DATASHEET

6 ungewöhnliche Datenverhalten, die auf Insider-Bedrohungen hinweisen

Die meisten Datenschutzverletzungen entstehen intern – durch Fehler oder gezielten Datendiebstahl.

Strategien gegen Insider-Bedrohungen müssen risikoreiches Verhalten schnell und effektiv erkennen, um Ihre sensibelsten Daten zu schützen.

Hier sind sechs Beispiele für Anomalien, die Ihre Insider-Bedrohungslösung erkennen sollte:

Downloads auf nicht verwaltete Geräte

Loki arbeitet remote – **wer merkt da Downloads von Salesforce-Berichten auf ein privates Gerät?**

Cloud-Doppelgänger

Marketing nutzt die Google-Firmenlizenz für E-Mails und Dateifreigaben. **Was hat es mit diesem großen Upload auf das persönliche Google-Drive-Konto auf sich?**

Dateityp-Mismatch

Thanos hat eine Datei in „Cute Cat Pix“ umbenannt und ihr die Endung .jpeg gegeben. Das Problem: Der Inhalt ist **Quellcode,** kein Bild.

Berechtigungswarnung

Ultron hat die Berechtigung für ein Google-Dokument auf „Jeder kann bearbeiten“ geändert. Und weißt du was? Es ist dein "geheimer Produktfahrplan". **Zeit, bei Ultron nachzufragen.**

Clevere Mitarbeiter planen ihren Ausstieg

Hela hat gerade gekündigt. Jeder kann beobachten, ob Hela in den nächsten zwei Wochen große Dateien herunterlädt.

Kannst du aber sehen, was in den letzten **90 Tagen verschoben wurde?**

Erkennst du schon Muster?

Manchmal ist es eine Reihe von Aktionen.

Wie damals, als Hydra 50 Dateien mit Kundenlisten verschlüsselte und an eine unbekannte E-Mail schickte.

Ungewöhnlich, oder?

Denke daran:

- Riskante Datenaktivitäten erfordern den richtigen Kontext, um sicher reagieren zu können
- Eine vollständige Übersicht aller Aktivitäten mit dem nötigen Kontext hilft, risikobehaftete Datenbewegungen zu identifizieren
- Das Problem der Insider-Bedrohungen entwickeln sich weiter (sind aber lösbar)