



دورة ECIH في ممارسة معالجة الحوادث السيبرانية



دورة ECIH في ممارسة معالجة الحوادث السيبرانية

المرجع: 157233_752 التاريخ: 27 سبتمبر – 1 أكتوبر 2027 المكان: القاهرة الرسوم: Euro 5200

نظرة عامة

دورة ECIH في ممارسة معالجة الحوادث السيبرانية دورة متوسطة لمدة 5 أيام لمحلي العمليات الأمنية ومعالجي الحوادث ومديري تقنية المعلومات ومدافعي الشبكات ووظائف دعم الأدلة والمخاطر، ويعود المشاركون منها بدليل معالجة الحوادث والتعافي. تربط الدورة الإعداد والكشف والتحقق وتحديد النطاق والاحتواء وحفظ الأدلة والاستئصال والتعافي والاتصال والتقارير والتحسين عبر قرارات مبنية على سيناريوهات. تطور أجايل للتدريب ممارسة معالجة الحوادث السيبرانية ECIH.

الفئة المستهدفة

- وظائف العمليات الأمنية المسؤولة عن التحقق من التنبيهات والفرز والتصعيد
- وظائف الاستجابة للحوادث المسؤولة عن تنسيق الإجراءات التقنية وإجراءات الأعمال
- وظائف إدارة التقنية المسؤولة عن الأنظمة والشبكات والحسابات المتأثرة والاستعادة
- وظائف دعم الأدلة المسؤولة عن حفظ أدلة الحادث ونقلها
- وظائف المخاطر والاستمرارية المسؤولة عن الأثر والاتصال وتنسيق التعافي

تفترض الدورة أن المشاركين يعملون مع التنبيهات الأمنية أو أدلة الأنظمة والشبكات أو الإجراءات التشغيلية أو أنشطة التعافي، وتستبعد تطوير البرمجيات الضارة والاستغلال الهجومي والاكتساب الجنائي المخبري والتحضير للشهادات والتدريب على الاختبارات.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تحتاج إلى معالجة منسقة للحوادث السيبرانية.

- العمليات الأمنية والدفاع السيبراني
- البنية التحتية لتقنية المعلومات وإدارة الخدمات
- المخاطر والاستمرارية وتنسيق الأزمات
- الخدمات المالية والرعاية الصحية
- الاتصالات والعمليات الصناعية والخدمات الرقمية



أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق توصيات NIST SP 800-61 Rev. 3 على معالجة الحوادث
- تحليل التنبيهات والأدلة والنطاق والشدة وأثر الأعمال
- بناء إجراءات الاحتواء وحفظ الأدلة والاتصال
- تقييم جاهزية الاستئصال والتعافي
- ترتيب التقارير والتسليمات وتحديثات أصحاب المصلحة
- بناء دليل معالجة الحوادث والتعافي

جدول الدورة

اليوم 1: إعداد معالجة الحوادث

- خريطة نتائج الاستجابة وفق NIST SP 800-61 Rev. 3
- مصفوفة أدوار معالجة الحوادث والمصالحات
- ورقة سياق الخدمات والأصول والتبعيات
- دليل الاتصال والتصعيد للحوادث
- قائمة جاهزية الاستجابة ومصادر الأدلة

اليوم 2: الكشف والتحقق وتحديد النطاق

- شجرة قرار التحقق من التنبيه ودرجة الثقة
- مصفوفة تصنيف الحوادث ودرجة الشدة
- ورقة الخط الزمني للأحداث وربطها
- سجل نطاق الأصول والحسابات المتأثرة
- تقييم أثر الحادث وأولوياته



اليوم 3: الاحتواء وحفظ الأدلة

- مخطط الاحتواء قصير الأجل والمستدام
- لوحة إجراءات الشبكة والأجهزة الطرفية والهوية
- دليل أولوية الأدلة المتطايرة والمحفوظة
- سجل معالجة الأدلة ونقلها
- قائمة التحقق من الاحتواء وإعادة تحديد النطاق

اليوم 4: الاستئصال والتعافي والتعلم

- خطة إزالة السبب الجذري وآليات الاستمرارية الخبيثة
- خريطة تسلسل استعادة الأنظمة والتبعيات
- سجل التحقق من التعافي والمراقبة
- تقرير حالة الحادث للإدارة
- سجل التعلم والتحسين بعد الحادث

اليوم 5: ممارسة معالجة الحوادث

- تمرين: التحقق من التنبيهات وتحديد نطاق الحادث
- تمرين: اختيار إجراءات الاحتواء وحفظ الأدلة
- تمرين: تنسيق الاستئصال والاستعادة
- تمرين: تقديم الحالة والتسليم والدروس المستفادة
- المشروع الختامي: دليل معالجة الحوادث والتعافي

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من الخدمات المالية والرعاية الصحية والاتصالات والعمليات الصناعية والخدمات الرقمية.

- نشاط مقترح: التحقق من التنبيهات وبناء خط زمني وتسجيل الأصول والحسابات وخدمات الأعمال المتأثرة.
- نشاط مقترح: اختيار إجراءات الاحتواء مع حفظ الأدلة المتطايرة والمحفوظة للمراجعة المصريح بها.
- نشاط مقترح: ترتيب الاستئصال والاستعادة والتحقق والمراقبة والاتصال بأصحاب المصلحة.
- نشاط مقترح: إعداد تقرير إداري وسجل تحسين من سيناريو حادث.



الأسئلة الشائعة

لمن تناسب دورة ECIH في معالجة الحوادث السيبرانية، وماذا تفترض؟

تناسب وظائف العمليات الأمنية والاستجابة وإدارة التقنية ودفاع الشبكات ودعم الأدلة والمخاطر والاستمرارية، وتفترض العمل مع التنبيهات أو الأدلة أو الإجراءات أو أنشطة التعافي.

كيف تختلف دورة ECIH في معالجة الحوادث عن تدريب الأدلة الجنائية الرقمية؟

تنسق دورة ECIH القرارات من الكشف إلى التعافي، بينما يركز تدريب الأدلة الجنائية الرقمية على الاكتساب والفحص والتفسير المتخصص للأدلة الرقمية.

كيف يدعم 3 NIST SP 800-61 Rev. معالجة الحوادث؟

يربط 3 NIST SP 800-61 Rev. اعتبارات الاستجابة للحوادث بإدارة المخاطر السيبرانية عبر الإعداد والكشف والاستجابة والتعافي والتحسين.

كيف يختار معالجو الحوادث إجراءات الاحتواء؟

يقارن معالجو الحوادث بين الإلحاح والخدمات المتأثرة ونشاط المهاجم ومخاطر الأدلة والأثر التشغيلي وخيارات العزل وإمكان إعادة تحديد النطاق قبل اختيار الاحتواء.

ماذا يتضمن دليل معالجة الحوادث والتعافي؟

يتضمن الدليل الأدوار ومصادر الأدلة ومعايير التصنيف والخطوط الزمنية وسجلات النطاق وخيارات الاحتواء وضوابط الأدلة وإجراءات الاستئصال والتعافي والاتصالات والتقارير ومالكي التحسين.

الخاتمة

يعود المشاركون بدليل معالجة الحوادث والتعافي الذي ينظم القرارات والأدلة والإجراءات والاتصالات. يحول الدليل رد الفعل المجزأ إلى مسار قابل للتتبع من التحقق وتحديد النطاق حتى الاحتواء والتعافي والتعلم. ويدعم التنسيق في الوقت المناسب والتسليمات القابلة للدفاع واستعادة الخدمات والتحسين بعد الحوادث.