

دورة التحضير لاختبار استخبارات المصادر المفتوحة

GIAC GOSI

10 – 14 مايو 2027

نيويورك

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة التحضير لاختبار استخبارات المصادر المفتوحة GIAC GOSI

المرجع: 262638_2223 **التاريخ:** 10 – 14 مايو 2027 **المكان:** نيويورك **الرسوم:** 12000 Euro

نظرة عامة

دورة التحضير لاختبار استخبارات المصادر المفتوحة GIAC GOSI هي دورة عملية تمتد أسبوع، مخصصة للمحللين والمحققين الرقميين ومختصي الأمن السيبراني لتمكينهم من جمع البيانات العلنية وتحليلها وإثبات الأدلة وفق المعايير المهنية المعتمدة. يعالج هذا البرنامج فجوات تأمين الهوية الرقمية التشغيلية وصعوبات تتبع الكيانات والتهديدات الخارجية ضمن بيئات التحقيق المعقدة، من خلال منهج تطبيقي يدمج تقنيات البحث المتقدم، واستخراج الأدلة الرقمية، وتوثيق سلاسل الحيازة. تقدم أجايل للتدريب تدريبات مكثفة تدمج أطر التحقيق الاحترافية وتطبيقات الفحص التقني.

الفئة المستهدفة

- محللو استخبارات التهديدات السيبرانية CTI ومسؤولو مراكز العمليات الأمنية SOC المعنيون بتتبع الخصوم ومراقبة تسريبات البيانات ومساحات الهجوم الخارجية.
- ممارسو الاستجابة للحوادث الرقمية والتحقيق الجنائي الرقمي DFIR المكلفون بإعادة بناء الآثار الرقمية والتحقق من الهويات المشبوهة.
- مختصو اختبار الاختراق والفرق الحمراء المسؤولون عن تنفيذ عمليات الاستطلاع الخارجي ومحاكاة هجمات الخصوم ضد الأصول التقنية.
- محققو مكافحة الاحتيال والتدقيق المؤسسي المعنيون بمكافحة غسل الأموال، والتحقق من ملكية الشركات، وتقييم المخاطر الخارجية.

تفترض الدورة امتلاك المشارك خبرة عملية في أساسيات شبكات الحاسب وأنظمة التشغيل ومفاهيم أمن المعلومات، بينما تستبعد البرمجة المتقدمة أو كتابة برمجيات الاستغلال.

الإدارات والقطاعات المستهدفة

توجه الدورة خدماتها المهنية للمختصين في إدارات حيوية عبر قطاعات متعددة تشمل الخدمات المالية، والاتصالات، وتقنية المعلومات، والطاقة:

- إدارات الأمن السيبراني ومراكز العمليات الأمنية واستخبارات التهديدات.
- قطاع الخدمات المالية والمصرفية وإدارات مكافحة الاحتيال المالي.
- قطاع الاتصالات وتقنية المعلومات وإدارات إدارة المخاطر الرقمية.
- إدارات التحقيق الداخلي والتدقيق الجنائي وإدارة الامتثال المؤسسي.

AGILE LEADERS
Training Center

أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق تقنيات الأمان التشغيلي وعزل البيئات الافتراضية لحماية الهوية الرقمية أثناء عمليات الجمع.
- استخراج البيانات العلنية باستخدام مشغلات البحث المتقدم وتقنيات الكشط الآلي عبر Python.
- تحليل البنية التحتية للنطاقات والأجهزة المتصلة بالإنترنت عبر أدوات Shodang Censys وإطار OWASP Amass.
- تقييم بيانات تسريبات الاعتماد وسجلات الدليل التجاري وتتبع ملكية الكيانات المشبوهة.
- بناء ملف استخباراتي متكامل وتوثيق سلاسل حيازة الأدلة الرقمية عبر Hunchly ورسوم Obsidian البيانية.

جدول الدورة

اليوم 1: منهجية استخبارات المصادر المفتوحة والأمان التشغيلي

- أسس دورة الاستخبارات وأطر تخطيط عمليات الجمع المعلوماتي
- عزل الأجهزة الافتراضية وتمويه البصمة الرقمية للأجهزة والمعدات
- إنشاء وإدارة الشخصيات الوهمية الافتراضية وحسابات التحري التكتيكية
- تقييم الامتثال لنظام حماية البيانات الشخصية SDAIA PDPL لجمع البيانات العلنية
- تحليل حدود جمع المعلومات وفق نظام مكافحة جرائم المعلوماتية بالمرسوم الملكي م/17

اليوم 2: مسارات البحث واستخراج البيانات وحفظ الأدلة الرقمية

- مشغلات البحث المتقدم على الويب واستغلال فهارس التخزين المؤقت
- نصوص الكشط الآلي للويب بالاعتماد على برمجيات استخراج البيانات بلغة Python
- تجزئة الأدلة الرقمية وسلاسل الحيازة والتوثيق عبر منصة Hunchly
- الأرشفة اللامركزية والتاريخية عبر Archive Todayg WayBack Machine
- بناء الرسوم البيانية المعرفية للربط والتحليل الجنائي باستخدام Obsidian

اليوم 3: تعقب الأفراد والشبكات الاجتماعية وجمع بيانات الشبكة المظلمة

- استخراج استخبارات التواصل الاجتماعي عبر المنصات المتعددة للحسابات المستهدفة
- مسارات التحقق عبر البحث العكسي لأسماء المستخدمين ومعرفات الحسابات والصور
- تحليل مستودعات قواعد البيانات المسربة وبيانات الاعتماد المخترقة
- تصفح شبكة التوجيه البصلي Tor واستخراج بيانات الخدمات المخفية
- التعامل مع استخبارات الاختراقات وفق الضابط 2-13-3-5 من ضوابط NCA ECC

اليوم 4: البنية التحتية للشبكات وتحليل الكيانات والشركات

- سجلات نظام أسماء النطاقات DNS وتقنيات الإسناد عبر استعلامات Whois العكسية
- اكتشاف الأجهزة والأنظمة المتصلة بالإنترنت عبر محركات Censysg Shodan
- تخطيط مساحة الهجوم الخارجي للأصول الرقمية باستخدام إطار OWASP Amass
- تعداد السجلات التجارية والتحقق من المستفيد الحقيقي للشركات عبر الحدود
- إعداد إشعارات مشاركة التهديدات السيبرانية بموجب الضابط 2-13-3-4 من NCA ECC

اليوم 5: محاكاة سيناريوهات الفحص والتقييم الختامي للتحقيق

- تمرين تطبيقي: تفعيل مسارات الجمع المعزولة وإدارة الشخصيات الوهمية
- تمرين تطبيقي: إسناد الكيانات عبر منصات التواصل وتوثيق الأدلة الرقمية
- تمرين تطبيقي: رسم خرائط انكشاف البنية التحتية وتقييم مخاطر الجهات الخارجية
- تمرين تطبيقي: محاكاة موقوتة لأسئلة تقييم GOSI الموضوعية المتضمنة 75 سؤالا
- المهمة الختامية: إسناد التهديدات وبناء ملف استخباراتي متوافق ومكتمل الأركان

التمارين التطبيقية

تعتمد الدورة مجموعة من الأنشطة المعملية المركزة على سيناريوهات استخباراتية وبيئات افتراضية تطبيقية محاكية للواقع العملي:

- نشاط مقترح: عزل بيئة التحقيق الرقمي وتجهيز الهويات المصطنعة لعمليات الرصد العلني الآمن.
- نشاط مقترح: تتبع مسار تسريب البيانات واستخراج الأدلة الرقمية وتثبيت تجزئتها عبر Hunchly.
- نشاط مقترح: مسح الأصول الرقمية الخارجية وتحليل النطاقات باستخدام OWASP Amassg Censys.
- المهمة الختامية: تنفيذ تحقيق متكامل لإسناد تهديد خارجي وإعداد تقرير استخباراتي نهائي موثق ومطابق لمعايير الامتثال.

الأسئلة الشائعة

من تناسب دورة التحضير لاختبار استخبارات المصادر المفتوحة GIAC GOSI وما متطلباتها؟

تناسب محللي استخبارات التهديدات، وممارسي الاستجابة للحوادث، ومختصي اختبار الاختراق، والمدققين الجنائيين؛ وتتطلب إلماما بأساسيات الشبكات وأنظمة التشغيل.

AGILE LEADERS
Training Center

كيف تختلف هذه الدورة عن دورات تحليل الاستخبارات العامة؟

تركز دورة التحضير لاختبار استخبارات المصادر المفتوحة GIAC GOSI على التقنيات الرقمية المتخصصة كالكشط الآلي وفحص البنية التحتية وعزل بيئات التحقيق، بخلاف البرامج العامة النظرية.

ما المواد التي يمكن الاستعانة بها أثناء محاولة اختبار GOSI؟

يسمح في اختبار GOSI باستخدام المواد المطبوعة والملاحظات والفهارس الشخصية المجهزة مسبقا، بينما تحظر الأجهزة الإلكترونية ومصادر الإنترنت الخارجية تماما.

كيف تعالج الدورة قوانين خصوصية البيانات المحلية أثناء جمع المصادر المفتوحة؟

توضح الدورة ضوابط الامتثال لنظام حماية البيانات الشخصية والأطر التنظيمية ذات الصلة، لضمان قانونية جمع وتحليل البيانات العلنية دون انتهاك الخصوصية.

ما الأدوات التقنية المطبقة في وحدات التحقيق الجنائي الرقمي؟

تشمل التدريبات أدوات متعددة مثل Python للكشط، Hunchly لحفظ الأدلة، ومحركات Shodang Censys لفحص الأصول، وإطار OWASP Amass، وبرمجية Obsidian للربط التحليلي.

الخاتمة

يغادر المشاركون الدورة بحقيبة توثيق متكاملة تشمل ملفات التحقيق، وفهارس الاستدعاء التقني، وسجلات الحيازة الرقمية المحققة. تدعم هذه المخرجات فرق العمل في رفع كفاءة التحريات السيبرانية وربط التهديدات الخارجية بمؤشرات قابلة للتنفيذ السريع. تسهم التطبيقات المكتسبة في تعزيز الجاهزية الدفاعية ودعم الامتثال القانوني للتحقيقات الرقمية داخل المؤسسات.