MERCURY

إدارة المخاطر السيبرانية وسلسلة التوريد

21 - 25 سبتمبر 2026
لندن (المملكة المتحدة)

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

MERCURY

إدارة المخاطر السيبرانية وسلسلة التوريد

الرمز : 121493_170480 تاريخ الإنعقاد: 21 - 25 سبتمبر 2026 دولة الإنعقاد: لندن (المملكة المتحدة) التكلفة: 5900 اليورو

مقدمة

تهدف دورة إدارة المخاطر السيبرانية وسلسلة التوريد إلى تزويد المشاركين بفهم عميق لإدارة مخاطر سلسلة التوريد الرقمية والتقنيات الأمنية المرتبطة بحماية أنظمة تكنولوجيا المعلومات. تركز الدورة على تحليل التهديدات السيبرانية التي تواجه الموردين والشركاء في الشبكات الرقمية وكيفية تقييم تأثيرها على أمن المؤسسة. تتضمن الدورة سياسات إدارة المخاطر والسيطرة على نقاط الضعف وتحديد الإجراءات الاستباقية للتخفيف من المخاطر والتعرضات الأمنية. كما تستعرض الدورة نماذج وتطبيقات عملية لتعزيز مهارات المشاركين في تصميم خطط أمن سلسة التوريد. تُعد هذه الدورة أساسية للمهتمين بحوكمة أمن المعلومات وعمليات تقييم سلسلة التوريد من منظور شامل. وبنهاية التدريب، يكون المشاركون قادرين على صياغة وتنفيذ استراتيجيات إدارة مخاطر تقنية المعلومات للموردين.

الفئات المستهدفة

هذه الدورة التدريبية إدارة المخاطر السيبرانية وسلسلة التوريد تستهدف محترفين يسعون للاكتساب المعرفة والمهارات:

- مديرو أمن المعلومات ومسؤولو الأمن السيبراني.
- مهندسو الشبكات وبنية وحوكمة تكنولوجيا المعلومات.
- محللو مخاطر تقنية المعلومات وسلسلة التوريد.
- مسؤولو الامتثال والحوكمة والرقابة الداخلية.
- مسؤولو المشتريات والتوريد المرتبط بتكنولوجيا المعلومات.
- قادة مشاريع تقنية المعلومات والمستشارون الأمنيون.
- باحثون في الأمن الرقمي والتحقيقات التقنية.

أهداف الدورة التدريبية

المشاركون سيحققون الأهداف التالية عند إتمام دورة إدارة المخاطر السيبرانية وسلسلة التوريد:

- فهم أساسيات إدارة مخاطر سلسلة التوريد الرقمية وأهميتها في بيئات المؤسسات.
- التمييز بين المخاطر الداخلية والخارجية وتأثيرها على نظم تكنولوجيا المعلومات.
- تحليل هجمات الأمن السيبراني الشائعة المرتبطة بسلسلة التوريد الرقمية.
- التعرّف على سياسات وإجراءات توثيق الموردين وتقويم أمنهم.
- تصميم إطار عملي لتحديد التهديدات ونقاط الضعف في نظم المعلومات الخاصة بالموردين.
- بناء قدرات تقييم تأثير المخاطر وتقدير مستوى التعرض الأمني.
- التخطيط لمعايير التخفيف الأمني وتقنيات حماية البيانات الحسّاسة.
- تطبيق حلول أمنية متقدمة لتعزيز مرونة سلسلة التوريد ضد التهديدات السيبرانية.
- تعزيز الاتساق بين إدارة المخاطر والتزام المؤسسة بلوائح حماية البيانات.
- تطوير خطط تنفيذية للاستجابة للحوادث وتأمين شبكات الإمداد الرقمي.

الكفاءات المستهدفة

المشاركون سيكتسبون الكفاءات التالية أثناء برنامج إدارة المخاطر السيبرانية وسلسلة التوريد:

- القدرة على تقييم مخاطر سلسلة التوريد الرقمية باستخدام أدوات تحليل متقدمة.
- مهارة تطبيق معايير الأمن السيبراني في بيئات الموردين المختلفة.
- الكفاءة في إعداد سياسات وتقارير تقييم المخاطر التقنية بوضوح.
- التمكن من توصيف نقاط الضعف وتصنيفها وفق مستويات أولويتها.
- القدرة على تصميم وتنفيذ أنظمة مراقبة الأنشطة المشبوهة لشبكات التوريد.
- مهارة اختيار وتطبيق ضوابط أمنية رقمية فعّالة.

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

- الكفاءة في وضع خطط الاستجابة للحوادث وتقليل تأثيرها على عمليات المؤسسة.
- مهارة التواصل الأمني الداخلي وتنسيق فرق العمل المتعددة.
- الإلمام بإجراءات الامتثال القانوني والتنظيمي لأمن سلسلة التوريد الرقمية.

دراسة سيناريوهات

في هذه الدورة إدارة المخاطر السيبرانية وسلسلة التوريد، يطور المشاركون المهارات من خلال السيناريوهات التالية:

- تقييم حالة هجوم إلكتروني على مورد رئيسي لشركة تقنية.
- تحليل ثغرة في نظام إمداد رقمي وتقدير تأثيرها على بيانات العملاء.
- وضع خطة استجابة سريعة لحادث اختراق في البنية التحتية للمورد.
- سيناريو محاكاة إدارة تحديثات أمنية عبر شبكات الموردين.
- تحليل كلفة المخاطر وتحديد أولوية تنفيذ الضوابط الأمنية.
- خطة تقويم دورية لامتثال الموردين لمعايير أمن المعلومات.
- سيناريو تواصل فريق عمل لحل أزمة اختراق معلومات الموردين.

محتوى الدورة التدريبية

الوحدة الأولى: أساسيات إدارة المخاطر السيبرانية وسلسلة التوريد

- مقدمة في مفاهيم الأمن السيبراني وأهمية حماية بيانات سلسلة التوريد الرقمية.
- التعريف بنظام إدارة المخاطر وسياقه في بيئات تكنولوجيا المعلومات الحديثة.
- العناصر الأساسية لمخاطر سلسلة التوريد الرقمية وتأثيرها على الأمن المؤسسي.
- فهم الفجوات الأمنية في شبكات الإمداد الرقمية وتحديد مصادر التهديد.
- أنواع الهجمات السيبرانية المرتبطة بالموردين وتأثيرها على الأداء المؤسسي.
- التمييز بين المخاطر التشغيلية والمخاطر التقنية في سلسلة التوريد.

الوحدة الثانية: سياسات إدارة المخاطر في سلسلة التوريد

- وضع سياسة موحدة لإدارة مخاطر الموردين وشركاء التوريد الرقمي.
- معايير اختيار الموردين بناءً على مستوى الأمان والامتثال.
- إجراءات توثيق الموردين وتاريخ الامتثال الأمني.
- تحديد صلاحيات الوصول والتحكم الأمني داخل الشبكات المشتركة.
- أساليب مراقبة الأنشطة الرقمية غير المصرح بها.
- تطبيق نماذج تقييم المخاطر والاستجابة لها.
- العوامل التنظيمية والقانونية في صياغة سياسات أمن سلسلة التوريد.

الوحدة الثالثة: تحديد التهديدات وتحليل نقاط الضعف

- منهجيات تحليل ثغرات نظم المعلومات في بيئات الموردين.
- أدوات وتقنيات تقييم التهديدات الرقمية.
- تحليل العلاقة بين الموردين والأنظمة الداخلية للشركة.
- استخدام نماذج التهديد لتصنيف التعرّض الأمني.
- تحديد مؤشرات الانتهاك الأمني ضمن سلسلة التوريد.
- توثيق نتائج تحليل نقاط الضعف وتحديد أولوياتها.
- قياس مستوى التعرض وفق معايير تقييم الأداء الأمني.

الوحدة الرابعة: تقييم تأثير التهديدات ووضع خطط التخفيف

- تحليل أثر الهجمات السيبرانية على استمرار الأعمال ضمن سلسلة التوريد.
- أساليب قياس خسائر البيانات وتأثيرها على سمعة المؤسسة.
- تصميم استراتيجيات التخفيف الأمني بناءً على تقييمات موثوقة.

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

- تقنيات تقليل تأثير اختراق بيانات الموردين.
- تطبيق معايير مقاومة المخاطر ضمن بيئات السحابة وخدمات الأطراف الثالثة.
- اختبارات محاكاة للاستجابة المؤسسة في حالات الهجوم.
- قياس فعالية الضوابط الأمنية بعد تنفيذ خطط التخفيف.

الوحدة الخامسة: أطر متقدمة واستدامة الأمن في سلاسل التوريد

- دمج أمن سلسلة التوريد في منظومة الحوكمة الشاملة للمؤسسة.
- إدارة تحديثات الأمن الدوري للموردين الخارجيين.
- تصميم برامج تدريب مستمرة لفرق العمل الرقمي.
- أدوات الذكاء الاصطناعي لرصد التهديدات المستقبلية.
- تطوير خطط استمرارية الأعمال بعد الحوادث الأمنية.
- قياس التحسن الأمني المستدام وتحديثات السياسات الدورية.
- بلورة ثقافة أمنية مشتركة بين المؤسسة والموردين.

خلاصة وتوصيات الدورة التدريبية

.تعزز هذه الدورة قدرة المشاركين على فهم وتطبيق منهجيات أمن سلسلة التوريد الرقمي وإدارة المخاطر السيبرانية بكفاءة عالية. تبني لديهم القدرة على تصميم وتنفيذ استراتيجيات حماية متكاملة وتقييم مستمر لتهديدات تكنولوجيا المعلومات في بيئات الموردين.

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

MERCURY

نموذج تسجيل :

إدارة المخاطر السيبرانية وسلسلة التوريد

الرمز : 121493 تاريخ الإنعقاد: 21 - 25 سبتمبر 2026 دولة الإنعقاد: لندن (المملكة المتحدة) التكلفة: 5900 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