BLACKBIRD FOR TRAINING

أمن المعلومات والأمن السيبراني

April 2027 16 – 12

كوالالمبور (ماليزيا)



أمن المعلومات والأمن السيبراني

المرجع: 147819_321492 **التاريخ:** 12 – 16 April 2027 **المكان:** كوالالمبور (ماليزيا) **الرسوم:** GBP 4900

مقدمة

في العصر الرقمي الحالي، أصبح فهم أمن المعلومات أمرًا بالغ الأهمية لحماية المؤسسات من الهجمات الإلكترونية المتزايدة. تقدم هذه الدورة للمشاركين فهمًا شاملاً لأهم التهديدات التي تواجه المؤسسات، وتعرض تقنيات أمن المعلومات الأساسية ووسائل التحكم لحماية الأنظمة من هذه التهديدات. من خلال التعليم التفصيلي، ستستكشف الأساسيات الخاصة بـ الأمن السيبراني وكيفية تصميم الأنظمة الآمنة، وستكتسب منظورًا عالميًا حول الأدوار المختلفة المطلوبة لتوفير حل أمني متكامل.

إضافةً إلى ذلك، ستستعرض أحدث الاتجاهات في التهديدات السيبرانية، وستتعلم أفضل ممارسات أمن المعلومات، بالإضافة إلى اكتساب الخبرة العملية في إدارة مخاطر الأمان داخل المؤسسة. بنهاية الدورة، سيحصل المشاركون على فهم واضح لكيفية تنفيذ استراتيجيات أمن المعلومات التي تتماشى مع أهداف المؤسسة.

أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- فهم التهديدات الإلكترونية والثغرات التي تواجهها المؤسسات وكيفية الحماية منها.
- اكتساب المعرفة بأساسيات أمن المعلومات، بما في ذلك التقنيات ووسائل التحكم لحماية الأنظمة.
- فهم المكونات الأساسية لـ نظام إدارة أمن المعلومات ISMS.
- استكشاف مبادئ حماية البيانات وكيفية حماية المعلومات الحساسة.
- التعرف على تهديدات الهندسة الاجتماعية وكيفية التخفيف من تأثيراتها.
- تحليل ثغرات البرمجيات وفهم الحلول الأمنية لتقليل مخاطر الاستغلال.
- التعرف على وسائل الأمان المادي وأهمية دمجها مع أمن تكنولوجيا المعلومات.
- استكشاف مبادئ أمن المعلومات وفهم تطبيقاتها داخل المؤسسة.
- تعلم كيفية تمييز الأمن السيبراني وأمن المعلومات وكيف يكمل كل منهما الآخر.



محاور الدورة

اليوم الأول: الوعي بالأمن السيبراني

- ما هو الأمن؟ - فهم المفاهيم الأساسية للأمن ودورها في حماية المؤسسات.
- السرية والنزاهة والتوافر - المبادئ الأساسية لأمن المعلومات.
- تأسيس معايير الأمان - وضع معايير لتقييم وسائل الأمان.
- أنواع التهديدات - دراسة التهديدات الإلكترونية الشائعة والناشئة.
- وسائل الأمان - المستويات المختلفة للتحكم التي يمكن تنفيذها لمنع الهجمات.
- ما هو الاختراق؟ - مقدمة إلى تقنيات الاختراق وكيفية الدفاع ضدها.
- إدارة المخاطر - فهم كيفية تقييم وإدارة المخاطر بشكل فعال.
- البيانات أثناء الحركة مقابل البيانات عند الاستراحة - تقنيات لحماية البيانات خلال دورة حياتها.
- اكتشاف الشبكة - الأدوات والأساليب لاكتشاف وتأمين الأصول الشبكية.

اليوم الثاني: بنية الأمان

- بنية الأمان - المكونات الأساسية لتصميم بيئة تكنولوجيا معلومات آمنة.
- أجهزة الشبكة والمناطق - فهم كيفية تكوين الأجهزة لتأمين الشبكة.
- تقسيم الشبكة والتحكم في الوصول - تقنيات تقليل سطح الهجوم والتحكم في الوصول.
- أمن البيانات والتشفير - تنفيذ التشفير والبروتوكولات التشفيرية لحماية البيانات الحساسة.
- مبادئ الأذونات - إدارة الوصول لضمان نزاهة البيانات والأنظمة.

اليوم الثالث: إدارة الهوية وتقوية الشبكة

- ما هي إدارة الهوية؟ - دور إدارة الهوية والوصول IAM في حماية الأصول الرقمية.
- العوامل المصادقة وخدمات الدليل - أفضل الممارسات لضمان عمليات المصادقة الآمنة.
- كسر كلمات المرور - تقنيات لاختبار أمان كلمات المرور وأفضل الممارسات لإنشاء كلمات مرور قوية.
- الهوية الموحدة والخدمات المستندة إلى الهوية IDaaS - أساليب متقدمة لحماية الهوية عبر المنصات.
- تقوية الشبكة - تأمين الأجهزة الشبكية وتقييد الوصول لتقليل الثغرات.
- تصفية حركة المرور والوصول عن بعد - منع الوصول غير المصرح به إلى الشبكة.



اليوم الرابع: أمان البرمجيات والأمان المادي

- هندسة البرمجيات وإرشادات الأمان - كيفية دمج الأمان في دورة حياة تطوير البرمجيات.
- ثغرات البرمجيات - تحليل الثغرات الأمنية الشائعة في البرمجيات.
- مراقبة البيئة - الأدوات والتقنيات لمراقبة الأحداث الأمنية بشكل فعال.
- وسائل الأمان المادي - التفاعل بين الأمان المادي وحماية المعلومات.
- الدفاع في العمق - استراتيجيات الأمان متعددة الطبقات لتعظيم الحماية.

اليوم الخامس: الاستجابة للحوادث واتجاهات الأمن السيبراني

- أنواع الكوارث والتحقيق في الحوادث - التحضير والاستجابة للحوادث الأمنية.
- التخطيط لاستمرارية الأعمال - إنشاء خطط فعالة لاستعادة الأعمال في حالة حدوث كارثة.
- الاستجابة للحوادث الجنائية - تقنيات التحقيق وحل الحوادث الأمنية.
- اتجاهات الأمن السيبراني - التحديات والابتكارات الحديثة في مجال الأمن السيبراني.
- معايير الأمن السيبراني والتدريب - فهم أحدث المعايير وأفضل الممارسات لتدريب الموظفين على الأمن.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- معرفة شاملة بالأمن السيبراني: من خلال حضور هذه الدورة، ستحصل على فهما عميقًا لـ أمن المعلومات و الفرق بين الأمن السيبراني وأمن المعلومات، مما يساعدك على حماية أي منظمة من التهديدات الإلكترونية.
- مهارات عملية: ستحصل على خبرة عملية في استخدام تقنيات الأمان و وسائل التحكم لحماية الأنظمة وتقليل المخاطر.
- نمو مهني: هذه الدورة هي نقطة انطلاق ممتازة إذا كنت ترغب في الانضمام إلى مجال الأمن السيبراني أو أن تصبح محلل أمن المعلومات. توفر لك هذه الدورة المعرفة الأساسية لأداء دورك بكفاءة.
- تطبيقات واقعية: ستتعلم أفضل ممارسات أمن المعلومات واستراتيجيات يمكن تنفيذها على الفور في مؤسستك.
- منظور عالمي: فهم كيفية التعامل مع التهديدات السيبرانية العالمية وتحقيق حماية أفضل للمؤسسة في بيئة متزايدة من المخاطر.

الخاتمة

تم تصميم هذه الدورة لتزويدك بالأدوات الأساسية والمعرفة لحماية مؤسستك من التهديدات الإلكترونية وفهم عالم أمن المعلومات بشكل أوسع. سواء كنت تبدأ رحلتك في مجال الأمن السيبراني أو ترغب في تعزيز معرفتك الحالية، ستزودك هذه الدورة بالمبادئ الأساسية وتدريب أمني ضروري لتحقيق النجاح. كما ستفتح أمامك فرصًا في مجال الأمن السيبراني المتنامي بسرعة، حيث الطلب على محللي أمن المعلومات في أعلى مستوياته.

