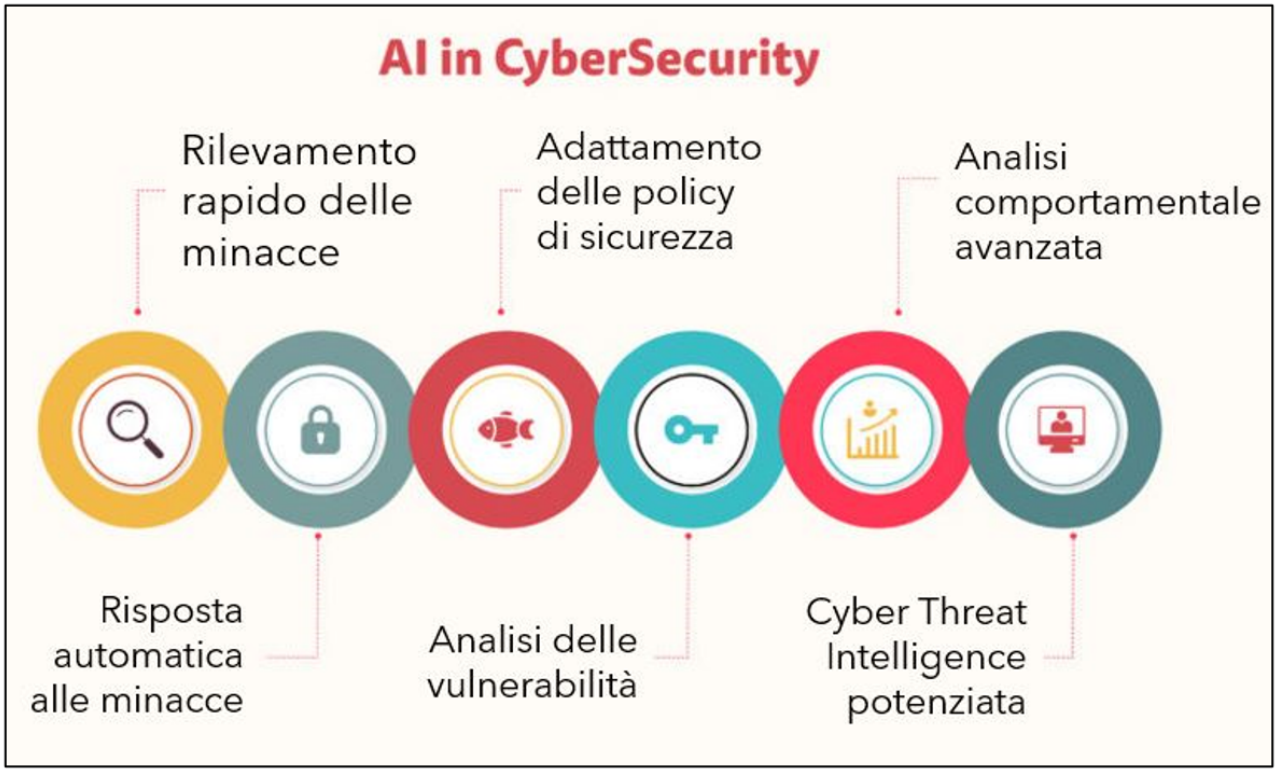
Artificial Intelligence → Applicazioni dell'AI nella Cybersecurity

L'intelligenza artificiale (IA) sta rivoluzionando il campo della Cybersecurity, fornendo nuovi strumenti e approcci per affrontare minacce sempre più sofisticate. Le tecnologie di IA hanno la capacità di trovare rapidamente nei dati correlazioni e pattern difficili da vedere da parte di un analista umano, il cui ruolo rimane comunque centrale in virtù della sua visione più completa e consapevole del contesto operativo dei sistemi. Infatti, ad oggi l'utilizzo dell'IA in Cybersecurity risulta essere perlopiù strumento di assistenza all'analista, inserito in un funzionamento semiautomatico. Con la maturazione sempre più concreta delle applicazioni di IA diversi processi potranno raggiungere una reale automazione entro pochi anni.



Sono tre le principali macroaree della Cybersecurity in cui si inseriscono efficacemente gli utilizzi delle tecnologie di Intelligenza Artificiale.

Rilevamento delle minacce

L'IA ha dimostrato un notevole successo nel rilevare minacce cibernetiche. Gli algoritmi di apprendimento automatico possono analizzare grandi quantità di dati in tempo reale (i.e. log, basi di dati, traffico di rete) per individuare comportamenti sospetti o modelli non convenzionali.

Alcuni esempi:

- Rilevamento delle anomalie: Gli algoritmi di IA possono identificare attività insolite all'interno di reti o sistemi, anche quando le minacce sono nuove o sconosciute.
- Analisi comportamentale: L'IA può monitorare il comportamento degli utenti e dei dispositivi per individuare attività potenzialmente dannose o non autorizzate.
- Rilevamento di malware: Gli strumenti basati sull'IA possono identificare e neutralizzare malware

noti e sconosciuti, basandosi su modelli di comportamento.

Automazione della risposta alle minacce

Oltre al rilevamento, l'IA consente anche un'automazione più efficace della risposta alle minacce. Questo significa che i sistemi di sicurezza possono rispondere più rapidamente ed efficientemente alle minacce in tempo reale.

Alcuni esempi di automazione nella risposta alle minacce includono:

- Sistema di risposta automatica: Gli algoritmi di IA possono bloccare l'accesso a risorse critiche, isolare dispositivi compromessi e applicare regole di sicurezza.
- Analisi delle vulnerabilità: L'IA può identificare e valutare le vulnerabilità dei sistemi e nel codice informatico, aiutando a mitigare le potenziali minacce in modo proattivo.
- Correlazione degli eventi: L'IA può correlare eventi apparentemente non collegati per identificare attacchi complessi e orchestrati.

Previsione e prevenzione

L'IA non si limita solo a rispondere alle minacce esistenti ma può anche prevedere e prevenire minacce future. L'analisi predittiva basata sull'IA può essere utilizzata per identificare possibili scenari di attacco, consentendo alle organizzazioni di prendere misure preventive.

Alcuni esempi includono:

- Modelli di previsione delle minacce: L'IA può analizzare dati storici e attuali per identificare tendenze e modelli che potrebbero indicare futuri attacchi.
- Simulazioni di attacco: Gli specialisti di sicurezza possono utilizzare l'IA per simulare potenziali scenari di attacco e valutare la resilienza dei sistemi.
- Adattamento delle politiche di sicurezza: L'IA può aiutare a regolare le politiche di sicurezza in tempo reale, in base alle minacce attuali e alle vulnerabilità rilevate.

L'NLP (Natural Language Processing) e la GenAI possono essere strumenti preziosi nella Cyber Threat Intelligence (CTI). L'NLP può essere utilizzato per analizzare grandi quantità di testo proveniente da fonti aperte, forum underground, dark web, social media, per identificare indizi, pattern e informazioni relative a minacce cibernetiche. La GenAI, d'altra parte, può essere utilizzata per generare modelli predittivi basati su dati storici e attuali per anticipare potenziali attacchi e sviluppare strategie di difesa. Insieme, queste tecnologie possono migliorare notevolmente la capacità di rilevare e mitigare le minacce cibernetiche in modo proattivo. Questa possibilità è da intendersi sia per utilizzi automatici, continui, con automatismi sempre alla ricerca di informazioni rilevanti, e sia in assistenza al lavoro dell’analista CTI che si doterebbe di un prezioso strumento per le sue analisi più specifiche.