Luiss
Libera Università Internazionale
degli Studi Sociali Guido Carli

L’uso dell’intelligenza artificiale nella Cyber Threat Intelligence

14 maggio 2024

Elisabetta Pietrocarlo

LUISS

Premessa.
Cybersecurity, Cyber Threat Intelligence e Intelligenza Artificiale

- Il nucleo duro della *cybersecurity* è la **prevenzione del rischio** e il **contenimento degli effetti negativi** che deriverebbero da un incidente informatico
  - attenta mappatura preventiva delle minacce cibernetiche (***risk assessment***)
  - razionale organizzazione delle risorse umane e strumentali al fine di ridurre l'esposizione ai fattori di rischio (***risk management***)

Premessa.
Cybersecurity, Cyber Threat Intelligence e Intelligenza Artificiale

- Queste attività, previste nell'ambito del quadro normativo in materia di *cybersecurity*, incontrano sempre maggiori ostacoli, tra cui:

➢ **Incremento** del numero di **attacchi** cibernetici

➢ Attacchi cibernetici sempre più **sofisticati**

➢ Attacchi cibernetici sempre più **nocivi** (progressiva digitalizzazione)

Premessa.
Cybersecurity, Cyber Threat Intelligence e Intelligenza Artificiale

Rafforzare la *cybersecurity* attraverso le attività di ***Cyber Threat Intelligence*** basate sull'**Intelligenza Artificiale**?

Premessa.
Cybersecurity, Cyber Threat Intelligence e Intelligenza Artificiale

- Alcuni riferimenti normativi…

➢ **Direttiva NIS 2**

❖ Considerando n. 51: Gli Stati membri dovrebbero incoraggiare **l'uso di ogni tecnologia innovativa**, **compresa l'intelligenza artificiale**, il cui utilizzo potrebbe **migliorare l'individuazione e la prevenzione degli attacchi informatici**, consentendo di **destinare in modo più efficace risorse per affrontare gli attacchi informatici**. Gli Stati membri dovrebbero pertanto incoraggiare, nelle loro strategie nazionali per la cibersicurezza, le attività di ricerca e sviluppo volte a facilitare l'uso di tali tecnologie, in particolare quelle relative agli strumenti automatizzati o semiautomatizzati nella cibersicurezza, e, se del caso, la condivisione dei dati necessari per formare gli utenti di tali tecnologie e migliorarle. L'utilizzo di tutte le tecnologie innovative, compresa l'intelligenza artificiale, dovrebbe rispettare il diritto dell'Unione in materia di protezione dei dati, compresi i principi di protezione dei dati con riguardo all'accuratezza, alla minimizzazione dei dati, all'equità e alla trasparenza, nonché alla sicurezza dei dati, come la più recente crittografia. I requisiti di protezione dei dati fin dalla progettazione e predefiniti di cui al regolamento (UE) 2016/679 dovrebbero essere pienamente rispettati»

Premessa.
Cybersecurity, Cyber Threat Intelligence e Intelligenza Artificiale

- V. inoltre

➢ **DDL Cybersicurezza**

❖ Amplia le funzioni della Agenzia per la Cybersicurezza Nazionale (ACN) [nuova lett. m-*quater*), art. 7, co. 1, d.l. 82/2021 conv. in l. 109/2021]

❖ L'Agenzia «promuove e sviluppa ogni iniziativa, anche di partenariato tra soggetti pubblici e privati, volta a **valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale**, anche al fine di favorire un uso etico e corretto dei sistemi basati su tale tecnologia».

Premessa.
Cybersecurity, Cyber Threat Intelligence e Intelligenza Artificiale

- V. inoltre

➢ **Strategia Nazionale di Cybersicurezza 2022-2026**

❖ tra gli obiettivi da perseguire: «la **conoscenza approfondita del quadro della minaccia cibernetica** e il possesso di adeguati strumenti tecnici, competenze specialistiche e capacità operative, in capo agli attori a vario titolo coinvolti»

❖ L'ulteriore **rafforzamento della *situational awareness*** mediante il monitoraggio continuo degli eventi cibernetici e la tempestiva condivisione delle connesse risultanze, secondo gli specifici ambiti di competenza, costituisce, infatti, condizione necessaria ai fini dell'**incremento** delle **capacità nazionali di difesa, resilienza, contrasto al crimine informatico e *cyber intelligence***. A tal fine, appare essenziale il **costante scambio informativo** pubblico-privato e pubblico-pubblico, anche mediante l'introduzione di **canali di comunicazione protetti** e di un **sistema integrato di gestione del rischio *cyber*** per identificare e analizzare vulnerabilità, minacce e rischi in chiave previsionale e programmatica

La Cyber Threat Intelligence: un inquadramento

- In linea generale, la *Cyber Threat Intelligence* (CTI) consiste in un **processo di raccolta, analisi e interpretazione di informazioni per identificare, monitorare e anticipare le minacce informatiche**.
- «L'impiego di tecniche di *intelligence* rappresenta un **complemento essenziale** ai classici presidi di *cybersecurity*» (Rapporto Clusit 2020)

La Cyber Threat Intelligence: un inquadramento

- I *security analysts* elaborano la *threat intelligence* attraverso la **raccolta**, da diverse fonti, di informazioni sulle minacce non elaborate e correlate alla sicurezza; successivamente, gli stessi procedono all'**analisi** dei dati raccolti al fine di **identificare** corrispondenze, collegamenti e ogni altro elemento utile a individuare minacce effettive o potenziali.

- Le informazioni che ne derivano rappresentano un **bagaglio conoscitivo** di estrema importanza, in quanto:
  - riguardano le **specifiche vulnerabilità** del contesto organizzativo di riferimento (e non relative, ad esempio, a elenchi di *malaware* comuni);
  - sono **estremamente dettagliate**, attenendo tanto alla **tipologia** di minacce per l'organizzazione quanto agli **autori** dei possibili attacchi, nonché alle **tecniche** utilizzate e agli **indicatori di compromissione** (IoC);
  - consentono agli analisti di assegnare la **priorità** alle minacce e di valutare l'adozione di nuove **misure di sicurezza**.

- Ulteriore elemento essenziale della CTI è l'***information sharing***: scambio di informazioni allargato funzionale a diffondere la consapevolezza della minaccia cibernetica e a rafforza la capacità sistemica di prevenirla e contrastarla

La Cyber Threat Intelligence: finalità

➢ **Prevenzione dei *cyberattack***

- Anzitutto la CTI risponde a un approccio di carattere **proattivo** che consente di comprendere le **minacce** e le vulnerabilità **prima che gli aggressori le sfruttino** nonché di studiare gli **attori** stessi delle minacce, i loro obiettivi e i metodi che impiegheranno in attacchi futuri

- Grazie alla CTI, potranno essere adottate **misure preventive specifiche**

- Esempio: un particolare *threat actor*, noto per prendere di mira le aziende utilizzando un *malware* o un metodo di attacco specifico, può essere identificato precocemente e, di conseguenza, i sistemi di rilevamento delle intrusioni possono essere orientati alla ricerca specifica di tali modelli

- Grazie alla CTI è inoltre possibile identificare le **minacce cyber più sofisticate** che riescono a eludere le misure di sicurezza tradizionali

La Cyber Threat Intelligence: finalità

➢ **Gestione degli attacchi in corso**

- In caso di attacchi, la CTI fornisce le **informazioni specifiche** sulle **minacce** coinvolte, consentendo di **rispondere** efficacemente e tempestivamente attraverso misure volte a mitigare gli effetti negativi

➢ **Suggerimenti strategici**

- Grazie alle informazioni raccolte nell'ambito della CTI, la *leadership* potrà assumere **decisioni informate** e implementare **piani di sicurezza** *ad hoc* per prevenire, rilevare e rispondere efficacemente a potenziali attacchi informatici, tenendo conto delle **specifiche modalità** utilizzate dai *threat actor*

La Cyber Threat Intelligence: esempi concreti

- creazione di *account* e-mail o di profili *social*
- accesso in *forum* aperti o riservati
- accesso *dark market*
- interazione con *threat actor*
- download o acquisizione di *data leaks* o *data breach*
- catalogazione di *virus*

L’Intelligenza Artificiale nella Cyber Threat Intelligence

- L’Intelligenza Artificiale (AI) presenta **enormi potenzialità** nel campo della CTI
- Sono note le straordinarie **capacità analitiche** dei sistemi di AI, specie se basati sul ***machine learning*** → fondamentali per assistere gli analisti che spesso, ad oggi, non hanno la capacità di analizzare la **mole di informazioni** in loro possesso

➢ Esistono già dei sistemi di AI sviluppati proprio per la CTI, volti ad automatizzare la **raccolta** e **l’elaborazione dei dati** in vista della rilevazione di *pattern* → ciò consente di **automatizzare la profilazione di minacce e *threat actor***, l’elaborazione di **bollettini** da condividere (*information sharing*) nonché la **risposta** agli incidenti

L’Intelligenza Artificiale nella Cyber Threat Intelligence

- Ancora più promettenti sono le applicazioni basate su **tecniche di AI generativa**, le quali rappresentano un valore aggiunto per molteplici attività di CTI:

➢ raccolta e analisi dei dati

➢ correlazione tra incidenti e minacce

➢ rilevazione delle minacce (es. campagne di *phishing*)

➢ capacità di adattamento nel tempo

L'Intelligenza Artificiale nella Cyber Threat Intelligence: un esempio concreto

- '**IntelQuery**' – prima applicazione italiana di AI per la CTI, ideata nell'ambito del progetto Double Extortion Platform, un osservatorio sul fenomeno del *ransomware* istituito nel 2020
- Si tratta di un sistema di AI basato sul *machine learning* e addestrato con dati provenienti dal terreno criminale, dati di *cyber intelligence* e modelli di estorsioni cibernetiche
- Esso è così in grado di **analizzare** puntualmente i **modelli di attacco** e, di conseguenza, **identificare** e **segnalare** in le **minacce** affinché possano essere **gestite**
- A livello operativo, il sistema è impostato per rispondere a diverse **domande**, quali, tra le altre:
  - «chi ha colpito il *target X?*»
  - «*quali dati sono stati rubati durante l'estorsione di X?*»
  - «quali estorsioni hanno colpito un determinato settore?»

L’Intelligenza Artificiale nella Cyber Threat Intelligence: un bilancio

- I vantaggi della CTI:

➢ maggiore precisione e rapidità di analisi;

➢ razionale sfruttamento del patrimonio informativo;

➢ automatizzazione dei processi;

➢ rafforzamento *cybersecurity ex ante;*

➢ migliore gestione eventuali attacchi

L'Intelligenza Artificiale nella Cyber Threat Intelligence: un bilancio

- Emergono, al contempo, alcuni **profili problematici** che non trovano una compiuta risposta a livello normativo:

➢ non è sempre chiara la **qualificazione giuridica** delle attività di *cyber intelligence*, sebbene si tratti di azioni poste in essere a scopo difensivo e preventivo di possibili *cyberattack*

➢ Spunti molto interessanti nel documento rilasciato dalla ***Cybersecurity Unit* del U.S. *Department of Justice*** nel febbraio 2020: alla luce degli interrogativi posti dalle organizzazioni private, suggerisce alcune ***best practice**** da seguire al fine di non incorrere in violazioni del diritto penale federale, ad esempio, nelle attività di **raccolta di informazioni** sulle minacce informatiche all'interno di *forum* frequentati da cybercriminali ovvero di *Dark Market*

  ➢ * Es.: ***Create «Rules of Engagement»; Be prepared to be investigated; Practice Good Cybersecurity***

L'Intelligenza Artificiale nella Cyber Threat Intelligence: un bilancio

- I dati ottenuti dagli analisti grazie alla CTI potrebbero essere **personali** (normativa *data protection*; conservazione dato; verifica della fonte)
- L'***Information Sharing*** sulla CTI è essenziale ma rimessa alla **volontarietà** (tema della reputazione; *data protection*)
- Laddove si utilizzi un sistema di AI, occorre prestare particolare attenzione alla **qualità dei dati** forniti in *input* (*bias*; *garbage-in/out*; rappresentatività del set di dati – v. *AI Act*; Considerando n. 51 Direttiva NIS: normativa *data protection* + '*privacy-by-design*')
- Il sistema di AI deve avere una **funzione di supporto** e non di sostituzione dell'analista (generale approccio *AI Act*)

L'Intelligenza Artificiale nella Cyber Threat Intelligence: un bilancio

- **Comunicazione con gli *Internet Service Providers* e le *Big Tech***
  - assicurare l'istaurazione di effettivi canali comunicativi a fronte di richieste di informazioni da parte dell'organizzazione che svolge attività di CTI (ad esempio necessarie per risalire agli autori dell'attacco; titolari indirizzo IP) ovvero di adozione di determinati provvedimenti (come il *takedown*, cioè la chiusura del dominio o del *sito web* intercettato)

- **Rapporti con l'autorità giudiziaria**
  - scambio di informazioni prima dell'apertura di un procedimento penale (a partire da quale momento?; quale consistenza delle prove raccolte?)
  - modalità di acquisizione e di utilizzabilità delle prove raccolte all'esito della CTI nel processo penale

Grazie per l'attenzione!

epietrocarlo@luiss.it