Anteprima

Enterprise Immune System V4

Darktrace Cyber AI Analyst

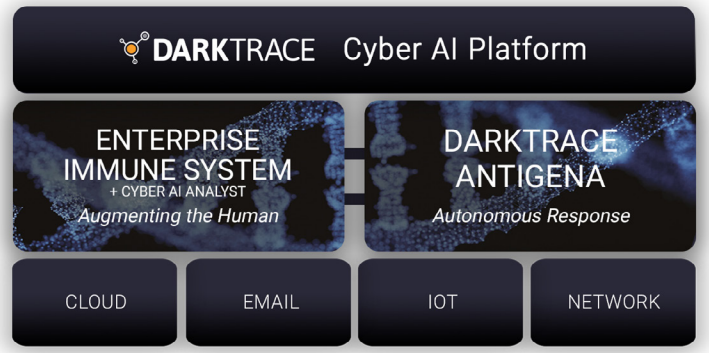
Cyber AI Analyst è frutto di un progetto di ricerca presso il Centro Ricerca & Sviluppo di Darktrace; questa tecnologia combina l'esperienza umana con la coerenza, la velocità e la scalabilità dell'intelligenza artificiale durante l'indagine. Oltre al Cyber AI Analyst, le nuove funzionalità della V4 comprendono un miglior supporto di ambienti cloud e container, così come una maggiore flessibilità e controllo delle capacità di risposta autonoma.

Oltre 70 nuove funzionalità, tra cui:

- Prima release della Cyber AI Platform Architecture - su larga scala ad alta velocità - che comprende l'Enterprise Immune System e Antigena Autonomous Response
- Prima release della tecnologia Cyber AI Analyst dal Centro Ricerca & Sviluppo di Darktrace
- Significativi miglioramenti del cloud tra cui:
  - nuovo supporto AWS VPC Traffic Mirroring e Azure vTAP
  - nuovo supporto per la modellazione di sistemi containerizzati (Docker, Kubernetes)
  - nuovo supporto per SharePoint, OneDrive e copertura di più domini di Office 365
- Maggiore flessibilità e controllo di Antigena dall'Enterprise Immune System su network, e-mail e cloud
- Prestazioni migliorate su tutta la piattaforma, inclusi data ingestion, core data processing e modellazione AI
- Informazioni contestuali migliorate nell'interfaccia utente del Threat Visualizer tramite integrazioni Active Directory / LDAP per informazioni aziendali e integrazioni STIX / TAXII per threat intelligence IOC
- Miglioramenti della Mobile App, tra cui una configurazione più semplice, notifiche push in tempo reale e nuovi output di Cyber AI Analyst
- Nuova App Darktrace per ServiceNow che crea voci personalizzate in ServiceNow per ogni allarme

Annuncio della Cyber AI Platform di Darktrace

La missione di Darktrace è rendere il mondo più sicuro di fronte alle minacce che si propagano alla velocità della macchina e agli attacchi mirati "human driven". Potenziando i team dedicati alla sicurezza e rispondendo autonomamente agli attacchi, la Cyber AI Platform di Darktrace riduce i rischi di furto di dati e di interruzione dei servizi tecnologici che le organizzazioni si trovano ad affrontare quotidianamente. Il software è offerto sulla base di abbonamento SaaS che comprende la sicurezza cloud, e-mail, IoT / OT e network.



La Cyber AI Platform di Darktrace è composta da due prodotti di punta strettamente integrati: l'Enterprise Immune System auto-apprendente e la tecnologia di risposta autonoma di Antigena. I clienti di Darktrace beneficiano di algoritmi straordinariamente efficaci utilizzati da migliaia di organizzazioni.

Con Darktrace Antigena è stata creata la prima soluzione di risposta autonoma in grado di reagire alla velocità della macchina; attualmente, questa tecnologia sta bloccando un attacco ogni 3 secondi in tutto il mondo. Ora, con l'Enterprise Immune System V4, Cyber AI Analyst potenzia i team dedicati alla sicurezza, automatizzando le indagini sulle minacce e riducendo drasticamente il tempo necessario alla comprensione approfondita della natura e della causa principale di un problema di sicurezza.

Cyber AI Analyst

Gli analisti umani indagano sulle minacce trovando schemi, formulando ipotesi, raggiungendo conclusioni e condividendo le loro scoperte con il resto dell'azienda. Questi sono passaggi ad alta intensità di lavoro che richiedono tempo e competenza. Tuttavia, imparando a indagare sulle minacce come gli esseri umani esperti, Cyber AI Analyst è in grado di formulare ipotesi e giungere alle conclusioni a una velocità e a un livello tali a cui nessun essere umano potrebbe mai arrivare.

Cyber AI Analyst utilizza varie forme di machine learning, come il deep learning, ed è alimentato da un insieme di dati ampio, complesso e in continua crescita che fa riferimento alle modalità con cui gli esperti analisti di Darktrace indagano sulle minacce rilevate dall'Enterprise Immune System.

Combinando questo ricco insieme di dati con l'Intelligenza Artificiale, Cyber AI Analyst può condurre indagini esperte, contemporaneamente, su centinaia di thread paralleli, correlando una moltitudine di allarmi e indicatori e sviluppando una comprensione significativa degli allarmi, alla velocità della macchina. Quindi comunica i risultati e le raccomandazioni sotto forma di report dettagliati sulla sicurezza che possono essere facilmente rivisti e gestiti sia da manager che end-user.

Riduzione del 92% del tempo necessario per il triage

Il fatto che Cyber AI Analyst svolga indagini prima di segnalare qualsiasi cosa al team della sicurezza, consente fin dall'inizio di scartare eventi a bassa priorità o benigni, presentando di volta in volta soltanto pochi allarmi ad alta priorità. Ciò consente agli utenti di dedicare meno tempo a esaminare gli allarmi e più tempo a privilegiare le attività strategiche, dalla risposta mirata al threat hunting fino alla modernizzazione della sicurezza e alla mitigazione dei rischi in tutta l'azienda.

Fondamentalmente, Cyber AI Analyst è in grado di adattarsi istantaneamente a situazioni nuove e uniche, automatizzando compiti ponderati anziché utilizzare manuali tecnici o conoscenze umane codificate. Questa è un'intelligenza artificiale che non dorme mai, che può correlare e comprendere in modo intelligente diversi data points alla velocità della macchina e che può comunicare i suoi risultati all'uomo in un modo tale da evidenziare rapidamente la presenza di una minaccia emergente.

Vantaggi

- Potenzia i team dedicati alla sicurezza esaminando le minacce rilevate dall'Enterprise Immune System
- Risparmia tempo in modo che i team della sicurezza possano concentrarsi sulle attività più strategiche e mitigare il rischio
- Formula ipotesi e motivi per trarre conclusioni a una velocità e a un livello a cui nessun essere umano potrebbe mai arrivare
- Segnala automaticamente gli allarmi sotto forma di specifiche reportistiche sulla sicurezza
- Sfrutta l'esperienza degli analisti Darktrace di fama mondiale e la rende disponibile a chiunque

> Abbiamo ottenuto risultati strabilianti. Cyber AI Analyst ha individuato un canale d'attacco AWS in cui i dati fuoriuscivano molto lentamente, nell'arco di due settimane. Ha mostrato agli analisti umani come l'attaccante aveva modellato il percorso.
>
> **Mike Beck,**
> **Global Director of Threat Analysis,**
> **Darktrace**