دورة عمليات الدفاع عن الشبكات والاستجابة للحوادث

29 أغسطس – 2 سبتمبر 2027

الكويت

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة عمليات الدفاع عن الشبكات والاستجابة للحوادث

المرجع: 222670_1660 **التاريخ:** 29 أغسطس – 2 سبتمبر 2027 **المكان:** الكويت **الرسوم:** Euro 5500

نظرة عامة

دورة عمليات الدفاع عن الشبكات والاستجابة للحوادث هي دورة تطبيقية لمدة أسبوع لفرق إدارة الشبكات والعمليات الأمنية والبنية التحتية والدعم التقني، ويعود المشاركون منها بحزمة عمليات الدفاع عن الشبكات. تربط الدورة بنية الشبكات الآمنة وسياسة جدار الحماية وتجزئة الشبكة ومراقبة حركة الشبكة وكشف التسلل والاستجابة للحوادث بأدلة تشغيلية قابلة للتتبع. وتطور أجايل للتدريب مهارات عمليات الدفاع عن الشبكات.

الفئة المستهدفة

- فرق الشبكات المسؤولة عن البنية والاتصال وضوابط حركة البيانات
- فرق العمليات الأمنية المسؤولة عن الكشف والفرز والاستجابة
- فرق البنية التحتية المسؤولة عن إعداد الأجهزة وتقويتها
- فرق الدعم التقني المسؤولة عن تصعيد مشكلات الشبكات والأجهزة
- فرق المخاطر المسؤولة عن الثغرات وأدلة الضوابط
- فرق الحوادث المسؤولة عن الاحتواء والاستعادة والدروس المستفادة

تفترض الدورة مشاركة المتدربين في دعم شبكات مؤسسية أو ضوابط أمنية، ولا تتناول إدارة منتج بعينه أو تطوير البرمجيات أو الإعداد للشهادات.

الإدارات والقطاعات المستهدفة

تخدم الدورة الإدارات والقطاعات التي تعتمد على شبكات متاحة وضوابط قابلة للرصد والاستجابة.

- تقنية المعلومات وتشغيل الشبكات
- الأمن السيبراني والعمليات الأمنية
- إدارة المخاطر واستمرارية الأعمال
- الخدمات المالية والتأمين والخدمات المهنية
- الرعاية الصحية والتعليم والخدمات العامة
- الطاقة والتصنيع والتجزئة والخدمات اللوجستية

AGILE LEADERS
Training Center

أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- بناء خرائط أصول الشبكة وسطح الهجوم
- تطبيق ضوابط جدار الحماية والتجزئة والتقوية
- تحليل حركة الشبكة والتنبيهات والسجلات الأمنية
- ترتيب أولويات الثغرات وإجراءات التحديث
- تشخيص حوادث الشبكات وخيارات الاحتواء
- بناء أدلة الاستجابة وخطط التحسين

جدول الدورة

اليوم 1: أصول الشبكة وبنية الدفاع

- جرد أصول الشبكة وخريطة تدفق البيانات
- مخطط سطح الهجوم وحدود الثقة
- نموذج طبقات ضوابط الدفاع المتعمق
- مصفوفة الوصول الإداري ومستوى الإدارة
- سجل مخاطر الدفاع عن الشبكات والملكية

اليوم 2: جدران الحماية والتجزئة والتقوية

- منهج سياسة جدار الحماية NIST SP 800-41 Rev. 1
- قاعدة المنع الافتراضي وسجل الاستثناءات
- تصميم VLAN وDMZ والمناطق الأمنية
- قائمة فحص تقوية أجهزة الشبكة
- خط أساس الإعداد وسجل ضبط التغيير

AGILE LEADERS
Training Center

اليوم 3: مراقبة الحركة وكشف التسلل

- خطة رؤية حركة الشبكة ونقاط الجمع
- ورقة تحليل تدفق الشبكة والحزم
- مصفوفة قواعد كشف التسلل والتنبيهات
- خريطة مصادر السجلات الأمنية والاحتفاظ بها
- شجرة قرار فرز التنبيهات وتصعيدها

اليوم 4: الثغرات والحوادث والاستعادة

- مصفوفة انكشاف الثغرات وأولوية التحديث
- ملف الاستجابة NIST SP 800-61 Rev. 3
- دليل احتواء حوادث الشبكات
- سجل التسلسل الزمني للأدلة وحيازتها
- سجل التحقق من الاستعادة والتحسين

اليوم 5: ممارسة عمليات الدفاع عن الشبكات

- تمرين رسم خدمة شبكة مكشوفة
- تمرين مراجعة قواعد جدار الحماية والتجزئة
- تمرين التحقيق في حركة الشبكة وتنبيهات الكشف
- تمرين احتواء حادث شبكة واستعادة الخدمة
- المشروع الختامي: حزمة عمليات الدفاع عن الشبكات

التمارين التطبيقية

تستخدم الأنشطة المقترحة مخططات شبكات وسجلات إعداد وأدلة حركة وتنبيهات وسيناريوهات حوادث.

- نشاط مقترح: رسم الأصول وحدود الثقة ومسارات الإدارة لبيئة خدمية
- نشاط مقترح: اختبار قرارات جدار الحماية والتجزئة والتقوية مقابل تدفقات مطلوبة
- نشاط مقترح: ربط أدلة التدفق والحزم والسجلات أثناء فرز تنبيه
- نشاط مقترح: توثيق الاحتواء والاستعادة والتحسين في حزمة عمليات

AGILE LEADERS
Training Center

الأسئلة الشائعة

لمن تناسب دورة عمليات الدفاع عن الشبكات وما متطلباتها؟

تناسب فرق الشبكات والبنية التحتية والعمليات الأمنية والدعم التقني والحوادث التي تدعم فعليا شبكات مؤسسية أو ضوابط أمنية.

كيف تختلف عمليات الدفاع عن الشبكات عن دورة عامة في الأمن السيبراني؟

تركز عمليات الدفاع عن الشبكات على البنية وضوابط الحركة والمراقبة والكشف ومعالجة الحوادث، بينما تغطي دورة الأمن السيبراني العامة نطاقا أوسع من مخاطر الأفراد والعمليات والتطبيقات والبيانات والتقنية.

ماذا يتضمن نموذج تشغيل الدفاع عن الشبكات؟

يتضمن النموذج ملكية الأصول وحدود الثقة وسياسة الحركة وخطوط التقوية ومصادر المراقبة وقرارات التنبيه وأولويات الثغرات وأدلة الحوادث ومسؤوليات الإثبات.

لماذا تعد تجزئة الشبكة مهمة في الدفاع عن الشبكات؟

تفصل تجزئة الشبكة الأنظمة حسب الغرض والمخاطر، وتقيد مسارات الحركة غير الضرورية، وتحد من الانتقال الجانبي، وتنشئ حدودا أوضح للمراقبة والسياسات.

كيف تعمل مراقبة الشبكات والاستجابة للحوادث معا؟

توفر المراقبة أدلة التدفق والحزم والتنبيهات والسجلات التي تدعم كشف الحادث وتحليله وقرارات الاحتواء والتحقق من الاستعادة.

الخاتمة

يعود المشاركون بحزمة عمليات الدفاع عن الشبكات التي تجمع خرائط الأصول والسياسات والتقوية والمراقبة والثغرات والاستجابة والأدلة. تربط الحزمة قرارات الضبط بحركة الشبكة والتنبيهات والمسؤوليات. وتساعد الفرق على اكتشاف الانحرافات واحتواء الحوادث وتحسين الضوابط باتساق.