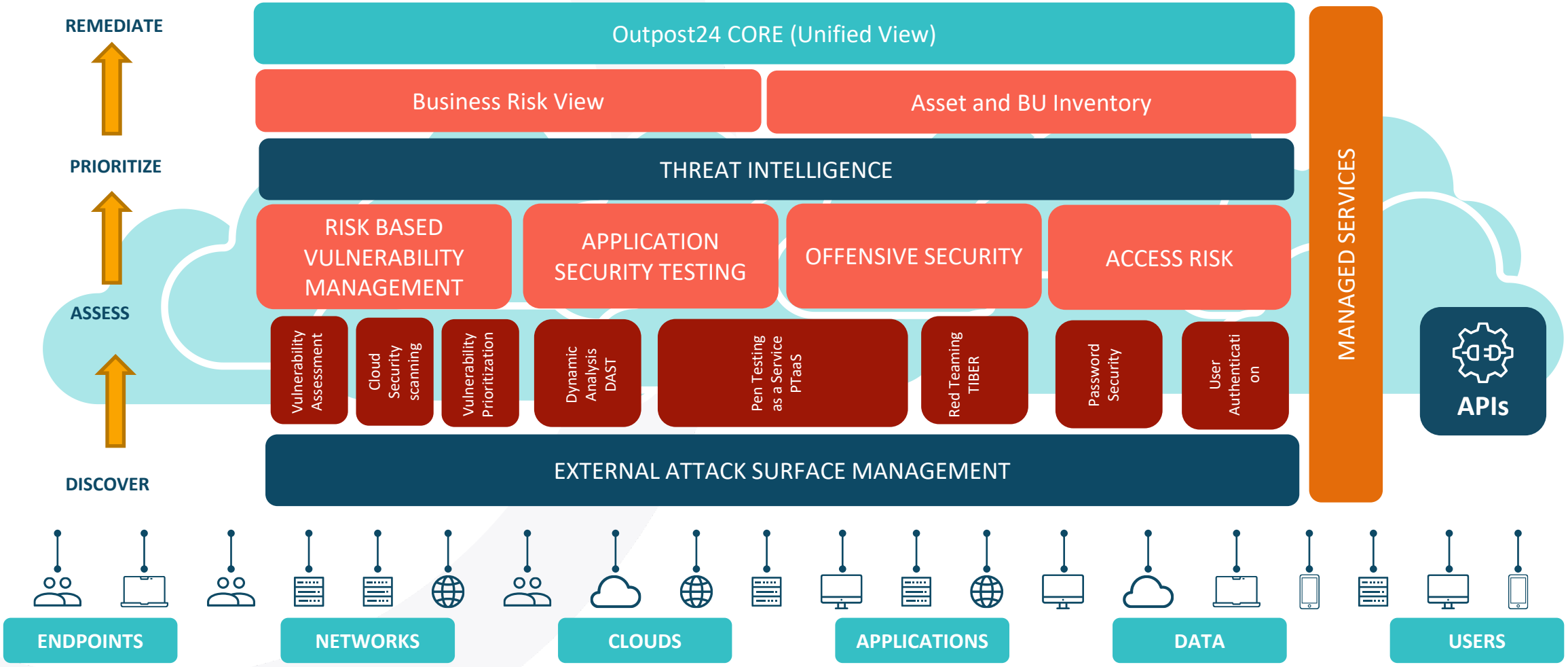
Wie Unternehmen die Kompromittierung von Zugangsdaten vermeiden

Stephan Halbmeier
Product Specialist | Outpost24

Outpost24

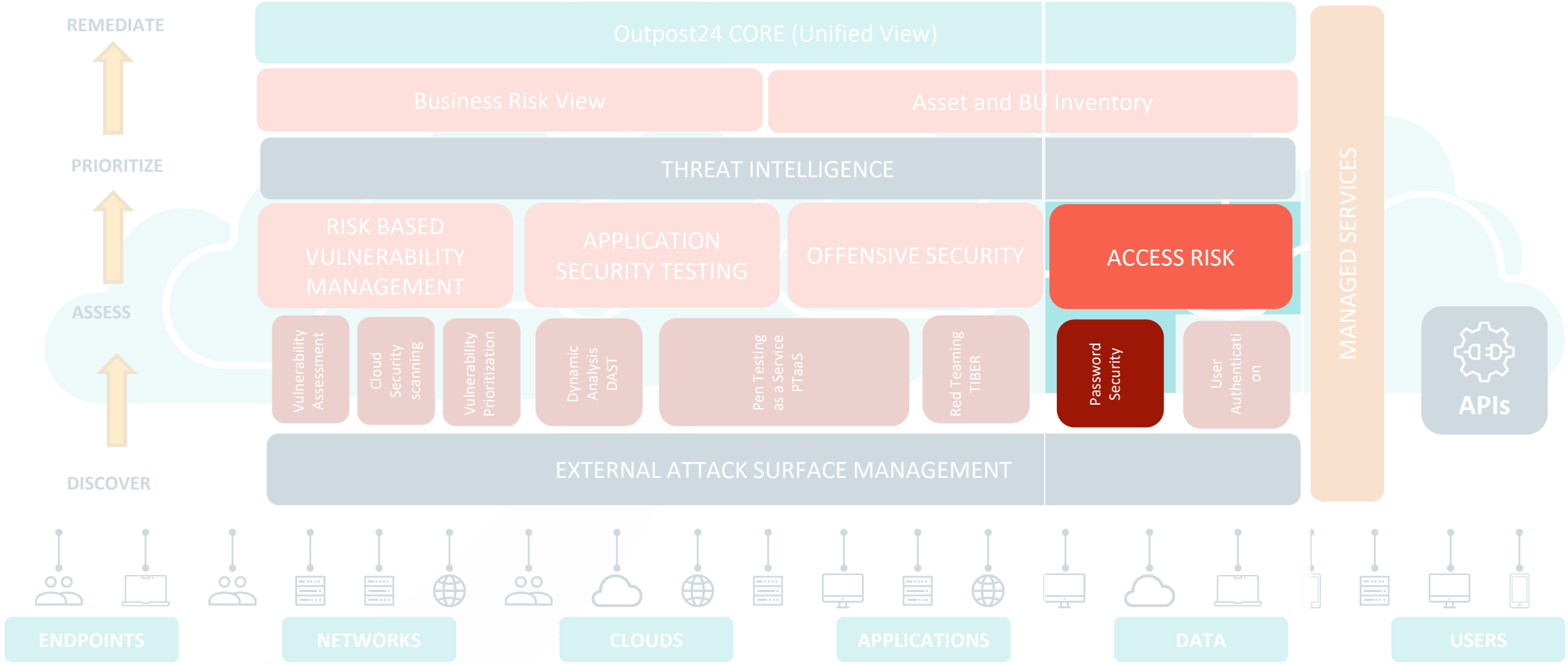

TWIX
Raider
Raider

OUTPOST24 CYBERSECURITY PLATTFORM ÜBERSICHT



Outpost24

OUTPOST24 CYBERSECURITY PLATTFORM ÜBERSICHT



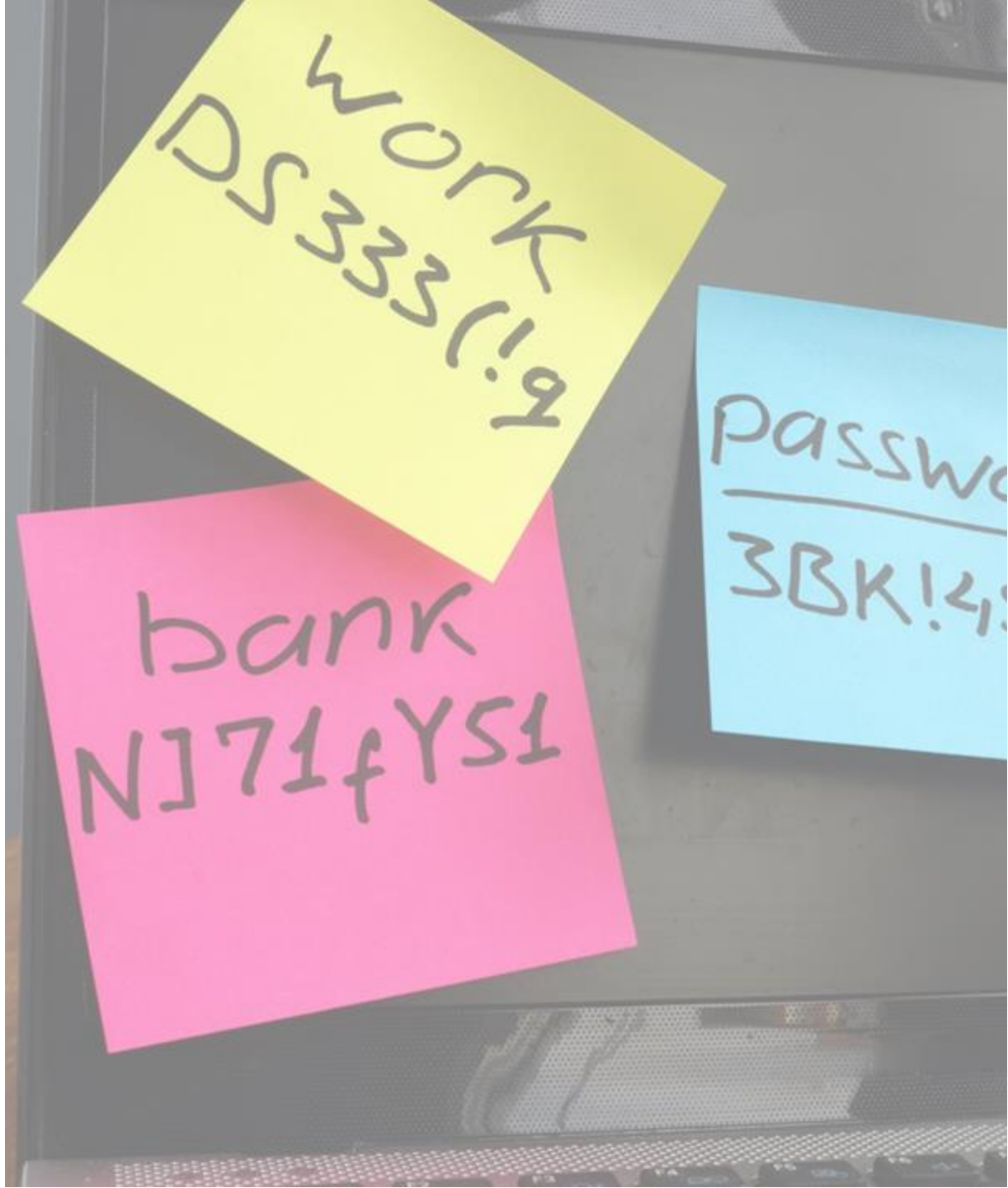
Outpost24

Was sind schwache Kennwörter?

Kandidat 1	Ferien1!	95/8
Kandidat 2	diedosismachtdasgift	26/20
Kandidat 3	DHZIplkö3457+#!?GHKU	95/20

1) Alle Kennwörter sind angemessen stark
2) Alle Kennwörter sind gleich schwach
3) Kandidat 1 ist das schwächste Kennwort
4) Kandidat 2 ist das schwächste Kennwort
5) Kandidat 3 ist das schwächste Kennwort
6) Möchte ich nicht beantworten

Outpost24

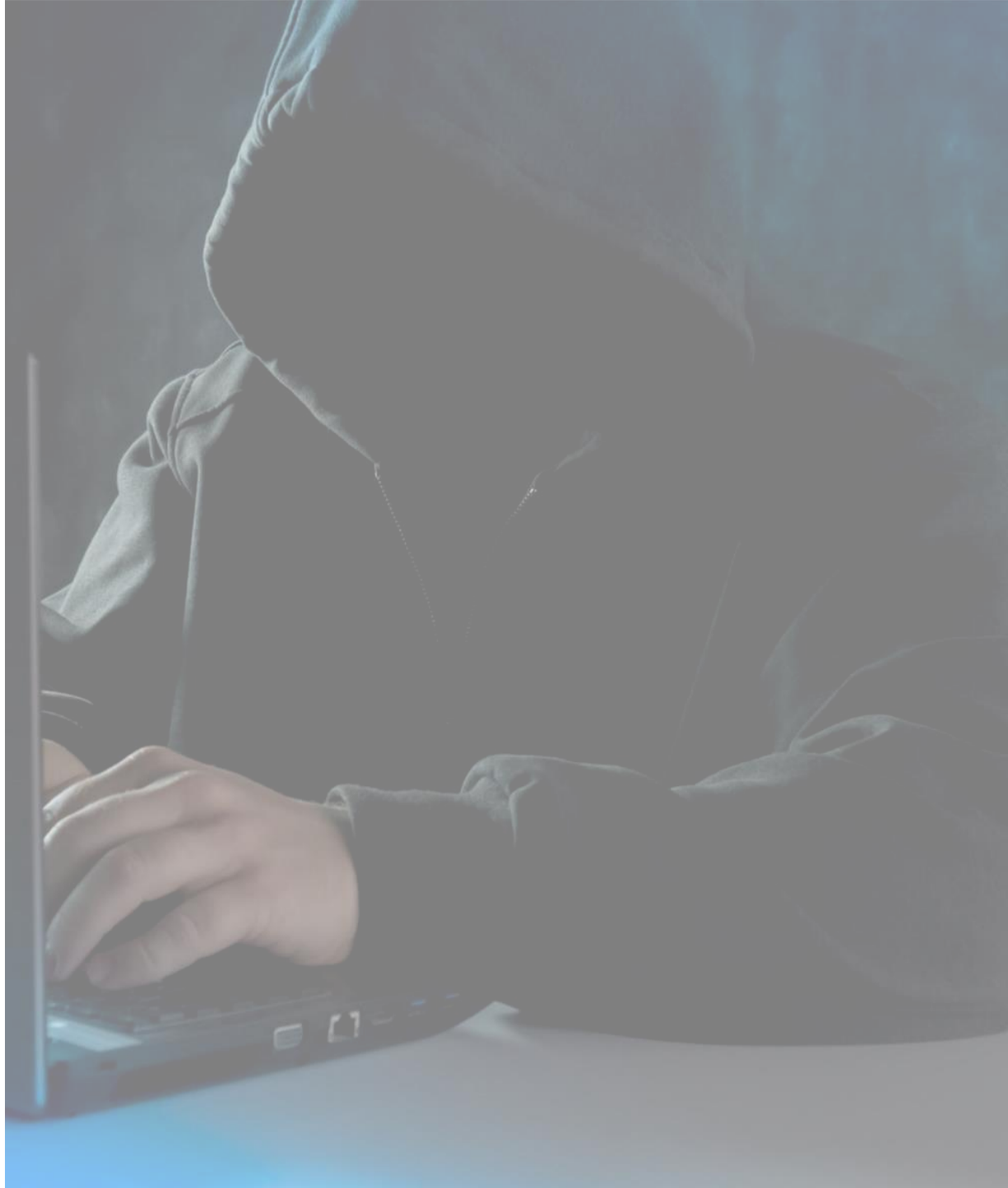


Regulatorische Anforderungen und Empfehlungen

Wer	Maßnahme
DS-GVO	„Unter Berücksichtigung des **Stands der Technik**…treffen der Verantwortliche…geeignete TOMs, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten…“
IT-Grundschutz	○ „Passwörter, die leicht zu erraten sind oder in gängigen **Passwortlisten** geführt werden, DÜRFEN NICHT verwendet werden.“ ○ „Es MÜSSEN Maßnahmen ergriffen werden, um die **Kompromittierung** von Passwörtern zu erkennen.“ ○ IT-Systeme oder Anwendungen SOLLTEN NUR mit einem validen Grund zum **Wechsel** des Passworts auffordern.
DORA	“die Nutzung von Authentifizierungsmethoden ist der gemäß Artikel 8…dem Gesamtrisikoprofil der IKT-Assets angemessen und **trägt führenden Praktiken** Rechnung…”
NIS2	“…Unter dem Begriff „Cyberhygiene“…werden verschiedene grundlegenden Verfahren…umschrieben, welche…zu einer Verbesserung des Cybersicherheitsniveaus… führen können. Dies beinhaltet beispielsweise ein Patchmanagement, **Regelungen für sichere Passwörter**…”

Ist die Sicherheit der Kennwörter in Ihrer AD in den letzten 6 Monaten ein Thema innerhalb Ihrer Organisation gewesen?

1) JA
2) NEIN
3) Möchte ich nicht beantworten



Outpost24

Mark as incident | Mark as favorite | Mark as unread | Delete threat | Comments · 0

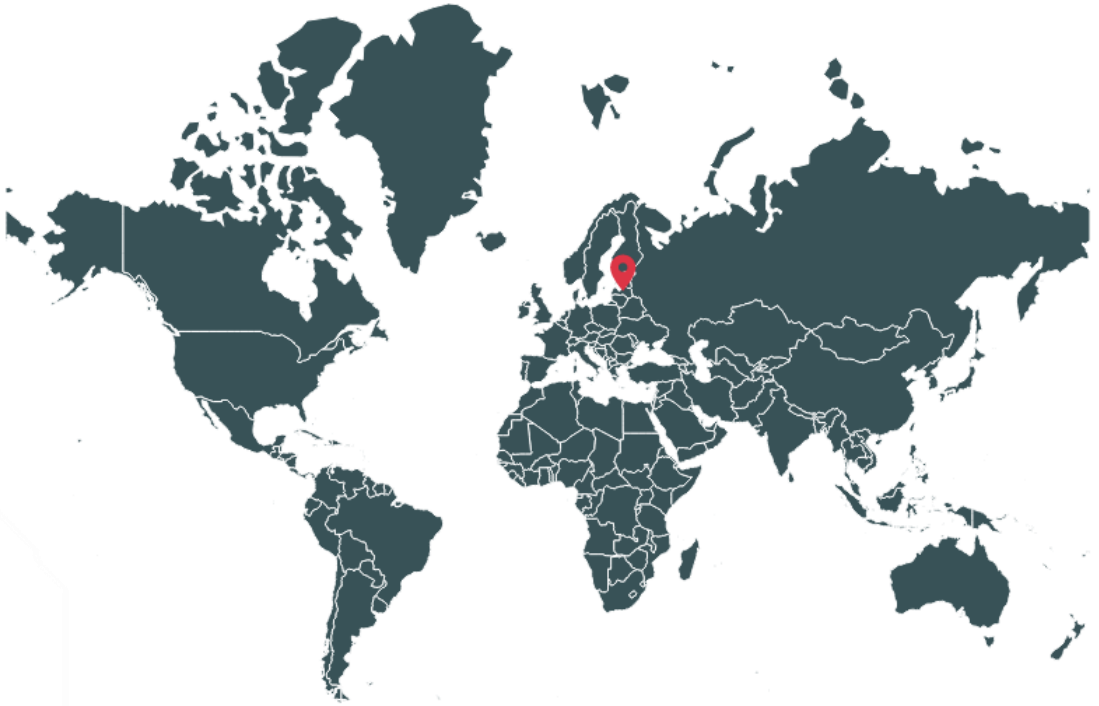
RATING	★★★☆☆	CREDENTIAL TYPE	Botnet
USERNAME	[redacted]	CLASSIFICATION	UNCLASSIFIED
PASSWORD	meinpasswort	IS EMAIL	
BOTNET TYPE	REDLINE	UPDATED AT	20/3/2024 15:26h
AFFECTED URL	https://www.amazon.de/ap/signin	REPORTED AT	11/3/2024 07:00h
LABELS	Botnet Credentials, Clear Password, [redacted], First Data Load, POC Corp_BotCred	BREACHED AT	28/6/2021 02:00h

Report Email

More Info

28/6/2021 02:00h - Helsinki, Finland

LOCATION	Helsinki, Finland
LATITUDE	60.1719
LONGITUDE	24.9347
BREACHED AT	28/6/2021 02:00h



Outpost24

Mark as incident | Mark as favorite | Mark as unread | Delete threat | Comments · 0

RATING	★★★☆☆	CREDENTIAL TYPE	Botnet
USERNAME	[redacted]	CLASSIFICATION	UNCLASSIFIED
PASSWORD	FG e34h01976	IS EMAIL	−
BOTNET TYPE	RISEPRO	UPDATED AT	20/3/2024 15:27h
AFFECTED URL	https://login.microsoftonline.co...	REPORTED AT	15/3/2024 01:38h
LABELS	Botnet Credentials, Clear Password, [redacted], First Data Load, POC Corp_BotCred	BREACHED AT	25/2/2024 15:17h

Report Email

More Info

25/2/2024 15:17h - Mahdia, Tunisia

LOCATION	Mahdia, Tunisia
LATITUDE	35.5051
LONGITUDE	11.0628
BREACHED AT	25/2/2024 15:17h

Mark as incident | Mark as favorite | Mark as unread | Delete threat | Comments · 0

RATING	★★★☆☆	CREDENTIAL TYPE	Botnet
USERNAME	[redacted]	CLASSIFICATION	UNCLASSIFIED
PASSWORD	Maandag$05	IS EMAIL	−
BOTNET TYPE	META	UPDATED AT	20/3/2024 15:26h
AFFECTED URL	https://adfs.[redacted]	REPORTED AT	8/2/2024 17:56h
LABELS	Botnet Credentials, Clear Password, [redacted], First Data Load, POC Corp_BotCred	BREACHED AT	24/1/2023 01:00h

Report Email

More Info

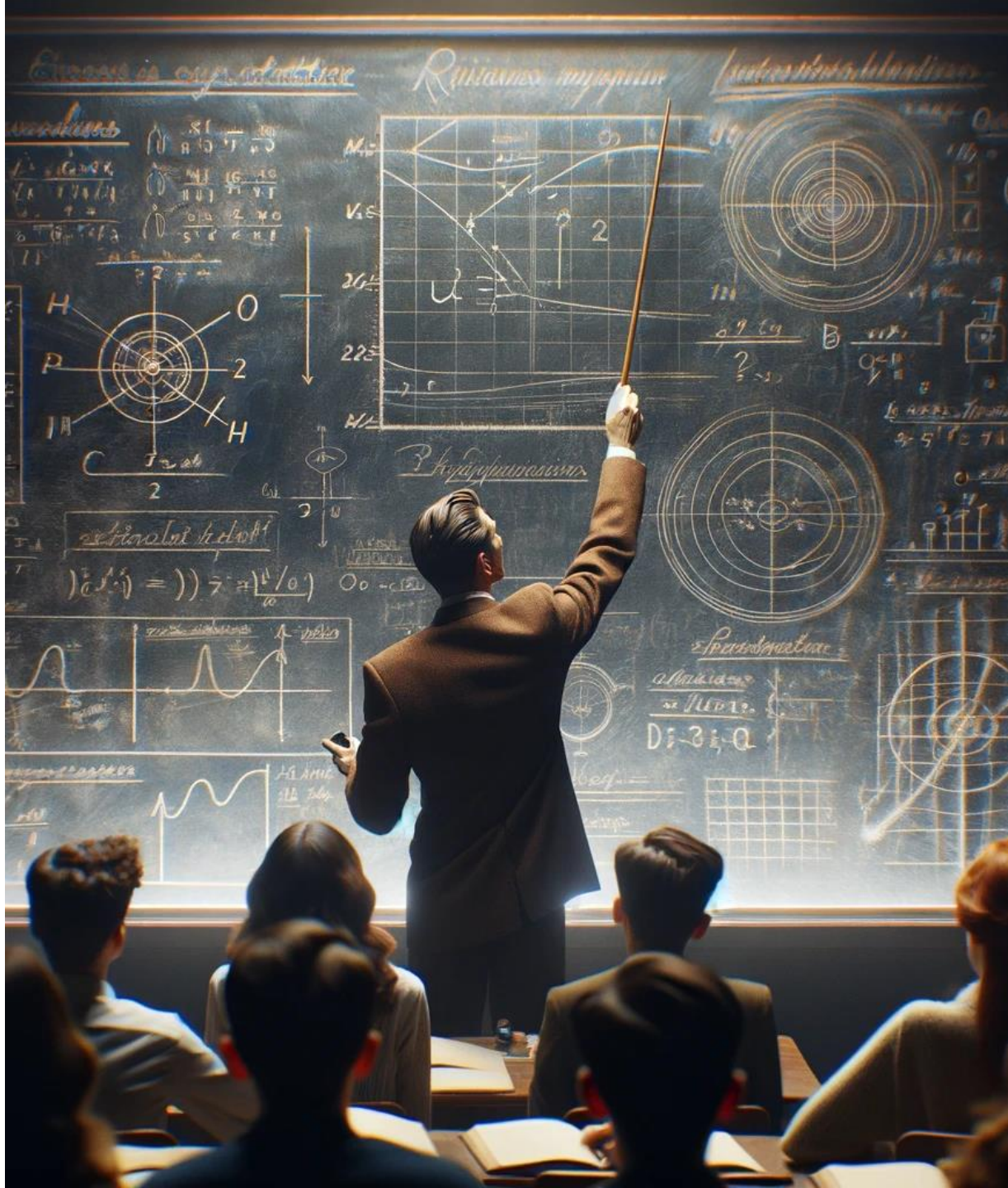
24/1/2023 01:00h - Putten, The Netherlands

LOCATION	Putten, The Netherlands
LATITUDE	52.2517
LONGITUDE	5.5872
BREACHED AT	24/1/2023 01:00h

Outpost24

Empfehlungen für starke Passwörter

- Passwörter müssen lang sein – Führen Sie Passphrasen ein!
- Passwörter brauchen nicht komplex zu sein!
- Privilegierte Konten mindestens 15 Zeichen!
- Validieren Sie Kennwörter gegen Listen mit kompromittierten Passwörtern!
- Blockieren Sie einfach zu erratenen Kennwörter durch Wortlisten!
- Unterschiedliche Regeln für Standard- und Admin Accounts!
- Lassen Sie Passwörter ablaufen!



Outpost24

Specops Password Auditor

Outpost24

Specops Password Policy

Outpost24

Fragen & Antworten

Outpost24

Vielen Dank für Ihre Aufmerksamkeit

Für weitere Fragen zum Thema: https://specopssoft.com/de/

E-Mail: stephan.halbmeier@outpost24.com

LinkedIn: https://www.linkedin.com/in/stephanhalbmeier

Outpost24