الدورة التدريبية: تحليل الطب الشرعي الرقمي - الأدوات وتقنيات: التحقيق في الجرائم السيبرانية



16 - 20 نوفمبر 2026
كاليفورنيا
7900 € (للشخص الواحد)
Ref: #CYB4827_327014

مقدمة الدورة التدريبية / لمحة عامة:

في عالمنا الرقمي المتسارع، أصبحت الجرائم السيبرانية أكثر تعقيدًا وتواترًا، مما يجعل تحليل الطب الشرعي الرقمي أداة لا غنى عنها للتحقيق في الحوادث الأمنية وجمع الأدلة الجنائية الرقمية. تقدم هذه الدورة التدريبية المتخصصة للمحترفين المعرفة والمهارات اللازمة لإجراء تحقيقات جنائية رقمية شاملة، بدءًا من الحفاظ على الأدلة وحتى تحليل البيانات المعقدة وتقديم التقارير القانونية. سنتناول في هذه الدورة مبادئ الطب الشرعي الرقمي، أدوات التحليل المتقدمة، وتقنيات استعادة البيانات من مختلف الأجهزة. سيكتسب المشاركون القدرة على تتبع المسارات الرقمية للمهاجمين، وكشف البرمجيات الخبيثة، والتعامل مع الأدلة الرقمية بطريقة تضمن صلاحيتها في المحاكم. تهدف الدورة إلى إعداد المتخصصين لمواجهة التحديات في التحقيق بالجرائم السيبرانية وبناء قدرات تحقيق رقمي قوية. يستند المحتوى إلى أحدث المعايير وأفضل الممارسات في مجال الطب الشرعي الرقمي، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور إيفان كيسي (Eoghan Casey)، مؤلف العديد من الأعمال المرجعية في التحقيق الجنائي الرقمي. يقدم BIG BEN Training Center هذه الدورة لتعزيز قدرات المحترفين في مكافحة الجريمة السيبرانية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- محققو الطب الشرعي الرقمي.
- متخصصو الأمن السيبراني.
- أفراد فرق الاستجابة للحوادث الأمنية.
- المحققون الجنائيون وضباط إنفاذ القانون.
- مدققو أمن المعلومات.
- أي مهني مسؤول عن جمع الأدلة الرقمية وتحليل الحوادث الأمنية.

القطاعات والصناعات المستهدفة:

- القطاع الحكومي والهيئات القضائية وما في حكمها.
- وكالات إنفاذ القانون والأمن الوطني.
- شركات الأمن السيبراني وخدمات الاستشارات الأمنية.
- القطاع المالي والمصرفي للتحقيق في الاحتيال السيبراني.
- شركات المحاماة المتخصصة في الجرائم التقنية.
- المؤسسات الكبرى التي تتعامل مع حوادث اختراق البيانات.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة المخاطر والامتثال.
- القسم القانوني.
- التحقيقات الداخلية.
- فرق الاستجابة للحوادث.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم مبادئ الطب الشرعي الرقمي وسلسلة الحضانة للأدلة.
- القدرة على جمع الأدلة الرقمية من مختلف المصادر (أجهزة الكمبيوتر، الأجهزة المحمولة، الشبكات).
- استخدام أدوات وتقنيات الطب الشرعي الرقمي لإجراء التحقيقات.
- تحليل سجلات الأنظمة وحركة مرور الشبكة لاكتشاف الأنشطة المشبوهة.
- استعادة البيانات المحذوفة والمخفية من الأقراص الصلبة.
- فحص البرمجيات الخبيثة وتحليل السلوكيات الضارة.
- إعداد تقارير الطب الشرعي الرقمي القابلة للاستخدام في المحاكم.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية عملية ومكثفة، تركز على تزويد المشاركين بالخبرة المباشرة في تحليل الطب الشرعي الرقمي. سيتمكن المتدربون من خلال المحاكاة العملية لسيناريوهات الجرائم السيبرانية وورش العمل التطبيقية من استخدام أدوات الطب الشرعي الرقمي الرائدة مثل Volatilityg FTK Imagerg Autopsy. تتضمن المنهجية دراسات حالة حقيقية لتحقيقات جنائية رقمية، مع تحليل مفصل لعمليات جمع الأدلة وتقنيات التحليل. سيتم التركيز على التعامل مع الأدلة الرقمية بطريقة تضمن سلامتها وقبولها في الإجراءات القانونية. يقدم BIG BEN Training Center هذه الدورة لتمكين المتخصصين من أن يصبحوا خبراء في التحقيق بالجرائم السيبرانية ودعم العدالة الرقمية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الطب الشرعي الرقمي والمبادئ القانونية

- مقدمة إلى الطب الشرعي الرقمي ودوره.
- مراحل التحقيق الجنائي الرقمي.
- سلسلة الحضانة (Chain of Custody) للأدلة الرقمية.
- المبادئ القانونية والأخلاقية في الطب الشرعي الرقمي.
- أنواع الجرائم السيبرانية وكيفية التحقيق فيها.
- الاستعداد للتحقيق في الحوادث.
- تخطيط الاستجابة لحوادث الأمن السيبراني.

الوحدة الثانية: جمع الأدلة الرقمية والحفاظ عليها

- تقنيات جمع الأدلة من أجهزة الكمبيوتر.
- الحصول على صور الأقراص الصلبة (Disk Imaging).
- جمع الأدلة من الذاكرة العشوائية (RAM Forensics).
- جمع الأدلة من الأجهزة المحمولة.
- جمع الأدلة من الشبكات.
- أدوات جمع الأدلة الرقمية.
- توثيق عملية جمع الأدلة.

الوحدة الثالثة: تحليل البيانات الرقمية واستعادة الأدلة

- تحليل أنظمة الملفات (File System Analysis).
- استعادة البيانات المحذوفة والبيانات المخفية.
- تحليل سجلات الأحداث (Log Analysis).
- تحليل سجلات المتصفح والبريد الإلكتروني.
- التعامل مع البيانات المشفرة والمضغوطة.
- أدوات تحليل البيانات الرقمية.
- بناء مخطط زمني للحوادث.

الوحدة الرابعة: الطب الشرعي للشبكات والبرمجيات الخبيثة

- مقدمة إلى الطب الشرعي للشبكات (Network Forensics).
- تحليل حزم البيانات (Packet Analysis).
- كشف الاختراقات عبر تحليل الشبكة.
- مقدمة إلى تحليل البرمجيات الخبيثة (Malware Analysis).
- أنواع البرمجيات الخبيثة وسلوكياتها.
- أدوات تحليل البرمجيات الخبيثة.
- تتبع مصادر الهجمات السيبرانية.

الوحدة الخامسة: إعداد التقارير القانونية وشهادة الخبراء

- كتابة تقارير الطب الشرعي الرقمي الاحترافية.
- هيكلة التقرير والمحتوى المطلوب.
- تقديم الأدلة في المحاكم.
- الشهادة كخبير في الطب الشرعي الرقمي.
- التحديات القانونية في قضايا الجرائم السيبرانية.
- التحسين المستمر لمهارات التحقيق.
- مستقبل الطب الشرعي الرقمي.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

في ظل التطور السريع للتقنيات الرقمية وأساليب المهاجمين، كيف يمكن لمحقق الطب الشرعي الرقمي أن يظل متقدمًا بخطوة على الجرائم السيبرانية، ليس فقط من خلال الأدوات والتقنيات الحالية، بل من خلال تطوير فهم عميق للأنظمة المستقبلية وتأثيرها على جمع وتحليل الأدلة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها العملي والمعمق على تحليل الطب الشرعي الرقمي، مما يوفر للمشاركين مهارات حقيقية للتحقيق في الجرائم السيبرانية. بدلاً من مجرد سرد المفاهيم، نغوص في التطبيق العملي لأدوات وتقنيات الطب الشرعي الرقمي، مما يميزها عن الدورات النظرية. تقدم الدورة سيناريوهات تحقيق واقعية ودراسات حالة مفصلة، مما يمنح المشاركين خبرة عملية لا تقدر بثمن في التعامل مع الأدلة الرقمية واستعادة البيانات. نركز على كيفية إعداد تقارير الطب الشرعي القابلة للاستخدام القانوني، وهي مهارة حاسمة للمحترفين في هذا المجال. إنها ليست مجرد دورة لتعلم الأدوات، بل هي برنامج تدريبي شامل يهدف إلى بناء خبراء تحقيق رقمي قادرين على كشف الحقيقة ودعم العدالة في العالم الرقمي.