

Spunti sull'impiego dell'AI per gli analisti di Threat Intelligence (e per gli avversari) – Francesco Schifilliti



Durante la Cyber Crime Conference del 2024, Francesco Schifilliti ha tenuto una presentazione intitolata “Spunti sull'impiego dell'AI per gli analisti di Threat Intelligence (e per gli avversari)”, esplorando le complessità e i duali usi dell'intelligenza artificiale nel contesto della cybersecurity e del cybercrime.

Guarda il video completo dell'intervento:

[embedded content]

Dualità dell'Intelligenza Artificiale nella Cybersecurity

La presentazione ha messo in luce come l'intelligenza artificiale (AI) sia divenuta uno strumento cruciale per gli analisti di Threat Intelligence, ma questa non è solo un mezzo per migliorare l'efficacia delle operazioni di sicurezza, poiché in mano di attori malevoli è capace di diventare una seria minaccia. Uno dei punti focali del suo discorso è stato l'uso ambivalente dell'AI, che può essere impiegata tanto per fini legittimi quanto per scopi malevoli. Gli esempi citati hanno incluso l'uso dell'AI per creare email e campagne di phishing sofisticate, dimostrando come la tecnologia possa essere sfruttata per perpetrare frodi e altri crimini informatici.

Evoluzione dell'Intelligenza Artificiale

Schifilliti ha descritto l'evoluzione dell'AI, illustrando il passaggio dal Machine Learning e Deep Learning a tecniche più avanzate che includono Big Data Analytics, Natural Language Processing (NLP) e Data Science. Questi sviluppi hanno ampliato le capacità dell'AI, rendendola uno strumento ancora più potente e versatile nel campo della cybersecurity.

Generative AI e Information Operations

Un punto cruciale della presentazione è stata la discussione sulla "generative AI", ovvero l'intelligenza artificiale capace di creare contenuti convincenti e persuasivi usati nelle "information operations". Il relatore ha citato esempi di false immagini e video prodotti durante il conflitto Russo-Ucraino, dimostrando come l'AI possa influenzare i contesti geopolitici.

Impatto dell'AI sul Ciclo di Vita dell'Intelligence

Schifilliti ha anche spiegato come l'AI influenzi il Ciclo di Vita dell'intelligence, dalla raccolta e l'elaborazione dei dati (collection e processing) all'analisi e alla diffusione delle informazioni (analysis e dissemination). L'AI può automatizzare compiti come la sintesi di testi, l'estrazione di indicatori di compromissione (IoC) e la generazione di allarmi, facilitando il lavoro degli analisti.

Limiti e Rischi dell'Intelligenza Artificiale

Un punto critico sollevato riguarda i limiti dell'AI, come il rischio di bias incorporato nei modelli, la loro opacità (black box problem) e la vulnerabilità agli attacchi mirati a manipolare o corrompere i dati di apprendimento. Questi

problemi sollevano importanti questioni di affidabilità ed etica nell'uso dell'AI in contesti di sicurezza.

Necessità di Trasparenza e Collaborazione nell'Uso dell'AI

Durante il suo intervento Schifilliti ha messo in guardia gli ascoltatori sui rischi associati all'uso dell'AI nella threat intelligence, invitando a un'adozione responsabile e informata di queste tecnologie. Ha sottolineato la necessità di una maggiore trasparenza nell'uso dell'AI e di collaborazione tra i diversi stakeholder per mitigare i rischi e massimizzare i benefici dell'intelligenza artificiale nel campo della cybersecurity.

Opportunità e Sfide dell'AI nella Sicurezza Informatica

La presentazione ha così offerto una panoramica comprensiva e critica su come l'AI sta trasformando il panorama della sicurezza informatica, presentando sfide e opportunità per gli analisti e i decision maker del settore.

Il programma completo della Cyber Crime Conference 2024 è disponibile al seguente link:
<https://www.ictsecuritymagazine.com/eventi/cybercrimeconference2024#programma>

Iscriviti alla nostra newsletter per rimanere aggiornate sulle nostre iniziative:
<https://www.ictsecuritymagazine.com/newsletter/>

Condividi sui Social Network:
<https://www.ictsecuritymagazine.com/cybersecurity-video/spunti-sullimpiego-dellai-per-gli-analisti-di-threat-intelligence-e-per-gli-avversari-francesco-schifilliti/>