



دورة التحقق المصرح به من مسارات هجمات الهوية



AGILE LEADERS
Training Center



دورة التحقق المصريح به من مسارات هجمات الهوية

نظرة عامة

دورة التحقق المصريح به من مسارات هجمات الهوية هي دورة مدتها أسبوع لممارسي الفريق الأحمر واختبار الاختراق وهندسة أمن الهوية ومحاكاة التهديدات والدفاع، ويعود المشاركون بحزمة التحقق من مسارات هجمات الهوية. تربط الدورة التحقق من مسارات هجمات الهوية ومحاكاة الخصم المصريح بها ومخاطر الهوية الهجينة وتحليل علاقات الصلاحيات ومراجعة الفريق البنفسجي داخل بيئات اختبار منضبطة. تحول الدورة نتائج الهوية المنفصلة إلى أدلة وقرارات معالجة ضمن نطاق واضح. تقدم أجائل للتدريب الدورة في التحقق المصريح به من مسارات هجمات الهوية.

الفئة المستهدفة

- الوظائف المسؤولة عن اختبارات الفريق الأحمر واختبارات الاختراق المصريح بها
- الفرق المسؤولة عن بنية الهوية المؤسسية وإدارة التعرض
- الوظائف المسؤولة عن محاكاة التهديدات والتحقق من الضوابط
- الفرق المسؤولة عن هندسة كشف هجمات الهوية والاستعداد للحوادث
- الوظائف المسؤولة عن ضمان المعالجة في البيئات الهجينة

تفترض الدورة أن المشاركين يمارسون اختبارات أمنية مصريح بها أو هندسة الهوية، ولا تتناول أهدافا خارجية حية أو تطوير البرمجيات الضارة أو الإجراءات التخريبية أو جمع بيانات اعتماد حقيقية أو التهرب غير المنضبط.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تتحقق من مخاطر الهوية ضمن تقييمات أمنية محكومة.

- فرق اختبار الأمن وهندسة الأمن السيبراني
- وظائف إدارة الهوية والوصول وخدمات الدليل
- عمليات البنية التقنية في الخدمات المالية والتقنية
- فرق ضمان الأمن في الرعاية الصحية والطاقة
- وظائف الأمن المدارة وإدارة مخاطر المؤسسات



أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق قواعد الاشتباك على اختبارات الهوية
- بناء نماذج علاقات الهوية ومسارات الهجوم
- تحليل مخاطر بيانات الاعتماد والرموز والصلاحيات بأمان
- مقارنة مسارات الدليل والسحابة والهوية الهجينة
- تقييم أدلة الكشف مقابل السلوكيات المحاكاة
- ترتيب أولويات المعالجة والتحقق من تغييرات الضوابط

جدول الدورة

اليوم 1: التفويض ونمذجة تهديدات الهوية

- مصفوفة قواعد الاشتباك والنطاق وفق NIST SP 800-115
- قائمة حدود اختبار الهوية وضوابط الحماية
- لوحة ربط تقنيات الهوية وفق MITRE ATT&CK
- سجل الهويات الحرجة والأصول الحساسة
- سجل افتراضات محاكاة الخصم وشروط الإيقاف

اليوم 2: رسم علاقات الهوية ومخاطر التعرض

- رسم حسابات الدليل والمجموعات وعلاقات الثقة
- خريطة صلاحيات حسابات الخدمة والهويات المدارة
- مصفوفة أدلة تعرض بيانات الاعتماد والرموز
- نموذج سيناريو بروتوكول Kerberos والمصادقة
- مسار انتقال الهوية الهجينة إلى الأصول الحساسة



اليوم 3: محاكاة هجمات الهوية المنضبطة

- بطاقة محاكاة الحسابات الصالحة وفق T1078
- ورقة ضبط سيناريو تذاكر Kerberos وفق T1558
- مصفوفة محاكاة تعديل الحسابات وفق T1098
- خطة الحركة الجانبية والتصعيد داخل المختبر
- سجل محاكاة الاستمرارية والاتصال المقيّد

اليوم 4: الكشف والأدلة والتحقق من المعالجة

- مصفوفة بيانات الهوية وتغطية الكشف
- سجل ربط التنبيهات والخط الزمني للمحاكاة
- منحج شدة النتيجة وتأثير مسار الهجوم
- خطة ملكية المعالجة وخفض التعرض
- قائمة أدلة إعادة الاختبار والتحقق من الضوابط

اليوم 5: ممارسة التحقق من مسارات الهوية

- تمرين تحديد نطاق اختبار الهوية وشروط الإيقاف
- تمرين بناء رسم لمسار هجوم في هوية هجينة
- تمرين تقييم أدلة الكشف للسلوكيات المربوطة
- تمرين ترتيب المعالجة وتصميم إعادة اختبار أمانة
- المهمة الختامية لحزمة التحقق من مسارات هجمات الهوية

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة في مختبرات معزولة مبنية على قطاعات الخدمات المالية والرعاية الصحية والتقنية والطاقة.

- نشاط مقترح: تحويل التفويض المكتوب إلى نطاق وضوابط حماية وجهات اتصال واستثناءات وشروط إيقاف.
- نشاط مقترح: رسم الصلاحيات وعلاقات الثقة من بيانات هوية هجينة افتراضية.
- نشاط مقترح: مقارنة سلوكيات الهوية المحاكية مع بيانات القياس وأدلة الكشف المتوقعة.
- نشاط مقترح: تحويل مسار متحقق منه إلى ملاك معالجة وتغييرات ضوابط ومعايير إعادة اختبار.



الأسئلة الشائعة

لمن تناسب دورة التحقق من مسارات هجمات الهوية وماذا تفترض؟

تناسب دورة التحقق من مسارات هجمات الهوية ممارسي الاختبارات الأمنية المصريح بها والمدافعين عن الهوية، وتفترض خبرة في المصادقة المؤسسية وخدمات الدليل والتقييمات الأمنية والمختبرات المنضبطة.

كيف تختلف دورة التحقق من مسارات هجمات الهوية عن اختبار الاختراق العام؟

تركز دورة التحقق من مسارات هجمات الهوية على الحسابات والصلاحيات والثقة والمصادقة والهوية الهجينة وأدلة الكشف والمعالجة، بينما يغطي اختبار الاختراق العام مخاطر أوسع في الشبكات والأنظمة والتطبيقات.

لماذا تستخدم مسارات هجمات الهوية رسوما للعلاقات؟

توضح رسوم العلاقات كيف تتصل الصلاحيات والعضويات والأدوار وهويات الخدمة وعلاقات الثقة لتكوين مسارات من هوية معرضة إلى أصل حساس.

كيف تدعم مراجعة الفريق البنفسجي التحقق من مسارات هجمات الهوية؟

تربط مراجعة الفريق البنفسجي المحاكاة المنضبطة ببيانات القياس وفجوات الكشف والقرارات الدفاعية وملكية المعالجة وإعادة الاختبار المبنية على الأدلة.

الخاتمة

يعود المشاركون إلى العمل بحزمة التحقق من مسارات هجمات الهوية. تجمع الحزمة قواعد الاشتباك ورسوم الهوية والسلوكيات المربوطة وضوابط الحماية وسجلات الأدلة وتغطية الكشف وقرارات المعالجة ومعايير إعادة الاختبار. تحول الحزمة نتائج الهوية المتفرقة إلى دورة تحقق محكومة تدعم خفض التعرض من دون نشاط هجومي غير منضبط.



فئات الدورات التدريبية

الدورات التدريبية في مجال البيئة والاستدامة	الأعمال الزراعية والأمن الغذائي
دورات إدارة الجودة وتطوير العمليات	دورات إدارة الأزمات واستمرارية الأعمال
دورات إدارة المرافق والعقارات	دورات إدارة الرعاية الصحية
دورات إدارة و تحليل البيانات ودورات علم البيانات	دورات إدارة المنظمات غير الحكومية والعمل الإنساني والتنمية
دورات إدارة وعمليات الطيران	دورات إدارة و تطوير الموارد البشرية
دورات الاتصال الجماهيري و السياسات والعلاقات العامة	دورات الأمن السيبراني ودورات تقنية المعلومات
دورات التسويق وإدارة علاقات العملاء وإدارة المبيعات	دورات التدريب القانوني والمشتريات والتعاقدات
دورات الحكومة الرقمية والخدمات العامة	دورات التعليم وتطوير التعلم
دورات السكرتارية و إدارة المكاتب	دورات الحوكمة وإدارة المخاطر والامتثال
دورات الصحة والسلامة والأمن المهني	دورات الشحن والملاحة البحرية والموانئ
دورات الضيافة والسياحة	دورات الصيانة ودورات المجالات الهندسية المتنوعة
دورات المهارات الشخصية وتطوير الذات	دورات المحاسبة و التمويل و دورات الإدارة المالية
دورات في مجالات القيادة والإدارة	دورات حفظ التراث وإدارة المتاحف



فئات الدورات التدريبية

دورات معتمدة من قبل هيئات دولية

دورات قطاع النفط والغاز ودورات تقنية متنوعة

دورات مكتب إدارة المشاريع وإدارة المشاريع الرشيقة



مدن التدريب

أديس أبابا إثيوبيا	أثينا اليونان	أبوظبي الإمارات العربية المتحدة
اسطنبول تركيا	أمستردام هولندا	أكرا غانا
القاهرة مصر	الدوحة قطر	الدار البيضاء المغرب
باريس فرنسا	المنامة مملكة البحرين	الكويت الكويت
بانكوك تايلاند	بالي جمهورية إندونيسيا	باكو أذربيجان
برلين ألمانيا	برشلونة إسبانيا	براغ جمهورية التشيك
بوكيت تايلاند	بورتلو البرتغال	بورت لويس موريشيوس
جاكرتا جمهورية إندونيسيا	تورنتو كندا	تبليسي جورجيا
دبي الإمارات العربية المتحدة	جوهانسبرغ جنوب إفريقيا	جنيف سويسرا
زيورخ سويسرا	زنجانر تنزانيا	روما إيطاليا
سيول كوريا الجنوبية	سنغافورة سنغافورة	سان دييغو الولايات المتحدة الأمريكية
طرابزون تركيا	شيكاغو الولايات المتحدة الأمريكية	شرم الشيخ مصر



مدن التدريب

عمان المملكة الأردنية الهاشمية	طوكيو اليابان	طشقند أوزبكستان
فيينا النمسا	فرانكفورت ألمانيا	عن بعد منصة زووم
لاغوس نيجيريا	كيب تاون جنوب إفريقيا	كوالالمبور ماليزيا
لندن المملكة المتحدة	لشبونة البرتغال	لانكاوي ماليزيا
مسقط سلطنة عمان	مدريد إسبانيا	ماريبا إسبانيا
ميونخ ألمانيا	ميلان إيطاليا	مونترو سويسرا
نيويورك الولايات المتحدة الأمريكية	نيس فرنسا	نيروبي كينيا