

Veränderungen der Bedrohungslandschaft durch künstliche Intelligenz am Beispiel E-Mail

Christian Doppelhofer / Duarte Alvarez del Olmo
Geschäftsführer eCURA GmbH / Enterprise Account Executive Darktrace
christian.doppelhofer@ecura.at / duarte.ado@darktrace.com
+43 699 1011 1210 / +49 174 186 40 95

Die Landschaft der E-Mail-Bedrohungen entwickelt sich ständig weiter

WO WIR IM JAHR 2024 STEHEN

Zunehmend ausgefeiltere Angriffe

+135 %

Zunahme der „neuartigen Social-Engineering-Angriffe“, entsprechend der Zunahme der ChatGPT-Nutzung¹

Zielgerichteter

45 %

der Phishing-E-Mails wurden als Spear-Phishing-Versuche identifiziert²

Mehr Angriffe mit mehrstufigen Nutzdaten

+59 %

Zunahme von Angriffen mit mehrstufiger Nutzlast³

1: [Darktrace/E-Mail Pressemitteilung](#) Kundendaten 1. Jan. – 28. Feb. 2023

2: [Darktrace End of Year Threat Report 2023](#) Kundendaten 1. Sept. – 31. Dez., 2023

3: [Darktrace End of Year Threat Report 2023](#) Kundendaten 1. Mai – 31. Juli 2023

Bestehende Lösungen sind in der Vergangenheit verhaftet

HERAUSFORDERUNGEN FÜR DIE BRANCHE

Komplexität der Angriffe + Schutz



58 %

der Phishing-E-Mails, die Darktrace Kunden erhalten haben, **durchdrangen alle bestehenden Sicherheitsebenen**¹

1. [Darktrace Threat Report 2023](#), Daten 1. Sept. – 31. Dez. 2023

Bestehende Lösungen sind in der Vergangenheit verhaftet

HERAUSFORDERUNGEN FÜR DIE BRANCHE

Komplexität der Angriffe + Schutz



58 %

der Phishing-E-Mails, die Darktrace Kunden erhalten haben, **durchliefen alle bestehenden Sicherheitsebenen¹**

1. Darktrace Threat Report 2023, Daten 1. Sept. – 31. Dez. 2023

Lebenszyklus der E-Mail-Sicherheit

VERBESSERUNG IHRES WORKFLOWS

Phase 1:

Eingangsvektor

Phase 2:

Endbenutzer

Phase 3:

Sicherheitsteam

Phase 4:

Symptome einer Kompromittierung

Phase 1: Eingangsvektor



VERBESSERUNG IHRES WORKFLOWS

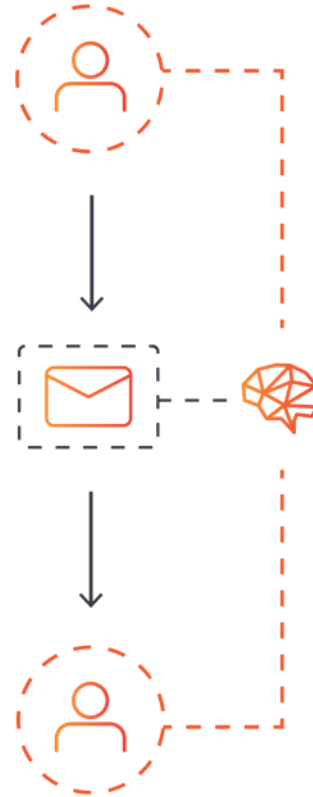
Traditioneller Ansatz

- Angreiferorientierte Daten
- Auf Nutzlasten konzentriert



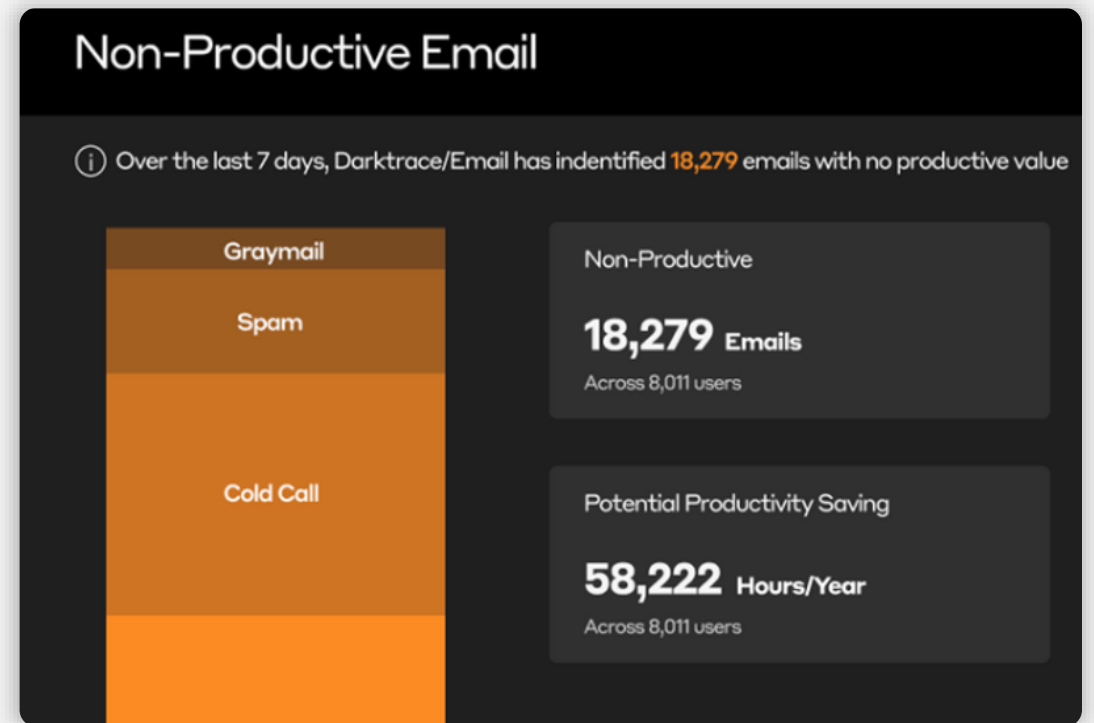
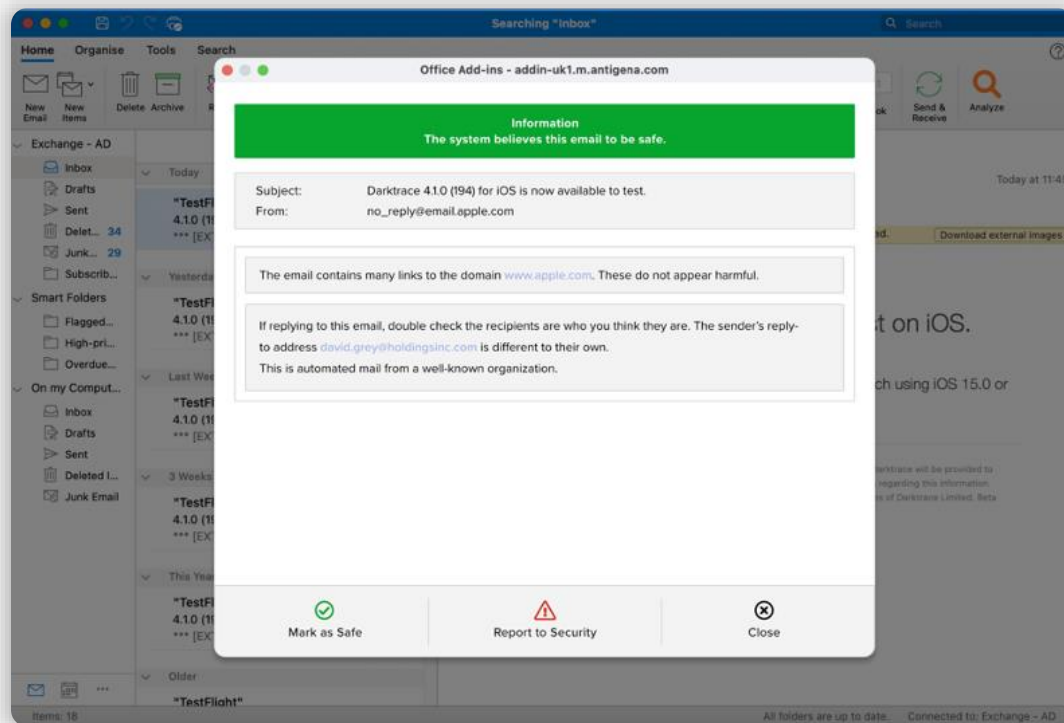
Neuartiger Ansatz

- Unternehmensorientierte Daten
- Fokus auf Nutzer/Verhalten



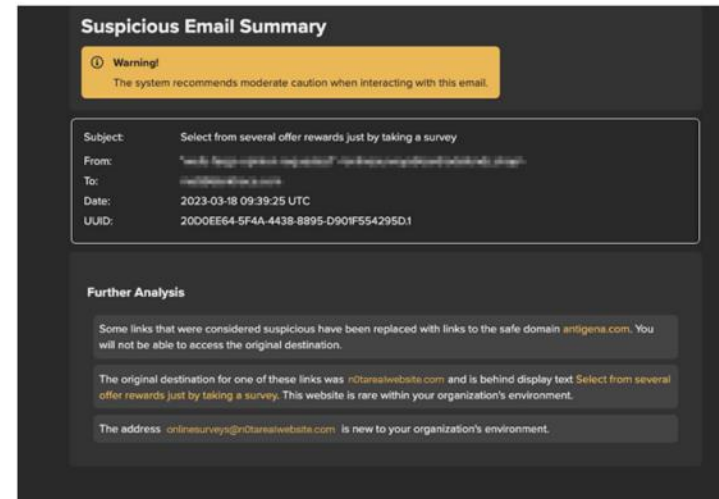
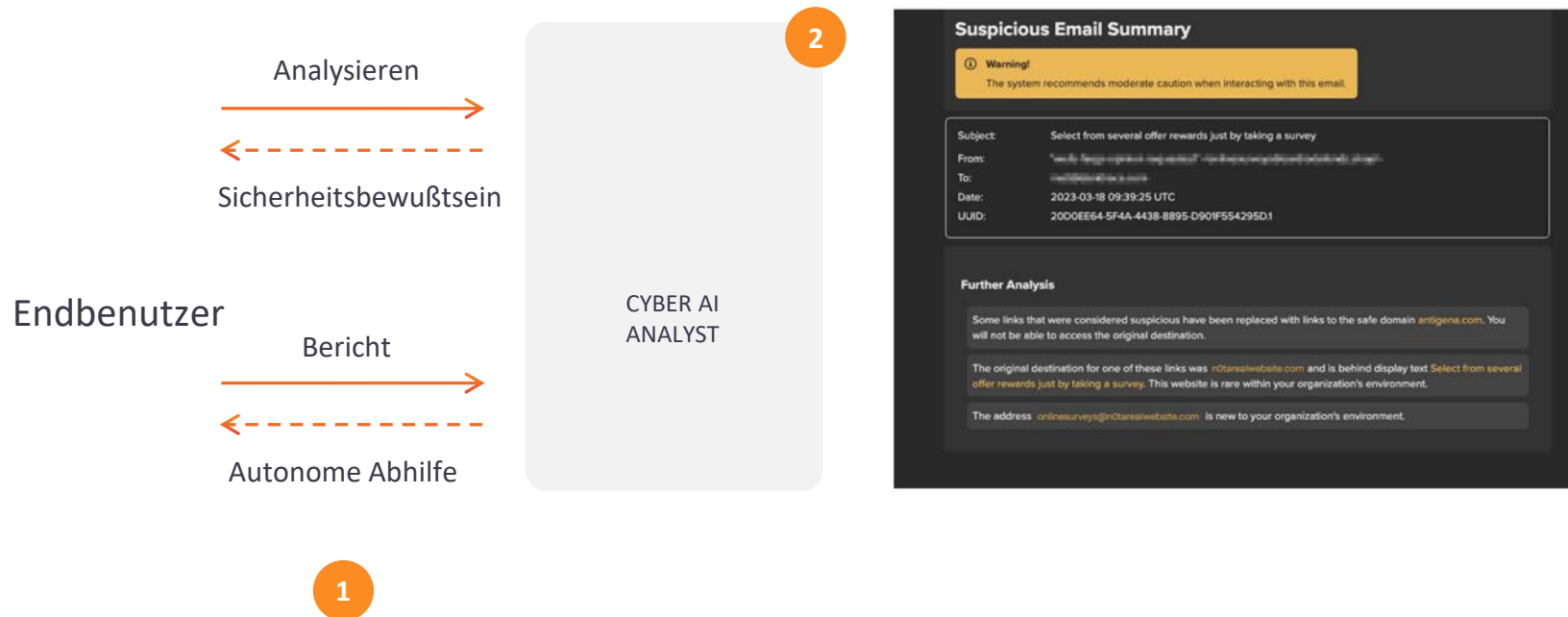
Phase 2: Interaktion mit dem Endbenutzer

VERBESSERUNG IHRES WORKFLOWS



Phase 2: Interaktion mit dem Endbenutzer

VERBESSERUNG IHRES WORKFLOWS

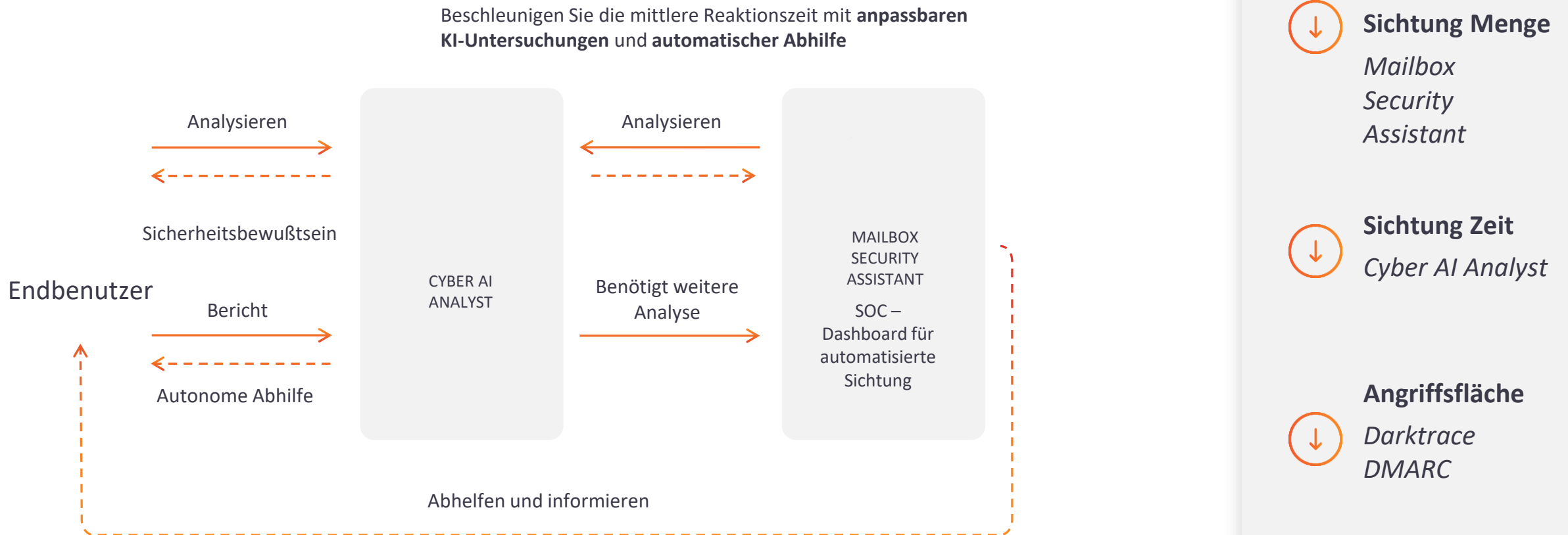


60 %¹

weniger gutartige E-Mails werden gemeldet¹

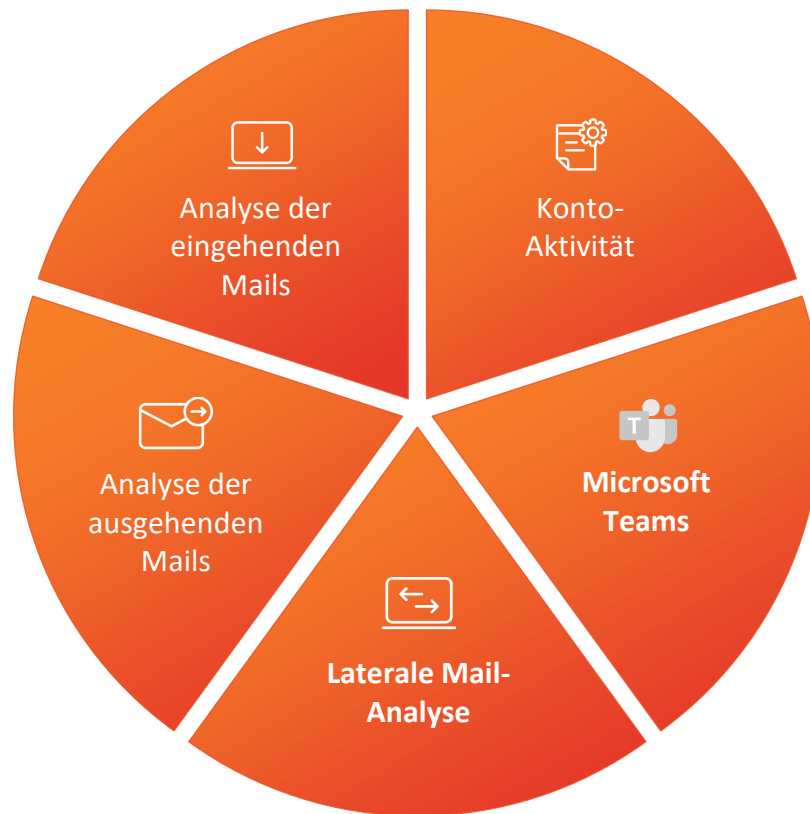
KI-gestützte Triage mit neuer Link-Analyse
20 Mal mehr Kontext¹

Phase 3: Mailbox Security Assistant



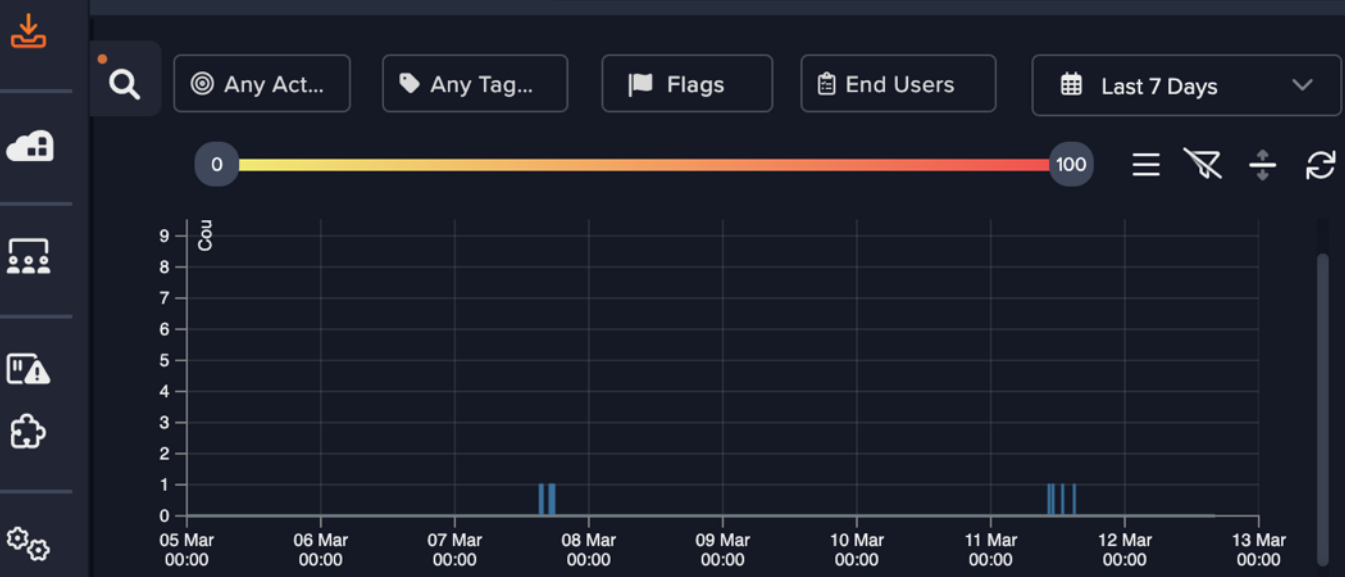
Phase 4: Symptome einer Kompromittierung

VERBESSERUNG IHRES WORKFLOWS



Reduziert die durchschnittliche Zeit bis zur Entdeckung eines angegriffenen Kontos von **über 200 Tagen auf einen Tag¹**

- Erkennt **frühzeitig Symptome** einer Kontenübernahme oder einer bösartigen Insider-Bedrohung
- Überwacht auf verdächtige **Microsoft Teams** und **laterale Mailaktivitäten**
- Verhaltensanalyse zur Unterbindung von **Angriffen ohne Nutzlast**



amy pond <amy.pond@edu1corp.com>

Data

← amy.pond@sharklasers.com

📧

🔗

🔒

☁

MON MAR 11 2024, 14:58:24

45%

amy pond <amy.pond@edu1corp.com>

Data

← amy.pond@sharklasers.com

📧

🔗

🔗

🔒

☁

MON MAR 11 2024, 14:56:27

45%

amy pond <amy.pond@edu1corp.com>

Data

← amy.pond@maildrop.cc

📧

🔗

🔗

🔒

☁

MON MAR 11 2024, 14:54:37

30%

Data

Amy Pond <Amy.Pond@edu1corp.com>

🗑

🗑

📄

To: amy.pond@sharklasers.com

🗑

🗑

📄

MON MAR 11 2024, 14:58:24

📧

📄

👤

⚠

Processed (unread)

🔒 Data Loss

🔒 Low Mailing History

🔒 New Correspondent File Transfer

🔒 Personal Account File Transfer

🔒 Personal Address

🔒 Known Domain Relationship

No Actions Taken

⚠

ANOMALY INDICATORS

The user amy pond appears to be emailing their own account, amy.pond@sharklasers.com.

🔗 ASSOCIATION

👤 1 User

📅 To

📁 CONTENT

📄

⚠

Company Passwords2.zip

30.3 KiB

Vielen Dank!

