MERCURY

دورة متقدمة في الأمن السيبراني: تقنيات الدفاع السيبراني

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

MERCURY

دورة متقدمة في الأمن السيبراني: تقنيات الدفاع السيبراني

مقدمة:

في ظل تصاعد التهديدات السيبرانية وتعقيد الهجمات الرقمية، أصبح تعزيز قدرات الدفاع السيبراني أولوية استراتيجية للمؤسسات. تهدف هذه الدورة المتقدمة في الأمن السيبراني إلى تزويد المشاركين بفهم عميق لتقنيات الدفاع السيبراني وأساليب الحماية من التهديدات المتقدمة.

تركز الدورة المتقدمة في الأمن السيبراني: تقنيات الدفاع السيبراني، على تمكين المختصين من اكتشاف نقاط الضعف ومعالجتها بفعالية، إلى جانب تطوير مهارات التحليل الجنائي الرقمي والاستجابة للحوادث الأمنية. كما تسلط الضوء على أحدث حلول تأمين الشبكات والأنظمة، مع تغطية مفصلة لتقنيات التشفير والتحكم في الوصول.

تستعرض دورة متقدمة في الأمن السيبراني: تقنيات الدفاع السيبراني، أساليب المحاكاة وبيئات التدريب التفاعلية لتعزيز التعلم العملي. تساهم في إعداد الكوادر القادرة على مواجهة الهجمات السيبرانية المعقدة وتطبيق استراتيجيات الوقاية والاستجابة. تم تصميم محتوى بما يتماشى مع المعايير العالمية ومع أفضل ممارسات التدريب المهني في الأمن السيبراني.

الفئات المستهدفة:

تستهدف دورة متقدمة في الأمن السيبراني: تقنيات الدفاع السيبراني، الفئات والمحترفين الذين يسعون لاكتساب المعرفة والمهارات:

- محللو الأمن السيبراني في المؤسسات الحكومية والخاصة.
- مسؤولو الشبكات والبنية التحتية الرقمية.
- مدراء تقنية المعلومات والأمن المعلوماتي.
- مبرمجون يرغبون في تعزيز مهارات الأمان البرمجي.
- مهندسو نظم يرغبون في حماية البنية التحتية الرقمية.
- خبراء تحليل المخاطر الإلكترونية.
- موظفو أقسام الرقابة والتدقيق الداخلي.
- محترفو تقنية المعلومات الراغبون في التخصص في الأمن السيبراني.
- مسؤولو الحوكمة وإدارة الامتثال في المجال الرقمي.
- المهتمون بالتحول الرقمي وأمن المعلومات.
- فرق الاستجابة للحوادث الأمنية داخل المنظمات.

الكفاءات المستهدفة:

سيكتسب المشاركون الكفاءات التالية من خلال برنامج متقدم في الأمن السيبراني: تقنيات الدفاع السيبراني:

- القدرة على تحديد التهديدات الإلكترونية وتحليلها بفعالية.
- مهارة إعداد استراتيجيات دفاع سيبراني متقدمة.
- التمكن من أدوات التحليل الرقمي الجنائي والتوثيق الأمني.
- كفاءة تطبيق ضوابط أمن المعلومات وفق المعايير الدولية.
- مهارة تنفيذ اختبارات الاختراق وتقييم الأمان.
- الفهم العميق لتقنيات التشفير وأنظمة المصادقة.
- تعزيز القدرة على الاستجابة للحوادث وتنفيذ خطط التعافي.
- الإلمام بالإطار القانوني لأمن المعلومات.
- التفاعل بفعالية مع الفرق الأمنية متعددة التخصصات.
- تطوير بيئات رقمية آمنة وفقاً لسياسات 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 المتقدم في الأمن السيبراني: تقنيات الدفاع السيبراني، سيكون المشاركون قادرين على:

- تحليل التهديدات السيبرانية الحديثة وتصنيفها بدقة.
- تقييم فعالية أنظمة الدفاع الحالية وتحديد الثغرات الأمنية.
- تطبيق استراتيجيات استباقية للكشف المبكر عن الهجمات الإلكترونية.
- تطوير خطط استجابة للحوادث السيبرانية بكفاءة عالية.
- استخدام أدوات التحليل الجنائي الرقمي لاكتشاف مصادر الهجمات.
- بناء نظم أمن معلومات قائمة على معايير الحماية المتقدمة.
- تحسين أنظمة إدارة الهوية والتحكم في الوصول.
- تعزيز قدرات التشفير والتوثيق لحماية البيانات الحساسة.
- تنفيذ اختبارات الاختراق لتقييم مستوى الأمان في الأنظمة.
- إعداد تقارير تحليل أمني احترافية لصناع القرار.
- فهم الأطر القانونية والتنظيمية المتعلقة بالأمن السيبراني.
- توظيف أنظمة ذكاء اصطناعي في الكشف عن الأنماط غير الطبيعية.
- تصميم بيئات محاكاة لهجمات سيبرانية لغرض التدريب.
- تطبيق مبادئ الأمن السيبراني في بنية الأنظمة السحابية.
- ضمان استمرارية الأعمال من خلال خطط الطوارئ الرقمية.

محتوى الدورة التدريبية:

الوحدة الأولى: مفاهيم متقدمة في الأمن السيبراني:

- تعريف التهديدات السيبرانية المعاصرة ومصادرها.
- تحليل اتجاهات الهجمات الإلكترونية في السنوات الأخيرة.
- التعرف على الهجمات المتقدمة المستمرة APT.
- تصنيف الأصول الرقمية وأولويات الحماية.
- الفروقات بين الأمن السيبراني وأمن المعلومات.
- تقنيات جمع وتحليل المعلومات التهديدية Intelligence Threat.
- أطر الحوكمة في الأمن السيبراني.
- تطبيقات الذكاء الاصطناعي في الأمن السيبراني.
- تحديات حماية البيانات في بيئات العمل السحابية والهجينة.

الوحدة الثانية: استراتيجيات الدفاع السيبراني المتقدمة:

- بناء بنية دفاعية متعددة الطبقات Depth in Defense.
- تقنيات الجدران النارية الحديثة وأنظمة كشف التسلل IPS/IDS.
- استراتيجيات منع فقدان البيانات DLP.
- دور الـ segmenting في تعزيز الأمن الشبكي.
- إدارة وتحديث الأنظمة الأمنية بفاعلية.
- استخدام أدوات SIEM لتحليل وتنبيهات الهجمات.
- دمج أدوات الأمن السيبراني في دورة حياة النظام.
- هندسة الأمن داخل البنية التحتية الرقمية.
- بناء مراكز عمليات الأمن SOC.

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

MERCURY

الوحدة الثالثة: التحليل الجنائي الرقمي والاستجابة للحوادث:

- خطوات الاستجابة للحوادث السيبرانية.
- جمع الأدلة الرقمية وفق المعايير القانونية.
- تحليل سجلات الأحداث Logs لتتبع الاختراقات.
- أدوات وتقنيات التحليل الجنائي الرقمية.
- الحفاظ على سلامة الأدلة ومنع التلاعب.
- إعداد تقارير مفصلة عن الحوادث الأمنية.
- استخدام محاكاة الحوادث لتدريب الفرق.
- التنسيق مع الجهات المختصة أثناء الأزمات.
- إنشاء خطط التعافي بعد الحوادث الأمنية.

الوحدة الرابعة: حماية البنية التحتية والتشفير:

- أنواع التشفير وتقنياته المتماثل وغير المتماثل.
- إدارة المفاتيح وأنظمة الشهادات الرقمية PKI.
- أنظمة كشف الهوية وإدارة الوصول IAM.
- حماية البيانات أثناء النقل والتخزين.
- سياسات أمن البريد الإلكتروني والاتصالات.
- تقنيات حماية قواعد البيانات والبنية التحتية الحرجة.
- تأمين بيئات العمل الافتراضية والسحابية.
- رصد التهديدات في الوقت الحقيقي باستخدام أدوات SIEM.
- تحديث السياسات الأمنية بشكل دوري.

الوحدة الخامسة: اختبارات الاختراق والمحاكاة الأمنية:

- منهجيات اختبارات الاختراق وفق OWASP.
- خطوات تنفيذ اختبار اختراق أمن.
- أدوات وتقنيات تنفيذ الاختبارات على التطبيقات.
- تحليل نتائج الاختبارات وتقديم التوصيات.
- إعداد سيناريوهات هجومية تدريبية.
- استخدام أدوات مفتوحة المصدر في بيئات الاختبار.
- دمج نتائج الاختبار في تطوير الخطط الأمنية.
- التقييم المستمر لنقاط الضعف الفنية.
- دور التدريب العملي في رفع كفاءة الدفاع.

خلاصة وتوصيات الدورة التدريبية:

تقدم هذه الدورة المتقدمة في الأمن السيبراني إطاراً شاملاً لفهم أحدث التهديدات الرقمية وتقنيات الدفاع. تمنح المشاركين خبرات عملية ونظرية عالية التأثير في حماية المؤسسات. يُوصى بتطبيق المفاهيم المكتسبة فوراً في بيئة العمل لتعزيز فعالية الأمن. ويُنصح بالاستمرار في التحديث والتعلم المستمر في هذا المجال المتجدد.