BLACKBIRD FOR TRAINING

# أمن المعلومات والأمن السيبراني

March – 9 April 2027 29

مالي (المالديف)



# أمن المعلومات والأمن السيبراني

**المرجع:** 154208_321503 **التاريخ:** 29 March – 9 April 2027 **المكان:** مالي (المالديف) **الرسوم:** GBP 10600

## مقدمة

في عالمنا المتصل بشكل متزايد، أصبح الأمن السيبراني أكثر أهمية من أي وقت مضى. تواجه المنظمات مجموعة متزايدة من التهديدات الإلكترونية، من اختراقات البيانات إلى الهجمات السيبرانية المتقدمة. توفر هذه الدورة للمشاركين فهماً شاملاً حول كيفية حماية مؤسساتهم من الهجمات السيبرانية. تغطي الدورة من الأساسيات إلى الاستراتيجيات المتقدمة في الدفاع السيبراني، مما يضمن أن يغادر جميع المشاركين بفهم واضح حول كيفية حماية بنيتهم التحتية.

من خلال هذه الدورة، ستتعرف على أحدث اتجاهات التهديدات في مجال الأمن السيبراني وتقنيات إدارة المخاطر، وكيفية تصميم وتنفيذ سياسة شاملة للأمن السيبراني. من خلال استعراض محاكاة الأمن السيبراني الواقعية، ستحصل على خبرة عملية في الحد من التهديدات السيبرانية الشائعة.

## أهداف الدورة

بنهاية هذه الدورة، سيتمكن المشاركون من:

- فهم التهديدات والثغرات السيبرانية التي تواجه المنظمات اليوم، والحاجة إلى استراتيجية شاملة للأمن السيبراني.
- تعلم تقنيات الأمن المعلوماتي وكيفية تطبيقها لحماية المنظمات من الهجمات السيبرانية، وضمان توافقها مع برنامج شامل للأمن السيبراني.
- فهم الأساسيات المتعلقة بـ نظام إدارة أمن المعلومات ISMS وكيفية دعمه للأهداف الأمنية الشاملة.
- استكشاف مبادئ حماية البيانات المختلفة، بما في ذلك تقنيات حماية البيانات أثناء التنقل وفي حالة السكون.
- التعمق في تهديدات الهندسة الاجتماعية، وأساليبها، وأهمية الدفاع السيبراني للتصدي لها.
- تحليل ثغرات البرمجيات واكتشاف حلول الأمان للحد من مخاطر الاستغلال.
- فحص الضوابط الأمنية الفيزيائية و تأثيرها المشترك مع أمن تكنولوجيا المعلومات.



## محاور الدورة

### اليوم 1: التوعية بالأمن السيبراني

- ما هو الأمان؟ تعريف المبادئ الأساسية للأمن السيبراني.
- السرية والنزاهة والتوافر: أساسيات الأمن المعلوماتي.
- أساسيات الأمان: إعداد المعايير لتأمين الأنظمة.
- القلق الأمني: البشر: فهم دور الموظفين في الأمن السيبراني.
- أنواع التهديدات: استكشاف الهجمات السيبرانية وتأثيراتها.
- ضوابط الأمان: تطبيق التدابير الأمنية لتقليل المخاطر.
- ما هو الاختراق؟ فهم أساليب المهاجمين.
- إدارة المخاطر: تأسيس استراتيجية شاملة للأمن السيبراني.

### اليوم 2: اكتشاف الشبكات

- مراجعة الشبكات: المفاهيم الأساسية لفهم أمان الشبكات.
- الاكتشاف، التتبع والمسح: تقنيات المهاجمين لتقييم الأنظمة.
- الثغرات المعروفة والتعرضات: تحديد الثغرات التي تؤثر على أمان الشبكات.
- سياسات الأمان: أهمية إنشاء سياسات للأمن السيبراني.

### اليوم 3: بنية الأمان

- بنية الأمان: فهم هيكل الأنظمة الآمنة.
- أجهزة الشبكات والمناطق: كيفية حماية محيط الشبكة والمناطق الداخلية.
- تقسيم الشبكات: تقنيات تأمين قنوات الاتصال.
- التحكم في الوصول إلى الشبكة: حماية نقاط الوصول وطرق الاتصال.

### اليوم 4: أمن البيانات

- التشفير: حماية البيانات باستخدام التشفير.
- مبادئ الأذونات: كيفية تنفيذ التحكم في الوصول المناسب.
- التخفي: إخفاء المعلومات داخل أشكال بيانات أخرى.



## اليوم 5: إدارة الهوية

- ما هي إدارة الهوية؟ دور التوثيق في الأمن السيبراني.
- المعلومات الشخصية القابلة للتحديد: كيفية حماية البيانات الحساسة.
- عوامل التوثيق وخدمات الدليل: تأمين هوية المستخدمين وكلمات المرور.
- سياسات كلمات المرور: تنفيذ ضوابط كلمات مرور قوية لمنع الوصول غير المصرح به.

## اليوم 6: تقوية الشبكة

- تقليل الوصول عن بُعد: تقليل النقاط الضعيفة من خلال ضوابط الوصول.
- تقسيم الشبكات: أفضل الممارسات لحماية حركة الشبكة.
- تقليل الوصول الفعلي: تقوية الأمان باستخدام آليات التحكم الفيزيائي.

## اليوم 7: أمان البرمجيات

- هندسة البرمجيات: تطوير تطبيقات آمنة.
- إرشادات الأمان والثغرات: كيفية منع العيوب في أنظمة البرمجيات.
- مراقبة البيئة: استخدام الأدوات لمتابعة وحماية نشاط الأنظمة.

## اليوم 8: الأمان الفيزيائي

- ما هو الأمان الفيزيائي؟ أهمية الحماية الفيزيائية في الأمن السيبراني.
- الدفاع متعدد الطبقات: نهج متعدد لحماية الأمان الفيزيائي وأمن تكنولوجيا المعلومات.

## اليوم 9: الاستجابة للحوادث

- أنواع الكوارث: كيفية الاستعداد للكوارث السيبرانية المحتملة.
- تحقيق الحوادث: فهم كيفية الرد على الاختراقات.
- التخطيط لاستمرارية الأعمال: إعداد خطة للاستجابة للحوادث والتعافي من الكوارث.

## اليوم 10: اتجاهات في الأمن السيبراني

- قيود تصميم الأمن السيبراني: كيف تشكل الأنظمة الحديثة استراتيجيات الأمان السيبراني.
- القوى المؤثرة في الأمن السيبراني: فهم العوامل الرئيسية التي تقود تطور الأمن السيبراني.
- معايير الأمن السيبراني والتدريب: أهمية الامتثال و التدريب على الأمن السيبراني لجميع الموظفين.



## لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- معرفة شاملة في الأمن السيبراني: احصل على فهم كامل حول الأمن السيبراني الشامل وكيفية دمجه في مؤسستك.
- إدارة فعالة للمخاطر: تعلم كيفية تقييم وإدارة المخاطر السيبرانية من خلال دورات تدريبية لإدارة المخاطر السيبرانية.
- تطبيق واقعي: من خلال محاكاة الأمن السيبراني، ستتمكن من مواجهة التهديدات السيبرانية الحقيقية، مما يحسن استعدادك للدفاع عن مؤسستك في بيئة تهديدات متزايدة.
- خبرة عملية: تعلم كيفية تطوير استراتيجية شاملة للأمن السيبراني وتنفيذ عمليات الدفاع السيبراني باستخدام سيناريوهات واقعية.

## الخاتمة

تم تصميم هذه الدورة المتقدمة لتوفير فهم شامل حول كيفية بناء وتنفيذ وإدارة استراتيجية شاملة للأمن السيبراني. من خلال دورات التدريب على الأمن السيبراني ودراسات الحالة الواقعية، ستكتسب المهارات اللازمة لحماية مؤسستك ضد التهديدات المتزايدة في بيئة الإنترنت اليوم.

**سواء كنت تتطلع إلى تعزيز مهاراتك القيادية في الأمن السيبراني أو تحسين مرونة بنيتك التحتية التقنية، فإن هذه الدورة تعتبر موردا أساسيا للمهنيين في مجال الأمن السيبراني.**

