Sfruttare il potere dell’XDR alimentato dall’AI

Molti professionisti della sicurezza informatica ritengono che nel prossimo futuro gli attacchi basati su intelligenza artificiale (AI) inizieranno ad aumentare. Stando ad AIMultiple, il 90% del personale dell’information security in USA e Giappone prevede un aumento delle campagne di attacco automatizzate dovuto, in gran parte, alla pubblica disponibilità della ricerca sull’AI, che gli attaccanti stanno sfruttando per i loro scopi malevoli.

In che modo gli attaccanti sfruttano l’AI

I risultati del sondaggio svolto da AIMultiple fanno sorgere una domanda importante: in che modo gli attaccanti usano l’AI per i loro obiettivi nefasti? Consideriamo due scenari di applicazione dell’AI. Nel primo, gli attaccanti usano l’AI per aumentare l’efficacia delle loro operazioni. Si continuano, infatti, a susseguire esempi in cui l’AI aiuta gli autori delle minacce a creare video ed e-mail sempre più convincenti e che portano gli utenti a fare quel “click”.

Inoltre, gli attaccanti possono usare l’AI per eludere il rilevamento e bypassare le tradizionali soluzioni di sicurezza. Nello specifico, AIMultiple ha notato che l’utilizzo del deepfake negli attacchi può consentire agli attaccanti di eludere le soluzioni di sicurezza biometrica, di passare inosservati alle protezioni dei social network e, infine, di ottenere l’accesso ai dati aziendali del destinatario dell’attacco.

Nel secondo scenario, gli attaccanti possono usare l’AI per identificare le potenziali opportunità di attacco nella fase di ricognizione. Per via della quantità di dati che i sistemi intelligenti possono raccogliere e analizzare in modo

autonomo, i tool basati sull'AI forniscono agli attaccanti un mezzo di identificazione delle vulnerabilità nelle reti, nei dispositivi e nelle applicazioni della vittima su larga scala, talvolta prima che i professionisti della sicurezza li rintraccino.

In assenza di soluzioni di monitoraggio in tempo reale, possono quindi essere in grado di muoversi in modo trasversale nella rete, estrapolare informazioni sensibili e aumentare la portata dell'attacco. L'AI può consentire agli attaccanti di automatizzare questi processi nella scelta dell'obiettivo e nella personalizzazione della sequenza di attacco, basandosi sulle specifiche della conformazione della rete della vittima, determinando elementi come i sistemi operativi in uso, rilevando i meccanismi di sandboxing e altre tattiche di difesa, nonché individuando il giusto payload da inviare.

Combattere l'AI con l'AI

In risposta a questi casi d'uso, le aziende possono contrastare l'abuso dell'AI con soluzioni basate sull'AI stessa, al fine di proteggere i loro sistemi e dati dagli attacchi automatizzati; tuttavia, le soluzioni di sicurezza tradizionali, che si basano sul triage manuale e l'investigazione, semplicemente non funzionano.

Come esempio, prendiamo il Security Information and Event Management (SIEM). Questi tool possono aiutare le aziende a centralizzare le informazioni sulle minacce trasversalmente ai loro ambienti. Tuttavia, il SIEM tende a generare una vasta gamma di alert e falsi positivi che sprecano il tempo dei professionisti della sicurezza e contribuiscono all'affaticamento del sistema di avvisi.

Se i SIEM potessero aiutare il personale a gestire tutti gli avvisi sarebbe fantastico, ma non è così. Semplicemente, i SIEM segnalano le potenziali minacce che richiedono un approfondimento da parte del personale per trovare

correlazioni tra gli avvisi generati al fine di determinare se la *minaccia è reale* e poi imbastire una risposta manuale.

Di conseguenza, i team di sicurezza devono ricorrere a processi manuali per comprendere cosa sta accadendo trasversalmente ai loro ambienti, dove gli attaccanti si stanno muovendo velocissimi grazie all'automazione nelle primissime fasi dell'attacco: tutti questi elementi generano un enorme svantaggio per i Defender.

Le soluzioni Endpoint Detection and Response (EDR) sono fondamentali per difendere gli endpoint, che rappresentano una porzione significativa della superficie di attacco di un'organizzazione, ma presentano anch'esse diverse lacune. Mentre l'EDR è di gran lunga migliore nel rilevare le minacce avanzate rispetto agli antivirus tradizionali e alle soluzioni antimalware, molti attaccanti hanno evoluto le loro campagne ben oltre l'individuazione dell'endpoint, oppure hanno progettato le loro operazioni al fine di ridurre al minimo l'attività dell'endpoint, rendendo l'EDR inefficace. All'EDR manca anche la capacità di correlare i rilevamenti dell'endpoint con la telemetria da asset non-endpoint, come suite per applicazioni, user personas e workload in cloud.

XDR alimentata con l'AI

Fortunatamente, le aziende non devono accontentarsi di soluzioni incomplete come SIEM ed EDR. Possono infatti scegliere una soluzione di Extended Detection and Response (XDR) basata su AI. L'XDR basata su AI estende continuamente il rilevamento delle minacce e il monitoraggio, insieme alla risposta automatizzata oltre gli endpoint, al fine di fornire correlazioni profondamente contestuali con la telemetria da applicazioni, tool di identificazione e accesso, containerizzazione di workload in cloud e molto altro.

L’XDR basata su AI comprende anche flussi di threat intelligence per consentire alle aziende di difendersi da attacchi noti, e utilizza l’AI e il machine learning (ML) per correlare automaticamente la telemetria trasversale a diversi tipi di asset, fornendo una cronologia completa dell’attacco in tempo reale. Questa funzionalità esonera gli analisti della sicurezza dalla necessità di gestire ogni alert generato, consentendo loro di concentrarsi più velocemente sulle minacce reali.

Molte aziende stanno passando a tool basati su Intelligenza Artificiale (AI) e Machine Learning (ML), al fine di consentire ai loro team di automatizzare il triage, l’investigazione e gli sforzi di risoluzione su larga scala. Oltre la metà (52%) dei dirigenti di aziende USA ha raccontato a PwC di aver accelerato i propri piani di adozione di AI/ML e una percentuale ancora maggiore (86%) ha affermato che AI ed ML sarebbero state le “tecnologie principali” usate nei loro ambienti entro la fine del 2021.

Inoltre, AI ed ML consentono ai team di sicurezza di farsi strada nel “rumore” prodotto dal flusso costante di alert di minacce, consentendo ai professionisti della sicurezza di perdere meno tempo nel passare al setaccio gli alert e nel cercare falsi positivi, mentre possono trascorrerne di più a migliorare la postura di sicurezza complessiva dell’azienda.

Le tecnologie AI ed ML sono eccellenti nell’analizzare set di dati su larga scala con un elevato grado di accuratezza per identificare eventi sospetti a una velocità e in una quantità che l’analisi umana non potrebbe eguagliare. Il vantaggio sta nell’automatizzazione del rilevamento degli eventi che prima richiedeva, appunto, l’analisi umana, e nel sollevare i team di sicurezza dal tedioso incarico di decifrare il segnale nonostante il “rumore”.

L’XDR alimentata dall’AI sfrutta anche l’analisi comportamentale e gli Indicatori di comportamento (IOB) al

fine di fornire una prospettiva più approfondita del modo in cui gli attaccanti conducono realmente le loro campagne. Questo approccio operation-centric è molto superiore nel rilevamento anticipato degli attacchi, in particolare quando si tratta di attacchi fortemente mirati e che utilizzano tool e tattiche mai viste prima, eludendo i tradizionali software per la sicurezza dell'endpoint.

Trovare il componente di un attacco tramite catene di comportamenti potenzialmente malevoli consente ai Defender di visualizzare l'intera operazione, dalla root cause fino a ciascun utente, dispositivo e applicazione vittima dell'attacco. È qui che l'XDR basato su AI è fondamentale per correlare automaticamente i dati a una gamma di milioni di eventi al secondo, mentre gli analisti avrebbero bisogno di più ore o giorni per interrogare manualmente dati e convalidare singoli alert.

Tale visibilità garantisce ai team di sicurezza di rispondere a un evento prima che diventi un problema di sicurezza e di introdurre misure atte ad ostacolare la scalata degli attaccanti.

L'utilizzo dell'AI non è una soluzione infallibile e, per il futuro prossimo, sarà necessario senza alcun dubbio un mix di collaborazione tra risorse umane e soluzioni basate su AI. Tuttavia, l'AI migliorerà l'efficienza di ogni membro del team di sicurezza e amplificherà l'efficacia dell'intero stack di sicurezza.

*A cura di **Yossi Naar**, co-fondatore e Chief Visionary Officer di Cybereason*

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/sfruttare-il-potere-dellxdr-alimentato-dallai/