Identity Intelligence Demystified

Technical deep dive into CII (formerly Oort)

Aaron T Woland - CCIE #20113
Distinguished Engineer, Security
loxx@cisco.com | @aaronwoland | aaronwoland

BRKSEC-2162

$ whoami

Cisco role: Distinguished Engineer, Security

Unofficial title:
“Cisco History Professor”

Experience: Old enough to wonder how I have been doing this for >30 years

Fun fact 1: Father of 5 daughters

Fun fact 2: Oldest works for Cisco now! Youngest is 3!

Fun fact 3: Just completed Cybersecurity Master’s Degree from SANS Institute (Oct 2024)

Sarcasm

“If we can’t laugh at ourselves, Then we cannot laugh at anything at all”

Disclaimer: *“All Comments are my own, and are not representative of Cisco… Any correlation to real live persons or situations was completely unintentional… Blah Blah Blah…”*

Please fill out the survey

Drop your email in the comments – I WILL respond!

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2162

Questions?

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

How

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

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

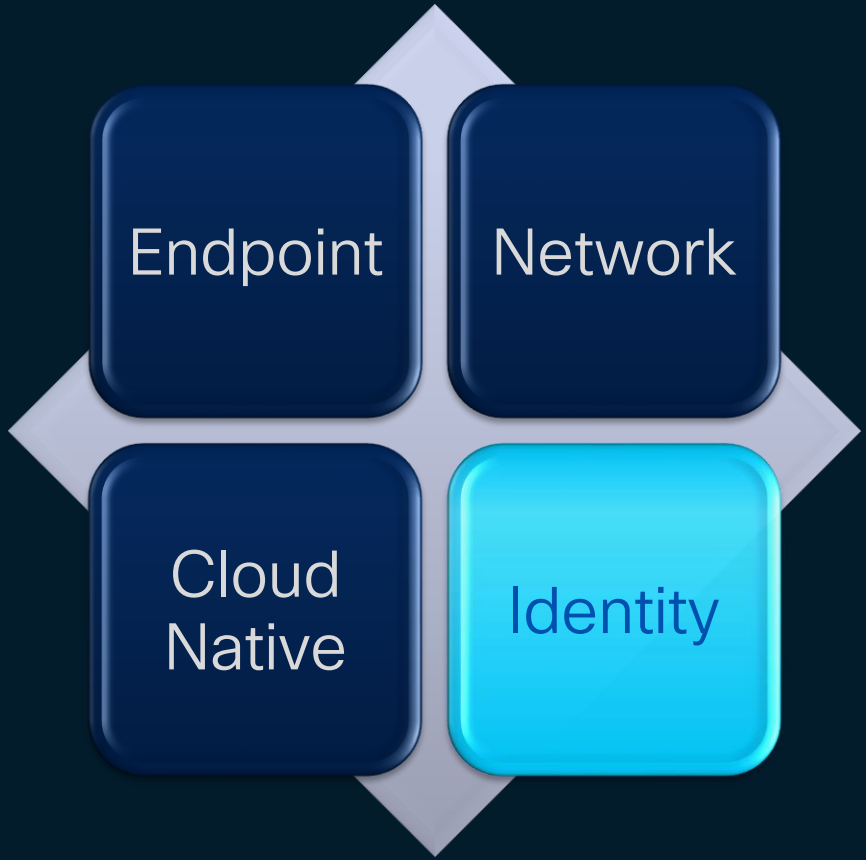
cisco Live!

Agenda

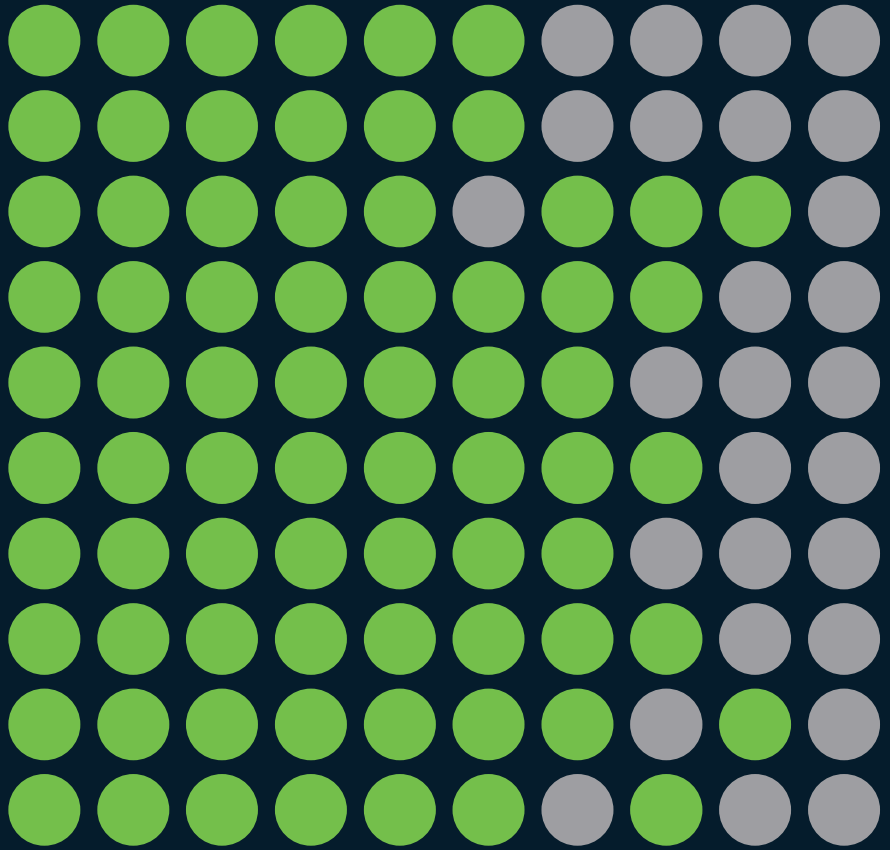
- What is Cisco Identity Intelligence
- Integrations & Users
- All about Checks
- Remediations
- Other Technical Nuggets
- User Trust Levels & Posture
- Let’s talk about APIs
- Call to Action

Prevention is not enough!

- Endpoint Detection & Response
- Network Detection & Response
- Cloud Native Detection & Response
- Identity Threat Detection & Response



Identity has become the attack surface



80%

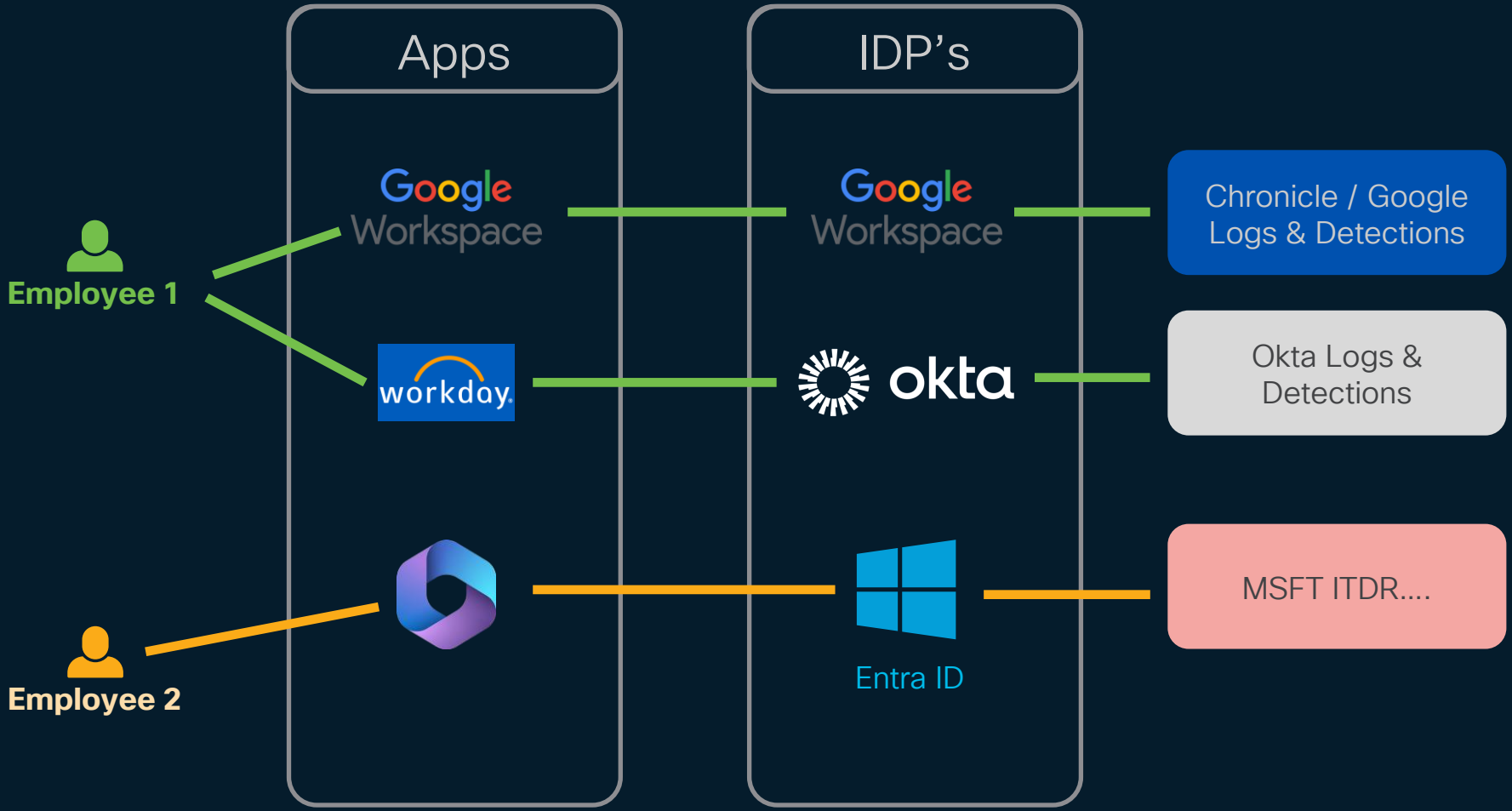
of breaches leveraged identity as a key component

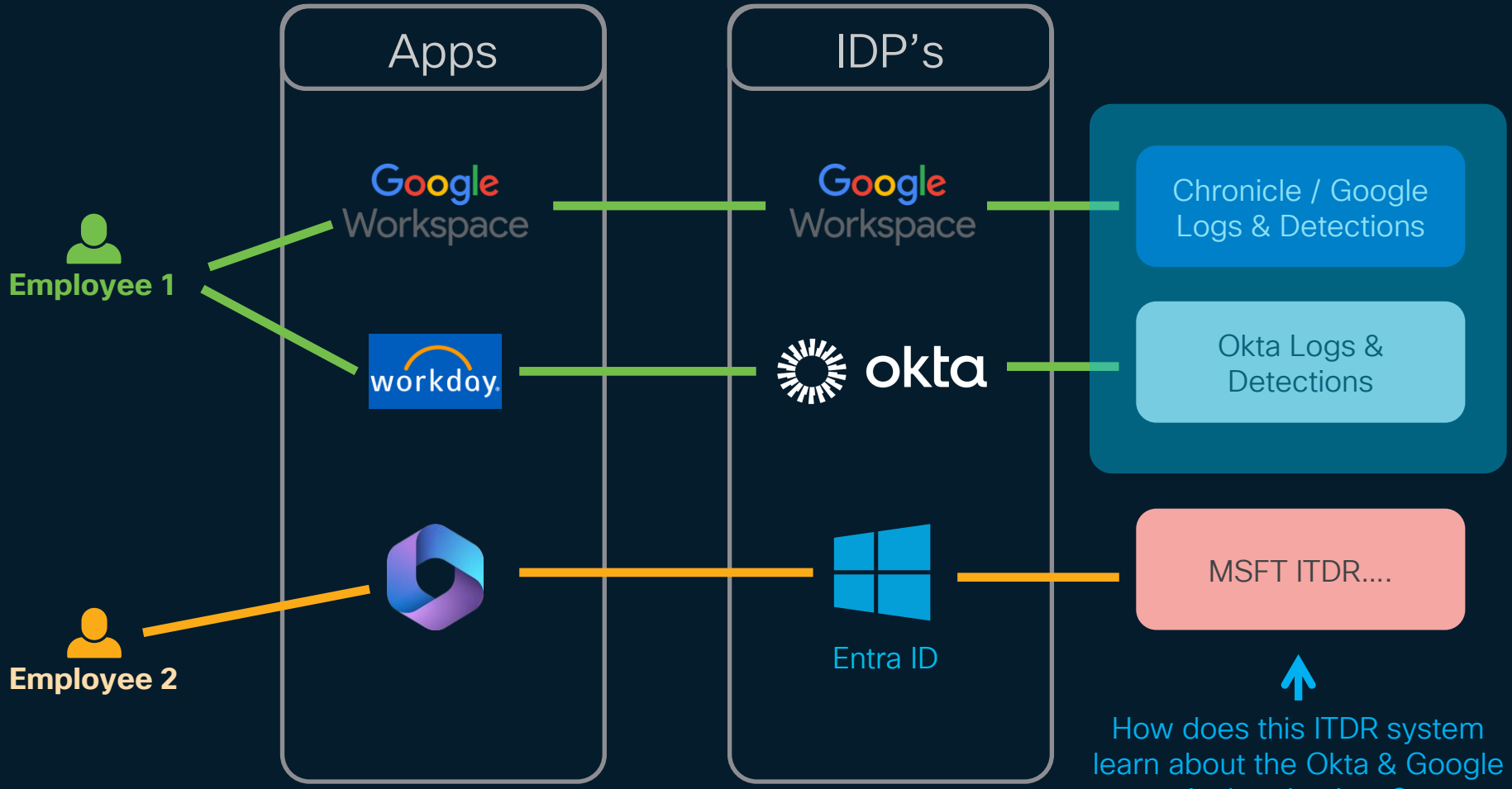
Cisco Talos Incident Response Data 2023-2024

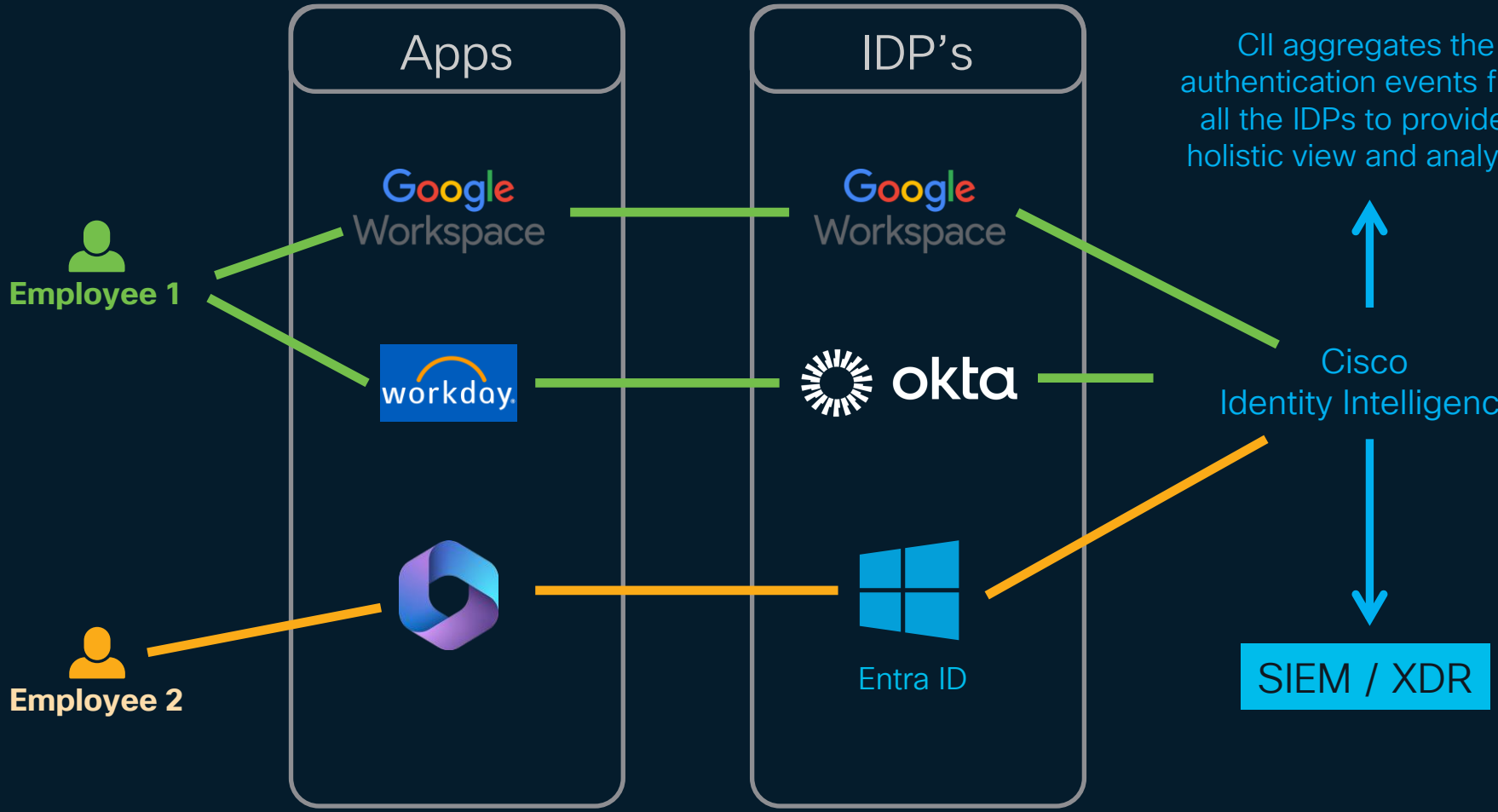
Breaches Occur: Fatigue with MFA “Nag”

Credit: Wizer Security
https://www.wizer-training.com

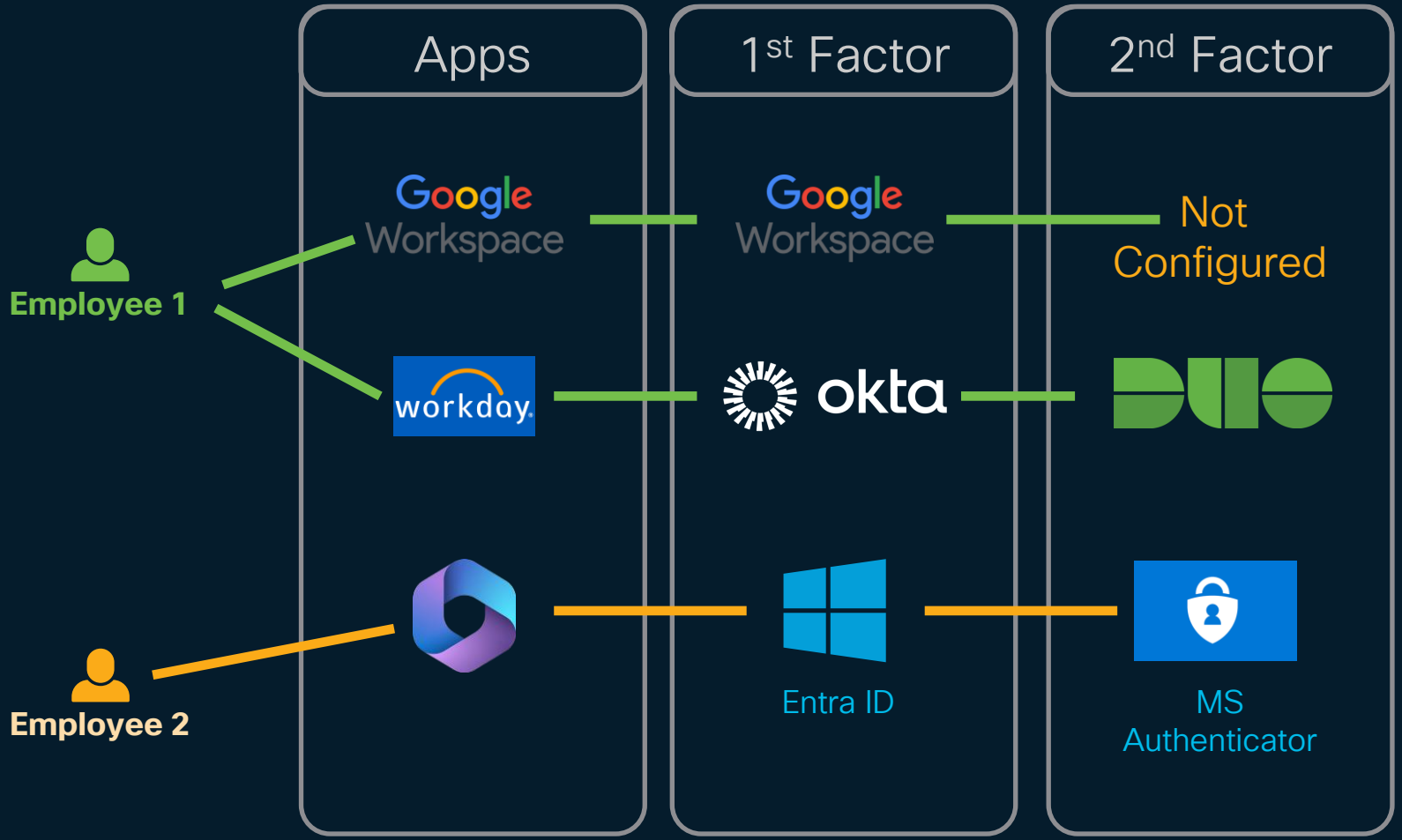
You cannot detect what you cannot see!







Are you sure that strong MFA is configured everywhere?



We see

Environments

Like This

All the Time

Cisco Identity Intelligence


Users


Machines


Services


Apps


Data


Behaviors

Auth0

Workday

Okta

GitHub

Salesforce

Microsoft

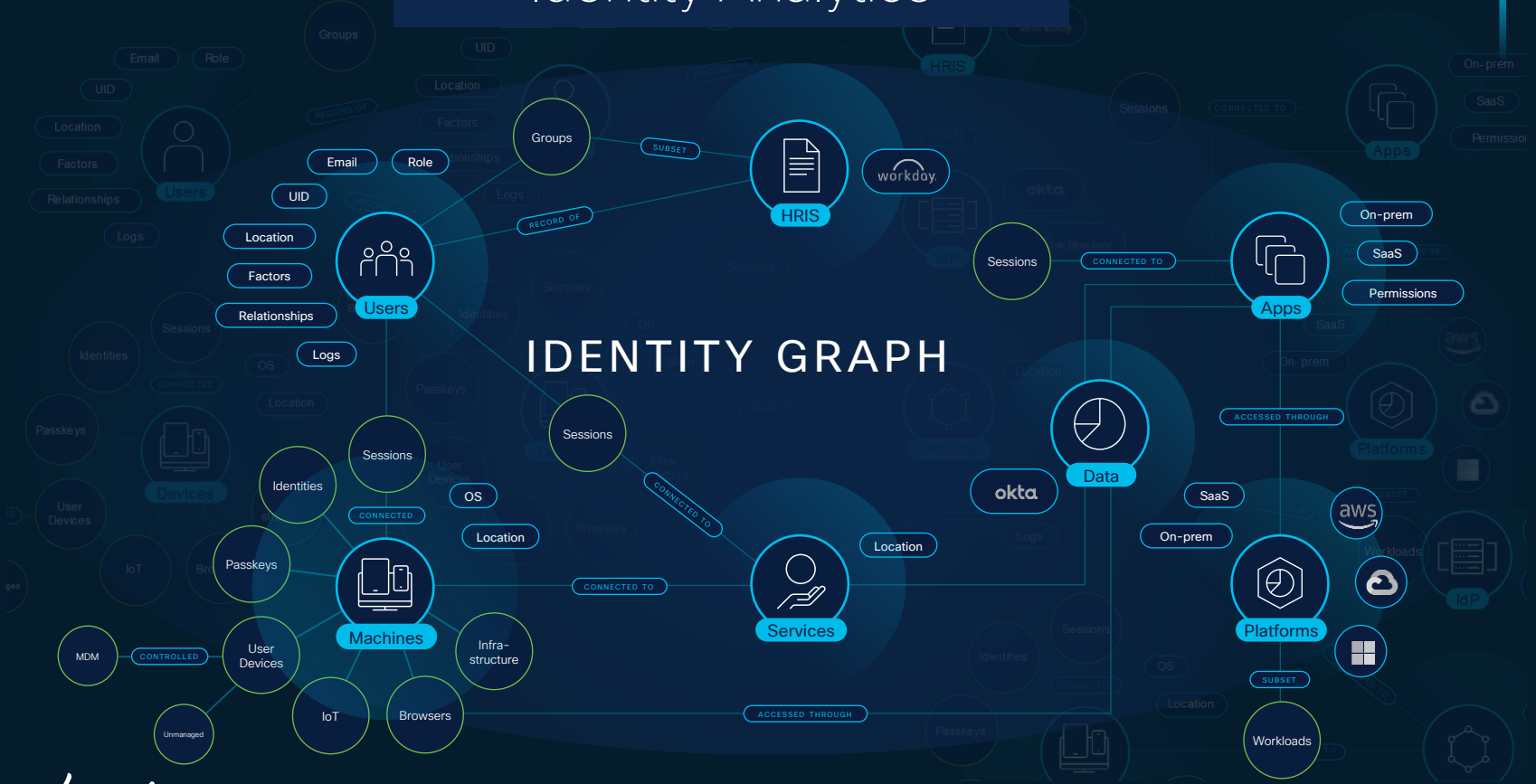
cisco

Google

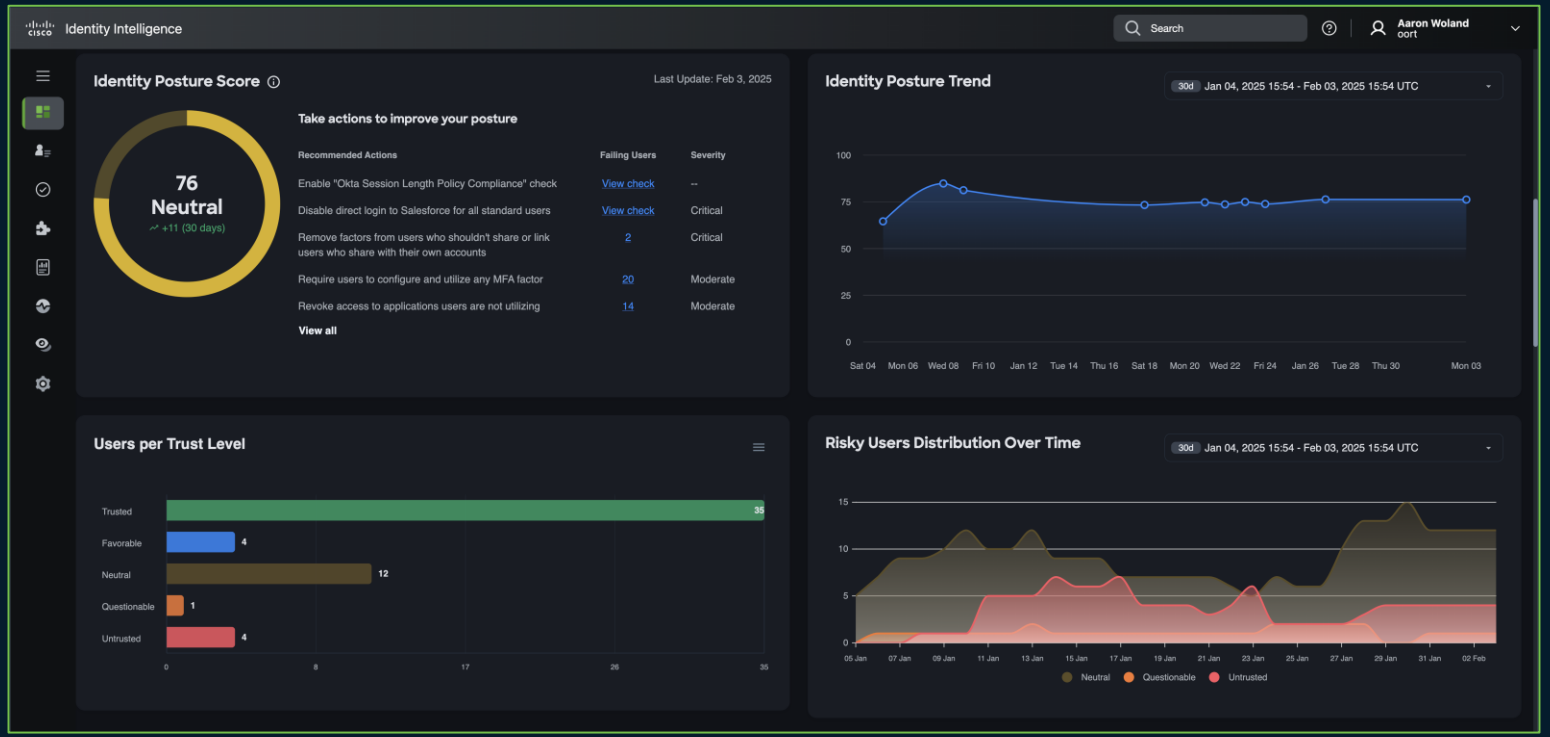
Amazon

cisco Live!

Identity Analytics

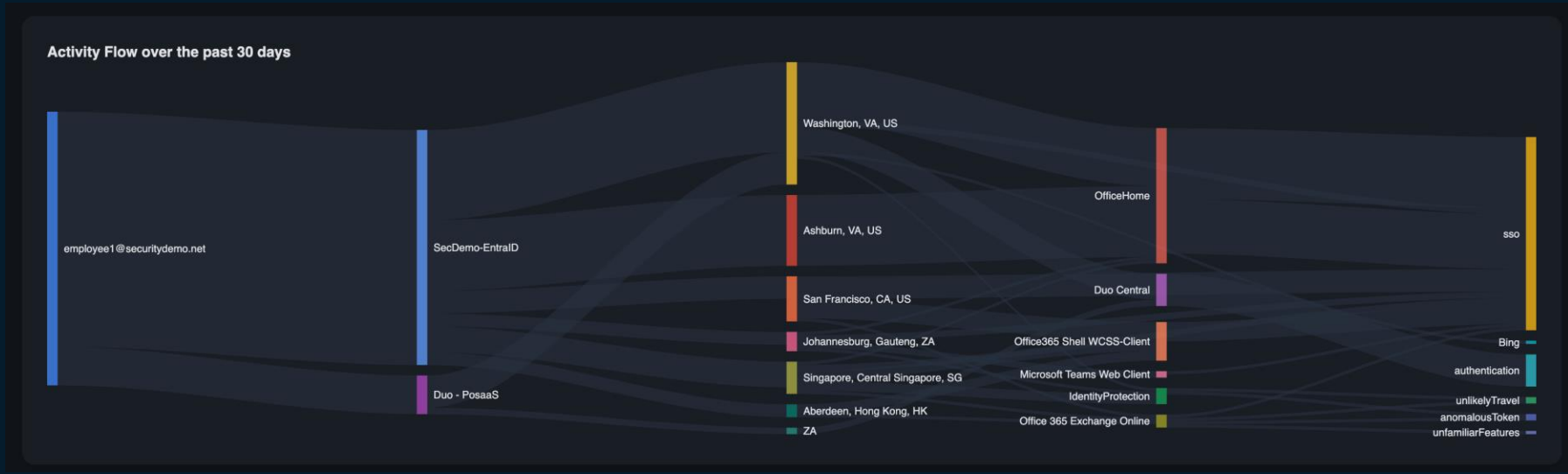


Provides information like this!



And this: Real life example of detection

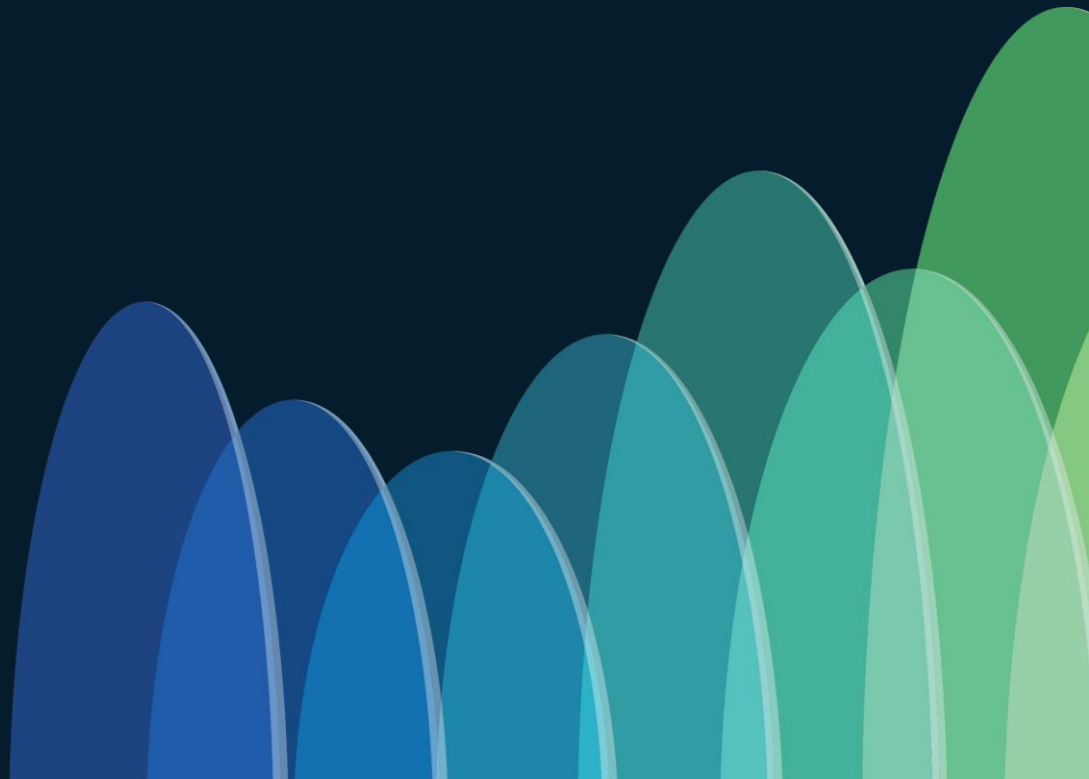
Identity graph - Threat analysis based on probed account



Agenda

- What is Cisco Identity Intelligence
- Integrations & Users
- All about Checks
- Remediations
- Other Technical Nuggets
- User Trust Levels & Posture
- Let’s talk about APIs
- Call to Action

Integrations Overview



cisco Live!

Integrations are the life's blood of CII

Identity Providers

CII integrates w/ many key (cloud-based) ID sources already.

These integrations are complex in nature.

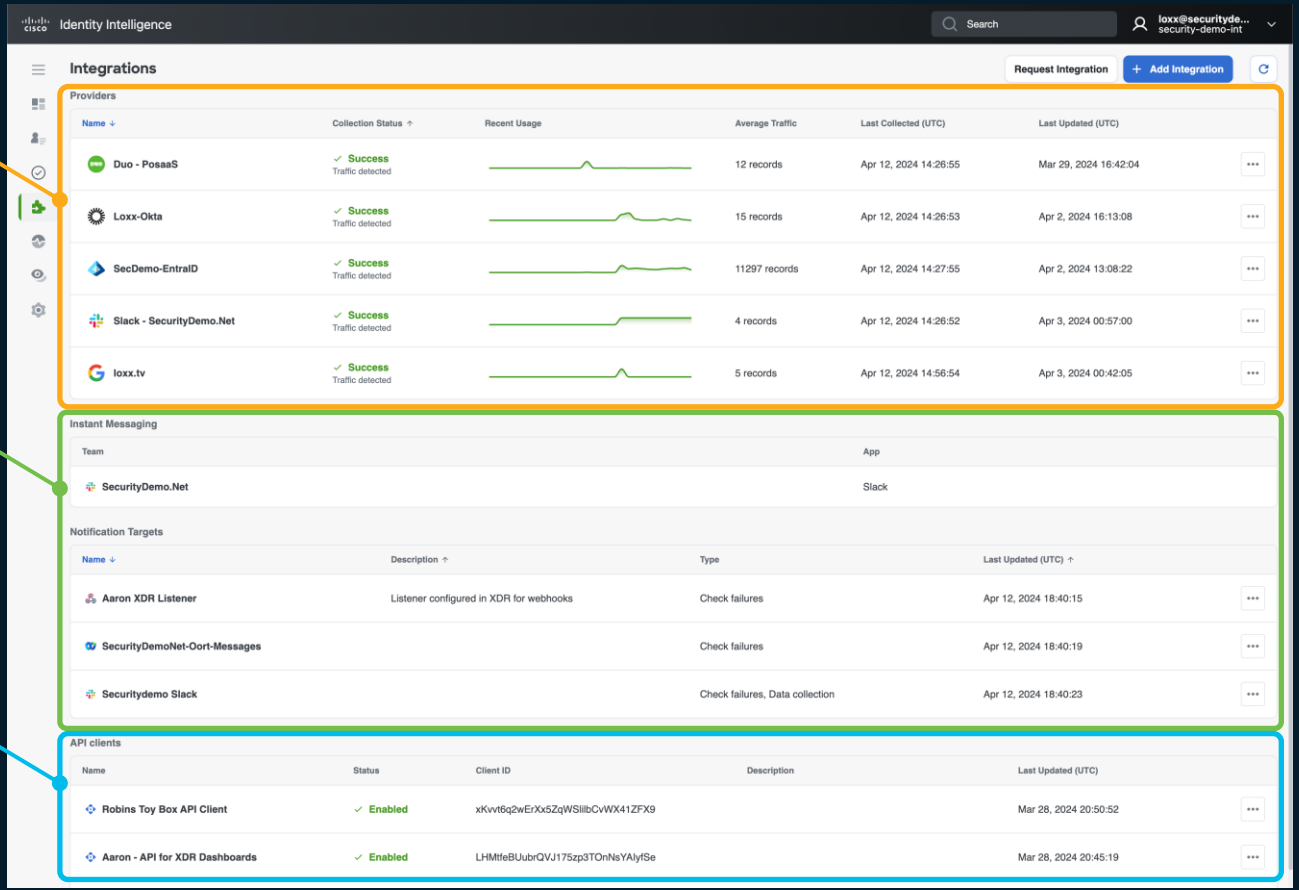
IM & Notification

Operational alerts and failed checks send to these integration targets.

Support of webhook destinations offers a standard interface for integrating CII to other systems.

API Clients

These are the client credentials for the public GraphQL API to query CII for information



Integrations are “Life’s blood” for CII

- Identity Intelligence is not an inline product
  - All CII’s information comes from integrations
  - CII integrates with Identity Providers, HRIS Systems and Applications
- Building the meta-directory of Users, Groups and Directory Structures
  - Uses APIs and Events
- Identifying Who is accessing What, from where and with which devices:
  - Authentication logs which can come across API syncs, or (preferably) streaming events
- Notifying users, administrators and investigators
  - CII integrates to send notices to email, collaboration tools, and SIEMs
- Some integrations are multi-purpose:
  - Slack is an IDP & a Notification System
  - Entra ID is required before you can add MS Teams as an integration source

Data collection methods

- Identity Intelligence utilizes native REST APIs of all supported sources
  - Full inventory sync – an API call to the source which results in the download of the full user database of this source. Such calls are executed on the initial sync and later over long enough intervals to avoid exhausting the API subsystem of the source.
  - Delta sync – when possible, uses API calls that return only changed information. Timestamps like 'last updated' are used to identify what has been changed after the last full or delta sync.
  - Streaming – the most desired way of getting data! May use AWS EventBridge, or Azure Event Hub & the providers will send all notifications to CII in near-real-time based on the events we are subscribed to.
    - Streaming is always preferred. API's have rate limits and throttles.

Identity sources and their methods

Identity Sources	Streaming	REST API Full Sync	REST API Delta Sync
Duo Security by Cisco	✓	✓	✓
Microsoft Entra (aka: Azure)	✓	✓	✓
Okta	✓	✓	✓
Slack[1]	X	✓	✓
Github	X	✓	✓
AWS	X	✓	✓
Google Workspace	X	✓	✓
Workday	X	✓	X
Salesforce	X	✓	partial
Auth0 (acquired by Okta)	✓	✓	X
Manual Upload (CSV/JSON)	X	X	X

[1] listed as notification, but also an identity source

Wait... Why not just use the IDP?

- Okta, Microsoft – they all claim to provide ID security!
  - But they can only detect what they see!
  - Most organizations have multiple IDPs, correlation is very difficult
- CII brings together the info!
  - All factors together in one analytical system
  - Greatly reduces the noise from the IDPs
  - Reducing false-positives
  - Proactive & Reactive Security
  - Work closely with Okta, MSFT & Duo to develop features together

"CII gets great insights from Entra, and I cannot believe how bad Entra is at using their own alerts"
- Fortune 100 Manufacturing Co

"I cannot believe how quickly we were able to find out about this attempted login from this unusual location"

Was a passed login w/ a failed MFA from Puerto Rico – related to someone whose account was breached, and they spent countless hours hunting that same thing in MSFT's portal.

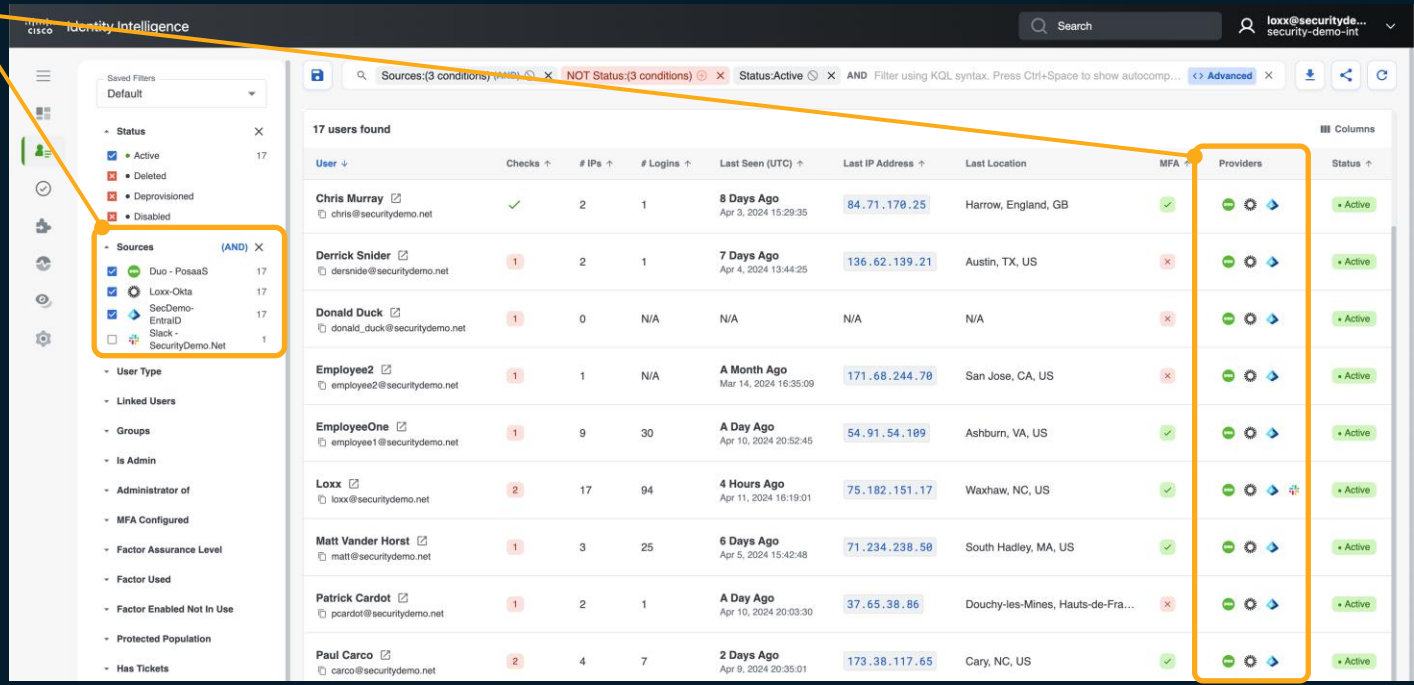
- Large MSP Business

Merged view of users – combined from all sources

Merged Users

The user inventory is built out based on the users from each provider.
When the user is the same across multiple providers, those users are merged for a combined view.

Usually see a 20-30% difference between what an organization *thinks* they have vs. what they *actually* have.



Users

User 360 View

The user details is known as the “user 360 view”

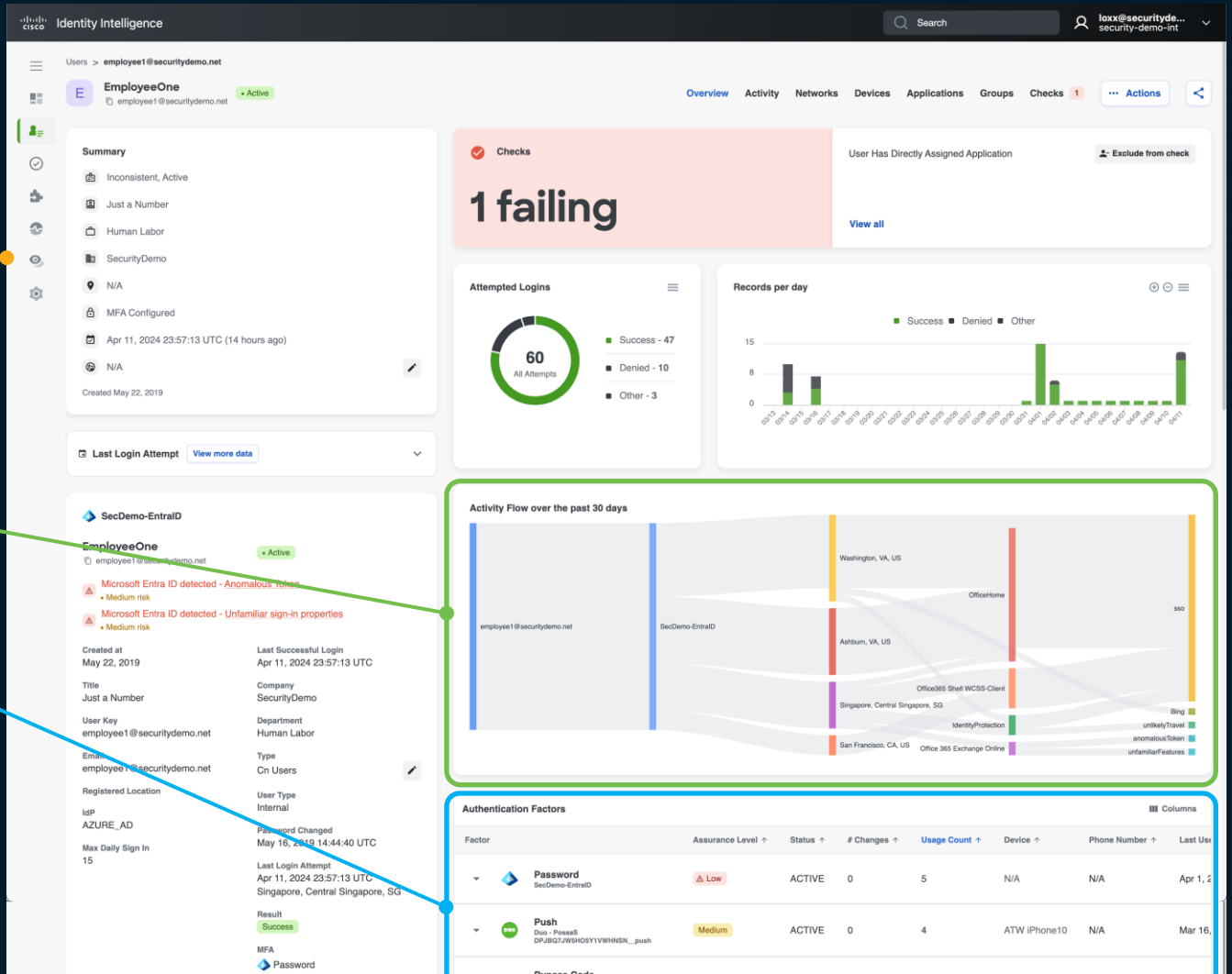
A true look at the user’s identity related security, activity and other important properties.

Activity Flow

Combined view of the user's activity patterns. Easily spot when deviations have occurred

Combined Auth Log

Combined view of the users authentications and factors across all the integrated IdPs



cisco Live!

Activity

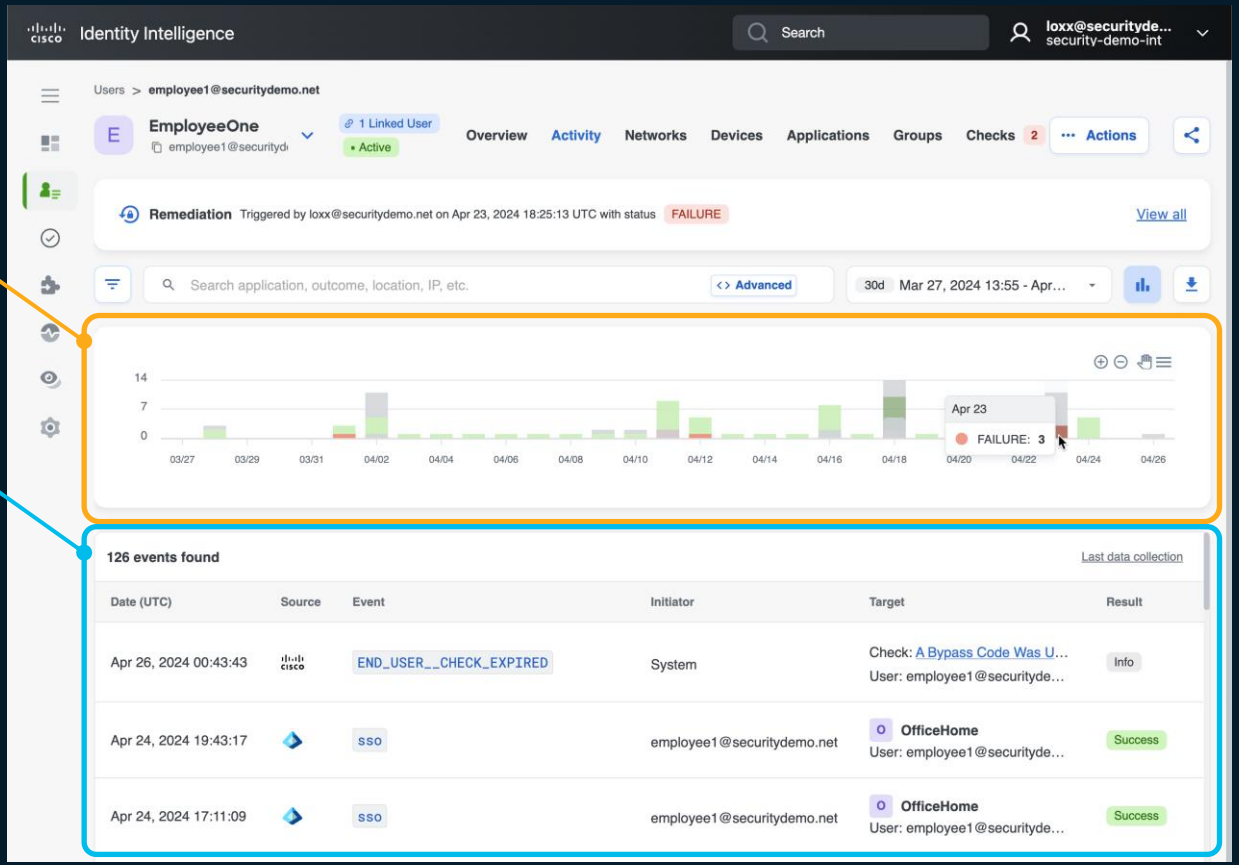
Activity Timeline

See the authentication trends across the timeline.

Zoom in & out.

Activity List

See the login activity, and click in for progressive-disclosure all the way to the detailed raw-logs



Networks

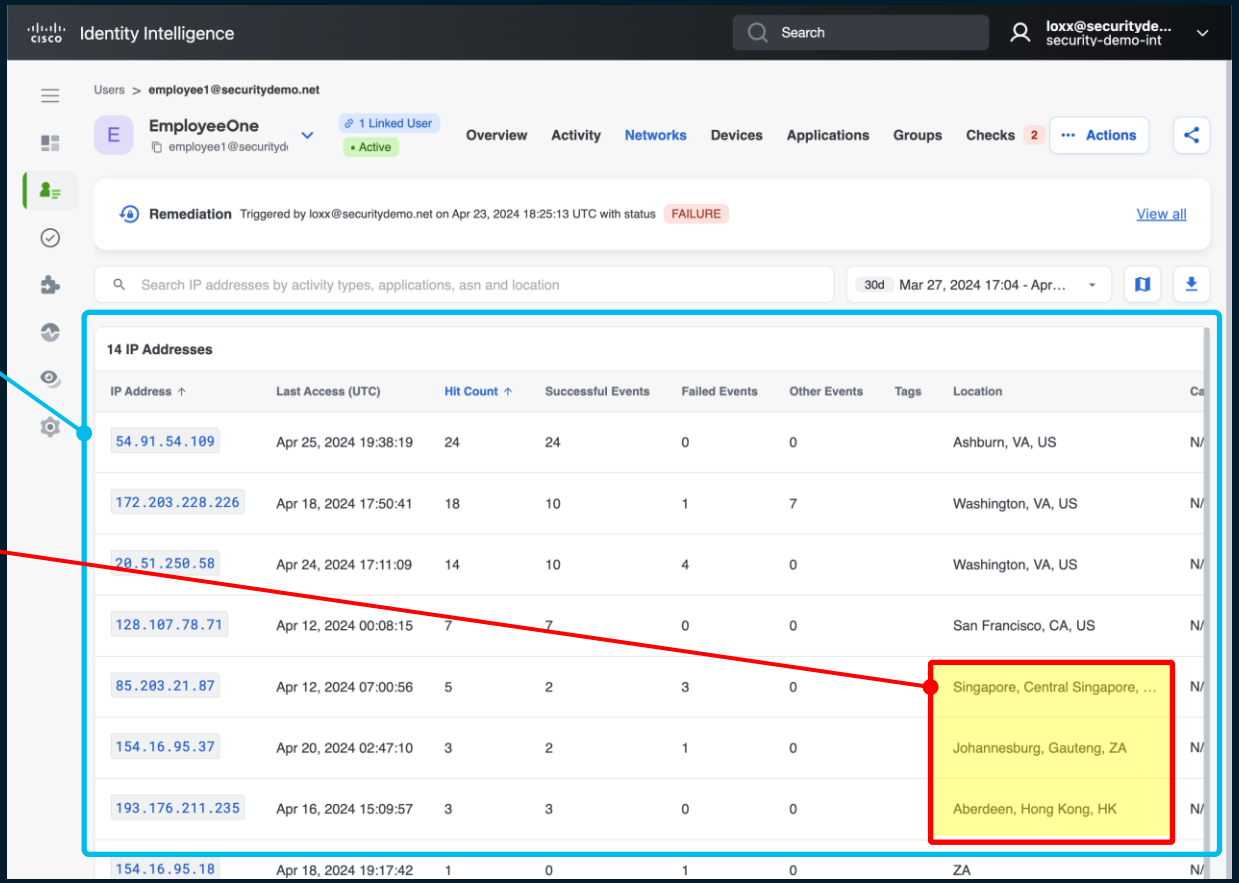
IP's recorded in IDP Logs

These are not the "internal IP's". These are the source IP's when the user-agent communicated to the IDP during auth flow

Locations

Do these seem normal for the user?

Is this suspicious?



Devices

Devices from IDPs

Not all IDPs are created equal with device information

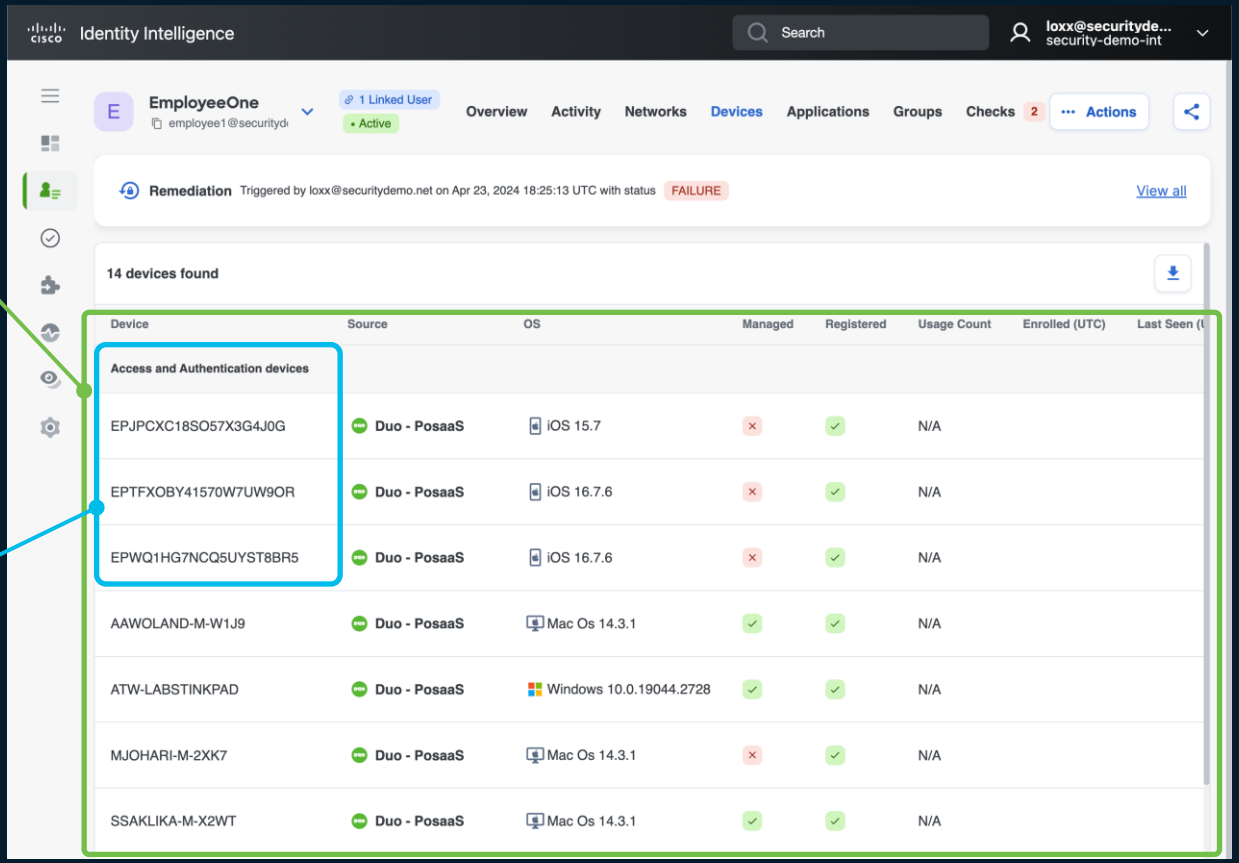
Duo is the best source for device data – when the Duo Auth includes the Health App.

Standard IDP would only see the user-agent string, no real device information.

List includes MFA devices and access devices.

Device starts with “EP”

These are the Duo Epkeys, a secure-cookie used to identify a user+device pair.



Applications

Usage Statistics

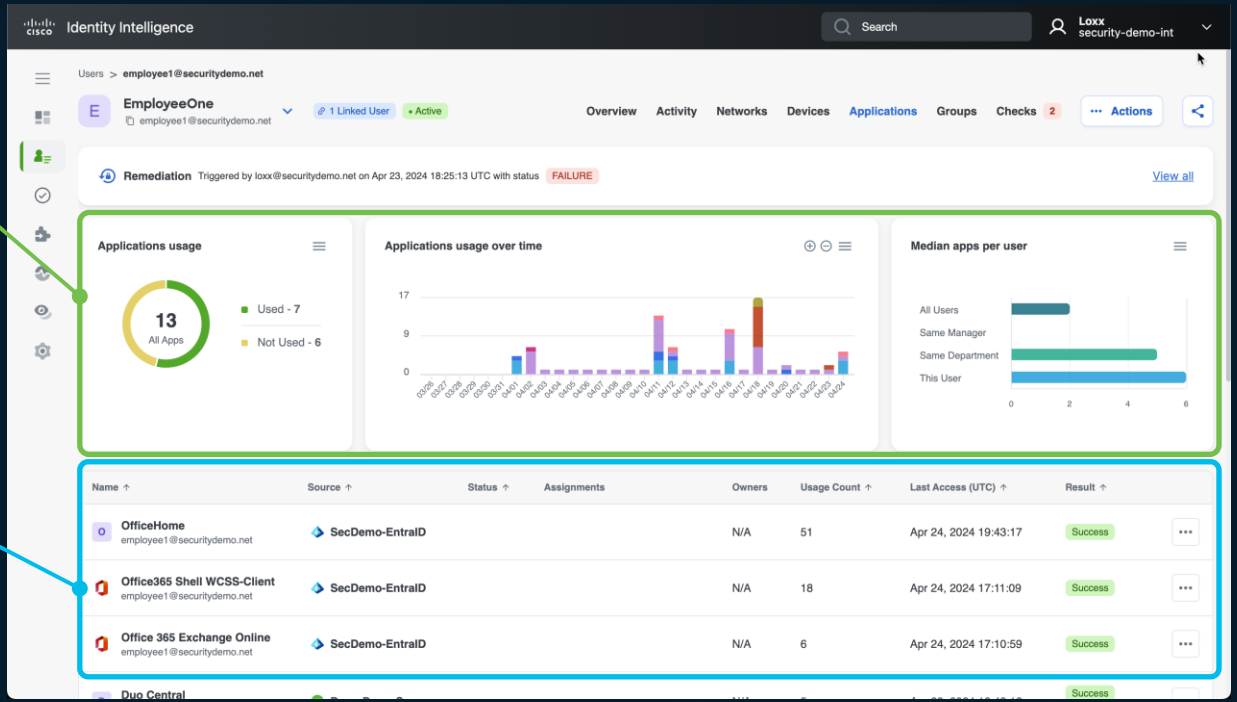
Quick overview of the apps used

Includes Apps not used

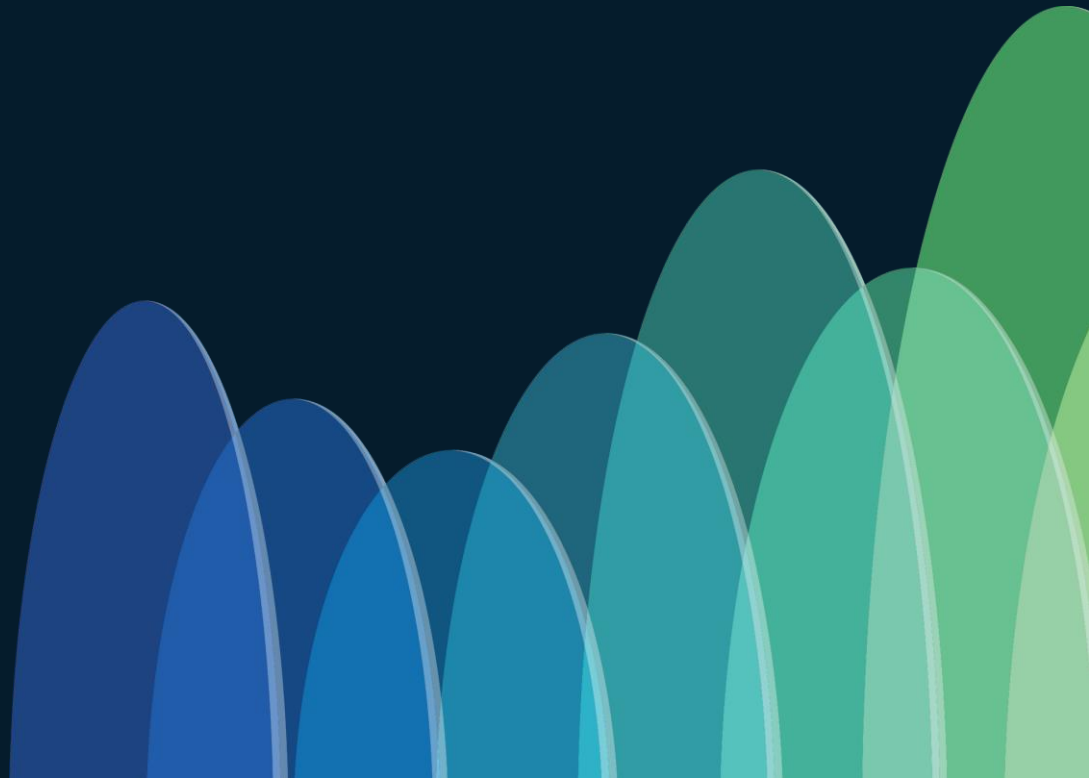
Application List

Which applications is the user accessing (according to the IDPs).

Which IDP reported the access & usage counts.



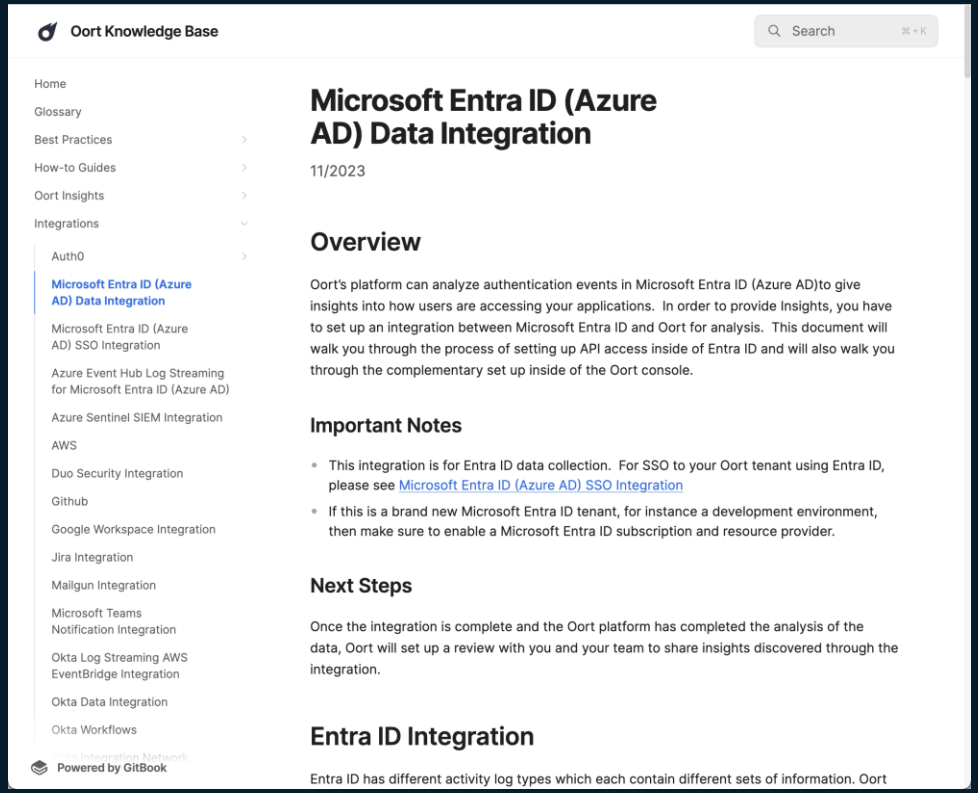
Integrations Deep Dive



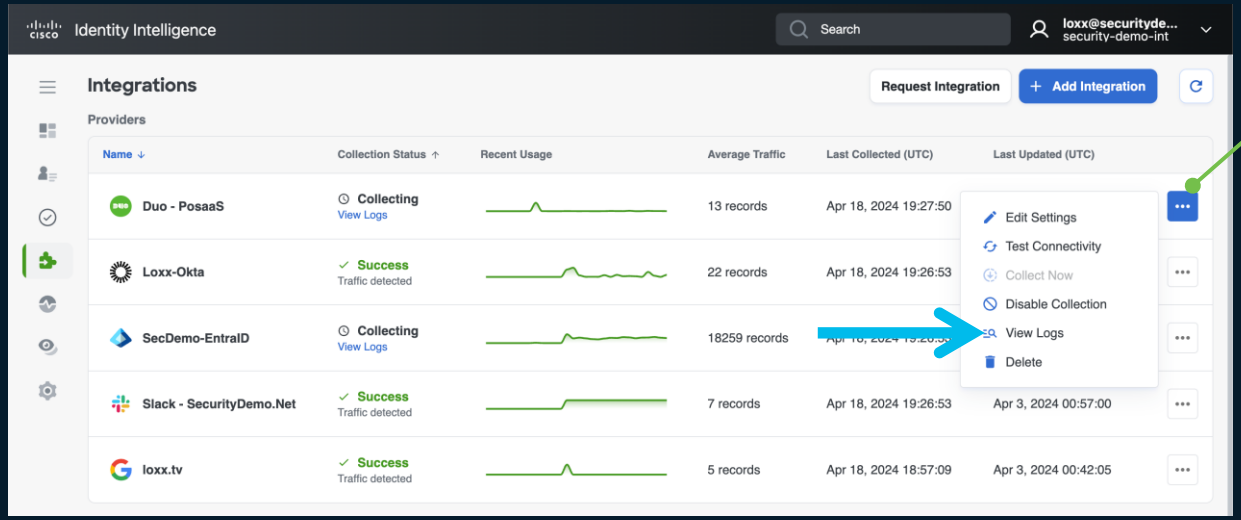
cisco Live!

Excellent Documentation

- All integrations have a detailed guide to go along with them
  - They will have links to the 3rd party vendors pages for specific sections of the integration
  - Keeps the CII documentation up to date, and puts the ownness of that portion on the vendor directly



View Logs



Ellipses (...)

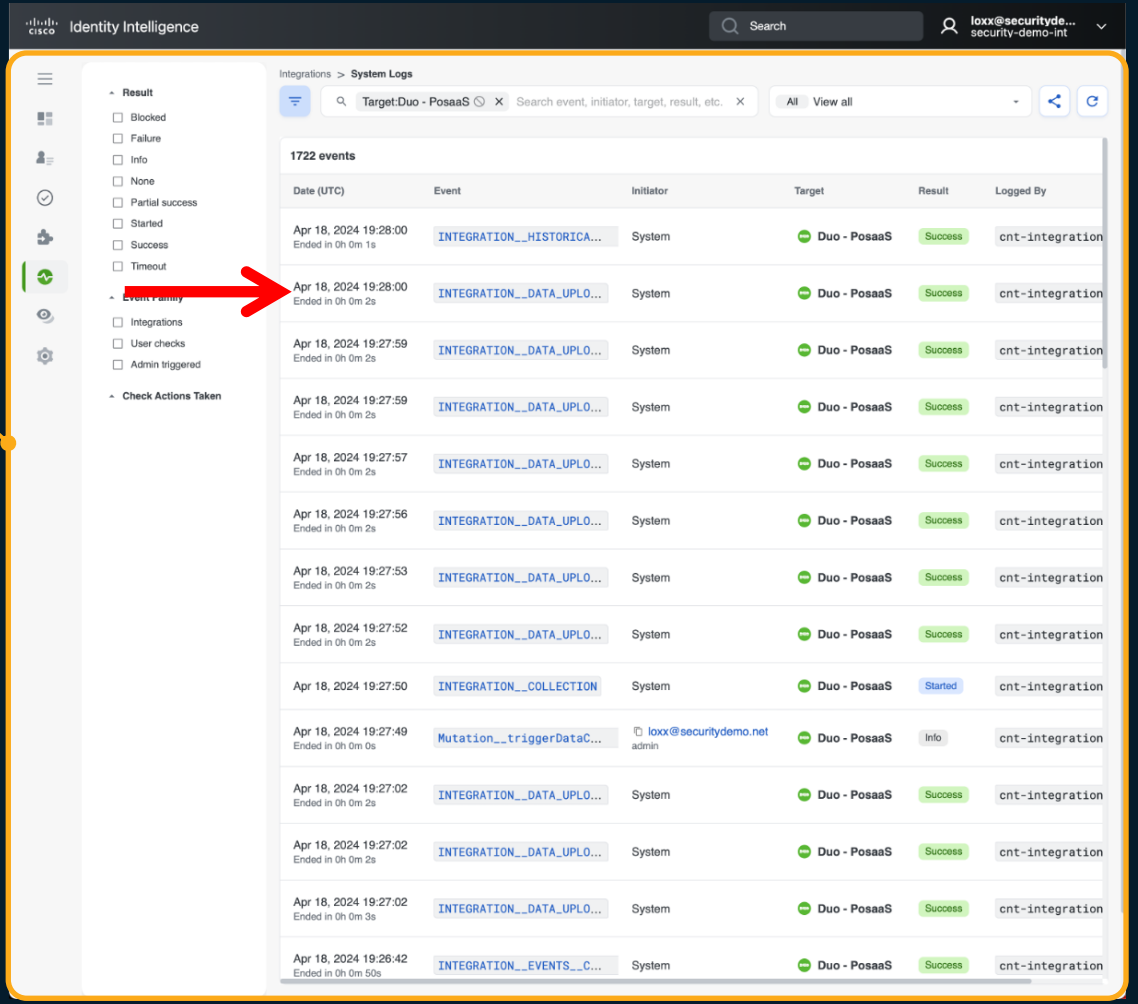
- Edit Settings
- Test connectivity – Terrific way to ensure the connection is working as expected
- Trigger collection (sync)
- Disable collection - use when there is an issue, and then enable again after that issue is resolved
- View Logs – see all logs related to the specific integration.
- Delete

View Logs

Integration Logs

Built into the UI, it will automatically filter and display all logs related to the integration, its syncs and any other related information.

You can click in & leverage progressive disclosure to view the raw log, too.



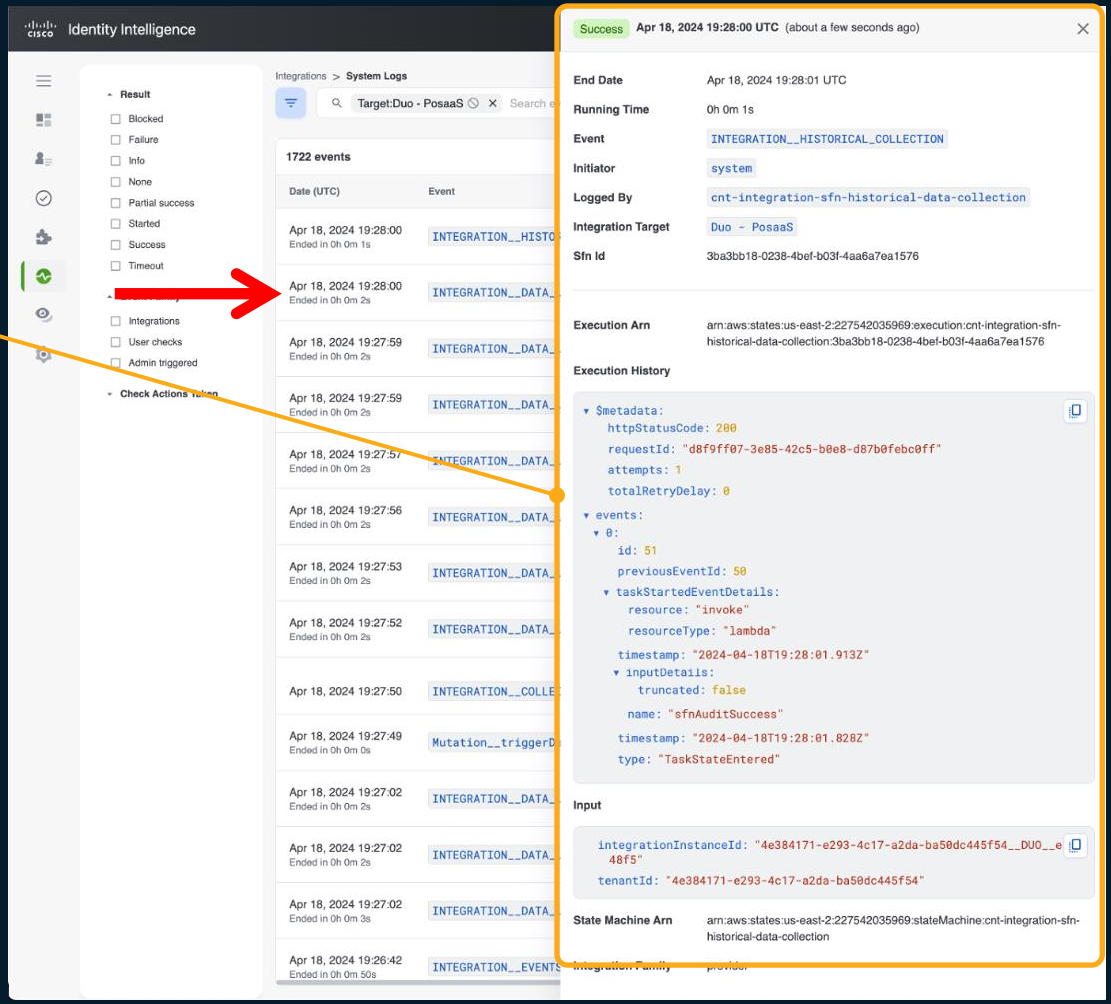
View Logs

Integration Logs

Built into the UI, it will automatically filter and display all logs related to the integration, its syncs and any other related information.

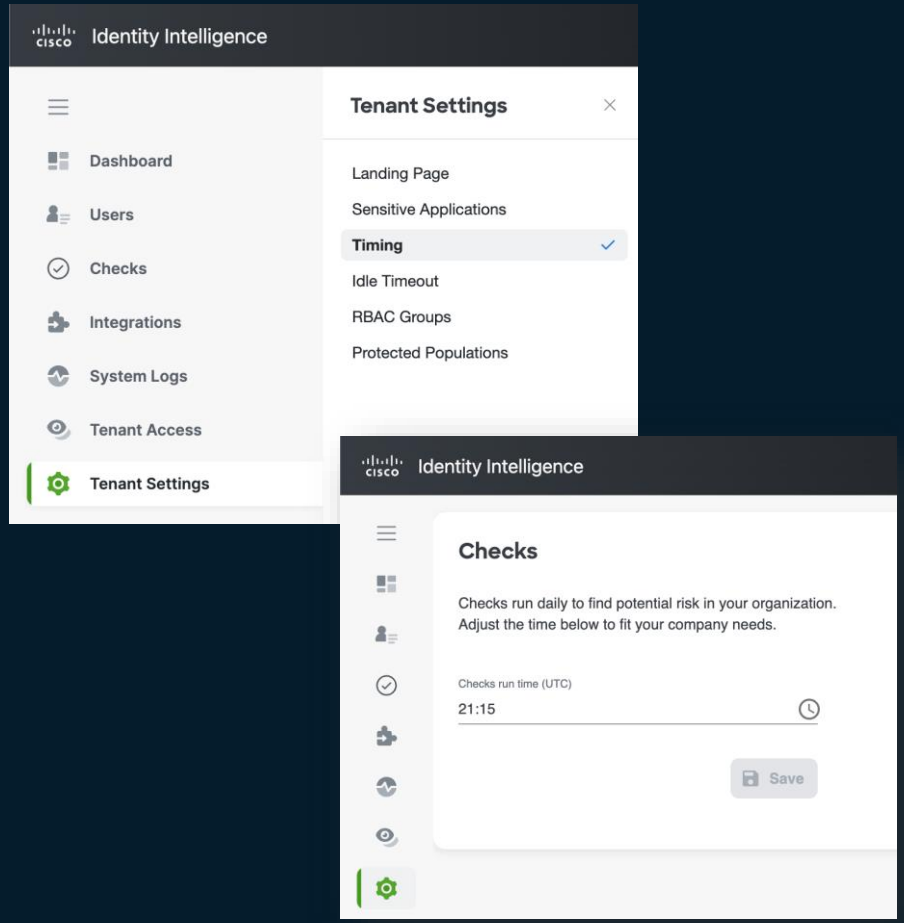
You can click in & leverage progressive disclosure to view the raw log, too.

Aids tremendously when troubleshooting why information isn't getting sync'd across.



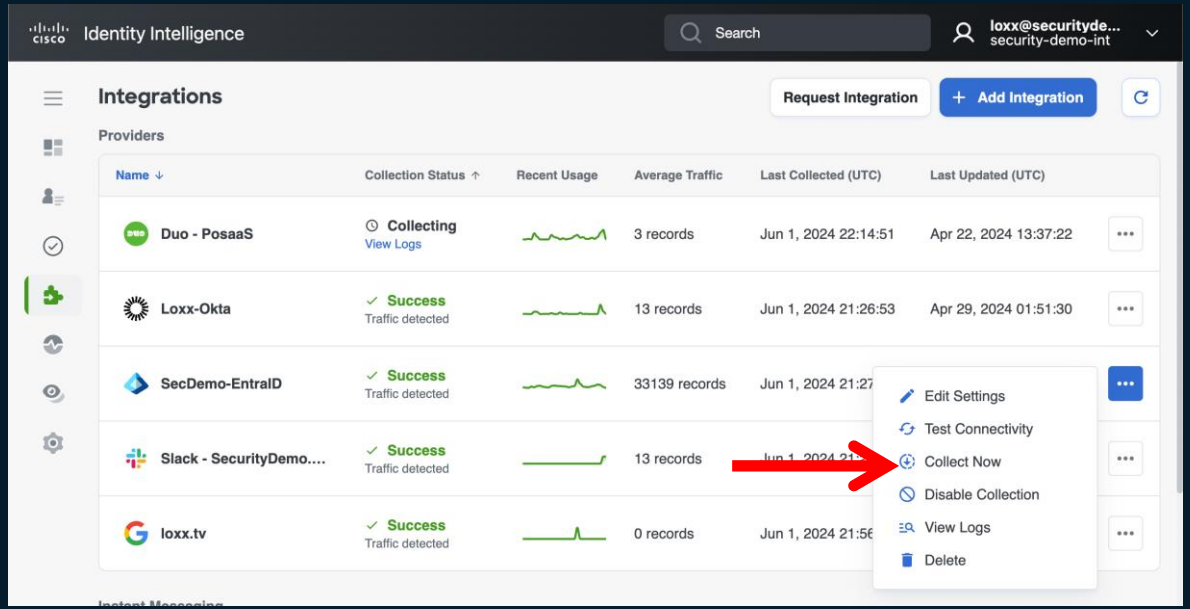
Sync Schedule

- Tenant-level configuration
  - The time of day when the bulk sync requests are made via API's
  - The time is chosen by the system automatically after the first integration is added
  - If a different time is preferred for your organization, you may change it here
  - Note: This does not affect the streaming logs (Okta, EntraID, Duo & Auth0)



Sync Schedule

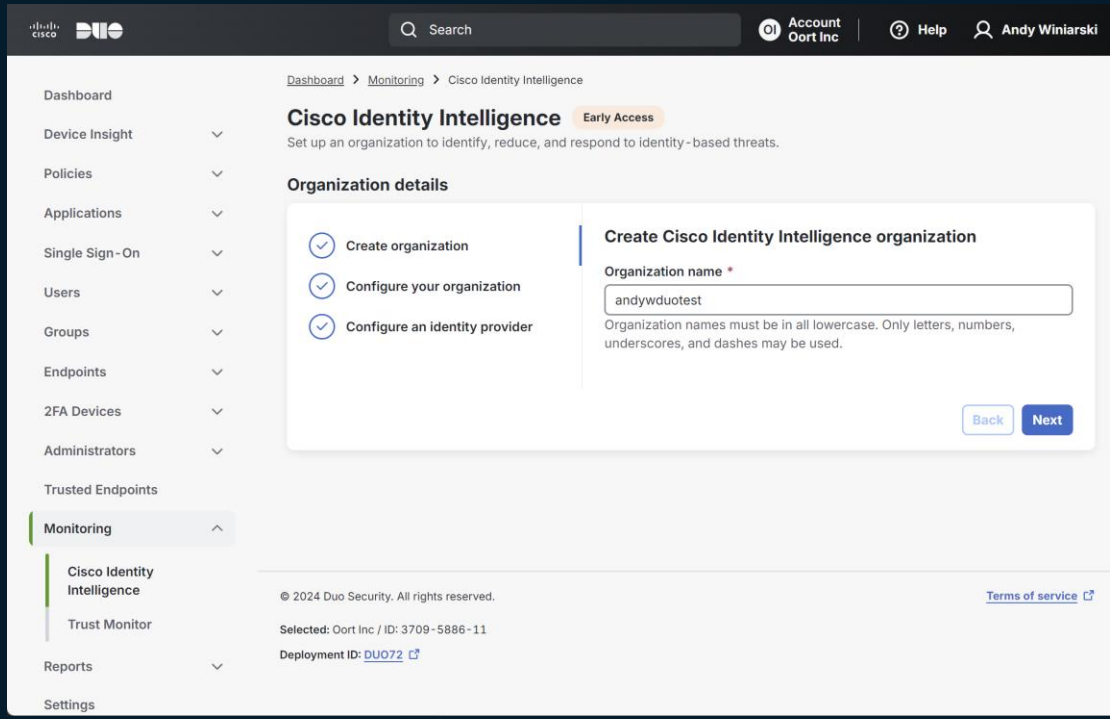
- Manually Collect on Demand
  - Also triggers a detection run when the collection is completed



Duo
a Cisco Company

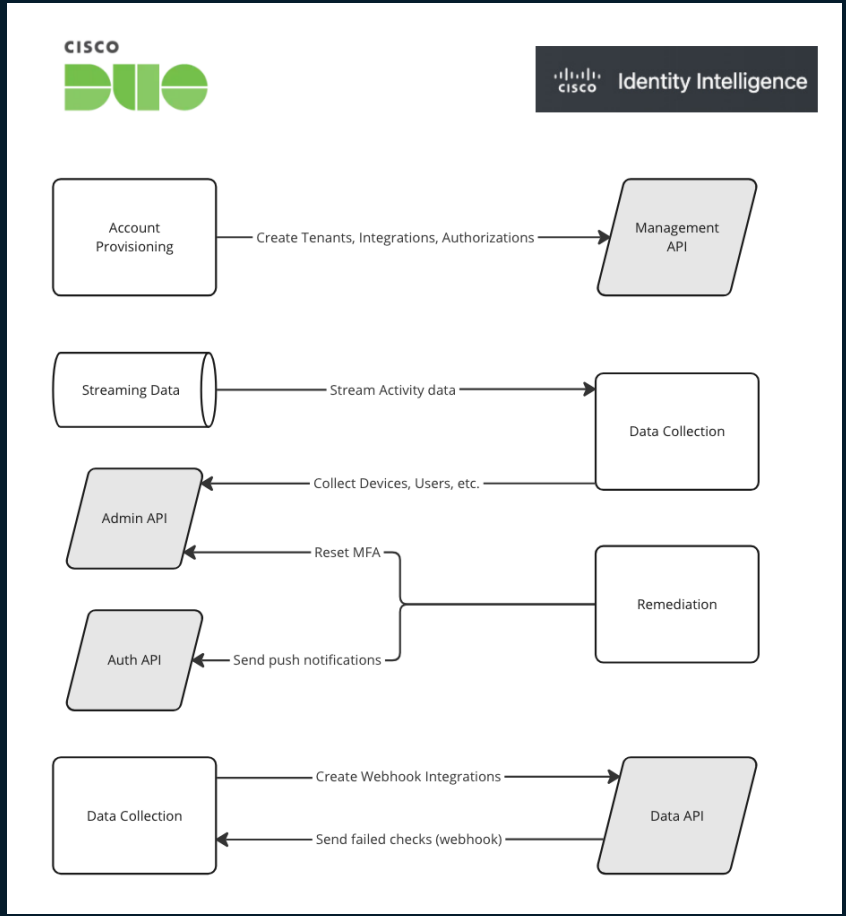
Duo <> CII Integration

- 3-step wizard to create and configure your CII tenant
  - Automatically integrates Duo data
  - Duo SSO setup or 3rd party SSO via OIDC
- Can use same wizard to setup an OIDC login w/ a 3rd party IDP
  - i.e.: MSFT Entra
- All new CII trials flow through the Duo/CII tenant provisioning



Duo Integration Details

- Three Duo API's in use:
  - Admin API
  - Auth API
  - Streaming API (new, non-public)
- Identity Intelligence
  - Management API (non-public)
  - Public API
  - Webhook notifications

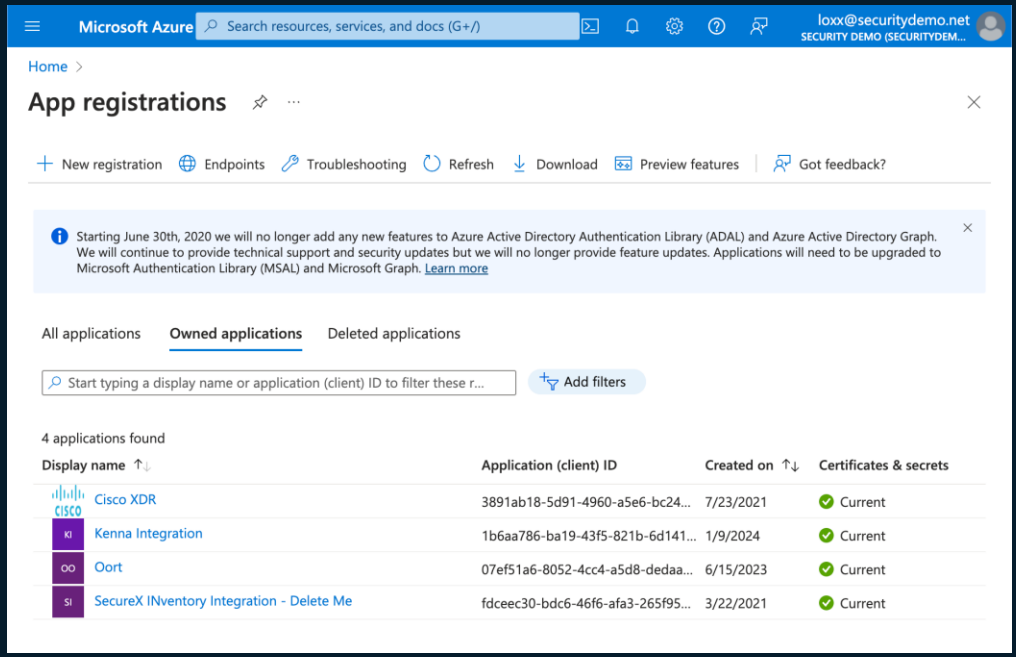


Microsoft Entra ID

Aka: Azure Active Directory (AAD)

MS Entra ID

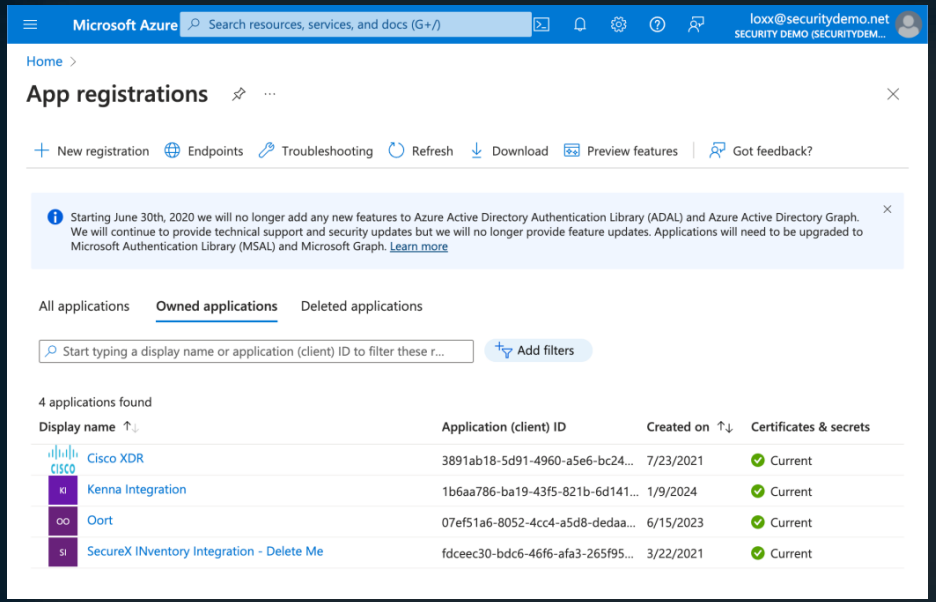
- All integrations w/ Azure go through an “App registration”
  - That’s where you configure & get the API keys
  - The “app” is given explicit or delegated permissions to a very granular set of controls / API



MS Entra ID

- Copies the directory data via the Graph API
- CII requires specific permissions
- Should setup event streaming for optimal integration
  - Customer needs to pay for a *subscription* for streamed events

Name	Remediation Type
`User.ReadWrite.All, User.ManageIdentities.All, Directory.ReadWrite.All`	Update User Type, Delete Guest User
`User.ReadWrite.All, Directory.ReadWrite.All`	User Log out
`UserAuthenticationMethod.ReadWrite.All`	Reset MFA
`User.ReadWrite.All`	Delete Guest User



MS Entra ID

General Settings

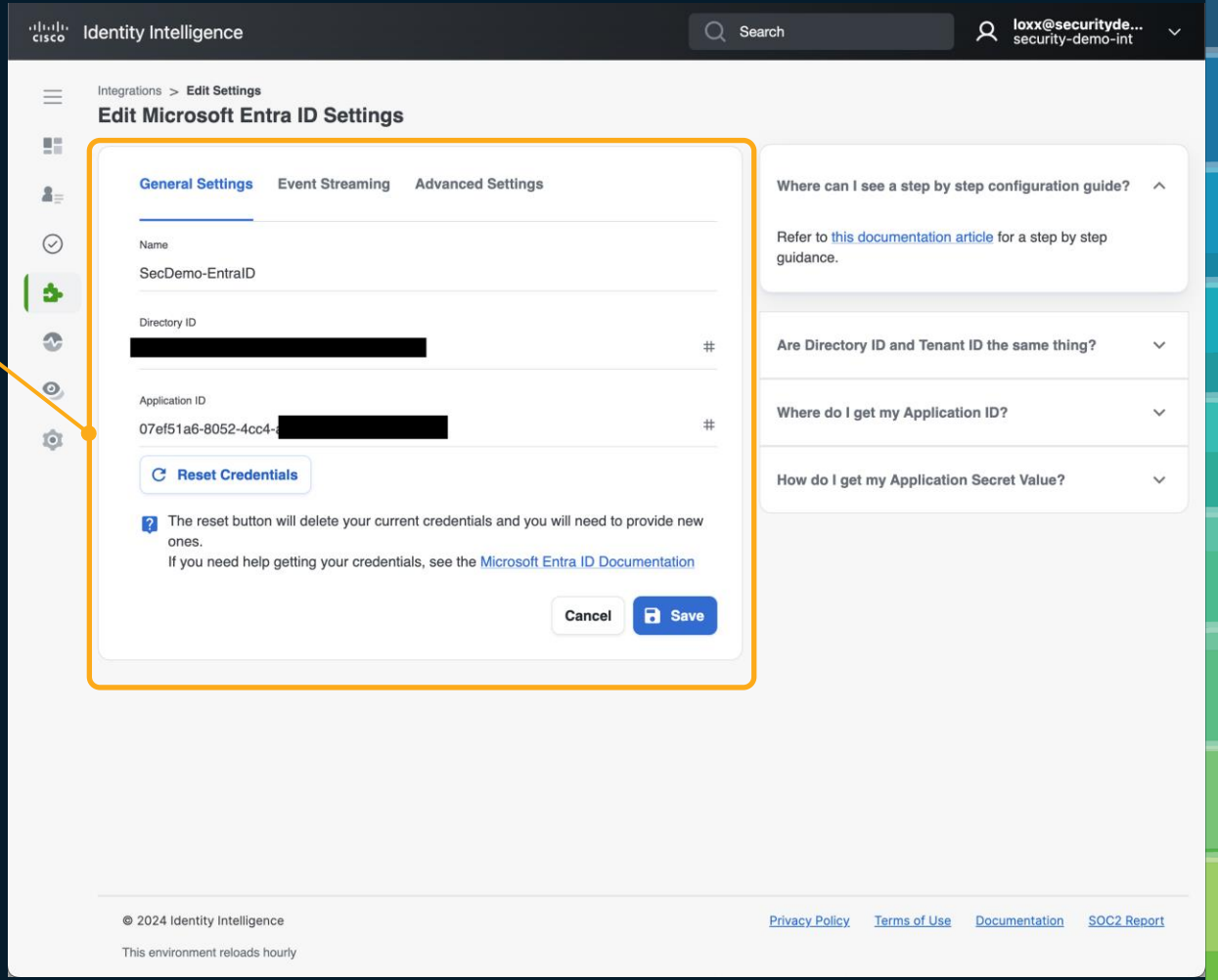
The credentials you obtained from the Azure “App” (ClientID, Secret Key, etc.)

The directory structure and attributes will be sync’d across this connection. However:

Microsoft’s Graph API is throttled extensively

CII will [sometimes] see a 429 error code or network timeouts

It is less-than-desirable to integrate with Azure only via the Graph API



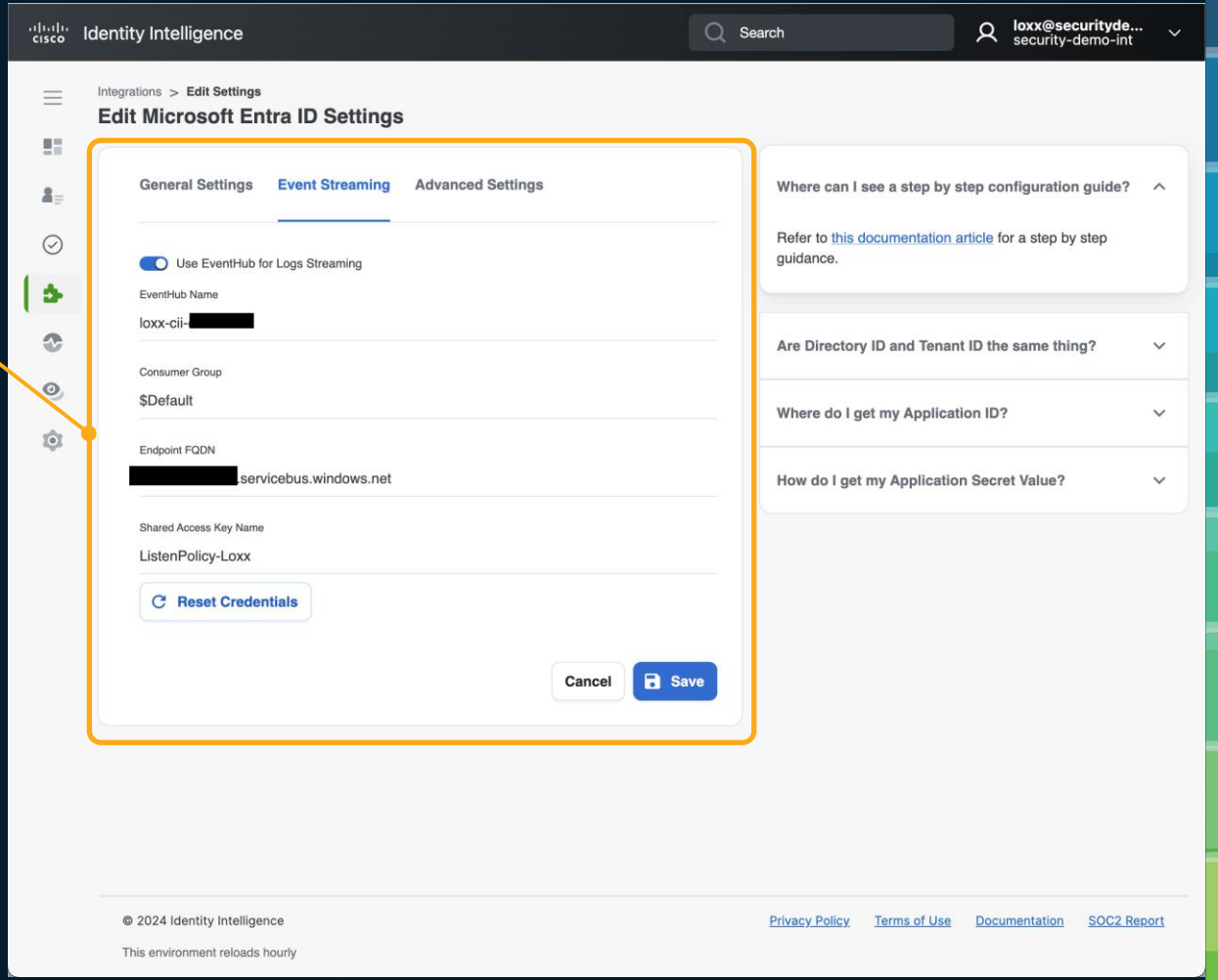
MS Entra ID

Event Streaming

Here you add the Event Hub that you created in Azure, to stream the events to CII.

It is not a true stream like Event Bridge in AWS offers, but it's close.

Event Hub will collect the events that CII has subscribed to & CII will pull those events on a schedule (15 minute intervals)

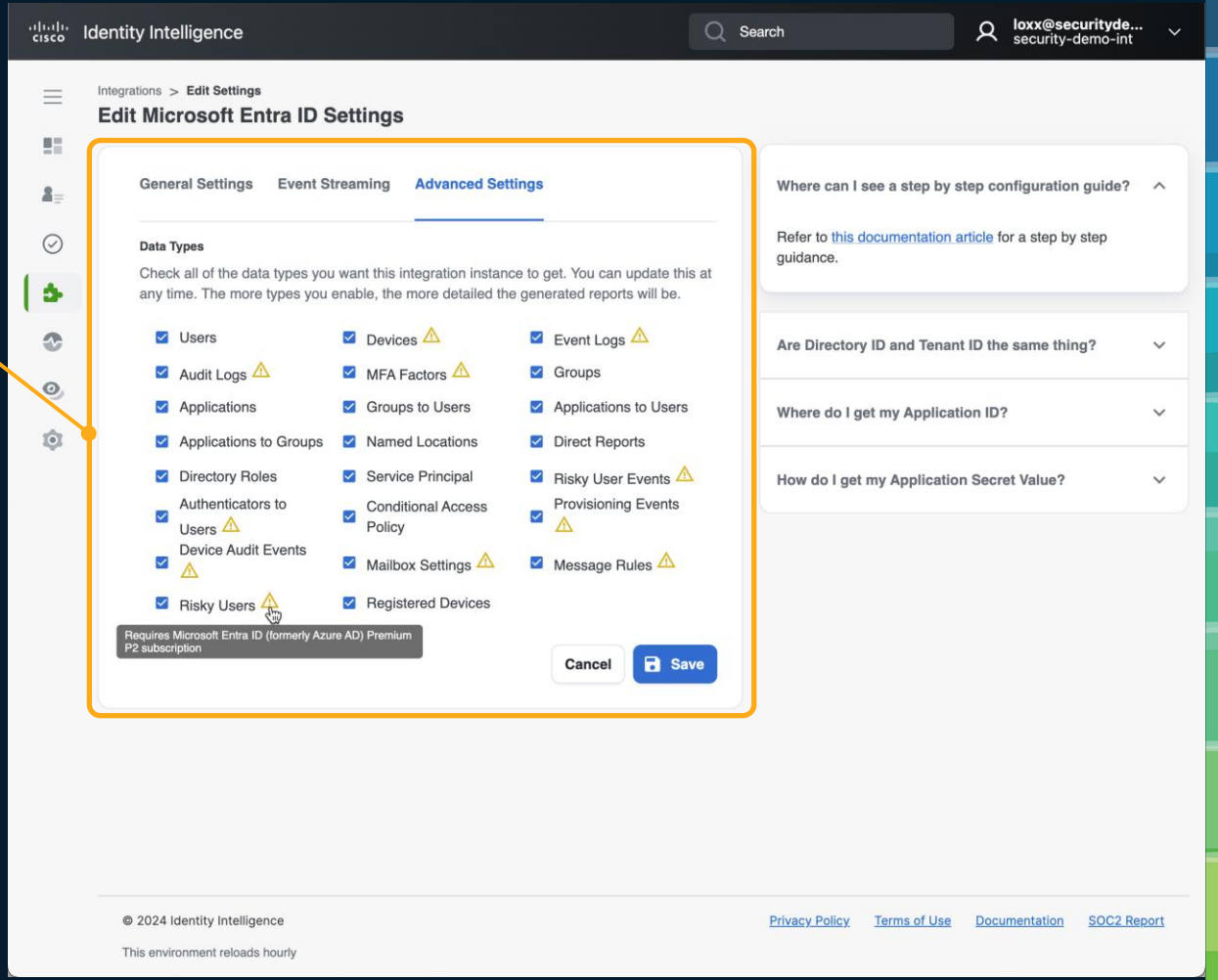


MS Entra ID

Advanced Settings

This is where you can tune which information CII should pull when performing sync's with Azure / Entra ID.

Some of the data types require Azure P1 or Azure P2 subscriptions, and CII leverages the information tool-tip to call those out.

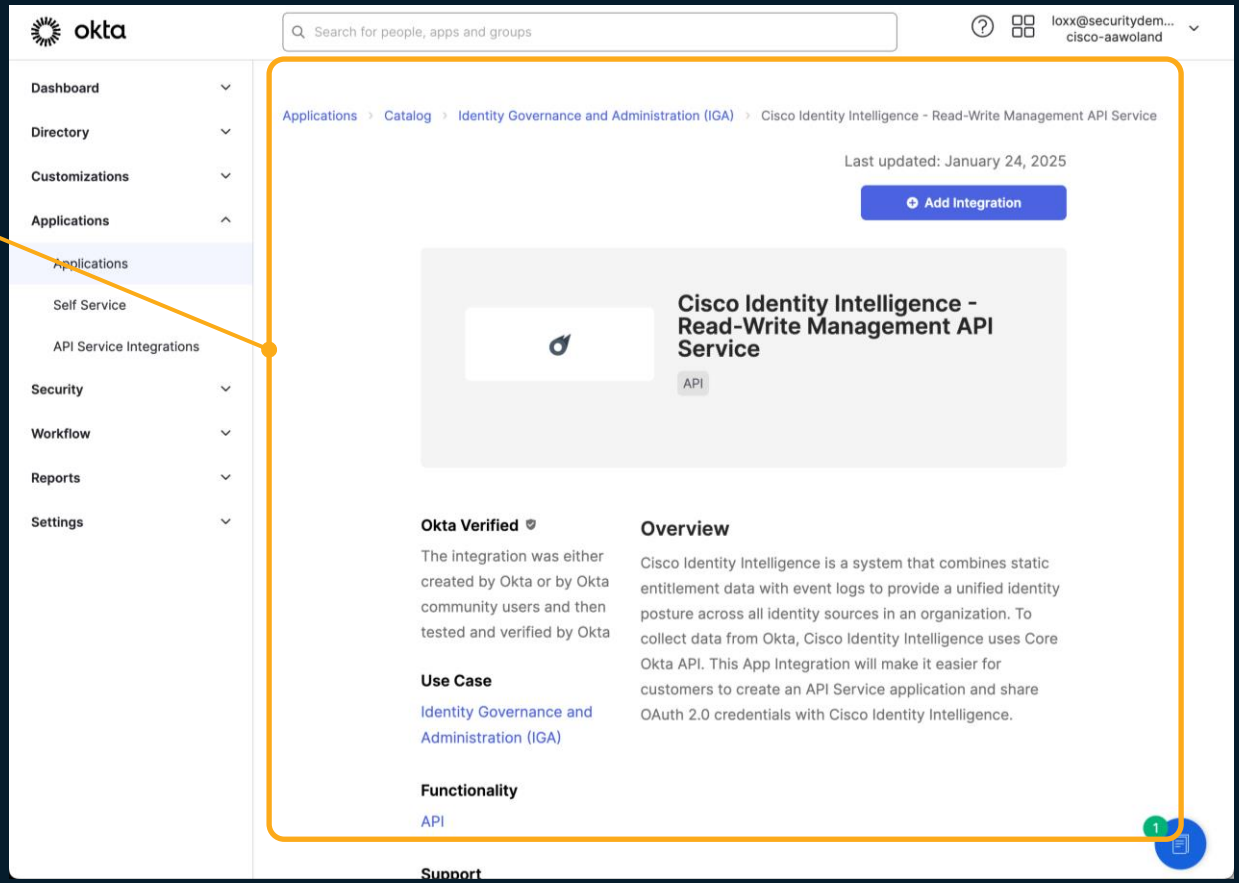


Okta Identity Engine

Okta

App Catalog

CII is an app in the Okta Catalog
- Sets up all the permissions
- Makes the integration dead-simple

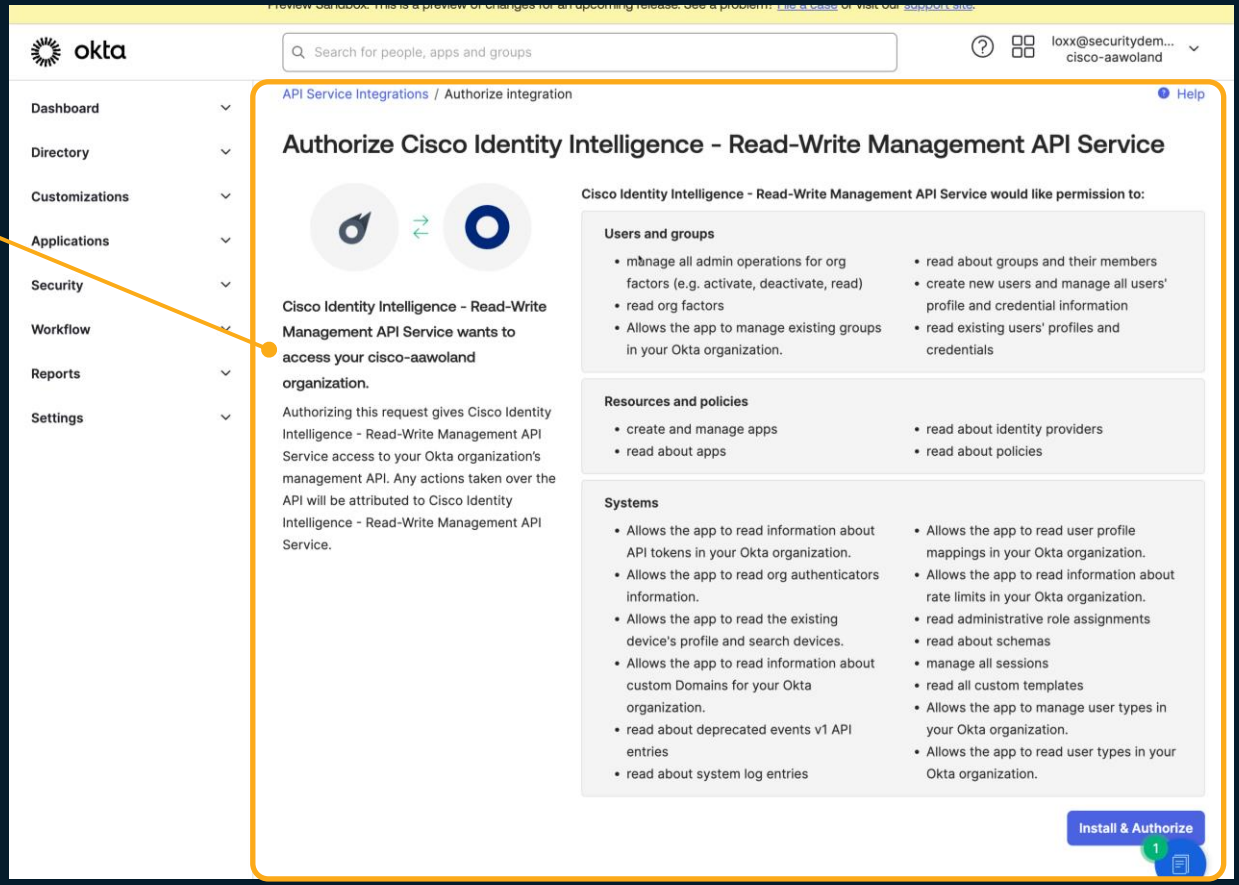


Okta

App Catalog

CII is an app in the Okta Catalog
- Sets up all the permissions
- Makes the integration dead-simple

Leverages OAuth to grant CII the exact correct permissions.

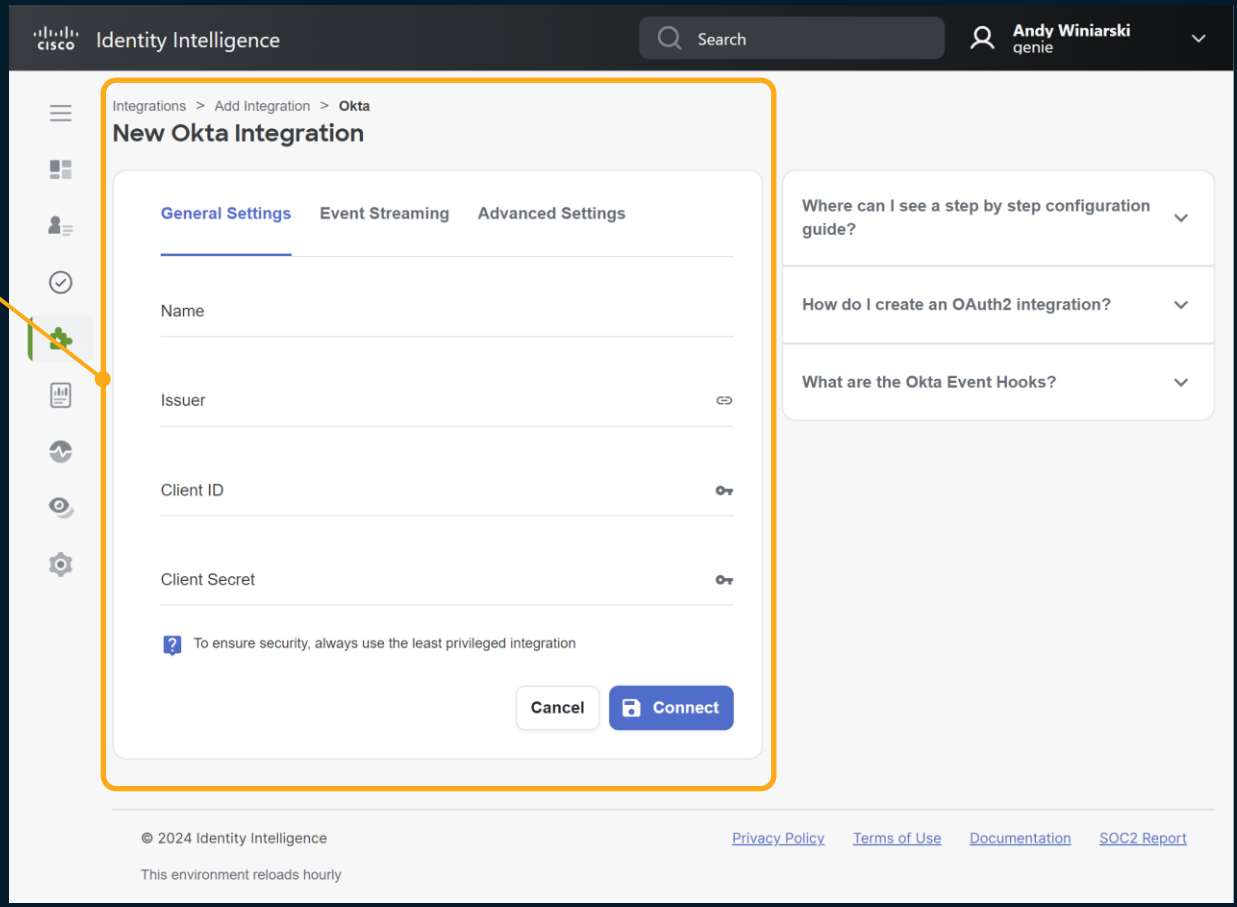


Okta

General Settings

The Okta integration uses an [OAuth2 application in the Okta app catalog]

The API is used to get directory information & syncs, but Event Streaming should be used for all log collection



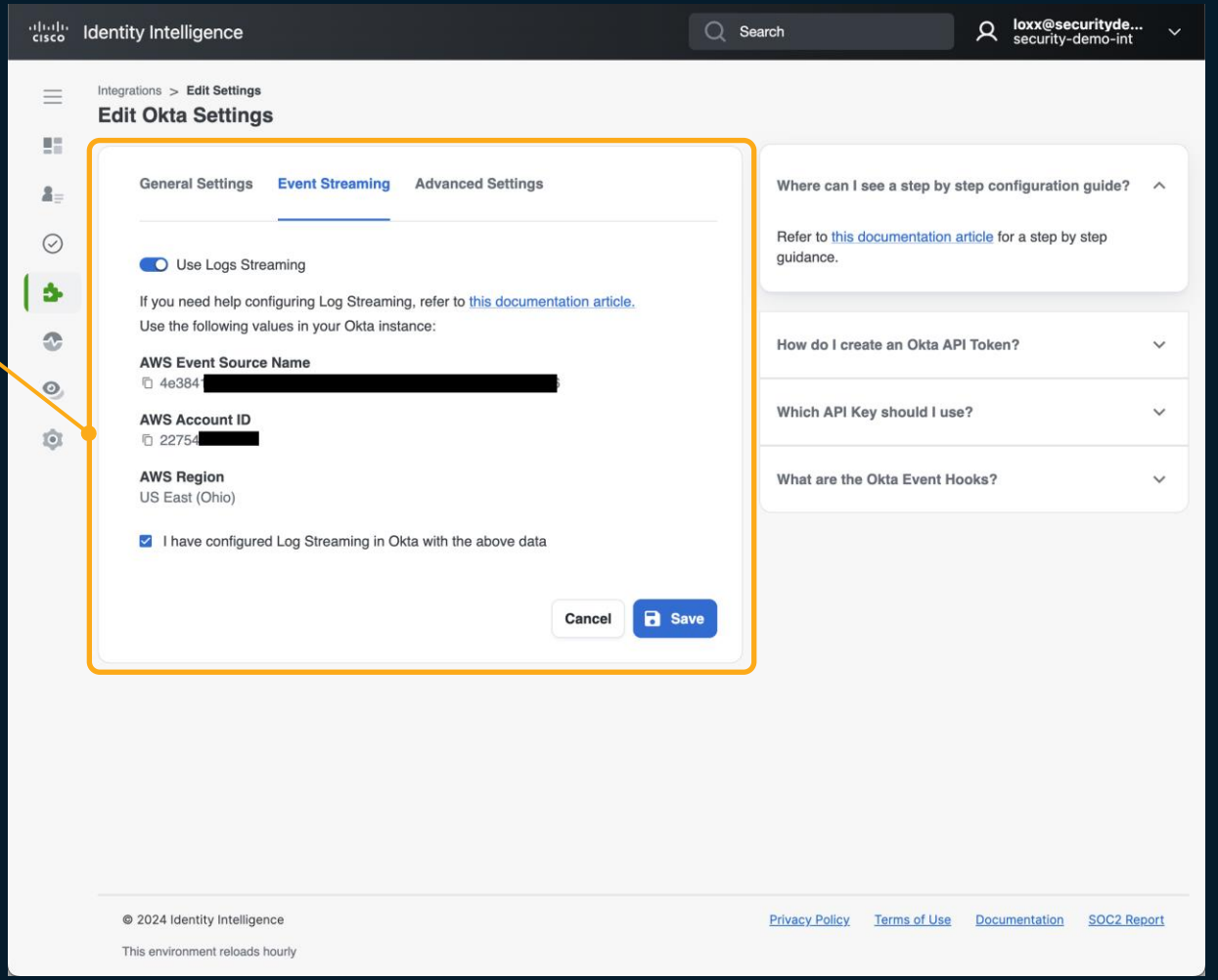
Okta

Event Streaming

Okta logs can be streamed to AWS Event Bridge

CII has its own Event Bridge, that Cisco pays for, so the customer does not have to (unlike Azure)

With Event Bridge, it really is more real-time than Azure Event Hub is. CII will get the logs in near-real-time & process



Okta

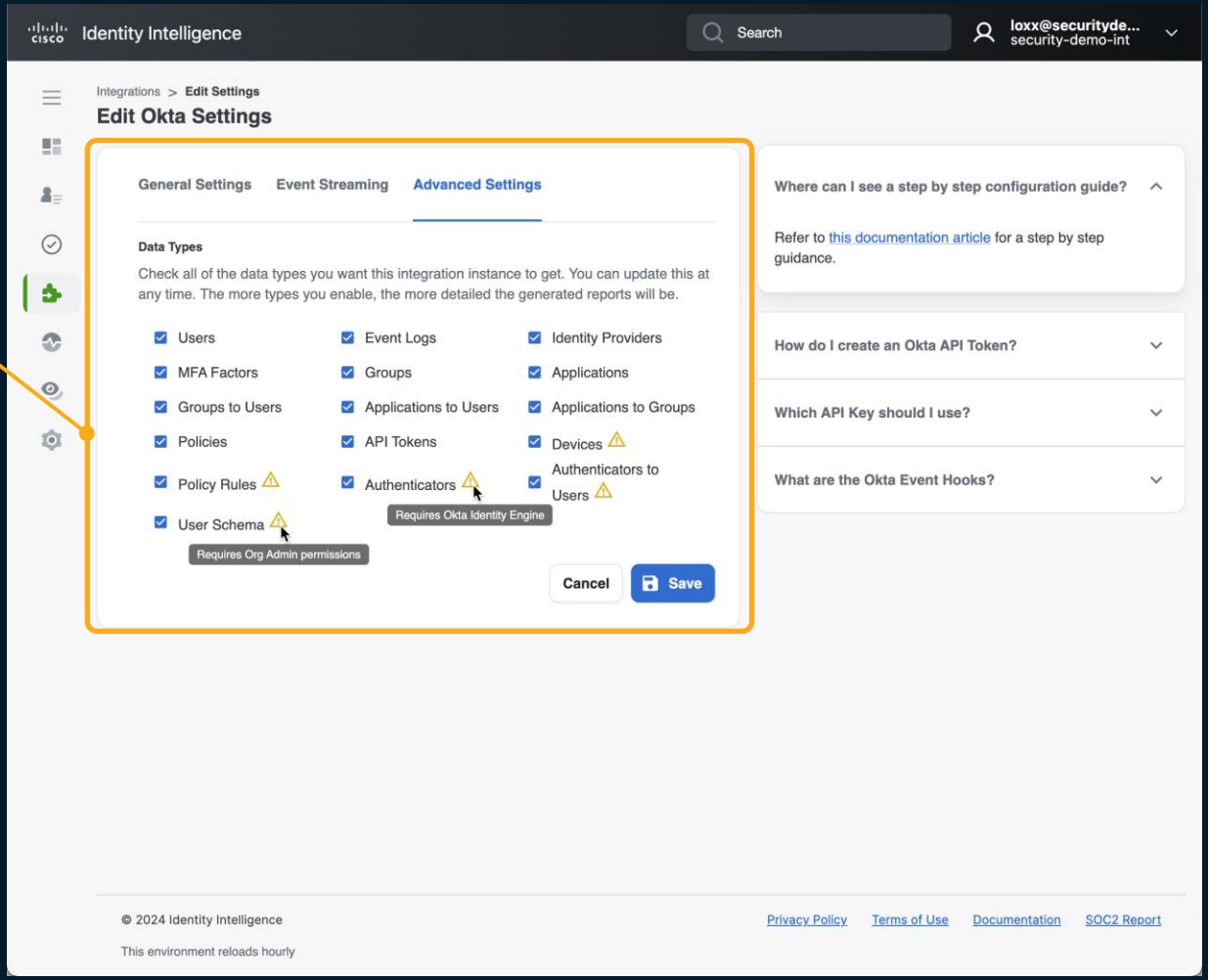
Advanced Settings

This is where you can tune which information CII should pull when performing sync's with Okta.

Some of the data types require the service account to be assigned Org Admin permissions.

Some of the data types are not available from Okta IdP but require customer to upgrade to Okta Identity Engine (OIE)

CII leverages the information tool-tip to call those out.

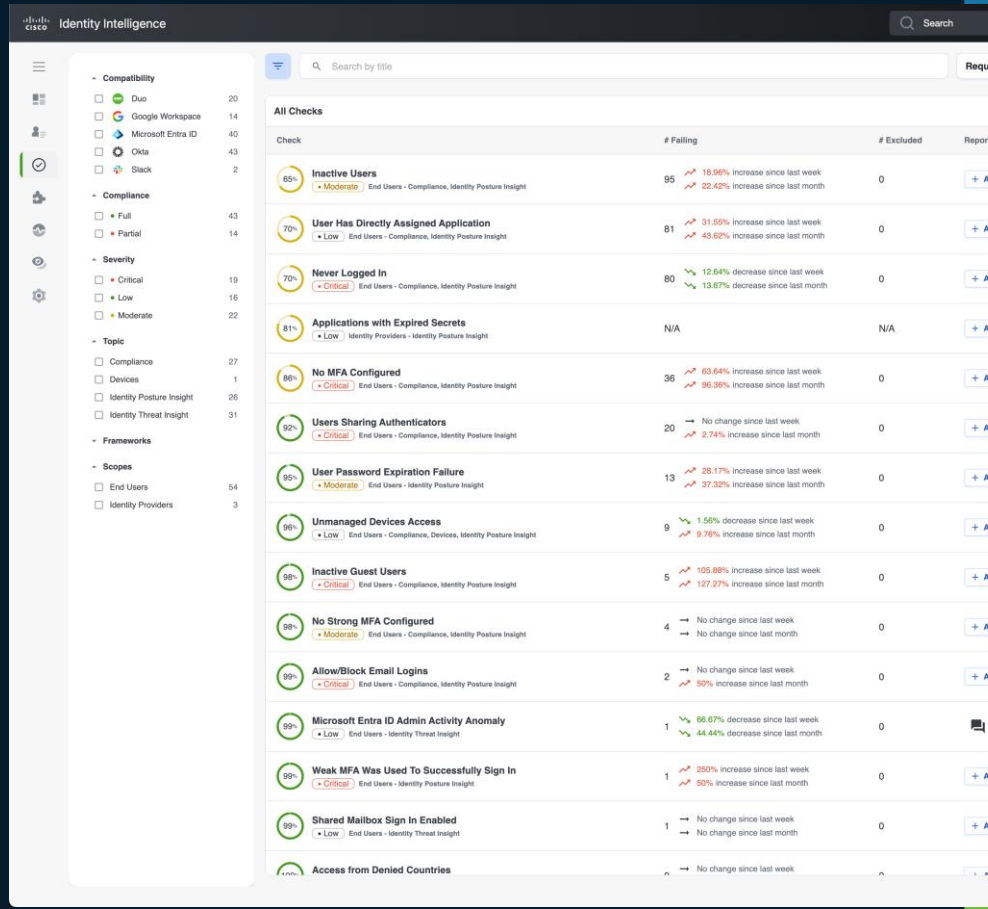


Agenda

- What is Cisco Identity Intelligence
- Integrations & Users
- All about Checks
- Remediations
- Other Technical Nuggets
- User Trust Levels & Posture
- Let’s talk about APIs
- Call to Action

What are Checks?

- Analytics, detections, rules... like “signatures” in an IDS
- When the collected data matches a check... That check is recorded as failed.



Compatibility

Not all checks are compatible with all providers / sources.

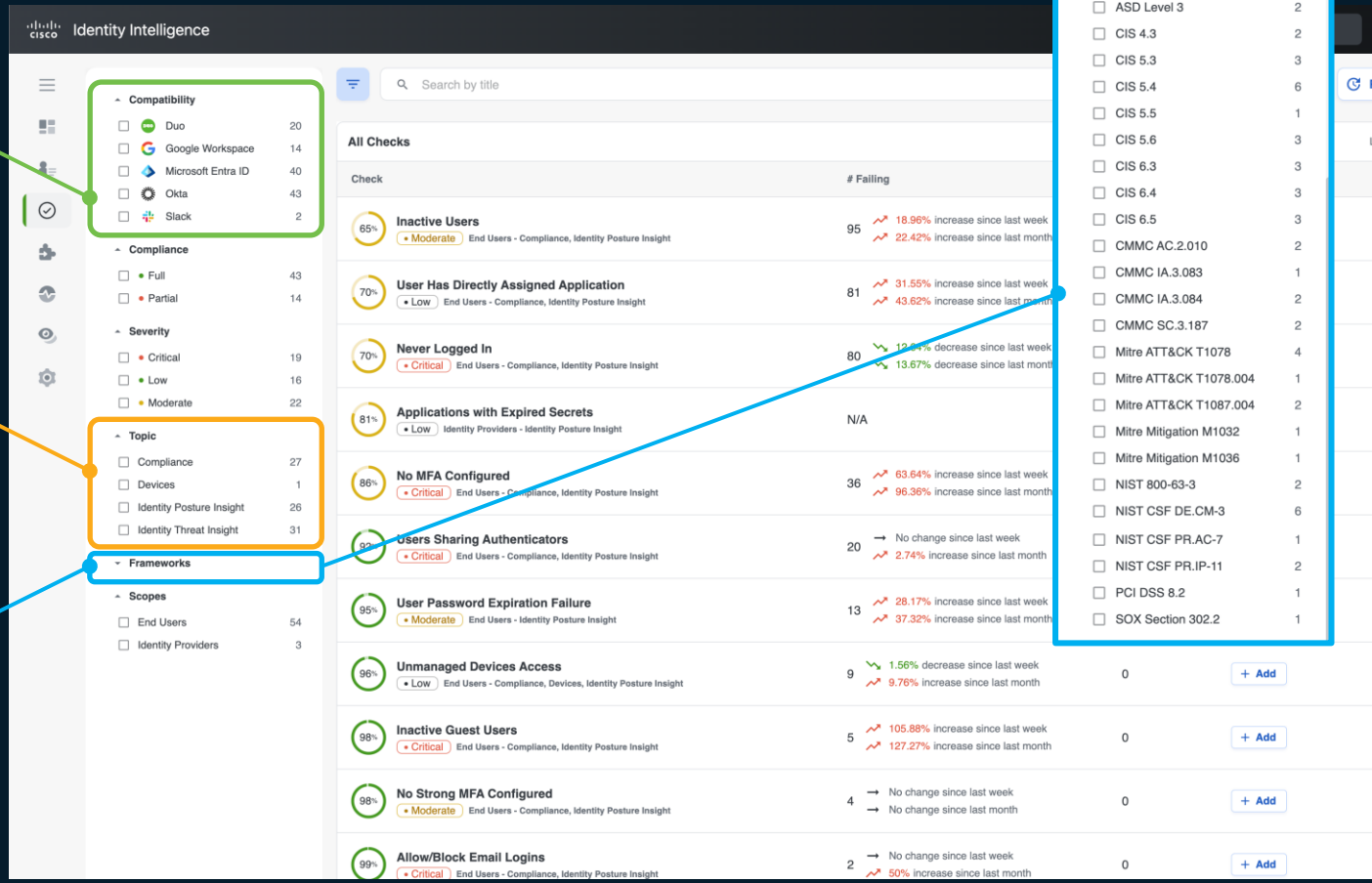
You can filter the list of checks based on the IdP source

Topics

Broken into categories and are very filterable.
A single check may belong to multiple Topics

Frameworks

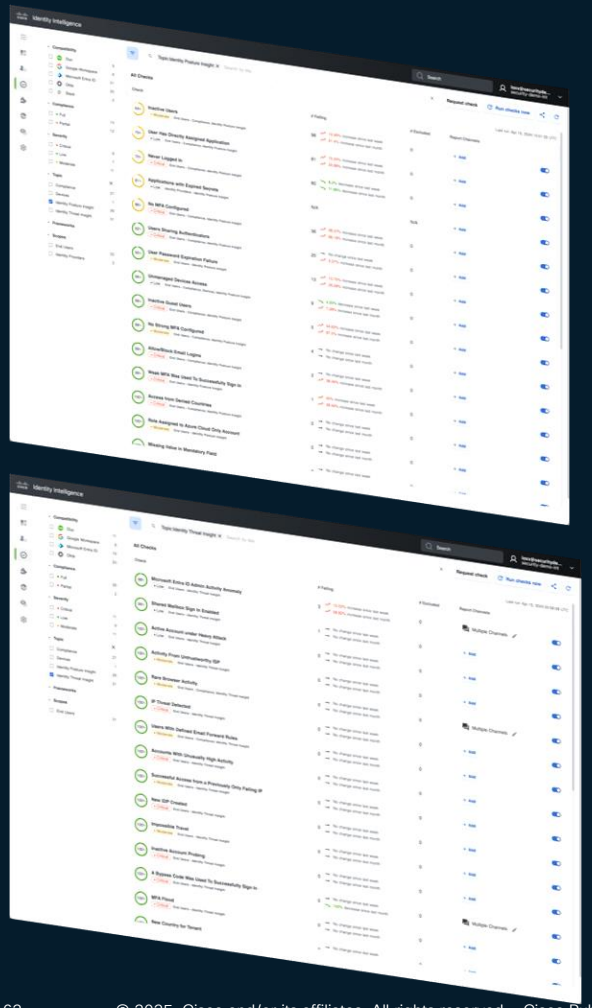
Checks are classified into their applicable risk frameworks – such as CIS, NIST, MITRE ATT&CK TTPs, etc.



Proactive vs. Reactive

- Posture Checks are Proactive – examining the authentications and account configurations – to reduce probability and blast radius

- Threat Checks are Reactive – examining the behavior of users and their authentications – to detect threats



Checks are Tunable

Check Settings

Depending on the check itself, there are multiple settings that can be adjusted / tuned.

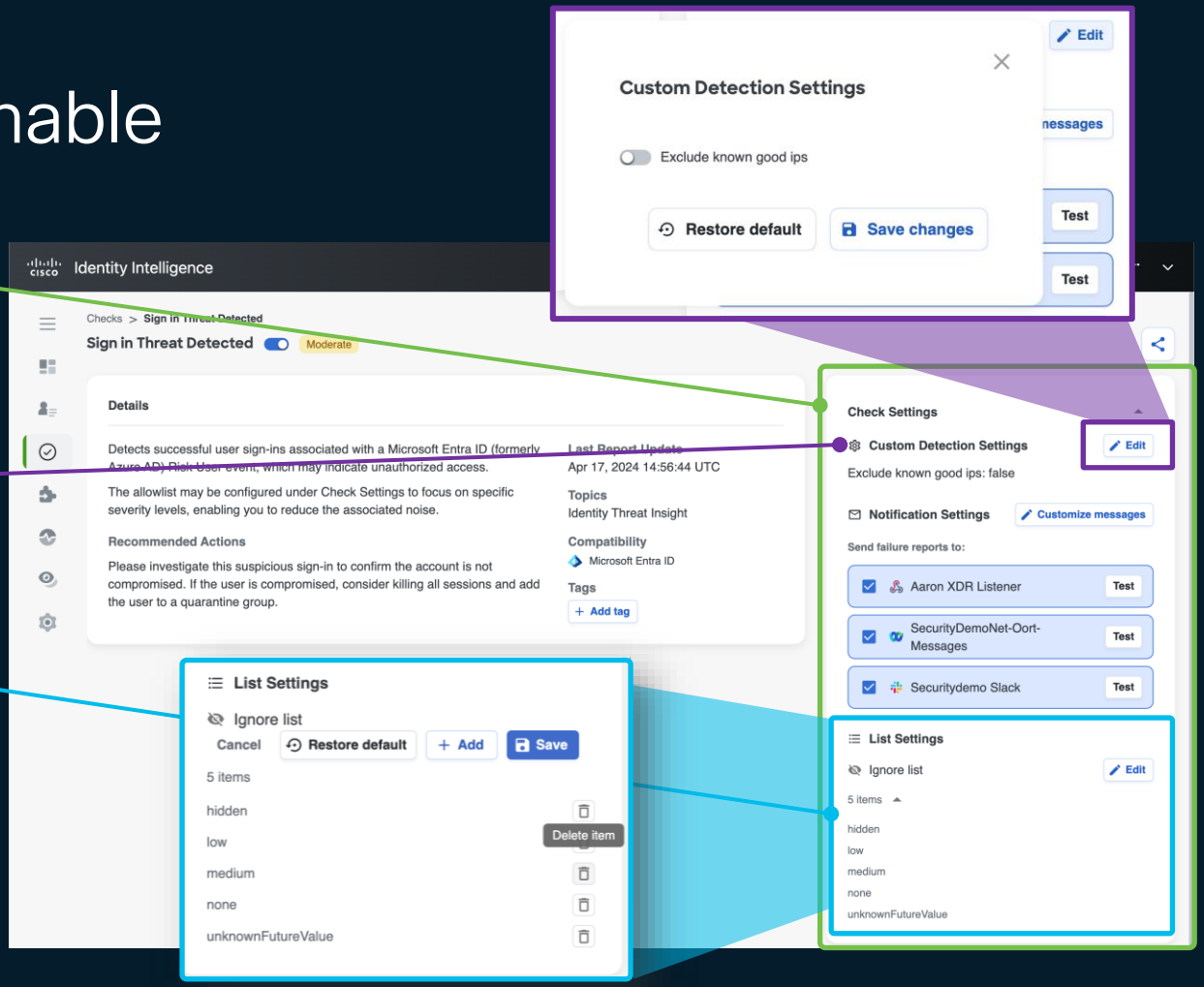
Custom Detection Settings

This one only customizes for exclusion of known-good IP's.

List Settings

In this case, we are defining which events from EntraID are not noteworthy enough to run against the check.

Default was: Ignore Medium & Below



Outbound Notifications

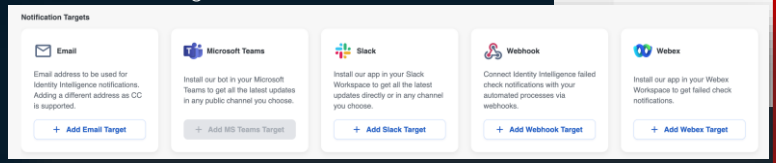
Notifications

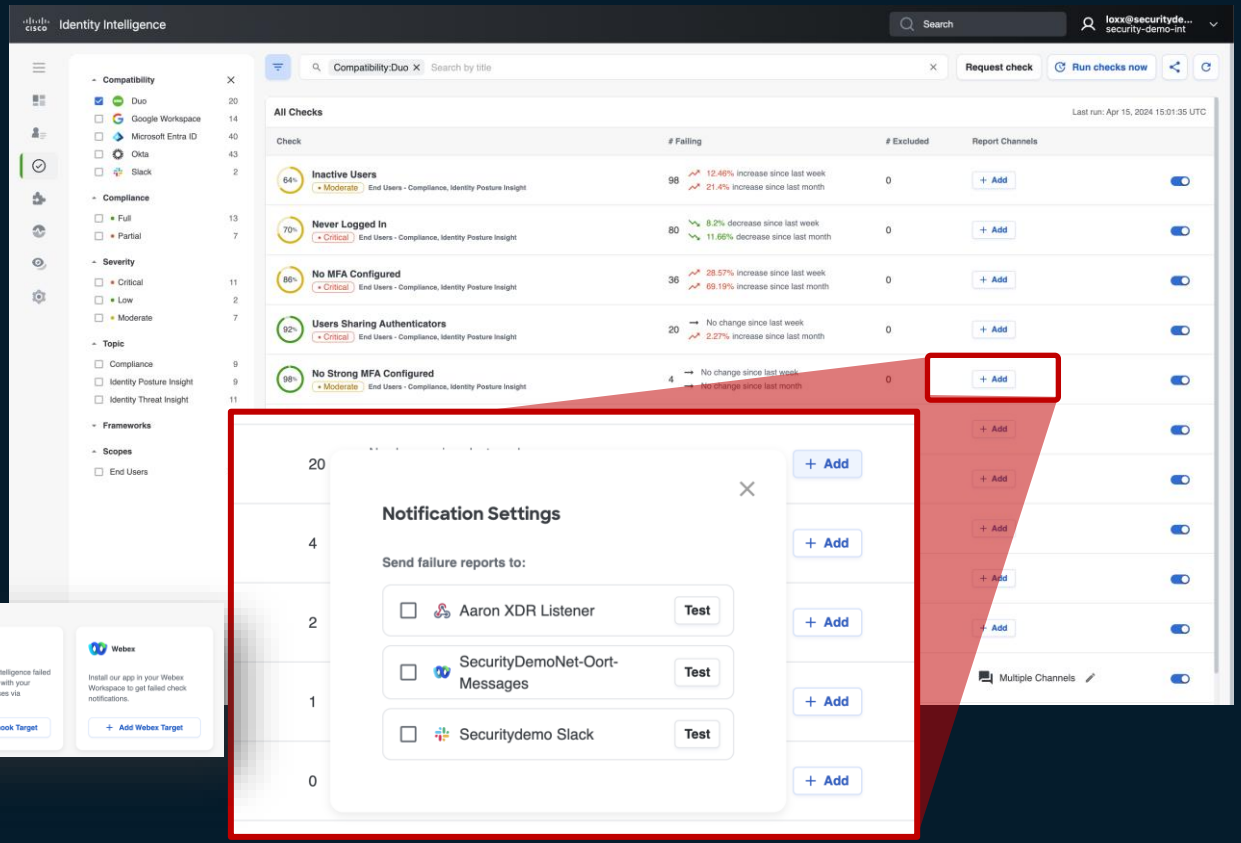
Notifications are configured per check.

Checks are run periodically, matching the data in the CII datastore to the requirements set in the check.

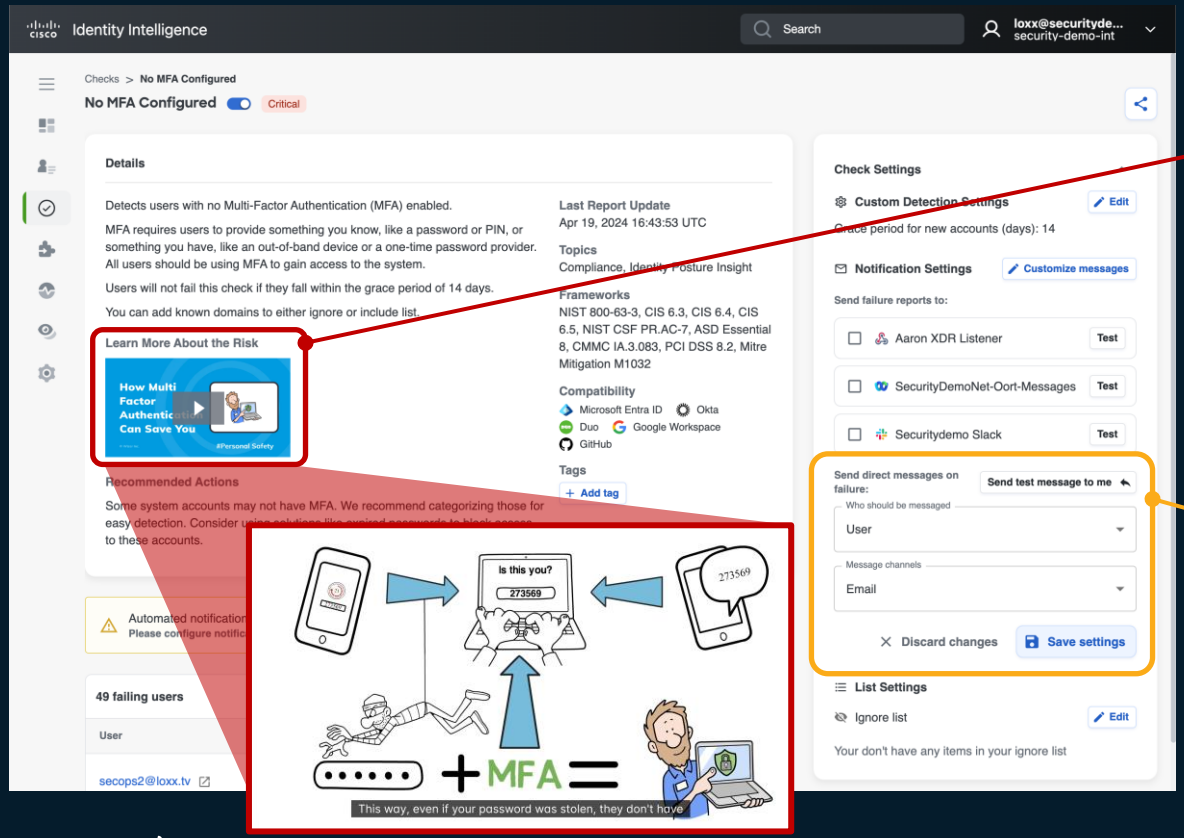
When there is matching criteria, that means a user, device or setting has “failed” that check, and all selected notification channels will be used.

Notifications Targets:





Direct User / Manager Notifications



Security Education

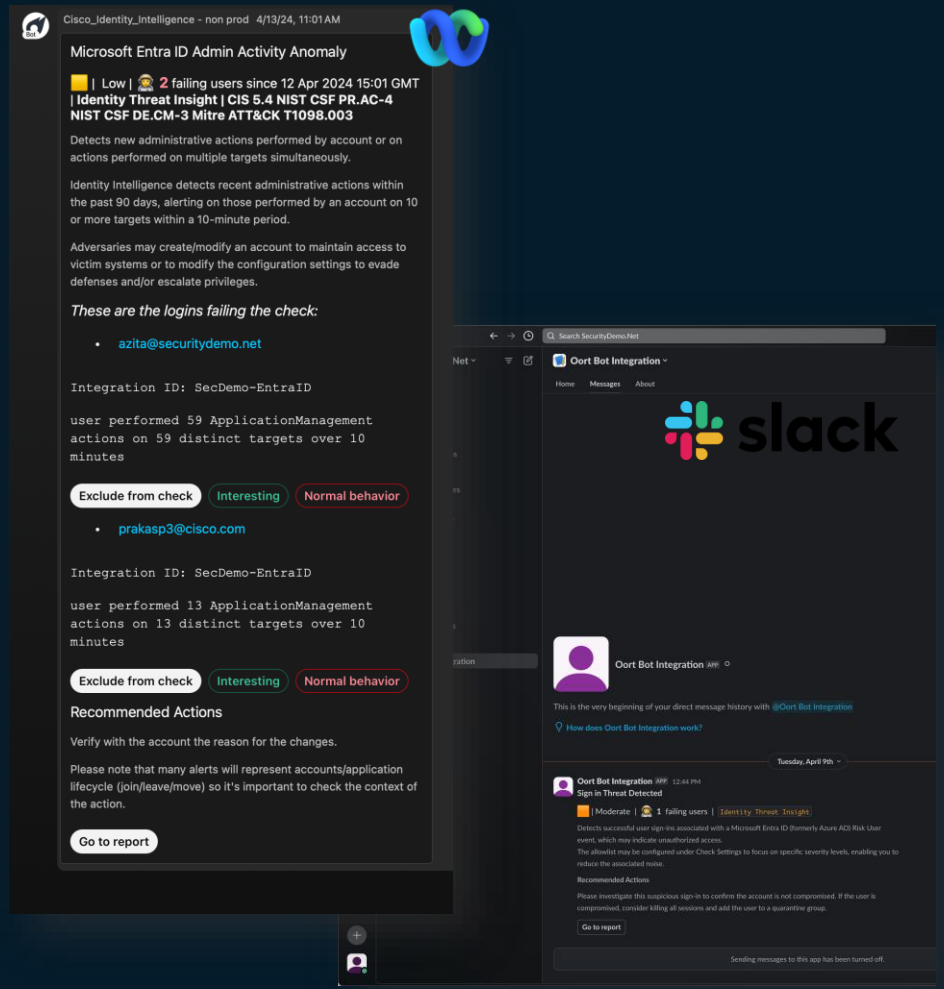
CII partners with Wizer (https://www.wizer-training.com/) and their very cool security education videos to help educate the end-user on what they did wrong & why it matters.

Educate the End-User

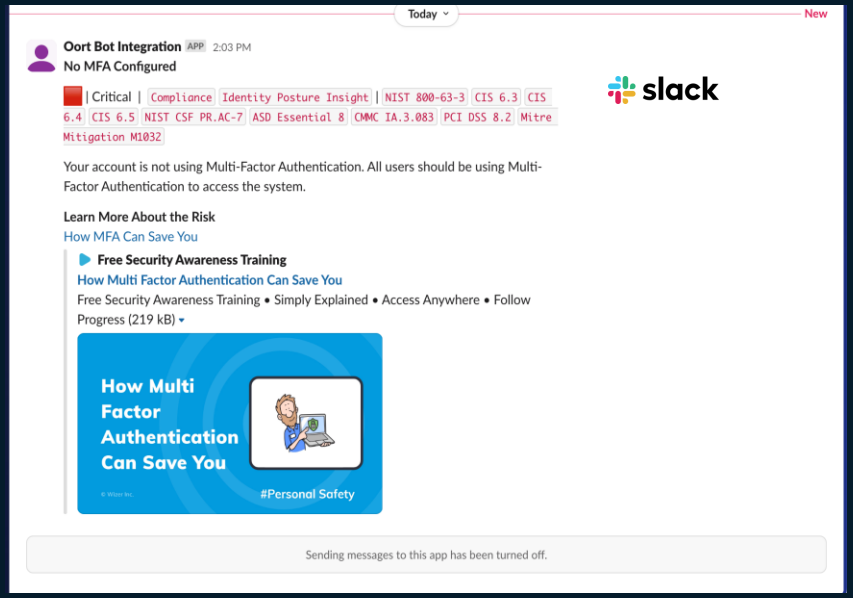
Notifications may be customized and sent to the end user via email or IM.

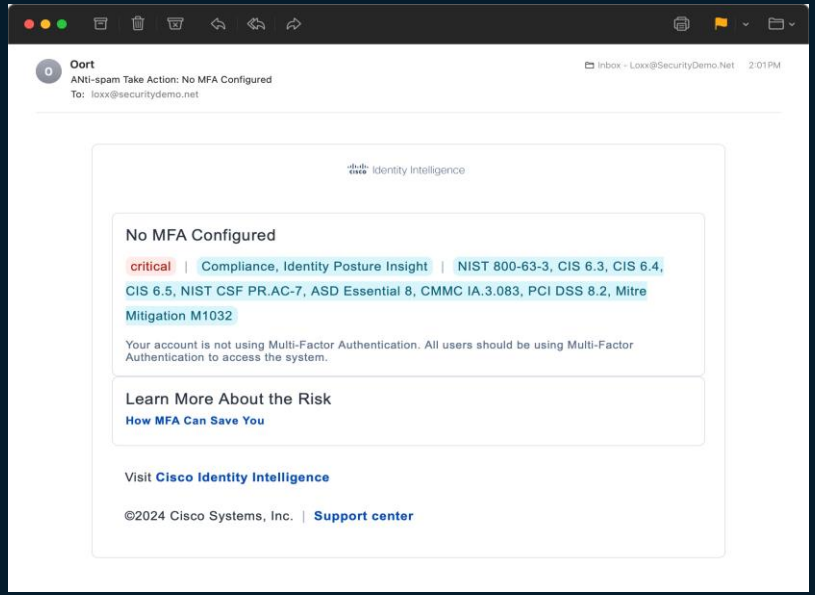
Chat Ops

- Many Cisco customers do all their workflows through the IM applications like Webex and Slack.
  - Provides not only notifications, but also responses such as:
    - Exclude from Check
    - Mark as Interesting
    - Mark as Normal Behavior



Chat Notification Targets





Agenda

- What is Cisco Identity Intelligence
- Integrations & Users
- All about Checks
- Remediations
- Other Technical Nuggets
- User Trust Levels & Posture
- Let’s talk about APIs
- Call to Action

Taking Action(s)

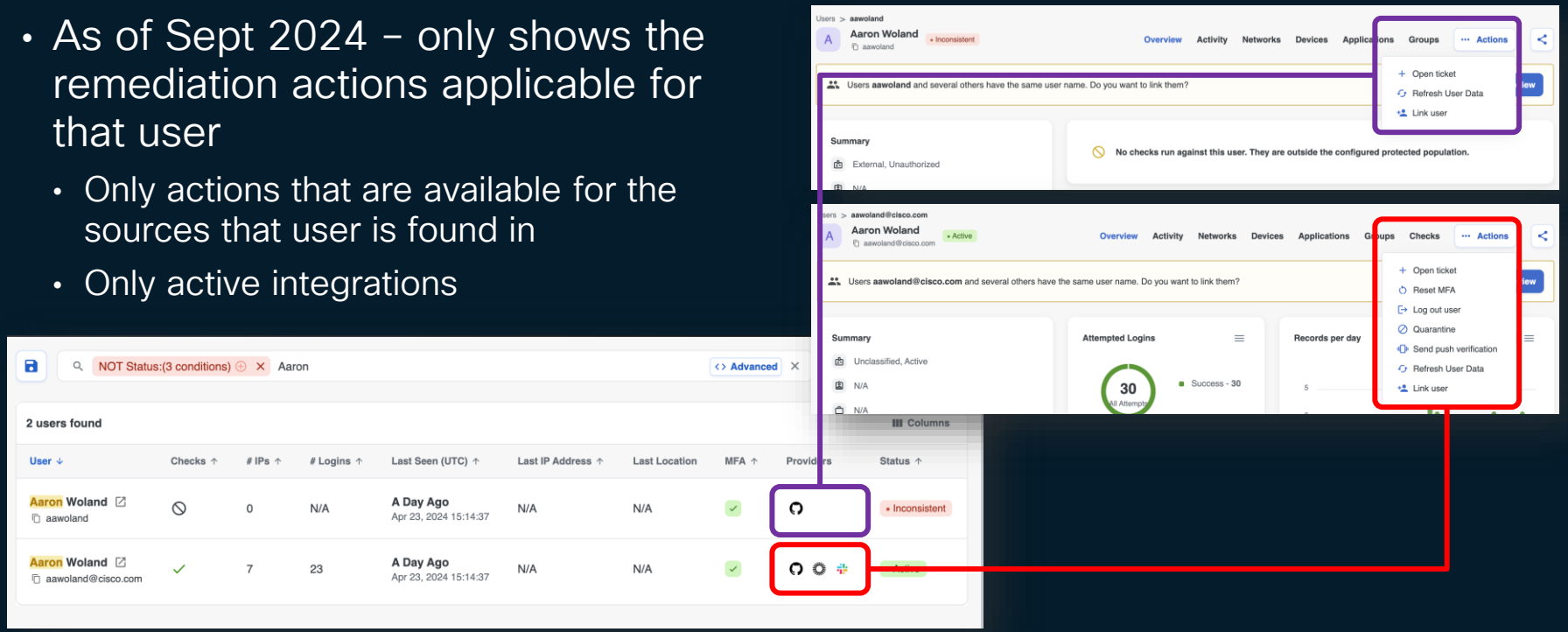
Remediation is available through CII, but it is up to the customer to determine if direct remediation is right for the organization

- Organizations have invested heavily in their response flows with ticketing systems like ServiceNow, or Automation Tools like XDR and SOAR.
- Those organizations should use webhooks to notify those other systems & respond through a robust workflow.

- Remediations are source specific
  - Not all sources support the same remediation.
  - Reset MFA is applicable to Okta & Duo only (for example)
- Remediation Nuggets:
  - CII only allows one remediation action at a time.
  - The provider must be configured to allow the actions (think "*write*" access)

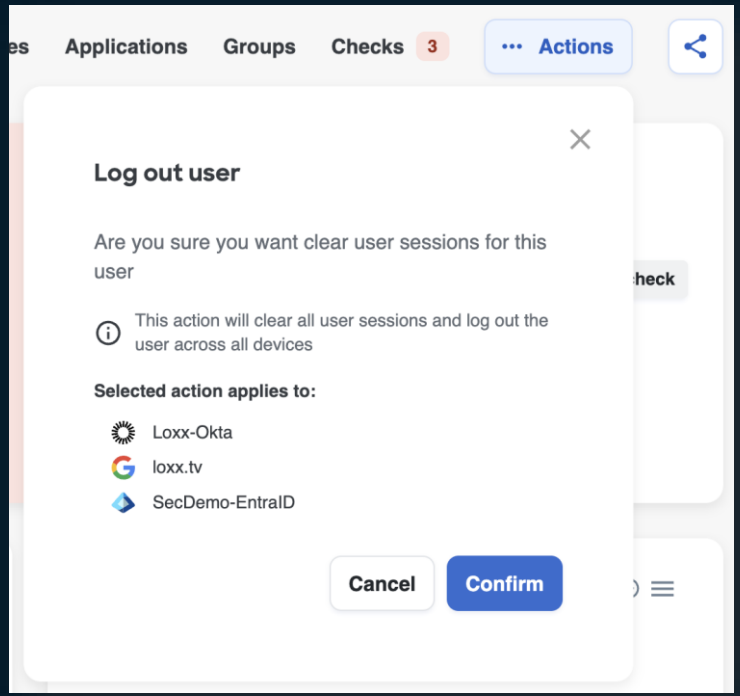
Context Specific Remediation Menu

- As of Sept 2024 – only shows the remediation actions applicable for that user
  - Only actions that are available for the sources that user is found in
  - Only active integrations



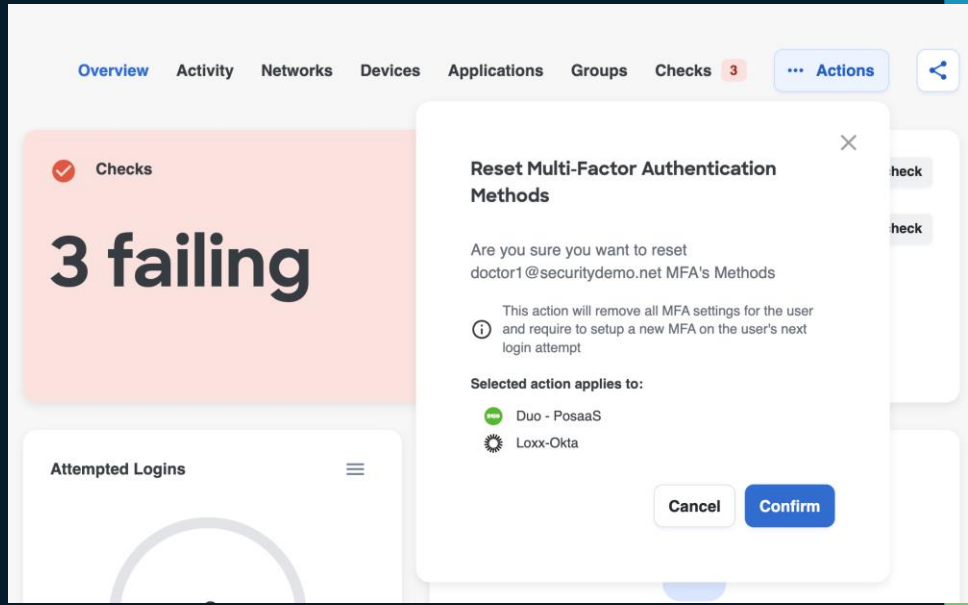
Log Out User

- Clears all user sessions
  - Logs out the user across apps that support action (O365, for example)
- Remember how WebAuth protocols work:
  - IDP signs token, session is issued based on valid token.
  - Session has expiration time
  - Until that time, session is VALID
  - Apps do not check with IDP again during that valid time
  - Sessions can last hours, days, or longer

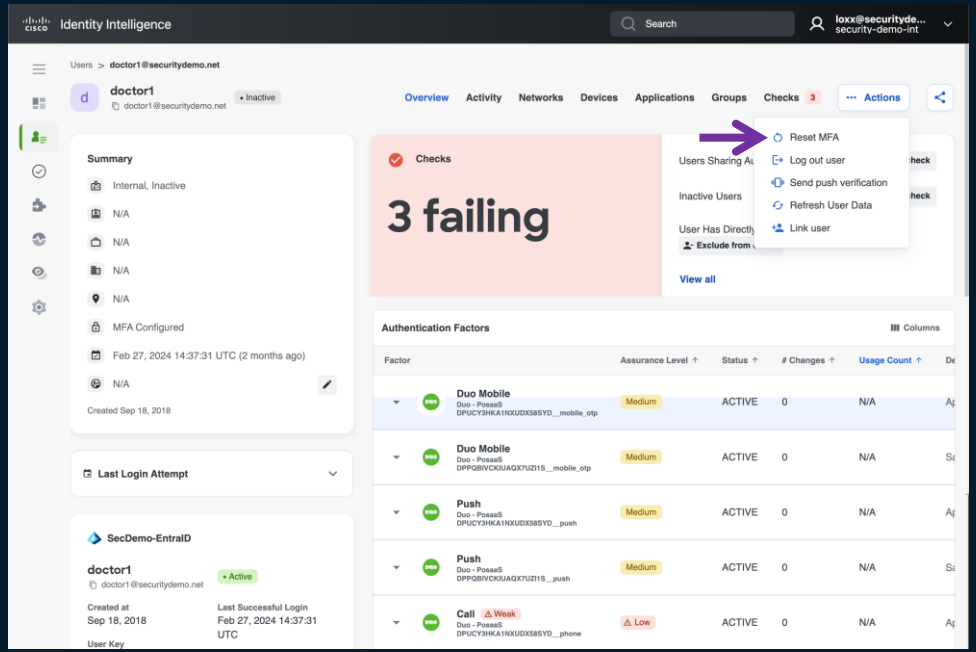


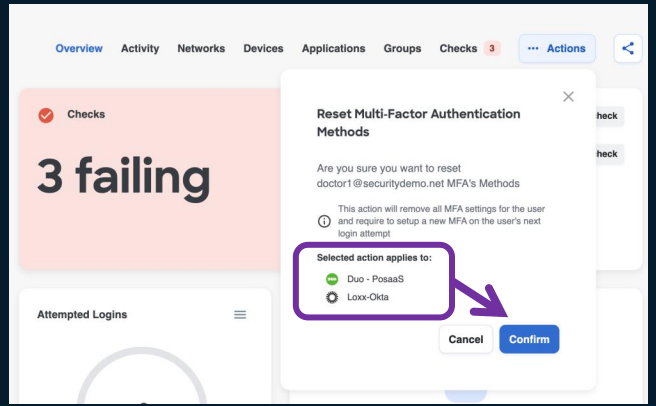
Reset MFA example w/ Duo

- CII queries the Duo Admin API
  - Learns all phones associated to user
  - Learns all hardware tokens for user
- CII Disassociates the user from the all their phones and tokens
  - User is as if they are brand-new
  - Have to setup MFA from scratch



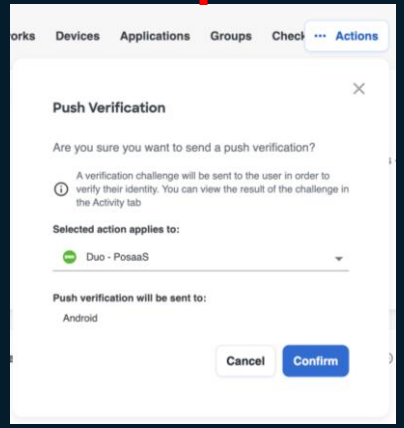
Duo’s Reset MFA

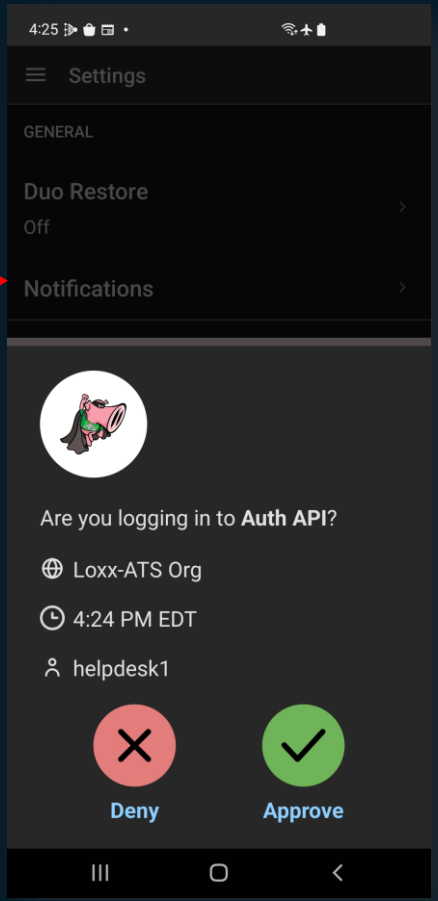




Send Push Notification

- To verify a user's identity
  - Send the user a one-time push notification to confirm they are who they say they are
  - Very helpful for help-desks to verify human calling them is indeed who they say they are
- Select the MFA provider
  - Click Confirm
  - Push notification is sent





Leveraging Your Security Operations Center (SOC)

Cisco XDR

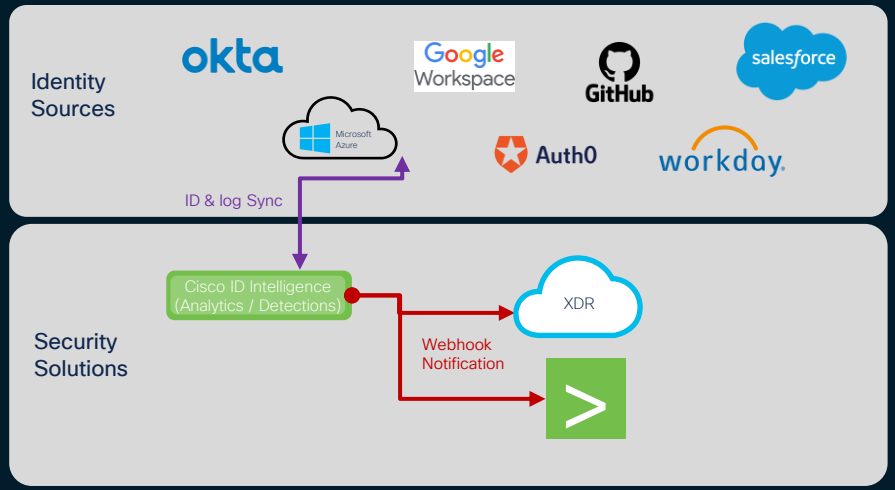
Splunk

...and other SOC Tools

Webhooks

A callback function that uses HTTP/S between two APIs based on events

- Send small amounts of data, reactively after a check-fails
- An example is CII sending a notice to Splunk SOAR or XDR of a check that failed
  - The automation playbook/workflow will extract the appropriate data and then proceed through the rest of the flow

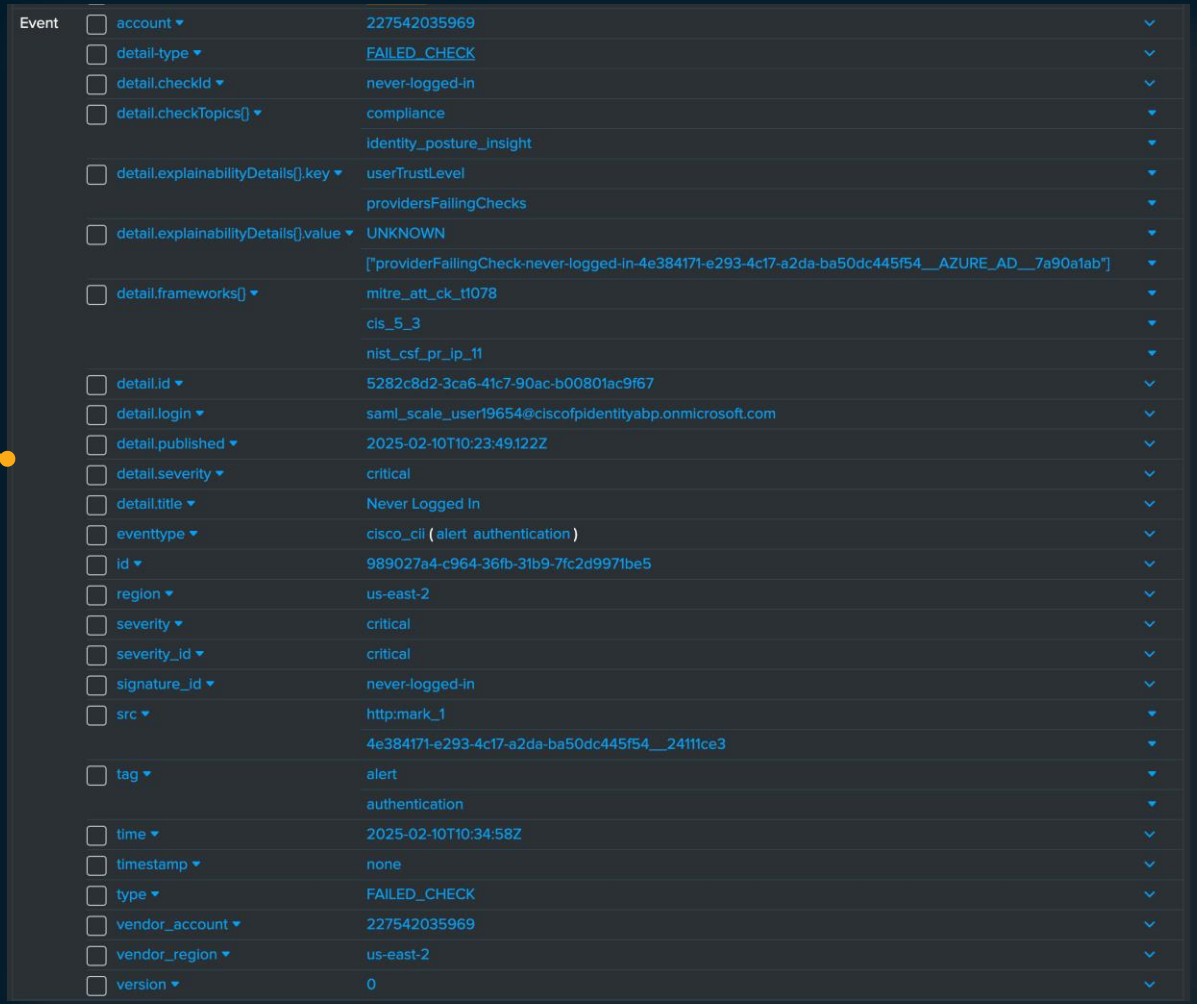


What's in the Webhook?

Failed Checks

Ie.: A matched signature.

- Check Name
- Details
- ATT&CK Categorization
- Severity
- Tags
- Unique ID's



Webhooks w/ Cisco XDR

Webhook URL

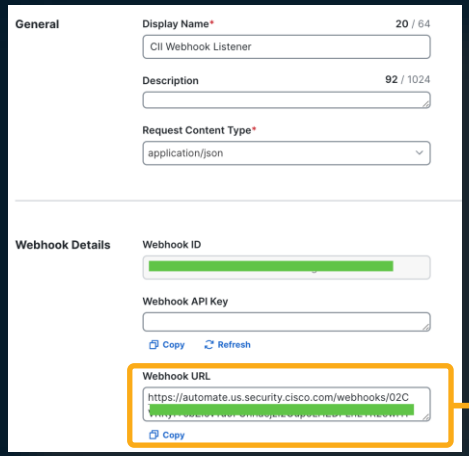
XDR listener has specific requirements
- API Key must be in the URL
- 2x Specific headers

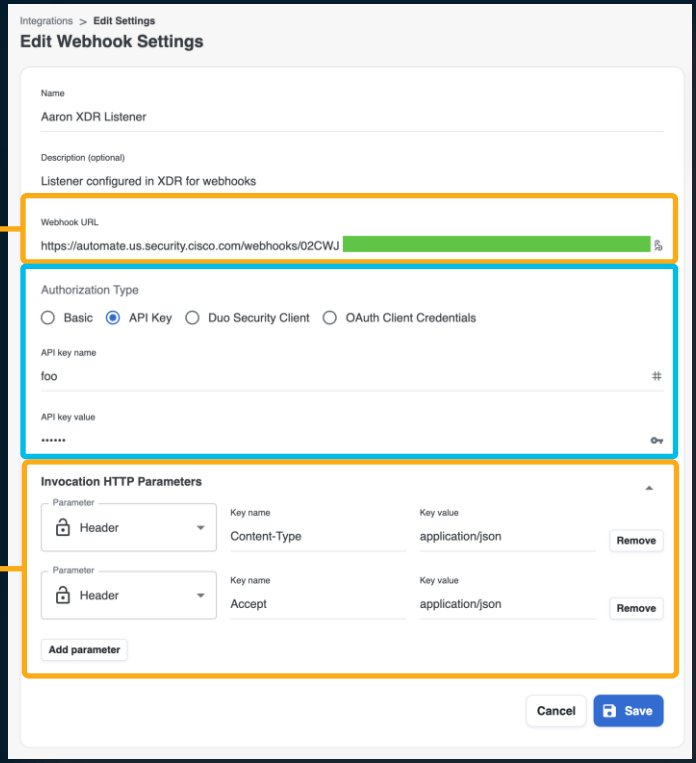
Authentication

- CII webhooks require authentication
- But we can lie to it, as long as the key is in the URL
- Here, we lied to it w/ Foo & Fake password

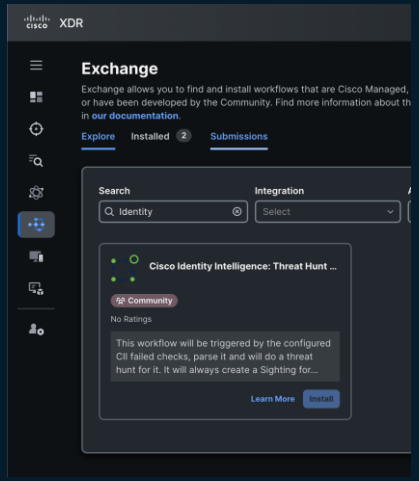
Setup Guide

Published here at Aaron Woland's blog



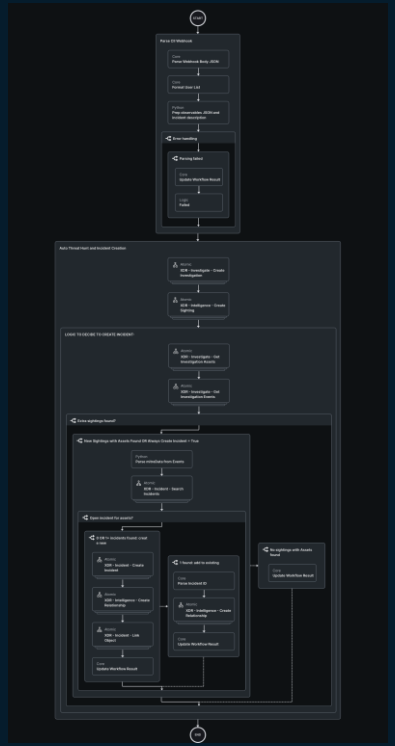


Webhooks w/ Cisco XDR



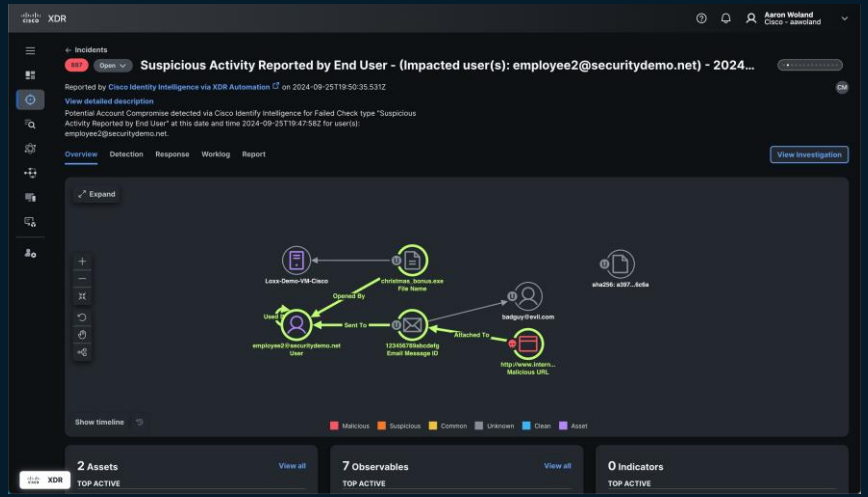
Published in Exchange

- A community-maintained XDR workflow.
- Takes the CII Webhook & parses it.
- Will enrich existing incidents, or none exist will create a new incident.



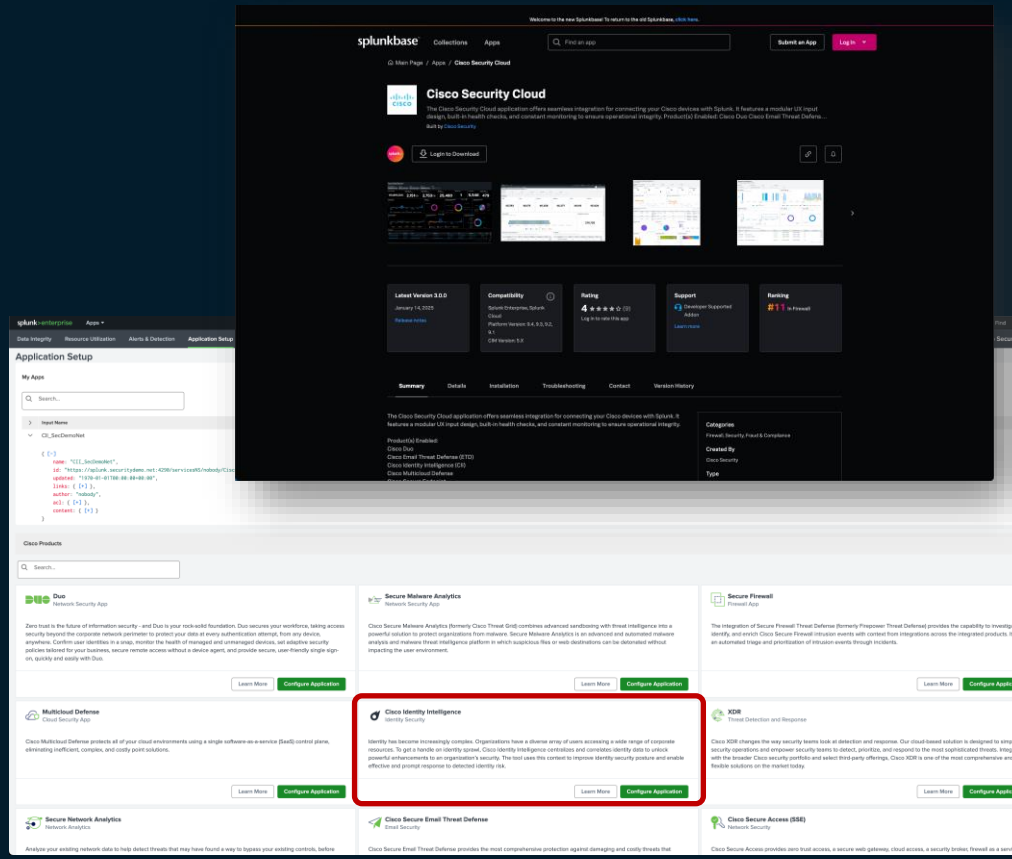
Merges with Incidents

- The CII source events are correlated with the detections from other security products.
- The CII ITDR detection is now part of the attack graph & investigations



App (TA) in Splunk

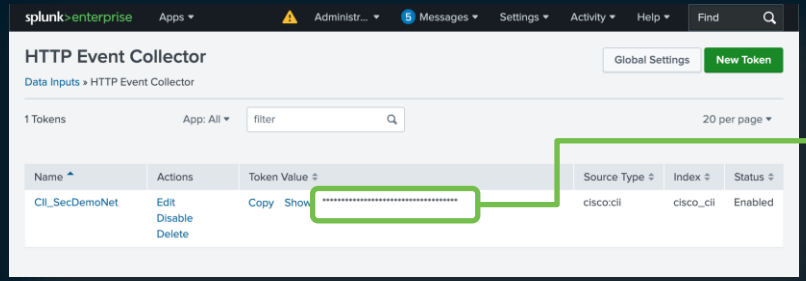
- Cisco Security Cloud App
  - Used for many Cisco Security Products, such as Duo, Firewall, etc.
  - Cisco Identity Intelligence is included.
  - Leverages an HTTP Event Collector (HEC) for Data input.
    - Must use a public signed certificate (today).

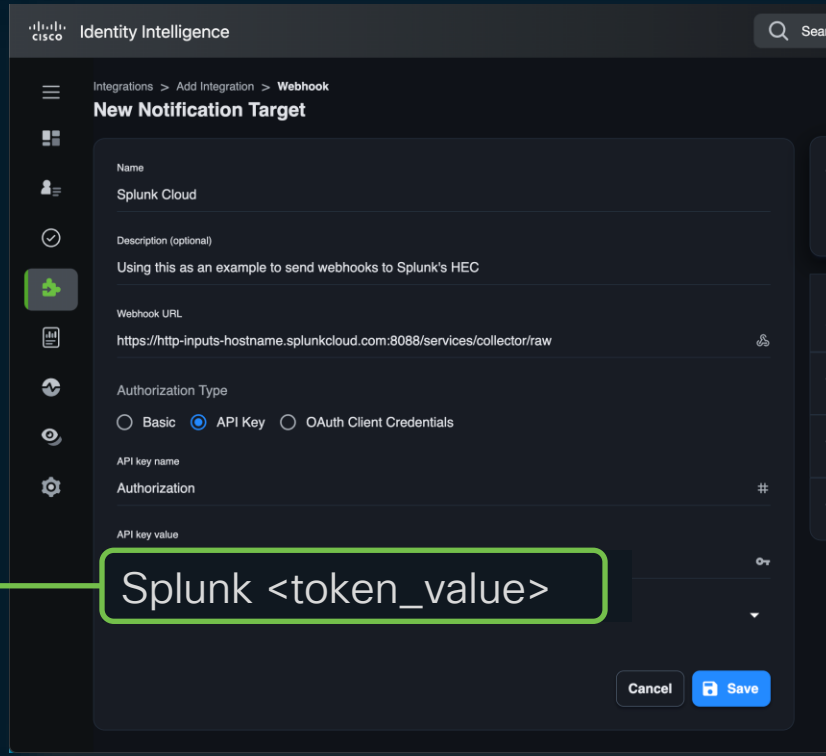


Cisco Security App (TA) in Splunk

Add webhook in CII for the HEC in Splunk

- Ensure the URL includes “/services/collector/raw”
- Authorization type = API Key
- API Key value must be “Splunk” + a space, then the token value.

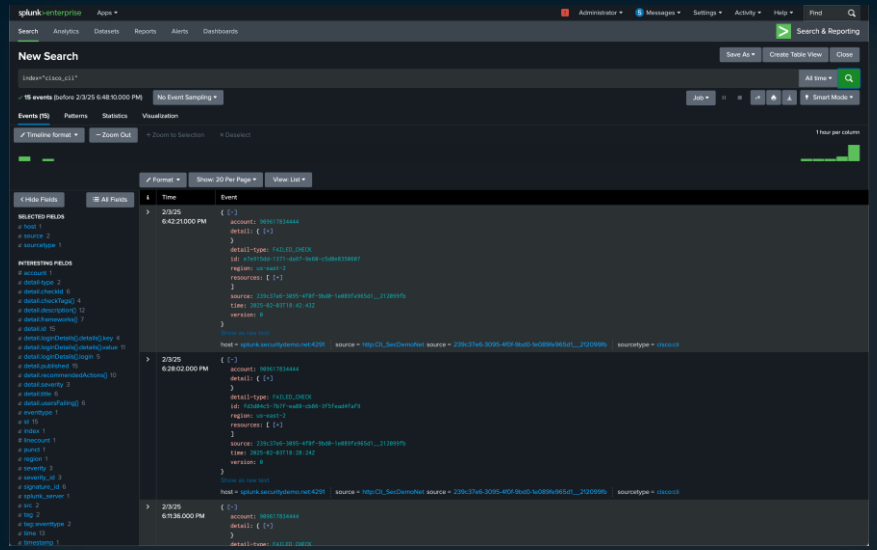


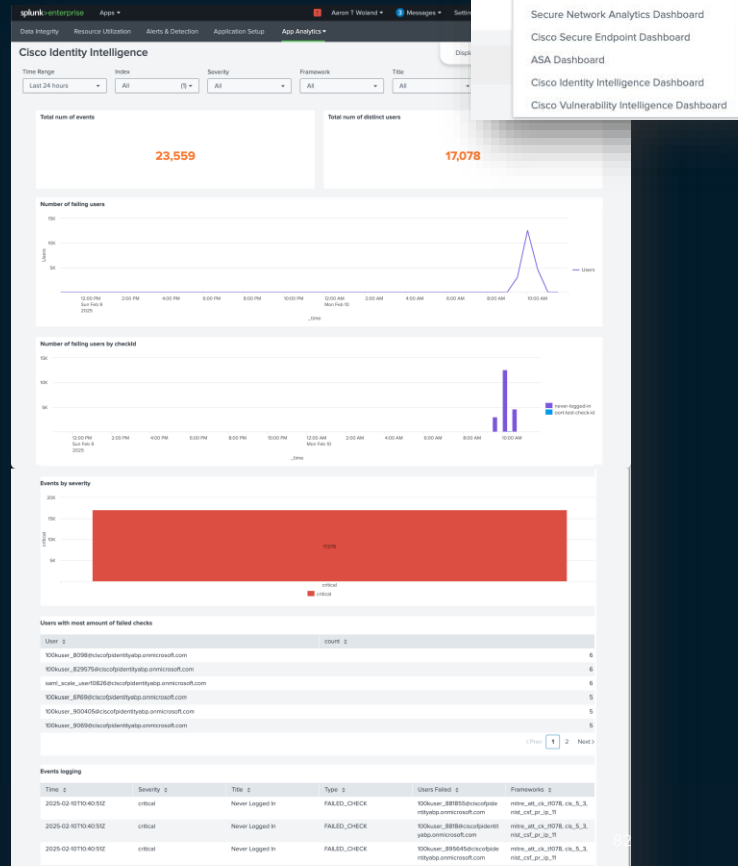


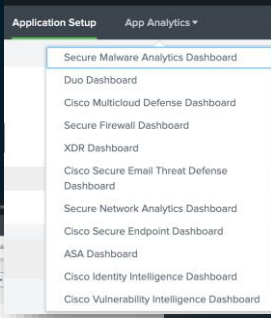
Cisco Security App (TA) in Splunk

Cisco Identity Intelligence app has a dashboard

- Creates the “cii_index"
- Has a dashboard for the data





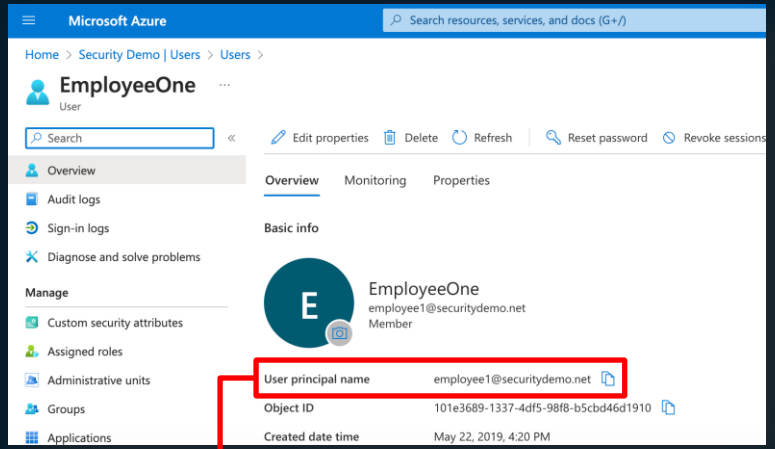


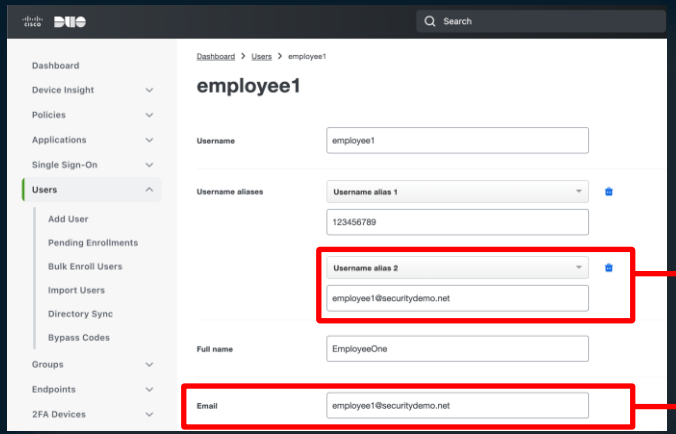
Agenda

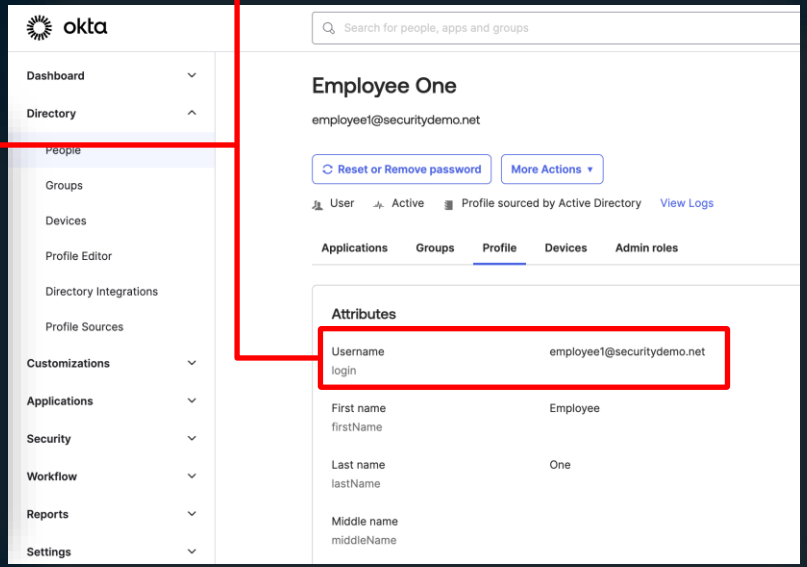
- What is Cisco Identity Intelligence
- Integrations & Users
- All about Checks
- Remediations
- Other Technical Nuggets
- User Trust Levels & Posture
- Let’s talk about APIs
- Call to Action

Account Merges

- Accounts from different IDPs are merged when:
  - UPN, email, Employee ID, or Duo Alias match.
- No “or” logic today. Must use one.





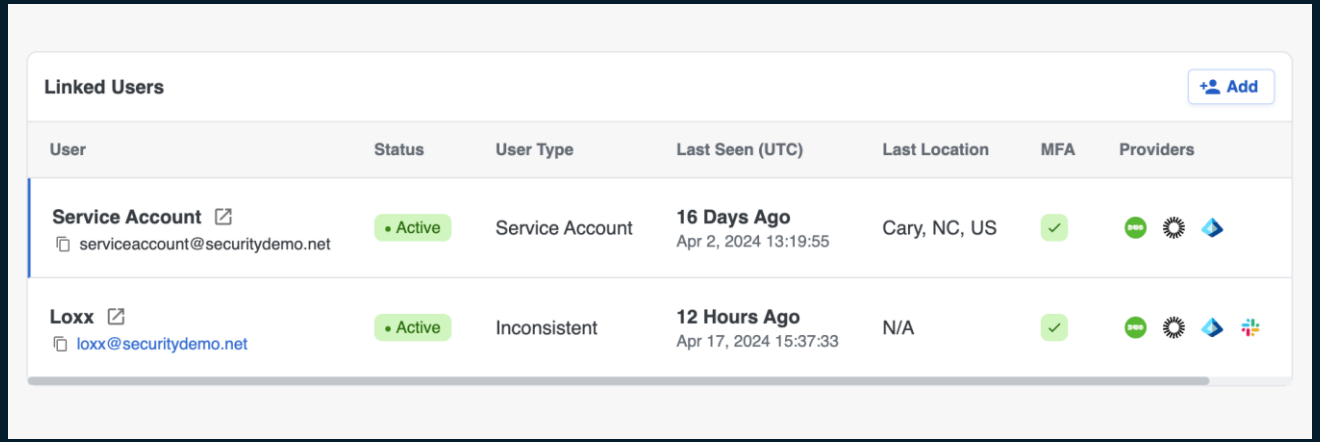


Linking Accounts

Not a merge, a linkage

For example, a privileged admin creates a service account.

That admin leaves company, HR system deletes the user's account; but the service-account will still exist with full privileges!



Suggesting Linkages

Link Suggestions

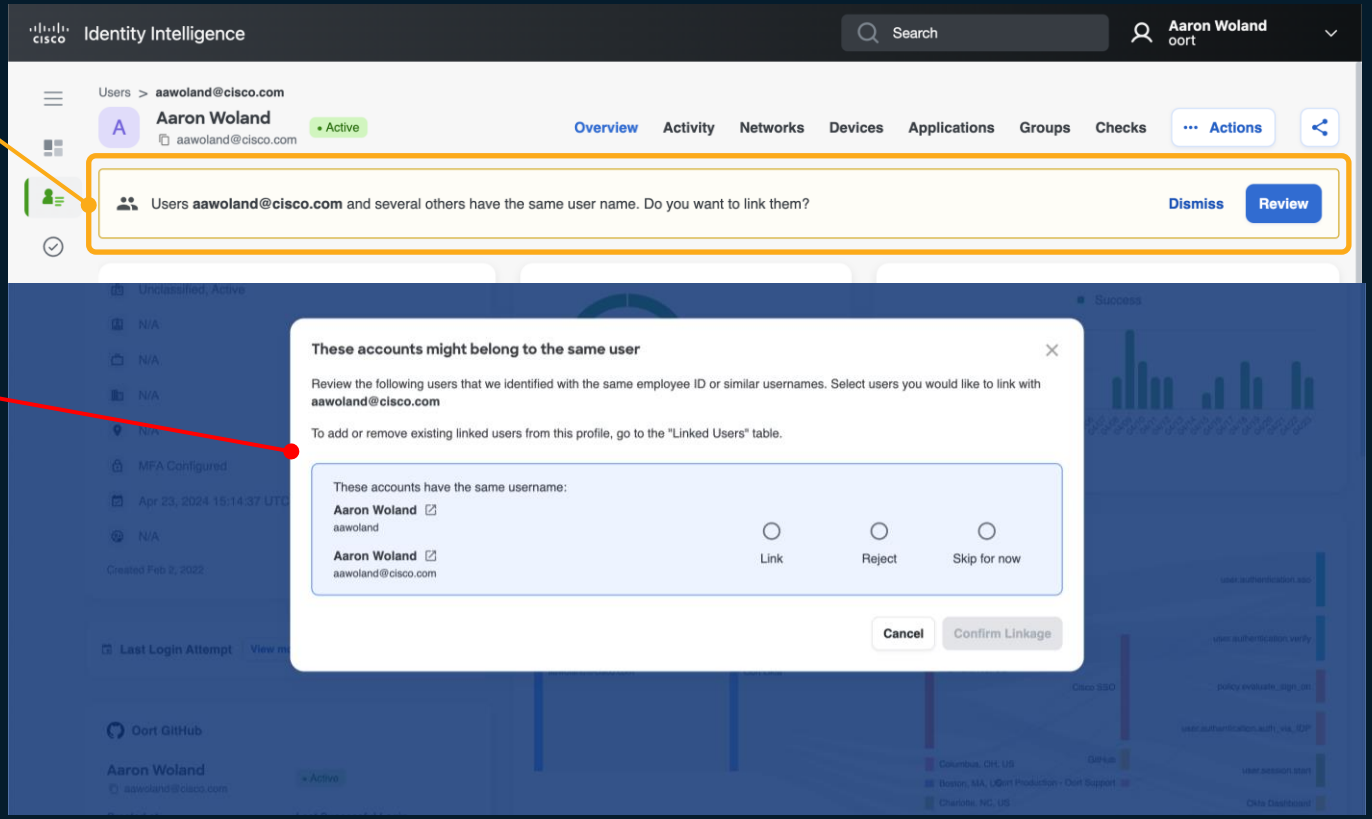
CII will merge accounts automatically.

When it seems similar accounts that aren't mergeable, it will suggest linking.

Link Suggestions

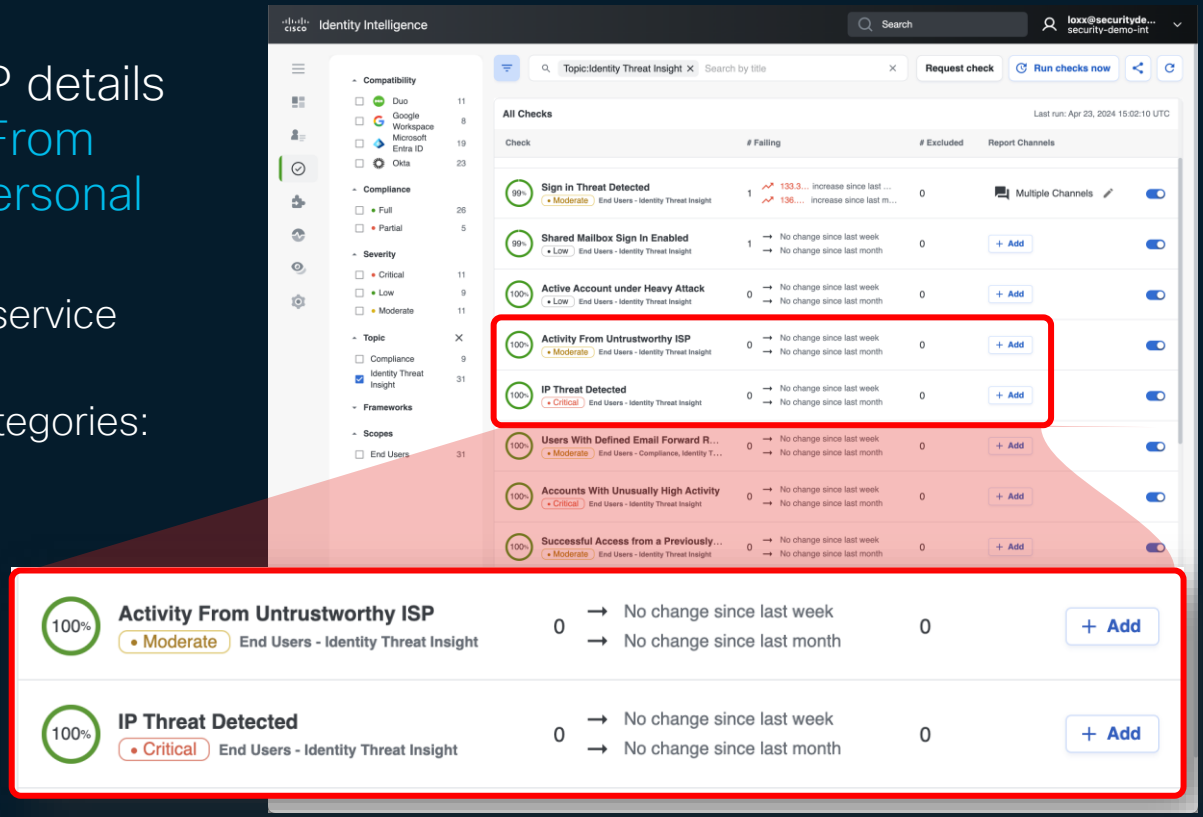
I call this the "Google photos" feature..

Is this the same user?
- Link
- Reject
- Skip for now



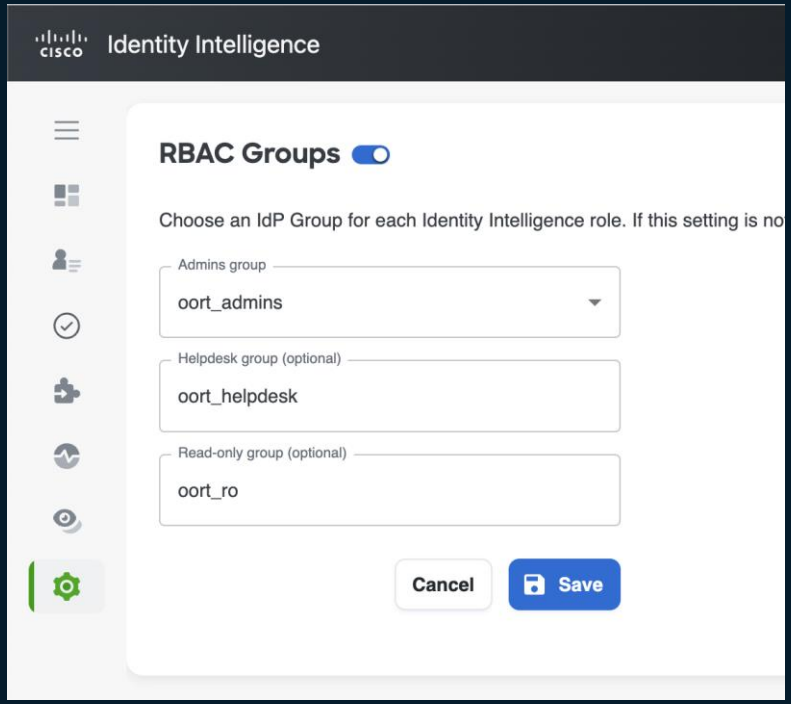
Threat Intel Nuggets

- How CII knows about ISP details for checks like “Activity From Untrustworthy ISP” & “Personal VPN Usage”:
  - CII is using the ASN of the service provider
  - Subscribe to IPInfo feed categories:
    - Hosting
    - Proxy
    - Tor
    - Vpn
    - Relay
    - Service
    - Malicious IP
    - Password Spray



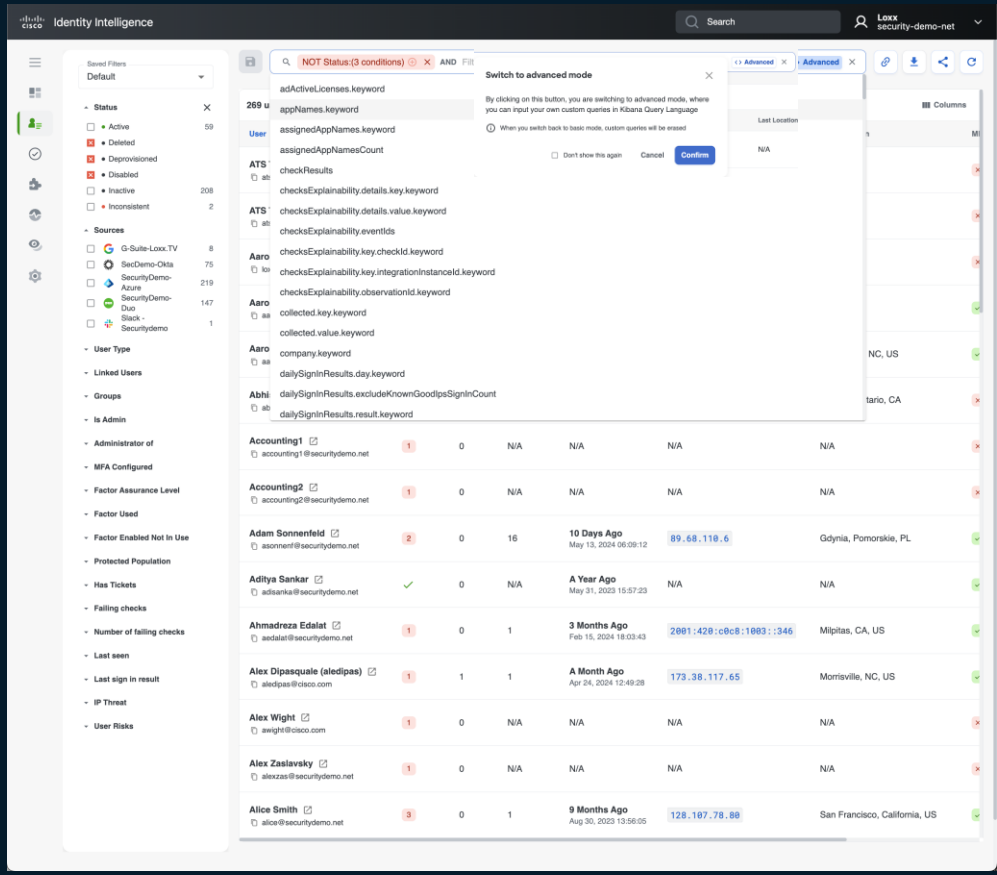
Role Based Access Control

- Three built in Roles:
  - Admins (Full Administrator)
  - Helpdesk
  - Read-only
- Manage roles via groups in the IDP
- No local admin accounts – IDP only

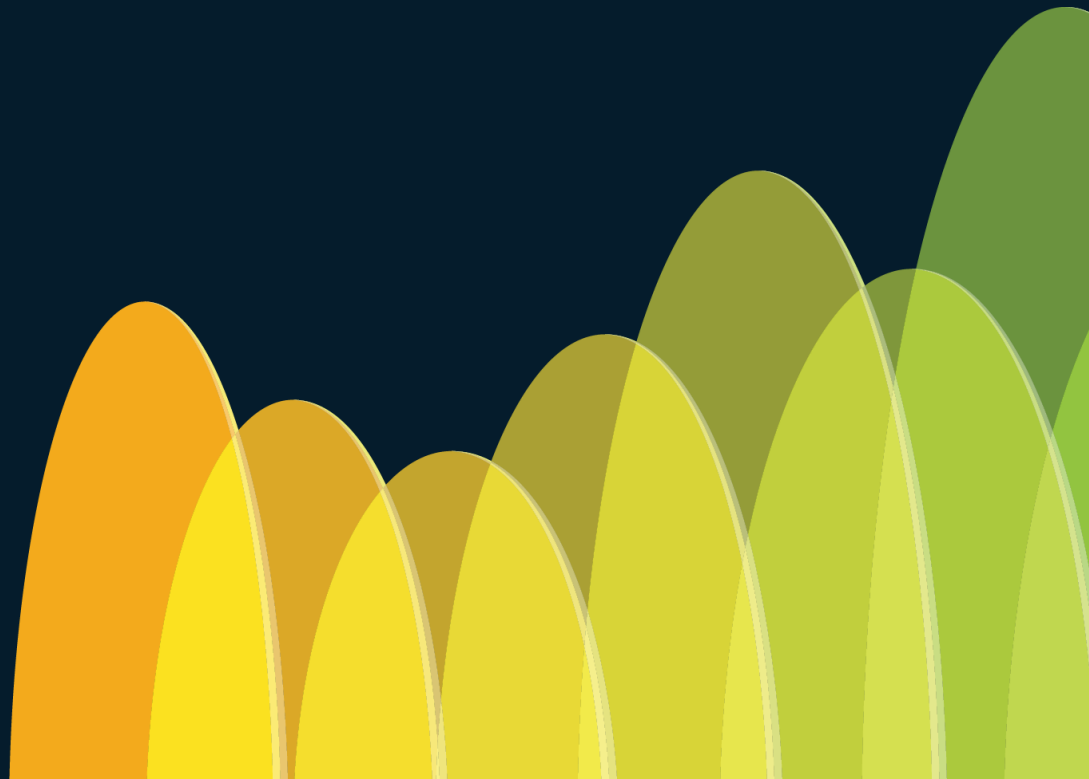


Advanced Search

- Switch to advanced mode
  - Uses Kibana Query Language (KQL)
  - Provides search operators:
    - AND
    - OR
    - NOT
    - _exists_
    - !_exists_
  - Use CTL + Space to get list of advanced query attributes
  - Save your adv queries in the UI!



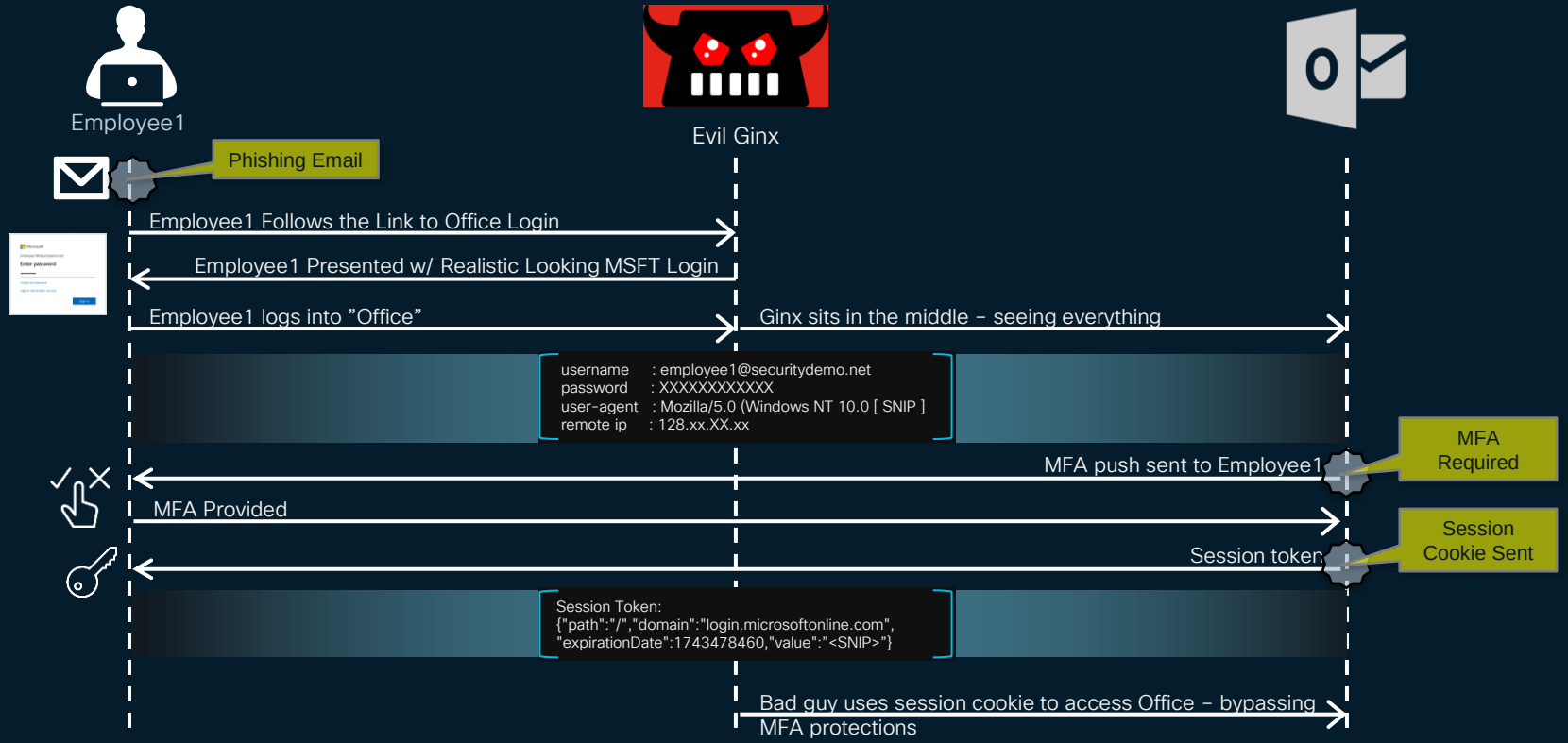
Session Hijacking Example



Session Hijacks are on the rise

- Can be accomplished with a machine-in-the-middle
  - Including malware that is installed on the endpoint
  - The bad-actor collects the session data from the victim
  - Uses the same session keys (Auth, or even Re-Auth tokens)
- These can be signed to last for hours, days, weeks or even longer!
  - The way “Modern Auth” (aka: WebAuth with SAML or OAuth/OIDC) works
  - The authenticating app (service provider) checks the validity of the bearer-token being signed by a trusted IdP w/ a valid lifetime > then issues the session cookie
  - The SP doesn’t check back with the IdP until the session expires!

Session Hijacking Example



What the Bad Actor sees

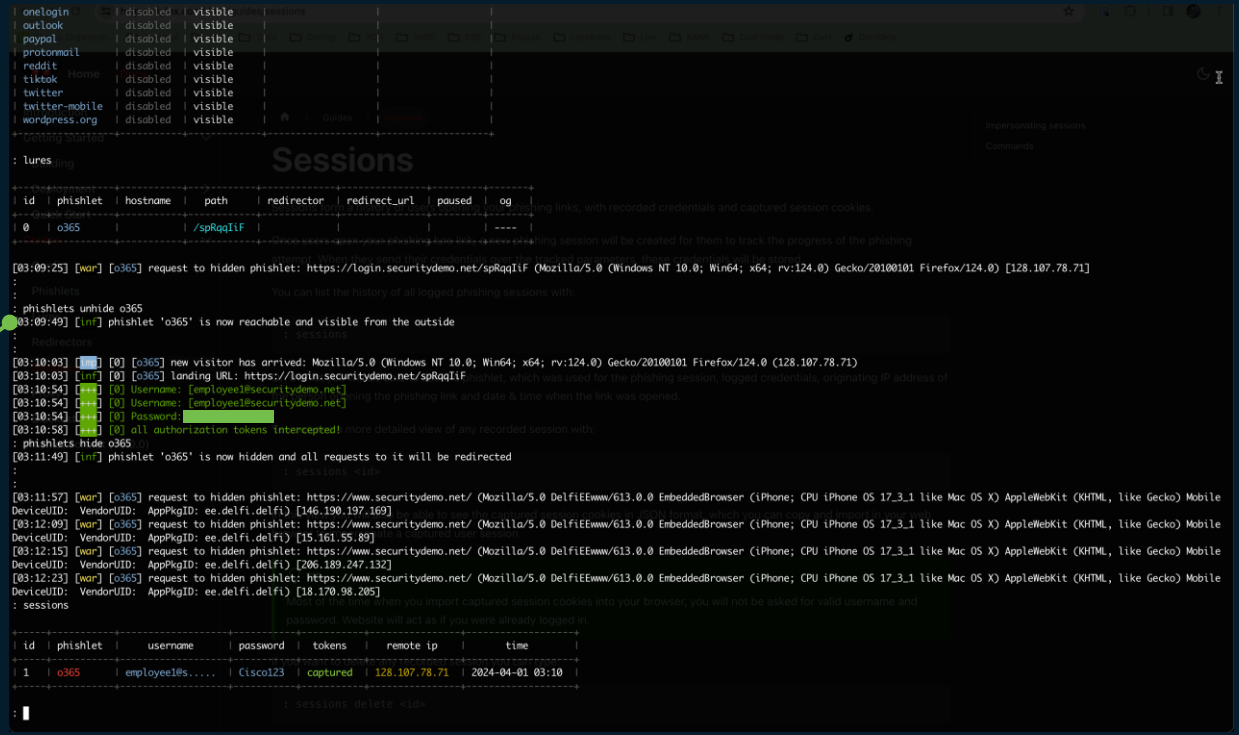
Lure them in

Usually starts with a phishing attack (still #1 vector)

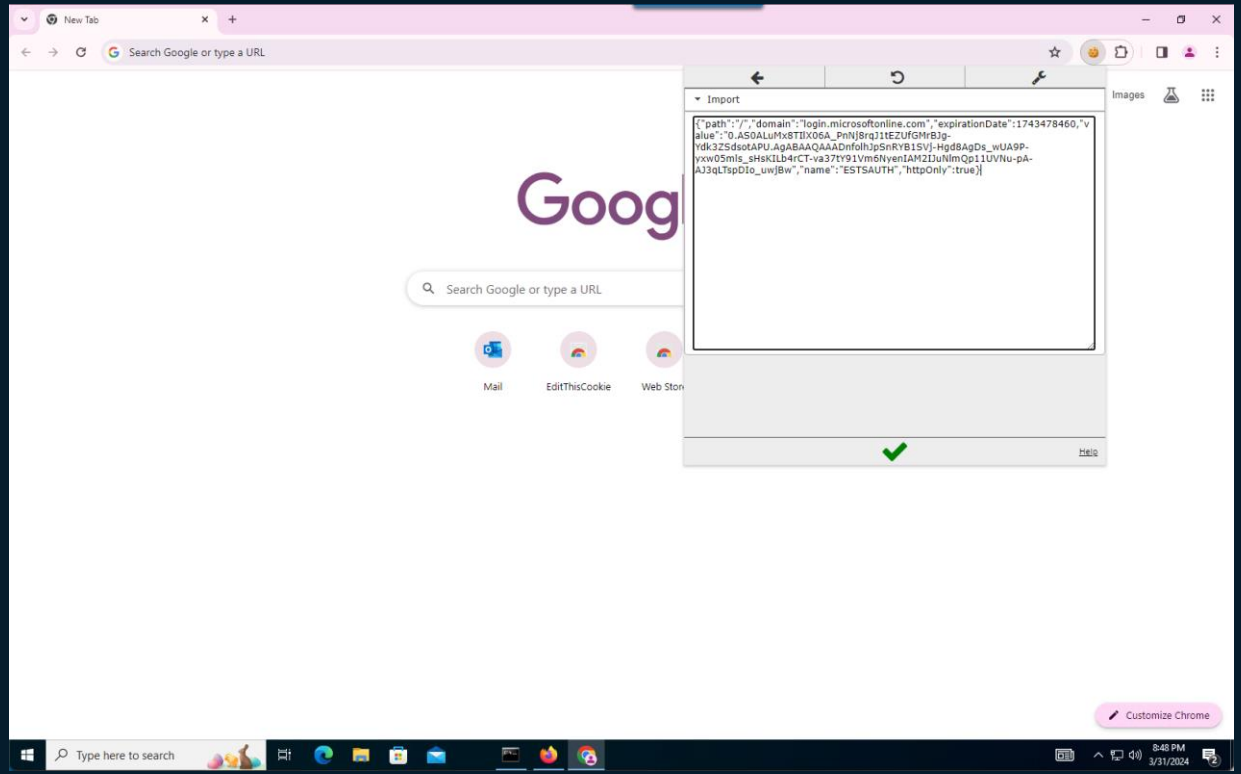
User follows the link & sees what looks exactly like the normal Microsoft Login flow

Bad Guy sees everything

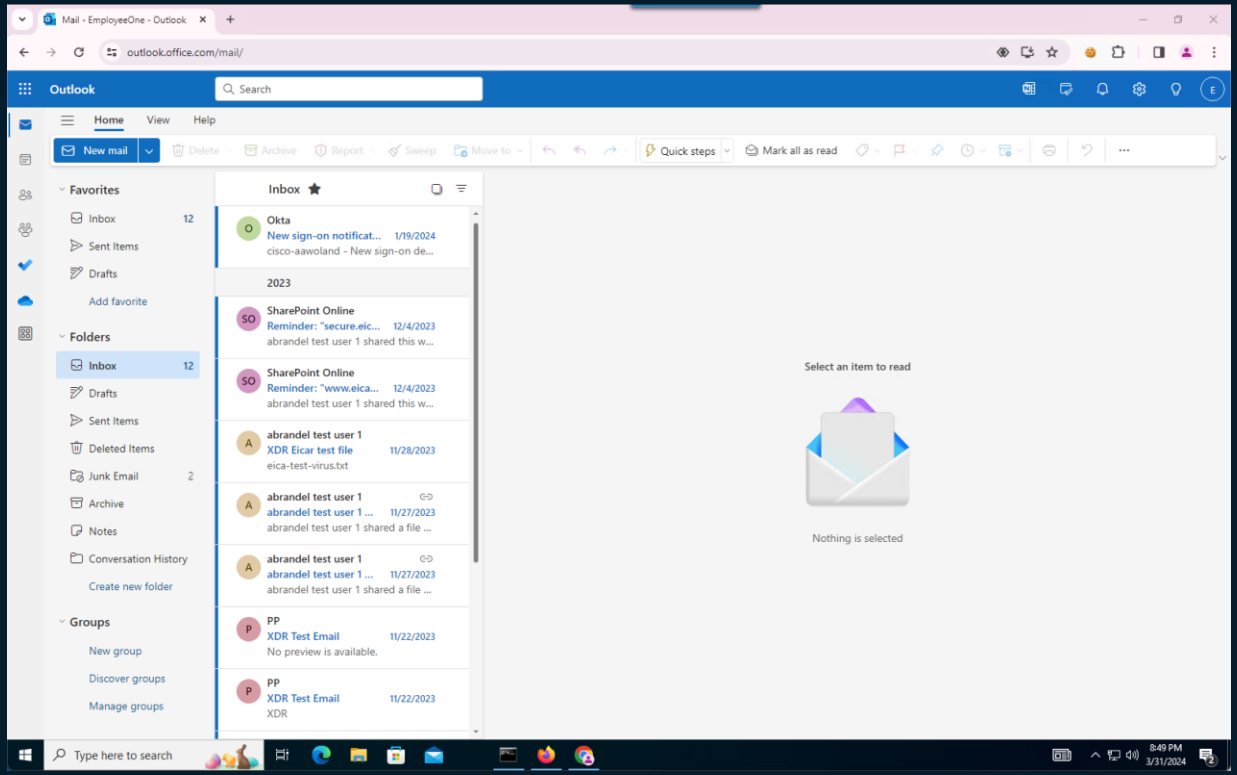
The bad guy is able to capture the username, password (most times) & more importantly the Session Info, including the cookie



Paste the Cookies into a plugin



Bam: Access as Employee1



Technical Nuggets

- With event-streaming, this gets detected much faster than Graph API sync
  - These signals from Entra fall into what are called “real-time checks”
  - Really near-real-time ☺
- Without event streaming it can take over 24 hours to detect this, if at all
- Entra will label these as “Medium" criticality events, even though it was a successful attack
  - Okta & Duo share the session info in their logs & makes it easier to detect

Agenda

- What is Cisco Identity Intelligence
- Integrations & Users
- All about Checks
- Remediations
- Other Technical Nuggets
- User Trust Levels & Posture
- Let’s talk about APIs
- Call to Action

User Trust Level

Who: Cross-Functional Team

Identity Intelligence, Duo, Talos, Secure Access, XDR Threat D&R, and Security Group CTO office

What it Is:

A single value, determined by a user's posture, behaviors, and events over time, for integrating solutions to leverage.

What it's Not:

Not a real-time measurement of risk, but a high-level approximation of the trust level of the account given the users posture and recent events

Not a numeric value!

Trust Level Approach

Trusted
Favorable
Neutral
Questionable
Untrusted

Simplicity

- Distilling down to a single attribute of a user that is shared via the APIs.
- Consuming products will be able to expose this simple property in their policy engines
- Each product does not need to concern itself with the hundreds of checks and values that went into the decision.

Explainability

- Explainability is very important to instill trust.
  - How the score was calculated, and which checks influenced the decision.
- Available in CII User Interface
- Also available from the API

Use Cases

Authentication, Authorization & Access decisions

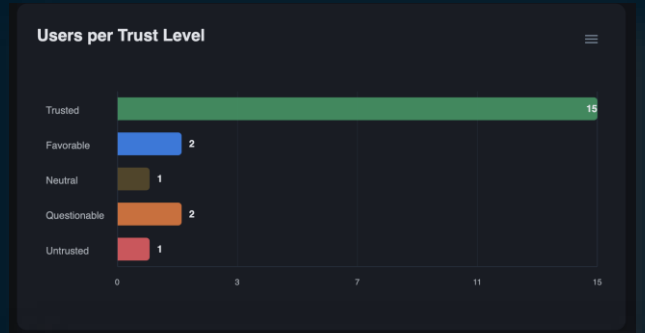
- Leverage the level as a condition of the security policy
- Help limit access for untrustworthy users or at least require additional assurance
- Step-up authentication or require a managed device, too
- Secure Access & Secure Connect, ISE, Firewall, Meraki

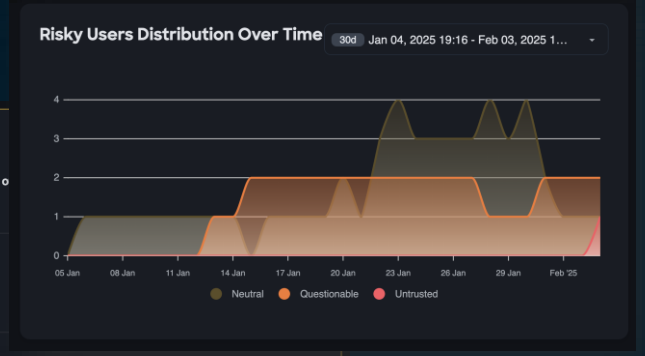
Threat Prioritization

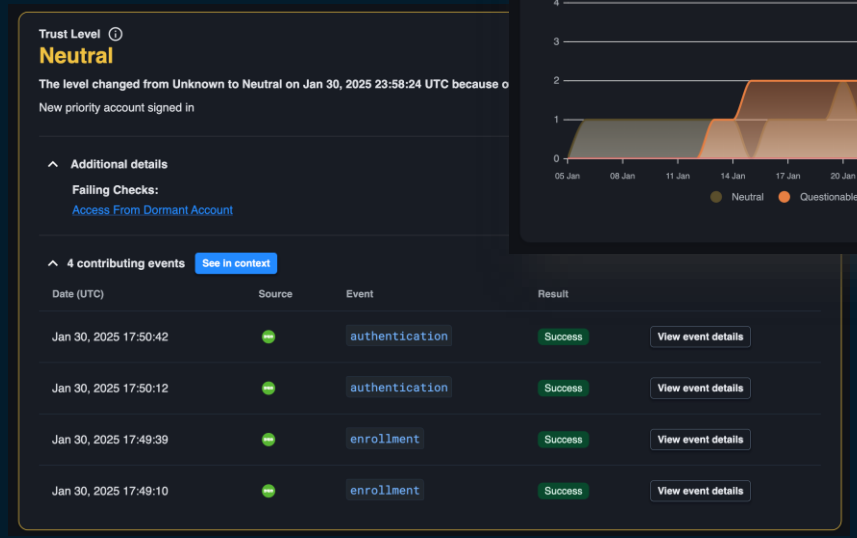
- Help influence the overall severity of a threat.
  - If Trust Level = Questionable or below, Then increase priority of incident (or similar)
- Products: Cisco XDR, Splunk Enterprise Security, Secure Network Analytics

Trust Level Nuggets

- User is assigned a trust level based on activity.
  - No activity = no level
  - Explainability shows why a user has the assigned level







Trust Level as Criteria in Security Policy

- Example of a basic security policy that is using Trust Score as one of the Criteria

Trusted
Favorable
Neutral
Questionable
Untrusted

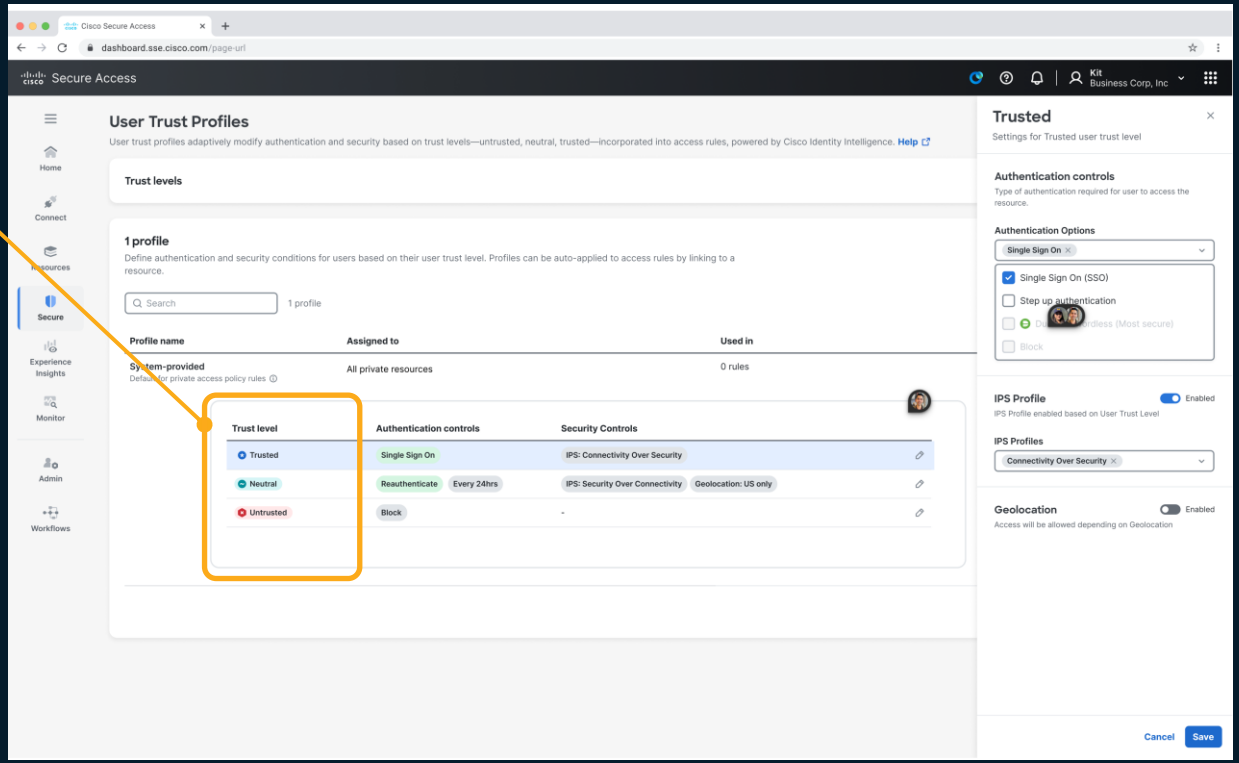
Source Criteria					Destination Criteria:			Result
IP Addr	User / Groups	SGT	Service	Trust Level	IP Addr	SGT	Service	Action
any	Big-Shots	-	any	Favorable+	any	HR Systems	https	permit
any	any	Employees	any	Questionable +	any	Helpdesk	https	permit

Example Wireframe: Secure Access

Trust Levels

Secure Access will influence their access policies with the Trust Levels of each user.

Note: this is not the final design

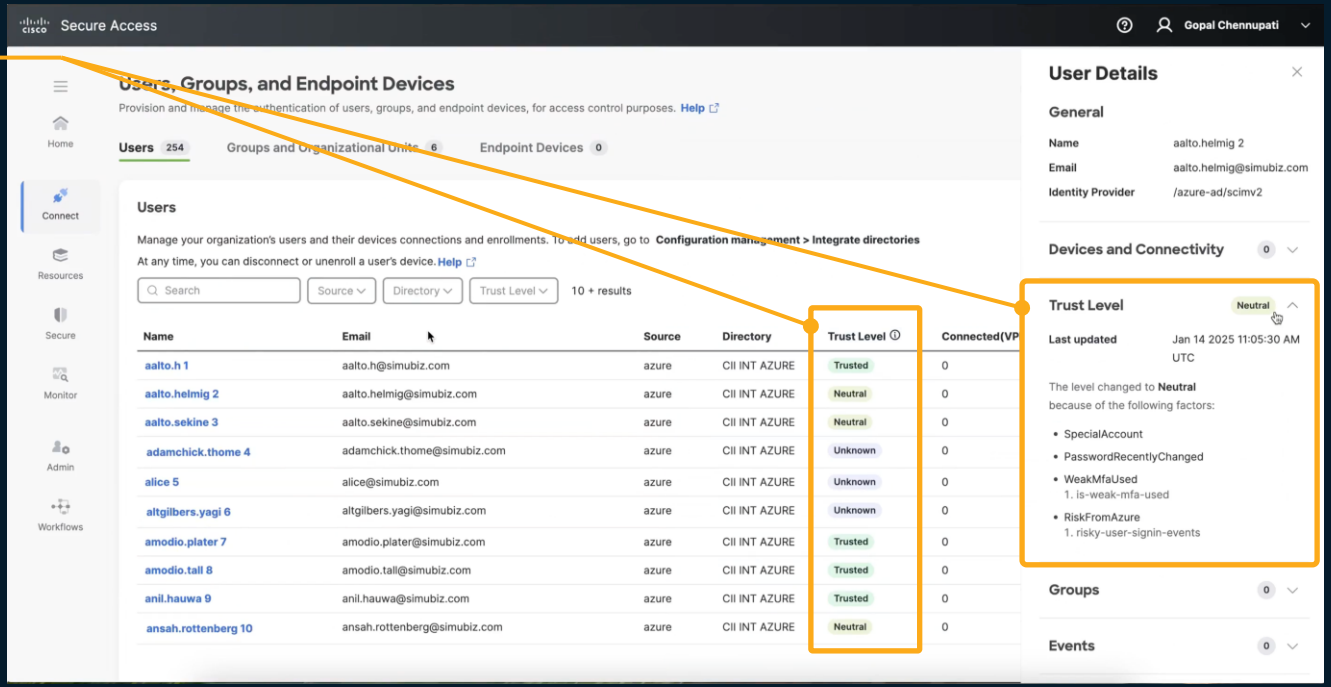


Users in Secure Access are flagged when risky

User Risks

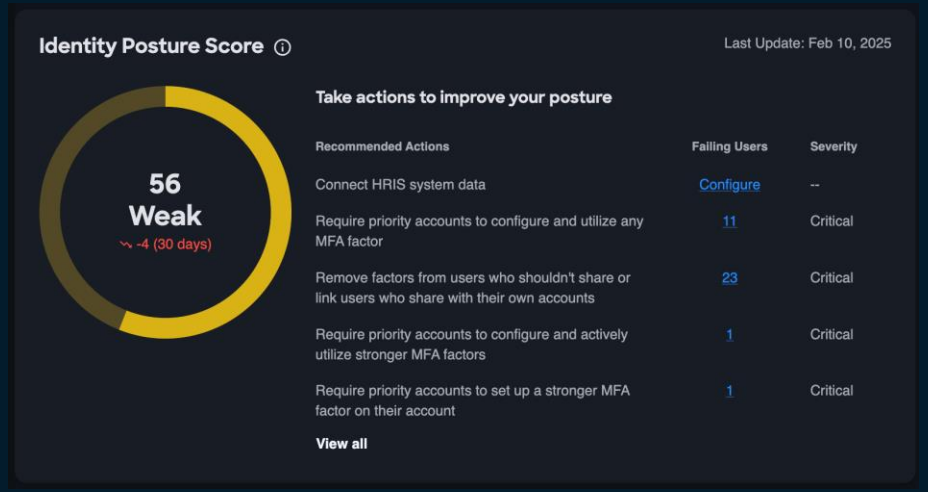
The users that have been synced to Secure Access from the Directory – now have context related to their threats discovered by CII

Screenshot from Early Trial. Final screens may be slightly different.



Identity Posture

- The overall level for your organization
- Provides a “guide” to gamify the cleanup of your ID environment & policies
- Can use the trend to ensure your organization is going in the right direction



Identity Posture

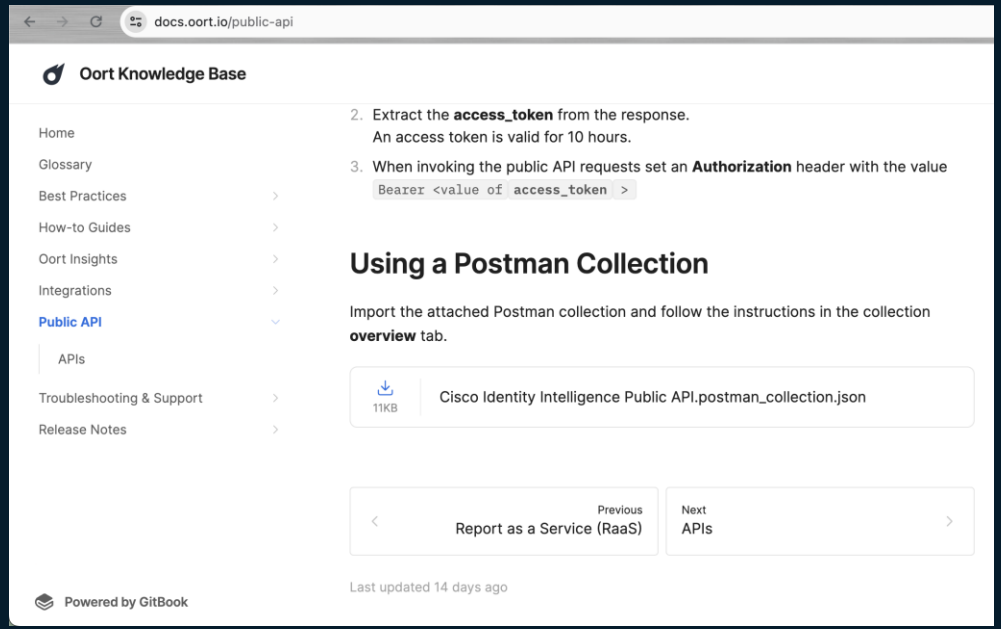
- The overall level for your organization
- Provides a “guide” to gamify the cleanup of your ID environment & policies
- Can use the trend to ensure your organization is going in the right direction

Agenda

- What is Cisco Identity Intelligence
- Integrations & Users
- All about Checks
- Remediations
- Other Technical Nuggets
- User Trust Levels
- Let’s talk about APIs
- Call to Action

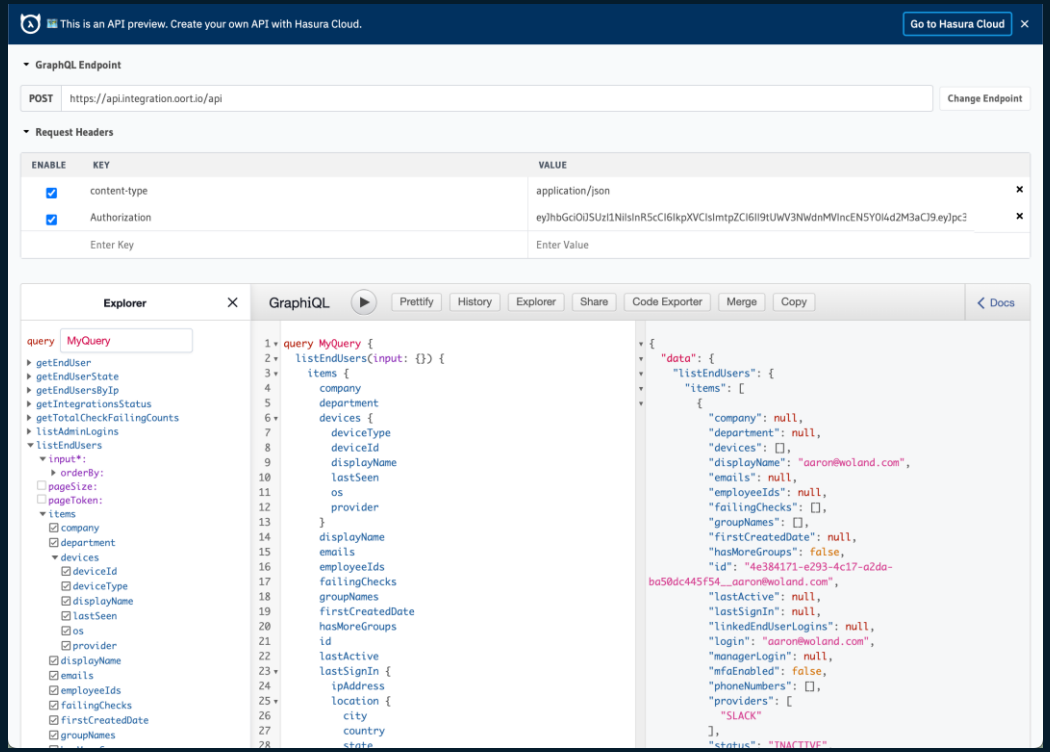
CII Public API

- https://docs.oort.io/public-api/apis
- GraphQL based API
  - Why graphQL – don't have to send EVERYTHING in the response..
  - Your request is structured as a query & CII sends only what you ask for.
- GraphQL self-documents its schema
- CII provides Postman collection, downloadable right from documentation



GraphQL Explorer Tools

- Hasura GraphQL Explorer
  - Wraps around the open_source GraphiQL UI
  - Exposes an “explorer” that allows you to check-off the fields you want, in order to build your specific query
  - https://cloud.hasura.io/public/graphiql?endpoint=[INSERT_URL]



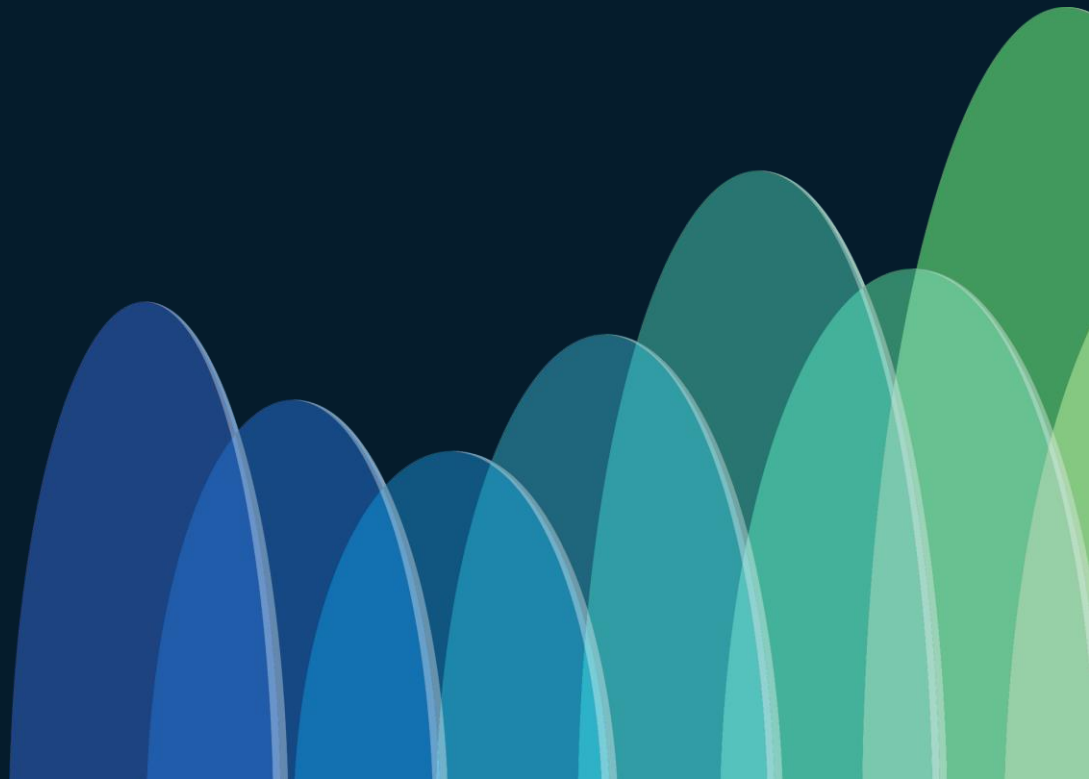
Agenda

- What is Cisco Identity Intelligence
- Integrations & Users
- All about Checks
- Remediations
- Other Technical Nuggets
- User Trust Levels & Posture
- Let’s talk about APIs
- Call to Action

Call to Action

- Login to the CII demo tenant (“Genie”) & get a feel for Identity Intelligence
  - Sign in with a social login option (Gmail, LinkedIn, etc)
- Provision your own CII tenant from Duo
  - Included with Duo Advantage or above
  - Free trial of Premier Edition
- Free Identity Security Assessment

Q & A



Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

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

Webex spaces will be moderated by the speaker until February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.


cisco
Thank you
cisco Live!