BLACKBIRD FOR TRAINING

العمليات المتقدمة للأمن السيبراني: المراقبة، إدارة التهديدات، والهندسة الآمنة

14 – 18 فبراير 2027

عمّان (الأردن)

العمليات المتقدمة للأمن السيبراني: المراقبة، إدارة التهديدات، والهندسة الآمنة

المرجع: 344752_3255556 **التاريخ:** 14 – 18 فبراير 2027 **المكان:** عمان (الأردن) **الرسوم:** GBP 4900

مقدمة

في عالم رقمي شديد الترابط وتتصاعد فيه التهديدات السيبرانية بشكل مستمر، لم يعد الاعتماد على الحلول الأمنية التفاعلية كافيًا لحماية المؤسسات. بل أصبحت الحاجة ملحّة إلى تبنّي نهج استباقي قائم على الاستخبارات والتحليل المستمر للتهديدات ضمن عمليات أمن سيبراني متقدمة وفعّالة.

تم تصميم هذه الدورة التقنية المتقدمة لمدة أسبوع لتزويد المختصين بالمعرفة العملية والمهارات اللازمة لمراقبة التهديدات السيبرانية، واكتشافها، والحد منها، والاستجابة لها بكفاءة داخل بيئات تقنية المعلومات الحديثة. تغطي الدورة بشكل متكامل مجالات المراقبة والكشف، إدارة الثغرات، التحكم الشبكي، الاستجابة للحوادث، الهندسة الأمنية، ومشهد التهديدات السيبرانية.

من خلال سيناريوهات واقعية، وتمارين تطبيقية، وأفضل الممارسات التشغيلية، سيتمكن المشاركون من تصميم وتنفيذ وإدارة دفاعات سيبرانية قوية تتوافق مع الأطر والمعايير العالمية مثل NIST CSF، NIST 800-53 و800-61، ISO 27001، إطار ATT&CK، MITRE، ونهج Zero Trust Architecture. وتهدف هذه الدورة إلى تعزيز مرونة المؤسسات السيبرانية، وتحسين الرؤية الأمنية، وتمكين فرق العمل من التعامل الحاسم مع الحوادث دون التأثير على استمرارية الأعمال.

أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- فهم مشهد التهديدات السيبرانية الحديثة وأساليب المهاجمين وتقنياتهم وإجراءاتهم TTPs
- تنفيذ قدرات فعّالة للمراقبة والكشف الأمني باستخدام السجلات، أنظمة SIEM، والاستخبارات الأمنية
- تحديد وتقييم وترتيب أولويات الثغرات الأمنية ومعالجتها وفق منهجيات منظمة لإدارة الثغرات
- تصميم وتطبيق ضوابط أمنية شبكية تقلل من سطح الهجوم وتحد من الحركة الجانبية داخل الشبكات
- إعداد وتنفيذ خطط الاستجابة للحوادث بما يتوافق مع أفضل الممارسات والمعايير الدولية
- تطبيق مبادئ الهندسة الأمنية لبناء بيئات تقنية معلومات وسحابة مرنة وقابلة للدفاع
- تحسين الوضع العام للأمن السيبراني من خلال المراقبة المستمرة، والاختبارات، والتحسين المتواصل

محاور الدورة

اليوم الأول: مشهد التهديدات السيبرانية وأساسيات المراقبة الأمنية

- نظرة شاملة على مشهد التهديدات السيبرانية العالمية واتجاهات الهجمات الناشئة
- أنواع الجهات المهاجمة: مجرمو الإنترنت، الجهات المدعومة من دول، التهديدات الداخلية، والناشطون إلكترونيًا
- فهم دورة حياة الهجوم وإطار MITRE ATT&CK
- أساسيات المراقبة والكشف الأمني
- إدارة السجلات والبيانات الأمنية وتحقيق الرؤية عبر الأنظمة الطرفية، الشبكات، والبيئات السحابية
- مقدمة إلى أنظمة SIEM وSOAR ومصادر استخبارات التهديدات

اليوم الثاني: عمليات المراقبة والكشف الأمني

- تصميم استراتيجية فعّالة للمراقبة الأمنية
- حالات الكشف الشائعة: هجمات التخمين، البرمجيات الخبيثة، الحركة الجانبية، وتسريب البيانات
- بناء قواعد الارتباط والتنبيهات وضبطها لتقليل الإنذارات الخاطئة
- دمج استخبارات التهديدات وإثراء البيانات الأمنية
- مؤشرات الأداء الرئيسية KPIs للمراقبة المستمرة
- تمرين عملي: بناء وتحليل سيناريوهات كشف التهديدات

اليوم الثالث: إدارة الثغرات وضوابط أمن الشبكات

- دورة حياة إدارة الثغرات: الاكتشاف، التقييم، تحديد الأولويات، المعالجة، والتحقق
- أدوات وتقنيات فحص الثغرات
- ترتيب أولويات المخاطر بناءً على CVSS، قابلية الاستغلال، وأهمية الأصول
- أساسيات أمن الشبكات: الجدران النارية، أنظمة IDS/IPS، تقسيم الشبكات، والإعدادات الآمنة
- مبادئ Zero Trust والدفاع متعدد الطبقات
- تقليل سطح الهجوم من خلال ضوابط شبكية محكمة

اليوم الرابع: الاستجابة للحوادث وإدارة الأزمات السيبرانية

- أطر الاستجابة للحوادث NIST 800-61، SANS
- تصنيف الحوادث وتقييم مستوى الخطورة
- أدوار ومسؤوليات فريق الاستجابة للحوادث
- مراحل الكشف، الاحتواء، الاستئصال، والتعافي
- أساسيات الأدلة الرقمية والتعامل مع الأدلة
- تحليل ما بعد الحادث، واستخلاص الدروس، وإعداد التقارير
- تمرين محاكاة: الاستجابة لحادث سيبراني افتراضي

اليوم الخامس: الهندسة الآمنة والمرونة التشغيلية

- مبادئ الهندسة الأمنية ونهج التصميم الآمن منذ البداية
- هندسة الأمن للبيئات المحلية، السحابية، والهجينة
- أساسيات إدارة الهوية والوصول IAM
- مفاهيم تصميم التطبيقات والبنية التحتية الآمنة
- دمج الأمن ضمن عمليات DevOps والنشر السحابي
- ورشة ختامية: تصميم بنية سيبرانية آمنة، مراقبة، وقابلة للصمود
- تقييم المعرفة ووضع خارطة طريق للتحسين المستمر

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- فهم واقعي للتهديدات السيبرانية وسلوك المهاجمين
- تعزيز قدرات المراقبة والكشف وتقليل زمن بقاء التهديد داخل الأنظمة
- تطوير منهجية فعّالة لإدارة الثغرات بناءً على المخاطر الحقيقية
- تقوية الدفاعات الشبكية باستخدام ضوابط حديثة ونهج Zero Trust
- اكتساب مهارات عملية للاستجابة الفعّالة للحوادث والأزمات السيبرانية
- تصميم أنظمة وبنى تقنية آمنة ومستدامة
- رفع مستوى المرونة السيبرانية للمؤسسة في مواجهة الهجمات المتقدمة

الخاتمة

تمثل هذه الدورة التقنية المتقدمة في الأمن السيبراني استثمارًا حقيقيًا لمحللي مراكز العمليات الأمنية SOC، ومهندسي الشبكات، ومهندسي الأمن، ومتخصصي المخاطر التقنية. فهي تجمع بين المعرفة النظرية العميقة، والتطبيق العملي، والتجارب الواقعية اللازمة لحماية البيئات الرقمية الحديثة.

بنهاية البرنامج، سيكون المشاركون قادرين على مراقبة التهديدات بشكل استباقي، وإدارة الثغرات بكفاءة، والاستجابة للحوادث بثقة، وتصميم بنى أمنية قوية تدعم الاستمرارية التشغيلية على المدى الطويل.

التحاقك بهذه الدورة هو خطوة استراتيجية نحو تعزيز قدراتك السيبرانية والمساهمة الفعالة في بناء مؤسسات آمنة، مرنة، وجاهزة للمستقبل.