CONCEPT

دورة Fortinet NSE 4 - FortiGate Security وتأمين الشبكات



دورة Fortinet NSE 4 - FortiGate Security وتأمين الشبكات

مقدمة:

تمثل دورة Fortinet NSE 4 - FortiGate Security برنامجا تدريبيا متخصصا يمتد أسبوع، موجها لمسؤولي أمن الشبكات ومهندسي الدفاع المحيطي ومختصي البنية التحتية ومحللي العمليات الأمنية، وتختتم بإعداد ملف نشر أمن وبنية FortiGate التحتية. تؤدي سياسات جدار الحماية غير المنسقة وضعف فحص حركة البيانات الداخلية والتعريف غير الدقيق للمستخدمين إلى ثغرات أمنية حرجة واضطرابات تشغيلية في شبكات المنشآت. يمتلك المرشحون خبرة سابقة في إدارة شبكات بروتوكول الإنترنت والتوجيه الثابت وضبط قوائم التحكم في الوصول، ويطورون كفاءتهم عبر التدريبات المعملية التطبيقية. وتقدم كور كونسبت هذه الدورة لترسيخ ضوابط دفاعية متينة وموثوقة لحماية المحيط الأمني عبر البنى المؤسسية.

أهداف الدورة:

- ضبط سياسات جدار الحماية FortiOS والملفات الأمنية وتقنيات ترجمة عناوين الشبكة لتطبيق ضوابط وصول أمنية إيجابية.
- تطبيق آلية تسجيل الدخول الموحد من فورتينت وقواعد جدار الحماية المستندة لهوية المستخدمين للتحقق من منسوبي المنشأة.
- إنشاء أنفاق IPsec الآمنة للربط بين المواقع وشبكات SSL VPN للوصول عن بعد لحماية الاتصالات في البيئات الموزعة.
- بناء مجموعات التوافر العالي لأجهزة FortiGate والنطاقات الافتراضية لضمان استمرارية الخدمة والفصل الآمن متعدد المستأجرين.
- تنفيذ إجراءات التشخيص المنهجي ومراجعة تكوينات جدار الحماية وسجلات الأمان للتحقق من الامتثال للسياسات وسلامة التشغيل.
- إعداد ملف نشر أمن وبنية FortiGate التحتية لتوحيد معايير الحماية المحيطية وفحص حركة البيانات الداخلية.

الفئة المستهدفة:

- مسؤولو أمن الشبكات المعنيون بإدارة سياسات جدار الحماية وتطبيق ضوابط الوصول والحفاظ على جاهزية البوابات المحيطية.
- مهندسو الدفاع المحيطي المكلفون بنشر الشبكات الافتراضية الخاصة وضبط أنظمة منع الاختراق وتأمين حدود الشبكة.
- مختصو البنية التحتية للأنظمة المسؤولون عن دمج خدمات الدليل وإعداد مجموعات التوافر العالي وتكوين واجهات التوجيه.
- محللو مراكز العمليات الأمنية المعنيون بمراقبة سجلات حركة البيانات وفحص أحداث التهديدات وتدقيق إعدادات قواعد الأمان.

محاور الدورة:

اليوم 1: معمارية نسيج الأمان والنشر الأولي للأجهزة

- الإعداد الأولي لنظام FortiOS 7.2 وتحديد عناوين الواجهات والوصول الإداري
- ملفات الإدارة في FortiGate وتكوين التحكم في الوصول القائم على الأدوار والمصادقة
- نشر نسيج الأمان FortiOS وتفعيل القياس عن بعد والرؤية المركزية
- نمط الشفافية في FortiGate وتوجيه وتصفية حزم البيانات في الطبقة الثانية
- إجراءات تدقيق أمن الشبكة ومراجعة التكوينات الأساسية لقواعد جدار الحماية

اليوم 2: سياسات جدار الحماية والمصادقة وإدارة الهوية

- جدار الحماية للجيل القادم في FortiOS وتحديد قواعد القائمة البيضاء الأمنية الإيجابية
- تسجيل الدخول الموحد من فورتينت وتكامل تعيينات هوية مستخدمي نطاق Active Directory
- ترجمة عناوين الشبكة المركزية في FortiGate وتكوين ترجمة المصدر والوجهة
- فحص الشهادات في FortiOS وتطبيق فك تشفير SSL العميق والتحقق من المرجع المصدق
- قواعد مصادقة المستخدمين في FortiGate وربط أذونات المجموعات بالسياسات الشبكية

اليوم 3: ملفات فحص التهديدات وحماية الوصول عن بعد

- محرك مكافحة الفيروسات في FortiGate وفحص البرمجيات الضارة بالتدفق والوكيل
- ملفات تصفية الويب في FortiOS وتصنيف روابط المواقع وحظر التهديدات
- ملفات التحكم في التطبيقات في FortiGate وتحديد وتقييد بروتوكولات طبقة التطبيقات
- نظام منع الاختراق في FortiGate وضبط خطوط التواقيع الأساسية ومصفيات الشذوذ
- شبكة SSL VPN في FortiGate وإنشاء أنفاق الاتصال الآمن والمصادقة متعددة العوامل

اليوم 4: توجيه البنية التحتية والمحاكاة الافتراضية والتوافر العالي

- التوجيه الثابت والديناميكي في FortiOS وتكوين بروتوكولات OSPF وBGP بين الشبكات الافتراضية
- النطاقات الافتراضية في FortiGate لتقسيم حركة البيانات والحدود الإدارية للمستأجرين
- التوافر العالي في FortiGate وتطبيق مجموعات العمل النشط الخامل والنشط المزدوج
- شبكة IPsec VPN في FortiGate وبناء الأنفاق الاحتياطية وتوجيه البيانات بين المواقع
- أوامر واجهة السطر البرمجي التشخيصية في FortiGate واستكشاف تدفق الحزم وجداول الجلسات

اليوم 5: المختبر العملي لأمن الشبكات المؤسسية والتركيب الفني

- مختبر FortiGate لتطبيق ضوابط التقسيم الدقيق لحركة البيانات في مراكز البيانات
- مختبر FortiGate لتحصين جدران الحماية المحيطية للمنشأة وأنفاق الشبكات الافتراضية
- مختبر FortiGate لمحاكاة الاستجابة المباشرة للتهديدات والتحويل التلقائي لحركة البيانات
- مختبر FortiGate لتنفيذ مراجعات دورة حياة قواعد جدار الحماية الممتدة لستة أشهر
- ملف نشر أمن وبنية FortiGate التحتية واستكمال وثائق التنفيذ والتشغيل المؤسسي

المهارات التي ستكتسبها:

- إدارة سياسات جدار الحماية للجيل القادم
- تكوين ضوابط الوصول القائمة على الهوية
- فحص حركة البيانات المشفرة عبر تقنية SSL
- ضبط تواقيع أنظمة منع الاختراق الشبكي
- بناء معمارية الشبكات الافتراضية الخاصة VPN
- تنفيذ مجموعات التوافر العالي لضمان الاستمرارية
- تقسيم النطاقات الافتراضية متعددة المستأجرين
- تدقيق ومراجعة تكوينات جدران الحماية الأمنية

لماذا تحضر هذه الدورة:

- تسليم ملف نشر أمن وبنية FortiGate التحتية لرئيس أمن المعلومات لتوحيد ضوابط الحماية المحيطية المؤسسية.
- تحديد أوضاع الفحص المناسبة وملفات المصادقة وسياسات التوجيه لموازنة أداء الشبكة مع متطلبات الحماية المشددة.
- الحد من التحركات الجانبية غير المراقبة وانحراف التكوينات وحركة البيانات المشفرة غير المفحوصة لتفادي الاختراقات المكلفة.
- توجيه مهندسي الفريق لتشخيص جداول جلسات النواة وإعداد تحويلات التوافر العالي وتنفيذ تدقيق دوري لقواعد الحماية.

الخاتمة:

تعتمد المنشأة في ختام الدورة ملف نشر أمن وبنية FortiGate التحتية لتوحيد معايير الحماية المحيطية وتقسيم الشبكات الداخلية عبر الوحدات التشغيلية. ويستند مدير البنية التحتية التقنية ومدير عمليات الأمن السيبراني إلى هذا المخرج لاعتماد تعديلات سياسات جدار الحماية، والتحقق من تكامل خدمات المصادقة، ومتابعة إعدادات التوافر العالي. ويتولى فريق عمليات الشبكة بعد ستة أشهر إجراء مراجعة هيكلية لقواعد جدار الحماية النشطة، وسجلات تجاوز الفشل، وكفاءة الملفات الأمنية لإلغاء مسارات الوصول غير النشطة وضمان الامتثال المستمر للمعايير الهندسية المعتمدة.

الأسئلة الشائعة:

ما الفئات الوظيفية المرشحة لحضور دورة Fortinet NSE 4 - FortiGate Security؟

ترشح المنشآت مسؤولي أمن الشبكات ومهندسي الدفاع المحيطي ومختصي البنية التحتية ومحللي مراكز العمليات الأمنية. ويتولى هؤلاء المهنيون مهام تشغيل واجهات جدران الحماية، وتطبيق قواعد الوصول الشبكي، وإدارة قنوات الاتصال عن بعد الآمنة، ومتابعة أحداث الأمان التقنية في بيئات العمل المؤسسية.

ما المتطلبات المهنية المسبقة لحضور دورة Fortinet NSE 4 - FortiGate Security؟

ينبغي للمرشحين إدارة شبكات بروتوكول الإنترنت وتشغيل بروتوكولات التوجيه الأساسية وقوائم التحكم في الوصول. وتضمن المعرفة بمفاهيم جدران الحماية ونظام تسمية النطاقات وأوامر الشبكات بنظم التشغيل التفاعل المباشر مع السياسات المتقدمة وملفات الفحص ومجموعات التوافر العالي خلال الجلسات.

ما المخرج العملي الذي تحققه المنشأة من دورة Fortinet NSE 4 - FortiGate Security؟

تتسلم المنشأة ملف نشر أمن وبنية FortiGate التحتية المكتمل. ويوفر هذا المجلد التشغيلي قوالب إعداد جاهزة للإنتاج، ومخططات محققة لمجموعات التوافر العالي، ومواصفات الشبكات الافتراضية الخاصة المشفرة، وإجراءات موثقة لتنفيذ مراجعات نصف سنوية لقواعد جدار الحماية عبر الشبكات التشغيلية.

ما المعايير والمسارات التي تتبعها دورة Fortinet NSE 4 - FortiGate Security؟

تتبع الدورة منهاج Fortinet Certified Professional ومسار Fortinet Network Security Expert المعتمد لنظام FortiOS. وتدمج الضوابط التقنية المستندة لمعايير أمن الشبكات، كالقوائم البيضاء الأمنية وتصفية التطبيقات وفرض قيود هوية المستخدمين وإجراءات مراجعة تكوينات جدار الحماية الدورية للأنظمة الحساسة.