McLaren Group

Fondata nel 1963 dal famoso pilota Bruce McLaren, da oltre quattro decenni la McLaren è all'avanguardia nel settore dell'automotive e tra le scuderie della Formula Uno. Nel corso degli anni, la McLaren è cresciuta fino a diventare molto più di un team di corsa, sviluppando tre principali business unit, McLaren Racing, McLaren Automotive e McLaren Applied, ognuna delle quali necessita di protezione.

In sintesi

- ✔ Forza lavoro dinamica e decentralizzata
- ✔ Specifico per attacchi e-mail personalizzati e sofisticati
- ✔ Scelta dell'AI per proteggere ogni aspetto dell'attività aziendale

"Darktrace agisce autonomamente, consentendo al nostro team di occuparsi di attività di alto livello."

Principal Digital Architect,
McLaren Racing

Adattarsi all'evoluzione del panorama delle minacce

Da esfiltrazione furtiva di IP leader al mondo ad attacchi alla velocità delle macchine in grado di crittografare i dispositivi in pochissimi secondi, un attacco informatico può fare la differenza tra il successo e il fallimento della McLaren. La protezione dei dati sensibili, spesso condivisi con partner e principali fornitori affidabili, è pertanto essenziale.

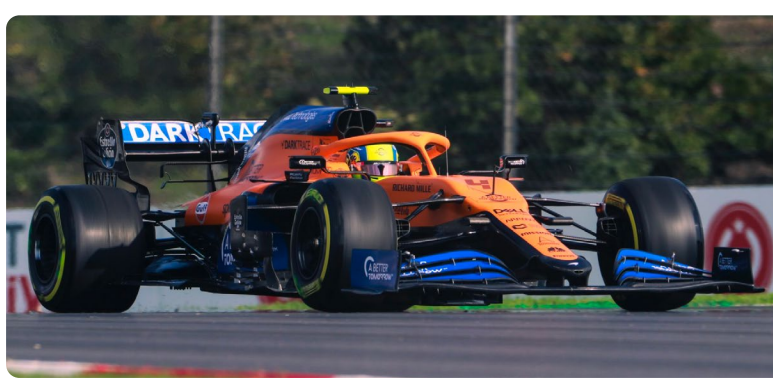
La forza lavoro McLaren è sempre stata incredibilmente dinamica, con i team abituati ad allestire efficacemente ogni settimana postazioni per la gestione dei dati di telemetria da remoto in differenti parti del mondo. L'ampia diffusione dello smart working ha ulteriormente ampliato la dipendenza dell'organizzazione da Cloud e strumenti SaaS come Dropbox e Microsoft Teams. Prima di Darktrace, questi ambienti erano protetti da una collezione eterogenea di singole soluzioni statiche che, per individuare minacce future, facevano affidamento su comportamenti pericolosi predefiniti.

Il team della sicurezza aveva pertanto bisogno di una piattaforma di cyber security completa e unificata, in grado di proteggere qualsiasi aspetto dell'attività aziendale. Dalle applicazioni Cloud e SaaS alle e-mail, alla McLaren serviva una soluzione in grado di bloccare nuove minacce, indipendentemente da dove provenissero.

Protezione autonoma

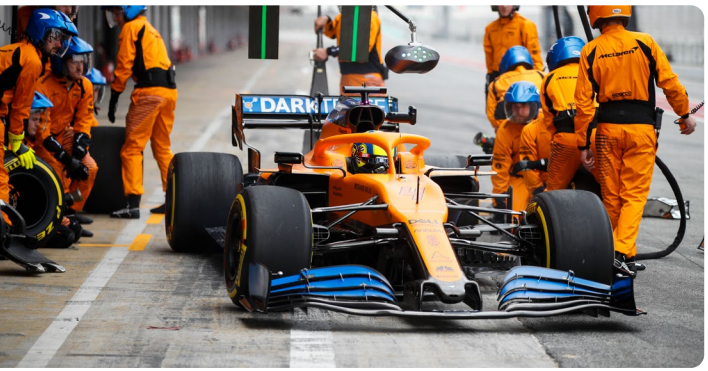
La McLaren ha scelto l'AI "self-learning" per individuare e analizzare le minacce in tempo reale, senza l'utilizzo di regole, firme o precedenti supposizioni.

Darktrace ha immediatamente iniziato ad apprendere il normale "pattern of life" relativo ad ogni utente e dispositivo all'interno dell'ecosistema digitale dell'organizzazione. Imparando il senso di "sé", il Darktrace Immune System è in grado di individuare le impercettibili deviazioni indicative di una minaccia informatica, da compromissioni di account ed esfiltrazioni di dati SaaS a malware zero-day e attacchi nation-state.



L'AI di Darktrace si integra facilmente con altri strumenti, grazie ad un'architettura aperta ed ampliabile, migliorando il valore degli stack di sicurezza McLaren esistenti e ampliando la visibilità all'interno di tutto l'ecosistema digitale. Grazie all'AI in grado di rispondere autonomamente agli attacchi ovunque si verificano, il team della sicurezza McLaren può dedicare all'innovazione il proprio prezioso tempo durante i week-end di gara, anziché a rispondere ad ogni allarme. "Non facciamo girare le macchine sul circuito fino a quando non riceviamo correttamente i dati di telemetria, quindi si tratta di una parte di infrastruttura fondamentale e super-importante per noi", afferma Edward Green, Principal Digital Architect, McLaren Racing.

> "È stato incredibile scoprire con quale rapidità l'AI ha appreso e capito i nostri normali comportamenti."
>
> Principal Digital Architect, McLaren Racing



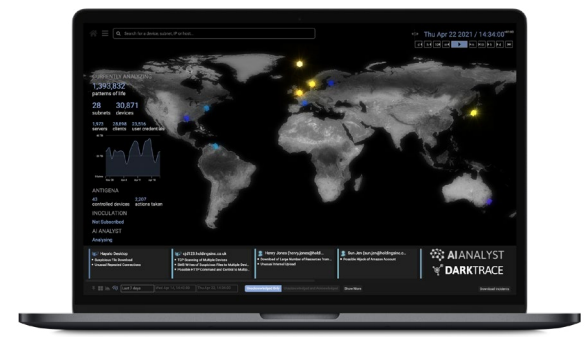
Una casella di posta in arrivo "self-healing"

Come qualsiasi altra organizzazione, la McLaren deve affrontare moltissime minacce e-mail, da social engineering a phishing e compromissione di account. In particolare, si sono verificati problemi relativi ad attacchi di spear phishing sofisticati che avevano preso di mira dirigenti di Livello C. Dato il continuo aumento di attacchi e-mail, la McLaren ha deciso di ampliare il proprio sistema di sicurezza basato su AI scegliendo Antigena Email per proteggere il proprio ambiente Microsoft 365 e tutelare la propria forza lavoro da e-mail pericolose.

Antigena Email è in grado di comprendere i pattern di ogni comunicazione che avviene tra gli utenti di posta elettronica, utilizzando lo stesso approccio di "self-learning" basato su AI per rilevare anche i più impercettibili indicatori di attacco. Anziché analizzare le e-mail in arrivo in base a regole e firme pre-definite, Darktrace analizza le e-mail nel contesto, rilevando se contengono attacchi nuovi e sofisticati, consentendo nel contempo la normale operatività aziendale senza alcuna interruzione.

Come spiega Green: "Abbiamo visto i risultati fin dai primi giorni. Il volume di e-mail di phishing segnalate da parte degli utenti è diminuito notevolmente e, nel corso del tempo, l'analisi regolare delle azioni di Antigena Email ci ha consentito di scoprire numerose campagne di phishing di cui prima non eravamo a conoscenza."

> "Quest'anno Darktrace ci ha garantito moltissima sicurezza, rilevando cose che le sole persone non sarebbero state in grado di rilevare."
>
> Principal Digital Architect, McLaren Racing



L'interfaccia dedicata di Darktrace per le minacce basate sul cloud

Per maggiori informazioni

- Prenota una prova gratuita
- Leggi il white paper sull'Immune System
- Visita il nostro canale YouTube