MERCURY

تقييم نقاط الضعف وتحليل مشكلات أمن النظام

7 – 11 مارس 2027

القاهرة (مصر)



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

MERCURY

تقييم نقاط الضعف وتحليل مشكلات أمن النظام

المرجع: 170544_121495 **التاريخ:** 7 – 11 مارس 2027 **المكان:** القاهرة (مصر) **الرسوم:** 4000 Euro

مقدمة

تقدم هذه الدورة التدريبية في تقييم نقاط الضعف وتحليل مشكلات أمن النظام، إطاراً منهجياً متكاملاً لاكتشاف الثغرات الأمنية وتقييم المخاطر في بيئات تقنية المعلومات الحديثة. تهدف إلى تنمية قدرة المشاركين على تحليل نتائج فحص الثغرات وبيانات الإعدادات بدقة واحترافية. كما تركز على تطبيق أفضل ممارسات تحليل الأمن السيبراني وربطها بمتطلبات إدارة المخاطر المؤسسية. وسيتعلم المشاركون كيفية اكتشاف أخطاء التهيئة وتحديد أولويات المعالجة وفق مستوى الخطورة وتأثير الأعمال. وتغطي أساليب تقييم أمن الشبكات والأنظمة والتطبيقات ضمن منظور عملي تحليلي. وسيصبح المتدرب قادراً على دعم برامج إدارة الثغرات وتعزيز مستوى الحماية المؤسسية.

الفئات المستهدفة

تستهدف دورة تقييم نقاط الضعف وتحليل مشكلات أمن النظام، الفئات والمحترفين لاكتساب المعرفة والمهارات:

- محللو الأمن السيبراني الراغبون في تطوير مهارات تقييم الثغرات.
- مختصو أمن المعلومات المسؤولون عن تقوية الأنظمة.
- مسؤولو الشبكات المشرفون على البنية التحتية الآمنة.
- خبراء إدارة المخاطر الداعمين لبرامج الأمن السيبراني.
- فرق مركز العمليات الأمنية SOC.
- مسؤولو الامتثال ومراقبة إعدادات الأمان.
- مدققو تقنية المعلومات والأمن.
- مسؤولو حماية الأنظمة المؤسسية.

أهداف الدورة التدريبية

في نهاية هذا البرنامج التدريبي في تقييم نقاط الضعف وتحليل مشكلات أمن النظام، سيكون المشاركون قادرين على:

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

- فهم المفاهيم الأساسية في تقييم نقاط الضعف الأمنية.
- التعرف على الثغرات الشائعة في الأنظمة والشبكات.
- تحليل نتائج فحص الثغرات بدقة منهجية.
- ربط بيانات الإعدادات بالمخاطر الأمنية المحتملة.
- تحديد أولويات المعالجة وفق مستوى الخطورة.
- تقييم نقاط الضعف في الشبكات والأنظمة والتطبيقات.
- تطبيق منهجيات تحليل مشكلات أمن النظام.
- دعم برامج إدارة الثغرات المستمرة.
- تحسين تقارير الأمن لمختلف أصحاب المصلحة.
- تعزيز استراتيجيات تقليل المخاطر السيبرانية.
- مواءمة تقييم الثغرات مع أفضل ممارسات الأمن.
- تطوير مهارات اتخاذ القرار المبني على البيانات.

الكفاءات المستهدفة

سيكتسب المشاركون الكفاءات التالية من خلال برنامج تقييم نقاط الضعف وتحليل مشكلات أمن النظام:

- تحليل احترافي لنتائج تقييم نقاط الضعف.
- اكتشاف أخطاء إعدادات الأنظمة الحرجة.
- تطبيق منهجيات ترتيب المخاطر الأمنية.
- تفسير تقارير الفحص الأمني بدقة.
- كشف ضعف تهيئة الشبكات والخوادم.
- تقييم المخاطر السيبرانية المؤسسية.
- قياس مستوى الوضع الأمني للأنظمة.
- توثيق نتائج الفحص الأمني بوضوح.
- التنسيق بين فرق الأمن وتقنية المعلومات.
- تبني عقلية المراقبة الأمنية المستمرة.

دراسة سيناريوهات

في تدريب تقييم نقاط الضعف وتحليل مشكلات أمن النظام، سيطور المشاركون قدراتهم عبر دراسة السيناريوهات:

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

- تحليل نتائج فحص الثغرات في بيئة مؤسسية.
- مراجعة إعدادات نظام غير آمنة.
- ترتيب أولويات الثغرات الحرجة.
- التحقيق في خوادم مكشوفة للخطر.
- تقييم فجوات التحديثات الأمنية.
- ربط معلومات التهديد بنتائج الفحص.
- فحص الانحرافات عن خط الأساس الأمني.
- إعداد تقارير أمنية للإدارة.

محتوى الدورة

الوحدة الأولى: أساسيات تقييم نقاط الضعف

- نظرة عامة على دورة حياة إدارة الثغرات.
- تعريف الثغرات ونقاط التعرض والهجوم.
- دور تقييم نقاط الضعف في الأمن السيبراني.
- أنواع نقاط الضعف في بيئات تقنية المعلومات.
- فهم أساليب استغلال الثغرات.
- العلاقة بين إدارة المخاطر وفحص الثغرات.
- المصطلحات الأساسية في التقييم الأمني.
- التحديات الشائعة في اكتشاف الثغرات.

الوحدة الثانية: فحص الثغرات وتحليل البيانات

- مبادئ استخدام أدوات فحص الثغرات.
- قراءة تقارير الفحص الأمني بفعالية.
- التحقق من الإيجابيات الكاذبة.
- استخدام معايير CVSS لتقييم الخطورة.
- تحليل بيانات الإعدادات الأمنية.
- ربط نتائج الفحص بأهمية الأصول.
- مراجعة فحوص الشبكات والأنظمة.
- وضع جداول الفحص الدورية.

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

MERCURY

الوحدة الثالثة: تحديد مشكلات أمن النظام

- اكتشاف أخطاء تهيئة الأنظمة.
- التعرف على ثغرات أنظمة التشغيل.
- تحليل مخاطر المنافذ المفتوحة.
- تقييم نقاط ضعف التطبيقات.
- مراجعة أخطاء التحكم في الوصول.
- تقييم فجوات التحديثات الأمنية.
- تحليل مخاطر تصعيد الصلاحيات.
- ربط الثغرات بمسارات الهجوم.

الوحدة الرابعة: ترتيب المخاطر وخطط المعالجة

- أطر ترتيب الثغرات حسب المخاطر.
- تقييم تأثير الثغرات على الأعمال.
- إعداد خطط المعالجة والتخفيف.
- تنسيق عمليات إدارة التصحيحات.
- متابعة تنفيذ المعالجة والتحقق منها.
- توصيل مستوى المخاطر للإدارة.
- دمج بيانات الثغرات في سجل المخاطر.
- دعم التحسين الأمني المستمر.

الوحدة الخامسة: إدارة الثغرات المستمرة والتقارير

- بناء برنامج فعال لإدارة الثغرات.
- إنشاء خطوط أساس لإعدادات الأمان.
- المراقبة المستمرة للوضع الأمني.
- مؤشرات الأداء لإدارة الثغرات.
- إعداد تقارير تقييم نقاط الضعف الاحترافية.
- دعم متطلبات الامتثال والتدقيق.
- مواءمة إدارة الثغرات مع العمليات الأمنية.
- تعزيز مرونة الأمن السيبراني المؤسسي.

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

MERCURY

خلاصة وتوصيات الدورة التدريبية

يعتمد نجاح تقييم نقاط الضعف على التحليل المستمر لبيانات الإعدادات ونتائج الفحص الأمني. إن تبني منهجية منظمة لإدارة الثغرات يعزز بشكل ملموس قوة الحماية السيبرانية للمؤسسات.