JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في تقييم الثغرات وتحصين الأنظمة

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في تقييم الثغرات وتحصين الأنظمة

تقييم الثغرات وتحصين الأنظمة دورة تدريبية متقدمة مدتها أسبوعين لمهندسي الأمن ومسؤولي الشبكات والأخصائيين التقنيين الذين يكتشفون نقاط الضعف في الخوادم والأجهزة الطرفية والشبكات ويغلقونها، وتنتهي بتقرير تقييم أمني تقني لبيئة مختبرية. فالمهاجمون يحولون الثغرات المنشورة حديثا إلى أدوات هجوم خلال أيام، لذا تحدد المسافة بين الاكتشاف والإصلاح حجم الانكشاف. وتقدم جوبيتر برايم للتدريب هذه الدورة للأخصائيين المسؤولين عن تضييق تلك المسافة.

لماذا يهم تقييم الثغرات وتحصين الأنظمة الآن

تتشكل هذه المهام اليوم تحت ثلاثة ضغوط: حجم العيوب البرمجية المعلنة حديثا الذي يفوق أي نافذة تصحيح، وبيئات هجينة تنحرف فيها صور السحابة والحاويات والخوادم القديمة عن خط الأساس الآمن، ومدققون وشركات تأمين يطلبون دليلا على الفحص والإصلاح وضبط الإعدادات. الأخصائي الذي يرتب الأولويات حسب قابلية الاستغلال ويحصن خطوط الأساس يقلص سطح الهجوم باطراد، أما من يلاحق كل نتيجة فحص فيرهق فريقه ويفوت القلة الخطرة. وتوائم الدورة أساليبها مع وظيفتي التحديد والحماية في إطار NIST CSF 2.0 NIST Cybersecurity Framework 2.0 ومع توقعات الضوابط في ISO/IEC 27001:2022.

المستفيدون من تقييم الثغرات وتحصين الأنظمة

- مهندسو الأمن الذين يشغلون الفحص ويتحققون من النتائج ويتابعون الإصلاح في البيئة
- مسؤولو الشبكات الذين يحصنون الموجهات والمبدلات وجدران الحماية وبوابات الوصول عن بعد
- مسؤولو الأنظمة الذين يبنون خطوط أساس خوادم Windows وLinux ويحافظون عليها
- أخصائيو عمليات الأمن الذين يضبطون المراقبة لرصد محاولات الاستغلال
- المقيمون التقنيون الذين يعدون أدلة الاختبار للمدققين والعملاء

تجني مجموعة البنية التحتية الفائدة الكبرى حين توفد مهندسي الأمن ومسؤولي الأنظمة والشبكات معا، لأن التحصين لا يثبت إلا حين يتشارك من يكتشف الضعف ومن يصلحه منهجا واحدا.

قدرات تقييم الثغرات وتحصين الأنظمة

يغادر المشاركون قادرين على الانتقال من مخرجات الفحص الخام إلى بيئة مرتبة الأولويات ومتحقق منها ومحصنة.

- تقييم الثغرات حسب قابلية الاستغلال والانكشاف وأهمية الأصل — أولوية الإصلاح لدى مالكي الأنظمة
- تطبيق أساليب اختبار الاختراق ضمن قواعد اشتباك متفق عليها — إثبات مسارات الهجوم الحقيقية
- بناء خطوط أساس للإعداد الآمن للخوادم والأجهزة الطرفية وأجهزة الشبكة — قرارات مجلس التغيير
- اختبار التحصين عبر تدقيق الإعدادات وإعادة الفحص — أدلة للمدققين
- تحليل سلوك البرمجيات الخبيثة بمستوى أساسي لدعم الاحتواء — معالجو الحوادث
- تحديد حالات استخدام المراقبة التي ترصد محاولات الاستغلال — مركز عمليات الأمن

مصطلحات تقييم الثغرات وتحصين الأنظمة الأساسية

- الثغرة — ضعف في البرمجيات أو الإعدادات أو الإجراءات يمكن للمهاجم استغلاله للدخول أو الإضرار.
- سطح الهجوم — مجموع النقاط مثل المنافذ المفتوحة والخدمات والحسابات والواجهات التي قد يحاول المهاجم الدخول منها.
- خط الأساس الآمن — إعداد معتمد وموثق يجب أن يطابقه كل نظام من النوع نفسه قبل التغييرات وبعدها.
- قواعد الاشتباك — النطاق والتوقيت والأساليب والحدود المكتوبة المتفق عليها قبل بدء أي اختبار اختراق.
- الإيجابية الكاذبة — نتيجة فحص تشير إلى ضعف غير موجود فعلا أو غير قابل للاستغلال.
- انحراف الإعدادات — ابتعاد تدريجي لإعدادات النظام الحية عن خط الأساس الآمن المعتمد بمرور الوقت.

تقييم الثغرات وتحصين الأنظمة يوما بيوم

اليوم 1: مشهد الانكشاف

- الإفصاح عن الثغرات والجداول الزمنية للاستغلال — إلحاح الإصلاح
- رسم خريطة سطح الهجوم — الانكشاف الخارجي والداخلي
- وظيفتا التحديد والحماية في NIST CSF 2.0 — موقع التقييم
- تقنيات اكتشاف الأصول — الأجهزة المجهولة والخدمات الخفية
- التعريف بالبيئة المختبرية — نطاق تمرين التقييم

اليوم 2: الفحص والحصر

- اكتشاف الشبكة بأداة Nmap — بصمة المنافذ والخدمات
- الفحص المصادق مقابل غير المصادق — مقايضات العمق والدقة
- فحص تطبيقات الويب — نتائج الحقن وأخطاء الإعداد
- جدولة الفحص وضبط سرعته — تجنب تعطيل بيئة الإنتاج
- حصر المستخدمين والمجلدات المشتركة والخدمات — مؤشرات الحركة الجانبية

اليوم 3: التحقق من النتائج وترتيب أولوياتها

- تقييم الخطورة وإشارات قابلية الاستغلال — ترتيب الإصلاح
- أساليب التحقق من الإيجابيات الكاذبة — توجيه جهد المحلل إلى ما يستحق
- ترجيح أهمية الأصل — الأثر التشغيلي لكل ضعف
- مسار متابعة الثغرات — الملكية ومستويات الخدمة
- سجلات الاستثناء والضوابط التعويضية — الانكشاف المتبقي المقبول

اليوم 4: أساليب اختبار الاختراق

- قواعد الاشتباك وتحديد النطاق — الحدود القانونية والتشغيلية
- مراحل الاستطلاع والاستغلال — إثبات مسارات الهجوم الفعلية
- هجمات كلمات المرور وإعادة استخدام بيانات الاعتماد — أدلة ضعف الهوية
- تقنيات تصعيد الصلاحيات — الانكشاف المحلي وعلى مستوى النطاق
- التنظيف بعد الاستغلال — إعادة الأنظمة إلى حالتها

اليوم 5: تحصين خوادم Linuxg Windows

- تحصين نهج المجموعات في Windows — إعدادات الحسابات والتدقيق والخدمات
- تقليص خدمات Linux وإعداد SSH — تضييق سطح الهجوم
- ضوابط المسؤول المحلي وصلاحيات sudo — احتواء الامتيازات
- جدار الحماية المضيف وقوائم التطبيقات المسموحة — خيارات ضبط التشغيل
- توثيق خطوط الأساس والصور الذهبية — بناء متكرر ومتسق

اليوم 6: تحصين الشبكات والوصول عن بعد

- تحصين الموجهات والمبدلات — حماية مستوى الإدارة
- مراجعة قاعدة قواعد جدار الحماية — القواعد المكررة والمفرطة الاتساع
- تجزئة الشبكة وتصميم الشبكات الافتراضية VLAN — احتواء الاختراق
- إعداد الشبكات الخاصة الافتراضية وبوابات سطح المكتب البعيد — انكشاف الوصول عن بعد
- إعدادات أمن الشبكات اللاسلكية — المصادقة ونقاط الوصول الدخيلة

اليوم 7: الإعداد الآمن في السحابة والحاويات

- أخطاء إعداد الهوية والتخزين السحابي — مخاطر الانكشاف العلني
- فحص صور الحاويات — الحزم الضعيفة قبل النشر
- فحوص البنية التحتية كشيفرة — التقاط القوالب غير الآمنة مبكرا
- رصد انحراف الإعدادات — المقارنة الآلية بخط الأساس
- وتيرة إدارة التصحيحات — الموازنة بين التشغيل المستمر والانكشاف

اليوم 8: أساسيات البرمجيات الخبيثة للمدافعين

- عائلات البرمجيات الخبيثة وطرق إيصالها — نقاط الدخول المرجحة
- المؤشرات الثابتة وبصمات الملفات — فرز سريع للعينات
- مراقبة السلوك في بيئة معزولة — مؤشرات الشبكة والاستمرار
- ضبط حماية الأجهزة الطرفية — كشف دون ضجيج مفرط
- حالات برمجيات خبيثة في التصنيع والتجزئة — دروس قطاعية

اليوم 9: المراقبة الأمنية والتحقق

- مصادر السجلات لرصد الاستغلال — تغطية الأنظمة المحصنة
- تصميم حالات الاستخدام في SIEM — تنبيهات لأساليب الهجوم المعروفة
- ضبط كشف التسلل — الإشارة مقابل الضجيج
- إعادة الفحص وتدقيق الإعدادات — إثبات ثبات الإصلاحات
- مقاييس برامج معالجة الثغرات — زمن الإصلاح ونطاق التغطية

اليوم 10: ممارسة تقرير التقييم الأمني التقني

- جولة فحص وتحقق في المختبر — قائمة النتائج المؤكدة
- استغلال موجه للثغرات ذات الأولوية — إثبات الأثر
- تطبيق توصيات التحصين على أجهزة المختبر — أدلة قبل وبعد
- إحاطة تنفيذية وتقنية بالنتائج — طلبات واضحة للمالكين
- استكمال تقرير التقييم الأمني التقني — النتائج والإصلاحات وخطوات التحقق

تطبيق تقييم الثغرات وتحصين الأنظمة بعد الدورة

- تشغيل فحص مصادق لمجموعة خوادم حرجة واحدة والتحقق من أهم نتائجه بطريقة ترتيب الأولويات التي جرى التدرب عليها
- صياغة خط أساس آمن لنوع واحد من الخوادم ومقارنة الأنظمة الحية به لقياس انحراف الإعدادات

أسئلة حول تقييم الثغرات وتحصين الأنظمة

ما تقييم الثغرات وتحصين الأنظمة ولماذا يهم الآن؟

تقييم الثغرات وتحصين الأنظمة هو اكتشاف نقاط الضعف في الأنظمة والشبكات وإغلاقها بالإعداد الآمن. ويهم الآن لأن المهاجمين يستغلون العيوب الجديدة خلال أيام، وانحراف الإعدادات يعيد فتح أبواب أغلقت سابقا.

من يستفيد أكثر من دورة تقييم الثغرات وتحصين الأنظمة؟

يستفيد أكثر مهندسو الأمن ومسؤولو الأنظمة والشبكات وأخصائيو عمليات الأمن والمقيمون التقنيون. وتزداد فائدتك إن كنت تشغل الفحص أو تحافظ على خطوط الأساس أو تحتاج إلى إثبات اكتشاف الضعف وإصلاحه أمام المدققين.

كيف تختلف دورة تقييم الثغرات وتحصين الأنظمة عن دورة الاختراق الأخلاقي؟

توازن الدورة بين اكتشاف نقاط الضعف وإصلاحها والتحقق منها بدلا من التركيز على الأساليب الهجومية. وتقدم أساليب اختبار الاختراق للتحقق من النتائج، إلى جانب التحصين والإعداد الآمن ومراقبة الأنظمة التي تدافع عنها.

ماذا تعود به من دورة تقييم الثغرات وتحصين الأنظمة؟

تعود بتقرير تقييم مكتمل لبيئة مختبرية وبالمنهج اللازم لتكراره في عملك. ويغطي النتائج المؤكدة وترتيب الأولويات وخطوات التحصين وأدلة إعادة الاختبار التي تثبت ثبات كل إصلاح.

تقييم الثغرات وتحصين الأنظمة: الطريق إلى الأمام

يوجه تقرير التقييم الأمني التقني أولا اختيار نقاط الضعف التي يصلحها مالكو الأنظمة في دورة التصحيح التالية وخطوط الأساس التي تتغير. ويحدثه مهندسو الأمن، وينفذ المسؤولون خطوات التحصين فيه، ويعتمد المدققون على أدلة إعادة الاختبار. وبعد أول تقييم فعلي تستحق أوزان الأولوية مراجعة جديدة، إذ تكشف البيئات الحية غالبا أن أهمية الأصل تفوق درجة الخطورة المجردة.