

Okta For Good and Bad

Hybrid Attack Paths Crossing
Okta Organizations

Michael Grafnetter
Principal Security Researcher

Lance Cain
Offensive Security Engineer - Consulting Services



Agenda

- 01 Okta Security Primer
- 02 Okta + Devices
- 03 Okta + JAMF
- 04 Okta + Active Directory
- 05 Okta + GitHub
- 06 BloodHound OpenGraph Collectors

Okta Security Primer

Understanding Okta Attack Paths

Why Okta?



Okta Is Secure by Default

Everybody gets MFA!

Catch-all Rule ENABLED Actions ▾

IF Any request THEN Access: Allowed with any 2 factor types

Your org's authenticators that satisfy this requirement:

Knowledge / Biometric factor types

Password or Okta Verify - FastPass¹

AND

Additional factor types

Google Authenticator or Okta Verify - FastPass¹ or Okta Verify - TOTP

Other authenticators that satisfy this requirement. These need to be configured for authentication:

Security Question or Okta Verify - Push¹ or FIDO2 (WebAuthn)¹ or Custom OTP⁵ or Email or Phone - SMS or Phone - Voice or Duo Security or IdP Authenticator - IdP Authenticator or RSA SecurID or On-Prem MFA or Symantec VIP or YubiKey OTP or Custom Authenticator - Custom Authenticator or Smart Card Authenticator

Okta Attack Paths Are Short

Compared to Active Directory (AD) and Microsoft Entra ID

No Group Nesting

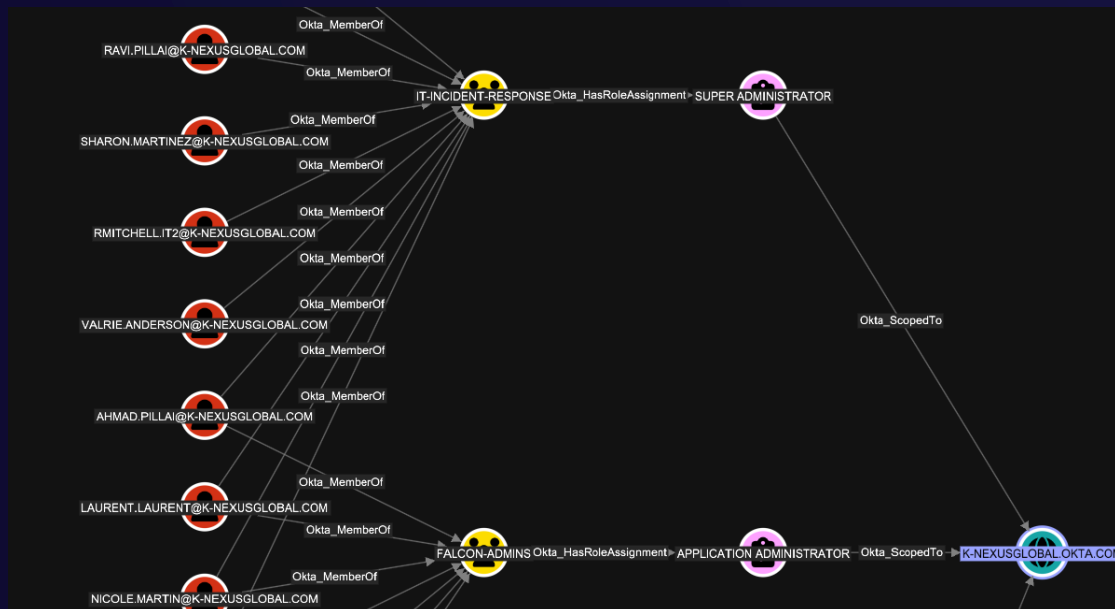
- Only users can be members of groups. Groups and applications cannot be added to groups
- Synchronized group membership gets correctly flattened

Privilege Elevation Minimized

- Only Super Admins can modify principals with role assignment
- True for users, groups, and apps
- Valid for built-in and custom roles

Lateral Movement Limited

- No built-in computer management
 - MDM
 - Group Policy
- No remote computer management
 - PowerShell Remoting
 - SSH
 - SMB
 - WMI
 - Windows RPC



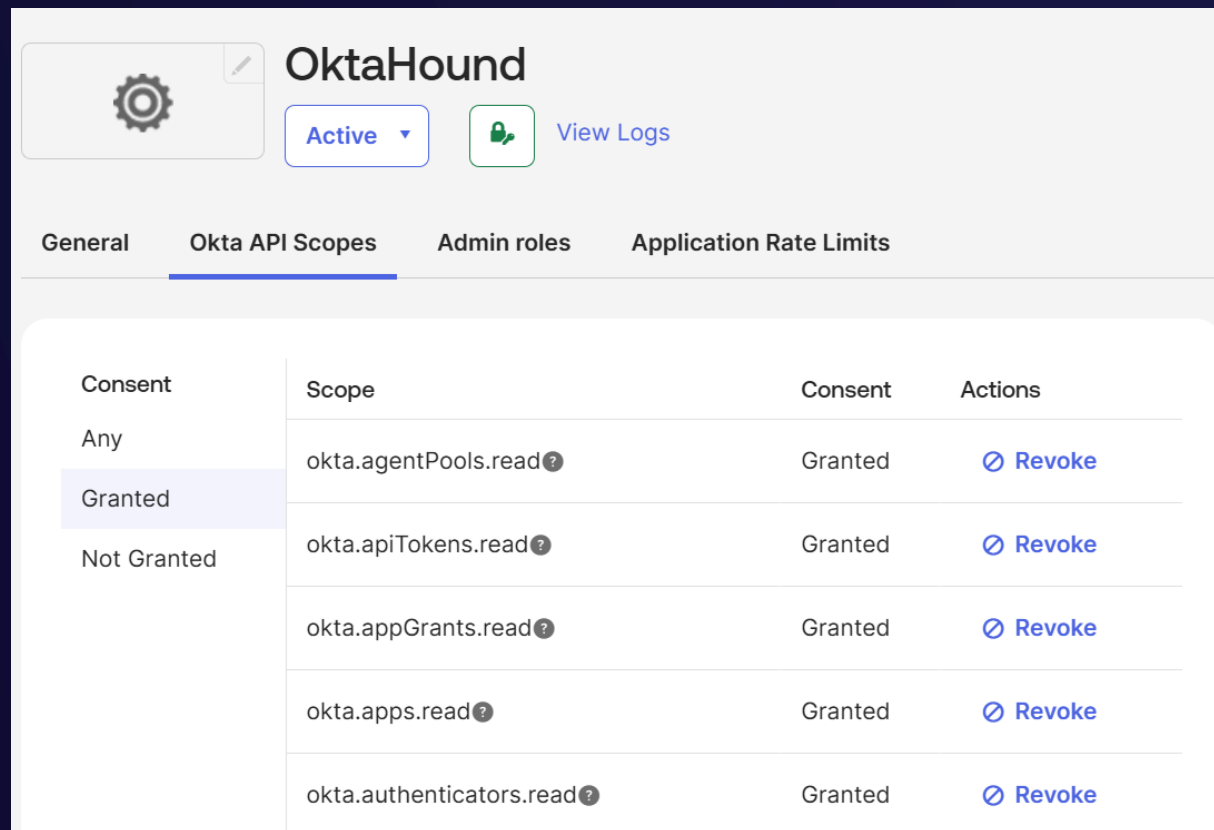
Okta Security Is Boring



Overprivileged Auditors

Security Auditors Are Typically Super Admins

- Read-Only Administrators role cannot read role assignments
- Permission to read OAuth 2.0 scopes grants cannot be delegated



The screenshot shows the OktaHound interface for configuring Okta API Scopes. The interface includes a header with a gear icon, the title "OktaHound", and a status dropdown set to "Active". Below the header are navigation tabs: "General", "Okta API Scopes" (selected), "Admin roles", and "Application Rate Limits". The main content area displays a table of API scopes with columns for Consent, Scope, Consent, and Actions.

Consent	Scope	Consent	Actions
Any	okta.agentPools.read?	Granted	Revoke
Granted	okta.apiTokens.read?	Granted	Revoke
Not Granted	okta.appGrants.read?	Granted	Revoke
	okta.apps.read?	Granted	Revoke
	okta.authenticators.read?	Granted	Revoke

Okta Privilege Elevation Paths

Read-Only Administrators

Vulnerable App

Active View Logs

General Okta API Scopes Admin roles Application Rate Limits

Client Credentials Edit

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

Client authentication Client secret Public key / Private key

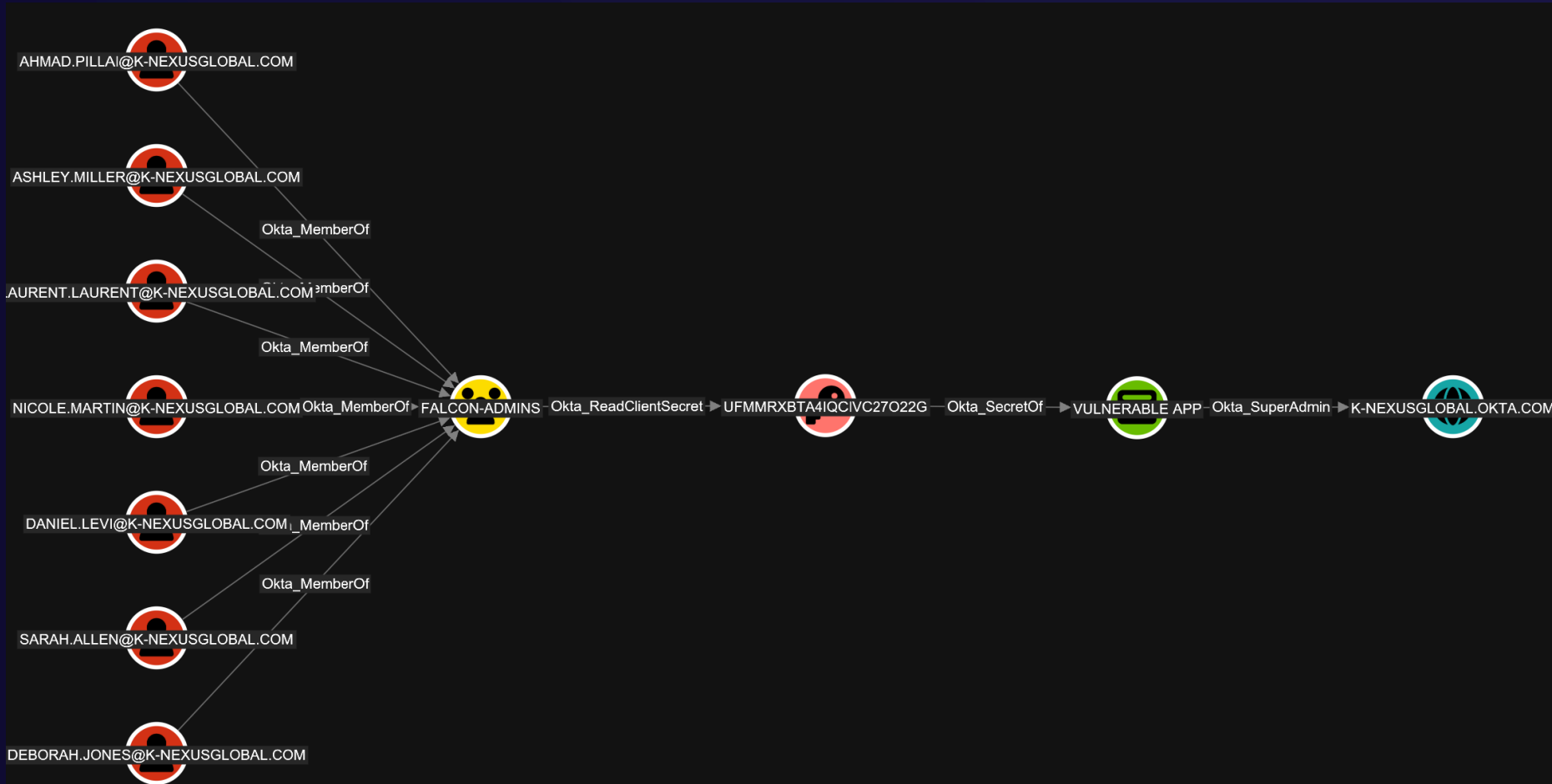
CLIENT SECRETS

Generate new secret

Creation date	Secret	Status
Mar 4, 2026	VVvDF9n5fl7wkqxMPS9Up2kaXC3n1MrtnGc Copy	Active ▼

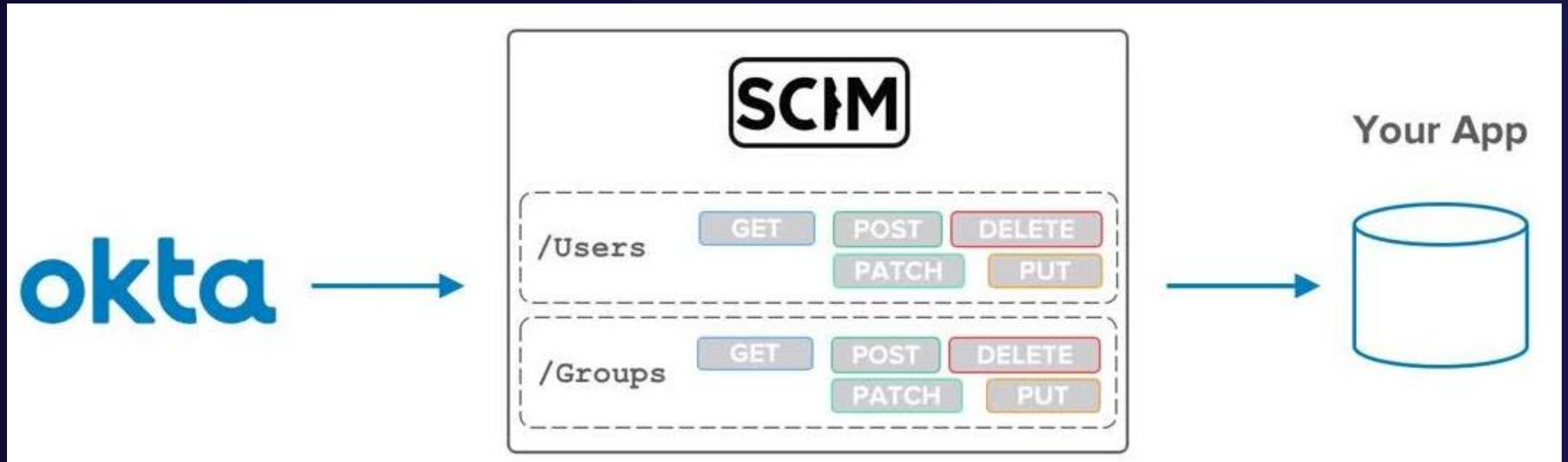
Okta Privilege Elevation Paths

Read-Only Administrators



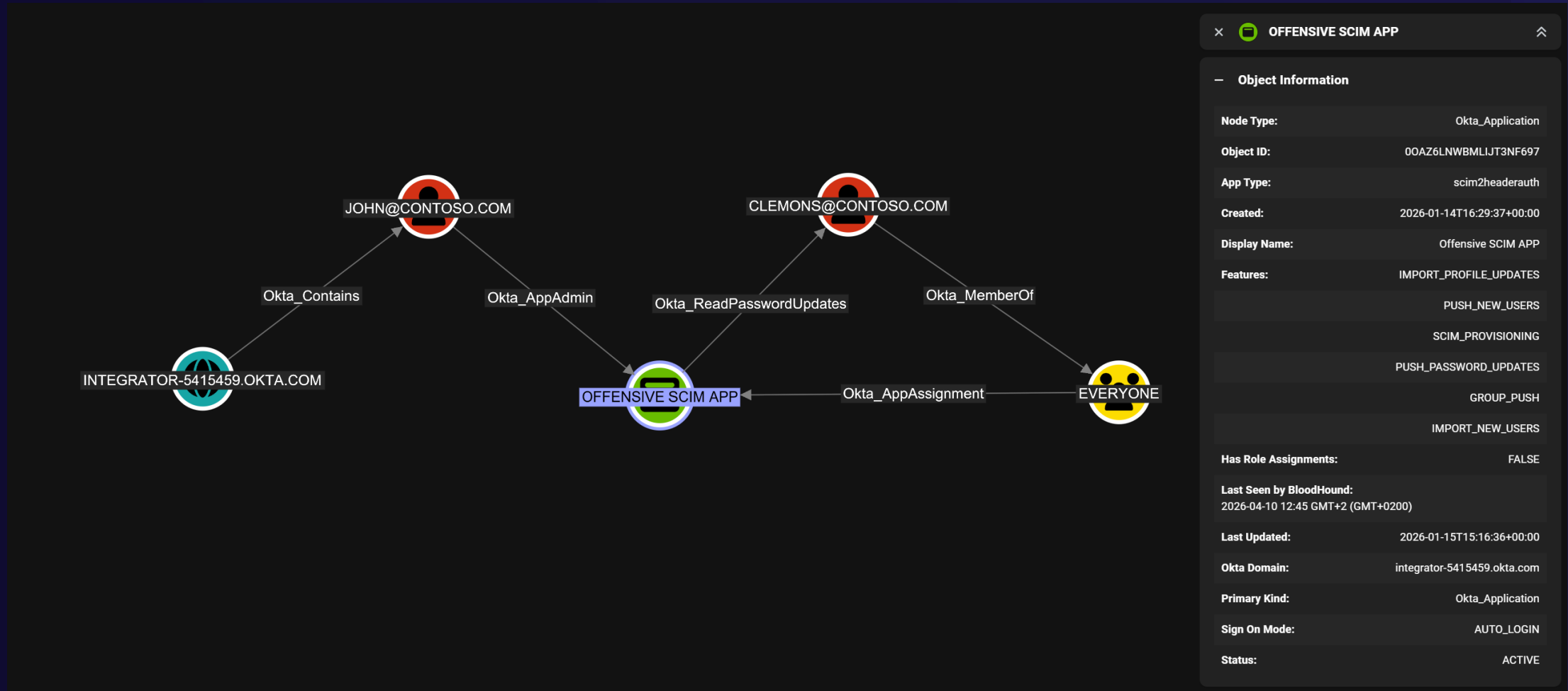
Okta Privilege Elevation Paths

SCIM: System for Cross-domain Identity Management



Okta Privilege Elevation Paths

SCIM: System for Cross-domain Identity Management



Okta Privilege Elevation Paths

Okta Workflows

The screenshot displays the Okta Workflows interface for a workflow titled "Salesforce Lead Flow". The workflow is composed of four steps:

- Okta Read User:** This step is used to retrieve user information. The "Profile Properties" section is expanded, showing fields for "First name", "Last name", "Organization", and "Primary email".
- Salesforce 2 Create Record:** This step is used to create a new record in Salesforce. The "Record Fields" section is expanded, showing fields for "LastName*", "FirstName", "Company*", and "Email".
- Text Compose:** This step is used to compose a message. The "output" field is expanded, showing the message content: "A new Salesforce Lead record has been created." followed by "Name: [First name] [Last name]", "Company: Organization", and "Email: Primary email".
- Slack Send Message to Channel:** This step is used to send a message to a Slack channel. The "Message" field is expanded, showing the message content: "A new Salesforce Lead record has been created." followed by "Name: [First name] [Last name]", "Company: Organization", and "Email: Primary email".

The interface also includes a navigation bar at the top with "Okta Sandbox", "Home", and "Settings". Below the navigation bar, there are tabs for "FLO", "FLO History", and "FLO Chart". A status bar indicates "FLO IS OFF". On the right side, there is an "Add Another" section with buttons for "App Action", "Function", "Add Note", and "Save and Test".

Okta Privilege Elevation Paths

Okta Workflows

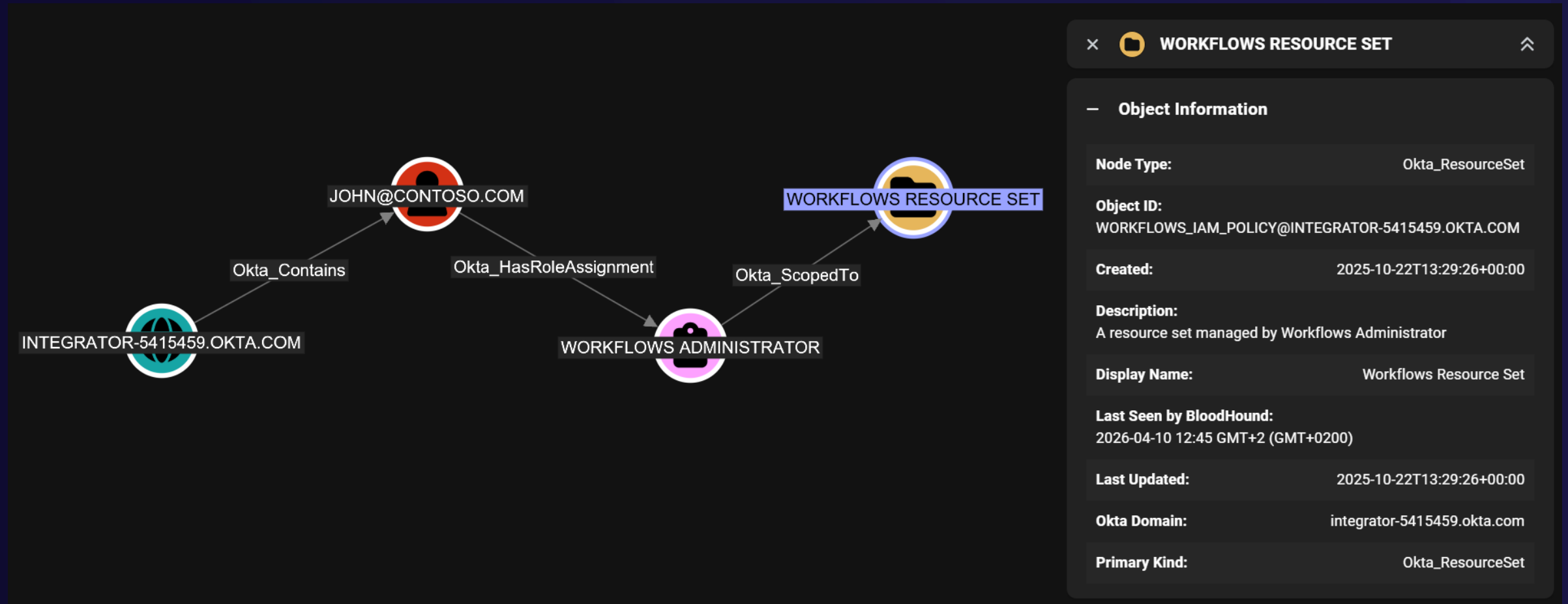
The screenshot shows the Okta Workflows configuration page. On the left, under "When this happens", there is a button labeled "Add event" and a link "What is an event?". The main area features a search bar "Search apps" and a checkbox "Include test connectors". Below these are "Built-in triggers" including Schedule, Helper Flow, API Endpoint, and Delegated Flow. The central part of the screen displays a grid of application icons for selection, including Airtable, Asana, Azure Active Directory, Box, Cisco Identity Intelligence, Evident ID, Excel Online, Freshservice, Github, Gmail, Google Calendar, Google Drive, Google Sheets, Hubspot CRM, Jira, Jira Service Management, Marketo, Mixpanel, Office 365 Mail, Okta, Okta Devices, OneDrive, Pager Duty, Proofpoint, Salesforce, and Smartsheet.

The screenshot shows a Microsoft Edge browser window with a sign-in page. A "Policies" dropdown menu is open, displaying a list of permissions. The permissions include:

- Perform user-impacting remote actions on Microsoft Intune devices
- Read and write Microsoft Intune devices
- Read and write Microsoft Intune RBAC settings
- Read and write Microsoft Intune configuration
- Access directory as the signed in user
- Read and write directory data
- Manage education app settings
- Have full access to all files user can access
- Read and write financials data
- Read and write all groups
- Read and write identity providers
- Read identity risk event information
- Read identity risky user information
- Read and write user and shared mail
- Send mail on behalf of others
- Read and write user mailbox settings
- Read hidden memberships
- Create user OneNote notebooks
- Read and write all OneNote notebooks that user can access
- Deliver and manage user notifications for this app
- Maintain access to data you have given it access to
- Manage on-premises published resources
- Read and write organization information
- Read all users' relevant people lists
- Read all company places
- Read your organization's policies
- Read and write your organization's trust framework policies
- Read and write privileged access to Azure AD
- Read and write privileged access to Azure resources
- Manage all programs that user can access
- Read all usage reports
- Read and write directory RBAC settings
- Read and update your organization's security actions
- Read and update your organization's security events
- Have full control of all site collections
- Create, read, update, and delete user's tasks and task lists
- Read and write user and shared tasks
- Manage threat indicators this app creates or owns
- Invite guest users to the organization
- Read and write all users' full profiles

Okta Privilege Elevation Paths

Okta Workflows



Okta Secure Web Authentication

1Password Business Active View Logs Monitor Imports

General **Sign On** Provisioning Import Assignments Push Groups

Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application. Application username is determined by the user profile mapping. [Configure profile mapping](#)

- Secure Web Authentication
 - User sets username and password
 - Administrator sets username and password
 - Administrator sets username, user sets password
 - Administrator sets username, password is the same as user's Okta password
 - Users share a single username and password set by administrator
- Bookmark-only
- OpenID Connect

Credentials Details

Application username format: Okta username

Update application username on: Create and update

Password reveal: Allow users to securely see their password (Recommended)

About

Secure Web Authentication (SWA) allows users to edit the credentials used for signing on to this application.

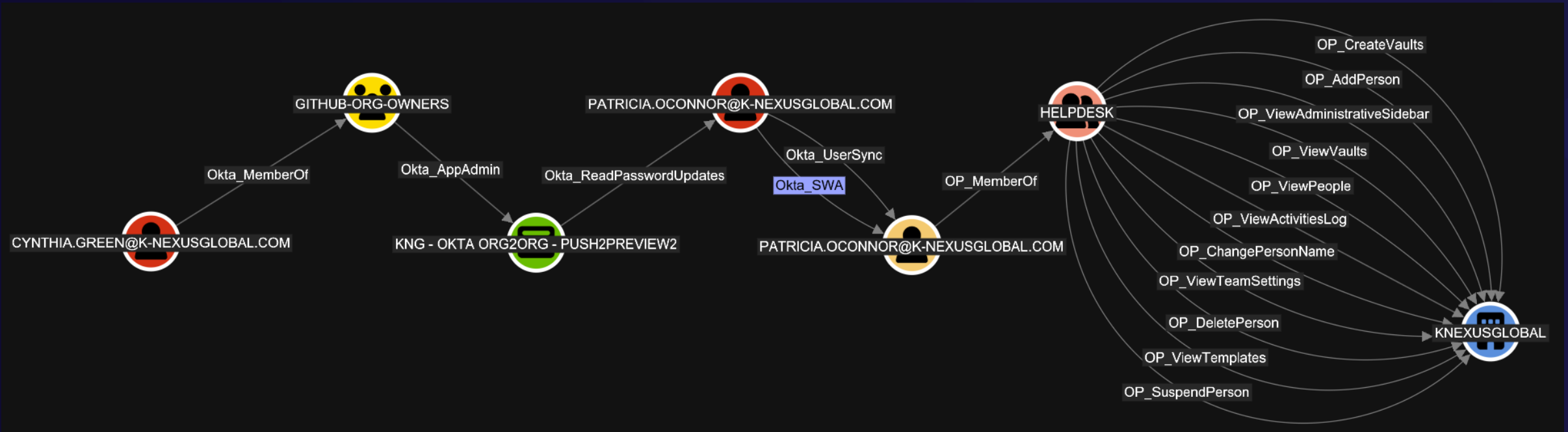
The **Okta browser plug-in** is required for SWA sign on to this application.

Application Username

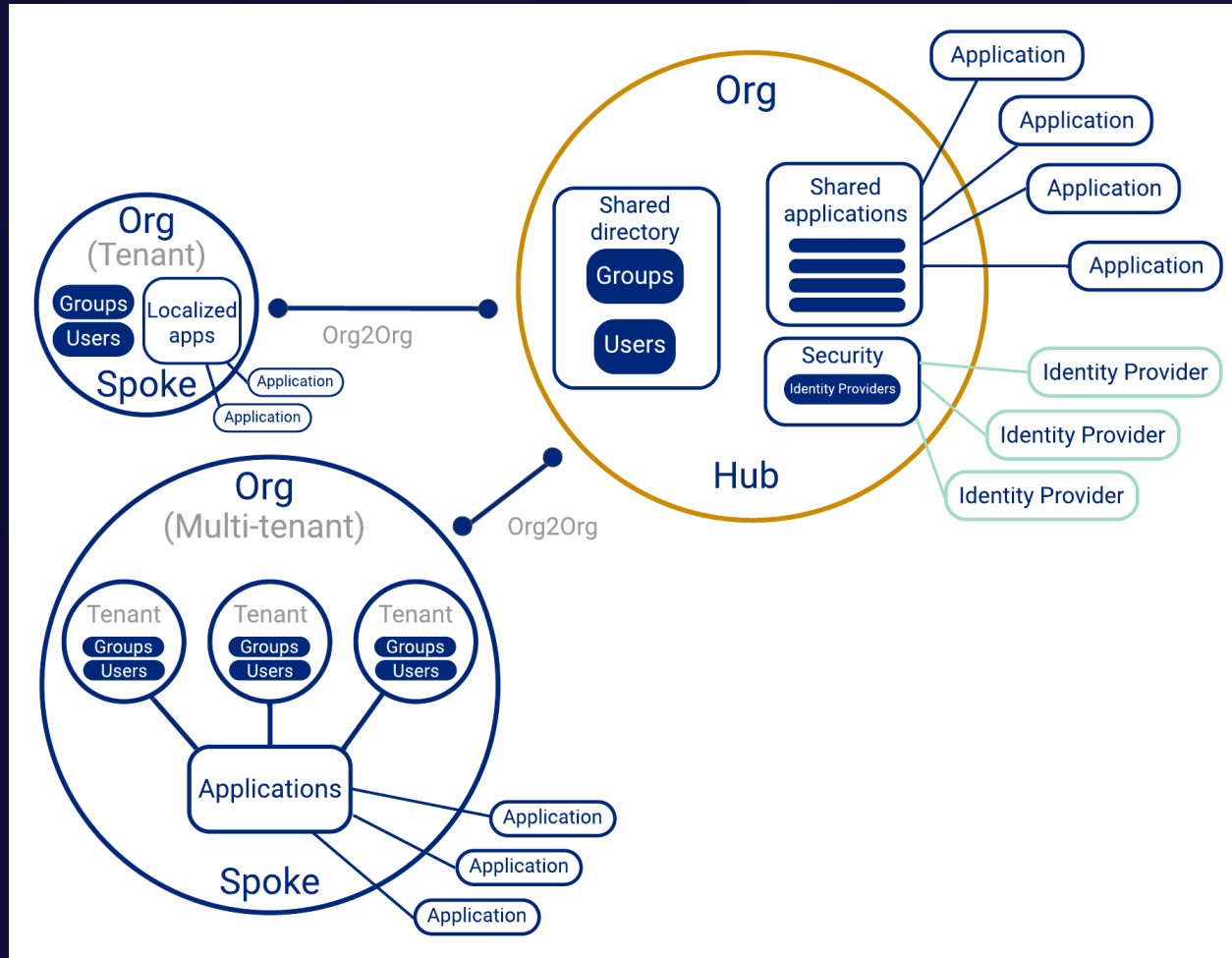
Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

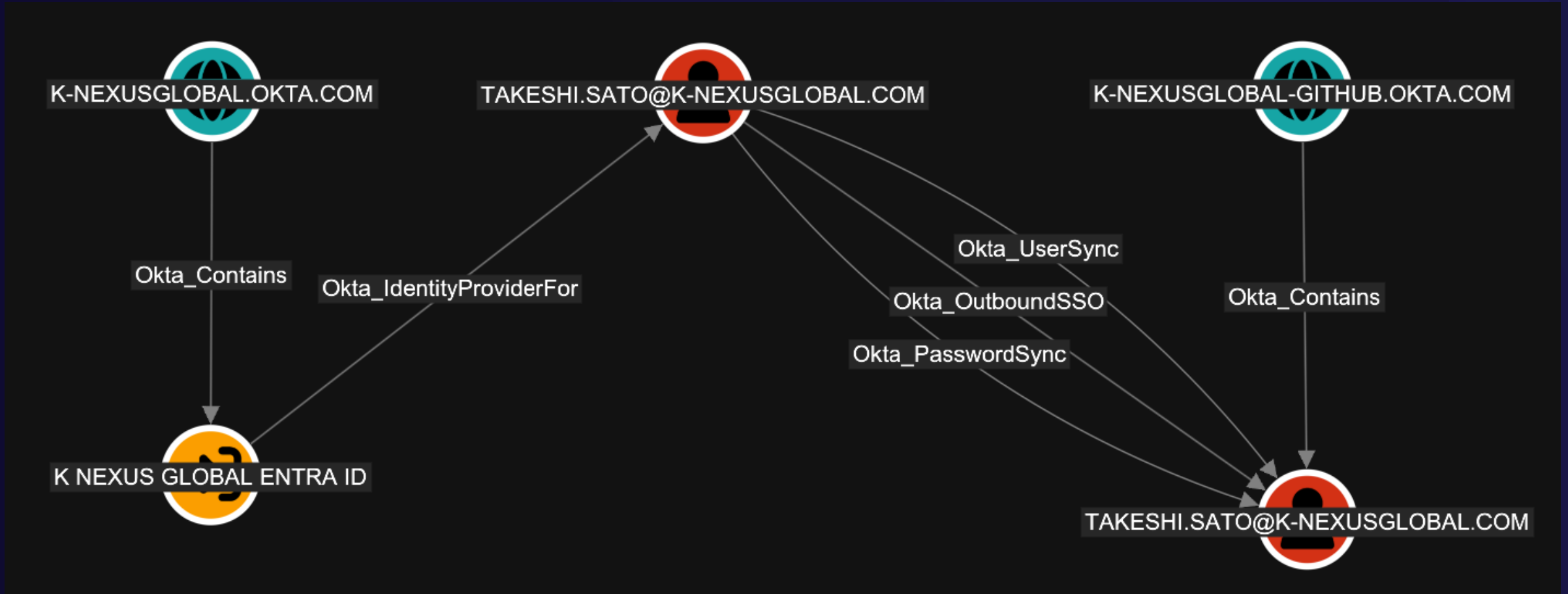
Okta Secure Web Authentication



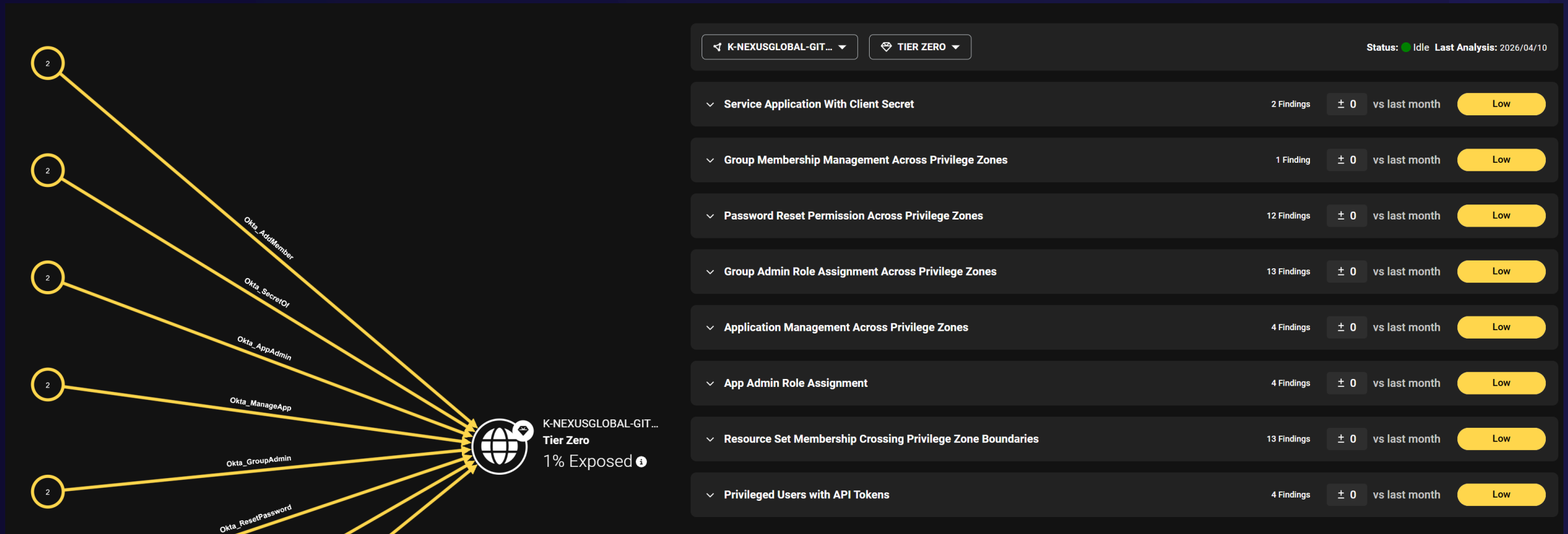
Okta Org2Org



Okta Org2Org



BloodHound Enterprise Findings



BloodHound Enterprise Findings

Privileged Users with API Tokens

Recommended Remediation

Prefer OAuth 2.0 access tokens over API tokens (SSWS tokens). Applications performing OAuth 2.0 authentication must be registered in Okta as service applications or API service integrations and assigned fine-grained permissions. Such applications then authenticate using public/private key pairs (preferred option) or client secrets (strong passwords).

In situations where the use of API tokens is justified, limit their validity to the minimum required duration and restrict the use of tokens to specific network zones.

Regularly audit API token usage to identify and revoke unnecessary tokens. Rotate tokens immediately if there is any suspicion of compromise.

Issue tokens only from dedicated low-privilege service identities rather than human administrator accounts. Alert on token usage from unusual network locations, devices, or access patterns.

Principals

Accepted

	Severity ⓘ	Exposure	Non-Tier Zero Source	⚡ Tier Zero Target	Impact
⋮	🟡	🟡 0	🔑 OKTAHOUND	👤 MGRAFI	🟡 10.8K
⋮	🟡	🟡 0	🔑 KNEXUS-ANSIBLE-API2	👤 JSYKOR	🟡 10.8K
⋮	🟡	🟡 0	🔑 OPENFETCH	👤 JDREIJE	🟡 10.8K
⋮	🟡	🟡 0	🔑 POSTMAN	👤 MGRAFI	🟡 10.8K

Description

Okta API tokens (SSWS tokens) are long-lived secrets used by applications and scripts to access the Okta API. Each token is tied to a specific user, and its permissions are inherited from that user's role assignments. For example, a token created by a Super Administrator has full access to all API endpoints. Because these tokens are often stored in plaintext in app configuration or environment variables, they are high-value targets. If exposed, attackers can perform administrative actions without interactive sign-in and bypass controls like MFA.

References

References not available.

📄 Export (.csv)

Okta and Devices

Targeting Okta Integrated Endpoints

Common Okta Integrations

- Okta Desktop MFA
 - Okta Verify device prompts or TOTP during local logon
 - Recommended in administrator forums as an addition to Platform SSO
- Okta Application Authentication
 - Okta Verify on macOS can satisfy MFA requirements
 - Admins configure compliance checks using Device Assurance policies
 - Advanced Posture Checks expand checks beyond Okta default queries

Desktop MFA - DoS

The screenshot shows the Okta Admin Console interface. On the left is a navigation sidebar with the Okta logo and menu items: Admin Console, Dashboard, Directory, People (highlighted), Groups, Devices, Profile Editor, Directory Integrations, and Profile Sources. The main content area displays the profile for 'Lance Cain' with email 'correspondance@lbcaain.com'. A search bar at the top says 'Search for people, apps and groups'. Below the user name are buttons for 'Reset or Remove password' and 'More Actions'. The 'More Actions' dropdown menu is open, listing: 'Reset Authenticators', 'Clear User Sessions', 'Reset Behavior Profile', 'Suspend', 'Deactivate', and 'Device Logout' (highlighted with a green box). Below the dropdown are tabs for 'Applications', 'Groups', 'Roles', and 'Pre-enrolled authenticators'. The 'Assigned Applications' section has an 'Assign Applications' button.

⚠ Devices perform a best-effort poll every 15 minutes to receive the sign-out command from Okta. This action requires an active connection between the device and your Okta org.

Desktop MFA - DoS


Log out from eligible Desktop MFA devices? ×

Lance Cain will be logged out of all devices:

- running macOS
- enrolled in Desktop MFA
- identified with SCEP
- that are online

This will not affect any other Okta applications.

[Cancel](#) [Log out all devices](#)



Admin initiated logout

You will be logged out of your desktop in 5 second(s).

[OK](#)

Desktop MFA - DoS

- Besides the manual method, how else can Device Logout be triggered?
 - Universal Logout
 - Okta Identity Threat Protection, if enabled, when risk status is elevated
 - User sessions and device factors are reset
 - When users are suspended or deactivated
 - Okta automates device logout on macOS

use this feature to handle employee lifecycle changes such as leaves of absence or offboarding. If a user is deactivated or suspended, Okta automatically signs the user out from all devices.

Desktop MFA - DoS

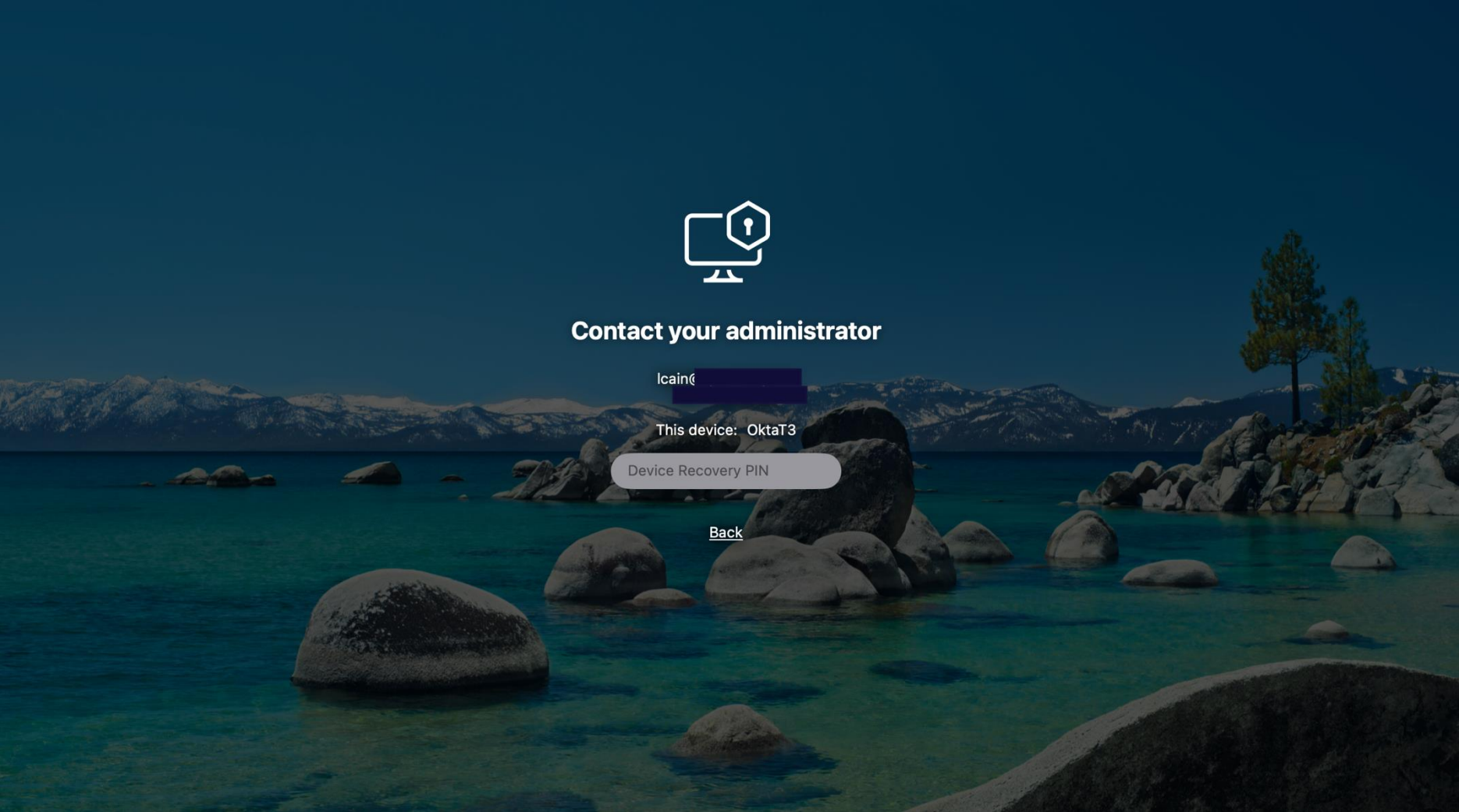
The screenshot shows a user profile on the left with a red icon and an email address ending in @GMAIL.COM. An arrow labeled 'OktaHasRole' points to a green icon representing the role 'DEVICE_LOGOUT_ADMINISTRATOR'. On the right, a sidebar displays the role's details:

Object Information	
Node Type:	OktaCustomRole
Object ID:	CR0XBK7DR4V1NLWYP697
Created:	2025-11-10T22:51:35+00:00
Display Name:	Device_Logout_Administrator
Last Seen by BloodHound:	2026-03-13 13:43 EDT (GMT-0400)
Last Updated:	2025-11-10T22:51:35+00:00
Okta Domain:	trial-1771280.okta.com
Permissions:	okta.devices.logoutUsers okta.users.lifecycle.logoutDevices
Primary Kind:	OktaCustomRole

The screenshot shows a green icon representing the role 'USER ADMINISTRATOR'. To its right, a list of permissions is displayed:

Permissions:	
	okta.users.read
	okta.users.create
	okta.users.lifecycle.delete
	okta.users.lifecycle.suspend
	okta.users.lifecycle.deactivate
	okta.users.lifecycle.activate
	okta.users.manage

Desktop MFA - DoS



Desktop MFA - DoS

- Recovery Options
 - Previously configured Device Recovery Pins
 - Admin re-enables and/or delivers recovery pins to users
 - *If a Super Admin was compromised, then only below two options*
 - MDM management removes Okta Verify with break-glass accounts
 - Contact Okta Support

Advanced Posture Checks - Leaking Information

- Advanced Posture Checks evaluate system attributes beyond what Okta natively supports
- Uses OSQuery when authentication events are triggered
 - Enabled/Disabled
 - TextBox
- Supported queries documented - <https://www.osquery.io/schema/5.18.1/>
 - docker_container_envs
 - file
 - plist
 - processes
 - process_envs
 - shell_history
 - many more

Advanced Posture Checks

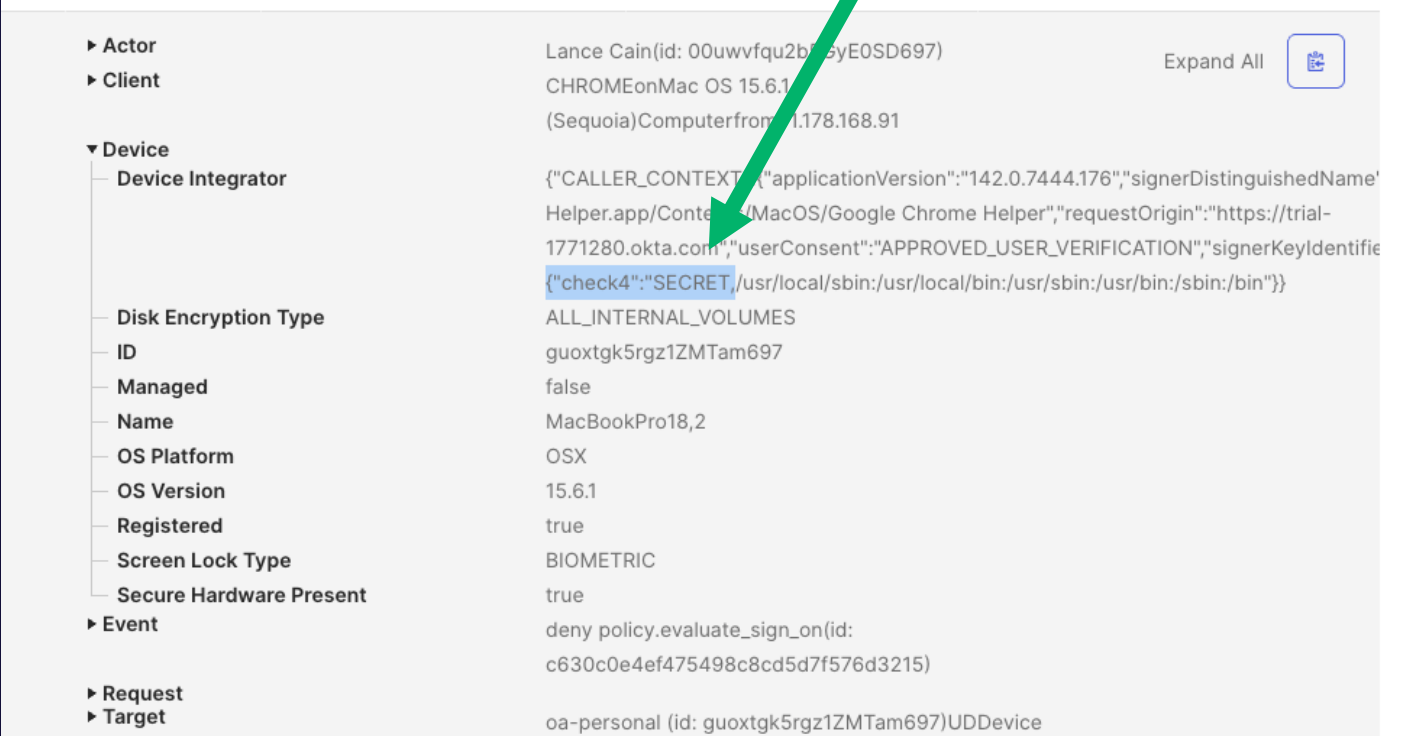
Create custom conditions for device assurance policies for MacOS to enforce device attributes that Okta doesn't support out-of-the-box.




Advanced Posture Checks - Leaking Information

- Advanced posture checks log output to Okta's System Log
- We have successfully leaked:
 - Docker Container environment variable secrets
 - Docker Container process arguments
 - Plist contents of configuration files
 - Process command line arguments
 - Root shell history

• `docker run -it -e MYSECRET=SECRET busybox sh`



▶ Actor	Lance Cain(id: 00uwvfqu2b75yE0SD697)	Expand All 
▶ Client	CHROMEonMac OS 15.6.1 (Sequoia)Computerfrom 1.178.168.91	
▼ Device		
Device Integrator	<pre>{ "CALLER_CONTEXT": { "applicationVersion": "142.0.7444.176", "signerDistinguishedName": "Helper.app/Content/Resources/MacOS/Google Chrome Helper", "requestOrigin": "https://trial-1771280.okta.com", "userConsent": "APPROVED_USER_VERIFICATION", "signerKeyId": "check4": "SECRET", "usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin" }</pre>	
Disk Encryption Type	ALL_INTERNAL_VOLUMES	
ID	guoxtgk5rgz1ZMTam697	
Managed	false	
Name	MacBookPro18,2	
OS Platform	OSX	
OS Version	15.6.1	
Registered	true	
Screen Lock Type	BIOMETRIC	
Secure Hardware Present	true	
▶ Event	deny_policy.evaluate_sign_on(id: c630c0e4ef475498c8cd5d7f576d3215)	
▶ Request		
▶ Target	oa-personal (id: guoxtgk5rgz1ZMTam697)UDDevice	

Advanced Posture Checks - Leaking Information



DEMO API SERVICES APP

Last Seen by BloodHound: 2026-04-09 16:06 EDT (GMT-0400)

Last Updated: 2026-04-09T20:02:52+00:00

Oauth Scopes: okta.logs.read

okta.devicePostureChecks.manage

Okta Domain: trial-1085861.okta.com

Primary Kind: Okta_Application

Advanced Posture Checks - Leaking Information

The screenshot displays the Okta Admin Console interface. At the top, a notification indicates "27 days left in your trial" with a link to "Contact us to extend or purchase a plan." The user's name, "Bob Cain", and ID, "lbcaim-trial-1085861", are visible in the top right corner. A search bar is located below the notification. The left sidebar contains the "Admin Console" menu with various options, including "Advanced Posture Checks" which is currently selected. The main content area is titled "Advanced posture checks" and has a "Documentation" link. Below this, there are tabs for "Default checks" and "Custom checks", with "Custom checks" being active. The "Edit custom posture check" section provides instructions: "Define custom conditions using osquery to add posture checks, ensuring user device security and compliance. Apply these checks to Okta policies." The configuration form includes:

- Posture check name:** A text input field containing "Firewall Enabled".
- Description:** A text input field containing "Checks Firewall status".
- Assign variable for this check:** A section explaining that variable names are used for policy conditions. Below it, a "Variable name" input field contains "FirewallEnabled".
- Platforms to check against:** A section explaining that Okta supports macOS and Windows. Below it, the "Platform" section has two radio buttons: "macOS" (which is selected) and "Windows".
- Write the query:** A section with the instruction "Write or paste in your query used for this posture check".

Advanced Posture Checks - Delivering Payloads

- Another capability of Advanced Posture Checks is presenting users with remediation steps
 - A custom error message to explain what failed
 - Can include hyperlinks to resources
- Compromise of posture check access means we can use Okta to direct users to download and run payloads
 - Prevent application access until payload is run

User remediation

Determine how users should remediate if their device fails this check.

User remediation message

Custom
 None

Users will see

Your system lacks our latest security tooling, please download and install.

75/100

Remediation link

Link to a custom page
 None

Custom page URL

<https://mycustom.link/>

Advanced Posture Checks - Delivering Payloads



DEMO API SERVICES APP

Last Seen by BloodHound: 2026-04-09 16:06 EDT (GMT-0400)

Last Updated: 2026-04-09T20:02:52+00:00

Oauth Scopes: ~~okta.logs.read~~

okta.devicePostureChecks.manage

Okta Domain: trial-1085861.okta.com

Primary Kind: Okta_Application

Advanced Posture Checks - Delivering Payloads

The screenshot displays the Okta Admin Console interface for configuring an advanced posture check. The browser address bar shows the URL `trial-1085861-admin.okta.com`. The page title is `Advanced posture checks`. The left sidebar contains the Okta logo and a navigation menu with items such as Identity Threat Protection, User Profile Policies, Identity Providers, Delegated Authentication, Networks, Behavior Detection, **Advanced Posture Checks** (highlighted), Device Assurance Policies, Device Integrations, Administrators, API, Workflow, and Reports. The main content area is titled **Advanced posture checks** and includes a search bar and a user profile for Bob Cain. Below this, there are tabs for `Default checks` and `Custom checks`. The `Custom checks` tab is active, showing the **Edit custom posture check** configuration page. This page includes a description: "Define custom conditions using osquery to add posture checks, ensuring user device security and compliance. Apply these checks to Okta policies." The configuration fields are: **Posture check name** (Firewall Enabled), **Description** (Checks Firewall status), **Assign variable for this check** (Variable name: FirewallEnabled), and **Platforms to check against** (Platform: macOS selected, Windows unselected). A **Write the query** section is also present at the bottom.

Hybrid Attack Paths

JAMF Pro + Okta

JAMF Pro + Okta - What's a JAMF Pro?

- Mobile Device Manager (MDM) that specializes in Apple device management
 - macOS
 - iOS
 - iPadOS
 - tvOS
- Administrators configure
 - policies
 - scripts
 - configuration profiles
 - applications
 - more

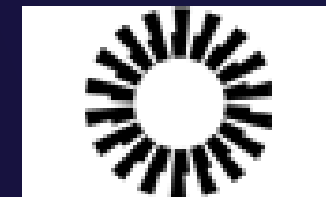


JAMF Pro + Okta

- JAMF Pro supports SSO using OIDC and SAML
 - OIDC requires *jamfcloud.com* and a JAMF Account
- Authentication occurs in Okta with a JAMF Pro app integration
 - Allows MFA, device compliance, and additional checks
- Okta sends JAMF Pro user attributes for a logon session
 - Can map attributes to local JAMF Pro accounts
 - emails
 - usernames
- User group assignments can optionally be transferred as user attributes
 - Okta group names can match to groups in JAMF Pro



Hey, can you tell me who this is?



That's Jimmy. His email is jim@localhost and he is in the SpecterRocks group.

Attack Okta -> JAMF

- Okta defaults **do** restrict low privileged admins from impacting privileged Okta Super Admins or groups
- Okta defaults **do not** restrict admins resetting user passwords or MFA of external privileged accounts
 - A compromised Okta Help Desk admin can reset a sync'd JAMF Pro administrator expanding a breach
- Application admins can assign new users to applications they control
 - A compromised App Admin can modify matched attributes sent to JAMF Pro
- Group admins and group membership admins can assign users to groups they control

10. Click **Username** or **Email** for **Jamf Pro User Mapping**.

These options determine how users in your IdP will be mapped to Jamf Pro users. By default, Jamf Pro gets information about the user from the IdP and matches it with existing Jamf Pro user accounts. **If the incoming user account does not exist in Jamf Pro, then group name matching occurs.**

11. Enter the SAML assertion attribute that defines users in the IdP in the **Identity Provider Group Attribute Name** field.

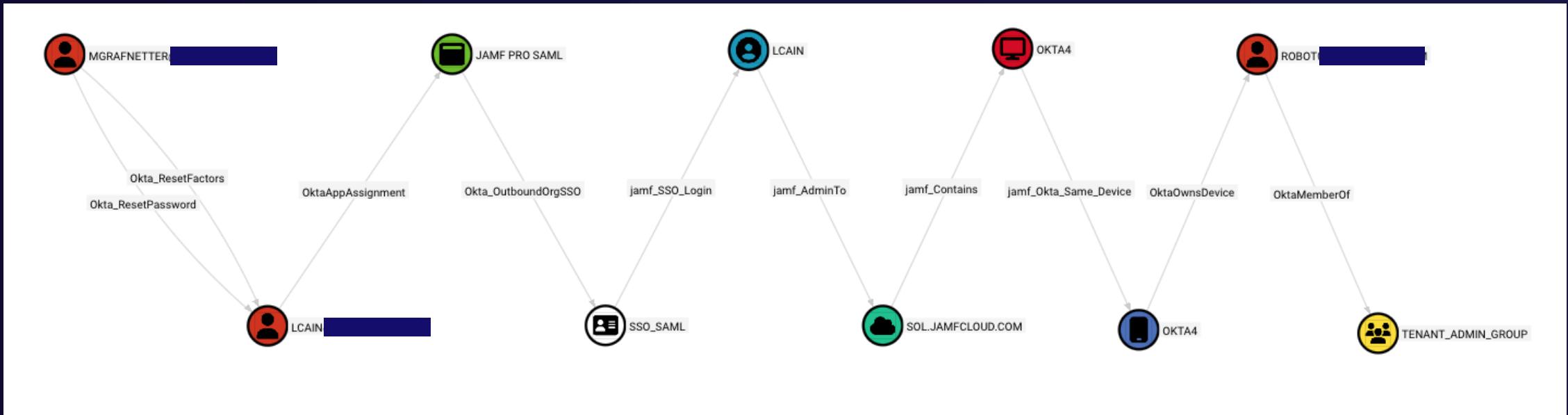
Jamf Pro matches each group from the Jamf Pro database and compares group names. Each user will be granted access privileges from all of the groups in the same manner as a local Jamf Pro user would. AttributeValue strings may be formatted as multiple strings, a single string, or semicolon-separated values.

Example: `http://schemas.xmlsoap.org/claims/Group`

Attack JAMF -> Okta

- Compromise of any type of MDM administrator, API client, or security pipeline is a big win for attackers
- Access to JAMF Pro allows target enumeration and payload execution
 - Eve toolkit
- We have leveraged JAMF Pro on red team assessments to pivot to privileged admins
 - Perform internal reconnaissance to identify Super Admins
 - Execute code on managed systems to
 - Access session tokens
 - Enable remote services
 - Exfiltrate API keys

Okta and JAMF Pro Hybrid Attack Path

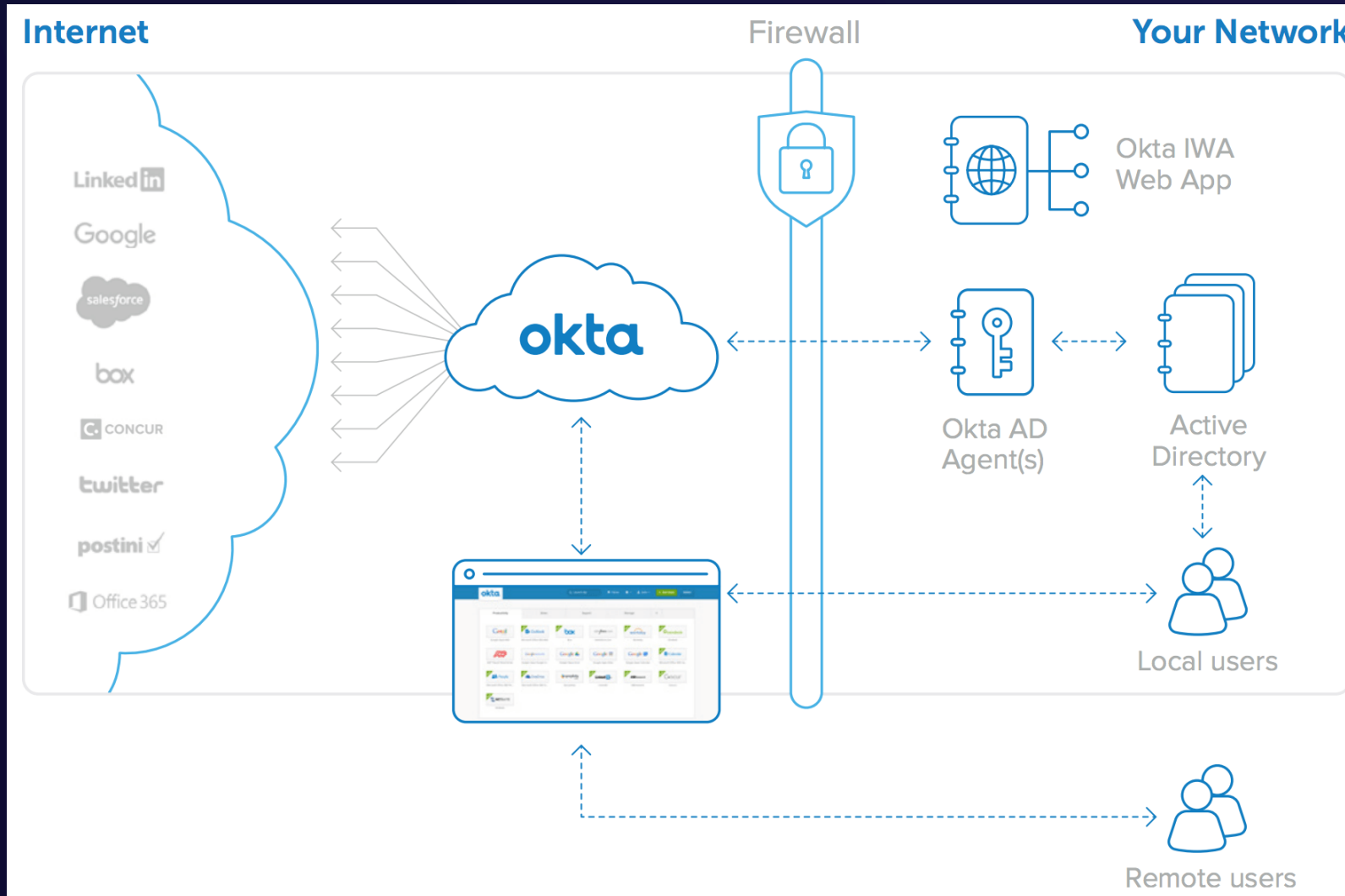


Hybrid Attack Paths

Active Directory

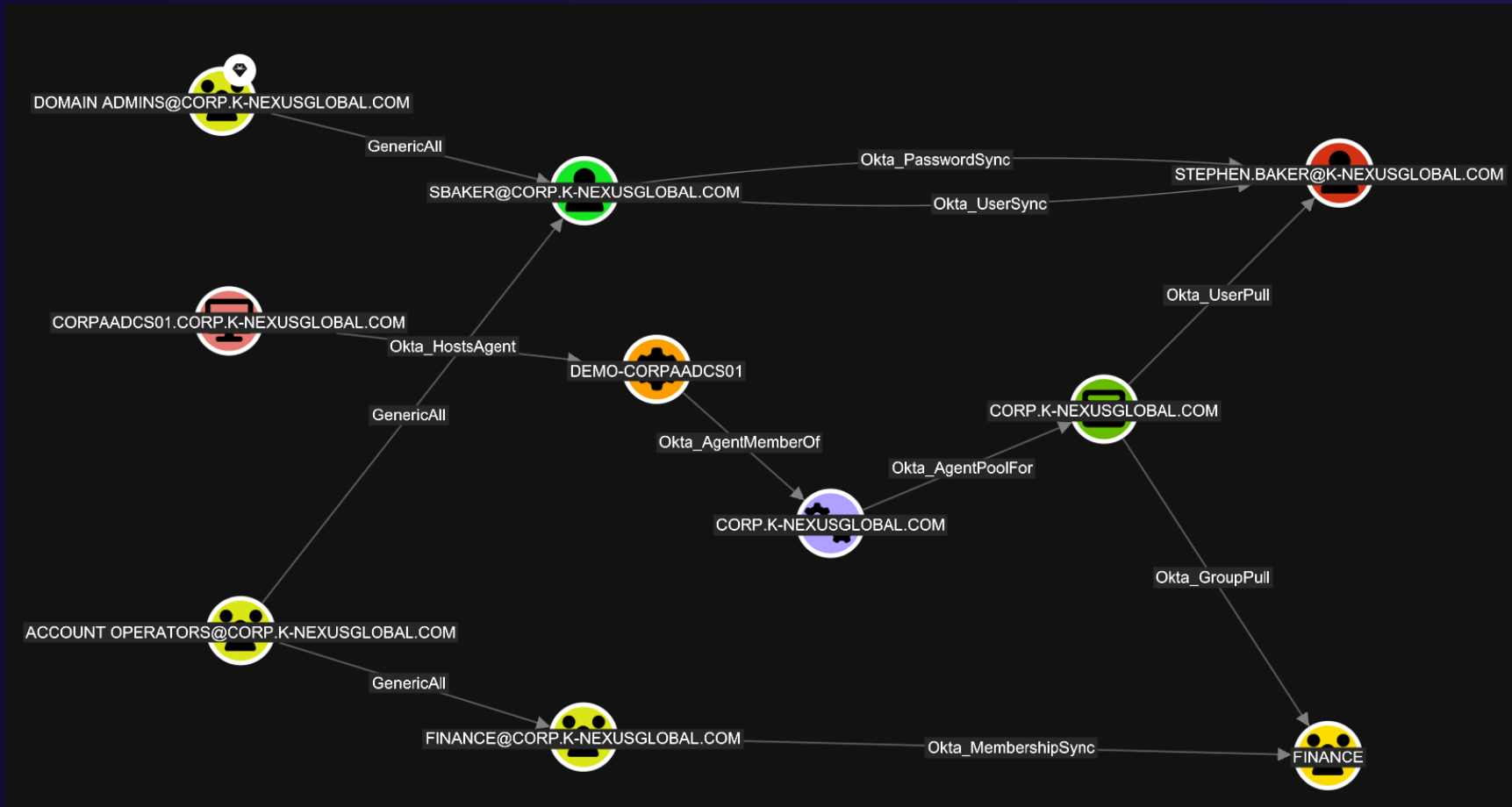
Okta AD Agents

Hybrid AD Deployment



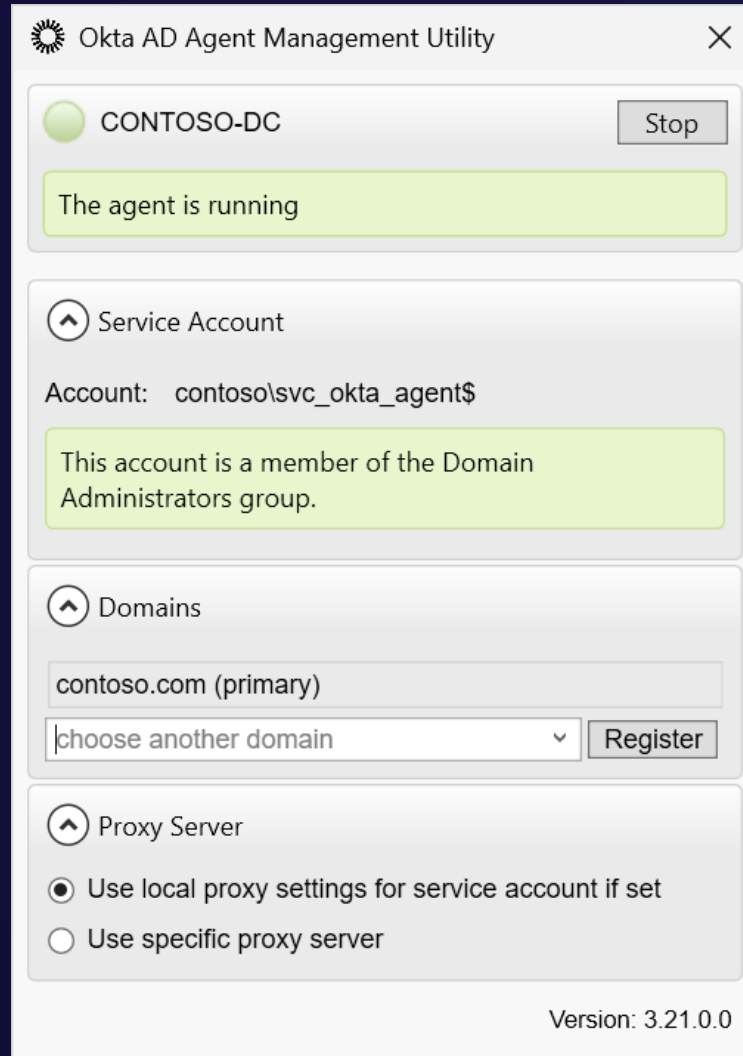
Okta AD Agents

Synchronization Model



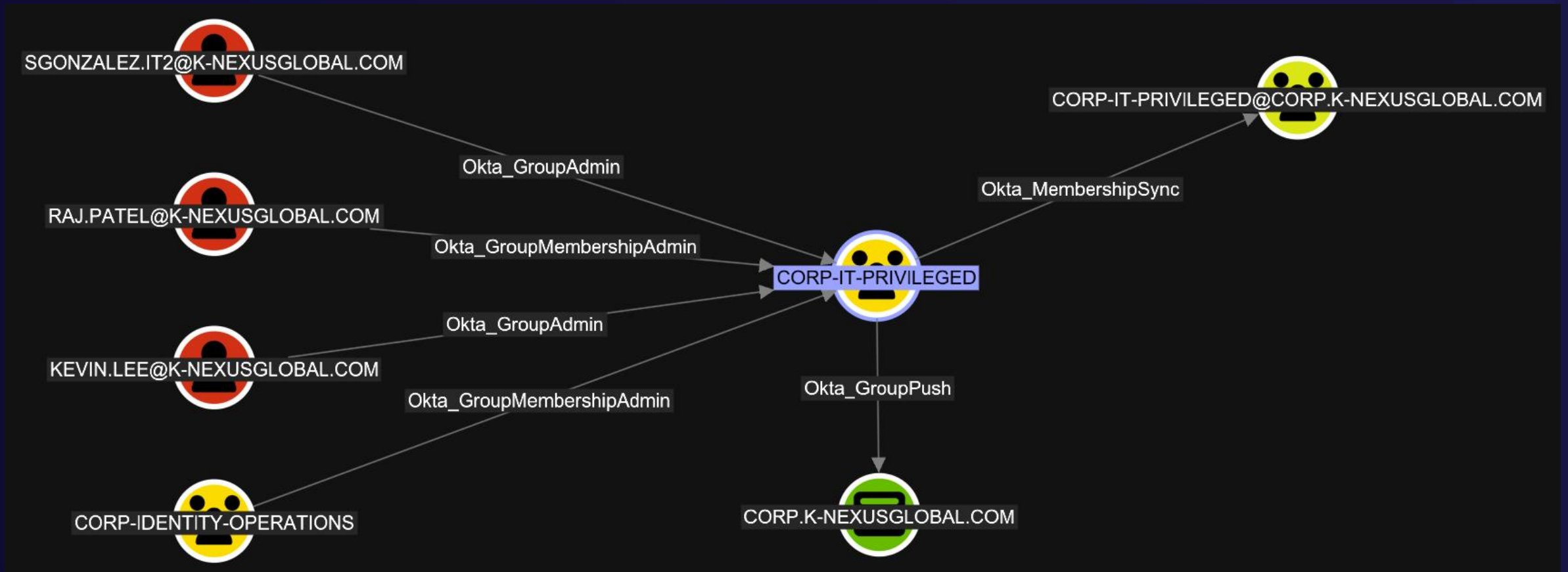
Okta AD Agents

Object Writeback Permissions



Okta AD Agents

Group Writeback



Agentless Desktop SSO

The diagram illustrates the SSO relationships between Active Directory users and an Okta application. It features four nodes: two Active Directory users (SVC-OKTASSO@CORP.K-N... and KLEE2@CORP.K-NEXUSGL...), one Okta application (ACTIVE_DIRECTORY), and one Okta user (KEVIN.LEE@K-NEXUSGLO...). Arrows indicate the relationships: Okta_KerberosSSO connects the first AD user to the Okta application; Okta_UserPull connects the Okta application to the Okta user; and Okta_UserSync connects the second AD user to the Okta user.

ACTIVE_DIRECTORY
OpenGraph | Okta_Application

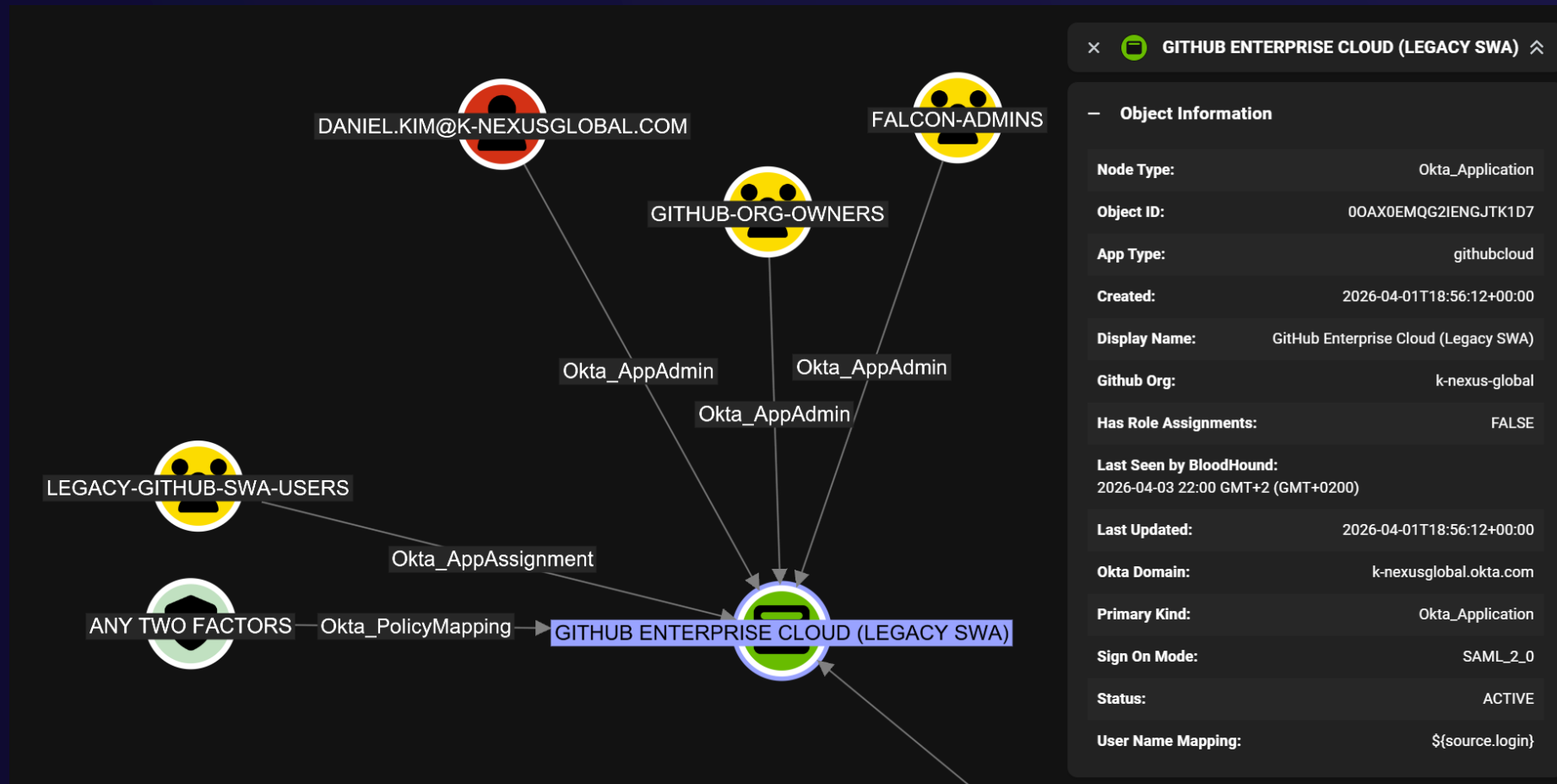
Object Information	
Node Type:	Okta_Application
Display Name:	corp.k-nexusglobal.com
Object ID:	00AVHTIZ7NBJQOJJ1D7
Collected:	TRUE
Created:	2026-02-25T18:45:22+00:00
Environmentid:	00ORUIRHUJF7PETTU1D7
Id:	0oavhtiz7nBjQoJj1d7
Last Seen by BloodHound:	2026-04-10 06:40 GMT+2 (GMT+0200)
Last Seen:	2026-04-10T02:19:54.352441+00:00
Last Updated:	2026-04-09T21:00:17+00:00
Name:	corp.k-nexusglobal.com
Operational Status:	OPERATIONAL
Orn:	orn:oktapreview:idp:00oruirhujf7peTtu1d7:apps:active_director...
Primary Kind:	Okta_Application
Status:	ACTIVE
Tenant:	00oruirhujf7peTtu1d7
Type:	AD

Hybrid Attack Paths

GitHub

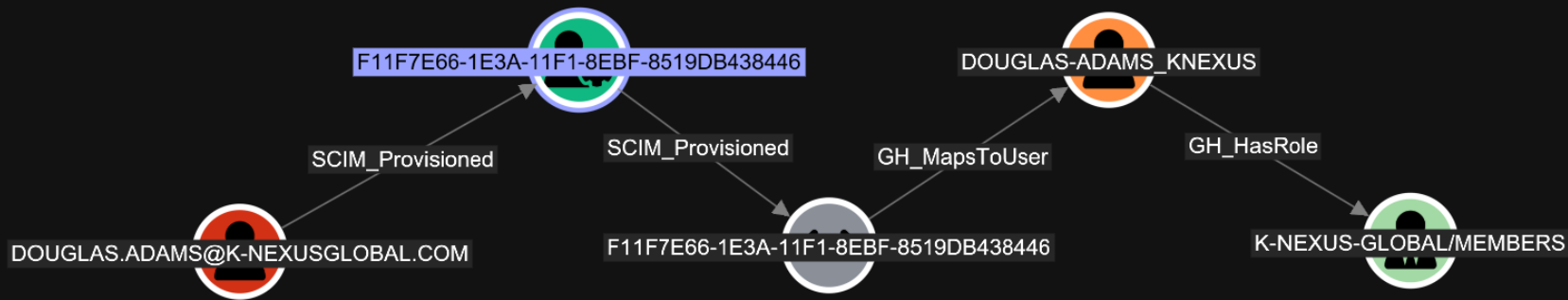
Hybrid Attack Paths

GitHub Application Configuration



Hybrid Attack Paths

GitHub User Synchronization / SCIM



×  F11F7E66-1E3A-11F1-8EBF-8519DB438446 ↗

Object Information

Node Type: SCIM_User

Object ID:
66313166376536362D316533612D313166312D386562662D3...

Enabled: FALSE

Enterprise: k-nexus-global

Id:
66313166376536362D316533612D313166312D386562662D3...

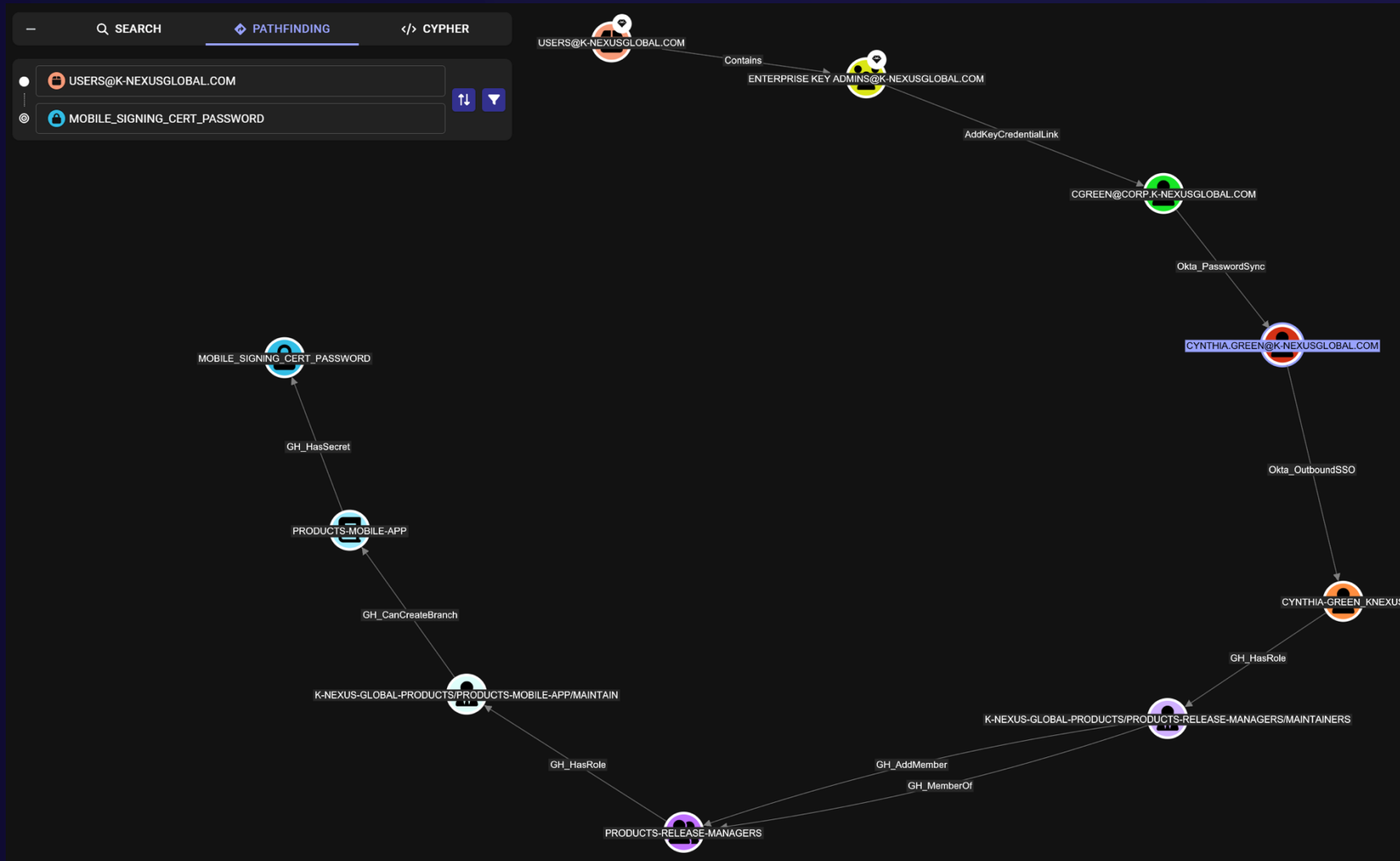
Last Seen by BloodHound:
2026-04-10 06:40 GMT+2 (GMT+0200)

Primary Kind: SCIM_User

Profile Url:
<https://api.github.com/scim/v2/enterprises/k-nexus-global/Users/f11f7e66-1e3a-11f1-8ebf-8519db438446>

Hybrid Attack Paths

Active Directory User -> Okta -> GitHub Secret

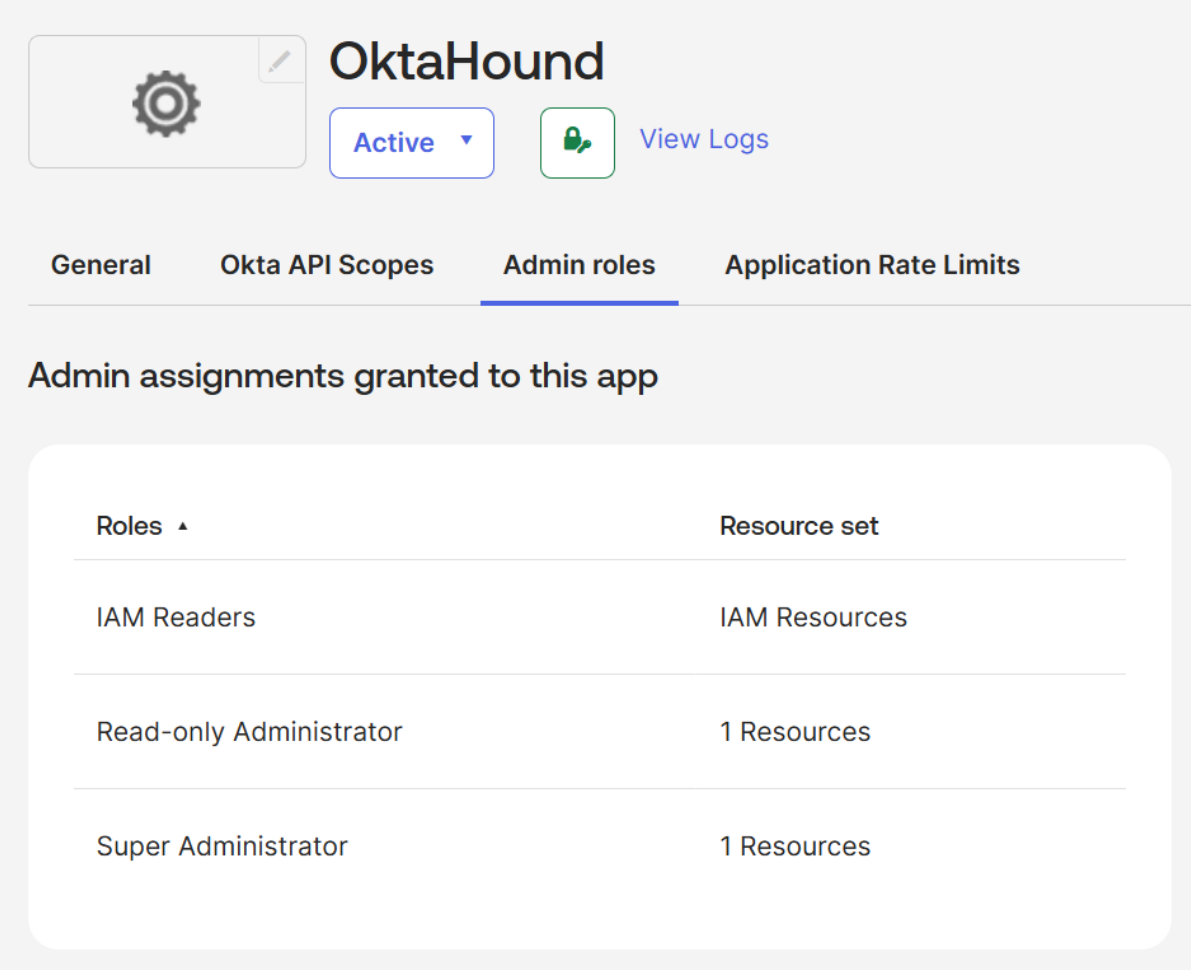


BloodHound OpenGraph Collectors

OktaHound

App Registration

Role Assignment



The screenshot shows the OktaHound application configuration page. At the top, there is a gear icon for settings, a pencil icon for editing, the app name "OktaHound", an "Active" status dropdown, a lock icon, and a "View Logs" link. Below this are four tabs: "General", "Okta API Scopes", "Admin roles" (which is selected), and "Application Rate Limits". The main content area is titled "Admin assignments granted to this app" and contains a table with two columns: "Roles" and "Resource set".

Roles	Resource set
IAM Readers	IAM Resources
Read-only Administrator	1 Resources
Super Administrator	1 Resources

App Registration

Okta Management API Scope Grants

The screenshot displays the Okta Management Console interface for an application named "OktaHound". At the top, there is a gear icon, a pencil icon, and the application name "OktaHound". Below this, there is a status indicator "Active" with a dropdown arrow, a lock icon, and a "View Logs" link. The main content area has four tabs: "General", "Okta API Scopes" (which is selected), "Admin roles", and "Application Rate Limits".

Under the "Okta API Scopes" tab, there is a table with the following columns: "Consent", "Scope", "Consent", and "Actions". The "Consent" column has a filter menu with options: "Any", "Granted" (which is selected), and "Not Granted". The table lists five API scopes, all of which are "Granted" and have a "Revoke" action available.

Consent	Scope	Consent	Actions
Any	okta.agentPools.read?	Granted	Revoke
Granted	okta.apiTokens.read?	Granted	Revoke
Not Granted	okta.appGrants.read?	Granted	Revoke
	okta.apps.read?	Granted	Revoke
	okta.authenticators.read?	Granted	Revoke

Data Collection

```
Ubuntu x + v
michael@GRAY:~/oktahound$ ./oktahound collect --zip --skip-mfa --verbosity Debug
[16:33:53] debug: OktaHound[0] Using existing output directory at /home/michael/oktahound/output.
[16:33:53] info: OktaHound[0] Loading Okta configuration...
[16:33:53] warn: OktaHound[0] Using API Token (SSWS) authentication. It is recommended to use OAuth 2.0 with an API Service App for better security and auditing.
[16:33:53] debug: OktaHound[0] Authenticating to https://integrator-5415459.okta.com using SSWS...
[16:33:53] info: OktaHound[0] Fetching Okta organization information...
[16:33:54] debug: OktaHound[0] Initializing the graph...
[16:33:54] info: OktaHound[0] Fetching users...
[16:33:54] info: OktaHound[0] Skipping user authentication factors collection.
[16:33:54] info: OktaHound[0] Fetching applications...
[16:33:54] info: OktaHound[0] Fetching API service integrations...
[16:33:54] info: OktaHound[0] Fetching identity providers...
[16:33:54] info: OktaHound[0] Fetching custom roles...
[16:33:54] info: OktaHound[0] Fetching policies...
[16:33:54] debug: OktaHound[0] Fetching OKTA_SIGN_ON policies...
[16:33:54] info: OktaHound[0] Fetching devices...
[16:33:54] info: OktaHound[0] Fetching realms...
[16:33:55] info: OktaHound[0] Fetching built-in roles...
[16:33:55] debug: OktaHound[0] Fetching info about the built-in role API_ACCESS_MANAGEMENT_ADMIN...
[16:33:55] debug: OktaHound[0] Fetching info about the built-in role GROUP_MEMBERSHIP_ADMIN...
[16:33:55] debug: OktaHound[0] Fetching info about the built-in role APP_ADMIN...
[16:33:55] info: OktaHound[0] Fetching custom resource sets...
[16:33:55] info: OktaHound[0] Fetching API tokens...
[16:33:55] info: OktaHound[0] Fetching agent pools...
[16:33:55] info: OktaHound[0] Fetching authorization servers...
[16:33:55] debug: OktaHound[0] Processing policy Default Policy (00pw0o8igxWLqAYQr697)...
[16:33:55] debug: OktaHound[0] Fetching PASSWORD policies...
[16:33:55] debug: OktaHound[0] Processing resource set Test resource set (iamwldyxudjNf2nnk697)...
[16:33:55] debug: OktaHound[0] Processing resource set IAM Resources (iamwwdsp2oNvvqr0s697)...
[16:33:55] debug: OktaHound[0] Processing resource set Workflows Resource Set (WORKFLOWS_IAM_POLICY)...
[16:33:55] info: OktaHound[0] Successfully processed 3 resource sets.
[16:33:55] debug: OktaHound[0] Processing API token OktaHound (00T3ugczs7Im9Qeju697)...
[16:33:55] debug: OktaHound[0] Processing API token Postman (00T36fk75smeJybKx697)...
```

Extension Schema

The screenshot displays the BloodHound Enterprise interface. The left sidebar contains navigation options: Attack Paths, Explore, Posture, Privilege Zones, Quick Upload, Profile, Download Collectors, Administration (highlighted), API Explorer, Docs and Support, Dark Mode (toggle), and Log Out. The main content area is titled "OpenGraph Management" and includes a "Custom Schema Upload" section with an "Upload File" button. Below this is a table of "Active Extensions" with a search bar.

Name	Version	
Active Directory	v0.0.1	🗑️
Azure	v0.0.1	🗑️
GitHub (GitHound)	v1.1.0	🗑️
JAMF (JamfHound)	1.1.1	🗑️
Okta (OktaHound)	2.8.0	🗑️
SCIM	1.2.0	🗑️

Extension Schema

Nodes	
Icon	Node Kind
	Okta_Agent
	Okta_AgentPool
	Okta_ApiServiceIntegration
	Okta_ApiToken
	Okta_Application
	Okta_AuthorizationServer
	Okta_ClientSecret
	Okta_CustomRole
	Okta_Device
	Okta_Group
	Okta_IdentityProvider
	Okta_JWK
	Okta_Organization
	Okta_Policy
	Okta_Realm
	Okta_ResourceSet
	Okta_Role
	Okta_RoleAssignment
	Okta_User

Edges	
Relationship Kind	Traversable
Okta_AddMember	✓
Okta_AgentMemberOf	✓
Okta_AgentPoolFor	✓
Okta_ApiTokenFor	✓
Okta_AppAdmin	✓
Okta_AppAssignment	✗
Okta_Contains	✓
Okta_CreatorOf	✗
Okta_DeviceOf	✗
Okta_GroupAdmin	✓
Okta_GroupMembershipAdmin	✓
Okta_GroupPull	✓
Okta_GroupPush	✗
Okta_HasRole	✗
Okta_HasRoleAssignment	✗
Okta_HelpDeskAdmin	✓
Okta_HostsAgent	✓
Okta_IdentityProviderFor	✓
Okta_IdpGroupAssignment	✗
Okta_InboundOrgSSO	✓
Okta_InboundSSO	✓
Okta_KerberosSSO	✓
Okta_KeyOf	✓
Okta_ManageApp	✓

Okta_ManagerOf	✗
Okta_MemberOf	✓
Okta_MembershipSync	✓
Okta_MobileAdmin	✓
Okta_OrgAdmin	✓
Okta_OrgSWA	✗
Okta_OutboundOrgSSO	✓
Okta_OutboundSSO	✓
Okta_PasswordSync	✓
Okta_PolicyMapping	✗
Okta_ReadClientSecret	✓
Okta_ReadPasswordUpdates	✓
Okta_RealmContains	✓
Okta_ResetFactors	✓
Okta_ResetPassword	✓
Okta_ResourceSetContains	✓
Okta_ScopedTo	✗
Okta_SecretOf	✓
Okta_SuperAdmin	✓
Okta_SWA	✗
Okta_UserPull	✗
Okta_UserPush	✗
Okta_UserSync	✗

BloodHound OpenGraph Collectors

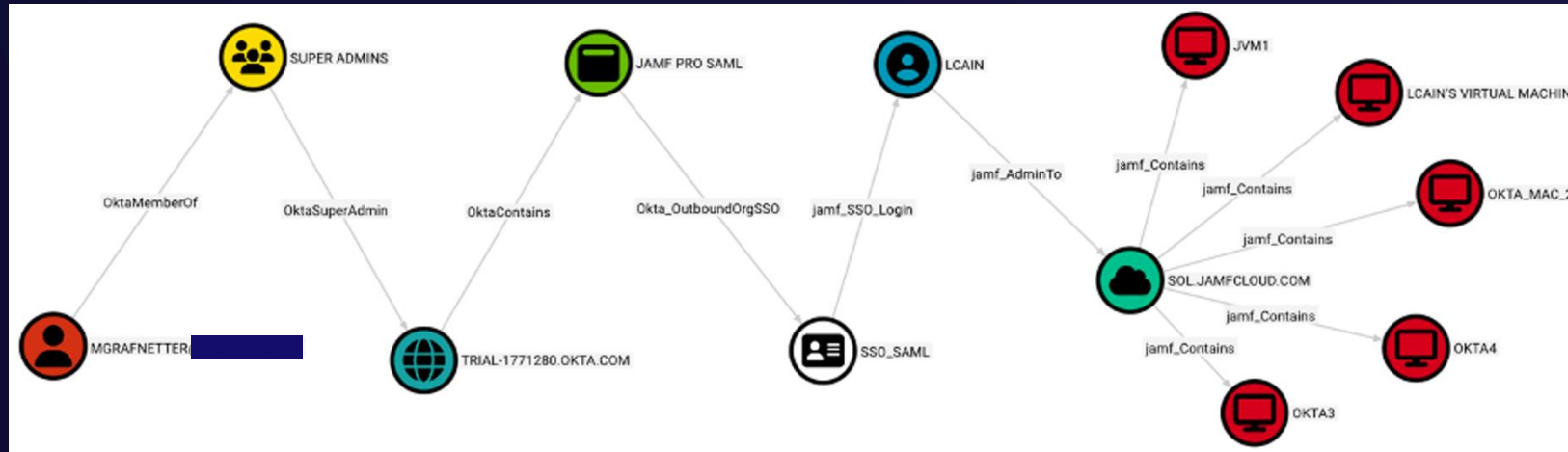
JamfHound

JamfHound

- OpenGraph collector for JAMF Pro cloud and on-site tenants
- Released at BlackHat USA 2025
- Continued researching attack paths in JAMF Pro
- As of March 2026, the latest version of the collector now supports new Okta hybrid paths
 - SSOIntegration Node
 - jamf_Okta_Same_Device Edge
 - jamf_SSO_Login Edge



JamfHound



Key Takeaways

- While defaults are secure, Okta doesn't inherently mitigate additions such as app integrations and custom roles
- MDM SSO support = expanded and conjoined attack surface with IDPs
 - Always a high-value target for attackers
- Okta protects what it knows about within the org (Super Admins), but does not know the privileges of external identities
 - i.e. JAMF Pro admins, GitHub admins, or AD domain admins
- *It's critical to know what the full attack surface looks like*
 - OpenGraph updates to BloodHound reveal complex attack paths across different technologies



Resources

- OktaHound OpenGraph Collector - <https://github.com/SpecterOps/OktaHound>
- JamfHound OpenGraph Collector - <https://github.com/SpecterOps/JamfHound>
- GitHound OpenGraph Collector - <https://github.com/SpecterOps/GitHound>
- SCIM OpenGraph Schema Extension - <https://github.com/SpecterOps/bloodhound-scim-extension>
- Eve JAMF Pro Exploitation Toolkit - <https://github.com/RobotOperator/Eve>
- JamfHound Okta Updates - <https://specterops.io/blog/2026/03/31/jamfhound-v1-1-update-sso-attack-paths-and-okta-additions/>

Thank you

