JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة التحقيق الجنائي في الحاسوب

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة التحقيق الجنائي في الحاسوب

التحقيق الجنائي في الحاسوب دورة تدريبية مدتها أسبوع لفاحصي الأدلة الرقمية والمحققين ومعالجي الحوادث الذين يستخرجون الأدلة من أجهزة الحاسوب ويفسرونها، ويخرج المشاركون منها بتقرير فحص جنائي يصمد أمام الطعن. أصبحت عمليات الاحتيال وإساءة الاستخدام الداخلية والاختراقات تترك أوضح آثارها على الأقراص والسجلات وقواعد التسجيل، فقد يؤدي التعامل غير السليم مع الدليل إلى سقوط قضية تأديبية أو مطالبة قانونية. تقدم جوبيتر برايم للتدريب هذه الدورة في التحقيق الجنائي في الحاسوب.

لماذا يهم التحقيق الجنائي في الحاسوب الآن

تشكل ثلاثة ضغوط العمل الجنائي الرقمي اليوم. فأحجام التخزين تتزايد، ووحدات التخزين ذات الحالة الصلبة والتشفير تعقد الاسترداد، والمحاكم والمدققون والخبراء المقابلون يدققون في كل خطوة من خطوات الاستحواذ على الدليل.
والمؤسسة التي تحفظ الأدلة بطريقة صحيحة تستطيع محاسبة الموظفين واسترداد الخسائر ومعرفة أسلوب المخترق بدقة، أما التي تهمل ذلك فتواجه نتائج مرفوضة وحوادث متكررة. وترتبط الجاهزية الجنائية بوظيفتي الاستجابة والتعافي في إطار الأمن السيبراني NIST CSF 2.0، وبضوابط أدلة الحوادث في المواصفة ISO/IEC 27001:2022 لنظم إدارة أمن المعلومات.

المستفيدون من التحقيق الجنائي في الحاسوب

- الفاحصون الذين يستحوذون على وسائط التخزين من الأجهزة المضبوطة وينسخونها ويحللونها
- المحققون الذين يتولون قضايا الاحتيال وسوء السلوك وسرقة البيانات
- معالجو الحوادث الذين يحفظون الأدلة المتطايرة وأدلة الأقراص أثناء الاختراقات
- محللو الأمن الذين يبنون الخطوط الزمنية من السجلات وآثار النظام
- مختصو التدقيق والامتثال الذين يطلبون النتائج الجنائية أو يعتمدون عليها

تستفيد وحدات التحقيق الداخلي في القطاع البنكي وقطاع الرعاية الصحية أكثر عندما يحضر الفاحصون ومحققو القضايا معا، لأنهم يعتمدون معيارا واحدا لمعالجة الأدلة.

قدرات التحقيق الجنائي في الحاسوب

ينتقل المشاركون من البحث العشوائي في الملفات إلى منهج فحص قابل للتكرار يمكن شرح كل خطوة فيه أثناء الاستجواب المضاد.

- تطبيق أساليب استحواذ سليمة تحفظ سلامة الوسائط الأصلية — المستشار القانوني
- بناء نسخ جنائية موثقة بقيم التجزئة المشفرة — محقق القضية
- تحليل أنظمة الملفات والبيانات المحذوفة وآثار قاعدة التسجيل — الفاحص الرئيسي
- إعادة بناء الخطوط الزمنية للأحداث من بيانات الملفات الوصفية وسجلات النظام — مدير الحوادث
- اختبار سلوك الأدوات الجنائية وتوثيقه قبل الاعتماد على نتائجها — مراجع الجودة
- عرض النتائج في تقارير وشهادات يفهمها غير المختصين — اللجنة التأديبية أو هيئة التحكيم

مصطلحات التحقيق الجنائي في الحاسوب الأساسية

- سلسلة الحيازة — السجل الموثق لمن حاز الدليل ومتى وأين ولماذا، من الضبط حتى العرض.
- النسخة الجنائية — نسخة مطابقة بتا ببت لوسيط التخزين بما فيها المساحة غير المخصصة، تفحص بدلا من الأصل.
- قيمة التجزئة — بصمة رقمية ثابتة الطول تثبت أن النسخة لم تتغير منذ الاستحواذ.
- مانع الكتابة — جهاز أو ضابط برمجي يمنع أي تغيير على الوسيط المصدر أثناء الاستحواذ.
- أثر قاعدة التسجيل — مدخل في سجل نظام Windows يكشف نشاط المستخدم أو الأجهزة الموصولة أو تشغيل البرامج.
- الخط الزمني الموسع — تسلسل زمني مدمج لأحداث نظام الملفات والسجلات والآثار لإعادة بناء النشاط.

التحقيق الجنائي في الحاسوب يوما بيوم

اليوم 1: المبادئ الجنائية والتحضير للقضية

- نموذج العملية الجنائية — ترتيب التحديد والحفظ والتحليل والعرض
- التحقق من السند القانوني — تأكيد الإذن قبل فحص الأجهزة
- نماذج سلسلة الحيازة — تسجيل كل انتقال للدليل
- الجاهزية الجنائية — ربط جمع الأدلة بوظيفة الاستجابة في NIST CSF 2.0
- مقابلة تحديد نطاق القضية — صياغة الأسئلة التي يجيب عنها الفحص

اليوم 2: الاستحواذ على الأدلة والنسخ الجنائي

- التقاط الذاكرة المتطايرة — تقرير ما يجمع قبل إيقاف التشغيل
- أساليب منع الكتابة — حماية الوسائط المصدر أثناء الاستحواذ
- صيغ نسخ الأقراص — الاختيار بين الحاويات الخام والمضغوطة
- التحقق بالتجزئة — إثبات سلامة النسخة عبر كل نسخة لاحقة
- اختبار التحقق من الأدوات — توثيق السلوك المعروف للبرمجيات الجنائية

اليوم 3: تحليل نظام الملفات وقاعدة التسجيل

- بنى أنظمة الملفات — تفسير البيانات الوصفية في NTFS و FAT
- استرداد الملفات المحذوفة — استخلاص البيانات من المساحة غير المخصصة
- فحص خلايا قاعدة التسجيل — تتبع نشاط المستخدم وأجهزة USB
- آثار المتصفح والبريد الإلكتروني — ربط المراسلات بالمشتبه بهم
- مؤشرات التشفير ومقاومة التحليل الجنائي — تقدير خطر العبث بالأدلة

اليوم 4: الخطوط الزمنية والربط بين الأدلة

- تفسير الطوابع الزمنية — معالجة فروق المناطق الزمنية وانحراف الساعة
- بناء الخط الزمني الموسع — دمج أحداث الملفات والسجلات والآثار
- تحليل سجلات الأحداث — تحديد عمليات الدخول والتشغيل والتنقل الجانبي
- اختبار الفرضيات — الموازنة بين التفسيرات المتنافسة لنشاط المستخدم
- مطابقة ضوابط الأدلة — مواءمة النتائج مع ضوابط التسجيل في ISO/IEC 27001:2022

اليوم 5: تطبيق تقرير الفحص الجنائي

- مراجعة سجل الاستحواذ — تأكيد أدلة الحيازة والتجزئة من اليوم 2
- اختيار نتائج الآثار — انتقاء أدلة قاعدة التسجيل والملفات للعرض
- إعداد مستند الخط الزمني — عرض الأحداث المعاد بناؤها بوضوح
- محاكاة الاستجواب المضاد — الدفاع عن الأساليب أمام أسئلة معادية
- تقرير الفحص الجنائي — إنهاء النتائج والقيود والمستندات المرفقة

تطبيق التحقيق الجنائي في الحاسوب بعد الدورة

- إعادة صياغة نموذج سلسلة الحيازة في الوحدة واختباره في عملية الضبط التالية.
- إجراء اختبار تحقق لأداة النسخ الرئيسية وحفظ نتائجه مع إجراءات القضايا.

أسئلة حول التحقيق الجنائي في الحاسوب

ما التحقيق الجنائي في الحاسوب ولماذا يهم الآن؟

هو الاسترداد المنضبط للأدلة الرقمية من أجهزة الحاسوب وتفسيرها بحيث تصمد النتائج أمام التدقيق. ويهم الآن لأن الاحتيال وسوء السلوك والاختراقات تترك آثارها الرئيسية على الوسائط الرقمية بصورة متزايدة.

ما الأدوار الأكثر استفادة من تدريب التحقيق الجنائي في الحاسوب؟

يستفيد أكثر فاحصو الأدلة الرقمية ومحققو القضايا ومعالجو الحوادث. كما يستفيد محللو الأمن ومختصو التدقيق الذين يعتمدون على النتائج الجنائية من معرفة طريقة الاستحواذ على الأدلة واختبارها.

كيف يختلف التحقيق الجنائي في الحاسوب عن دورة الاستجابة للحوادث؟

يركز التحقيق الجنائي على عمق الدليل وقبوله وكتابة التقرير. أما دورة الاستجابة للحوادث فتركز على الاحتواء السريع والتعافي، بينما تفحص هنا الوسائط بالتفصيل وتدافع عن كل نتيجة.

ماذا تعود به من تدريب التحقيق الجنائي في الحاسوب؟

تعود بتقرير فحص جنائي أعددته من نسخة قضية تدريبية، يضم سجلات الحيازة ومستندات الخط الزمني والقيود المعلنة، جاهزا للاستخدام نموذجا في وحدتك.

التحقيق الجنائي في الحاسوب: الطريق إلى الأمام

يحدد تقرير الفحص الجنائي أولا ما إذا كانت القضية ستنتقل إلى إجراء تأديبي أو مدني أو جزائي. ويستخدمه المحققون والمستشارون القانونيون ولجان القرار لتقدير قوة الأدلة. وبعد استخدامه الأول يستحق التحقق من مدى فهم غير المختصين لمستندات الخط الزمني، وتبسيط كل نتيجة أثارت أسئلة متكررة، ثم تحديث النموذج قبل القضية التالية في الوحدة.