Cybersecurity & Artificial Intelligence

Connessioni e sfide

Federico Santi
Cybersecurity Director DXC

Overview

AI Act e implicazioni con la Cybersecurity

Approvato il Regolamento sull'Intelligenza artificiale

Di cosa si tratta e quali sono le implicazioni con la sicurezza informatica?

- In un mondo interconnesso come quello in cui viviamo la protezione dei sistemi e dei dati assume fondamentale importanza. La crescente complessità ed interconnessione dei sistemi informativi, unita alla frammentazione delle informazioni rende la **gestione della sicurezza informatica** un compito sempre più articolato basato su processi e soluzioni tecnologiche avanzate e su una capacità di intercettare, comprendere e contenere i flussi di attacco (**counterintelligence**).

- L'AI Act rappresenta il **primo tentativo di regolamentazione generale** dei sistemi e delle applicazioni di Intelligenza Artificiale

- Lo **scopo dell'AI Act** è quello di istituire un quadro giuridico uniforme europeo non solo per quanto riguarda lo sviluppo, l'immissione sul mercato e la messa in servizio dei sistemi di Intelligenza Artificiale, ma anche e soprattutto per quanto riguarda il corretto utilizzo di tali sistemi

- Il concetto di intelligenza artificiale ha da tempo abbandonato l'ambito puramente tecnologico in cui è stato sviluppato per entrare nel linguaggio comune e addentrarsi nella commune **user experience**.
  In particolare **l'AI nell'ambito della cybersecurity** può essere un potente alleato ai fini difensivi e di prevenzione (**AI for Cyber**) e contemporaneamente pggetto di misure di sicurezza e Privacy che ne contengano alcune minacce implicite (**Cyber for AI**)

Analisi predittive e comportamentali

Finalità, applicazioni cyber e focus Sanità

L'AI quale valido strumento per l'analisi predittiva e comportamentale (1/2)

Potenzialità legate alla valorizzazione dei dati

Valorizzando i dati grazie all'Intelligenza artificiale e al machine learning, le organizzazioni riescono a **stimare i rischi** e le **tendenze future** per sviluppare piani di azione, sia come mitigazione che come strategia proattiva

- **L'analisi predittiva e comportamentale consiste nell'utilizzare dati, algoritmi statistici e tecniche di intelligenza artificiale e machine learning per individuare la probabilità di risultati futuri basandosi sui dati storici (particolarmente interessante in ambito di ricerca, anche medica)**
- **La qualità dei risultati finali dipende dalla qualità dei dati (Data quality) e dalla selezione del modello statistico e probabilistico per la loro elaborazione (algoritmo), al fine di proiettare scenari**
- **L'analisi predittiva e comportamentale è strettamente collegata alla Business Intelligence e infatti, pur svolgendo ruoli differenti, collaborano e interagiscono fornendosi reciprocamente dati e informazioni**

L'AI quale valido strumento per l'analisi predittiva e comportamentale (2/2)

Il processo predittivo non è statico, ma viene costantemente affinato sulla base dei risultati ottenuti e dell'analisi dettagliata del suo comportamento, in un ciclo di feedback periodicamente alimentato per migliorare l'affidabilità delle previsioni (**approccio ricorsivo e di continuous improvement**)

Alcuni esempi di analisi predittiva e comportamentale, applicata all'AI:

Settore finance

L'AI viene impiegata per **rilevare frodi** o problemi di conformità ma anche per **individuare trend comportamentali** leciti ma potenzialmente indicativi di futuri eventi illeciti.

Settore marketing

Si può **prevedere la propensione al consumo** di classi di clienti con determinate caratteristiche o dati storici e trend

Pharma

In ambito farmaceutico si può **prevedere i valori di produzione/fatturato, di determinati farmaci**, sfruttando informazioni come campagne pubblicitarie, variazioni di prezzo e stagionalità

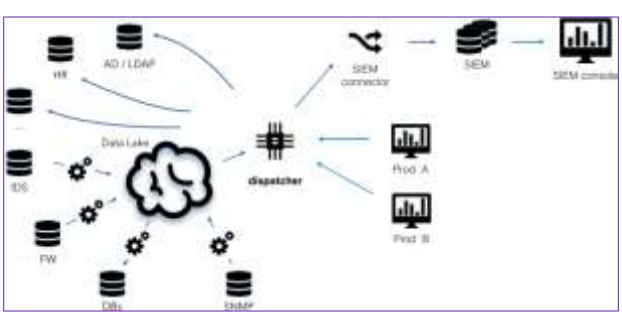
Giustizia predittiva

L'IA potrà avere un impatto rilevante nel settore penale, Anche lavorando su dati aggregati e nel rispetto della Privacy si possono **indirizzare risorse umane e finanziarie su aree specifiche del crimine** finanziario o della criminalità organizzata in genere.

Use Cases

A fianco della più semplice IA, vi sono i sistemi di AI generativa (GenAI), che, attraverso l'addestramento su vasti set di dati e l'apprendimento automatico, sono in grado di produrre contenuti di vario genere.

Di seguito un **esempio macro di applicazione di next GenAI SOC**



Ottimizzazione della ricerca nei data lake per log/IOC specifici

Estensione delle capacità di indagine del SIEM in tempo reale ai data lakes di security

Analisi predittiva

Implicazioni dell'AI nel mondo della sanità

Nell'ambito della sanità l'Intelligenza artificiale può supportare sia la **ricerca** che la **conduzione operativa** delle attività mediche e relative **decisioni cliniche**.

Da alcuni esempi di applicazioni sperimentali dell'AI in sanità risulta evidente la necessità di applicare processi e tecnologie di sicurezza per favorire la tutela della **riservatezza dei dati sensibili** ma anche per garantire **l'integrità e la correttezza** non solo delle **informazioni** trattate ma anche delle **logiche e** degli **algortimi AI** utilizzati visto l'impatto potenziale sulla salute delle persone:

Università Aldo Moro e politecnico di Bari

E' stato sviluppato un algoritmo di intelligenza artificiale capace di **identificare**, in immagini di risonanza magnetica, **cambiamenti patologici dovuti alla malattia di Alzheimer in una fase precoce** della malattia

Policlinico Gemelli di Roma

E' stata sviluppata una piattaforma digitale che integra e combina una grande quantità di dati e informazioni di fonte e contenuto eterogeneo (consulti cardiologici, farmaci assunti ecc.) per progettare e addestrare dei modelli predittivi a più parametri allo scopo di **individuare in anticipo la re-ospedalizzazione del paziente**

ASST della Brianza

Viene utilizzata una piattaforma che acquisisce i dati della cartella clinica elettronica dei pazienti su cui testa e **addestra modelli predittivi a supporto delle decisioni cliniche**.

In questo caso l'IA può suggerire al medico di verificare se un paziente soffre di ipertiroidismo visto che ha avuto di recente l'insorgenza di fibrillazione atriale