BLACKBIRD FOR TRAINING

دورة أمن البنية التحتية السحابية للمؤسسات وإدارة مخاطرها

November 2027 18 – 14

القاهرة (مصر)



دورة أمن البنية التحتية السحابية للمؤسسات وإدارة مخاطرها

المرجع: 363802_104 **التاريخ:** 14 – 18 November 2027 **المكان:** القاهرة (مصر) **الرسوم:** GBP 4900

مقدمة:

تمنحك دورة أمن البنية التحتية السحابية للمؤسسات وإدارة مخاطرها على مدى أسبوع القدرة على تقييم المنصات السحابية التي تعتمد عليها مؤسستك وحمايتها وحوكمتها، بدءا من الهويات والشبكات وصولا إلى أحمال العمل والبيانات والموردين. ستعد خلالها خطة مخاطر وحوكمة لأمن البنية التحتية السحابية تربط كل خطر محدد بضابط واضح ومالك مسؤول وهدف للتعافي. يكفي أن تكون لديك خبرة عملية في الخدمات السحابية أو تشغيل البنية التحتية، وفهم أساسي للشبكات والهوية ومفاهيم الأمن. وتتدرب عبر دراسات حالة تعمل فيها على مخططات معمارية وملفات إعدادات وردود موردين وتسلسلات حوادث مأخوذة من قطاعات متعددة.

أهداف الدورة:

- مطابقة بيئتك السحابية مع نموذج المسؤولية المشتركة CSA Shared Security Responsibility Model وتقييم مخاطرها في سجل يعتمد مصفوفة الاحتمالية والأثر.
- صياغة قواعد دورة حياة الهوية والوصول المميز لحساباتك السحابية بالاستناد إلى إرشادات NIST SP 800-210 الخاصة بضبط الوصول.
- بناء مصفوفة ضوابط لعزل الشبكات وحماية البيانات في أحمال عملك باستخدام ضوابط ISO/IEC 27017 المخصصة للخدمات السحابية.
- اختبار إعدادات أحمال العمل مقابل خطوط الأساس المعتمدة باستخدام قواعد السياسات البرمجية ونتائج فحص الوضع الأمني.
- تقييم موردیك السحابيين باستبيان مبني على مصفوفة CCM وإعداد دليل تشغيل للحوادث يخدم فريق المراقبة لديك.
- عرض خطة للمرونة والامتثال تربط ضوابطك بأهداف التعافي وبأدلة الامتثال وفق ISO/IEC 27001 لأنظمة إدارة أمن المعلومات.



الفئة المستهدفة:

- أنت تبني البنية التحتية السحابية أو الشبكات أو بيئات الإطلاق وتشغلها، وتحتاج إلى ضوابط أمنية تصمد في بيئة الإنتاج.
- أنت تحلل التنبيهات الأمنية أو تراجع التصاميم المعمارية أو تصمم ضوابط لأحمال العمل والخدمات السحابية.
- أنت تقيم مخاطر تقنية المعلومات أو تجمع أدلة الامتثال أو ترد على طلبات التدقيق المتعلقة بالخدمات السحابية في مؤسستك.
- أنت تقود فريق منصة سحابية أو فريق عمليات، وتقرر أي المخاطر تعالج أو تقبل أو تصعد.
- أنت تراجع الموردين السحابيين أو العقود أو التكاملات، وتحتاج إلى طريقة منظمة للحكم على مستوى أمنهم.

محاور الدورة:

اليوم 1: تقييم البيئات السحابية للمؤسسات ومتطلبات المخاطر

- مطابقة نماذج الخدمة السحابية مع نموذج المسؤولية المشتركة
- تحليل التهديدات السحابية للمؤسسة باستخدام لوحة نمذجة التهديدات
- تقييم مخاطر البنية التحتية السحابية بمصفوفة الاحتمالية والأثر
- استخلاص المتطلبات الأمنية من مجالات CSA Cloud Controls Matrix
- البناء: جرد الأصول السحابية وسجل المخاطر الأولي

اليوم 2: تصميم ضوابط الهوية وتأمين الاتصال السحابي

- تصميم مسارات دورة حياة الهوية للموظفين الجدد والمنتقلين والمغادرين
- تطبيق إرشادات NIST SP 800-210 لضبط الوصول على الأدوار السحابية
- ضبط الوصول المميز بالرفع المؤقت للصلاحيات وتسجيل الجلسات
- تقسيم الشبكات السحابية باستخدام النقاط الطرفية الخاصة ومجموعات الأمان
- البناء: مصفوفة ضوابط الهوية وعزل الشبكات

اليوم 3: حماية البيانات السحابية وتحصين أحمال العمل

- تصنيف البيانات السحابية بمصفوفة للتشفير وإدارة المفاتيح
- تطبيق ضوابط ISO/IEC 27017 على الاحتفاظ بالبيانات وحذفها
- تحصين الأجهزة الافتراضية والحاويات وفق خطوط أساس الإعدادات المعتمدة
- رصد انحراف الإعدادات بالسياسات البرمجية وفحوص الوضع الأمني
- البناء: قائمة تحقق لحماية البيانات وتحصين أحمال العمل



اليوم 4: تحليل مخاطر الأطراف الثالثة وتنسيق الحوادث السحابية

- تقييم مزودي الخدمات السحابية باستبيان أمني مبني على CCM
- تتبع مخاطر سلسلة الإمداد عبر الاعتماديات وتكاملات الأطراف الثالثة
- تجميع سجلات التدقيق السحابية في مسار موحد للمراقبة الأمنية
- إدارة فرز الحوادث السحابية بدليل تصعيد مشترك
- البناء: بطاقة تقييم مخاطر الأطراف الثالثة ودليل تشغيل الحوادث السحابية

اليوم 5: دراسة حالة: اختبار المرونة واستكمال الحوكمة السحابية

- اختبار أهداف زمن التعافي ونقطة التعافي مقابل سجل مخاطرك
- محاكاة انقطاع خدمة سحابية باستخدام دليل تشغيل الحوادث
- ربط مصفوفة ضوابطك بأدلة الامتثال وفق ISO/IEC 27001
- عرض المخاطر المتبقية وقرارات الحوكمة أمام لجنة مراجعة
- البناء: خطة مخاطر وحوكمة أمن البنية التحتية السحابية

المهارات التي ستكتسبها:

- مطابقة المسؤولية المشتركة
- تقييم سجل المخاطر السحابية
- تصميم الوصول المميز
- تخطيط تقسيم الشبكات
- إدارة مفاتيح التشفير
- رصد انحراف الإعدادات
- تقييم أمن الموردين
- تصعيد الحوادث السحابية

لماذا تحضر هذه الدورة:

- قيم مخاطر سحابية حقيقية في سجل تعيد استخدامه لبيئتك في الأسبوع التالي.
- تدرب على التعامل مع انقطاع سحابي باستخدام دليل تشغيل الحوادث الخاص بك قبل أن تحتاجه فعليا.
- قارن ردود الموردين باستبيان ترسله إلى مزودك السحابي القادم.
- عد بخطة مخاطر وحوكمة لأمن البنية التحتية السحابية جاهزة للعرض على مالكي المنصات لديك.



الخاتمة:

في أسبوعك الأول بعد دورة بلاك بيرد للتدريب، افتح خطة المخاطر والحوكمة واستبدل بيانات دراسة الحالة بحساباتك وأحمال عملك ومورديك، مبتدئا بأعلى ثلاثة مخاطر في تقييمك. اعرض مصفوفة الضوابط على مالك المنصة ومسؤول الأمن وزميلك في المخاطر أو الامتثال، واتفقوا على مالك وموعد مستهدف لكل إجراء معالجة. وبعد تطبيق أول تغيير، تحقق من وصول السجلات المرتبطة به إلى مسار المراقبة، ومن أن مسار التصعيد في دليل التشغيل ما زال يعمل، ومن أن الأدلة التي ربطتها تنتج فعلا.

الأسئلة الشائعة:

ما الذي ستتمكن من فعله بعد دورة أمن البنية التحتية السحابية للمؤسسات وإدارة مخاطرها؟

ستتمكن من تقييم مخاطر البنية التحتية السحابية، وتصميم ضوابط الهوية والشبكات والبيانات وأحمال العمل، وتقييم الموردين السحابيين، وتنسيق الاستجابة للحوادث، وربط ضوابطك بأهداف التعافي وأدلة الامتثال، وكل ذلك في خطة واحدة للمخاطر والحوكمة تطبقها على منصاتك.

ما المعرفة التي تحتاجها قبل بدء تدريب أمن البنية التحتية السحابية وإدارة المخاطر؟

تحتاج إلى خبرة عملية في منصة سحابية واحدة على الأقل أو في تشغيل البنية التحتية، مع فهم أساسي لمصطلحات الشبكات والهوية والأمن. لا يلزمك تدريب سابق في إدارة المخاطر، فالدورة تعلمك تقييم المخاطر ومعالجتها خطوة بخطوة.

ماذا تبني خلال دورة أمن البنية التحتية السحابية وإدارة المخاطر؟

تبني خطة مخاطر وحوكمة لأمن البنية التحتية السحابية. يضيف كل يوم جزءا منها: جرد الأصول وسجل المخاطر، ثم مصفوفة الهوية والعزل، فقائمة تحقق التحصين، فبطاقة تقييم الموردين ودليل الحوادث، وأخيرا أهداف التعافي وربط الامتثال.

كيف تختلف دورة أمن البنية التحتية السحابية وإدارة المخاطر عن دورات المخاطر العامة أو دورات الشهادات؟

تتناول دورات المخاطر المؤسسية العامة المخاطر على مستوى المؤسسة كلها، وتتبع دورات الشهادات منهج اختبار محددا. أما هذه الدورة فتركز على البنية التحتية السحابية، وتجمع الضوابط العملية مع تقييم المخاطر والحوكمة، ليعمل المهندسون والمحللون وموظفو المخاطر على خطة واحدة.

