DARKTRACE

Il machine learning nell’era della cyber IA

Una rassegna degli approcci “machine learning” alla cyber security e della tecnologia alla base di Darktrace.

WHITE PAPER

Panoramica: una nuova era per la cyber IA

È iniziata una nuova era per la sicurezza informatica. Negli ambienti digitali complessi di oggi, le macchine combattono contro le macchine e attaccanti esperti e organizzazioni criminali inventano metodi nuovi e sofisticati per perpetrare le loro missioni. La rete aziendale è diventata un campo di battaglia nella quale la posta in gioco è il controllo delle risorse digitali e, in sostanza, la capacità dell'organizzazione di essere operativa.

Il pericolo oggi non consiste solo nei classici scenari di furto dei dati o di compromissione di un sito web, ma nella minaccia silente che si nasconde sotto la superficie. Questi attaccanti sono silenziosi, si insinuano senza preavviso e cambiano furtivamente i dati a piacimento o installano "kill switch" pronti per essere attivati. Usando un codice personalizzato, attraversando solo una volta il confine perimetrale e non inviando mai informazioni all'esterno, queste minacce sono quasi impossibili da scoprire.

Contro questa nuova realtà, i sistemi di sicurezza legacy stanno fallendo e molti rischiano di scomparire. Questo perché l'approccio tradizionale alla sicurezza informatica si basa sulla capacità di definire in anticipo la minaccia. Programmato rigidamente per rilevare solo minacce note, questo approccio non è più praticabile.

Dagli attacchi nuovi e in rapida diffusione agli insider più abili, dai dispositivi IoT hackerati alle supply chain compromesse, il panorama delle minacce si evolve in modo imprevedibile e un nuovo approccio alla cyber-difesa è urgentemente necessario.

Con questo nuovo paradigma, l'intelligenza artificiale può identificare e neutralizzare minacce informatiche mai viste prima. Mentre il machine learning ha il potere di trasformare la cyber defense, la sfida di farlo funzionare su vasta scala in una varietà di ambienti dati dinamici, mentre rileva minacce autentiche in tempo reale senza intervento umano, non è di certo banale.

Introducendo per la prima volta l'intelligenza artificiale per la cyber defense e applicandola con successo in diversi contesti digitali, Darktrace si è dimostrato leader mondiale nel rilevare e rispondere autonomamente alle minacce informatiche che i sistemi legacy non colgono. Alimentata dal machine learning e dagli algoritmi di intelligenza artificiale, la tecnologia del "sistema immunitario" di Darktrace viene utilizzata da migliaia di organizzazioni in tutto il mondo.

Questo white paper spiega l'approccio al machine learning di Darktrace e mette in luce l'interazione unica tra machine learning "unsupervised", machine learning "supervised" e il deep learning della principale tecnologia di cyber IA al mondo.

"Non viviamo più in un'epoca in cui gli attacchi informatici sono limitati al desktop o al server. Il machine learning di Darktrace combatte la battaglia ancor prima che inizi."

City of Las Vegas

L'approccio legacy

Le minacce informatiche odierne sono sempre più avanzate. Alcune sono automatiche e rapide, altre lente e furtive. Nel frattempo, le reti sono diventate sempre più complesse.

Con un numero di connessioni interne ed esterne in continua crescita, è diventato sempre più difficile tenere traccia di tutte le attività della rete e impostare parametri e firme che siano in grado di fornire solo il livello base di protezione. I perimetri delle reti sono sostanzialmente diventati ridondanti, mentre le minacce informatiche evolvono in modi imprevedibili.

Secondo il paradigma tradizionale, i firewall, i metodi di sicurezza degli endpoint e altri strumenti come SIEM e sandbox vengono implementati per applicare policy specifiche e fornire protezione contro le minacce riconosciute.

Sebbene questi strumenti abbiano un ruolo da svolgere all'interno dell'impostazione complessiva di difesa dell'organizzazione, non sono sufficienti nella nuova era delle minacce informatiche in rapida evoluzione. Alcuni sono diventati inutili dato che le reti crescono e le minacce avanzate possono aggirare sempre di più questi controlli con relativa facilità.

L'analisi comportamentale

L'analisi comportamentale è una tecnica che si basa sulla correlazione. Ad esempio, se una scansione di una porta esterna è seguita da una serie di tentativi di accesso non riusciti a un sistema esterno, un motore di correlazione può decidere che tale attività sembri sospetta.

Il problema critico è che i sistemi di grandi dimensioni hanno sempre un certo grado di correlazione. Inoltre, la correlazione tra due variabili non implica la causalità. Se il sistema non lo capisce, vengono inevitabilmente prodotte delle false correlazioni.

"Gli strumenti tradizionali, programmati per individuare le minacce note, non sono più sufficienti."

Heritage Education Fund

I limiti dell'approccio legacy

- I controlli del perimetro dipendono dalle signature, dalle regole e dall'euristica: se non colgono un attacco al punto di entrata, hanno fallito e non possono intraprendere ulteriori azioni.
- La sicurezza degli endpoint dipende dalle signature e dagli attacchi rilevati che sono stati precedentemente identificati e non sono in grado di affrontare le sfide delle minacce non ancora viste.
- Le sandbox vengono aggirate dagli attacchi moderni che capiscono se si trovano in uno spazio falso e quindi ritardano l'esecuzione delle attività dannose.
- Gli strumenti di log e i database SIEM richiedono uno sforzo manuale eccessivo per garantire che i dati vengano raccolti in modo coerente nell'intera organizzazione e abbinati alle previsioni delle minacce da parte dei team di sicurezza. Oltre a richiedere un gran numero di risorse, fanno affidamento sul team di sicurezza perché immaginino tutto ciò che potrebbe andare storto senza inondare gli analisti di allarmi.
- La cosiddetta "analisi comportamentale" non è in grado di rilevare le nuove minacce man mano che emergono, ma si affidano a un paradigma basato sulle regole per configurare il modo in cui determinate figure professionali o dispositivi dovrebbero "comportarsi" e quindi cercare le deviazioni. Questo approccio non riesce ad adattarsi alla complessità delle aziende moderne.

In definitiva, i sistemi legacy sono stati superati dalla moderna complessità del business e dall'innovazione adottata da chi attacca a causa di alcuni limiti fondamentali:

- Hanno bisogno di conoscere tutti gli attacchi precedenti.
- Hanno bisogno di comprendere perfettamente il business e le regole specifiche che lo riguardano.
- Hanno bisogno di utilizzare un modo perfetto per condividere informazioni di alta qualità sui nuovi attacchi.
- Devono indovinare quale aspetto avranno tutti gli attacchi futuri e quali saranno le debolezze del software.
- Devono essere in grado di trasformare tutte le insight di cui sopra in regole o firme che funzionino.

Soprattutto, gli strumenti legacy richiedono delle vittime prima di poter fornire delle soluzioni. L'epoca degli attacchi imprevedibili e in rapido movimento ha reso questo approccio carente.

Il machine learning finora

Il machine learning “supervised”

La proliferazione di dati nel mondo moderno significa che non solo è improduttivo, ma è impossibile per gli esseri umani, setacciare la grande quantità di informazioni generate ogni minuto all’interno di una tipica rete aziendale.

Il machine learning è difficile da sviluppare e da fornire, poiché richiede algoritmi complessi e un framework globale per interpretare i risultati prodotti. Se applicati correttamente, questi approcci possono supportare le macchine nel prendere decisioni logiche basate sulla probabilità, aumentando le capacità dei team umani e scoprendo intuizioni precedentemente inimmaginabili.

Il tipo di apprendimento automatico più ampiamente applicato è il machine learning “supervised”, utilizzato in molti campi commerciali e industriali ai fini della classificazione. Per esempio:

- Le aziende che processano i pagamenti possono utilizzare tecniche di apprendimento automatico all’avanguardia per creare modelli in grado di identificare pagamenti fraudolenti, in tempo reale.
- I servizi video online utilizzano algoritmi per comprendere le preferenze di visione dei propri clienti al fine di fornire consigli personalizzati agli abbonati.
- Le agenzie pubblicitarie sono in grado di utilizzare le analisi della cronologia di navigazione del browser per determinare il posizionamento degli annunci, prendendo decisioni mirate che contribuiscono a un successo maggiore di quanto sarebbe altrimenti possibile affidandosi solo a commerciali umani.
- I computer delle automobili producono enormi quantità di dati che possono essere filtrati per fornire agli ingegneri una migliore comprensione di come i clienti effettivamente utilizzano il veicolo ed essere utili anche nella previsione di un guasto parziale.
- Nel settore sanitario, i processi di raccolta dei dati significano che il benessere può essere monitorato da vicino e che i problemi possono essere individuati prima; quindi, il rischio di sviluppare situazioni gravi può essere ridotto.

Il machine learning “supervised” funziona utilizzando dati classificati in precedenza, dai quali la macchina apprende il sistema di classificazione. In uno scenario nel quale i comportamenti sono ben compresi e le classificazioni sono facili da determinare, l’output di questi sistemi può essere estremamente accurato.

Ad esempio, in alcuni casi, i sistemi evoluti di classificazione delle immagini hanno prestazioni maggiori rispetto agli esseri umani. In effetti, ciò che rende il machine learning “supervised” così potente è la sua capacità di imparare a gestire gli errori e il “rumore” del mondo reale, attraverso un approccio statistico.

Per questo motivo, i sistemi di apprendimento automatico “supervised” sono i meglio equipaggiati per poter dare una risposta esplicita basata sulla conoscenza precedente. Ad esempio, un sistema alimentato con molti casi di ransomware conosciuti sarà in grado di apprendere quali siano gli indicatori comuni di quel malware e sarà capace di rilevare attacchi simili in futuro.

Allo stesso modo, se si vuole essere in grado di distinguere i “gatti” dai “cani” all’interno di una serie di immagini, il machine learning “supervised” è immensamente efficace perché al mondo esistono molte immagini di cani e gatti conosciuti che possono essere sfruttate per formare il sistema e raramente compaiono nuove specie di cani e di gatti.

Tuttavia, l’overfitting è un problema comune nel machine learning “supervised”, in cui i parametri del modello sono troppo sintonizzati sui dati di training. Invece di imparare l’essenza di una categoria, la macchina impara un esempio particolare: ad esempio, può imparare a riconoscere un pastore tedesco, ma non riesce a capire i “cani” come categoria, e le caratteristiche che rendono quel pastore tedesco parte del gruppo.

Deep learning

Il deep learning è un sottogruppo di apprendimento “supervised” che utilizza molti livelli di processi matematici interconnessi per creare motori decisionali non lineari. Il deep learning tende a superare nettamente gli altri approcci supervisionati perché è in grado di gestire rappresentazioni o convinzioni molto più complesse sul mondo senza che gli esseri umani debbano dire al sistema di che cosa sono composti i dati.

Tuttavia, questa potente rappresentazione ha un costo, dal momento che il deep learning richiede una potenza di calcolo di un diverso ordine di grandezza per essere in grado di addestrare i motori matematici.

Ci si aspetta che il deep learning sostituisca sempre più gli approcci algoritmici tradizionali in tutto il computing in cui sono disponibili dati di input sufficienti, esempi di output previsto e una modalità automatica per misurare se l’algoritmo ha successo.

Machine learning e cyber security

Gli approcci tradizionali alla cyber security si basano sull'individuazione di attività che assomiglino ad attacchi precedentemente noti - i cosiddetti "known knowns". Questo di solito viene ottenuto con un approccio signature-based, in base al quale viene creato un database di comportamenti dannosi noti. Le nuove attività sono referenziate con il database e quelle corrispondenti sono contrassegnate come minacce.

Queste soluzioni a volte utilizzano anche metodi basati sul machine learning "supervised", che aiutano a classificare l'output delle signature. Utilizzando questo approccio "supervised", un sistema viene alimentato con un set di dati di training in cui ogni voce è stata etichettata come appartenente a una di una serie di classi distinte.

Nel contesto della sicurezza delle informazioni, il sistema viene istruito utilizzando un database di comportamenti visti in precedenza, in cui ogni comportamento è noto per essere maligno o benigno e viene etichettato come tale.

Le nuove attività vengono quindi analizzate per vedere se corrispondono più strettamente a quelle della classe maligna o a quelle della classe benigna. Qualsiasi strumento che sia valutato come molto probabilmente dannoso viene nuovamente contrassegnato come minaccia.

I sistemi che fanno affidamento esclusivamente sul machine learning "supervised" presentano punti deboli fondamentali:

- I comportamenti dannosi che si discostano sufficientemente da quelli visti in precedenza non saranno classificati come tali, quindi passeranno inosservati.
- È necessaria una grande quantità di input umano per etichettare i dati di training.
- Qualsiasi dato errato o pregiudizio umano introdotto può seriamente compromettere la capacità del sistema di classificare correttamente le nuove attività.

Il machine learning ha offerto un'opportunità significativa al settore della cyber security. I nuovi metodi di machine learning possono migliorare notevolmente l'accuratezza del rilevamento delle minacce e migliorare la visibilità della rete grazie alla maggiore quantità di analisi computazionale che possono gestire. Stanno inoltre inaugurando una nuova era di autonomous response, in cui un sistema di macchine è sufficientemente intelligente da capire come e quando combattere contro le minacce in corso.

La combinazione unica di Darktrace di più approcci di machine learning

Sebbene il machine learning "supervised" possa essere potente, Darktrace ha nel proprio DNA la visione di costruire la prima piattaforma self-learning di cyber defense. Utilizzare il machine learning "unsupervised" consentiva al sistema di scoprire minacce rare e mai viste prima, che non si basavano su insiemi di dati di training intrinsecamente imperfetti. I dati relativi agli attacchi storici non proteggono necessariamente da quelli futuri.

Avendo costruito il sistema di machine learning leader a livello mondiale per la cyber security che si basa su questo approccio unico, Darktrace utilizza anche tecniche di deep learning per integrare il suo motore di intelligenza artificiale con le competenze specialistiche degli esperti analisti cyber di Darktrace.

Implementate in migliaia di ambienti di rete reali, queste nuove tecniche sono sempre più potenti e alimentano le nostre reti neurali consentendo di rafforzare ulteriormente la potenza del machine learning "unsupervised".

> "Con Darktrace, l'IA applicata alla cyber security è diventata realtà"
>
> **Ovum**

Machine learning “unsupervised”

Il machine learning “unsupervised” di Darktrace è fondamentale perché, a differenza degli approcci “supervised”, non richiede dati di addestramento etichettati. Invece è in grado di identificare i modelli chiave e le tendenze nei dati, senza la necessità di input umani. L’apprendimento “unsupervised” può quindi portare l’elaborazione del computer oltre ciò che i programmatori già sanno o possono immaginare e scoprire relazioni precedentemente sconosciute.

Darktrace utilizza algoritmi unici di machine learning “unsupervised” per analizzare i dati di rete in scala e fare miliardi di calcoli basati sulla probabilità in base alle prove che vede. Invece di fare affidamento sulla conoscenza delle minacce passate, classifica in modo indipendente i dati e rileva schemi validi. Da ciò, forma una comprensione dei comportamenti “normali” attraverso la rete, relativi a dispositivi, utenti o gruppi di entrambi e rileva le deviazioni da questo “modello di comportamento” in evoluzione che potrebbero indicare una minaccia in via di sviluppo.

I principi fondamentali del machine learning di Darktrace

- Impara cosa è normale all’interno di una rete “sul campo” e non dipende dalla conoscenza degli attacchi precedenti.
- Si sviluppa in base alla scala, alla complessità e alla diversità delle imprese moderne, in cui ogni dispositivo e persona è unico.
- Rivede costantemente le ipotesi sul comportamento, usando la matematica probabilistica.
- È sempre aggiornato e non dipende dall’input umano.

L’impatto del machine learning “unsupervised” di Darktrace sulla cyber security è trasformativo. La sua tecnologia di cyber IA si è rapidamente rivelata in grado di identificare eventi informatici fino ad ora sconosciuti, da una varietà di fonti di minacce, che altrimenti sarebbero passate inosservate. Questi includono:

- Minaccia interna: maligna o accidentale.
- Attacchi zero-day: exploit precedentemente inediti e insoliti.
- Vulnerabilità latenti - o dormienti che non sono state scoperte, spesso a causa della mancanza di visibilità sulla rete.
- Attacchi machine-speed: ransomware e altri aggressori automatici che si propagano e/o mutano rapidamente e sono praticamente impossibili da fermare e neutralizzare utilizzando meccanismi di risposta dipendenti dall’uomo.
- Attacchi silenziosi e furtivi che si annidano nelle reti inosservati.

Thomas Bayes

La matematica all’avanguardia nell’approccio di machine learning di Darktrace è ancorata al lavoro del matematico britannico Thomas Bayes (1702-1761). La sua teoria della probabilità condizionata fornisce un ponte matematico tra i metodi sviluppati, oggettivi e il mondo soggettivo che popoliamo. Un approccio avanzato alla teoria bayesiana, sviluppato dai matematici dell’Università di Cambridge, fornisce un filtro per accertare il vero significato di dati vaghi e abbondanti.

L’uso di Darktrace della probabilità bayesiana come parte del proprio approccio di machine learning con apprendimento “unsupervised” consente alla tecnologia di Darktrace di:

- Scoprire relazioni precedentemente sconosciute. Classificare in modo indipendente i dati.
- Rilevare modelli validi che definiscano ciò che potrebbe essere considerato un comportamento normale.
- Lavorare senza ipotesi precedenti, quando necessario.

“Il machine learning può rilevare cose che non possiamo prevedere e definire. È come trovare un ago in un enorme pagliaio.”

Steelcase

Riepilogo tecnico

L'approccio trasformativo di Darktrace alla cyber defense si basa su metodi probabilistici sviluppati dai matematici di Cambridge. Impiegando molteplici tecniche di apprendimento "unsupervised", "supervised" e deep learning in un quadro bayesiano, l'Enterprise Immune System può integrare un vasto numero di indicatori deboli di comportamento anomalo per produrre una singola misura chiara delle probabilità di minaccia.

Per ogni ambiente unico, Darktrace genera milioni di modelli matematici interconnessi che sono correlati per assicurare che venga rilevato solo un comportamento veramente anomalo, senza una profusione di falsi positivi. A differenza del calcolo basato su regole, i risultati generati dalla matematica probabilistica non possono semplicemente essere classificati come "sì" o "no", ma indicano invece gradi di certezza che riflettono le ambiguità che inevitabilmente esistono negli ambienti di dati dinamici.

Classificare le minacce

L'Enterprise Immune System tiene conto delle ambiguità distinguendo tra i livelli di prova leggermente diversi che caratterizzano i dati di rete. Invece di generare il semplice output binario "maligno" o "benigno", gli algoritmi matematici di Darktrace producono output contrassegnati con diversi gradi di potenziale minaccia. Ciò consente agli utenti del sistema di classificare gli avvisi in modo rigoroso e dare la priorità a quelli che richiedono più urgentemente un'azione, rimuovendo il problema dei numerosi falsi positivi associati a un approccio basato su regole.

Nella sua essenza, Darktrace caratterizza matematicamente ciò che costituisce un comportamento "normale", basato sull'analisi di un gran numero di diverse misure di comportamento della rete di un dispositivo, tra cui:

- Accesso al server
- Volumi di dati
- Tempistiche degli eventi
- Uso di credenziali
- Tipo di connessione, volume e direzionalità
- Direzionalità di upload / download
- Tipo di file
- Attività di amministrazione
- Richieste di risorse e informazioni

Clustering di dispositivi

Per modellare ciò che dovrebbe essere considerato normale per un dispositivo, il suo comportamento viene analizzato nel contesto di altri dispositivi simili nella rete. Darktrace sfrutta la potenza dell'apprendimento "unsupervised" per identificare in modo algoritmico raggruppamenti significativi di dispositivi, un'attività impossibile da eseguire manualmente anche su reti di dimensioni modeste.

Per creare un'immagine olistica delle relazioni all'interno della rete, Darktrace utilizza diversi metodi di clustering, tra cui clustering basato su matrici, clustering basato sulla densità e tecniche di clustering gerarchico. I cluster risultanti vengono quindi utilizzati per informare la modellizzazione dei comportamenti normativi dei singoli dispositivi.

Topologia di rete

Una rete è molto più della somma delle sue singole parti e gran parte del suo significato è contenuto nelle relazioni tra le diverse parti. Darktrace impiega molti metodi matematici per modellare i molteplici aspetti della topologia di una rete, consentendole di evidenziare minimi cambiamenti nella struttura che sono indicativi di minacce.

Un approccio si basa su metodi a matrice iterativa che rivelano importanti strutture di connettività all'interno della rete, in modo simile agli algoritmi avanzati di classificazione delle pagine. Insieme a questi, Darktrace ha sviluppato applicazioni innovative di modelli dal campo della fisica statistica, che consentono di modellare il "contesto energetico" di una rete per rivelare sottostrutture anomale che potrebbero rappresentare i primi sintomi di compromissione.

"La tecnologia IA di Darktrace per la cyber defense è un punto di svolta: ci consente di sostenere la resilienza di fronte a un panorama di minacce in rapida evoluzione."

Raspberry Pi

Struttura della rete

Un'ulteriore sfida importante nella modellazione dei comportamenti di una rete in continua evoluzione è l'enorme numero di potenziali variabili predittive. Per l'osservazione del traffico di pacchetti e dell'attività host all'interno di una LAN o WAN aziendale, in cui sia l'input che l'output possono contenere molte funzionalità correlate (protocolli, macchine di origine e di destinazione, modifiche di registro e trigger di regole, ecc.), è fondamentale l'apprendimento di una funzione predittiva strutturata sparsa e coerente.

In questo contesto, Darktrace utilizza un approccio computazionale su larga scala per comprendere la struttura sparsa in modelli di connettività di rete basati sull'applicazione di tecniche di regolarizzazione L1 (il metodo lasso). Ciò consente all'Enterprise Immune System di scoprire le vere associazioni tra i diversi elementi di una rete che possono essere parte di problemi di ottimizzazione convessa risolvibili in modo efficiente e produrre modelli parsimoniosi.

Stima Bayesiana ricorsiva

Per combinare queste molteplici analisi del comportamento della rete, generando una singola immagine completa dello stato dei dispositivi che costituiscono una rete, Darktrace sfrutta la potenza della Recursive Bayesian Estimation (RBE). Utilizzando la RBE, i modelli matematici di Darktrace sono in grado di adattarsi costantemente alle nuove informazioni man mano che diventano disponibili per il sistema. Ricalcolando continuamente i livelli di minaccia alla luce dei nuovi dati, il sistema immunitario aziendale può individuare modelli significativi nei flussi di dati indicativi di attacchi, in cui i metodi convenzionali basati sulle signature vedono solo il caos.

Darktrace e il Deep Learning

Darktrace utilizza anche il deep learning per migliorare i processi di modellazione. Il deep learning è un sottoinsieme del machine learning che utilizza le interazioni a cascata di processi matematici stratificati - noti come reti neurali - per offrire ai sistemi intelligenti un livello più alto di visione. Le reti neurali a più strati possono migliorare il rilevamento e la correzione di alcune minacce, ad esempio nell'identificazione delle anomalie DNS, che sono monitorate in modo meno efficace da altri metodi di auto-apprendimento. Il sistema di deep learning di Darktrace assegna un punteggio a tutti i dati DNS da un dispositivo, allo scopo di identificare attività sospette ancora più velocemente.

Darktrace raggruppa anche i dispositivi in gruppi "peer", basandosi sulla propria comprensione di come questi dispositivi si comportano, e usa l'apprendimento "supervised" per scoprire sequenze di violazioni, schemi insoliti o per rilevare attività anomale a un livello più alto e olistico. Ad esempio, il ransomware WannaCry è stato facilmente rilevato da Darktrace in quanto viola diversi "pattern of life". Usando l'apprendimento "supervised", Darktrace può replicare il processo di un'interpretazione umana di vari insiemi di violazioni per un dispositivo o una rete nel tempo e quindi presentare allarmi correlati anziché una moltitudine.

L'apprendimento "supervised" viene utilizzato da Darktrace anche per comprendere meglio l'ambiente, senza che un essere umano debba etichettarlo. Osservando milioni di smartphone diversi, ad esempio, Darktrace diventa sempre più veloce nell'individuare un nuovo dispositivo come uno "smartphone" e persino quale tipo di smartphone sia.

Utilizzando tecniche profonde e "supervised" per integrare i suoi algoritmi di apprendimento automatico "unsupervised", Darktrace crea apprendimenti unici e contestuali sull'attività di rete e integra le intuizioni delle implementazioni globali per migliorare il rilevamento delle minacce.

Infine, Darktrace utilizza anche tecniche di deep learning per automatizzare le attività ripetitive e lunghe che vengono eseguite durante i flussi di lavoro di ricerca. Analizzando il modo in cui gli esperti cyber analisti interagiscono con il Threat Visualizer, classificano gli alert e sfruttano le fonti di terze parti, Darktrace è in grado di replicare tali comportamenti esperti e automatizzare alcune funzioni degli analisti. Ciò consente agli analisti di qualsiasi livello di maturità di svolgere indagini sempre più efficienti e semplificate. Fornisce inoltre ai team di sicurezza il tempo di cui hanno bisogno per concentrarsi su attività strategiche di alto valore, come la gestione del rischio e la possibilità di concentrarsi su come migliorare il business.

Risposta autonoma con Darktrace Antigena

Poiché l'apprendimento automatico di Darktrace è in grado di comprendere, a livello granulare, il "pattern of life", e quindi di rilevare deviazioni specifiche dalla normale attività, è anche in grado di generare una risposta autonoma appropriata a un attacco in corso.

Autorizzando la macchina a combattere autonomamente per la prima volta, Darktrace Antigena funziona come gli anticorpi all'interno del sistema immunitario, neutralizzando una minaccia applicando il "pattern of life" conosciuto di un dispositivo o utente.

Grazie all'apprendimento "unsupervised" di Darktrace, questa soluzione può anche apprendere da sé e apprendere passivamente dai dati che osserva. Ad esempio, quando Darktrace Antigena genera un'azione di risposta autonoma, viene attivato un ciclo di feedback di rinforzo. I comportamenti risultanti sulla rete sono analizzati a loro volta per facilitare la diagnosi e informare ogni ulteriore azione. Diversamente dall'apprendimento guidato di rinforzo, questo processo è guidato autonomamente dalla macchina stessa piuttosto che da un operatore umano.

Darktrace Antigena è basato su un machine learning "unsupervised", in grado di rilevare solo gli eventi informatici più anormali con un livello di precisione tale da consentire di intraprendere azioni precise in risposta. L'apprendimento automatico usato in questo modo non sostituisce la funzione umana, ma in definitiva serve a migliorarla. Antigena agisce più velocemente di un umano, facendo guadagnare all'operatore tempo prezioso per recuperare e prendere ulteriori precauzioni, se necessario.

"Darktrace ha completamente cambiato il nostro approccio alla sicurezza informatica. La risposta autonoma consente al mio team di spendere tempo e sforzi laddove è davvero necessario."

Campari

Conclusioni

La nostra generazione sta assistendo alla rivoluzione del machine learning. Stiamo constatando cambiamenti nelle pratiche lavorative determinati dalla sostituzione della forza umana con la macchina, dall'automazione di compiti ripetitivi e ora dalla sostituzione di compiti di basso valore e ponderati con macchine in grado di gestire grandi quantità di dati e fare calcoli enormi.

Poiché le reti sono cresciute in termini di portata e complessità, le opportunità per gli aggressori di sfruttare le lacune sono aumentate. Per proteggere la rete aziendale non è più sufficiente proteggere il perimetro e gli strumenti basati su regole non possono tenere il passo con tutti i possibili vettori di attacco. Un panorama di attacco cibernetico in continua evoluzione richiede un aumento delle nostre capacità di rilevamento, utilizzando l'apprendimento automatico per comprendere l'ambiente, filtrare il "rumore" e intervenire laddove vengono identificate le minacce.

Grazie all'utilizzo della matematica probabilistica bayesiana sviluppata dai matematici dell'Università di Cambridge, Darktrace è leader mondiale nell'apprendimento automatico e nell'intelligenza artificiale. L'interazione unica di machine learning "unsupervised", machine learning "supervised" e deep learning che alimentano l'Enterprise Immune System, ha permesso a Darktrace di diventare l'azienda leader mondiale per la cyber defense.

Con questo nuovo paradigma, possiamo fornire alle organizzazioni il proprio sistema immunitario in grado di catturare e combattere autonomamente le minacce informatiche che gli altri non riescono a cogliere, senza alcun input umano o pregiudizi su cosa sia "cattivo".

La tecnologia di Darktrace è diventata uno strumento vitale per i team di sicurezza che cercano di capire la scalabilità della loro rete, osservare i livelli di attività e rilevare le aree di potenziale debolezza. Questi non devono più essere cercati manualmente, ma vengono segnalati dal sistema automatico e classificati in base al loro significato.

La tecnologia di machine learning è l'alleata fondamentale nella difesa dei sistemi dagli hacker e dalle moderne minacce interne e nella formulazione della risposta a metodi sconosciuti di attacco informatico. È un cambiamento epocale nella sicurezza informatica.

A proposito di Darktrace

Darktrace è la principale azienda di cyber IA al mondo e ideatrice della tecnologia di risposta autonoma. La sua IA auto-apprendente è modellata sul sistema immunitario umano e utilizzata da oltre 3.000 organizzazioni per proteggere dalle minacce al cloud, e-mail, IoT, network e sistemi industriali.

L'azienda ha oltre 900 dipendenti e sede a San Francisco e Cambridge, UK, con uffici a Milano e Roma. Ogni 3 secondi, l'IA di Darktrace combatte contro una minaccia cyber, impedendole di causare danni.

Contattaci

Nord America: +1 (415) 229 9100

Europa: +44 (0) 1223 394 100

Asia-Pacifico: +65 6804 5010

America Latina: +55 11 97242 2011

info@darktrace.com

darktrace.com