MERCURY

إدارة جودة البيانات وتقييم أنظمة الأمن الرقمي

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

إدارة جودة البيانات وتقييم أنظمة الأمن الرقمي

المقدمة

تقدم هذه الدورة التدريبية في إدارة جودة البيانات وتقييم أنظمة الأمن الرقمي، إطارًا متكاملًا لضمان موثوقية البيانات وتعزيز الحماية السيبرانية في المؤسسات الحديثة. تركز على الربط بين حوكمة جودة البيانات وممارسات تقييم الأمن الرقمي لدعم اتخاذ القرار المبني على بيانات دقيقة وآمنة. كما يتعرف المشاركون على منهجيات تقييم واختبار والتوصية وتنسيق ومراقبة وصيانة سياسات وإجراءات وأنظمة الأمن الرقمي بكفاءة عالية. تنمّي القدرة على التحقق من الأنظمة والتطبيقات وفق أفضل الممارسات الأمنية المؤسسية. وتركز أيضاً على تصميم الشبكات الآمنة ونشر الخوادم وأنظمة أمن النقاط الطرفية ضمن بيئات تقنية معقدة. وسيصبح المشاركون قادرين على رفع مستوى سلامة البيانات وتقليل المخاطر السيبرانية ودعم التحول الرقمي الآمن.

الفئات المستهدفة

تستهدف دورة إدارة جودة البيانات وتقييم أنظمة الأمن الرقمي، الفئات والمحترفين لاكتساب المعرفة والمهارات:

- مديرو جودة البيانات وحوكمة البيانات.
- مختصو الأمن السيبراني وأمن المعلومات.
- مدققو تقنية المعلومات وإدارة المخاطر.
- مسؤولو الشبكات والأنظمة.
- مديرو التحول الرقمي والامتثال.
- خبراء حماية البيانات المؤسسية.
- الاستشاريون التقنيون وقادة مشاريع IT.
- العاملون في تشغيل البنية التحتية الآمنة.

أهداف الدورة التدريبية

في نهاية هذا البرنامج التدريبي في إدارة جودة البيانات وتقييم أنظمة الأمن الرقمي، سيكون المشاركون قادرين على:

- فهم مفاهيم إدارة جودة البيانات المؤسسية.
- تحديد معايير حوكمة البيانات وسلامتها.
- تقييم سياسات وإجراءات الأمن الرقمي.
- اختبار الضوابط الأمنية بطرق منهجية.
- التوصية بتحسينات فعالة للبنية السيبرانية.
- تنسيق عمليات الأمن عبر بيئات تقنية مختلفة.
- مراقبة الامتثال لمتطلبات حماية البيانات.
- صيانة الأنظمة والبنى التحتية الآمنة.
- التحقق من إعدادات الأنظمة والتطبيقات.
- تصميم شبكات مؤسسية آمنة.
- نشر الخوادم وفق ضوابط أمنية متقدمة.
- تطبيق أنظمة أمن النقاط الطرفية.
- دعم اتخاذ القرار المبني على المخاطر.
- تعزيز التحسين المستمر في الأمن وجودة البيانات.

الكفاءات المستهدفة

سيكتسب المشاركون الكفاءات التالية من خلال برنامج إدارة جودة البيانات وتقييم أنظمة الأمن الرقمي:

- إدارة أطر جودة البيانات المؤسسية.

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

- تطبيق تقنيات تدقيق وتنقية البيانات.
- تنفيذ تقييمات المخاطر السيبرانية.
- تحليل سياسات وإجراءات الأمن الرقمي.
- مراقبة الضوابط الأمنية والامتثال.
- التحقق من جاهزية الأنظمة والتطبيقات.
- تصميم بنى الشبكات الآمنة.
- نشر الخوادم وأنظمة أمن الأطراف.
- تنسيق أنشطة الأمن متعددة الفرق.
- دعم مبادرات التحسين الأمني المستمر.

دراسة سيناريوهات

في تدريب إدارة جودة البيانات وتقييم أنظمة الأمن الرقمي، سيطوّر المشاركون قدراتهم عبر دراسة السيناريوهات:

- تحليل فجوات جودة البيانات في قواعد البيانات المؤسسية.
- مراجعة فعالية سياسات الأمن الرقمي.
- اختبار جاهزية الاستجابة للحوادث السيبرانية.
- التحقق من إعدادات أمن التطبيقات.
- تصميم نموذج شبكة مؤسسية آمنة.
- نشر حماية النقاط الطرفية في بيئات موزعة.
- مراقبة الامتثال لمعايير حماية البيانات.
- تقديم توصيات لتحسين البنية الأمنية.

محتوى الدورة

الوحدة الأولى: أساسيات إدارة جودة البيانات وحوكمتها

- مقدمة في مفاهيم إدارة جودة البيانات وأهميتها المؤسسية.
- أبعاد جودة البيانات في البيئات الرقمية الحديثة.
- بناء إطار حوكمة بيانات فعال ومستدام.
- تحديد ملكية البيانات ومسؤوليات الإشراف.
- تطبيق أدوات تحليل جودة البيانات.
- تنفيذ تقنيات تنظيف البيانات والتحقق منها.
- مراقبة مؤشرات دقة واكتمال البيانات.
- مواءمة جودة البيانات مع أهداف التحول الرقمي.

الوحدة الثانية: سياسات الأمن الرقمي وتقييم المخاطر

- نظرة شاملة على أطر الأمن السيبراني الحديثة.
- بناء سياسات وإجراءات أمن رقمي فعالة.
- إجراء تقييم مخاطر الأمن السيبراني.
- تحليل الضوابط الأمنية في بيئات تقنية مختلفة.
- اختبار الامتثال باستخدام منهجيات تدقيقية.
- تنسيق حوكمة الأمن مع إدارة المخاطر المؤسسية.
- مراقبة الالتزام بمتطلبات حماية البيانات.
- تطوير توصيات قائمة على مستوى النضج الأمني.

الوحدة الثالثة: التحقق من الأنظمة والتطبيقات

- أساسيات تأمين الأنظمة وتقويتها.
- التحقق من أنظمة التشغيل وفق معايير أمنية.
- تقييم أمن التطبيقات وإدارة الإعدادات.
- تنفيذ اختبارات الثغرات الأمنية.

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

- مراجعة ضوابط الهوية وإدارة الوصول.
- التحقق من آليات التسجيل والمراقبة.
- توثيق نتائج التحقق وخطط المعالجة.
- دعم دورة حياة تطوير الأنظمة الآمنة.

الوحدة الرابعة: تصميم الشبكات الآمنة وحماية البنية التحتية

- مبادئ تصميم الشبكات الآمنة للمؤسسات.
- تقسيم الشبكات لتقليل المخاطر السيبرانية.
- تصميم استراتيجيات الجدران النارية والتوجيه الآمن.
- تطبيق مفاهيم الثقة الصفرية والتحكم في الوصول.
- حماية البيانات أثناء النقل باستخدام التشفير.
- تقييم أنظمة كشف التسلل ومراقبة الشبكة.
- تخطيط شبكات مرنة وقابلة للتوسع.
- مواءمة تصميم الشبكة مع استراتيجية الأمن المؤسسي.

الوحدة الخامسة: نشر الخوادم وأنظمة أمن النقاط الطرفية

- إعداد بيئات نشر خوادم آمنة.
- تقوية خوادم Windows وLinux وفق أفضل الممارسات.
- تطبيق حلول أمن النقاط الطرفية المتقدمة.
- إدارة التحديثات ومعالجة الثغرات.
- مراقبة تهديدات الأجهزة الطرفية.
- تنسيق الاستجابة للحوادث مع فرق الأمن.
- الحفاظ على المراقبة الأمنية المستمرة.
- إدارة دورة حياة الضوابط الأمنية.

خلاصة وتوصيات الدورة التدريبية

إن التكامل بين إدارة جودة البيانات وتقييم أنظمة الأمن الرقمي يمثل أساسًا حاسمًا لبناء بيئات رقمية موثوقة وآمنة. إتقان هذه الممارسات يمكّن المؤسسات من تقليل المخاطر وتعزيز سلامة البيانات واستدامة الأمن المؤسسي.