MERCURY

دورة الأمن السيبراني للشركات: تأمين البيانات والامتثال

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

MERCURY

دورة الأمن السيبراني للشركات: تأمين البيانات والامتثال

مقدمة:

في ظل تصاعد التهديدات السيبرانية وتزايد الاعتماد على الأنظمة الرقمية في الشركات، أصبحت حماية البيانات وامتثال الأنظمة من الأولويات الحيوية لضمان استمرارية الأعمال. تهدف هذه الدورة التدريبية في الأمن السيبراني للشركات: تأمين البيانات والامتثال، المتخصصة إلى تمكين المشاركين من فهم الأبعاد المتعددة للأمن السيبراني في بيئة الشركات.

تغطي دورة الأمن السيبراني للشركات: تأمين البيانات والامتثال، أفضل الممارسات العالمية في حماية البيانات والامتثال التشريعي والتنظيمي. كما تسلط الضوء على آليات التصدي للاختراقات والهجمات السيبرانية، وتطوير سياسات أمنية فعالة تلبي متطلبات الهيئات الرقابية. يتم تدريب المشاركين على كيفية تقييم المخاطر وتطبيق استراتيجيات التخفيف ضمن البنية التحتية الرقمية للمؤسسات.

تشمل الدورة التدريبية في الأمن السيبراني للشركات: تأمين البيانات والامتثال، أيضًا الجوانب القانونية والتنظيمية المرتبطة بحوكمة البيانات والخصوصية. بنهاية الدورة، سيكون المشاركون قادرين على بناء إطار شامل للأمن السيبراني يعزز من جاهزية الشركة ويضمن الامتثال المستدام.

الفئات المستهدفة:

تستهدف دورة الأمن السيبراني للشركات: تأمين البيانات والامتثال، الفئات والمحترفين الذين يسعون لاكتساب المعرفة والمهارات:

- مدراء تقنية المعلومات في المؤسسات.
- مسؤولو الأمن السيبراني في الشركات.
- خبراء الامتثال القانوني والتنظيمي.
- مسؤولو حماية البيانات.
- مدراء المخاطر التشغيلية.
- موظفو إدارة البنية التحتية الرقمية.
- مدراء مراكز البيانات.
- محللو أمن المعلومات.
- الاستشاريون في تكنولوجيا المعلومات.
- موظفو أقسام الحوكمة والامتثال.
- المهندسون المتخصصون في نظم الحماية الرقمية.

الكفاءات المستهدفة:

سيكتسب المشاركون الكفاءات التالية من خلال برنامج الأمن السيبراني للشركات: تأمين البيانات والامتثال:

- القدرة على تصميم إطار عمل متكامل للأمن السيبراني.
- مهارة تحليل التهديدات الرقمية وقياس مخاطرها.
- فهم عميق لقوانين حماية البيانات والخصوصية.
- إتقان أدوات التحقق من الامتثال الرقمي.
- التفاعل مع الحوادث السيبرانية بكفاءة واستجابة فورية.
- إعداد خطط النسخ الاحتياطي والتعافي بعد الكوارث.
- استخدام أنظمة إدارة الحماية والشبكات بأمان.
- تطوير استراتيجيات حماية المعلومات الحساسة.
- تحسين ثقافة الأمن داخل المؤسسة.
- دعم اتخاذ القرار المبني على بيانات أمنية وتحليل المخاطر.

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

MERCURY

أهداف الدورة التدريبية:

في نهاية هذا البرنامج التدريبي في الأمن السيبراني للشركات: تأمين البيانات والامتثال، سيكون المشاركون قادرين على:

- تحديد أهم التهديدات السيبرانية التي تواجه الشركات.
- تحليل نقاط الضعف في البنية التحتية الرقمية المؤسسية.
- تصميم سياسات أمن معلومات متوافقة مع التشريعات التنظيمية.
- تنفيذ استراتيجيات لحماية البيانات الحساسة من التسريب.
- تقييم المخاطر الإلكترونية ووضع خطط استجابة فعالة.
- تطبيق تقنيات التشفير والنسخ الاحتياطي لحماية البيانات.
- تطوير خطة استجابة للحوادث السيبرانية بكفاءة عالية.
- تمييز الفروقات بين المعايير الدولية في أمن المعلومات.
- مراقبة الامتثال المستمر للأنظمة المحلية والدولية.
- بناء ثقافة أمن معلومات شاملة داخل بيئة العمل.
- استخدام أدوات تحليل التهديدات للكشف المبكر عن الاختراقات.
- تحسين الوعي السيبراني بين الموظفين للحد من الهجمات.
- دمج الأمن السيبراني ضمن استراتيجيات الحوكمة المؤسسية.
- إعداد تقارير امتثال دقيقة تلبي متطلبات التدقيق والجهات الرقابية.

محتوى الدورة التدريبية:

الوحدة الأولى: مقدمة في الأمن السيبراني والامتثال المؤسسي:

- التعريف بمفهوم الأمن السيبراني وأهميته في الشركات الحديثة.
- العلاقة بين حماية البيانات وحوكمة المعلومات.
- الفرق بين أمن المعلومات والأمن السيبراني.
- استعراض أبرز التهديدات السيبرانية في بيئة الأعمال.
- أهمية الامتثال التنظيمي لحماية سمعة المؤسسة.
- الدور القانوني للامتثال في أمن المعلومات.
- نظرة عامة على المعايير الدولية مثل ISO/IEC 27001 وGDPR.
- أثار اختراق البيانات على استمرارية الأعمال.
- كيفية بناء ثقافة أمن سيبراني مستدامة.

الوحدة الثانية: حماية البيانات وتقنيات الأمان الحديثة:

- أنواع البيانات المؤسسية وطرق تصنيفها.
- تطبيق تقنيات التشفير لحماية البيانات أثناء النقل والتخزين.
- اليات التحقق من الهوية وإدارة الوصول.
- استخدام الجدران النارية ونظم الكشف عن التسلل.
- أدوات حماية الأجهزة الطرفية والبنية السحابية.
- تأمين تطبيقات الويب والأنظمة التشغيلية.
- الحماية من البرامج الخبيثة وهجمات الفدية.
- استراتيجيات النسخ الاحتياطي والتخزين الآمن.
- التحكم في مشاركة البيانات الداخلية والخارجية.

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

MERCURY

الوحدة الثالثة: تقييم المخاطر السيبرانية واستمرارية الأعمال:

- مفاهيم تقييم المخاطر والتحليل الاحتمالي.
- إعداد سجل شامل لمخاطر الأمن السيبراني.
- بناء خطة استجابة فعالة للحوادث.
- تطوير خطة استمرارية الأعمال واستعادة البيانات.
- منهجيات تحليل تأثير المخاطر على العمليات التشغيلية.
- ربط خطط الطوارئ بالأمن السيبراني.
- استخدام نظم إدارة الحوادث السيبرانية.
- تدريب الفرق على تنفيذ الاستجابة للحوادث.
- قياس فعالية خطط الطوارئ وتحديثها دوريًا.

الوحدة الرابعة: الامتثال التنظيمي والحوكمة السيبرانية:

- المتطلبات القانونية المتعلقة بحماية البيانات.
- قوانين وتشريعات الأمن السيبراني في الدول العربية والعالم.
- دور الامتثال في تفادي الغرامات والعقوبات.
- إعداد سياسات وإجراءات تنظيمية واضحة.
- التدقيق الداخلي والرقابة على الامتثال.
- تقارير الامتثال ومستندات الإثبات.
- تطبيق مبادئ الشفافية والمساءلة في الأمن السيبراني.
- استعراض حالات عملية لفشل الامتثال وتأثيرها المالي.
- العلاقة بين الامتثال والسمعة المؤسسية.

الوحدة الخامسة: بناء بيئة أمنية مستدامة داخل الشركات:

- التوعية المستمرة للموظفين بالمخاطر السيبرانية.
- تصميم برامج تدريبية لتعزيز السلوك الأمني.
- تبني نموذج الأمن متعدد الطبقات Depth in Defense.
- التكامل بين الفرق التقنية والإدارية في تنفيذ السياسات.
- مراقبة الأنظمة بشكل دوري للكشف المبكر.
- تطوير نظام للبلاغات عن التهديدات الداخلية.
- تعزيز التعاون بين الأقسام لضمان الامتثال الجماعي.
- دور القيادة التنفيذية في إنجاح برامج الأمن السيبراني.
- مراجعة دورية للإستراتيجيات الأمنية وتحديثها بناءً على التهديدات المتغيرة.

خلاصة وتوصيات الدورة التدريبية:

تشكل دورة الأمن السيبراني للشركات: تأمين البيانات والامتثال، ركيزة أساسية لتطوير البنية الأمنية للشركات وتعزيز الامتثال الرقمي. من خلال التعمق في التهديدات السيبرانية وتقنيات الحماية، يستطيع المشاركون بناء استراتيجيات فعالة لحماية بيانات مؤسساتهم. الامتثال التنظيمي لم يعد خيارًا بل ضرورة لضمان الاستمرارية والثقة. نوصي الشركات باعتماد برامج تدريب دورية لضمان جاهزية كوادرها في مواجهة التحديات السيبرانية.