BLACKBIRD FOR TRAINING

دورة عمليات الشبكات واستكشاف أخطائها: ACI

Palo Altog F5g Catalyst Centerg SD-WANg Cisco



دورة عمليات الشبكات واستكشاف أخطائها: Palo Altog F5g Catalyst Centerg SD-WANg Cisco ACI

مقدمة:

عمليات الشبكات واستكشاف أخطائها هي العمل اليومي الذي يحافظ على سلامة نسيج مراكز البيانات وروابط الشبكات الواسعة ووحدات تسليم التطبيقات وجدران الحماية، ويعزل الأعطال ويصلحها عند توقف الخدمات. تقدم بلاك بيرد للتدريب هذه الدورة على مدى أسبوع لمهندسي الشبكات ومراكز البيانات والشبكات الواسعة وجدران الحماية، وفرق التشغيل في مراكز NOC وSOC، ومعماريي البنية التحتية وقادة الفرق، ويخرج كل مشارك بدليل تشغيلي لاستكشاف الأعطال عبر منصات متعددة الموردين. والدورة مكثفة بمستوى متقدم، موجهة لمن يعرف أساسيات Cisco ACI وCisco Catalyst SD-WANg Cisco Catalyst Centerg F5 BIG-IPg وجدران Palo Alto Networks، وتعتمد على مختبرات عملية يومية.

أهداف الدورة:

- تفسير أعطال Cisco ACI وأحداثها ودرجات السلامة وقواعد التقسيم لعزل مشكلات نقاط النهاية والعقود وL3Outg في نسيج قيد التشغيل
- التمييز بين أعطال مستوى التحكم وأعطال مستوى البيانات في Cisco Catalyst SD-WAN، وتطبيق السياسات المركزية والمحلية وخصائص الأمن تطبيقا صحيحا
- تطبيق لوحات السلامة وتتبع المسار والالتقاط الذكي في Cisco Catalyst Center Assurance لتحديد سبب مشكلة يبلغ عنها مستخدم أو تطبيق
- المقارنة بين خيارات موازنة الأحمال والاستمرارية والمراقبة في F5 BIG-IP LTM، واختيار نهج سياسة F5 Advanced WAF الملائم لتطبيق محدد
- تطبيق فهم مسار الحزم في PAN-OS والعدادات والتقاط الحزم للفصل بين أسباب إسقاط الحركة الناتجة عن التوجيه أو NAT أو السياسة أو App-ID
- تبرير تسلسل عزل متكامل عبر المنصات وتوثيقه في دليل تشغيلي تتبعه فرق التشغيل أثناء الحوادث



الفئة المستهدفة:

- مهندسو شبكات مراكز البيانات الذين يشغلون نسيج Cisco ACI، ويقررون هل يقع العطل في نموذج السياسات أم في سياسات الوصول أم في النسيج المادي
- مهندسو الشبكات الواسعة والفروع الذين يديرون شبكات Cisco Catalyst SD-WAN، ويحكمون على أي سياسة أو نفق أو حالة متحكم تضعف أداء تطبيق
- مهندسو أمن الشبكات وجدران الحماية الذين يديرون F5 Advanced WAF وجدران Palo Alto Networks، ويقررون هل الحظر هجوم حقيقي أم خطأ في السياسة
- فرق التشغيل في مراكز NOC وSOC الذين يفرزون التنبيهات الواردة من Cisco Catalyst Center وغيرها، ويختارون الفريق والمنصة التي يصعد إليها الحادث
- معماريو البنية التحتية وقادة فرق التشغيل الذين يضعون معايير استكشاف الأعطال، ويقررون خطوات العزل التي يتضمنها الدليل التشغيلي المشترك

محاور الدورة:

اليوم 1: تشغيل Cisco ACI واستكشاف أعطاله: النسيج ونموذج السياسات ونقاط النهاية

- واجهة APIC الرسومية وسطر الأوامر وأداة moquery: قراءة الكائنات المدارة أثناء التشغيل
- الأعطال مقابل الأحداث مقابل سجلات التدقيق: تتبع ما تغير ومتى
- درجات السلامة واكتشاف النسيج: تشخيص مشكلات المبدلات الطرفية والفقرية والمتحكمات
- تعلم نقاط النهاية والعقود: التحقق من قواعد التقسيم بين مجموعات نقاط النهاية
- اتصال L3Out ومرآة SPAN والعدادات الذرية: عزل أعطال التوجيه الخارجي وفقد الحزم

اليوم 2: تشغيل Cisco Catalyst SD-WAN واستكشاف أعطاله والسياسات المتقدمة والأمن

- Validatorg Controllerg SD-WAN Manager: أعطال انضمام مستوى التحكم والشهادات الرقمية
- جلسات OMP وTLOC وBFD: التحقق من مسارات الشبكة المتراكبة وسلامة الأنفاق
- السياسة المركزية مقابل السياسة المحلية: الطوبولوجيا والتوجيه الواعي بالتطبيقات وجودة الخدمة
- جدار الحماية المؤسسي ومنع التسلل وتصفية العناوين: تأمين الفروع ذات الوصول المباشر للإنترنت
- الممارسات المعتمدة في SD-WAN: تنظيم القوالب وتسلسل الترقيات وخطوط الأساس للمراقبة



اليوم 3: تنفيذ Cisco Catalyst Center وإدارته لأغراض Assurance

- بنية Catalyst Center والاكتشاف: الجرد والمواقع ومتطلبات تهيئة الأجهزة المسبقة
- سلامة الشبكة مقابل سلامة العملاء: تفسير لوحات Assurance ودرجاتها
- مشكلات Assurance والرؤى المدعومة بالذكاء الاصطناعي: ترتيب أولوية الأعطال السلكية واللاسلكية المتكررة
- تتبع المسار واختبارات المستشعرات والالتقاط الذكي: إثبات موضع تراجع تجربة المستخدم
- إدارة Assurance: العتبات والإشعارات والصلاحيات المبنية على الأدوار وإعدادات التكامل

اليوم 4: تهيئة F5 BIG-IP LTM وتهيئة F5 Advanced WAF

- الخوادم الافتراضية والمجمعات وأدوات المراقبة في BIG-IP LTM: بناء تسليم تطبيقات مرن
- الاستمرارية مقابل أساليب موازنة الأحمال: الملفات التعريفية وSNAT وقرارات تفريغ SSL
- قواعد iRules والتوافر العالي: منطق توجيه الحركة والتحويل التلقائي بين مجموعات الأجهزة
- نموذج الأمن الإيجابي مقابل السلبي: أداة Policy Builder وتواقيع الهجمات في Advanced WAF
- ضبط Advanced WAF: مقترحات التعلم والحماية من الروبوتات ومعالجة الإنذارات الكاذبة

اليوم 5: استكشاف أعطال جدران Palo Alto Networks ومختبر حالة متكاملة متعددة الموردين

- مسار الحزم في PAN-OS والعدادات والتقاط الحزم: تحديد المرحلة التي تسقط فيها الحركة
- الحركة الموجهة للجهاز مقابل الحركة العابرة: استكشاف أعطال NAT وApp-ID وفك التشفير وUser-ID
- حالة مختبرية متكاملة: تتبع انقطاع تطبيق عبر نسيج ACI وشبكة SD-WAN
- الربط بين المنصات: مطابقة بيانات Catalyst Center Assurance مع سجلات BIG-IP وسجلات حركة الجدار
- الدليل التشغيلي لاستكشاف الأعطال متعددة الموردين: استكمال خطوات العزل والأوامر ومسارات التصعيد

المهارات التي ستكتسبها:

- تحليل أعطال APIC
- التحقق من قواعد التقسيم
- تشخيص الشبكات المتراكبة في SD-WAN
- تفسير بيانات Assurance
- تهيئة تسليم التطبيقات
- ضبط جدار حماية تطبيقات الويب
- تحليل مسار الحزم في PAN-OS
- عزل الأعطال عبر المنصات



لماذا تحضر هذه الدورة:

- من الاستجابة لتنبيهات كل وحدة تحكم على حدة إلى قراءة بيانات السلامة في Catalyst Centerg ACI دليلا على موضع العطل
- من تعديل سياسات SD-WAN وجدران الحماية بالتجربة والخطأ إلى توقع سلوك كل سياسة قبل نشرها
- من تخفيف سياسات WAF لإيقاف شكاوى المستخدمين إلى ضبط التواقيع ومقترحات التعلم مع توثيق سبب كل تغيير
- من تصعيد الحوادث بين فرق الموردين دون أدلة إلى اتباع دليل تشغيلي لاستكشاف الأعطال متعددة الموردين بخطوات عزل محددة

الخاتمة:

يعني التشغيل المتقن لشبكة متعددة الموردين تحويل التنبيهات المتفرقة من وحدات تحكم عديدة إلى سلسلة أدلة مرتبة تشير إلى الطبقة المعطلة. وتوضح الدورة الفرق بين أعطال السياسات وأعطال النسيج أو الأنفاق، وبين أعراض مستوى التحكم وأعراض مستوى البيانات، وبين الهجوم الحقيقي وسياسة الأمن المهيأة خطأ. وتناسب المهندسين وفرق التشغيل الذين يعملون يوميا على منصات Cisco وF5g وPalo Alto Networks، ويحتاجون إلى عزل أسرع وقابل للتكرار عبرها جميعا أثناء الحوادث الفعلية.

الأسئلة الشائعة:

ما الذي يحتاج المهندس إلى معرفته قبل الالتحاق بدورة عمليات الشبكات واستكشاف أخطائها؟

يحتاج المشارك إلى خبرة أساسية في تهيئة منصتين على الأقل من المنصات المشمولة، وإلى إلمام جيد بالتوجيه والتبديل وبروتوكولات TCP/IP والعمل عبر سطر الأوامر. ولا تتناول الدورة التثبيت الأولي، بل تنتقل مباشرة إلى التشغيل والأعطال والعزل داخل المختبرات.

ما الفرق بين دورة عمليات الشبكات واستكشاف أخطائها ودورة تنفيذ لمنصة مورد واحد؟

تركز هذه الدورة على تشغيل منصات قائمة فعلا وإصلاحها عبر عدة موردين، لا على بناء منصة واحدة من الصفر. ويتناول كل يوم أهم الأعطال وخطوات الفحص، ثم يجمعها اليوم الأخير في حادث واحد يمتد عبر المنصات.

لماذا تصعب عمليات الشبكات واستكشاف أخطائها عبر منصات Cisco ACI وSD-WANg F5g وPalo Altog؟

لأن لكل منصة نموذج سياسات وسجلات ومصطلحات خاصة تخفي الأعطال خلفها، فيبدو الانقطاع الواحد كأنه أربع مشكلات منفصلة. ومن دون ترتيب متفق عليه للعزل تفحص الفرق الطبقات نفسها مرارا، وتصعد الحوادث بين الموردين دون أدلة.



ماذا يعود به المشارك إلى عمله من دورة عمليات الشبكات واستكشاف أخطائها؟

يعود المشارك بدليل تشغيلي لاستكشاف الأعطال متعددة الموردين يحدد خطوات العزل والأوامر الأساسية ومصادر السجلات ونقاط التصعيد لكل منصة، إضافة إلى خبرة مختبرية في تطبيقه على انقطاع واقعي يمتد عبر مراكز البيانات والشبكة الواسعة وتسليم التطبيقات وجدران الحماية.

