CONCEPT

حماية المعلومات ومنع تسرب البيانات في Purview Microsoft: تسميات الحساسية والتسمية التلقائية

28 مارس – 1 أبريل 2027

الرياض - فندق خمس نجوم في حي كافد

حماية المعلومات ومنع تسرب البيانات في Microsoft Purview: تسميات الحساسية والتسمية التلقائية

المرجع: 18655_673 **التاريخ:** 28 مارس – 1 أبريل 2027 **المكان:** الرياض - فندق خمس نجوم في حي كافد **الرسوم:** SAR 20000

مقدمة:

تزداد الحاجة إلى حماية المعلومات ومنع تسرب البيانات في Microsoft Purview لأن الملفات والرسائل الحساسة تغادر بيئات 365 Microsoft يوميا عبر البريد المعاد توجيهه وروابط المشاركة المفتوحة ومحادثات Teams والنسخ إلى وحدات USB، دون أن يعرف أحد أي العناصر سرية. فالتسميات موجودة على الورق ولا تطبق، وقواعد DLP إما لا تمنع شيئا أو تمنع كل شيء. تدرب هذه الدورة من كور كونسبت المسؤولين على تصنيف المحتوى ونشر تسميات الحساسية وفرض سياسات منع فقدان البيانات على البريد والملفات والمحادثات والأجهزة والاحتفاظ بما يجب حفظه. ويبني المشاركون تصميما لحماية المعلومات ومنع التسرب لمؤسسة نموذجية.

أهداف الدورة:

- تحديد مواقع المحتوى الحساس في بيئة Microsoft 365 باستخدام أنواع المعلومات الحساسة والمصنفات القابلة للتدريب ومستكشف المحتوى ومستكشف النشاط
- تصميم هيكل تسميات الحساسية ونشره مع سياسات التسميات والعلامات المرئية وقيود الوصول وإعدادات التشفير
- ضبط التسمية التلقائية من جهة العميل ومن جهة الخدمة لتصل التسميات إلى المستندات والبريد دون الاعتماد على المستخدمين
- بناء سياسات Microsoft Purview DLP وضبطها لخدمات Exchange وSharePoint وOneDrive وTeams وأجهزة Windows الطرفية مع تلميحات السياسة والتجاوزات وتنبيهات الحوادث
- تطبيق سياسات الاحتفاظ وتسميات الاحتفاظ وإعدادات السجلات، واستخدام بحث التدقيق وإشارات المخاطر الداخلية وحالات eDiscovery للتحقيق في حوادث البيانات
- إعداد تصميم لحماية المعلومات ومنع التسرب يربط الضوابط التقنية بمستويات تصنيف البيانات وواجبات الخصوصية في المؤسسة

الفئة المستهدفة:

- المسؤولون عن إعداد بيئة Microsoft 365 عبر Exchange Online SharePointg OneDriveg Teamsg
- مسؤولو الأمن والامتثال الذين يبنون السياسات ويديرونها في بوابة Microsoft Purview
- العاملون في حماية المعلومات الذين يملكون مخطط التصنيف في المؤسسة ويقودون إطلاق التسميات
- العاملون في إدارة السجلات والمعلومات الذين يضبطون الاحتفاظ بالمحتوى الإلكتروني والتخلص منه
- محللو العمليات الأمنية الذين يفرزون تنبيهات DLP ويحققون في حوادث انكشاف البيانات

محاور الدورة:

اليوم 1: البيانات الحساسة في البيئة وبوابة Purview

- البيانات المخزنة والمتنقلة وقيد الاستخدام في البريد والملفات والمحادثات والأجهزة
- جولة في بوابة Microsoft Purview: الحلول ومجموعات الأدوار والصلاحيات
- نموذج Purview لحماية المعلومات: اعرف بياناتك واحمها وامنع فقدانها
- خط أساس المشاركة الزائدة: روابط المشاركة ووصول الضيوف والمحتوى غير المصنف
- ورقة جرد البيانات الحساسة حسب وحدة العمل والخدمة

اليوم 2: تصنيف البيانات: أنواع المعلومات الحساسة والمصنفات

- أنواع المعلومات الحساسة المدمجة: الأنماط والكلمات المفتاحية ومستويات الثقة والتقارب
- أنواع معلومات حساسة مخصصة بالتعبيرات النمطية وقواميس الكلمات المفتاحية
- المصنفات القابلة للتدريب: الفئات المدمجة والمحتوى الأولي للنماذج المخصصة
- مراجعة العناصر المصنفة في مستكشف المحتوى ومستكشف النشاط
- خطة اختبار التصنيف: عينات النتائج الإيجابية الخاطئة والسلبية الخاطئة

اليوم 3: تسميات الحساسية والتشفير والتسمية التلقائية

- هيكل تسميات الحساسية: التسميات الرئيسية والفرعية وأولوية التسمية
- سياسات التسميات: التسمية الافتراضية والتسمية الإلزامية ومبرر خفض التسمية
- تشفير التسميات والعلامات المرئية وتشفير الرسائل في Microsoft Purview
- سياسات التسمية التلقائية في وضع المحاكاة لخدمات Exchangeg OneDriveg SharePoint
- تسميات Teams ومجموعات Microsoft 365 والمواقع: إعدادات الخصوصية والمشاركة الخارجية

اليوم 4: سياسات DLP والأجهزة الطرفية والاحتفاظ والتحقيقات

- بناء سياسة DLP: الشروط والإجراءات وتلميحات السياسة وتجاوزات المستخدم
- منع فقدان البيانات على أجهزة Windows: وحدات USB والطباعة والرفع السحابي وضوابط المتصفح
- DLP لمحادثات Teams وقنواتها وفرز التنبيهات في لوحة تنبيهات DLP
- سياسات الاحتفاظ وتسميات الاحتفاظ وإعلان السجلات للبريد والملفات
- إشارات المخاطر الداخلية وبحث سجل التدقيق وأساسيات حالات eDiscovery

اليوم 5: البناء في المختبر وتصميم حماية المعلومات ومنع التسرب

- مختبر: مجموعة تسميات مع التشفير منشورة لمجموعة تجريبية
- مختبر: سياسة DLP للبيانات المالية والشخصية مختبرة بالمحاكاة ثم مفعلة
- مصفوفة ربط الضوابط: مستويات التصنيف مع التسميات وقواعد DLP والاحتفاظ
- خطة الإطلاق المرحلي: التجربة والتواصل مع المستخدمين ودورية ضبط السياسات
- عرض تصميم حماية المعلومات ومنع التسرب ومراجعته مع الزملاء

المهارات التي ستكتسبها:

- إعداد أنواع المعلومات الحساسة
- تقييم المصنفات القابلة للتدريب
- تصميم هيكل تسميات الحساسية
- ضبط سياسات التسمية التلقائية
- إدارة DLP على الأجهزة الطرفية
- فرز تنبيهات DLP
- إدارة تسميات الاحتفاظ
- التحقيق عبر تدقيق Purview

لماذا تحضر هذه الدورة:

- العودة بتصميم لحماية المعلومات ومنع التسرب مختبر في بيئة تجريبية وقابل للتكييف مع بيئة Microsoft 365 في مؤسستك
- خفض ضجيج DLP بمعرفة مستويات الثقة والشروط والتجاوزات التي توقف التسرب الفعلي دون تعطيل العمل اليومي
- معرفة كيفية نقل التسمية من خيار اختياري للمستخدم إلى تغطية تلقائية للبريد والملفات والمواقع
- مقارنة تجارب إطلاق التسميات وDLPs مع مسؤولين من قطاعات المال والصحة والطاقة والقطاع العام

الخاتمة:

تنجح حماية المعلومات في Microsoft 365 حين يكتشف المحتوى الحساس ويسمى وتحكمه سياسات تلازمه في البريد والملفات والمحادثات والأجهزة. تنتقل الدورة من حالات البيانات الحساسة وبوابة Purview، مرورا بأنواع المعلومات الحساسة والمصنفات، إلى تسميات الحساسية والتشفير والتسمية التلقائية، ثم سياسات DLP للخدمات والأجهزة الطرفية وأدوات الاحتفاظ والتحقيق. ويحول المشاركون في اليوم الأخير عمل المختبر إلى تصميم لحماية المعلومات ومنع التسرب مرتبط بمستويات التصنيف وواجبات الخصوصية في المؤسسة.