# So schützen Sie Ihren Helpdesk wirkungsvoll vor modernen Social Engineering Angriffen

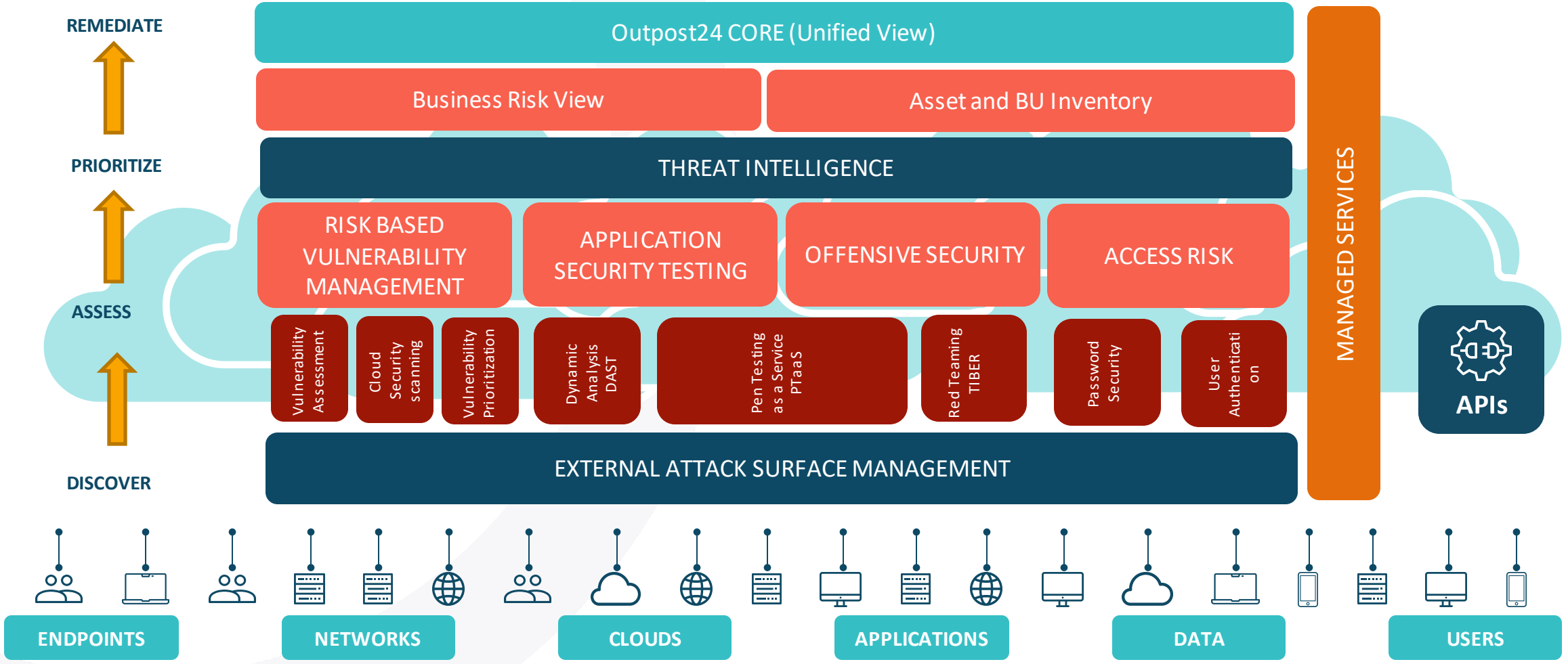
Stephan Halbmeier
Product Specialist | Outpost24

Patrick Lehnis
Marketing Manager DACH | Outpost24

Outpost24

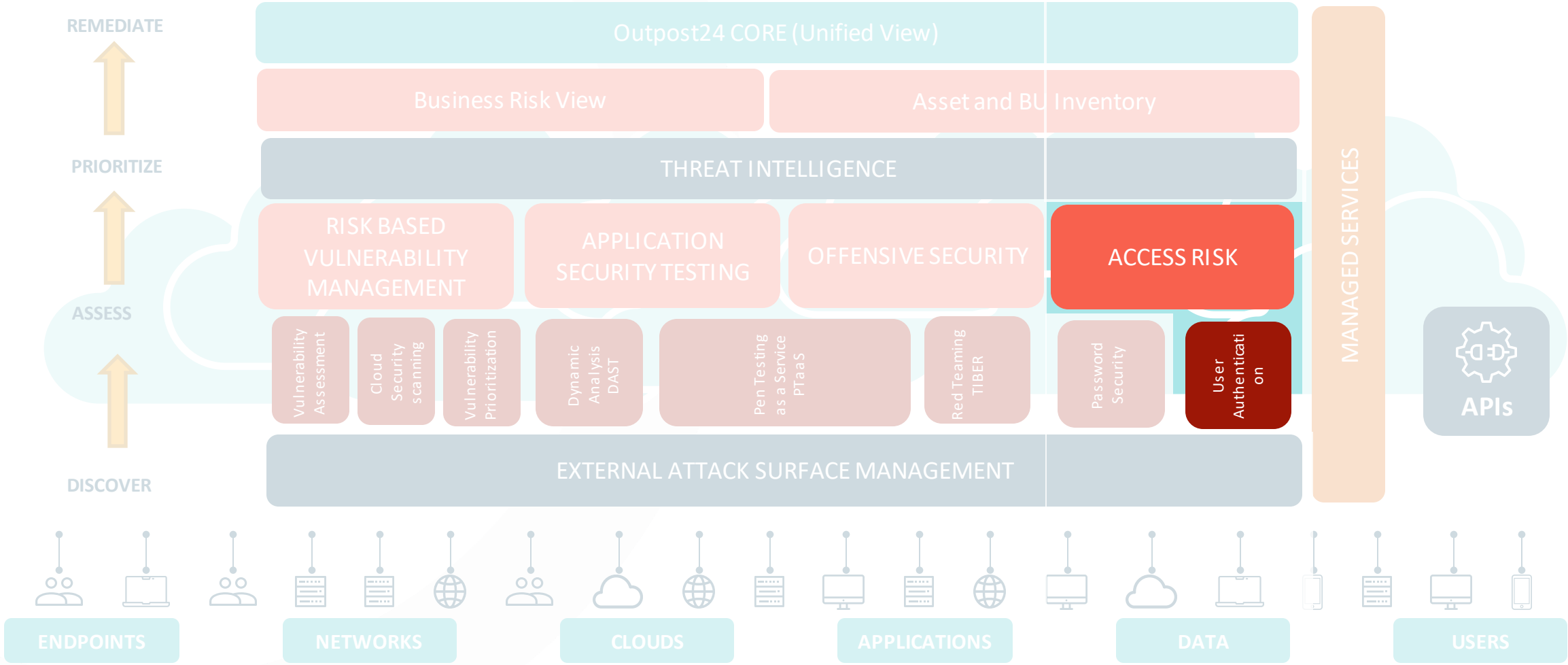

TWIX
Raider
Raider

# OUTPOST24 CYBERSECURITY PLATTFORM ÜBERSICHT




Outpost24

# OUTPOST24 CYBERSECURITY PLATTFORM ÜBERSICHT




Outpost24

***Social Engineering*** *beschreibt die Beeinflussung von Menschen mit dem Ziel, sie zu bestimmten Verhaltensweisen, Preisgabe von vertraulichen Informationen, dem Missachten von Prozessen oder Umgehen von Schutzmaßnahmen zu bewegen.*

Outpost24

ACTORS

# Jia Tan

Report | Export | Back to list

| | | | |
|---|---|---|---|
| ORIGIN | - | STATUS | Active |
| FIRST SEEN | 26/01/2021 | TYPES | nation-state |
| LAST SEEN | 22/04/2024 | SOPHISTICATION | strategic |
| TLP | | | |

Description | Indicators(9) | Campaigns(0) | Tools(0) | CVEs(1) | Attack Patterns(13) | Signatures(0) | Targets(0)

## Aliases

- Jia Tan
- Hans Jansen
- Dennis Ens
- Jigar Kumar
- JiaT75
- Jia Cheong Tan

## Key points

- "*Jia Tan*" is the alias of the GitHub user responsible of implanting a backdoor in XZ Utils package (CVE-2024-3094).
- The attacker performed a highly sophisticated social engineering scheme, which allegedly include the use of other fake identities to pressure and persuade XZ Utils project maintainer to gain control of the project.
- Cybersecurity community speculated that *Jia Tan* could be a fake persona operated by an unknown state-sponsored group.

## Assessment

"*Jia Tan*" and "*Jia Cheong Tan*" are the alias of the GitHub user "*@JiaT75*"[1] the attacker allegedly responsible of implanting a backdoor in XZ Utils package [2] [3].

*Jia Tan* created a GitHub account in January 2021 and the adversary first activity in the platform was tracked back to October of the same year. Since February 2022 the attacker performed a highly sophisticated social engineering scheme, which allegedly include the use of other fake identities "*Jigar Kumar*", "*Hans Jansen*" and "*Dennis Ens*" to pressure and

# 0ktapus

Report | Export | Back to list

| | | | |
|---|---|---|---|
| **ORIGIN** | United States | **STATUS** | Active |
| **FIRST SEEN** | 20/07/2022 | **TYPES** | crime-syndicate |
| **LAST SEEN** | 26/02/2024 | **SOPHISTICATION** | advanced |
| **TLP** | | | |

# Description | Indicators(340) | Campaigns(1) | Tools(28) | CVEs(2) | Attack Patterns(55) | Signatures(0) | Targets(59)

## Aliases

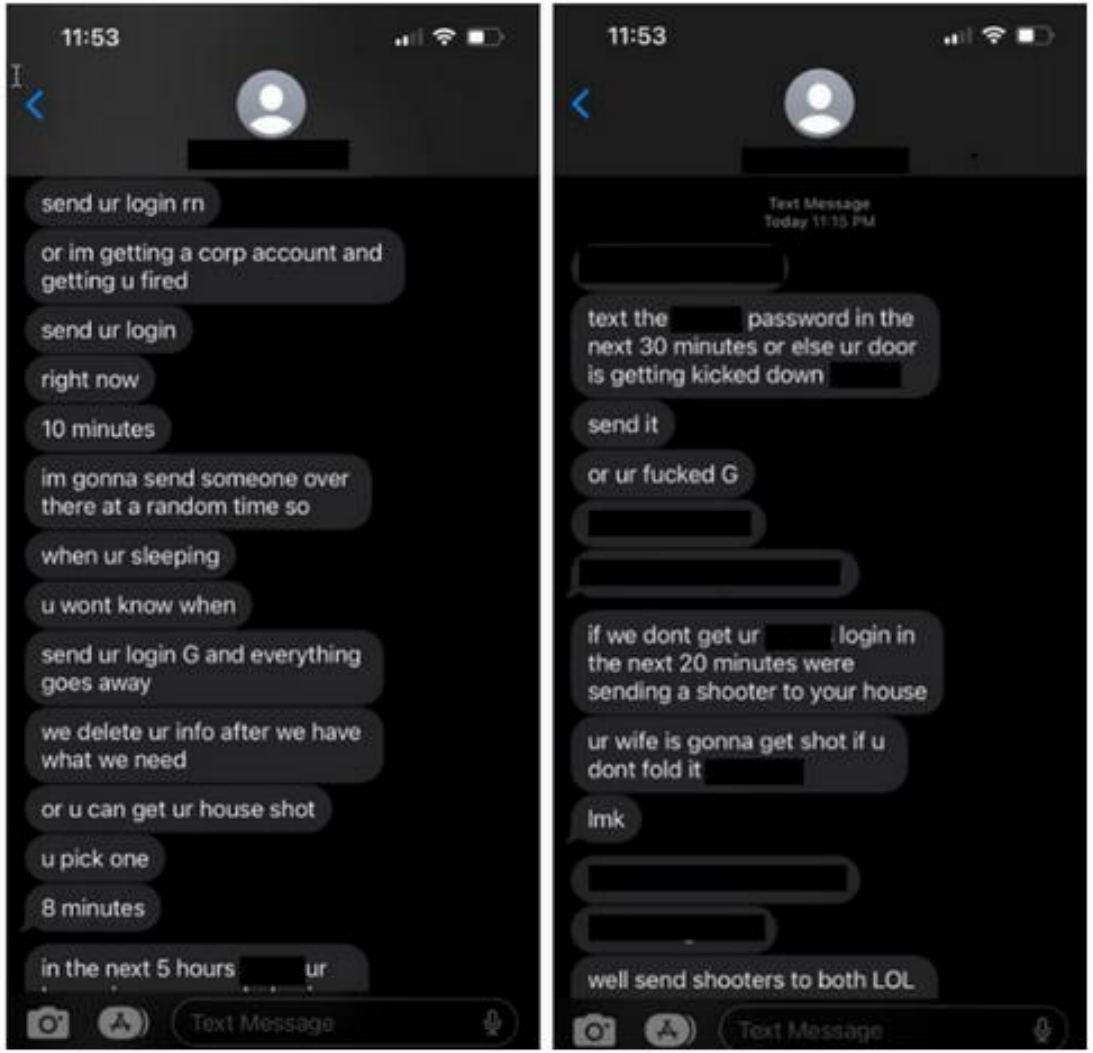
- Storm-0875
- Scatter Swine
- 0ktapus
- Oktapus
- SCATTERED SPIDER
- UNC3944
- Roasted 0ktapus
- ScatteredSpider
- Muddled Libra
- GOLD HARVEST
- LUCR-3
- Starfraud
- Octo Tempest
- Sosa
- Elijah
- King Bob
- Anthony Ramirez
- Noah Michael Urban

## Key points

- "*0ktapus*" is a financially-motivated threat actor targeting technology companies, telecommunications providers, and business process outsourcing (BPO) companies.
- The threat actor performs large smishing campaigns, social engineering, or vulnerability exploitation, and either directs victims to a credential harvesting site or directs them to run commercial remote monitoring and management (RMM) tools.
- *0ktapus* goal is compromising corporate credentials to conduct further supply-chain attacks or ransomware deployment by authenticating and gaining unauthorized access to any enterprise resources the victims have access to.
- The adversary is an affiliate of "*BlackCat*" ransomware operation. Furthermore, 0ktapus is related to an underground community of young English-speaking cyber criminals called "*The Comm*".

# 0ktapus (Octo Tempest)

Microsoft analysts have detected that this threat actor which they dubbed "Octo Tempest" has also been impersonating newly hired employees in their attempts to blend into normal on-hire processes.
Researchers have also detected, in rare instances, Octo Tempest using fear-mongering tactics, targeting specific individuals through phone calls and texts.




*Source: Microsoft Security*[8]

Outpost24


INSIDE
POLICE

# Ablauf Anrufer Verifizierung Secure Service Desk


1

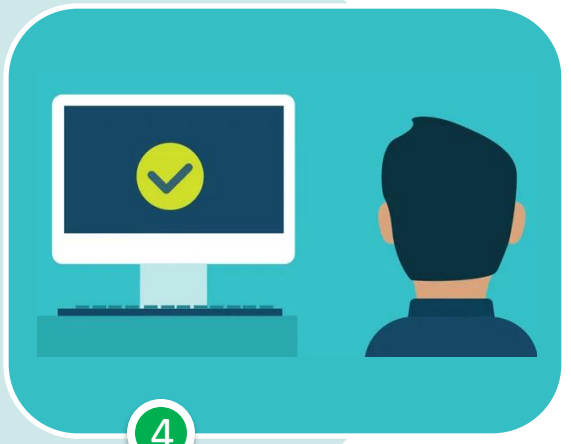
Anruf


2

Challenge


3

Response



4

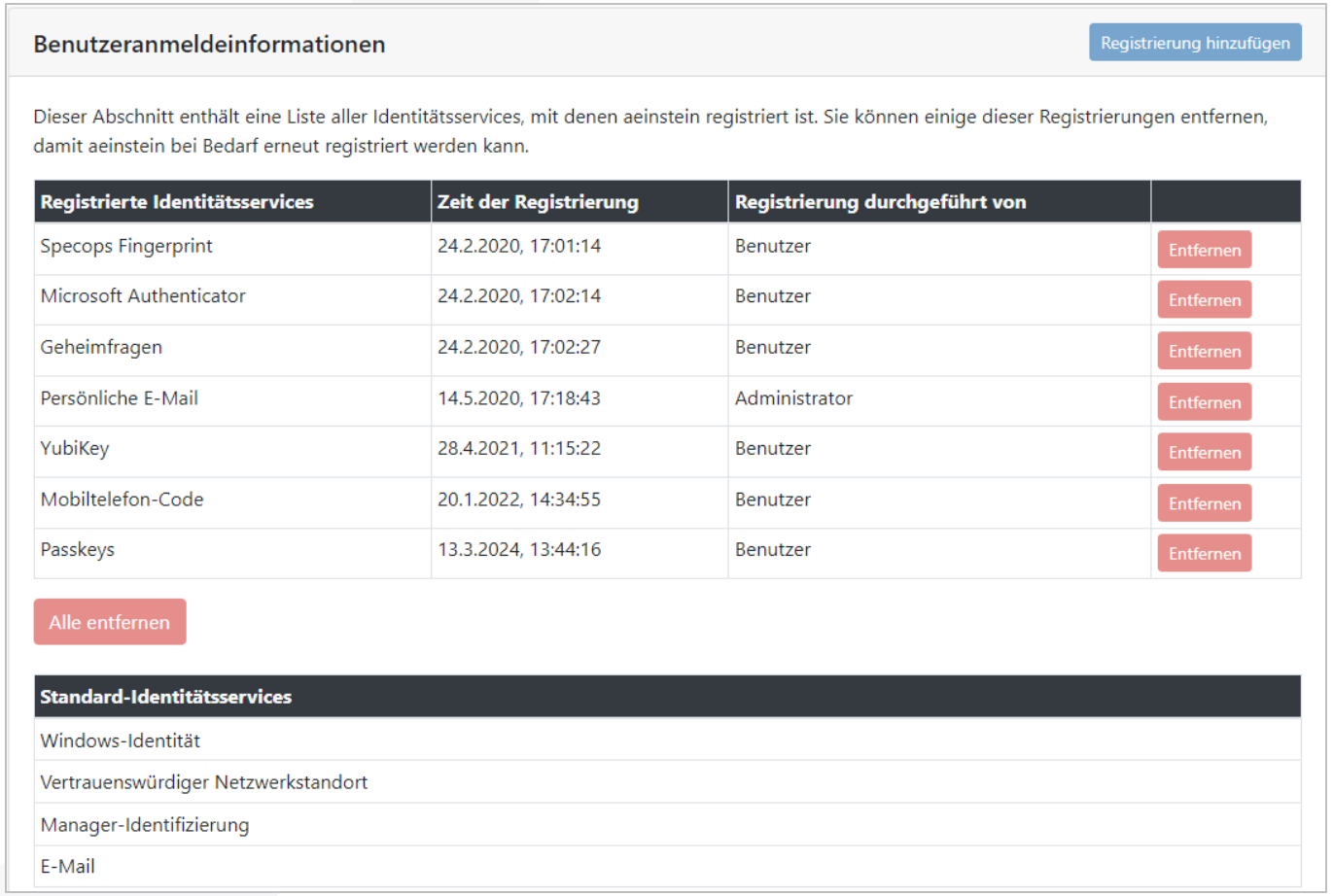
Freigabe

Outpost24

# Demo:
# Anruferverifizierung durch Specops Secure Service Desk

Outpost24

# Ausgangssituation: User hat sich für MFA registriert



**Benutzeranmeldeinformationen**

Registrierung hinzufügen

Dieser Abschnitt enthält eine Liste aller Identitätsservices, mit denen aeinstein registriert ist. Sie können einige dieser Registrierungen entfernen, damit aeinstein bei Bedarf erneut registriert werden kann.

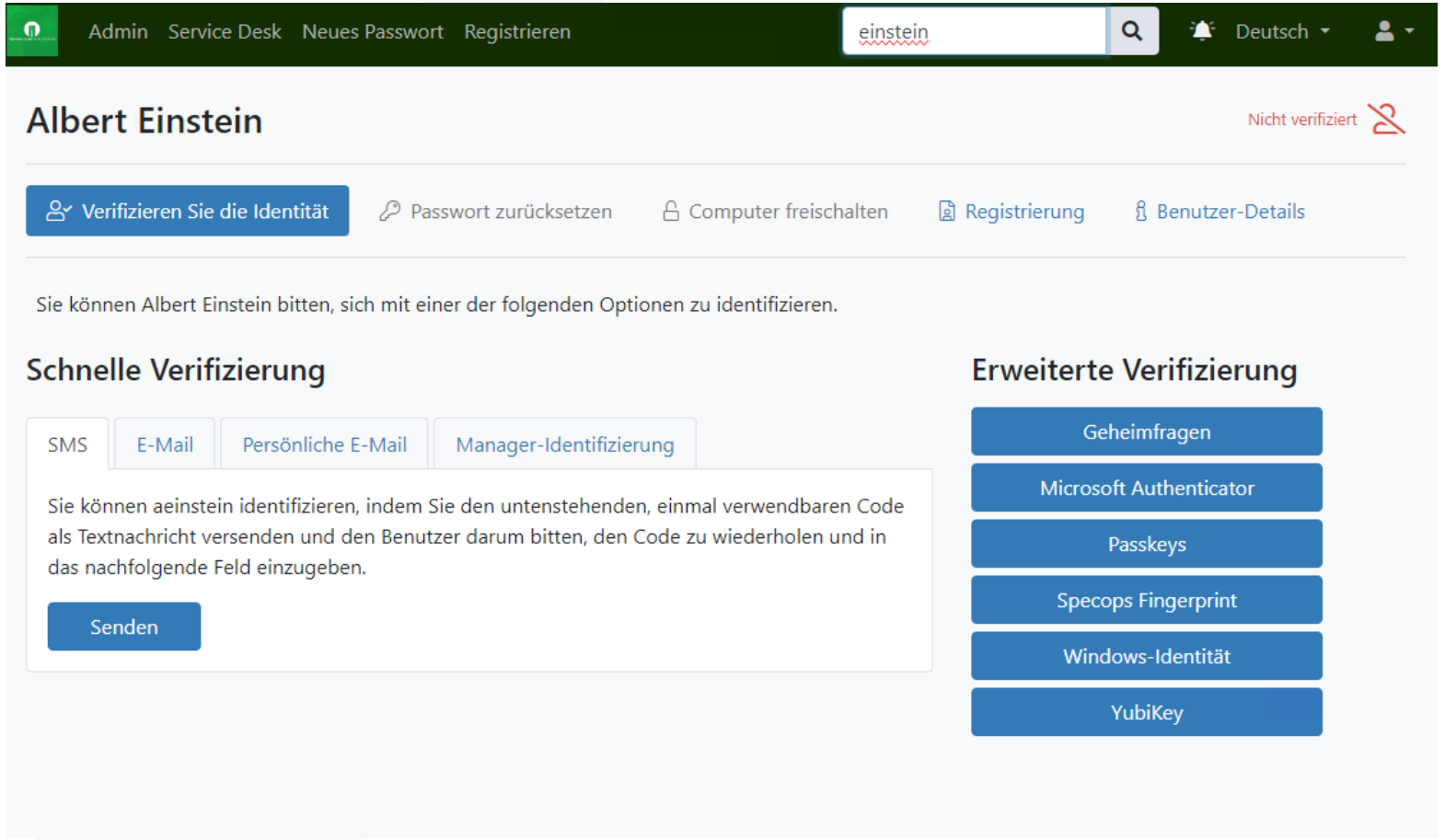
| Registrierte Identitätsservices | Zeit der Registrierung | Registrierung durchgeführt von | |
|---|---|---|---|
| Specops Fingerprint | 24.2.2020, 17:01:14 | Benutzer | Entfernen |
| Microsoft Authenticator | 24.2.2020, 17:02:14 | Benutzer | Entfernen |
| Geheimfragen | 24.2.2020, 17:02:27 | Benutzer | Entfernen |
| Persönliche E-Mail | 14.5.2020, 17:18:43 | Administrator | Entfernen |
| YubiKey | 28.4.2021, 11:15:22 | Benutzer | Entfernen |
| Mobiltelefon-Code | 20.1.2022, 14:34:55 | Benutzer | Entfernen |
| Passkeys | 13.3.2024, 13:44:16 | Benutzer | Entfernen |

Alle entfernen

| Standard-Identitätsservices |
|---|
| Windows-Identität |
| Vertrauenswürdiger Netzwerkstandort |
| Manager-Identifizierung |
| E-Mail |

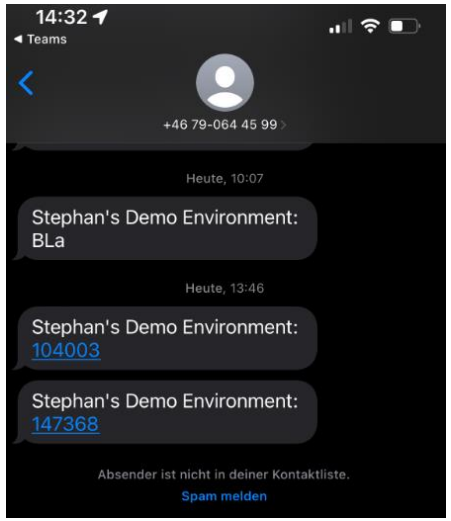
Outpost24

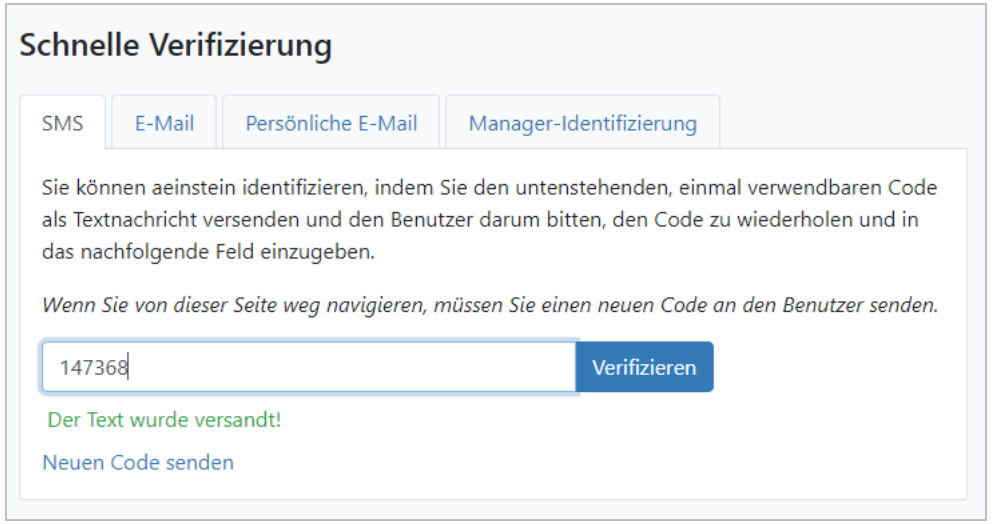
# Verifizierung über SMS durch den ServiceDesk 1/2

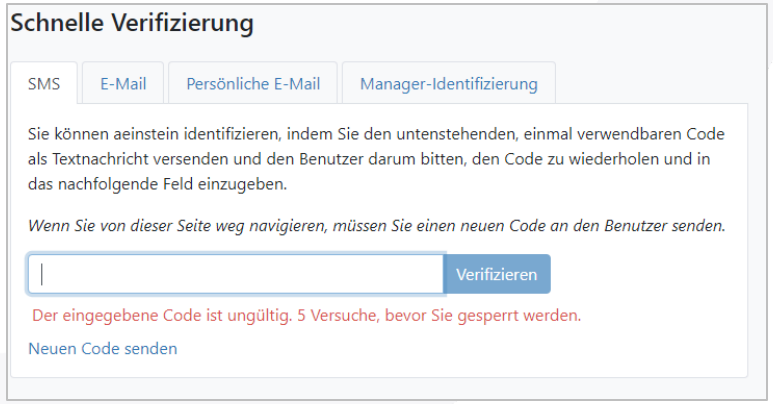


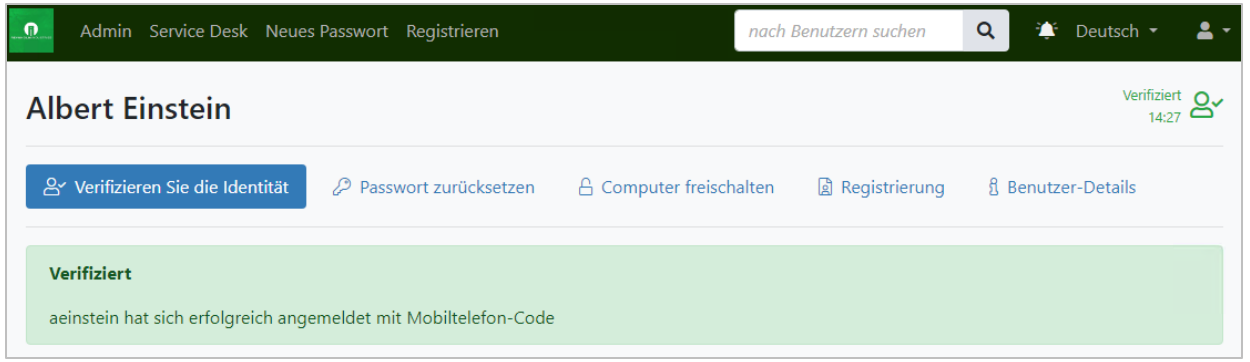

Outpost24

# Verifizierung über SMS durch den ServiceDesk 2/2



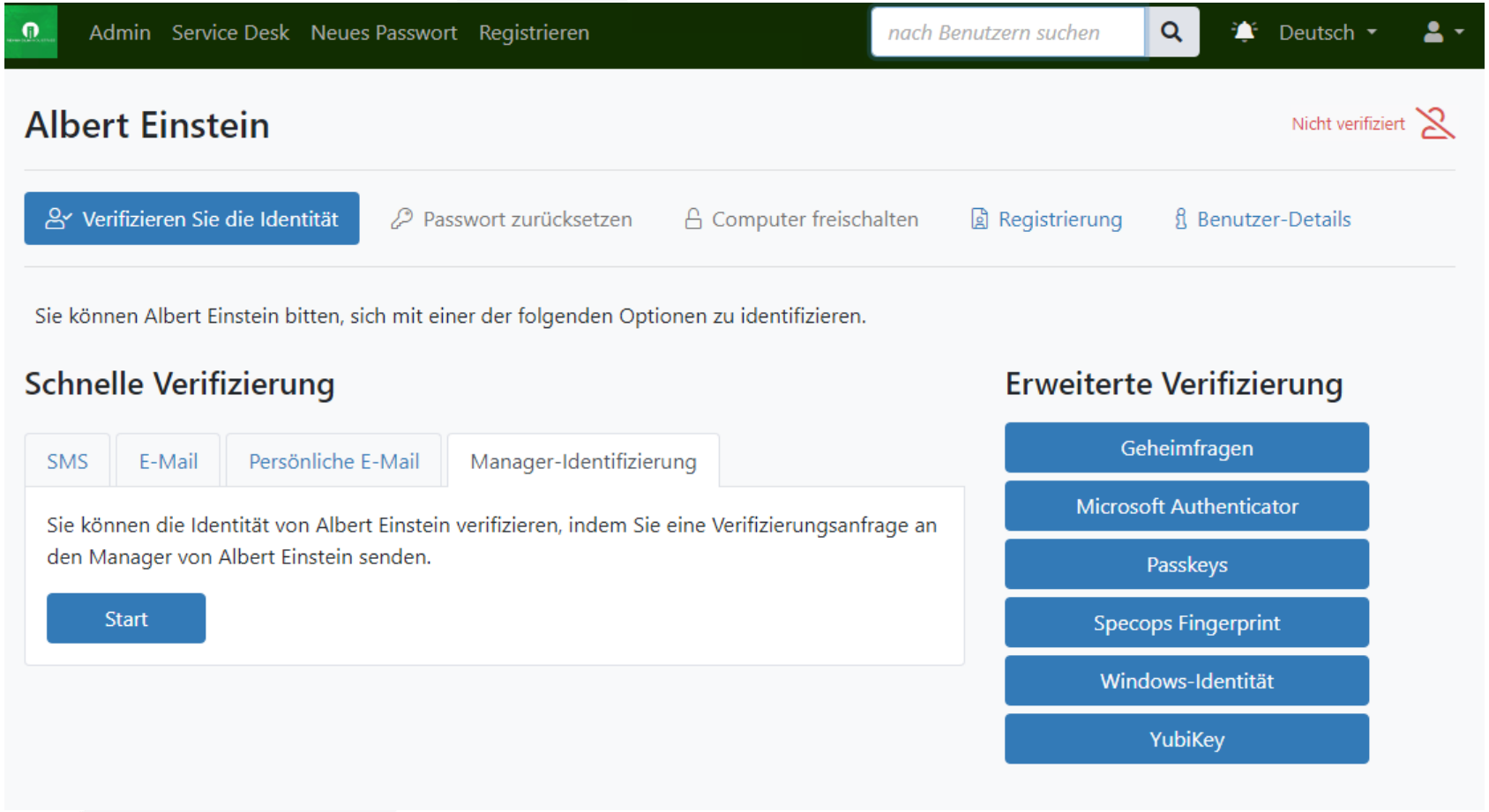



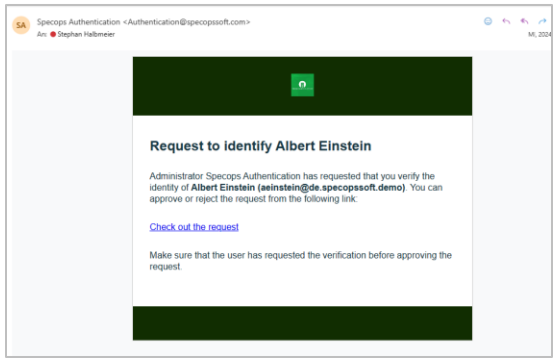

Outpost24

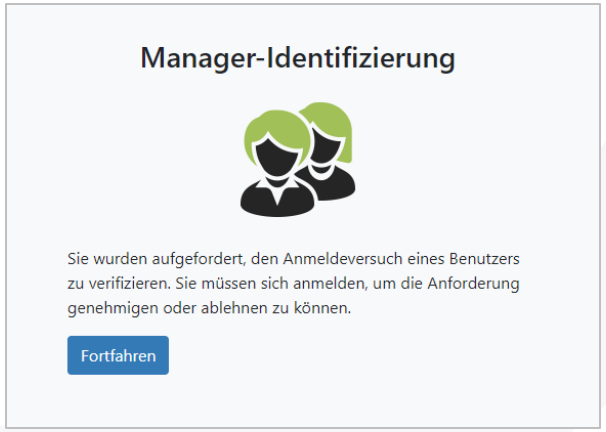
# Verifizierung über Vorgesetzten durch ServiceDesk 1/2

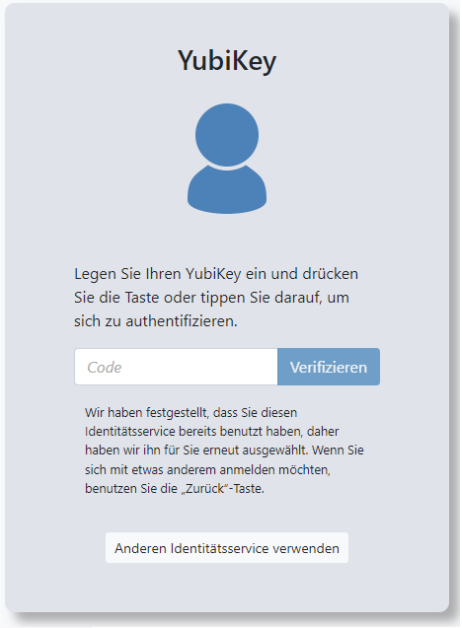


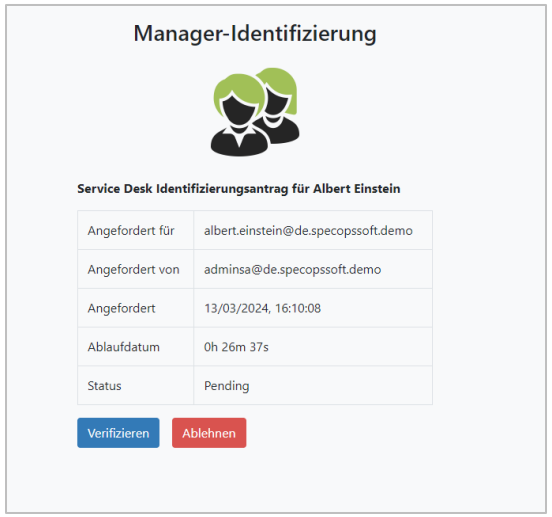

Outpost24

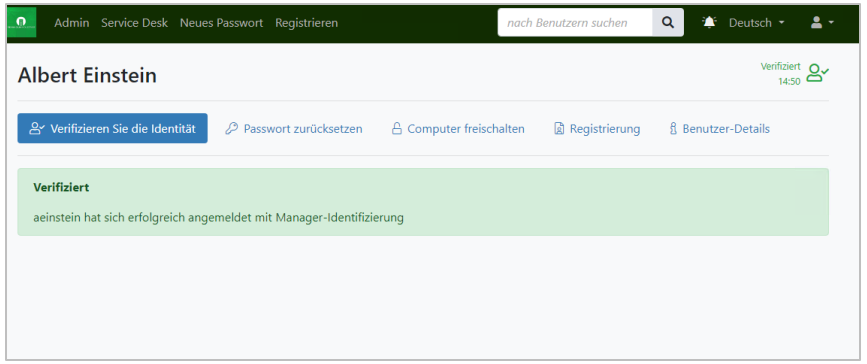
# Verifizierung über Vorgesetzten durch ServiceDesk 2/2




Outpost24

# Vielen Dank für Ihre Aufmerksamkeit

Für weitere Fragen zum Thema: https://outpost24.com/de/

E-Mail: stephan.halbmeier@outpost24.com

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

Outpost24