



دورة الاستجابة الجنائية للحوادث وحفظ الأدلة الرقمية



دورة الاستجابة الجنائية للحوادث وحفظ الأدلة الرقمية

المرجع: 157809_760 التاريخ: 31 مايو - 4 يونيو 2027 المكان: القاهرة الرسوم: Euro 4100

نظرة عامة

دورة الاستجابة الجنائية للحوادث وحفظ الأدلة الرقمية دورة متوسطة لمدة 5 أيام لمستجبي الحوادث ومحلي مراكز العمليات وممارسي التحليل الجنائي وفرق الأمن ومنسقي التحقيق، ويعود المشاركون منها بسجل حالات الاستجابة الجنائية للحوادث. تدمج الدورة الجاهزية الجنائية وأولويات البيانات المتطابقة وحفظ الأدلة وربط الأحداث وقرارات الاحتواء والتحقق من التعافي والتسليم القابل للدفاع أثناء الحوادث النشطة. وتوازن بين سرعة الاستجابة وسلامة الأدلة. تطور أجايل للتدريب ممارسة الاستجابة الجنائية للحوادث وحفظ الأدلة الرقمية.

الفئة المستهدفة

- وظائف الاستجابة للحوادث المسؤولة عن الفرز والاحتواء والتعافي والتنسيق
- وظائف العمليات الأمنية المسؤولة عن تصعيد التنبيهات وحفظ سياق التحقيق
- وظائف التحليل الجنائي الرقمي المسؤولة عن سلامة الأدلة وتحليلها وتتبعها
- وظائف العمليات التقنية المسؤولة عن الوصول إلى الأنظمة واستعادتها والتحقق منها
- وظائف تنسيق التحقيق المسؤولة عن النطاق والتوثيق والتسليم

تفترض الدورة أن المشاركين يدعمون الحوادث السيبرانية أو المراقبة أو إدارة الأنظمة أو التحقيقات الرقمية، وتستبعد الملاحظة الجنائية والهندسة العكسية للبرمجيات الخبيثة والتخصص في الأجهزة المحمولة والتحضير للشهادات والتدريب على الاختبارات.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تستجيب للحوادث من دون فقد الأدلة الرقمية.

- العمليات السيبرانية والاستجابة للحوادث والتحقيقات الرقمية
- تقنية المعلومات والمرونة والمخاطر والتوكيد الداخلي
- الخدمات المالية والرعاية الصحية
- الطاقة والعمليات الصناعية والاتصالات
- الخدمات العامة والتعليم والمنصات الرقمية



أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق معايير قرارات الاستجابة للحوادث والجاهزية الجنائية
- ترتيب أولويات الأدلة المتطايرة والثابتة والشبكية والتطبيقية
- استخدام سجلات الحفظ والاكتساب وسلسلة الحيازة والسلامة
- تحليل المؤشرات والآثار لبناء خط زمني قابل للدفاع
- تقييم إجراءات الاحتواء والتعافي وفق أثرها في الأدلة
- بناء سجل حالات الاستجابة الجنائية للحوادث

جدول الدورة

اليوم 1: تأسيس جاهزية الاستجابة الجنائية

- خريطة اعتبارات الاستجابة وفق NIST SP 800-61 Rev. 3
- دورة دمج التحليل الجنائي وفق NIST SP 800-86
- مصفوفة سلطة الحادث ونطاقه وتصعيده
- سجل الجاهزية الجنائية ومصادر الأدلة
- تعيين أدوار الاستجابة وسلسلة الحيازة

اليوم 2: حفظ أدلة الحادث النشط

- مصفوفة أولويات جمع البيانات المتطايرة
- خريطة مصادر أدلة الأنظمة والشبكات والتطبيقات
- قائمة مخاطر الاكتساب الحي وجدواه
- سجل سلامة الأدلة وبصمتها التشفيرية
- حزمة توثيق الحفظ والحيازة والنقل



اليوم 3: فرز الأحداث وإعادة بنائها

- لوحة أسئلة وفرضيات الفرز الجنائي
- مصفوفة ربط المؤشرات والآثار والمصادر
- أسلوب توحيد الطوابع الزمنية وتسلسل الأحداث
- لوحة إعادة بناء الخط الزمني للحادث عبر الأنظمة
- سجل التناقضات والفجوات والوزن الاستدلالي

اليوم 4: موازنة الاحتواء والتعافي

- مصفوفة إجراءات الاحتواء وأثرها في الأدلة
- شجرة قرار العزل والإيقاف والمراقبة
- سجل تغييرات الاستئصال وتتبع الأدلة
- قائمة التحقق من التعافي والمؤشرات المتبقية
- قالب تقرير النتائج والقيود والتسليم

اليوم 5: ممارسة الاستجابة الجنائية للحوادث

- تمرين: تحديد نطاق حادث وتعيين أولويات الأدلة
- تمرين: حفظ الأدلة المتطيرة والثابتة
- تمرين: إعادة بناء خط زمني للحادث عبر المصادر
- تمرين: الدفاع عن قرارات الاحتواء والتعافي
- المشروع الختامي: سجل حالات الاستجابة الجنائية للحوادث

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من الخدمات المالية والرعاية الصحية والطاقة والاتصالات والمنصات الرقمية.

- نشاط مقترح: فرز اختراق نشط وترتيب مصادر الأدلة قبل أن يغير الاحتواء البيئة.
- نشاط مقترح: توثيق قرارات الاكتساب والسلامة والحيارة والنقل للأدلة المتطيرة والثابتة.
- نشاط مقترح: ربط آثار الأنظمة والشبكات والتطبيقات في خط زمني يتضمن الفجوات والتناقضات.
- نشاط مقترح: عرض الاحتواء والتحقق من التعافي والقيود وتسليم تشغيلي قابل للدفاع.



الأسئلة الشائعة

لمن تناسب دورة الاستجابة الجنائية للحوادث، وماذا تفترض؟

تناسب وظائف الاستجابة للحوادث والعمليات الأمنية والتحليل الجنائي الرقمي والعمليات التقنية وتنسيق التحقيق، وتفترض المشاركة العملية في الحوادث أو المراقبة أو الأنظمة أو الأدلة الرقمية.

كيف تختلف الاستجابة الجنائية للحوادث عن تدريب التحليل الجنائي للحاسب؟

تحفظ الاستجابة الجنائية للحوادث الأدلة وتحللها أثناء احتواء الحادث والتعافي منه، بينما يركز التحليل الجنائي العام للحاسب على اكتساب آثار الحاسب وفحصها بعد وقوع الحدث بنطاق أوسع.

ما الأدلة التي تحفظها الاستجابة الجنائية للحوادث أولاً؟

ترتب الأدلة وفق سرعة تغييرها وقيمتها للتحقيق وجدوى جمعها وأثرها في الأعمال والسلطة المتاحة واحتمال تعديلها أو إتلافها بفعل الاحتواء أو التعافي.

كيف تحمي قرارات الاحتواء الأدلة الرقمية؟

توثق قرارات الاحتواء والإجراء والغرض والتوقيت والأنظمة المتأثرة والأثر المتوقع في الأدلة والبدائل والموافقات والبيانات المحفوظة وفحوص السلامة والتغير الناتج في خط التحقيق الزمني.

كيف يتم التحقق من التعافي أثناء الاستجابة الجنائية للحوادث؟

يتم التحقق بفحص الأصول المستعادة والمؤشرات المتبقية وتغييرات الحسابات والوصول وتشغيل الضوابط وتغطية المراقبة ومسارات الاستمرارية المعروفة ووظائف الأعمال وتتبعها إلى نتائج الحادث.

الخاتمة

يعود المشاركون بسجل حالات الاستجابة الجنائية للحوادث الذي يربط السلطة وأولويات الأدلة والحفظ وتحليل الخط الزمني والاحتواء والتحقق من التعافي والتسليم. يحول السجل إجراءات الاستجابة والتحقيق المتنافسة إلى قرارات تشغيلية قابلة للتتبع. ويدعم سلامة الأدلة وسرعة التنسيق والمفاضلات المعقدة ومراجعة النظراء والتواصل القابل للدفاع بشأن النتائج والقيود.