



التحليل الجنائي لأنظمة Windows والتحقيق المتقدم في NTFS



AGILE LEADERS
Training Center

13 - 17 Sep 2027
لندن



التحليل الجنائي لأنظمة Windows والتحقيق المتقدم في NTFS

المرجع: 103600651_82912 التاريخ: 13 - 17 Sep 2027 الموقع: لندن الرسوم: Euro 5700

نظرة عامة على الدورة

تطور دورة التحليل الجنائي لأنظمة Windows والتحقيق المتقدم في NTFS المهارات العملية اللازمة للتحقيق في أنظمة التشغيل، وإعادة بناء أنشطة المستخدمين، ودعم الاستجابة للحوادث السيبرانية. يدرس المشاركون الندلة الجنائية المستهدفة من سجل النظام، وسجلات الأحداث، والملفات التمهيدية، وذاكرة التخزين الموقت، وأثار التصفح، والملفات المرتبطة بالمستخدمين، وأجهزة USB، والتطبيقات السحابية. تعزز الدورة التدريبية المعايير التقليدية للتحقيق الرقمي من خلال التركيز على نظام ملفات NTFS، بما في ذلك تحليل جدول الملفات الرئيسي، وسجلات التغيير، والملفات المحذوفة، والطوابع الزمنية، والخط الزمني لأنظمة التهديدات الواقعية التحقيق سيناريوهات تغطي. النتائج دقيقة لضمان واحد مصدر على الاعتماد من بدلا المتعددة الندلة ربط كيفية المشاركون يتعلم Windows الداخلية، وتسريب البيانات، وأنشطة البرمجيات الخبيثة، والوصول غير المصرح به، والملفات الوعد تسميتها، والندلة المحذوفة، والوسائط القابلة للإزالة، وسلوكيات مكافحة الندلة الجنائية. توضح دراسة حالة تسريب البيانات من المعهد الوطني للمعايير والتقنية كيفية دمج أدلة البريد الإلكتروني، والمتصفحات، والبحث، والتخزين السحابي، ونظام الملفات في خط زمني تحقيقي واحد متكامل.

الفئة المستهدفة

- محللو الندلة الرقمية
- أخصائيو الاستجابة للحوادث والاستجابة السيبرانية
- محللو مراقبة العمليات الأمنية والأمن السيبراني
- فاحصو الندلة الجنائية للكمبيوتر
- محققو جرائم الكمبيوتر
- صانعو التهديدات
- محترفو أمن نقاط النهاية
- فرق التحقيق الداخلي والتحقيقات المؤسسية
- محترفو أمن تكنولوجيا المعلومات

الإدارات المستهدفة

- التحقيقات الرقمية والاستجابة للحوادث
- الأمن السيبراني وعمليات مراقبة أمن المعلومات
- الأمن المؤسسي والتحقيقات
- التحقيق الداخلي والامتثال
- الشؤون القانونية والاكتشاف الإلكتروني
- إدارة الاحتيال والمخاطر الداخلية
- البنية التحتية لتكنولوجيا المعلومات وأمن نقاط النهاية



القطاعات المستهدفة

- الخدمات المصرفية والمالية
- القطاع الحكومي والدفاع
- النفط والغاز والطاقة
- الاتصالات
- الرعاية الصحية
- البنية التحتية الحرجة
- تكنولوجيا المعلومات والخدمات السحابية
- التصنيع

أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- شرح عملية التحقيق الجنائي لمنظومة التشغيل
- تحديد مواقع الأدلة الرئيسية وملفات النظام المختلفة
- وصف آليات الفرز السريع لأدلة نقاط النهاية
- مناقشة هندسة نظام الملفات وبياناته الوصفية
- تمييز دور جداول الملفات الرئيسية وسجلات التغيير
- تصنيف الملفات المحذوفة والمنقولة والمعاد تسميتها
- مقارنة أدلة سجل نظام التشغيل وملفات التنفيذ
- توضيح آلية فحص الوسائط القابلة للإزالة وأجهزة التخزين
- تلخيص طرق تحليل سجلات الأحداث والخطوط الزمنية

محاور الدورة

اليوم الأول: التحقيق الجنائي لنظم التشغيل وفهرز الأدلة

- فهم عملية التحقيق الجنائي لنظم التشغيل
- تحديد الأدلة الرئيسية ومواقع الملفات المرتبطة بها
- جمع وترتيب أولويات الأدلة أثناء الفهرز الجنائي
- تثبيت وفحص صور الأدلة الجنائية لنظم التشغيل
- تحليل البيانات الوصفية للملفات

اليوم الثاني: التحقيق المتقدم في نظام الملفات والبيانات الوصفية

- دراسة هندسة نظام الملفات NTFS بعوق
- تحليل جدول الملفات الرئيسي وسجلات التغيير
- فحص الملفات المحذوفة واستعادة النثر الرقمية
- فهم وتفسير الطوابق الزمنية بدقة
- إنشاء وتحليل الخطوط الزمنية لنظم التشغيل

اليوم الثالث: تحليل سجل النظام وأدلة تنفيذ البرامج

- فحص الهيكل الداخلي لسجل النظام
- تحديد آثار تنفيذ البرامج والتطبيقات
- دراسة الملفات المرتبطة بالارتباطات والقوائم المختصرة
- تتبع نشاط المستخدمين عبر مسارات التصفح والمجلدات
- تحليل سجلات الأجهزة الموصلة والوسائط القابلة للإزالة

اليوم الرابع: تحليل سجلات الأحداث والأنشطة الشبكية والسحابية

- استعراض وتحليل سجلات الأحداث لنظام التشغيل
- تتبع أنشطة المتصفحات واستخراج الأدلة الرقمية
- فحص أدلة البريد الإلكتروني والتطبيقات السحابية
- ربط أدلة الأجهزة الطرفية بالأنشطة المشبوهة
- دراسة سلوكيات وكافة الأدلة الجنائية وكشفها

اليوم الخامس: التطبيقات العملية ودراسات الحالة المتقدمة

- تطبيق سيناريو تسريب البيانات العملي للمعهد الوطني للمعايير والتقنية
- ربط أدلة البريد الإلكتروني والبحث والتخزين السحابي
- اختبار الفرضيات التحقيقية وإعادة بناء الحوادث
- تقييم أدلة التهديدات الداخلية والملفات المعد تسميتها
- صياغة وتقديم النتائج التحقيقية بشكل احترافي

الأسئلة الشائعة

- هل تتطلب الدورة خبرة مسبقة في الأمن السيبراني؟

تفضل وجود خلفية أساسية في مفاهيم الشبكات وأنظمة التشغيل لضمان الاستفادة القصوى من المحتوى المتقدم.

- هل يتم توفير تراخيص برامج تحليل جنائي خلال التدريب؟

لا يتم توفير برامج أو تراخيص تجارية، ولكن تركز الدورة على المنهجيات التحقيقية مع استعراض أمثلة توضيحية للحوادث ذات الصلة.

- كيف تساعد الدورة في سيناريوهات العمل اليومية؟

تزود المشاركين بالقدرة على ربط الندوة المتعددة واستخدام التحقيق المتقدم في نظام NTFS لمواجهة الحوادث المعقدة بكفاءة.

فئات الدورات التدريبية

الدورات التدريبية في مجال البيئة والاستدامة	دورات إدارة الجودة وتطوير العمليات
دورات إدارة و تحليل البيانات ودورات علم البيانات	دورات إدارة و تطوير الموارد البشرية
دورات الذهن السيرياني ودورات تقنية المعلومات	دورات الاتصال الجماهيري و السياسات والعلاقات العامة
دورات التدريب القانوني والهشتريات والتعاقدات	دورات التسويق وإدارة علاقات العملاء وإدارة المبيعات
دورات الحوكمة وإدارة المخاطر والامتثال	دورات السكرتارية و إدارة المكاتب
دورات الصحة والسلامة والذهن المهني	دورات الصيانة ودورات المجالات الهندسية المتنوعة
دورات المحاسبة و التهويل و دورات الإدارة المالية	دورات المهارات الشخصية وتطوير الذات
دورات في مجالات القيادة والإدارة	دورات معتمدة من قبل هيئات دولية
دورات مكتب إدارة المشاريع وإدارة المشاريع الرشيقية	



مدن التدريب

أهستردام هولندا	أكرا غانا	أثينا اليونان
الدار البيضاء المغرب	الجبيل المملكة العربية السعودية	استنبول تركيا
القاهرة مصر	الرياض المملكة العربية السعودية	الدوحة قطر
باريس فرنسا	الهناوة مملكة البحرين	الكويت الكويت
براغ جمهورية التشيك	بانكوك تايلند	باكو أذربيجان
بورتو البرتغال	برلين ألمانيا	برشلونة إسبانيا
تورنتو كندا	تيليسي جورجيا	بوكيت تايلاند
جوهانسبرغ جنوب افريقيا	جنيف سويسرا	جاكرتا جمهورية اندونيسيا
زنجار تنزانيا	روما إيطاليا	حلي الإمارات العربية المتحدة
سيول كوريا الجنوبية	سنغافورة سنغافورة	سان دييغو الولايات المتحدة الأمريكية
طرابزون تركيا	شيكاغو الولايات المتحدة الأمريكية	شرم الشيخ مصر
عمان المملكة الأردنية الهاشمية	طوكيو اليابان	طشقند أوزبكستان
فيينا النمسا	فرانكفورت ألمانيا	عن بعد منصة زووم

مدن التدريب

لانكاوي ماليزيا	كيب تاون جنوب افريقيا	كوالالمبور ماليزيا
هاربيا اسبانيا	لندن المملكة المتحدة	لشبونة البرتغال
هونتر سويسرا	مسقط سلطنة عمان	مدريد اسبانيا
نيروبي كينيا	ميونخ المانيا	ميلان ايطاليا
		نيويورك الولايات المتحدة الأمريكية