DARKTRACE

Die Evolution der Autonomous Response

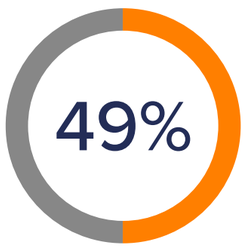
Schutz und Verteidigung in einer neuen Ära von Cyberbedrohungen

Eine neue Ära der Cyberbedrohungen

Dem Weltwirtschaftsforum zufolge rangieren Cyberangriffe auf Platz 4 der deutlichsten und unmittelbarsten Gefahren für die Menschheit. Die Bedrohungsakteure gehen immer raffinierter vor und die Unternehmen sind in zunehmend fragmentierten digitalen Ökosystemen tätig – mit dem Ergebnis, dass traditionelle Sicherheitstools entweder zu langsam oder zu isoliert sind, um den Bedrohungen wirklich etwas entgegenzusetzen.

Hybride Arbeitsformen haben diese Herausforderung zweifelsohne weiter erschwert, da sensible Daten jetzt über ein komplexes Geflecht von Clouddiensten, SaaS-Plattformen, Unternehmensnetzwerken und Mitarbeitergeräten ausgetauscht werden. Cyberkriminelle haben schnell herausgefunden, wie sie diese immer größer werdende Angriffsfläche für sich nutzen können.

Spear-Phishing und Ransomware bereiten den Sicherheitsexperten weiterhin am meisten Sorge. Da die Cyberkriminellen sich immer neue Methoden einfallen lassen und ihre Angriffe schneller denn je an neue Gegebenheiten anpassen, steht die Welt an der Schwelle zu einer neuen Ära von Cyberbedrohungen.



der Befragten im World Economic Risk Report 2021 gehen davon aus, dass Defizite in der Cybersicherheit in 3–5 Jahren zu einer kritischen Bedrohung für die Welt werden.

World Economic Forum

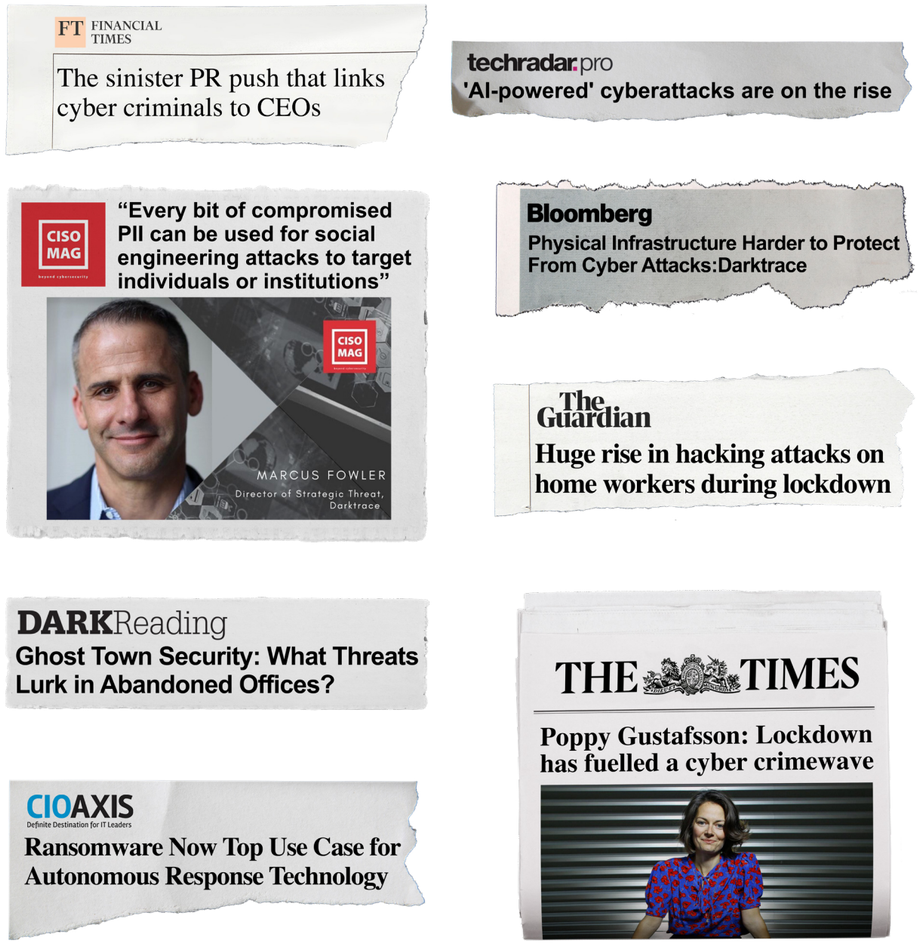


Abbildung 1: Cyberangriffe beherrschen immer wieder die Schlagzeilen, vom Colonial-Pipeline-Angriff bis SolarWinds

Ein Kampf der Maschinen: KI gegen KI

Sicherheitsteams haben jetzt schon Probleme, mit den heutigen Bedrohungen Schritt zu halten. Wie groß werden die Schwierigkeiten erst sein, wenn KI-gestützte Angriffe in normalen Benutzerumgebungen auftauchen? In einem kürzlich von MIT Tech Review veröffentlichten Artikel heißt es, dass „offensive KI“ die Dimension, die Schnelligkeit und die Komplexität von Angriffen erhöhen und damit jede Stufe der „Kill Chain“ noch gefährlicher machen dürfte.

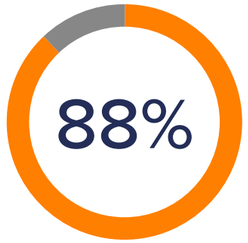
Mithilfe von Deep-Learning-Analytik kann KI den Personalisierungsgrad von Angriffen steigern, was die Präzision und die Erfolgsquote erhöht. Gleichzeitig sind Cyberkriminelle besser in der Lage, die Ausgestaltung und die Abwehrstrategie der digitalen Infrastruktur und der Daten ihrer Angriffsziele vorherzusagen.

Die heutige Cybersicherheit ist nicht mehr nur ein Problem auf menschlicher Ebene, sondern ein Kampf Maschine gegen Maschine. Es ist unabdingbar, dass Unternehmen defensive KI nutzen, um sich vor dieser nächsten Generation automatisierter Angriffe zu schützen.

Der Autonomous-Response-Technologie kommt eine fundamentale Bedeutung bei der Abwehr laufender Bedrohungen zu, egal wie neuartig oder raffiniert sie sind. Selbstlernende KI weiß, wie und wann sie reagieren muss, um schädliche Aktivitäten gezielt und verhältnismäßig unter Kontrolle zu bringen, ohne den normalen Geschäftsbetrieb zu stören.

der Führungskräfte haben bereits begonnen, sich für KI-gestützte Cyberangriffe zu wappnen.

MIT Tech Review Report



der Cybersicherheitsexperten gehen davon aus, dass KI-gestützte Angriffe bald üblich sein werden.

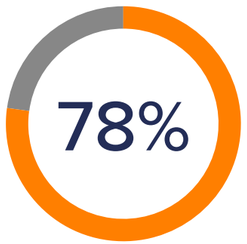
Forrester

Die Grenzen eines traditionellen Ansatzes

Viele gängige Sicherheitstools – von Firewalls und Antivirus-Programmen bis hin zu E-Mail-Gateways und Präventionsmechanismen – basieren auf einem retrospektiven Ansatz für die Bedrohungserkennung. Da sie auf vordefinierte Regeln, Signaturen und Playbooks angewiesen sind, können sie keine neuartigen Angriffe stoppen.

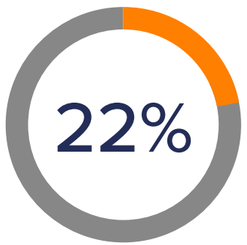
Hinzu kommt, dass sich die Cybersicherheit in Silos entwickelt hat. Angesichts unvorhersehbaren Mitarbeiterverhaltens über unterschiedlichste Dienste und Infrastrukturen hinweg fehlt es isolierten Punktlösungen an Sichtbarkeit und Kontext, ohne die sich schädliche Aktivitäten aber nicht von unschädlichen unterscheiden lassen.

Traditionelle Tools gleichen dieses fehlende Kontextwissen dadurch aus, dass sie sehr aggressive Maßnahmen ergreifen, was zu einer Flut an Fehlalarmen und einer destruktiven Reaktion führt.



der IT-Experten halten die Cybersicherheit Ihres Unternehmens für unzureichend.

IDG



der Unternehmen haben keinen ausreichenden Überblick über die Cloud.

Cybersecurity Insiders

Automatisierte vs. autonome Reaktion

Angesichts der Schnelligkeit, der Dimension und der Komplexität moderner Cyberbedrohungen sind menschliche Teams allein nicht mehr in der Lage, den Angreifern zuvorzukommen. Unternehmen brauchen eine Technologie, die Angriffe nicht nur erkennt, sondern auch abwehrt – ohne dass ein Mensch die entsprechende Maßnahme vorher genehmigen muss.

Aus dieser Notwendigkeit heraus wurden automatisierte Response-Lösungen wie SOARs, E-Mail-Gateways und „Next-Gen“-IPS entwickelt. Diese Tools kommen mit bekannten Bedrohungen zurecht, sind aber auf historische Angriffsdaten und vordefinierte Regeln angewiesen.

Das macht ihre Response-Mechanismen mechanisch, unflexibel und schwerfällig – sie bieten keine situativ angepassten Maßnahmen, sondern ein Standardprogramm. Bei Angriffsformen wie z.B. Ransomware gibt es nur eine Lösung, entweder werden die Systeme verschlüsselt oder der Geschäftsbetrieb wird heruntergefahren.

Für die Verteidigung ist eine eigenständige Reaktion notwendig – nur so können laufende Cyberangriffe wirklich gezielt und verhältnismäßig gestoppt werden.

Die Autonomous-Response-Technologie entwickelt ein Verständnis der normalen Verhaltensweisen jedes Benutzers und Geräts in einem Unternehmen sowie der Beziehungen untereinander. Dadurch erkennt die KI selbst subtile Hinweise auf eine Bedrohung und ergreift in Echtzeit minimalinvasive Maßnahmen, um die schädliche Aktivität zu stoppen. Der Geschäftsbetrieb kann dabei ganz normal weiterlaufen.

Autonome Selbstlernende KI

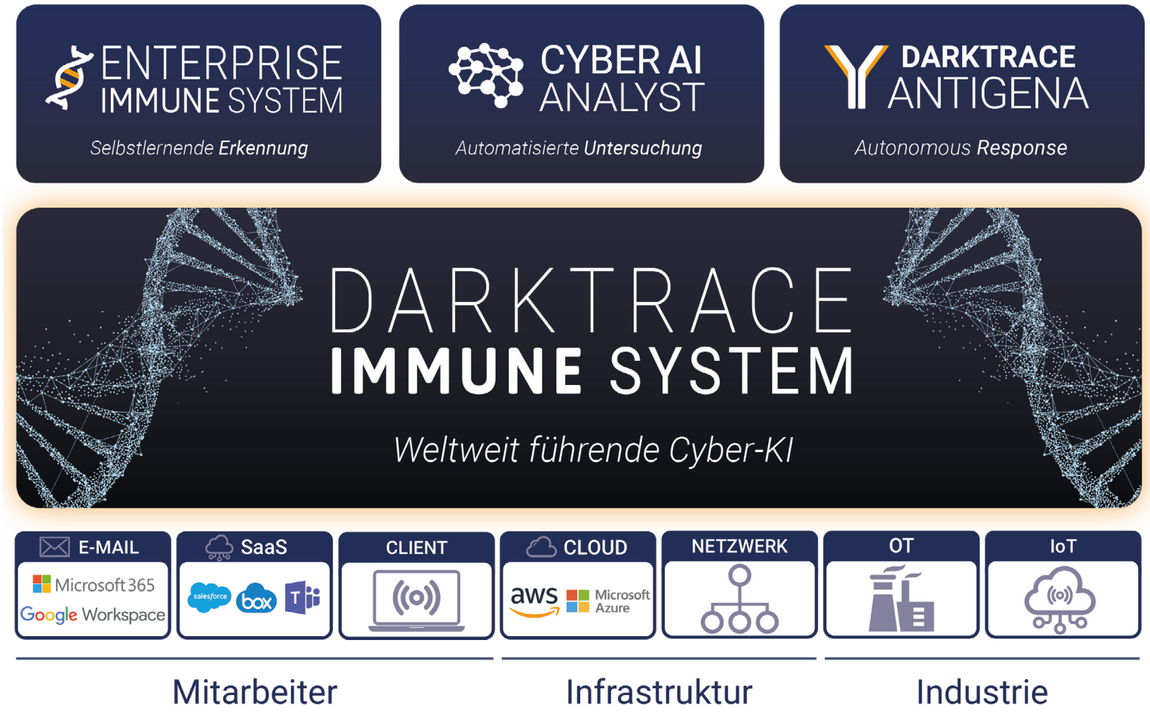


Abbildung 2: Die Immune System Platform von Darktrace

„Wir hatten schon alle herkömmlichen Sicherheitsmaßnahmen ergriffen, aber wir brauchten eine neue Lösung, weil sie uns nicht vor Zero-Day-Exploits schützten. Man liegt immer einen Tag zurück."

Head of Information Security, British Land

Autonome selbstlernende KI wehrt laufende Cyberangriffe Sekunden nach ihrem Auftreten ab, ohne dass ein Mensch eingreifen muss.

Während traditionelle Lösungen vordefinieren, was „schädlich" oder „unschädlich" ist, kennt autonome selbstlernende KI die digitale DNA eines Unternehmens und kann gezielte Angriffe aufspüren und stoppen. Diese dynamische und anpassungsfähige Technologie beruht auf nicht überwachtem maschinellem Lernen und wehrt Bedrohungen ab, die statische Tools übersehen.

Darktrace Antigena ergreift Maßnahmen gegen Cyberbedrohungen in der gesamten digitalen Umgebung, vom Unternehmensnetzwerk über das E-Mail-System bin hin zu Cloudanwendungen.

Autonomous Response: Stoppt Angriffe gezielt und schneller als jeder Mensch

Darktrace Antigena ist eine KI-gestützte Entscheidungsinstanz, die binnen Sekunden aktiv wird, um minimalinvasiv bekannte und unbekannte Bedrohungen in Echtzeit abzuwehren und Unternehmen zu unterstützen, sich selbst zu verteidigen.

Autonomous-Response-Technologie bestimmt eigenständig, welche Maßnahme die beste ist, um laufende Angriffe blitzschnell abzuwehren. Im Gegensatz zu traditionellen Tools verlässt sich selbstlernende KI nicht auf vorprogrammierte, statische Maßnahmen und Regeln, sondern reagiert situativ und dynamisch auf ungewöhnliche Aktivitäten.

Dabei setzt die Technologie die normalen Verhaltensmuster, die sogenannten „Patterns of Life“, der kompromittierten Benutzer und Geräte durch. Nur die schädlichen Aktivitäten werden unterbunden, damit Mitarbeiter und Systeme wie gewohnt weiterarbeiten können.

Die verhältnismäßigen und extrem präzisen Maßnahmen von Darktrace Antigena sind nur möglich, weil die Technologie sich fortwährend ein granulares Bild der „normalen“ Verhaltensweisen jedes Teils des digitalen Ökosystems macht.

> „Die eigenständige Cyber-Response von Darktrace ist nicht nur deshalb so wichtig, weil der Mensch allein mit den heutigen Bedrohungen nicht Schritt halten kann, sondern auch, weil uns in Zukunft rein KI-basierte Angriffe erwarten.“
>
> CIO, Elias Neocleous

Highlights

- Stoppt auch unvorhersehbare und besonders schnelle Angriffe
- Ergreift minimalinvasive und verhältnismäßige Maßnahmen, die den Geschäftsbetrieb nicht stören
- Passt sich an beständige, sich entwickelnde Bedrohungen an
- Überwacht das gesamte digitale Ökosystem
- Schützt rund um die Uhr – auch nachts und am Wochenende

Abbildung 3: Autonomous Response neutralisiert Bedrohungen, egal wo und wann sie auftreten – ohne dass ein Mensch eingreifen muss

Rund um die Uhr geschützt

Tausende Unternehmen weltweit setzen auf Autonomous-Response-Technologie, um Bedrohungen binnen Sekunden zu stoppen. Darktrace Antigena schützt kritische Daten und Systeme eigenständig und rund um die Uhr, wenn IT-Teams überfordert, unvorbereitet oder einfach nicht im Büro sind – nachts, am Wochenende oder in der Urlaubszeit.

Darktrace Antigena bietet Schutz vor dem gesamten Bedrohungsspektrum:

- Ransomware
- Datenexfiltration
- Spear-Phishing
- Malware
- Cryptojacking
- Kompromittierung von SaaS-Zugangsdaten

Darktrace Antigena neutralisiert jede Sekunde irgendwo auf der Welt eine Bedrohung – und verschafft damit den Mitarbeitern wertvolle Zeit für strategische Aufgaben.

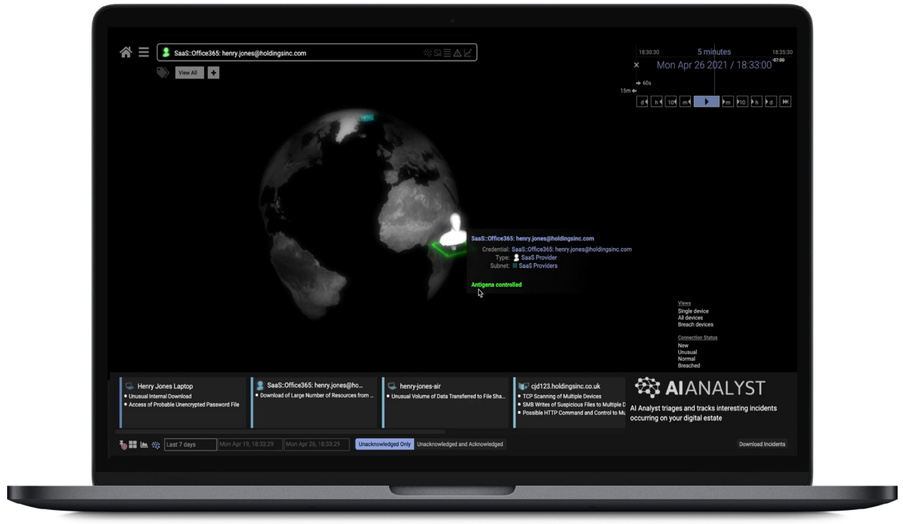


Abbildung 4: Antigena ergreift gezielte und verhältnismäßige Maßnahmen, um Bedrohungen zu stoppen und gleichzeitig den normalen Geschäftsbetrieb aufrechtzuerhalten

„Da KI Angriffe eigenständig binnen Sekunden stoppt, können wir sicher sein, dass unsere Daten vor Cyberkriminellen geschützt sind – obwohl unsere Branche von Tag zu Tag anfälliger wird."

General Manager, Global Travel

Selbstlernende KI im gesamten Unternehmen: Aufbau von Cyber-Resilienz

Ganzheitliche Schutzmaßnahmen sind angesichts sich weiterentwickelnder Bedrohungen und wachsender Komplexität heute wichtiger denn je.

Darktrace Antigena kennt und versteht den gesamten digitalen Fußabdruck der Mitarbeiter. Durch diesen umfassenden, gebündelten Ansatz kann die KI von einem unscheinbaren isolierten Verhalten auf eine viel breitere schädliche Aktivität schließen.

Die selbstlernende KI entwickelt sich mit ihrer Umgebung und passt sich an, wenn neue Technologien, Mitarbeiter und Systeme hinzukommen. Dies ist der entscheidende Faktor für den Aufbau von Cyber-Resilienz, denn die KI lernt im Einsatz und überprüft fortwährend ihr Bild der normalen Verhaltensweisen. So kann sie schädliche Aktivitäten minimalinvasiv neutralisieren.

Eigenständig handelnde selbstlernende KI lässt Angreifern keinen Raum, sich zu verstecken.

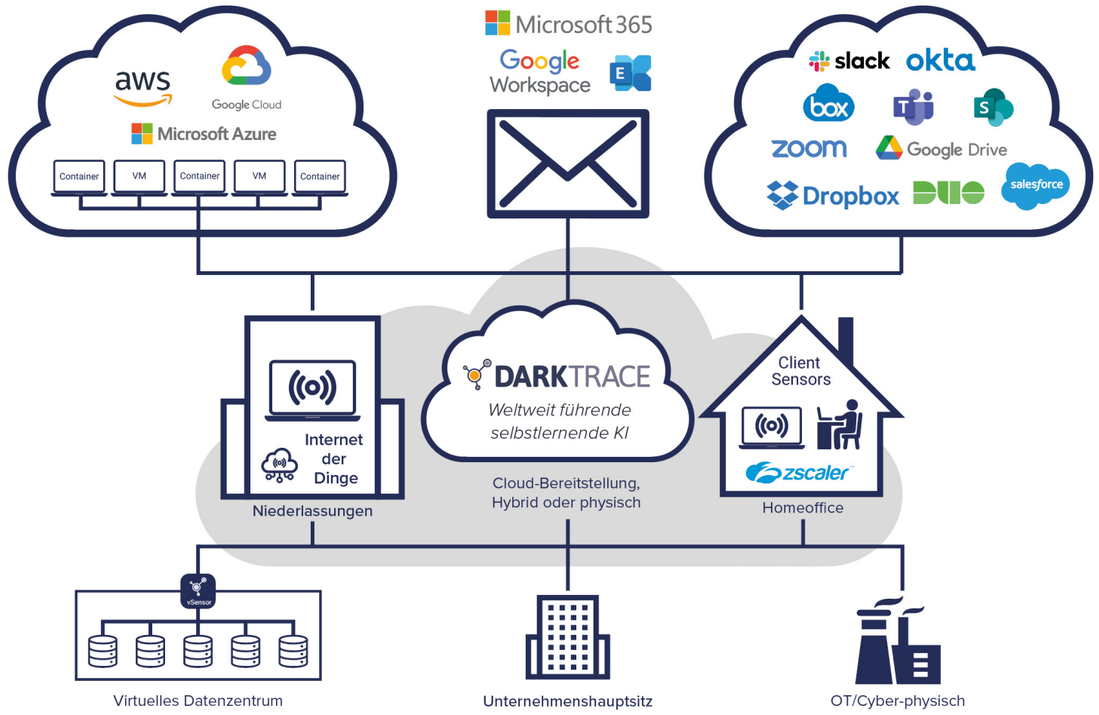


Abbildung 5: Darktrace schützt eigenständig digitale Infrastruktur, sensible Daten und Mitarbeiter – jederzeit und überall

Dynamische Bedrohungen jederzeit neutralisieren

Darktrace Antigena passt sich den Bedrohungen an, während sie sich entwickeln, und ist in der Lage, Angriffe an jedem Punkt und in jeder Phase der „Kill Chain“ in Echtzeit zu stoppen. Die Autonomous-Response-Technologie basiert auf nicht überwachtem maschinellem Lernen und kann daher mit dem Unternehmen wachsen, ohne dass eine manuelle Konfiguration oder Feinabstimmung nötig ist – selbst bei erheblichen Veränderungen.

Blitzschnelle Abwehr von Ransomware

Antigena Network neutralisiert die gesamte Bandbreite von Bedrohungen im Unternehmensnetzwerk und Internet der Dinge – von Ransomware mit ultraschneller Ausbreitung bis hin zu „Low & Slow“-Angriffen und Zero-Day-Exploits.

Die Entscheidungen von Antigena Network basieren auf dem Verständnis der normalen Verhaltensweisen, das fortwährend angepasst wird und in das auch Erkenntnisse aus Cloud-, SaaS- und E-Mail-Umgebungen sowie Mitarbeitergeräten einbezogen werden.

So ergreift die selbstlernende KI für jede Bedrohung andere Maßnahmen, weil sie weiß, wie, wann und wo schädliche Aktivität zu neutralisieren ist. Der normale Geschäftsbetrieb läuft dabei weiter.

> „Darktrace hilft uns, mit den aktuellen Veränderungen im digitalen Bereich Schritt zu halten.“
>
> CIO, McLaren Group

Schutz vor Spear-Phishing

Antigena Email neutralisiert gezielte Spear-Phishing-Kampagnen und Impersonation-Angriffe, die von traditionellen Tools übersehen werden. Darktrace kennt die normalen Verhaltensmuster – die „Patterns of Life“ – jedes Benutzers und Kommunikationspartners und ist die einzige Technologie, die tatsächlich den Menschen hinter den E-Mail-Kommunikation versteht.

So erkennt die KI genau, wenn eine bestimmte E-Mail stark von den normalen Interaktionen zwischen Absender, Empfänger und dem breiteren Unternehmen abweicht, und kann die Bedrohung im Keim ersticken.

Antigena Email sperrt eigenständig Links, wandelt Anhänge in harmlose Dateitypen um und hält E-Mails zurück, um die dynamische Belegschaft vor dem gesamten Bedrohungsspektrum zu schützen.

Schutz von Cloud- und SaaS-Umgebungen

Von unachtsamen Insidern in SharePoint und kompromittierten Microsoft Teams-Zugangsdaten bis hin zu Konfigurationsfehlern in OneDrive und Zoom – Antigena SaaS ist auf einzigartige Weise in der Lage, aufkommende cloudbasierte Bedrohungen selbstständig und frühzeitig zu erkennen und abzuwehren.

Die KI setzt Aktivitäten innerhalb und außerhalb des VPN in Echtzeit zum Traffic in Hybrid- und Multi-Cloud-Umgebungen in Beziehung. So erkennt Darktrace im breiteren Kontext des Unternehmens die tatsächliche Gefahr, die von scheinbar harmlosen Aktivitäten ausgeht.

Schutz von Endgeräten innerhalb und außerhalb des VPN

Darktrace Antigena bietet eigenständigen Schutz für mobile Mitarbeiter innerhalb und außerhalb des VPN und erkennt bekannte und unbekannte Bedrohungen wie Insider, latente Malware-Stämme, Downloads von nicht autorisierten Anwendungen und Programmen sowie Compliance-Probleme.

Die KI analysiert Echtzeit-Traffic von Benutzern und setzt die vielen verschiedenen Verbindungen zueinander in Beziehung, um sich ein Bild von den normalen Verhaltensweisen der Mitarbeiter zu machen. So ist Darktrace nicht nur in der Lage, Cyberbedrohungen auf Endgeräten zu erkennen, sondern ergreift auch minimalinvasive und verhältnismäßige Maßnahmen.

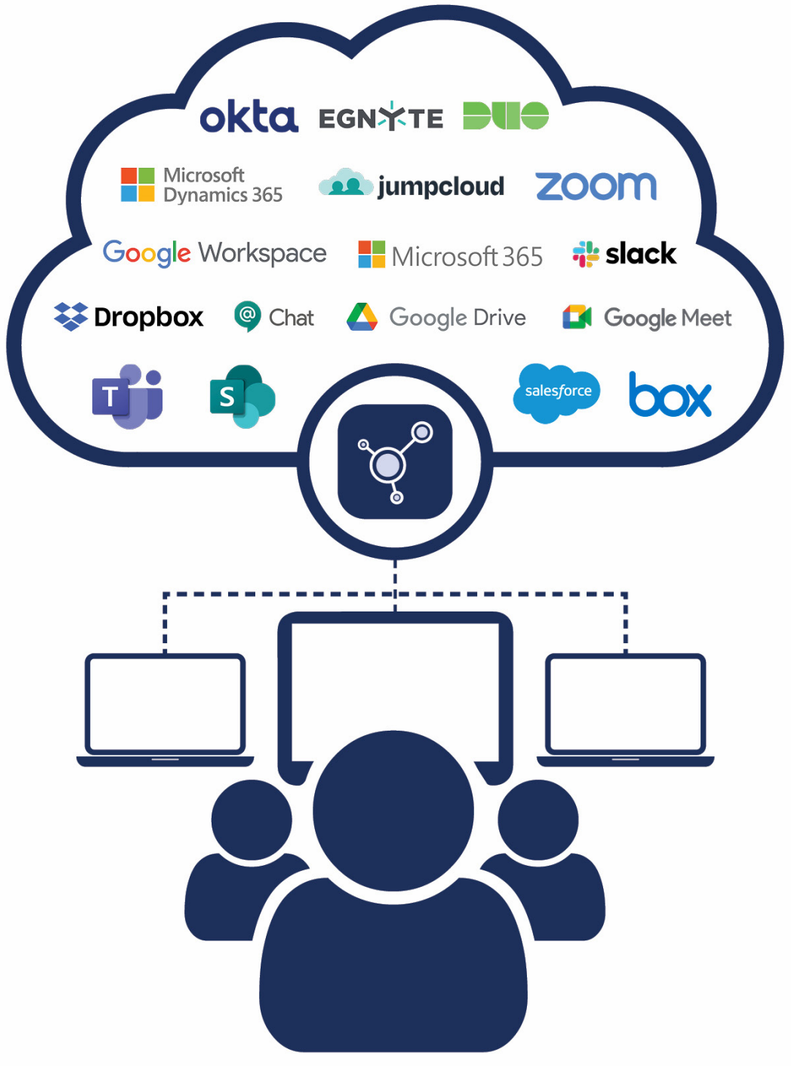


Abbildung 6: Darktrace integriert sich nahtlos in eine Vielzahl von Cloud- und SaaS-Technologien

KI-gestützte Entscheidungen: Ein intelligentes Response-Konzept

Bei schädlichen Aktivitäten kann Antigena entweder eigenständig dagegen vorgehen oder Erkenntnisse zu Vorfällen an vorhandene Drittanbieter-Sicherheitssysteme übermitteln. In jedem Fall entscheidet Darktrace Antigena selbst darüber, welche Maßnahme am sinnvollsten ist. Die Maßnahmen, die Darktrace Antigena ergreifen kann, lassen sich grob zwei Kategorien zuordnen:

Taktische Reaktion

Mit der taktischen Reaktion ergreift Darktrace eigene Maßnahmen, um Angriffe binnen Sekunden unschädlich zu machen.

Jede Reaktion erfolgt mit äußerster Präzision und beruht auf dem granularen Verständnis der normalen Verhaltensmuster jedes Benutzers, jedes Geräts und jeder Vergleichsgruppe sowie des Unternehmens als Ganzes. So kann Darktrace Antigena entscheiden, welche Ereignisse Autonomous Response erfordern, während der Geschäftsbetrieb ganz normal weiterläuft.

> „Die Integration von Darktrace in unser SIEM war für unser Team kinderleicht. Dabei hat die Einbindung des Immune System an all den verschiedenen Integrationspunkten ein enormes Potenzial in unserem SOC freigesetzt."
>
> Security Engineer, A&M

Strategische Reaktion

Bei der strategischen Reaktion agiert Darktrace als „KI-Gehirn" der gesamten Sicherheitsinfrastruktur.

Das bedeutet, dass Darktrace Erkenntnisse über die von der KI zuverlässig erkannten Bedrohungen an Drittanbieter-Systeme als Response-Mechanismus weiterreicht.

Durch aktive Integrationen kann sich Antigena Network nahtlos in die vorhandene Sicherheitsinfrastruktur des Unternehmens einklinken. Dadurch erhalten Firewalls, Netzwerkgeräte, Zero-Trust-Technologien und Lambda-Funktionen Informationen zu Angriffen, die es geschafft haben, in das System einzudringen.

Darktrace kann sogar die Maßnahmen von Drittanbieter-Systemen basierend auf den Spezifikationen der Systembetreiber steuern.

Bedrohungsvorfälle: Ransomware

Die letzte Phase der „Kill Chain“ eines Angriffs, die Ransomware, ist eine der schnellsten und gefährlichsten Bedrohungen. Die selbstlernende KI von Darktrace erkennt neuartige und heimtückische Ransomware und stoppt die Bedrohungen minimalinvasiv binnen Sekunden mit Autonomous Response.

Eigenständige Neutralisierung von Zero-Day-Ransomware

Darktrace Antigena stoppte einen Zero-Day Ransomware-Angriff auf einen Elektronikhersteller. Die Bedrohung wurde frühzeitig erkannt und neutralisiert.

Es wurde beobachtet, dass das Gerät ungewöhnlich viele Verbindungen aufbaute, mehrere SMB-Dateien schrieb und Daten intern zu einem Server übertrug, mit dem es normalerweise nicht kommunizierte. Es erfolgte dann ein Zugriff auf mehrere hundert Dropbox-bezogene Dateien in SMB-Freigaben. Einige dieser Dateien wurden verschlüsselt und es wurde die Erweiterung [HELP_ DECRYPT] angehängt.

Darktrace Antigena trat eine Sekunde später in Aktion. Die Technologie setzte das normale Verhaltensmuster des Geräts durch und stoppte sofort die Verschlüsselung. Zu dem Zeitpunkt, als die selbstlernende KI eingriff, waren erst vier dieser Dateien verschlüsselt.

.

Dieser Ransomware-Stamm konnte nicht mit öffentlich bekannten Kompromittierungsindikatoren in Verbindung gebracht werden. Dennoch blieb der Angriff Darktrace nicht verborgen, weil die Technologie die normalen Verhaltensmuster jedes Geräts und Benutzers im Unternehmen kennt.

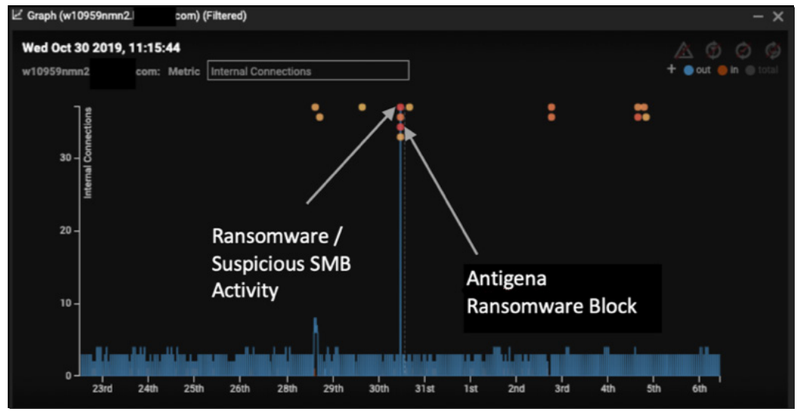


Abbildung 7: Am 30. Oktober wurden vier Modellabweichungen festgestellt. Die gepunktete Linie zeigt die Maßnahmen von Darktrace Antigena

Automatisierte Erpressung vor der Verschlüsselung gestoppt

Darktrace erkannte an einem Freitagabend eine Erpressungskampagne und reagierte entsprechend.

Ein Mitarbeiter rief seine privaten E-Mails mit einem Firmen-Smartphone ab und ließ sich dazu verleiten, eine schädliche Datei herunterzuladen. Diese enthielt Ransomware. Sekunden später verband sich das Gerät mit einem externen Server im Tor-Netzwerk und die SMB-Verschlüsselungsaktivitäten begannen.

Nur neun Sekunden später erkannte Darktrace die Bedrohung und gab eine Warnmeldung mit hoher Priorität aus. Da sich an dem Verhalten in den darauffolgenden Sekunden nichts änderte, korrigierte die KI ihre Einschätzung der Schwere der Bedrohung.

Das Sicherheitsteam war bereits im Wochenende, doch zum Glück war Darktrace Antigena zur Stelle und griff ein. Die selbstlernende KI stoppte den Angriff eigenständig, unterband alle Versuche, verschlüsselte Dateien in Netzwerkfreigaben zu schreiben, und verhinderte, dass auch nur eine einzige Datei verschlüsselt wurde.

> „Die Autonomous-Response-Technologie schaltet auch die heimtückischsten Ransomware-Angriffe aus, und das nur wenige Sekunden, nachdem die Bedrohung auftaucht."
>
> Chief Security Officer, Sun Life

Abbildung 8: Selbstlernende KI erkennt einen Ransomware-Angriff und neutralisiert die Bedrohung blitzschnell

Bedrohungsvorfälle: E-Mail-Angriffe

Traditionelle Gateways gleichen einzelne E-Mails mit Listen früherer Angriffe ab; die selbstlernende KI dagegen kennt die normalen Muster einer E-Mail-Kommunikation und registriert subtile Abweichungen, die auf eine Bedrohung hindeuten.

Abgreifen von Zugangsdaten verhindert

An einem der wichtigsten Rennwochenenden der Formel 1 wurde ein Mitglied der Führungsetage von McLaren Ziel eines Phishing-Angriffs, bei dem die betreffende Person aufgefordert wurde, ein Finanzdokument zu unterzeichnen. Die E-Mail kam scheinbar von DocuSign und enthielt einen schädlichen Link, der hinter dem Text „Dokument prüfen“ verborgen war.

Die E-Mail war sehr gut geschrieben und enthielt keine offensichtlichen Hinweise auf bösartige Absichten – dennoch erkannte Antigena Email die latente Bedrohung. Der Technologie fiel auf, dass der Absender im Kontext des Unternehmens und des Empfängers sehr ungewöhnlich war, zudem stufte sie die verborgene URL als verdächtig ein. Die KI entschied, den Link doppelt zu sperren und die E-Mail in den Spam-Ordner des Managers zu verschieben.

Hätte der Manager den Link angeklickt, wäre er zu einer Fake-Anmeldeseite gelangt, wo man seine Zugangsdaten abgegriffen hätte. Gleichzeitig enthielt die völlig normal aussehende Rechnung die Bankdaten der Verbrecher und wartete nur darauf, bezahlt zu werden.

Die Bedrohung wurde eigenständig neutralisiert, ohne dass das Cybersicherheitsteam alarmiert werden musste. So konnte sich das Team voll und ganz auf das Rennen konzentrieren.

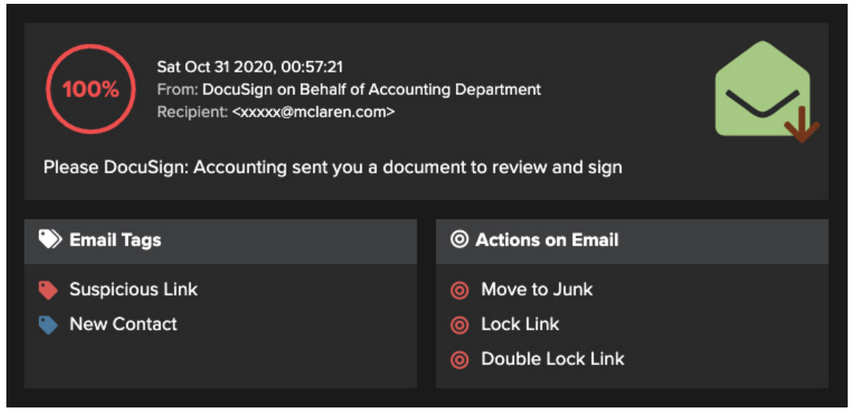


Abbildung 9: Snapshot der Benutzeroberfläche von Antigena Email nach der Entdeckung der E-Mail

> „Antigena Email hat Angriffe gestoppt, die sonst eingedrungen wären.“
>
> CISO, Calligo

Abwehr eines Siemens-Impersonation-Angriffs, der 78.000 USD gekostet hätte

In einem akademischen Institut hatte ein Angreifer die Kontrolle über ein internes Microsoft 365-Konto übernommen und schickte eine betrügerische Rechnung an die Buchhaltung der Einrichtung. Die Rechnung, die vorgeblich von Siemens kam, enthielt kaum merklich bearbeitete Bankdaten und das Institut zahlte über 60.000 USD auf das Bankkonto des Angreifers.

Zu diesem Zeitpunkt beschloss die Einrichtung, Antigena Email zu nutzen.

Eine Woche nach dem ersten Angriff wurde ein weiteres SaaS-Mitarbeiterkonto kompromittiert und es wurden neue E-Mail-Verarbeitungsregeln eingerichtet. Der Cyberkriminelle erstellte daraufhin eine E-Mail-Adresse, die vorgeblich zu Siemens gehörte, und kommunizierte mit dem gekaperten Mitarbeiterkonto.

Als der Cyberkriminelle sich erneut mit einer Siemens-Rechnung, dieses Mal über 78.000 USD, bei der Buchhaltung des Instituts meldete, erkannte Darktrace die Bedrohung. Die E-Mail wurde zurückgehalten und die Buchhaltung dadurch geschützt. Daraufhin griff der Angreifer eine unternehmensweite Kontaktliste ab und startete damit eine generischere Phishing-Kampagne an Dutzende von E-Mail-Nutzern im Unternehmen, um ihre Konten zu kompromittieren.

Antigena Email stufte jede dieser E-Mails als 100% anormal ein und hielt sie alle zurück.

Abbildung 10: Die intuitive Benutzeroberfläche von Antigena Email zeigt die Bedrohungstrends im Zeitverlauf

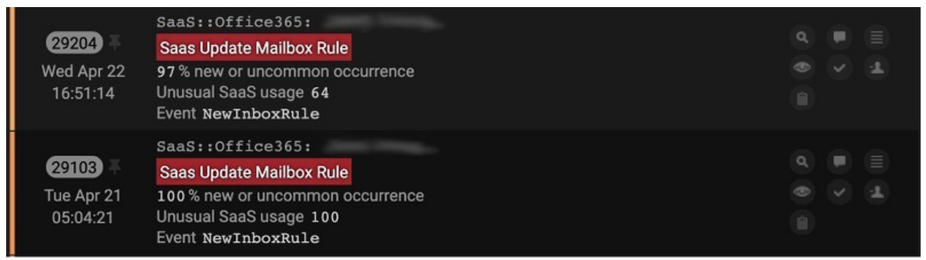


Abbildung 11: Darktrace erkennt die anormale Posteingangsregel und weist der Aktivität einen Anomaliewert von 97–100% zu.

Bedrohungsvorfälle: Kontoübernahmen

Cyberkriminelle können Unternehmenskonten auf vielfältige Weise kapern, von E-Mail-Angriffen bis hin zu Kommunikation im Dark Web. Das Ziel besteht letztendlich darin, entweder Daten zu stehlen oder über die E-Mail-Konten der Benutzer eine schädliche Massenkampagne zu starten. Während traditionelle Tools diesen Bedrohungsvektor häufig übersehen, ist Darktrace mit seinem Kontextwissen über die individuellen Verhaltensweisen jedes Benutzers in der Lage, Kontoübernahmen zu erkennen und abzuwehren.

Kompromittierung eines Microsoft 365-Kontos in SharePoint und Outlook

In einem führenden Technologieunternehmen wurde ein Mitarbeiter über das Wochenende Ziel einer Kontokompromittierung. Darktrace erkannte die Bedrohung frühzeitig – und hätte mit Darktrace Antigena im aktiven Modus die Bedrohung stoppen können, bevor Schaden entstand.

Der Angriff begann damit, dass sich ein Mitarbeiter von einem ungewöhnlichen Ort anmeldete. Der Benutzer richtete dann neue Posteingangsregeln ein und schaute sich mehrere sensible Dateien in Dateifreigaben an – alles außerhalb der normalen „Patterns of Life“ des betreffenden Mitarbeiters.

Mit Antigena Email und Antigena SaaS wäre die Bedrohung an dieser Stelle gestoppt worden. Da sich die KI aber im „Human Confirmation“-Modus befand, konnte der Angreifer mehr als 200 Phishing-E-Mails verschicken, die einen Link zu einer Microsoft OneDrive-Landingpage namens „Contract & Proposal – Customer“ enthielten. Auf der Seite befand sich ein Phishing-Link, der hinter dem Anzeigetext „Click to Review Fax Document“ verborgen war.

Kaum eine Stunde nach dem Versand der Phishing-E-Mails erkannte die Darktrace KI eine weitere ungewöhnliche Anmeldung von derselben IP-Adresse bei einem zweiten Konto im Unternehmen – was darauf hindeutete, dass auch dieses Konto kompromittiert worden war.

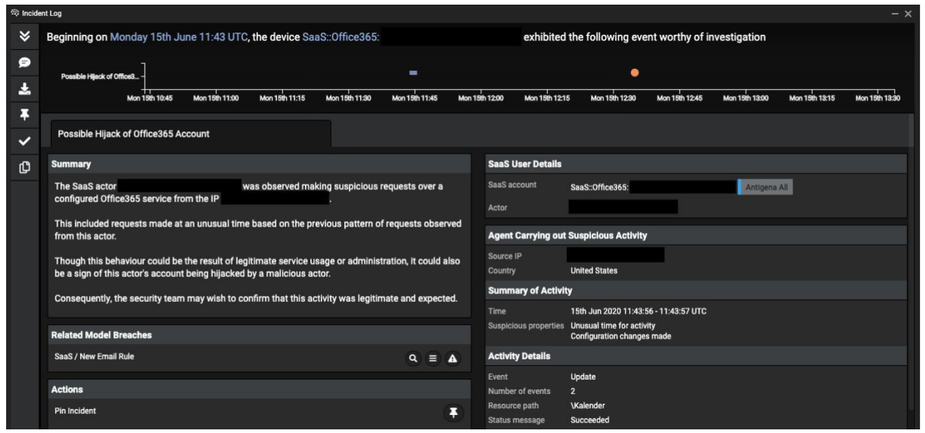


Abbildung 12: Auszug aus dem Bericht des Cyber AI Analyst zu der Kontoübernahme

Phishing-E-Mail führt zur Kompromittierung eines Microsoft 365-Kontos

Während der Testphase erkannte Darktrace einen laufenden Angriff auf ein Logistikunternehmen. Ein Cyberangreifer hatte die Konten einiger vertrauenswürdiger Zulieferer und Partner des Unternehmens gekapert und mehrere gezielte E-Mails von diesen Konten versendet.

15 dieser E-Mails wurden geöffnet. Ein Mitarbeiter klickte auf einen schädlichen Link, der ihn auf eine gefälschte Microsoft-Anmeldeseite führte, um seine Zugangsdaten abzugreifen. Hätte sich Antigena Email im aktiven Modus befunden, wären diese E-Mails gar nicht erst in die Posteingänge der Mitarbeiter gelangt.

Drei Stunden später wurde eine anormale SaaS-Anmeldung eines Mitarbeiters bei dem Konto festgestellt: Sie stammte von einer IP-Adresse, die in dem Unternehmen vorher noch nie benutzt worden war. An dieser Stelle hätte Antigena SaaS reagiert, das Konto des Benutzers gesperrt und sein „Pattern of Life“ durchgesetzt.

Stattdessen versendete der Angreifer weitere bösartige E-Mails von diesem Konto an Geschäftspartner des Unternehmens. Er folgte dabei derselben Methodik und verschickte gezielt gefälschte Angebotsanfragen, um sich unbefugt Zugangsdaten zu beschaffen.

Darktrace erkannte eigenständig dieses anormale Verhalten und zeigte grafisch an, dass der Angreifer binnen 25 Minuten gezielt mehr als 1.600 E-Mails verschickte. Der Managed Security Service Provider (MSSP), der sich um die Cloudsicherheit des Unternehmens kümmerte, hatte die feindliche Kontoübernahme nicht bemerkt.

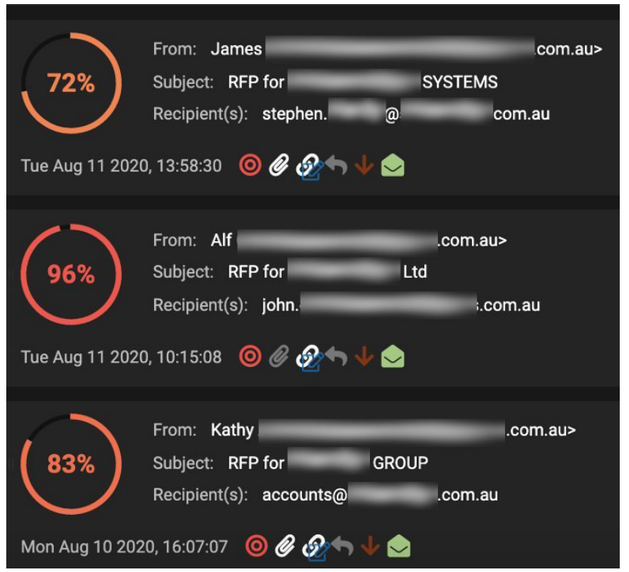


Abbildung 13: Beispiel für die schädlichen E-Mails, die von den gekaperten Konten gesendet wurden. Das rote Symbol zeigt an, dass Antigena Email diese E-Mails zurückgehalten hätte

„Mein Darktrace SaaS-Konnektor meldete ein kompromittiertes Microsoft-Konto. Dank dieser Warnmeldung konnte ich den Angreifern einen Strich durch die Rechnung machen und die Benutzerpasswörter innerhalb von 7 Minuten nach dem ersten unerlaubten Zugriff zurücksetzen.“

IT Manager, Hydrotech

Bedrohungsvorfälle: Datenexfiltration

Exfiltrationsangriffe können unterschiedliche Formen annehmen, von Insiderbedrohungen bis hin zu Malware-Installationen. Während es traditionellen Tools am unternehmensweiten Einblick fehlt, um übergeordnete Muster zu erfassen, die auf eine Bedrohung hindeuten, erkennt Darktrace mit genau diesem Wissen die subtilen Hinweise auf einen Angriff.

Gekränkter IT-Administrator versucht, Daten auszuschleusen

Darktrace erkannte eine Insiderbedrohung durch einen entlassenen IT-Systemadministrator.

Der Angriff begann damit, dass sich der ehemalige IT-Administrator bei seinem SaaS-Account anmeldete und schnell mehrere sensible Dateien aus der Kundendatenbank herunterlud, darunter Kontaktdaten und Kreditkartennummern. Er versuchte dann, diese über einen der regulären Datentransferdienste des Unternehmens auf einen Server bei sich zu Hause zu übertragen. Der IT-Administrator wusste, dass dieser spezielle Dienst vom Unternehmen genehmigt und zudem cloudbasiert war, und ging davon aus, dass das Sicherheitsteam kaum Einblick in diesen Bereich hatte.

Darktrace erkannte jedoch sofort die ungewöhnlich großen Dateidownloads und die Ausschleusung, woraufhin Darktrace Antigena umgehend den versuchten Upload blockierte.

Die anschließende Untersuchung ergab, dass der Mitarbeiter nach dem ersten fehlgeschlagenen Versuch weiter versuchte, die Daten auf anderen Wegen auszuschleusen – zunächst über sein Cloudkonto im Unternehmen und dann über sein Remote-Endgerät außerhalb des VPN. Darktrace Antigena unterband diese Versuche jedoch in jeder Phase.

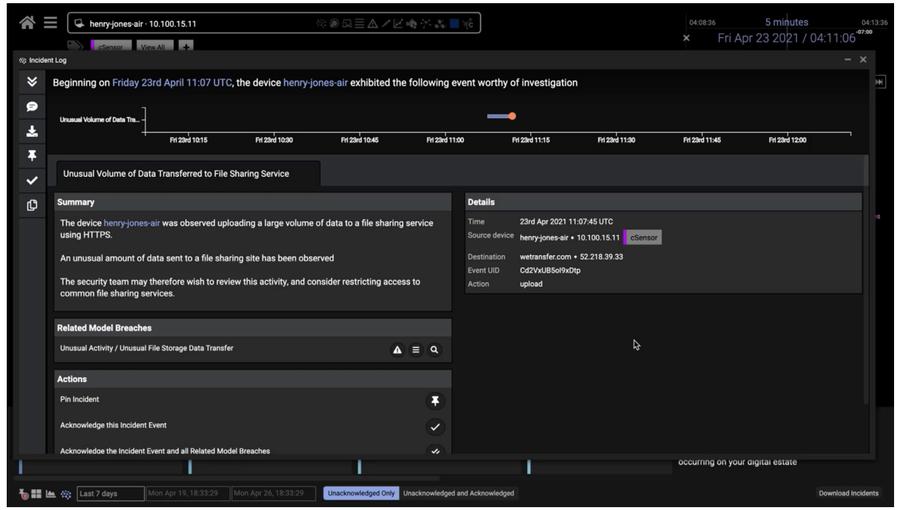


Abbildung 14: Zusammenfassung des Vorfalls durch den Cyber AI Analyst, einschließlich der Modellabweichungen und der ergriffenen Maßnahmen

Banking-Trojaner Cerberus gestoppt

In einem kanadischen Unternehmen wurde das Gerät eines Mitarbeiters durch eine bösartige E-Mail kompromittiert. Der Angreifer gelangte in das Unternehmensnetzwerk, indem er Malware installierte und sich als legitimer Benutzer ausgab. Er bewegte sich dann lateral im Unternehmen und suchte nach sensiblen Dateien und Daten.

Darktrace beobachtete ungewöhnliche Dateidownloads auf dem infizierten Gerät, auf die der Versuch folgte, Command & Control-Traffic einzurichten. Der Angreifer wollte vermutlich die gesammelten Daten ausschleusen, aber Darktrace Antigena unterband dies sofort.

Nachdem die KI eingegriffen hatte, nahm das Unternehmen das betreffende Gerät aus dem Netzwerk, scannte es und entfernte die Malware.

Bei der Malware handelte es sich um den Banking-Trojaner Cerberus. Diese frei verfügbare Malware kursiert in einschlägigen Hackerforen und dient der Auskundschaftung, dem Abfangen von Kommunikation, der Manipulation von Gerätefunktionen und der Ausschleusung sensibler Daten – einschließlich Banking-Daten.

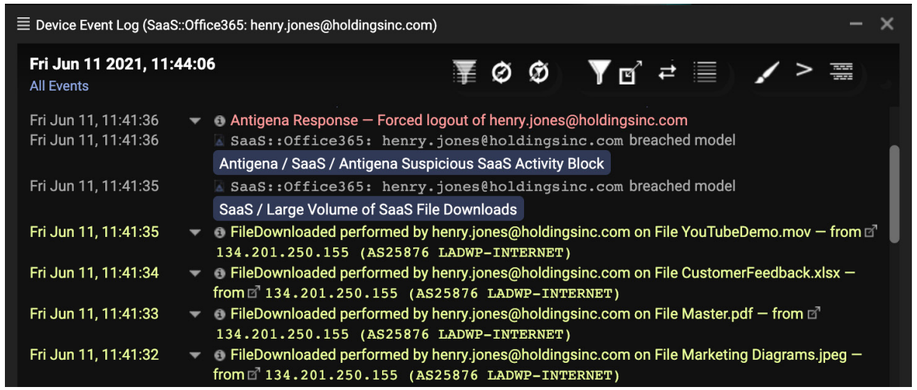


Abbildung 15: Darktrace Antigena schreitet ein und blockiert ungewöhnliche Dateidownloads

„Antigena, die Autonomous-Response-Lösung von Darktrace, ergreift Maßnahmen gegen laufende Cyberbedrohungen."

Jamie Snowdon, Principal Analyst, HFS Research

Bedrohungsvorfälle: IoT-Bedrohungen

Durch die zunehmende Vernetzung von alltäglichen Geräten gibt es in den Unternehmen immer mehr „blinde Flecken“. Während traditionellen Lösungen der Überblick fehlt und sie kaum in der Lage sind, neuartige Angriffe zu erkennen, schützt Darktrace mit seinem ganzheitlichen Ansatz das gesamte digitale Ökosystem.

Hacking einer Überwachungskamera

Bei einem japanischen Investmentberater stellte Darktrace fest, dass ein mit dem Internet verbundenes Videoüberwachungssystem von unbekannten Angreifern infiltriert worden war. Die Eindringlinge hatten das Gerät genutzt, um sich Zugang zum Netzwerk zu verschaffen, und konnten sich somit alle Videoaufzeichnungen der Kamera anschauen.

Die KI von Darktrace erkannte schnell, dass etwas nicht stimmte. Es wurde ein riesiges Datenvolumen zu und von dem unverschlüsselten Videoüberwachungsserver übertragen, da der Angreifer Daten sammelte, um die Ausschleusung sensibler Informationen vorzubereiten.

Als der Angreifer versuchte, die Daten auszuschleusen, ergriff Darktrace Antigena schnelle und präzise Abwehrmaßnahmen. Die KI unterband gezielt und präzise Datenbewegungen von dem Gerät zu einem externen Server und verhinderte damit einen fatalen Diebstahl markt-sensibler Informationen, aber ohne die Videoüberwachung an sich zu beeinträchtigen.

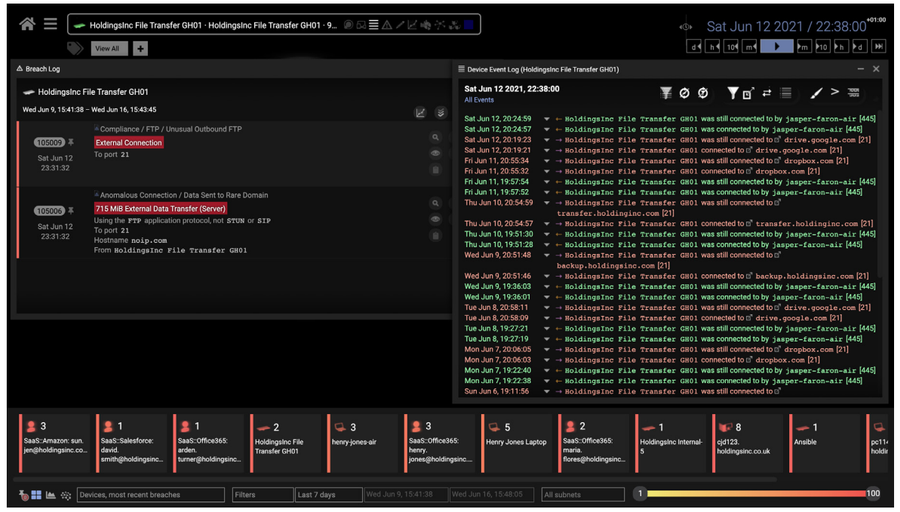


Abbildung 16: Ein Beispiel, wie Darktrace eine versuchte externe Datenübertragung erkennt und stoppt – und den Schutz sensibler Daten sicherstellt

Datenexfiltration über ein intelligentes Schließfach

In einem Vergnügungspark in Nordamerika versuchte ein Bedrohungsakteur, sensible Kundendaten über ein ungeschütztes IoT-Gerät zu entwenden: ein „smartes“ Schließfach für die persönlichen Gegenstände der Besucher.

Die KI von Darktrace erkannte den Angriff, kurz nachdem das Schließfach anfing, eine auffällig große Menge unverschlüsselter Daten an eine ungewöhnliche externe Website zu senden. Die Verbindungen waren an die üblichen Kommunikationszeiten mit der Plattform des Anbieters angepasst, was darauf hindeutete, dass es sich um einen „Low and Slow“-Angriff handelte, mit dem die regelbasierten Abwehrmechanismen umgangen werden sollten.

Binnen Sekunden nach Entstehung der Bedrohung wurde Darktrace Antigena aktiv und blockierte alle ausgehenden Verbindungen von dem kompromittierten Gerät. Dies verschaffte dem Sicherheitsteam Zeit, die Bedrohung abzustellen.

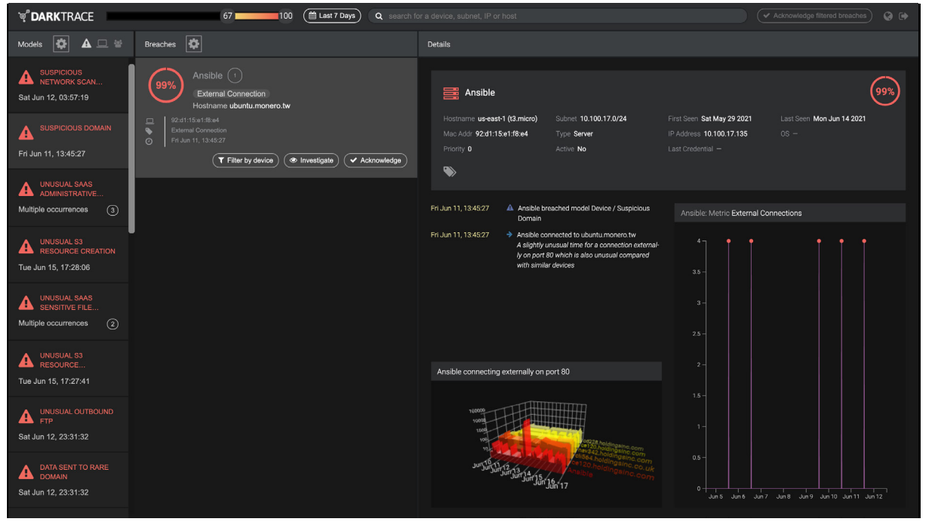


Abbildung 17: Ein Beispiel, wie Darktrace anormale externe Verbindungen erkennt und stoppt

> „Egal ob gezielte Kampagne oder versehentliche Kompromittierung – ich weiß, dass die Darktrace KI laufende Bedrohungen stoppt und unsere Unternehmens- und Industriesysteme schützt, bevor es zu spät ist.“
>
> IT Manager, Berry Gardens

Branchenauszeichnungen

TIME100 Most Influential Companies 2021 – als eines der 100 einflussreichsten Unternehmen genannt

Microsoft 20/20 Award Winner – Security Trailblazer

2021 SC Awards Europe
Winner – Best Security Company
Highly Commended – Best Email Security Solution (Antigena Email)

BIG Innovation Awards
Winner – Products
(Cyber AI Analyst)

CDM Global Infosec Awards 2021
Artificial Intelligence and Machine Learning (Best Product)

The Sales and Customer Service Awards (The Stevies®)
2021 – Bronze – Artificial Intelligence/ Machine Learning Solution (Antigena Email)

Cybersecurity Excellence Awards 2021: Gold – Best Cybersecurity Company, North America

2021 Globee Awards
Gold – Customer Service and Support Team of the Year
(Darktrace Customer Success)

Über Darktrace

Darktrace (DARK:L), ein weltweit führender Anbieter von KI für Cybersicherheit, liefert erstklassige Technologie, die mehr als 5.000 Kunden weltweit vor fortschrittlichen Bedrohungen schützt, darunter Ransomware sowie Cloud- und SaaS-Angriffe. Der grundlegend neuartige Ansatz des Unternehmens wendet selbstlernende KI an, um Maschinen zu helfen, das individuelle Unternehmen zu verstehen, um es selbstständig zu verteidigen. Das Unternehmen mit Hauptsitz in Cambridge, UK, hat 1.500 Mitarbeiter und über 30 Niederlassungen weltweit. Darktrace wurde vom TIME Magazine zu einem der „Most Influential Companies“ für 2021 ernannt.

Weitere Informationen

- Besuchen Sie uns auf darktrace.com/de
- Demo buchen
- Besuchen Sie unseren YouTube-Kanal
- Folgen Sie uns auf Xing
- Folgen Sie uns auf LinkedIn