CYBERARK®

Lessons Learned from Okta

A Security-first Approach to Mitigating Identity Provider Risk

CYBERARK®

Andy Thompson

Andy.Thompson@CyberArk.com

- Global Research Advisor/Evangelist
- SSCP/CISSP
- GPEN Pen-tester
- Dallas Hackers Association
- Travel-Hacker

- Linkedin: in/andythompsoninfosec
- GitHub: github.com/binarywasp
- Twitter: @R41nMkr

Cast of Characters

Okta

- Identity & Access Management
- San Francisco, CA

Sitel/Sykes

- Managed Service Provider
- Miami, FL

LAPSUS$

LAPSUS$

- Threat Actor
- South American (Brazil?) based.

Okta's Published Timeline

- **January 20, 2022**
  - Okta Discovers Intrusion
- **March 17, 2022**
  - Okta receives report from Sitel indicating breach
- **March 22, 2022**
  - LAPSUS$ shares screenshots online
  - Okta publishes blog announcing breach

https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise
https://www.okta.com/blog/2022/03/oktas-investigation-of-the-january-2022-compromise/

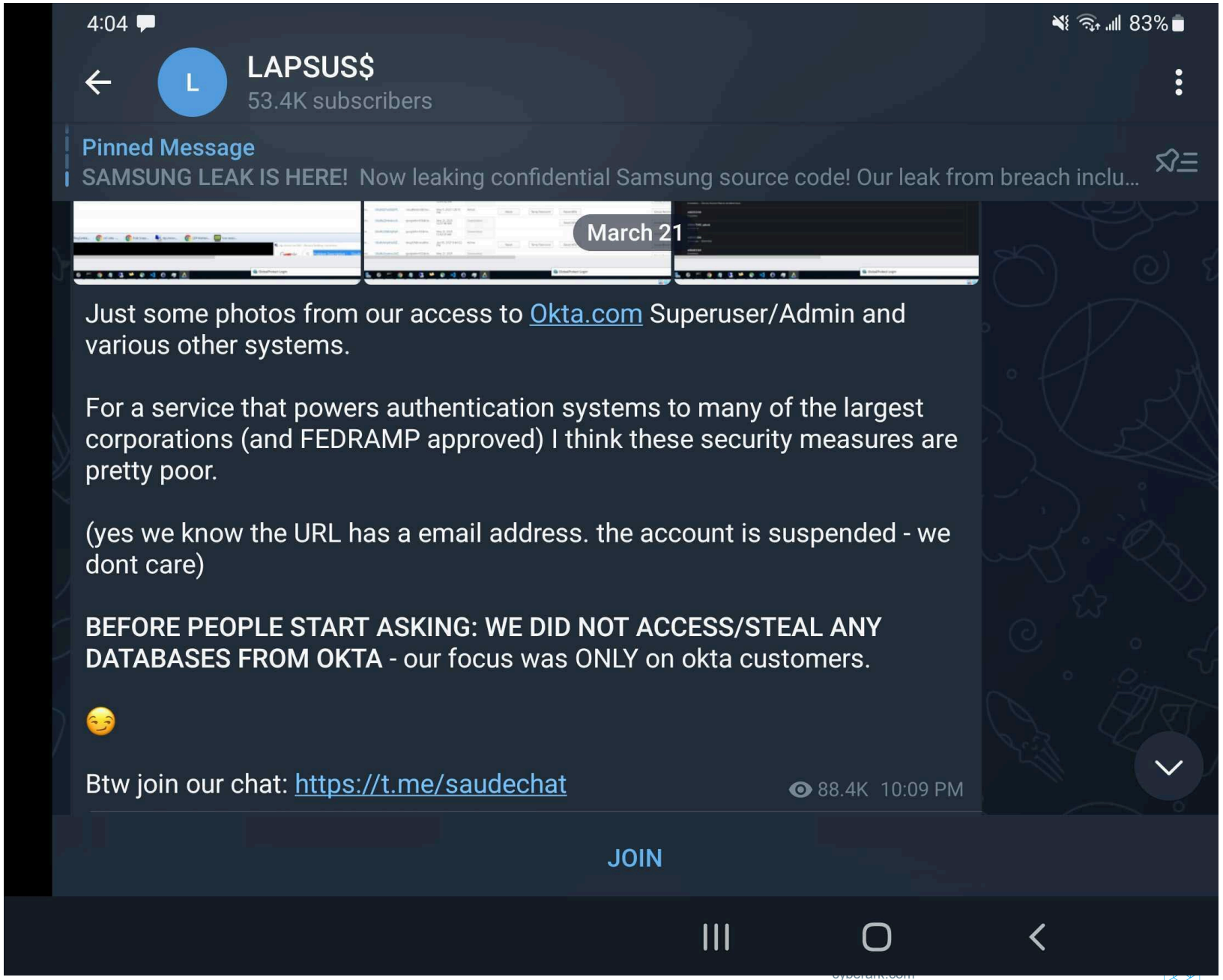
Intrusion Timeline

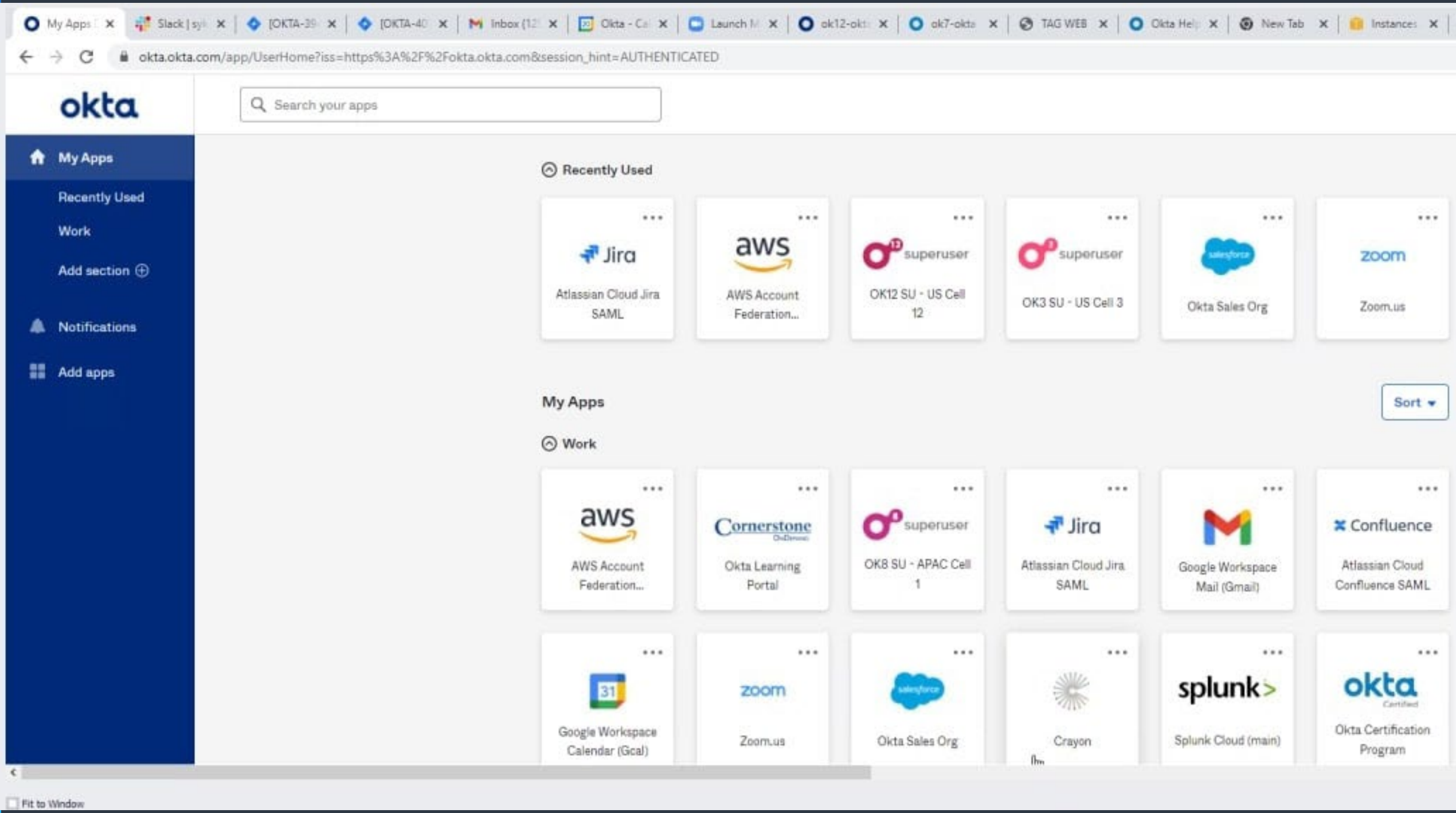
Table 1 lists the major dates, associated events, and the applicable attack phase for the intrusion. All timestamps in this report are in Coordinated Universal Time (UTC), unless otherwise noted. For a detailed description of each attack phase, refer to **Appendix A: Targeted Attack Lifecycle.**

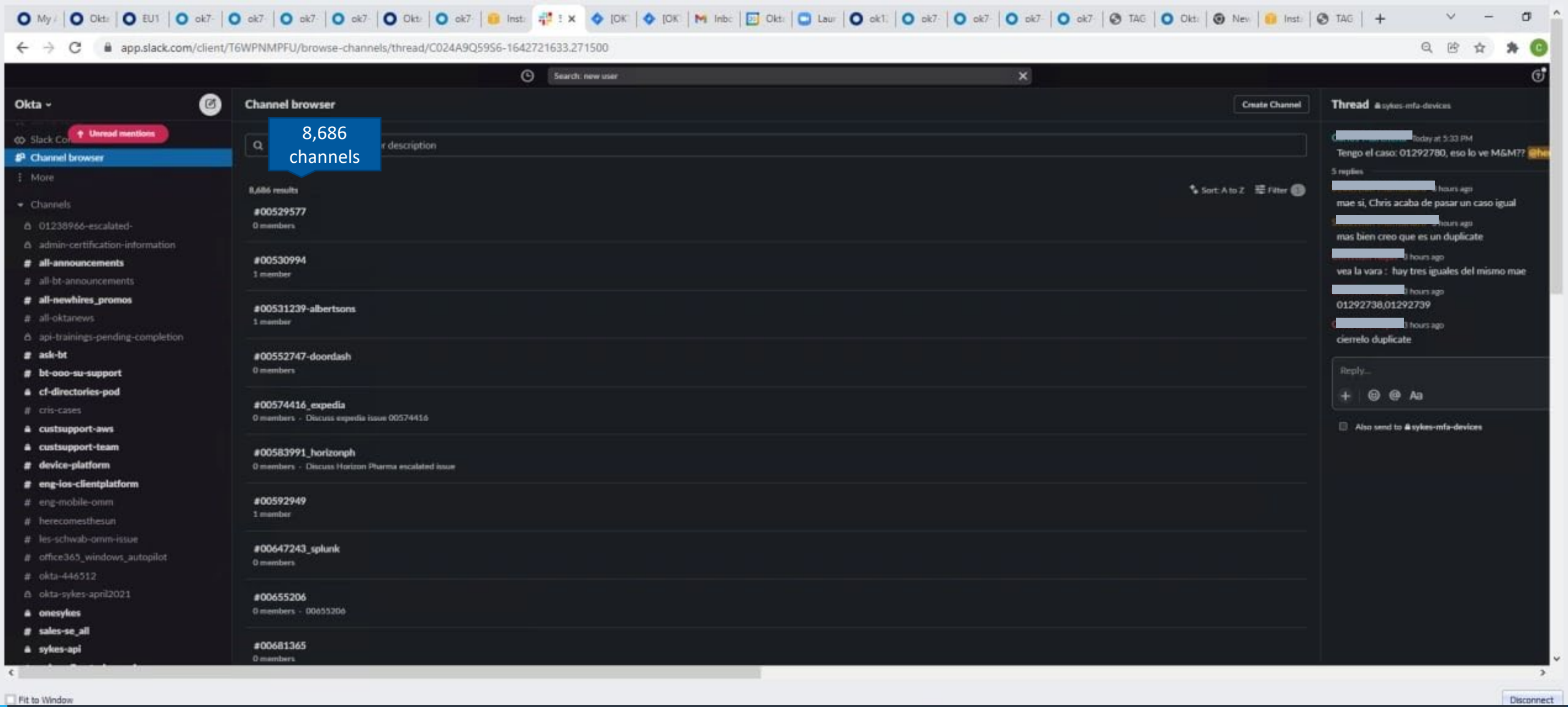
Date (UTC)	Event	Attack Phase
2022-01-16 00:33:23	First logon event from [SYSTEM NAME REDACTED]. Logon to [SYSTEM NAME REDACTED] from [SYSTEM NAME REDACTED] (10.112.137.64)	Initial Compromise
2022-01-19 19:19:47	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Initial Compromise
2022-01-19 19:45:39	Bing search for Privilege escalation tools on Github by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01 19:47:58	UserProfileSvcEop.exe downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:31:19	Account [ACCOUNT NAME REDACTED] created on [SYSTEM NAME REDACTED]	Maintain Presence
2022-01-20 18:32:32	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Move Laterally
2022-01-20 18:39:43	Bing search for Process Explorer by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:40:04	Process Explorer executed by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:43:51	Bing search for Process Hacker by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:01	Process Hacker downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:17	Process Hacker execution by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:46:22	FireEye Endpoint Agent service terminated on [SYSTEM NAME REDACTED]	Establish Foothold
2022-01-20 18:46:55	Bing search for Mimikatz by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:48:28	Mimikatz downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:50:10	Mimikatz executed by [ACCOUNT NAME REDACTED] on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:55:29	C:\Windows\System32\sam.hiv created on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:55:41	C:\sam.hiv created on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:56:00	C:\system.hiv created on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:57:17	C:\Users\[ACCOUNT NAME REDACTED]\Documents\mimikatz_trunk\x64\hash.txt	Escalate Privileges
2022-01-20 18:58:05	hxxps://pastebin.com/7E30i24r by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 19:06:43	RDP logon by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED] from [SYSTEM NAME REDACTED]	Move Laterally
2022-01-20 19:53:31	Bing search for Process Hacker by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 19:55:37	Process Hacker downloaded from hxxps://objects.githubusercontent.com	Establish Foothold
2022-01-20 19:55:58	Bing search for Mimikatz by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 19:57:07	Mimikatz downloaded from hxxps://github.com by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 20:58:31	RDP disconnect from [SYSTEM NAME REDACTED] by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED]	Move Laterally
2022-01-20 23:02:41	First malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to O365	Initial Compromise
2022-01-21 00:05:15	[ACCOUNT NAME REDACTED]@sykes[.]com accessed hxxps://[INTERNAL URL REDACTED]/personal/[INTERNAL USER NAME REDACTED]/Documents/Projects/ryk/DomAdmins-LastPass.xlsx via SecureLink	Internal Recon
2022-01-21 05:29:50	[ACCOUNT NAME REDACTED] account created by [ACCOUNT NAME REDACTED]@sykes[.]com	Maintain Presence
2022-01-21 05:29:51	[ACCOUNT NAME REDACTED] added to TenantAdmins group by [ACCOUNT NAME REDACTED]@sykes[.]com	Maintain Presence
2022-01-21 05:39:13	Malicious Email Transport rule to forward to BCC all mail to the accounts [ACCOUNT NAME REDACTED]@sykes[.]com and [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-21 14:11:38	Last malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to O365	Complete Mission

LAPSUS$ PR

- Uses Telegram instead of dark web (.onion) sites
- Posts news and updates
- Bit-torrents to data dumps




okta
Search your apps
My Apps
Recently Used
Work
Add section
Notifications
Add apps
Recently Used
Atlassian Cloud Jira SAML
AWS Account Federation...
OK12 SU - US Cell 12
OK3 SU - US Cell 3
Okta Sales Org
Zoom.us
My Apps
Sort
Work
AWS Account Federation...
Okta Learning Portal
OK8 SU - APAC Cell 1
Atlassian Cloud Jira SAML
Google Workspace Mail (Gmail)
Atlassian Cloud Confluence SAML
Google Workspace Calendar (Gcal)
Zoom.us
Okta Sales Org
Crayon
Splunk Cloud (main)
Okta Certification Program


app.slack.com/client/T6WPNMPFU/browse-channels/thread/C024A9Q59S6-1642721633.271500
Okta
Channel browser
Create Channel
8,686 channels
Unread mentions
Channel browser
More
Channels
01238966-escalated-
admin-certification-information
all-announcements
all-bt-announcements
all-newhires_promos
all-oktanews
api-trainings-pending-completion
ask-bt
bt-ooo-su-support
cf-directories-pod
cris-cases
custsupport-aws
custsupport-team
device-platform
eng-ios-clientplatform
eng-mobile-omm
herecomesthesun
les-schwab-omm-issue
office365_windows_autopilot
okta-446512
okta-sykes-april2021
onesykes
sales-se_all
sykes-api
8,686 results
Sort: A to Z
Filter
#00529577
0 members
#00530994
1 member
#00531239-albertsons
1 member
#00552747-doordash
0 members
#00574416_expedia
0 members · Discuss expedia issue 00574416
#00583991_horizonph
0 members · Discuss Horizon Pharma escalated issue
#00592949
1 member
#00647243_splunk
0 members
#00655206
0 members · 00655206
#00681365
0 members
Thread
sykes-mfa-devices
Today at 5:33 PM
Tengo el caso: 01292780, eso lo ve M&M??
5 replies
mae si, Chris acaba de pasar un caso igual
mas bien creo que es un duplicate
vea la vara : hay tres iguales del mismo mae
01292738,01292739
cierrelo duplicate
Reply...
Also send to sykes-mfa-devices
Fit to Window
Disconnect

oktainc.atlassian.net/browse/OKTA-394994

Your work | Projects | Filters | Dashboards | People | Apps | Create | Search

Add a comment...

Pro tip: press M to comment

Edit · Delete

June 2, 2021, 9:19 PM

>create an app instance for us to make sure

Can you elaborate on it? Are you asking to remove the "Microsoft ADFS (MFA)" app once and create the same app and reconfigure everything again?

Edit · Delete

MM June 2, 2021, 2:28 PM

Can you ask the customer to verify again? The changes we have applied seems to have been overridden, we are figuring out why it happened. We have applied the app version again, so the customer should be able to test it out now.

Could you also ask them to create an app instance for us to make sure the issuer modes are set properly in the database?

Edit · Delete

MM June 1, 2021, 6:09 PM

We are checking to see if the applied changes are still in place.

Edit · Delete

HH June 1, 2021, 6:06 PM

Analysed the latest har file. I see the issuer in the idtoken is set to https://zen2dev.okta.com when its expected to be https://login.zen2dev.jp

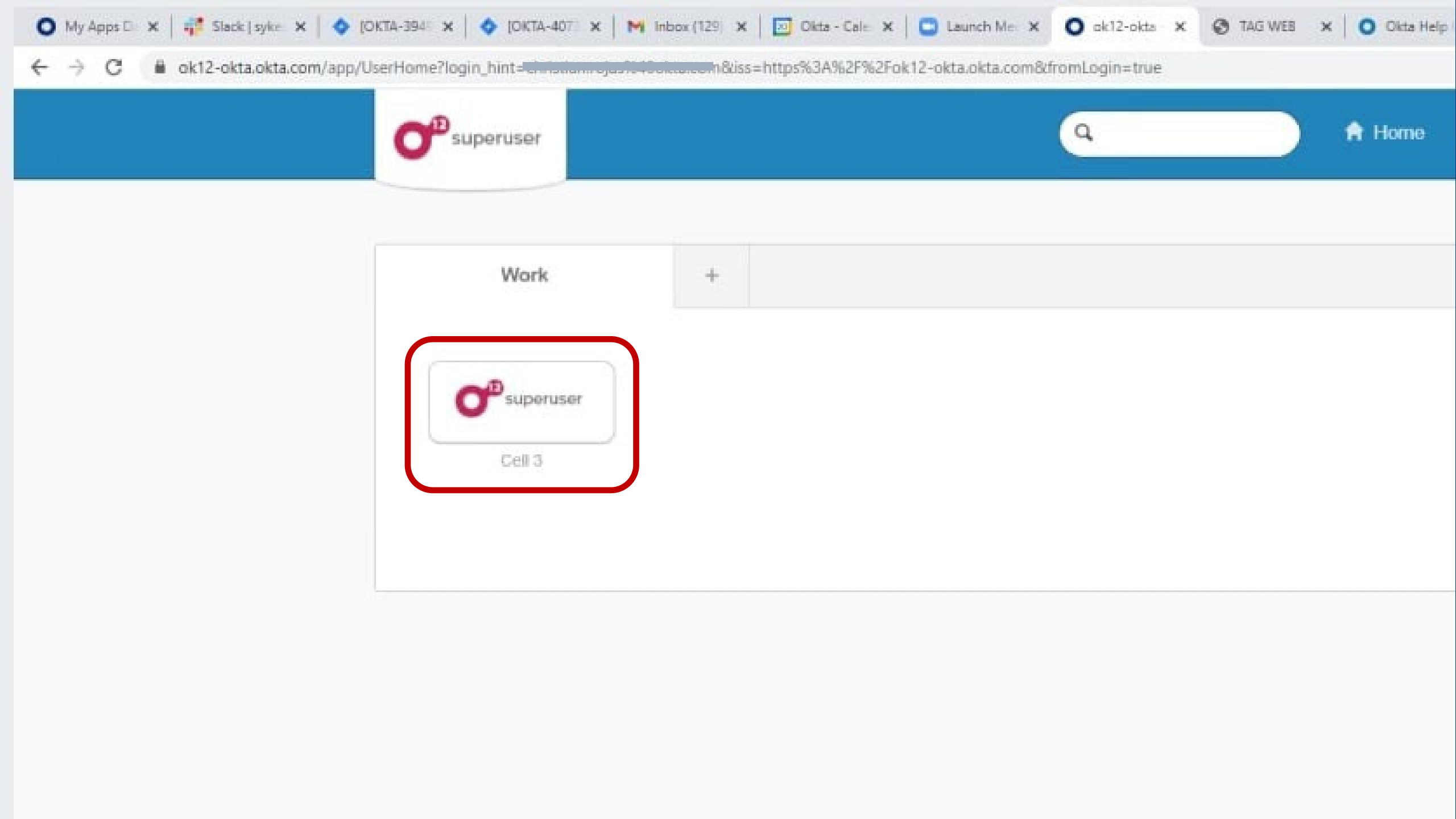
11

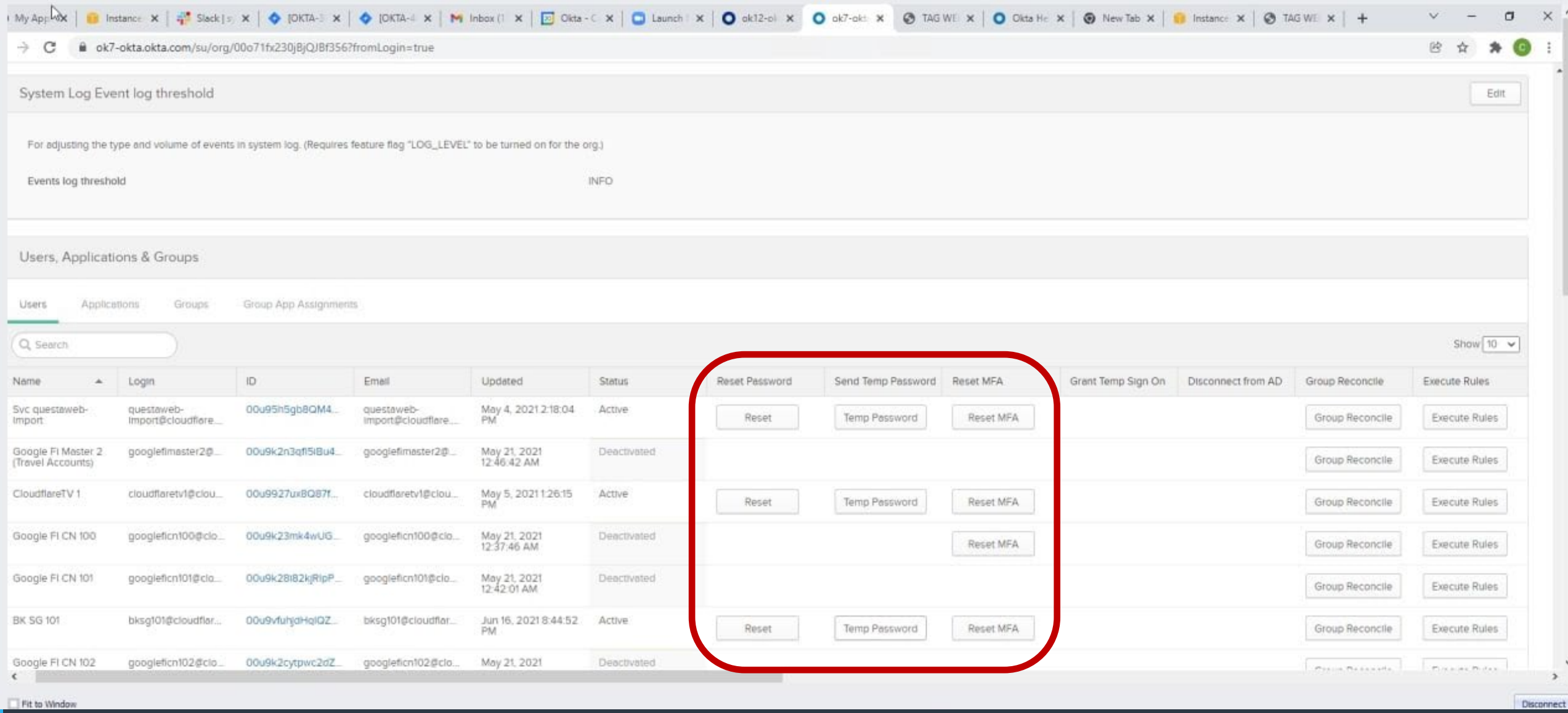
Resolved | Done

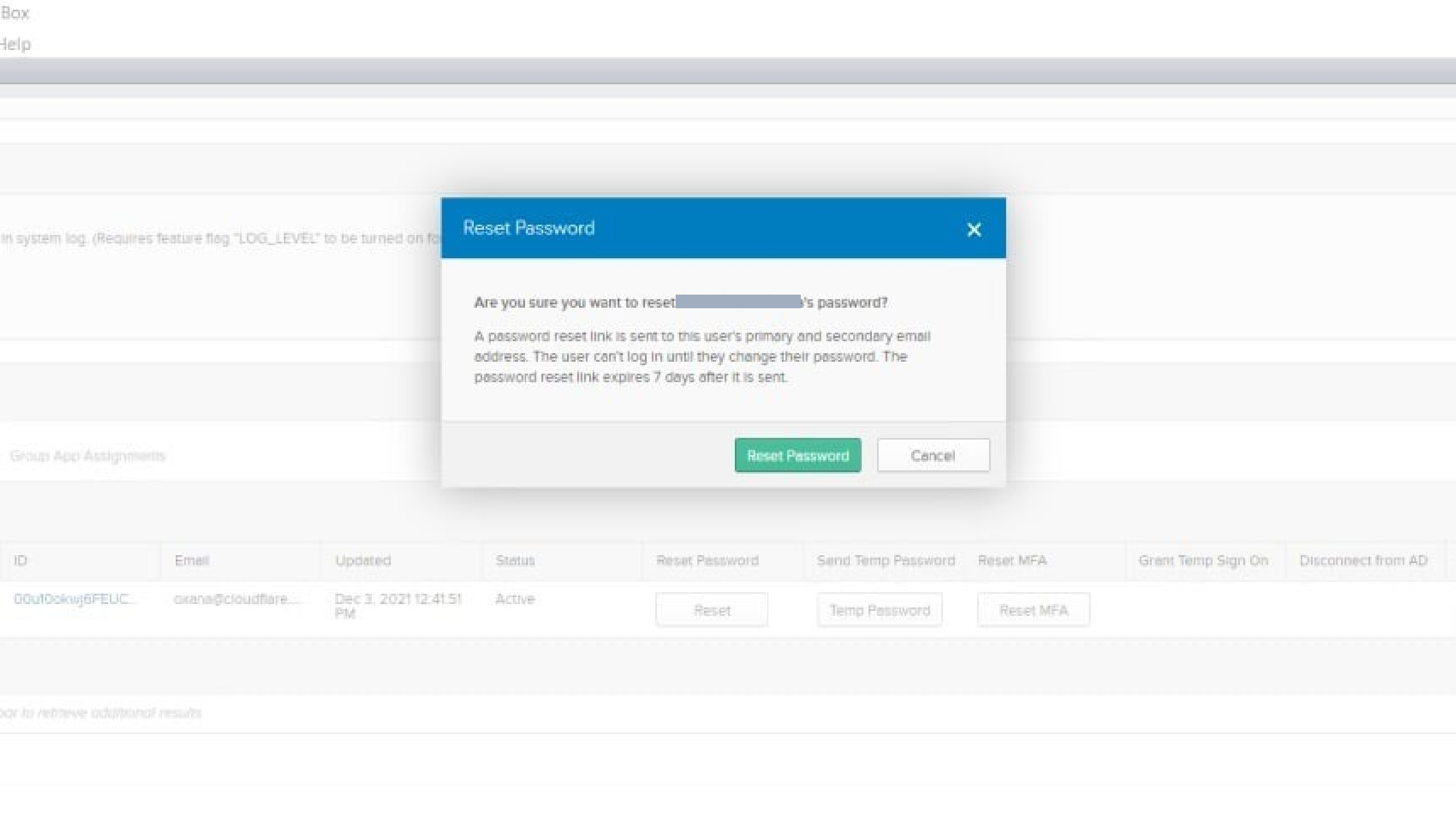
Details

Assignee	MM
Reporter	
Components	Team: EEP, Team: EnterpriseAuth, Team: Federation
Development	Create Branch, 1 pull request
Labels	Support_EEP, home_handoff
Affected Customer(s)	
Reason if JIRA is blocked	not currently blocked
Support Ticket ID	01050881
Eng Mgr Review of Regression	None
Root Cause	None

Fit to Window


My Apps
Slack | syke
[OKTA-394
[OKTA-407
Inbox (129)
Okta - Cale
Launch Me
ok12-okta
TAG WEB
Okta Help
ok12-okta.okta.com/app/UserHome?login_hint=
n&iss=https%3A%2F%2Fok12-okta.okta.com&fromLogin=true
superuser
Home
Work
+
superuser
Cell 3


ok7-okta.okta.com/su/org/00o71fx230j8jQJBf356?fromLogin=true
System Log Event log threshold
Edit
For adjusting the type and volume of events in system log. (Requires feature flag "LOG_LEVEL" to be turned on for the org.)
Events log threshold
INFO
Users, Applications & Groups
Users
Applications
Groups
Group App Assignments
Search
Show 10
Name
Login
ID
Email
Updated
Status
Reset Password
Send Temp Password
Reset MFA
Grant Temp Sign On
Disconnect from AD
Group Reconcile
Execute Rules
Svc questaweb-import
questaweb-import@cloudflare...
00u95h5gb8QM4...
questaweb-import@cloudflare...
May 4, 2021 2:18:04 PM
Active
Reset
Temp Password
Reset MFA
Group Reconcile
Execute Rules
Google FI Master 2 (Travel Accounts)
googlefimaster2@...
00u9k2n3qfl5iBu4...
googlefimaster2@...
May 21, 2021 12:46:42 AM
Deactivated
Group Reconcile
Execute Rules
CloudflareTV 1
cloudflaretv1@clou...
00u9927ux8Q87f...
cloudflaretv1@clou...
May 5, 2021 1:26:15 PM
Active
Reset
Temp Password
Reset MFA
Group Reconcile
Execute Rules
Google FI CN 100
googleficn100@clo...
00u9k23mk4wUG...
googleficn100@clo...
May 21, 2021 12:37:46 AM
Deactivated
Reset MFA
Group Reconcile
Execute Rules
Google FI CN 101
googleficn101@clo...
00u9k28i82kjRipP...
googleficn101@clo...
May 21, 2021 12:42:01 AM
Deactivated
Group Reconcile
Execute Rules
BK SG 101
bksg101@cloudflar...
00u9vfuhjdHqlQZ...
bksg101@cloudflar...
Jun 16, 2021 8:44:52 PM
Active
Reset
Temp Password
Reset MFA
Group Reconcile
Execute Rules
Google FI CN 102
googleficn102@clo...
00u9k2cytpwc2dZ...
googleficn102@clo...
May 21, 2021
Deactivated
Fit to Window
Disconnect


Box
Help
in system log. (Requires feature flag "LOG_LEVEL" to be turned on fo
Reset Password
Are you sure you want to reset 's password?
A password reset link is sent to this user's primary and secondary email address. The user can't log in until they change their password. The password reset link expires 7 days after it is sent.
Reset Password
Cancel
Group App Assignments
ID
Email
Updated
Status
Reset Password
Send Temp Password
Reset MFA
Grant Temp Sign On
Disconnect from AD
00ul0ckwj6FEUC...
oxana@cloudflare....
Dec 3, 2021 12:41:51 PM
Active
Reset
Temp Password
Reset MFA
oor to retrieve additional results

Immediate actions if you suspect your IdP is compromised.

Check your logs

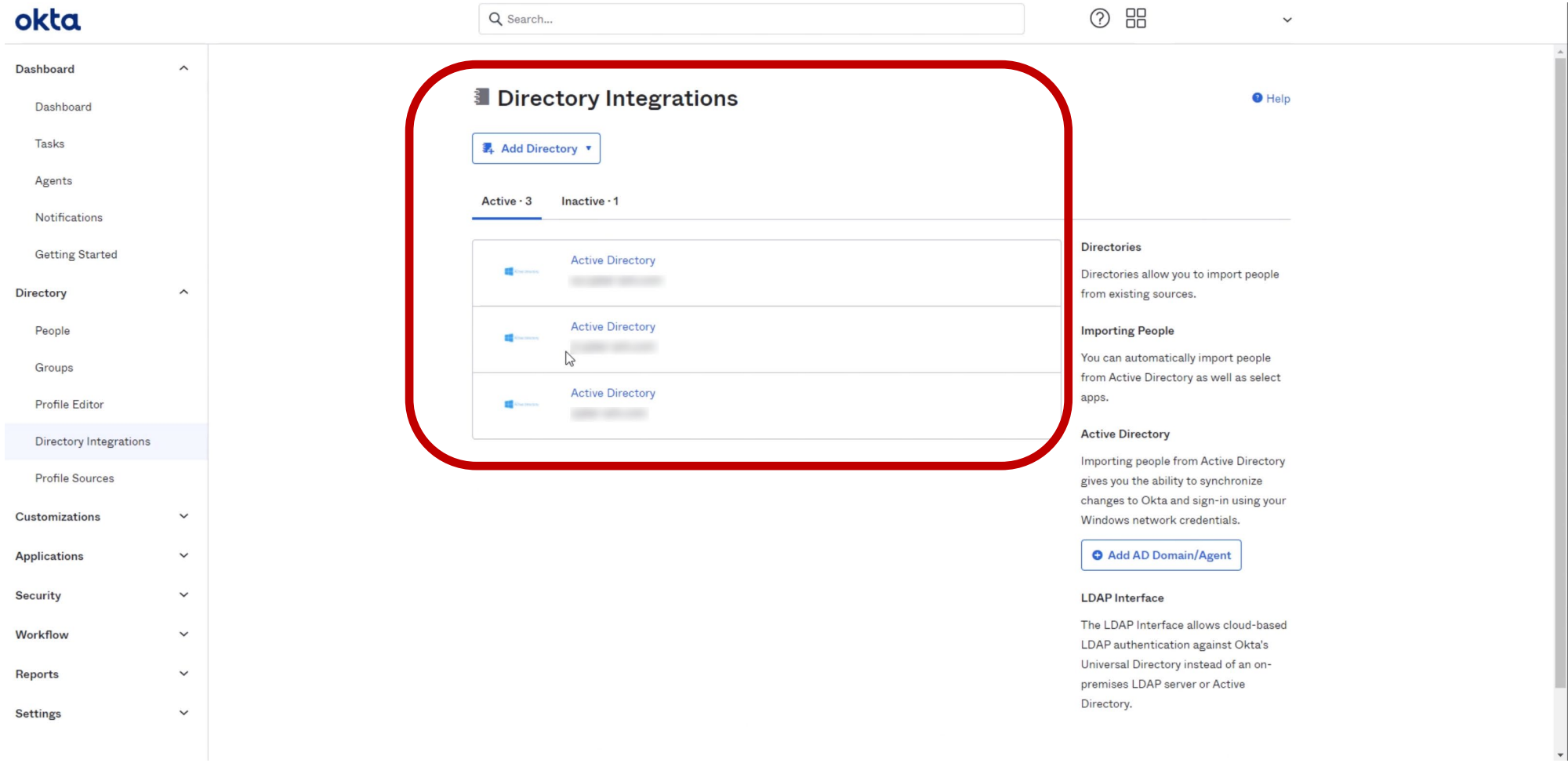
- New MFA devices or changes
- MFA configuration changes
- Identity Provider (IdP) configuration changes
- Password and MFA reset attempts
- Permission and role changes and the creation of new users.

Okta-specific configurations

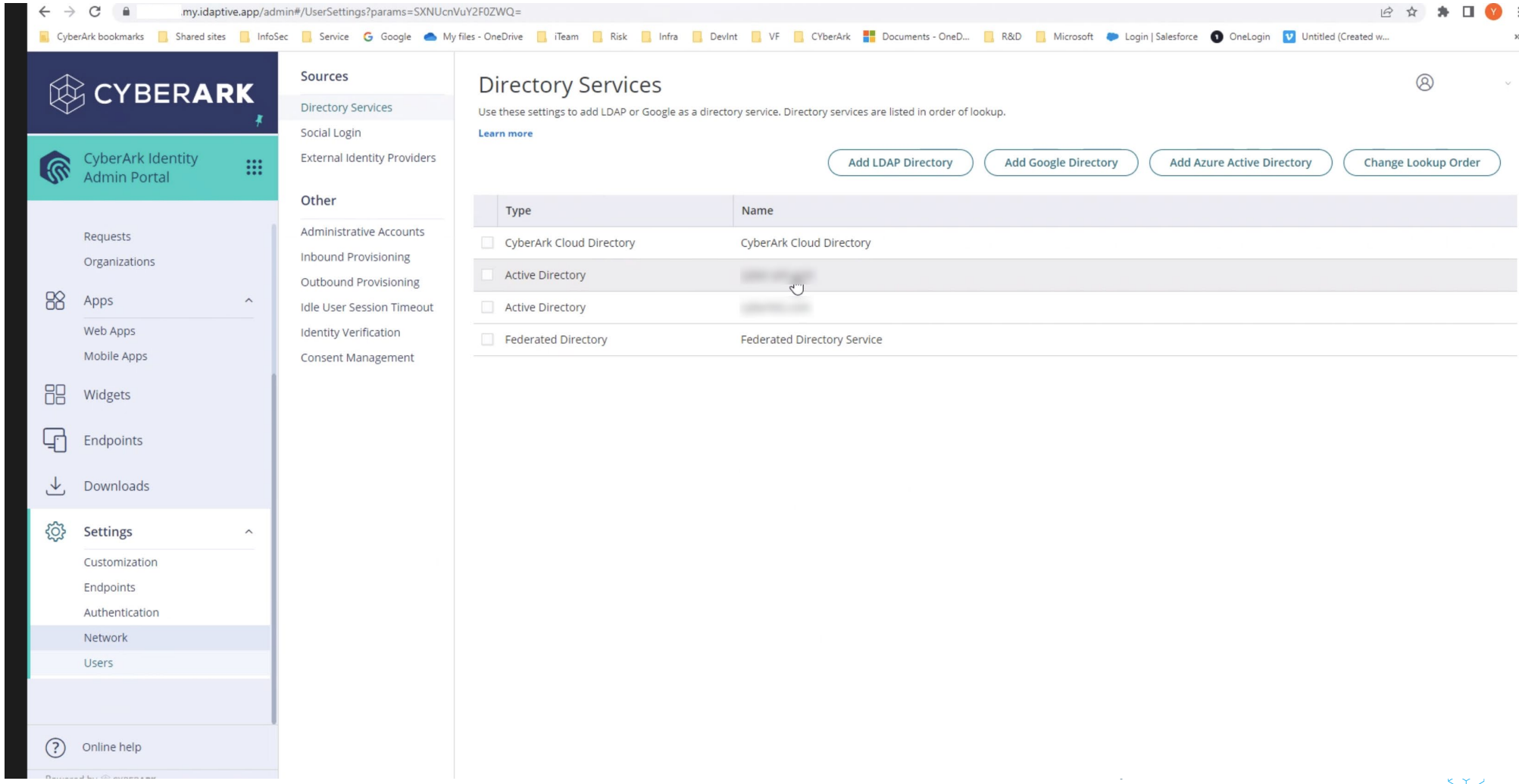
user.account.reset_password
user.mfa.factor.update
system.mfa.factor.deactivate
user.mfa.attempt_bypass
user.session.impersonation.initiate

severity	event_type	display_message	timestamp	outcome.result	outcome.reason	actor.id
INFO	user.mfa.factor.deactivate	Reset factor for user	2022-03-10T00:53:02.836Z	SUCCESS	User reset OKTA_SOFT_TOKEN factor	00ucbibecrz2cS8CL1t7
INFO	user.mfa.factor.deactivate	Reset factor for user	2022-02-17T17:37:48.078Z	SUCCESS	User reset DUO_SECURITY factor	00uj5svjyiG8Yj8LG1t7
INFO	user.mfa.factor.deactivate	Reset factor for user	2022-01-04T05:29:21.681Z	SUCCESS	User reset OKTA_SOFT_TOKEN factor	00ulgn3d1aU3n7dIN1t7
INFO	user.mfa.factor.deactivate	Reset factor for user	2021-10-14T06:14:03.616Z	SUCCESS	User reset OKTA_SOFT_TOKEN factor	00ui8yhlfmASENQ2L1t7
INFO	user.mfa.factor.deactivate	Reset factor for user	2021-10-25T12:11:26.153Z	SUCCESS	User reset OKTA_SOFT_TOKEN factor	00ujqcxvey4P3NZcg1t7

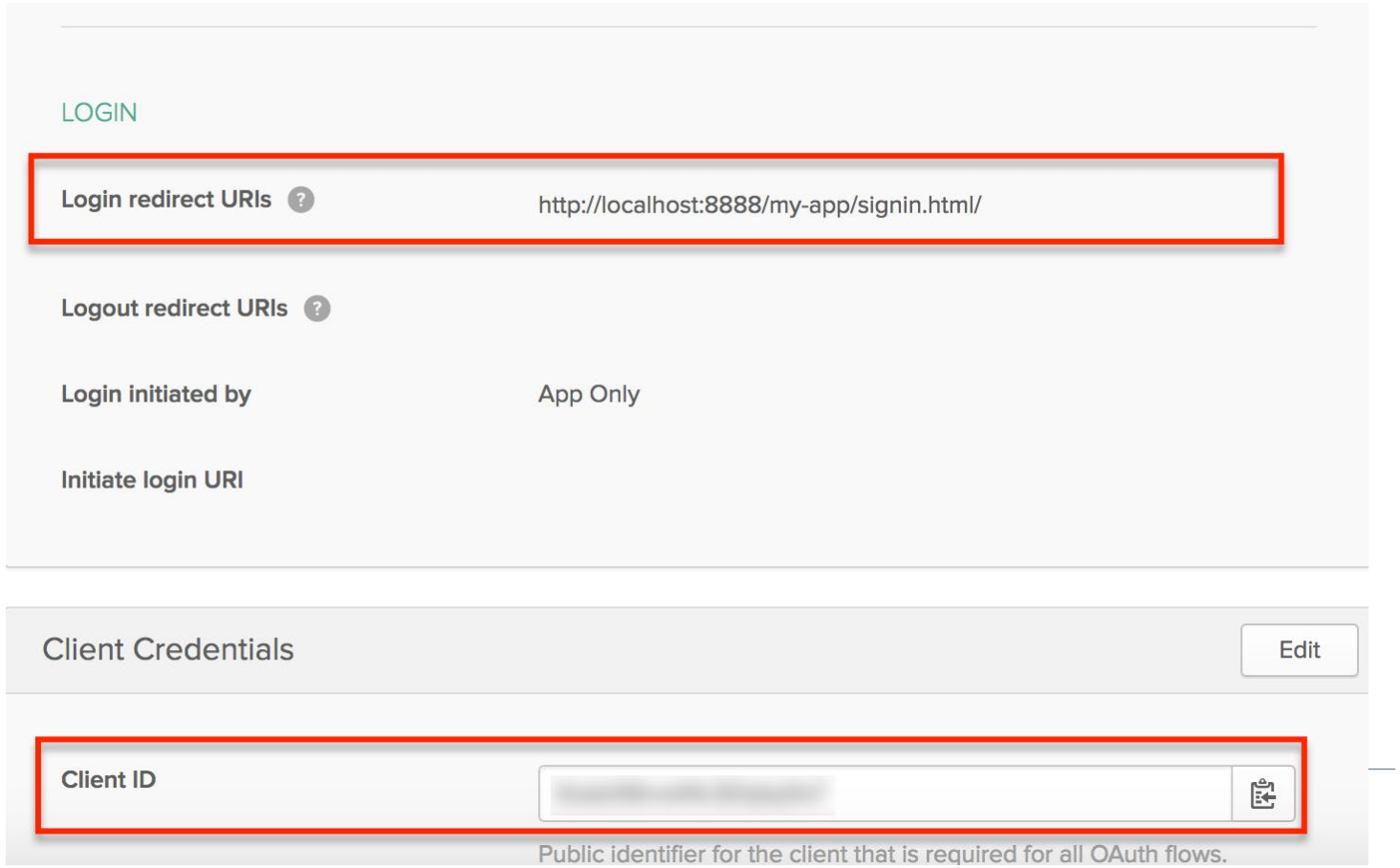
Confirm your AD integrations



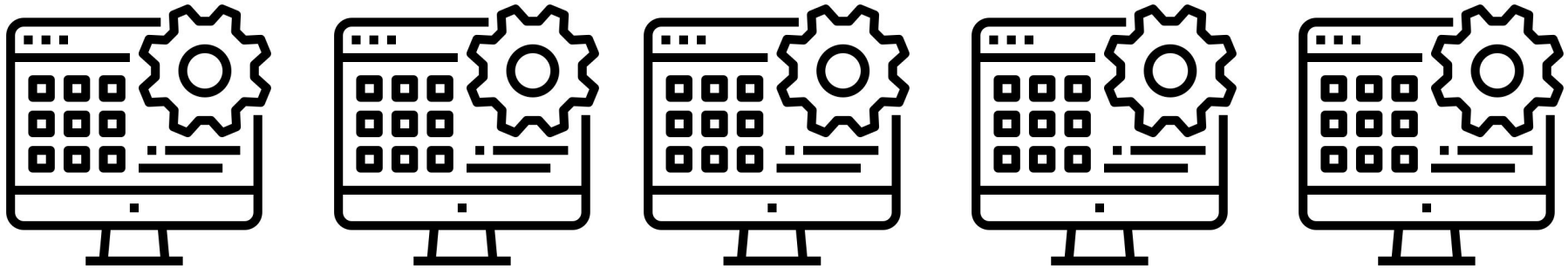
Review your directory sources



Look for advanced attack methods



Verify your apps



Implement Least Privilege

- Just-in-Time
- Dynamic elevation capabilities
- MFA Policies

Rotate credentials

- Rotate **ALL** privileged accounts
- Strong Credentials
  - Complex
  - Unique
  - Frequently changing

Restrict Access

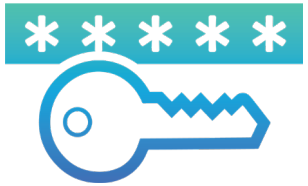
- Specific managed devices
- Management subnets
- Privileged Access Management (PAM) solutions

Multi-layered approach to Identity Security

Monitor and audit
high-risk web sessions

Secure access
with MFA

Provide secure
third-party access

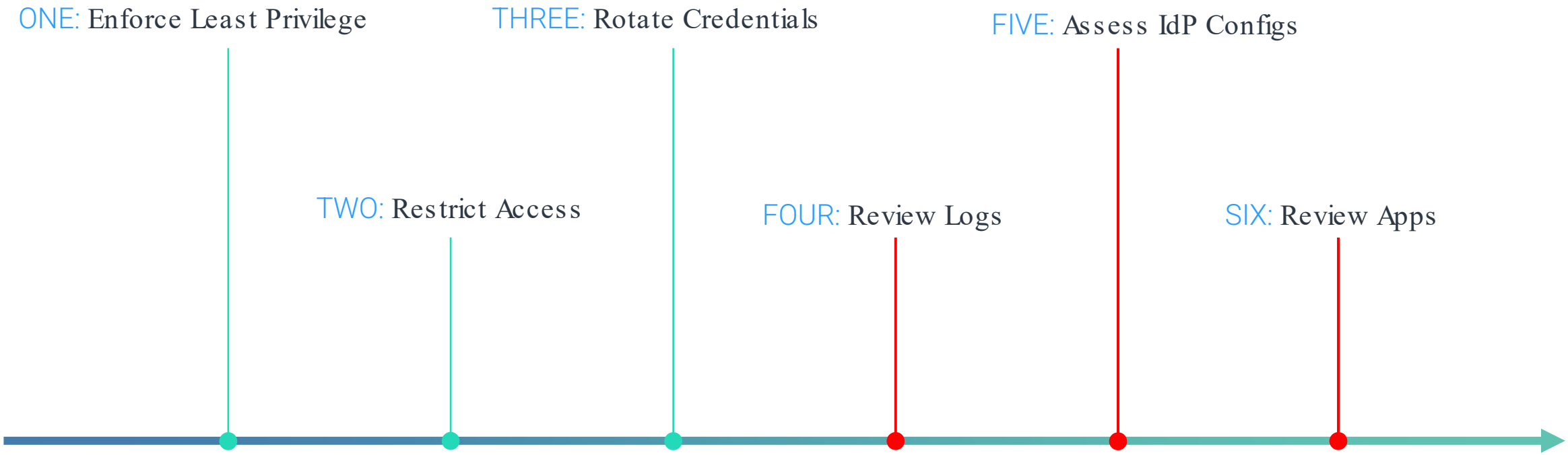


Secure credentials
and items

Protect endpoints and
enforce least privilege

Key Takeaways

Six actions for success in Identity Security



Next steps

- **Evaluate** your IT landscape and existing controls
- **Prioritize** access controls to Tier-0 infrastructure and high-risk applications
- **Understand** how defense-in-depth can close security gaps and provide additional assurances

More Information

- Visit Okta-LAPSUS$ resources page
- Contact CyberArk remediation services
- Sign-up for our defense-in-depth webinar