MERCURY

دورة أمن الشبكات وإدارة جدران الحماية NSE 4

Fortinet

7 – 11 ديسمبر 2026

روما (إيطاليا)



Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

دورة أمن الشبكات وإدارة جدران الحماية Fortinet NSE 4

المرجع: 46_188989 **التاريخ:** 7 – 11 ديسمبر 2026 **المكان:** روما (إيطاليا) **الرسوم:** 7200 Euro

تزود دورة أمن الشبكات وإدارة جدران الحماية Fortinet NSE 4 مهندسي الشبكات ومديري الأنظمة ومحللي أمن المعلومات بالمهارات الفنية لإعداد سياسات الفحص والتحكم في النطاقات وتأمين الاتصال المشفر عبر بيئات التشغيل خلال أسبوع تدريبي. يمارس المشاركون إعداد جدران الحماية وبناء مسارات التوجيه الافتراضية والربط مع أنظمة الهوية لتجميع ملف أمن وبنية FortiOS التحتية. تقدم ميركوري للتدريب هذه الدورة لتمكين الكوادر التقنية من إدارة جدران حماية الجيل القادم وحماية البيئات المؤسسية بثبات وموثوقية.

نبذة عن الدورة

تؤدي الإعدادات غير الدقيقة لسياسات جدران الحماية وغياب الفحص العميق لحركة البيانات المشفرة إلى تعريض الشبكات المؤسسية للاختراقات وانقطاع الخدمات التشغيلية. تتطلب متابعة هذه الدورة معرفة مسبقة بأساسيات توجيه حزم البيانات وعناوين بروتوكول الإنترنت وترجمة العناوين ومبادئ الدفاع الشبكي. يتدرب المشاركون عمليا على نشر محركات الفحص وتكوين الأنفاق المشفرة وإعداد مصفوفات التوافر العالي للحفاظ على استمرارية العمليات.

لمن هذه الدورة

- المسؤولون عن إعداد سياسات فحص جدران الحماية من الجيل القادم وقواعد ترجمة عناوين الشبكة.
- المسؤولون عن نشر أنفاق بروتوكول الإنترنت المشفرة IPsec والشبكات الافتراضية الخاصة لاتصال الفروع والعمل عن بعد.
- المسؤولون عن إدارة مصفوفات التوافر العالي لجدران الحماية ومسارات توجيه الشبكات واسعة النطاق المعرفة برمجيا SD-WAN.
- المسؤولون عن دمج خوادم المصادقة المركزية وأدلة المستخدمين مع بوابات الحماية لتطبيق سياسات الوصول المبنية على الهوية.

لا تناسب هذه الدورة الفنيين المبتدئين في الدعم الفني الباحثين عن أساسيات صيانة الحاسب وتناسبهم دورات الدعم الفني التأسيسية، كما لا تناسب مسؤولي الحوكمة والمخاطر الساعين وراء أطر السياسات النظرية وتناسبهم دورات إدارة المخاطر المؤسسية العامة.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

الكفاءات المستهدفة

- تطبيق ملفات الحماية المتقدمة: نشر محركات فحص الفيروسات والتحكم في التطبيقات وتصفية مواقع الويب ومنع الاختراق لتأمين حركة المرور عبر الحدود الشبكية.
- هندسة الأنفاق المشفرة: إنشاء وإدارة أنفاق الشبكات الخاصة الافتراضية ونقاط الوصول الآمن عن بعد لحماية حركة البيانات المؤسسية الحساسة.
- إدارة البنية التحتية المرنة: تهيئة بروتوكولات مجموعات جدران الحماية والتوجيه المبني على السياسات لتفادي انقطاع الخدمة وضمان الجاهزية التشغيلية.
- تكامل الهوية والتحكم بالوصول: ربط خدمات الدليل النشط مع ميزات تسجيل الدخول الموحد لفرض سياسات أمنية تعتمد على هوية المستخدم.
- عزل النطاقات الشبكية: تقسيم جدران الحماية المادية إلى نطاقات افتراضية مستقلة لمنع التحركات الجانبية وفصل بيئات العمل والبيانات.

ما ستتمكن من إنجازه

بنهاية الدورة ستتمكن من إنجاز المهام الآتية:

- انطلاقا من متطلبات الأمن المؤسسية، إعداد سياسات جدران الحماية وتفعيل الفحص العميق لحزم البيانات المشفرة لحظر التطبيقات والأنشطة غير المصرح بها.
- بالنظر إلى مخططات الفروع البعيدة، بناء أنفاق مشفرة آمنة ومترابطة عبر بروتوكول IPsec مع آليات التحويل التلقائي عند انقطاع المسارات.
- باستخدام خوادم الدليل النشط، دمج حلول الدخول الموحد FSSO لفرض قواعد وصول تستند إلى هويات المستخدمين ومجموعات العمل.
- انطلاقا من معايير استمرارية الأعمال، إعداد مصفوفات التوافر العالي لجدران الحماية بحالة النشط والمبادر لضمان تزامن الجلسات وسرعة التعافي.
- بالنظر إلى تصاميم الشبكات متعددة البيئات، تهيئة النطاقات الافتراضية VDOMs ومسارات الربط الداخلي بينها لعزل العمليات التشغيلية المختلفة.
- باستخدام شاشات متابعة الحوادث التشغيلية، ضبط ملفات تسجيل الأحداث والتنبيهات المنسجمة مع متطلبات التدقيق الدوري للأمن السيبراني.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

محتوى الدورة

اليوم 1: بنية النظام وإعداد السياسات الأساسية

- هندسة نظام التشغيل FortiOS وتهيئة واجهات الإدارة الشبكية وتأمين الوصول.
- إنشاء سياسات جدران الحماية وتعريف كائنات العناوين والخدمات والبروتوكولات.
- تطبيق قواعد ترجمة عناوين الشبكة والمنافذ لمسارات الحركة الصادرة والواردة.
- تحليل جلسات جدران الحماية وتطبيق أساليب الفحص المعتمدة على التدفق والوكيل.
- تحديد أدوار الإدارة القائمة على الصلاحيات وإجراءات النسخ الاحتياطي للإعدادات.

اليوم 2: ملفات الحماية وتكامل التحقق من الهوية

- تهيئة ملفات فحص الفيروسات واكتشاف البرمجيات الخبيثة المتقدمة وعزل التهديدات.
- تطبيق ضوابط تصفية محتوى الويب والتحكم في التطبيقات وفك تشفير SSL.
- تفعيل محركات منع التطفل وحماية الخوادم والخدمات المنشورة من الاستغلال الثغري.
- دمج خدمات الدليل النشط وتفعيل برنامج الدخول الموحد FSSO لربط الهوية بالسياسات.
- ضبط سياسات التوثيق متعدد العوامل للوصول الإداري وحسابات المسؤولين.

اليوم 3: هندسة الشبكات الافتراضية الخاصة وحماية المسارات

- بناء أنفاق IPsec المعتمدة على المسارات لربط المواقع والفروع الخارجية بمركز البيانات.
- تكوين الشبكات الافتراضية الخاصة للوصول عن بعد باستخدام تقنيات SSL VPN الآمنة.
- إعداد معايير التشفير القوي وإدارة الشهادات الرقمية ومفاتيح المصادقة المشتركة.
- تصميم مسارات التوجيه الثابت والتوجيه القائم على السياسات لحزم البيانات المشفرة.
- تطبيق سياسات التوجيه الذكي ومراقبة جودة الروابط ضمن حلول SD-WAN للمؤسسات.

اليوم 4: التوافر العالي وتقسيم النطاقات الافتراضية

- تهيئة مصفوفات التوافر العالي بنمط النشط والمحايد لضمان تماثل الجلسات التشغيلية.
- فحص إشارات نبض الحياة وتكوين منافذ المراقبة للتحويل التلقائي عند الأعطال.
- تقسيم جدار الحماية إلى نطاقات افتراضية VDOMs لعزل المستأجرين والبيئات التشغيلية.
- بناء مسارات التوجيه بين النطاقات الافتراضية وضبط ضوابط نقل البيانات المشتركة.
- إجراء تدقيق ومراجعة لقواعد وسياسات جدران الحماية والتحقق من سريان مفعولها.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

اليوم 5: التطبيق المتكامل وإعداد وثيقة البنية التحتية

- تمرين: نشر سياسات الحماية متعددة الطبقات وفحص البيانات المشفرة لبيئة مركز البيانات.
- تمرين: إعداد نفق IPsec متكرر وتطبيق اختبارات التحويل التلقائي للمسار عند انقطاع الاتصال.
- تمرين: تكوين نطاق افتراضي معزول وربطه بالمستخدمين عبر بروتوكولات الهوية المعتمدة.
- تمرين: ضبط إعدادات التنبيه وتصدير سجلات العمليات لمحطات المراقبة والتحليل الأمني.
- اعتماد وتجميع مخرجات ملف أمن وبنية FortiOS التحتية وتوثيق إجراءات التشغيل.

دراسات الحالة والتمارين

تتضمن الدورة أنشطة مقترحة تمكن المشاركين من ممارسة الإجراءات المهنية في بيئات متعددة:

- دراسة حالة: إعادة تصميم سياسات الفحص والتحكم في التطبيقات لمؤسسة مالية لمنع تسريب البيانات وعزل حركة تعاملات البطاقات المصرفية.
- تمرين: بناء مسار اتصال مشفر وآمن يربط فروع منشأة رعاية صحية متعددة المواقع مع مركز البيانات مع تفعيل التبديل التلقائي.
- دراسة حالة: تقسيم جدران الحماية عبر النطاقات الافتراضية لشركة خدمات لوجستية لتفصل بين شبكات العمليات التشغيلية وشبكات الأعمال الإدارية.
- تمرين: إعداد مصفوفة التوافر العالي وتطبيق سيناريو انقطاع أحد الأجهزة والتحقق من استمرار جلسات المستخدمين دون توقف.

ما ستعود به إلى عملك

ستعود إلى عملك مزودا بأداة ملف أمن وبنية FortiOS التحتية لاستخدامها في تقييم أداء جدران الحماية ومطابقة السياسات الأمنية وتوثيق مسارات التوجيه خلال شهرك الأول. تمثل الأداة سجلا فنيا متكاملا لتوثيق وتطبيق سياسات الحماية المؤسسية، وتشتمل على المحتويات الآتية:

- مصفوفة توثيق قواعد جدران الحماية وسياسات الترجمة وتعيين كائنات العناوين والخدمات.
- دليل ضبط معايير ملفات الفحص العميق ومحركات منع التطفل والتحكم في التطبيقات وتصفية الويب.
- إجراءات التشغيل القياسية لإعداد وتتبع أنفاق IPsec ومصفوفات التوافر العالي والنطاقات الافتراضية.
- نماذج المراجعة الدورية لقواعد الجدران وسجلات الأحداث وتنبيهات أمن الشبكات.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

إجابات سريعة عن الأسئلة الشائعة

ما الذي أحتاج إلى معرفته قبل دورة أمن الشبكات وإدارة جدران الحماية Fortinet NSE 4؟

تحتاج إلى فهم مبادئ توجيه البيانات الشبكية، ونموذج العناوين IP، وآليات ترجمة عناوين الشبكة، والمفاهيم الأساسية لأمن الشبكات وتقنيات المنافذ والبروتوكولات الشائعة.

بم تختلف دورة أمن الشبكات وإدارة جدران الحماية Fortinet NSE 4 عن الدورات العامة لأساسيات الشبكات؟

تركز هذه الدورة على التهيئة المتقدمة لجدران حماية الجيل القادم وإدارة أنظمة FortiOS وبناء ملفات الفحص والتوافر العالي وتأمين البيئات المؤسسية المشتركة عمليا.

كيف يساهم الفحص العميق للبيانات المشفرة في منع التهديدات؟

يتيح فحص الحركة المشفرة بواسطة جدران الحماية اكتشاف البرمجيات الضارة المتخفية داخل قنوات الاتصال الآمنة وحظر تسريب البيانات الحساسة دون التأثير على سير العمليات المصرح بها.

ما الوثيقة التي أخرج بها من دورة أمن الشبكات وإدارة جدران الحماية Fortinet NSE 4؟

تخرج بأداة ملف أمن وبنية FortiOS التحتية المشتملة على معايير تهيئة السياسات الأمنية، وتصاميم الأنفاق المشفرة، وإجراءات إدارة النطاقات الافتراضية وتدقيق القواعد في شبكتك.

لمديرك

سيكتسب الموظف القدرة على إدارة جدران حماية الجيل القادم وبناء سياسات الفحص والتشفير وعزل النطاقات الافتراضية بكفاءة وموثوقية عالية. ويعود إلى موقع عمله مزودا بأداة ملف أمن وبنية FortiOS التحتية، حيث يبدأ بمراجعة قواعد المرور وتأمين مسارات الاتصال المشفر ورفع جاهزية الشبكة للتصدي للتهديدات السيبرانية المؤسسية.