JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في تصميم شبكات المؤسسات الآمنة والدفاع عنها

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في تصميم شبكات المؤسسات الآمنة والدفاع عنها

تصميم شبكات المؤسسات الآمنة والدفاع عنها دورة تدريبية متقدمة مدتها أسبوعين لفنيي الشبكات وممارسي الأمن المبتدئين المنتقلين من إبقاء الشبكة عاملة إلى إبقاء المهاجمين خارجها، وتنتهي بمخطط شبكة مؤسسية مجزأة يبنى في المختبر. فالشبكات المسطحة ما زالت تسمح لحاسوب محمول مصاب بالوصول إلى خوادم الرواتب ووحدات تحكم المصانع، لذا تحدد خيارات الطوبولوجيا مدى انتشار التسلل. وتقدم جوبيتر برايم للتدريب هذه الدورة للممارسين المتجهين إلى الدفاع الشبكي.

لماذا يهم تصميم شبكات المؤسسات الآمنة والدفاع عنها الآن

ثلاثة تحولات تعيد تشكيل دور ممارس الشبكات: اندماج حركة المكاتب والسحابة والتقنيات التشغيلية على بنية مشتركة، وتوسع الوصول عن بعد واللاسلكي الذي يذيب المحيط القديم، وفرق أمن تنتظر من كوادر الشبكات تزويدها ببيانات الرصد واحتواء الحوادث لا مجرد استعادة الاتصال. المنشآت ذات الشبكات المقسمة إلى مناطق مراقبة وموثقة تعزل العدوى خلال دقائق، أما ذات التصاميم المسطحة غير الموثقة فتواجه توقفات تمتد عبر المواقع. وتوائم الدورة خيارات التصميم والمراقبة مع وظيفتي الحماية والكشف في إطار NIST CSF 2.0 NIST Cybersecurity Framework 2.0.

المستفيدون من تصميم شبكات المؤسسات الآمنة والدفاع عنها

- فنيو الشبكات الذين يهيئون المبدلات والموجهات ووحدات التحكم اللاسلكية يوميا
- ممارسو الأمن المبتدئون الذين يحتاجون إلى فهم عملي لمسارات الحركة الفعلية
- كوادر دعم البنية التحتية الذين يتولون نقل المواقع والفروع الجديدة وتوسعات الحرم
- مشغلو مراكز عمليات الشبكة الذين يراقبون صحة الروابط ويطلب منهم اليوم رصد الحركة المريبة
- كوادر الأنظمة الذين يديرون خدمات الدليل وأسماء النطاقات وتوزيع العناوين التي تعتمد عليها الشبكة

يجني فريق عمليات الشبكة الفائدة الكبرى حين يوفد فنييه مع أحدث كوادر الأمن، لأن الطرفين يتعلمان قراءة المخططات والتنبيهات ذاتها.

قدرات تصميم شبكات المؤسسات الآمنة والدفاع عنها

يغادر المشاركون قادرين على رسم شبكة وبنائها ومراقبتها بحيث تبطئ بنيتها ذاتها حركة المهاجم.

- تصميم خطط العناوين ومناطق الثقة التي تفصل المستخدمين والخوادم والأنظمة الحرجة — معماريو الشبكات ومالكوها
- تطبيق ضوابط التوجيه والتبديل التي تمنع الانتحال والحلقات — عمليات الشبكة
- تحديد مواضع جدران الحماية وأنواع الشبكات الخاصة الافتراضية وسياسات الوصول بين المناطق — هندسة الأمن
- بناء ضبط الوصول اللاسلكي والقائم على المنافذ للموظفين والضيوف والأجهزة — المرافق ودعم التقنية
- اختبار تغطية كشف التسلل ومراقبة التدفقات عبر التصميم — مركز عمليات الأمن
- إيصال تصميم الشبكة ومواضع انكشافها المتبقية عبر مخططات واضحة — المديرون والمدققون

مصطلحات تصميم شبكات المؤسسات الآمنة والدفاع عنها الأساسية

- منطقة الثقة — مجموعة مقاطع شبكية تتشارك المستوى الأمني نفسه وتخضع الحركة بينها للضبط والفحص.
- الشبكة المحلية الافتراضية VLAN — تقسيم نسيج المبدلات المادي إلى نطاقات بث منفصلة لمجموعات مختلفة.
- ضبط الوصول إلى الشبكة — فحص الجهاز والمستخدم قبل السماح بالاتصال، غالبا بالمصادقة القائمة على المنافذ.
- المنطقة المنزوعة السلاح — مقطع عازل يضم الخدمات المواجهة للإنترنت ويفصلها عن الإنترنت والشبكة الداخلية معا.
- سجل التدفق — ملخص لمحادثة شبكية يذكر المصدر والوجهة والمنافذ والحجم ويستخدم للمراقبة والتحقيق.
- الحركة الأفقية الداخلية — الاتصال بين الأنظمة داخل الشبكة، حيث يتنقل المهاجمون بعد الاختراق الأول.

تصميم شبكات المؤسسات الآمنة والدفاع عنها يوما بيوم

اليوم 1: كيف تهاجم الشبكات

- طبقات نموذجي OSI وTCP/IP تحت الهجوم — موضع ضربة كل تهديد
- حالات اختراق الشبكات المسطحة — كلفة غياب التجزئة
- وظيفتا الحماية والكشف في NIST CSF 2.0 — واجبات ممارس الشبكات
- معايير توثيق الشبكة ومخططاتها — الرؤية قبل التغيير
- التعريف بطوبولوجيا المختبر — الشبكة الابتدائية للمخطط

اليوم 2: العناوين والخدمات الأساسية

- خطط عناوين IPv4 وIPv6 — مساحة للمناطق والنمو
- تتبع DHCP ومنع الخوادم الدخيلة — توزيع عناوين موثوق
- أمن DNS وتصفيته — حجب النطاقات الخبيثة مبكرا
- تبعيات التوقيت الشبكي وخدمات الدليل — مصادقة وسجلات موثوقة
- سجلات إدارة عناوين IP — المساءلة عن كل شبكة فرعية

اليوم 3: أمن التبديل

- تصميم الشبكات الافتراضية وتشذيب الوصلات الرئيسية — تقييد البث والقفز بين المقاطع
- خصائص حماية بروتوكول الشجرة الممتدة — منع الحلقات والاستيلاء
- أمن المنافذ وتحديد عناوين MAC — ضبط الأجهزة غير المصرح بها
- الفحص الديناميكي لبروتوكول ARP — إيقاف هجمات الوسيط
- الشبكات الافتراضية الخاصة — عزل الأجهزة داخل المقطع الواحد

اليوم 4: أمن التوجيه

- مصادقة OSPF وتصميم مناطقه — تبادل مسارات موثوق
- تصفية BGP وضوابط البادئات — حماية حافة الإنترنت
- قوائم التحكم في الوصول على الموجهات — تصفية أولية بين المواقع
- التحقق من المسار العكسي — مكافحة انتحال العناوين على الحافة
- فصل مستوى الإدارة — خيارات الإدارة خارج النطاق

اليوم 5: التجزئة ومناطق الثقة

- تصميم نموذج المناطق — المستخدمون والخوادم والضيوف والأنظمة الحرجة
- تموضع المنطقة المنزوعة السلاح — عزل الخدمات المواجهة للإنترنت
- تجزئة التقنيات التشغيلية — حماية أنظمة المصانع والمباني
- خيارات التجزئة الدقيقة — ضبط الحركة الأفقية الداخلية
- مصفوفة الحركة بين المناطق — توثيق التدفقات المسموحة

اليوم 6: جدران الحماية والوصول الآمن عن بعد

- تموضع جدران الحماية من الجيل التالي — نقاط الفحص المحيطية والداخلية
- السياسات المدركة للتطبيقات — قواعد حسب الخدمة لا المنفذ
- أنفاق IPsec بين المواقع — تصميم ربط الفروع
- الشبكات الخاصة الافتراضية للوصول عن بعد وفحص وضع العميل — انكشاف العاملين عن بعد
- وسطاء الوصول بانعدام الثقة — بدائل الأنفاق الشبكية الكاملة

اليوم 7: الشبكات اللاسلكية وضبط الوصول إلى الشبكة

- إعداد WPA3 للمؤسسات — مصادقة لاسلكية قوية
- المصادقة القائمة على المنافذ وفق 802.1X — قبول الأجهزة السلكية واللاسلكية
- إدخال أجهزة الضيوف وإنترنت الأشياء — شبكات معزولة للأجهزة غير الموثوقة
- كشف التسلل اللاسلكي — نقاط الوصول الدخيلة والمزيفة
- حالات لاسلكية من قطاعي التجزئة والضيافة — دروس تصميم قطاعية

اليوم 8: كشف التسلل ومنعه

- استراتيجية تموضع المستشعرات — تغطية المناطق ونقاط الاختناق
- الكشف بالتواقيع عبر Snort — أنماط الهجوم المعروفة
- الكشف السلوكي عبر Zeek — شذوذ البروتوكولات وبياناتها الوصفية
- المنع المباشر مقابل الكشف السلبي — مقايضات التوافر
- مسار فرز التنبيهات — التصعيد إلى عمليات الأمن

اليوم 9: مراقبة الشبكة والاستجابة

- جمع سجلات NetFlow وIPFIX — رؤية الحركة الأفقية الداخلية
- ملفات الحركة المرجعية — رصد الأحجام والوجهات غير المألوفة
- تركيز سجلات Syslog من أجهزة الشبكة — أدلة تغيير الإعدادات
- إجراءات الاحتواء الشبكي — شبكات الحجر وإغلاق المنافذ
- حالات حوادث من التصنيع والمرافق — دروس العزل الشبكي

اليوم 10: ممارسة مخطط الشبكة المؤسسية المجزأة

- تطبيق تصميم المناطق والعناوين على المختبر — حدود ثقة موثقة
- بناء التبديل والتوجيه وجدران الحماية — ضوابط مفروضة بين المناطق
- إعداد ضبط الوصول والشبكة اللاسلكية — اختبار قبول الأجهزة
- تسلل محاكى وفحص الكشف — التحقق من تغطية المستشعرات والتدفقات
- استكمال مخطط الشبكة المؤسسية المجزأة — المخططات والسياسات وخطة المراقبة

تطبيق تصميم شبكات المؤسسات الآمنة والدفاع عنها بعد الدورة

- رسم خريطة الحركة الحالية بين مقاطع المستخدمين والخوادم والأنظمة الحرجة باستخدام سجلات التدفق واقتراح أول مصفوفة للحركة بين المناطق
- تفعيل تتبع DHCP والفحص الديناميكي لبروتوكول ARP وأمن المنافذ على مجموعة مبدلات وصول واحدة وتسجيل أثر ذلك على الأجهزة الدخيلة

أسئلة حول تصميم شبكات المؤسسات الآمنة والدفاع عنها

ما تصميم شبكات المؤسسات الآمنة والدفاع عنها ولماذا يهم الآن؟

تصميم شبكات المؤسسات الآمنة والدفاع عنها هو بناء الشبكة وضبطها ومراقبتها بحيث تبطأ الهجمات وتكتشف وتحتوى. ويهم الآن لأن حركة المكاتب والسحابة والمصانع تتشارك البنية نفسها، والشبكات المسطحة تسمح لعدوى واحدة بالانتشار في كل مكان.

من يستفيد أكثر من دورة تصميم شبكات المؤسسات الآمنة والدفاع عنها؟

يستفيد أكثر فنيو الشبكات وممارسو الأمن المبتدئون ومشغلو مراكز عمليات الشبكة وكوادر دعم البنية التحتية. وتزداد فائدتك إن كنت تهيئ المبدلات والموجهات اليوم وينتظر منك تولي التجزئة والمراقبة والاحتواء.

كيف تختلف دورة تصميم شبكات المؤسسات الآمنة والدفاع عنها عن دورة أساسيات الشبكات؟

تفترض الدورة أنك تهيئ أجهزة الشبكة بالفعل وتضيف فوق ذلك طبقة التصميم الأمني. فأنت تعمل على مناطق الثقة وضبط الوصول وكشف التسلل والاحتواء بدلا من الكابلات والتوجيه البسيط وتجهيز الأجهزة.

ماذا تعود به من دورة تصميم شبكات المؤسسات الآمنة والدفاع عنها؟

تعود بمخطط شبكة مجزأة بني واختبر في المختبر. ويضم مخططات المناطق والعناوين والتدفقات المسموحة وسياسات الوصول وخطة مراقبة يمكنك تكييفها مع مواقعك.

تصميم شبكات المؤسسات الآمنة والدفاع عنها: الطريق إلى الأمام

يوجه مخطط الشبكة المؤسسية المجزأة أولا اختيار المناطق وقواعد العبور بينها في التغيير الشبكي التالي. ويبني منه فنيو الشبكات، ويضبط عليه فريق الأمن المستشعرات، ويستخدم المديرون مخططاته في الاعتمادات. وبعد أول تغيير في التجزئة تستحق مصفوفة الحركة مراجعة جديدة، إذ تكشف التدفقات الفعلية عادة تبعيات غابت عن التصميم.