WHITE PAPER

Utilizzare l'intelligenza artificiale per contrastare le minacce informatiche

Rafforzare chi si difende e disarmare chi attacca

Sintesi

Fino a qualche anno fa, gran parte dei dibattiti sull'intelligenza artificiale (AI) si basavano su aspetti più teorici che pratici. Oggi invece l'innovazione dell'AI e gli impatti positivi e negativi che può avere sulle organizzazioni stanno avanzando a un ritmo senza precedenti. Nella cybersecurity, l'avvento di nuovi strumenti di AI efficaci e innovativi, e il loro utilizzo da parte dei criminali informatici, ha reso più complicata e urgente la protezione delle organizzazioni e delle loro infrastrutture digitali dalle nuove minacce. La buona notizia è che i vendor di cybersecurity applicano da anni varie tecnologie AI. Ma se il futuro sarà animato da cattivi attori che utilizzano tattiche basate su AI, è essenziale che i responsabili e i team della sicurezza e dell'IT trasformino le loro strategie di security per rispondere a queste sofisticate minacce basate su AI.

Innovare per fortificare

Le organizzazioni oggi avviano regolarmente nuove iniziative di digitalizzazione e nel farlo espandono le loro superfici d'attacco. Iniziative come l'adozione del cloud, l'abbattimento dei gap tra Information Technology (IT) e Operational Technology (OT), il proliferare di dispositivi Internet-of-Things (IoT) che si connettono alla rete o la realtà della forza lavoro ibrida stanno mettendo a dura prova le risorse dei team di sicurezza e IT in molte organizzazioni. E ora, l'uso di strumenti AI da parte di cattivi attori sta aggravando una situazione già difficile e dinamica.

Di recente, alcuni criminali hanno utilizzato dei deepfake del CFO di un'azienda e di altri dipendenti in una videochiamata convincendo un dipendente a effettuare un bonifico di 25,6 milioni di USD.[1]

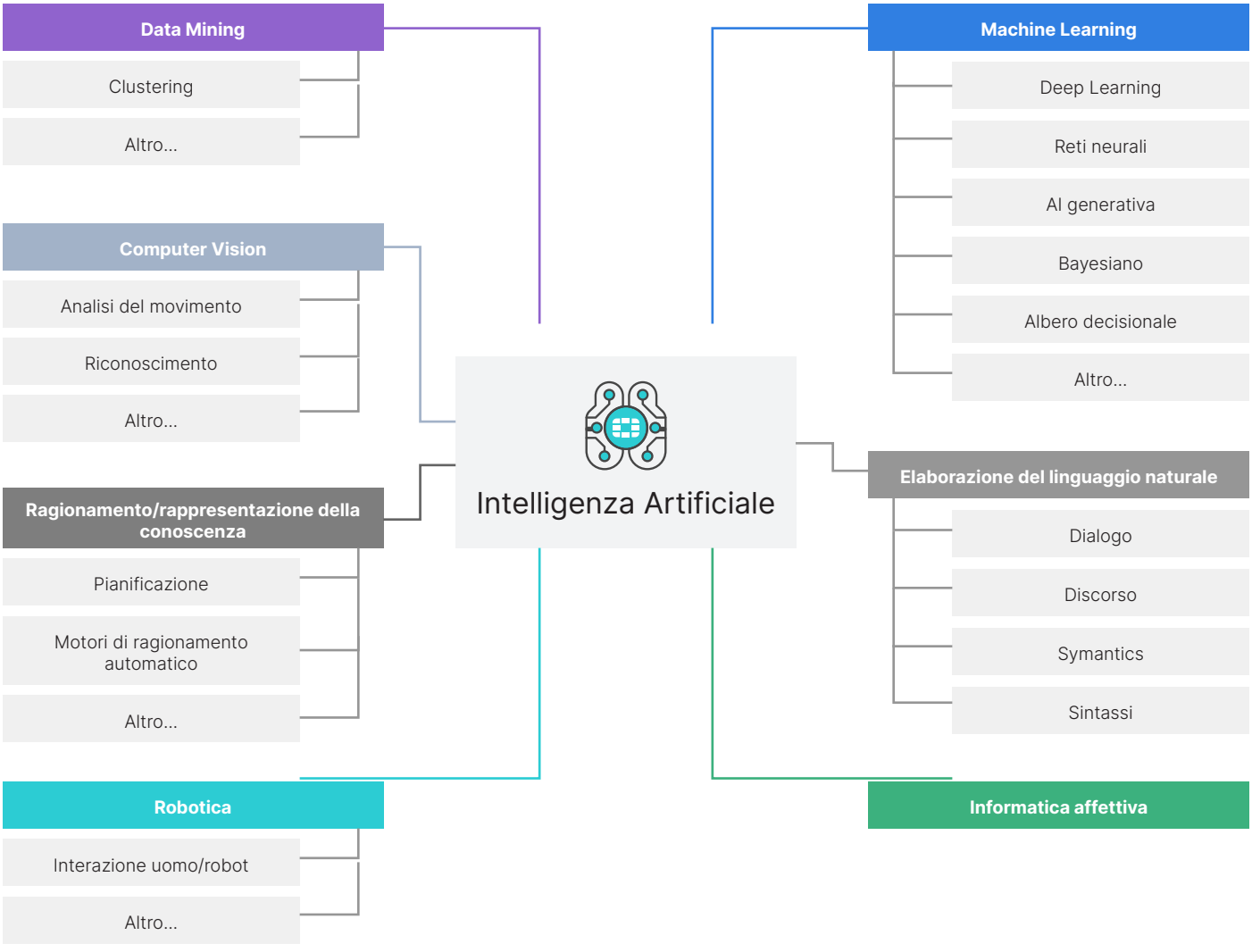


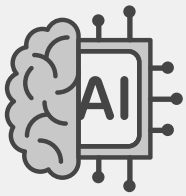
Figura 1: Sottocampi o aree di applicazione dell'intelligenza artificiale

L'uso dell'AI da parte di chi attacca

Gli hacker oggi sfruttano le capacità dell'AI per sviluppare e utilizzare minacce nuove, più avanzate e convincenti, tra cui le minacce zero-day. Grazie all'AI, gli attacchi possono essere più mirati e lanciati con una rapidità prima impossibile. Ecco alcuni effetti prodotti dall'AI quando viene usata da cattivi attori:

- Le tecnologie AI, come i trasformatori generativi preaddestrati (GPT) o l'AI generativa (GenAI), stanno rendendo più facile l'uso degli attacchi da parte di criminali meno preparati. Oggi, con questa tecnologia, una persona di qualsiasi parte del mondo che non parla inglese può creare attacchi di phishing e social engineering via email con una sintassi inglese fluente e naturale.
- L'AI consente di creare nuovi codici nocivi e di abbreviare e semplificare di molto lo sviluppo di nuove minacce informatiche.
- L'uso della tecnologia deepfake da parte di cattivi attori ha già destabilizzato la classe politica e l'elettorato, rendendo possibile il cybercrime su larga scala.
- L'AI si può usare per rilevare e sfruttare più rapidamente le vulnerabilità delle applicazioni, e questo fa aumentare i rischi per le supply chain delle organizzazioni in tutto il mondo.
- Con l'AI si possono creare varianti adattive di malware e lanciare attacchi a sciame e multivettoriali coordinati.

Oggi, le tattiche di AI nocive coprono l'intero ciclo di vita dell'attacco delineato nel framework MITRE ATT&CK. Il MITRE ha sviluppato una base di conoscenze chiamata ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) che descrive in dettaglio le tattiche e le tecniche avversarie basate su AI.[2]



Gli scienziati informatici della University of Illinois Urbana-Champaign hanno testato l'utilizzo di Chat GPT-4 di Open-AI in collaborazione con LangChain e il browser web Playwright come agente nocivo per scansionare i siti web alla ricerca di vulnerabilità e per comprometterli senza l'intervento umano. Gli autori hanno dichiarato che lo strumento è stato in grado di eseguire un processo in 38 fasi associato a un attacco SQL Union.[3]

Sfide amplificate

L'uso dell'AI da parte dei criminali informatici amplifica le sfide generate dalla continua evoluzione delle minacce moderne, aumentando il carico sui già oberati team di sicurezza e IT. Proteggere da queste nuove minacce un ambiente di rete e una superficie d'attacco in espansione è più complicato che mai a causa di:

- Visibilità isolata di alcuni ambienti
- Mancanza di un'applicazione e di un'esecuzione centralizzata e coordinata delle policy
- Utilizzo di vari strumenti e console di sicurezza disparati che rendono il monitoraggio, il triage degli avvisi e l'indagine e la risposta agli incidenti molto dispendiosi in termini di tempo
- Difficoltà continue nel reclutare e fidelizzare professionisti competenti in sicurezza

Per gestire l'AI con efficacia, le organizzazioni devono ridurre complessità e attriti, semplificando anche le operazioni.

L'uso dell'AI da parte di chi si difende

La convergenza tra AI e cybersecurity non rappresenta solo un avanzamento tecnologico. È un'evoluzione necessaria e sempre più urgente che può aiutare le organizzazioni a migliorare la difesa delle loro moderne superfici d'attacco contro le nuove minacce. Molti fornitori di cybersecurity applicano da anni varie tecnologie AI. Ad esempio, Fortinet si dedica alla ricerca e all'utilizzo di tecnologie AI da oltre 10 anni e continua ad adattarsi e a rispondere alle sfide generate dalle moderne superfici di attacco con le sue difese basate su tecnologie AI.

Intelligence sulle minacce basata su AI

Il principale utilizzo dell'AI nel campo della cybersecurity è per il rilevamento e la protezione dalle minacce. Un elemento chiave del rilevamento e della protezione dalle minacce è la creazione e il continuo miglioramento dell'intelligence sulle minacce. L'uso applicato delle tecnologie AI è decisivo per la raccolta, l'analisi, la correlazione e, infine, la formulazione dei dati in un'intelligence utilizzabile. Questo tipo di intelligence sulle minacce con tecnologia AI si può utilizzare tramite le integrazioni per rispondere a un'ampia serie di vettori e tipi di minacce, abilitate da AI o meno. Il modo in cui un vendor applica l'AI e la sua ampiezza di fonti di dati e di dati è importante. Più un vendor ha visibilità sui propri dati, più i modelli AI possono apprendere da tale visibilità.

Capire la natura dell'intelligence sulle minacce che alimenta l'infrastruttura di sicurezza primaria della tua organizzazione è un ottimo punto di partenza per comprendere come i tuoi vendor utilizzano la tecnologia AI. Un'area importante è anche l'infrastruttura del firewall, che rappresenta la prima linea di difesa.

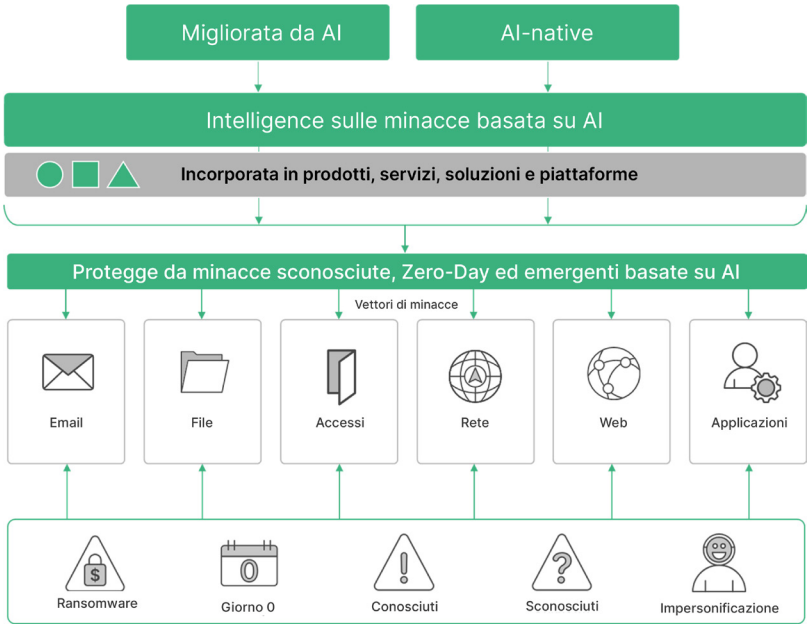


Figura 2: Capacità migliorate con AI e capacità AI-native incluse nella formulazione dell'intelligence sulle minacce

Capire la natura dell'intelligence sulle minacce che alimenta l'infrastruttura di sicurezza primaria della tua organizzazione è un ottimo punto di partenza per comprendere come i tuoi vendor utilizzano la tecnologia AI. Un'area importante è anche l'infrastruttura del firewall, che rappresenta la prima linea di difesa.

Gli attuali Next-Generation Firewall (NGFW) offrono un insieme di funzionalità che vanno oltre i firewall tradizionali. Ad esempio, il tuo firewall può avere la prevenzione delle intrusioni integrata, la protezione anti-malware con antivirus e sandboxing, nonché funzionalità di sicurezza web come il filtraggio DNS e URL. Chiedi al vendor in che modo viene applicata l'AI per migliorare le capacità del firewall, valutando le sue diverse funzioni e l'importanza di ognuna di esse.

Se il vendor non è in grado di fornire informazioni sull'uso dell'AI, è opportuno velocizzare il ciclo di refresh e affidarsi a vendor che stanno effettivamente usando le tecnologie più recenti per migliorare l'efficacia delle loro soluzioni.

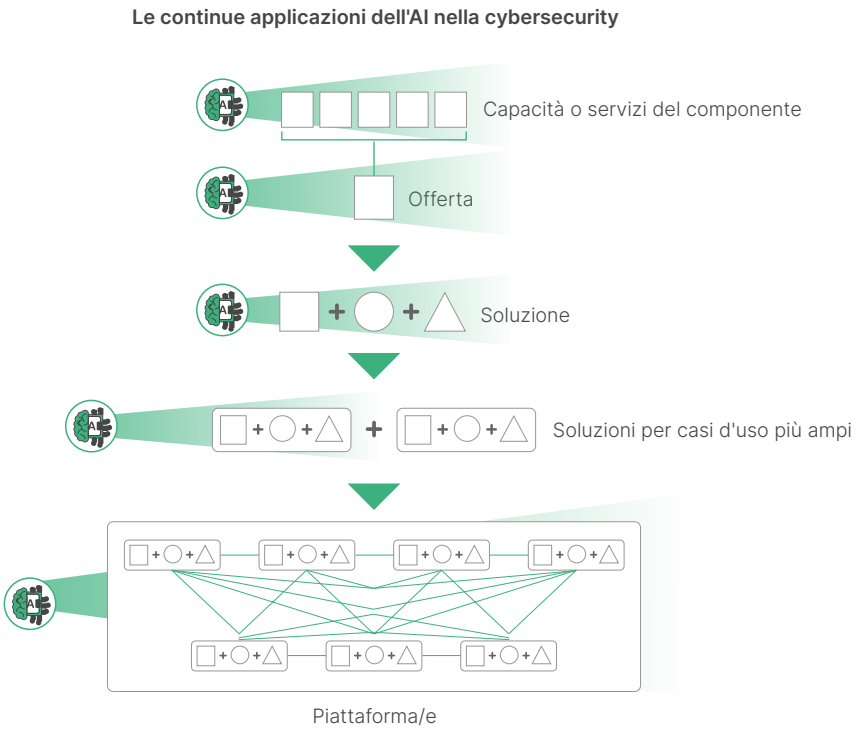


Figura 3: L'applicazione dell'AI e dell'intelligence sulle minacce, dal componente alla piattaforma

Oggi le soluzioni potenziate da AI possono contribuire a migliorare i risultati con vantaggi sia per i vendor che per i clienti:

- **Firewall:** i firewall NGFW includono funzionalità di sicurezza spesso supportate da vari modelli AI operativi in background. Funzionalità come la prevenzione delle intrusioni, l'antivirus, la sicurezza web e il sandboxing in linea possono utilizzare tecnologie AI per rafforzare le singole funzionalità integrate nel firewall. Se i firewall mesh ibridi vengono combinati con NGFW, è possibile ottenere un doppio vantaggio: una protezione dalle minacce rafforzata da AI e miglioramenti nella visibilità del firewall e nella gestione centralizzata di policy e firewall.
- **Scansione dell'applicazione:** anche se i cattivi attori possono utilizzare l'AI per creare agenti nocivi, le soluzioni di scansione delle applicazioni e i penetration tester possono utilizzare la stessa capacità per trovare e correggere più rapidamente le vulnerabilità sia in fase di sviluppo che di produzione.
- **Rilevamento e risposta degli endpoint (EDR):** una soluzione EDR utilizza le reti neurali per riconoscere i pattern e attribuire un senso a tutti i dati degli eventi acquisiti su un endpoint, inclusi i dati su attività, processi, modifiche al registro e accessi alla memoria.
- **Gestione delle informazioni e degli eventi di sicurezza (SIEM):** un SIEM utilizza modelli di machine learning (ML) supervisionati e non, per eseguire sofisticate regressioni lineari come la regressione dei vettori di supporto, la regressione dei processi gaussiani e la regressione degli alberi decisionali. Inoltre, utilizza la tecnologia ML per eseguire vari algoritmi di clustering. Questa analisi aiuta la soluzione SIEM a identificare con precisione le minacce e le vulnerabilità, riducendo al minimo i falsi positivi. Le soluzioni SIEM utilizzano anche la tecnologia GPT e l'elaborazione del linguaggio naturale (NLP) per offrire un'esperienza guidata e con più informazioni al personale dei centri operativi di sicurezza. Gli analisti possono interrogare direttamente il motore AI e ottenere informazioni sulle minacce e indicazioni sulle azioni di risposta adeguate.
- **Analisi delle immagini:** la computer vision, il riconoscimento delle immagini e la tecnologia delle reti neurali sono combinati per l'analisi delle immagini. È possibile che vengano utilizzati anche algoritmi di prossimità. Le immagini in arrivo incorporate in un'email o scaricate da Internet possono essere scansionate per stabilire se presentano rischi o esposizioni. Queste immagini possono includere codici QR, immagini pornografiche, immagini violente ed estremiste o immagini con armi, alcol o droghe.
- **Test di penetrazione:** è possibile utilizzare Chat GPT4 di OpenAI per avanzare nei test di penetrazione, e numerosi video online mostrano come utilizzare il Large Language Model di Chat GPT4 per scrivere in pochi minuti script Python e Bash per i test di penetrazione.

Il potenziale dell'AI non si ferma alla formulazione e all'applicazione dell'intelligence sulle minacce basata su AI. Ad esempio, Fortinet usa le tecnologie AI per migliorare la piattaforma Fortinet Security Fabric e renderla ancora più proattiva, unificata e intelligente.

Cybersecurity basata su AI

Le nuove soluzioni di cybersecurity basate fin dall'origine su funzionalità AI vengono spesso definite "cybersecurity AI-native". Anche se non esiste una definizione standard del termine nel settore, gli strumenti di cybersecurity AI-native operano alla velocità della macchina. Ad esempio, l'analisi delle potenziali minacce, l'emissione di un verdetto e l'esecuzione delle azioni prescritte avvengono alla velocità della macchina. Eseguire le azioni più rapidamente comporta vantaggi sia dal punto di vista della cybersecurity che da quello commerciale. Gli strumenti di cybersecurity AI-native offrono di norma le seguenti caratteristiche:

- Modelli AI progettati ad hoc
- AI integrata nel core o come fondamento
- Apprendimento e adattamento continuo alle nuove minacce
- Esecuzione di azioni alla velocità della macchina
- Operatività in tempo reale

Casi d'uso e raccomandazioni

I team di sicurezza e IT esterni al settore della cybersecurity, devono capire che oggi i vendor di cybersecurity applicano l'AI e, più nello specifico, quale tipo di AI viene applicata, come viene applicata e in che modo l'AI genera vantaggi diretti per l'organizzazione.

La Figura 4 rappresenta i modi in cui i vendor di cybersecurity possono applicare le tecnologie AI nelle loro soluzioni, i processi di supporto e i diversi vantaggi. Puoi usare l'elenco della Figura 4 come guida per chiedere ai vendor in che modo la loro AI migliora la sicurezza dei clienti, in particolare contro le minacce basate su AI.

Se vuoi integrare l'AI nelle tue strategie di sicurezza, valuta le seguenti raccomandazioni.

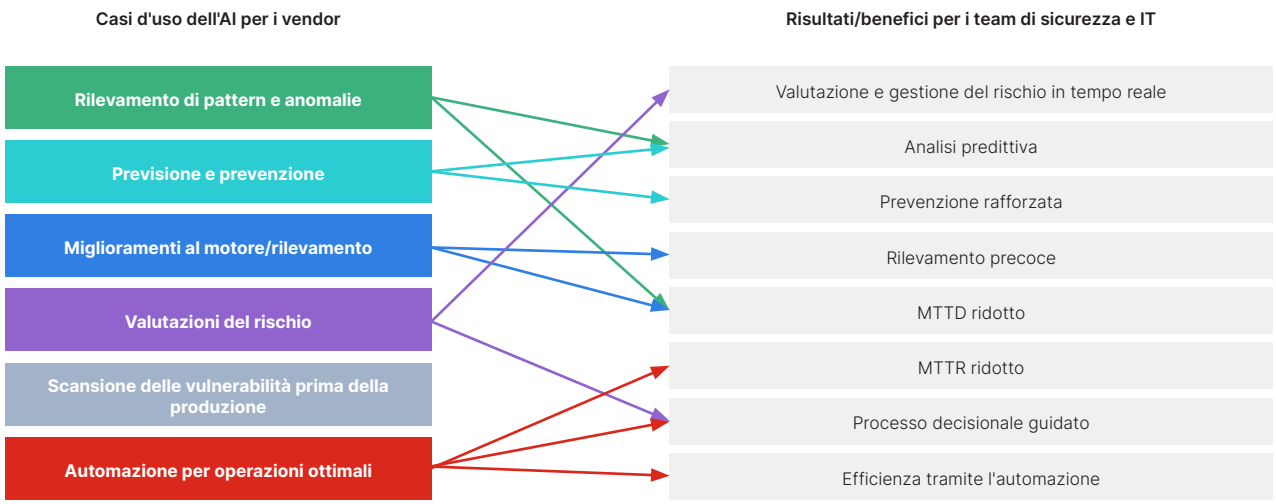


Figura 4: Fattori per l'utilizzo dell'AI da parte dei vendor e vantaggi per i clienti

Assegna la priorità all'AI

Metti l'intelligenza artificiale al primo posto nelle attività del tuo team. Valuta l'attuale consapevolezza del team sulle tecnologie e sui principi dell'AI. Imposta l'adozione dell'AI come obiettivo strategico per tutte le principali aree della tua infrastruttura di sicurezza e IT e dai priorità alle verifiche su tali aree. Considerato che un vendor può in qualche misura utilizzare l'AI nelle sue soluzioni, crea un questionario e una procedura per valutare i vendor in base ai meriti del loro know-how e della loro integrazione dell'AI.

Informati

I leader della sicurezza e IT hanno il compito di adottare misure per formare se stessi e i loro team sull'AI e su come usarla per migliorare le rispettive attività e le soluzioni che acquistano. Questa formazione sarà importante anche per riconoscere quando l'organizzazione sta attivamente testando o usando le tecnologie AI per i propri fini. I team saranno più in grado di porre le domande giuste su questi casi d'uso. Esistono molte risorse online che offrono un certo livello di formazione gratuita sull'AI. Una volta che i leader e i team hanno acquisito una formazione di base, può essere utile valutare contenuti di formazione online a pagamento o partecipare a corsi di formazione di organizzazioni di cybersecurity affidabili come SANS.

Continua a informarti

Rimani al passo con i nuovi sviluppi dell'AI applicata alla cybersecurity. Con il rapido progredire dell'innovazione, è facile rimanere indietro.

Verifica la tua infrastruttura di sicurezza

Valuta come utilizzare la tecnologia AI nella tua infrastruttura di sicurezza. Come prima cosa, considera quali vantaggi può avere l'organizzazione se utilizza le tecnologie AI per le sue linee di difesa principali. Quindi, esamina gli altri tipi di controlli che applichi. Per molti aspetti, questa verifica può procedere seguendo le attuali priorità di rischio dell'ambiente complessivo (in cui la priorità delle verifiche si basa sulle aree di maggior rischio).

Fai domande

Chiedi ai vendor di cybersecurity con cui collabori come utilizzano l'AI. Scopri quali tecnologie applicano, quali sono le modalità di applicazione e soprattutto che vantaggi offre l'AI ai clienti. Ecco alcune domande da cui iniziare:

- Quale visibilità sulle minacce e sulle relative fonti di dati utilizza la tua organizzazione per formulare l'intelligence sulle minacce che supporta i vostri prodotti, servizi e soluzioni?
- Come viene utilizzata l'AI nella formulazione dell'intelligence sulle minacce?
- Qual è l'esperienza della tua organizzazione sull'uso delle tecnologie AI nei vostri prodotti, servizi e soluzioni?
- Quale o quali tecnologie AI specifiche vengono applicate a questo prodotto, servizio o soluzione e come vengono applicate?
- Quali fonti di dati utilizza il prodotto, il servizio o la soluzione per il feed delle tecnologie AI?
- Come si addestra e si riqualifica il modello o i modelli AI?
- Esiste un modo per interagire direttamente con l'AI?
- Come ci si protegge dal data poisoning da parte di cattivi attori?
- In che modo la tua applicazione dell'AI contribuisce a:
  - Ridurre il rischio
  - Aumentare la prevenzione
  - Ridurre il tempo medio di rilevamento
  - Ridurre i falsi positivi
  - Supportare il triage degli avvisi e le indagini sugli incidenti
  - Ridurre il tempo medio di remediation
  - Aiutare gli analisti delle operazioni di sicurezza nelle loro attività quotidiane

Questo non è un elenco completo di domande sull'AI, ma una buona guida. Aggiungi o personalizza le domande in base alle specifiche esigenze della tua organizzazione.

Aggiungi l'AI ai criteri dei vendor

Fai in modo che l'uso dell'AI venga incluso nei documenti di richiesta di offerte. Usa le domande sopra e altre per chiarire l'uso dell'AI tra i vendor di cybersecurity. Questo consentirà non solo di chiarire come un determinato vendor utilizza le tecnologie AI per conto dei clienti, ma anche di confrontare le risposte per stabilire se l'applicazione dell'AI da parte di un vendor offre vantaggi reali alla tua organizzazione.

Conclusione

I leader e i professionisti della sicurezza e dell'IT devono avere più familiarità con le varie tecnologie connesse all'AI. È importante essere proattivi nel capire l'AI e il suo potenziale nella cybersecurity. Dato che molte soluzioni di sicurezza oggi provengono da vendor che usano l'AI, è importante capirne le varie applicazioni e i casi d'uso prima di includere in modo estensivo eventuali strumenti abilitati all'AI nella propria organizzazione. Prima di prendere decisioni di acquisto, è essenziale porre domande precise ai vendor su come sfruttano i benefici dell'AI nelle loro soluzioni. Capire il modo in cui le soluzioni integrano l'AI nelle operazioni IT e della sicurezza, aiuta a reagire alle sofisticate minacce attuali basate su AI.

[1] Heather Chen e Kathleen Magramo, Finance worker pays out $25 million after video call with deepfake "chief financial officer" CNN, 4 febbraio 2024.

[2] MITRE ATLAS Adversarial Threat Landscape for Artificial-Intelligence Systems.

[3] Richard Fang, et al, "LLM Agents can Autonomously Hack Websites," 6 febbraio 2024.

03 dicembre 2024 16:44 / 2604482-A-0-IT