

So schützen Sie Ihren Helpdesk wirkungsvoll vor modernen Social Engineering Angriffen



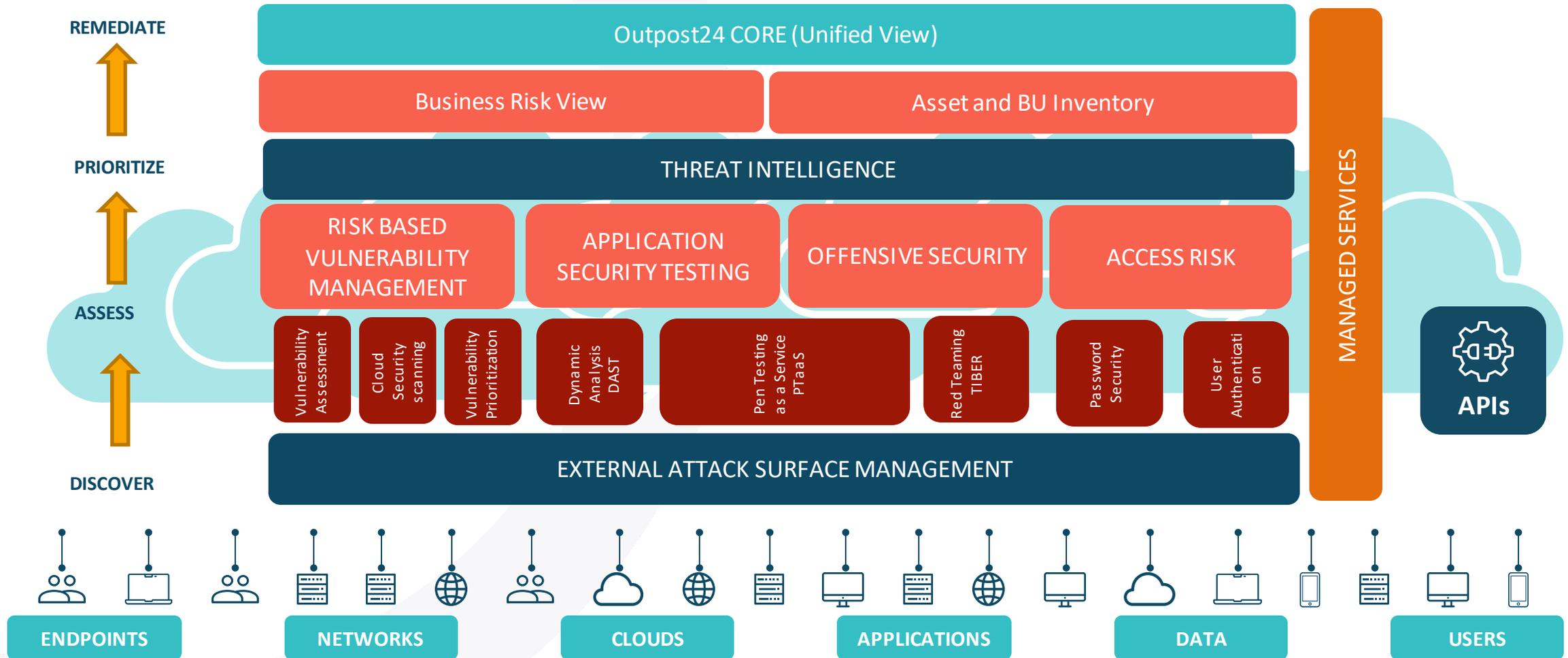
Stephan Halbmeier
Product Specialist | Outpost24



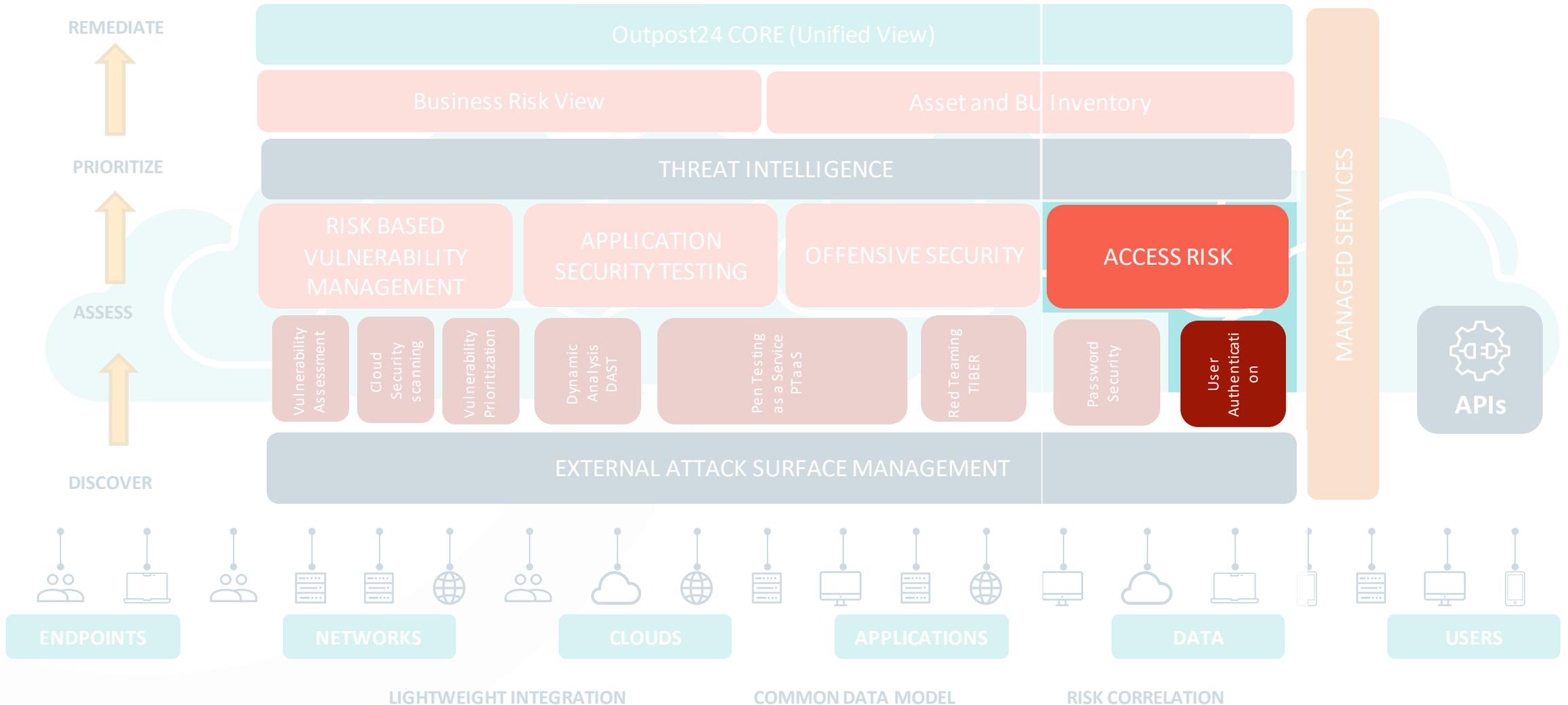
Patrick Lehnis
Marketing Manager DACH | Outpost24



OUTPOST24 CYBERSECURITY PLATTFORM ÜBERSICHT



OUTPOST24 CYBERSECURITY PLATTFORM ÜBERSICHT



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.



 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





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

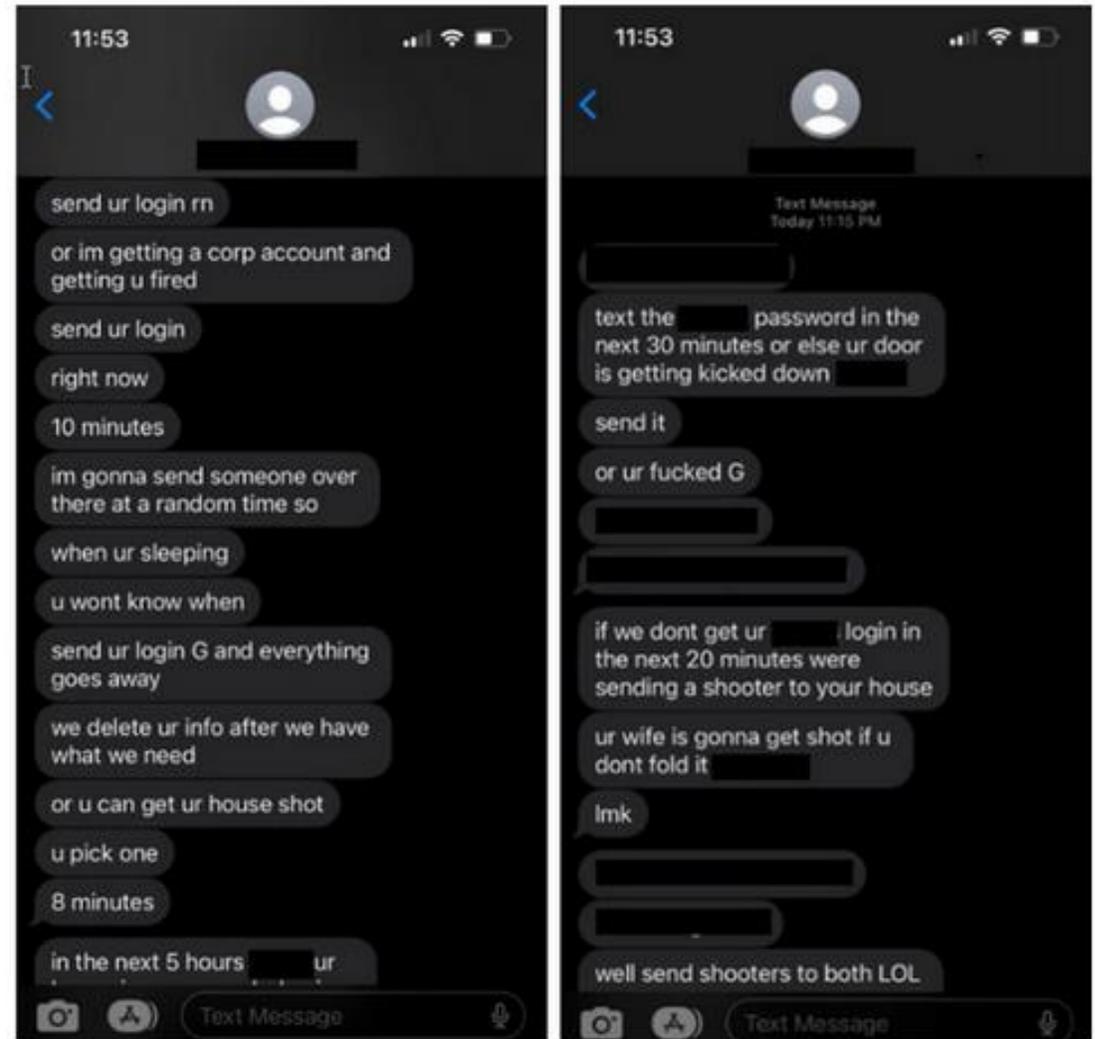
Key points

- "*Oktapus*" 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.
- *Oktapus* 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, Oktapus is related to an underground community of young English-speaking cyber criminals called "*The Comm*".

Oktapus (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]



Velket

INSIDE

POLICE

Ablauf Anrufer Verifizierung Secure Service Desk



1

Anruf



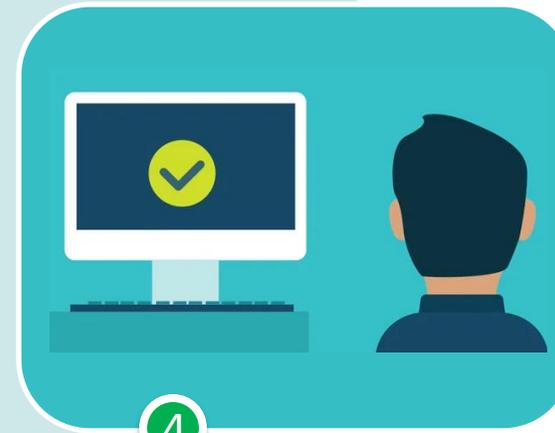
2

Challenge



3

Response



4

Freigabe



Demo:
Anruferverifizierung durch
Specops Secure Service Desk

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

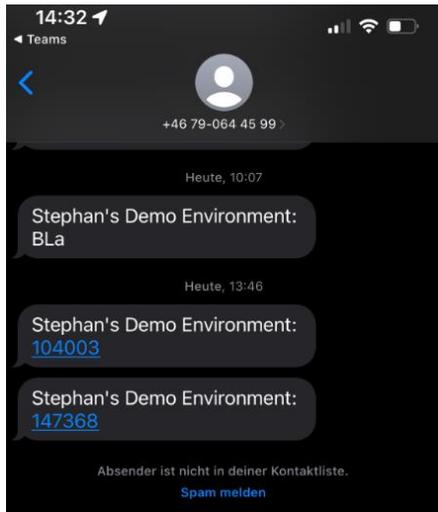
Standard-Identitätsservices

- Windows-Identität
- Vertrauenswürdiger Netzwerkstandort
- Manager-Identifizierung
- E-Mail

Verifizierung über SMS durch den ServiceDesk 1/2

The screenshot shows a user verification interface for 'Albert Einstein'. At the top, there is a navigation bar with links for 'Admin', 'Service Desk', 'Neues Passwort', and 'Registrieren'. A search bar contains the text 'einstein'. The user's name 'Albert Einstein' is displayed, along with a status 'Nicht verifiziert' and a red lock icon. Below this, there are several action buttons: 'Verifizieren Sie die Identität' (highlighted in blue), 'Passwort zurücksetzen', 'Computer freischalten', 'Registrierung', and 'Benutzer-Details'. A message states: 'Sie können Albert Einstein bitten, sich mit einer der folgenden Optionen zu identifizieren.' Under the heading 'Schnelle Verifizierung', there are four tabs: 'SMS' (selected), 'E-Mail', 'Persönliche E-Mail', and 'Manager-Identifizierung'. A text box explains: 'Sie können aeinstein identifizieren, indem Sie den untenstehenden, einmal verwendbaren Code als Textnachricht versenden und den Benutzer darum bitten, den Code zu wiederholen und in das nachfolgende Feld einzugeben.' Below this is a 'Senden' button. On the right, under 'Erweiterte Verifizierung', there are six blue buttons: 'Geheimfragen', 'Microsoft Authenticator', 'Passkeys', 'Specops Fingerprint', 'Windows-Identität', and 'YubiKey'.

Verifizierung über SMS durch den ServiceDesk 2/2



Schnelle Verifizierung

SMS E-Mail Persönliche E-Mail Manager-Identifizierung

Sie können aeinstein identifizieren, indem Sie den untenstehenden, einmal verwendbaren Code als Textnachricht versenden und den Benutzer darum bitten, den Code zu wiederholen und in das nachfolgende Feld einzugeben.

Wenn Sie von dieser Seite weg navigieren, müssen Sie einen neuen Code an den Benutzer senden.

Der Text wurde versandt!
Neuen Code senden



Schnelle Verifizierung

SMS E-Mail Persönliche E-Mail Manager-Identifizierung

Sie können aeinstein identifizieren, indem Sie den untenstehenden, einmal verwendbaren Code als Textnachricht versenden und den Benutzer darum bitten, den Code zu wiederholen und in das nachfolgende Feld einzugeben.

Wenn Sie von dieser Seite weg navigieren, müssen Sie einen neuen Code an den Benutzer senden.

Der eingegebene Code ist ungültig. 5 Versuche, bevor Sie gesperrt werden.
Neuen Code senden



Admin Service Desk Neues Passwort Registrieren nach Benutzern suchen Deutsch

Albert Einstein

Verifiziert 14:27

Verifizieren Sie die Identität Passwort zurücksetzen Computer freischalten Registrierung Benutzer-Details

Verifiziert
aeinstein hat sich erfolgreich angemeldet mit Mobiltelefon-Code

Verifizierung über Vorgesetzten durch ServiceDesk 1/2

The screenshot shows the ServiceDesk interface for a user named Albert Einstein. The user's status is 'Nicht verifiziert' (Not verified). The interface provides several options for verification and account management.

Navigation: Admin, Service Desk, Neues Passwort, Registrieren

Search: nach Benutzern suchen

Language: Deutsch

Albert Einstein

Nicht verifiziert

[Verifizieren Sie die Identität](#) [Passwort zurücksetzen](#) [Computer freischalten](#) [Registrierung](#) [Benutzer-Details](#)

Sie können Albert Einstein bitten, sich mit einer der folgenden Optionen zu identifizieren.

Schnelle Verifizierung

SMS | E-Mail | **Persönliche E-Mail** | Manager-Identifizierung

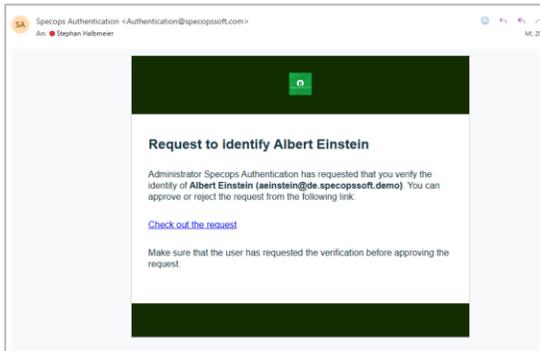
Sie können die Identität von Albert Einstein verifizieren, indem Sie eine Verifizierungsanfrage an den Manager von Albert Einstein senden.

[Start](#)

Erweiterte Verifizierung

- [Geheimfragen](#)
- [Microsoft Authenticator](#)
- [Passkeys](#)
- [Specops Fingerprint](#)
- [Windows-Identität](#)
- [YubiKey](#)

Verifizierung über Vorgesetzten durch ServiceDesk 2/2



Manager-Identifizierung



Sie wurden aufgefordert, den Anmeldeversuch eines Benutzers zu verifizieren. Sie müssen sich anmelden, um die Anforderung genehmigen oder ablehnen zu können.

[Fortfahren](#)



YubiKey



Legen Sie Ihren YubiKey ein und drücken Sie die Taste oder tippen Sie darauf, um sich zu authentifizieren.

Code [Verifizieren](#)

Wir haben festgestellt, dass Sie diesen Identitätsservice bereits benutzt haben, daher haben wir ihn für Sie erneut ausgewählt. Wenn Sie sich mit etwas anderem anmelden möchten, benutzen Sie die „Zurück“-Taste.

[Anderen Identitätsservice verwenden](#)



Manager-Identifizierung



Service Desk Identifizierungsantrag für Albert Einstein

Angefordert für	albert.einstein@de.specopsoft.demo
Angefordert von	admins@de.specopsoft.demo
Angefordert	13/03/2024, 16:10:08
Ablaufdatum	0h 26m 37s
Status	Pending

[Verifizieren](#) [Ablehnen](#)



Admin Service Desk Neues Passwort Registrieren Deutsch

Albert Einstein

Verifiziert 14:50

[Verifizieren Sie die Identität](#) [Passwort zurücksetzen](#) [Computer freischalten](#) [Registrierung](#) [Benutzer-Details](#)

Verifiziert

aeinstein hat sich erfolgreich angemeldet mit Manager-Identifizierung

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>

