



دورة مركز عمليات الشبكات NOC المستوى الأول: مراقبة الشبكات والإنذارات ونظام التذاكر واستكشاف الأعطال



دورة مركز عمليات الشبكات NOC المستوى الأول: مراقبة الشبكات والإنذارات ونظام التذاكر واستكشاف الأعطال

مقدمة:

دورة مركز عمليات الشبكات NOC المستوى الأول، بمحاورها في مراقبة الشبكات والإنذارات ونظام التذاكر واستكشاف الأعطال، تمتد 5 أيام وتخاطب الموظفين الجدد في عمليات الشبكات ومكاتب الخدمة والدعم الفني للبنية التحتية، وتنتهي بدليل مناوبة المستوى الأول. فالإنذارات الفائتة والتذاكر المبهمة والتصعيد المتأخر تطيل مدة الانقطاع وتحمل كبار المهندسين أعطالا روتينية. ويستخدم المشاركون الحاسوب وأساسيات الشبكات في عملهم لكنهم جدد على المراقبة على مدار الساعة، ويتعلمون في مختبر عملي على لوحات مراقبة فعلية ونظام تذاكر وأعطال شبكية محاكاة. وتقدم كور كونسبت هذه الدورة العملية لمشغلي مركز عمليات الشبكات.

أهداف الدورة:

- متابعة سلامة الأجهزة والوصلات والخدمات على لوحات أنظمة إدارة الشبكة مثل Zabbix و PRTG و SolarWinds ورصد القراءات غير الطبيعية مبكرا
- الإقرار بالإنذارات وتصنيفها وترتيب أولويتها حسب الخطورة وأثرها على الخدمة اعتمادا على إشعارات SNMP وسجلات Syslog
- فتح تذاكر الحوادث وتحديثها وإغلاقها في ServiceNow أو Jira Service Management بسجلات واضحة ومكتملة
- تنفيذ استكشاف الأعطال في المستوى الأول بأمر ping و traceroute وفحص المنافذ لعزل أعطال الوصلات والطاقة والأجهزة
- تصعيد الأعطال إلى المستويين الثاني والثالث وفرق الموردين مع الأدلة التي يحتاجونها وفق دليل التشغيل
- تسليم المناوبة بملاحظات حالة دقيقة وإعداد دليل مناوبة المستوى الأول للاستخدام اليومي

الفئة المستهدفة:

- الموظفون المكلفون حديثا بمراقبة الشبكات والخدمات على مدار الساعة في مركز العمليات
- موظفو مكتب الخدمة والدعم الفني المسؤولون عن التعامل الأولي مع حوادث الشبكة
- الفنيون المبتدئون في الشبكات والأنظمة المسؤولون عن عزل الأعطال البسيطة وفحص الأجهزة
- موظفو عمليات الاتصالات ومراكز البيانات المسؤولون عن متابعة إنذارات الوصلات والطاقة والبيئة
- الخريجون التقنيون الجدد المنضمون إلى فرق العمليات المسؤولة عن المراقبة وتسجيل الحوادث

محاورة الدورة:

اليوم 1: دور مركز عمليات الشبكات وأساسيات الشبكات وبيئة المراقبة

- نموذج مستويات الدعم الأول والثاني والثالث ومسؤوليات كل مستوى
- عناوين TCP/IP والشبكات الفرعية والمنافذ لموظفي المراقبة
- أساسيات VLAN والتوجيه لقراءة خرائط الشبكة
- مخططات طوبولوجيا الشبكة وجولة على سجل الأجهزة
- جولة على لوحة نظام إدارة الشبكة وألوان الحالة

اليوم 2: بروتوكولات المراقبة وأدواتها وعملية إدارة الحوادث

- استطلاع SNMP وإشعارات Traps وقيم MIB
- بنية رسائل Syslog ومستويات الخطورة ومراجعة السجلات
- عروض المضيفات والمحفزات في Nagios و PRTG و Zabbix
- أساسيات إدارة الحوادث والأحداث والمشكلات وفق ITIL
- ربط أثر الخدمة من الجهاز إلى خدمة العميل

اليوم 3: فرز الإنذارات والتعامل مع التذاكر

- إجراء الإقرار بالإنذار وتصنيف درجة خطورته
- التعرف على الإنذارات المكررة والمتذبذبة والمتراكبة
- دورة حياة التذكرة في Jira Service Management و ServiceNow
- كتابة تذكرة الحادث بالأعراض والأثر والتسلسل الزمني
- قوالب رسائل تحديث الحالة للعملاء وأصحاب المصلحة

اليوم 4: استكشاف الأعطال في المستوى الأول وحالات التصعيد

- تسلسل عزل الأعطال بأمر ping و traceroute
- فحص حالة المنافذ وعدادات الأخطاء والمعالج والذاكرة
- حالات انقطاع الوصلة وقطع الألياف وانقطاع الطاقة
- تنفيذ خطوات دليل التشغيل وإجراءات التشغيل القياسية
- مسار التصعيد إلى المستويين الثاني والثالث ودعم الموردين

اليوم 5: مناوبة عملية في المختبر ودليل مناوبة المستوى الأول

- قائمة بدء المناوبة في المختبر وفحص سلامة اللوحات
- تمرين مختبري لفرز موجة إنذارات وإنشاء التذاكر
- تمرين مختبري لعزل عطل وتسليمه للتصعيد
- كتابة مذكرة تسليم المناوبة ومراجعتها مع الزملاء
- استكمال دليل مناوبة المستوى الأول ومراجعتها

المهارات التي ستكتسبها:

- مراقبة سلامة الشبكة
- فرز الإنذارات حسب الخطورة
- قراءة إشعارات SNMP وسجلات Syslog
- توثيق تذاكر الحوادث
- عزل الأعطال في المستوى الأول
- التصعيد المنظم
- إعداد تقارير تسليم المناوبة

لماذا تحضر هذه الدورة:

- تسليم دليل مناوبة المستوى الأول إلى مشرف مركز العمليات ورئيس هندسة المستوى الثاني، ومعه قوائم الفرز والتذاكر واستكشاف الأعطال
- البت فيما إذا كان الإنذار يحتاج إلى تذكرة أو فترة متابعة أو تصعيد فوري
- تفادي الإنذارات الفائتة والتذاكر المكررة والتصعيد المتأخر الذي يطيل الانقطاع ويثقل كاهل كبار المهندسين
- توجيه الزملاء الجدد في استخدام اللوحات وقوائم التذاكر وتسلسل عزل الأعطال الذي طبق في المختبر

الخاتمة:

بعد العودة إلى العمل يسلم المشاركون دليل مناوبة المستوى الأول إلى مشرف مركز العمليات ورئيس هندسة المستوى الثاني. وتستند الوحدة إليه في الاتفاق على الإنذارات التي يعالجها المستوى الأول وحده، وحقوق التذكرة التي يجب استكمالها قبل التصعيد، والفحوص الأولية التي تسبق الاتصال بالموارد. وبعد الشهر الأول من المناوبات تأخذ الوحدة عينة من التذاكر المغلقة، وتقرن حالات التصعيد بقواعد الفرز في الدليل، ثم تحدث القوائم حيث فاتت أعطال أو صعدت قبل أوانها.

الأسئلة الشائعة:

ما الذي يحتاجه المشارك قبل دورة مركز عمليات الشبكات NOC المستوى الأول؟

يحتاج المشارك إلى مهارات حاسوبية أساسية وتصور عام لمفهوم الشبكة، ولا تشترط خبرة سابقة في مراكز العمليات. ويفيد الإلمام بعناوين IP، وراجع اليوم الأول أساسيات TCP/IP اللازمة لقراءة لوحات المراقبة.

بم تختلف دورة مركز عمليات الشبكات NOC المستوى الأول عن دورات إدارة مراكز العمليات؟

تدرب هذه الدورة المشغل على العمل أمام الشاشة: متابعة اللوحات وفرز الإنذارات وكتابة التذاكر وإجراء الفحوص الأولية. أما دورات الإدارة فتتناول تصميم قواعد الإنذار وجدول المناوبات ومستويات الخدمة وتقارير الأداء للمشرفين والمديرين.

لماذا تركز دورة مركز عمليات الشبكات على فرز الإنذارات قبل استكشاف الأعطال؟

لأن معظم الانقطاعات تظهر أولاً في صورة سيل من الإنذارات. والمشغل الذي يصنفها حسب الخطورة وأثرها على الخدمة يصل إلى العطل الحقيقي أسرع، ويتجنب التذاكر المكررة، ويصعد المشكلة الصحيحة أولاً، فتقصر مدة الانقطاع.

ماذا يعود به المشارك من دورة مركز عمليات الشبكات NOC المستوى الأول؟

يعود المشارك بدليل مناوبة المستوى الأول، ومعه قائمة بدء المناوبة ومصفوفة فرز الإنذارات وقوالب التذاكر وتسلسل عزل الأعطال وجهات التصعيد ونموذج تسليم المناوبة.