**PROPOSAL**

**Data Science Batch 3**

**“Penerapan Data Science Terhadap Kebocoran Data Perusahaan”**

**Oleh:**

**ROMA ULINA**

**DAFTAR ISI**

**BAB I PENDAHULUAN**

* **Latar Belakang…………………………………………………………………………..**
* **Rumusan Masalah……………………………………………………………………….**
* **Tujuan Penelitian…………………………………………………………………………**
* **Manfaat Penelitian……………………………………………………………………….**

**BAB II METODOLOGI**

* **Metode Penelitian…………………………………………………………………………**
* **Teknik Pengumpulan Data……………………………………………………………….**
* **Teknik Analisis Data………………………………………………………………………**
* **Implementasi Solusi……………………………………………………………………….**

**DAFTAR PUSAKA**

**BAB I**

**PENDAHULUAN**

Kebocoran data perusahaan merupakan salah satu isu penting dalam keamanan informasi. Dengan perkembangan teknologi, risiko kebocoran data semakin meningkat. Oleh karena itu, penerapan data science dalam mengatasi kebocoran data menjadi solusi yang penting untuk diteliti.

**RUMUSAN MASALAH**

Bagaimana penerapan data science dapat membantu mengidentifikasi, menghentikan, dan mencegah kebocoran data di perusahaan?

**TUJUAN PENELITIAN**

1. Mengidentifikasi metode data science yang dapat digunakan untuk mendeteksi kebocoran data.

2. Menyusun langkah-langkah pencegahan kebocoran data dengan menggunakan data science.

3. Menganalisis efektivitas penerapan data science dalam mengatasi kebocoran data perusahaan.

**MANFAAT PENELITIAN**

1. Memberikan solusi praktis bagi perusahaan untuk mengatasi kebocoran data.

2. Meningkatkan keamanan data perusahaan.

3. Membantu perusahaan dalam mengelola risiko kebocoran data secara lebih efektif.

**BAB II**

**METODE PENELITIAN**

1. Observasi: Melakukan observasi langsung terhadap sistem keamanan data perusahaan.

2. Wawancara: Melakukan wawancara dengan tim IT dan keamanan informasi perusahaan.

3. Dokumentasi: Mengumpulkan dokumen-dokumen terkait kebijakan dan prosedur keamanan data perusahaan.

**TEKNIK ANALISIS DATA**

Data yang dikumpulkan akan dianalisis menggunakan metode analisis konten dan analisis tematik untuk mengidentifikasi pola dan tema utama terkait kebocoran data dan penerapan data science.

**IMPLEMENTASI SOLUSI**

1. Pembersihan Data:

- Lakukan validasi data untuk memastikan tidak ada data berbahaya yang tersimpan.

- Gunakan tools seperti antivirus dan anti-malware untuk memeriksa sistem.

2. Peningkatan Keamanan:

- Implementasi firewall aplikasi web (WAF) untuk melindungi dari serangan serupa di masa depan.

- Terapkan enkripsi pada data sensitif untuk mengurangi risiko saat terjadi kebocoran data.

3. Identifikasi dan Hentikan Kebocoran:

- Hentikan sumber kebocoran segera setelah ditemukan.

- Lakukan analisis forensik untuk mengidentifikasi bagaimana kebocoran terjadi.

4. Penanganan Insiden:

- Komunikasikan insiden dengan tim manajemen dan stakeholder yang relevan.

- Informasikan pengguna atau klien jika data pribadi mereka terkena dampak, sesuai dengan peraturan yang berlaku.

5. Audit dan Evaluasi:

- Tinjau semua sistem dan proses keamanan untuk menemukan dan memperbaiki kelemahan.

- Periksa apakah ada data yang telah diubah atau disusupi oleh pihak yang tidak berwenang.

6. Perbaikan dan Pencegahan:

- Implementasi enkripsi untuk data saat dalam penyimpanan dan transmisi.

- Terapkan kontrol akses yang lebih ketat dan otentikasi dua faktor (2FA).

- Tingkatkan pelatihan keamanan bagi seluruh staf.

7. Pemulihan Data:

- Jika data telah diubah atau hilang, pulihkan dari cadangan (backup) yang aman.

- Verifikasi integritas data yang dipulihkan.

**DAFTAR PUSAKA**

https://journal.unnes.ac.id/sju/index.php/ipmhi/article/download/53698/20902

https://journal.uii.ac.id/JON/article/view/31046