MERCURY

إدارة أمن المعلومات (الأمن السيبراني)

11 - 15 ابريل 2027

كوالا لامبور (ماليزيا)

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

MERCURY

إدارة أمن المعلومات (الأمن السيبراني)

الرمز : 721_125893 تاريخ الإنعقاد: 11 - 15 ابريل 2027 دولة الإنعقاد: كوالا لامبور (ماليزيا) التكلفة: 4900 اليورو

المقدمة:

تُعَدّ دورة إدارة أمن المعلومات الأمن السيبراني، من أهم البرامج التدريبية التي تستهدف رفع كفاءة الأفراد والمنظمات في مواجهة التهديدات السيبرانية المتزايدة. في ظل تسارع التحول الرقمي، أصبحت حماية البيانات وحوكمة أمن المعلومات من الأولويات الاستراتيجية لأي مؤسسة.

تهدف هذه الدورة التدريبية في إدارة أمن المعلومات الأمن السيبراني، إلى تمكين المشاركين من فهم أعمق لمخاطر الأمن السيبراني وتطوير مهاراتهم في إدارة السياسات الأمنية والتقنيات الحديثة. تشمل تطبيقات عملية ومشاريع تقييم مبنية على المعايير العالمية مثل ISO 27001، مع التركيز على كيفية حماية البنية التحتية الرقمية.

تتناول الدورة التدريبية في إدارة أمن المعلومات الأمن السيبراني، التهديدات السيبرانية مثل البرمجيات الخبيثة، وهجمات DDoS، والابتزاز الإلكتروني، وطرق التصدي لها. يحصل المشاركون على كتيبات وأدلة عملية لتطبيق معايير أمن الشبكات. وتتضمن تمارين محاكاة لاختبار الاختراق والتحقيقات الرقمية لتعزيز فهمهم العملي.

صمم هذا البرنامج التدريبي في إدارة أمن المعلومات الأمن السيبراني، ليناسب مختلف المستويات، بدءًا من المبتدئين إلى المهنيين المتقدمين في مجال تطبيق معايير الأمن السيبراني في الشركات. كما يعزز هذا البرنامج قدرة الأفراد على تطوير سياسات أمن المعلومات المتكاملة لمؤسساتهم.

الفئات المستهدفة:

تستهدف دورة إدارة أمن المعلومات الأمن السيبراني المعتمدة، الفئات والمحترفين الذين يسعون لاكتساب المعرفة والمهارات:

- مسؤولو أمن المعلومات ومسؤولو تقنية المعلومات.
- المختصون في أمن الشبكات وتكنولوجيا المعلومات.
- مسؤولو البنية التحتية الرقمية في المؤسسات الحكومية والخاصة.
- مدققو الأنظمة الإلكترونية والمخاطر السيبرانية.
- مدراء المشاريع التقنية ومطورو الأنظمة.
- العاملون في أقسام الحوكمة والامتثال.
- موظفو أقسام الدعم الفني والشبكات.
- مسؤولو حماية البيانات والخصوصية.
- المهتمون بالحصول على شهادة إدارة أمن المعلومات الاحترافية.
- الأفراد الراغبون في دخول مجال التدريب على الأمن السيبراني للمبتدئين.

الكفاءات المستهدفة:

سيكتسب المشاركون الكفاءات التالية من خلال برنامج إدارة أمن المعلومات الأمن السيبراني:

- احتراف إدارة أمن المعلومات في بيئات العمل المعقدة.
- تطوير مهارات تقييم المخاطر والثغرات الأمنية.
- استخدام أدوات الحماية من الهجمات الإلكترونية.
- تحليل وقراءة البيانات الأمنية بفعالية.
- صياغة وتحديث سياسات الأمن المؤسسية.
- التعامل مع تهديدات القرصنة الأخلاقية وغير الأخلاقية.
- فهم تقنيات التشفير وحماية البيانات.
- تنفيذ حلول حوكمة أمن المعلومات.
- التفاعل المهني مع فرق الاستجابة للحوادث السيبرانية.
- تحسين التواصل الأمني داخل المؤسسة.

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 إدارة أمن المعلومات الأمن السيبراني، سيكون المشاركون قادرين على:

- توظيف المعرفة لتحليل مخاطر الأمن السيبراني ضمن بيئة العمل.
- تطبيق إجراءات فحص التهديدات السيبرانية بفعالية.
- صياغة استراتيجيات لحماية البيانات والبنية التحتية الرقمية.
- بناء خطط استجابة للحوادث الأمنية تشمل أمن المعلومات والتقنيات الحديثة.
- تصميم وتطبيق سياسات أمنية داخل المؤسسات.
- التمييز بين أنواع التهديدات السيبرانية وأدوات الهجوم الرقمي.
- استخدام أدوات اختبار الاختراق للكشف عن الثغرات الأمنية.
- بناء فرق أمن إلكترونية فعّالة باستخدام إطار CSIRT.
- تحليل سلوك المستخدمين وتعزيز ثقافة الأمن السيبراني.
- تقييم نظم التحكم في الوصول والامتثال لمعايير الحوكمة الرقمية.
- تطوير قدرات المشاركين على مواجهة تحديات الهندسة الاجتماعية والهجمات المركبة.
- إكساب المشاركين القدرة على إعداد تقارير احترافية وتحقيقات جنائية رقمية.
- تعزيز مهارات مسؤول أمن المعلومات في التعامل مع البيانات الحساسة.
- تطبيق المعايير الدولية مثل IEC/ISO 27001 و COBIT في إدارة أمن المعلومات.
- تطوير القدرة على إدارة الأمن في بيئات سحابية وهجينة.

محتوى الدورة التدريبية:

الوحدة الأولى: المعايير الدولية والتقنيات الموثقة في أمن المعلومات:

- فهم المعايير العالمية مثل IEC/ISO 27001 و DSS-PCI.
- التعرف على إطار COBIT للتحكم في تكنولوجيا المعلومات.
- تحليل نظام PAS 555 في التقييم الأمني الشامل.
- مراجعة أفضل ممارسات حوكمة أمن المعلومات.
- تطبيق أهداف الرقابة الأمنية وتقييم الامتثال.
- دراسة نماذج إدارة المخاطر المعتمدة عالميًا.
- التعرف على آليات تحديد نقاط الضعف الأمنية.
- تنفيذ تقييم الأثر الأمني للمشاريع التقنية.
- التكيف مع تغيرات سياسات أمن المعلومات.
- الربط بين التهديدات السيبرانية والتصميم الأمني المؤسسي.

الوحدة الثانية: السياسات المستقبلية والأطر القانونية:

- تطبيق IEC/ISO 2017 في حماية الأنظمة الحديثة.
- فهم قوانين حماية البيانات مثل GDPR.
- دراسة متطلبات الامتثال الحكومي المحلي والدولي.
- تحليل تأثير التنظيمات الدولية على إدارة أمن المعلومات.
- إدارة حقوق الوصول للبيانات الحساسة في المنظمات.
- دمج متطلبات السياسات الأمنية مع نظم التشغيل.
- تطوير سياسة حماية البيانات في البيئة السحابية.
- تحديد نطاق المسؤولية القانونية عند خرق البيانات.
- فهم التحديات القانونية المرتبطة بالتحقيقات الجنائية الرقمية.
- تحليل الثغرات القانونية في التعامل مع الهجمات السيبرانية.

training@mercury-training.com
www.mercury-training.com

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

MERCURY

الوحدة الثالثة: الدفاعات الفنية ومعمارية الأمن المؤسسي:

- فهم بنية المؤسسة الأمنية وتوزيع المهام.
- إعداد الجدران النارية وأنظمة كشف التسلل IDS.
- تفعيل أنظمة منع التعدي IPS وتقنيات التصفية.
- تطبيق تقنيات تصفية الإنترنت وإدارة المحتوى.
- حماية شبكات Fi-Wi عبر بروتوكولات أمنية محدثة.
- أمن VoIP وتأمين المكالمات عبر الإنترنت.
- تحديد مخاطر GRC الحوكمة والمخاطر والامتثال.
- تصميم دورة حياة البرمجيات الآمنة SDL.
- ربط تطبيقات SEIM بأنظمة تشغيل الحوادث.
- حماية النظم السحابية وتقييم المخاطر المرتبطة بها.
- التعامل مع الطرف الثالث والامتثال الأمني.
- إدارة مخاطر الأمن السيبراني المرتبطة بتكامل الأنظمة.

الوحدة الرابعة: الاستجابة للحوادث والأدوات الجنائية:

- فهم هيكلية فرق الاستجابة للحوادث CSIRT.
- تطبيق منهجيات جمع الأدلة الرقمية.
- التعرف على أدوات التحقيقات الجنائية الرقمية.
- تنفيذ اختبار اختراق وفق بروتوكولات مهنية.
- التمييز بين القرصنة الأخلاقية وغير الأخلاقية.
- التفاعل مع تهديدات DoS / DDoS.
- فهم تحديات SCADA ومتطلبات الأمن الصناعي.
- إعداد خطط الطوارئ الأمنية للمؤسسات.
- التدريب على استخدام أدوات OSINT.
- تقنيات تقليل تأثير APTs والبرمجيات الخبيثة.
- استخدام NLP لتغيير السلوكيات الأمنية للموظفين.
- تطوير خطة استجابة شاملة للحوادث الأمنية المعقدة.

الوحدة الخامسة: بناء بيئة أمنية متكاملة:

- إنشاء مركز عمليات أمنية SOC فعّال.
- تطوير نموذج حوكمة أمن المعلومات داخل المؤسسة.
- نشر وتفعيل فرق CSIRT في الأقسام التقنية.
- إعداد نظم SIEM لرصد التهديدات.
- الحد من استخدام وسائط الإدخال الخارجية.
- تقنيات مواجهة حقن الأكواد النشطة.
- بناء ثقافة أمنية مؤسسية مستدامة.
- تطوير برامج تدريب موظفي الشركات على أمن المعلومات.
- إدارة الوصول إلى البيانات والملفات الحساسة.
- دمج معايير الأمن السيبراني في دورة حياة المشاريع.
- التحليل المستمر للمخاطر باستخدام أدوات ذكاء الأعمال.
- تأمين البنية التحتية الرقمية وبيئات التشغيل الهجينة.

خلاصة وتوصيات الدورة التدريبية:

تقدم دورة إدارة أمن المعلومات الأمن السيبراني، إطارًا شاملًا لفهم وتحليل التهديدات الرقمية. تمكّن المشاركين من تطبيق أدوات وتقنيات الحماية الحديثة في بيئاتهم الوظيفية. كما تساعد في تطوير السياسات الأمنية المؤسسية وفقًا للمعايير الدولية. يُوصى باستمرار المتابعة والتدريب العملي لمواكبة التغيرات في بيئة الأمن السيبراني. وتعتبر هذه الدورة أساسًا قويًا للحصول على شهادات مهنية متقدمة في المجال.

training@mercury-training.com
www.mercury-training.com

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

training@mercury-training.com
www.mercury-training.com

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

MERCURY

نموذج تسجيل :
إدارة أمن المعلومات (الأمن السيبراني)

الرمز : 721 تاريخ الإنعقاد: 11 - 15 ابريل 2027 دولة الإنعقاد: كوالا لامبور (ماليزيا) التكلفة: 4900 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