



دورة إدارة مركز عمليات الشبكة NOC: مراقبة الشبكات ومعالجة الإنذارات وتشغيل المناوبات



دورة إدارة مركز عمليات الشبكة NOC: مراقبة الشبكات ومعالجة الإنذارات وتشغيل المناوبات

مقدمة:

دورة إدارة مركز عمليات الشبكة NOC دورة تدريبية مدتها خمسة أيام تغطي مراقبة الشبكات ومعالجة الإنذارات وتشغيل المناوبات، وتوجه لفرق المراقبة وقادة المناوبات ومهندسي الشبكات، وتنتهي ببناء نموذج تشغيل لمركز العمليات ومجموعة أدلة تشغيل ولوحة مؤشرات أداء لشبكة حالة دراسية. تفقد المنشآت جزءاً من توافرية خدماتها حين تغرق سيول الإنذارات العطل الجذري، وتغيب مسارات التصعيد الواضحة، وتسلم كل مناوبة معلومات ناقصة لمن يليها. يعمل المرشحون فعلاً على شاشات المراقبة أو معالجة أعطال الشبكة، وتعتمد الدورة دراسات حالة مبنية على بيانات إنذارات وتذاكر وحركة من شبكات اتصالات ومؤسسات. وتقدم كور كونسبت هذه الدورة في إدارة مراكز عمليات الشبكات.

أهداف الدورة:

- تحديد ميثاق مركز عمليات الشبكة ونموذج تشغيله وهيكل التوظيف المتدرج، مع واجهات واضحة مع فرق المشكلات والتغيير والميدان والأمن
- تهيئة تصميم مراقبة يجمع استطلاع SNMPv3 بروتوكول إدارة الشبكات البسيط ورسائل التنبيه، وسجلات تدفق IPFIX، ومستويات خطورة Syslog، ومجسات الاختبار الاصطناعي
- تطبيق قواعد خطورة الإنذارات وكتبها وربط الأحداث وفق طوبولوجيا الشبكة لإظهار الإنذار الجذري أثناء عواصف الإنذارات
- إدارة تصعيد الحوادث المتدرج وجدول المناوبات وتسليمها بدعم من أدلة التشغيل ومقالات قاعدة المعرفة
- قياس مؤشرات MTTR و MTDD والتوافرية والأداء مقابل اتفاقيات مستوى الخدمة، والإبلاغ عن حالات الإخلال لمالكي الخدمات
- التنسيق مع مركز العمليات الأمنية، وتوظيف اتجاهات السعة والمعالجة الآلية بالنصوص البرمجية لمنع تكرار الانقطاعات

الفئة المستهدفة:

- فرق المراقبة في مراكز عمليات الشبكات المسؤولة عن متابعة الإنذارات على مدار الساعة واستعادة الخدمة في المستوى الأول
- قادة المناوبات المسؤولون عن جداول العمل وجودة التسليم وقرارات التصعيد في كل مناوبة
- فرق هندسة الشبكات المسؤولة عن معالجة الأعطال في المستويين الثاني والثالث لشبكات النقل و IP والوصول
- فرق البنية التحتية في المؤسسات المسؤولة عن مراقبة روابط الشبكات الواسعة وشبكات الحرم ومراكز البيانات
- فرق ضمان الخدمة المسؤولة عن تقارير مستوى الخدمة وأرقام التوافرية وإشعارات الانقطاع للعملاء
- فرق أدوات المراقبة المسؤولة عن أنظمة الاستطلاع والمجسات والمجمعات وإعداد قواعد الإنذارات

محاوَر الدورة:

اليوم 1: دور مركز عمليات الشبكة ونموذج تشغيله وتقييم الوضع الحالي

- ميثاق مهمة المركز وتحديد نطاق الخدمات الخاضعة للمراقبة
- نماذج التشغيل المركزي والمتتابع بين المواقع على مدار الساعة والهجين
- نموذج التوظيف المتدرج من المستوى الأول إلى المستوى الثالث
- واجهات المركز مع فرق المشكلات والتغيير والعمل الميداني
- قياس نضج المركز من سجلات الإنذارات والتذاكر المصدرة

اليوم 2: معمارية المراقبة ومصادر بيانات القياس عن بعد والأدوات

- استطلاع SNMPv3 وطلبات GetBulk واختيار كائنات قاعدة MIB
- تصميم مستقبلات رسائل التنبيه والإشعارات القادمة من الأجهزة
- تصدير تدفقات IPFIX وموقع المجمعات وتصنيف حركة البيانات
- مستويات خطورة Syslog وفق RFC 5424 لتصفية الرسائل
- مجسات المعاملات الاصطناعية لفحص التأخير وإمكانية الوصول

اليوم 3: معالجة الإنذارات وتصعيد الحوادث وممارسات المناوبة

- مصفوفة خطورة الإنذارات وقواعد كبت إنذارات الروابط المتذبذبة
- ربط الأحداث وفق طوبولوجيا الشبكة وتحديد الإنذار الجذري
- مصفوفة التصعيد المتدرج للحوادث وإرسال الموردين والفرق الميدانية
- جدول المناوبات وتناوب الاستدعاء وسجل تسليم المناوبة
- بنية أدلة التشغيل ومقالات قاعدة المعرفة للأعطال المتكررة

اليوم 4: مؤشرات أداء المركز والتنسيق مع مركز العمليات الأمنية والسعة والأتمتة

- قياس MTDD MTTRg وMTTR عبر مراحل الحادثة
- حساب التوافرية وتقارير الإخلال بمستوى الخدمة لمالكي الخدمات
- دليل مشترك بين مركزي الشبكة والأمن لهجمات DDoS والحركة المريبة
- عتبات اتجاهات السعة من استخدام المنافذ وبيانات التدفق
- المعالجة الآلية بالنصوص البرمجية وإثراء التذاكر ضمن حدود الموافقة

اليوم 5: دراسة حالة: نموذج تشغيل المركز ومجموعة أدلة التشغيل ولوحة المؤشرات

- عرض شبكة الحالة الدراسية بمواقع اتصالات ومؤسسات مختلطة
- تمرين عاصفة إنذارات بتطبيق قواعد الربط والتصعيد
- كتابة مجموعة أدلة تشغيل لخمسة أنواع إنذارات متكررة
- بناء لوحة مؤشرات تعرض MTTR والتوافرية ومستوى الخدمة
- استكمال نموذج تشغيل المركز وعرضه أمام لجنة المراجعة

المهارات التي ستكتسبها:

- تصميم معمارية المراقبة
- ضبط قواعد الإنذارات
- تحليل ربط الأحداث
- إدارة تصعيد الحوادث
- تنظيم تسليم المناوبات
- كتابة أدلة التشغيل
- إعداد تقارير مؤشرات أداء المركز
- تحليل اتجاهات السعة

لماذا تحضر هذه الدورة:

- تسليم نموذج تشغيل ومجموعة أدلة تشغيل ولوحة مؤشرات أداء لشبكة حالة دراسية إلى رئيس عمليات الشبكة ومسؤول ضمان الخدمة
- تقرير الإنذارات التي تكبت أو تربط أو تصعد، ومتى ترسل الفرق الميدانية أو الموردون
- تجنب الانقطاعات الطويلة وغرامات مستوى الخدمة والأعطال المتكررة الناتجة عن سيول الإنذارات وضعف تسليم المناوبات
- نقل قوالب أدلة التشغيل وسجلات التسليم وقواعد الربط إلى النظراء في كل مناوبة

الخاتمة:

بعد العودة إلى العمل يسلم المشاركون رئيس عمليات الشبكة ومسؤول ضمان الخدمة نموذج تشغيل لمركز العمليات ومجموعة أدلة تشغيل ولوحة مؤشرات أداء يمكن تكييفها مع الشبكة الحية. وتعتمد عليها الإدارة في تحديد التوظيف المتدرج وقواعد كبت الإنذارات والتصعيد، واختيار الأعطال التي تنتقل إلى المعالجة الآلية. ويستخدم مالكو الخدمات اللوحة لمتابعة MTTR والتوافرية وحالات الإخلال بمستوى الخدمة. وبعد الشهر الأول من العمل بالقواعد الجديدة تراجع الوحدة أعداد الإنذارات وأوقات التصعيد وثمرات التسليم مقابل خط الأساس في اللوحة.

الأسئلة الشائعة:

ما الذي يحتاج المشاركون إلى معرفته قبل دورة إدارة مركز عمليات الشبكة؟

يكفي أن يعمل المشاركون مع إنذارات الشبكة أو التذاكر أو شاشات المراقبة وأن يفهم أساسيات التوجيه والتبديل في شبكات IP، ولا تشترط مهارة البرمجة. ويساعد إحضار أعداد إنذارات أو تذاكر مجهولة الهوية أو جدول مناوبات من مركزه على تطبيق دراسات الحالة.

بم تختلف دورة إدارة مركز عمليات الشبكة عن دورات AIOps أو تحليل حزم البيانات؟

تتناول الدورة تنظيم المركز وتشغيله: تصميم المراقبة وقواعد الإنذارات والتصعيد والمناوبات وأدلة التشغيل والمؤشرات. أما تعلم الآلة في العمليات وتحليل الحزم على مستوى الإطارات فيردان سياقاً فقط، وتعالجها دورات متخصصة بعمق.

لماذا يهم ربط الأحداث في إدارة مركز عمليات الشبكة؟

قد يطلق قطع ليف ضوئي واحد أو انقطاع تغذية كهربائية مئات الإنذارات التابعة. ويجمعها الربط وفق الطوبولوجيا تحت الإنذار الجذري، فتفتح المناوبة حادثة واحدة وترسل الفريق المناسب وتتجنب التذاكر المكررة التي ترفع MTTR.

ماذا يعود به المشاركون من دورة إدارة مركز عمليات الشبكة؟

يعود المشاركون بنموذج تشغيل للمركز ومجموعة أدلة تشغيل لأنواع الإنذارات المتكررة ولوحة مؤشرات تعرض MTTR و MTTRg والتوافرية والأداء مقابل مستوى الخدمة، وكلها مبنية لشبكة حالة دراسية وقابلة للتكييف مع عمليات مركزه.