CONCEPT

التعافي من كوارث تقنية المعلومات والمرونة التشغيلية



التعافي من كوارث تقنية المعلومات والمرونة التشغيلية

العمق التقني: ممارس · **أسلوب التطبيق:** محاكاة

مقدمة

باتت هجمات برامج الفدية وانقطاعات الخدمات السحابية وأعطال مراكز البيانات توقف خدمات أعمال كاملة، في حين تعتمد خطط تعاف كثيرة على نسخ احتياطية لا يمكن استعادتها، وتسلسلات لم يتدرب عليها أحد، ومزودين لم يقيموا قط. ولم يعد مجلس الإدارة والمدققون يسألون عن وجود وثيقة للتعافي، بل عن قدرة الخدمات المهمة على البقاء ضمن حدود التعطل المقبولة. تزود هذه الدورة من كور كونسبت مديري تقنية المعلومات والمرونة بمهارات تصميم قدرات التعافي وتوثيقها واختبارها وفق المعايير الدولية. ويتدرب المشاركون على قرارات التعافي في تمارين محاكاة تحت ضغط الوقت، ويخرجون بخطة التعافي من كوارث تقنية المعلومات وجدول اختبارات المرونة لخدمة حيوية.

أهداف الدورة

- تحديد خدمات الأعمال المهمة ورسم الاعتماديات التقنية والبيانات والأطراف الثالثة التي تقوم عليها
- تطبيق ISO/IEC 27031 وNIST SP 800-34 لهيكلة برنامج جاهزية تقنية المعلومات والاتصالات وخطط الطوارئ
- اختيار بنى التعافي واستراتيجيات النسخ الاحتياطي التي تحقق أهداف زمن التعافي ونقطة التعافي المتفق عليها
- كتابة أدلة تشغيل للتعافي قابلة للتنفيذ وتحديد الأدوار ومعايير إعلان الكارثة، بما في ذلك الهجمات السيبرانية
- تخطيط اختبارات التعافي وتقييمها ومراجعة مرونة المزودين ومعالجة ما بعد الحوادث
- إعداد خطة التعافي من كوارث تقنية المعلومات وجدول اختبارات المرونة لخدمة حيوية

الفئة المستهدفة

- مديرو البنية التحتية والعمليات التقنية المسؤولون عن توافر المنصات
- مديرو التعافي من الكوارث واستمرارية خدمات تقنية المعلومات
- مديرو أمن المعلومات المسؤولون عن التعافي من الحوادث وضمان النسخ الاحتياطي
- مديرو الحوسبة السحابية ومراكز البيانات المشرفون على ترتيبات الاستضافة والتحويل
- مديرو مخاطر تقنية المعلومات والمرونة التشغيلية المسؤولون عن تقارير قدرات التعافي
- مالكو التطبيقات والخدمات المسؤولون عن أنظمة الأعمال الحيوية

محاور الدورة

اليوم الأول: أسس التعافي التقني والمرونة التشغيلية

- مفهوما خدمات الأعمال المهمة وحدود تحمل التعطل
- نظرة عامة على مبادئ لجنة بازل BCBS للمرونة التشغيلية
- رسم اعتماديات خدمات تقنية المعلومات: التطبيقات والبنية التحتية والبيانات والأطراف الثالثة
- دليل سيناريوهات التعطل: برامج الفدية وفقدان الموقع وانقطاع المنطقة السحابية وإخفاق المورد
- قائمة التقييم المرجعي لقدرات التعافي

اليوم الثاني: المعايير وبنية التعافي

- جاهزية تقنية المعلومات والاتصالات لاستمرارية الأعمال وفق ISO/IEC 27031:2025
- عملية التخطيط للطوارئ وفق NIST SP 800-34
- ضوابط ISO/IEC 27001:2022 رقم 5.30 و8.13 و8.14 لاستمرارية تقنية المعلومات والنسخ الاحتياطي والتكرار
- ممارسة إدارة استمرارية الخدمة في ITIL 4
- أنماط بنية التعافي: النسخ والاستعادة والتشغيل الأدنى Pilot Light والاستعداد الدافئ والتشغيل النشط المزدوج

اليوم الثالث: بناء قدرة التعافي

- مواءمة أهداف التعافي: RTO وRPO وتسلسل التعافي حسب الخدمة
- تصميم استراتيجية النسخ الاحتياطي بقاعدة 3-2-1-1-0 والنسخ غير القابلة للتعديل
- كتابة أدلة التشغيل للتحويل والعودة واستعادة البيانات
- أدوار التعافي وشجرة الاتصال ومعايير إعلان الكارثة
- تخطيط التعافي السيبراني بوظيفة Recover في NIST CSF 2.0 والدليل SP 800-184

اليوم الرابع: الاختبار ومخاطر المزودين والتحسين

- أنواع اختبارات التعافي: المراجعة الإجرائية واستعادة المكونات والتشغيل المتوازي والانقطاع الكامل
- هندسة الفوضى Chaos Engineering وحقن الأعطال المضبوط
- العناية الواجبة لمرونة مزودي الخدمات السحابية والمسندة وخطط الخروج
- مقاييس التعافي: نسبة نجاح الاختبارات وزمن التعافي المحقق وحجم فقدان البيانات المقاس
- مراجعة ما بعد الحادث وسجل متابعة المعالجة

اليوم الخامس: المحاكاة وخطة التعافي من كوارث تقنية المعلومات

- محاكاة التعافي من برامج الفدية: قرارات الاستعادة في بيئة نظيفة
- محاكاة فقدان الموقع: تسلسل التحويل تحت ضغط الوقت
- استخلاص الدروس من المحاكاة مقارنة بحدود تحمل التعطل
- إعداد مسودة خطة التعافي من كوارث تقنية المعلومات لخدمة حيوية من مؤسسة المشارك
- بناء جدول اختبارات المرونة ومراجعته مع الزملاء

المهارات المكتسبة

- رسم اعتماديات الخدمات
- اختيار بنية التعافي
- تصميم استراتيجية النسخ الاحتياطي
- إعداد أدلة تشغيل التعافي
- تخطيط التعافي السيبراني
- إدارة اختبارات التعافي
- تقييم مرونة المزودين
- تحديد حدود تحمل التعطل

لماذا تحضر هذه الدورة

- تعود بخطة التعافي من كوارث تقنية المعلومات وجدول اختبارات المرونة لخدمة حيوية، بعد مراجعتها مع الزملاء
- تخوض قرارات التعافي تحت ضغط الوقت قبل أن تواجهها في انقطاع حقيقي
- تقدم لمالكي الخدمات والمدققين ومجلس الإدارة أدلة على إمكانية تحقيق أهداف التعافي فعلا
- تتعلم من مديري البنية التحتية والأمن في قطاعات البنوك والاتصالات والجهات الحكومية والصناعة

الخاتمة

لا تثبت قدرة التعافي إلا باستعادة الخدمات ضمن الحدود المتفق عليها. تنتقل هذه الدورة من خدمات الأعمال المهمة ورسم الاعتماديات، مرورا بمعايير جاهزية تقنية المعلومات وبنى التعافي، وصولا إلى أدلة التشغيل وتصميم النسخ الاحتياطي والتعافي السيبراني والاختبار ومرونة المزودين. ويضع اليوم الأخير المشاركين في محاكاة لهجوم برامج الفدية وفقدان الموقع، ثم يحول الدروس إلى خطة التعافي من كوارث تقنية المعلومات وجدول اختبارات المرونة، فيمتلكون أساسا مختبرا لإثبات قدرتهم على استعادة الخدمات الحيوية وقت الحاجة.