاقم التدريس المرموق المكون من خبراء الأمن السيبراني النشطين"

الأهداف العامة

- تحليل دور المحلل في الأمن السيبراني
- التعمق في الهندسة الاجتماعية وأساليبها
- فحص منهجيات OSINT و HUMINT و OWASP و PTEC. OSSTMM, OWISAM
- إجراء تحليل للمخاطر ومعرفة مقاييس المخاطر
- تحديد الاستخدام الصحيح لإخفاء الهوية واستخدام الشبكات مثل TORو I2P و Freenet
- تجميع اللوائح الحالية بشأن الأمن السيبراني
- توليد المعرفة المتخصصة لإجراء التدقيق الأمني
- تطوير سياسات الاستخدام المناسبة
- استعراض أنظمة الكشف والوقاية من أهم التهديدات
- تقييم أنظمة الكشف الجديدة عن التهديدات، وكذلك تطورها فيما يتعلق بالحلول الأكثرتقليدية
- تحليل منصات المحمول الرئيسية الحالية وخصائصها واستخدامها
- تحديد وتحليل وتقييم المخاطر الأمنية لإجزاء مشروع إنترنت الأشياء
- 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 الطب الشرعي
- تقديم تقرير الطب الشرعيعلى النحو الواجب
- تحليل الوضع الحالي والمستقبلي لأمن تقنية المعلومات
- دراسة مخاطر التكنولوجيات الجديدة الناشئة
- تجميع التقنيات المختلفة فيما يتعلق بأمن تقنية المعلومات
- توليد المعرفة المتخصصة حول نظام المعلومات وأنواعه والجوانب الأمنية التي يجب أخذها في الاعتبار
- تحديد نقاط الضعف في نظام المعلومات
- تطوير التنظيم القانوني وتجريم الاعتداء على الأنظمة المعلوماتية
- تقييم نماذج البنية الأمنية المختلفة لتحديد النموذج الأنسب للمؤسسة
- تحديد الأطر التنظيمية المعمول بها والأسس التنظيمية لها
- تحليل الهيكل التنظيمي والوظيفي لمجال أمن المعلومات (مكتب CISO)
- تحليل وتطوير مفهوم المخاطرة وعدم اليقين في البيئة التي نعيش فيها
- فحص نموذج إدارة المخاطر استنادًا إلى ISO 31.000
- دراسة علم التشفير وعلاقته بفروعه: علم التشفير وتحليل الشفرات وعلم إخفاء المعلومات وتحليل إخفاء المعلومات
- تحليل أنواع التشفير وفقاً لنوع الخوارزمية ووفقاً لاستخدامها
- فحص الشهادات الرقمية
- فحص البنية التحتية للمفاتيح العامة (PKI)
- تطوير مفهوم إدارة الهوية
- تحديد طرق المصادقة
- توليد المعرفة المتخصصة حول منظومة أمن الحاسبات
- تقييم المعرفة بالأمن السيبراني
- تحديد مجالات الأمن في Cloud
- تحليل الخدمات والأدوات في كل مجال من مجالات الأمن
- تطوير مواصفات الأمن لكل تقنية من تقنيات شبكات LPWAN الطاقة المنخفضة
- تحليل مقارن لأمن تقنيات شبكات LPWAN

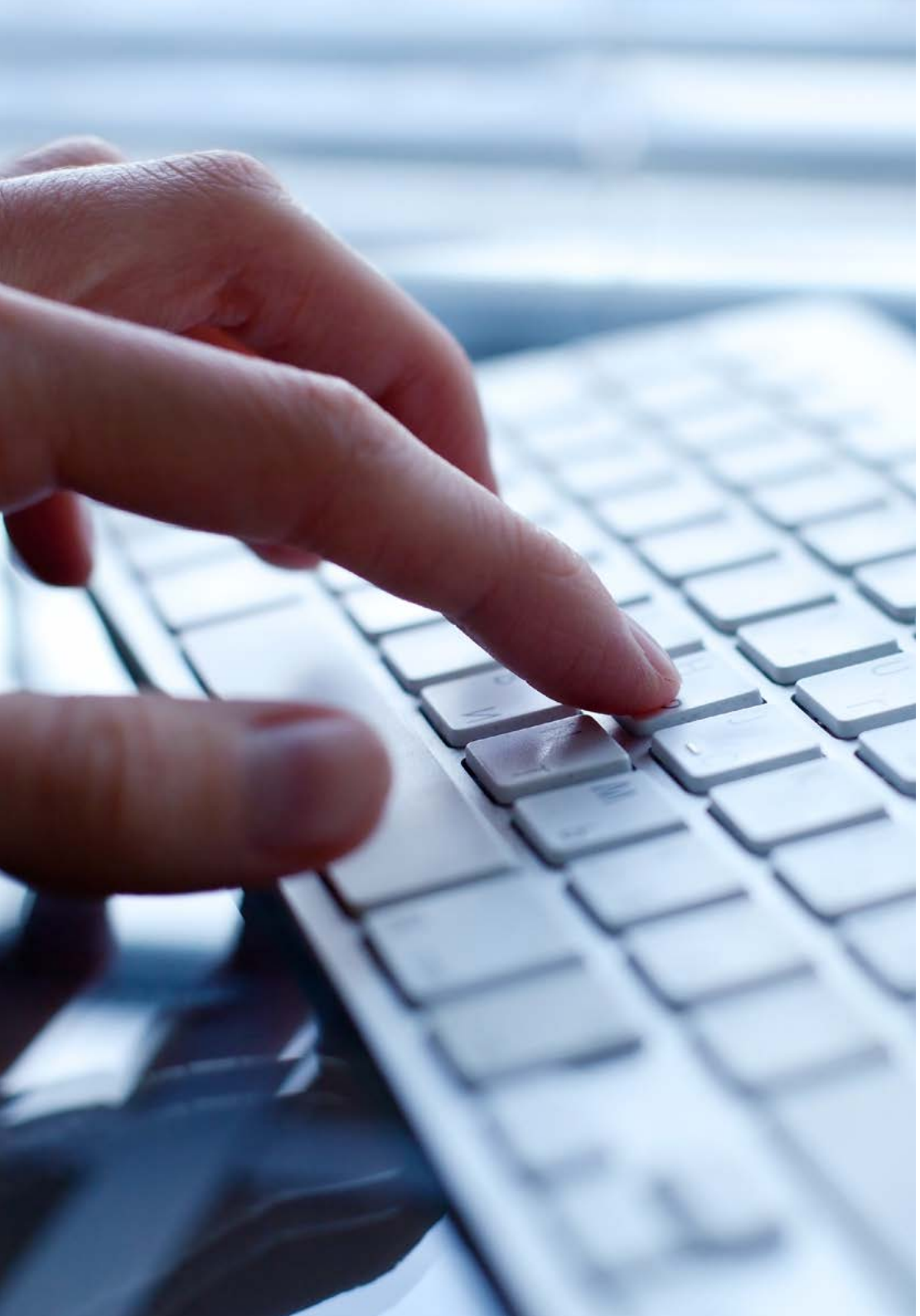
الأهداف المحددة

الوحدة 1. الذكاء والأمن السيبراني

- تطوير المنهجيات المستخدمة في مجال الأمن الإلكترونى
- دراسة دورة الاستخبارات وإثبات تطبيقها في مجال الاستخبارات الإلكترونية
- تحديد دور المحلل الاستخباري ومعوقات نشاط الاخلاء
- تحليل منهجيات استخبارات المصادر المفتوحة و الأمن في الشبكات اللاسلكية و دليل منهجية اختبار الأمان مفتوح المصدر ومنهجية اختبار الاختراق وفتح مشروع أمان تطبيقات الويب
- إنشاء الأدوات الأكثر شيوعًا لإنتاج المعلومات الاستخبارية
- إجراء تحليل المخاطر ومعرفة المقاييس المستخدمة
- تحديد خيارات إخفاء الهوية واستخدام الشبكات مثل تور (شبكة TOR) و مشروع الإنترنت المخفية FreeNet
- تفاصيل لوائح الأمن الإلكتروني الحالية

الوحدة 2. أمان Host

- تحديد سياسات backup للبيانات الشخصية والمهنية
- تقييم الأدوات المختلفة لتقديم حلول لمشاكل أمنية محددة
- إنشاء آليات للحصول على نظام محدث
- تحليل المعدات للكشف عن المتسللين
- تحديد قواعد الوصول إلى النظام
- فحص وتصنيف رسائل البريد الإلكتروني لمنع الاحتيال
- وضع قوائم بالبرامجيات المسموح بها



الوحدة 3. أمان الشبكة (المحيط)

- تحليل هياكل الشبكة الحالية لتحديد المحيط الذي يجب علينا حمايته
- تطوير الإعدادات الأساسية لجدار الحماية firewall ولينيكس Linux للتخفيف من الهجمات الأكثر شيوعا
- تجميع الحلول الأكثر استخدامًا مثل Snort و Meerkat، بالإضافة إلى إعداداتها
- فحص الطبقات الإضافية المختلفة التي توفرها جدران الحماية Firewalls من الجيل الجديد ووظائف الشبكة في بيئات Cloud
- تحديد أدوات حماية الشبكة وشرح سبب أهميتها للدفاع متعدد الطبقات

الوحدة 4. أمن الهواتف الذكية smartphones

- فحص نواقل الهجوم المختلفة لتجنب أن تصبح هدفًا سهلاً
- تحديد الهجمات وأنواع البرامج الضارة الرئيسية التي يتعرض لها مستخدمو الأجهزة المحمولة
- تحليل أحدث الأجهزة لتأسيس أمان أكبر في الاعداد
- تحديد الخطوات الرئيسية لإجراء اختبار الاختراق على كل من أنظمة iOS وأنظمة Android
- تطوير المعرفة المتخصصة حول أدوات الحماية والأمن المختلفة
- تأسيس ممارسات جيدة في البرمجة الموجهة للأجهزة المحمولة

الوحدة 5. الأمن في إنترنت الأشياء IoT

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

الوحدة 6. Hacking أخلاقيات الاختراق

- فحص طرق استخبارات المصادر المفتوحة
- جمع المعلومات المتاحة في الوسائط العامة
- مسح الشبكات بحثاً عن معلومات الوضع النشط
- تطوير معامل الاختبار
- تحليل الأدوات لأداء pentesting
- فهرسة وتقييم مواطن الضعف المختلفة في النظام
- تحديد منهجيات القرصنة المختلفة

الوحدة 7. الهندسة العكسية

- تحليل مراحل جامع البيانات
- فحص بنية المعالج x86 وبنية معالج معمارية آرم
- تحديد الأنواع المختلفة من التحليل
- تطبيق وضع الحماية في بيئات مختلفة
- تطوير تقنيات تحليل البرامج الضارة المختلفة
- إنشاء أدوات تهدف إلى تحليل البرمجيات الخبيثة

الوحدة 8. التطوير الآمن

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

الوحدة 9. التنفيذ العملي لسياسات الأمان في البرامج والأجهزة

- تحديد ماهية التوثيق وتحديد الهوية
- تحليل طرق التوثيق المختلفة الموجودة وتطبيقها العملي
- تنفيذ سياسة التحكم في الوصول الصحيحة للبرامجsoftware والأنظمة
- إنشاء تقنيات تحديد الهوية الحالية الرئيسية
- توليد معرفة متخصصة حول المنهجيات المختلفة الموجودة لتأسيس.الأنظمة

الوحدة 10. التحليل الجنائي

- التعرف على العناصر المختلفة التي تضع دليل على الجريمة
- توليد المعرفة المتخصصة للحصول على البيانات من وسائط مختلفة قبل فقدانها
- استعادة البيانات التي تم حذفها عن قصد
- تحليل سجلات النظام والسجلات
- تحديد كيفية تكرار البيانات حتى لا يتم تغيير النسخ الأصلية
- إثبات الأدلة على أنها متسقة
- إنشاء تقرير متين وبدون ثغرات
- عرض النتائج بشكل متماسك
- تحديد كيفية الدفاع عن التقرير أمام السلطة المختصة
- وضع استراتيجيات لجعل العمل عن بعد آمنًا

الوحدة 11. السلامة في التصميم وتطوير الأنظمة

- تقييم أمن نظام المعلومات بجميع مكوناته وطبقاته
- التعرف على أنواع التهديدات الأمنية الحالية واتجاهاتها
- وضع المبادئ التوجيهية الأمنية من خلال تحديد سياسات وخطط الأمن والطوارئ
- تحليل الاستراتيجيات والأدوات اللازمة لضمان سلامة وأمن نظم المعلومات
- تطبيق التقنيات والأدوات المحددة لكل نوع من أنواع الهجمات أو الثغرات الأمنية
- حماية المعلومات الحساسة المخزنة في نظام المعلومات
- التوفر على الإطار القانوني وتصنيف الجريمة، واستكمال الرؤية بتصنيف الجاني والمجني عليه

الوحدة 12. هياكل ونماذج أمن المعلومات

- مواءمة الخطة الرئيسية الأمنية مع الأهداف الاستراتيجية للمؤسسة
- إنشاء إطار عمل مستمر لإدارة المخاطر كجزء لا يتجزأ من الخطة الرئيسية الأمنية
- تحديد المؤشرات الملائمة لرصد تنفيذ نظام إدارة نظم إدارة المعلومات الإدارية المتكاملة
- وضع استراتيجية أمنية قائمة على السياسات
- تحليل الأهداف والإجراءات المرتبطة بخطة توعية الموظفين والموردين والشركاء
- تحديد اللوائح والشهادات والقوانين المنطبقة على كل مؤسسة ضمن الإطار التنظيمي
- تطوير العناصر الأساسية التي يتطلبها معيار ISO 27001:2013
- تنفيذ نموذج إدارة الخصوصية بما يتماشى مع اللوائح الأوروبية اللائحة العامة لحماية البيانات/اللائحة العامة لحماية البيانات

الوحدة 13. نظام إدارة أمن المعلومات

- تحليل اللوائح والمعايير المطبقة حالياً على نظم نظام إدارة أمن المعلومات
- تطوير المراحل اللازمة لتنفيذ نظام إدارة أمن المعلومات في المؤسسة
- تحليل إدارة حوادث أمن المعلومات وإجراءات تنفيذها

الوحدة 14. إدارة الأمن IT

- التعرف على الهياكل المختلفة التي يمكن أن تحتويها منطقة أمن المعلومات
- تطوير نموذج أمني يستند إلى ثلاثة خطوط دفاعية
- عرض اللجان الدورية والاستثنائية المختلفة التي يشارك فيها مجال الأمن السيبراني
- تحديد الأدوات التكنولوجية التي تدعم الوظائف الرئيسية لفريق العمليات الأمنية (SOC)
- تقييم تدابير التحكم في نقاط الضعف المناسبة لكل سيناريو
- تطوير إطار العمليات الأمنية استنادًا إلى إطار عمل المعهد الوطني للمعايير والمقاييس والمواصفات الأمنية
- تحديد نطاق الأنواع المختلفة من عمليات التدقيق (Red Team، Pentesting، Bug Bounty، etc)
- اقتراح الأنشطة التي سيتم تنفيذها بعد وقوع حادث أمني
- إنشاء مركز قيادة لأمن المعلومات يشمل جميع الجهات الفاعلة ذات الصلة (السلطات والعملاء والموردين وما إلى ذلك)

الوحدة 15. سياسات إدارة الحوادث الأمنية

- تطوير الخبرة في كيفية إدارة الحوادث الناجمة عن أحداث أمن تكنولوجيا المعلومات
- تحديد عملية فريق التعامل مع الحوادث في مجال الأمن
- تحليل المراحل المختلفة لإدارة أحداث أمن تكنولوجيا المعلومات
- فحص البروتوكولات الموحدة للتعامل مع الحوادث الأمنية

الوحدة 16. تحليل المخاطر وبيئة أمن تكنولوجيا المعلومات

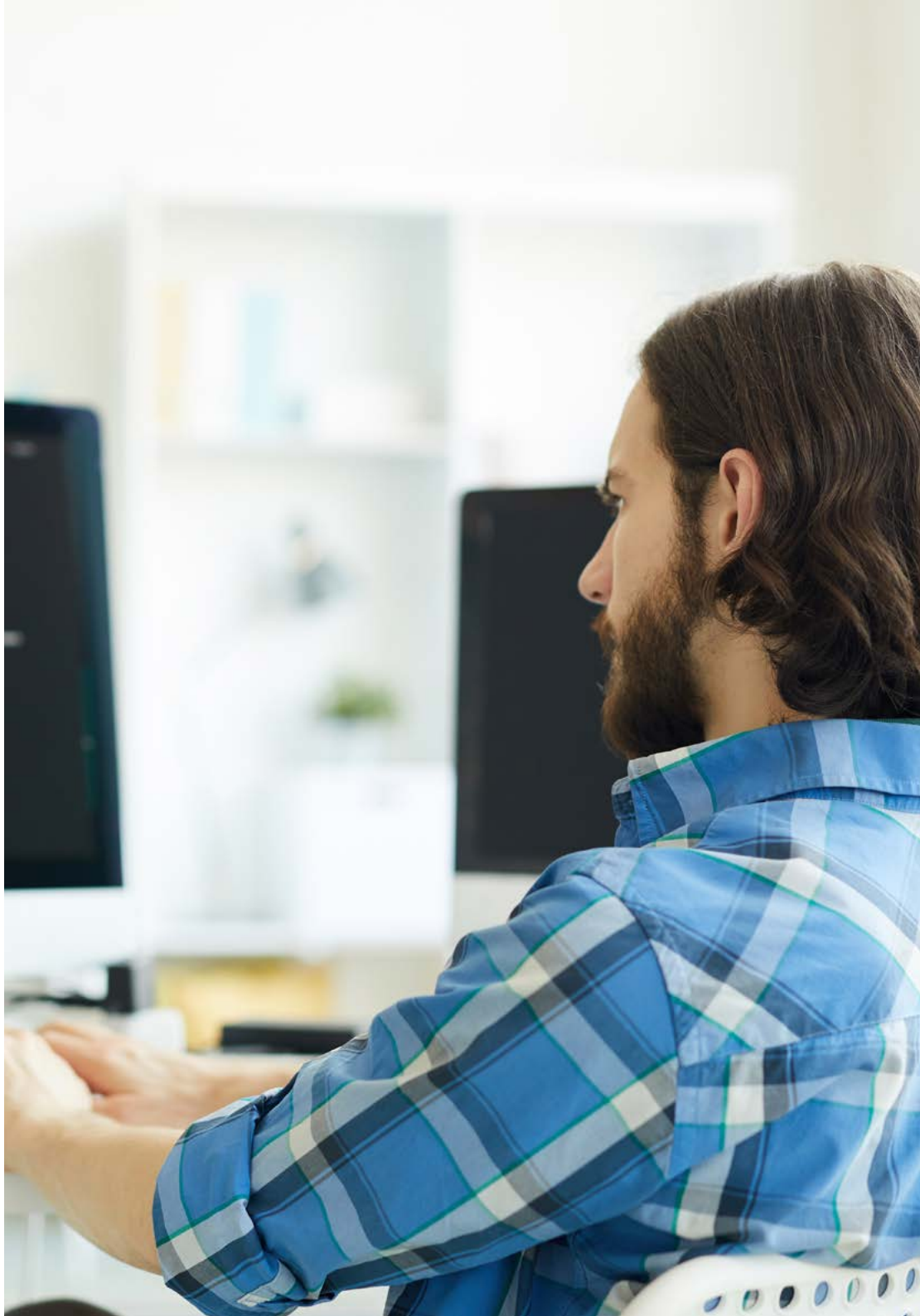
- دراسة البيئة التي نتحرك فيها بنظرة شمولية.
- تحديد المخاطر والفرص الرئيسية التي قد تؤثر على تحقيق أهدافنا
- تحليل المخاطر على أساس أفضل الممارسات المتاحة لنا
- تقييم الأثر المحتمل لهذه المخاطر والفرص
- تطوير التقنيات التي تسمح لنا بالتعامل مع المخاطر والفرص بطريقة تزيد من قيمة المساهمة
- دراسة متعمقة للتقنيات المختلفة لتحويل المخاطر والقيمة
- توليد قيمة من تصميم النماذج الخاصة لإدارة المخاطر الرشيقة
- فحص النتائج لاقتراح تحسينات مستمرة في إدارة المشاريع والعمليات استنادًا إلى نماذج الإدارة القائمة على المخاطرRisk-Driven
- ابتكار البيانات العامة وتحويلها إلى معلومات ذات صلة لاتخاذ القرارات القائمة على المخاطر

الوحدة 17. السياسات الأمنية لتحليل التهديدات في أنظمة الكمبيوتر

- تحليل معنى التهديدات
- تحديد مراحل الإدارة الوقائية للتهديدات
- مقارنة منهجيات إدارة التهديدات المختلفة

الوحدة 18. التنفيذ العملي للسياسات الأمنية في مواجهة الهجمات

- تحديد الهجمات الفعلية المختلفة على نظام المعلومات لدينا
- تقييم سياسات الأمان المختلفة للتخفيف من حدة الهجمات
- تنفيذ تدابير للتخفيف من المخاطر الرئيسية من الناحية التقنية



الوحدة 19. التشفير في تكنولوجيا المعلومات

- تجميع العمليات الأساسية (XOR، الأعداد الكبيرة، الاستبدال والتحويل) والمكونات المختلفة (الوظائف أحادية الاتجاه، التجزئة، مولدات الأرقام العشوائية)
- تحليل تقنيات التشفير
- تطوير خوارزميات التشفير المختلفة
- توضيح استخدام التوقيعات الرقمية وتطبيقها في الشهادات الرقمية
- تقييم أنظمة إدارة المفاتيح وأهمية أطوال مفاتيح التشفير
- دراسة خوارزميات اشتقاق المفاتيح
- تحليل دورة حياة المفاتيح
- تقييم أوضاع تشفير الكتل وتشفير التدفق
- تحديد مولدات الأرقام العشوائية الزائفة
- تطوير حالات تطبيق التشفير في العالم الحقيقي، مثل Kerberos أو PGP أو البطاقات الذكية
- فحص الجمعيات والهيئات ذات الصلة، مثل ISO أو NIST أو NCSC
- تحديد التحديات في التشفير في الحوسبة الكمية

الوحدة 20. إدارة الهوية والوصول في أمن تكنولوجيا المعلومات

- تطوير مفهوم الهوية الرقمية
- تقييم التحكم المادي في الوصول إلى المعلومات
- الأساس المنطقي للمصادقة البيومترية ومصادقة MFA
- تقييم الاعتداءات المتعلقة بسرية المعلومات
- تحليل اتحاد الهويات
- إنشاء التحكم في الوصول إلى الشبكة

الوحدة 21. الأمن في الاتصالات وتشغيل البرامج

- تطوير الخبرة في مجال الأمن المادي والمنطقي
- إظهار المعرفة بالاتصالات والشبكات
- تحديد الهجمات الخبيثة الرئيسية
- إنشاء إطار تطوير آمن
- إثبات فهم اللوائح التنظيمية الرئيسية لنظام إدارة أمن المعلومات
- تأسيس تشغيل مركز عمليات الأمن السيبراني
- توضيح أهمية وجود ممارسات الأمن السيبراني في مواجهة الكوارث المؤسسية

الوحدة 22. الأمان في البيئات السحابيةCloud

- تحديد مخاطر نشر البنية الأساسية السحابية العامة Cloud
- تحديد المتطلبات الأمنية
- وضع خطة أمنية للنشر السحابيCloud
- تحديد الخدمات السحابية Cloudالتي سيتم نشرها لتنفيذ خطة الأمن
- تحديد الترتيبات التشغيلية اللازمة للآليات الوقائية
- وضع مبادئ توجيهية لنظام Loggingالتسجيل والمراقبة
- اقتراح إجراءات الاستجابة للحوادث

الوحدة 23. أدوات مراقبة السياسة الأمنية لنظم المعلومات

- تطوير مفهوم المراقبة وتنفيذ المقاييس
- إعداد مسارات التدقيق على الأنظمة ومراقبة الشبكات
- تجميع أفضل أدوات مراقبة النظام المتوفرة حالياً في السوق

الوحدة 24. أمن اتصالات أجهزة إنترنت الأشياء

- تقديم بنية إنترنت الأشياء المبسطة
- تبرير الفروق بين تقنيات الاتصال العامة وتقنيات الاتصال الخاصة بإنترنت الأشياء
- ترسيخ مفهوم المثلث الحديدي لاتصال إنترنت الأشياء
- تحليل المواصفات الأمنية لتقنية LoRaWAN تقنية NB-IoT وتقنية WiSUN
- تبرير اختيار تقنية إنترنت الأشياء المناسبة لكل مشروع

الوحدة 25. خطة استمرارية الأعمال المرتبطة بالأمن

- عرض العناصر الرئيسية لكل مرحلة وتحليل خصائص خطة استمرارية الأعمال
- إثبات الحاجة إلى خطة استمرارية الأعمال
- تحديد خرائط النجاح والمخاطر لكل مرحلة من مراحل خطة استمرارية الأعمال
- تحديد كيفية وضع خطة عمل للتنفيذ
- تقييم مدى اكتمال خطة استمرارية الأعمال
- وضع خطة للتنفيذ الناجح لخطة استمرارية الأعمال.

الوحدة 26. سياسة التعافي من الكوارث الأمنية العملية

- توليد المعرفة المتخصصة حول في مفهوم أمن المعلومات
- تطوير خطط استمرارية الأعمال
- تحليل خطة استمرارية تكنولوجيا المعلومات والاتصالات
- تصميم خطة التعافي من الكوارث

الوحدة 27. تطبيق سياسات الأمن المادي والبيئي في الشركة

- تحليل مصطلح المنطقة الآمنة والمحيط الآمن
- فحص القياسات الحيوية وأنظمة القياسات الحيوية
- تنفيذ سياسات أمنية سليمة للأمن المادي
- تطوير اللوائح الحالية الخاصة بالمجالات الآمنة لأنظمة تكنولوجيا المعلومات

الوحدة 28. سياسات الاتصالات الآمنة في المؤسسة

- تأمين شبكة الاتصالات عن طريق تقسيم الشبكة
- تحليل خوارزميات التشفير المختلفة المستخدمة في شبكات الاتصالات
- تنفيذ تقنيات التشفير المختلفة في الشبكة مثل TLS أو VPN أو SSH

الوحدة 29. الجوانب التنظيمية لسياسة أمن المعلومات

- تنفيذ نظام إدارة أمن المعلومات في الشركة
- تحديد الأقسام التي ينبغي أن يغطيها تطبيق نظام إدارة الأمن
- تنفيذ التدابير الأمنية المضادة اللازمة في العملية

03

الكفاءات

سيكتسب المحترف من خلال هذا الماجستير المتقدم سلسلة من الأدوات والكفاءات التي ستمكنه من العمل في إدارة الأمن السيبراني في شركة كبيرة. لهذا السبب، لا يركز هذا البرنامج على جوانب تكنولوجيا المعلومات فحسب، بل يهتم بعملية الرقمنة والتقنيات الناشئة وكيفية تأثير هذه العناصر على الأنشطة اليومية المشتركة للمؤسسات. وبهذه الطريقة، سيكون الخريج قادراً على التكيف مع السياق الحالي، ومعرفة أفضل الحلول الأمنية لكل شركة.

طوّر مهاراتك لتصبح أفضل متخصص
في الأمن السيبراني في بيئتك"

الكفاءات العامة

- معرفة المنهجيات المستخدمة في مجال الأمن السيبراني
- معرفة كيفية تقييم كل نوع من أنواع التهديد لتقديم الحل الأمثل في كل حالة
- القدرة على خلق حلول ذكية كاملة لميكنة السلوكيات في حالة وقوع حوادث
- كيفية تقييم المخاطر المرتبطة بنقاط الضعف خارج الشركة وداخلها على حد سواء
- التعرف على تطور وتأثير إنترنت الأشياء بمرور الوقت
- القدرة على إظهار ضعف نظام، ومهاجمته لأغراض وقائية وحل المشكلات المذكورة
- كيفية تطبيق صندوق الحمايةsandbox في بيئات مختلفة
- التعرف على الإرشادات التي يجب على المطور الجيد اتباعها من أجل الامتثال للأمان المطلوب
- تطبيق التدابير الأمنية الأكثر ملاءمة حسب التهديدات
- تحديد سياسة وخطة أمن نظم المعلومات الخاصة بالشركة، واستكمال تصميم وتنفيذ خطة الطوارئ
- إنشاء برنامج تدقيق يلبي احتياجات التقييم الذاتي للأمن السيبراني للمؤسسة
- تطوير برنامج لمسح ومراقبة الثغرات الأمنية وخطة استجابة لحوادث الأمن السيبراني
- تعظيم الفرص المتاحة والتخلص من التعرض لجميع المخاطر المحتملة من التصميم نفسه
- تجميع أنظمة الإدارة الرئيسية
- تقييم أمن المعلومات في الشركة
- تحليل أنظمة الوصول إلى المعلومات
- تطوير أفضل الممارسات في التطوير الآمن
- عرض المخاطر التي تتعرض لها الشركات من عدم وجود بيئة آمنة لتكنولوجيا المعلومات

> سيأخذك هذا البرنامج إلى مستقبل الأمن السيبراني"

الكفاءات المحددة

- التعرف على كيفية تنفيذ عمليات الأمن الدفاعية
- امتلاك تصور عميق ومتخصص لأمن الحاسوب
- امتلاك معارف متخصصة في مجال الأمن السيبراني والذكاء السيبراني
- امتلاك معرفة عميقة بالجوانب الأساسية مثل دورة الاستخبارات، ومصادر الذكاء، والهندسة الاجتماعية، ومنهجية OSINT، و HUMINT، وإخفاء الهوية، وتحليل المخاطر، والمنهجيات الحالية (OWASP، و OWISAM، و OSSTM، و PTES) واللوائح الحالية بشأن الأمن السيبراني
- فهم أهمية ابتكار دفاع متعدد الطبقات، والمعروف أيضًا باسم "Defense in Depth"، والذي يغطي جميع جوانب شبكة الشركة حيث يمكن أيضًا استخدام بعض المفاهيم والأنظمة التي سنراها وتطبيقها في البيئة المحلية
- التعرف على كيفية تطبيق عمليات الأمان على الهواتف الذكية والأجهزة المحمولة
- التعرف على وسائل تنفيذ مايسمى Hacking الأخلاقي وحماية الشركة من أي هجوم إلكتروني
- القدرة على التحقيق في حادث الأمن السيبراني
- التعرف على تقنيات الهجوم والدفاع المختلفة الموجودة
- تحليل دور كبير مسؤولي أمن المعلومات (CISO)
- معرفة وظيفة الهندسة الاجتماعية وأساليبها
- تطوير نظام إدارة أمن المعلومات
- تحديد العناصر الرئيسية التي تشكل نظم إدارة أمن المعلومات
- تطبيق منهجية MAGERIT لتطوير النموذج والمضي به خطوة إلى الأمام
- تصميم منهجيات جديدة لإدارة المخاطر، بناءً على مفهوم agile Risk Management
- تحديد وتحليل وتقييم ومعالجة المخاطر التي يواجهها المحترف من منظور تجاري جديد يعتمد على نموذج Risk-Driven أو مدفوع بالمخاطر والذي لا يسمح فقط بالبقاء في بيئته الخاصة، ولكن أيضًا لتعزيز مساهمة القيمة الخاصة بالفرد
- فحص عملية تصميم استراتيجية الأمن عند نشر خدمات السحابة Cloud للشركات
- تقييم الاختلافات في التطبيقات الملموسة لموردي Cloud العامة المختلفين
- تقييم خيارات الاتصال بإنترنت الأشياء للتعامل مع المشروع، مع التركيز بشكل خاص على تقنيات LPWAN
- تقديم المواصفات الأساسية لتقنيات شبكات LPWAN الرئيسية لإنترنت الأشياء

04

هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

يحتوي هذا الماجستير المتقدم في الإدارة العليا للأمن السيبراني (كبير مسؤولي أمن المعلومات CISO) على هيئة تدريس مكونة من محترفين نشطين يعرفون الوضع الحالي لهذا المجال بإتقان، وبالتالي سينقلون جميع مفاتيح الأمن السيبراني الحالي إلى الطالب. وبهذه الطريقة، يضمن لطالب هذا البرنامج الحصول على أحدث التطورات في هذا المجال، حيث يمكنه الوصول إليها بفضل هيئة التدريس المرموقة التي اختارتها TECH.

التحق بالدورة التدريبية وابدأ في الوصول إلى المعرفة الأكثر تقدماً في هذا المجال، والتي ينقلها متخصصون يتمتعون بخبرة واسعة في مجال الأمن السيبراني"

المدير الدولي المستضاف

الدكتور Frederic Lemieux معروف عالميًا كخبير مبتكر وقائد ملهم في مجالات الاستخبارات والأمن القومي والأمن الداخلي والأمن السيبراني والتقنيات الثورية. 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

- باحث في الاستخبارات والأمن السيبراني والتقنيات الثورية في جامعة Georgetown
- مدير برنامج الماجستير في Technology ManagementInformation في جامعة Georgetown
- مدير برنامج الماجستير في Technology Management في جامعة Georgetown
- مدير برنامج الماجستير في Cybersecurity Risk Management في جامعة Georgetown
- مدير برنامج الماجستير في Applied Intelligence بجامعة Georgetown
- أستاذ التدريب العملي في جامعة Georgetown
- دكتوراه في علم الجريمة من la School of Criminology جامعة Montreal
- بكالوريوس في علم الاجتماع وحاص 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

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. في 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

أ. Olalla Bonal, Martín

- كبير مديري ممارسات Blockchain في EY
- أخصائي تقني عميل Blockchain لشركة IBM
- مدير الهندسة المعمارية ل Blocknitive
- منسق من فريق في قواعد البيانات الموزعة غير العلائقية لشركة wedoIT (شركة IBM الفرعية)
- مهندس البنية التحتية في Bankia
- رئيس قسم التخطيط في T-Systems
- منسق القسم لشركة Bing Data España.شركة ذات مسؤولية SL

الأساتذة

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. 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

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 في 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
- مُركّب معدات وخدمات الاتصالات في Grupo Zener، Castilla،León
- مُركّب معدات وخدمات الاتصالات في Lican Comunicaciones SL، Castilla،León
- شهادة في أمن معلومات معلومات والفروق الدقيقة من المركز المرجعي الوطني لتطوير الحاسوب والاتصالات Getafe، مدريد
- تقني عالي في أنظمة الاتصالات والحاسوب من معهد 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. Nogales Ávila, Javier

- Quint في Enterprise Cloud y Sourcing Senior Consultant
- Indra في Cloud y Technology Consultant
- Accenture في Associate Technology Consultant
- خريج هندسة المؤسسات الصناعية من جامعة Jaén
- MBA في إدارة وتسيير الشركات من كلية في ThePower Business Schooll

أ. Gómez Rodríguez, Antonio

- مهندس الحلول السحابية الرئيسي لشركة Oracle
- منظم مشارك في ملتقى مطوري ملقة للمطورين
- مستشار متخصص في مجموعة سوبرا جروب وإيفريس
- قائد فريق في System Dynamics
- مطور برمجيات في شركة SGO للبرمجيات
- ماجستير في الأعمال الإلكترونية من كلية La Salle لإدارة الأعمال
- شهادة الدراسات العليا في تكنولوجيا ونظم المعلومات من المعهد الكاتالوني للتكنولوجيا
- بكالوريوس في هندسة الاتصالات من جامعة البوليتكنيك كاتالونيا

أ. Gonzalo Alonso, Félix

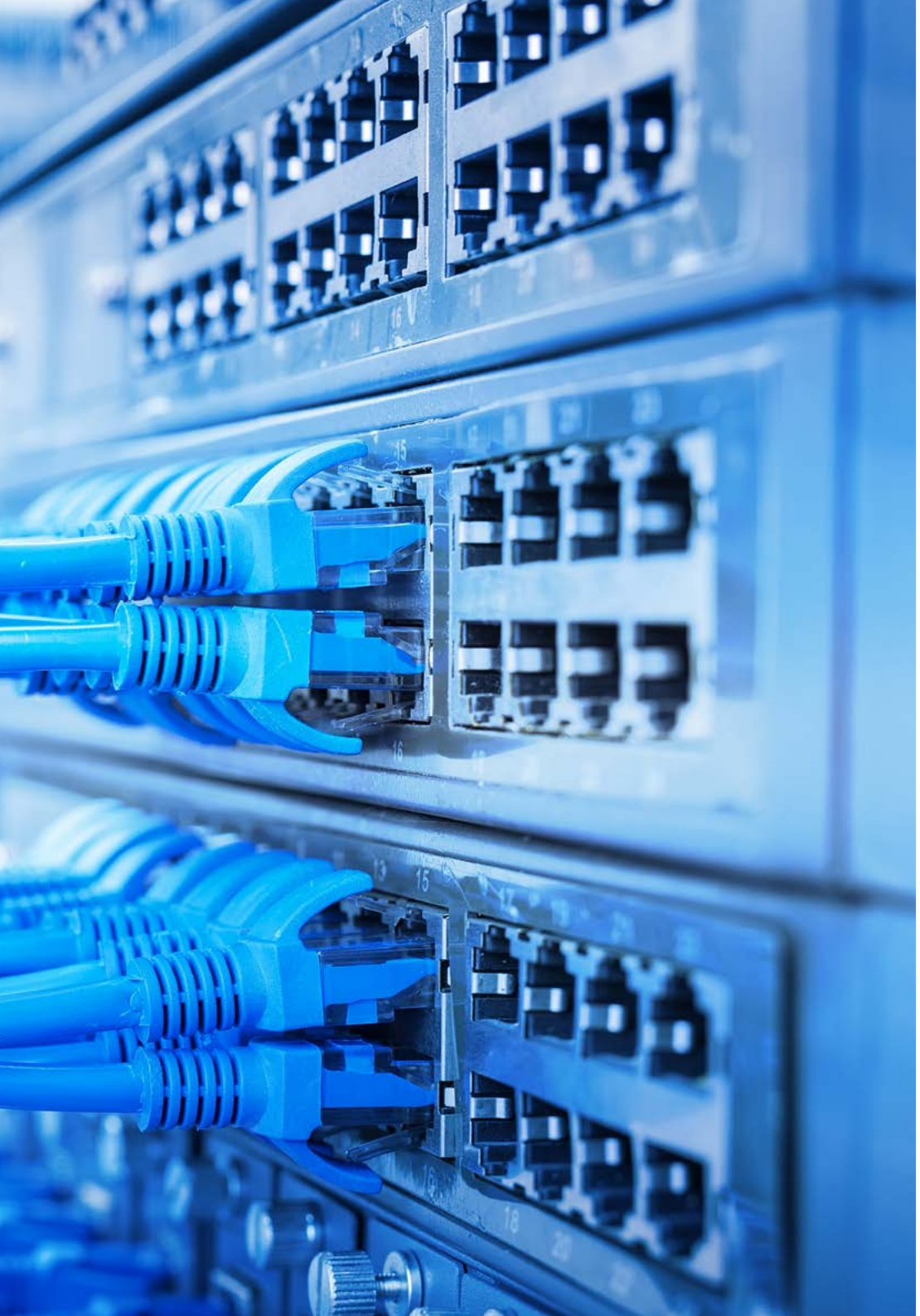
- المدير العام والمؤسس لشركة Smart REM Solutions
- رئيس قسم هندسة المخاطر والابتكار في شركة Dynargy
- المدير الإداري والشريك المؤسس لشركة الاستشارات التكنولوجية Risknova
- ماجستير في إدارة التأمين من معهد التعاون بين شركات التأمين
- شهادة في الهندسة الصناعية التقنية، تخصص إلكترونيات صناعية، جامعة Comillas البابوية

أ. del Valle Arias, Jorge

- مهندس اتصالات مع خبرة في تطوير الأعمال التجارية
- Smart City Solutions & Software Business Development Manager España. Itron, Inc
- مستشار انترنت الأشياء
- مدير أعمال مؤقت في إنترنت الأشياءIoT. TCOMET
- رئيس وحدة أعمال إنترنت الأشياء IoT، وحدة أعمال الصناعة 4.0. Diode España
- مدير مبيعات المنطقة لإنترنت الأشياء IoT والاتصالات. Aicox Soluciones
- المدير الفني ومدير تطوير الأعمال (CTO) ومدير تطوير الأعمال. Consultoría TELYC
- المؤسس والرئيس التنفيذي لشركة Sensor Intelligence
- رئيس العمليات والمشاريع. codio
- مدير العمليات في Codium Networks
- كبير مهندسي تصميم الأجهزة والبرامج الثابتة. AITEMIN
- الرئيس الإقليمي لتخطيط وتحسين الترددات اللاسلكية - شبكة LMDS 3.5 جيجا هرتز. clearwire
- مهندس اتصالات من الجامعة البوليتكنيك بمدريد
- ماجستير في إدارة الأعمال التنفيذية من كلية الدراسات العليا الدولية في La Salle في مدريد
- ماجيستير في الطاقات المتجددة. CEPYME

أ. Gozalo Fernández, Juan Luis

- مدير المنتجات القائمة على Blockchain في Open Canarias
- مدير تطوير عمليات Blockchain DevOps Alastria
- مدير تكنولوجيا مستوى الخدمة في سانتاندير إسبانيا
- مدير تطوير تطبيقات الهاتف المحمول Tinkerlink في Cronos Telecom
- مدير تكنولوجيا إدارة خدمات تكنولوجيا المعلومات في Barclays Bank España
- شهادة في هندسة الحاسب الآلي من جامعة UNED
- التخصص في Deep Learning في DeepLearning.ai



أ. Jurado Jabonero, Lorena

- رئيسة أمن المعلومات (CISO) في شركة Grupo Pascual
- مديرة الأمن السيبراني في KPMG إسبانيا
- استشارية إدارة ومراقبة عمليات تكنولوجيا المعلومات ومشاريع البنية التحتية والرقابة عليها في Bankia
- مهندسة أدوات التشغيل في Dalkia
- مطورة في مجموعة Grupo Banco Popular
- مطورة تطبيقات في جامعة البوليتكنيك في مدريد
- بكالوريوس في هندسة الحاسوب من جامعة Alfonso X el Sabio
- مهندس تقني في إدارة الكمبيوتر من جامعة البوليتيكنيك في مدريد
- Certified Data Privacy Solutions Engineer (CDPSE) por ISACA

أ. Simarro Ruiz, Mario

- محامي خبير في تكنولوجيا المعلومات والاتصالات وحماية البيانات في مكتب Martínez-Echevarría للمحامين
- المسؤول القانوني عن Branddocs SL
- محلل مخاطر قطاع الشركات الصغيرة والمتوسطة في BBVA
- أستاذ في الدراسات العليا المتعلقة بالقانون
- بكالوريوس في الحقوق من جامعة Rey Juan Carlos
- بكالريوس في إدارة الأعمال والإدارة من جامعة Rey Juan Carlos
- درجة الماجستير في التكنولوجيات الجديدة والإنترنت والقانون السمعي البصري من مركز للدراسات الجامعيه Villanueva

أ. Mérida Téllez, Juan Manuel

- شريك مؤسس في شركة Ismet Tech
- مدير أمن المعلومات في مجموعة Ecix Group
- Operational Security Officer في شركة Atos لحلول وخدمات تكنولوجيا المعلومات A/S
- محاضر في إدارة الأمن السيبراني في الدراسات الجامعية
- بكالوريوس في علم الهندسة من جامعة Valladolid
- ماجستير في نظم الإدارة المتكاملة من جامعة CEU San Pablo

أ. Entrenas, Alejandro

- مدير مشروع في الأمن الإلكترونى. Entelgy Innotec Security
- مستشار الأمن السيبراني. Entelgy
- محلل أمن المعلومات. Innovery España
- محلل أمن المعلومات. atos
- بكالوريوس في الهندسة التقنية في أنظمة الكمبيوتر من جامعة قرطبة
- درجة الماجستير في تسيير وإدارة أمن المعلومات من جامعة البوليتكنيك في مدريد
- شهادة ITIL v4 التأسيسية في إدارة خدمات تكنولوجيا المعلومات. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

أ. Ortega Esteban, Octavio

- أخصائي التسويق وتطوير الويب
- مبرمج تطبيقات كمبيوتر ومطور ويب مستقل
- Chief Operating Officer في Smallsquid SL
- مسؤول التجارة الإلكترونية فيOrtega y Serrano
- أستاذ في محاضرات شهادة الاحتراف في الحاسوب والاتصالات
- مدرس دورات أمن الحاسوب
- متخرج في علم النفس من جامعة كاتالونيا المفتوحة
- تقني جامعي عالي في تحليل البرمجيات وتصميمها وحلولها
- تقني جامعي عالي في البرمجة المتقدمة

05

الهيكل والمحتوى

يتألف هذا الماجستير المتقدم في الإدارة العليا للأمن السيبراني (كبير مسؤولي أمن المعلومات CISO) من 30 وحدة دراسية، وقد صُمم بعناية ليجعل المحترف أكثر قرباً من أحدث التطورات في هذا المجال. ستتعرف على أحدث التطورات في قضايا مثل الأمان في الهواتف الذكية، والأمان في إنترنت الأشياء، والتطوير الآمن، والتشفير، والأمان في بيئات الحوسبة السحابية Cloud Computing.. بالتالي، من خلال هذا المنهج، سيحصل عالم الحاسوب على أحدث المعارف وأكثرها اكتمالاً، مما يؤهله بسرعة ليصبح متخصصاً مرموقاً في الأمن السيبراني.

لن تجد محتوى أكثر شمولاً من هذا
المحتوى لإطلاعك على آخر المستجدات
في مجال الأمن السيبراني"

الوحدة 1. الذكاء والأمن السيبراني

1.1. الذكاء السيبراني
1.1.1. الذكاء السيبراني
1.1.1.1 الذكاء
1.1.1.1.1. دورة ذكاء
2.1.1.1 الذكاء السيبراني
3.1.1.1 الذكاء والأمن السيبراني
2.1.1. محلل الذكاء
1.2.1.1 دور المحلل الاستخباراتي
2.2.1.1 تحيز محلل الاستخبارات في النشاط التقييمي
2.1. الأمن السيبراني
1.2.1. طبقات الأمان
2.2.1. التعرف على التهديدات السيبراني
1.2.2.1 التهديدات الخارجية
2.2.2.1 التهديدات الداخلية
3.2.1. الإجراءات العكسية
1.3.2.1 الهندسة الاجتماعية
2.3.2.1 الطرق الشائعة الاستخدام
3.1. تقنيات وأدوات الذكاء
1.3.1. استخبارات المصادر المفتوحة
2.3.1. ذكاء وسائل التواصل الاجتماعي
3.3.1. الاستخبارات البشرية
4.3.1. توزيعات وأدوات لينكس
5.3.1. منهجية تقييم الأمن اللاسلكى المفتوح
6.3.1. مشروع أمان تطبيق الويب المفتوح
7.3.1. معيار أداء اختبار الاختراق PTES
8.3.1. دليل منهجية اختبار الأمان مفتوح المصدر OSSTM
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 الذكاء
5.1. التدقيق والتوثيق
1.5.1. التدقيق الأمني لتكنولوجيا المعلومات
2.5.1. أذونات التوثيق والتدقيق
3.5.1. أنواع التدقيق
4.5.1. المخرجات
1.4.5.1 التقرير التقني
2.4.5.1 التقرير التنفيذي
6.1. الخصوصية على الشبكة
1.6.1. استخدام الخصوصية
2.6.1. تقنيات إخفاء الهوية (Proxy، VPN)، الشبكة الخصوصية الافتراضية
3.6.1. شبكات TOR، مشروع الانترنت المخفية Freenet وI2P
7.1. التهديدات وأنواع الأمن
1.7.1. أنواع التهديدات
2.7.1. الأمن المادي
3.7.1. الامن في الشبكات
4.7.1. الأمن المنطقي
5.7.1. الأمان في تطبيقات الويب
6.7.1. الأمن في الأجهزة المحمولة
8.1. اللوائح والامتثال compliance
1.8.1. النظام الأوروبي العام لحماية البيانات
2.8.1. الإستراتيجية الوطنية للأمن الإلكترونى 2019
3.8.1. مجموعة من المعايير الدولية لأمن المعلومات ISO 27000
4.8.1. إطار عمل الأمن الإلكترونى من المعهد الوطني للمعايير والتكنولوجيا
5.8.1. PIC
6.8.1. CUGBP Elav-like family member 23027
7.8.1. اللوائح cloud
8.8.1. SOX
9.8.1. PCI

9.1. تحليل المخاطر والمعايير
1.9.1. مدى المخاطر
2.9.1. الأصول
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. إطار الأمن السيبراني NIST
2.10.1. وكالة الاتحاد الأوروبي للأمن السيبراني
3.10.1. منظمة الدول الأمريكية
4.10.1. UNASUR - PROSUR

الوحدة 2. أمان Host

1.2. نسخ احتياطية
1.1.2. استراتيجيات النسخ الاحتياطية
2.1.2. أدوات ويندوز
3.1.2. أدوات لنظام Linux
4.1.2. أدوات لنظام MacOS
2.2. برنامج مكافحة الفيروسات للمستخدم
1.2.2. أنواع مضادات الفيروسات
2.2.2. مضاد فيروسات Windows
3.2.2. مضاد فيروسات Linux
4.2.2. مضاد فيروسات لنظام MacOS
5.2.2. مضاد فيروسات للهواتف الذكية smartphones
3.2. أجهزة كشف التسلل - HIDS
1.3.2. طرق كشف التسلل
2.3.2. Sagan
3.3.2. Aide
4.3.2. Rkhunter
4.2. Firewall محلى
1.4.2. Firewalls لـ Windows
2.4.2. Firewalls لـ Linux
3.4.2. Firewalls لـ MacOS
5.2. مديرى كلمات المرور
1.5.2. Password
2.5.2. LastPass
3.5.2. KeePass
4.5.2. StickyPassword
5.5.2. RoboForm
6.2. أجهزة كشف التصيد phishing
1.6.2. الكشف اليدوي عن التصيد
2.6.2. أدوات antiphishing
7.2. Spyware
1.7.2. آليات التجنب
2.7.2. أدوات مكافحة برامج التجسس antispyware
8.2. أجهزة التتبع
1.8.2. تدابير لحماية النظام
2.8.2. أدوات مكافحة التعقب
9.2. EDR End Point Detection and Response
1.9.2. سلوك نظام كشف نقطة النهاية والاستجابة لها
2.9.2. الاختلافات بين كشف نقطة النهاية والاستجابة لها ومكافحة الفيروسات
3.9.2. مستقبل أنظمة كشف نقطة النهاية والاستجابة لها
10.2. السيطرة على تثبيت software
1.10.2. المستودعات ومحلات البرمجيات
2.10.2. قوائم البرامج المسموح بها أو المحظورة
3.10.2. معايير التحديث
4.10.2. امتيازات تثبيت البرامج

الوحدة 3. أمان الشبكة (المحيط)

1.3. أنظمة الكشف عن التهديدات والوقاية منها
1.1.3. الإطار العام للحوادث الأمنية
2.1.3. أنظمة الدفاع الحالية: Defense in Depth ومركز العمليات الأمنية
3.1.3. معماريات الشبكات الحالية
4.1.3. أنواع أدوات الكشف والوقاية من الحوادث
1.4.1.3 أنظمة قائمة على شبكات
2.4.1.3 أنظمة قائمة على المضيف
3.4.1.3 أنظمة مركزية
5.1.3. الاتصال واكتشاف الحالات/المضيفين والحاويات واللاسيرفرات

.2.3 Firewall

.1.2.3 أنواع firewalls

.2.2.3 الهجمات والتخفيف من آثارها

.3.2.3 Firewalls الشائعة فى نواة (نظم تشغيل) kernel لينيكس

UFW 1.3.2.3

iptables و Nftables 2.3.2.3

Firewalld 3.3.2.3

.4.2.3 أنظمة الكشف على أساس سجلات النظام

TCP Wrappers أغلفة بروتوكول التحكم بالنقل 1.4.2.3

BlockHosts و DenyHosts 2.4.2.3

ban2Fai 3.4.2.3

.3.3 أنظمة كشف التسلل والوقاية منه

.1.3.3 الهجمات على أنظمة كشف التسلل وأنظمة الوقاية منه

.2.3.3 أنظمة كشف التسلل وأنظمة الوقاية منه

نظام كشف التسلل الأكثر شعبية 1.2.3.3

موتور كشف ومنع التسلل 2.2.3.3

.4.3 Firewalls جدران الحماية من الجيل القادم

.1.4.3 الاختلافات بين الجيل القادم من جدران الحماية وجدار الحماية التقليدي

.2.4.3 القدرات الأساسية

.3.4.3 حلول الأعمال

.4.4.3 جدران الحماية للخدمات السحابية cloud

بنية VPC السحابية 1.4.4.3

سحابة ACLs 2.4.4.3

Security Group 3.4.4.3

.5.3 Proxy

.1.5.3 أنواع proxy

.2.5.3 استخدام proxy. المميزات والعيوب

.6.3 محركات مكافحة الفيروسات

.1.6.3 السياق العام للبرامج الضارة وبطاقات

.2.6.3 مشاكل محرك مكافحة الفيروسات

.7.3 أنظمة حماية البريد

.1.7.3 مكافحة البريد الغير مرغوب فيه Antispam

القوائم السوداء والبيضاء 1.1.7.3

مرشحات بايزي 2.1.7.3

Mail Gateway MGW .2.7.3

.8.3 المعلومات الأمنية وإدارة الأحداث

.1.8.3 المكونات والعمارة

.2.8.3 قواعد الارتباط وحالات الاستخدام

.3.8.3 التحديات الحالية للمعلومات الأمنية وإدارة الأحداث

.9.3 التنسيق الأمني والأتمتة والاستجابة

.1.9.3 SOAR و SIEM: أعداء أو حلفاء

.2.9.3 مستقبل أنظمة التنسيق الأمني والأتمتة والاستجابة

.10.3 نظم أخرى قائمة في الشبكات

.1.10.3 جدار الحماية لتطبيقات الويب

.2.10.3 التحكم في الوصول إلى الشبكة

.3.10.3 HoneyPots و HoneyNets

.4.10.3 وسيط أمان الوصول إلى السحابة

الوحدة 4. أمن الهواتف الذكية smartphones

.1.4 عالم الأجهزة النقالة

.1.1.4 أنواع منصات الهواتف المحمولة

.2.1.4 أجهزة Ios

.3.1.4 أجهزة Android

.2.4 إدارة أمن الأجهزة المحمولة

.1.2.4 فتح مشروع أمان تطبيقات الويب على الأجهزة المحمولة

أهم 10 نقاط ضعف 1.1.2.4

.2.2.4 الاتصالات والشبكات وأنماط الاتصال

.3.4 الجهاز المحمول في بيئة الأعمال

.1.3.4 المخاطر

.2.3.4 سياسات الأمن

.3.3.4 مراقبة الاجهزة

.4.3.4 إدارة الأجهزة المحمولة

.4.4 خصوصية المستخدم وأمن البيانات

.5.4 حالة المعلومات

.6.4 حماية البيانات والسرية

.1.6.4 أذونات

التشفير 1.1.6.4

2.6.4. تخزين البيانات بشكل آمن
1.2.6.4 تخزين آمن في iOS
2.2.6.4 تخزين آمن في Android
4.4.4. الممارسات الجيدة في تطوير التطبيقات
7.4. نقاط الضعف ونواقل الهجوم
1.7.4. نقاط الضعف
2.7.4. نواقل الهجوم
1.2.7.4 البرامج الضارة
2.2.7.4 استخراج البيانات
3.2.7.4 التلاعب بالبيانات
8.4. التهديدات الرئيسية
1.8.4. مستخدم غير مجبر
2.8.4. البرامج الضارة
1.2.8.4 أنواع البرامج الضارة malware
3.8.4. الهندسة الاجتماعية
4.8.4. تسرب البيانات
5.8.4. سرقة المعلومات
6.8.4. الشبكات اللاسلكية wi-fi غير آمنة
7.8.4. برامج غير محدثة
8.8.4. تطبيقات خبيثة
9.8.4. كلمات مرور ضعيفة
10.8.4. إعدادات أمان ضعيفة أو غير موجودة
11.8.4. الوصول المادي
12.8.4. فقدان أو سرقة الجهاز
13.8.4. سرقة الهوية (النزاهة)
14.8.4. تشفير ضعيف أو مكسور
15.8.4. رفض الخدمة (DoS)
9.4. الهجمات الرئيسية
1.9.4. هجمات phishing
2.9.4. الهجمات المتعلقة بأساليب الاتصال
3.9.4. هجمات smishing
4.9.4. هجمات Criptojacking
5.9.4. Man in The Middle

10.4. القرصنة Hacking
1.10.4. Rooting و jailbreaking
2.10.4. تشريح هجوم محمول
1.2.10.4 انتشار التهديد
2.2.10.4 تركيب البرمجيات الخبيثة على الجهاز
3.2.10.4 المثابرة
4.2.10.4 تنفيذ الحمولة واستخراج المعلومات
3.10.4. Hacking أجهزة iOS: الآليات والأدوات
4.10.4. Hacking أجهزة Android: الآليات والأدوات
11.4. اختبارات الاختراق
1.11.4. iOS PenTesting
2.11.4. Android pentesting
3.11.4. الأدوات
12.4. الحماية والأمن
1.12.4. اعدادات الامان
1.1.12.4 في أجهزة iOS
2.1.12.4 في أجهزة Android
2.12.4. إجراءات السلامة
3.12.4. أدوات الحماية

الوحدة 5. الأمن في إنترنت الأشياء IoT

1.5. الأجهزة
1.1.5. أنواع الأجهزة
2.1.5. هياكل قياسية
1.2.1.5 مشروع الشراكة العالمية
2.2.1.5 المنتدى العالمي لإنترنت الأشياء IoTWF
3.1.5. بروتوكولات التطبيق
4.1.5. تقنيات الاتصال
2.5. أجهزة إنترنت الأشياء. مجالات التطبيق
1.2.5. SmartHome
2.2.5. SmartCity
3.2.5. وسائل النقل
4.2.5. الأجهزة القابلة للارتداء Wearables
5.2.5. قطاع الصحة
6.2.5. إنترنت الأشياء

3.5. بروتوكولات الاتصال
1.3.5. برتوكول MQTT
2.3.5. فتح بروتوكول تحالف المحمول
3.3.5. بروتوكول إدارة أجهزة تحالف الجوال المفتوح OMA-DM
4.3.5. التقرير الفني 069
4.5. SmartHome
1.4.5. أتمتة المنزل
2.4.5. شبكات التواصل
3.4.5. الأجهزة المنزلية
4.4.5. المراقبة والأمن
5.5. SmartCity
1.5.5. الإضاءة
2.5.5. علم الارصاد الجوية
3.5.5. الأمان
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 Wearables
1.7.5. ملابس ذكية
2.7.5. مجوهرات ذكية
3.7.5. الساعات الذكية
8.5. قطاع الصحة
1.8.5. مراقبة التمرين/معدل ضربات القلب
2.8.5. مراقبة المرضى وكبار السن
3.8.5. الغرسات
4.8.5. الروبوتات الجراحية
9.5. الاتصال
1.9.5. Wi-Fi/Gateway
2.9.5. بلوتوث
3.9.5. الاتصال المدمج
10.5. التأمين
1.10.5. الشبكات المعنية
2.10.5. مدير كلمات المرور
3.10.5. استخدام البروتوكولات المشفرة
4.10.5. نصائح الاستخدام

الوحدة 6. أخلاقيات Hacking

1.6. بيئة العمل
1.1.6. توزيعات Linux
1.1.1.6 كالي لينكس - الأمن الهجومي
Parrot OS 2.1.1.6
3.1.1.6 نظام تشغيل متعدد الاستخدامات Ubuntu
2.1.6. أنظمة المحاكاة الافتراضية
3.1.6. صندوق الحماية
4.1.6. نشر المختبرات
2.6. المنهجيات
1.2.6. دليل منهجية اختبار الأمان مفتوح المصدر OSSTM
2.2.6. مشروع أمان تطبيقات الويب المفتوحة OWASP
3.2.6. إطار الأمن السيبراني NIST
4.2.6. معيار أداء اختبار الاختراق PTES
5.2.6. إطار عمل مفتوح المصدر للتحليل والاختبار الأمني ISSAF
3.6. بصمات الأقدام Footprinting
1.3.6. الاستخبارات مفتوحة المصدر (OSINT)
2.3.6. البحث عن الخروقات ونقاط الضعف في البيانات
3.3.6. استخدام الأدوات السلبية
4.6. مسح الشبكات
1.4.6. أدوات المسح
1.1.4.6 اختصار مخطط الشبكة
2.1.4.6 مولد حزم مفتوح المصدر
3.1.4.6 أدوات المسح الأخرى
2.4.6. تقنيات المسح
3.4.6. تقنيات النهرب من IDSs firewall
4.4.6. Banner Grabbing
5.4.6. مخططات الشبكة

5.6. تعداد
1.5.6. تعداد نظام اسم المجال
2.5.6. تعداد نظام اسم المجال
3.5.6. تعداد بروتوكول إنترنت وسامبا (برنامج)
4.5.6. تعداد بروتوكول الوصول الى الدليل خفيف الوزن
5.5.6. تعداد بروتوكول إدارة الشبكات البسيطة
6.5.6. تقنيات التعداد الأخرى
6.6. فحص الثغرات الأمنية
1.6.6. حلول فحص الثغرات الأمنية
Qualys 1.1.6.6
2.1.6.6 نيساسNessus
3.1.6.6 إدارة التصحيح وفحص الثغرات الأمنية وتدقيق الشبكة
2.6.6. أنظمة تسجيل نقاط الضعف
1.2.6.6 نظام تسجيل نقاط الضعف المشتركة
2.2.6.6 نقاط الضعف والتعرضات الشائعة
7.6. هجمات الشبكات اللاسلكية
1.7.6. منهجيات hacking فى الشبكات اللاسلكية
Wi-Fi Discovery 1.1.7.6
2.1.7.6 تحليل حركة المرور
3.1.7.6 هجمات aircrack
1.3.1.7.6. هجمات الشبكة العنكبوتية العالمية
2.3.1.7.6. هجمات وصول محمي للشبكات اللاسلكية / الوصول المحمي بتقنية Wi-Fi 2
4.1.7.6 هجمات Evil Twin
5.1.7.6 هجمات إعداد واي فاي المحمي
6.1.7.6 التشويش
2.7.6. أدوات الأمن اللاسلكية
8.6. القرصنة على خوادم الويب
1.8.6. Cross Site Scripting
2.8.6. تزوير الطلب عبر المواقع
3.8.6. Session Hijacking
4.8.6. SQLinjection
9.6. استغلال نقاط الضعف
1.9.6. استخدام exploits المعروفة
2.9.6. استخدام metasploit
3.9.6. استخدامmalware
1.3.9.6 التعريف والنطاق
2.3.9.6 توليدالبرامج الضارة malware
3.3.9.6 تجاوز حلول مكافحة الفيروسات
10.6. المثابرة
1.10.6. تثبيت rootkits
2.10.6. استخدام ncat
3.10.6. استخدام المهام المجدولة للأبواب الخلفية backdoors
4.10.6. إنشاء المستخدم
5.10.6. نظام كشف التسلل القائم على المضيف

الوحدة 7. الهندسة العكسية

1.7. المجمعين
1.1.7. أنواع الأكواد
2.1.7. مراحل مجمع البيانات
3.1.7. جدول الرموز
4.1.7. مدير الأخطاء
5.1.7. مجموعة مترجمات جنو
2.7. أنواع التحليل في المجمعين
1.2.7. تحليل معجمي
1.1.2.7 المصطلحات
2.1.2.7 المكونات المعجمية
3.1.2.7 محلل معجمي القانون الكنسي LEX
2.2.7. التحليل النحوي
1.2.2.7 قواعد نحوية خالية من السياق
2.2.2.7 أنواع التحليل النحوي
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 المحللين النحويين
1.4.2.2.7. محللين مجزئ يسار يمين (Left To Right)
2.4.2.2.7. محلليين مجزئ يسار يمين
3.2.7. التحليل الدلالي
1.3.2.7 قواعد السمات
2.3.2.7 القواعد المنسوبة التي تحتوي على السمات المركبة S-atribuidas
3.3.2.7 القواعد المنسوبة التي تحتوي على السمات المركبة L-Atribuidas
3.7. هياكل بيانات المجمّع
1.3.7. المتغيرات
2.3.7. Arrays
3.3.7. المؤشرات
4.3.7. الهياكل
5.3.7. العناصر
4.7. هياكل الكود في المجمع
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 break
3.4.7. المهام
5.7. بنية الأجهزة 68x
1.5.7. بنية المعالج 86x
2.5.7. بنية البيانات في 86x
3.5.7. بنية الكود فى 86x
3.5.7. بنية الكود فى 86x
6.7. بنية أجهزة معمارية ARM
1.6.7. بنية معالج معمارية ARM
2.6.7. بنية بيانات معمارية ARM
3.6.7. بنية الكود في معمارية ARM

7.7. تحليل الشفرة الثابتة
1.7.7. المفككات
2.7.7. المفكك التفاعلي IDA
3.7.7. معيدي بناء الكود
8.7. تحليل الشفرة الديناميكية
1.8.7. تحليل السلوك
1.1.8.7 الاتصالات
2.1.8.7 المراقبة
2.8.7. مصححات كود Linux
3.8.7. مصححات كود Windows
9.7. صندوق الحماية
1.9.7. هندسة معمارية 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. صندوق الحماية في لينكس Sandbox en Linux
7.9.7. صنودق الحماية في ويندوزSandbox en Windows
8.9.7. صندوق الحماية Sandbox en MacOS في MacOS
9.9.7. صندوق الحماية Sandbox en Android في Android
10.7. تحليل البرامج الضارة
1.10.7. مناهج تحاليل malware
2.10.7. تقنيات تشويش البرمجيات الخبيثة malware
1.2.10.7 التعتيم على الملفات التنفيذية
2.2.10.7 تقييد بيئات التنفيذ
3.10.7. أدوات تحليل البرمجيات الخبيثة

الوحدة 8. التطوير الآمن

1.8. التطوير الآمن
1.1.8. الجودة والوظيفة والسلامة
2.1.8. السرية والنزاهة والتوافر
3.1.8. دورة حياة تطوير software
2.8. مرحلة المتطلبات
1.2.8. التحكم في المصادقة
2.2.8. السيطرة على الأدوار والامتيازات
3.2.8. المتطلبات الموجهة للمخاطر
4.2.8. اعتماد الامتيازات
3.8. مرحلة التحليل والتصميم
1.3.8. الوصول إلى المكونات وإدارة النظام
2.3.8. مسارات التدقيق
3.3.8. إدارة الجلسات
4.3.8. بيانات تاريخية
5.3.8. التعامل السليم مع الأخطاء
6.3.8. الفصل بين الوظائف
4.8. مرحلة التنفيذ والتشفير
1.4.8. ضمان البيئة التطويرية
2.4.8. إعداد الوثائق الفنية
3.4.8. تشفير آمن
4.4.8. أمن الاتصالات
5.8. الممارسات الجيدة للتشفير الآمن
1.5.8. التحقق من صحة البيانات المدخلة
2.5.8. تشفير بيانات الإخراج
3.5.8. أسلوب البرمجة
4.5.8. إدارة سجل التغيير
5.5.8. ممارسات التشفير
6.5.8. إدارة الأخطاء والسجلات
7.5.8. إدارة السجلات
8.5.8. إدارة الذاكرة
9.5.8. توحيد وإعادة استخدام وظائف الأمن
6.8. إعداد الخادم وتقويته
1.6.8. إدارة المستخدمين والمجموعات والأدوار على الخادم
2.6.8. تثبيت البرامج
3.6.8. Hardening الخادم
4.6.8. اعداد قوي لبيئة التطبيق
7.8. إعداد قاعدة البيانات وتقويتها
1.7.8. تحسين محرك قاعدة البيانات
2.7.8. إنشاء مستخدم خاص للتطبيق
3.7.8. تعيين الامتيازات الدقيقة للمستخدم hardening من قواعد البيانات
8.8. مرحلة الإختبار
1.8.8. مراقبة الجودة في الضوابط الأمنية
2.8.8. فحص الرمز على مراحل
3.8.8. التحقق من إدارة التهيئة
4.8.8. اختبار الصندوق الأسود
9.8. تحضير خطوة الإنتاج
1.9.8. مراقبة التغيير
2.9.8. تنفيذ إجراء خطوة إلى الإنتاج
3.9.8. تنفيذ إجراء rollback
4.9.8. الاختبارات في مرحلة ما قبل الإنتاج
10.8. مرحلة الصيانة
1.10.8. التأمين على أساس المخاطر
2.10.8. اختبارات صيانة سلامة الصندوق الأبيض
3.10.8. اختبارات صيانة سلامة الصندوق الاسود

الوحدة 9. التنفيذ العملي لسياسات الأمان في البرامج والأجهزة

1.9. التنفيذ العملي لسياسات الأمان في البرامج والأجهزة
1.1.9. تنفيذ التعرف والتفويض
2.1.9. تنفيذ تقنيات التعرف
3.1.9. إجراءات التصريح التقنية
2.9. تقنيات التعرف والتفويض
1.2.9. المُعرّف ورقم التعريف الشخصي (OTP)
2.2.9. رمز USB أو بطاقة PKI الذكية
3.2.9. مفتاح "الدفاع السري
4.2.9. تحديد الهوية بالتردد اللاسلكي النشط

3.9. السياسات الأمنية الخاصة بالوصول إلى البرامج والأنظمة
1.3.9. تنفيذ سياسات التحكم في الوصول
2.3.9. تنفيذ سياسات الوصول إلى الاتصالات
3.3.9. أنواع أدوات الأمان للتحكم في الوصول
4.9. إدارة وصول المستخدم
1.4.9. إدارة حقوق الوصول
2.4.9. الفصل بين الأدوار ووظائف الوصول
3.4.9. تطبيق حقوق الوصول في الأنظمة
5.9. التحكم في الوصول إلى الأنظمة والتطبيقات
1.5.9. قاعدة الحد الأدنى من الوصول
2.5.9. تقنيات تسجيل الدخول الآمن
3.5.9. سياسات أمان كلمات المرور
6.9. تقنيات نظام تحديد الهوية
1.6.9. الدليل النشط
2.6.9. OTP
3.6.9. PAP, CHAP
4.6.9. KERBEROS, DIAMETER, NTLM
7.9. ضوابط CIS لتأسيس النظام
1.7.9. ضوابط CIS الأساسية
2.7.9. الضوابط الرئيسية لـ CIS
3.7.9. ضوابط CIS التنظيمية
8.9. أمن العمليات
1.8.9. الحماية من الشفرات البرمجية الخبيثة
2.8.9. نسخ احتياطية
3.8.9. سجل النشاط والإشراف
9.9. إدارة الثغرات التقنية
1.9.9. نقاط الضعف التقنية
2.9.9. إدارة الثغرات التقنية
3.9.9. القيود على تثبيت software
10.9. تنفيذ ممارسات السياسة الأمنية
1.10.9. الثغرات المنطقية
2.10.9. تنفيذ السياسات الدفاعية

الوحدة 10. التحليل الجنائي

1.10. الحصول على البيانات ونسخها
1.1.10. الحصول على البيانات المتقلبة
1.1.1.10 معلومات النظام
2.1.1.10 معلومات الشبكة
3.1.1.10 ترتيب التقلب
2.1.10. الحصول على البيانات الثابتة
1.2.1.10 إنشاء صورة منسوخة
2.2.1.10 إعداد وثيقة لسلسلة الحيازة
3.1.10. طرق التحقق من صحة البيانات المكتسبة
1.3.1.10 منهجيات Linux
2.3.1.10 منهجيات Windows
2.10. تقييم تقنيات مكافحة الطب الشرعي وهزيمتها
1.2.10. أهداف تقنيات مكافحة الطب الشرعي
2.2.10. مسح البيانات
1.2.2.10 حذف البيانات والملفات
2.2.2.10 استرجاع الملفات
3.2.2.10 استرجاع الأقسام المحذوفة
3.2.10. الحماية بكلمة مرور
4.2.10. إخفاء المعلومات
5.2.10. الحذف الآمن للأجهزة
6.2.10. التشفير
3.10. التحليل الجنائي لنظام التشغيل
1.3.10. التحليل الجنائي لويندوز
2.3.10. التحليل الجنائي ل Linux
3.3.10. التحليل الجنائي لل Mac
4.10. التحليل الجنائي للشبكة
1.4.10. تحليل السجلات
2.4.10. ترابط البيانات
3.4.10. بحث الشبكة
4.4.10. الخطوات الواجب اتباعها في التحليل الجنائي للشبكة

5.10. التحليل الجنائي على الويب
1.5.10. التحقيق في هجمات الويب
2.5.10. كشف الهجمات
3.5.10. تعقب عناوين نظام منع الاختراق IPs
6.10. التحليل الجنائي لقواعد البيانات
1.6.10. التحليل الجنائي لل MSSQL
2.6.10. التحليل الجنائي لل MySQL
3.6.10. التحليل الجنائي لل PostgreSQL
4.6.10. التحليل الجنائي ل MongoDB
7.10. التحليل الجنائي لل Cloud
1.7.10. أنواع الجرائم فى Cloud
1.1.7.10 Cloudالسحابة كمشتبه
2.1.7.10 Cloudالسحابة كغرض
3.1.7.10. Cloudالسحابة كأداة
2.7.10. تحديات التحليل الجنائى فى Cloud
3.7.10. البحث فى خدمات التخزين Cloud
4.7.10. أدوات الادلة الجنائية Cloud
8.10. التحقيق في جرائم البريد الإلكتروني
1.8.10. أنظمة البريد
1.1.8.10 عملاء البريد
2.1.8.10 خادم البريد
3.1.8.10 خادم البريد الصادر SMTP
4.1.8.10 خادم 3POP
5.1.8.10 خادم روتوكول الوصول إلى رسائل الإنترنت
2.8.10. جرائم البريد
3.8.10. رسالة بريدية
1.3.8.10 رؤوس قياسية
2.3.8.10 رؤوس ممتدة
4.8.10. خطوات التحقيق في هذه الجرائم
5.8.10. أدوات جنائية للبريد الإلكتروني
9.10. التحليل الجنائي للهواتف المحمولة
1.9.10. شبكات خلوية
1.1.9.10. أنواع الشبكات
2.1.9.10. محتويات إثبات الاستلام CDR
2.9.10. وحدة تعريف المشترك (SIM)
3.9.10. الاستحواذ المنطقي
4.9.10. الاستحواذ المادي
5.9.10. اكتساب نظام الملفات
10.10. كتابة التقارير الجنائية والعرض التقديمي
1.10.10. الجوانب المهمة لتقرير الأدلة الجنائية
2.10.10. تصنيف الأنواع الأدلة الجنائية
3.10.10. دليل كتابة التقرير الجنائي
4.10.10. عرض التقرير الجنائي
1.4.10.10 التحضير المسبق للإدلاء بشهادة
2.4.10.10 شهادة
3.4.10.10 التعامل مع الوسائط

الوحدة 11. السلامة في التصميم وتطوير الأنظمة

1.11. نظم المعلومات
1.1.11. المجالات في نظام المعلومات
2.1.11. المكونات في نظام المعلومات
3.1.11. الأنشطة في نظام المعلومات
4.1.11. دورة حياة نظام المعلومات
5.1.11. الموارد في نظام المعلومات
2.11. نظم المعلومات الأنماط
1.2.11. أنواع نظام المعلومات
1.1.2.11 إدارة الأعمال
2.1.2.11 الاستراتيجية
3.1.2.11 حسب نطاق التطبيق
4.1.2.11 محددة
2.2.11. نظم المعلومات أمثلة حقيقية
3.2.11. التطور في نظام المعلومات: المراحل
4.2.11. المنهجيات في نظم المعلومات
3.11. الأمان في نظم المعلومات. الآثار القانونية
1.3.11. الدخول الى البيانات
2.3.11. التهديدات الأمنية نقاط الضعف
3.3.11. الآثار القانونية: الجرائم
4.3.11. إجراءات الصيانة لنظام المعلومات

4.11. الأمان في نظام المعلومات. بروتوكولات الأمن
1.4.11. الأمان في نظام المعلومات
1.1.4.11 النزاهة
2.1.4.11 السرية
3.1.4.11 التوفر
4.1.4.11 المصادقة
2.4.11. خدمات أمنية
3.4.11. بروتوكولات أمن المعلومات. الأنماط
4.4.11. الحساسية في نظام المعلومات
5.11. الأمان في نظام المعلومات. تدابير وأنظمة مراقبة الدخول
1.5.11. إجراءات السلامة
2.5.11. نوع التدابير الاحتياطية
1.2.5.11 الوقاية
2.2.5.11 الكشف
3.2.5.11 التصحيح
3.5.11. أنظمة التحكم في الدخول. الأنماط
4.5.11. علم التشفير
6.11. أمن الشبكات والإنترنت
1.6.11. جدران الحماية
2.6.11. التعريف الرقمي
3.6.11. الفيروسات والديدان
4.6.11. القرصنة Hacking
5.6.11. أمثلة وحالات حقيقية
7.11. الجرائم الحاسوبية
1.7.11. الجريمة الحاسوبية
2.7.11. الجرائم الحاسوبية الأنماط
3.7.11. الجرائم الحاسوبية الهجوم الأنماط
4.7.11. حالة الواقع الافتراضي
5.7.11. لمحات عن الجناة والضحايا. تجريم الجريمة
6.7.11. الجرائم الحاسوبية أمثلة وحالات حقيقية

8.11. مخططات الأمان في نظام المعلومات
1.8.11. خطة الأمن الأهداف
2.8.11. خطة الأمن المخطط
3.8.11. خطة المخاطر. التحليلات
4.8.11. سياسات الأمن التنفيذ في المنظمة
5.8.11. خطة الأمن التنفيذ في المنظمة
6.8.11. الإجراءات الأمنية الأنواع
7.8.11. خطة الأمن الأمثلة
9.11. خطة الطوارئ
1.9.11. خطة الطوارئ المهام
2.9.11. خطة الطوارئ العناصر والأهداف
3.9.11. خطة الطوارئ في المنظمة. التنفيذ
4.9.11. خطة الطوارئ الأمثلة
10.11. حوكمة أمن نظم المعلومات
1.10.11. تنظيمات قانونية
2.10.11. المعايير
3.10.11. الشهادات
4.10.11. التقنيات

الوحدة 12. هياكل ونماذج أمن المعلومات

1.12. بنية أمن المعلومات
1.1.12. SGSI/PDS
2.1.12. التوافق الاستراتيجي
3.1.12. إدارة المخاطر
4.1.12. قياس الأداء
2.12. نماذج أمن المعلومات
1.2.12. استناداً إلى السياسات الأمنية
2.2.12. استنادًا إلى أدوات الحماية
3.2.12. قائمة على الفريق
3.12. نموذج الأمن. المكونات الرئيسية
1.3.12. تعريف المخاطر
2.3.12. تعريف الضوابط
3.3.12. التقييم المستمر لمستويات المخاطر
4.3.12. خطة التوعية للموظفين والموردين والشركاء وغيرهم

4.12. عمليات ادارة المخاطر
1.4.12. تحديد الأصول
2.4.12. الاستجابة للتهديد
3.4.12. تقييم المخاطر
4.4.12. تحديد أولويات الضوابط
5.4.12. إعادة التقييم والمخاطر المتبقية
5.12. إجراءات الأعمال لأمن المعلومات
1.5.12. عمليات الأعمال
2.5.12. تقييم المخاطر بناءً على معايير العمل
3.5.12. تحليل أثر الأعمال
4.5.12. العمليات التجارية وأمن المعلومات
6.12. عملية التحسين المستمر
1.6.12. دورة الحياة Deming
1.1.6.12 للتخطيط
2.1.6.12 الفعل
3.1.6.12 تحقق
4.1.6.12 الفعل
7.12. معماريات الأمن
1.7.12. اختيار التقنيات وتجانسها
2.7.12. إدارة الهوية المصادقة
3.7.12. إدارة الوصول. الإذن
4.7.12. أمن البنية التحتية للشبكة
5.7.12. تقنيات وحلول التشفير
6.7.12. أمن المعدات الطرفية (EDR)
8.12. الإطار التنظيمي
1.8.12. اللوائح القطاعية
2.8.12. الشهادات
3.8.12. التشريع
9.12. معيار ISO 27001
1.9.12. التنفيذ
2.9.12. الشهادات
3.9.12. عمليات التدقيق واختبارات الاختراق
4.9.12. إدارة المخاطر
5.9.12. تصنيف المعلومات
10.12. تشريعات الخصوصية. RGPD GDPR
1.10.12. نطاق اللائحة العامة لحماية البيانات (RGPD)
2.10.12. بيانات شخصية
3.10.12. الأدوار في معالجة البيانات الشخصية
4.10.12. حقوق ARCO
5.10.12. El DPO. المهام

الوحدة 13. نظام إدارة أمن المعلومات

1.13. أمن المعلومات الجوانب الرئيسية
1.1.13. أمن المعلومات
1.1.1.13 السرية
2.1.1.13 النزاهة
3.1.1.13 التوفر
4.1.1.13 تدابير أمن المعلومات
2.13. نظام إدارة أمن المعلومات
1.2.13. نماذج إدارة أمن المعلومات
2.2.13. وثائق تنفيذ نظام إدارة أمن المعلومات
3.2.13. مستويات وضوابط نظام إدارة أمن المعلومات
3.13. القواعد والمعايير الدولية
1.3.13. المعايير الدولية لأمن المعلومات
2.3.13. أصل وتطور المعيار
3.3.13. معايير إدارة أمن المعلومات الدولية
4.3.13. معايير مرجعية أخرى
4.13. معيار ISO ISO / IEC 27000
1.4.13. الغرض والنطاق
2.4.13. بنية المادة
3.4.13. الشهادات
4.4.13. مراحل الاعتمادات
5.4.13. مزايا معيار ISO ISO / IEC 27000
5.13. تصميم وتنفيذ نظام أمن المعلومات الشامل
1.5.13. مراحل تنفيذ نظام أمن المعلومات الشامل
2.5.13. خطط استمرارية الأعمال

6.13. المرحلة الأولى: التشخيص
1.6.13. التشخيص الأولي
2.6.13. تحديد مستوى التقسيم الطبقي
3.6.13. مستوى الامتثال للمعايير/القواعد
7.13. المرحلة الثانية: الإعداد
1.7.13. سياق المنظمة
2.7.13. تحليل لوائح السلامة المعمول بها
3.7.13. نطاق نظام أمن المعلومات الشامل
4.7.13. مراحل تنفيذ نظام أمن الشامل
5.7.13. أهداف نظام أمن المعلومات الشامل
8.13. المرحلة الثالثة: التخطيط
1.8.13. تصنيف الأصول
2.8.13. تقييم المخاطر
3.8.13. تحديد التهديدات والمخاطر
9.13. المرحلة الرابعة: التنفيذ والرصد
1.9.13. تحليل النتائج
2.9.13. توزيع المسؤوليات
3.9.13. توقيت خطة العمل
4.9.13. المراقبة والتدقيق
10.13. السياسات الأمنية في إدارة الحوادث
1.10.13. المراحل
2.10.13. تصنيف الحوادث
3.10.13. إدارة الحوادث وإجراءاتها

الوحدة 14. إدارة الأمن IT

1.14. إدارة الأمن
1.1.14. العمليات الأمنية
2.1.14. الجوانب القانونية والتنظيمية
3.1.14. مؤهلات العمل
4.1.14. إدارة المخاطر
5.1.14. إدارة الهوية والوصول
2.14. هيكل المنطقة الأمنية. مكتب مدير أمن المعلومات
1.2.14. الهيكل التنظيمي موقع رئيس أمن المعلومات في الهيكلية CISO
2.2.14. خطوط الدفاع
3.2.14. المخطط التنظيمي لمكتب رئيس أمن المعلومات CISO
4.2.14. إدارة الميزانية
3.14. حكومة الأمن
1.3.14. اللجنة الأمنية
2.3.14. لجنة مراقبة المخاطر
3.3.14. لجنة التدقيق
4.3.14. لجنة الأزمات
4.14. الحكومة الأمنية. المهام
1.4.14. السياسات والمعايير
2.4.14. خطة الأمن
3.4.14. لوحات التحكم
4.4.14. التوعية والتدريب
5.4.14. أمن سلسلة التوريد
5.14. العمليات الأمنية
1.5.14. إدارة الهوية والوصول
2.5.14. تكوين قواعد أمان الشبكة. جدران الحماية
3.5.14. إدارة منصة IDS/IPS
4.5.14. فحص الثغرات الأمنية
6.14. إطار عمل الأمن السيبراني. NIST CSF
1.6.14. منهجية NIST
1.1.6.14 تحديد
2.1.6.14 الحماية
3.1.6.14 الكشف
4.1.6.14 رد
5.1.6.14 التعافي
7.14. مركز العمليات الأمنية المهام
1.7.14. الحماية Red Team، pentesting، threat intelligence
2.7.14. الكشف SIEM، user behavior analytics، fraud prevention
3.7.14. رد

8.14. التدقيق الأمني
1.8.14. اختبار التطفل
2.8.14. تمارين الفريق الأحمر
3.8.14. تدقيق شفرة المصدر. التطوير الآمن
4.8.14. سلامة المكونات (سلسلة توريد البرمجيات)software supply chain
5.8.14. التحليل الجنائي
9.14. الاستجابة للحوادث
1.9.14. تحضير
2.9.14. الكشف والتحليل والإبلاغ
3.9.14. الاحتواء والاستئصال والتعافي
4.9.14. نشاط ما بعد الحادث
1.4.9.14 الاحتفاظ بالأدلة
2.4.9.14 التحليل الجنائي
3.4.9.14 إدارة الثغرات
5.9.14. الإرشادات الرسمية لإدارة الحوادث السيبرانية
10.14. إدارة الثغرات الأمنية
1.10.14. فحص الثغرات الأمنية
2.10.14. تقييم الثغرات الأمنية
3.10.14. تأسيس النظام
4.10.14. نقاط ضعف اليوم صفر. يوم الصفر

الوحدة 15. سياسات إدارة الحوادث الأمنية

1.15. سياسات إدارة حوادث أمن المعلومات وتحسيناتها
1.1.15. إدارة الحوادث
2.1.15. المسؤوليات والإجراءات
3.1.15. الإشعار بالحدث
2.15. أنظمة كشف التسلل والوقاية منه
1.2.15. بيانات تشغيل النظام
2.2.15. أنواع أنظمة كشف التطفل
3.2.15. معايير تحديد موقع IDS / IPS
3.15. الاستجابة للحوادث الأمنية
1.3.15. إجراءات جمع البيانات
2.3.15. عملية التحقق من التطفل
3.3.15. هيئات فريق الاستجابة للطوارئ الحاسوبية
4.15. عملية الإخطار بمحاولة التطفل وإدارتها
1.4.15. المسؤوليات في عملية الإخطار
2.4.15. تصنيف الحوادث
3.4.15. عملية الحل والاسترداد
5.15. التحليل الجنائي كسياسة أمنية
1.5.15. الأدلة المتطايرة وغير المتطايرة
2.5.15. تحليل وجمع الأدلة الإلكترونية
1.2.5.15 تحليل الأدلة الإلكترونية
2.2.5.15 جمع الأدلة الإلكترونية
6.15. أدوات تجربة العملاء أنظمة كشف التطفل والوقاية منه (IDS/IPS)
1.6.15. Snort
2.6.15. Suricata
3.6.15. Solar-Winds
7.15. أدوات مركزية الحدث
1.7.15. إدارة المعلومات الأمنية (SIM)
2.7.15. إدارة الأحداث الأمنية (SEM)
3.7.15. SIEM (إدارة المعلومات الأمنية والأحداث)
8.15. دليل أمان CCN-STIC 817
1.8.15. إدارة الحوادث السيبرانية
2.8.15. المقاييس والمؤشرات
9.15. NIST / SP 800-61
1.9.15. القدرة على الاستجابة للحوادث الأمنية الحاسوبية
2.9.15. التعامل مع الحادث
3.9.15. التنسيق ومشاركة المعلومات
10.15. معايير ISO 27035
1.10.15. معايير ISO 27035. مبادئ إدارة الحوادث
2.10.15. إرشادات لتطوير خطة إدارة الحوادث
3.10.15. إرشادات عمليات الاستجابة للحوادث

الوحدة 16. تحليل المخاطر وبيئة أمن تكنولوجيا المعلومات

1.16. تحليل البيئة
1.1.16. تحليل الموقف التعليمى
1.1.1.16 بيئة VUCA
1.1.1.1.16. متقلبة
2.1.1.1.16. ضبابية
3.1.1.1.16. معقدة
4.1.1.1.16. غامضة
2.1.1.16 بيئة BANI
1.2.1.1.16. هشة
2.2.1.1.16. قلقة
3.2.1.1.16. غير خطية
4.2.1.1.16. غير مفهوم
2.1.16. تحليل البيئة العامة. PESTEL
1.2.1.16 السياسي
2.2.1.16 اقتصادية
3.2.1.16 اجتماعي
4.2.1.16 التقنيات
5.2.1.16 إيكولوجي / بيئي
6.2.1.16 الشرعية
3.1.16. تحليل الوضع الداخلي. التحليل الرباعي SWOT
1.3.1.16 الأهداف
2.3.1.16 التهديدات
3.3.1.16 الفرص
4.3.1.16 نقاط القوة
2.16. المخاطر وعدم اليقين
1.2.16. المخاطر
2.2.16. إدارة المخاطر
3.2.16. معايير إدارة المخاطر
3.16. مراجعة إدارة الجودة ISO 31000: 2018
1.3.16. عنصر
2.3.16. البداية
3.3.16. الإطار المرجعي
4.3.16. العملية
4.16. منهجية تحليل وإدارة مخاطر نظم المعلومات (MAGERIT)
1.4.16. منهجية MAGERIT
1.1.4.16 الأهداف
2.1.4.16 منهج
3.1.4.16 العوامل
4.1.4.16 التقنيات
5.1.4.16 الأدوات المتاحة (PILAR)
5.16. نقل المخاطر السيبرانية
1.5.16. نقل المخاطر
2.5.16. المخاطر السيبرانية. الأنماط
3.5.16. التأمين ضد المخاطر السيبرانية
6.16. منهجيات مرنة لإدارة المخاطر
1.6.16. المنهجيات الرشيقة
2.6.16. Scrum لإدارة المخاطر
3.6.16. AGILE Risk Management
7.16. تقنيات إدارة المخاطر
1.7.16. الذكاء الاصطناعي المطبق على إدارة المخاطر
2.7.16. Blockchain والتشفير. طرق الحفاظ على القيمة
3.7.16. الحوسبة الكمية الفرصة أو التهديد
8.16. تخطيط مخاطر تكنولوجيا المعلومات على أساس المنهجيات الرشيقة
1.8.16. تمثيل الاحتمالية والتأثير في البيئات الرشيقة
2.8.16. المخاطر كتهديد للقيمة
3.8.16. إعادة التطوير في إدارة المشاريع الرشيقة والعمليات القائمة على مؤشرات الأداء الرئيسية
9.16. Risk driven في إدارة المخاطر
1.9.16. Risk driven
2.9.16. Risk driven في إدارة المخاطر
3.9.16. تطوير نموذج لإدارة الأعمال قائم على المخاطر
10.16. الابتكار والتحول الرقمي في إدارة مخاطر تكنولوجيا المعلومات
1.10.16. الإدارة الرشيقة للمخاطر كمصدر للابتكار في الأعمال التجارية
2.10.16. تحويل البيانات إلى معلومات مفيدة في اتخاذ القرار
3.10.16. نظرة شمولية للمؤسسة من خلال المخاطر

الوحدة 17. السياسات الأمنية لتحليل التهديدات في أنظمة الكمبيوتر

1.17. إدارة التهديدات في سياسات الأمان
1.1.17. إدارة المخاطر
2.1.17. المخاطر الأمنية
3.1.17. منهجيات في إدارة التهديدات
4.1.17. تطبيق المنهجيات
2.17. مراحل إدارة التهديدات
1.2.17. التعرف
2.2.17. التحليلات
3.2.17. موقع
4.2.17. تدابير الحماية
3.17. أنظمة التدقيق لتحديد موقع التهديد
1.3.17. تصنيف وتدفقالمعلومات
2.3.17. تحليل العمليات الضعيفة
4.17. تصنيف المخاطر
1.4.17. أنواع المخاطر
2.4.17. حساب احتمالات التهديد
3.4.17. المخاطر المتبقية
5.17. علاج المخاطر
1.5.17. تنفيذ تدابير الحماية
2.5.17. التحويل أو الاستلام
6.17. السيطرة على المخاطر
1.6.17. العملية المستمرة لإدارة المخاطر
2.6.17. تنفيذ مقاييس الأمان
3.6.17. النموذج الاستراتيجي لمقاييس أمن المعلومات
7.17. المنهجيات العملية لتحليل التهديدات والسيطرة عليها
1.7.17. دليل التهديدات
2.7.17. دليل تدابير الرقابة
3.7.17. دليل الضمانات
8.17. معايير ISO 27005
1.8.17. تحديد المخاطر
2.8.17. تحليل المخاطر
3.8.17. تقييم المخاطر
9.17. مصفوفة المخاطر والتأثيرات والتهديدات
1.9.17. البيانات والأنظمة والموظفين
2.9.17. احتمالية التهديد
3.9.17. حجم الضرر
10.17. تصميم المراحل والعمليات في تحليل التهديدات
1.10.17. تحديد العناصر الحرجة في المنظمة
2.10.17. تحديد التهديدات والآثار
3.10.17. تحليل الأثر والمخاطر
4.10.17. المنهجيات

الوحدة 18. التنفيذ العملي للسياسات الأمنية ضد الهجمات

1.18. System Hacking
1.1.18. المخاطر ونقاط الضعف
2.1.18. التدابير المضادة
2.18. DoS في الخدمات
1.2.18. المخاطر ونقاط الضعف
2.2.18. التدابير المضادة
3.18. Session Hijacking
1.3.18. عملية Hijacking
2.3.18. التدابير المضادة لعملية Hijacking
4.18. تجاوز أنظمة IDS، الجدران النارية (Firewalls)، وفخاخ Honeypots
1.4.18. تقنيات التجاوز
2.4.18. تنفيذ التدابير المضادة
5.18. Hacking Web Servers
1.5.18. الهجمات على خوادم الويب
2.5.18. تنفيذ تدابير الدفاع
6.18. Hacking Web Applications
1.6.18. الهجمات على تطبيقات الويب
2.6.18. تنفيذ تدابير الدفاع
7.18. Hacking Wireless Networks
1.7.18. نقاط الضعف في شبكات wifi
2.7.18. تنفيذ تدابير الدفاع

8.18. Hacking Mobile Platforms
1.8.18. نقاط ضعف منصات الهواتف المحمولة
2.8.18. تنفيذ التدابير المضادة
9.18. برامج الفدية الخبيثة
1.9.18. الثغرات الأمنية المسببة لبرامج الفدية Ransomwareالخبيثة
2.9.18. تنفيذ التدابير المضادة
10.18. الهندسة الاجتماعية
1.10.18. أنواع الهندسة الاجتماعية
2.10.18. التدابير المضادة للهندسة الاجتماعية

الوحدة 19. التشفير في تكنولوجيا المعلومات

1.19. علم التشفير
1.1.19. علم التشفير
2.1.19. أساسيات حسابية
2.19. علم التشفير
1.2.19. علم التشفير
2.2.19. تحليل الشفرات
3.2.19. إخفاء المعلومات وتحليل إخفاء المعلومات
3.19. بروتوكولات التشفير
1.3.19. الكتل الأساسية
2.3.19. البروتوكولات الأساسية
3.3.19. البروتوكولات الوسيطة
4.3.19. البروتوكولات المتقدمة
5.3.19. البروتوكولات الخارجية
4.19. تقنيات التشفير
1.4.19. طول المفتاح
2.4.19. الإدارة الرئيسية
3.4.19. أنواع الخوارزميات
4.4.19. ملخص الوظائف. تجزئة
5.4.19. مولدات الأرقام العشوائية الزائفة
6.4.19. استخدام الخوارزميات
5.19. التشفير المتماثل
1.5.19. شفرات التشفير المجمعة
2.5.19. DES Data Encryption Standard
3.5.19. خوارزمية 4RC
4.5.19. AES Advanced Encryption Standard
5.5.19. مزيج من شفرات الكتل
6.5.19. اشتقاق المفتاح
6.19. التشفير غير المتماثل
1.6.19. Diffie-Hellman
2.6.19. DSA (خوارزمية التوقيع الرقمي)
3.6.19. RSA Rivest، Shamir y Adleman
4.6.19. المنحنى البيضاوي
5.6.19. التشفير غير المتماثل الأنماط
7.19. شهادات رقمية
1.7.19. التوقيع الرقمي
2.7.19. شهادات 509X
3.7.19. البنية التحتية للمفاتيح العامة (PKI)
8.19. التنفيذ
1.8.19. Kerberos
2.8.19. IBM CCA
3.8.19. Pretty Good Privacy PGP
4.8.19. ISO Authentication Framework
5.8.19. SSL y TLS
6.8.19. Tarjetas inteligentes en medios de pago EMV
7.8.19. بروتوكولات الاتصال الهاتفي عبر الهاتف المحمول
8.8.19. Blockchain
9.19. إخفاء المعلومات
1.9.19. إخفاء المعلومات
2.9.19. تحليل التخفي
3.9.19. تطبيقات واستخدامات
10.19. التشفير الكمي
1.10.19. خوارزميات الكم
2.10.19. حماية الخوارزميات من الحوسبة الكمية
3.10.19. توزيع المفاتيح الكمية

الوحدة 20. إدارة الهوية والوصول في أمن تكنولوجيا المعلومات

1.20. إدارة الهوية والوصول (IAM)
1.1.20. الهوية الرقمية
2.1.20. إدارة الهوية
3.1.20. اتحاد الهويات
2.20. التحكم في الوصول المادي
1.2.20. أنظمة الحماية
2.2.20. أمن المناطق
3.2.20. مرافق الاسترداد
3.20. التحكم في الوصول المنطق
1.1.20. المصادقة الأنماط
2.1.20. بروتوكولات التوثيق
3.1.20. هجمات المصادقة
4.20. التحكم في الوصول المنطق مصادقة MFA
1.4.20. التحكم في الوصول المنطق مصادقة MFA
2.4.20. كلمة المرور: الأهمية
3.4.20. هجمات المصادقة
5.20. التحكم في الوصول المنطق المصادقة البيومترية
1.5.20. التحكم في الوصول المنطقي. المصادقة البيومترية
1.1.5.20 المصادقة البيومترية المتطلبات
2.5.20. التشغيل
3.5.20. أدوات وتقنيات
6.20. نظام إدارة الشركة
1.6.20. Single sign on
2.6.20. Kerberos
3.6.20. أنظمة AAA
7.20. أنظمة إدارة المصادقة: أنظمة AAA
1.7.20. TACACS
2.7.20. RADIUS
3.7.20. DIAMETER
8.20. خدمات التحكم في الوصول
1.8.20. FW-حائط الحماية من الحرائق FIREWALL
2.8.20. الشبكات الخاصة الافتراضية VPN
3.8.20. IDS- أنظمة الكشف عن التسلل
9.20. أنظمة التحكم في الوصول إلى الشبكة
1.9.20. التحكم في الوصول إلى الشبكة
2.9.20. الهندسة المعمارية والعناصر
3.9.20. التشغيل والتوحيد القياسي
10.20. دخول الشبكات اللاسلكية
1.10.20. أنواع الشبكات اللاسلكية
2.10.20. أمان الشبكة اللاسلكية
3.10.20. هجمات الشبكات اللاسلكية

الوحدة 21. الأمن في الاتصالات وتشغيل البرامج

1.21. أمن الكمبيوتر في الاتصالات وتشغيل البرامج
1.1.21. أمان تكنولوجيا المعلومات
2.1.21. الأمن السيبراني
3.1.21. أمان السحابة
2.21. أمن الكمبيوتر في الاتصالات وتشغيل البرامج الأنماط
1.2.21. الأمن المادي
2.2.21. الأمن المنطقي
3.21. أمن الاتصالات
1.3.21. العناصر الرئيسية
2.3.21. أمن الشبكة
3.3.21. أفضل الممارسات
4.21. الذكاء السيبراني
1.4.21. الهندسة الاجتماعية
2.4.21. Deep web
3.4.21. Phishing
4.4.21. البرامج الضارة

5.21. التطوير الآمن في الاتصالات وتشغيل البرامج
1.1.21. التطوير الآمن بروتوكول HTTP
2.1.21. التطوير الآمن دورة الحياة
3.1.21. التطوير الآمن أمان PHP
4.1.21. التطوير الآمن أمان NET
5.1.21. التطوير الآمن أفضل الممارسات
6.21. أنظمة إدارة أمن معلومات الاتصالات وتشغيل البرمجيات
1.6.21. GDPR
2.6.21. CUGBP Elav-like family member 27017
3.6.21. ISO 18/27017
7.21. تكنولوجيا SIEM
1.7.21. تكنولوجيا SIEM
2.7.21. تشغيل SOC
3.7.21. SIEM vendors موردو SIEM
8.21. دور الأمن في التعبير عن الذات
1.8.21. الأدوار في المنظمات
2.8.21. دور متخصصي إنترنت الأشياءIoT في الشركات
3.8.21. الشهادات المعترف بها في السوق
9.21. التحليل الجنائي
1.9.21. التحليل الجنائي
2.9.21. التحليل الجنائي المنهجية
3.9.21. التحليل الجنائي الأدوات والتنفيذ
10.21. الأمن السيبراني اليوم
1.10.21. الهجمات السيبرانية الرئيسية
2.10.21. توقعات التوظيف
3.10.21. التحديات

الوحدة 22. الأمان في البيئات السحابيةCloud

1.22. الأمن في بيئات Cloud Computing
1.1.22. الأمن في بيئات Cloud Computing
2.1.22. الأمن في بيئات Cloud Computing التهديدات والمخاطر الأمنية
3.1.22. الأمن في بيئات Cloud Computing. الجوانب الأمنية الأساسية
2.22. أنواع البنية التحتية Cloud
1.2.22. عامة
2.2.22. خاصة
3.2.22. هجينة
3.22. نموذج الإدارة المشتركة
1.3.22. ميزات الأمن التي يديرها البائع
2.3.22. العناصر التي يديرها العميل
3.3.22. تحديد الاستراتيجية الأمنية
4.22. الآليات الوقائية
1.4.22. نظام إدارة الشركة
2.4.22. نظام إدارة الإذن: سياسة الدخول
3.4.22. أنظمة الإدارة الرئيسية
5.22. تأمين الأنظمة
1.5.22. التأمين أنظمة التخزين
2.5.22. حماية أنظمة قواعد البيانات
3.5.22. تأمين البيانات أثناء النقل
6.22. حماية البنية التحتية
1.6.22. تصميم الشبكة الآمنة وتنفيذها
2.6.22. أمن موارد الحوسبة
3.6.22. أدوات وموارد لحماية البنية التحتية
7.22. الكشف عن التهديدات والهجمات
1.7.22. أنظمة التدقيق و Logging والمراقبة
2.7.22. أنظمة الفعاليات والإنذار
3.7.22. أنظمة SIEM
8.22. الاستجابة للحوادث
1.8.22. خطة الاستجابة للحوادث
2.8.22. استمرارية الأعمال
3.8.22. التحليل الجنائي ومعالجة الحوادث من نفس الطبيعة
9.22. الأمن في السحابة العامةClouds
1.9.22. AWS(خدمات أمازون على الويب)
2.9.22. Microsoft Azure
3.9.22. Google GCP
4.9.22. Oracle Cloud

10.22. اللوائح التنظيمية والامتثال
1.10.22. الامتثال للوائح السلامة
2.10.22. إدارة المخاطر
3.10.22. أشخاص الإجراءات في المنظمات

الوحدة 23. أدوات مراقبة السياسة الأمنية لنظم المعلومات

1.23. سياسات مراقبة نظم المعلومات
1.1.23. مراقبة النظم
2.1.23. المقاييس
3.1.23. أنواع المقاييس
2.23. التدقيق والتسجيل في الأنظمة
1.2.23. التدقيق والتسجيل في Windows
2.2.23. التدقيق والتسجيل في Linux
3.23. بروتوكول SNMP Simple Network Management Protocol
1.3.23. بروتوكول SNMP
2.3.23. تشغيل SNMP
3.3.23. أدوات SNMP
4.23. مراقبة الشبكة
1.4.23. مراقبة الشبكة في أنظمة التحكم
2.4.23. أدوات المراقبة لأنظمة التحكم
5.23. Nagios. نظام مراقبة الشبكة
1.5.23. Nagios
2.5.23. تشغيل Nagios
3.5.23. تثبيت Nagios
6.23. Zabbix. نظام مراقبة الشبكة
1.6.23. Zabbix
2.6.23. تشغيل Zabbix
3.6.23. تثبيت Zabbix
7.23. Cacti. نظام مراقبة الشبكة
1.7.23. Cacti
2.7.23. تشغيل Cacti
3.7.23. تثبيت Cacti
8.23. Pandora. نظام مراقبة الشبكة
1.8.23. Pandora
2.8.23. تشغيل Pandora
3.8.23. تثبيت Pandora
9.23. SolarWinds. نظام مراقبة الشبكة
1.9.23. SolarWinds
2.9.23. تشغيل SolarWinds
3.9.23. تثبيت SolarWinds
10.23. اللوائح الخاصة بالمراقبة
1.10.23. ضوابط CIS بشأن التدقيق والتسجيل
2.10.23. NIST 123-800 (EEUU)

الوحدة 24. أمن اتصالات أجهزة إنترنت الأشياء

1.24. من القياس عن بُعد إلى إنترنت الأشياءIoT
1.1.24. القياس عن بُعد
2.1.24. الاتصال من آلة إلى آلة M2M
3.1.24. إضفاء الطابع الديمقراطي على القياس عن بُعد
2.24. النموذج المرجعي
1.2.24. النموذج المرجعي
2.2.24. بنية إنترنت الأشياء المبسطةIoT
3.24. الثغرات الأمنية في إنترنت الأشياءIoT
1.3.24. أجهزة إنترنت الأشياء.
2.3.24. أجهزة إنترنت الأشياء. دراسات حالة الاستخدام
3.3.24. أجهزة إنترنت الأشياء. نقاط الضعف
4.24. اتصال إنترنت الأشياء IoT
1.4.24. شبكات PAN و LAN و WAN
2.4.24. تقنيات لاسلكية غير إنترنت الأشياء IoT
3.4.24. التقنيات اللاسلكيةLPWAN
5.24. تكنولوجيا LPWAN
1.5.24. المثلث الحديدي لشبكات LPWAN
2.5.24. نطاقات التردد الحر مقابل الفرق الموسيقية المرخصة
3.5.24. خيارات تقنية LPWAN

6.24. تقنية LoRaWAN
1.6.24. تقنية LoRaWAN
2.6.24. حالات الاستخدام LoRaWAN المنظومة
3.6.24. الأمن في LoRaWAN
7.24. تقنية Sigfox
1.7.24. تقنية Sigfox
2.7.24. حالات الاستخدام Sigfox. المنظومة
3.7.24. الأمن في Sigfox
8.24. تقنية إنترنت الأشياء الخلوية IoT
1.8.24. تقنية إنترنت الأشياء الخلوية (NB-IoT LTE-Mg)
2.8.24. حالات استخدام إنترنت الأشياء الخلوي. المنظومة
3.8.24. الأمن في الخلايا إنترنت الأشياء IoT
9.24. تقنية WiSUN
1.9.24. تقنية WiSUN
2.9.24. حالات الاستخدام المنظومة
3.9.24. أمن WiSUN
10.24. تقنيات IoT الأخرى
1.10.24. تقنيات IoT الأخرى
2.10.24. حالات الاستخدام والنظام البيئي لتقنيات إنترنت الأشياء الأخرى
3.10.24. الأمن في تقنيات إنترنت الأشياء الأخرى

الوحدة 25. خطة استمرارية الأعمال المرتبطة بالأمن

1.25. خطة استمرارية الأعمال
1.1.25. خطط استمرارية الأعمال
2.1.25. خطة استمرارية الأعمال الجوانب الرئيسية
3.1.25. خطة استمرارية الأعمال لتقييم الشركة
2.25. المقاييس في خطة استمرارية الأعمال
1.2.25. Recovery Time Objective (RTO) y Recovery Point Objective RPO
2.2.25. الحد الأقصى للوقت المسموح به
3.2.25. الحد الأدنى لمستويات الاسترداد
4.2.25. هدف نقطة الاسترداد
3.25. مشاريع الاستمرارية. الأنماط
1.3.25. خطة استمرارية الأعمال
2.3.25. خطة استمرارية تكنولوجيا المعلومات والاتصالات
3.3.25. خطة التعافي من الكوارث
4.25. إدارة المخاطر المرتبطة بخطة استمرارية تصريف الأعمال
1.4.25. تحليل أثر الأعمال
2.4.25. فوائد تنفيذ خطة استمرارية تصريف الأعمال
3.4.25. العقلي القائم على المخاطر
5.25. دورة حياة خطة استمرارية الأعمال
1.5.25. المرحلة 1: تحليل التنظيم
2.5.25. المرحلة 2: تحديد استراتيجية المستمر
3.5.25. المرحلة 3: الاستجابة للطوارئ
4.5.25. المرحلة 4: الاختبار والصيانة والتدقيق
6.25. مرحلة التحليل التنظيمي لخطة استمرارية تصريف الأعمال
1.6.25. تحديد العمليات التي تقع في نطاق خطة استمرارية تصريف الأعمال
2.6.25. تحديد مجالات العمل الحرجة
3.6.25. تحديد التبعيات بين المجالات والعمليات
4.6.25. تحديد أفضل التقنيات المتاحة في أفضل التقنيات المتاحة
5.6.25. الإنجازات وضع خطة
7.25. مرحلة تحديد استراتيجية الاستمرارية في خطة استمرارية تصريف الأعمال
1.7.25. الأدوار في مرحلة تحديد الاستراتيجية
2.7.25. المهام في مرحلة تحديد الاستراتيجية
3.7.25. الإنجازات
8.25. مرحلة الاستجابة للطوارئ في خطة استمرارية تصريف الأعمال
1.8.25. الأدوار في مرحلة الاستجابة
2.8.25. المهام في هذه المرحلة
3.8.25. الإنجازات
9.25. مرحلة اختبار وصيانة ومراجعة خطة استمرارية تصاميم استمرارية الأعمال
1.9.25. الأدوار في مرحلة الاختبار والصيانة والمراجعة
2.9.25. المهام في مرحلة الاختبار والصيانة والإصلاح الشامل
3.9.25. الإنجازات
10.25. معايير ISO المرتبطة بخطط استمرارية الأعمال
1.10.25. ISO 2019:22301
2.10.25. ISO 2020:22313
3.10.25. معايير ISO والمعايير الدولية الأخرى ذات الصلة

الوحدة 26. سياسة التعافي العملية من الكوارث الأمنية

1.26. خطة التعافي من الكوارث خطة التعافي من الكوارث
1.1.26. أهداف خطة التعافي من الكوارث
2.1.26. فوائد خطة التعافي من الكوارث
3.1.26. عواقب عدم وجود خطة التعافي من الكوارث وعدم تحديثها باستمرار
2.26. إرشادات حول تحديد خطة التعافي من الكوارث
1.2.26. النطاق والأهداف
2.2.26. تصميم استراتيجية التعافي
3.2.26. توزيع الأدوار والمسؤوليات
4.2.26. جرد الأجهزة softwareg والخدمات
5.2.26. تحمل وقت التعطل وفقدان البيانات
6.2.26. تحديد الأنواع المحددة من تقييمات خطة التعافي من الكوارث المطلوبة
7.2.26. تنفيذ خطة للتدريب والتوعية والتواصل.
3.26. نطاق و أهداف خطة التعافي من الكوارث
1.3.26. ضمان الاستجابة
2.3.26. المكونات التكنولوجية
3.3.26. نطاق سياسة الاستمرارية
4.26. تصميم استراتيجية التعافي من الكوارث
1.4.26. إستراتيجية التعافي من الكوارث
2.4.26. الميزانية
3.4.26. الموارد البشرية والبدنية
4.4.26. المناصب الإدارية المعرضة للخطر
5.4.26. التقنيات
6.4.26. بيانات
5.26. استمرارية عمليات المعلومات
1.5.26. تخطيط الاستمرارية
2.5.26. تنفيذ الاستمرارية
3.5.26. التحقق من تقييم الاستمرارية
6.26. نطاق خطة استمرارية الأعمال
1.6.26. تحديد العمليات الأكثر أهمية
2.6.26. النهج القائم على الأصول
3.6.26. النهج القائم على العملية
7.26. تنفيذ العمليات الآمنة للأعمال التجارية
1.7.26. الأنشطة ذات الأولوية
2.7.26. أوقات التعافي المثالية
3.7.26. استراتيجيات البقاء على قيد الحياة
8.26. تحليل التنظيم
1.8.26. الحصول على المعلومات
2.8.26. تحليل الأثر على الأعمال
3.8.26. تحليل المخاطر في المنظمة
9.26. الاستجابة للطوارئ
1.9.26. خطة الأزمات
2.9.26. خطط استعادة البيئة التشغيلية
3.9.26. الإجراءات التقنية للعمل أو الحوادث
10.26. المعيار الدولي ISO 27031 ISO 27031 BCP
1.10.26. الأهداف
2.10.26. المصطلحات والتعريفات
3.10.26. عملية

الوحدة 27. تطبيق سياسات الأمن المادي والبيئي في الشركة

1.27. المناطق الامنة
1.1.27. المحيط الأمني المادي
2.1.27. العمل في المناطق الآمنة
3.1.27. أمن المكاتب والمرافق والموارد
2.27. الضوابط المادية للدخول
1.2.27. سياسات التحكم في الوصول المادي
2.2.27. أنظمة التحكم المادي في الدخول
3.27. نقاط ضعف الدخول المادي
1.3.27. نقاط الضعف المادية الرئيسية
2.3.27. تنفيذ تدابير الحماية
4.27. أنظمة القياسات الحيوية الفسيولوجية
1.4.27. البصمة
2.4.27. التعرف على الوجه
3.4.27. التعرف على القزحية وشبكية العين
4.4.27. أنظمة القياسات الحيوية الفسيولوجية الأخرى

5.27. الأنظمة البيومترية السلوكية
1.5.27. التعرف على التواقيع
2.5.27. التعرف على الكاتب
3.5.27. التعرف الصوتي
4.5.27. الأنظمة البيومترية السلوكية الأخرى
6.27. إدارة المخاطر في القياسات الحيوية
1.6.27. تنفيذ أنظمة القياسات الحيوية
2.6.27. نقاط الضعف في الأنظمة البيومترية
7.27. تطبيق السياسة على المضيفين
1.7.27. تركيب كابلات الإمداد والأمن
2.7.27. مواقع المعدات
3.7.27. خروج المعدات إلى خارج المبنى
4.7.27. معدات تكنولوجيا المعلومات غير المراقبة وسياسة تطهير المكاتب
8.27. حماية البيئة
1.8.27. نظام الحماية من الحرائق
2.8.27. نظام الحماية من الهزات
3.8.27. أنظمة الحماية من الزلازل
9.27. الأمن في مركز معالجة البيانات
1.9.27. أبواب الأمان
2.9.27. نظم المراقبة بالفيديو (CCTV)
3.9.27. التحكم الأمني
10.27. لوائح السلامة البدنية الدولية
1.10.27. IEC 1-2-64243 الأوربية
2.10.27. NERC CIP 5-005 (EEUU)
3.10.27. NERC CIP 2-014 (EEUU)

الوحدة 28. سياسات الاتصالات الآمنة في المؤسسة

1.28. إدارة أمن الشبكة
1.1.28. التحكم في الشبكة ومراقبتها
2.1.28. فصل الشبكات
3.1.28. أنظمة أمن الشبكات
2.28. بروتوكولات الاتصال الأمنة
1.2.28. نموذج TCP / IP
2.2.28. بروتوكول IPSEC
3.2.28. بروتوكول TLS
3.28. بروتوكول TLS 1.3
1.3.28. مراحل عملية 1.3TLS
2.3.28. بروتوكول المصافحة بالأيدي Handshake
3.3.28. بروتوكول التسجيل
4.3.28. الاختلافات مع TLS 1.2
4.28. خوارزميات التشفير
1.4.28. خوارزميات التشفير المستخدمة في الاتصالات
2.4.28. Cipher-suites
3.4.28. خوارزميات التشفير المسموح بها في TLS 1.3
5.28. وظائف Digest
1.5.28. MD6:
2.5.28. SHA
6.28. البنية التحتية للمفاتيح العامة PKI
1.6.28. PKI والكيانات التابعة لها
2.6.28. شهادة رقمية
3.6.28. أنواع الشهادات الرقمية
7.28. الاتصالات عبر الأنفاق والنقل
1.7.28. اتصالات الأنفاق
2.7.28. اتصالات النقل
3.7.28. تنفيذ النفق المشفر
8.28. SSH. Secure Shell
1.8.28. SSH. كبسولة آمنة
2.8.28. تشغيل SSH
3.8.28. أدوات SSH

9.28. التدقيق في أنظمة التشفير
1.9.28. اختبار السلامة
2.9.28. اختبار نظام التشفير
10.28. أنظمة التشفير
1.10.28. نقاط ضعف أنظمة التشفير
2.10.28. الضمانات في التشفير

الوحدة 29. الجوانب التنظيمية لسياسة أمن المعلومات

1.29. التنظيم الداخلي
1.1.29. توزيع المسؤوليات
2.1.29. الفصل بين المهام
3.1.29. الاتصالات مع السلطات
4.1.29. أمن المعلومات في إدارة المشاريع
2.29. إدارة الأصول
1.2.29. التزامات الأصول
2.2.29. تصنيف المعلومات
3.2.29. التعامل مع وسائط التخزين
3.29. السياسات الأمنية في عمليات الأعمال
1.3.29. تحليل عمليات الأعمال المعرضة للخطر
2.3.29. تحليل أثر الأعمال
3.3.29. تصنيف العمليات فيما يتعلق بتأثيرها على الأعمال
4.29. السياسات الأمنية المرتبطة بالموارد البشرية
1.4.29. قبل التعيين
2.4.29. أثناء التعيين
3.4.29. إنهاء الخدمة أو تغيير المنصب
5.29. السياسات الأمنية في الادارة
1.5.29. إرشادات الإدارة بشأن أمن المعلومات
2.5.29. تحليل تأثير الأعمال- تحليل الأثر
3.5.29. خطة التعافي كسياسة أمنية
6.29. اقتناء نظم المعلومات وصيانتها
1.6.29. متطلبات الأمان في نظم المعلومات
2.6.29. أمن بيانات التطوير والدعم
3.6.29. بيانات الاختبار

7.29. الأمن مع الموردين
1.7.29. أمن تكنولوجيا المعلومات مع الموردين
2.7.29. إدارة تقديم الخدمات مع ضمان تقديم الخدمات
3.7.29. أمن سلسلة التوريد
8.29. السلامة في العمليات
1.8.29. المسؤوليات في العملية
2.8.29. الحماية من الشفرات البرمجية الخبيثة
3.8.29. النسخ الاحتياطية
4.8.29. سجل النشاط والإشراف
9.29. الإدارة الأمنية والتنظيمية
1.9.29. الامتثال للمتطلبات القانونية
2.9.29. مراجعات أمن المعلومات
10.29. الأمن في إدارة استمرارية الأعمال
1.10.29. استمرارية أمن المعلومات
2.10.29. حالات التكرار

ستتمكن من التعمق أكثر في قضايا مثل خطة استمرارية الأعمال المرتبطة بالأمن أو إدارة الهوية والوصول في أمن تكنولوجيا المعلومات"

05

المنهجية

يقدم هذا البرنامج التدريبي طريقة مختلفة للتعلم. فقد تم تطوير منهجيتنا من خلال أسلوب التعليم المرتكز على التكرار: ***Relearning*** أو ما يعرف بمنهجية إعادة التعلم.

يتم استخدام نظام التدريس هذا، على سبيل المثال، في أكثر كليات الطب شهرة في العالم، وقد تم اعتباره أحد أكثر المناهج فعالية في المنشورات ذات الصلة مثل مجلة نيو إنجلند الطبية ***(New England Journal of Medicine)***.

اكتشف منهجية *Relearning* (منهجية إعادة التعلم)، وهي نظام يتخلى عن التعلم الخطي التقليدي ليأخذك عبر أنظمة التدريس التعليم المرتكزة على التكرار: إنها طريقة تعلم أثبتت فعاليتها بشكل كبير، لا سيما في المواد الدراسية التي تتطلب الحفظ"

منهج دراسة الحالة لوضع جميع محتويات المنهج في سياقها المناسب

يقدم برنامجنا منهج ثوري لتطوير المهارات والمعرفة. هدفنا هو تعزيز المهارات في سياق متغير وتنافسي ومتطلب للغاية.

مع جامعة TECH يمكنك تجربة طريقة تعلم تهز أسس الجامعات التقليدية في جميع أنحاء العالم"

سيتم توجيهك من خلال نظام التعلم القائم على إعادة التأكيد على ما تم تعلمه، مع منهج تدريس طبيعي وتقدمي على طول المنهج الدراسي بأكمله.

منهج تعلم مبتكرة ومختلفة

إن هذا البرنامج المُقدم من خلال TECH هو برنامج تدريس مكثف، تم خلقه من الصفر، والذي يقدم التحديات والقرارات الأكثر تطلبًا في هذا المجال، سواء على المستوى المحلي أو الدولي. تعزز هذه المنهجية النمو الشخصي والمهني، متخذة بذلك خطوة حاسمة نحو تحقيق النجاح. ومنهج دراسة الحالة، وهو أسلوب يرسي الأسس لهذا المحتوى، يكفل اتباع أحدث الحقائق الاقتصادية والاجتماعية والمهنية.

> يعدك برنامجنا هذا لمواجهة تحديات جديدة في بيئات غير مستقرة ولتحقيق النجاح في حياتك المهنية"

كان منهج دراسة الحالة هو نظام التعلم الأكثر استخدامًا من قبل أفضل كليات الحاسبات في العالم منذ نشأتها. تم تطويره في عام 1912 بحيث لا يتعلم طلاب القانون القوانين بناءً على المحتويات النظرية فحسب، بل اعتمد منهج دراسة الحالة على تقديم مواقف معقدة حقيقية لهم لاتخاذ قرارات مستنيرة وتقدير الأحكام حول كيفية حلها. في عام 1924 تم تحديد هذه المنهجية كمنهج قياسي للتدريس في جامعة هارفارد.

أمام حالة معينة، ما الذي يجب أن يفعله المهني؟ هذا هو السؤال الذي سنواجهك بها في منهج دراسة الحالة، وهو منهج تعلم موجه نحو الإجراءات المتخذة لحل الحالات. طوال المحاضرة الجامعية، سيواجه الطلاب عدة حالات حقيقية. يجب عليهم دمج كل معارفهم والتحقيق والجدال والدفاع عن أفكارهم وقراراتهم.

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

منهجية إعادة التعلم *(Relearning)*

تجمع جامعة TECH بين منهج دراسة الحالة ونظام التعلم عن بعد، 100٪ عبر الانترنت والقائم على التكرار، حيث تجمع بين عناصر مختلفة في كل درس.

نحن نعزز منهج دراسة الحالة بأفضل منهجية تدريس 100٪ عبر الانترنت في الوقت الحالي وهي: منهجية إعادة التعلم والمعروفة بـ *Relearning*.

في عام 2019، حصلنا على أفضل نتائج تعليمية متفوقين بذلك على جميع الجامعات الافتراضية الناطقة باللغة الإسبانية في العالم.

في TECH ستتعلم بمنهجية رائدة مصممة لتدريب مدراء المستقبل. وهذا المنهج، في طليعة التعليم العالمي، يسمى *Relearning* أو إعادة التعلم.

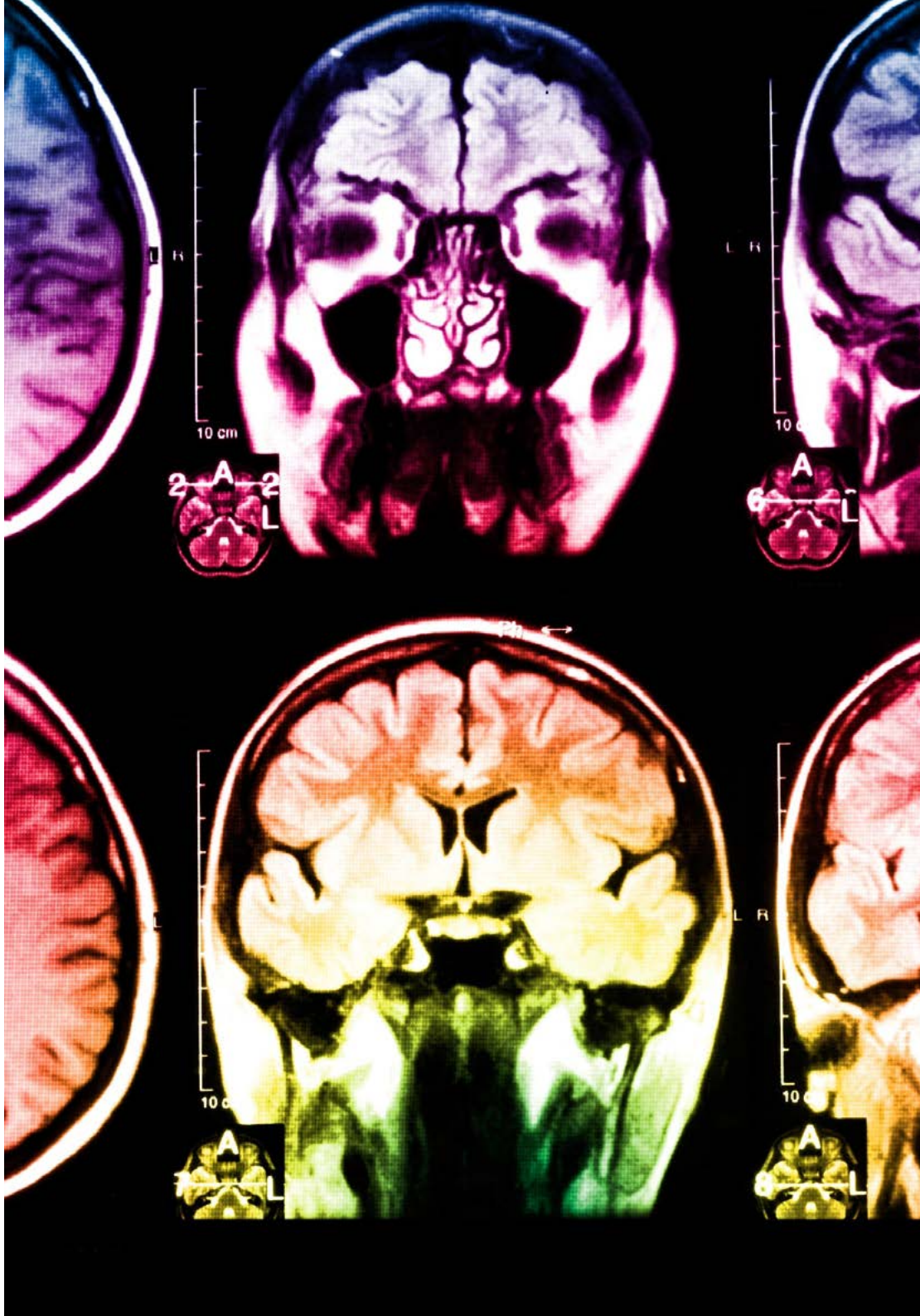
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

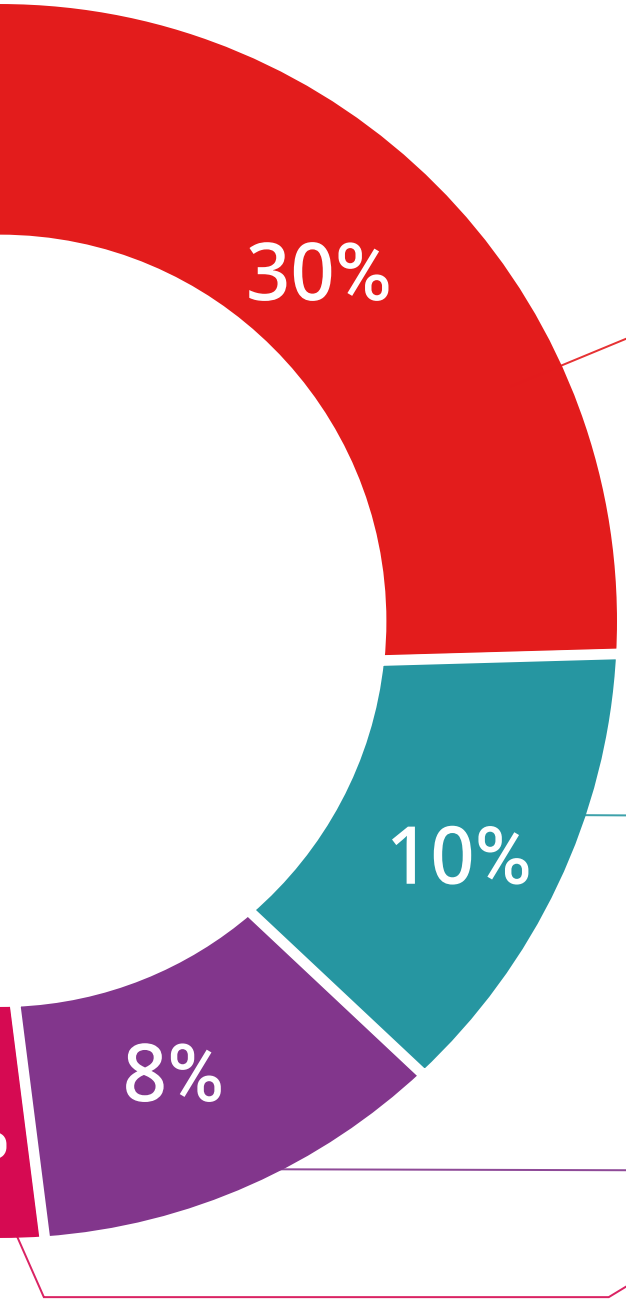
في برنامجنا، التعلم ليس عملية خطية، ولكنه يحدث في شكل لولبي (نتعلّم ثم نطرح ماتعلمناه جانبًا فننساه ثم نعيد تعلمه). لذلك، نقوم بدمج كل عنصر من هذه العناصر بشكل مركزي. باستخدام هذه المنهجية، تم تدريب أكثر من 650000 خريج جامعي بنجاح غير مسبوق في مجالات متنوعة مثل الكيمياء الحيوية، وعلم الوراثة، والجراحة، والقانون الدولي، والمهارات الإدارية، وعلوم الرياضة، والفلسفة، والقانون، والهندسة، والصحافة، والتاريخ، والأسواق والأدوات المالية. كل ذلك في بيئة شديدة المتطلبات، مع طلاب جامعيين يتمتعون بمظهر اجتماعي واقتصادي مرتفع ومتوسط عمر يبلغ 43.5 عاماً.

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

استنادًا إلى أحدث الأدلة العلمية في مجال علم الأعصاب، لا نعرف فقط كيفية تنظيم المعلومات والأفكار والصور والذكريات، ولكننا نعلم أيضًا أن المكان والسياق الذي تعلمنا فيه شيئًا هو ضروريًا لكي نكون قادرين على تذكرها وتخزينها في الحُصين بالمخ، لكي نحتفظ بها في ذاكرتنا طويلة المدى.

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





يقدم هذا البرنامج أفضل المواد التعليمية المُعَدَّة بعناية للمهنيين:

المواد الدراسية

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

ثم يتم تطبيق هذه المحتويات على التنسيق السمعي البصري الذي سيخلق منهج جامعة TECH في العمل عبر الإنترنت. كل هذا بأحدث التقنيات التي تقدم أجزاء عالية الجودة في كل مادة من المواد التي يتم توفيرها للطالب.

المحاضرات الرئيسية

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

إن مفهوم ما يسمى *Learning from an Expert* أو التعلم من خبير يقوي المعرفة والذاكرة، ويولد الثقة في القرارات الصعبة في المستقبل.

التدريب العملي على المهارات والكفاءات

سيقومون بتنفيذ أنشطة لتطوير مهارات وقدرات محددة في كل مجال مواضيعي. التدريب العملي والديناميكيات لاكتساب وتطوير المهارات والقدرات التي يحتاجها المتخصص لنموه في إطار العولمة التي نعيشها.

قراءات تكميلية

المقالات الحديثة، ووثائق اعتمدت بتوافق الآراء، والأدلة الدولية. من بين آخرين. في مكتبة جامعة TECH الافتراضية، سيتمكن الطالب من الوصول إلى كل ما يحتاجه لإكمال تدريبه.

دراسات الحالة (Case studies)

سيقومون بإكمال مجموعة مختارة من أفضل دراسات الحالة المختارة خصيصًا لهذا المؤهل. حالات معروضة ومحللة ومدروسة من قبل أفضل المتخصصين على الساحة الدولية.

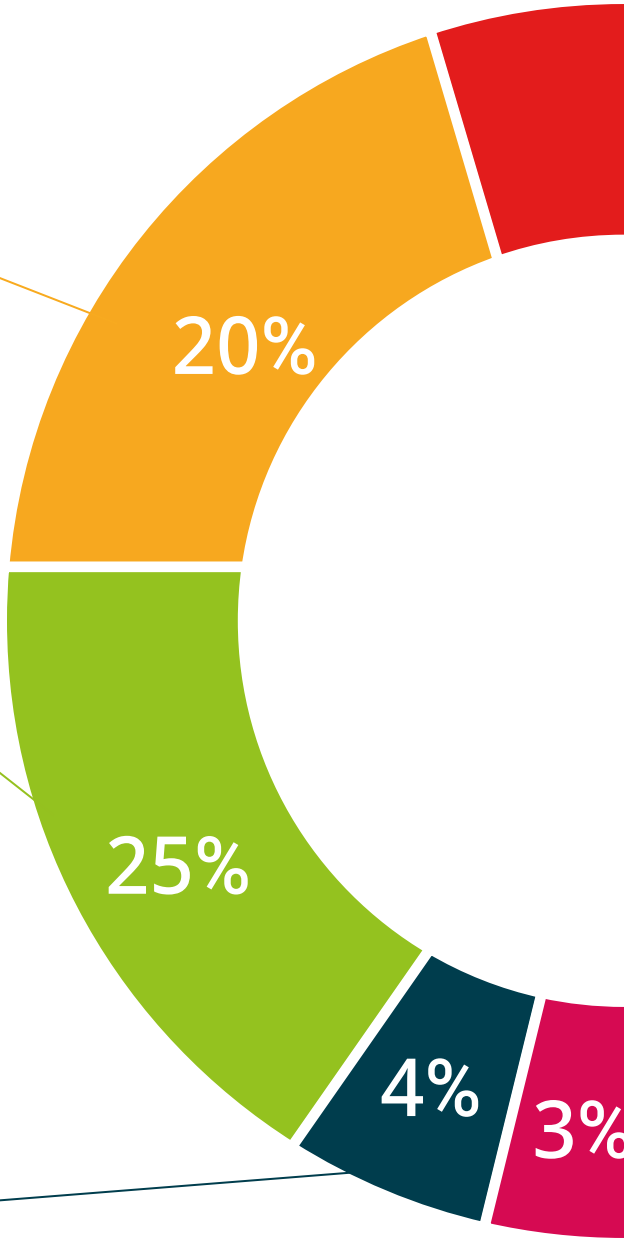
ملخصات تفاعلية

يقدم فريق جامعة TECH المحتويات بطريقة جذابة وديناميكية في أقراص الوسائط المتعددة التي تشمل الملفات الصوتية والفيديوهات والصور والرسوم البيانية والخرائط المفاهيمية من أجل تعزيز المعرفة.

اعترفت شركة مايكروسوف بهذا النظام التعليمي الفريد لتقديم محتوى الوسائط المتعددة على أنه "قصة نجاح أوروبية".

الاختبار وإعادة الاختبار

يتم بشكل دوري تقييم وإعادة تقييم معرفة الطالب في جميع مراحل البرنامج، من خلال الأنشطة والتدريبات التقييمية وذاتية التقييم: حتى يتمكن من التحقق من كيفية تحقيق أهدافه.



06

المؤهل العلمي

يضمن الماجستير المتقدم في الإدارة العليا للأمن السيبراني (كبير مسؤولي أمن المعلومات CISO) بالإضافة إلى التدريب الأكثر دقة وحداثة، الحصول على مؤهل الماجستير المتقدم الصادر عن TECH الجامعة التكنولوجية.

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

تحتوي درجة **الماجستير المتقدم في الإدارة العليا للأمن السيبراني (كبير مسؤولي أمن المعلومات CISO)** 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 الإدارة العليا للأمن السيبراني (كبير مسؤولي أمن المعلومات CISO)**

طريقة الدراسة: **عبر الإنترنت**

مدة الدراسة: **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

الإدارة العليا للأمن السيبراني (كبير مسؤولي أمن المعلومات CISO)

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 الإدارة العليا للأمن السيبراني (كبير مسؤولي أمن المعلومات CISO)

التوزيع العام للخطة الدراسية

الدورة	المادة	الطريقة	عدد الساعات
1°	الذكاء والأمن السيبراني	إجباري	100
1°	أمان Host	إجباري	100
1°	أمان الشبكة (المحيط)	إجباري	100
1°	أمن الهواتف الذكية smartphones	إجباري	100
1°	الأمن في إنترنت الأشياء IoT	إجباري	100
1°	Hacking اختلافيات الاختراق	إجباري	100
1°	الهندسة العكسية	إجباري	100
1°	التطوير الآمن	إجباري	100
1°	التنفيذ العملي لسياسات الأمان في البرامج والأجهزة	إجباري	100
1°	التحليل الجنائي	إجباري	100
1°	السلامة في التصميم وتطوير الأنظمة	إجباري	100
1°	هياكل ونماذج أمن المعلومات	إجباري	100
1°	نظام إدارة أمن المعلومات	إجباري	100
1°	إدارة الأمن IT	إجباري	100
1°	سياسات إدارة الحوادث الأمنية	إجباري	100

الدورة	المادة	الطريقة	عدد الساعات
2°	تحليل المخاطر وبيئة أمن تكنولوجيا المعلومات	إجباري	100
2°	السياسات الأمنية لتحليل التهديدات في أنظمة الكمبيوتر	إجباري	100
2°	التنفيذ العملي للسياسات الأمنية في مواجهة الهجمات	إجباري	100
2°	التشفير في تكنولوجيا المعلومات	إجباري	100
2°	إدارة الهوية والوصول في أمن تكنولوجيا المعلومات	إجباري	100
2°	الأمن في الاتصالات وتشغيل البرامج	إجباري	100
2°	الأمان في البيئات السحابيةCloud	إجباري	100
2°	أدوات مراقبة السياسة الأمنية لنظم المعلومات	إجباري	100
2°	أمن الحالات أجهزة إنترنت الأشياء	إجباري	100
2°	خطة استمرارية الأعمال المرتبطة بالأمن	إجباري	125
2°	سياسة التعافي من الكوارث الأمنية العملية	إجباري	125
2°	تطبيق سياسات الأمن المادي والبيئي في الشركة	إجباري	125
2°	سياسات الاتصالات الآمنة في المؤسسة	إجباري	125
2°	الجوانب التنظيمية لسياسة أمن المعلومات	إجباري	125

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 مؤسسة TECH EDUCATION الإجراءات المناسبة لكي يحصل عليها وذلك بتكلفة إضافية.

الجامعة التيكنولوجية

ماجستير متقدم
الإدارة العليا للأمن السيبراني
(كبير مسؤولي أمن المعلومات CISO)

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

ماجستير متقدم
الإدارة العليا للأمن السيبراني
(كبير مسؤولي أمن المعلومات CISO)

tech الجامعة التيكنولوجية