BLACKBIRD FOR TRAINING

دورة إدارة وتشغيل جدار الحماية (NSE 4 –
FortiGate (FortiOS Administrator



دورة إدارة وتشغيل جدار الحماية FortiGate (FortiOS Administrator – NSE 4)

مقدمة:

تؤهلك دورة إدارة وتشغيل جدار الحماية FortiGate FortiOS Administrator – NSE 4 لضبط وتشغيل وتأمين جدران الحماية المحيطية للمؤسسات بالاعتماد على نظام FortiOS خلال أسبوع تطبيقية مكثفة. تبني خلال التدريب البنية التحتية لأمن شبكات FortiGate وخط الأساس للسياسات التشغيلية متضمنة الجاهزية العالية وتوثيق تغييرات القواعد وملفات فحص التهديدات المتقدمة. تقدم بلاك بيرد للتدريب هذا المحتوى للمختصين الممتلكين لمعارف مسبقة في مفاهيم الشبكات وعناوين بروتوكول الإنترنت وبروتوكولات التوجيه الأساسية، حيث تباشر التطبيق المخبري الفعلي لنشر سياسات الأمان وتكوين مسارات الشبكات الافتراضية الخاصة وفلاتر الحماية مباشرة على أجهزة FortiGate النشطة.

أهداف الدورة:

- تكوين واجهات شبكة FortiGate وضبط التوجيه الثابت ضمن بيئات التشغيل المزدوجة.
- بناء سياسات جدار الحماية وعناصر العناوين لفرض الحدود الأمنية المقسمة للشبكة.
- نشر ملفات أمان FortiOS المتضمنة مكافحة الفيروسات ومنع الاختراق وفلترة الويب والتحكم في التطبيقات.
- تطبيق أنفاق IPsec المعتمدة على التوجيه وبوابات الوصول عن بعد عبر SSL VPN للمستخدمين المصرحين.
- ضبط مجموعات الجاهزية العالية النشطة والساكنة وقواعد SD-WAN لضمان مرونة واستمرارية الاتصال الشبكي.
- تدقيق قواعد الوصول لجدار الحماية وطلبات ترجمة عناوين الشبكة وفق معايير التوثيق لضوابط NCA Control 7-4.

الفئة المستهدفة:

- تتولى إعداد وتشغيل أجهزة جدران الحماية المحيطية ضمن البيئات الشبكية للمؤسسات.
- تدير ضوابط الوصول الأمني وتراقب تنبيهات الاختراق والتهديدات داخل فرق العمليات الأمنية.
- تنشر البنية التحتية للشبكات وتربط الفروع بالمقر الرئيسي ضمن أقسام هندسة النظم.
- تدقق تعديلات قواعد جدران الحماية وتتحقق من الامتثال لخطوط الأساس الأمنية في إدارات أمن المعلومات.



محاور الدورة:

اليوم 1: إعداد واجهات شبكة FortiGate والتوجيه

- نشر واجهات FortiOS باستخدام نمط NAT القياسي والنمط الشفاف
- ضبط المسارات الثابتة ومسافات التوجيه الإدارية لبوابات الاتصال الصاعد
- إدارة صلاحيات الوصول الإداري وملفات التعريف القائمة على الأدوار في FortiOS
- تكوين خدمات الشبكة المحلية وخوادم التوزيع الديناميكي للعنوان بروتوكول DHCP
- بناء نموذج خط الأساس الأولي لتوجيه واجهات FortiGate والوصول الإداري

اليوم 2: تطبيق سياسات جدار الحماية ونسيج الأمان

- هيكلة سياسات جدار الحماية باستخدام كائنات المصدر والوجهة المحددة
- تطبيق مجمعات ترجمة العناوين المركزية SNAT وترجمة العناوين الواردة DNAT
- دمج قياسات نسيج الأمان Fortinet Security Fabric عبر الأصول الشبكية المتصلة
- توثيق تعديلات قواعد سياسات جدار الحماية وفق متطلبات ضابط NCA Control 7-4
- بناء مصفوفة الوصول لسياسات جدار الحماية المؤسسي ونسيج الأمان

اليوم 3: نشر ملفات أمان إدارة التهديدات الموحدة

- تكوين ملفات الفحص العميق لبروتوكول SSL باستخدام الشهادات الرقمية الداخلية للمؤسسة
- نشر تواقيع مكافحة الفيروسات ومنع التسلل IPS لتأمين الحدود المحيطية
- فرض تصنيفات تصفية الويب وحماية نظام أسماء النطاقات DNS
- تطبيق مستشعرات التحكم في التطبيقات لمنع البرمجيات المؤسسية غير المعتمدة
- بناء معمارية ملفات الفحص الموحد للتهديدات وتصفية المحتوى الرقمي

اليوم 4: تكوين الشبكات الافتراضية الخاصة والجاهزية العالية

- بناء أنفاق IPsec للربط بين المواقع المستندة إلى التوجيه مع التحويل التلقائي
- تجهيز بوابات الوصول عن بعد عبر SSL VPN مع المصادقة متعددة العوامل للمستخدمين
- ضبط مجموعات الجاهزية العالية بنمط نشط وساكن لتشغيل الشبكة المقاوم للأعطال
- توجيه مسارات حركة البيانات عبر تقنية SD-WAN على واجهات إنترنت متعددة
- بناء قالب أنفاق الربط المكررة ومجموعة الجاهزية العالية المقاومة للأعطال



اليوم 5: تنفيذ العمليات المعملية وتدقيق الامتثال

- تشخيص حزم البيانات المفقودة باستخدام أدوات الفحص عبر واجهة أوامر FortiOS
- تقسيم الموارد الإدارية وتوجيه بيانات المستأجرين عبر النطاقات الافتراضية VDOMs
- مراجعة قواعد جدار الحماية نصف السنوية استنادا إلى معيار CSCC-1:2019
- تحصين إعدادات نظام FortiOS ضد التعديلات الإدارية غير المصرح بها
- بناء البنية التحتية لأمن شبكات FortiGate وخط الأساس للسياسات التشغيلية

المهارات التي ستكتسبها:

- إعداد واجهات نظام FortiOS
- هندسة قواعد جدران الحماية المحيطية
- فحص التهديدات عبر ملفات الأمان
- تجهيز أنفاق الربط IPsec المعتمدة على التوجيه
- إدارة بوابات الوصول عن بعد عبر SSL VPN
- إدارة مجموعات الجاهزية العالية
- توجيه مسارات حركة البيانات عبر SD-WAN
- تدقيق الامتثال لتعديلات قواعد جدار الحماية

لماذا تحضر هذه الدورة:

- بناء البنية التحتية لأمن شبكات FortiGate وخط الأساس للسياسات التشغيلية للتطبيق المباشر في بيئة الإنتاج.
- إتقان أوامر الإعداد وضوابط الواجهة الرسومية لنظام FortiOS لتطبيق قواعد الوصول المتقدمة وملفات الحماية.
- إنشاء طوبولوجيا شبكية مرنة باستخدام مجموعات الجاهزية العالية وتوجيه حركة البيانات الذكي عبر تقنية SD-WAN.
- مواءمة عمليات إدارة قواعد جدران الحماية وترجمة العناوين مع أطر الحوكمة الصادرة مثل ضابط 4-7 NCA Control.

الخاتمة:

تشرع في أسبوعك الأول بعد الدورة بتطبيق نموذج البنية التحتية لأمن شبكات FortiGate وخط الأساس للسياسات لتقييم السياسات الحالية للمنظمة وروابط الواجهات. ستعرض ملفات الأمان المعتمدة وإعدادات الجاهزية العالية ونماذج توثيق التغييرات على مدير تشغيل الشبكات ورئيس أمن المعلومات للاعتماد الرسمي. وعقب النشر الأولي، تفحص سجلات جلسات FortiGate ومخرجات حزم البيانات للتحقق من امتثال حركة المرور لحدود الأمان دون أي تأثير سلبي على جودة الخدمات.



الأسئلة الشائعة:

ما الذي ستتمكن من تنفيذه بعد دورة إدارة وتشغيل جدار الحماية FortiOS Administrator – NSE 4 FortiGate؟

ستتمكن من نشر وإعداد وصيانة جدران حماية FortiGate العاملة بنظام FortiOS، وبناء سياسات جدار الحماية المتينة ودمج ملفات إدارة التهديدات وإنشاء أنفاق IPsec وSSL VPN وإدارة مجموعات الجاهزية العالية واستكشاف الأعطال التشغيلية بالأدوات الإدارية المتخصصة.

ما المتطلبات المسبقة للالتحاق بدورة إدارة وتشغيل جدار الحماية FortiOS Administrator – NSE 4 FortiGate؟

تتطلب الدورة فهما راسخا لمفاهيم الشبكات الأساسية وتقسيم عناوين IPv4 وعمليات بروتوكول TCP/IP ومبادئ التوجيه الأساسية، ويستحسن الإلمام العام بأساسيات أمن الشبكات، ولا يشترط امتلاك خبرة تشغيلية سابقة في التعامل مع أجهزة Fortinet.

ما المخرج العملي الذي تبنيه خلال دورة إدارة وتشغيل جدار الحماية FortiOS Administrator – NSE 4 FortiGate؟

تبني البنية التحتية لأمن شبكات FortiGate وخط الأساس للسياسات كدليل تطبيقي متكامل، متضمنا توجيه الواجهات وقواعد الوصول المقسمة وملفات فحص المحتوى وأنفاق IPsec المزدوجة ومجموعات الجاهزية العالية وسجلات التعديلات الجاهزة لعمليات التدقيق والامتثال.

كيف تختلف دورة إدارة وتشغيل جدار الحماية FortiGate FortiOS Administrator – NSE 4 عن الدورات العامة؟

تركز الدورة مباشرة على الإدارة العملية والتشغيل الأمني لأجهزة FortiGate بنظام FortiOS، متجاوزة المفاهيم النظرية العامة لترسخ مهارات تطبيقية تشمل المهام التشغيلية اليومية وإدارة المجموعات المكررة وتوثيق السجلات وفق المعايير والضوابط المعتمدة.

