



**دورة التحقيق الجنائي الرقمي والاستجابة للحوادث
DFIR لفرق مراكز العمليات الأمنية SOC و CSIRT**



دورة التحقيق الجنائي الرقمي والاستجابة للحوادث DFIR لفرق مراكز العمليات الأمنية SOC وCSIRT

دورة التحقيق الجنائي الرقمي والاستجابة للحوادث DFIR لفرق SOC وCSIRT دورة تدريبية مدتها 5 أيام لمحللي مركز العمليات الأمنية وأعضاء فرق الاستجابة للحوادث. تتدرب فيها على فرز التنبيهات، وجمع البيانات المتطايمة من الأجهزة المخترقة، وتتبع تحرك المهاجم داخل الشبكة، ثم احتواء الحادثة دون فقد ما يكشف ما جرى. وتعود بدليل تشغيل الاستجابة للحوادث لفريقك. وتقدم هذه الدورة من ميركوري للتدريب.

نبذة عن الدورة

تستقبل فرق المراقبة آلاف التنبيهات، وحين يقع اختراق حقيقي تسارع إلى إعادة تشغيل الأجهزة فتضيع آثار المهاجم. لمتابعة الدورة يجب أن تعمل في مراقبة الأمن أو الاستجابة للحوادث وأن تقرأ سجلات الأنظمة. وتتدرب في مختبر على اختراق محاكي من أول تنبيه حتى تقرير الحادثة.

لمن هذه الدورة

- المسؤولون عن مراقبة التنبيهات الأمنية وفرزها وتصعيدها في مركز العمليات الأمنية
- المسؤولون عن قيادة الاستجابة للحوادث السيبرانية وتنسيق فريقها
- المسؤولون عن إدارة أنظمة الخوادم ونقاط النهاية والمشاركة في احتواء الاختراق
- المسؤولون عن البحث الاستباقي عن التهديدات وتحليل البرمجيات الخبيثة
- المسؤولون عن إدارة مخاطر الأمن السيبراني وإعداد تقارير الحوادث للإدارة

لا تناسب هذه الدورة المحققين الذين يعدون الأدلة الرقمية للقضايا أمام الجهات القضائية، فالأنسب لهم دورة في التحقيق الجنائي القانوني، ولا المبتدئين في الأمن السيبراني، فالأنسب لهم دورة تأسيسية في أساسيات أمن المعلومات.

الكفاءات المستهدفة

- فرز التنبيهات: تميز الحادثة الحقيقية من الإنذار الكاذب وتحدد درجة خطورتها بسرعة
- جمع البيانات المتطايمة: تلتقط الذاكرة والعمليات الجارية قبل أي إجراء يغير حالة الجهاز
- تحليل آثار النظام: تقرأ سجلات الأحداث وآثار التشغيل لتحديد ما نفذ المهاجم ومتى
- تتبع الحركة الجانبية: تربط الحسابات المخترقة وآليات البقاء بمسار المهاجم عبر الشبكة
- الاحتواء المدروس: تعزل الأنظمة المصابة دون إتلاف الآثار التي يحتاجها التحقيق
- تقرير الحادثة: تكتب الخط الزمني والأثر والدروس المستفادة بلغة تفهمها الإدارة

ما ستتمكن من إنجازه

بنهاية الدورة ستتمكن من:

- باستخدام دورة حياة الاستجابة في 3 Rev. NIST SP 800-61 توصيات الاستجابة للحوادث، ربط أدوار فريقك بمراحل الاستجابة وتحديد الفجوات
- انطلاقاً من مجموعة تنبيهات، فرزها بمعايير خطورة مكتوبة وقرار التصعيد من عدمه
- بالنظر إلى جهاز مشتببه به، التقاط الذاكرة والبيانات المتطيرة بترتيب صحيح وتوثيق كل خطوة
- انطلاقاً من سجلات الأحداث وآثار التشغيل، بناء خط زمني يبين الدخول الأول والتحرك الجانبي وآليات البقاء
- بالنظر إلى نطاق الاختراق، اختيار خيار الاحتواء وخطوات الإزالة والتعافي مع حفظ الآثار
- باستخدام نموذج تقرير الحادثة، كتابة ملخص للإدارة وتقرير فني مع توصيات التحسين

محتوى الدورة

اليوم 1: الاستعداد والفرز

- دورة حياة الاستجابة وفق 3 Rev. NIST SP 800-61 ووظائف CSF 2.0 الست
- أدوار مركز العمليات الأمنية وفريق الاستجابة ومسارات التصعيد
- معايير تصنيف خطورة الحوادث وأولوياتها
- فرز تنبيهات نظام إدارة الأحداث الأمنية واستبعاد الإنذارات الكاذبة
- جاهزية الفريق من أدوات وصلاحيات وقوائم اتصال

اليوم 2: الجمع الجنائي من الأجهزة

- ترتيب جمع البيانات حسب درجة تطايرها
- التقاط الذاكرة وتحليل العمليات والاتصالات الجارية
- الجمع عن بعد من نقاط النهاية في الشبكات المؤسسية
- توثيق سلسلة حفظ الآثار والتجزئة الرقمية
- الموازنة بين سرعة الاحتواء وحفظ الآثار

اليوم 3: تحليل آثار الاختراق

- آثار التشغيل في أنظمة ويندوز وما تكشفه عن المهاجم
- تحليل سجلات الأحداث وعمليات الدخول المشبوهة
- كشف الحسابات المخترقة وإساءة استخدام الصلاحيات
- تتبع الحركة الجانبية بين الخوادم
- البحث عن آليات البقاء والشفرة الخبيثة

اليوم 4: الاحتواء والتعافي والتقرير

- خيارات الاحتواء قصير المدى وطويل المدى
- الإزالة والتعافي والتحقق من خلو الأنظمة
- بناء الخط الزمني الموحد للحادثة
- كتابة تقرير الحادثة الفني والملخص التنفيذي
- مراجعة ما بعد الحادثة وتحديث قواعد الرصد

اليوم 5: التطبيق العملي على اختراق محاكي

- تمرين فرز تنبيهات الاختراق المحاكى وتصعيدها
- تمرين جمع الذاكرة وتحليل آثار جهازين مصابين
- تمرين تتبع مسار المهاجم وبناء الخط الزمني
- محاكاة اجتماع قرار الاحتواء مع الإدارة
- استكمال دليل تشغيل الاستجابة للحوادث

دراسات الحالة والتمارين

فيما يلي أنشطة مقترحة خلال الدورة.

- دراسة حالة: مصرف يرصد دخولا مشبوها بحساب مسؤول نظام خارج الدوام، فتفرز التنبيه وتقرر التصعيد ونطاق الجمع.
- دراسة حالة: شركة طاقة تجد برمجية فدية على خادم ملفات، فتختار بين العزل الفوري والمراقبة المؤقتة وتبرر القرار.
- تمرين: مستشفى اخترق فيه حساب بريد إلكتروني، فتبني الخط الزمني من سجلات الدخول وتحدد البيانات المكشوفة.
- تمرين: جهة حكومية تنهي حادثة، فتكتب الملخص التنفيذي وتوصيات تحديث قواعد الرصد.

ما ستعود به إلى عملك

تعود بدليل تشغيل الاستجابة للحوادث، مبني على أدوات فريقك وبيئتك. وتستخدمه خلال شهرك الأول للعودة إلى العمل لاعتماد معايير الفرز والتصعيد، وتجهيز أدوات الجمع، وتنفيذ تمرين مكتبي مع فريقك على حادثة محاكاة.

- معايير الفرز والتصنيف ومصفوفة التصعيد
- إجراءات جمع البيانات المتطيرة والآثار
- خيارات الاحتواء وشروط استخدام كل منها
- نموذج تقرير الحادثة ومراجعة ما بعد الحادثة

إجابات سريعة عن الأسئلة الشائعة

ما الذي أحتاج إلى معرفته قبل دورة التحقيق الجنائي الرقمي والاستجابة للحوادث DFIR؟

يجب أن تعمل في مراقبة الأمن أو الاستجابة للحوادث، وأن تعرف أساسيات الشبكات وأنظمة ويندوز وقراءة السجلات. والتمارين عملية في مختبر، لذلك تساعدك المعرفة بسطر الأوامر.

بم تختلف دورة DFIR لفرق SOC وCSIRT عن دورات التحقيق الجنائي القانوني؟

تخدم دورات التحقيق القانوني من يعدون الأدلة للقضايا. أما هذه الدورة فتخدم فرق الأمن داخل المؤسسة، وتركز على اكتشاف المهاجم وتتبع حركته واحتواء الاختراق وإعادة الأنظمة للعمل بسرعة.

ما الذي تغير في NIST SP 800-61 Rev. 3 لفرق الاستجابة للحوادث؟

يربط الإصدار الثالث الاستجابة للحوادث بإدارة مخاطر الأمن السيبراني كلها، ويوزعها على وظائف CSF 2.0 الست: الحوكمة والتحديد والحماية والرصد والاستجابة والتعافي، بدل التعامل معها نشاطا منفصلا.

ماذا أعود به من دورة التحقيق الجنائي الرقمي والاستجابة للحوادث DFIR؟

تعود بدليل تشغيل الاستجابة للحوادث، ويشمل معايير الفرز والتصعيد وإجراءات جمع البيانات المتطيرة وخيارات الاحتواء ونموذج تقرير الحادثة.

لمديرك

بعد الدورة سيتمكن الموظف من فرز التنبيهات بمعايير واضحة، وجمع آثار الاختراق قبل ضياعها، وتتبع مسار المهاجم، واحتواء الحادثة وكتابة تقريرها. ويعود بدليل تشغيل الاستجابة للحوادث، ويستخدمه أولاً لاعتماد معايير التصعيد وتنفيذ تمرين مكتبي مع الفريق.