



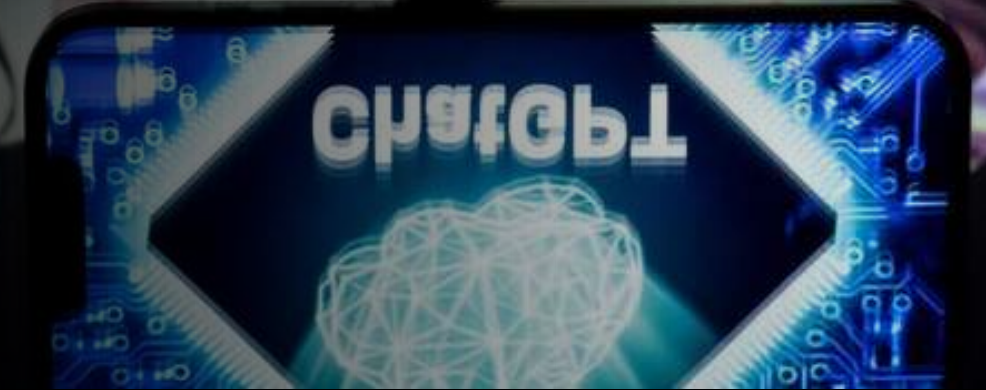
DARKTRACE

Neue Innovationen in E-Mail-Sicherheit - Anwendung von verhaltensbasierter KI

Max Heinemeyer
/ Chief Product Officer



Auswirkungen der generativen KI auf Cyber- Angriffe



Die Raffinesse der Angriffe nimmt zu

27% Zunahme der durchschnittlichen sprachlichen Komplexität von Phishing-E-Mails

15% Rückgang der E-Mails mit bösartigen Links

Dies wird nicht
gegen
generative KI-
Angriffe
funktionieren

KNOWLEDGE BASE
PHISHING ATTACKS 



Darktrace Cyber KI Forschungszentrum

- Forschungsorientiert mit einem "problemorientierten" Ansatz
- Experten in mehreren Disziplinen
- Spitzenleistung - Scheitern erlaubt
- Die Forschung von heute ist das Produkt von morgen

28% F&E-
Personalwachstum
im GJ22

20 Doktorate

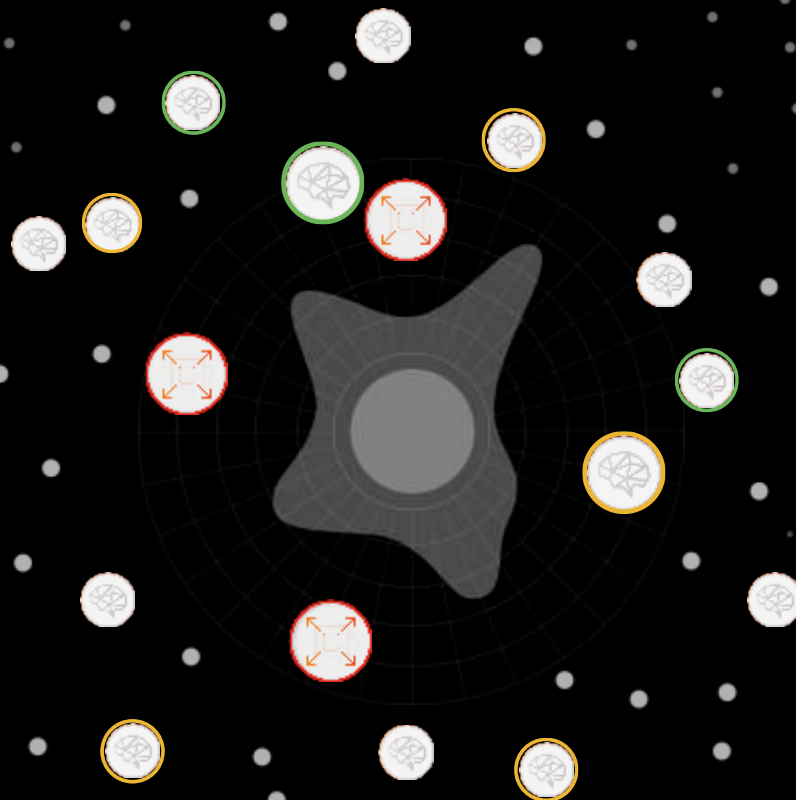
100 Master-
Abschlüsse

Darktrace versteht Sie

Schutz für Ihr Unternehmen durch
Verständnis für Sie

- / Um die raffiniertesten Angriffe auf den **Posteingang zu stoppen**
- / Kombiniert mit dem Schutz vor **verhaltensbedingter Kontoübernahme**
- / Einsatz von KI zur **Produktivitätssteigerung** - Mitarbeiter-KI-Feedback-Schleife und Verwaltung unproduktiver Post
- / Verhaltensbasierte Erkennung von **fehlgeleiteten E-Mails**
- / Integration von E-Mails mit Daten über den **gesamten digitalen Bereich** hinweg

Darktrace/Email



QR-Code Phishing

Server Access June 22, 2023 19:13:56 PM - 12520

IT-voicemail@banes-gn.com

To: [Redacted]

THU JUN 22 2023, 13:29:15

100%

Held

- Credential Harvesting
- Internal IT Impersonation
- Lookalike Domain
- Multistage Payload
- Low Mailing History
- No Association
- Spoofting Indicators
- Unknown Correspondent

ANOMALY INDICATORS

The sender appears to be impersonating an internal service by referencing [Redacted] in their **display name**. This tactic allows attacks to avoid any validation checks which apply to this domain.

The email has an attachment containing a highly suspicious link to a host `227wmp5mft.execute-api.us-gov-west-1.amazonaws.com` which the system believes will **redirect** the user to a different destination upon clicking. The host has a **100%** rarity score based on references in internal traffic.

The domain `banes-gn.com` was registered only **6 days ago**.

HISTORY 0 Users 0 Days

This is the **first** time any mail has been seen from the organization `banes-gn.com`.

ASSOCIATION 0 Users Never

There has been **no outbound email communication** with the organization `banes-gn.com` previously. Its overall rarity score based on references in internal traffic is **100%**.

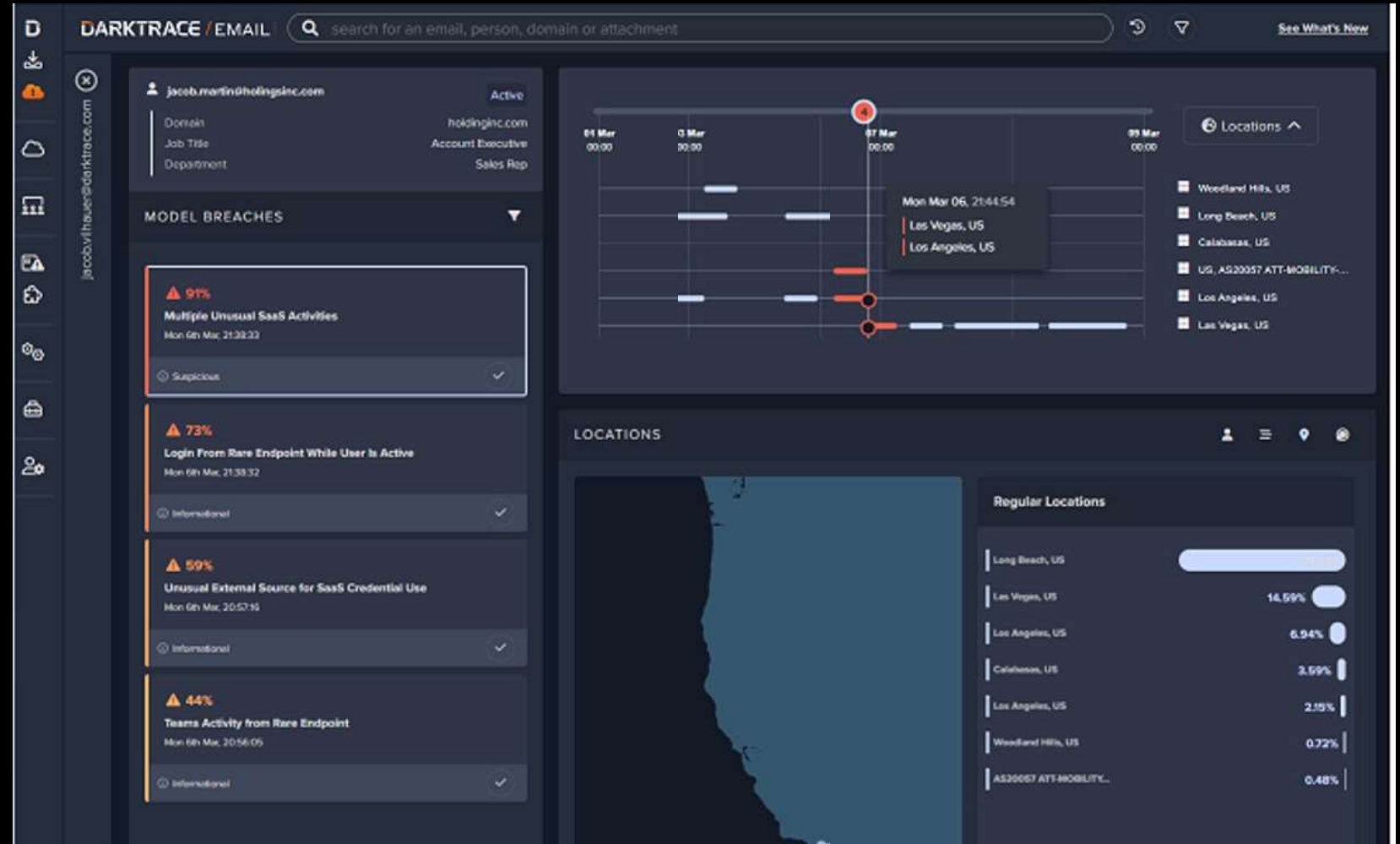
VALIDATION SPF **all** DKIM **all** DMARC **all**

The email was sent from an authentic source for `banes-gn.com`. This was verified via **DKIM**.

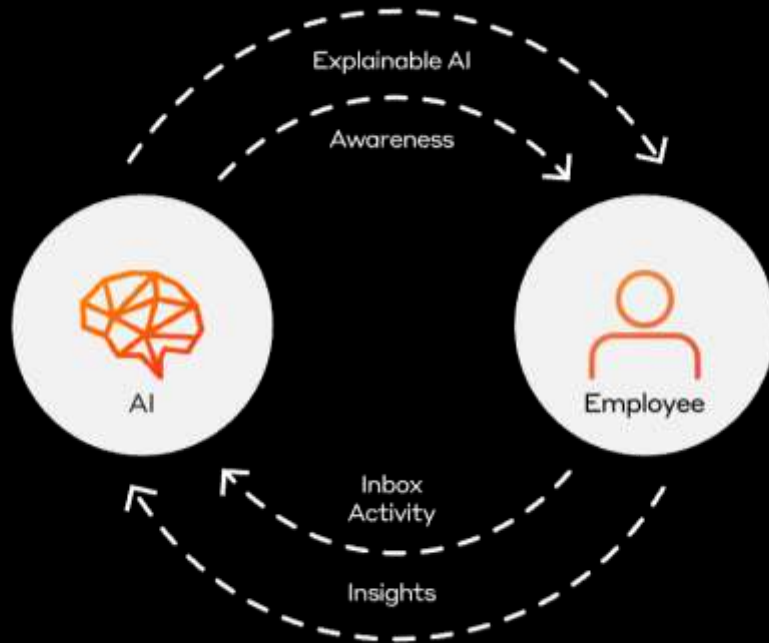
The connection source for the email is **United States**.

Kontoübernahmen

Erkennung von Abweichungen von der normalen Aktivität, wie z. B. Login- und Posteingangsaktivitäten



Mitarbeiter-KI Loop

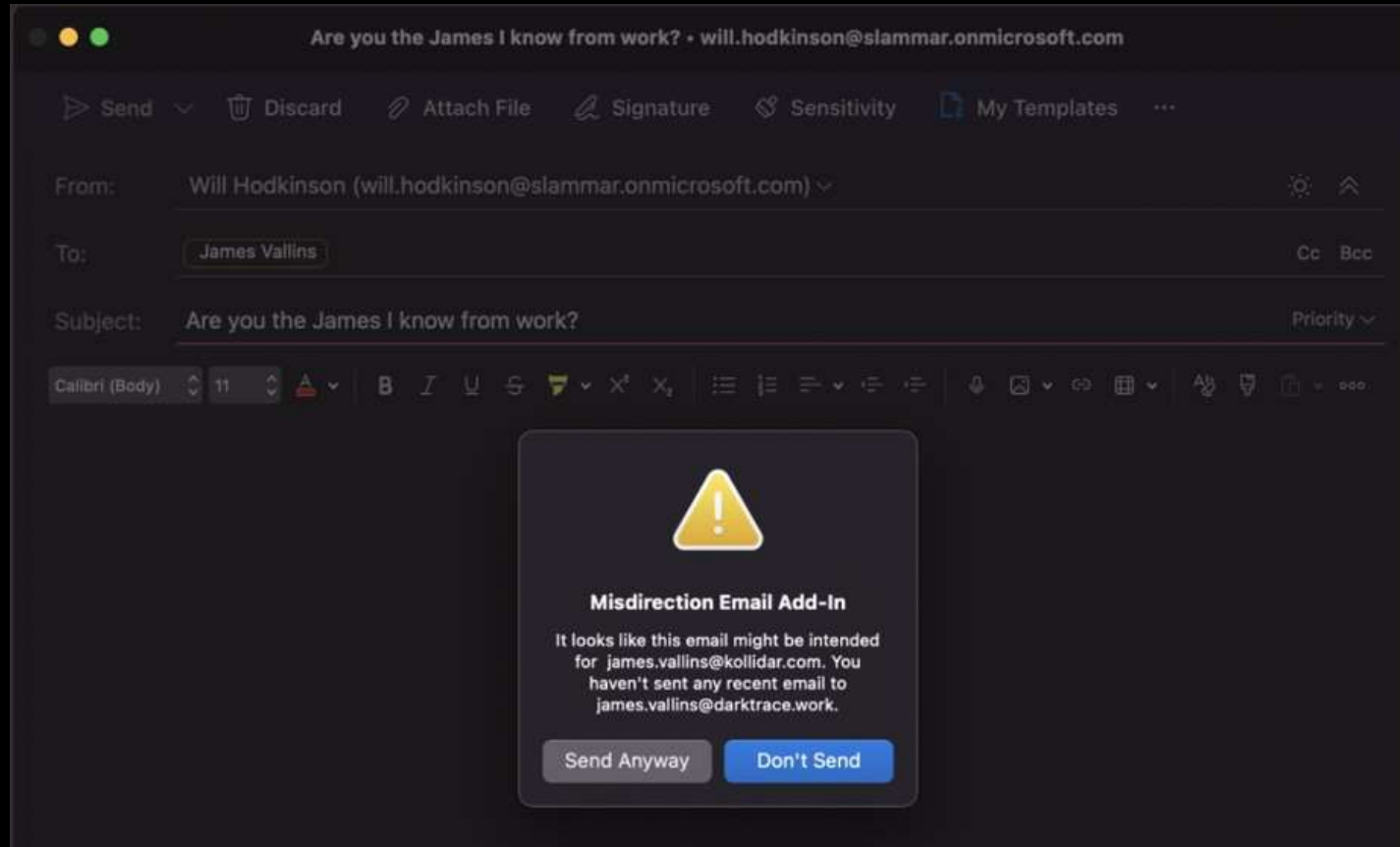


**Ausgewogene
Mitarbeiter-Feedback-
Schleife**

**Verbessertes
Sicherheitsbewusstsein**

**Verbesserte
Präzision**

Vermeidung von E-Mail-Pannen



Angriffe über den Posteingang hinaus

Critical AI Analyst Incident

Beginning on Monday 13th February 08:13 GMT, the device [redacted] exhibited the following events worthy of investigation

	Mon 13th 08:00	Mon 13th 09:00	Mon 13th 10:00	Mon 13th 11:00	Mon 13th 12:00	Mon 13th 13:00	Mon 13th 14:00	Mon 13th 15:00	
Possible HTTP Command and ...	[Timeline bar]							[Yellow dot]	
Suspicious Email Identifie...							[Blue bar]		
Suspicious Chain of Admini...							[Yellow dot]		

1. Possible HTTP Command and Control to Multiple Endpoints **2. Possible HTTP Command and Control to Multiple Endpoints** **3. Suspicious Email Identified by Darktrace/Email** **4. Suspicious Chain of Administrative Connections**

SUMMARY

Darktrace/Email identified a suspicious email from [redacted] to [redacted] containing a link to the potentially malicious hostname www.foodsofengland.co.uk.

Since this hostname was also observed in another event of this incident, this email may relate to the overall activity identified, for instance as a source of initial compromise by phishing.

Consequently, the security team may wish to investigate further.

Please see this email [object Object] for further details.

[Initial Access](#)

LINKED INCIDENT EVENTS

ACTIONS

Acknowledge this Incident Event

EMAIL DETAILS

Time	13th Feb 2023 14:23:02 GMT
Sender	[redacted]
Recipient	[redacted]
Subject	Recommendation
Hostname Present	www.foodsofengland.co.uk
Darktrace/Email UUID	[object Object]

Q&A