04.12.2025 – 14:23 Uhr

Darktrace erweitert Darktrace / EMAIL(TM): neue Funktionen für domänenübergreifende Erkennung, Outbound-Schutz und SOC-Integrationen

München (ots) -

- *Rund 17 Prozent der E-Mail-Bedrohungen umgehen Secure E-Mail Gateways - Darktrace-KI stoppt sie*
- *Neue Funktionen gegen kanalübergreifende Angriffe (u. a. E-Mail-Bombing, 100x mehr Nachrichten) und zur Absicherung der Kommunikation bei stark steigendem Black Friday Phishing (+1.317 Prozent)*
- *Gartner® Magic Quadrant(TM) 2025: Darktrace / EMAIL(TM) als Leader bei E-Mail Security Platforms (ESP) ausgezeichnet*

Social-Engineering-Angriffe beschränken sich heute nicht mehr ausschließlich auf E-Mails: Sie kombinieren Posteingang, Identitätsmissbrauch sowie SaaS- und Collaboration-Tools. Darktrace, ein globaler Anbieter von KI für Cybersicherheit, hat deshalb heute eine Reihe von Erweiterungen für Darktrace / EMAIL(TM) angekündigt. Ziel ist es, kanalübergreifende Angriffsmuster früher zu erkennen, ausgehende Kommunikation besser abzusichern und Schnittstellen in SOC-Prozessen zu vereinfachen.

Darktrace stützt sich dabei auf Erkenntnisse aus realen Kundenumgebungen: Trotz mehrschichtiger E-Mail-Sicherheitsmaßnahmen gelangen weiterhin relevante Mengen schädlicher Nachrichten durch. In realen Deployments identifizierte Darktrace / EMAIL(TM) unmittelbar rund 17 Prozent der Bedrohungen, die Secure E-Mail Gateways umgingen - darunter Social-Engineering-Nachrichten ohne offensichtliche Malware-Payload, etwa Impersonation, gefälschte Zahlungs- oder Änderungsanfragen im Lieferantenkontext.

Verbesserter Schutz vor kanalübergreifenden Angriffen

Kampagnen wie E-Mail-Bombing setzen auf Masse, um Posteingänge mit unkritischen Nachrichten zu überfluten. Deshalb erfolgt die eigentliche Kontaktaufnahme häufig über weitere Kanäle (z. B. Microsoft Teams oder Telefon) - etwa unter dem Vorwand von IT-Support. Zwischen April und Juli 2025 stieg das beobachtete Volumen solcher Nachrichten um das 100-Fache (von 200.000 auf mehr als 20 Millionen E-Mails laut Darktrace-Kundenbasis).

Hierfür gibt es eine neue Integration zwischen Darktrace / EMAIL(TM) und Darktrace / IDENTITY(TM): Erkennt Darktrace / EMAIL(TM) Muster, die zu E-Mail-Bombing passen, kann dieses Signal an Darktrace / IDENTITY(TM) weitergegeben werden. Dadurch lassen sich auffällige Login- oder Übernahmeversuche im Umfeld des betroffenen Accounts früher erkennen. Die domänenübergreifende Korrelation lässt sich zudem auf Business-Anwendungen wie Salesforce ausweiten, etwa indem aus E-Mails heraus erzeugte Tickets in die Bewertung einbezogen werden.

Ergänzend reichert Darktrace Alarme durch Threat-Intelligence-Kontext an, u. a. über integrierte Antivirus-Verdikte und strukturierte Feeds, um die Erstbewertung (Triage) zu beschleunigen.

Absicherung ausgehender Kommunikation und Daten

Darktrace beobachtete im November einen Anstieg von Black-Friday-bezogenem Phishing um 1.317 Prozent gegenüber dem Vormonat. Das unterstreicht, dass neben dem Blockieren eingehender Angriffe auch die Authentizität ausgehender Kommunikation relevanter wird.

Dafür unterstützt Darktrace / EMAIL(TM)-DMARC nun BIMI (Brand Indicators for Message Identification), um verifizierte Markenlogos im Posteingang anzeigen zu können. Gleichzeitig adressiert Darktrace Outbound-Risiken durch Fehlversand: Eine label-freie, verhaltensbasierte DLP - gestützt durch ein domänenspezifisches Sprachmodell - kann über 35 zusätzliche Kategorien von PII/PHI in E-Mails und Anhängen automatisch erkennen und bei ungewöhnlichem Outbound-Verhalten intervenieren.

Neue Integrationen für SOC-Workflows

Zur Einbindung in bestehende Prozesse ergänzt Darktrace / EMAIL(TM) neue Integrationen:

- **Jira und ServiceNow:** automatische Ticket-Erstellung zur Dokumentation und Nachverfolgung von Meldungen

- **Sandbox-Analyse:** Analyse von Payload-Verhalten in isolierten Umgebungen direkt in der Darktrace-Oberfläche

Bestehende Integrationen werden ergänzt, darunter die Integration mit Microsoft Defender for Office 365 (u. a. für Quarantäne-Management) sowie der Darktrace E-Mail Analysis Agent für Microsoft Security Copilot, der Darktrace / EMAIL(TM)-Erkenntnisse in Copilot-Untersuchungen verfügbar macht.

"E-Mail ist häufig der Einstiegspunkt - die Eskalation verläuft dann über Identitäten und weitere Tools. Mit den Erweiterungen verknüpfen wir Signale über E-Mail, Identity und SaaS hinweg und stärken zugleich Schutzmaßnahmen für ausgehende Kommunikation", sagt ***Connie Stride, SVP of Product, Darktrace****.*

Darktrace / EMAIL(TM) wurde außerdem als Leader im Gartner® Magic Quadrant(TM) 2025 für Email Security Platforms (ESP) ausgezeichnet und erhielt den Gartner® Peer Insights(TM) Customers' Choice 2025 für ESP.

Weitere Ressourcen

- Schalten Sie am 9. Dezember zum Innovation-Launch von Darktrace ein, um mehr über unsere neuesten Innovationen zu erfahren.
- Mehr zu Darktrace / EMAIL(TM) finden Sie auf der Produktseite.
- Laden Sie hier eine Kopie des Gartner® Magic Quadrant(TM) 2025 für Email Security Platforms Reports herunter.
- Erfahren Sie mehr aus Darktrace' Black-Friday-Phishing-Analyse und entdecken Sie hier Top-Tipps, um sicher zu bleiben.

Über Darktrace

Darktrace ist ein weltweit führendes Unternehmen im Bereich KI-gestützter Cybersicherheit. Gegründet 2013, schützt die firmeneigene KI-Plattform Unternehmen vor unbekannten Bedrohungen - in Echtzeit und über alle digitalen Bereiche hinweg: Netzwerk, Cloud, E-Mail, Endpunkte und mehr. Die Darktrace ActiveAI Security Platform(TM) ermöglicht proaktive Cyber-Resilienz, Frühwarnungen und autonome Reaktionen. Innovationen aus den Darktrace-Forschungsteams in Cambridge (UK) und Den Haag (NL) führten zu über 200 Patentanmeldungen. Mit mehr als 2.300 Mitarbeitenden schützt Darktrace fast 10.000 Kunden weltweit. Mehr Informationen unter:www.darktrace.com

Pressekontakt:

PIABO Communications
Lukas Pfeiffer
darktrace@piabo.net