



دورة ECIH في ممارسة معالجة الحوادث السيبرانية



AGILE LEADERS
Training Center

دورة ECIH في ممارسة معالجة الحوادث السيبرانية

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 أجائل 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.



فئات الدورات التدريبية

الدورات التدريبية في مجال البيئة والاستدامة	الأعمال الزراعية والأمن الغذائي
دورات إدارة الجودة وتطوير العمليات	دورات إدارة الأزمات واستمرارية الأعمال
دورات إدارة المرافق والعقارات	دورات إدارة الرعاية الصحية
دورات إدارة و تحليل البيانات ودورات علم البيانات	دورات إدارة المنظمات غير الحكومية والعمل الإنساني والتنمية
دورات الأمن السيبراني ودورات تقنية المعلومات	دورات إدارة و تطوير الموارد البشرية
دورات التدريب القانوني والمشتريات والتعاقدات	دورات الاتصال الجماهيري و السياسات والعلاقات العامة
دورات التعليم وتطوير التعلم	دورات التسويق وإدارة علاقات العملاء وإدارة المبيعات
دورات الحوكمة وإدارة المخاطر والامتثال	دورات الحكومة الرقمية والخدمات العامة
دورات الشحن والملاحة البحرية والموانئ	دورات السكرتارية و إدارة المكاتب
دورات الصيانة ودورات المجالات الهندسية المتنوعة	دورات الصحة والسلامة والأمن المهني
دورات المحاسبة و التمويل و دورات الإدارة المالية	دورات الضيافة والسياحة
دورات حفظ التراث وإدارة المتاحف	دورات المهارات الشخصية وتطوير الذات
دورات قطاع النفط والغاز ودورات تقنية متنوعة	دورات في مجالات القيادة والإدارة



فئات الدورات التدريبية

دورات مكتب إدارة المشاريع وإدارة المشاريع الرشيق

دورات معتمدة من قبل هيئات دولية



مدن التدريب

أكرا غانا	أثينا اليونان	أبوظبي الإمارات العربية المتحدة
الدار البيضاء المغرب	استنبول تركيا	أمستردام هولندا
الكويت الكويت	القاهرة مصر	الدوحة قطر
باكو أذربيجان	باريس فرنسا	المنامة مملكة البحرين
براغ جمهورية التشيك	بانكوك تايلند	بالي جمهورية إندونيسيا
بورت لويس موريشيوس	برلين ألمانيا	برشلونة إسبانيا
تبليسي جورجيا	بوكيت تايلند	بورتو البرتغال
جنيف سويسرا	جاكرتا جمهورية إندونيسيا	تورنتو كندا
روما إيطاليا	دبي الإمارات العربية المتحدة	جوهانسبرغ جنوب إفريقيا
سان دييغو الولايات المتحدة الأمريكية	زيورخ سويسرا	زنبار تنزانيا
شم الشيخ مصر	سيول كوريا الجنوبية	سنغافورة سنغافورة
طشقند أوزبكستان	طرابزون تركيا	شيكاغو الولايات المتحدة الأمريكية



مدن التدريب

عن بعد منصة زووم	عمان المملكة الأردنية الهاشمية	طوكيو اليابان
كوالالمبور ماليزيا	فيينا النمسا	فرانكفورت ألمانيا
لشبونة البرتغال	لانكاوي ماليزيا	كيب تاون جنوب إفريقيا
مدريد إسبانيا	ماريبا إسبانيا	لندن المملكة المتحدة
ميلان إيطاليا	مونترال سويسرا	مسقط سلطنة عمان
نيس فرنسا	نيروبي كينيا	ميونخ ألمانيا
		نيويورك الولايات المتحدة الأمريكية