

# Security Prioritäten

## CIO Agenda 2023

David Etzelstorfer – Proofpoint / Henning Dey - Serviceware

10.10.2022

LSZ CIO Kongress 2022

# Top-Prioritäten

## SICHTBARKEIT

- Risikoeinschätzung
- Bedrohungsintelligenz
- Angreifer erkennen
- Impactanalyse

## Reaktionsvermögen

- Incident-Response
- Workflows
- Notfallhandbücher
- Backup-Konzepte

## Reaktionsvermögen..



# Top Themen

## Security Strategie

### Schutz von Identitäten

- Alle Plattformen
- Erkennung von unerwartetem Verhalten
- Automatisierte Aktionen (Sperrung, PW-Reset, MFA)
- Threat-Hunting
- Logging / Monitoring

### OT-Security

- Maschinenidentitäten
- Kommunikationsanalyse
- Segmentierung
- Sicherer Zugriff
- Asset und Change Management
- Schwachstellenerkennung

### Informationssicherheit

- Alle Plattformen
- Gesamter Lebenszyklus
- Mit Klassifizierung
- Ohne Klassifizierung
- UEBA / UBA
- Verschlüsselung

# Top Themen

## Security Operations

### Bedrohungsintelligenz

- Aktoren/Angreifer
- Indikatoren
- Ziele
- Wirksame Maßnahmen
  
- Automatisierte Feeds

### Automatisierung

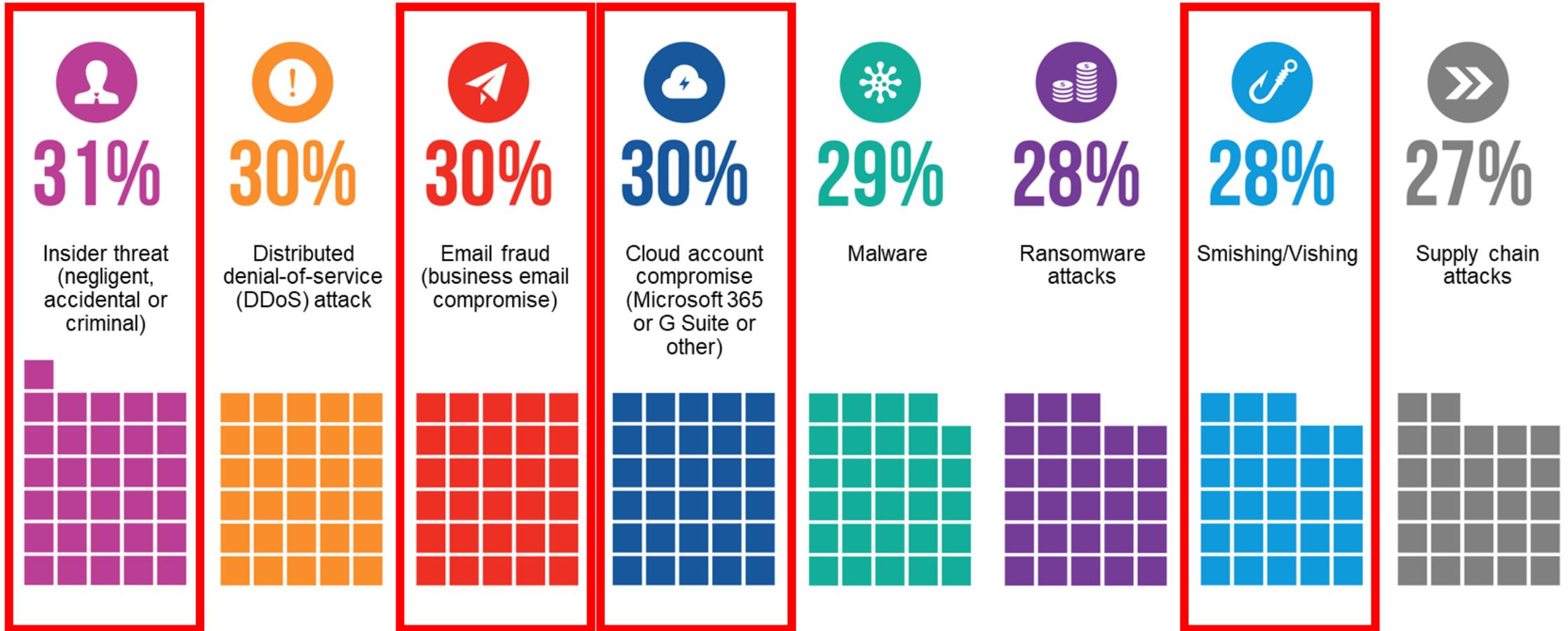
- Xtended Detection and Response
- API / SOAR
- Playbooks / Workflows
  
- Kein Copy/Paste

### Validierung

- Breach and Attack Simulation
- Blackbox Test
- Greybox Test
- Purple Team
  
- Nach jedem Change
- Nach Produktwechsel
- Nach Anpassung



# Der Faktor Mensch



# The Great Resignation

Eine LinkedIn Umfrage ergab, dass 41% der weltweiten Angestellten überlegen ihren Arbeitgeber zu wechseln



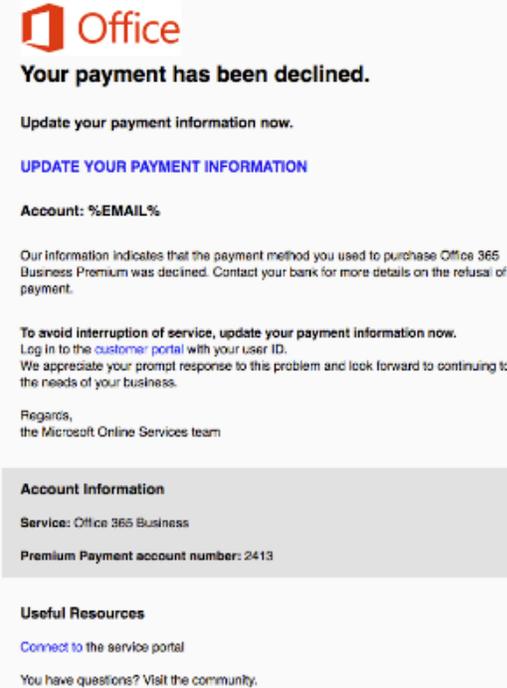
# Risiken frühzeitig erkennen

## Simulierte Phishing & USB Kampagnen

- › Real existierende Templates von Proofpoint
- › eigene Vorlagen für realistische Simulationen

## Wissenstests

- › Sind meine Benutzer doch schon fit genug?
- › An welchen Stellen müssen wir mit Schulung unterstützen?
- › Verbessern sich die Teilnehmer über die Zeit?



**Office**  
**Your payment has been declined.**

Update your payment information now.

[UPDATE YOUR PAYMENT INFORMATION](#)

Account: %EMAIL%

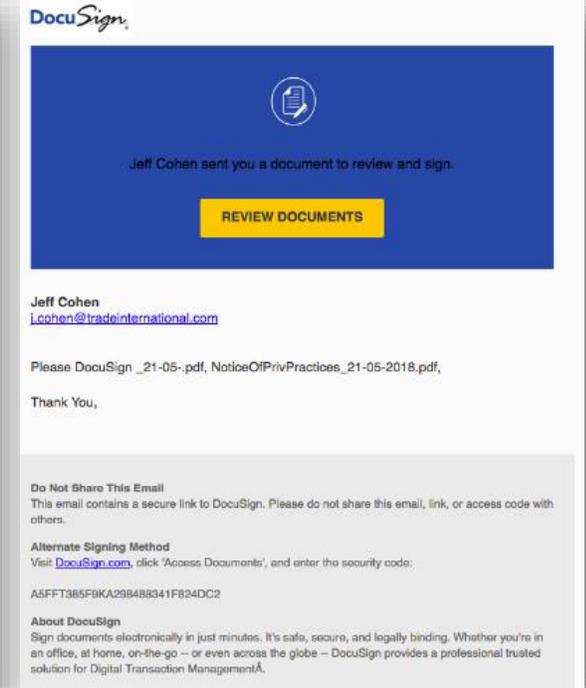
Our information indicates that the payment method you used to purchase Office 365 Business Premium was declined. Contact your bank for more details on the refusal of payment.

To avoid interruption of service, update your payment information now. Log in to the [customer portal](#) with your user ID. We appreciate your prompt response to this problem and look forward to continuing to meet the needs of your business.

Regards,  
the Microsoft Online Services team

**Account Information**  
Service: Office 365 Business  
Premium Payment account number: 2413

**Useful Resources**  
[Connect to the service portal](#)  
You have questions? Visit the community.



**DocuSign**

Jeff Cohen sent you a document to review and sign.

[REVIEW DOCUMENTS](#)

Jeff Cohen  
[j.cohen@tradeinternational.com](mailto:j.cohen@tradeinternational.com)

Please DocuSign \_21-05-.pdf, NoticeOfPrivPractices\_21-05-2018.pdf,

Thank You,

Do Not Share This Email  
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method  
Visit [DocuSign.com](#), click 'Access Documents', and enter the security code:  
A5FFT3B5F8KA298488341F824DC2

About DocuSign  
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go – or even across the globe – DocuSign provides a professional trusted solution for Digital Transaction Management.

**Congratulations! You have successfully completed this assessment.**



**Build Safe Passwords**

[More](#)



**Identify Phishing Threats**

[More](#)

# Email Assessment zur besseren Einschätzung

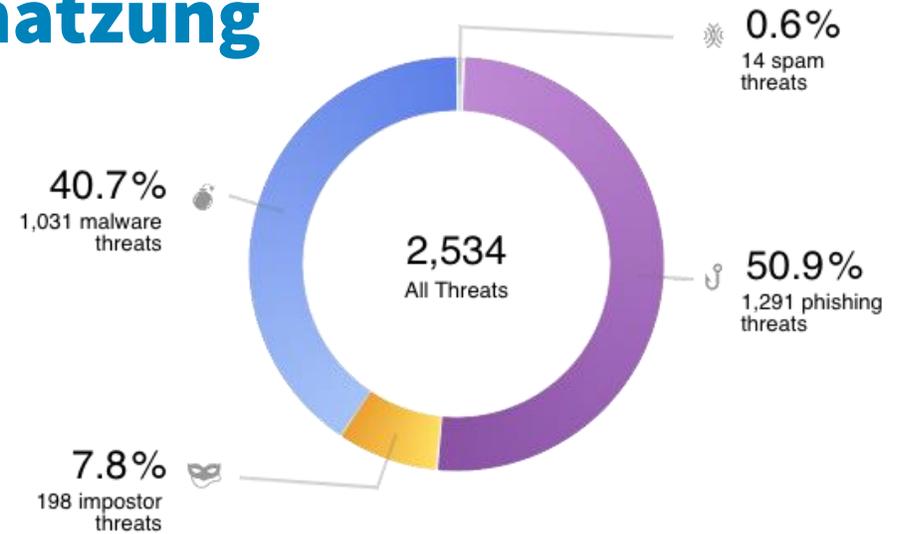
2 Wochen Analyse in ca. 24 Stunden

## Bedrohungs-zentriert

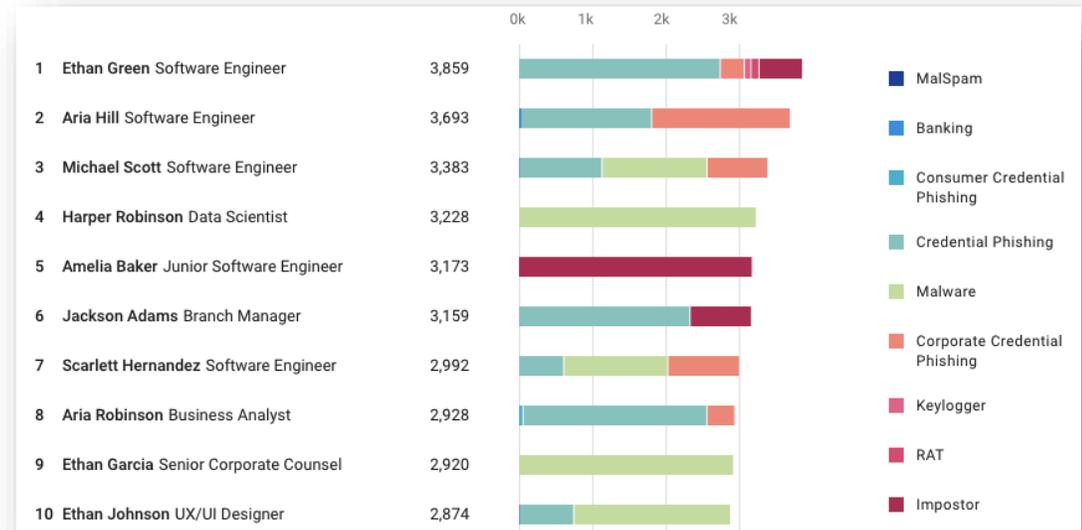
- › Potentielle Ransomware & Malware
- › Business email compromise (BEC)
- › Credential Phishing und andere Bedrohungen

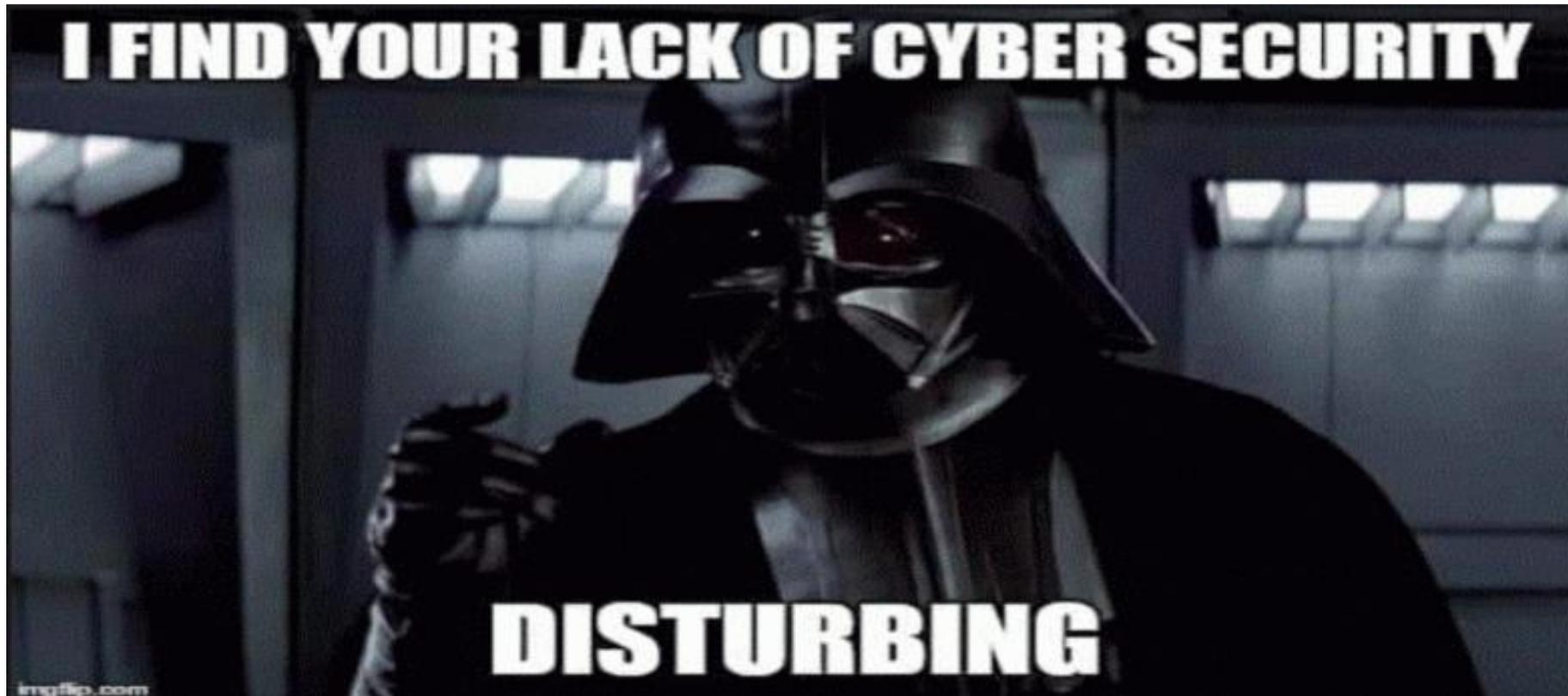
## Personen-zentriert

- › Welche Benutzer werden durch wen angegriffen?



## Retrospektivische Sicht ihrer Risikosituation





# Sichtbarkeit in Risiken der Lieferkette

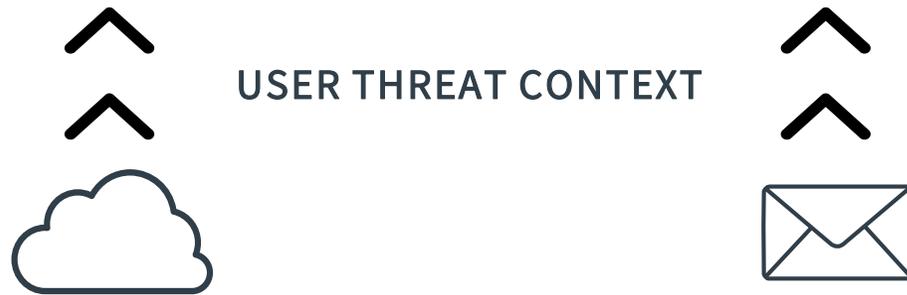
The screenshot displays the Proofpoint Supplier Risk Explorer interface. The main table lists 50,324 supplier domains. The 'keeblepharma.com' entry is highlighted with a red box, showing a 'Very High' risk level. The detailed view on the right shows the 'Lookalikes' tab, which is also highlighted with a red box. It displays a 'Very High Risk' status and a 'Threats to you' section with the following counts: Phishing (3), Imposter (6), Malware (0), and Spam (1). A 'Spread' section shows the reach of these threats across various customer segments.

Domain	Type	Risk	Threats To You	Is Lookalike	Company	Message Volume
keeblepharma.com	Supplier	Very High	10		Keeble Pharma	58
service-now.com	Discovered	High	2		Service Now	1,297,606
epic.com	Discovered	High	3		Epic	56,761
keeble.com	Discovered	High	2		Keeble Pharma	577,744
keeble.us.com	Discovered	High	3		Keeble Pharma	44,695
snow.com	Supplier	Medium	2		Service Now	12,345
intuit.com	Discovered	Medium	3		Intuit Inc.	22
onmicrosoft.com	Discovered	Medium	1		Microsoft Cor...	7,095
microsoft.com	Supplier	Low	1		Microsoft Cor...	21,231
ups.com	Discovered	Low	2		United Parcel...	89
dhl.com	Discovered	No Discovered Risk	3		DHL	281
ibm.com	Supplier	No Discovered Risk	1		IBM	87
apple.com	Discovered	No Discovered Risk	1		Apple Inc.	6
pagerduty.com	Discovered	No Discovered Risk	0		PagerDuty	4

## Kriminelle Taktiken

- Accounts von Zulieferern kompromittieren
- Identitäten fälschen oder Websites fälschen
- Falsche Rechnungen ausstellen oder Kontoänderung anfordern
- Automatische Erkennung aus dem E-Mailverkehr
- Risiko für Ihre Organisation messen
- Gefälschte Domains erkennen
- DMARC sinnvoll und geführt einsetzen
- Adaptive Kontrollen einführen

# Sichtbarkeit auf Bedrohungen von innen



## Cloud Threat Telemetry

- Login patterns
- Third-party app installations
- File sharing activity

## Email Threat Telemetry

- Clicks on malicious content
- Persistent targeting
- VAP metrics



## Identify User Type

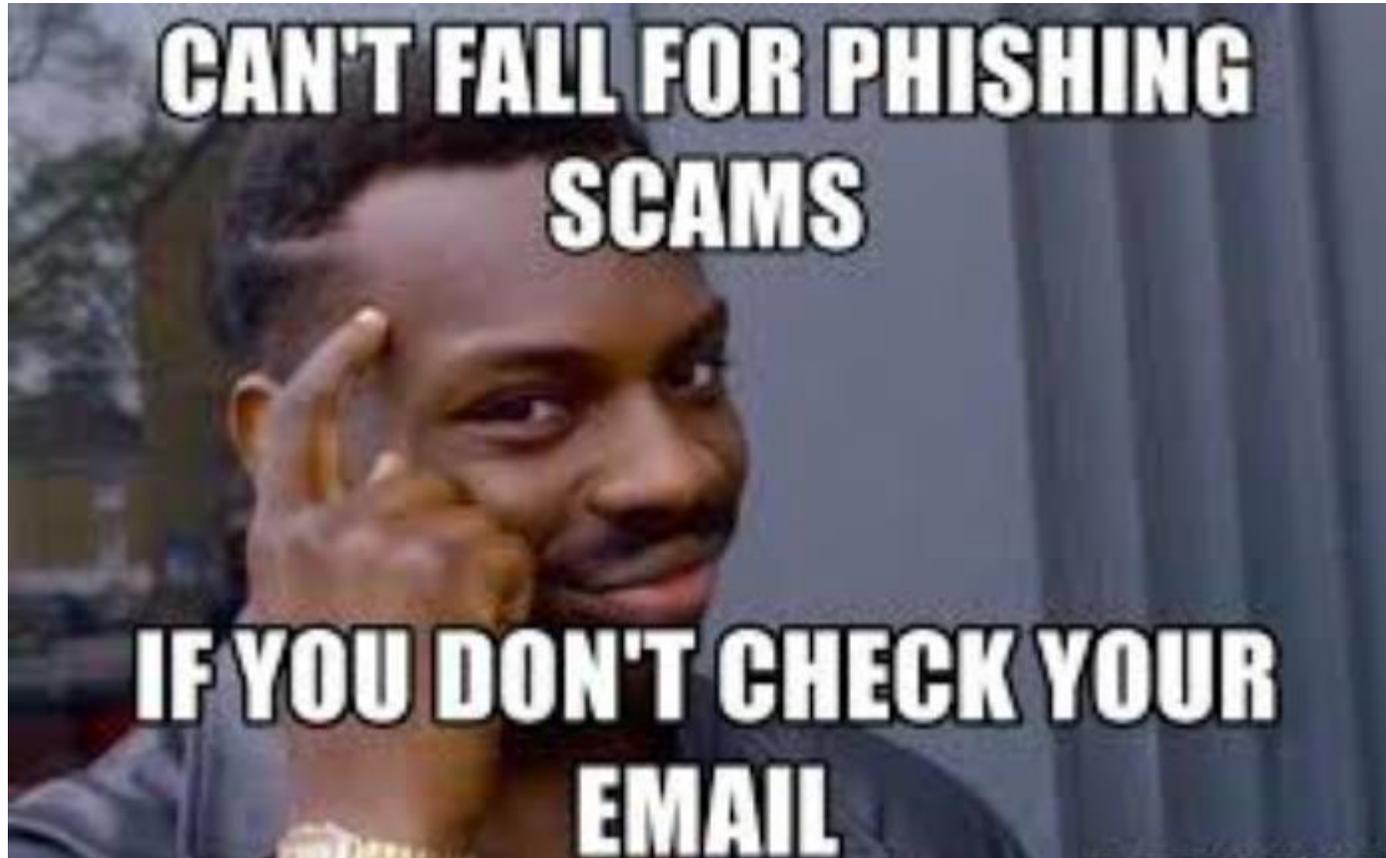


## Prioritize DLP Alerts

## Channel-specific Remediation

## Compliance Reporting

**Und am besten...**



**Vielen Dank!**