BLACKBIRD FOR TRAINING

شهادة أساسيات أمن المعلومات من سانس وجياك

11 – 15 يوليو 2027

القاهرة (مصر)



شهادة أساسيات أمن المعلومات من سانس وجياك

المرجع: 346226_3255610 **التاريخ:** 11 – 15 يوليو 2027 **المكان:** القاهرة (مصر) **الرسوم:** GBP 4900

مقدمة

تعد شهادة أساسيات أمن المعلومات من سانس وجياك من الشهادات المهنية المتخصصة التي تركز على بناء فهم متكامل لمبادئ حماية الأنظمة والشبكات داخل المؤسسات.

تغطي هذه الشهادة الأسس التقنية والتنظيمية لأمن المعلومات، وتوضح كيفية التعامل مع التهديدات الإلكترونية المتزايدة بطريقة منهجية تعتمد على التحليل والتقييم المستمر.

كما تربط بين الجوانب التقنية وإدارة المخاطر والحوكمة المؤسسية لضمان تكامل الأمن مع الأهداف الاستراتيجية.

تستهدف هذه الدورة القيادات التنفيذية، ومديري الإدارات، ومسؤولي تقنية المعلومات، ومختصي أمن المعلومات، إضافة إلى العاملين في إدارات المخاطر والرقابة والامتثال.

وتخدم مختلف القطاعات التي تعتمد على البنية الرقمية في عملياتها اليومية، مثل القطاع المالي، والطاقة، والاتصالات، والمؤسسات الصناعية والخدمية.

الفائدة العملية لهذه الشهادة تتمثل في تمكين المشاركين من فهم بنية التهديدات الحديثة، وتطبيق ضوابط الحماية الأساسية، وتحليل الثغرات، وتعزيز الجاهزية المؤسسية أمام المخاطر الإلكترونية.

كما تساعد على تطوير مهارات التقييم الأمني، وتحسين إجراءات الحماية، ورفع مستوى الثقة في الأنظمة التقنية داخل المؤسسة.

أهداف الدورة

تهدف دورة شهادة أساسيات أمن المعلومات من سانس وجياك إلى تحقيق نتائج عملية قابلة للتطبيق، وتشمل:



- التعرف على المفاهيم الجوهرية لأمن المعلومات.
- فهم مبادئ السرية وسلامة البيانات وتوافرها.
- تحليل أنواع التهديدات والهجمات الإلكترونية الشائعة.
- تقييم نقاط الضعف في الشبكات والأنظمة.
- تطبيق ضوابط الحماية الأساسية على الخوادم وأجهزة المستخدمين.
- إدارة صلاحيات الوصول وفق منهج منظم.
- استخدام آليات الكشف عن البرمجيات الضارة.
- تنفيذ خطوات الاستجابة للحوادث الأمنية.
- فهم مبادئ التشفير واستخداماته في حماية البيانات.
- إعداد تقارير تقييم أمني للإدارة العليا.
- تعزيز ثقافة الوعي الأمني داخل المؤسسة.
- ربط أمن المعلومات بإدارة المخاطر واستمرارية الأعمال.

محاور الدورة

اليوم الأول: المفاهيم الأساسية لأمن المعلومات وبنية الشبكات

- تعريف أمن المعلومات وأهميته المؤسسية.
- مبادئ السرية وسلامة البيانات والتوافر.
- مكونات الشبكات وآلية انتقال البيانات.
- تحليل نقاط الضعف في تصميم الشبكات.
- إدارة المخاطر على مستوى البنية التحتية التقنية.
- تمرين عملي لتحليل سيناريو تهديد محتمل.

اليوم الثاني: التهديدات الإلكترونية وأساليب الحماية الأولية

- أنواع البرمجيات الضارة وطرق انتشارها.
- هجمات تعطيل الخدمات وتأثيرها على العمليات.
- أساليب الاحتيال الإلكتروني والهندسة الاجتماعية.
- إعداد ضوابط التحكم في الوصول.
- إدارة الثغرات الأمنية وتحديث الأنظمة.
- دراسة حالة لتحليل حادث أمني واقعي.



اليوم الثالث: حماية أنظمة التشغيل وإدارة الصلاحيات والتشفير

- تأمين أنظمة التشغيل ضد الاختراق.
- تنظيم حسابات المستخدمين والصلاحيات.
- تطبيق مبدأ أقل صلاحية ممكنة.
- أساسيات التشفير وأنواعه واستخداماته.
- حماية قواعد البيانات والمعلومات الحساسة.
- تمرين عملي على إعداد سياسات وصول آمنة.

اليوم الرابع: كشف الاختراقات والاستجابة للحوادث

- مراقبة الأنظمة واكتشاف الأنشطة غير الطبيعية.
- تحليل سجلات الأحداث الأمنية.
- خطوات الاستجابة الأولية للحوادث.
- احتواء الحادث والحد من انتشاره.
- جمع الأدلة الرقمية بطريقة منظمة.
- تنفيذ محاكاة عملية لإدارة حادث أمني.

اليوم الخامس: التقييم الشامل وبناء بيئة أمنية مستدامة

- مراجعة شاملة لمفاهيم الأمن الأساسية.
- تقييم مستوى الحماية الحالي داخل المؤسسة.
- إعداد خطة تحسين مرحلية للأمن.
- ربط أمن المعلومات بإدارة المخاطر المؤسسية.
- عرض نتائج التمارين التطبيقية.
- تقييم نهائي من خلال دراسة حالة متكاملة.



لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات!

- تعزيز قدرة المؤسسة على حماية بياناتها وأنظمتها.
- تقليل احتمالية التعرض للاختراقات.
- تحسين الامتثال للضوابط التنظيمية.
- تطوير مهارات تحليل المخاطر الأمنية.
- رفع كفاءة فرق تقنية المعلومات.
- دعم اتخاذ القرار المبني على تقييم أمني دقيق.
- تحسين الجاهزية للحوادث الإلكترونية.
- تعزيز ثقة العملاء والشركاء في البنية التقنية.

الخاتمة

تمثل شهادة أساسيات أمن المعلومات من سانس وجياك إطارًا عمليًا لفهم المبادئ الأساسية لحماية الأنظمة والشبكات داخل المؤسسات. تغطي الدورة مفاهيم الشبكات، والتشفير، وإدارة الصلاحيات، والاستجابة للحوادث بطريقة منهجية واضحة. كما تساعد المشاركين على تحليل التهديدات الحديثة وتطبيق ضوابط الحماية المناسبة بما يضمن تقليل المخاطر التقنية.

يسهم تطبيق المفاهيم المكتسبة في رفع مستوى الجاهزية الأمنية، وتعزيز استمرارية الأعمال، وتحسين الحوكمة التقنية داخل المؤسسة. إن بناء قاعدة قوية في أمن المعلومات يعد عنصرًا أساسيًا في حماية الأصول الرقمية وضمان استقرار العمليات التشغيلية. وتوفر هذه الشهادة مرجعًا مهنيًا يعكس قدرة المتخصصين على إدارة المخاطر التقنية بكفاءة ومسؤولية.

