Erweiterte KI-Lösung für die Erkennung von Malware

Eine Anwendung, die auf den Speichersystemen (SAN) von Unternehmensrechenzentren ausgeführt wird. Überwacht die SAN Aktivität in Echtzeit. Setzt fortschrittliche KI-Lösungen ein, um Anomalien zu erkennen und Malware daran zu hindern, Unternehmensdaten zu beschädigen.

Übersicht _

Kunde:
- ProLion GmbH
- Cybersecurity, Anti-Malware-Lösungen
- Wien, AT

Geschäftsfall:
- Aufspüren und Verhindern von ransome-ware-Angriffen
- Überwachen der Speichernutzung

Industrie _

- IT-Dienste
- Rechenzentren
- Speicherung
- Cyber-Sicherheit

Dienstleistungen _

- Entwicklung kundenspezifischer Software
- Produktentwicklung

Art des Projekts _

- Web
- Verteiltes Backend

Technologie _

- Java
- NetApp geclusterte Daten ONTAP
- Hazelcast
- Docker
- REST endpoints
- AWS-Virtualisierung
- Maschinelles Lernen

Beschreibung _

Eine Anwendung, die auf den Rechenzentrums-Speichersystemen (SAN) eines Unternehmens läuft und die SAN-E/A-Aktivität in Echtzeit überwacht. Sie verwendet eine fortschrittliche KI-Lösung zur Erkennung von Anomalien, die es ermöglicht, Malware daran zu hindern, Unternehmensdaten zu beschädigen.

Herausforderungen _

Da Malware in vielen verschiedenen Formen zuschlagen und schwere Auswirkungen auf den Endnutzer haben kann, müssen wir:

- Eine leistungsfähige Lösung bereitstellen, die vor allen Bedrohungen (sowohl bekannten als auch neuen/unbekannten) schützt.
- Die höchste Genauigkeit bei der Erkennung von Malware gewährleisten, während wir die Anzahl der Fehlalarme auf einem Minimum (oder auf Null) halten.
- Echtzeit-Erkennung und -Schutz bieten, der sich über das gesamte SAN-Netzwerk erstreckt.
- Die SAN-Leistung unbeeinträchtigt erhalten.

Lösungen _

Wir haben die hohen Erwartungen des Kunden durch eine Reihe technologieübergreifender Lösungen erfüllt:

- Techniken zur Erkennung von KI-Anomalien, die bestimmen, was „normaler“ Datenverkehr ist, und diesen durchlassen, während „verdächtiger“ Datenverkehr blockiert wird.
- Modelltraining und -auswertung mit umfangreichen realen Daten, die aus Produktions-SAN-Protokollen gesammelt werden.
- Verarbeitung und Verbesserung des gesammelten Datensatzes, um einen noch größeren synthetischen, „real-ähnlichen“ Datensatz zu erhalten.
- Einrichtung von simulierten SAN-Umgebungen und kontrollierter Übertragung von Malware zur Sammlung von Spuren.
- Anpassung der Modellparameter, um höchste Präzision und Rückrufwerte zu gewährleisten.
- Implementierung einer verteilten Architektur mit Sensoren auf jedem SAN-Knoten und dedizierten Verarbeitungsknoten zur Ausführung des Erkennungsmodells.
- Erarbeitung einer selbst entwickelten Entscheidungsbaumvariante, die sowohl genau als auch leicht genug für den Anwendungsfall ist.
- Hyperparameter-Abstimmung zur Minimierung des Modells unter Beibehaltung der Genauigkeit.