NAMA: FERNALDY FERDINAND
NIM: 2602068605
KELAS: LA09

ESSAY

1. Ketika menghadapi risiko keamanan dari serangan ransomware dan memastikan model prediksi berjalan dengan baik di produksi, kita perlu memahami bahwa serangan ransomware dapat dianggap sebagai salah satu bentuk serangan data poisoning. Serangan data poisoning adalah serangan di mana data pelatihan atau input model diubah atau dirusak untuk merusak kinerja model atau menghasilkan prediksi yang salah.

   Testing yang saya gunakan untuk memastikan bahwa model prediksi akan berjalan dengan baik.

   - Data testing dilakukan untuk memastikan bahwa data yang akan kita gunakan dalam melakukan model prediksi telah tervalidasi secara menyeluruh sebelum dijalankan oleh model. Dimana serangan ransomware ini dapat memanipulasi data. Jadi Data testing ini bertujuan untuk memastikan faktor – faktor seperti akurasi, kelengkapan, konsistensi, relevansi, dan ketepatan waktu data dapat terpenuhi. Lalu kontrol terhadap data, mengatur pipelines data secara hati – hati untuk menghindari duplikat data, tata Kelola data dengan integritas yang ditegakkan, dan menjaga ketertelusuran dan garis keturunan ujung ke ujung merupakan langkah – langkah penting untuk menjaga keamanan data sebelum akan digunakan didalam model.

   - Model Testing dilakukan untuk melakukan evaluasi pada performa model sebelum diimplementasikan secara luas dalam lingkungan produksi. Proses ini bertujuan untuk memastikan tidak hanya akurasi prediksi yang tinggi, tetapi juga kesiapan model dalam menghadapi variasi data yang kompleks tanpa mengalami kendala yang signifikan. Dalam pengujian model juga meliputi beberapa aspek keamanan dan keandalan untuk mengidentifikasi dan mengurangi potensi resiko sebelum model itu digunakan secara operaSsional. Dengan mengikuti proses data testing dan modeling testing yang ada, maka perusahaan dapat mengurangi resiko kerentanan terhadap manipulasi data dan dapat memastikan bahwa model yang telah diimplementasikan berfungsi secara optimal dalam lingkungan produksi yang sebenernya.

2. Untuk melindungi data dari serangan ransomware, perlu dilakukan proses monitoring yang komprehensif. Berikut adalah langkah-langkah yang dapat diambil:
   a. **Monitoring Aktivitas Jaringan**: Implementasikan sistem deteksi intrusi yang dapat memonitor dan mengidentifikasi aktivitas mencurigakan dalam jaringan, seperti upaya akses tidak sah atau anomali dalam pola lalu lintas data.
   b. **Pemantauan Keamanan Sistem**: Tinjau dan perbarui secara teratur sistem keamanan seperti firewall, antivirus, dan sistem deteksi malware untuk menghalangi dan mendeteksi masuknya ransomware ke dalam sistem.

c. **Backup dan Restore Rutin**: Lakukan backup data secara berkala dan pastikan proses backup tersebut terotomatisasi dan terenkripsi. Hal ini memastikan bahwa data dapat dipulihkan dengan cepat jika terjadi serangan ransomware.
d. **Pendidikan dan Pelatihan Karyawan**: Berikan pelatihan kepada karyawan tentang praktik keamanan digital, termasuk cara mengidentifikasi email phishing dan langkah-langkah untuk melaporkan kegiatan mencurigakan.
e. **Implementasi Kebijakan Akses**: Terapkan kebijakan yang ketat terkait dengan pengelolaan akses, termasuk hak akses berbasis peran dan otorisasi yang diperlukan untuk mengurangi risiko akses tidak sah ke data sensitif.
f. **Monitoring dan Pemantauan Log**: Aktifkan logging untuk semua aktivitas sistem dan aplikasi yang kritis. Tinjau log secara berkala untuk mendeteksi pola aneh atau aktivitas yang mencurigakan yang dapat mengindikasikan serangan ransomware.
g. **Pembaruan Keamanan Reguler**: Pastikan semua perangkat lunak dan sistem operasi diperbarui dengan patch keamanan terbaru untuk mengatasi kerentanan yang dapat dieksploitasi oleh serangan ransomware.

Dengan mengikuti proses monitoring yang terstruktur dan proaktif seperti ini, perusahaan dapat meningkatkan pertahanan mereka terhadap serangan ransomware dan mengamankan data dengan lebih baik.