

KrakenAI



www.intelligenesislhc.com | info@intelligenesislhc.com



KrakenAI™ is a groundbreaking TRL 6 Large Language Model solution specifically crafted for the cybersecurity domain. With its advanced text generation techniques, efficient distributed computing, and tailored-scoring system, KrakenAI redefines language model applications, catering uniquely to the needs of cybersecurity professionals.

► FEATURES:

- Distributed Computing: Enhanced speed and application efficiency
- Session Management: Secure, vast data storage and personalized user experience
- Data Persistence and Caching: Boosted application speed and groundwork for user-driven question analytics
- Advanced Text Generation Techniques: Enhanced result diversity and relevance

► USE CASES:

- Enumerate Network and Domain
- Identify potential vulnerabilities in network
- Mimic Threats
- Dark Web Threats
- Usernames Enumeration
- Cyber Threat Intel
- Phishing Campaigns
- Social Engineering Scenarios
- Threat Intelligence
- Attack Prediction and Prevention



Model Details

Model Name: OPT IGLabs Cyber

Version: 0.2

Last Trained: 2023-07-06

do you know about cyber security risks?

Yes, I am familiar with cybers security risk assessment and mitigation strategies. I can identify and assess potential threats, develop effective mitigation strategies, and implement solutions to protect networks and systems from cybe attacks.

Can you provide me a paragraph summarizing StuxNet?

Stuxnet is a highly sophisticated computer worm that was designed to target industrial control systems. It was created by the United States and Israel to disrupt Iran's nuclear program and was released in 2010. The worm is capable of infecting computers running Windows and can cause physical damage to industrial equipment.

What is APT1 and what are their current capabilities?

APT1 is a highly sophisticated cybergang that has been active since 2012. They are known for conducting targeted attacks against organizations in the Middle East, particularly those involved in politics, government, and defense. APT1's current tactics include spear-phishing, social engineering, espionage malware, data exfiltration, ransomware and more.

What are you trained on?

A. Advanced threat detection techniques B. Malware analysis and reverse engineering C. Threat intelligence and threat hunting D. Penetration testing and vulnerability assessment E. Security architecture and design F. Compliance and regulatory requirements.

Type a question

Clear