



دورة إدارة الثغرات الأمنية وإدارة سطح الهجوم: بناء برنامج مؤسسي لمعالجة الثغرات



دورة إدارة الثغرات الأمنية وإدارة سطح الهجوم: بناء برنامج مؤسسي لمعالجة الثغرات

مقدمة:

دورة إدارة الثغرات الأمنية وإدارة سطح الهجوم دورة تمتد 5 أيام لفرق عمليات الأمن والبنية التحتية وإدارة التحديثات الأمنية، وتنتهي بإعداد خطة برنامج إدارة الثغرات لمؤسسة دراسة حالة. فكثير من المؤسسات تتراكم لديها نتائج فحص مفتوحة بأعداد كبيرة، وتغيب عنها أصول مكشوفة على الإنترنت لم يسجلها أحد، وتعالج الثغرات وفق درجة الخطورة وحدها، فتبقى ثغرات مستغلة فعلياً مفتوحة لأشهر، ويتولى المرشحون في عملهم تشغيل الفحص أو إدارة الخوادم أو جدولة دورات التحديث، ويتدربون في مختبر عملي على بيانات فحص وسجل أصول وبيانات EPSS وأداة لتتبع المعالجة. وتقدم كور كونسبت هذه الدورة بوصفها تمريناً عملياً لبناء برنامج مؤسسي متكامل.

أهداف الدورة:

- تحديد نطاق برنامج إدارة الثغرات وملكيته وحوكمته عبر ميثاق للبرنامج ومصفوفة RACI لتوزيع المسؤوليات
- مطابقة سجلات الأصول ورسم سطح الهجوم الخارجي بحيث يصل الفحص إلى كل نظام داخلي أو مكشوف على الإنترنت
- تصميم تغطية الفحص الموثق ببيانات الاعتماد عبر الوكلاء البرمجيين ومساحات الشبكة وواجهات الحوسبة السحابية
- ترتيب أولويات النتائج بدمج درجات CVSS واحتمالات EPSS وبيانات فهرس KEV مع مستويات أهمية الأصول
- وضع مستويات اتفاقيات الخدمة للمعالجة وموافقات الاستثناء وتنسيق التحديثات وفق ممارسات التخطيط في 40-800 NIST SP
- رفع مؤشرات التعرض إلى القيادة وإعداد خطة برنامج إدارة الثغرات لمؤسسة دراسة حالة

الفئة المستهدفة:

- موظفو عمليات الأمن المسؤولون عن تشغيل فحص الثغرات وفرز نتائجه
- فرق البنية التحتية والخوادم المسؤولة عن تثبيت التحديثات الأمنية وتصحيح الإعدادات
- منسقي التحديثات والإصدارات المسؤولون عن نوافذ الصيانة وموافقات التغيير
- مهندسو الحوسبة السحابية والشبكات المسؤولون عن الخدمات المكشوفة على الإنترنت ودرجة تعرضها
- موظفو مخاطر تقنية المعلومات والحوكمة المسؤولون عن مستويات الخدمة للمعالجة والاستثناءات والتقارير

محاوِر الدورة:

اليوم 1: أسس برنامج إدارة الثغرات ومراجعة الوضع الراهن

- دورة حياة إدارة الثغرات من الاكتشاف حتى التحقق من المعالجة
- سجلات CVE وCWE وNVD مصادر بيانات للبرنامج
- ميثاق البرنامج ونطاقه ونموذج ملكية الأصول
- مصفوفة RACI لفرق الأمن وعمليات التقنية ومالكي الأنظمة
- تقييم نضج ممارسات الفحص والتحديث في الوضع الراهن

اليوم 2: اكتشاف الأصول ورسم سطح الهجوم وبنية الفحص

- مطابقة سجل الأصول بين قاعدة CMDB والسحابة وخدمات الدليل
- رسم سطح الهجوم الخارجي للنطاقات والشهادات ونطاقات عناوين IP
- الفحص الموثق مقابل غير الموثق وإدارة بيانات الاعتماد
- تصميم مواقع الماسحات بالوكلاء والشبكة وواجهات API السحابية
- قوائم SBOM وبيانات تركيب البرمجيات للمكونات الخارجية

اليوم 3: ترتيب الأولويات وفق المخاطر ومسار المعالجة

- درجات CVSS الأساسية مقابل سياق البيئة والتهديد
- احتمالات الاستغلال في EPSS لترتيب أولويات المعالجة
- تطابق فهرس KEV محفزاً للمعالجة العاجلة
- مستويات أهمية الأصول ونموذج ترجيح سياق الأعمال
- توجيه تذاكر المعالجة إلى الفرق المالكة عبر إدارة الخدمات

اليوم 4: تنسيق التحديثات والاستثناءات والإدارة المستمرة للتعرض

- ممارسات تخطيط إدارة التحديثات المؤسسية وفق NIST SP 800-40
- حلقات التحديث ونوافذ الصيانة وخطط التراجع
- مستويات اتفاقيات الخدمة للمعالجة ومسار اعتماد استثناءات المخاطر
- الضوابط التعويضية للأنظمة القديمة وغير القابلة للتحديث
- مراحل CTEM من تحديد النطاق والاكتشاف إلى التحقق والتعبئة

اليوم 5: عمل مختبري على دراسة حالة وخطة برنامج إدارة الثغرات

- بناء سجل الأصول والتعرض الخارجي لمؤسسة الحالة في المختبر
- قائمة معالجة مرتبة بالأولوية لمؤسسة الحالة باستخدام CVSS و EPSS و KEV
- صياغة سجل مستويات الخدمة والاستثناءات لمؤسسة الحالة
- لوحة مؤشرات التعرض ومتوسط مدة المعالجة
- استكمال خطة برنامج إدارة الثغرات ومراجعتها بين المشاركين

المهارات التي ستكتسبها:

- مطابقة سجلات الأصول
- رسم سطح الهجوم الخارجي
- تصميم الفحص الموثق
- الترتيب وفق احتمال الاستغلال
- حوكمة مستويات خدمة المعالجة
- تخطيط حلقات التحديث
- معالجة استثناءات المخاطر
- إعداد تقارير مؤشرات التعرض

لماذا تحضر هذه الدورة:

- تسليم خطة برنامج إدارة الثغرات إلى رئيس أمن المعلومات ورئيس عمليات تقنية المعلومات متضمنة النطاق ومستويات الخدمة والمؤشرات
- تحديد النتائج التي تعالج عاجلاً وتلك التي تجدر في حلقة التحديث التالية وتلك التي تقبل ضمن استثناء موثق
- تجنب الاختراقات الناتجة عن ثغرات مستغلة تبقى مفتوحة على أصول مكشوفة غير مسجلة
- إرشاد فرق البنية التحتية والتطبيقات إلى قراءة قوائم الأولوية والوفاء بمستويات خدمة المعالجة

الخاتمة:

بعد العودة إلى العمل يعرض المشاركون خطة برنامج إدارة الثغرات على رئيس أمن المعلومات ورئيس عمليات تقنية المعلومات، فيعتمدان بها نطاق الفحص ومستويات اتفاقيات الخدمة للمعالجة وإجراءات الاستثناء قبل دورة التحديث التالية. ويتسلم مالكو الأصول بعدها قوائم معالجة مرتبة بالأولوية بدلاً من مخرجات الماسحات الخام. وبعد أول دورة تقارير شهرية، تراجع الوحدة متوسط مدة المعالجة وتغطية الفحص والاستثناءات المفتوحة مقارنة بالخطة، وتعديل أي عتبة أنتجت حالات معالجة عاجلة تفوق الطاقة المتاحة أو تقل عن الحاجة الفعلية.

الأسئلة الشائعة:

ما الذي يحتاجه المشارك قبل دورة إدارة الثغرات الأمنية وإدارة سطح الهجوم؟

يحتاج المشارك إلى فهم الشبكات وأنظمة التشغيل وطريقة نشر التحديثات في مؤسسته، وتفيد الخبرة في تشغيل الماسحات أو متابعة تذاكر المعالجة، ولا تتطلب الدورة البرمجة، إذ يراجع اليوم الأول سجلات CVE وCWE وNVD قبل تصميم البرنامج.

بم تختلف دورة إدارة الثغرات الأمنية وإدارة سطح الهجوم عن دورة اختبار الاختراق؟

تبنى هذه الدورة عملية مستمرة لاكتشاف الأصول وفحصها وترتيب أولوياتها وتحديثها على مستوى البيئة التقنية كلها. أما اختبار الاختراق فهو ممرح به محدود المدة والنطاق يثبت إمكانية استغلال الثغرات ثم يرفع نتائجه في تقرير.

لماذا يجمع برنامج إدارة الثغرات الأمنية بين EPSS وفهرس KEV ودرجات CVSS؟

لأن CVSS يقيس الخطورة التقنية لا احتمال الهجوم، ويقدر EPSS احتمال استغلال الثغرة، ويسرد فهرس KEV الثغرات المستغلة فعلياً، ويتيح الجمع بينها للفرق معالجة النتائج الأهم أولاً.

ماذا يعود به المشارك من دورة إدارة الثغرات الأمنية وإدارة سطح الهجوم؟

يعود المشارك بخطة برنامج إدارة الثغرات تضم سجل الأصول والتعرض الخارجي ونموذج ترتيب الأولويات ومستويات خدمة المعالجة مع سجل الاستثناءات وجدول حلقات التحديث ومجموعة مؤشرات للقيادة، جاهزة لمراجعة قادة الأمن وعمليات التقنية.