MERCURY

البرنامج المتقدم في أمن المعلومات الالكترونية

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

MERCURY

البرنامج المتقدم في أمن المعلومات الالكترونية

مقدمة عن البرنامج المتقدم في أمن المعلومات الإلكترونية:

في عالمٍ يتسم بالتحول الرقمي المتسارع، أصبحت الحاجة إلى أمن المعلومات المتقدم ضرورة ملحة لضمان استمرارية الأعمال وحماية الأصول الرقمية. تعاني المؤسسات من تحديات متزايدة في ظل التهديدات السيبرانية المتطورة، مما يستوجب تأهيلاً متخصصًا للتصدي لها بفعالية. يهدف البرنامج المتقدم في أمن المعلومات الإلكترونية، إلى تزويد المشاركين بالمعرفة التطبيقية والمهارات العملية الضرورية لتعزيز البنية التحتية للأمن السيبراني.

يعالج برنامج أمن المعلومات المتقدم، جوانب متعددة تشمل التهديدات السيبرانية، تحليل المخاطر، أمن الشبكات، الحوسبة السحابية، وإدارة الحوادث الأمنية. كما يركّز على التطورات الحديثة في تدريب أمن المعلومات ويعزز الوعي القانوني والأخلاقي المرتبط بالمجال. يدمج هذا البرنامج بين الجانب النظري والتدريب العملي في أمن المعلومات المتقدم.

يستهدف برنامج تدريبي لأمن المعلومات المتقدم، محترفي التقنية الراغبين في التخصص في الأمن السيبراني للمحترفين من خلال برنامج تدريبي عالي المستوى. كما يُعد البرنامج فرصةً ثمينة لاكتساب تدريب متخصص في أمن المعلومات الإلكترونية وفق أحدث المعايير الدولية. إن الوعي المتكامل بأمن المعلومات الإلكترونية لم يعد ترفًا، بل هو عنصر حيوي لاستدامة الأداء المؤسسي في العصر الرقمي.

الفئات المستهدفة:

تستهدف دورة تدريبية متقدمة في أمن المعلومات الإلكترونية، الفئات والمحترفين الذين يسعون لاكتساب المعرفة والمهارات:

- مديرو أمن المعلومات في المؤسسات العامة والخاصة.
- محللو المخاطر والتهديدات الإلكترونية.
- مهندسو الشبكات وأمن النظم المتقدمة.
- موظفو أقسام تكنولوجيا المعلومات في مختلف القطاعات.
- متخصصو الحوسبة السحابية والأمن السحابي.
- مسؤولو الامتثال للتشريعات الأمنية الرقمية.
- مبرمجو التطبيقات الراغبون في تعزيز أمن برمجياتهم.
- طلاب وخريجو تخصصات الحاسوب وتقنية المعلومات.
- مهتمون بالحصول على دورة معتمدة في أمن المعلومات المتقدم.
- العاملون في مجالات التحقيقات الرقمية والتحليل الجنائي الإلكتروني.
- الراغبون في الالتحاق بـ برنامج تدريبي لأمن المعلومات المتقدم.
- الموظفون الحكوميون في أقسام التحول الرقمي والحوكمة الإلكترونية.

الكفاءات المستهدفة:

سيكتسب المشاركون الكفاءات التالية من خلال البرنامج المتقدم في أمن المعلومات الإلكترونية:

- الكفاءة في تطبيق حلول الأمن السيبراني المتقدم.
- القدرة على تحليل الهجمات واستنتاج الأنماط السيبرانية.
- تصميم سياسات أمنية مرنة تتناسب مع التغيرات التكنولوجية.
- استيعاب مبادئ التشفير والبروتوكولات الآمنة.
- التفاعل مع تقنيات الحوسبة السحابية الآمنة.
- تنفيذ اختبارات اختراق باستخدام أدوات متقدمة.
- إدارة مخاطر الأمن الإلكتروني بكفاءة عالية.
- التعامل مع التحقيقات الرقمية وتوثيق الأدلة.
- إعداد خطط استجابة للطوارئ وحوادث الخرق الأمني.
- الامتثال للمعايير القانونية والأخلاقية في أمن المعلومات.
- تعزيز ثقافة أمن المعلومات في بيئة العمل.

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 المتقدم في أمن المعلومات الإلكترونية، سيكون المشاركون قادرين على:

- تعريف المشاركين بمفاهيم أمن المعلومات المتقدم واستخداماته.
- تمكينهم من تحليل التهديدات وتحديد نقاط الضعف في الأنظمة.
- تطوير قدراتهم على تصميم استراتيجيات وقائية فعالة.
- تنفيذ أدوات كشف الهجمات السيبرانية والاستجابة لها بكفاءة.
- إعداد سياسات وإجراءات متكاملة لأمن المعلومات الإلكترونية.
- تطبيق مفاهيم التشفير وتأمين البيانات أثناء النقل والتخزين.
- تحليل سيناريوهات حقيقية لحوادث أمنية وتقديم حلول استراتيجية.
- تقييم بنية الشبكات من منظور الأمان وتحديد الثغرات التقنية.
- تحسين استجابتهم للطوارئ عبر خطط استعادة البيانات.
- توظيف تقنيات الحوسبة السحابية ضمن بيئة آمنة ومرنة.
- اختبار الأنظمة عمليًا عبر تمارين اختراق متقدمة.
- ربط الجانب القانوني بالتطبيقات العملية لأمن المعلومات.
- بناء ثقافة داخل المؤسسة لتعزيز الوعي الأمني بين الموظفين.
- تأهيل المشاركين للحصول على تدريب مهني في الأمن السيبراني المتقدم.
- تطوير قدرة التفكير النقدي وحل المشكلات الأمنية المعقدة.
- إعداد تقارير أمنية احترافية تتوافق مع المعايير الدولية.

محتوى الدورة التدريبية:

الوحدة الأولى: الأساسيات المتقدمة في أمن المعلومات:

- تعريف شامل بأمن المعلومات الإلكتروني في السياق الحديث.
- تطور التهديدات والهجمات السيبرانية وأساليبها.
- المبادئ الأساسية لتأمين الأنظمة والمعلومات.
- استخدام تقنيات التشفير الحديثة وتطبيقاتها.
- نماذج اختراق الأنظمة وآليات الاستجابة لها.
- العلاقة بين الحوكمة الرقمية وأمن المعلومات.
- التعرف على أدوات تحليل المخاطر في أمن المعلومات.
- تطبيق الإطار العام لحماية البيانات في المؤسسات.
- المقارنة بين أمن المعلومات والأمن السيبراني.
- دمج أمن المعلومات في دورة حياة تطوير النظام SDLC.
- دور الذكاء الاصطناعي في اكتشاف التهديدات الحديثة.
- التمييز بين التهديدات الداخلية والخارجية.

الوحدة الثانية: تحليل وتقييم المخاطر والتهديدات الأمنية:

- تحديد الأصول الحيوية وتصنيفها حسب الأولوية الأمنية.
- تحليل التهديدات بناءً على احتمالية الحدوث والأثر المحتمل.
- بناء مصفوفات تحليل المخاطر المتقدمة.
- تصميم خطط التخفيف والاستجابة المستندة إلى تحليل دقيق.
- تحديد الثغرات الأمنية في البرمجيات والبنية التحتية.
- تقنيات اكتشاف التهديدات الصامتة والمتقدمة.
- بناء منهجية متكاملة لتقييم أمان التطبيقات.
- أدوات التحقق من الثغرات الأمنية واستخدامها العملي.
- تطوير سيناريوهات لاختبار الجاهزية الأمنية.
- ربط تحليل المخاطر بعمليات اتخاذ القرار المؤسسي.
- توظيف التقارير الأمنية في تحسين الأداء الوقائي.
- العلاقة بين إدارة الحماية الإلكترونية المتقدمة والحوكمة الأمنية.

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

MERCURY

الوحدة الثالثة: أمن الشبكات والبروتوكولات المتقدمة:

- تأمين بنية الشبكات الداخلية والخارجية.
- استخدام جدران الحماية المتقدمة وحلول IDS/IPS.
- التهيئة الصحيحة لأجهزة التوجيه والمبدلات من منظور الأمان.
- التحكم في الوصول باستخدام سياسات دقيقة للهوية والمصادقة.
- حماية البيانات أثناء التبادل عبر الشبكات العامة.
- البروتوكولات الآمنة HTTPS، TLS، SSH واستخداماتها.
- تحليل حركة الشبكة لاكتشاف السلوكيات غير الطبيعية.
- استخدام أدوات مراقبة الشبكة للكشف عن التسلل.
- فهم أنواع هجمات الشبكة وأساليب الوقاية منها.
- حماية الحواسيب الطرفية والأنظمة المتصلة بالشبكة.
- تطوير سياسات استخدام الشبكة المؤسسية بأمان.
- تدريب عملي في أمن المعلومات المتقدم في بيئات شبكية.

الوحدة الرابعة: أمن المعلومات في بيئة الحوسبة السحابية:

- التعرف على خصائص الحوسبة السحابية وأنواعها.
- المخاطر الأمنية المرتبطة بالخدمات السحابية العامة والخاصة.
- حماية البيانات في مراكز البيانات السحابية.
- التحكم في الهوية والوصول داخل بيئة الحوسبة السحابية.
- سياسات تشفير البيانات المخزنة والمنقولة عبر السحابة.
- تقنيات عزل العملاء في السحابة متعددة المستأجرين.
- أدوات المراقبة وتحليل النشاط في البيئات السحابية.
- توثيق الحوادث ومعالجتها في البيئة السحابية.
- اختيار مزود خدمة سحابية موثوق وفق معايير الأمان.
- الامتثال لمعايير الخصوصية الدولية مثل GDPR وISO 27018.
- تصميم بنى آمنة لتكامل السحابة مع الشبكات الداخلية.
- دمج البرنامج المتقدم في أمن المعلومات الإلكترونية مع منصات SaaS وIaaS.

الوحدة الخامسة: تقنيات متقدمة لاختبار الأمان والاستجابة للحوادث:

- إجراء اختبارات اختراق احترافية ومهيكلة.
- تحليل نتائج الاختبارات وتحديد مستوى المخاطر.
- استخدام أدوات اختبار مشهورة مثل Linux Kali وSuite Burp.
- محاكاة الهجمات المتقدمة وتقييم استجابة الأنظمة.
- جمع الأدلة الرقمية وتحليل سجلات الأنظمة Analysis Log.
- إجراءات احتواء الحوادث والحد من آثارها.
- إعداد خطط استعادة النظام بعد الحوادث السيبرانية.
- تطوير تقارير تحليلية توثق الحادث الأمني بالكامل.
- أساليب التوثيق وفق الإجراءات القانونية والأخلاقية.
- العلاقة بين تقارير الحوادث ومتطلبات المراجعة والتدقيق.
- تصميم نظام إنذار مبكر للهجمات الإلكترونية.
- تدريب متخصص في أمن المعلومات الإلكترونية من خلال سيناريوهات حقيقية.

خلاصة وتوصيات الدورة التدريبية:

يشكل هذا البرنامج التدريبي مرجعًا احترافيًا شاملاً في مجال الأمن السيبراني المتقدم. يسهم في تعزيز المعرفة التقنية والتطبيقية للمشاركين، ويؤهلهم لتولي أدوار قيادية في أمن المعلومات. نوصي بتحديث المعرفة الأمنية بشكل دوري نظرًا لتغير طبيعة التهديدات. كما يُفضل تطبيق ما تم تعلمه ضمن بيئة العمل لتعزيز الفاعلية المؤسسية. ويُعد الحصول على دورة احترافية في أمن المعلومات الإلكترونية خطوة متقدمة نحو التميز المهني.