MERCURY

إدارة مخاطر سلسلة توريد تكنولوجيا المعلومات

7 – 11 ديسمبر 2026

فيينا (النمسا)

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

MERCURY

إدارة مخاطر سلسلة توريد تكنولوجيا المعلومات

المرجع: 170422_121491 **التاريخ:** 7 – 11 ديسمبر 2026 **المكان:** فيينا (النمسا) **الرسوم:** Euro 5900

مقدمة

تهدف هذه الدورة التدريبية في إدارة مخاطر سلسلة توريد تكنولوجيا المعلومات، إلى تمكين المشاركين من فهم شامل لمخاطر الأمن السيبراني المرتبطة بسلسلة التوريد في بيئة تكنولوجيا المعلومات. تغطي السياسات والمعايير الدولية لإدارة مخاطر سلسلة التوريد ومتطلبات الامتثال المختلفة. كما تساعد المشاركين على تحديد التهديدات ونقاط الضعف المحتملة وتأثيراتها على عمليات المؤسسة. وتركز على تطوير خطط التخفيف من المخاطر وتعزيز الأمن السيبراني عبر سلسلة التوريد. وتتيح للمشاركين استخدام أدوات وتقنيات تقييم المخاطر بشكل عملي ونظري. وتدعم التعلم التطبيقي والنظري مع التركيز على أفضل الممارسات العالمية في إدارة المخاطر.

الفئات المستهدفة

تستهدف هذه الدورة التدريبية متخصصين يسعون لاكتساب المعرفة والمهارات:

- موظفو تقنية المعلومات ومسؤولو الأمن السيبراني.
- مدراء سلسلة التوريد وتقنيات العمليات.
- متخصصو الامتثال وإدارة المخاطر.
- خبراء تدقيق الأنظمة وتقنيات التحكم الداخلي.
- القادة والمسؤولون عن استمرارية الأعمال.
- المستشارون في تقييم المخاطر السيبرانية.
- أي مهنيين يعملون مع الموردين أو الشركاء التقنيين.

أهداف الدورة التدريبية

يحقق المشاركون الأهداف التالية عند إتمام دورة إدارة مخاطر سلسلة توريد تكنولوجيا المعلومات:

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

- فهم مفاهيم إدارة المخاطر السيبرانية المرتبطة بسلسلة التوريد.
- التعرف على سياسات ومعايير إدارة مخاطر سلسلة التوريد.
- تحديد التهديدات ونقاط الضعف المرتبطة بتكنولوجيا المعلومات.
- تقييم تأثير المخاطر على العمليات والأنظمة.
- تطوير خطط استراتيجية للتخفيف من المخاطر.
- تحسين القدرة على اتخاذ القرارات الأمنية المستندة إلى تقييم المخاطر.
- تعزيز قدرات مراقبة الامتثال والسياسات الداخلية.
- دمج أفضل الممارسات العالمية في حماية سلسلة التوريد.
- إدارة العلاقات مع الموردين لضمان الأمن المستدام.
- استخدام أدوات وتقنيات تقييم المخاطر بشكل عملي وفعّال.

الكفاءات المستهدفة

يكتسب المشاركون الكفاءات التالية خلال برنامج إدارة مخاطر سلسلة توريد تكنولوجيا المعلومات:

- القدرة على تحليل المخاطر وتحديد التهديدات.
- معرفة متعمقة بسياسات حماية سلسلة التوريد.
- مهارات تقييم نقاط الضعف والتأثيرات المحتملة.
- قدرة تطوير خطط التخفيف والاستجابة للطوارئ.
- مهارات إدارة المخاطر السيبرانية ضمن بيئة المؤسسات.
- فهم طرق قياس أداء الأمن السيبراني.
- القدرة على التعامل مع الموردين لضمان الامتثال.
- مهارات اتخاذ قرارات أمنية استراتيجية وفعّالة.
- استخدام الأدوات والتقنيات الحديثة لتقييم المخاطر.
- تعزيز الوعي بالتهديدات الإلكترونية وحماية المعلومات الحساسة.

دراسة سيناريوهات

في تدريب إدارة مخاطر سلسلة توريد تكنولوجيا المعلومات، يطور المشاركون المهارات من خلال السيناريوهات التالية:

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

- تحليل تهديدات سلسلة التوريد لتحديد نقاط الضعف.
- دراسة حالات فشل الأمن السيبراني وتأثيرها على المؤسسات.
- تقييم إجراءات الموردين وممارساتهم الأمنية.
- وضع خطط استجابة لمخاطر محتملة.
- اختبار تقنيات تقليل المخاطر وتطبيقها في بيئة افتراضية.
- محاكاة الهجمات السيبرانية على سلاسل التوريد.
- مراجعة استراتيجيات الامتثال والسياسات الداخلية.

محتوى الدورة

الوحدة 1: مفاهيم وأساسيات إدارة مخاطر سلسلة التوريد

- تعريف إدارة مخاطر سلسلة التوريد وأهميتها.
- العلاقة بين الأمن السيبراني وسلسلة التوريد.
- أنواع التهديدات السيبرانية وتأثيرها على سلسلة التوريد.
- دور السياسات والمعايير الدولية في إدارة المخاطر.
- التعرف على العناصر الأساسية لسلسلة التوريد الرقمية.
- المفاهيم الأساسية لتقييم المخاطر ونقاط الضعف.

الوحدة 2: سياسات ومعايير إدارة المخاطر

- استعراض سياسات إدارة المخاطر الداخلية والخارجية.
- المعايير الدولية لحماية سلسلة التوريد لتكنولوجيا المعلومات.
- متطلبات الامتثال وأهميتها في حماية الأعمال.
- دور الإجراءات والسياسات في الوقاية من المخاطر.
- تطوير سياسات أمنية متوافقة مع أفضل الممارسات.
- دمج الأمن السيبراني في عمليات سلسلة التوريد.

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

MERCURY

الوحدة 3: تحديد التهديدات ونقاط الضعف

- أساليب التعرف على التهديدات الرقمية والموردين.
- أدوات تقييم نقاط الضعف والتأثيرات المحتملة.
- تقييم المخاطر المرتبطة بالتعاقدات والشركاء.
- دراسة سيناريوهات الهجمات المحتملة على سلسلة التوريد.
- تحديد أولويات المخاطر وفق تأثيرها على العمليات.
- استخدام مؤشرات الأداء لمتابعة نقاط الضعف.

الوحدة 4: استراتيجيات التخفيف وخطط الطوارئ

- تطوير خطط التخفيف من المخاطر المحتملة.
- استراتيجيات إدارة المخاطر السيبرانية المستمرة.
- إعداد خطط استجابة للطوارئ وحالات الانقطاع.
- تكامل خطط الأمن السيبراني مع استمرارية الأعمال.
- طرق حماية البيانات الحساسة والمعلومات الحيوية.
- مراجعة وتحديث الخطط بشكل دوري لضمان الفاعلية.

الوحدة 5: تقييم الأداء والتحسين المستمر

- قياس فعالية خطط إدارة المخاطر.
- استخدام مؤشرات الأداء لقياس الأمن السيبراني.
- مراجعة نتائج التقييم وتحديد التحسينات المطلوبة.
- تطوير خطط تحسين مستمرة لأمن سلسلة التوريد.
- دمج أفضل الممارسات العالمية لضمان حماية مستدامة.
- متابعة الابتكارات والتقنيات الحديثة في مجال الأمن السيبراني.
- تقديم تقارير شاملة للإدارة العليا عن مستوى المخاطر والسياسات.

خلاصة وتوصيات الدورة التدريبية

تعزز الدورة قدرة المشاركين على إدارة مخاطر سلسلة توريد تكنولوجيا المعلومات بفعالية. توفر أدوات واستراتيجيات عملية لتقليل التهديدات وتعزيز الأمن السيبراني داخل المؤسسات.