



Lessons Learned from Okta

A Security-first Approach to Mitigating
Identity Provider Risk





Andy Thompson

Andy.Thompson@CyberArk.com

- Global Research Advisor/Evangelist
- SSCP/CISSP
- GPEN Pen-tester
- Dallas Hackers Association
- Travel-Hacker
- LinkedIn: [in/andythompsoninfosec](https://www.linkedin.com/in/andythompsoninfosec)
- GitHub: github.com/binarywasp
- Twitter: [@R41nMkr](https://twitter.com/R41nMkr)



Cast of Characters



okta

Okta

- Identity & Access Management
- San Francisco, CA



Site/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



Intrusion Timeline

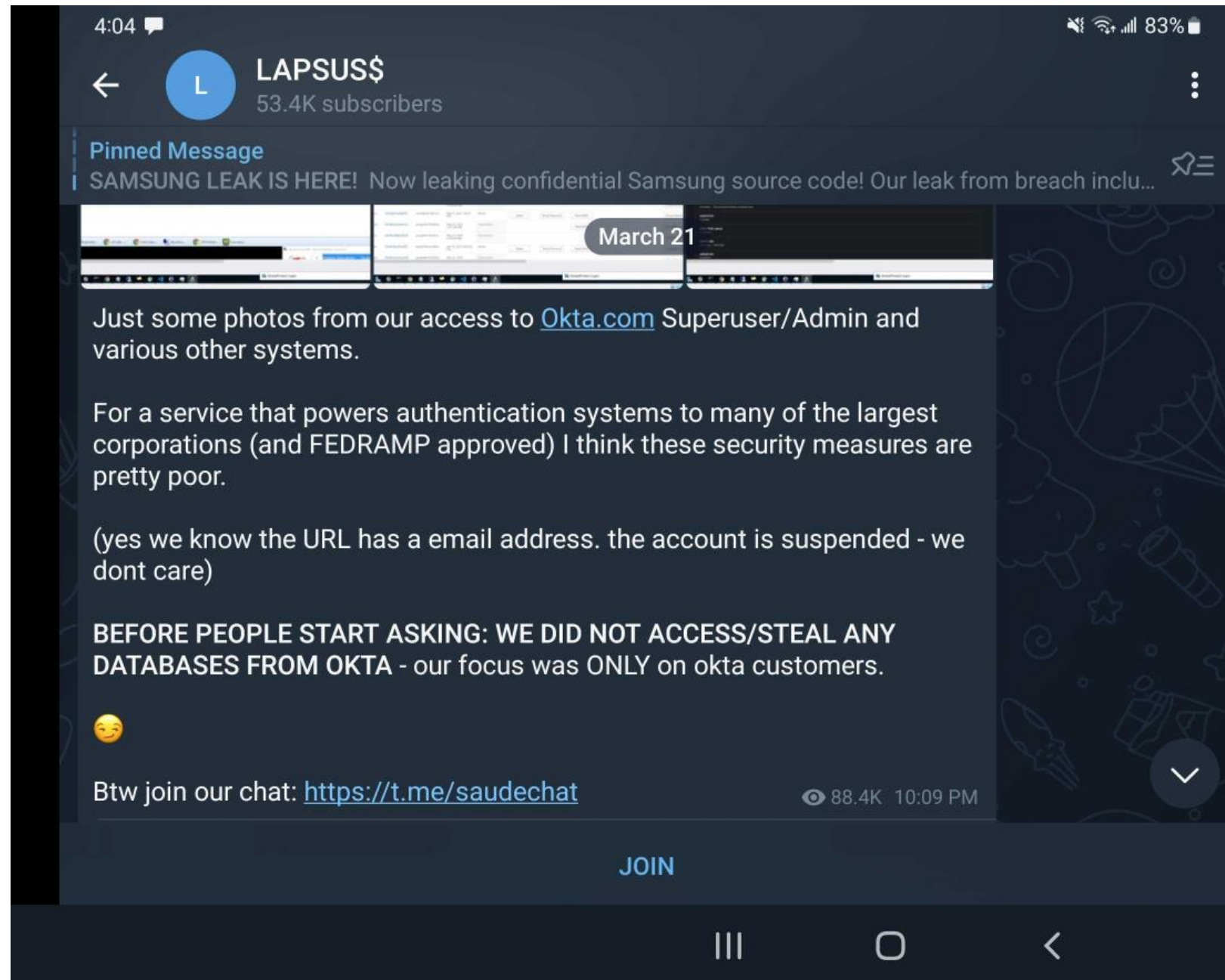
Table 1 lists the major dates, associated events, and the applicable attack phase for the intrusion. All timestamps in this report are in Coordinated Universal Time (UTC), unless otherwise noted. For a detailed description of each attack phase, refer to **Appendix A: Targeted Attack Lifecycle**.

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

My Apps

Recently Used

Work


Add section +

Notifications

Add apps


Search your apps

Recently Used




Jira

Atlassian Cloud Jira SAML




aws

AWS Account Federation...




superuser

OK12 SU - US Cell 12




superuser

OK3 SU - US Cell 3



Okta Sales Org




Zoom.us

My Apps


Sort ▼

Work




aws

AWS Account Federation...




Okta Learning Portal




superuser

OK8 SU - APAC Cell 1




Jira

Atlassian Cloud Jira SAML




Google Workspace Mail (Gmail)




Confluence


Atlassian Cloud Confluence SAML




Google Workspace Calendar (Gcal)




Zoom.us




Okta Sales Org



Crayon



Splunk Cloud (main)



Okta Certification Program

Okta -

Slack Con

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-omni

herecomessthesun

les-schwab-omni-issue

office365_windows_autopilot

okta-446512

okta-sykes-april2021

onesykes

sales-se_all

sykes-api

Channel browser

Search: new user

8,686 results

#00529577
0 members

#00530994
1 member

#00531239-albertsons
1 member

#00552747-doordash
0 members

#00574416_expedia
0 members - Discuss expedite 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

Create Channel

Thread #sykes-mfa-devices

Today at 5:33 PM

Tengo el caso: 01292780, eso lo ve M&M??

5 replies

hours ago

mae si, Chris acaba de posar un caso igual

hours ago

mas bien creo que es un duplicate

hours ago

vea la vara : hay tres iguales del mismo mae

hours ago

01292738,01292739

hours ago

cierefo duplicate

Reply...

+ @ Aa

Also send to #sykes-mfa-devices



Add a comment...

Pro tip: press **M** to comment

Edit · Delete ·

June 2, 2021, 9:19 PM
[redacted]
> 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 ·

June 2, 2021, 2:28 PM
[redacted] 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 ·

June 1, 2021, 6:09 PM
We are checking to see if the applied changes are still in place.
Edit · Delete ·

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`

Resolved Done

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



Home

Work



Cell 3

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...	00u95n5gb8QM4...	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@...	00u9k2n3qf5iBu4...	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...	00u9k28i82kjRipF...	googleficn101@clo...	May 21, 2021 12:42:01 AM	Deactivated						Group Reconcile	Execute Rules
BK 5G 101	bks101@cloudflar...	00u9vfu1jdHqIQZ...	bks101@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						Group Reconcile	Execute Rules

in system log. (Requires feature flag "LOG_LEVEL" to be turned on for

Reset Password



Are you sure you want to reset [REDACTED]'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
00kd0cknij8FEUC...	osana@cloudflare...	Dec 3, 2021 12:41:51 PM	Active	<button>Reset</button>	<button>Temp Password</button>	<button>Reset MFA</button>		

API 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

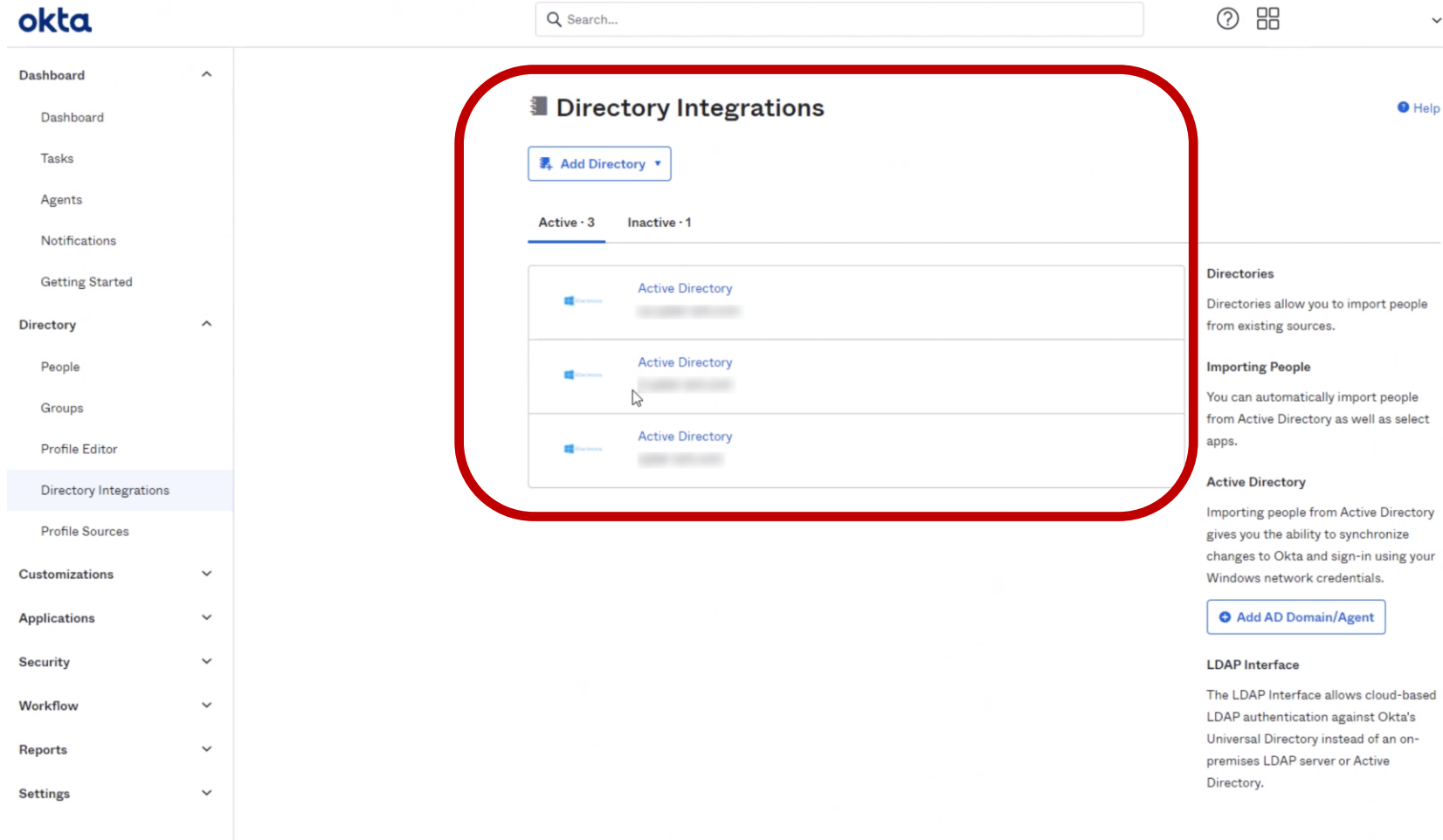
user.session.impersonation.initiate



severity	event_type	display_message	timestamp	outcome.result	outcome.reason	actor.id
INFO	user.mfa.factor.deactivate	Reset factor for user	2022-03-	.836Z SUCCESS	User reset OKTA_SOFT_TOKEN factor	00ucbibecr
INFO	user.mfa.factor.deactivate	Reset factor for user	2022-02-	.078Z SUCCESS	User reset DUO_SECURITY factor	00uj5svjyiC
INFO	user.mfa.factor.deactivate	Reset factor for user	2022-01-	.681Z SUCCESS	User reset OKTA_SOFT_TOKEN factor	00ulgn3d1a
INFO	user.mfa.factor.deactivate	Reset factor for user	2021-10-	.616Z SUCCESS	User reset OKTA_SOFT_TOKEN factor	00ui8yhlfm
INFO	user.mfa.factor.deactivate	Reset factor for user	2021-10-	.153Z SUCCESS	User reset OKTA_SOFT_TOKEN factor	00ujqcxvey



Confirm your AD integrations






The screenshot shows the Okta admin console interface. On the left is a navigation sidebar with the following items: Dashboard, Tasks, Agents, Notifications, Getting Started, Directory (expanded), People, Groups, Profile Editor, Directory Integrations (highlighted), Profile Sources, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area is titled "Directory Integrations" and includes a search bar, a help icon, and a "Help" link. Below the title is an "Add Directory" button. There are two tabs: "Active - 3" (selected) and "Inactive - 1". The "Active" tab displays a list of three "Active Directory" integrations, each with a Microsoft icon and a blurred name. A red rounded rectangle highlights the "Add Directory" button and the list of active integrations. To the right of the list, there are three sections: "Directories" (explaining that directories allow importing people from existing sources), "Importing People" (explaining that people can be imported from Active Directory and select apps), and "Active Directory" (explaining that importing from Active Directory allows synchronizing changes to Okta and sign-in using Windows network credentials). Below these sections are buttons for "Add AD Domain/Agent" and "LDAP Interface" (which explains that the LDAP interface allows cloud-based LDAP authentication against Okta's Universal Directory instead of an on-premises LDAP server or Active Directory).

Directory Integrations [Help](#)

[Add Directory](#)

Active - 3 Inactive - 1

Icon	Name
	Active Directory
	Active Directory
	Active Directory

Directories

Directories allow you to import people from existing sources.

Importing People

You can automatically import people from Active Directory as well as select apps.

Active Directory

Importing people from Active Directory gives you the ability to synchronize changes to Okta and sign-in using your Windows network credentials.

[Add AD Domain/Agent](#)

LDAP Interface

The LDAP Interface allows cloud-based LDAP authentication against Okta's Universal Directory instead of an on-premises LDAP server or Active Directory.



Review your directory sources

The screenshot displays the CyberArk Identity Admin Portal interface. The left sidebar contains the following navigation items: Requests, Organizations, Apps (with a sub-menu for Web Apps and Mobile Apps), Widgets, Endpoints, Downloads, Settings (with sub-items: Customization, Endpoints, Authentication, Network, and Users), and Online help. The main content area is titled 'Directory Services' and includes a description: 'Use these settings to add LDAP or Google as a directory service. Directory services are listed in order of lookup.' Below this, there are four buttons: 'Add LDAP Directory', 'Add Google Directory', 'Add Azure Active Directory', and 'Change Lookup Order'. A table lists the configured directory services:

Type	Name
<input type="checkbox"/> CyberArk Cloud Directory	CyberArk Cloud Directory
<input checked="" type="checkbox"/> Active Directory	Active Directory
<input type="checkbox"/> Active Directory	Active Directory
<input type="checkbox"/> Federated Directory	Federated Directory Service



Look for advanced attack methods

LOGIN

Login redirect URIs ?

http://localhost:8888/my-app/signin.html/

Logout redirect URIs ?

Login initiated by

App Only

Initiate login URI

Client Credentials

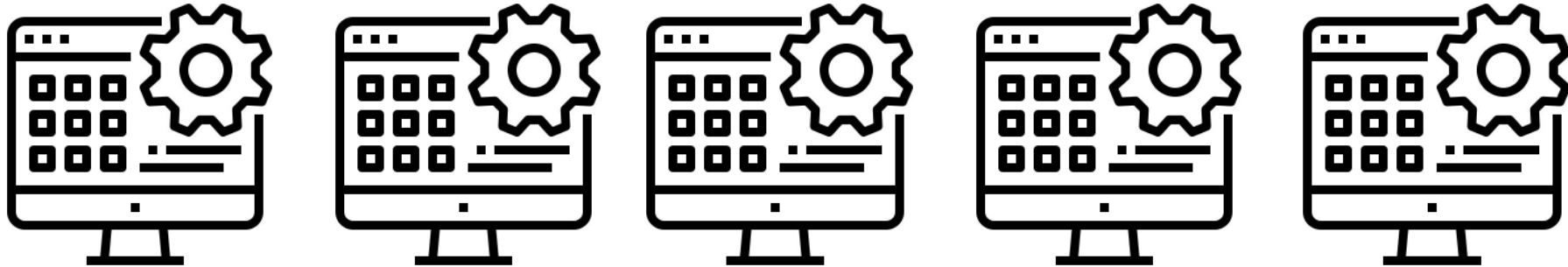
Edit

Client ID

Public identifier for the client that is required for all OAuth flows.



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

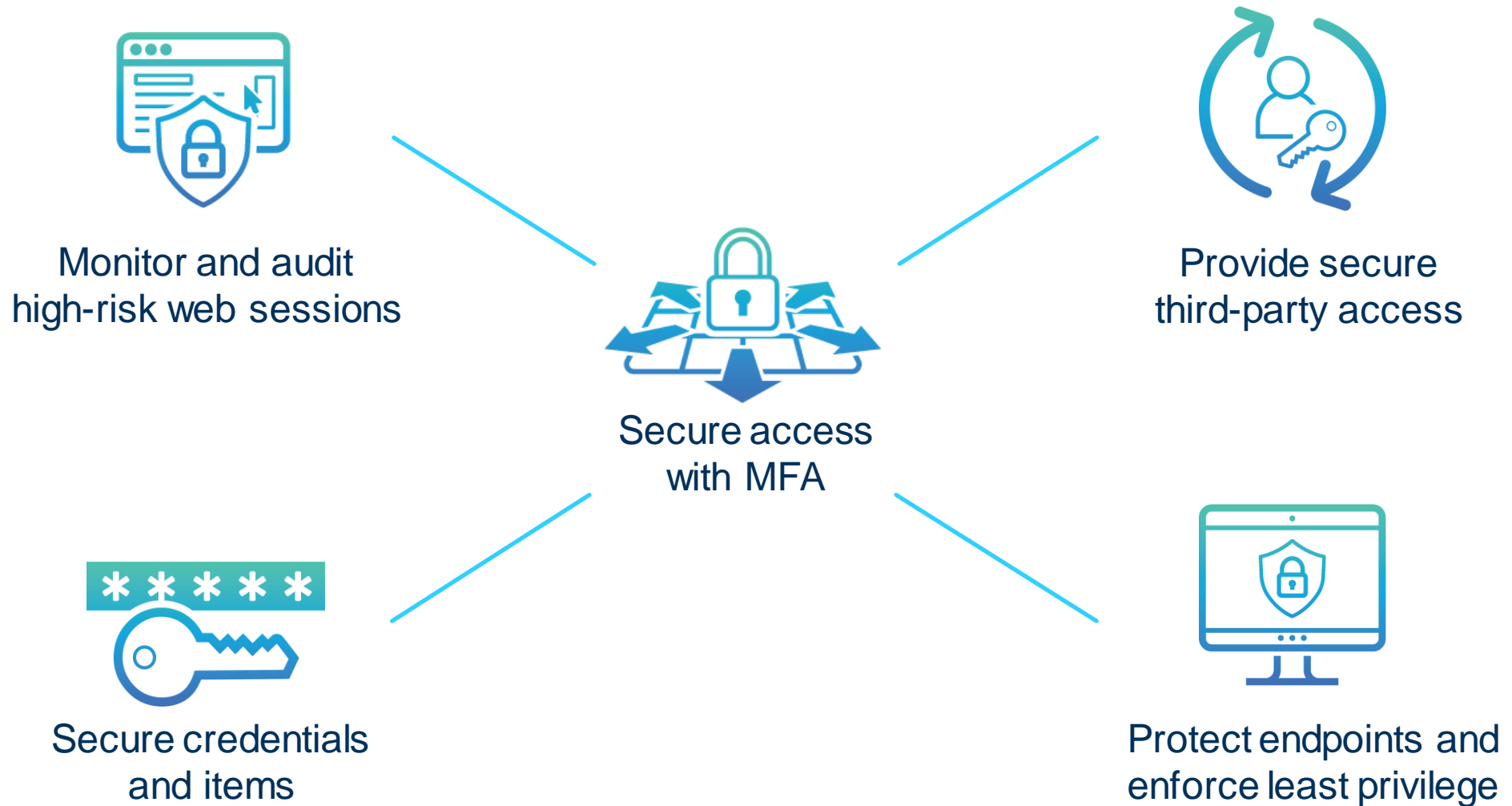


Restrict Access

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



Multi-layered approach to Identity Security



Key Takeaways



Six actions for success in Identity Security

ONE: Enforce Least Privilege

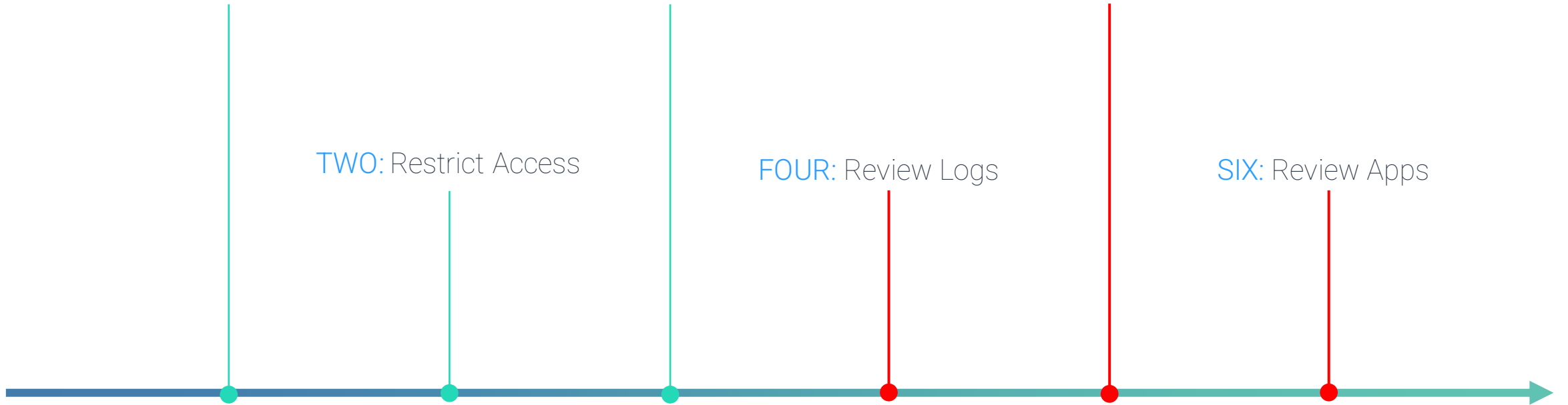
THREE: Rotate Credentials

FIVE: Assess IdP Configs

TWO: Restrict Access

FOUR: Review Logs

SIX: Review Apps



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

