

Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on May 21, 2024 and its most recent report on Form 10-K filed on September 7, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

Splunk and Splunk> are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2024 Splunk Inc. All rights reserved.

Cloud Identity Crisis

Defending Identities in an Okta® Environment

SEC1648B



Speakers



Mauricio Velazco

Principal Threat Research Engineer
Splunk



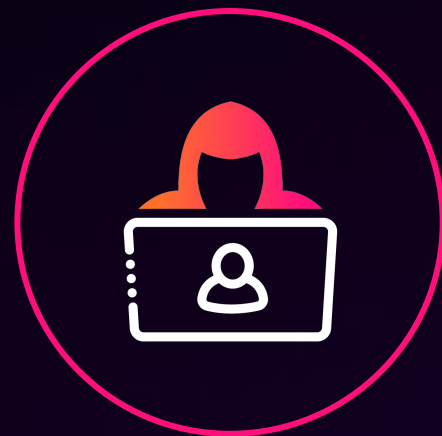
Bhavin Patel

Senior Threat Research Engineer
Splunk

Agenda

- Introduction
- Getting Okta Telemetry in Splunk
- Detection Opportunities
- Takeaways

Splunk Threat Research Team



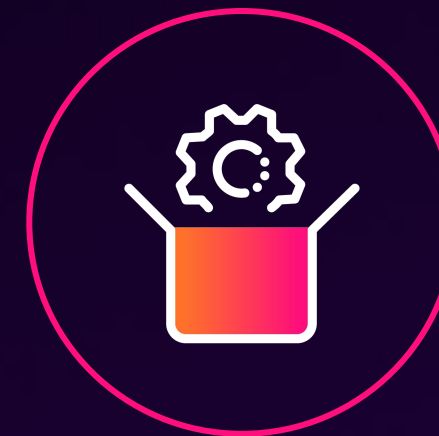
**Study
Threats**



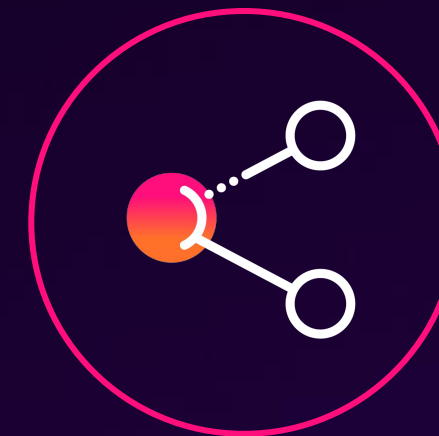
**Create
Datasets**



**Build
Detections**



**Release
Tools**



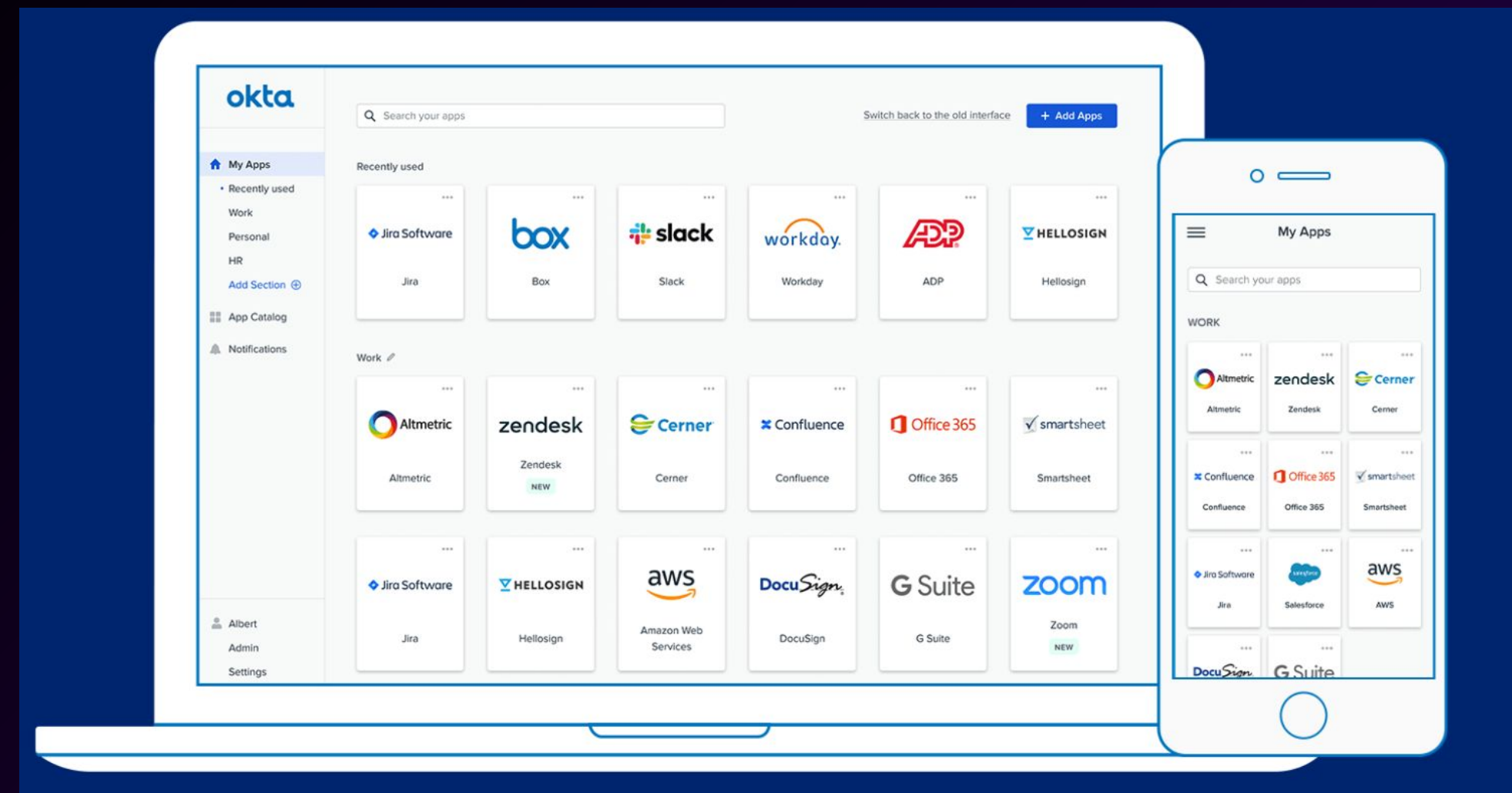
**Share with
Community**

What is OKTA?

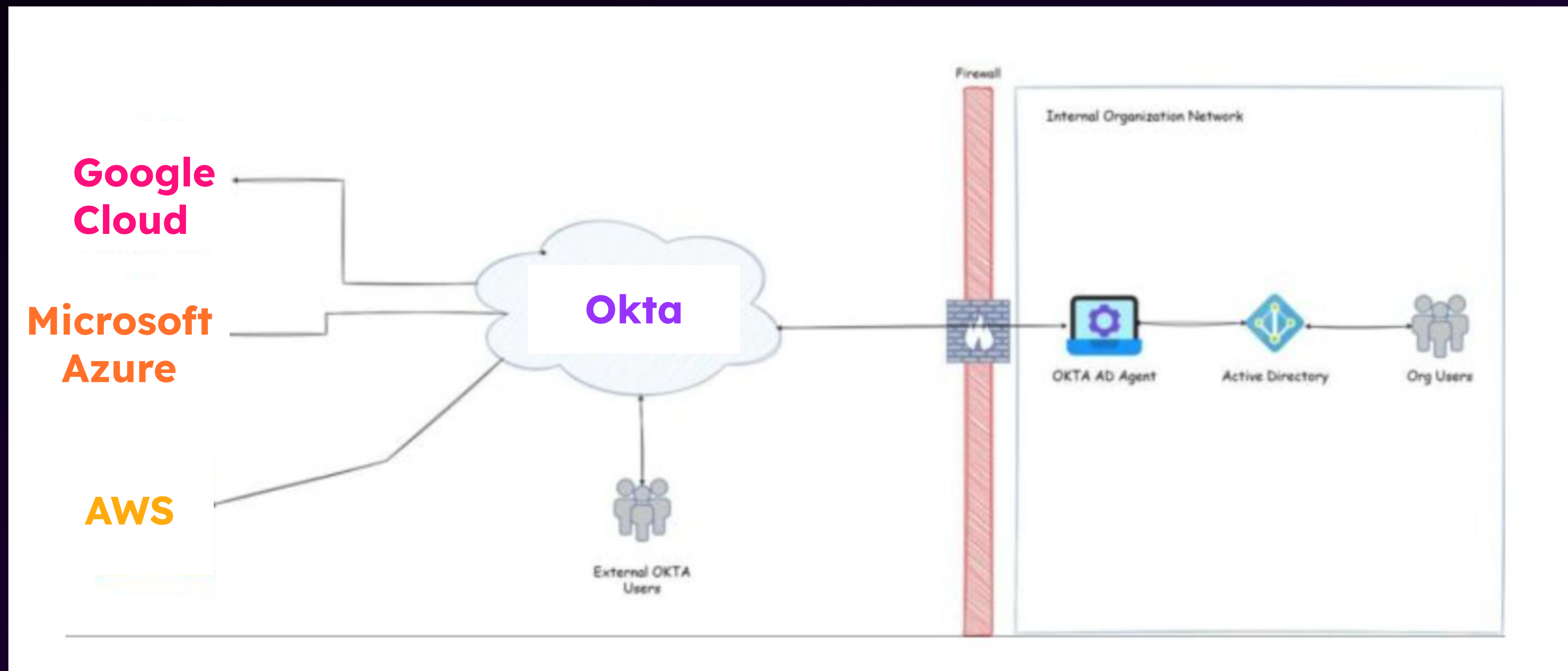
“An okta is a unit of measurement used to describe the amount of cloud cover at any given location such as a weather station.”

Okta is a **cloud-based** identity and access management (**IAM**) platform that allows users to login to applications **securely** from any device.

Allows administrators to **efficiently** handle user identities, **authentication**, and **permissions** for different applications and systems.



Common Okta Use Case



Authentication Policies

Flexible rules that manage authentication requirements for users accessing integrated applications.

Granular controls enforce one or more authentication factors (password complexity, MFA, device trust, platform) based on user groups, applications, and network zones.




These policies enhance security and ensure **only authorized users** access critical resources.

Authentication policies

Define how a user must authenticate to gain access to an app

Add a policy

Search...

Policy name	Applies to
admin_sfa	0 Apps View
Classic Migrated Policy created during OIE upgrade and applied to all applications that were protected by the default app-sign on policy in Classic.	1 App View 
Default Policy Default	1 App View 
Okta Admin Console Application-specific policy	1 App View 



Cloud Identity Crisis



TECH SCIENCE BUSINESS HEALTH CULTURE DEALS & REVIEWS JOBS   

HOME > SECURITY

SECURITY DEFENSE APPS/SOFTWARE SECURITY GOOGLE GADGETS

Unprecedented Surge in Credential Stuffing Hacks Observed by Okta

A nearing spike in credential stuffing attacks.

Aldohn Domingo, Tech Times | 29 April 2024, 12:04 am

Credential stuffing **cyberattacks** have recently reached record levels, **warns** identity and access management (IAM) services provider Okta.

MOST POPULAR

1.



China Launches World's Largest Electric Container Ship, Slashing

Cloud Identity Crisis

TECH
TIMES

TECHSCIENCEBUSINESSHEALTHCULTUREDEALS & REVIEWSJOBSS

HOME > SECURITY

SECURITYDEFENSEAPPS/SOFTWARESECURITYGOOGLEGADGETS

Unprecedented Surge in Credential Stuffing Hacks Observed by Okta

A nearing spike in credential stuffing attacks.


Aldohn Domingo, Tech Times | 29 April 2024, 12:04 am

Credential stuffing **cyberattacks** have recently reached record levels, according to a report from identity management (IAM) services provider Okta.

NEWS

Okta: Caesars, MGM hacked in social engineering campaign

Identity management vendor Okta had previously disclosed that four unnamed customers had fallen victim to a social engineering campaign that affected victims' MFA protections.



By Alexander Culafi, Senior News Writer

Published: 20 Sep 2023

ADVERTISEMENT

AI in IAM?
Sounds like
fantasy

Join the webinar on

Cloud Identity Crisis

Cross-Tenant Impersonation: Prevention and Detection

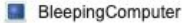


Defensive Cyber Operations

Summary

- Okta has observed attacks in which a threat actor used social engineering to attain a highly privileged role in an Okta customer Organization (tenant).
- When successful, the threat actor demonstrated novel methods of lateral movement and defense evasion.
- These methods are preventable and present several detection opportunities for defenders.


Cloud Identity Crisis

 BleepingComputer

Okta warns of "unprecedented" credential stuffing attacks on customers

Okta warns of an "unprecedented" spike in credential stuffing attacks targeting its identity and access management solutions,...


3 days ago

 SC Media

Okta breach linked to employee's personal Google account

A previously disclosed breach of Okta's backend support case management system allowed attackers to access files relating to 134 customers.

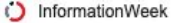
Nov 6, 2023

 Tech Times

Unprecedented Surge in Credential Stuffing Hacks Observed by Okta

Credential stuffing attacks have recently surged at record levels as more tools are becoming more available for threat actors, says Okta.


1 day ago

 InformationWeek


Massive Okta Breach: What CISOs Should Know

After Okta's admission last week that 100% of its 18400 customers were exposed to a breach of its customer support system, security experts...


Dec 6, 2023




 TechCrunch

Okta admits hackers accessed data on all customers during recent breach



In-depth security news and investigation





[HOME](#) [ABOUT THE AUTHOR](#) [ADVERTISING/SPEAKING](#)

Hackers Stole Access Tokens from Okta’s Support Unit

October 20, 2023 15 Comments

Okta, a company that provides identity tools like multi-factor authentication and single sign-on to thousands of businesses, has suffered a security breach involving a compromise of its customer support unit, KrebsOnSecurity has learned. Okta says the incident affected a “very small number” of customers, however it appears the hackers responsible had access to Okta’s support platform for at least two weeks before the company fully contained the intrusion.

Mailing List

Subscribe here

Search KrebsOnSecurity

SEARCH

Stay Ahead

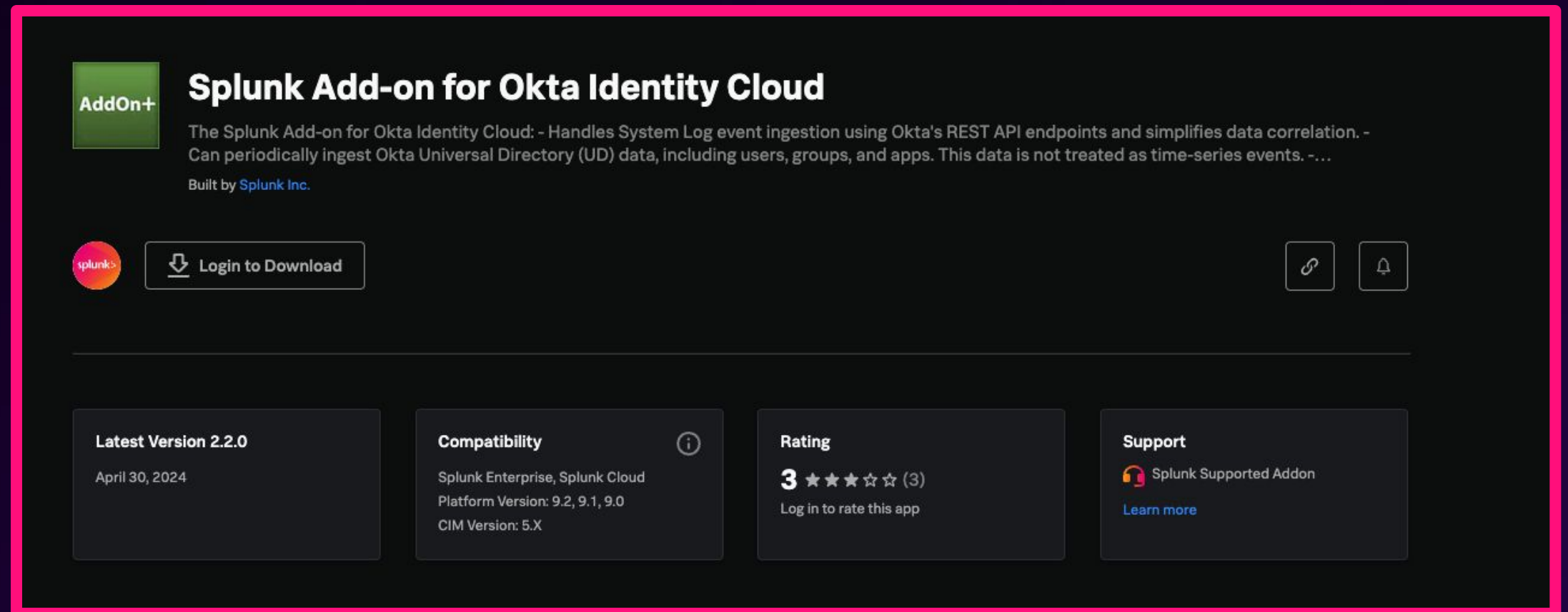
- In the realm of cloud computing, **identity** has become the new **perimeter**.
- Okta serves as the **gateway to all** your applications and data.
- Detecting unusual behavior **early** can **prevent** potential security breaches and protect **sensitive** information.

Getting Okta Telemetry in Splunk

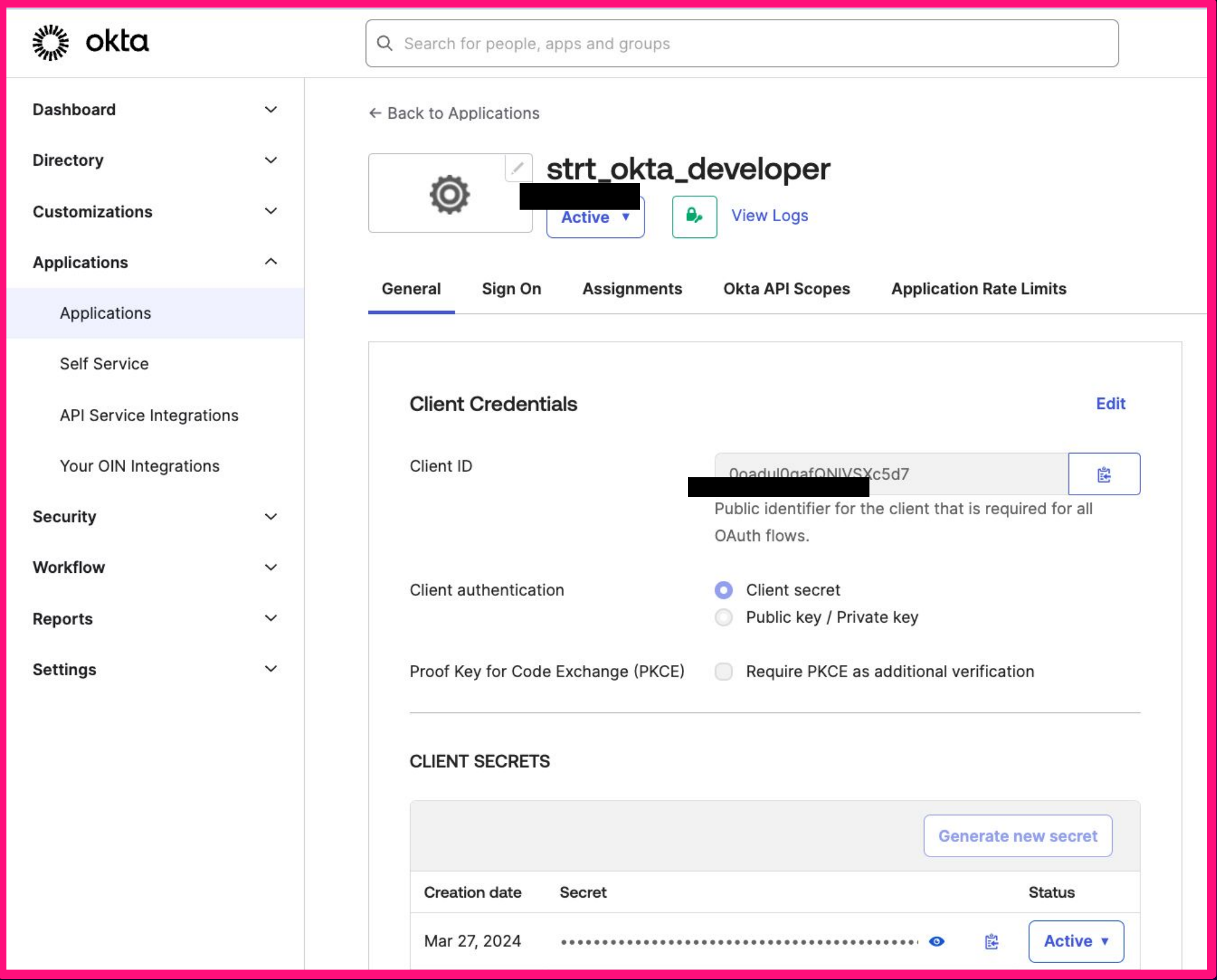
Splunk Add-on for Okta Identity Cloud

<https://splunkbase.splunk.com/app/6553>

- OktaIM2:log
- OktaIM2:user
- OktaIM2:group
- OktaIM2:app
- OktaIM2:groupUser
- OktaIM2:appUser



The screenshot shows the Splunk Add-on for Okta Identity Cloud page. At the top, there is a green 'AddOn+' icon and the title 'Splunk Add-on for Okta Identity Cloud'. Below the title, a description states: 'The Splunk Add-on for Okta Identity Cloud: - Handles System Log event ingestion using Okta's REST API endpoints and simplifies data correlation. - Can periodically ingest Okta Universal Directory (UD) data, including users, groups, and apps. This data is not treated as time-series events. -...'. It is built by 'Splunk Inc.'. Below this, there is a 'Login to Download' button and a 'splunk' logo. To the right of the button are icons for a link and a notification bell. Below the main content area, there are four informational boxes: 'Latest Version 2.2.0' (dated April 30, 2024), 'Compatibility' (listing Splunk Enterprise, Splunk Cloud, Platform Version: 9.2, 9.1, 9.0, and CIM Version: 5.X), 'Rating' (3 stars out of 5, with a note to log in to rate), and 'Support' (labeled as a Splunk Supported Addon with a 'Learn more' link).



Okta Admin Dashboard

sourcetype = OktaIM2:log

Create Web Application

- Client ID
- Client secret

Application Scope

- okta.users.read
- okta.logs.read
- okta.groups.read
- okta.apps.read

Splunk Add-on for Okta Identity Cloud

<https://splunkbase.splunk.com/app/6553>

splunk>enterprise

Apps

InputsConfigurationMonitoring

Configuration

Set up your add-on

Okta AccountsAdd-on Settings

1 Item

Okta Account Name

dev_strt_okta

Update Okta Accounts

Okta Account Name

dev_strt_okta

Enter a unique name for this Okta account.

Auth Type

OAuth 2.0 Authentication

Client ID

Unique Client ID

Enter the Okta App Client ID.

Client Secret

Enter the Okta App Client Secret.

Redirect Url

https://35.90.2.227:8000/en-US/app/Splunk_TA_

Copy and paste this URL into your Okta App sign-in redirect url.

Okta Domain

<your comapany name>.okta.com

Enter the Okta domain name for the account. Example: yourdomain.okta.com

Scope

offline_access okta.users.read okta.groups.read

Requested scopes from Okta Web App

Cancel

Update

Add Okta Identity Cloud Input

Name

Name

okta_im2_logs

Enter a unique name for the data input

Interval

300

Time interval of input in seconds.

Index

main

Okta Account

dev_strt_okta

Select the Okta Account from the list which you want to collect the events.

Start Date

Start Date to start the data collection, in UTC timezone. Format: YYYY-MM-DDTHH:MM:SS.SSSZ

Metric

Metric

Select...

Logs

Users

Groups

Apps (not recommended)

Cancel

Add

© 2024 SPLUNK INC.

Okta Log Event

sourcetype = OktaIM2:log

- actor.{}
 - alternateId
 - detailEntry
 - displayName
 - id
 - type
- authenticationContext { [-]
- client { [+] }
- debugContext { [+] }
- device
- displayMessage
- eventType
- legacyEventType
- outcome { [+] }
- published
- request { [+] }
- securityContext { [+] }
- severity
- target [[+]]
- transaction { [+] }
- uuid
- version

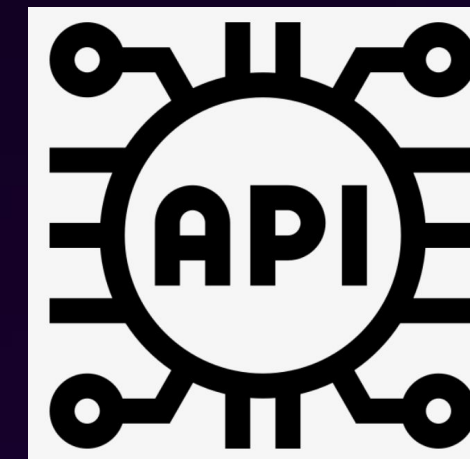
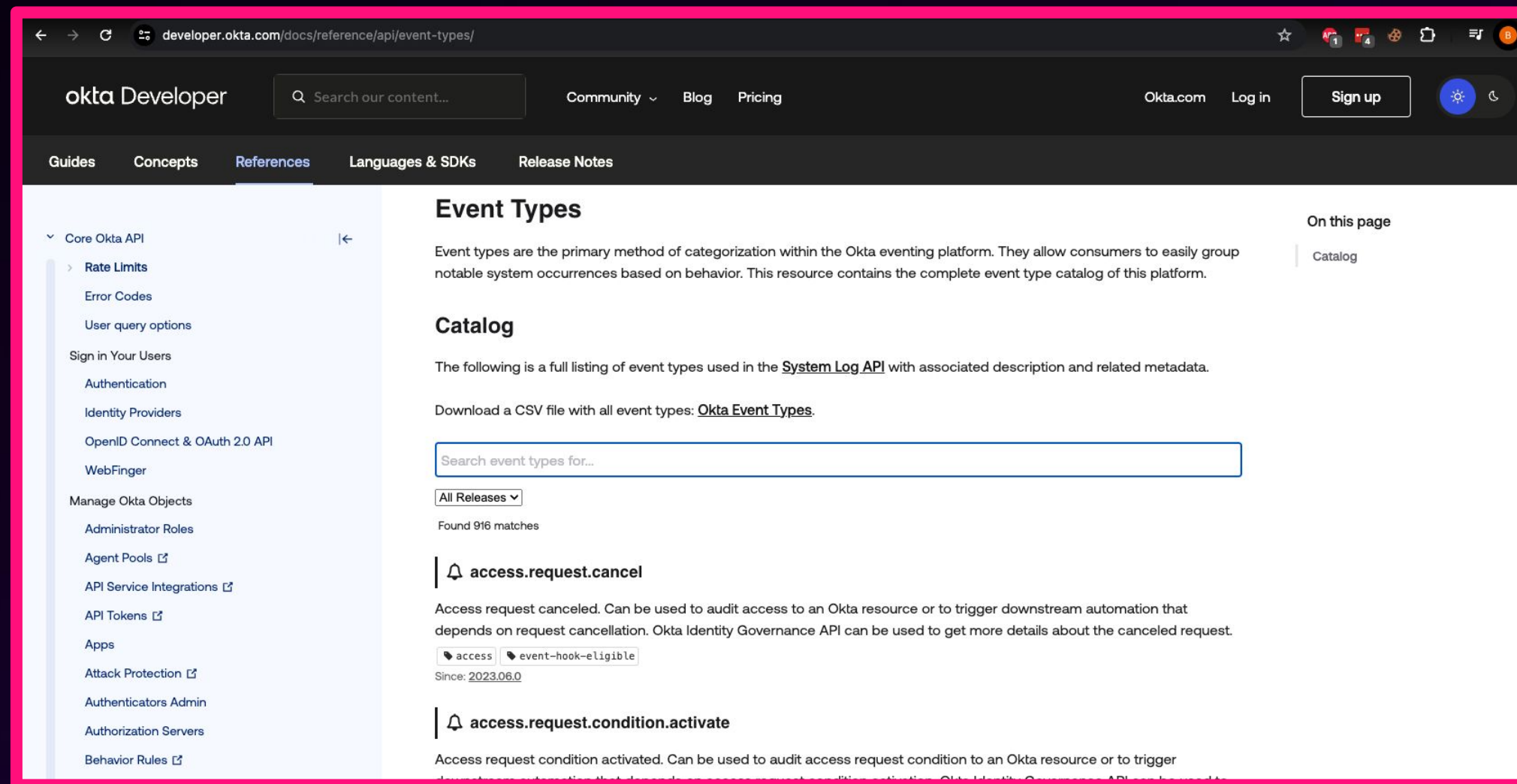
```
> 5/13/24 4:56:15.788 PM { [-]
  actor: { [-]
    alternateId: [REDACTED]@gmail.com
    detailEntry: null
    displayName: [REDACTED]
    id: 00ufgmc7x27vTGT1L5d7
    type: User
  }
  authenticationContext: { [-]
    authenticationProvider: null
    authenticationStep: 0
    credentialProvider: null
    credentialType: null
    externalSessionId: 102LKeZ0QhjSK2J1nMyG1rjRg
    interface: null
    issuer: null
  }
  client: { [+] }
  debugContext: { [+] }
  device: null
  displayMessage: User accessing Okta admin app
  eventType: user.session.access_admin_app
  legacyEventType: app.admin.sso.login.success
  outcome: { [+] }
  published: 2024-05-13T20:56:15.788Z
  request: { [+] }
  securityContext: { [+] }
  severity: INFO
  target: [ [+] ]
  transaction: { [+] }
  uuid: 3d35bf51-116b-11ef-ac6f-8db93646f463
  version: 0
}
```

Show as raw text

What now?

An **Awesome** Resource...

916 documented event types



<https://developer.okta.com/docs/reference/api/event-types/>

Critical Events in OKTA



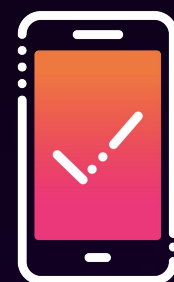
User Authentication Events

- User login attempts
- Multi factor authentication (MFA) events



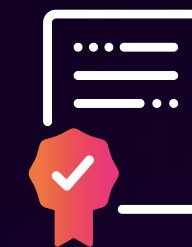
User Account Management Events

- User creation, modification and deletion
- Privilege escalation events



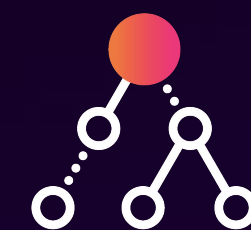
Application Access and Management

- Application addition and removal
- Changes in application permissions



System Configuration and Policy Changes

- Changes to security settings and policies
- IDP modifications



API Token Management

- Creation of API Token
- Modification, or revocation of API tokens

Okta Detection Opportunities

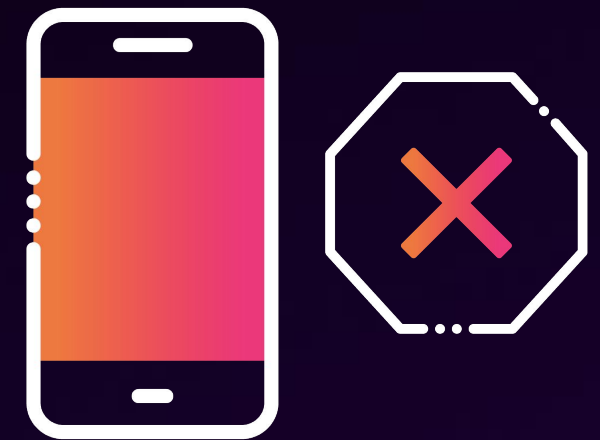
Use Case

Account Takeover

- Okta multiple failed MFA requests For user
- Okta suspicious use of a session cookie



Okta Multiple Failed MFA Requests For User



- **eventType**
 - user.authentication.auth_via_mfa
- **Mitre ATT&CK® Tactic**
 - Credential access
- **Mitre Technique ID**
 - T1621
- **Mitre Technique Name**
 - Multi-factor authentication request generation
- **This type of activity were reported in several adversary campaigns**
 - Scattered spider
 - Scatter swine
 - August 31, 2023 - Okta breach disclosure
 - August 4, 2022- Okta phishing campaign against Twilio

© 2024 SPLUNK INC.

Okta Suspicious Use of a Session Cookie

- **eventType**
 - policy.evaluate_sign_on
- **Mitre ATT&CK Tactic**
 - Credential access
- **Mitre Technique ID**
 - T1539
- **Mitre Technique Name**
 - Steal web session cookie
- **This type of activity were reported in several adversary campaigns**
 - Scattered spider
 - Lapsus\$
 - Okta | Keeping phishing adversaries out of the middle



Okta Suspicious Use of a Session Cookie



SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save As>Create Table ViewClose

index=strt_okta eventType IN (policy.evaluate_sign_on) outcome.result IN (ALLOW, SUCCESS)
| stats earliest(_time) as _time, values(client.ipAddress) as src_ip, values(client.userAgent.os) as userAgentOS_list, values(client.geographicalContext.city) as city, values(client.userAgent
.browser) as userAgentBrowser_list dc(client.userAgent.browser) as dc_userAgentBrowser, dc(client.userAgent.os) as dc_userAgentOS, dc(client.ipAddress) as dc_src_ip, values(outcome.reason)
as reason values(client.userAgent.rawUserAgent) as user_agent by debugContext.debugData.dtHash, user
| where dc_src_ip>1 AND (dc_userAgentOS>1 OR dc_userAgentBrowser>1)
| `okta_suspicious_use_of_a_session_cookie_filter`

All time

Q

257 events (before 5/15/24 9:05:01.000 PM) No Event Sampling

JobPauseStopRefreshDownloadVerbose Mode

Events (257)PatternsStatistics (4)Visualization

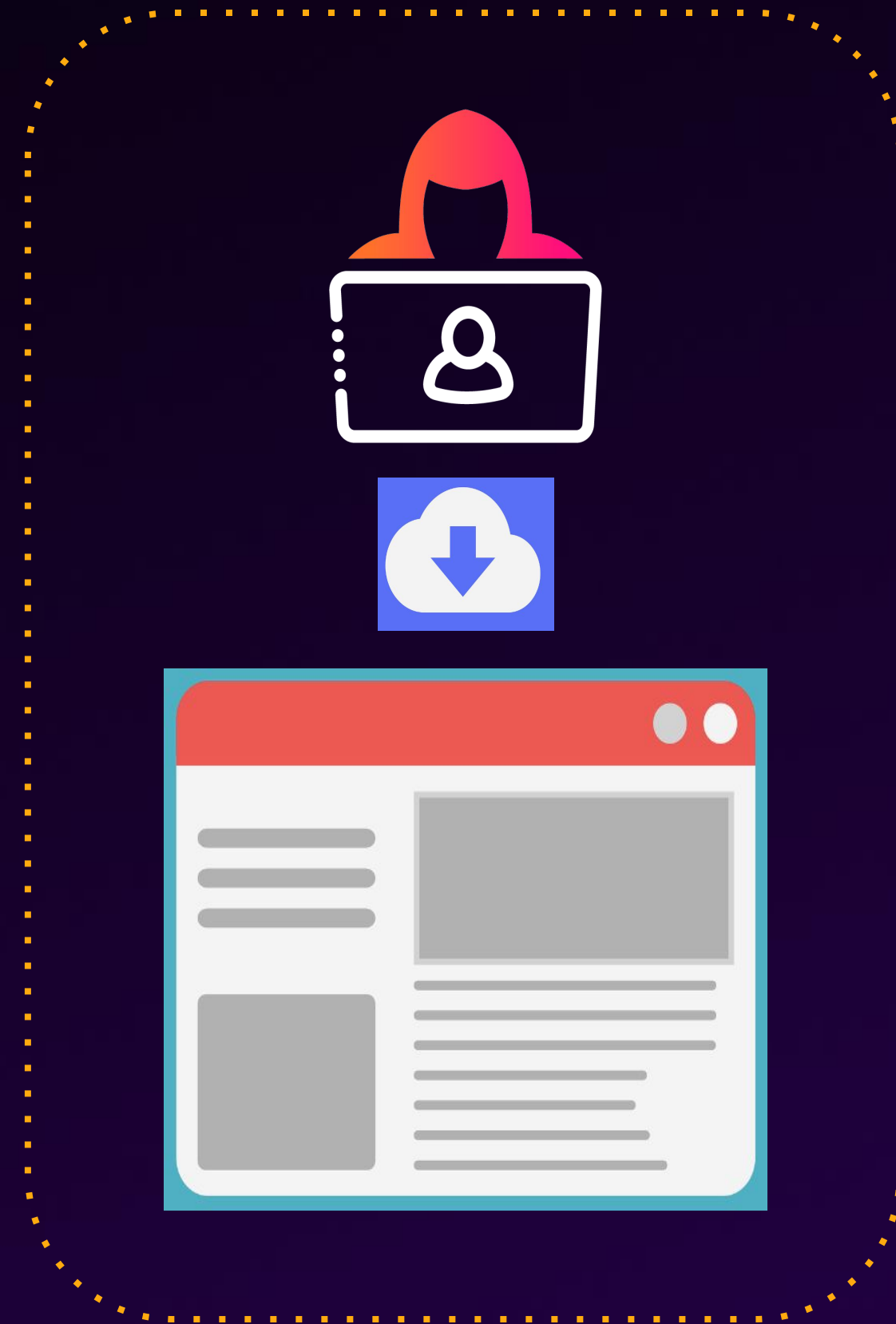
100 Per PageFormatPreview

	user	_time	src_ip	userAgentOS_list	city	userAgentBrowser_list	dc_userAgentBrowser	dc_userAgentOS	dc_src_ip	reason	user_a
58f059647f4bda318	@gmail.com	2024-03-13 16:35:35.647	147 216	Mac OS 13.4.0 (Ventura) Mac OS 13.6.6 (Ventura)		CHROME	1	2	2	Sign-on policy evaluation resulted in AUTHENTICATED	Mozill (Macin Mac OS AppleV (KHTML Gecko) Chrome

Use Case

Exfiltration

- Export user information from identity cloud
- Okta new API token created



Export User Information from Identity Cloud

- **eventType**
 - analytics.reports.export.download
 - analytics.reports.export.generate
 - analytics.reports.export.request
- **Mitre ATT&CK® Tactic** - Discovery, exfiltration
- **Mitre Technique ID** - T1087.004
- **Mitre Technique Name** - Account discovery: cloud account
- **This type of activity were reported in several adversary campaigns**
 - Scattered spider
 - MGM breach
 - Lapsus\$

	A	B	C	D
1	User	Login	MFA Factor	Last Enrolled_ISO8601
2	madhavi ma	madhavi.ma	Password	2021-01-14T22:26:07.0
3	madhavi ma	madhavi.ma	FIDO2 (WebAuthn)	2021-02-10T18:53:44.0
4	madhavi ma	madhavi.ma	Security Question	2021-01-15T16:48:33.0
5	madhavi ma	madhavi.ma	Email Authentication	
6	madhavi ma	madhavi.ma	SMS Authentication	2021-02-10T18:53:23.0
7	madhavi ma	madhavi.ma	Voice Call Authentication	2021-02-10T18:53:23.0
8	madhavi ma	madhavi.ma	Signed Nonce	2021-03-03T17:52:48.0
9	madhavi ma	madhavi.ma	Okta Verify Push	2021-03-04T21:22:33.0
10	madhavi ma	madhavi.ma	Okta Verify	2021-03-03T17:52:08.0
11	madhavi ma	madhavi.ma	Google Authenticator	2021-02-22T21:08:02.0
12				
13				

T3				
T5				
T7	madhavi ma	madhavi.ma	Google Authenticator	2021-03-03T17:52:08.0
T9	madhavi ma	madhavi.ma	Okta Verify	2021-03-03T17:52:08.0

Export User Information from Identity Cloud

splunk>enterpriseApps

Administrator3 MessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboardsSearch & Reporting

New SearchSave AsCreate Table ViewClose

index=strt_okta eventType IN ("analytics.reports.export.request", "analytics.reports.export.download", "analytics.reports.export.generate")

| stats count min(_time) as firstTime max(_time) as lastTime values(target{}.id) as target_id values(target{}.type) as target_modified by src dest src_user_id user user_agent command description

| `security_content_ctime(firstTime)`

| `security_content_ctime(lastTime)`

| `okta_idp_lifecycle_modifications_filter`

8 events (before 5/14/24 6:52:51.000 PM)No Event SamplingJobVerbose Mode

Events (8)PatternsStatistics (4)Visualization

100 Per PageFormatPreview

src	dest	src_user_id	user	user_agent	command	description	count	firstTime	lastTime	target_id	target_modified
0.147	okta.com	00udu2s40phRtye7K5d7		Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36	analytics.reports.export.request	Report CSV Export Requested	1	2024-01-24T21:29:37	2024-01-24T21:29:37	custom-admin-roles	Report
0.147	okta.com	00ufgmc7x27vTGT1L5d7	1@gmail.com	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36	analytics.reports.export.download	Report CSV Export Downloaded	1	2024-04-24T17:32:10	2024-04-24T17:32:10	access-users-app-instances	Report
0.147	okta.com	00ufgmc7x27vTGT1L5d7	1@gmail.com	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36	analytics.reports.export.request	Report CSV Export Requested	2	2024-04-24T17:31:32	2024-04-24T17:32:08	access-users-app-instances password-health	Report
1.216	okta.com	00ufgmc7x27vTGT1L5d7	1@gmail.com	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36	analytics.reports.export.download	Report CSV Export Downloaded	1	2024-05-14T17:49:20	2024-05-14T17:49:20	access-users-app-instances	Report

Okta New API Token Created



- **eventType**
 - system.api_token.create
- **Mitre ATT&CK Tactic** - Persistence, privilege escalation, exfiltration
- **Mitre Technique ID** - T1098.001
- **Mitre Technique Name** - Account manipulation: additional cloud credentials
- **This type of activity were reported in several adversary campaigns**
 - Okta **October 2023** security incident investigation closure
 - Krebs - Hackers stole tokens from Okta's support unit

Okta New API Token Created

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save AsCreate Table ViewClose

| tstats `security_content_summariesonly` count max(_time) as lastTime, min(_time) as firstTime from datamodel=Change where All_Changes.action=created AND All_Changes.command=system.api_token.create by _time span=5m All_Changes.user All_Changes.result All_Changes.command sourcetype All_Changes.src All_Changes.action All_Changes.object_category

| `drop_dm_object_name("All_Changes")`

| `security_content_ctime(firstTime)`

| `security_content_ctime(lastTime)`

| `okta_new_api_token_created_filter`

All time

4 events (before 5/15/24 9:41:13.000 PM)No Event Sampling

JobPauseStopRefreshDownloadVerbose Mode

Events (4)PatternsStatistics (4)Visualization

100 Per PageFormatPreview

_time	user	result	command	sourcetype	src	action	object_category	count	lastTime	firstTime
2023-12-14 20:20:00	[redacted]@github.oktaidp	Create API token	system.api_token.create	OktaIM2:log	[redacted]13.13	created	Token	1	2023-12-14T20:22:41	2023-12-14T20:22:41
2024-03-06 15:05:00	[redacted]@plunk.com	Create API token	system.api_token.create	OktaIM2:log	[redacted]21.43	created	Token	1	2024-03-06T15:08:34	2024-03-06T15:08:34

Use Case:

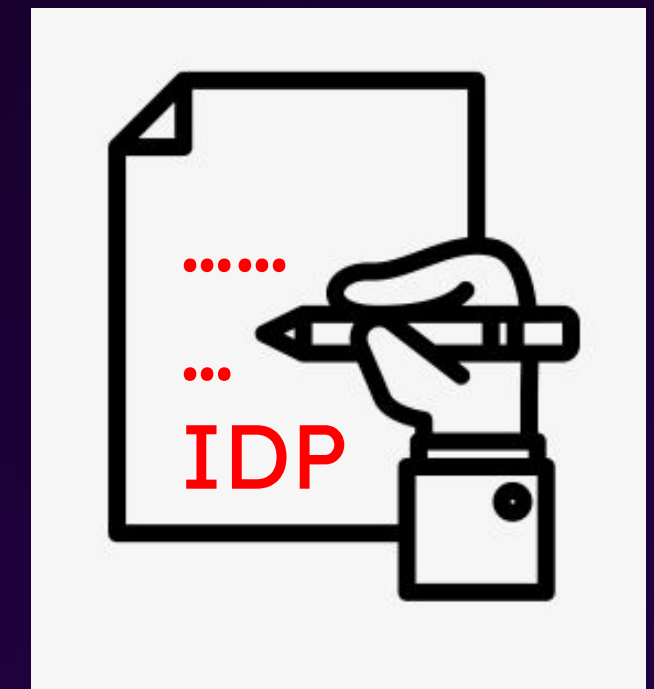
Persistence

- Okta IDP lifecycle modifications
- Global session policy modifications



Okta IDP Lifecycle Modifications

- **eventType**
 - system.idp.lifecycle.activate
 - system.idp.lifecycle.create
 - system.idp.lifecycle.delete
 - system.idp.lifecycle.deactivate
- **Mitre ATT&CK Tactic** - Credential access, defense evasion, persistence
- **Mitre Technique ID** - T1556
- **Mitre Technique Na26me** - Modify authentication process
- **This type of activity were reported in several adversary campaigns**
 - Behind the breach: Cross-tenant impersonation in Okta



Okta IDP Lifecycle Modifications

New Search

Save As>Create Table View>Close

index=strt_...okta eventType IN ("system.idp.lifecycle.activate","system.idp.lifecycle.create","system.idp.lifecycle.delete","system.idp.lifecycle.deactivate")
| stats count min(_time) as firstTime max(_time) as lastTime values(target{}.id) as target_id values(target{}.type) as target_modified by src dest src_user_id user user_agent command description
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `okta_idp_lifecycle_modifications_filter`

All time

5 events (before 5/14/24 6:50:10.000 PM) No Event SamplingJob Verbose Mode

Events (5)PatternsStatistics (4)Visualization

100 Per PageFormatPreview

src	dest	src_user_id	user	user_agent	command	description	count	firstTime	lastTime	target_id	target_modified
213.13	dev-...okta.com	00udu2s40phRtye7K5d7	@github.oktaidp	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	system.idp.lifecycle.activate	Activate an Identity Provider	1	2023-12-14T21:12:51	2023-12-14T21:12:51	0oadup8giv0zAemm65d7	IdentityProvider
213.13	dev-...7.okta.com	00udu2s40phRtye7K5d7	@github.oktaidp	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	system.idp.lifecycle.create	Create an Identity Provider	1	2023-12-14T21:12:17	2023-12-14T21:12:17	0oadup8giv0zAemm65d7	IdentityProvider
213.13	dev-...okta.com	00udu2s40phRtye7K5d7	@github.oktaidp	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	system.idp.lifecycle.deactivate	Deactivate an Identity Provider	2	2023-12-14T21:12:48	2023-12-14T21:13:58	0oadup8giv0zAemm65d7	IdentityProvider
213.13	dev-...okta.com	00udu2s40phRtye7K5d7	@github.oktaidp	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)	system.idp.lifecycle.delete	Delete an Identity Provider	1	2023-12-14T21:14:35	2023-12-14T21:14:35	0oadup8giv0zAemm65d7	IdentityProvider

Global Session Policy Modifications



- **eventType**
 - policy.rule.update
- **Mitre ATT&CK Tactic** - Credential access, defense evasion, persistence
- **Mitre Technique ID** - T1556.006
- **Mitre Technique Name** - Modify authentication process: Multi-factor authentication
- This type of activity were reported in several adversary campaigns
 - Scattered Spider | CISA
 - Behind the Breach: Cross-tenant impersonation in Okta
 - How threat actors leveraged HAR files to attack Okta's customers

Global Session Policy Modifications

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboardsSearch & Reporting

New Search

Save As>Create Table ViewClose

index=oktaeventType=policy.rule.updatetarget{}.detailEntry.policyType= "Okta:SignOn"
| rename debugContext.debugData.* as *
| search oldPolicyRuleRequirementsJson =*2FA* newPolicyRuleRequirementsJson=*1FA*
| table _time user target{}.detailEntry.policyType
 eventType oldPolicyRuleRequirementsJson newPolicyRuleRequirementsJson target_data
|

All time

2 events (before 5/14/24 2:51:05.000 AM)No Event Sampling

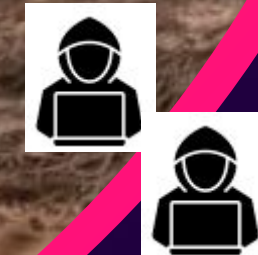
JobPauseStopRefreshDownloadVerbose Mode

Events (2)PatternsStatistics (2)Visualization

100 Per PageFormatPreview

	target{}.detailEntry.policyType	eventType	oldPolicyRuleRequirementsJson	newPolicyRuleRequirementsJson
Okta:SignOn	policy.rule.update		<div>OLD = *2FA*</div> <div><pre>{ "verificationMethod": { "factorMode": "2FA", "type": "ASSURANCE", "reauthenticateIn": "PT0S", "constraints": [{ "knowledge": { "types": ["password"] }, "reauthenticateIn": "PT100H", "possession": { "deviceBound": "REQUIRED" } }] } }</pre></div>	<div>NEW = *1FA*</div> <div><pre>{ "verificationMethod": { "factorMode": "1FA", "type": "ASSURANCE", "reauthenticateIn": [{ "knowledge": { "types": ["password"] } }] } }</pre></div>

**Do you even
threat hunt?**



Okta MFA Exhaustion Hunt

New Search

Save As

Create Table View

Close

All time

```

index=okta eventType=system.push.send_factor_verify_push OR ((legacyEventType=core.user.factor.attempt_success) AND (debugContext.debugData.factor=OKTA_VERIFY_PUSH)) OR
((legacyEventType=core.user.factor.attempt_fail) AND (debugContext.debugData.factor=OKTA_VERIFY_PUSH))
| stats count(eval(legacyEventType="core.user.factor.attempt_success")) as successes count(eval(legacyEventType="core.user.factor.attempt_fail")) as failures count(eval
(eventType="system.push.send_factor_verify_push")) as pushes by user,_time
| stats latest(_time) as lasttime earliest(_time) as firsttime sum(successes) as successes sum(failures) as failures sum(pushes) as pushes by user
| eval seconds=lasttime-firsttime
| eval lasttime=strftime(lasttime, "%c")
| search (pushes>1)
| eval totalattempts=successes+failures
| eval finding="Normal authentication pattern"
| eval finding=if(failures==pushes AND pushes>1,"Authentication attempts not successful because multiple pushes denied",finding)
| eval finding=if(totalattempts==0,"Multiple pushes sent and ignored",finding)
| eval finding=if(successes>0 AND pushes>3,"Probably should investigate. Multiple pushes sent, eventual successful authentication!",finding)
| `okta_mfa_exhaustion_hunt_filter`

```

✓ 25 events (before 5/14/24 7:03:21.000 PM)

No Event Sampling

Job

Verbose Mode

Events (25)

Patterns

Statistics (1)

Visualization

100 Per Page

Format

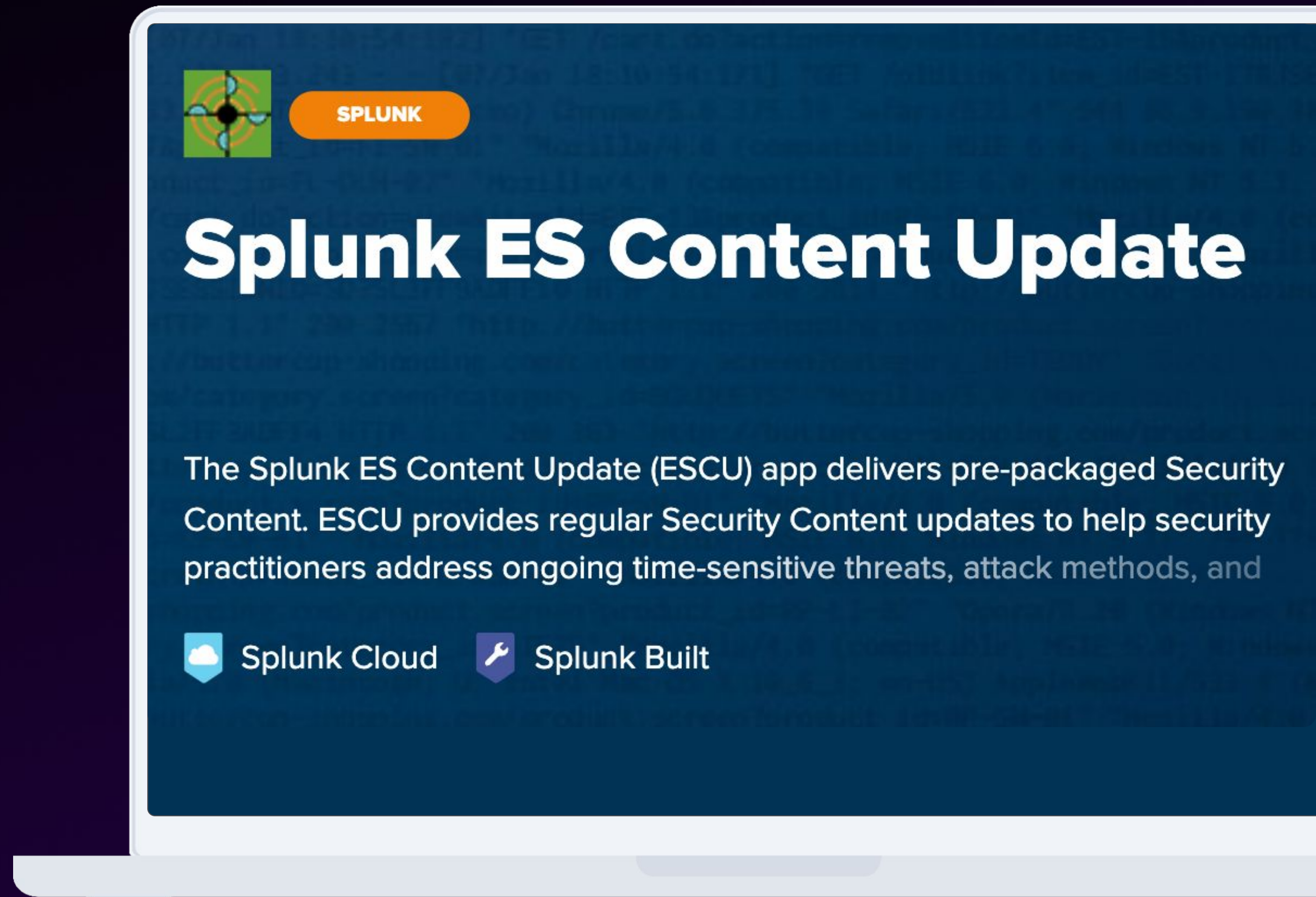
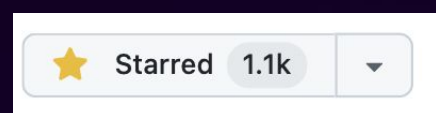
Preview

user	lasttime	firsttime	successes	failures	pushes	finding	seconds	totalattempts
@gmail.com	Sat May 11 02:40:28 2024	1712615970.937	8	0	13	Probably should investigate. Multiple pushes sent, eventual successful authentication!	2779257.813	8

Splunk® Enterprise Security Content Update

In 2024...
12 ESCU version released

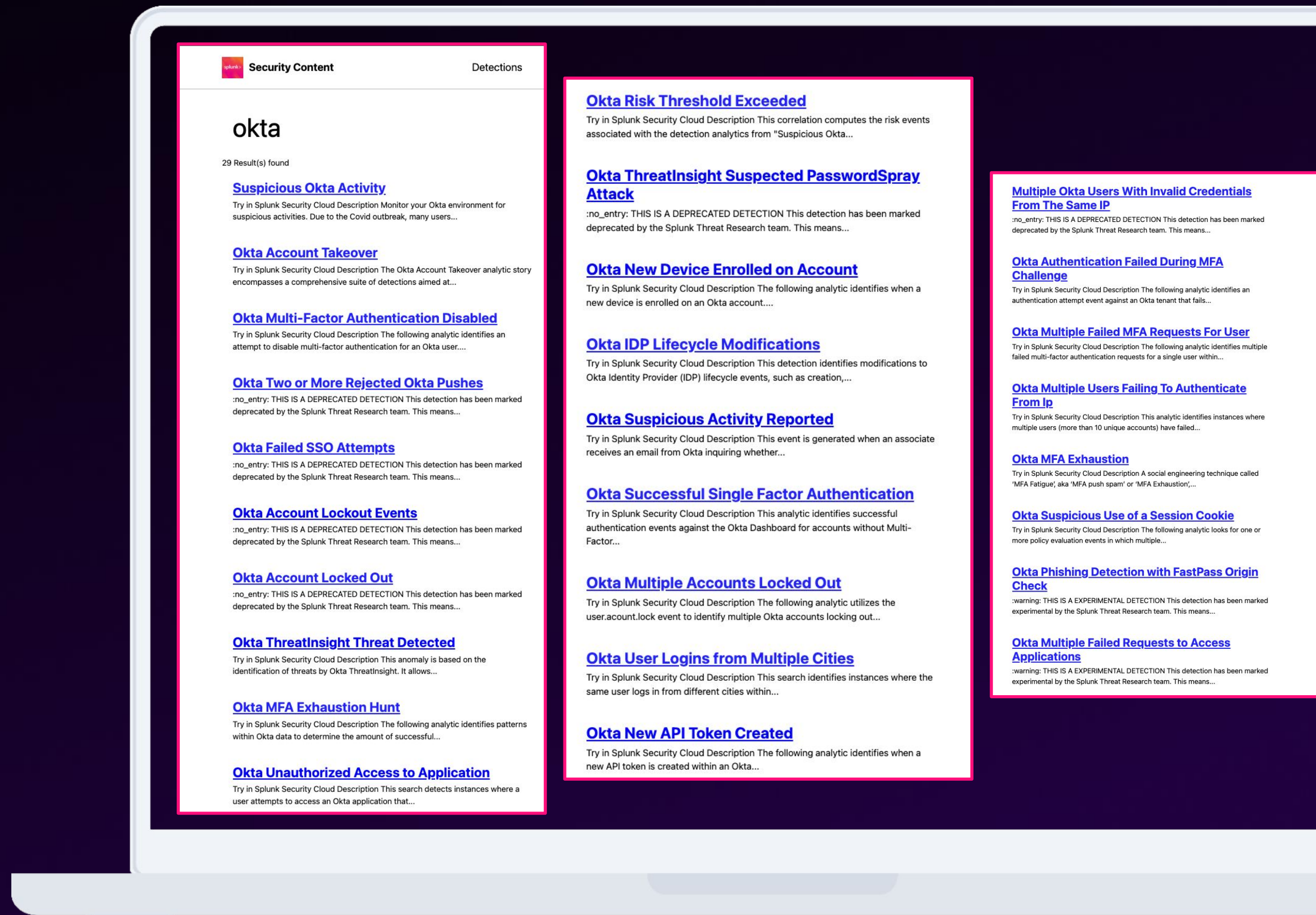
[Security Content Github](#)





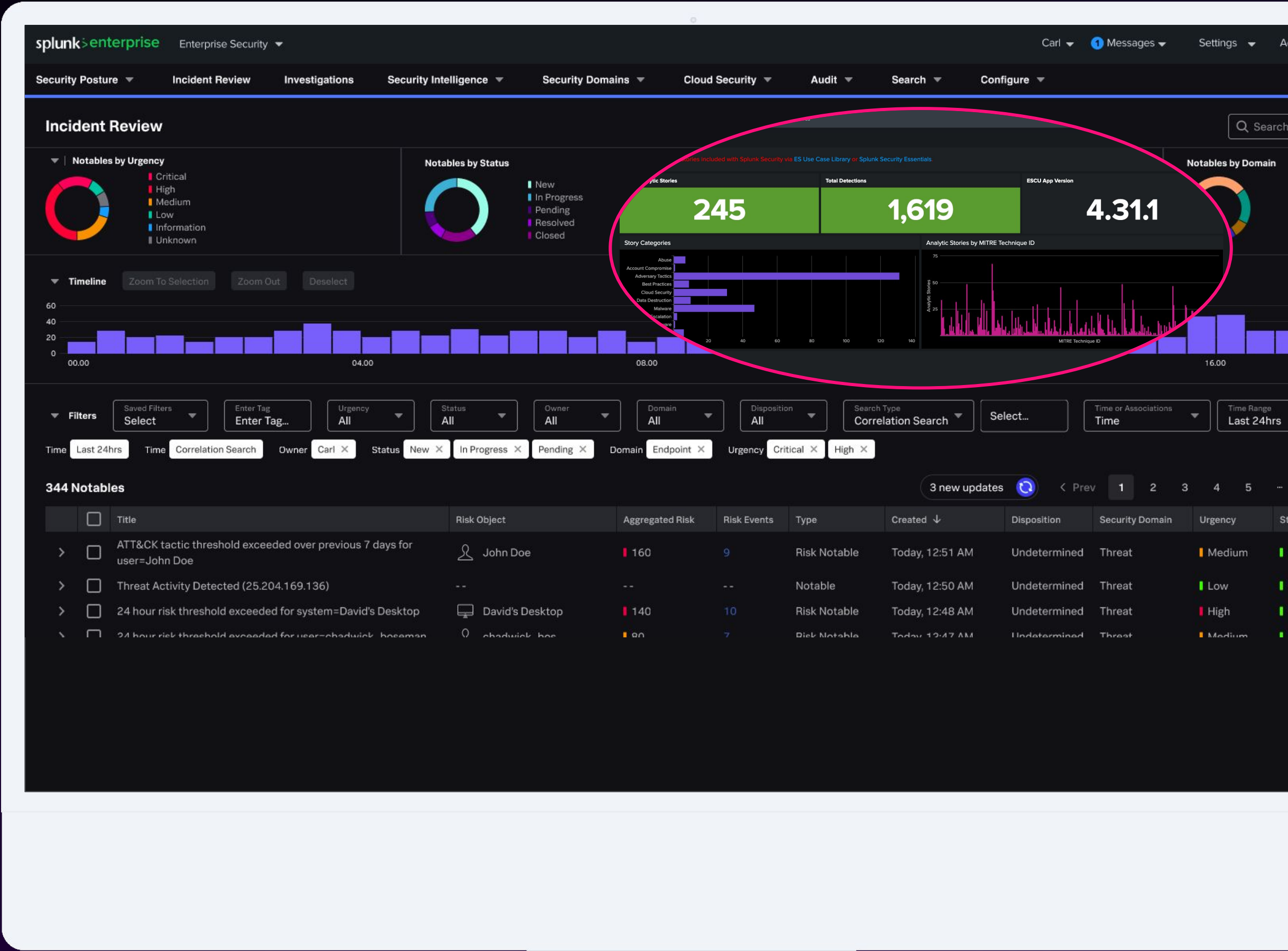
Detections

- Total Detections
 - 20 +
- Mitre Coverage:
 - 11 technique IDs
- Mitre ATT&CK Tactic
 - Credential access
 - Discovery
 - Exfiltration
 - Persistence
 - Privilege escalation



Splunk Enterprise Security

- Use case library
- Risk analysis framework
- Incident management
- Respond using SOAR



Analytic Story

Okta account takeover

- 18 Detections
- Types
 - TTP: 7
 - Anomaly: 9
 - Correlation: 1
 - Hunting: 1

Analytic Story Details: Okta Account Takeover

Use Case: Adversary Tactics

[Back to Use Case Library](#)

Description

The Okta Account Takeover analytic story encompasses a comprehensive suite of detections aimed at identifying unauthorized access and potential takeover attempts of Okta accounts. This collection leverages diverse data points and behavioral analytics to safeguard user identities and access within cloud environments. Monitor for activities and techniques associated with Account Takeover attacks against Okta tenants.

Narrative

Okta is a cloud-based identity management service that provides organizations with a secure way to manage user access to various applications and services. It enables single sign-on (SSO), multi-factor authentication (MFA), lifecycle management, and more, helping organizations streamline the user authentication process. Account Takeover (ATO) is an attack whereby cybercriminals gain unauthorized access to online accounts by using different techniques like brute force, social engineering, phishing & spear phishing, credential stuffing, etc. By posing as the real user, cyber-criminals can change account details, send out phishing emails, access sensitive applications, or use any stolen information to access further accounts within the organization. This analytic story groups detections that can help security operations teams identify the potential compromise of Okta accounts.

References

- <https://attack.mitre.org/techniques/T1586/>
- <https://www.imperva.com/learn/application-security/account-takeover-ato/>
- <https://www.barracuda.com/glossary/account-takeover>
- <https://www.okta.com/customer-identity/>

Created: N/A

Last Modified: 2024-03-06

Version: 1

Edit

CIS 20

CIS 10

Kill Chain

DeliveryExploitationInstallationWeaponization

MITRE ATT&CK

T1586T1586.003T1078T1078.004T1621T1110T1556T1556.006T1550.004T1538T1110.003T1078.001T1098T1098.005T1539T1087.004

NIST

DE.CMDE.AE

Technologies

Okta

Detection

ESCU - Okta Authentication Failed Duri...

ESCU - Okta MFA Exhaustion Hunt - Rule

ESCU - Okta Mismatch Between Source ...

ESCU - Okta Multi-Factor Authentication ...

ESCU - Okta Multiple Accounts Locked ...

ESCU - Okta Multiple Failed MFA Reque...

ESCU - Okta Multiple Failed Requests to ...

ESCU - Okta Multiple Users Failing To Au...

ESCU - Okta New API Token Created - R...

ESCU - Okta New Device Enrolled on Ac...

ESCU - Okta Phishing Detection with Fas...

ESCU - Okta Risk Threshold Exceeded - ...

ESCU - Okta Authentication Failed During MFA Challenge - Rule

Description

The following analytic identifies an authentication attempt event against an Okta tenant that fails during the Multi-Factor Authentication (MFA) challenge. This detection is written against the Authentication datamodel and we look for a specific failed events where the authentication signature is user.authentication.auth_via_mfa. This behavior may represent an adversary trying to authenticate with compromised credentials for an account that has multi-factor authentication enabled.

Explanation

The following analytic identifies an authentication attempt event against an Okta tenant that fails during the Multi-Factor Authentication (MFA) challenge. This detection is written against the Authentication datamodel and we look for a specific failed events where the authentication signature is user.authentication.auth_via_mfa. This behavior may represent an adversary trying to authenticate with compromised credentials for an account that has multi-factor authentication enabled.

Search

```
1 | tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime values(Authentication.app) as app values(Authentication.reason) as reason values(Authentication.signature) as signature values (Authentication.method) as method from datamodel=Authentication where Authentication.signature=user.authentication.auth_via_mfa Authentication.action = failure by _time Authentication.src Authentication.user Authentication.dest Authentication.action | `drop_dm_object_name("Authentication")` | `security_content_ctime (firstTime)` | `security_content_ctime(lastTime)` | iplocation src | `okta_authentication_failed_during_mfa_challenge_filter`
```

Custom time

Q

© 2024 SPLUNK INC.

Risk Based Alerting Using Splunk Enterprise Security



▼

RBA:

Okta Risk Threshold Exceeded

13908

247

Risk Notable

Today, 9:51 PM

Undetermined

Access

Medium

New

unassigned

▼

▼

MITRE ATT&CK Posture for this Notable

The highlighted techniques were detected on the risk object **bpatel@splunk.com**

🔍

Detections in Notable

8

🕒

Detections in Selected Time Range

0

Sub-Techniques (1) ▼

Last 30 days ▼

<div>Reconnaissance 🔗</div> <div>0 of 10 Techniques (0%)</div>	<div>Resource Development 🔗</div> <div>1 of 8 Techniques (13%)</div> <div>🔍</div> <div>Compromise Accounts</div> <div>Cloud Accounts</div>	<div>Initial Access 🔗</div> <div>1 of 13 Techniques (8%)</div> <div>🔍</div> <div>Valid Accounts</div> <div>Cloud Accounts</div>	<div>Execution 🔗</div> <div>0 of 36 Techniques (0%)</div>	<div>Persistence 🔗</div> <div>2 of 71 Techniques (3%)</div> <div>🔍</div> <div>Valid Accounts</div> <div>Cloud Accounts</div> <div>🔍</div> <div>Account Manipulation</div> <div>Device Registration</div>	<div>Privilege Escalation 🔗</div> <div>2 of 41 Techniques (5%)</div> <div>🔍</div> <div>Valid Accounts</div> <div>Cloud Accounts</div> <div>🔍</div> <div>Account Manipulation</div> <div>Device Registration</div>	<div>Defense Evasion 🔗</div> <div>1 of 89 Techniques (1%)</div> <div>🔍</div> <div>Valid Accounts</div> <div>Cloud Accounts</div>	<div>Credential Access 🔗</div> <div>1 of 30 Techniques (3%)</div> <div>🔍</div> <div>Multi-Factor Authentication Request Generation</div>	<div>Discovery 🔗</div> <div>1 of 33 Techniques (3%)</div> <div>🔍</div> <div>Account Discovery</div> <div>Cloud Account</div>	<div>Lateral Movement 🔗</div> <div>0 of 20 Techniques (0%)</div>
--	--	---	---	--	---	--	--	--	--

Description

This correlation computes the risk events associated with the detection analytics from "Suspicious Okta Activity", "Okta Account Takeover", and "Okta MFA Exhaustion" analytic stories. This analytic will trigger a notable event in your incident review when there are 5 or more distinct TTPs related to these analytic stories in the last 24 hours. This incident highlights potentially suspicious activity by a compromised user.

Additional Fields

Value

Risk Object

bpatel@splunk.com

Risk Object Type

user

Original Splunk Source

ESCU - Okta Authentication Failed During MFA Challenge - DM - Rule

ESCU - Okta New Device Enrolled on Account - Rule

ESCU - Okta Unauthorized Access to Application - DM - Rule

ESCU - Okta User Logins from Multiple Cities - DM - Rule

Severity

high

Annotation Framework

analytic_story

cis20

kill_chain_phases

mitre_attack

nist

Annotations

DE.AE

Installation

T1078

Okta Account Takeover

Action

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

Related Investigations

Currently not investigated.

Correlation Search

ESCU - Okta Risk Threshold Exceeded - Rule [🔗](#)

History

[View all review activity for this Notable Event](#) [🔗](#)

Adaptive Responses

Response

Mode

Time

User

Status

[Notable](#) [🔗](#)

saved

2024-05-13T21:51:21-0400

admin

🟢 success

[View Adaptive Response Invocations](#) [🔗](#)

Next Steps

📘

No next steps defined.

© 2024 SPLUNK INC.

Takeaways

- Okta serves as the **gateway** to all your applications and data, making it a **critical** point of access that must be closely monitored.
- To complete their goals, attackers often **abuse legitimate management features**.
- Leveraging **Splunk's analytics** with **Okta logs** is key to uncovering ongoing attacks and defending against **sophisticated identity threats**.



Thank you

A HUGE shout out to the AMAZING COMMUNITY
for their contributions on this topic!

- Michael Haag (Splunk)
- James Brodsky (Google)
- John Murphy, Felicity Robson, Jordan Ruocco (Okta)
- Eli Guy (XM Cyber)
- Elastic Security labs
- David French
- Nick VanGilder
- and many more!

