MERCURY

دورة الأمن السيبراني وإدارة المخاطر المؤسسية

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

MERCURY

دورة الأمن السيبراني وإدارة المخاطر المؤسسية

مقدمة:

تهدف هذه الدورة التدريبية في الأمن السيبراني وإدارة المخاطر المؤسسية، إلى تمكين المشاركين من فهم شامل لكيفية حماية أصول المعلومات من التهديدات السيبرانية المتزايدة في بيئة الأعمال الحديثة. تستعرض العلاقة التكاملية بين الأمن السيبراني وإدارة المخاطر المؤسسية، مع التركيز على تقييم المخاطر وتنفيذ الضوابط الأمنية المناسبة. ستزود المتدربين بالمعرفة الضرورية لفهم الهجمات السيبرانية وأساليب الوقاية منها وكيفية تطوير استراتيجية متكاملة لإدارة المخاطر.

تشمل دورة الأمن السيبراني وإدارة المخاطر المؤسسية، تحليل الثغرات، والاستجابة للحوادث، واستمرارية الأعمال، بالإضافة إلى الامتثال للتشريعات والمعايير الدولية. يتناول المحتوى تطبيق أدوات وأساليب تحليل المخاطر على مستوى المؤسسات لتحقيق حماية فعالة للبنية التحتية الرقمية. كما تهدف إلى تعزيز قدرة المشاركين على اتخاذ قرارات مبنية على تحليل دقيق للمخاطر الأمنية. الدورة مصممة لتزويد المتدربين بالمهارات التطبيقية والاستراتيجية التي تؤهلهم للمشاركة الفعالة في بناء بيئة عمل آمنة ومستقرة.

الفئات المستهدفة:

تستهدف دورة الأمن السيبراني وإدارة المخاطر المؤسسية، الفئات والمحترفين الذين يسعون للاكتساب المعرفة والمهارات:

- مسؤولو الأمن السيبراني في المؤسسات.
- مدراء المخاطر المؤسسية والحوكمة.
- موظفو تكنولوجيا المعلومات والشبكات.
- المحللون الأمنيون والاستراتيجيون الرقميون.
- قادة التحول الرقمي.
- مستشارو الامتثال وإدارة المخاطر.
- مدراء الأنظمة ومشاريع البنية التحتية.
- مسؤولو حماية البيانات والخصوصية.
- الراغبون في التخصص في أمن المعلومات.
- العاملون في قطاع الخدمات المالية والطاقة والصحة.

أهداف الدورة التدريبية:

في نهاية هذا البرنامج التدريبي في الأمن السيبراني وإدارة المخاطر المؤسسية، سيكون المشاركون قادرين على:

- تحليل التهديدات السيبرانية وتقييم تأثيرها على المؤسسات.
- تحديد مواطن الضعف في الأنظمة الرقمية واقتراح حلول فعالة.
- تصميم استراتيجيات أمنية قابلة للتنفيذ ضمن الهيكل المؤسسي.
- تطبيق ضوابط أمن المعلومات وفقاً للمعايير العالمية.
- تقييم الأثر التشغيلي والمالي للمخاطر السيبرانية.
- تطوير خطط الاستجابة للحوادث وتعزيز استمرارية الأعمال.
- بناء نظام متكامل لإدارة المخاطر المؤسسية يدعم الأهداف التنظيمية.
- دمج الأمن السيبراني ضمن ثقافة المؤسسة واستراتيجياتها.
- تحسين قدرات اتخاذ القرار في ظل بيئة تهديدات متغيرة.
- تقييم الالتزام باللوائح الوطنية والدولية ذات الصلة.
- مراقبة وتحديث نظم الحماية باستمرار بناءً على تحليل البيانات.
- تطبيق أفضل الممارسات لإدارة الحوكمة الأمنية والسياسات المؤسسية.
- تعزيز الوعي المؤسسي تجاه التهديدات السيبرانية.
- تنفيذ إجراءات حماية استباقية تقلل من احتمالية التعرض للاختراقات.

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

MERCURY

الكفاءات المستهدفة:

سيكتسب المشاركون الكفاءات التالية من خلال برنامج الأمن السيبراني وإدارة المخاطر المؤسسية:

- مهارة تحليل التهديدات الرقمية وتفسيرها.
- القدرة على تصميم أنظمة حماية فعالة.
- تقييم المخاطر واتخاذ قرارات استراتيجية.
- فهم شامل لمعايير الأمن السيبراني الدولية.
- مهارة إدارة الحوادث الرقمية والاستجابة لها.
- دمج نظم الحوكمة والمخاطر والامتثال.
- تطوير خطط استمرارية الأعمال.
- تحليل تأثير المخاطر على العمليات المؤسسية.
- مراقبة أداء الأمن السيبراني وتحسينه.

محتوى الدورة التدريبية:

الوحدة الأولى: أساسيات الأمن السيبراني:

- مقدمة عن الأمن السيبراني وأهميته في العصر الرقمي.
- مفاهيم رئيسية في حماية المعلومات وأنواع الأصول الرقمية.
- الفرق بين التهديدات والهجمات والاختراقات.
- تصنيفات الهجمات الإلكترونية وأساليب تنفيذها.
- مفاهيم المصادقة، التشفير، والتكامل.
- أمن الشبكات وأنظمة الحماية متعددة الطبقات.
- الأثر التشغيلي والمالي للاختراقات.
- أمثلة على اختراقات كبيرة وتأثيرها المؤسسي.

الوحدة الثانية: مقدمة في إدارة المخاطر المؤسسية:

- تعريف إدارة المخاطر وأنواع المخاطر المؤسسية.
- علاقة المخاطر المؤسسية بالأمن السيبراني.
- خطوات تقييم وتحليل المخاطر.
- أدوات ومنهجيات تحليل المخاطر مثل: SWOT, ISO 31000.
- تحديد أولويات المخاطر وترتيبها وفق التأثير والاحتمال.
- تطوير استراتيجيات الاستجابة للمخاطر.
- دمج إطار إدارة المخاطر في عمليات الأعمال.
- مراجعة خطط الطوارئ واستمرارية الأعمال.

الوحدة الثالثة: الامتثال والمعايير الدولية:

- أهمية الامتثال في الأمن السيبراني وحوكمة المخاطر.
- نظرة عامة على معايير مثل ISO/IEC 27001 وNIST.
- متطلبات الامتثال للائحة حماية البيانات العامة GDPR.
- تقييم جاهزية المؤسسات للامتثال.
- دور المدقق الداخلي في التحقق من الالتزام.
- تصميم سياسات الأمن السيبراني الفعالة.
- بناء إطار الحوكمة الأمنية.
- تحليل الفجوات وإعداد خطط الامتثال.

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

MERCURY

الوحدة الرابعة: الاستجابة للحوادث وإدارة الطوارئ:

- تعريف الحوادث الأمنية الرقمية.
- منهجيات الاستجابة للحوادث الإلكترونية.
- إنشاء فريق الاستجابة للحوادث CSIRT.
- خطوات التحقيق الرقمي وتحليل الأدلة.
- إدارة الاتصالات خلال الأزمة السيبرانية.
- استخدام أدوات كشف التهديدات والرد السريع.
- إعادة تشغيل الأنظمة والتعافي بعد الهجوم.
- مراجعة الحوادث وتحديد فرص التحسين.

الوحدة الخامسة: استمرارية الأعمال والتعافي من الكوارث:

- مفاهيم الاستمرارية المؤسسية في بيئة التهديدات.
- تحليل تأثير الأعمال BIA.
- تحديد الوظائف الحيوية وضمان تشغيلها أثناء الأزمات.
- تطوير خطة التعافي من الكوارث DRP.
- اختبار السيناريوهات وتحسين الخطط.
- دور تقنيات الحوسبة السحابية في الاستمرارية.
- تنسيق العمل بين فرق تكنولوجيا المعلومات والإدارة العليا.
- مراجعة السياسات وإعادة تقييم المخاطر بعد الطوارئ.

الوحدة السادسة: بناء ثقافة مؤسسية للأمن السيبراني:

- دور القيادة في ترسيخ الوعي الأمني.
- تنفيذ برامج التوعية والتدريب للعاملين.
- تعزيز سلوكيات الأمان الرقمي في بيئة العمل.
- تطوير مؤشرات أداء ثقافة الأمن السيبراني.
- قياس فعالية المبادرات التوعوية.
- ربط الأمن السيبراني بالأهداف الاستراتيجية.
- استخدام الذكاء الاصطناعي في تعزيز الوعي.
- دمج الأمن ضمن إجراءات التوظيف والتقييم المؤسسي.
- بناء شراكات أمنية استراتيجية داخل المؤسسة وخارجها.

خلاصة وتوصيات الدورة التدريبية:

تُعد هذه الدورة التدريبية في الأمن السيبراني وإدارة المخاطر المؤسسية، منصة متكاملة لفهم العلاقة الحيوية بين الأمن السيبراني وإدارة المخاطر المؤسسية. تقدم أدوات واستراتيجيات حديثة لحماية المؤسسات من التهديدات الإلكترونية. كما تُمكّن المشاركين من تطبيق ضوابط أمنية فعالة ضمن إطار الحوكمة الشاملة. نوصي بتطبيق المفاهيم المكتسبة في تطوير سياسات أمنية فعالة تضمن استدامة الأداء المؤسسي.