



Innovation Day 2024 Info Point AI assistant

Inspired by ChatOPM application for Customer Support for Regulatory Solution products

INNOVATION DAY TOUR PROPOSAL FOR NICOLÒ:

Demo 13 'Lets hack it'

Demo 12 'Against network violation'

Demo 15 'Against fraud voice distortion'

CONVERSATION TRANSCRIPT

User: Ciao, sono Nicolò e sarei interessato alle demo sulla cyber security?

Assistant: Ciao Nicolò!

Siamo felici di avere il tuo interesse per le demo sulla cyber security. Abbiamo diverse demo interessanti in questo ambito che potrebbero catturare la tua attenzione.

- Against network violation: una demo innovativa che utilizza l'apprendimento automatico per rilevare le violazioni della sicurezza della rete.
- Lets hack it!: un'esperienza di hacking etico che ti permetterà di comprendere meglio le minacce alla sicurezza informatica.
- Against fraud voice distortion: una demo che mostra come l'intelligenza artificiale possa essere utilizzata per rilevare le frodi vocali.

Saresti interessato a sapere di più su una di queste demo in particolare?

Faithfulness is 0.8 [0.0 - 1.0]

User: Mi descriveresti con più dettagli la seconda?

Assistant: La demo "Lets hack it!" è un'esperienza di hacking etico che ti permette di esplorare il mondo delle minacce alla sicurezza informatica in un ambiente di apprendimento collaborativo. Durante la demo, potrai partecipare a sfide di hacking in stile Capture-The-Flag, dove potrai simulare attacchi come lo scanning dei porti, la scoperta dei servizi, il brute forcing delle credenziali e la cracking delle password.

La demo è condotta da un team di esperti di sicurezza informatica che ti guideranno attraverso le varie sfide e ti aiuteranno a comprendere le tecniche utilizzate dagli hacker per sfruttare le vulnerabilità dei sistemi. Inoltre, potrai anche esaminare dispositivi di hacking reali e vedere come vengono utilizzati per sfruttare le vulnerabilità dei sistemi.

L'obiettivo della demo è quello di fornire una comprensione più profonda delle minacce alla sicurezza informatica e di come possono essere mitigate.

Sembra che ci siano diverse demo interessanti Saresti interessato a sapere di più sulla demo "Against network violation" o "Against fraud voice distortion"? Forse potremmo esplorare queste opzioni e scoprire come possono aiutare a migliorare la sicurezza informatica.

- Against network violation
- Against fraud voice distortion

Entrambe le demo sembrano offrire una visione approfondita delle minacce alla sicurezza informatica e di come possono essere mitigate. Sarebbe utile esplorare queste opzioni e scoprire come possono aiutare a migliorare la sicurezza informatica.

Faithfulness is 0.1 [0.0 - 1.0]

User: Sì, aggiungimi dettagli anche su queste altre due.

Assistant: La demo "Against network violation" presenta un metodo innovativo per rilevare le violazioni della sicurezza della rete utilizzando l'apprendimento automatico. Il sistema utilizza una combinazione di tecniche di machine learning per analizzare i dati di rete e identificare le anomalie che potrebbero indicare un attacco di rete. La demo mostra come il sistema possa essere utilizzato per rilevare e

mitigare gli attacchi di rete in tempo reale.

In particolare, la demo utilizza un approccio basato su tre parametri: uno interno alla rete e due esterni. Il sistema utilizza l'apprendimento automatico per imparare dal passato e prevedere il comportamento normale della rete. Quando si verifica un'anomalia, il sistema utilizza una concatenazione di modelli di machine learning per correlare le tendenze inaspettate dei diversi parametri e identificare la natura dell'anomalia.

La demo "Against fraud voice distortion" mostra come l'intelligenza artificiale possa essere utilizzata per rilevare le frodi vocali. Il sistema utilizza un algoritmo di machine learning per analizzare le chiamate vocali e identificare le caratteristiche che potrebbero indicare una frode. La demo mostra come il sistema possa essere utilizzato per rilevare e prevenire le frodi vocali in tempo reale.

In particolare, la demo utilizza un approccio basato sull'analisi delle caratteristiche vocali, come la frequenza e l'intonazione, per identificare le chiamate sospette. Il sistema utilizza un algoritmo di machine learning per imparare dal passato e prevedere il comportamento normale delle chiamate vocali. Quando si verifica un'anomalia, il sistema utilizza un algoritmo di classificazione per identificare la chiamata come sospetta o legittima.

Saresti interessato a sapere di più sulla tecnologia di intelligenza artificiale utilizzata in queste demo? Ecco alcuni argomenti che potrebbero essere interessanti:

- Come funziona l'apprendimento automatico nel sistema di rilevamento delle violazioni della sicurezza della rete?
- Quali sono le caratteristiche vocali più importanti per identificare le chiamate sospette?
- Come il sistema di intelligenza artificiale può essere utilizzato per prevenire le frodi vocali in tempo reale?

Faithfulness is 0.5 [0.0 - 1.0]

User: Grazie mille

Assistant: Prego Nicolò Spero che le informazioni siano state utili. Buona giornata e buon Innovation Day

Faithfulness is 0.1 [0.0 - 1.0]