MERCURY

أمن الشبكات والمعلومات وتقييم الأنظمة الرقمية

09 - 13 مايو 2027

دبي (الإمارات العربية المتحدة)

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

أمن الشبكات والمعلومات وتقييم الأنظمة الرقمية

الرمز : 121494_170506 تاريخ الإنعقاد: 09 - 13 مايو 2027 دولة الإنعقاد: دبي (الإمارات العربية المتحدة) التكلفة: 4900 اليورو

مقدمة

تقدم هذه الدورة التدريبية في أمن الشبكات والمعلومات وتقييم الأنظمة الرقمية، إطارًا متكاملًا لحماية البنية التحتية الرقمية في المؤسسات الحديثة. تركز على تقييم سياسات وإجراءات الأمن السيبراني وتحسين فعالية الضوابط التقنية والتنظيمية. كما يتعرف المشاركون على منهجيات فحص أمن الشبكات والتحقق من سلامة الأنظمة والتطبيقات في بيئات العمل الواقعية. وتغطي تصميم الشبكات الآمنة ونشر الخوادم وأنظمة حماية الأجهزة الطرفية وفق أفضل الممارسات. وتركز على المراقبة المستمرة والتنسيق الفعّال لعمليات الأمن الرقمي. ويصبح المتدرب قادرًا على دعم استدامة الأمن السيبراني واتخاذ قرارات تقنية مدروسة.

الفئات المستهدفة

تستهدف دورة أمن الشبكات والمعلومات وتقييم الأنظمة الرقمية، الفئات والمحترفين للاكتساب المعرفة والمهارات:

- مختصو أمن المعلومات الراغبون في تطوير مهارات التقييم.
- مهندسو الشبكات المسؤولون عن تصميم البنية الآمنة.
- مسؤولو الأنظمة والخوادم في المؤسسات.
- محللو الأمن السيبراني ومراكز العمليات الأمنية.
- مدققو تقنية المعلومات والامتثال الرقمي.
- مسؤولو المخاطر وإدارة الحوكمة التقنية.
- فنيو الدعم التقني المتجهون لمجال الأمن.
- العاملون في حماية البنية التحتية الرقمية.

أهداف الدورة التدريبية

في نهاية هذا البرنامج التدريبي في أمن الشبكات والمعلومات وتقييم الأنظمة الرقمية، سيكون المشاركون قادرين على:

- فهم المفاهيم الأساسية في أمن الشبكات والمعلومات.
- تقييم سياسات وإجراءات الأمن الرقمي بفعالية.
- تحليل الثغرات في بيئات الشبكات المؤسسية.
- اختبار الضوابط الأمنية باستخدام منهجيات منظمة.
- تقديم توصيات لتحسين إطار الأمن السيبراني.
- تصميم شبكات آمنة تدعم متطلبات الأعمال.
- التحقق من أمن الأنظمة والتطبيقات المؤسسية.
- نشر الخوادم وفق معايير التهيئة الآمنة.
- تطبيق حلول حماية الأجهزة الطرفية.
- تنسيق عمليات المراقبة الأمنية المستمرة.
- متابعة حركة الشبكة باستخدام أدوات تحليل متقدمة.
- الحفاظ على الجاهزية الأمنية بشكل استباقي.
- دعم الامتثال لمعايير الأمن السيبراني الدولية.
- تعزيز القدرة على الاستجابة للحوادث الأمنية.

الكفاءات المستهدفة

سيكتسب المشاركون الكفاءات التالية من خلال برنامج أمن الشبكات والمعلومات وتقييم الأنظمة الرقمية:

- مهارات تقييم أمن الشبكات واكتشاف المخاطر.
- القدرة على مراجعة سياسات الأمن المعلوماتي.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

- إتقان تصميم الشبكات الآمنة وتقسيمها.
- كفاءة التحقق من أمن الأنظمة والتطبيقات.
- مهارات تقوية الخوادم ونشرها بشكل آمن.
- القدرة على إعداد ومراقبة حماية الأجهزة الطرفية.
- تطبيق تقنيات اختبار الأمن السيبراني.
- تنسيق عمليات الأمن وإعداد التقارير.
- استخدام أدوات المراقبة والتحليل الأمني.
- فهم عملي لاستراتيجيات الدفاع السيبراني المؤسسي.

دراسة سيناريوهات

في تدريب أمن الشبكات والمعلومات وتقييم الأنظمة الرقمية، سيطوّر المشاركون قدراتهم عبر دراسة السيناريوهات:

- تقييم الوضع الأمني لشبكة مؤسسة متوسطة الحجم.
- مراجعة سياسة أمن معلومات وتحديد فجواتها.
- تصميم بنية شبكة آمنة لبيئة أعمال متنامية.
- التحقق من إعدادات خادم وفق معايير الحماية.
- تحليل تنبيهات أمن الأجهزة الطرفية.
- تنسيق المراقبة ضمن مركز عمليات أمنية.
- اقتراح معالجات بعد اختبار الثغرات.
- الحفاظ على الحماية المستمرة في بيئة هجينة.

محتوى الدورة

الوحدة الأولى: أساسيات أمن الشبكات والمعلومات

- مفاهيم ومبادئ أمن الشبكات والمعلومات الحديثة.
- تطور التهديدات السيبرانية في البيئات الرقمية.
- فهم سطح الهجوم في البنية التحتية المؤسسية.
- مكونات أطر أمن المعلومات المؤسسية.
- مبادئ السرية والسلامة والتوافر في حماية الشبكات.
- مدخل إلى إدارة المخاطر السيبرانية.
- حوكمة الأمن الرقمي وتوزيع المسؤوليات.
- مواءمة استراتيجية الأمن مع استمرارية الأعمال.

الوحدة الثانية: تقييم سياسات وإجراءات الأمن الرقمي

- خصائص سياسات أمن المعلومات الفعّالة.
- منهجيات مراجعة وتدقيق إجراءات الأمن السيبراني.
- ربط السياسات بمتطلبات الامتثال التنظيمي.
- اكتشاف الفجوات في الأطر الأمنية الحالية.
- تطبيق منهج قائم على المخاطر في التحسين.
- تنسيق تنفيذ السياسات بين الإدارات.
- مراقبة فعالية السياسات عبر مؤشرات الأداء.
- إدارة توثيق وتحديث إجراءات الأمن.

الوحدة الثالثة: تصميم بنية الشبكات الآمنة

- مبادئ تصميم الشبكات الآمنة للمؤسسات.
- استراتيجيات التقسيم الشبكي والدفاع متعدد الطبقات.
- إعدادات التوجيه والتحويل الآمن.
- تأمين الوصول في الشبكات المحلية والسحابية.
- تطبيق الجدران النارية وضوابط الشبكة.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

- نشر الشبكات الافتراضية الخاصة VPN بأمان.
- التحكم في الوصول للشبكة المبني على الهوية.
- تحقيق التوافر العالي في البيئات الآمنة.

الوحدة الرابعة: نشر الخوادم وحماية الأنظمة الطرفية

- تقنيات تقوية الخوادم ونشرها الآمن.
- التحقق من إعدادات أنظمة التشغيل والتطبيقات.
- منصات حماية الأجهزة الطرفية وإعدادها.
- إدارة التحديثات ومعالجة الثغرات الأمنية.
- مراقبة الأجهزة الطرفية وكشف التهديدات.
- تأمين التطبيقات المؤسسية والخدمات.
- أساسيات التسجيل والتنبيه الأمني.
- الحفاظ على خطوط أساس أمنية موحدة.

الوحدة الخامسة: اختبار الأمن والمراقبة المستمرة

- منهجيات اختبار الأمن السيبراني المؤسسي.
- أساليب تقييم الثغرات الأمنية.
- المراقبة المستمرة وتحليل حركة الشبكة.
- تنسيق عمليات مركز الأمن والاستجابة.
- قياس الأداء الأمني بمؤشرات المخاطر.
- تعزيز الجاهزية السيبرانية المستدامة.
- إعداد توصيات تحسين مبنية على النتائج.
- بناء ثقافة التحسين الأمني المستمر.

خلاصة وتوصيات الدورة التدريبية

تمكّن هذه الدورة المشاركين من تقييم وتصميم وتشغيل بيئات أمن الشبكات والمعلومات بكفاءة عالية. كما تعزز قدرتهم على تطبيق المراقبة المستمرة وتحسين الوضع الأمني المؤسسي بشكل منهجي ومستدام.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

نموذج تسجيل :
أمن الشبكات والمعلومات وتقييم الأنظمة الرقمية

الرمز : 121494 تاريخ الإنعقاد: 09 - 13 مايو 2027 دولة الإنعقاد: دبي (الإمارات العربية المتحدة) التكلفة: 4900 اليورو

معلومات المشارك

الأسم الكامل (السيد / السيدة):
.....
المسمى الوظيفي: .....
الهاتف / الجوال: .....
البريد الإلكتروني الشخصي: .....
البريد الإلكتروني الرسمي: .....

معلومات جهة العمل

اسم الشركة: .....
العنوان: .....
المدينة / الدولة: .....

معلومات الشخص المسؤول عن ترشيح الموظفين

الأسم الكامل (السيد / السيدة):
.....
المسمى الوظيفي: .....
الهاتف / الجوال: .....
البريد الإلكتروني الشخصي: .....
البريد الإلكتروني الرسمي: .....

طرق الدفع

☐ الرجاء إرسال الفاتورة لي

☐ الرجاء إرسال الفاتورة لشركتي