Enterprise Immune System und Darktrace Antigena

Cyber-KI für Cloud- und SaaS-Plattformen

Die auf der weltweit führenden KI-Technologie basierende Cyber AI Platform von Darktrace gewährleistet die Sicherheit dynamischer Cloud- und SaaS-Plattformen jeglicher Art und ist in der Lage, sich im Zuge der Weiterentwicklung und Erweiterung dieser Lösungen autonom anzupassen. Darktrace deckt zuvor unbemerkte Bedrohungen – egal ob Insider-Bedrohungen, kompromittierte Zugangsdaten oder kritische Fehlkonfigurationen – in der Cloud auf, um Ihre Daten unabhängig von ihrem Speicherort effektiv zu schützen.

Die wichtigsten Vorteile im Überblick

- ✔ Erlernt den „Normalzustand" einer Plattform, um Cloud-basierte Bedrohungen aufzudecken, die anderen Lösungen entgehen
- ✔ Einheitlicher Schutz über Hybrid- und Multi-Cloud-Umgebungen hinweg
- ✔ 100-prozentige Echtzeit-Sichtbarkeit für eine zuverlässige Erkennung von Angreifern
- ✔ Autonomous Response zur sekundenschnellen Neutralisierung von Bedrohungen, sobald diese auftreten

Die KI von Darktrace erkennt:

- Datendiebstahl durch Insider
- Kompromittierte Zugangsdaten
- Social Engineering
- Kritische Fehlkonfigurationen
- Supply-Chain-Angriffe
- Lateral Movement (Seitwärtsbewegung)

Cloud-nativer Schutz

box, salesforce, Google Cloud Platform, G Suite, OneDrive, aws, Microsoft Azure, Microsoft 365, Dropbox, SharePoint

Das zuverlässige Immunsystem für Ihre Cloud-Umgebung

Unternehmen setzen heute zunehmend auf die Cloud, um ihre Betriebsabläufe zu optimieren und Innovationen zu fördern. Vor diesem Hintergrund hat die Herausforderung, wichtige Daten zu schützen, eine ganz neue Dimension angenommen. Für viele Sicherheitsteams ist die Cloud in all ihren Ausprägungen oft noch Neuland – ein Umstand, dessen sich niemand besser bewusst ist als Cyberkriminelle.

Die Cyber-KI von Darktrace schützt Ihre Cloud-Umgebung vor Angriffen, indem sie die einzigartigen „normale Verhaltensmuster (Patterns of Life)" all Ihrer Benutzer, Container und VMs von Grund auf analysiert und mit dem Rest des Unternehmens in Verbindung setzt. Anhand dieser Echtzeit-Informationen über den „Normalzustand" ist Darktrace in der Lage, schwer aufzuspürende Bedrohungen oder Fehlkonfigurationen in der Cloud, die anderen Tools entgehen, zu erkennen und zu beseitigen.

Einheitlicher und maßgeschneiderter Schutz

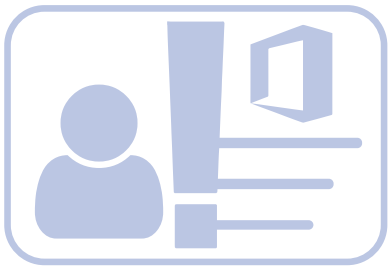
Cyberkriminelle nehmen immer häufiger mehrere Technologien auf einmal ins Visier. Daher ist es für Unternehmen von entscheidender Bedeutung, einheitliche Schutzmaßnahmen für ihre gesamte digitale Geschäftsaktivität zu konfigurieren. Banale Vorfälle wie ein kompromittiertes Passwort können zu einem gleichzeitigen Angriff auf mehrere Infrastrukturen führen. In einer Zeit, in der Sicherheit keine Frage des Schutzes einzelner Technologien mehr ist, spielt die Erkennung solcher Bedrohungen in Echtzeit eine entscheidende Rolle.

Die selbstlernenden Lösungen von Darktrace sind einzigartig aufgestellt, um neuartige Angriffe und Insider-Bedrohungen in der Cloud zu erkennen und abzuwehren. Warum? Weil sie die Fähigkeit besitzen, die individuelle „DNA" Ihrer gesamten Organisation zu entschlüsseln. Für sich betrachtet, erscheinen subtile Anzeichen eines Angriffs häufig vermeintlich harmlos. Darktrace liefert Ihnen individuellen, unternehmensübergreifenden Kontext, der selbst schwer zu erkennende Bedrohungen ans Licht bringt.

Native Cloud Security in AWS, Azure & GCP

Für Organisationen, die Infrastruktur via AWS, Azure und GCP betreiben, bietet Darktrace native Unterstützung über AWS VPC Traffic Mirroring, Azure vTAP und GCP Packet Mirroring. Diese Systeme bieten Darktrace detaillierte Echtzeit-Einblicke in den Cloud-Datenverkehr, ohne dass Capture Agents erforderlich wären.

Fallstudie: Kompromittierte Zugangsdaten in Microsoft 365



Eine internationale Organisation konnte dank Darktrace einen Sicherheitsvorfall im Rahmen eines Microsoft-365-Kontos aufdecken, der zuvor von den integrierten Kontrollfunktionen von Azure Active Directory unbemerkt blieb. Zwar verfügt die Organisation über Niederlassungen in jedem Winkel der Welt, doch die KI-Technologie von Darktrace wurde auf eine Anmeldung über eine für die betreffende Benutzerin und ihre Peer-Group ungewöhnliche IP-Adresse aufmerksam. Das Sicherheitsteam wurde umgehend über den Vorfall in Kenntnis gesetzt.

Wie Darktrace meldete, wurde über das Konto eine neue E-Mail-Verarbeitungsregel zur Löschung eingehender E-Mails eingerichtet – ein klares Anzeichen eines Sicherheitsvorfalls. Das Sicherheitsteam handelte schnell und konnte das Konto sperren, bevor der Angreifer Schaden anrichten konnte.

Kundenstimmen

> Als wir beschlossen, Darktrace zum Schutz unserer Cloud-Umgebung einzurichten, war es, als hätten wir in einem dunklen Raum den Lichtschalter umgelegt.
>
> **- Leiter der IT-Abteilung von TRJ Télécom**

> Kein anderer Anbieter kann Darktrace das Wasser reichen, wenn es darum geht, Cloud-basierte Bedrohungen zu erkennen, bevor sie zu einem Problem werden.
>
> **- CISO, Aptean**

> Darktrace setzt völlig neue Maßstäbe in der KI-basierten Cyber-Verteidigung. Unser Team profitiert jetzt von umfassendem Echtzeit-Schutz im Rahmen all unserer SaaS-Anwendungen und Cloud-Container.
>
> **- Leiter der IT-Abteilung der Stadtverwaltung Las Vegas**

Weitere Informationen

Jetzt Demo anfordern

Cloud-Whitepaper

Das sagen unsere Kunden