McLaren Group

McLaren wurde 1963 von dem erfolgreichen Rennfahrer Bruce McLaren gegründet und ist seit über vierzig Jahren führend in der Automobilindustrie und der Formel 1. Mit den Jahren hat sich McLaren vom Motorsportteam zu einem Unternehmen mit drei Kernbereichen entwickelt: McLaren Racing, McLaren Automotive und McLaren Applied – und sie alle müssen geschützt werden.

Auf einen Blick

- ✔ Dynamische und dezentrale Belegschaft
- ✔ Ziel von raffinierten, personalisierten E-Mail-Angriffen
- ✔ Entscheidung für KI zum Schutz aller Bereiche des Unternehmens

„Darktrace agiert eigenständig, sodass unser Team Zeit hat, sich mit anspruchsvolleren Aufgaben zu beschäftigen."

Principal Digital Architect, McLaren Racing

Anpassung an immer neue Bedrohungen

Angefangen bei der heimlichen Ausschleusung von wertvollem geistigem Eigentum bis hin zu ultraschnellen Angriffen, die binnen Sekunden Geräte verschlüsseln – ein Cyberangriff könnte über Sieg oder Niederlage von McLaren entscheiden. Der Schutz sensibler Daten, die häufig auch an vertrauenswürdige Partner und wichtige Zulieferer geschickt werden, ist daher extrem wichtig.

Die Belegschaft von McLaren ist sehr dynamisch. Das Team ist es gewohnt, jedes Wochenende in einem anderen Teil der Welt sein Büro an der Rennstrecke einzurichten. Verstärkte Remote-Arbeit hat die Nutzung von Cloud- und SaaS-Tools wie Dropbox und Microsoft Teams noch weiter intensiviert. Vor Darktrace wurden diese Umgebungen durch isolierte Punktlösungen geschützt, die Bedrohungen nur anhand bereits definierter „bösartiger" Verhaltensweisen erkannten.

Das Sicherheitsteam brauchte daher eine umfassende, zentrale Plattform für Cybersicherheit, die jeden Bereich des Unternehmens, von Cloud- und SaaS-Anwendungen bis hin zum E-Mail-System, schützt. Die Sicherheitslösung von McLaren sollte neuartige Bedrohungen stoppen, egal wann und wo sie auftauchen.

Eigenständiger Schutz

McLaren entschied sich für selbstlernende KI, die Bedrohungen in Echtzeit erkennt und untersucht, ohne von Regeln, Signaturen oder Mutmaßungen abhängig zu sein.

Darktrace begann sofort, die normalen Verhaltensmuster, die „Patterns of Life", aller Benutzer und Geräte im digitalen Ökosystem des Unternehmens zu lernen. Das Darktrace Immune System macht sich ein Bild vom „Wesen" des Unternehmens und erkennt daher subtile Abweichungen, die auf eine Cyberbedrohung hindeuten – von SaaS-Kontoübernahmen über Zero-Day-Malware bis hin zu nationalstaatlichen Angriffen.

Die KI von Darktrace integriert sich über eine offene und erweiterbare Architektur nahtlos in andere Tools. Das macht die bereits vorhandene Sicherheitsinfrastruktur effektiver und erhöht die Transparenz des gesamten digitalen Ökosystems. Da die KI stets zur Stelle ist und eigenständig Angriffe abwehrt, muss sich das Sicherheitsteam von McLaren nicht um jede Warnmeldung kümmern und hat an den Rennwochenenden mehr Zeit für innovative Projekte. „Ohne Telemetrie schicken wir kein Fahrzeuge auf die Strecke. Die Technologie ist ein kritischer Teil der Infrastruktur und extrem wichtig für uns“, sagt Edward Green, Principal Digital Architect, McLaren Racing.

> „Ich war beeindruckt, wie schnell die KI unsere normalen Verhaltensweisen gelernt hat.“
>
> Principal Digital Architect, McLaren Racing

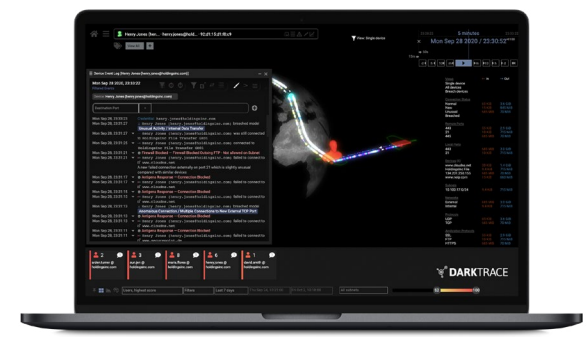
Ein Posteingang, der eigenständig für Sicherheit sorgt

Wie jedes Unternehmen ist auch McLaren diversen E-Mail-Bedrohungen ausgesetzt, von Social-Engineering über Phishing bis hin zu Kontoübernahmen. Vor allem raffinierte und gezielte Spear-Phishing-Angriffe auf Führungskräfte bereiteten dem Unternehmen Sorge. Angesichts der zunehmenden E-Mail-Angriffe erweiterte McLaren sein KI-basiertes Sicherheitssystem mit Antigena Email, um seine Microsoft 365-Umgebung und seine Belegschaft vor schädlichen E-Mails zu schützen.

Antigena Email basiert ebenfalls auf einem selbstlernenden, KI-gestützten Ansatz. Die Technologie kennt die Kommunikationsmuster zwischen den einzelnen E-Mail-Nutzern und registriert daher subtile Hinweise auf einen Angriff. Anstatt eingehende E-Mails mit vordefinierten Regeln und Signaturen abzugleichen, analysiert Darktrace E-Mails im Kontext. Neuartige und raffinierte Angriffe werden abgewehrt und der Geschäftsbetrieb läuft ohne Unterbrechung ganz normal weiter.

„Schon nach wenigen Tagen sahen wir erste Ergebnisse“, so Green. „Das Volumen der von Nutzern gemeldeten Phishing-E-Mails ging stark zurück, und durch die regelmäßige Analyse der von Antigena Email ergriffenen Maßnahmen entdeckten wir viele bisher unbemerkte Phishing-Kampagnen.“

> „Darktrace hat in diesem Jahr so viele Bedrohungen erkannt, dazu wäre ein Mensch nicht in der Lage gewesen. Das gibt uns ein gutes Gefühl.“
>
> Principal Digital Architect, McLaren Racing



Der Threat Visualizer macht Bedrohungen in Cloud-, SaaS- und E-Mail-Umgebungen sowie im Unternehmensnetzwerk sichtbar

Weitere Informationen

- Kostenlose Testversion anfordern
- Whitepaper: Darktrace Immune System
- Besuchen Sie unseren YouTube-Kanal