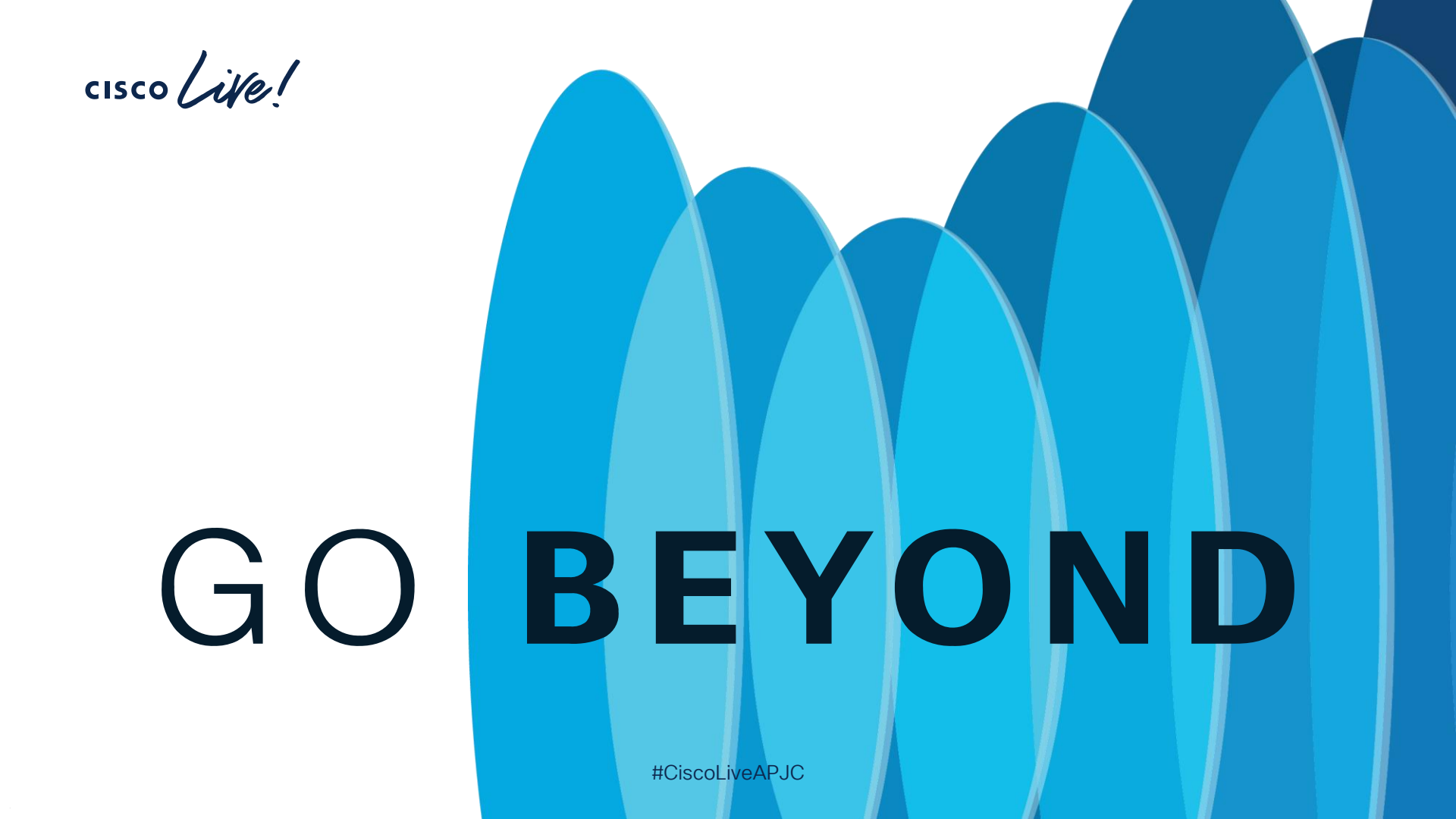

cisco Live!
GO BEYOND
#CiscoLiveAPJC

Stop Identity-Based Attacks and Enhance User Experience

Through Cisco Continuous Identity Security

Sheela Kishan, Solutions Engineer
sheelaknetwork (Linkedin)

BRKSEC-2233

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2233

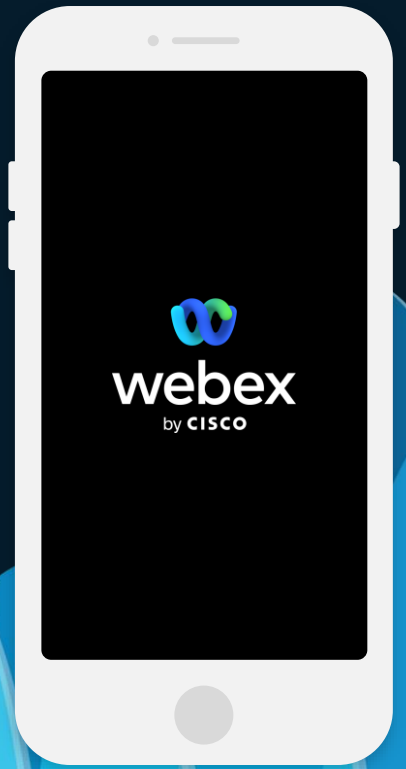
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

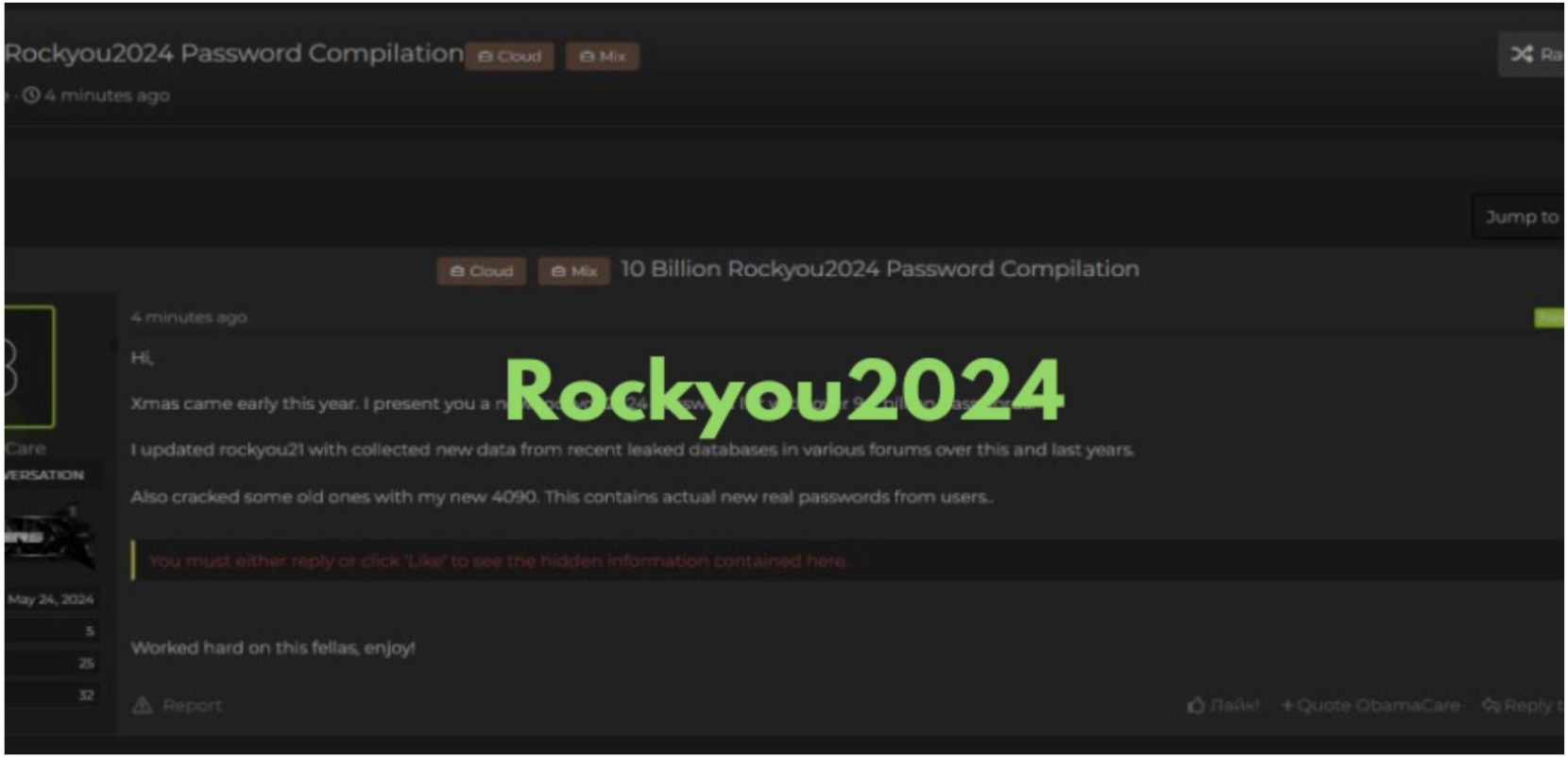
Are your password controls enough?

Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

RockYou2024: Massive Data Breach Exposes Nearly 10 Billion Passwords

Jul 9, 2024 *News*

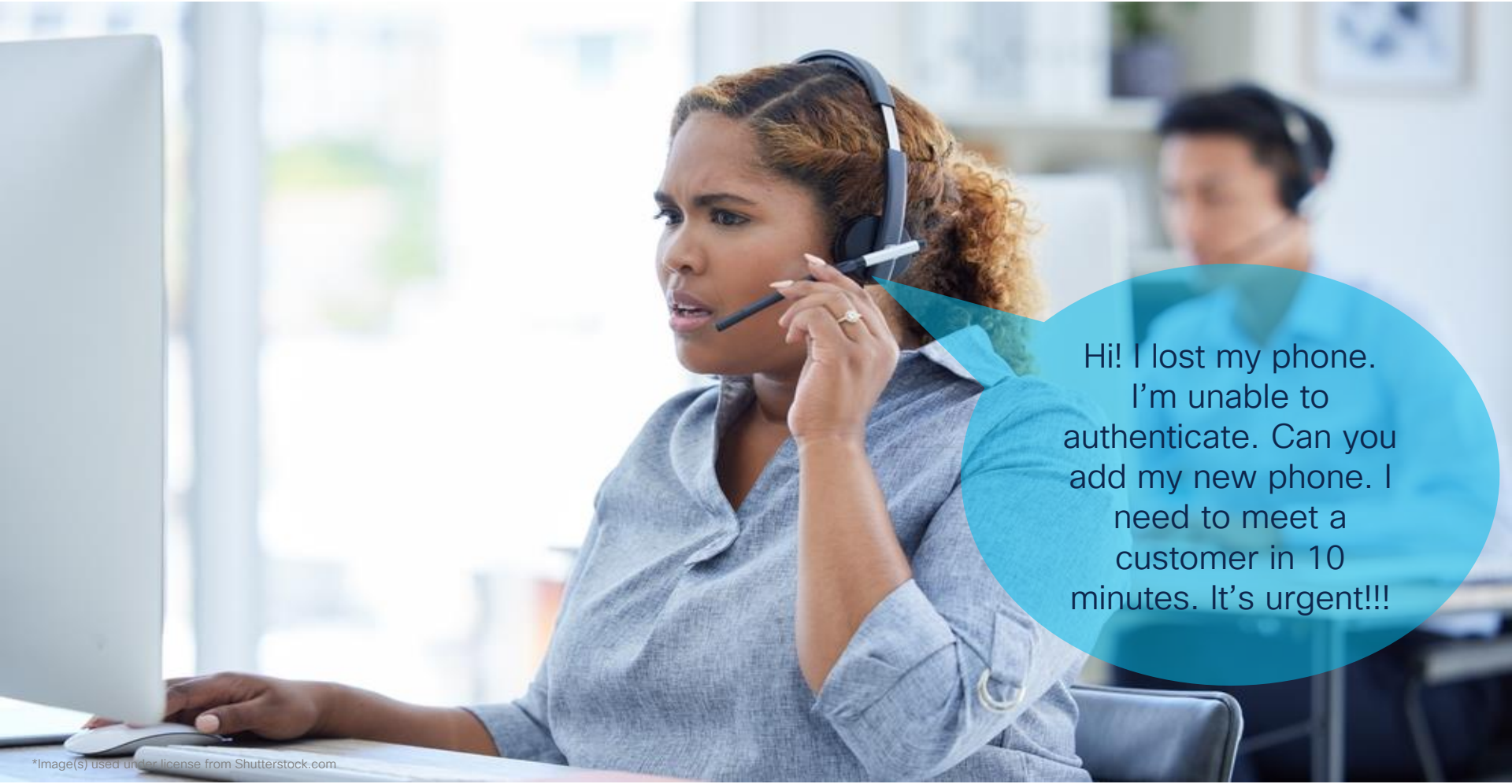


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

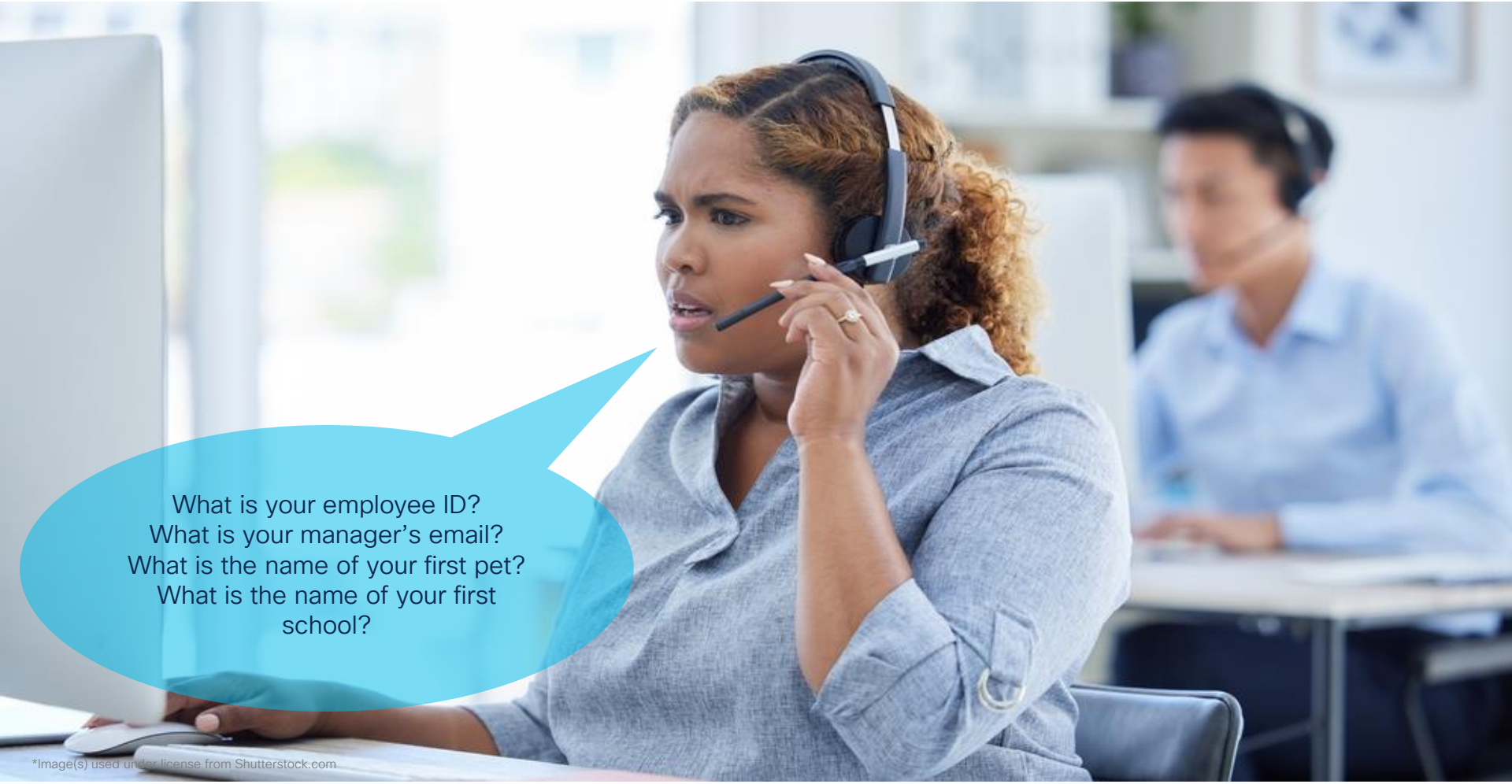
*Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



*Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



*Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity breaches

* Based on CyberArk Identity Security Threat Report 2024

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Challenges in Securing Identity
- Common Identity Attack Techniques
- Continuous Identity Security
- Key Takeaways

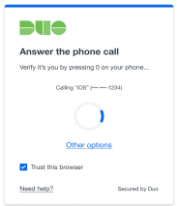
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Challenges in Security Identity

Evolution of authentication and attack tactics

Password tactics
- Password spray
- Brute force

MFA 1.0
- SMS
- Phone Callback



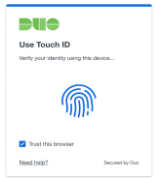
MFA bypass 1.0
- Telephony attacks
- Social engineering

MFA 2.0
- Mobile push
- App OTP

MFA bypass 2.0
- Push bombing
- Adversary-in-the-middle

Microsoft okta cisco

MFA 3.0
- WebAuthn
- Number matching



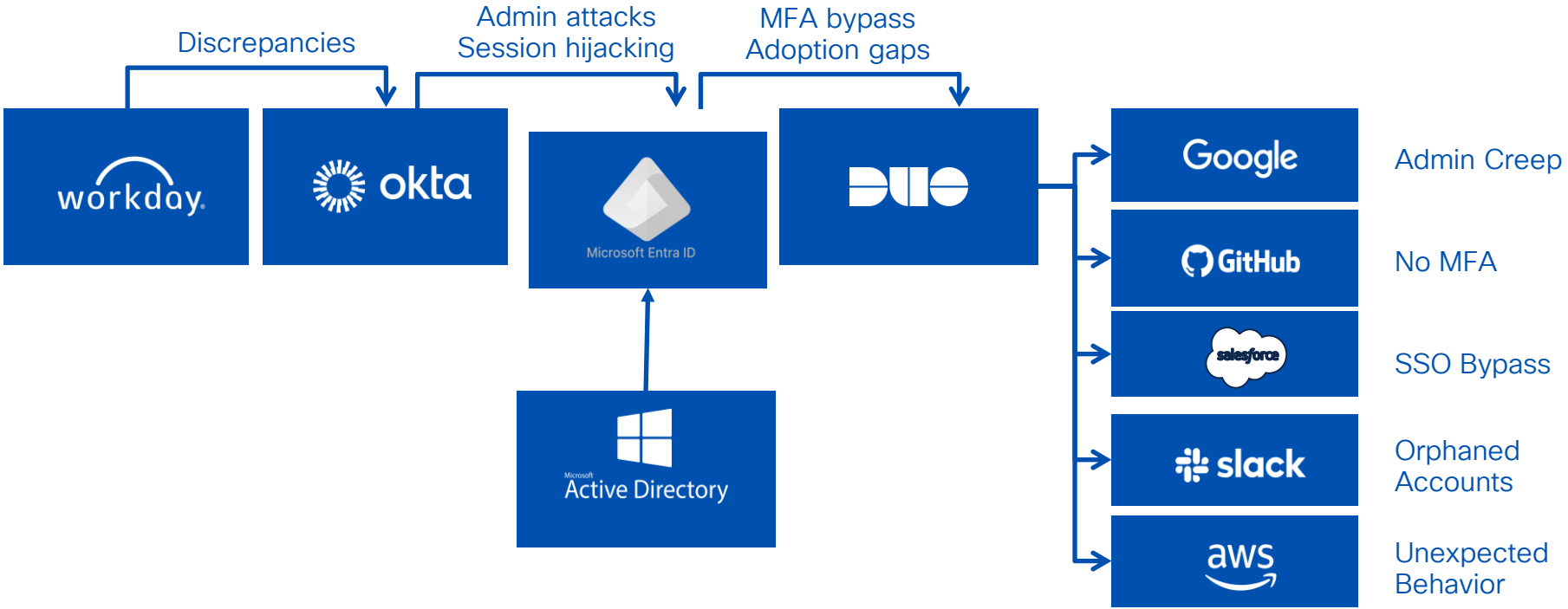
Next attack

?

?

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fragmented identity ecosystem



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

*Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Rise of machine identities

*Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

User Experience Matters

*Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Common Identity Attack Techniques

*Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scattered Spider* Attack Technique

Social engineering

Gain credentials / MFA code

Privilege escalation

Gains access to data

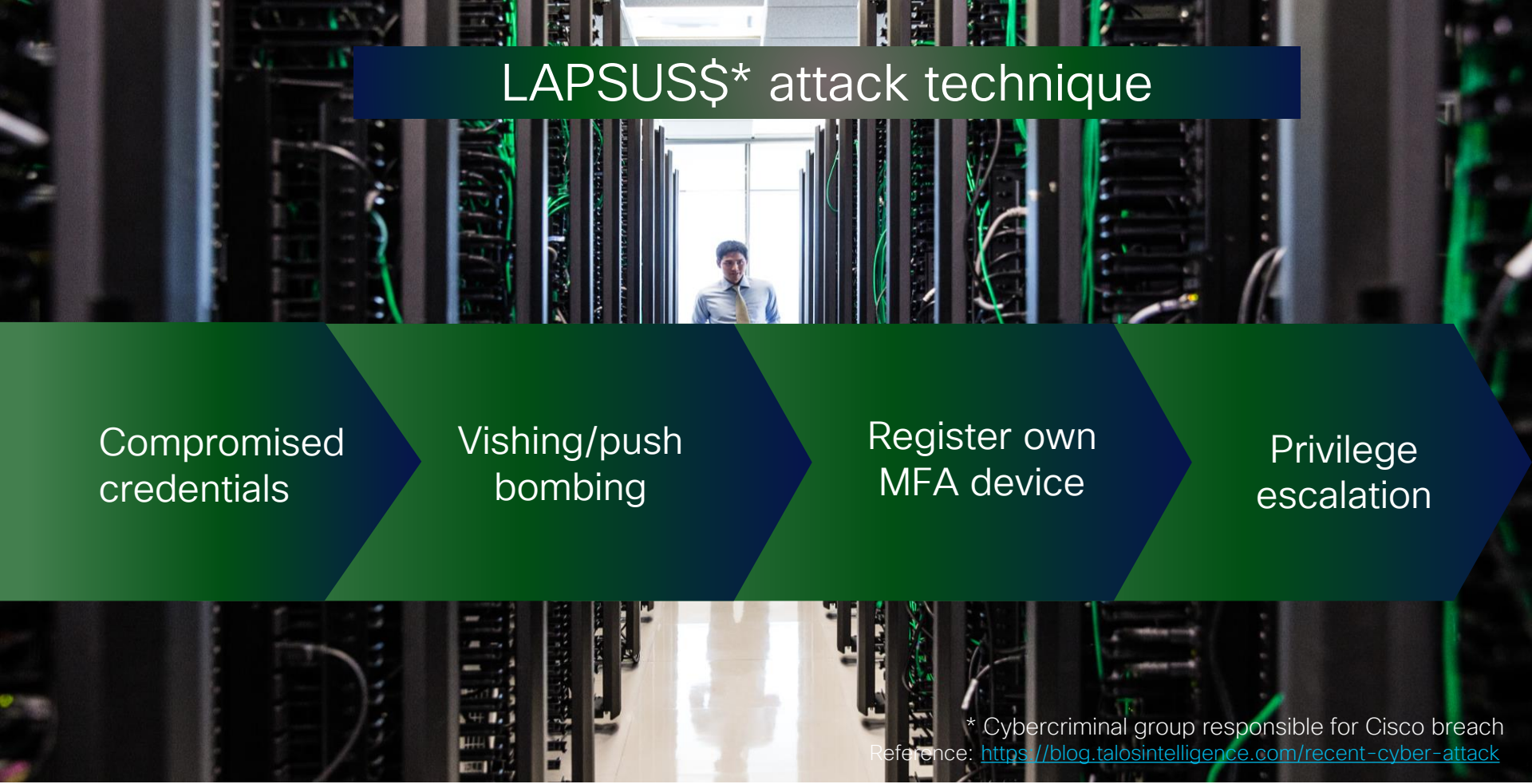
* Cybercriminal group responsible for MGM breach

Reference: https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf

*Image(s) used under license from Shutterstock.com

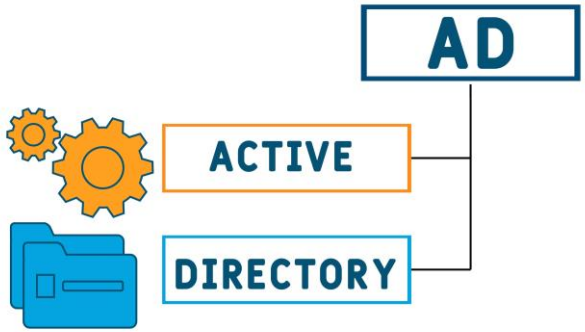
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

LAPSUS$* attack technique



* Cybercriminal group responsible for Cisco breach
Reference: https://blog.talosintelligence.com/recent-cyber-attack

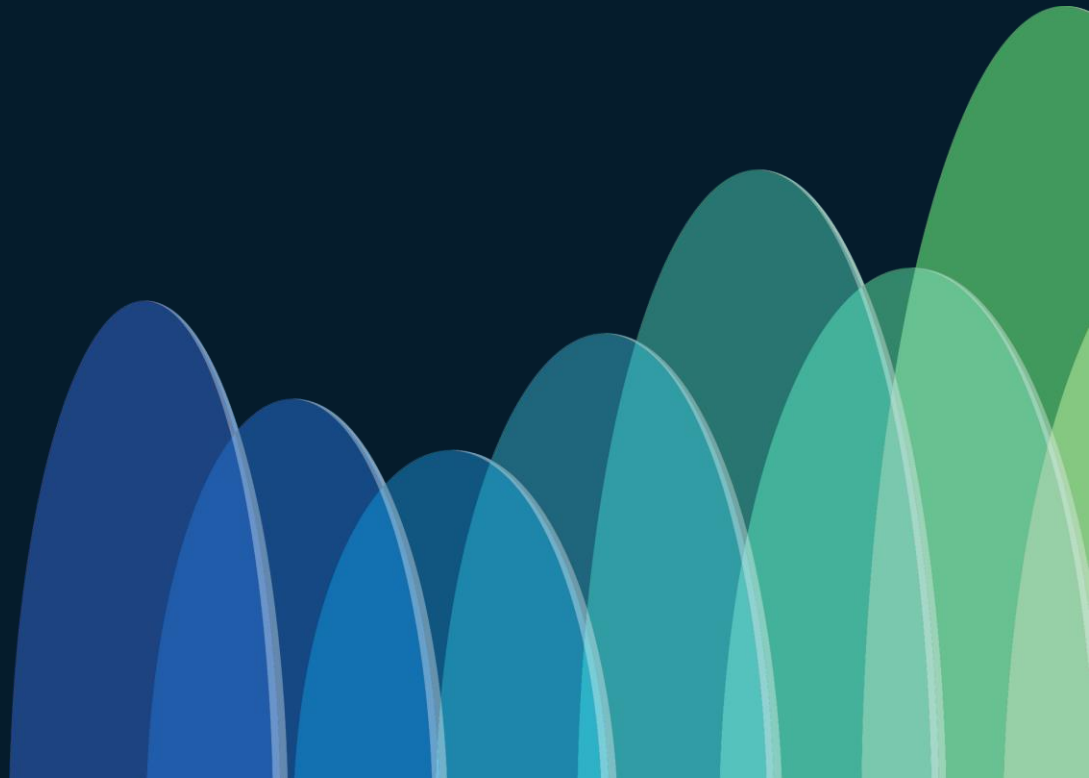
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



*Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continuous Identity Security

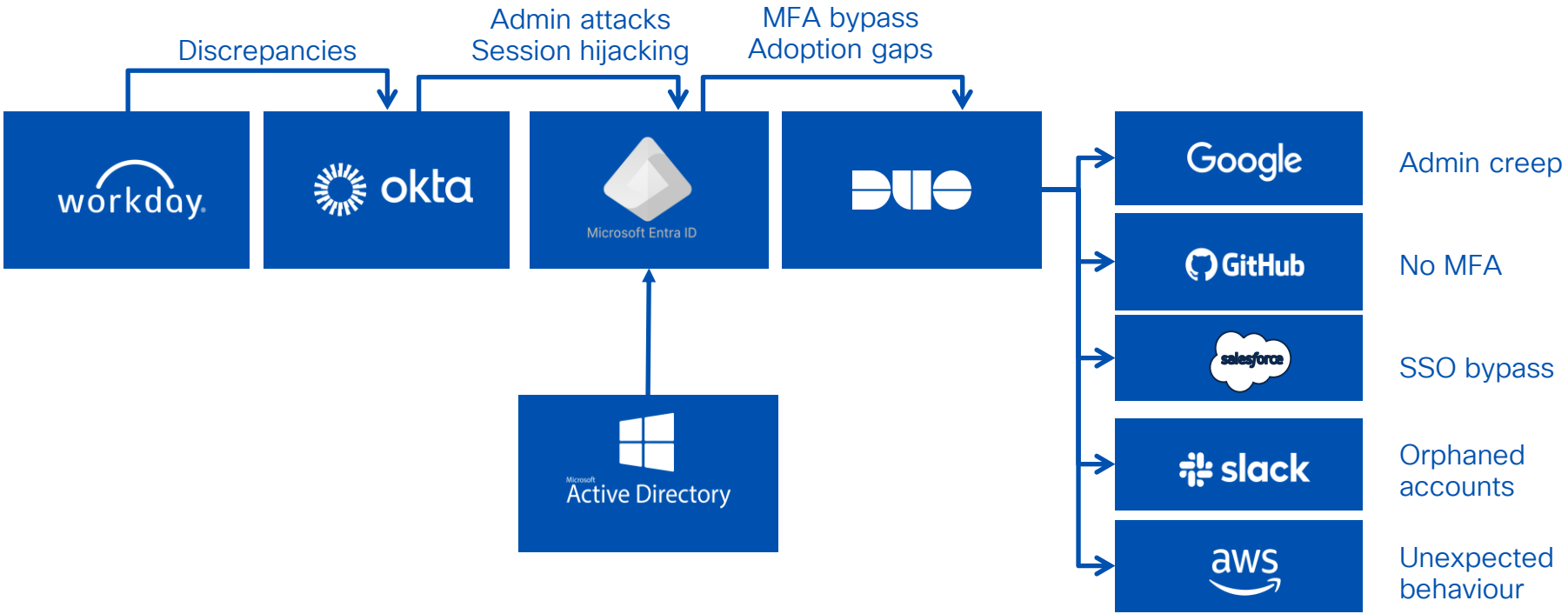


cisco Live!

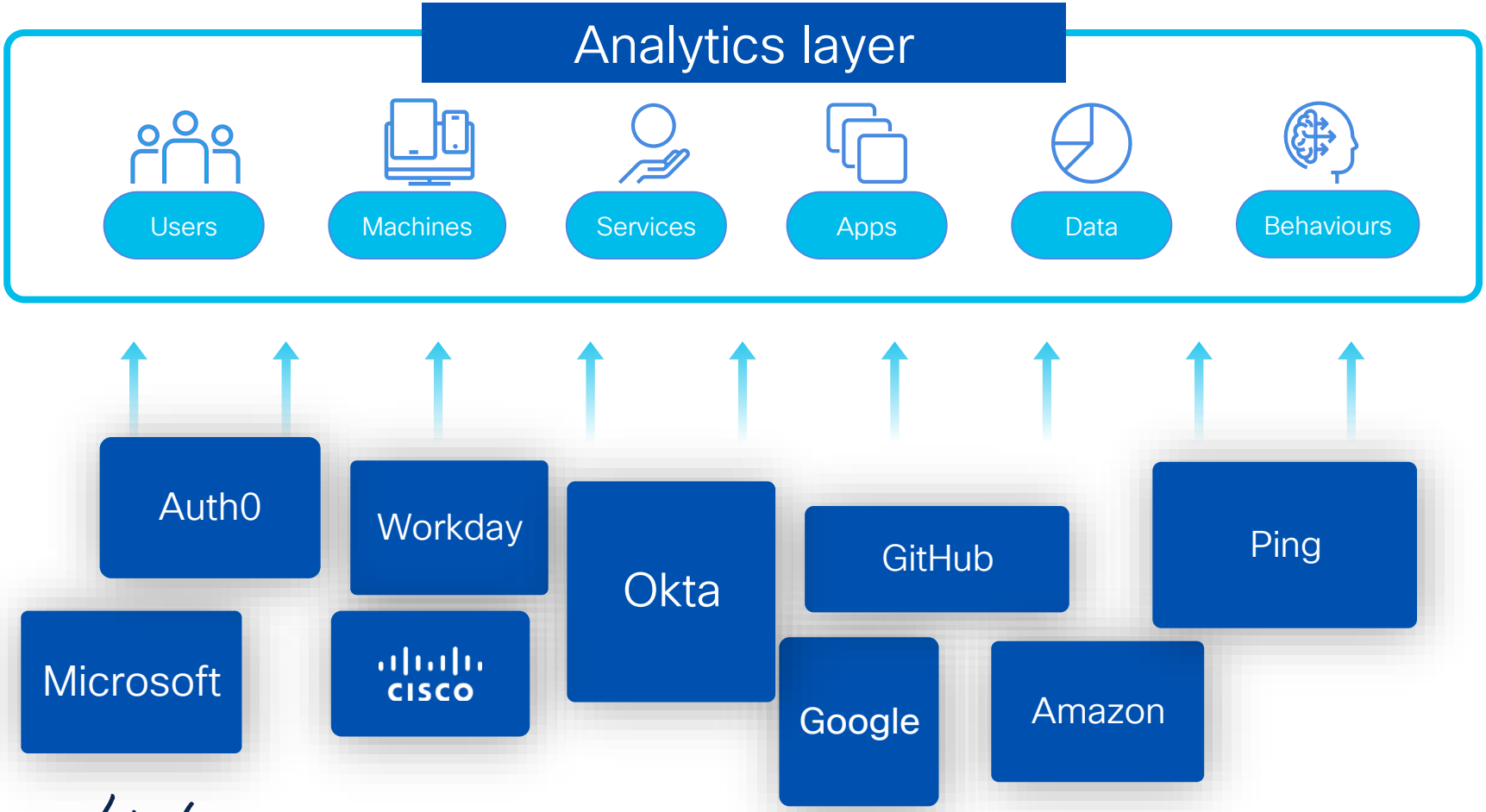
Cisco Identity Intelligence

cisco Live!

Fragmented identity ecosystem

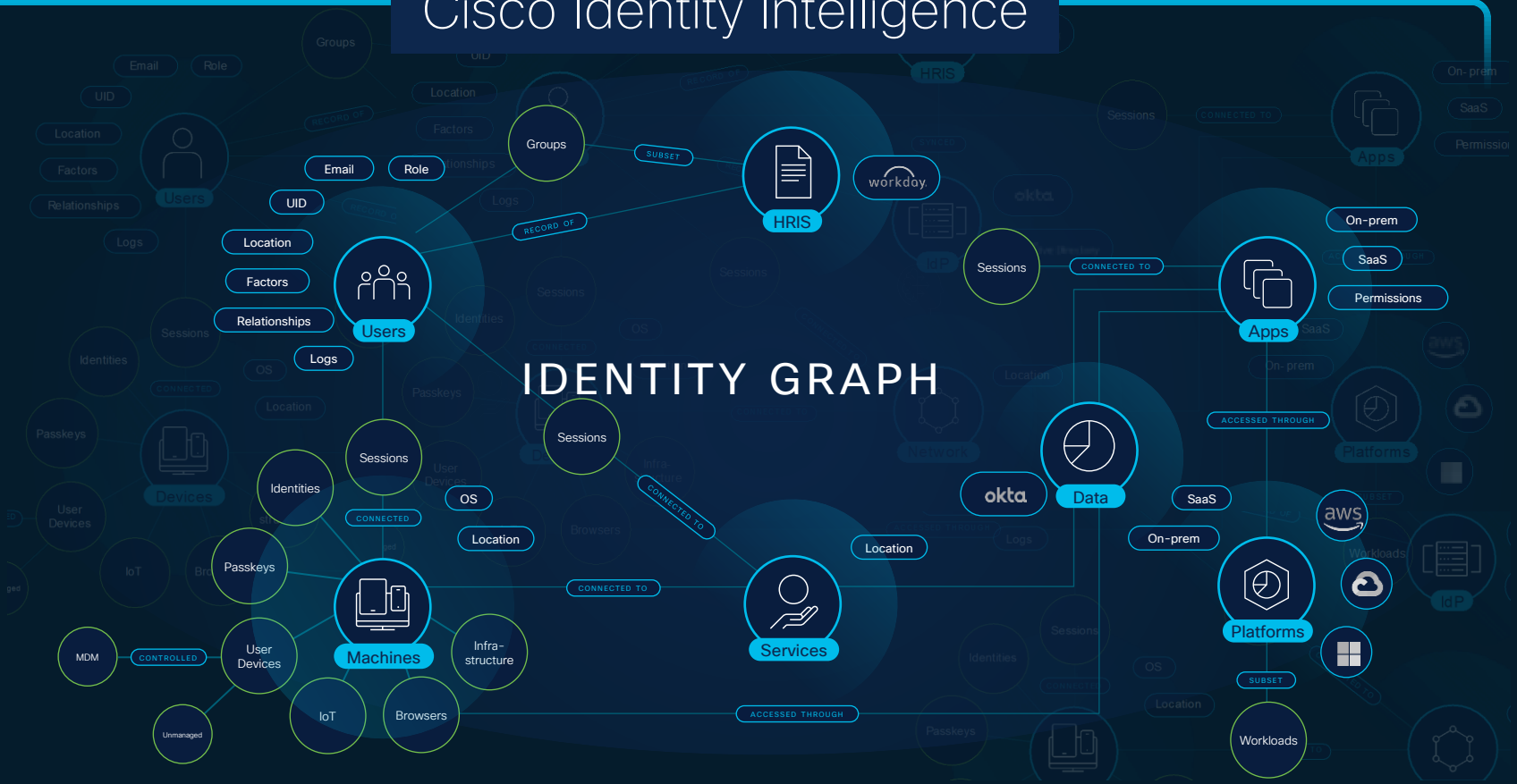


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



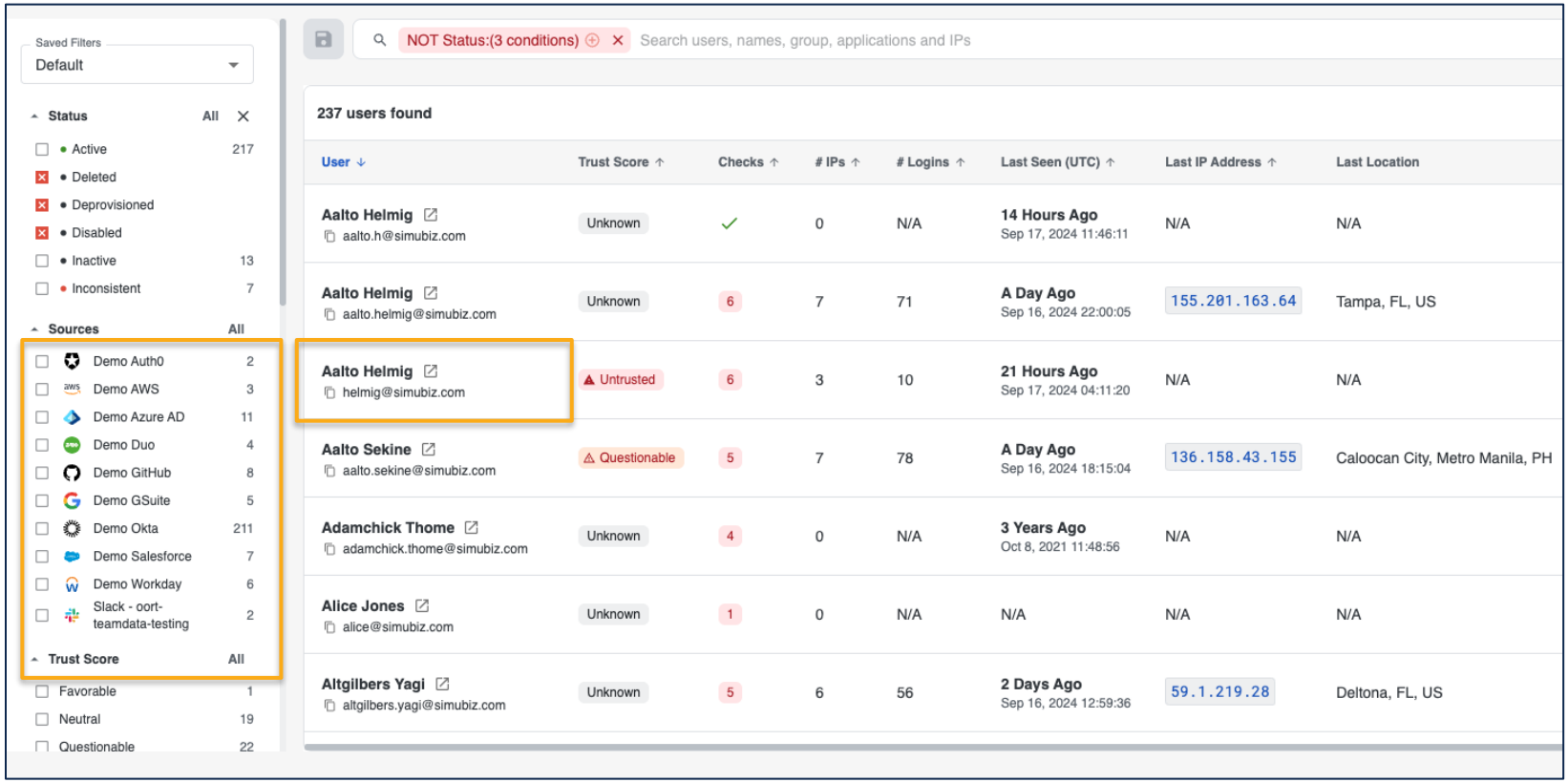
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Identity Intelligence



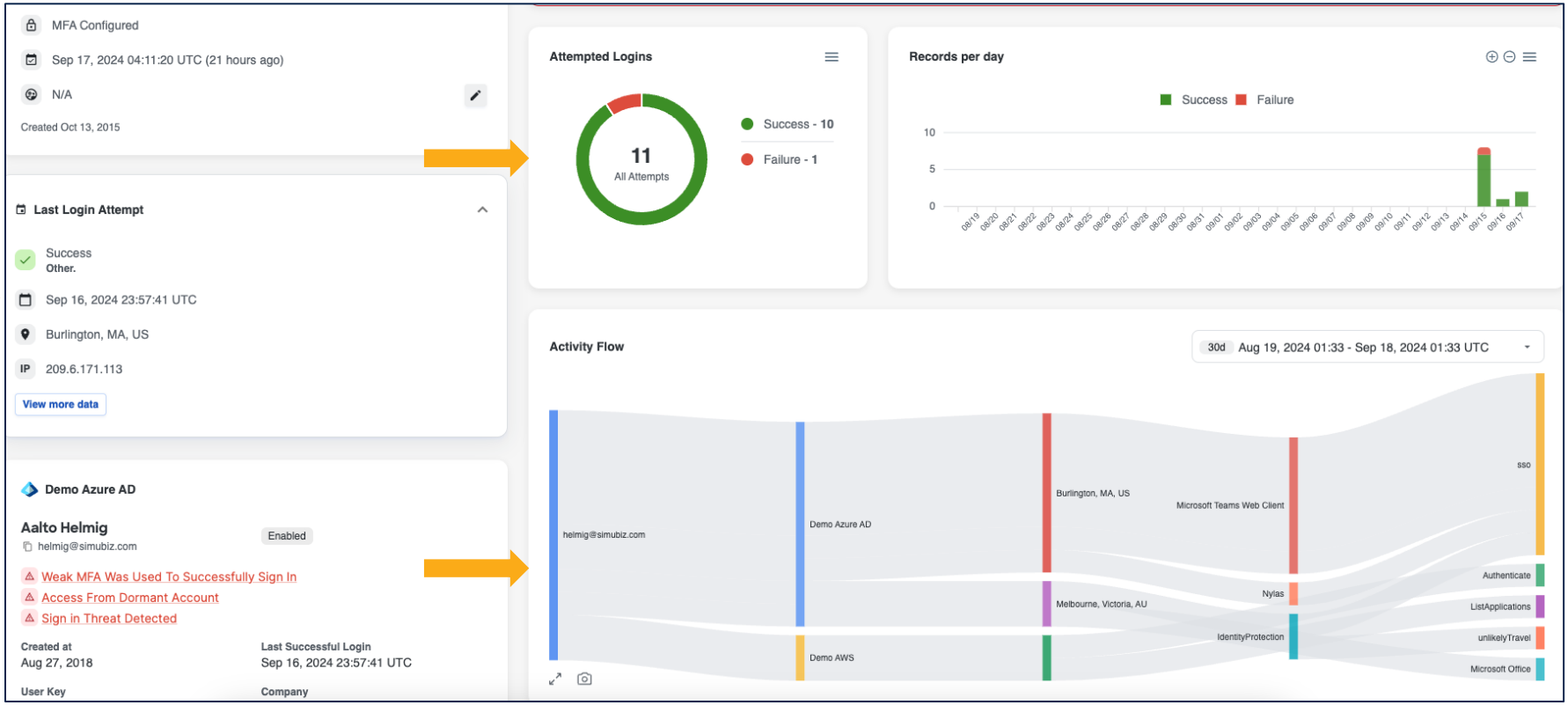
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

User 360



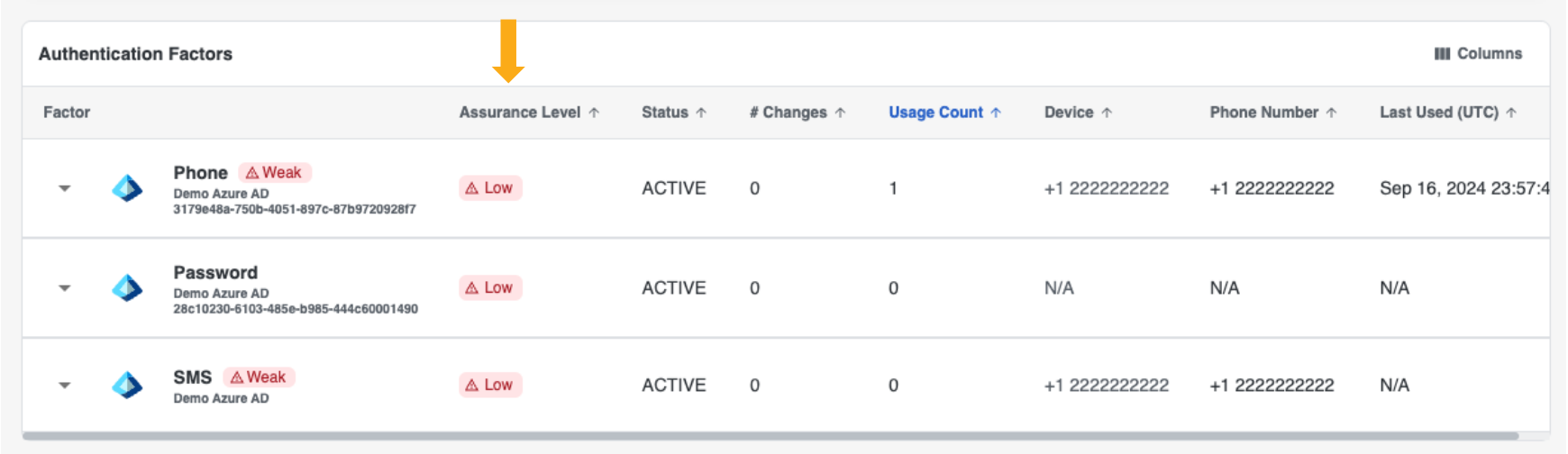
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

User 360



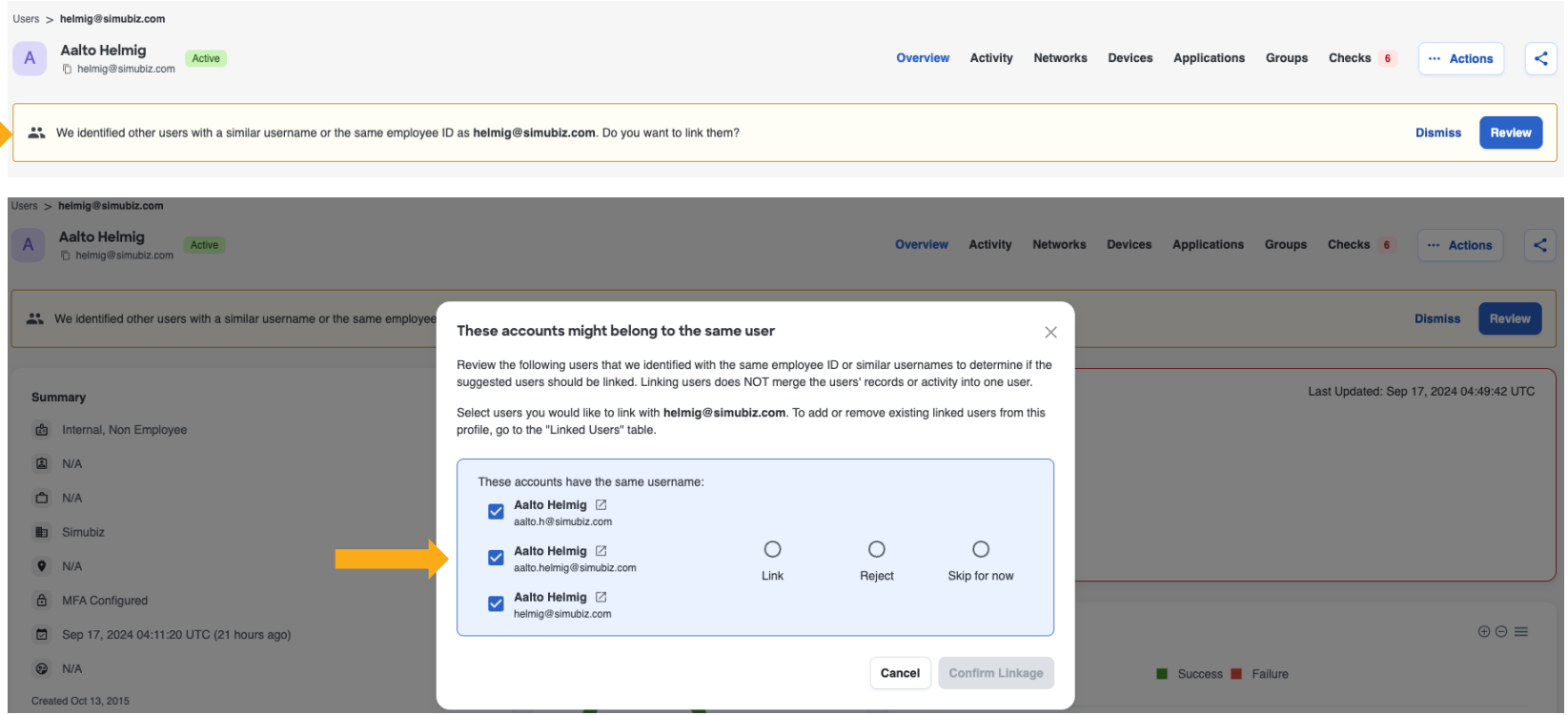
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

User 360



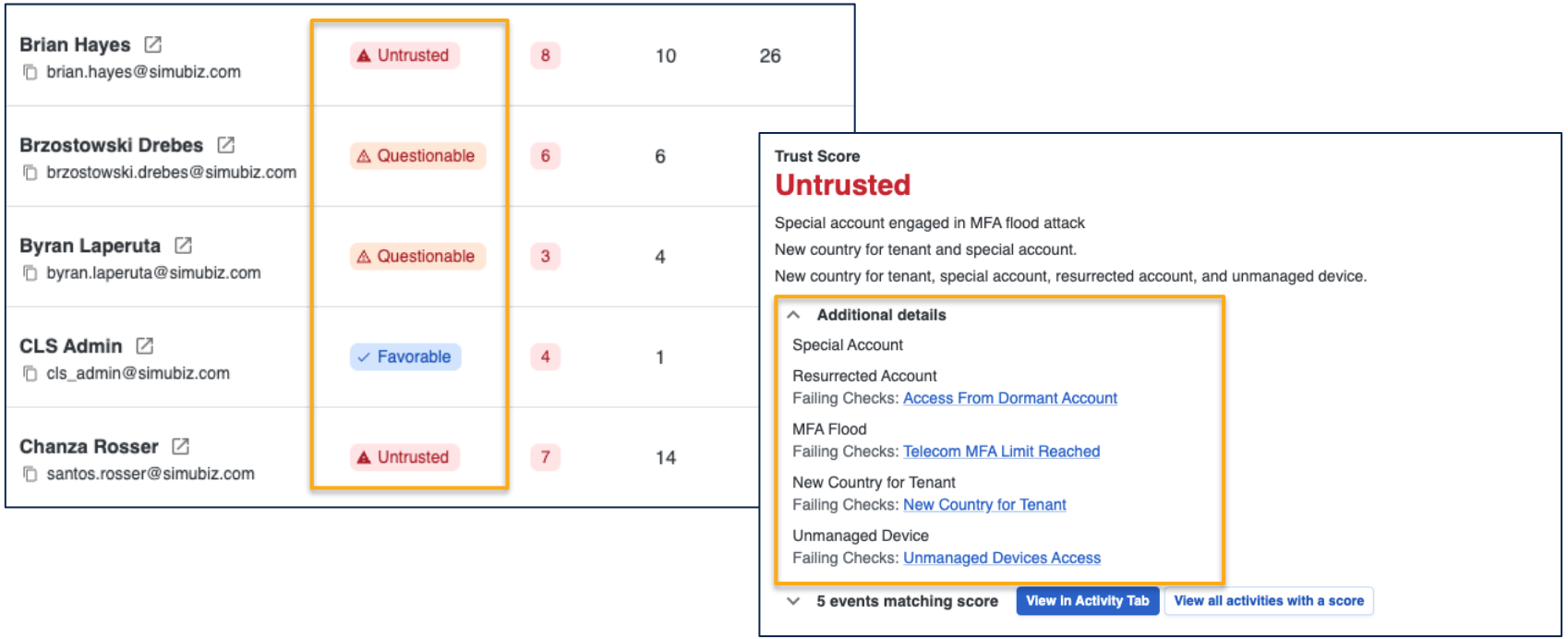
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

User 360



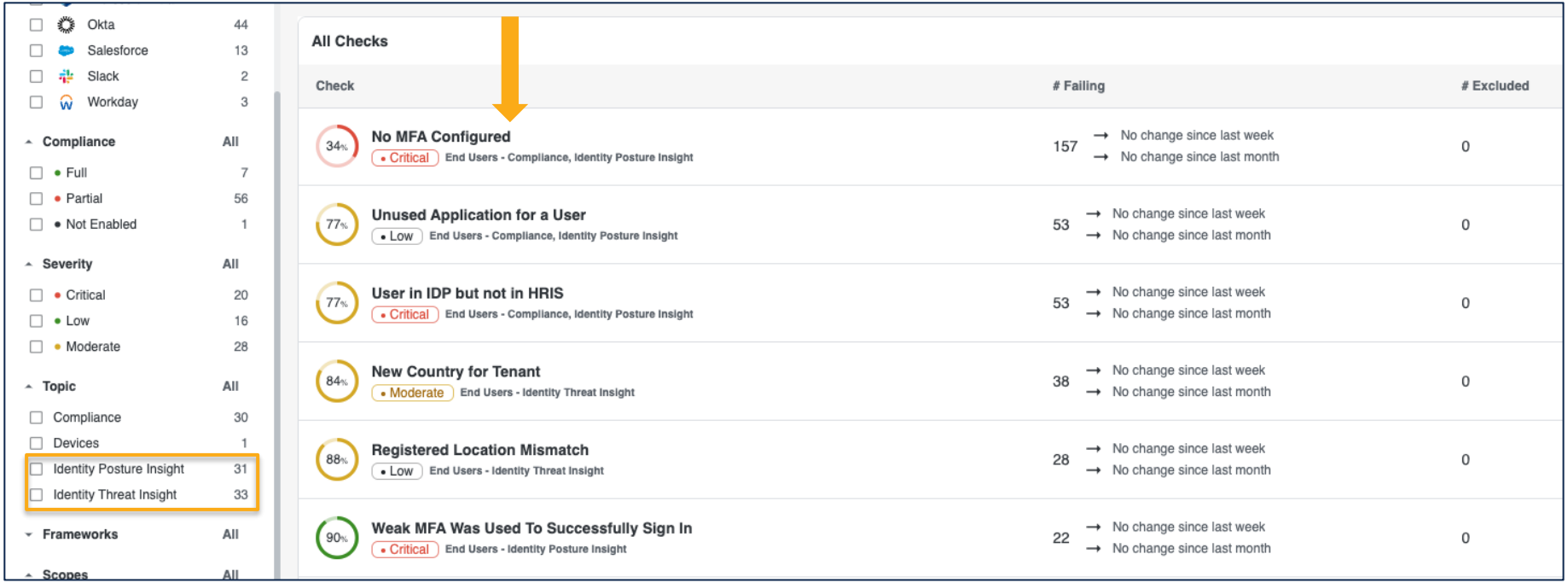
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

User trust score



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity checks



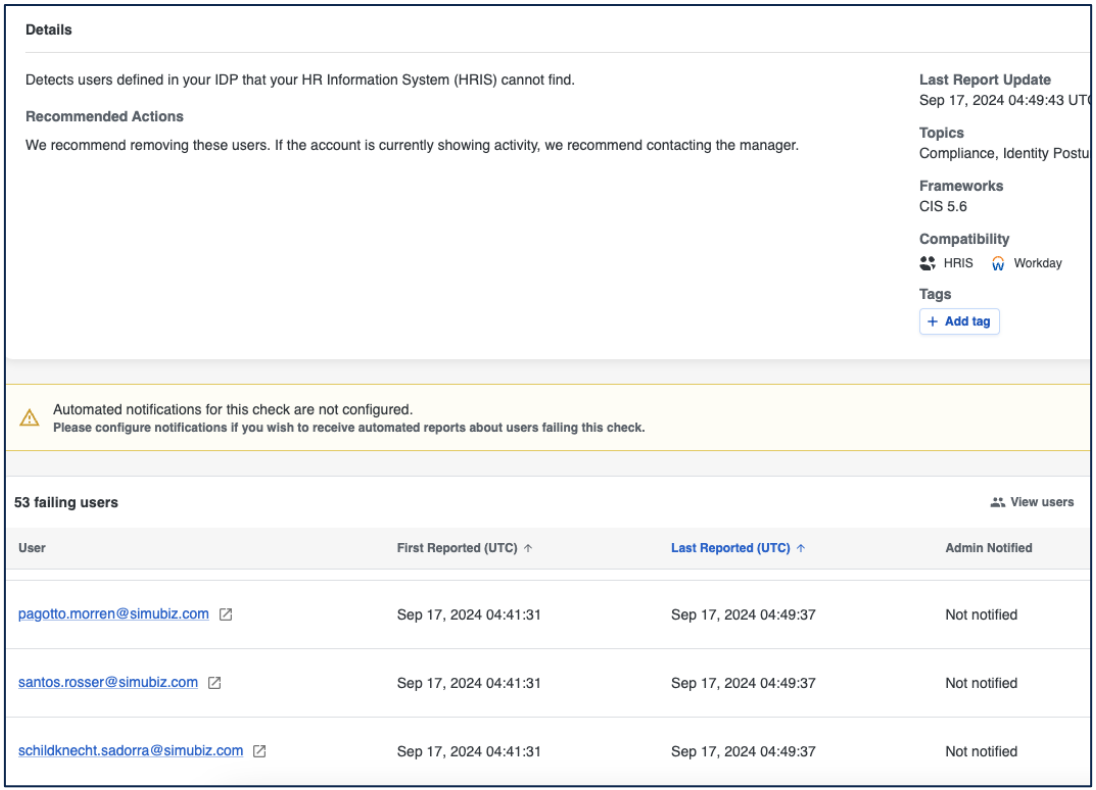
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity posture insight

Check	# Failing
34% **No MFA Configured** • Critical End Users - Compliance, Identity Posture Insight	157 → No change since last week → No change since last month
77% **Unused Application for a User** • Low End Users - Compliance, Identity Posture Insight	53 → No change since last week → No change since last month
77% **User in IDP but not in HRIS** • Critical End Users - Compliance, Identity Posture Insight	53 → No change since last week → No change since last month
90% **Weak MFA Was Used To Successfully Sign In** • Critical End Users - Identity Posture Insight	22 → No change since last week → No change since last month
90% **No Strong MFA Configured** • Moderate End Users - Compliance, Identity Posture Insight	22 → No change since last week → No change since last month
97% **User Password Expiration Failure** • Moderate End Users - Identity Posture Insight	6 → No change since last week → No change since last month
97% **User Stuck in Non-functional State** • Moderate End Users - Compliance, Identity Posture Insight	5 → No change since last week → No change since last month

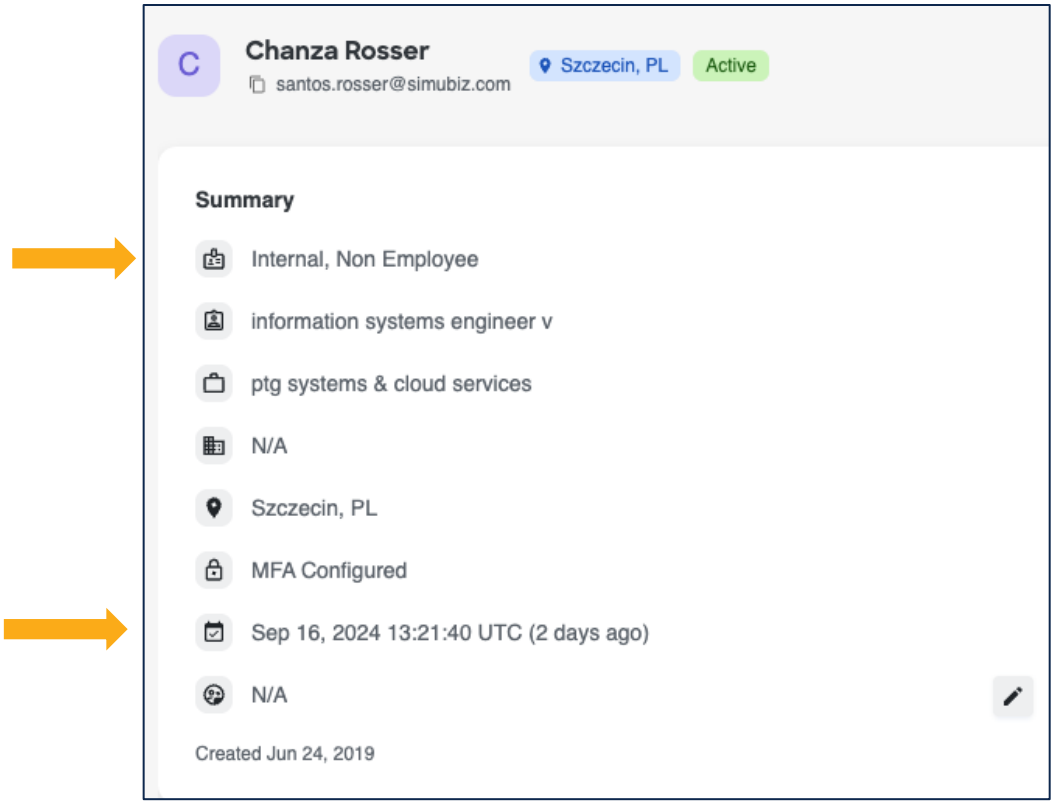
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity posture insight



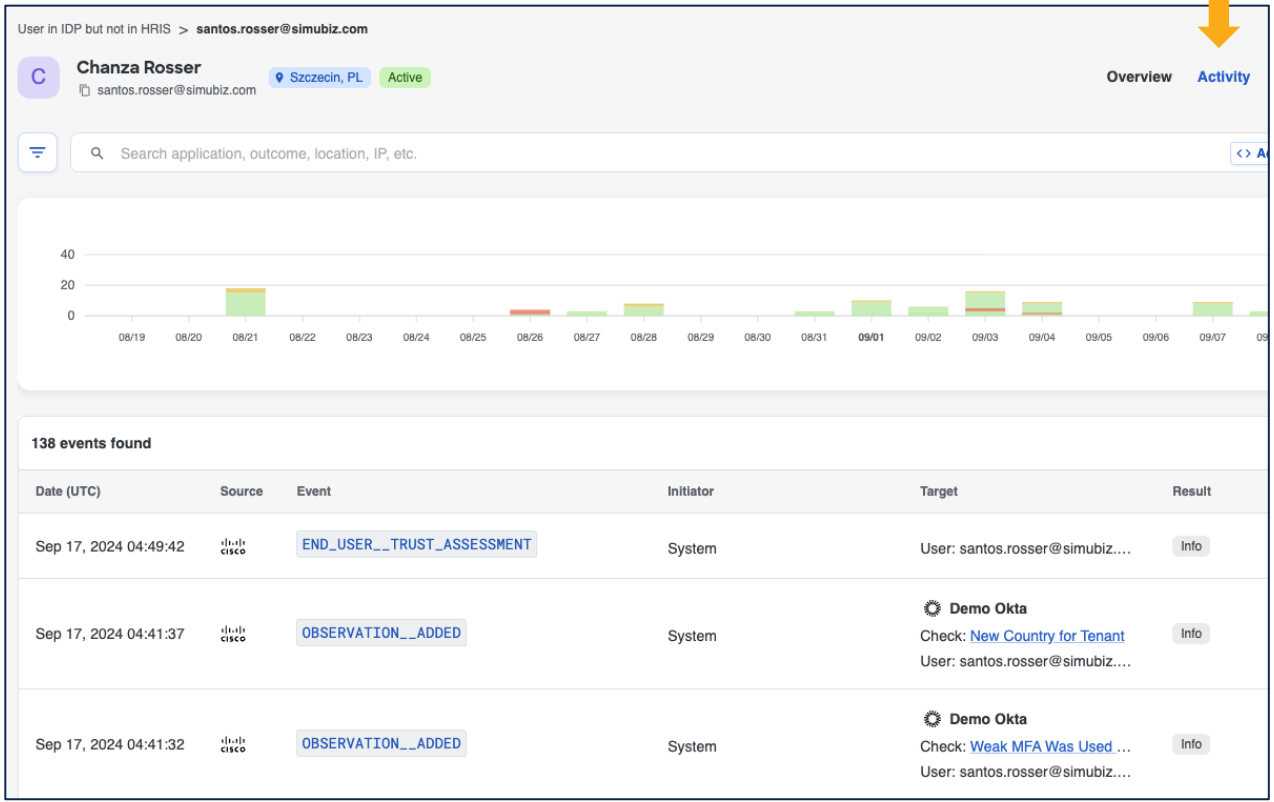
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity posture insight



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity posture insight



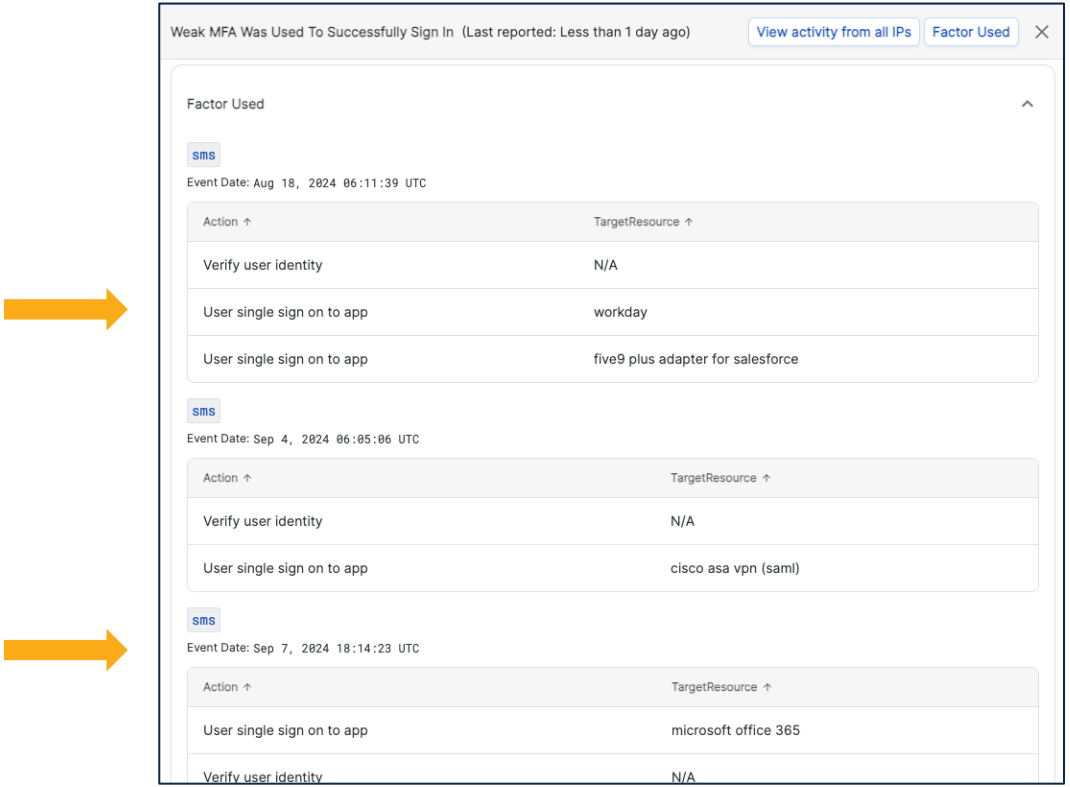
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity posture insight

Check	# Failing
77% User in IDP but not in HRIS • Critical End Users - Compliance, Identity Posture Insight	53 → No change since last week → No change since last month
90% Weak MFA Was Used To Successfully Sign In • Critical End Users - Identity Posture Insight	22 → No change since last week → No change since last month
90% No Strong MFA Configured • Moderate End Users - Compliance, Identity Posture Insight	22 → No change since last week → No change since last month
97% User Password Expiration Failure • Moderate End Users - Identity Posture Insight	6 → No change since last week → No change since last month
97% User Stuck in Non-functional State • Moderate End Users - Compliance, Identity Posture Insight	5 → No change since last week → No change since last month
97% Upcoming App Key Expiration • Low End Users - Identity Posture Insight	5 → No change since last week → No change since last month
98% Inactive Users • Moderate End Users - Compliance, Identity Posture Insight	4 → No change since last week → No change since last month

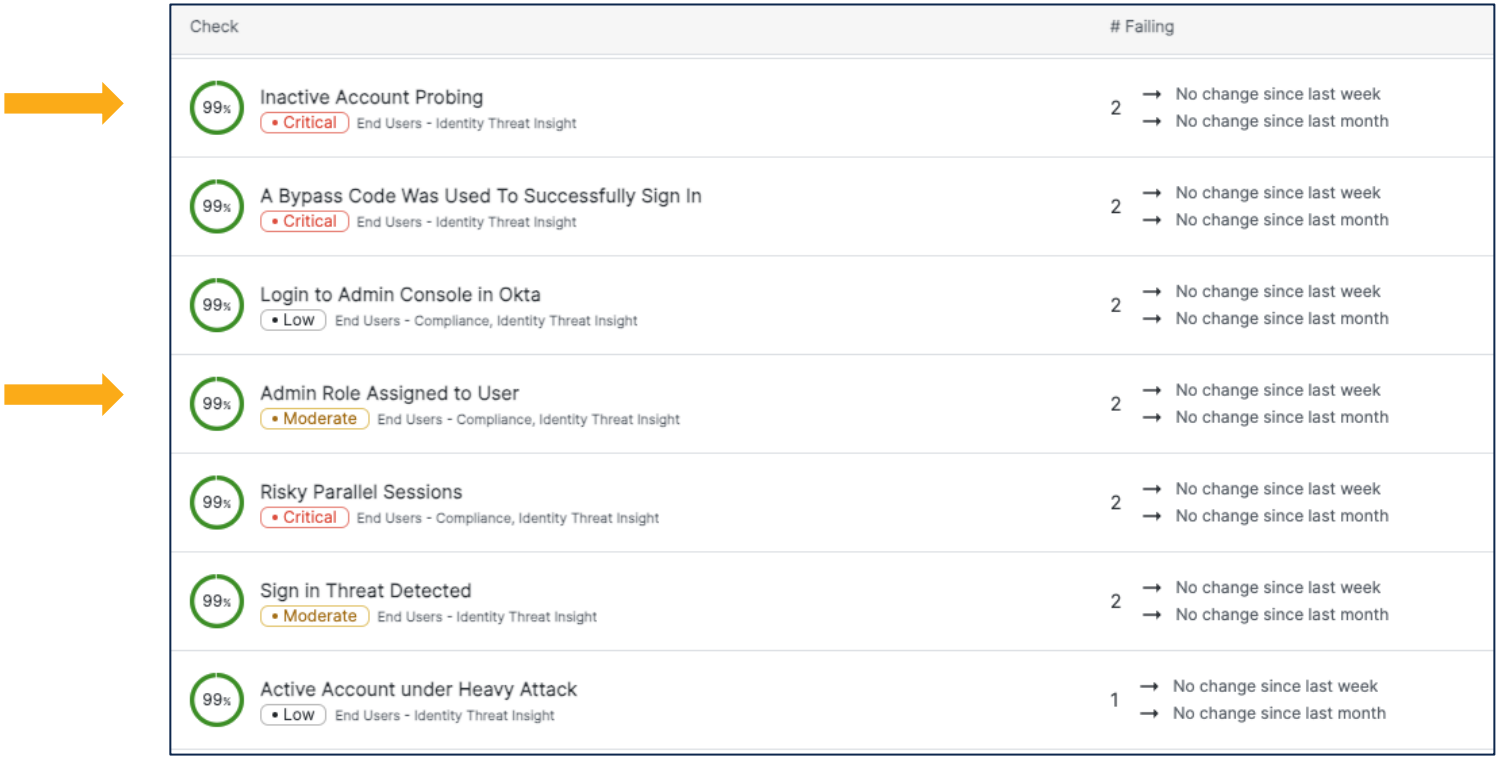
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity posture insight



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

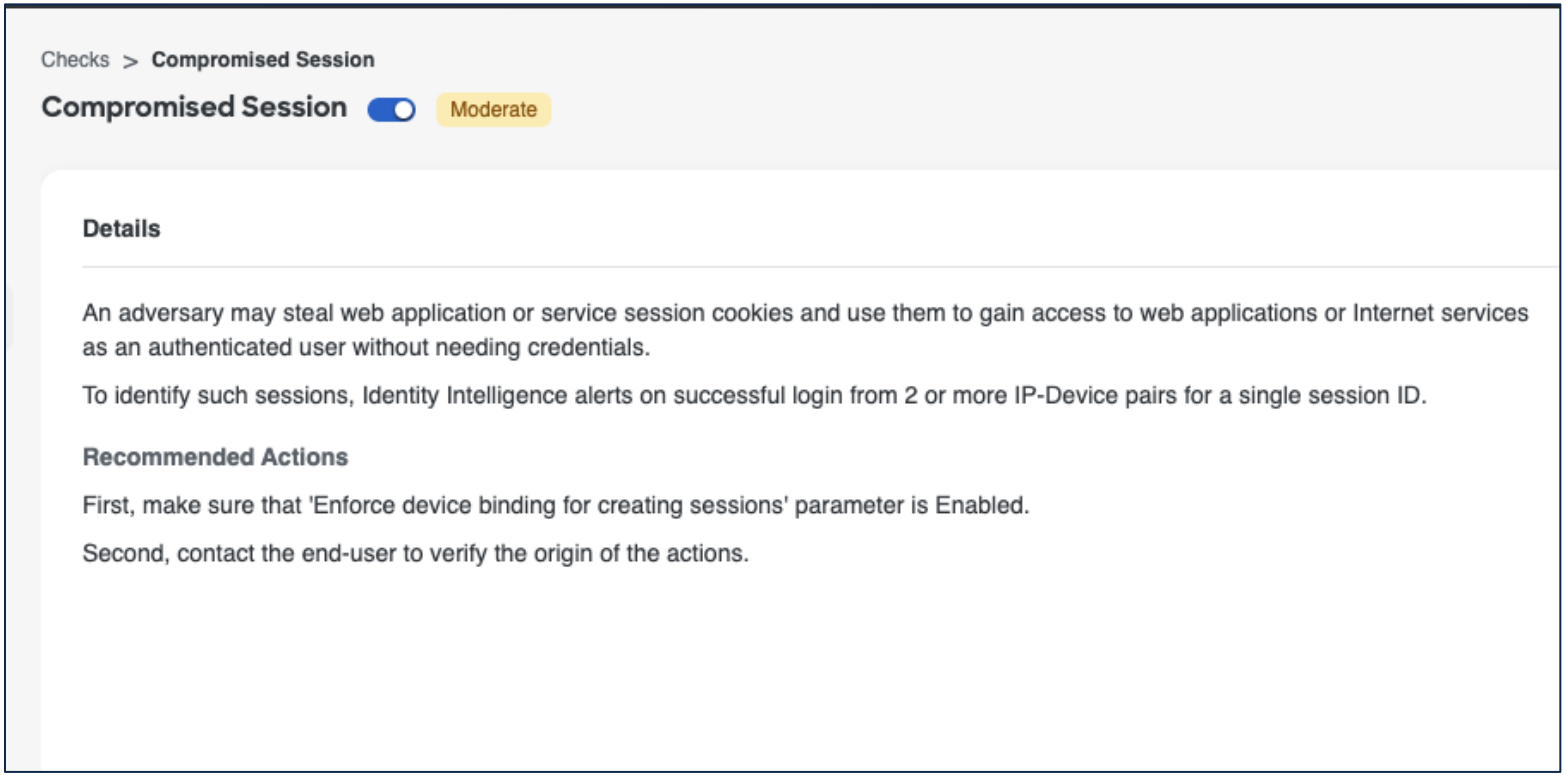
Identity threat insight



Check	# Failing
99% Inactive Account Probing • Critical End Users - Identity Threat Insight	2 → No change since last week → No change since last month
99% A Bypass Code Was Used To Successfully Sign In • Critical End Users - Identity Threat Insight	2 → No change since last week → No change since last month
99% Login to Admin Console in Okta • Low End Users - Compliance, Identity Threat Insight	2 → No change since last week → No change since last month
99% Admin Role Assigned to User • Moderate End Users - Compliance, Identity Threat Insight	2 → No change since last week → No change since last month
99% Risky Parallel Sessions • Critical End Users - Compliance, Identity Threat Insight	2 → No change since last week → No change since last month
99% Sign in Threat Detected • Moderate End Users - Identity Threat Insight	2 → No change since last week → No change since last month
99% Active Account under Heavy Attack • Low End Users - Identity Threat Insight	1 → No change since last week → No change since last month

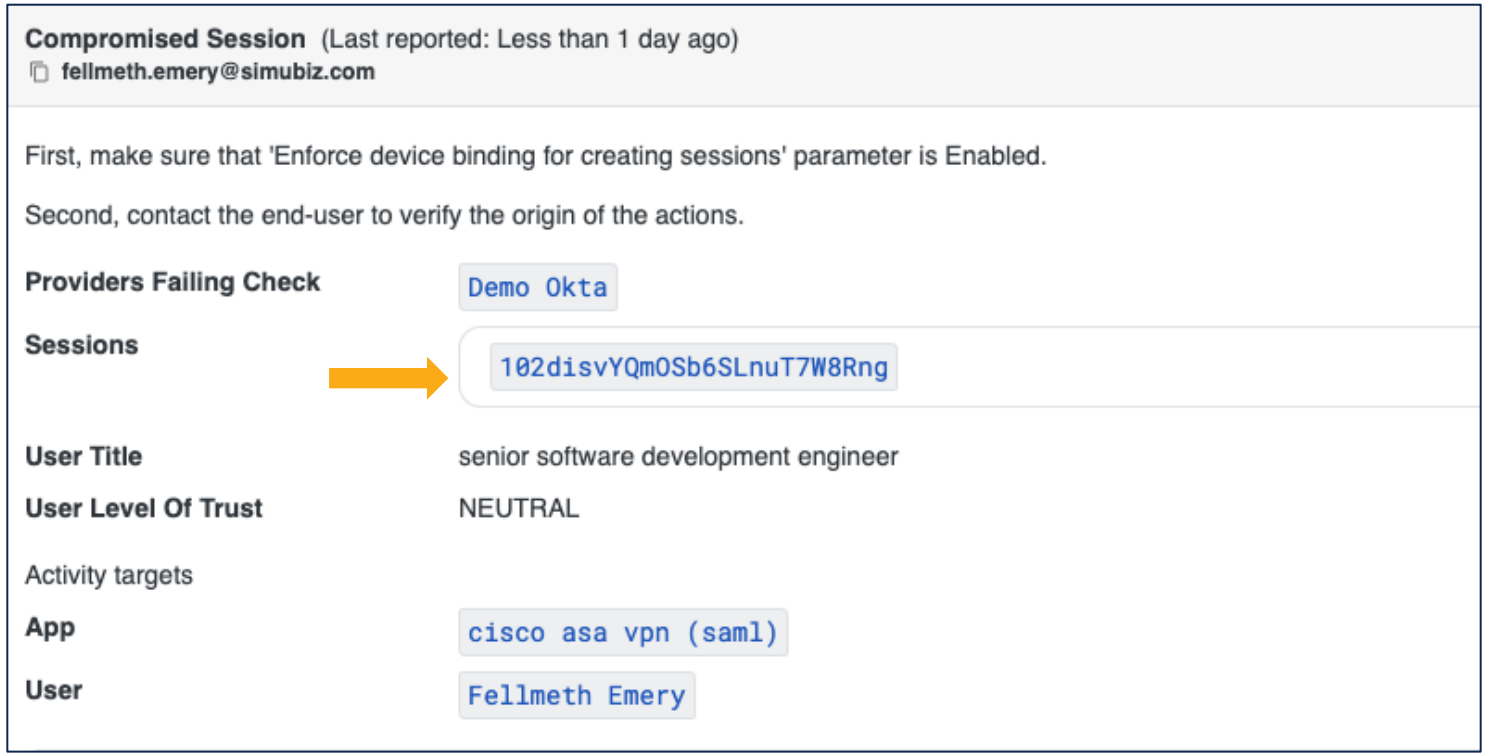
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity threat insight



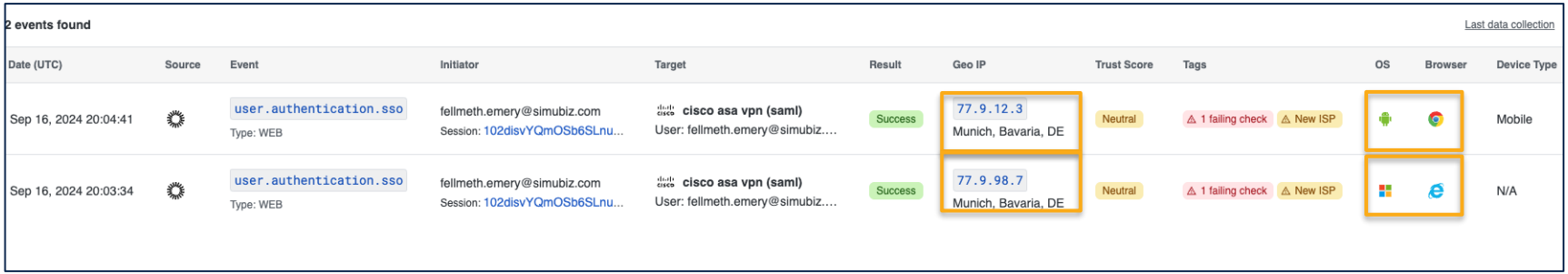
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity threat insight



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identity threat insight



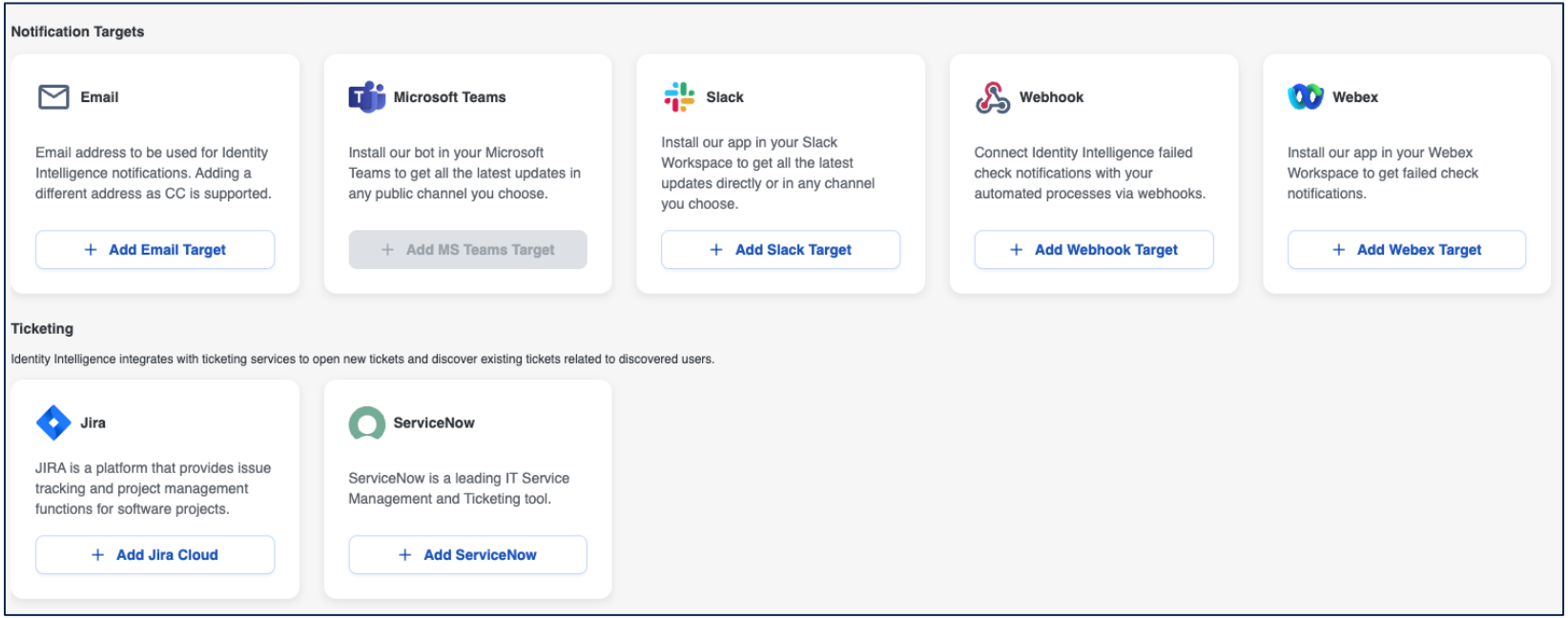
2 events found

Last data collection

Date (UTC)	Source	Event	Initiator	Target	Result	Geo IP	Trust Score	Tags	OS	Browser	Device Type
Sep 16, 2024 20:04:41		user.authentication.sso Type: WEB	fellmeth.emery@simubiz.com Session: 102disvYQmOSb6SLnu...	cisco asa vpn (saml) User: fellmeth.emery@simubiz....	Success	77.9.12.3 Munich, Bavaria, DE	Neutral	1 failing check, New ISP			Mobile
Sep 16, 2024 20:03:34		user.authentication.sso Type: WEB	fellmeth.emery@simubiz.com Session: 102disvYQmOSb6SLnu...	cisco asa vpn (saml) User: fellmeth.emery@simubiz....	Success	77.9.98.7 Munich, Bavaria, DE	Neutral	1 failing check, New ISP			N/A

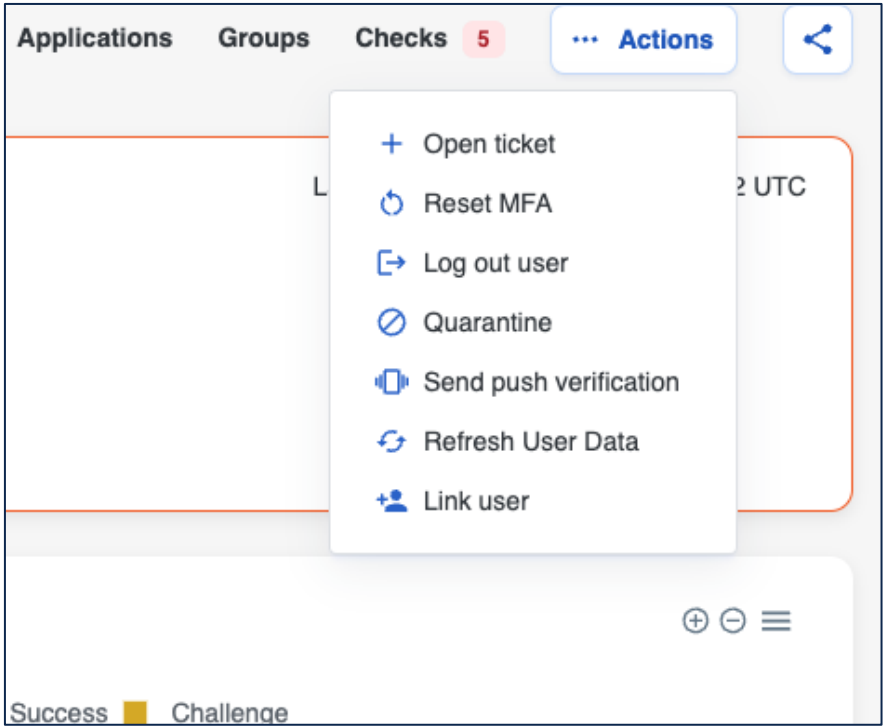
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Notification and remediation

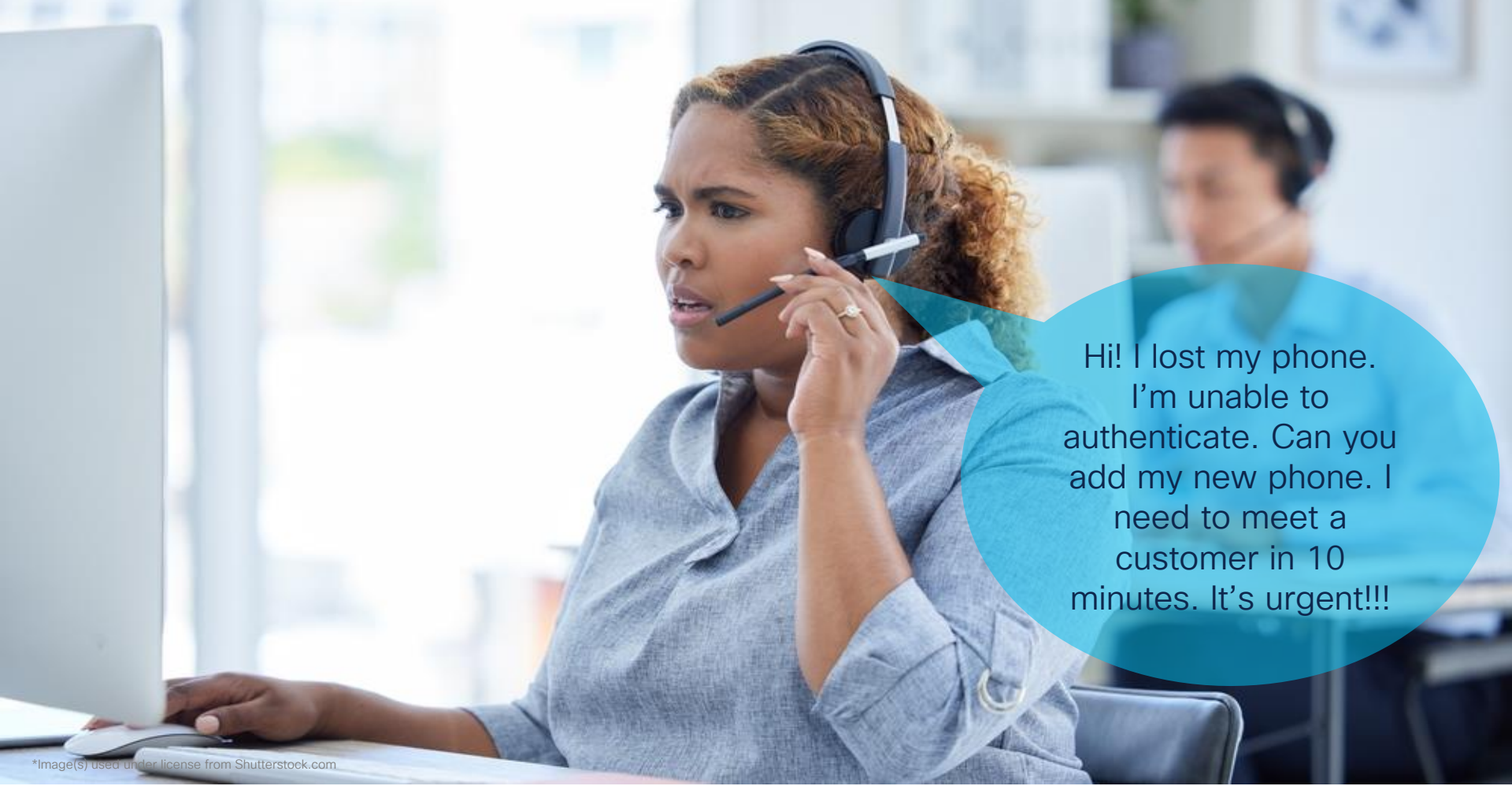


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Notification and remediation



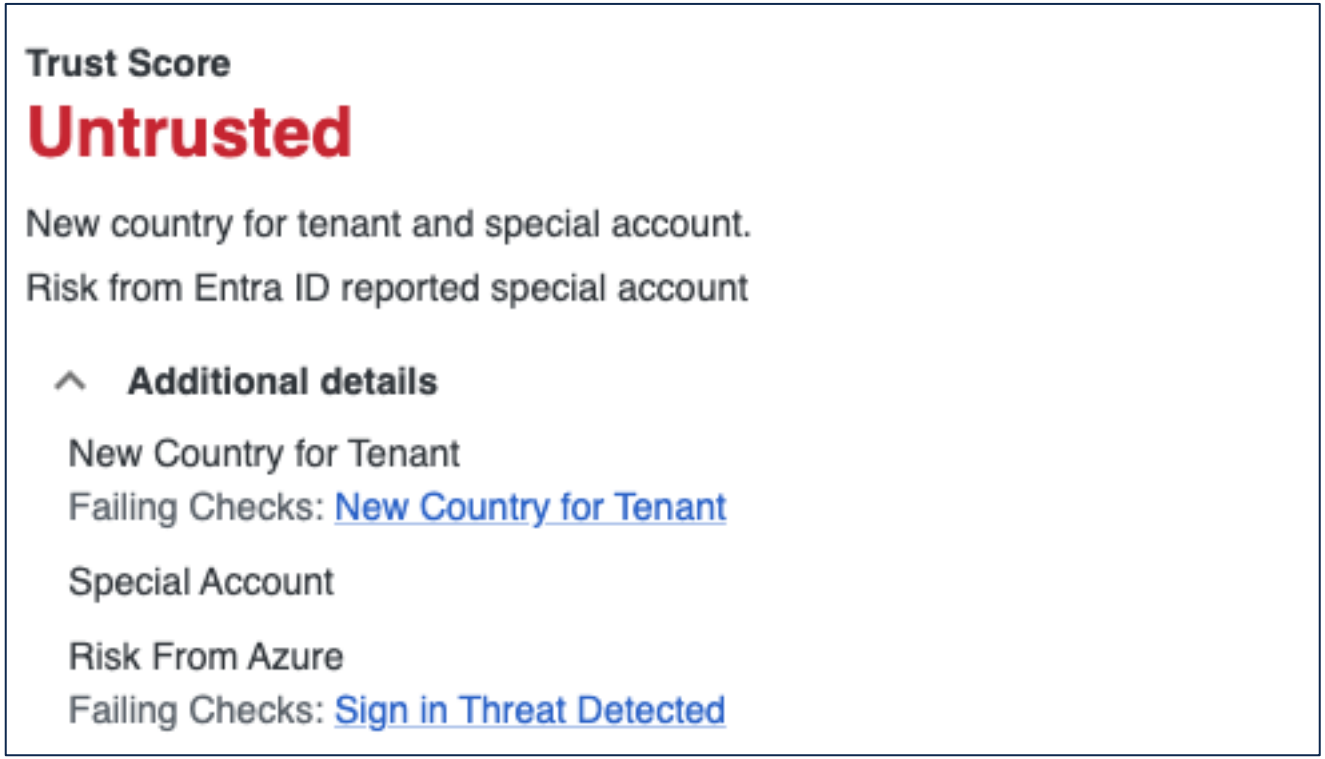
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



*Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Help Desk Verification



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Help Desk Verification

Name	Source	Status	Assignments	Owners	Usage Count	Last Access (UTC)	Result
cisco asa vpn (munich) deatrick.deroberts@simubiz.com	Demo Okta		vpn-full-access-ipsec	Not supported	96	Sep 13, 2024 14:17:34	Success
five9 plus adapter for sale... • Sensitive deatrick.deroberts@simubiz.com	Demo Okta		sg-okta-simubiz-fulltime	Not supported	31	Sep 16, 2024 12:36:52	Success
microsoft office 365 for simubiz deatrick.deroberts@simubiz.com	Demo Okta		sg-okta-simubiz-fulltime	Not supported	6	Sep 16, 2024 06:24:30	Success
atlassian cloud deatrick.deroberts@simubiz.com	Demo Okta		sg-jira-endusers	Not supported	3	Sep 10, 2024 09:53:16	Success
cisco asa vpn (pinewood uk) deatrick.deroberts@simubiz.com	Demo Okta		vpn-full-access-ipsec	Not supported	3	Sep 5, 2024 17:54:53	Success
servicenow • Sensitive deatrick.deroberts@simubiz.com	Demo Okta		sg-okta-simubiz-fulltime	Not supported	3	Sep 4, 2024 05:13:31	Success
workday • Sensitive zumbrum@simubiz.com	Demo Okta		sg-okta-simubiz-fulltime	Not supported	1	Sep 16, 2024 06:38:23	Success

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Help Desk Verification

	Duo Mobile Demo Duo DPUW9OMLI9IU8XFVU4RF	Medium	ACTIVE	0	0	Apple iPhone 14 Pro Max	+9722222222
	Push Demo Duo DPUW9OMLI9IU8XFVU4RF	Medium	ACTIVE	0	0	Apple iPhone 14 Pro Max	+9722222222
	Call ⚠ Weak Demo Duo DPUW9OMLI9IU8XFVU4RF	⚠ Low	ACTIVE	0	0	Apple iPhone 14 Pro Max	+9722222222
	SMS ⚠ Weak Demo Duo DPUW9OMLI9IU8XFVU4RF	⚠ Low	ACTIVE	0	0	Apple iPhone 14 Pro Max	+9722222222
	Push Demo Okta opf11otl4mlIH4efn357	Medium	ACTIVE	1	15	Pixel 3	N/A
	Microsoft Authenticator App Demo Azure AD e74c2660-857e-4d54-9666-e1c5316d3d57	Medium	PENDING	0	0	iPhone 12 Pro Max	N/A

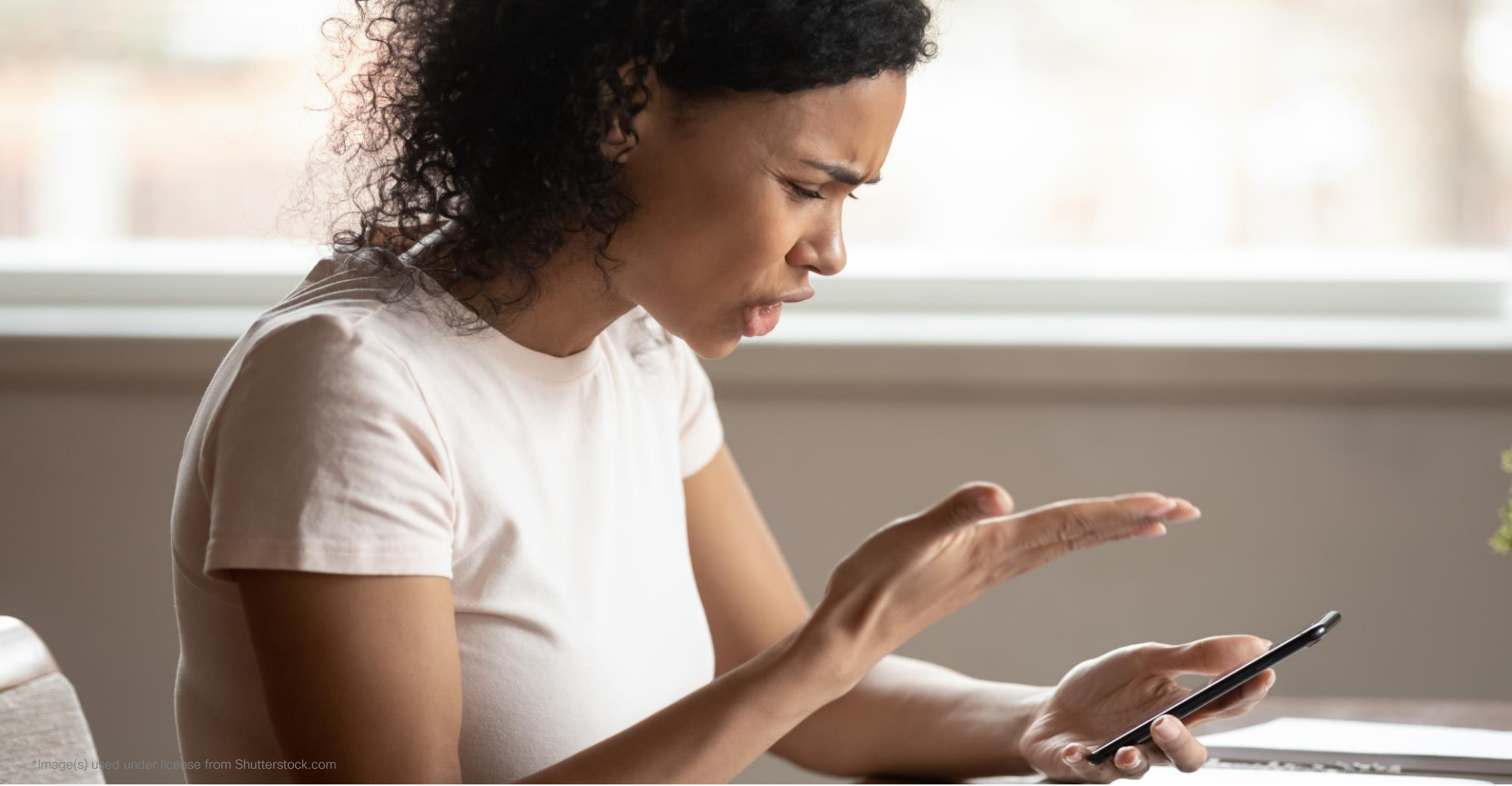
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

*Image(s) used under license from Shutterstock.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Duo Passport

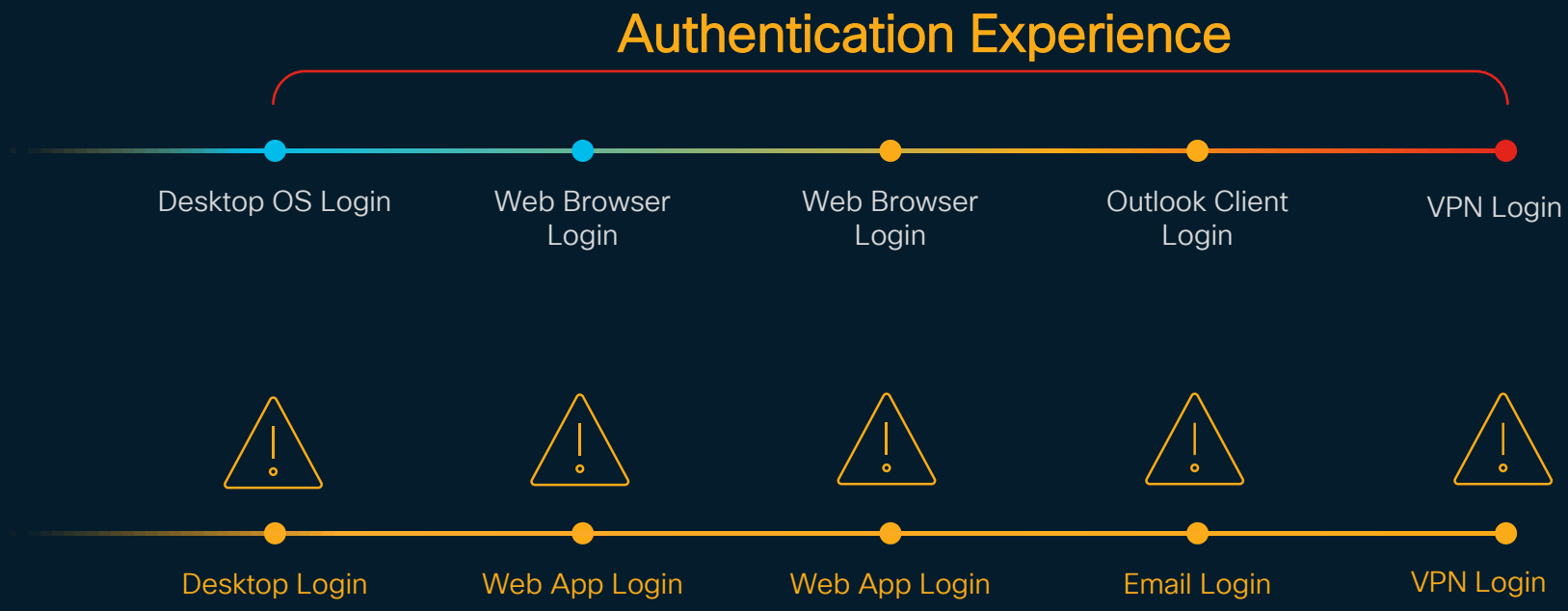
cisco Live!



*Image(s) used under license from Shutterstock.com

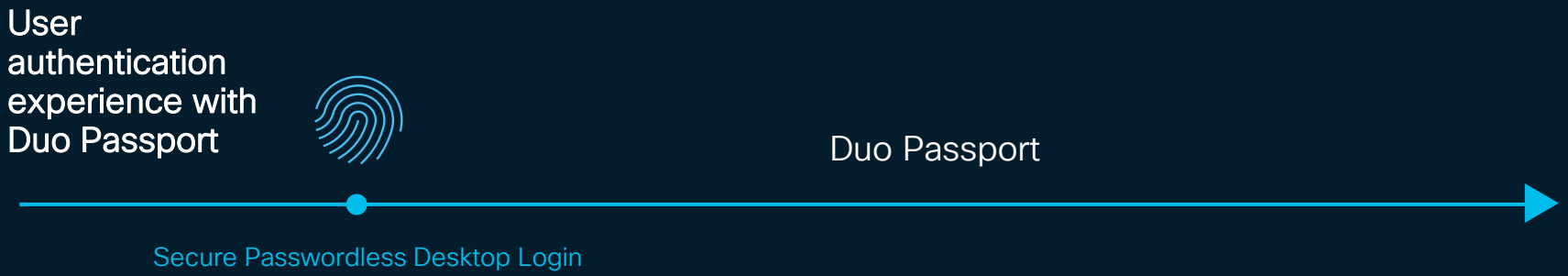
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Anatomy of frustration



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Duo Passport



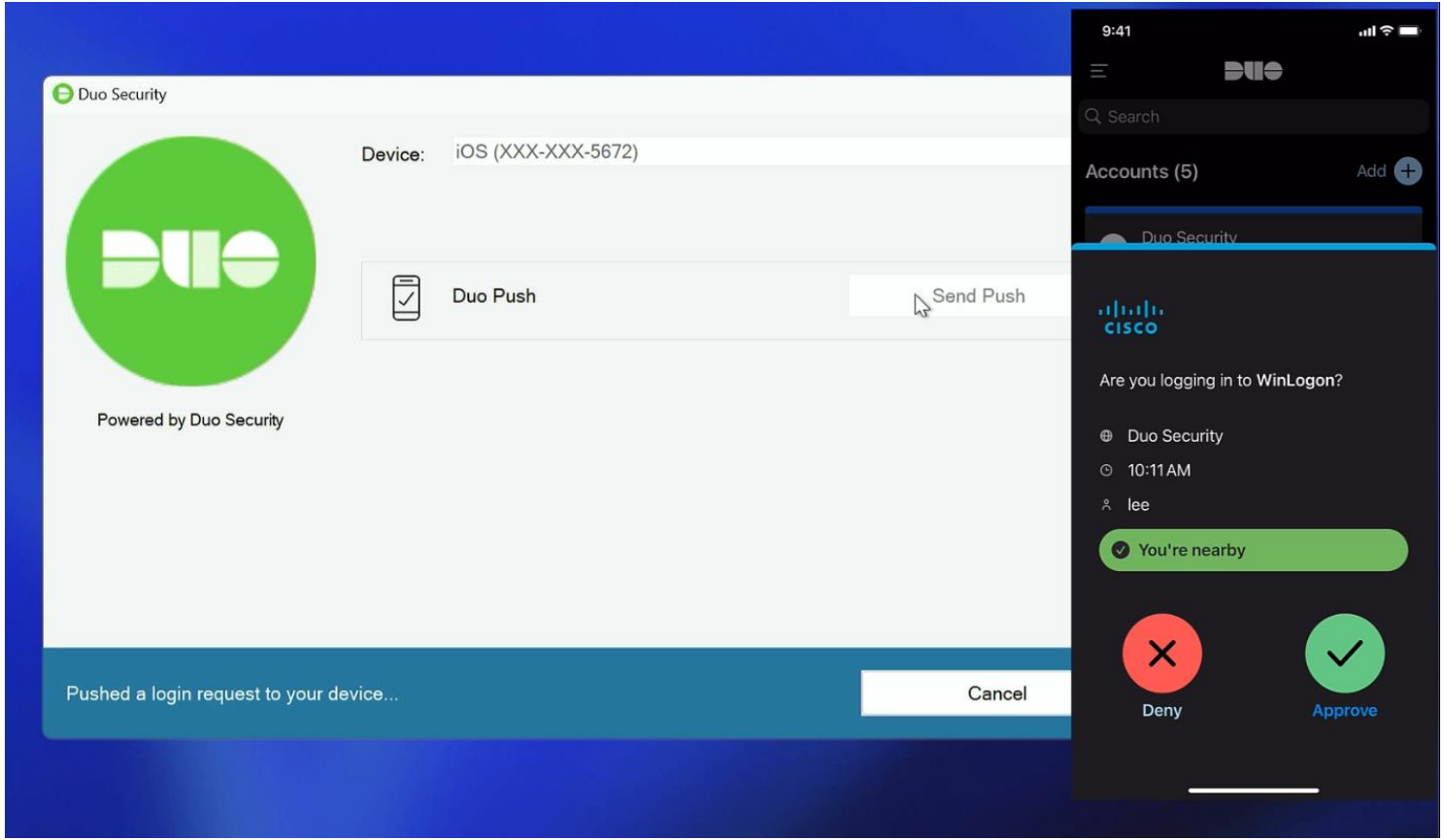
Log in once

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Duo Passport – User Experience

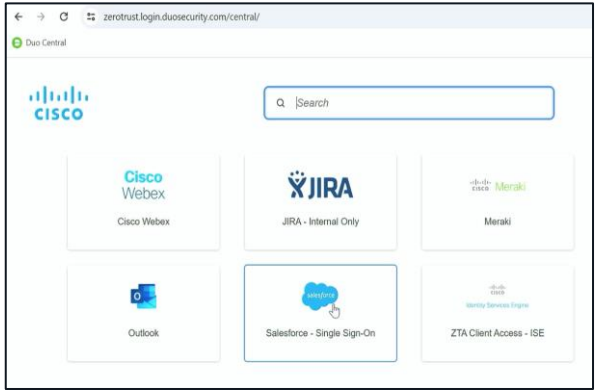
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

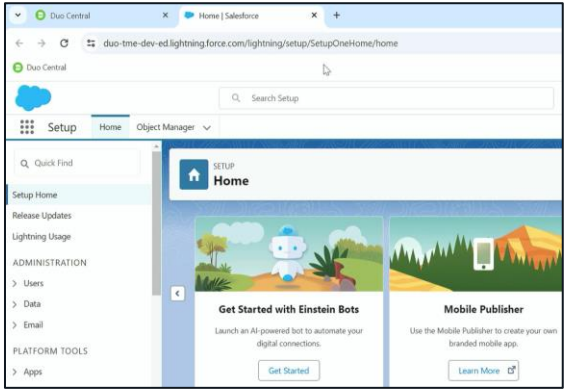
Duo Passport – User Experience

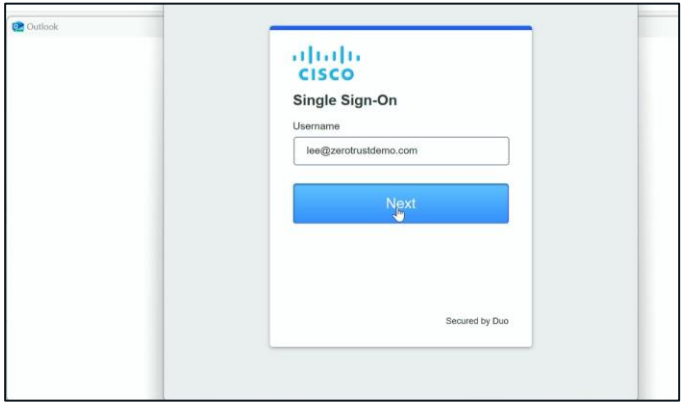


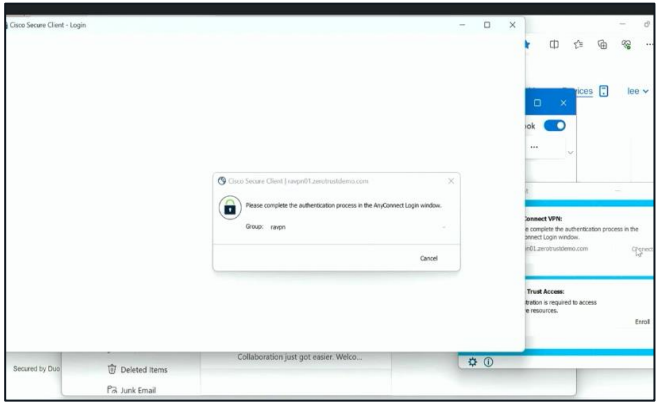
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Duo Passport – User Experience







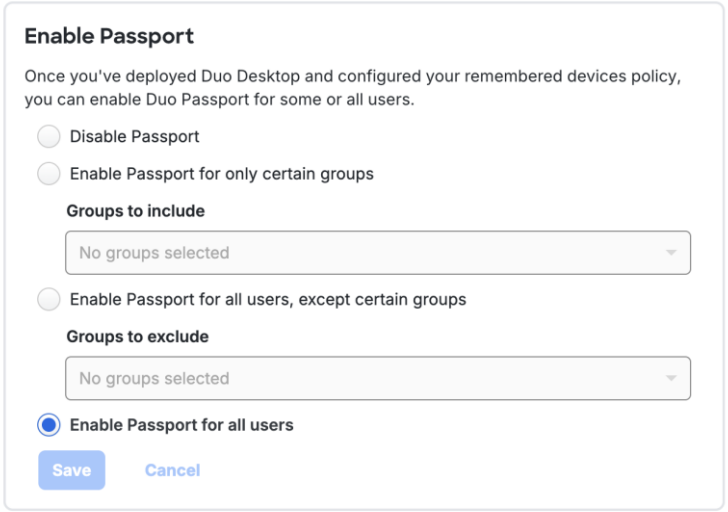


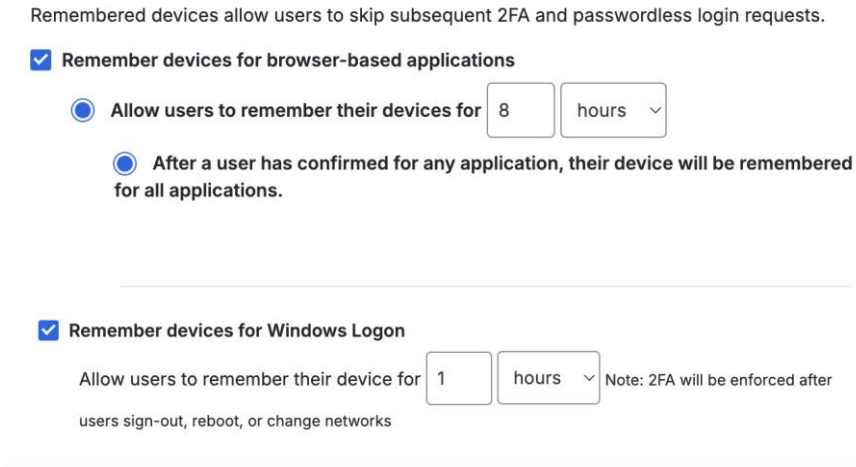
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Duo Passport – User Experience

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Duo Passport – Admin Experience

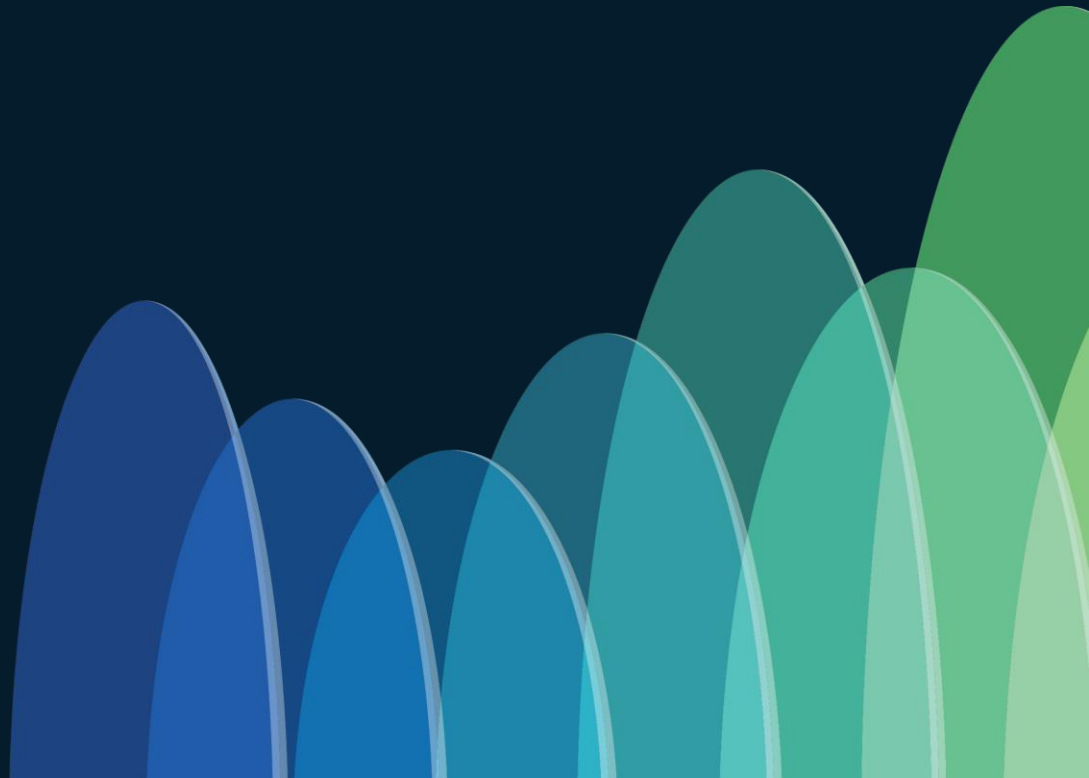




1:47:59 PM 18 SEP 2024	✓ Granted Remembered device via Passport	skishan-admin@bdreams.co	Secure Access-SSO	**No detections**	› Windows 11, version 22H2 (22621.3155) As reported by Duo Desktop	Remembered Device Location Unknown
1:47:57 PM 18 SEP 2024	✓ Granted Remembered device via Passport	skishan-admin@bdreams.co	Secure Access-SSO	**No detections**	› Windows 11, version 22H2 (22621.3155) As reported by Duo Desktop	Remembered Device Location Unknown

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Takeaways



Re-think Identity Security

Identify

- Process and policy
- Governance and lifecycle management
- Identity inventory

Protect

- Effective MFA on every application
- Device posture and trust
- Build dynamic, risk-based access policy

Detect

- Cross platform identity visibility
- Establish behaviour
- Analyse suspicious activity

Respond

- Step-up or block risky logins
- Powerful remediation actions
- Automate quarantine actions

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

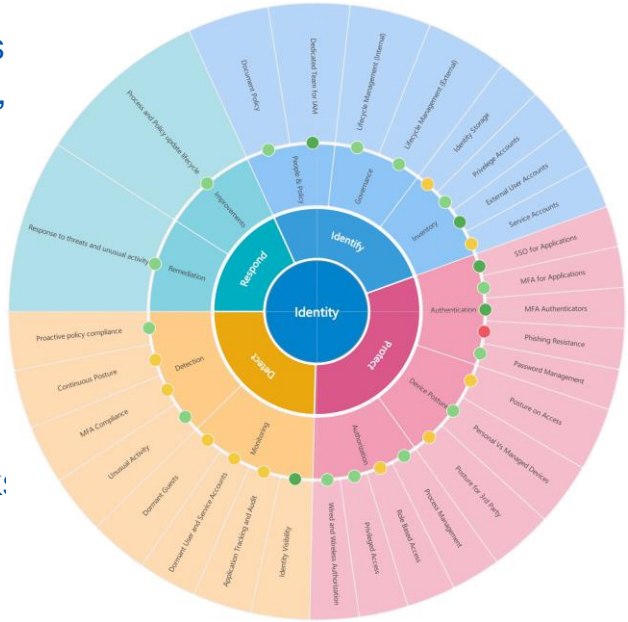
Free Identity Security Assessment

IAM posture evaluation
IAM hygiene review that identifies no/weak MFA, dormant accounts, over-privileged users and more

Identity population insight
Unified view of all identities with detailed
activity and device mappings

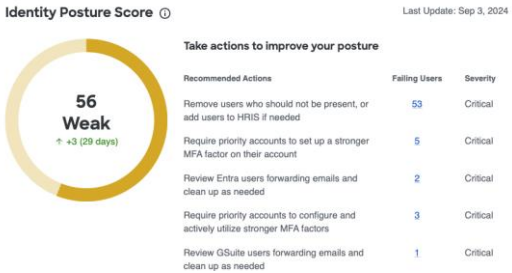
Identity threats
Insight into identity-related attacks

License usage
Idle license insight



Identity Security Workshop / Identity Security Assessment - Register Interest

https://forms.office.com/r/xJBCxyLdRX



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Takeaways

- Identity threats are constantly evolving
- Identity Security needs to go beyond password and MFA controls
  - Identify
  - Protect
  - Detect
  - Respond
- User Experience is equally important
- Cisco Identity Intelligence with Duo Passport provides seamless secure authentication experience

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco Live!

Keynote Deep Dives

Wednesday
10:30am –11:30am

Experiences Amplified: How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106

Smart, Secure, Seamless: Transforming Experiences with Next-Generation Networking

Level 2
Room 204

Harness a Bold New Era: Transform Data Centre and Service Provider Connectivity

Level 2
Room 203

Securing User to Application and Everything in Between

Level 2
Melbourne Room 2

Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

#CiscoLiveAPJC

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

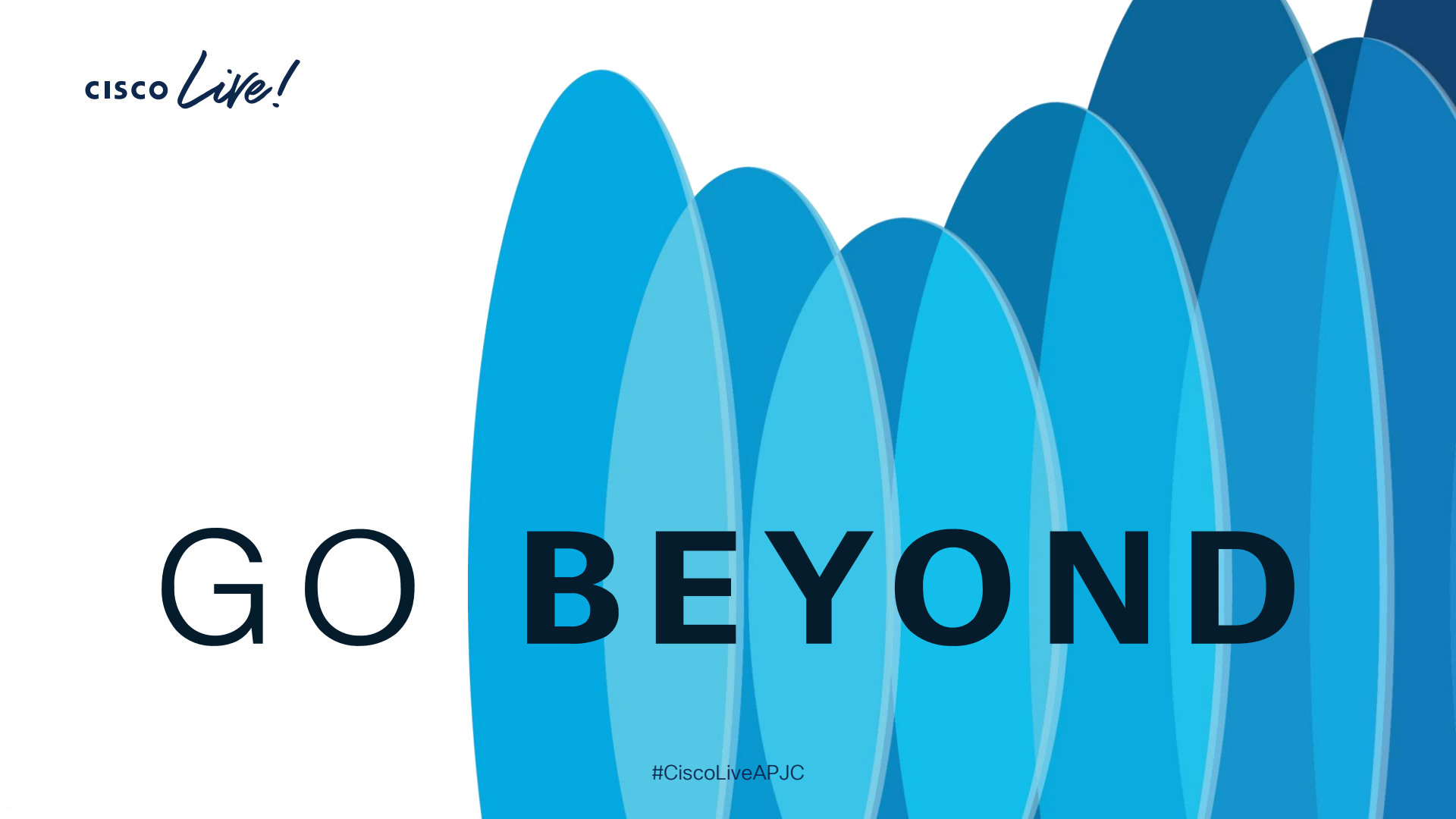
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Register your interest in Identity Security Workshop and Assessment
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC