June 11, 2019

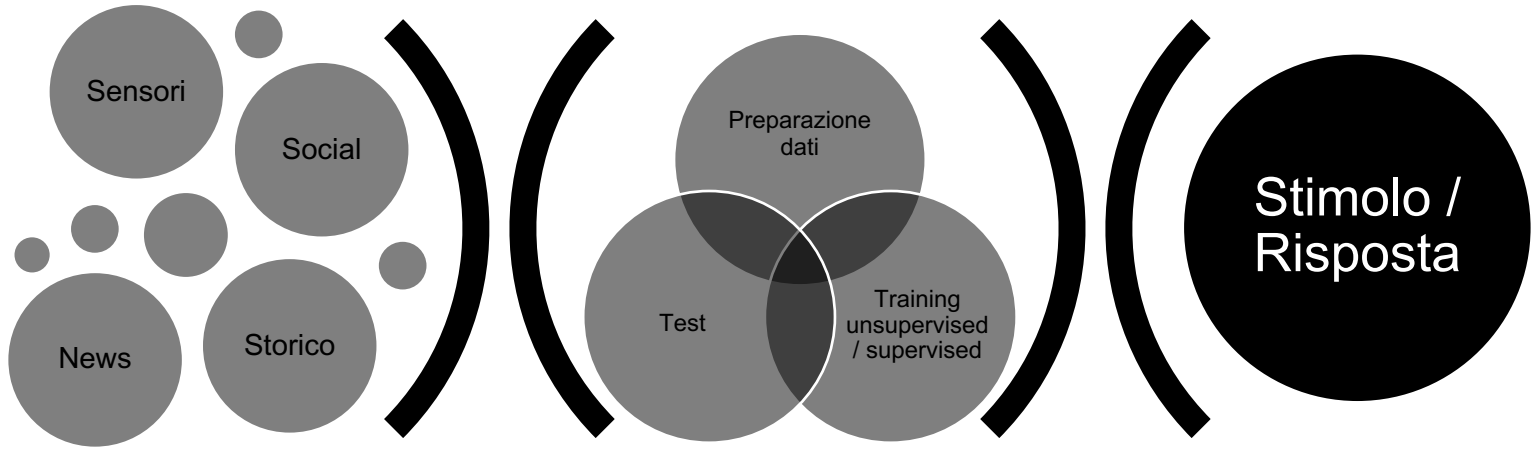
Intelligenza Artificiale e Cybersecurity

Il buono, il brutto, il cattivo

DXC.technology

Intelligenza artificiale e Machine Learning

Un rapido riassunto per introdurre il tema



Raccolta dati | Addestramento | Inferenza

Tradizionale: Applicativi specifici per elaborare dati generici
IA/ML: Algoritmi generici addestrati con dati specifici

L'algoritmo di ML «impara» dai dati a identificare una specifica dinamica o a riconoscere determinate caratteristiche presenti nei dati

Il sistema è pronto: ricevendo in ingresso dei dati appartenenti alla stessa distribuzione/dinamica, sarà in grado di riconoscerli/catalogarli

Quali usi per l'IA

Dal punto di vista tecnico, possiamo indicare alcune famiglie di applicazioni

Riconoscimento

- Riconoscimento vocale
- Riconoscimento immagini
- Identificazione SPAM e malware

Previsioni

- Previsione serie temporali
- Prevenzione guasti
- Variazioni baseline

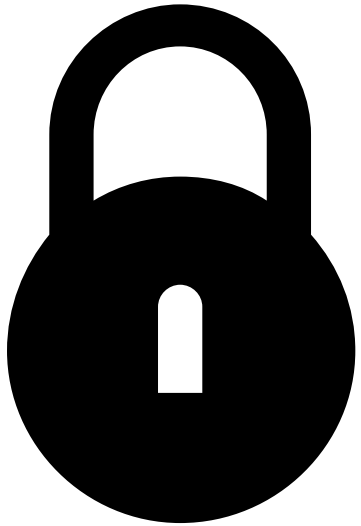
Suggerimenti

- Prodotti suggeriti
- Sistemi esperti

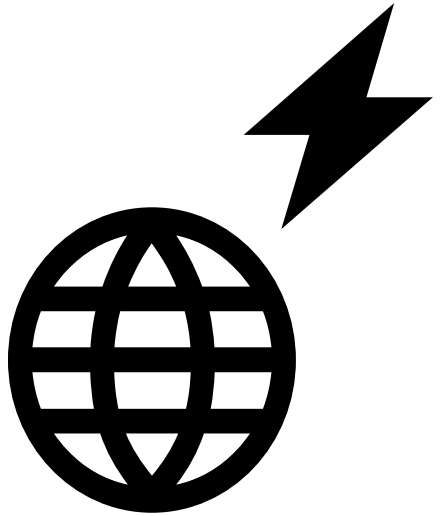
Comportamenti intelligenti

- Giochi (Go…)
- Agenti intelligenti
- Guida autonoma

L’intelligenza artificiale è intrinsecamente dual use



Rafforzare le difese di un’organizzazione.



Potenziare le capacità di attacco

Intelligenza artificiale nei sistemi di protezione

Identificazione del bersaglio
Esplorazione delle vulnerabilità
- Tecniche
- Umane

Scelta del vettore di attacco

Preparazione del vettore
Attivazione dell'attacco
Evidenza che l'attacco ha avuto successo

Attivazione accesso remoto
Esplorazione della rete / degli asset
Mantenimento della presenza
Disattivazione sistemi di sicurezza

Accesso ed esfiltrazione dati sensibili
Manomissione sistemi

Protezione potenziata dall'AI

«Powered by AI» è la frase che ormai si trova su ogni prodotto di sicurezza. Quali sono i benefici?

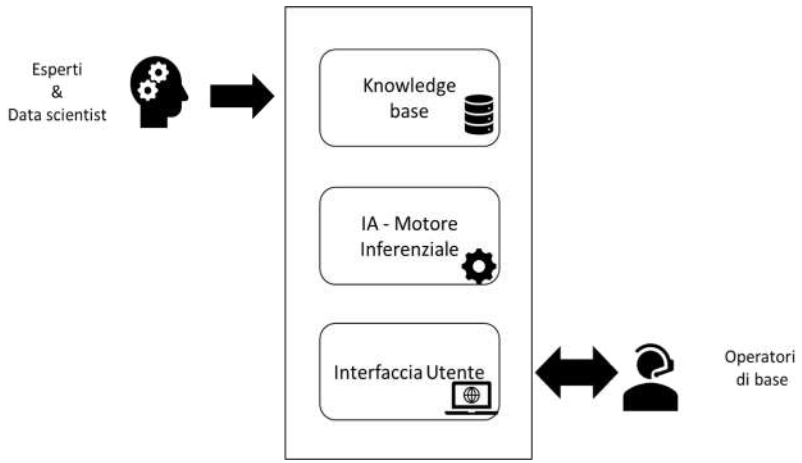
Rilevazione

Il principale vantaggio dell'AI: identificare **relazioni non immediatamente evidenti** in grandi moli di data

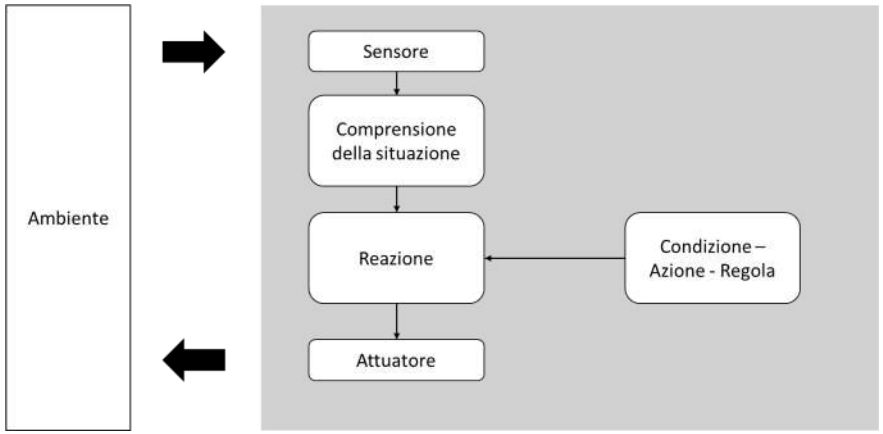
- Riconoscimento baseline
- Identificazione di attività anomale
- Riconoscimento pattern (es. filtri antispam)

Supporto decisionale

Sistemi esperti basati su moderne tecniche di IA possono aiutare ad aumentare l'efficacia degli esperti umani



Agente intelligente



AI confine tra attività civili e militari, gli agenti intelligenti possono «autonomamente» attivare contromisure

Abbiamo risolto ogni problema?

L’Intelligenza Artificiale è un sistema automatico, non esente da vulnerabilità

Il sistema può essere battuto

Non sfugge al primo teorema dell’informatica:
garbage in, garbage out

E’ uno strumento che affianca l’esperto umano, non lo sostituisce

AI nel «lato oscuro»

Framework IA
Tensor Flow, CNTK, Caffè …

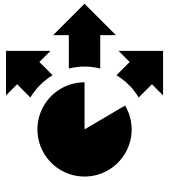
Attacchi consolidati
Zero day, Malware,
Trojan, X-script, SQL-I

Social Engineering
FB, Linkedin, Instagram…

Weaponization

Welcome to the dark side!

AI nelle mani dei «bad actors»



Espansione delle minacce esistenti

- Automatizzazione delle attività
- Maggiore scalabilità degli attacchi
- Personalizzazione su larga scala

Sviluppo di nuove minacce

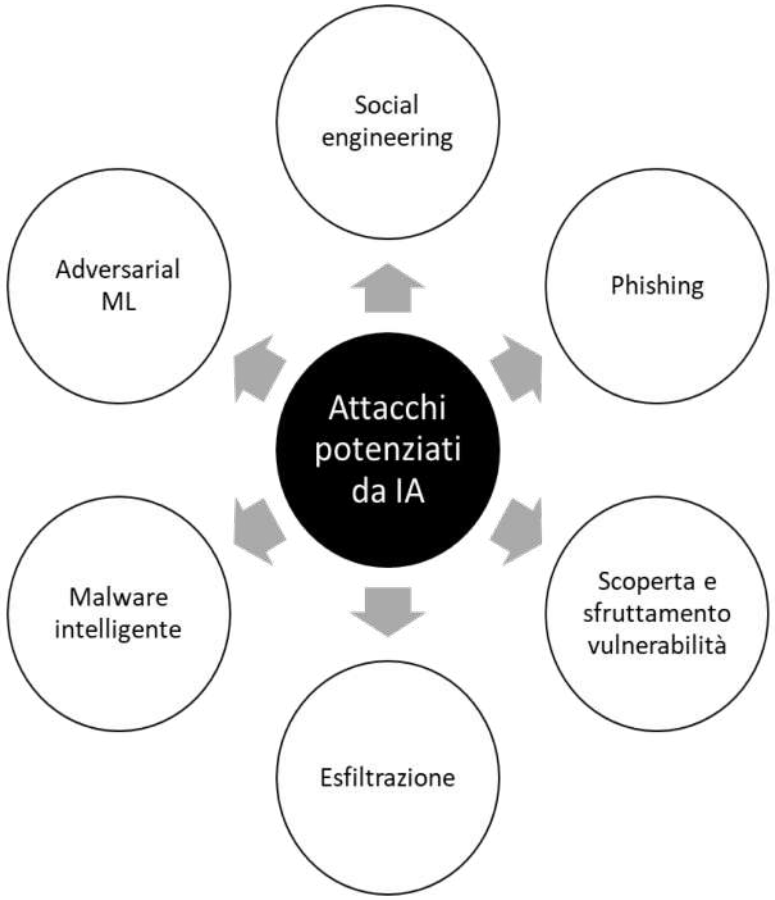
- Deep fake
- Impersonificazione
- Attacchi all'IA

Evoluzione delle minacce esistenti

- Agenti intelligenti
- Mascheramento
- Violazione di sistemi di sicurezza (Capcha anyone?)

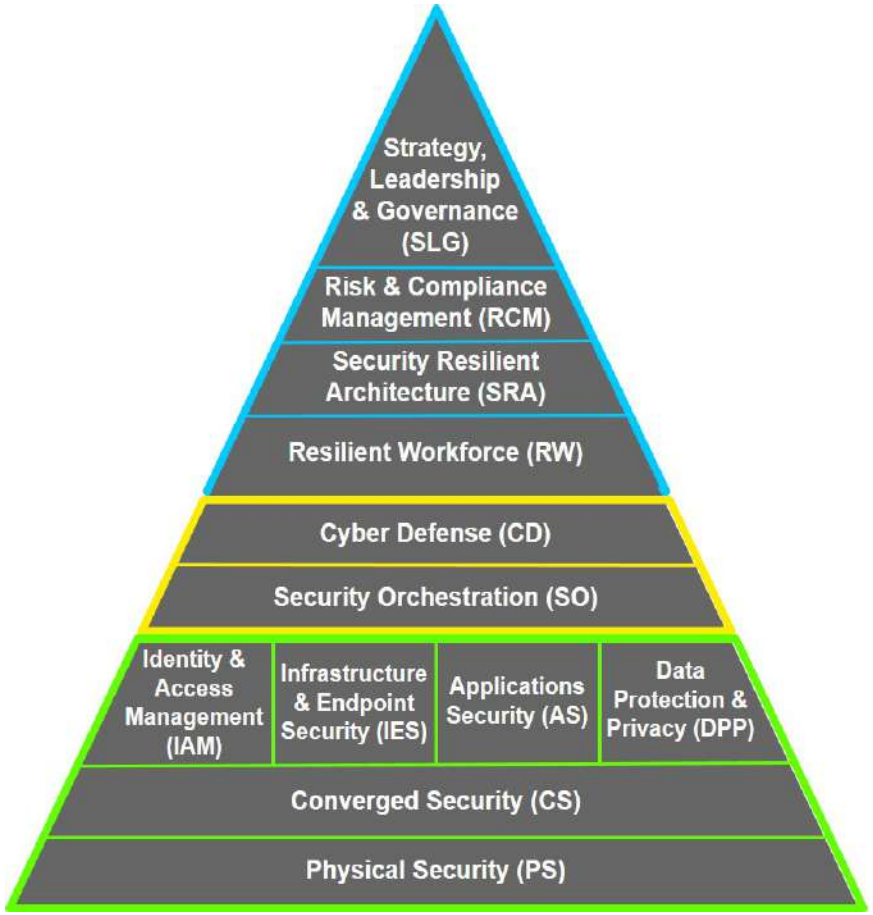
Una corsa agli armamenti?

La «corsa agli armamenti» che vede attacco e difesa confrontarsi già da decenni nello spazio cyber, è destinata ad estendersi all'impiego dell'IA



Come prepararsi?

L'utilizzo di framework consolidati mantiene la sua importanza



- Valutazione del rischio, esteso all'impiego di sistemi IA, anche quando non usati in ambito sicurezza
- Revisione delle esigenze di formazione (e se il malware vi… telefonasse?)
- Identificazione nuovi scenari di attacco

- Comprensione delle capacità e dei limiti dei sistemi di difesa «powered by IA»
- Identificazione nuovi use case, IoC, IoA relativi alle nuove minacce

- Revisione e adattamento tecnologico sulla base della nuova analisi dei rischi
- Revisione vulnerabilità fisiche

Grazie e… Via alla discussione