Githa Fadilla O.P

TUGAS ASINKRON 6

1. Salah satu manajemen perlindungan risiko yang ditawarkan Microsoft adalah Insider Risk

    a. Jelaskan pengertian Insider Risk.
    b. Uraikan dan jelaskan alur kerja insider risk management.

    Jawaban :

    a) Insider Risk adalah risiko keamanan yang timbul dari tindakan atau perilaku yang tidak pantas dari orang dalam (insider) suatu organisasi, seperti karyawan, kontraktor, atau mitra bisnis yang memiliki akses ke informasi rahasia atau kritis. Insider Risk dapat berasal dari niat jahat (seperti pencurian data atau spionase) atau tidak sengaja (seperti kebocoran data karena kelalaian atau kesalahan).
    b) Alur kerja Insider Risk Management yang ditawarkan oleh Microsoft terdiri dari empat tahap:

        Identify: Tahap pertama adalah mengidentifikasi risiko insider di organisasi.

        Investigate: Tahap kedua adalah menyelidiki insiden yang terjadi. Tim Insider Risk Management dari Microsoft bekerja sama dengan tim keamanan informasi dan kepatuhan untuk menyelidiki dan mengevaluasi insiden dan menentukan apakah ada tindakan yang harus diambil.

        Respond: Tahap ketiga adalah menangani insiden dan mengurangi risiko. Microsoft menyediakan alat dan layanan untuk membantu organisasi dalam menangani insiden dan mengurangi risiko.

        Monitor: Tahap keempat adalah memantau aktivitas insider secara terus-menerus untuk mengidentifikasi risiko lebih awal.

        Dengan menggunakan alur kerja ini, organisasi dapat meningkatkan keamanan dan melindungi data rahasia mereka dari risiko insider.

2. E-Discovery dapat membantu organisasi Anda menanggapi masalah hukum atau penyelidikan internal dengan menemukan data di tempatnya berada. E-Discovery ini dapat diterapkan ke berbagai bagian.
    a. Uraikan implementasi eDiscovery pada Teams
    b. Uraikan implementasi e-Discovery pada Sharepoint

Lengkapi dengan referensi yang Anda pakai.

Jawaban :

a) **Berikut adalah implementasi eDiscovery pada Teams:**

- Buat kasus:

  Pertama-tama, organisasi perlu membuat kasus untuk investigasi atau tuntutan hukum di pusat keamanan dan kepatuhan Microsoft 365. Dalam kasus tersebut, organisasi dapat menetapkan tim dan kriteria pencarian.

- Buat kriteria pencarian:

  Setelah kasus dibuat, organisasi perlu membuat kriteria pencarian. Ini dapat mencakup kata kunci, tanggal, jenis pesan, dan lain-lain.

- Pencarian:

  Setelah kriteria pencarian dibuat, Teams akan mulai mencari data yang terkait dengan kasus tersebut. Hasil pencarian dapat diulang-ulang untuk memastikan semua data yang relevan telah ditemukan.

- Analisis data:

  Setelah data ditemukan, organisasi dapat menganalisis data dengan menggunakan alat pencarian dan filter untuk membantu mempersempit pencarian. Selain itu, organisasi juga dapat menandai atau mengelompokkan data untuk memudahkan pemrosesan data.

- Ekspor data:

  Setelah data dianalisis, organisasi dapat mengekspor data dalam format yang sesuai dengan kebutuhan investigasi atau tuntutan hukum.

b) **Berikut adalah implementasi eDiscovery pada Teams:**

- Buat kasus:

  Pertama-tama, organisasi perlu membuat kasus untuk investigasi atau tuntutan hukum di pusat keamanan dan

kepatuhan Microsoft 365. Dalam kasus tersebut, organisasi dapat menetapkan tim dan kriteria pencarian.

- Buat kriteria pencarian:

  Setelah kasus dibuat, organisasi perlu membuat kriteria pencarian. Ini dapat mencakup kata kunci, tanggal, jenis pesan, dan lain-lain.

- Pencarian:

  Setelah kriteria pencarian dibuat, Teams akan mulai mencari data yang terkait dengan kasus tersebut. Hasil pencarian dapat diulang-ulang untuk memastikan semua data yang relevan telah ditemukan.

- Analisis data:

  Setelah data ditemukan, organisasi dapat menganalisis data dengan menggunakan alat pencarian dan filter untuk membantu mempersempit pencarian. Selain itu, organisasi juga dapat menandai atau mengelompokkan data untuk memudahkan pemrosesan data.

- Ekspor data:

  Setelah data dianalisis, organisasi dapat mengekspor data dalam format yang sesuai dengan kebutuhan investigasi atau tuntutan hukum.

Referensi :

- "Manage eDiscovery cases in Microsoft Teams" (Microsoft)
- "eDiscovery in Microsoft Teams" (Microsoft)
- "eDiscovery in SharePoint Server" (Microsoft)
- "eDiscovery in SharePoint Online" (Microsoft)

3. Bagaimana advanced eDiscovery Lanjutan dan Audit Lanjutan dapat mendukung organisasi dalam menanggapi kewajiban hukum, peraturan, dan kepatuhan? Uraikan, sertakan referensi yang mendukung jawaban Anda.

   Jawaban:

   Berikut adalah penjelasan singkat tentang bagaimana kedua fitur ini dapat mendukung organisasi dalam hal tersebut:

Advanced e-Discovery:

Advanced e-Discovery memungkinkan organisasi untuk mengekstrak, menganalisis, dan mengekspor data secara efektif dan efisien dalam hal investigasi atau tuntutan hukum. Dalam hal ini, fitur ini dapat membantu organisasi untuk memenuhi kewajiban hukum dan peraturan dengan cara menemukan dan mengumpulkan data dengan cepat dan efisien, serta menyederhanakan proses analisis dan pengolahan data yang relevan.

Audit Lanjutan:

Audit Lanjutan memungkinkan organisasi untuk melacak dan menganalisis aktivitas pengguna dan administrator dalam lingkungan Microsoft 365. Fitur ini dapat membantu organisasi memenuhi persyaratan kepatuhan dan peraturan dengan cara memberikan visibilitas atas kejadian dan aktivitas dalam lingkungan, serta mengaudit dan meninjau catatan aktivitas pengguna dan administrator.

Referensi:

- "Advanced eDiscovery" (Microsoft)
- "Audit Log" (Microsoft)

4. Azure Blueprints memungkinkan arsitek cloud dan grup teknologi informasi pusat menentukan serangkaian sumber daya Azure berulang yang menerapkan serta mematuhi standar, pola, dan persyaratan organisasi. Azure Blueprints memungkinkan tim pengembangan untuk membangun dan mendirikan lingkungan baru dengan cepat dengan kepercayaan yang mereka bangun dalam kepatuhan organisasi dengan serangkaian komponen bawaan, seperti jaringan, untuk mempercepat pengembangan dan penyediaan.

   Uraikan 2 implementasi Blueprints, berikan referensi yang mendukung.

   Jawaban :

   Berikut adalah dua implementasi Azure Blueprints yang dapat membantu organisasi dalam mengelola lingkungan cloud mereka:

   Implementasi Standar Keamanan:

   Azure Blueprints dapat membantu organisasi dalam mematuhi kebijakan keamanan yang diterapkan di dalam organisasi dengan menerapkan serangkaian konfigurasi keamanan standar pada lingkungan Azure mereka. Hal ini dapat memastikan bahwa sumber daya cloud organisasi terlindungi

dengan baik dan memenuhi standar keamanan yang diperlukan. Contoh konfigurasi keamanan standar termasuk pembatasan akses dan pengaturan jaringan untuk mencegah serangan dari luar.

Implementasi Infrastruktur sebagai Kode (IaC):

Azure Blueprints dapat digunakan untuk mengelola infrastruktur sebagai kode (IaC) pada lingkungan Azure organisasi. Dengan Azure Blueprints, tim pengembangan dapat membuat blueprints untuk membangun lingkungan Azure dengan cepat dan konsisten menggunakan skrip yang sudah disediakan, sehingga memastikan konsistensi dan kepatuhan pada setiap pembangunan lingkungan baru. Dalam hal ini, Azure Blueprints dapat membantu organisasi dalam meningkatkan efisiensi dan mengurangi kesalahan manusia dalam pembangunan dan pengelolaan infrastruktur cloud mereka.

Referensi:

- "Azure Blueprints Overview" (Microsoft)
- "Azure Blueprint Samples" (Microsoft)