How AI in Cybersecurity Addresses Challenges Faced by Today’s SOC Analysts

Valutiamo in che modo l'IA usata nella Cybersecurity supporta le sfide affrontate dagli analisti SOC ai nostri tempi.

16 Aprile 2021 Di Banu Yuceer 2 min lettura

Gli odierni Security Operations Center (SOC) devono gestire dati, strumenti e team sparsi in tutta l'organizzazione, rendendo difficile il rilevamento delle minacce e il lavoro di squadra. Ci sono molti fattori che guidano un lavoro di sicurezza complesso. Molte persone ora lavorano da casa con colleghi in luoghi lontani.

Anche il costo e la manutenzione degli strumenti legacy e la migrazione al cloud rendono tutto più complesso. Così fanno gli ambienti ibridi e i molteplici strumenti e fornitori in uso.

Tenendo conto di tutti questi fattori, il lavoro dell'analista medio è diventato più difficile che mai. Spesso, rintracciare un singolo incidente richiede ore o addirittura giorni di raccolta delle prove. È qui che entra in gioco l'intelligenza artificiale (AI) nella sicurezza informatica.

Gli analisti potrebbero dedicare molto tempo a cercare di raccogliere dati, setacciare gigabyte di eventi e log e individuare i pezzi rilevanti. Mentre cercano di far fronte all'enorme volume di avvisi, gli aggressori sono liberi di escogitare modi sempre più creativi per condurre gli attacchi e nascondere le loro tracce.

Approfondisci

Cosa può fare l'IA nella sicurezza informatica

L'intelligenza artificiale rende il SOC più efficace riducendo l'analisi manuale, la raccolta di prove e la correlazione delle informazioni sulle minacce, fornendo risposte più rapide, coerenti e accurate.

Alcuni modelli di intelligenza artificiale possono dire quale tipo di prove raccogliere e da quali fonti di dati. Possono anche individuare i rumori rilevanti, i pattern spot utilizzati in molti incidenti comuni e metterli in correlazione con i dati di sicurezza più recenti. L'intelligenza artificiale nella sicurezza informatica può generare una sequenza temporale della catena di attacchi per l'incidente. Tutto ciò apre la strada a una rapida risposta e riparazione.

Gli strumenti di sicurezza dell'IA sono molto efficaci nel trovare falsi positivi. Dopo tutto, la maggior parte dei falsi positivi segue schemi comuni. Steve Ocepek, Chief Technology Officer di X-Force Red Hacking, riferisce che il suo team vede gli analisti dedicare fino al 30% del tempo a studiare i falsi positivi. Se un'intelligenza artificiale può occuparsi prima di questi avvisi, gli esseri umani avranno più tempo e meno stanchezza quando si occupano delle attività più importanti.

L'elemento umano nella sicurezza guidata dall'IA

Mentre la domanda di analisti SOC qualificati è in aumento, diventa sempre più difficile per i datori di lavoro trovarli e trattenerli. Dovresti invece mirare ad automatizzare completamente il SOC e non assumere affatto persone?

La risposta è no. L'intelligenza artificiale nella sicurezza informatica è qui per aumentare la produzione degli analisti, non per sostituirla. L'analista di Forrester Allie Mellen ha recentemente condiviso un ottimo punto di vista su questo problema.

In "Stop Trying To Take Humans Out Of Security Operations", Allie sostiene che il rilevamento di nuovi tipi di attacchi e la gestione di incidenti più complessi richiedono intelligenza umana, pensiero critico e creativo e lavoro di squadra. Spesso parlare in modo efficace con utenti, dipendenti e stakeholder può portare a nuove intuizioni laddove i dati sono carenti. Se utilizzato insieme all'automazione, l'IA rimuove gli elementi più noiosi del lavoro. Ciò consente agli analisti il tempo di pensare, ricercare e apprendere, dando loro la possibilità di stare al passo con gli aggressori.

L'intelligenza artificiale aiuta i team SOC a creare flussi di lavoro intelligenti, connettere e correlare i dati da diversi sistemi, semplificare i loro processi e generare informazioni su cui possono agire. Un'intelligenza artificiale efficace si basa su dati coerenti, accurati e semplificati. I flussi di lavoro creati con l'aiuto dell'IA generano a loro volta dati di migliore qualità necessari per riqualificare i modelli. I team SOC e l'IA nella sicurezza informatica crescono e migliorano insieme mentre si potenziano e si supportano a vicenda.

È ora di mettere l'IA al lavoro nel tuo SOC? Ponetevi prima queste domande.

Fonte:

https://securityintelligence.com/posts/ai-in-cybersecurity-addresses-challenges-soc-analysts/