DARKTRACE

Aufbau einer modernen Sicherheitsinfrastruktur

Warum Ihre NDR- und E-Mail-Sicherheitslösungen miteinander arbeiten müssen

Inhalt

Kurz-fassung

Obwohl viele Cyberangriffe in der Inbox starten, ist diese nur selten das Ziel. Angreifer lancieren zunehmend KI-gesteuerte, mehrstufige Angriffe, die mit E-Mails starten und sich schnell über Netzwerke und Cloud-Umgebungen ausbreiten. In einer solchen Situation haben Insellösungen Probleme, die Angriffe richtig einzuordnen, wodurch kritische Blindstellen entstehen, die die Abwehr verlangsamen. Die effektivste Verteidigung gegen moderne Bedrohungen ist ein einheitlicher KI-Ansatz, der E-Mail- und Netzwerksicherheit eng miteinander verbindet.

Dieses Whitepaper befasst sich mit den folgenden Themen:

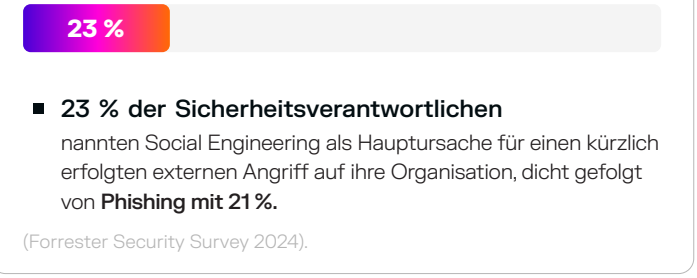
- **Wie KI mehrstufige, bereichsübergreifende Angriffe beschleunigt**
- **Warum isolierte E-Mail- und Netzwerklösungen nicht mehr mithalten können**
- **Wie ein einheitlicher, mehrschichtiger KI-Ansatz die Erkennung und Reaktion auf Bedrohungen verbessert**
- **Sicherheitsbezogene, betriebliche und wirtschaftliche Vorteile eines integrierten Ansatzes**

Warum einheitliche Sicherheit unerlässlich ist

KI-gestützte E-Mail-Angriffe werden immer raffinierter

E-Mails sind nach wie vor einer der beliebtesten und effektivsten ersten Angriffspunkte für Cyberkriminelle, und KI macht diese Bedrohungen immer überzeugender und schwerer zu erkennen. Angreifer nutzen generative KI, um hochgradig personalisierte Phishing-E-Mails in großem Umfang zu erstellen. Dabei setzen sie auch neue Techniken wie QR-Code-Phishing ein.

Laut Gartner ist E-Mail nach wie vor ein bedeutender Angriffsvektor für Malware und den Diebstahl von Anmeldedaten – mit dem Ziel, das Netzwerk zu kompromittieren.



- **23 % der Sicherheitsverantwortlichen** nannten Social Engineering als Hauptursache für einen kürzlich erfolgten externen Angriff auf ihre Organisation, dicht gefolgt von **Phishing mit 21 %.**

(Forrester Security Survey 2024).

...und das Gleiche gilt für Netzwerkbedrohungen

Sobald sie sich innerhalb einer Organisation befinden, können Angreifer KI einsetzen, um jede Phase des Angriffszyklus zu beschleunigen und zu automatisieren.

Dazu gehören:

- Ermittlung potenzieller Infrastruktur und kostenloser Hosting-Anbieter
- Schnellere Aufklärung von Zielorganisationen
- Adaptives Malware-Verhalten
- Groß angelegtes Sammeln von Anmeldedaten
- Entwicklung der Nutzlast
- Hilfe bei der Entwicklung von schädlichen Skripten und Umgehungstechniken

Diese Fortschritte ermöglichen es Angreifern, schneller, präziser und in viel größerem Umfang als zuvor zu agieren. Laut dem britischen National Cyber Security Centre (NCSC) wird KI bis zum Jahr 2027 höchstwahrscheinlich die Fähigkeit von Angreifern verbessern, Schwachstellen auszunutzen, wodurch sowohl staatliche als auch nicht staatliche Akteure leichter komplexe Angriffe starten können.

Bereits jetzt geben 74 % der Sicherheitsexperten an, dass KI-gesteuerte Angriffe eine große Herausforderung für ihre Organisationen darstellen. (State of AI Cybersecurity 2025)

Warum isolierte Lösungen nicht ausreichen

Als Reaktion auf eine komplexe Bedrohungslandschaft haben viele Organisationen eine Vielzahl von Best-of-Breed-Tools zusammengestellt: eines für E-Mail-Sicherheit, ein anderes für die Netzwerküberwachung, weitere für die Endpunkt- oder Cloud-Sicherheit. Aber diese isolierten Lösungen funktionieren nur selten in echter Symbiose.

In den meisten Fällen tauschen sie Daten über eine SIEM- oder SOAR-Plattform aus und generieren Warnmeldungen, denen jedoch der notwendige Kontext fehlt, um das gesamte Ausmaß eines Angriffs zu verstehen. Dieser fragmentierte Ansatz kann zu Blindstellen zwischen verschiedenen Phasen der Angriffskette führen, sodass Sicherheitsteams Ereignisse aus unverbundenen Dashboards und Protokollen manuell zusammenfügen müssen. Da Angreifer sich immer schneller und besser getarnt durch Umgebungen bewegen, können sich diese Verzögerungen bei der Erkennung und Untersuchung als katastrophal erweisen.

Selbst hohe Investitionen in EDR- und XDR-Lösungen hinterlassen oft Lücken, insbesondere im Bereich der Netzwerkaktivität, was zu einem falschen Vertrauen in die Transparenz des SOC führt. Agents können nicht überall in einem modernen Netzwerk installiert werden und herkömmliche Tools, die sich lediglich auf „bekannte bösartige“ Aktivitäten konzentrieren, erkennen keine unbekannten, neuartigen oder Insider-Bedrohungen.

Die Realität ist klar:

Nur eine wirklich integrierte Lösung, die E-Mail und Netzwerktelemetrie nahtlos miteinander verbindet, kann die Geschwindigkeit, Transparenz und Flexibilität bieten, die erforderlich sind, um die heutigen KI-gestützten Angriffe zu erkennen und darauf zu reagieren.

Im Inneren des Angriffs: Wie Bedrohungen von der Inbox in das interne System gelangen

Hier ein Beispiel für einen kürzlich von Darktrace beobachteten Angriff.

Der betreffende Kunde hatte Darktrace im reinen Erkennungsmodus konfiguriert, ohne dass eine Reaktion aktiviert war. Das bedeutete, dass sich die Sicherheitsverletzung weiter ausbreiten konnte, bis das Sicherheitsteam auf die von Darktrace ausgelösten Warnmeldungen reagierte.

Wäre die autonome Reaktion aktiviert gewesen, wären umgehend Maßnahmen ergriffen worden, um den Angriff einzudämmen. Dennoch gelang es Darktrace, Transparenz über verschiedene Bereiche der digitalen Infrastruktur des Kunden zu schaffen und den Angriff zu rekonstruieren, sodass der Kunde schnell Abhilfemaßnahmen ergreifen konnte. Das folgende Diagramm zeigt, wie sich der Angriff in dessen Umgebung entwickelt hat.

Diese Bedrohungslage verdeutlicht ein gängiges Muster moderner Angriffe:

Sie bewegen sich reibungslos durch die gesamte digitale Umgebung, von E-Mails über Netzwerke bis hin zu weiteren Bereichen. Wenn die Sicherheit abgeschottet ist, haben die Verteidiger nur einen fragmentierten Überblick, was die Erkennung verzögert, die Reaktion stört und letztendlich den Angreifern die Oberhand gibt.

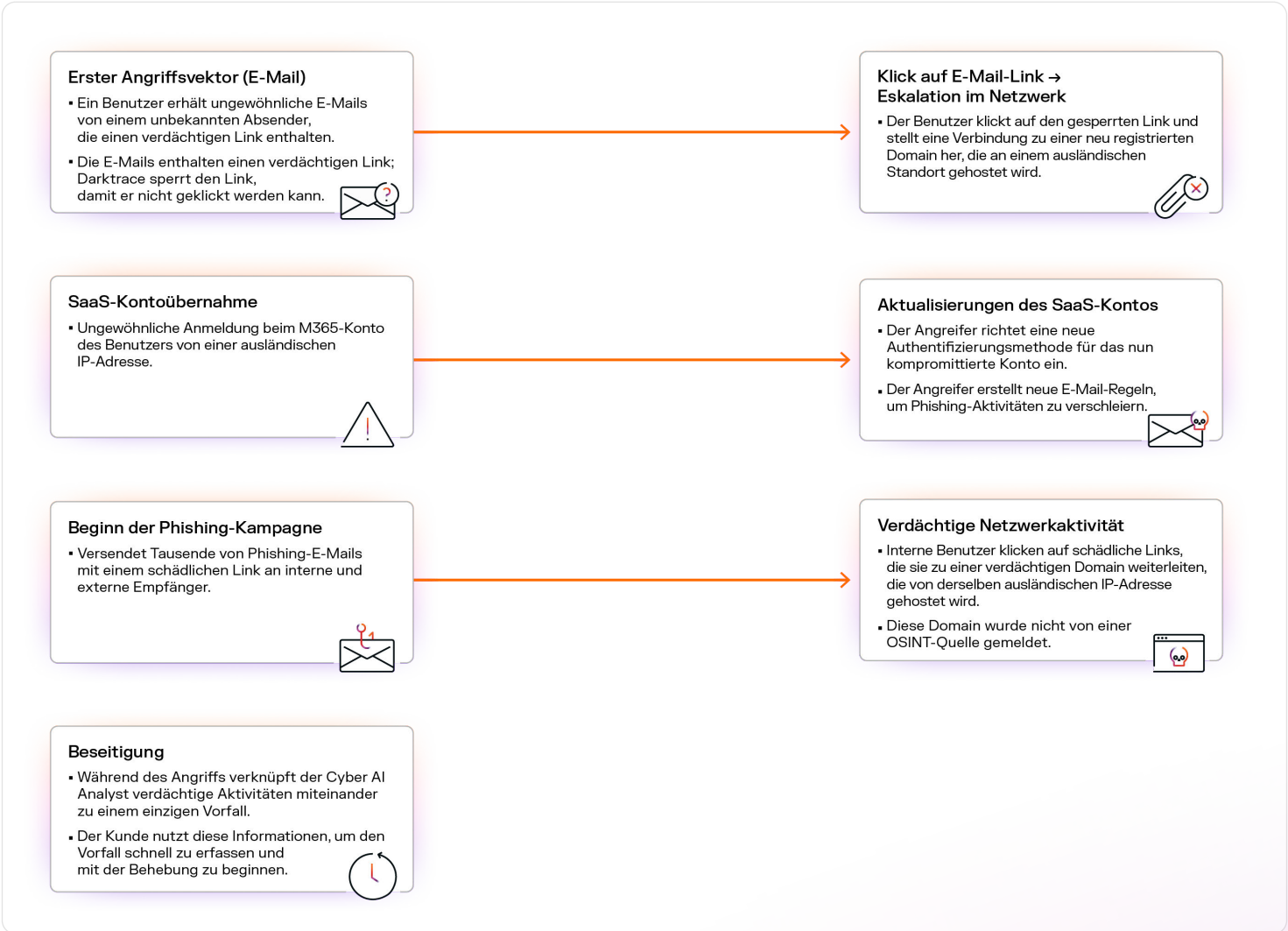


Abbildung 1: Diagramm, das einen Angriff vom E-Mail-Kanal über das Netzwerk bis hin zu SaaS darstellt

Darktrace / NETWORK + / EMAIL

Zwei erstklassige Lösungen, ein vielschichtiger KI-Ansatz

Individuell gesehen sind Darktrace / NETWORK und Darktrace / EMAIL leistungsstarke, branchenführende Lösungen.

/ NETWORK

Als führendes Unternehmen im Gartner® Magic Quadrant™ for NDR 2025 anerkannt, bringt Darktrace / NETWORK seine leistungsstarke, mehrschichtige KI in Ihr modernes Netzwerk und neutralisiert bekannte sowie unbekannte Bedrohungen in Echtzeit.

Gartner Peer Insights: ★★★★★ 4,7* (465 Bewertungen, Stand: August 2025)

99 %

Darktrace / NETWORK reduziert nachweislich die Anzahl falscher Alarme um **fast 99 % im Vergleich zu einem bestehenden traditionellen NDR-Anbieter.**

(Darktrace-Kunde aus dem Energiesektor)

08

Darktrace / NETWORK erkennt und begrenzt Zero-Day-Schwachstellen durchschnittlich **8 Tage vor ihrer öffentlichen Bekanntgabe**.

(Darktrace-Studie)

/ EMAIL

Ausgezeichnet als „Customers' Choice" in der Gartner® Peer Insights™ Voice of the Customer for Email Security 2025 bringt Darktrace / EMAIL branchenweit erste KI-Innovationen in das gesamte Messaging-Ökosystem, um neuartige und gezielte Angriffe zu stoppen.

Gartner Peer Insights: ★★★★★ 4,8* (323 Bewertungen, Stand: August 2025)

55 %

55 % der Bedrohungen, die von Darktrace / EMAIL erkannt wurden, haben alle vorherigen Sicherheitsebenen durchdrungen

(Jährlicher Bedrohungsbericht 2024)

13

Darktrace / EMAIL erkennt Bedrohungen **13 Tage früher als andere Lösungen**

(Darktrace-Studie)

Ein einzigartiger KI-Ansatz im Mittelpunkt

Was macht die Netzwerk- und E-Mail-Produkte von Darktrace **so leistungsstark**?

Die KI, die ihnen zugrunde liegt.

Die meisten Anbieter von Cybersicherheitslösungen verlassen sich nach wie vor auf veraltete Erkennungsmethoden, die auf Regeln und Signaturen basieren. Selbst wenn KI eingesetzt wird, beschränkt sich dies in der Regel auf überwachte Modelle, die anhand von gekennzeichneten Angriffsdaten und Bedrohungsinformationen trainiert wurden. Diese Modelle sind zwar bei der Identifizierung bekannter Bedrohungen effektiv, müssen jedoch ständig neu trainiert werden und haben nach wie vor Probleme mit neuartigen oder KI-gesteuerten Angriffen, die nicht den bisherigen Mustern entsprechen. Dies führt zu nicht überprüfbaren Anomalien und einer Flut von Warnmeldungen mit geringer Zuverlässigkeit, die die Sicherheitsteams überfordern, zu Warnmüdigkeit beitragen und zu schwerfälligen oder ungenauen Reaktionen führen.

Die selbstlernende KI von Darktrace bietet einen grundlegend anderen Ansatz für Cybersicherheit, indem sie die einzigartige digitale Umgebung jeder Organisation **kontinuierlich erlernt**. Mithilfe eines mehrschichtigen KI-Ansatzes integriert sie strategisch eine Reihe von KI-Techniken – darunter unüberwachtes maschinelles Lernen, LLMs, GNNs und NLP – sowohl sequenziell als auch hierarchisch.

Dadurch kann sie sich **an neue Bedrohungen anpassen** und ein dynamisches Verständnis des normalen Verhaltens von Benutzern, Geräten und Systemen aufbauen. Durch die Kombination dieser KI-Modelle kann unsere selbstlernende KI tatsächlich schädliche Aktivitäten von unbekannten, aber harmlosen Ereignissen unterscheiden – ohne sich auf Signaturen, Regeln oder manuelle Anpassungen zu stützen.

Unsere selbstlernende KI bildet die Grundlage der ActiveAI-Sicherheitsplattform von Darktrace, die Telemetriedaten bereichsübergreifend korreliert und so eine vollständige End-to-End-Abdeckung einschließlich E-Mail und Netzwerk gewährleistet. **Dadurch kann Darktrace Einblicke aus verschiedenen Umgebungen miteinander verknüpfen und so eine einheitliche Risikobetrachtung erstellen.**

Verhaltenssignale aus einem Bereich – wie beispielsweise eine verdächtige Anmeldung im Netzwerk – können sofort in die Entscheidungsfindung im E-Mail-Bereich einfließen und umgekehrt. Diese enge Integration ermöglicht eine schnellere Erkennung von Bedrohungen, erweiterte und kontextbezogene Warnmeldungen sowie intelligentere autonome Maßnahmen, ohne dass menschliches Eingreifen oder komplexe regelbasierte Integrationen erforderlich sind.

Mit einer ganzheitlichen, KI-gestützten Verteidigung für Netzwerk und E-Mail profitieren Sie von einem einheitlichen Schutz, der mehr ist als die Summe seiner Teile. Er bietet nahtlosen, adaptiven Schutz, der reale Angriffe widerspiegelt und so den Verteidigern einen konsistenten, einheitlichen Vorteil verschafft.

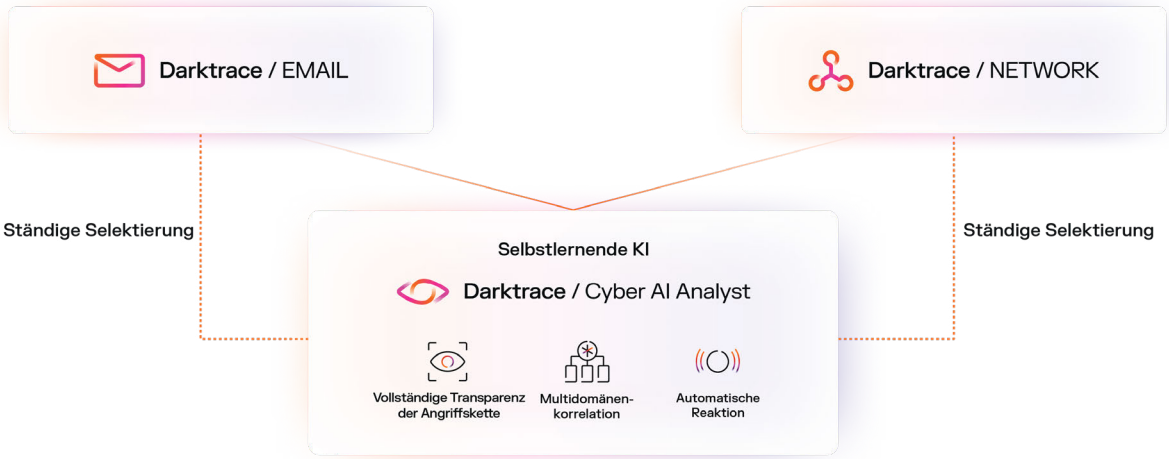


Abbildung 2: Gemeinsam verbinden Darktrace / NETWORK und / EMAIL proaktive Resilienz mit einheitlicher Transparenz sowie Erkennung von Bedrohungen nd unterstützen Sie so beim Übergang zu einem KI-gesteuerten SOC.

Ihr Begleiter bei der Recherche: Cyber AI Analyst

Wenn selbstlernende KI eine bereichs-übergreifende Erkennung und Reaktion auf Bedrohungen ermöglicht, ist der Cyber AI Analyst der **unermüdliche digitale Detektiv** Ihres SOC.

Dabei handelt es sich um ein Agent-basiertes KI-System, das alle relevanten Sicherheitswarnungen – sowohl von Darktrace als auch von Sicherheitstools von Drittanbietern (Firewalls, EDR, SIEMs) – autonom untersucht. Nicht nur ein Chatbot mit generativer KI. Cyber AI Analyst nutzt mehrere Arten von KI, um den menschlichen Untersuchungsprozess nachzubilden, darunter maschinelles Lernen, Modelle, die auf dem Verhalten von erfahrenen Analysten trainiert wurden, sicherheitsspezifische benutzerdefinierte LLMs und NLP.

Es führt Untersuchungen und Analysen durch, die den SOC-Stufen 1 und 2 entsprechen:

- Hypothesen bilden und verfeinern
- Abfragen und Korrelieren von Informationen
- Verfolgung komplexer Angriffe über mehrere Bereiche hinweg
- Kritische Vorfälle zur Überprüfung durch das Personal aufzeigen
- Vorschläge für Gegenmaßnahmen auf der Grundlage einer Analyse der Lebensmuster

In der Regel kommt es innerhalb weniger Minuten zu einem Ergebnis und präsentiert eine übersichtliche, interaktive Zusammenfassung des Vorfalls – komplett mit verknüpften Warnmeldungen, Kontextanalysen und grafischen interaktiven Visualisierungen –, sodass selbst die komplexesten Angriffe leicht zu untersuchen und zu verstehen sind.

Durch die Bearbeitung von Untersuchungen und die Selektierung nach einem SOC-Standard der Stufe 2 entlastet Cyber AI Analyst menschliche Analysten, sodass diese sich auf die proaktive Suche nach Bedrohungen und eingehendere Untersuchungen konzentrieren können.

10-fache Beschleunigung bei Ermittlungen mit Cyber AI Analyst

Sparen Sie jährlich bis zu 50.000 Analystenstunden ein.

Das entspricht der Einstellung von bis zu 30 Vollzeit-SOC-Analysten.

■ Fallstudie

In einem Monat hat Cyber AI Analyst einem Kunden **1.104 Stunden manueller Ermittlungsarbeit** eingespart, indem es die Selektierung und Untersuchung von 23 Millionen Warnmeldungen automatisierte.

(Kundenfallstudie, Aviso)

Vorteile eines einheitlichen Ansatzes

Die Zusammenführung von Netzwerk- und E-Mail-Sicherheit bietet jeder Organisation eine Reihe quantitativer und qualitativer Vorteile, die sich grob in technische, betriebliche und wirtschaftliche Vorteile unterteilen lassen. **Werfen wir einen Blick darauf.**

Technischer Vorteil

Auf technischer Ebene lassen sich die Vorteile in Vorwarninformationen und alarmbezogene Informationen unterteilen.

Vorab-Warninformationen: Daten sammeln, bevor die Bedrohung zuschlägt

Viele Sicherheitstools beginnen mit der Analyse erst, wenn eindeutige Anzeichen für eine Kompromittierung vorliegen. Im Gegensatz zu anderen Tools erfasst und analysiert unsere KI kontinuierlich Daten sowohl aus E-Mails als auch aus dem Netzwerk – auch wenn keine Warnmeldungen vorliegen. Diese fortlaufende Analyse liefert ein detailliertes Bild des Verhaltens jedes Benutzers, jedes Geräts und jedes Bereichs, die innerhalb der Organisation interagieren.

Das bedeutet, dass Darktrace bereits über Kontextinformationen zur Domain des Absenders verfügt, wenn eine E-Mail in der Inbox eines Benutzers landet, und zwar basierend auf seiner Netzwerksichtbarkeit. Wenn eine verdächtige Domain in einer E-Mail auftaucht, wird diese Information sofort genutzt, um zukünftige Netzwerkaktivitäten zu interpretieren. Dieses gemeinsame Verständnis erstreckt sich über das gesamte Darktrace-Ökosystem – unabhängig davon, ob die Informationen aus E-Mails, Netzwerken, Endpunkten oder externen Quellen wie Feeds mit Bedrohungsinformationen stammen. Sie müssen nur einmal erhoben werden. Von dort aus verbessert es die Erkennung und Reaktion über alle Produkte hinweg und gewährleistet konsistente, kontextbezogene Entscheidungen.

Das Ergebnis ist ein dynamischer Prozess zur Erfassung und Weitergabe von Informationen, der Wissen innerhalb des Tools aufbaut – nicht über Bedrohungen, sondern über Verhaltensgrundwerte in Echtzeit, wodurch Darktrace Bedrohungen melden kann, ohne dass es zu einem Kompromiss kommen muss.

Alarmbezogene Informationen: In Echtzeit die Zusammenhänge erkennen

Wenn ein Sicherheitsalarm ausgelöst wird, beginnt Cyber AI Analyst sofort mit der Untersuchung, indem es Hypothesen aufstellt und Echtzeit- sowie historische Daten bereichsübergreifend analysiert. Es verbindet selbstständig zusammenhängende Verhaltensweisen, beispielsweise indem es eine verdächtige E-Mail mit ungewöhnlichen Netzwerkaktivitäten auf dem Gerät des Empfängers verknüpft. So erstellt es einen einzigen umfassenden Vorfall, den das SOC überprüfen kann.

Dieser Prozess läuft in wenigen Minuten und in großem Umfang ab, wodurch die Anzahl der Warnmeldungen und die manuelle Selektierung drastisch reduziert werden.

Darüber hinaus stellt diese automatische Korrelation sicher, dass Angriffsketten intakt bleiben, und bietet so kontinuierliche Transparenz vom ersten Angriff bis hin zu lateralen Bewegungen oder Datenexfiltration. Diese allgemeine Sichtbarkeit ermöglicht eine gezielte Reaktion, die dem Ausmaß und Umfang des Angriffs entspricht.

Im Gegensatz zu Punktlösungen oder SIEM-Workflows, bei denen Analysten häufig fragmentierte Warnmeldungen ohne vollständigen Kontext manuell zusammenfügen müssen, bietet Darktrace einheitliche Informationen nach der Warnmeldung, unabhängig davon, wo die Bedrohung zuerst aufgetreten ist.

Unser Ansatz beschleunigt nicht nur die Untersuchungen und verbessert die Zuverlässigkeit von Reaktionsentscheidungen, sondern unterstützt auch einen Kerngedanken der Sicherheitsphilosophie von Darktrace: Verteidiger sollten den Angreifer nach seinem ersten Eindringen niemals aus den Augen verlieren.

Auch wenn E-Mails generell zum Einstieg dienen,

der nächste Schritt der Angreifer ist in der Regel die Netzwerkinfrastruktur oder Cloud-Konten, sodass eine kontinuierliche, umgebungsübergreifende Korrelation zwischen E-Mail und Netzwerk unerlässlich ist.

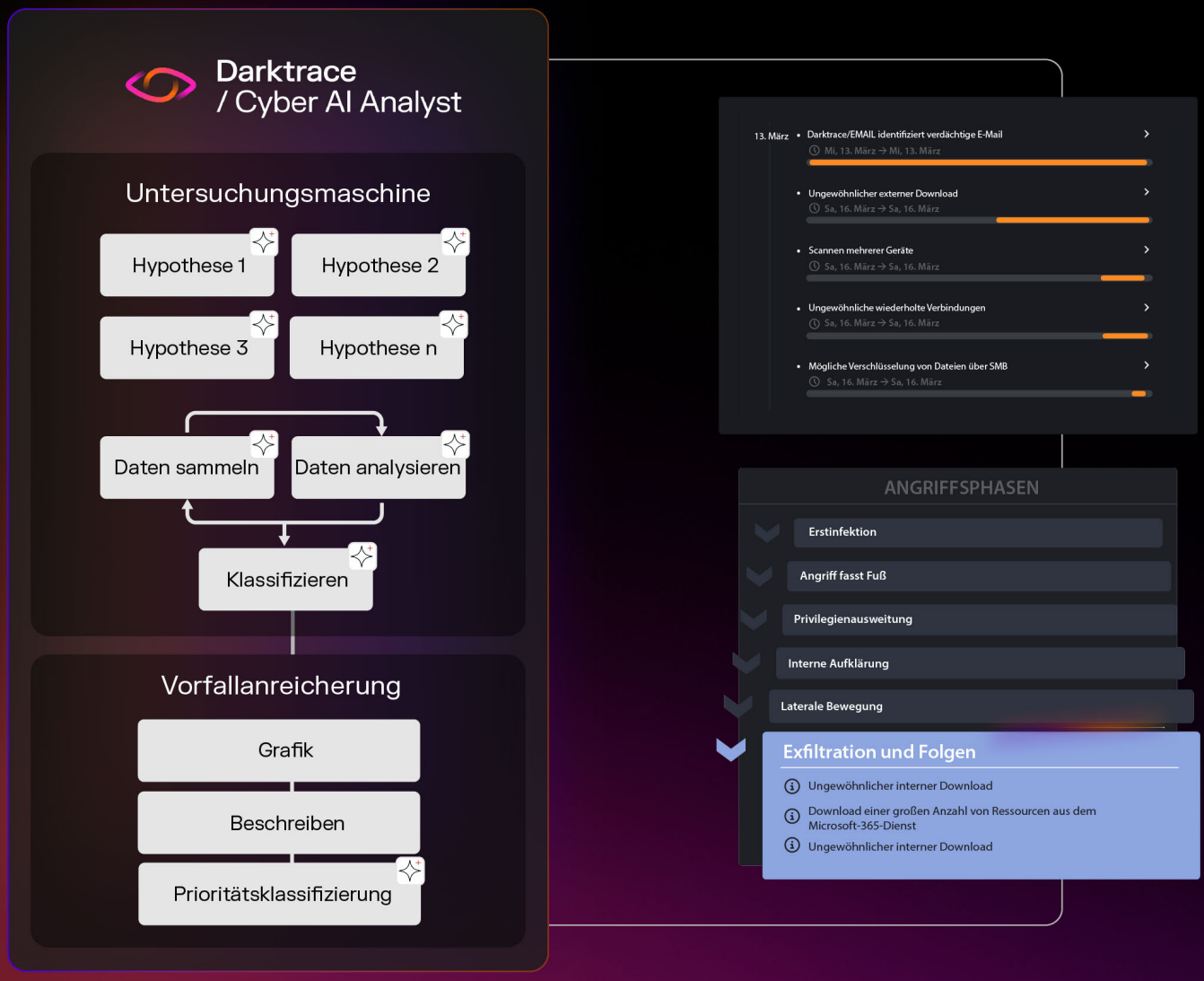


Abbildung 3: Phasen eines Angriffs, ausgehend von einer E-Mail, der sich auf das Netzwerk ausbreitet, wobei die verschiedenen Phasen der Angriffskette mit Cyber AI Analyst korreliert werden.

„Die Fähigkeit von Darktrace, große Datenmengen effektiv zu filtern, eliminiert Störsignale, sodass sich das Team auf echte Risiken konzentrieren kann, ohne von irrelevanten Informationen überwältigt zu werden."

■ **CISO, Kommunalverwaltung**

Operativer Vorteil

Optimierung der Sicherheitsoperationen über Teams hinweg

In vielen Organisationen werden E-Mail-Sicherheit und Incident Response noch immer von verschiedenen Teams vorgenommen. E-Mails fallen oft in den Bereich des IT-Betriebs, während Netzwerkverteidigung und Incident Response im SOC untergebracht sind. Diese Trennung führt zu operativen Konflikten, insbesondere da E-Mails nach wie vor der häufigste Einstiegspunkt für Cyberangriffe sind.

Durch den gemeinsamen Einsatz von Netzwerk- und E-Mail-Sicherheit – innerhalb einer einzigen Plattform und eines einzigen Bedrohungsvisualisierers – sind wichtige E-Mail-Informationen nicht auf eine separate Konsole oder ein separates Team beschränkt, sondern direkt innerhalb der Kern-Workflows des SOC zugänglich.

Diese gemeinsame Sichtbarkeit verschafft dem Incident-Response-Team einen besseren Einblick in E-Mail-Angriffsvektoren, ohne dass die Anfrage eskaliert oder ausgelagert werden muss. Dies ebnet den Weg für eine bessere Zusammenarbeit zwischen verschiedenen Bereichen des Sicherheitsteams.

Verkürzung der „Time to Meaning“ und schnellere Reaktion

Da Netzwerk- und E-Mail-Daten auf einer einzigen Plattform vereint sind, müssen Sicherheitsteams nicht mehr zwischen verschiedenen Tools hin- und herspringen, um unterschiedliche Warnmeldungen miteinander in Zusammenhang zu bringen. Die gemeinsame Philosophie, die sowohl für das Netzwerk als auch für E-Mails gilt, sorgt nicht nur für eine manuelle Optimierung, sondern reduziert auch die Zeit, die Benutzer benötigen, um Informationen zu verstehen.

Ebenso ermöglicht die integrierte Bedrohungskorrelation zwischen E-Mail und Netzwerk über den Cyber AI Analyst eine schnellere Selektierung und sicherere, koordinierte Reaktionen über alle Umgebungen hinweg. Im Gegensatz zu herkömmlichen Workflows, die auf SIEM-Korrelation oder SOAR-Playbooks basieren, verbindet Darktrace die Punkte in Echtzeit und automatisiert intelligente Reaktionsmaßnahmen.

Wirtschaftlicher Wert

Die gemeinsame Bereitstellung von Netzwerk- und E-Mail-Sicherheit ist nicht nur ein technischer und betrieblicher Gewinn, sondern hat auch wirtschaftliche Vorteile.

Mit einem einzigen Anbieter profitieren Organisationen von einer einzigen Geschäftsbeziehung, wodurch alles von der Beschaffung über die Verhandlungen bis hin zum laufenden Support vereinfacht wird. Anstatt mehrere Verträge zu verwalten, erhalten Kunden ein einheitliches Account-Team und einen optimierten Geschäftsprozess. Der Prozess der Einbindung zusätzlicher Managed Services oder Professional Services für beide Produkte wird ebenfalls vereinfacht, sodass Sie von einheitlichem Fachwissen für die gesamte Sicherheitsumgebung profitieren.

Besonders wichtig ist, dass die Investition in eine einzige KI-gestützte Plattform eine solide Grundlage für die zukünftige Expansion darstellt.

Da E-Mail und Netzwerk unter einem Dach vereint sind, müssen Sie Ihre Architektur nicht neu überdenken, wenn Sie in Zukunft neue Funktionen hinzufügen möchten – beispielsweise Identitäts- oder Cloud-Abdeckung –, denn die Plattform ist so konzipiert, dass sie mit Ihrem Unternehmen mitwächst.

Einzellösungen mögen auf den ersten Blick flexibel erscheinen, führen jedoch häufig zu einer fragmentierten Abdeckung, doppelten Ausgaben und Integrationsproblemen. Für Organisationen, die ein modernes, KI-fähiges SOC aufbauen möchten, ist der Kauf einer Best-of-Suite-Lösung nicht nur einfacher, sondern auch strategischer als der Kauf einer Best-of-Breed-Lösung. **Mit Darktrace müssen Sie bei der Umstellung auf einen Plattformansatz keine Qualitätseinbußen hinnehmen – jeder einzelne Kauf stärkt die Kernplattform, verbessert die gemeinsame Intelligenz und liefert im Verlauf der Zeit einen Mehrwert.**

Darktrace hat Integrität, Geduld und echtes Interesse daran gezeigt, eine starke Beziehung zu meinem Team aufzubauen. Deshalb sind wir heute hier.

- **CISO, Global Technology Provider**

Kaufszenarien

Sehen wir uns zwei Kaufszenarien an: eines für eine Organisation, die eine Einzellösungsstrategie umsetzt, und eines für eine Organisation, die einen konsolidierten Sicherheitsstack anstrebt.

Szenario 1: Punktuelle Lösungen

Ersteinrichtung

Eine Organisation wählt ein separates E-Mail-Sicherheitstool aus – möglicherweise vom IT- oder Messaging-Team gewählt – und implementiert später über das Sicherheitsteam ein separates Produkt zur Netzwerkerkennung und -reaktion (NDR). Oder die Organisation hat überhaupt kein NDR-Tool und verwendet stattdessen ein EDR- oder XDR-Tool. Um Informationen miteinander zu verknüpfen, stützt sie sich auf eine bestehende SIEM- oder SOAR-Plattform, um Daten zu korrelieren und Reaktionsabläufe zu koordinieren.

Betriebsphase

Diese Vorgehensweise bietet zwar Flexibilität und nutzt vorhandene Werkzeuge, ist aber auch sehr komplex. Das SOC muss mehrere Dashboard- und Warnsysteme verwalten. Die Ermittlungsprozesse können langsamer sein, da Analysten Ereignisse manuell über verschiedene Tools hinweg miteinander verknüpfen müssen, die jeweils über ein eigenes Datenmodell und eine eigene Erkennungslogik verfügen.

Skalierung

Die Ausweitung der Erfassung auf Cloud-, Identitäts- oder Anwendungsebenen erfordert die Beschaffung zusätzlicher Einzelprodukte, deren Integration in das SIEM und die entsprechende Anpassung von Richtlinien oder Playbooks.

Im Laufe der Zeit wächst die Belastung für die Ingenieure und den Betrieb – mit doppelter Arbeit für verschiedene Tools, fragmentierter Sichtbarkeit und uneinheitlicher Koordinierung der Maßnahmen.

Szenario 2: Plattform-Sicherheit

Ersteinrichtung

Eine Organisation nutzt E-Mail- und Netzwerkerkennungsfunktionen desselben Anbieters, die über eine gemeinsame KI-gestützte Plattform und eine einzige Bedienoberfläche bereitgestellt werden. Beide Schnittstellen fließen in dasselbe Verhaltensmodell ein, wobei die Erkenntnisse nahtlos in der gesamten Umgebung geteilt werden und die Transparenz durchgängig vorhanden ist.

Betriebsphase

Sicherheitsteams profitieren von vorintegrierten Workflows, konsistenten Warnmeldungen und der nativen Korrelation von Vorfällen. Wenn ein E-Mail-Anhang zu verdächtigen internen Aktivitäten führt, werden beide in einer einheitlichen Ansicht angezeigt – dadurch wird die Untersuchungszeit verkürzt und Lücken zwischen Tools oder Teams müssen nicht mehr manuell überbrückt werden. Optionale Dienste wie MDR können ohne Doppelungen auf beiden Oberflächen ausgeführt werden.

Skalierung

Da sich die Bedrohungslandschaft weiterentwickelt, kann die Erweiterung auf andere Bereiche – wie Cloud-Konten, Benutzeridentitäten oder Endpunkte – schrittweise erfolgen, ohne dass die Architektur neu gestaltet werden muss. Zusätzliche Funktionen werden in dasselbe Modell integriert, wodurch der Kontext erhalten bleibt und ein einheitlicher Schutz für die gesamte digitale Infrastruktur ermöglicht wird.

Den nächsten Schritt machen

Da Angreifer zunehmend KI einsetzen, um zu recherchieren, zu automatisieren und zu beschleunigen, können es sich Verteidiger nicht leisten, sich auf oberflächlich integrierte Tools oder manuelle Prozesse zu verlassen. Bei der Vereinheitlichung der Netzwerk- und E-Mail-Sicherheit geht es nicht nur um Effizienz, sondern auch um die Schaffung eines Sicherheitsökosystems, das mehr ist als die Summe seiner Teile.

Wir haben die Darktrace ActiveAI Security Platform entwickelt, um proaktive, korrelierte Sicherheit zu bieten, die wie ein Angreifer denkt – und Ihnen die Transparenz und Agilität zu geben, sich gegen gezielte, bereichsübergreifende Bedrohungen zu verteidigen, die isolierte Erkennungsmaßnahmen umgehen.

Bereit für den nächsten Schritt?

Fordern Sie eine maßgeschneiderte Demoversion an, um den integrierten Schutz in Aktion zu sehen.

Demo anfordern ↗

Erfahren Sie, wie dieser Kunde mit Darktrace die MTTC um 80 % reduziert hat

Fallstudie ↗

Berechnen Sie Ihren ROI mit Darktrace / EMAIL

Erhalten Sie Ihren ROI ↗

Über Darktrace

Darktrace ist ein weltweit führendes Unternehmen für KI-Cybersicherheit, das Organisationen vor täglich neuen Bedrohungen schützt. Das Unternehmen wurde 2013 in Cambridge, Großbritannien, gegründet und bietet eine wichtige Cybersicherheitsplattform, die Organisationen mit Hilfe von KI in Echtzeit vor noch unbekannten Gefahren beschützt. Die Plattform und Dienstleistungen von Darktrace mit seinen über 2.700 Mitarbeitern werden von knapp 10.000 Kunden weltweit benutzt. Weitere Informationen finden Sie unter www.darktrace.com.

Nordamerika: +1 (415) 229 9100 Europa: +44 (0) 1223 394 100 Asien-Pazifik-Raum: +65 6804 5010 Lateinamerika: +55 11 4949 7696

darktrace.com | info@darktrace.com