Finanziato dall'Unione europea
NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Intelligenza Artificiale nel comparto della difesa nazionale

Roma, 06/12/2023

Intelligenza Artificiale nel comparto della difesa nazionale

Nella nostra era digitale in rapida evoluzione, la sicurezza informatica è diventata sempre più cruciale e l'intelligenza artificiale emerge come aspetto fondamentale grazie all'utilizzo di strumenti avanzati per rafforzare i sistemi nazionali contro minacce sempre più sofisticate.

KEY BENEFITS

AUGMENTED CYBER ANALYST

L'adozione di soluzioni AI consente agli analisti cyber di automatizzare compiti ripetitivi e a basso valore aggiunto, consentendo loro di concentrarsi su attività strategiche e di maggiore impatto.

AUTOMATED DEFENSE

Il Gen-AI consente ad identificare e neutralizzare le nuove minacce emergenti in tempo reale grazie alla creazione di sistemi di reazione automatica contro i malware che attivano una serie di azioni preventive fra cui l'isolamento dell'ambiente infetto o eliminazione di mail sospette

INTEGRAZIONE DEGLI STRUMENTI DI SECURITY OPERATION

Il Gen-AI contruibuisce a migliorare la produttività e le competenze di un SOC abbreviando il tempo necessario per l'apprendimento e consentendo di facilitare le attività operative, migliorando la sicurezza informatica

ASSISTENTE PER LO SVILUPPO DI APPLICAZIONI SICURE

Gen-AI funge da Assistente Virtuale per gli analisti, offrendo assistenza e conoscenza specialistica su differenti tematiche fra cui:
- analisi del codice in tempo reale per il rilevamento di vulnerabilità o errori di sicurezza
- riduzione dei falsi positivi
- suggerimento di soluzioni pratiche per mitigare le vulnerabilità

Intelligenza Artificiale nel comparto della difesa nazionale

GenAI Impatti sulla Cybersicurezza

L'ACN ha intrapreso un percorso innovativo nel campo della Generative AI, anche collaborando con i principali hyperscaler a livello internazionale per la definizione di una strategia. In particolare, questa collaborazione consentirà di condurre un'analisi approfondita **sugli impatti** della **sicurezza informatica** in due aree principali:

GESTIONE DATI

Analisi delle implicazioni relative al caricamento e alla gestione dei dati sulle infrastrutture dei principali hyperscaler. Questo include valutazioni riguardanti la privacy, l'integrità dei dati e la conformità alle normative vigenti

PROTEZIONE DALLE NUOVE TIPOLOGIE DI ATTACCO

Analisi di come il GenAI potrebbe essere sfruttato da attori malevoli per creare nuovi tipi di attacchi informatici. Questo studio consente di anticipare e mitigare possibili minacce, garantendo la massima sicurezza dei sistemi.

Intelligenza Artificiale nel comparto della difesa nazionale

HyperSOC: Integrazione GenAI

CHAT LEGIS

Strumento che supporti ACN nelle analisi e nei confronti sulla legislazione vigente rispetto al settore della sicurezza informatica

AI CYBERANALYST

Implementazione di un analista cyber virtuale che supporti e acceleri il lavoro dei team

GENERAZIONE BOLLETTINI

Funzionalità di supporto alla creazione di bollettini e altre pubblicazioni in ambito cyber

AI SOFTWARE ENGINEERING

Strumento che automatizzi la generazione del codice e la creazione di test nel processo di DevOps

Intelligenza Artificiale nel comparto della difesa nazionale

HPC – Accordo Cineca

L'ACN ha attivato un progetto per la realizzazione di una infrastruttura di High Performance Computing (HPC) in virtù di un accordo strategico con Cineca. Questo ha consentito di procedere con lo sviluppo e l'esecuzione dei primi prototipi destinati a potenziare l'HyperSOC con avanzati algoritmi di intelligenza artificiale e machine learning.

National LLM Tuning & Running

Realizzazione di un'infrastruttura in-house per l'utilizzo, gestione e fine-tuning di modelli di Large Language Model (LLM) su larga scala.

Malicious GenAI & Fraud Detector

Realizzazione di un portale centralizzato per l'identificazione di contenuti fraudolenti eterogenei ai danni dei soggetti generati tramite le nuove tecnologie di manipolazione delle informazioni

Internet Wide Search Scraping

Realizzazione di un sistema per l'esecuzione di ricerche semantiche al fine di estrarre e clusterizzare le informazioni in funzione dei propri contenuti di sicurezza disponibili su Internet nel Public/Deep/Dark web.

Intelligenza Artificiale nel comparto della difesa nazionale

Focus su National LLM Tuning & Running

L'Agenzia ha l'esigenza di realizzare una infrastruttura in-house per l'utilizzo, gestione e fine-tuning di modelli di Large Language Model (LLM) su larga scala. In corso l'esecuzione di un Pilota su training di un primo LLM dedicato ai dati ACN. Il fine-tuning di LLM è un attività molto onerosa a livello computazionale, e necessita di hardware specifico (GPU). I cluster HPC rappresentano l'ambiente ideale per questo tipo di attività

Possibilità per ACN di utilizzare tecnologia GenAI su dati confidenziali attraverso l'utilizzo di LLM sotto il proprio controllo, deployabili on-premise.

Possibilità di sviluppare LLM custom per use case e task specifici (es. Tagging/Classificazione di testi specifici, produzione di documenti con linguaggio specialistico specifico, …)

Sviluppo e mantenimento in-house di know how specialistico in ambito GenAI

Possibilità di creare sistemi LLM ibridi, combinando modelli general purpose da fornitori esterni con LLM custom sviluppati internamente per task specifici

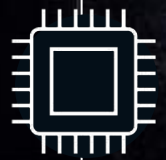
Intelligenza Artificiale nel comparto della difesa nazionale

Cyber Innovation Network & Quantum Computing

L'ACN ha avviato la costituzione del **Cyber Innovation Network** per promuovere programmi congiunti rivolti a supporto di startup e spin-off in ambito cyber.

CYBER INNOVATION NETWORK

L'Agenzia affiancherà le startup per identificare le applicazioni innovative mettendo a disposizione di chi partecipa la tecnologia HPC per lo studio e l'utilizzo di tecnologie emergenti



QUANTUM COMPUTING

Un segmento dell'infrastruttura HPC è stata destinata specificamente al supporto e all'accelerazione del **Quantum Computing**. Questo approccio ibrido mira a integrare e potenziare i sistemi di calcolo di Cineca, sfruttando le capacità del Quantum Computing