SERVICEWARE

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

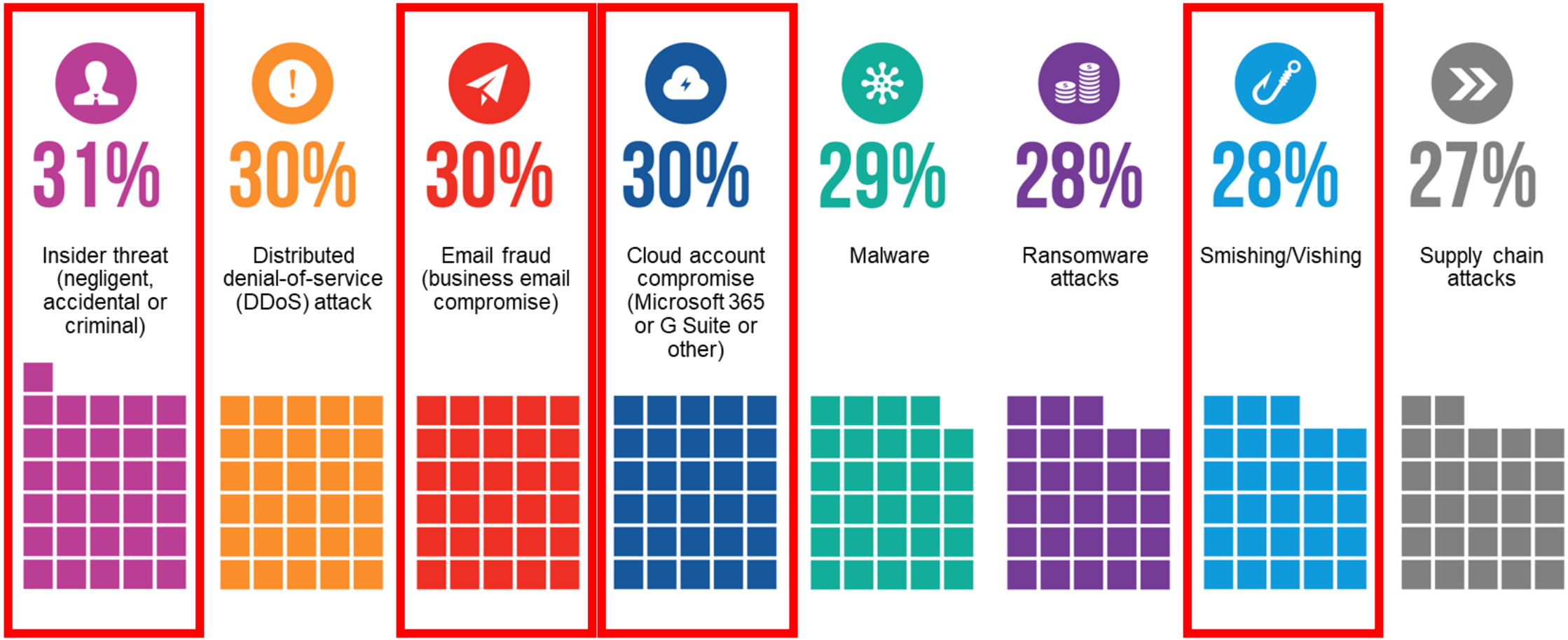
Top Themen

Security Operations

Bedrohungsintelligenz	Automatisierung	Validierung
• Aktoren/Angreifer • Indikatoren • Ziele • Wirksame Maßnahmen • Automatisierte Feeds	• Xtended Detection and Response • API / SOAR • Playbooks / Workflows • Kein Copy/Paste	• Breach and Attack Simulation • Blackbox Test • Greybox Test • Purple Team • Nach jedem Change • Nach Produktwechsel • Nach Anpassung

SERVICEWARE

Der Faktor Mensch



The Great Resignation

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

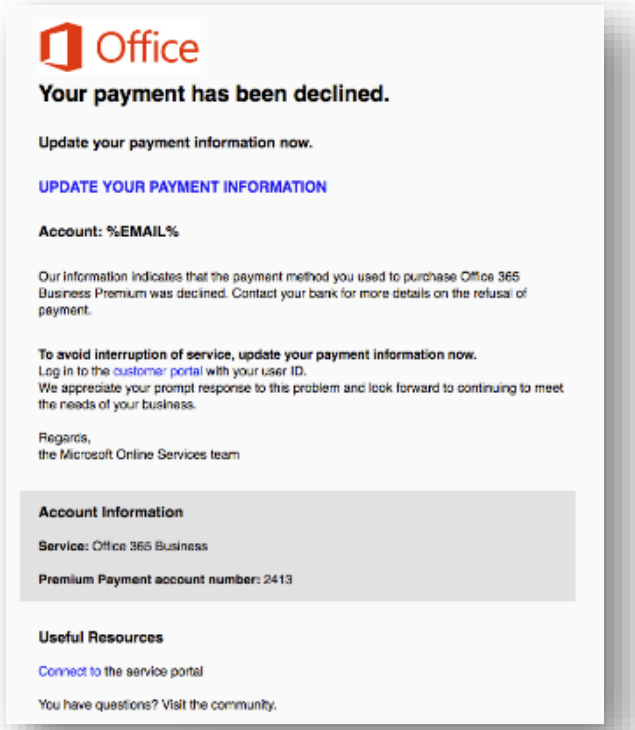
Risiken frühzeitig erkennen

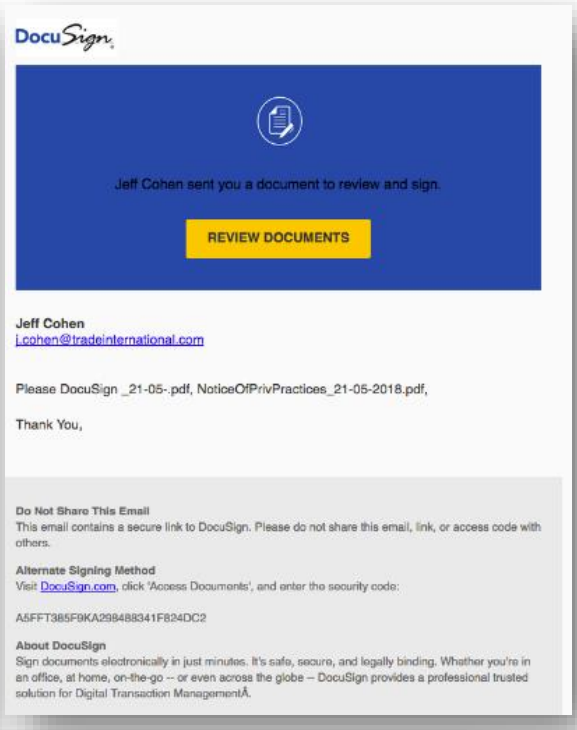
Simulierte Phishing & USB Kampagnen

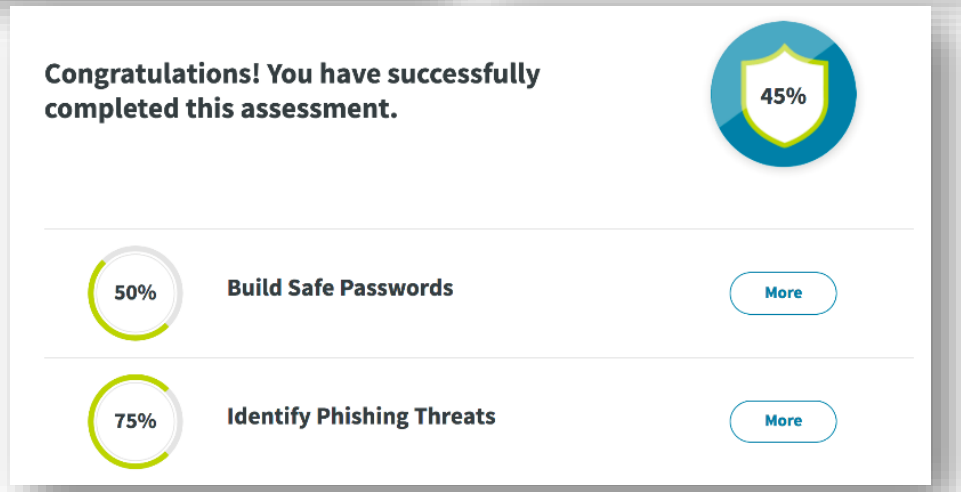
- Real existierende Templates von Proofpoint
- eigene Vorlagen für realistische Simulationen

Wissenstests

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







SERVICEWARE

Email Assessment zur besseren Einschätzung

2 Wochen Analyse in ca. 24 Stunden

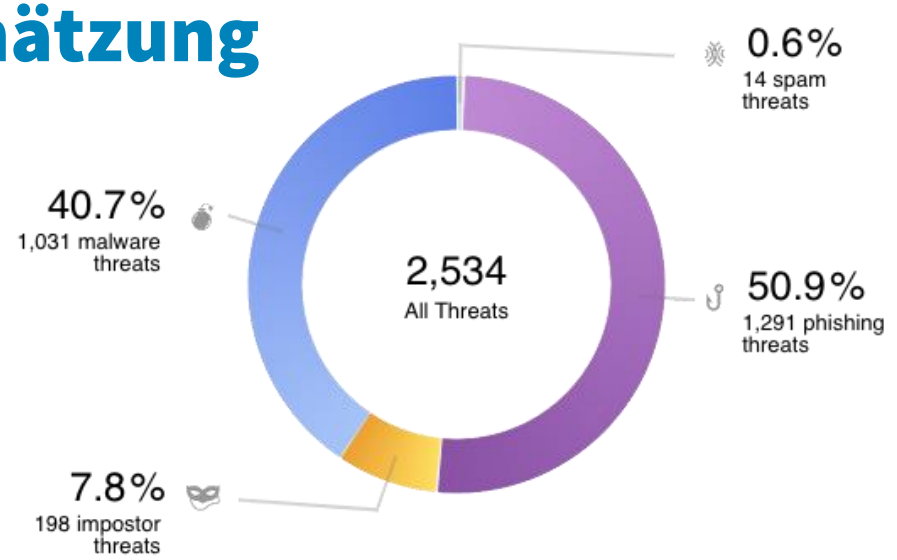
Bedrohungs-zentriert

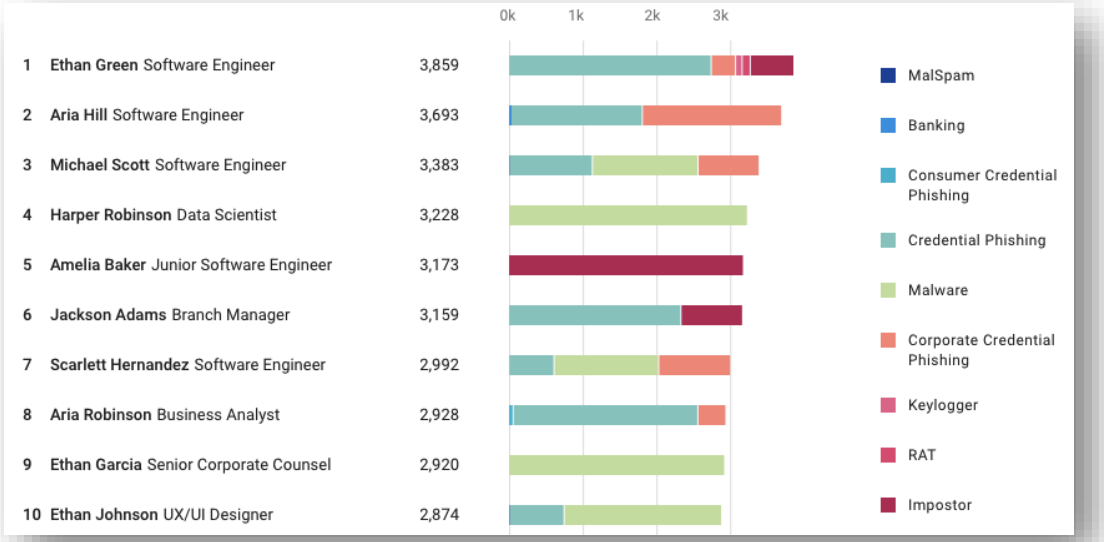
- Potentielle Ransomware & Malware
- Business email compromise (BEC)
- Credential Phishing und andere Bedrohungen

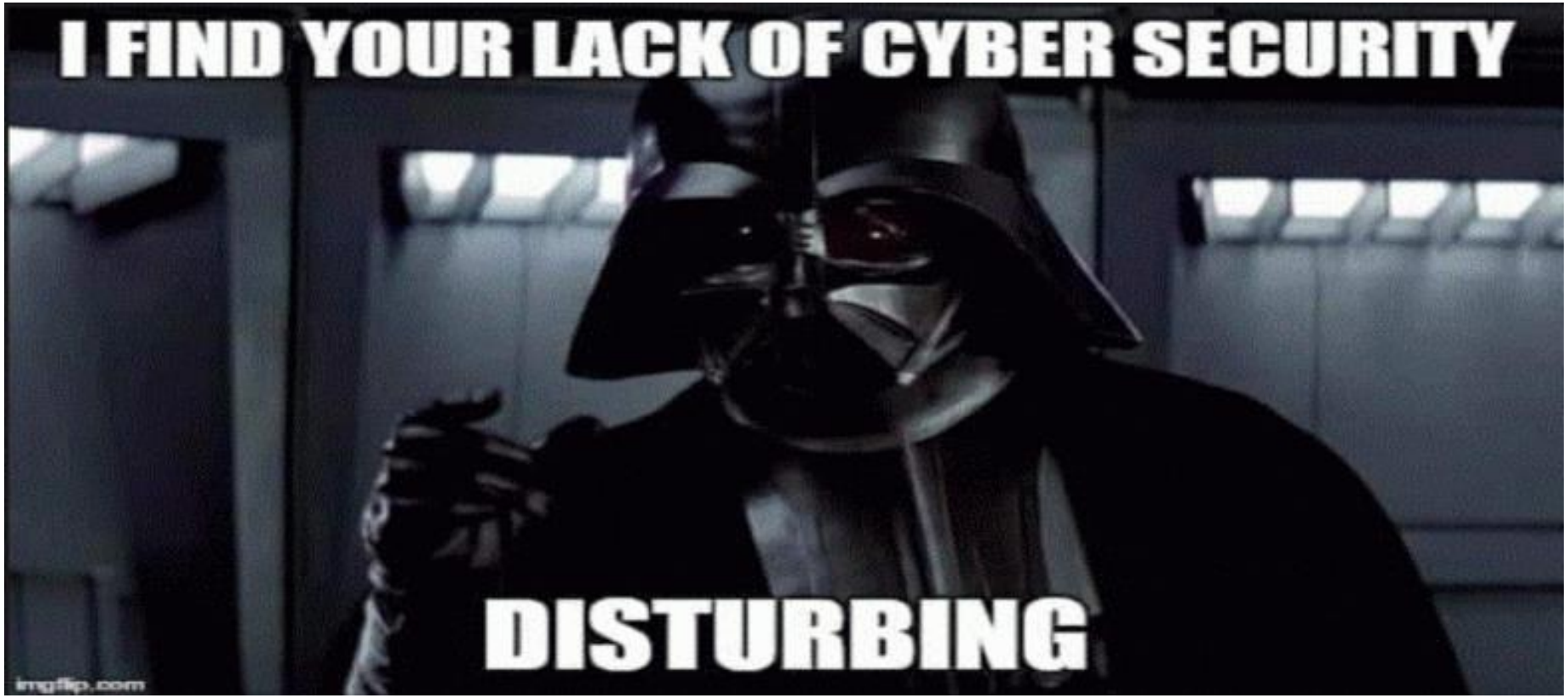
Personen-zentriert

- Welche Benutzer werden durch wen angegriffen?

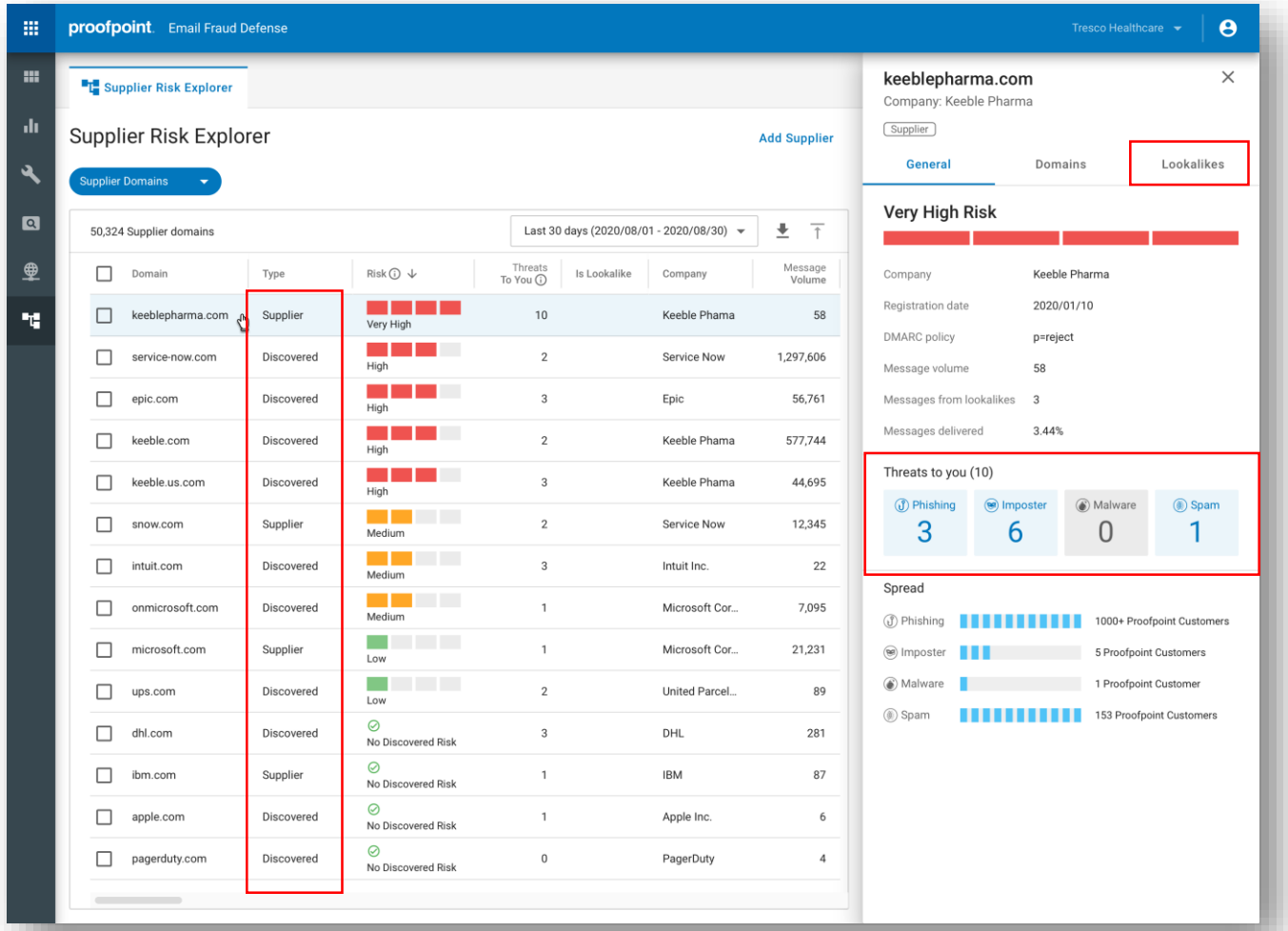
Retrospektivische Sicht ihrer Risikosituation






I FIND YOUR LACK OF CYBER SECURITY
DISTURBING
imgflip.com

Sichtbarkeit in Risiken der Lieferkette



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

SERVICEWARE

Sichtbarkeit auf Bedrohungen von innen

USER THREAT CONTEXT

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

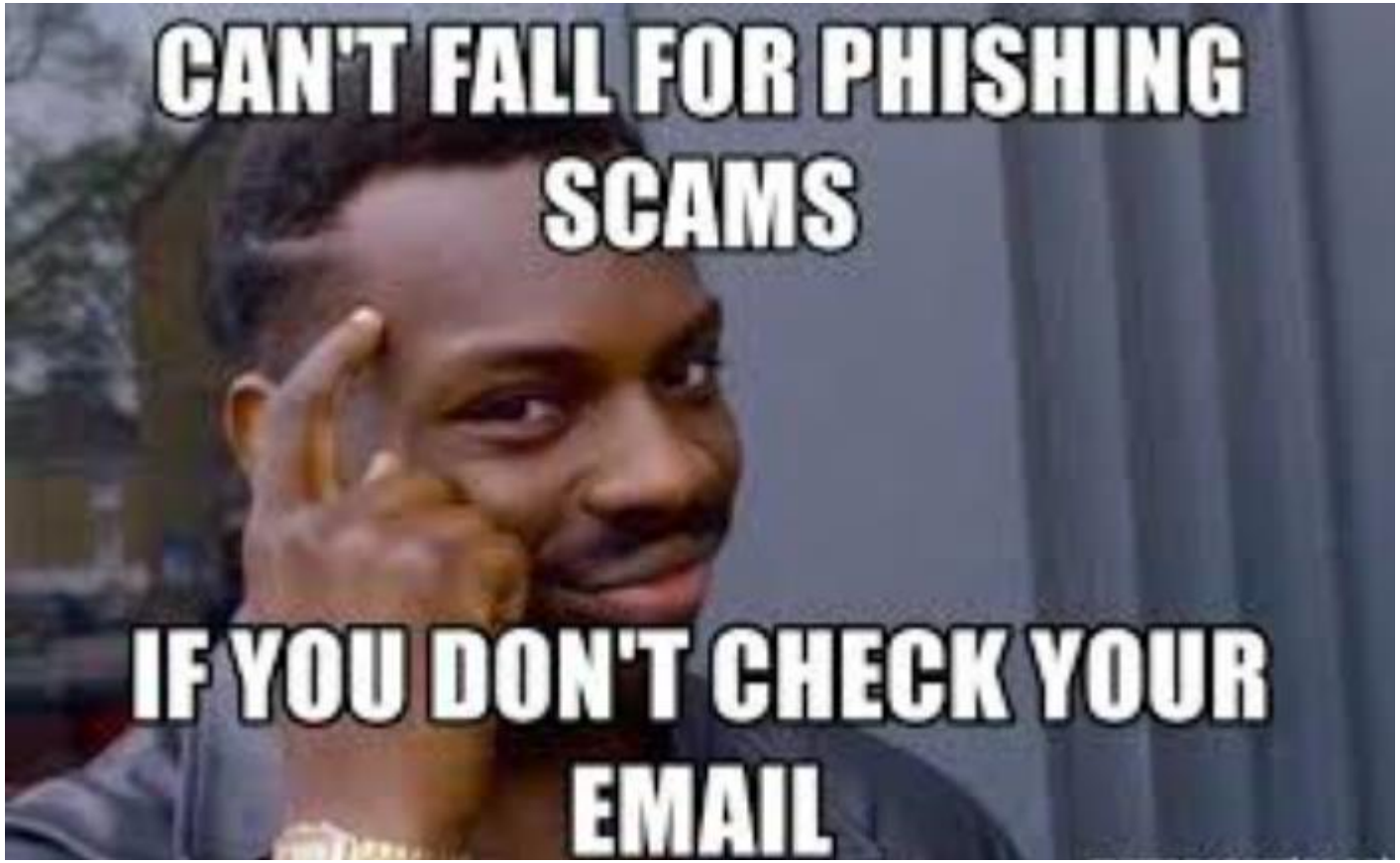
Prioritize DLP Alerts

Channel-specific Remediation

Compliance Reporting

SERVICEWARE

Und am besten…



SERVICEWARE

Vielen Dank!

Security-experts@serviceware.de