Identity Intelligence Demystified

Technical deep dive into CII (formerly Oort)

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

Session ID: BRKSEC-2162

Cisco Webex App

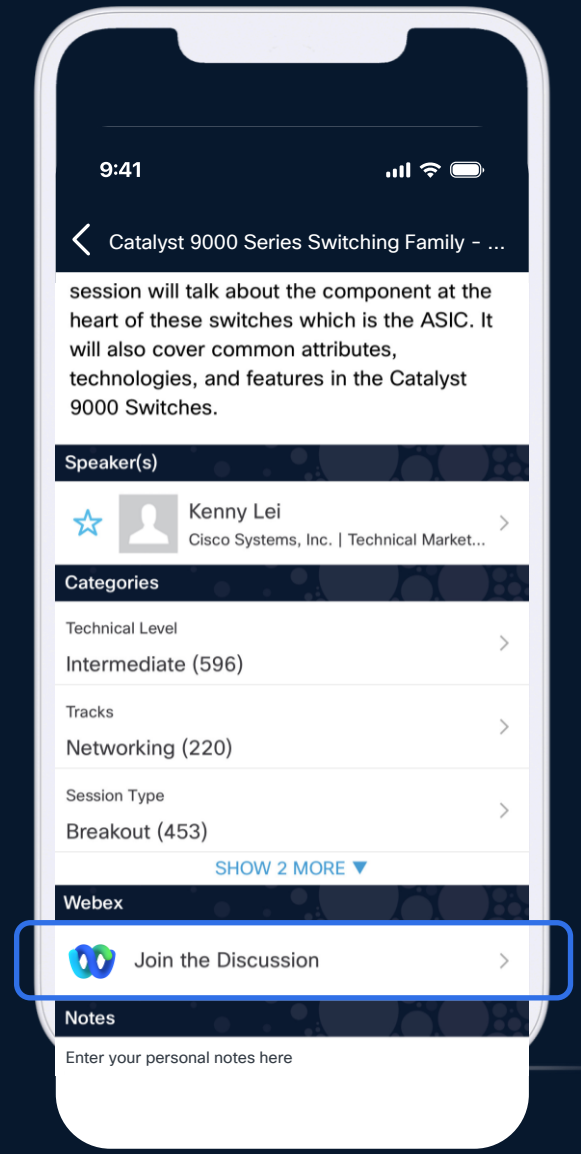
Questions?

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 14 November 2025.



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

ABSTRACT

- Modern Auth and SSO explained for Network Engineers

- AAA: Authentication, Authorization & Accounting does not mean “RADIUS”.

  Those of us in Network Security are usually familiar with 802.1X and authenticating to networks for wireless, wired, and even VPN. AAA is a principle, not a product.

  The concepts are universal and still apply when you hear the “new” authentication protocol types like: OAuth, SAML, OIDC, FIDO, etc. This session will focus on explaining modern web-based authentication protocols & teaching about them in a way that compares & contrasts them to network security authentication methods. In other words: come learn about the latest in authentication protocols and how to understand them with your networking background. If you know all about SAML & OAuth already, but don’t understand 802.1X or EAP – this session is also for you!

- Aaron Woland, an expert leader from Cisco's Duo Security business, will entertain you while educating you on this important and growing area of security.

$whoami

Cisco role:	Distinguished Engineer, Identity Security
Unofficial title:	“Cisco History Professor”
What do I do:	Focus on New Stuff
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 4!

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

If there is anything we can improve, please let us know!

Agenda

01 What is Cisco Identity Intelligence

02 Identity Security Posture

03 Monitoring Auth Factor Progression

04 Threat Detection & Response

05 User Trust Levels

06 Identity Security Assessments

07 Putting the “R” in ITDR

08 Call to Action

Cisco Identity Intelligence: What & why is it?

Identity Threat Detection & Response

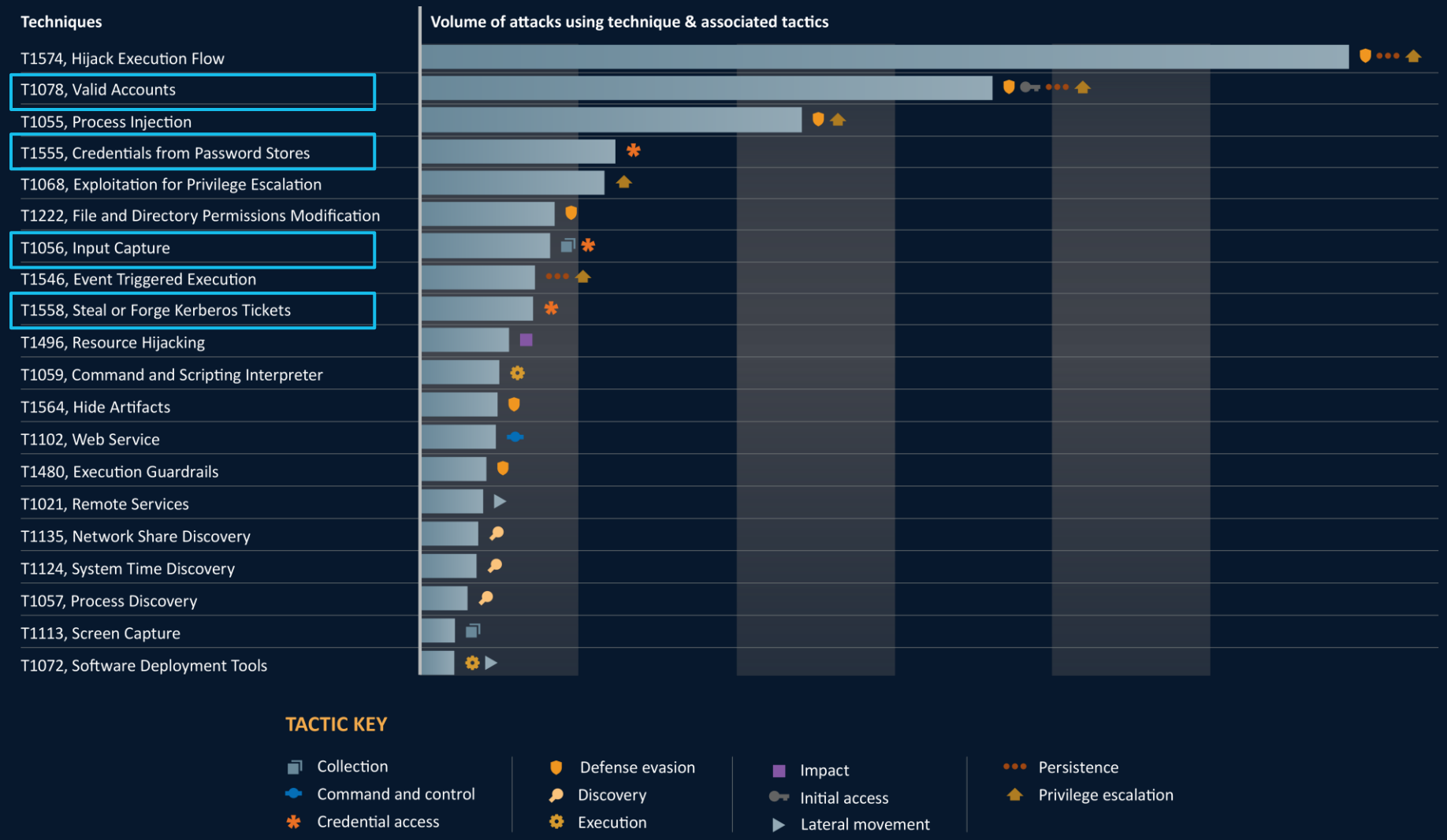
...a security discipline that encompasses threat intelligence, best practices, a knowledge base, tools, and processes to protect identity systems. It works by implementing **detection mechanisms**, **investigating suspicious posture changes and activities**, and **responding to attacks** to restore the integrity of the identity infrastructure...

Gartner

Top MITRE ATT&CK techniques

For Your Reference

Volume of attacks using technique and associated tactics

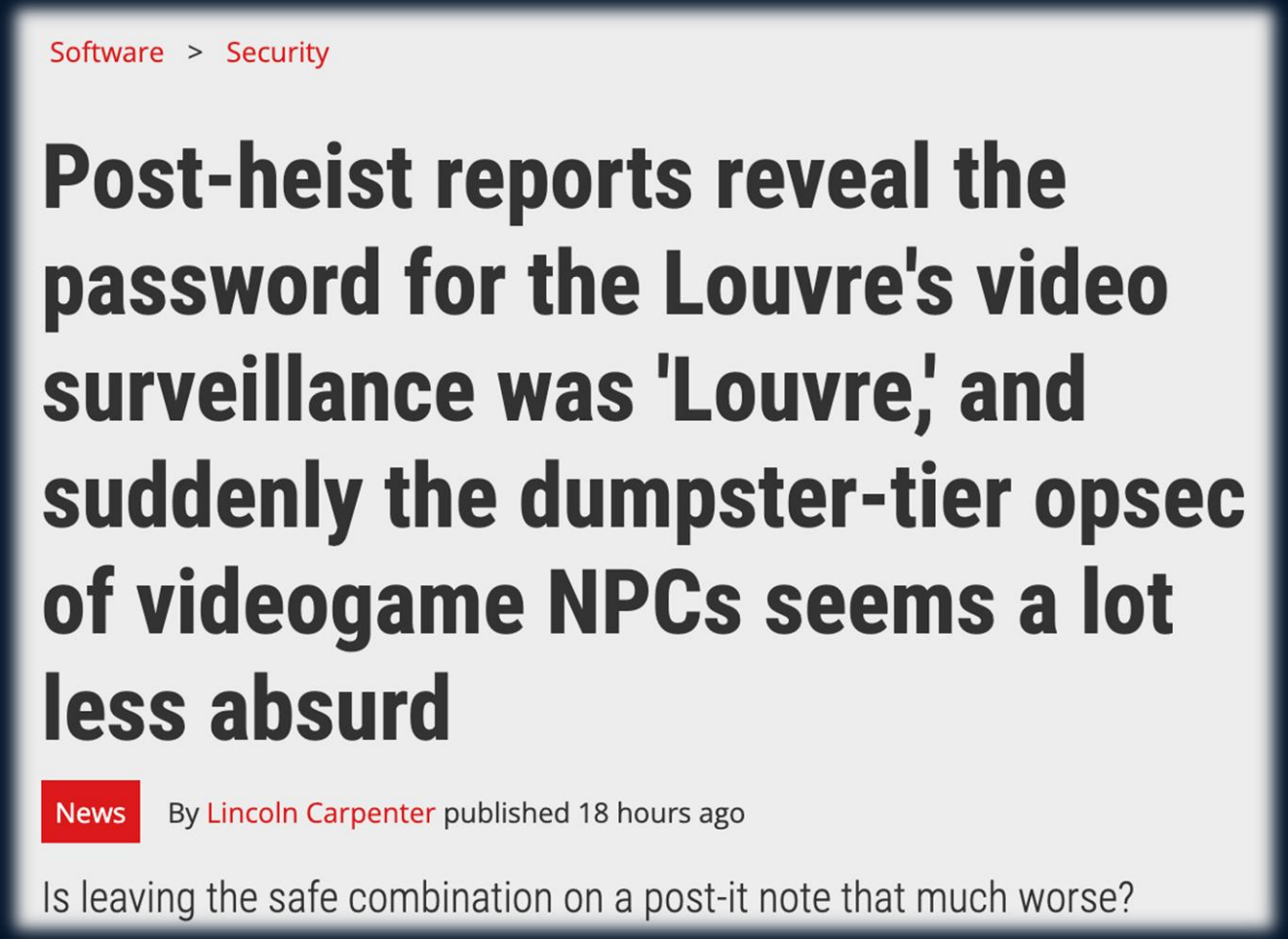


Source: Cisco Secure Endpoint

Identity has become the attack surface

Identity has become the attack surface

Strong MFA is Critical!



Software > Security

Post-heist reports reveal the password for the Louvre's video surveillance was 'Louvre,' and suddenly the dumpster-tier opsec of videogame NPCs seems a lot less absurd

News By Lincoln Carpenter published 18 hours ago

Is leaving the safe combination on a post-it note that much worse?

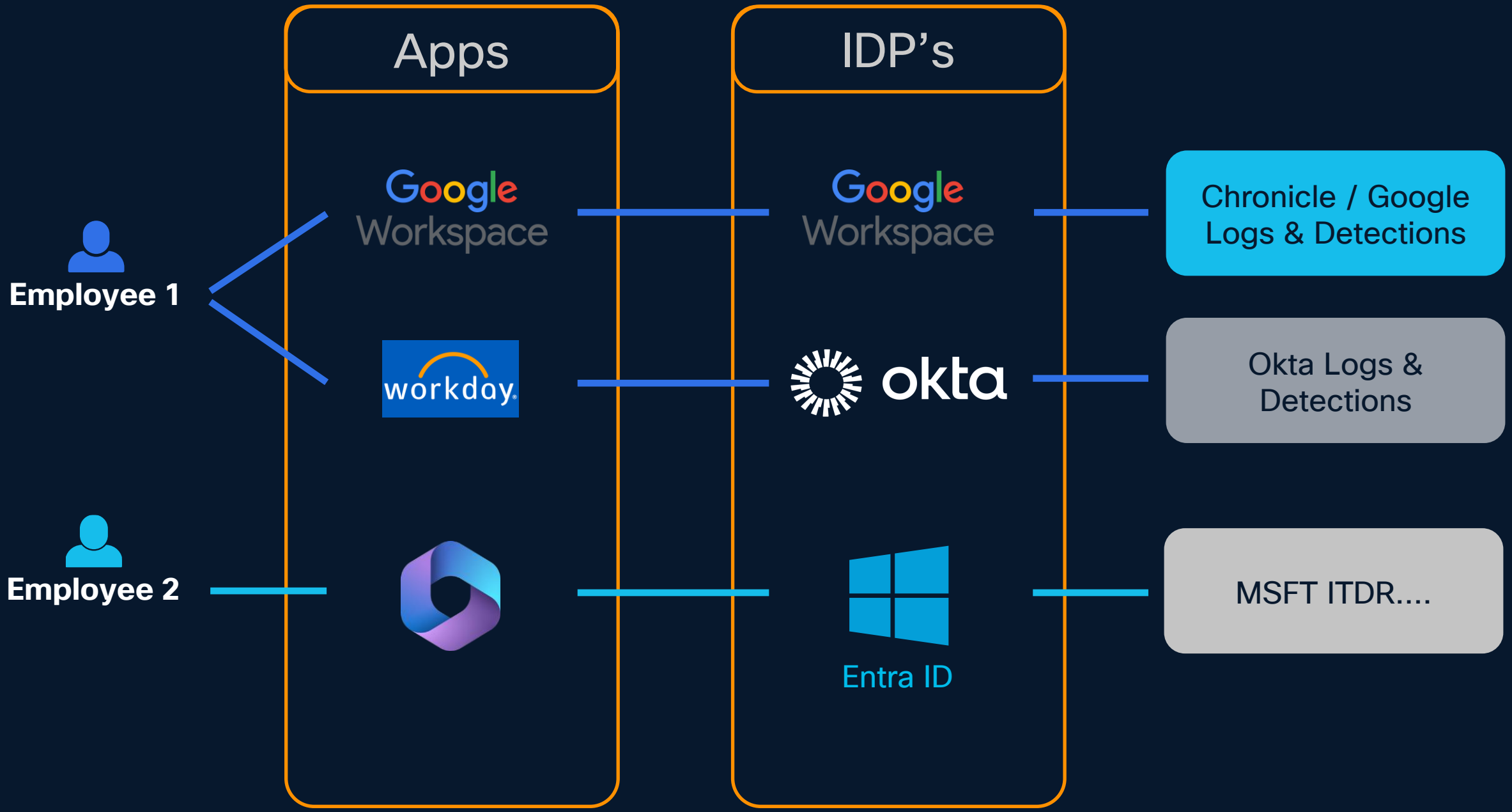
of breaches
leveraged identity
as a key component

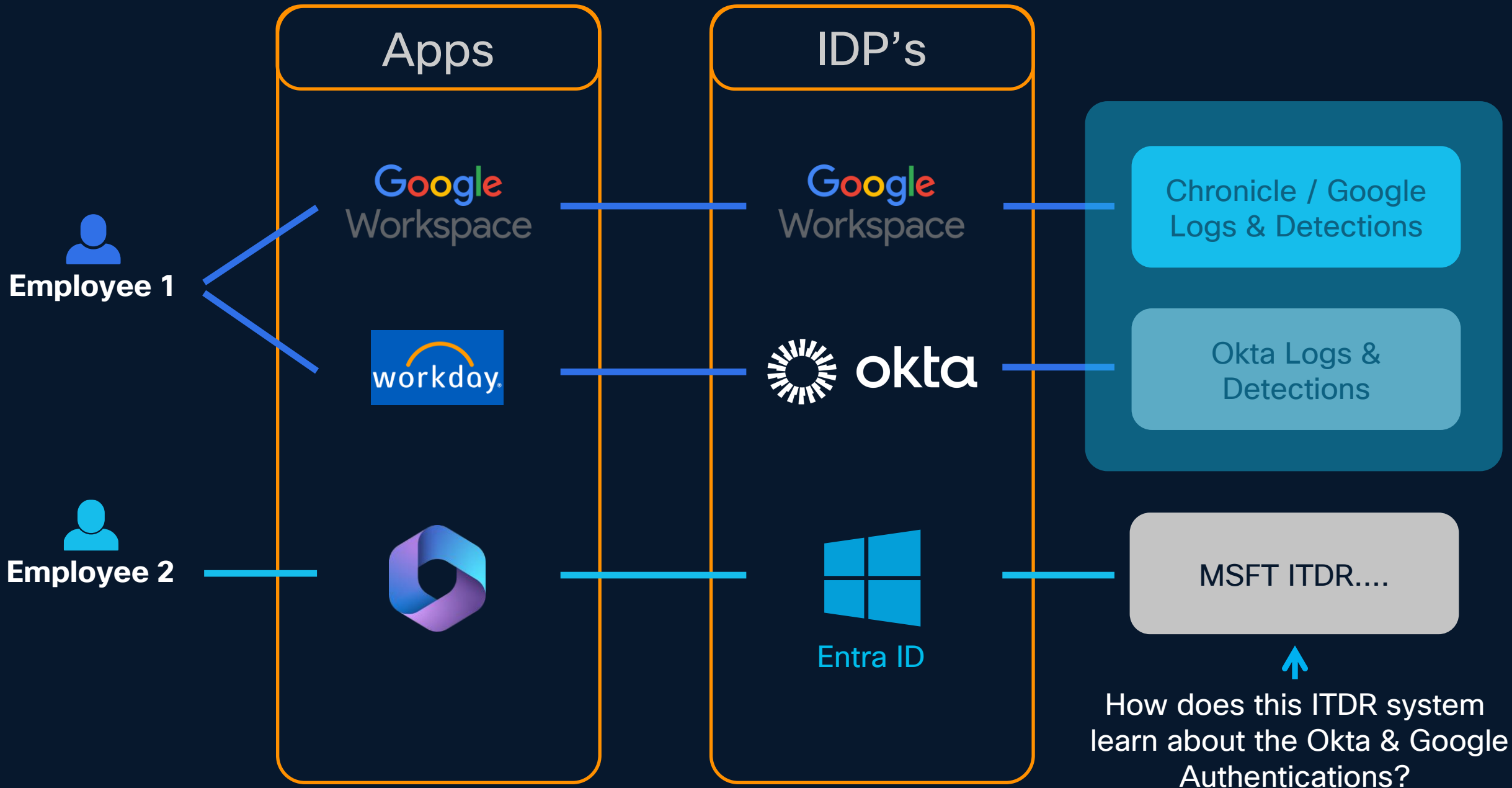
Cisco Talos Incident Response | Year in Review 2024

Breaches Occur: Fatigue with MFA “Nag”

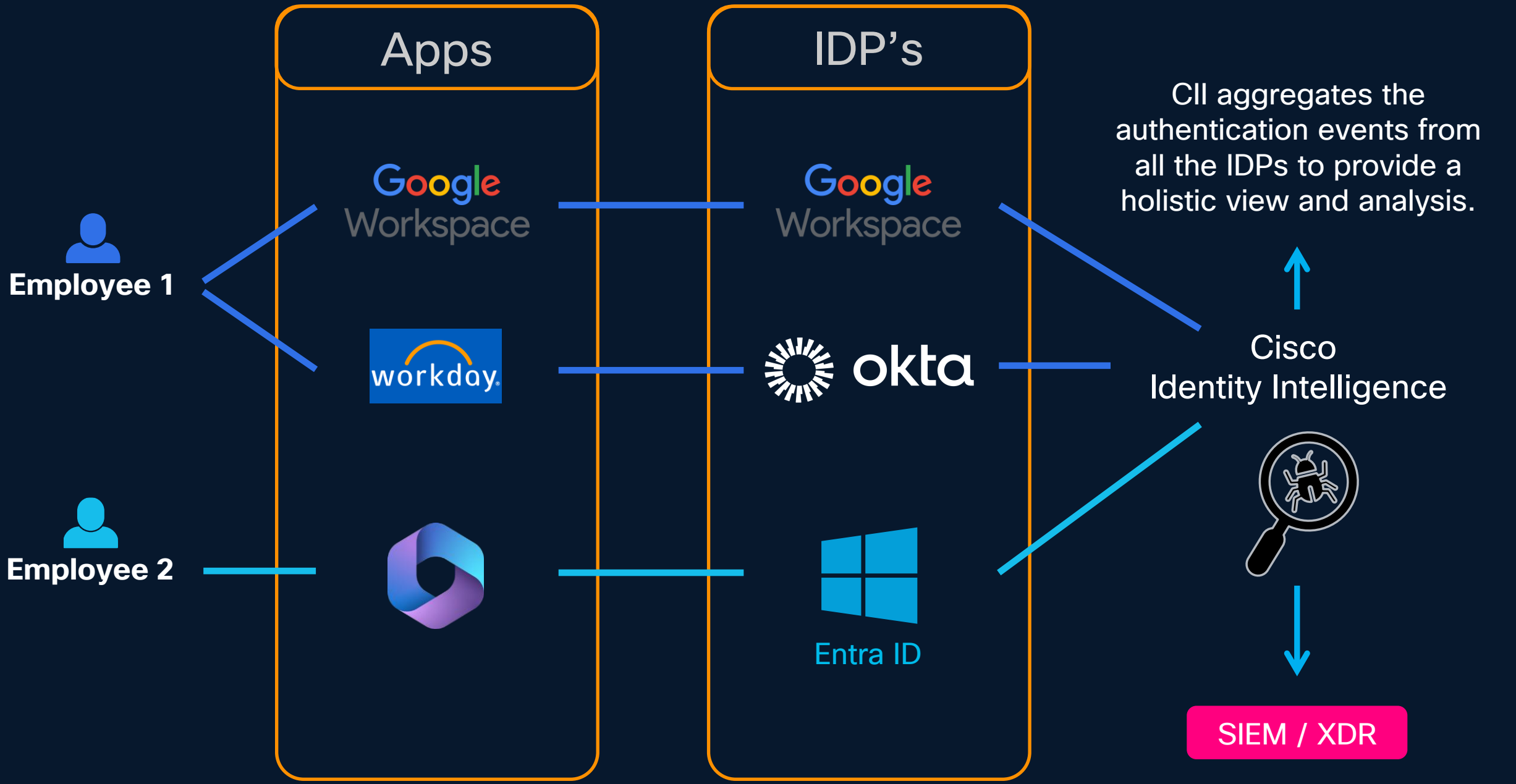
Credit: Wizer Security
https://www.wizer-training.com

You cannot detect what you cannot see!





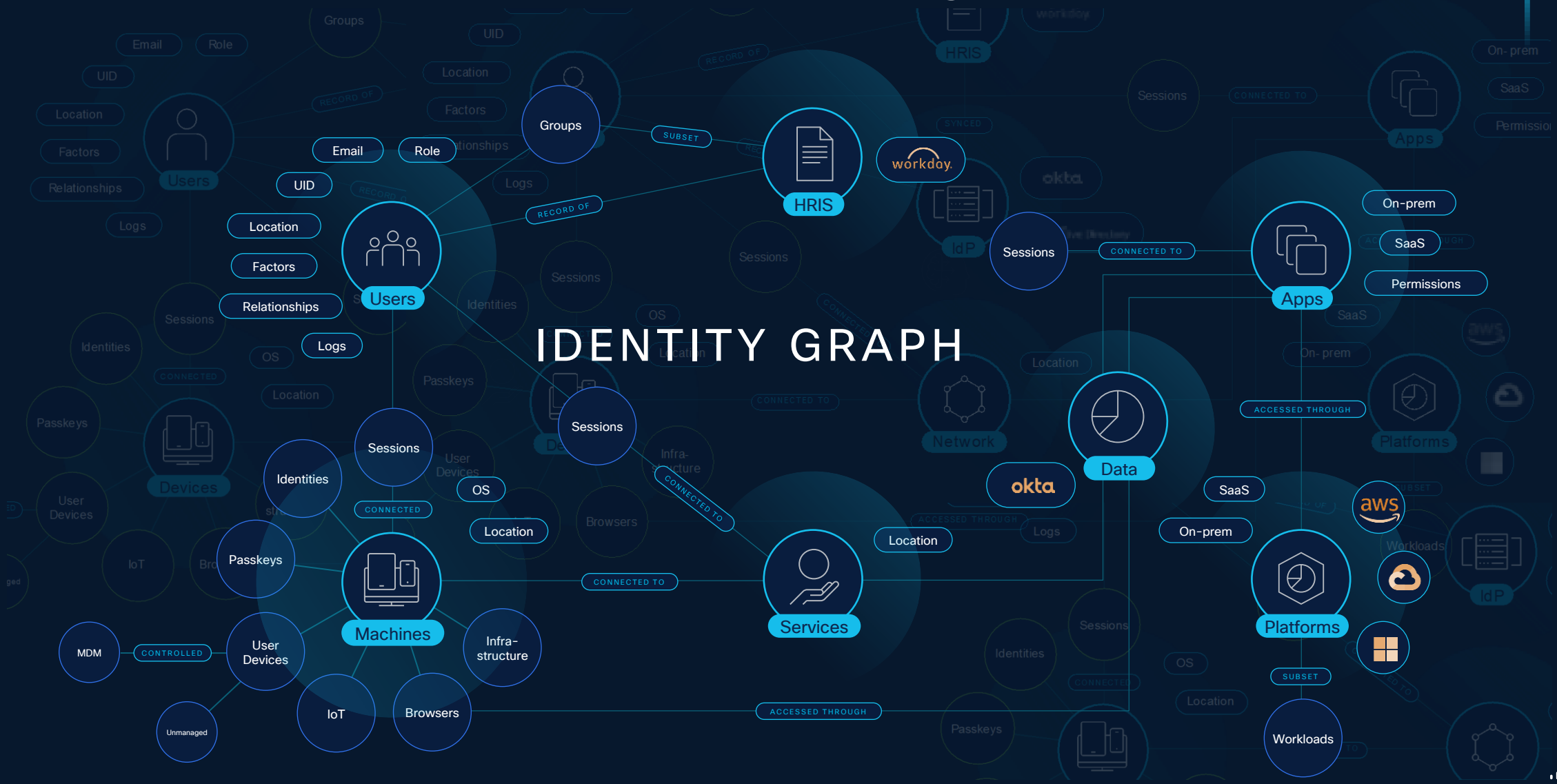
“But I send all of this to my SIEM…”



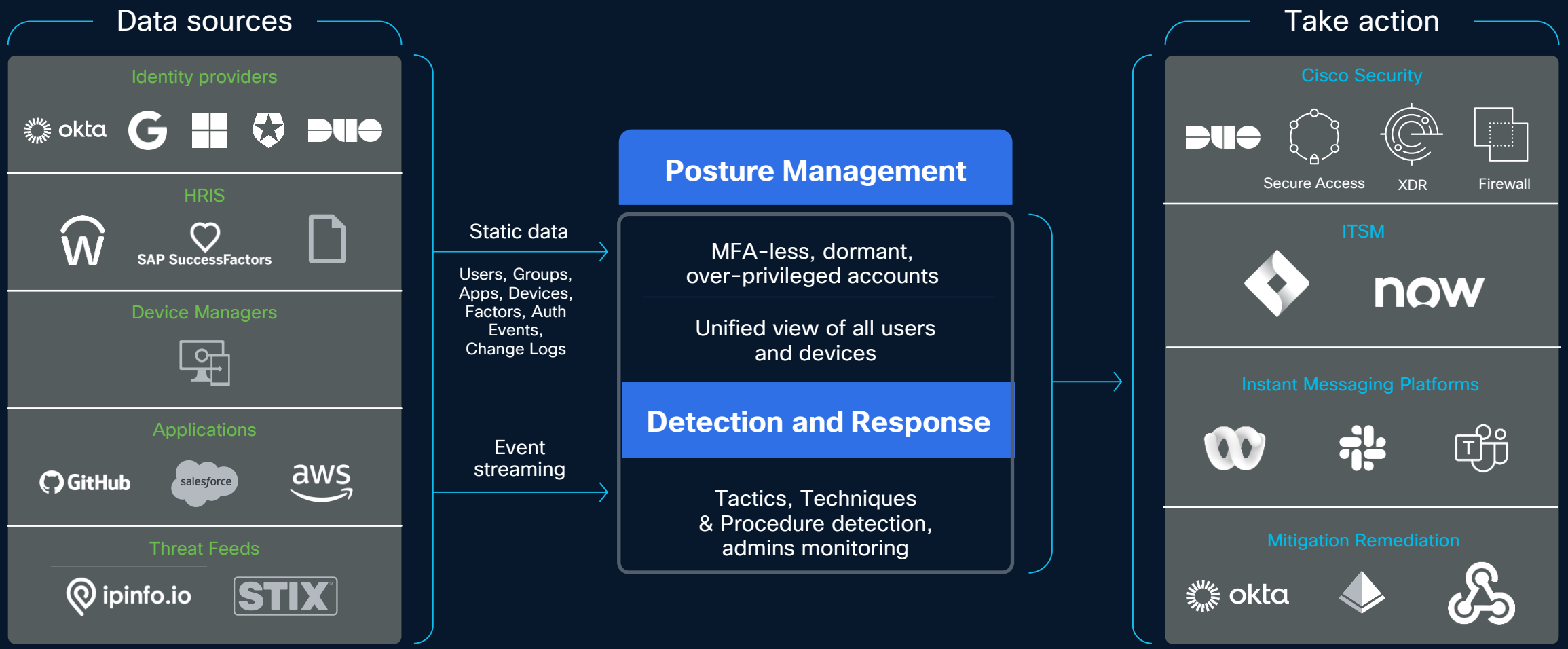
Cisco Acquires

Now Cisco Identity Intelligence

Cross-Platform Insights



Powerful insights for visibility, posture, detection and response



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

Integrations are the life's blood of CII

Identity Providers

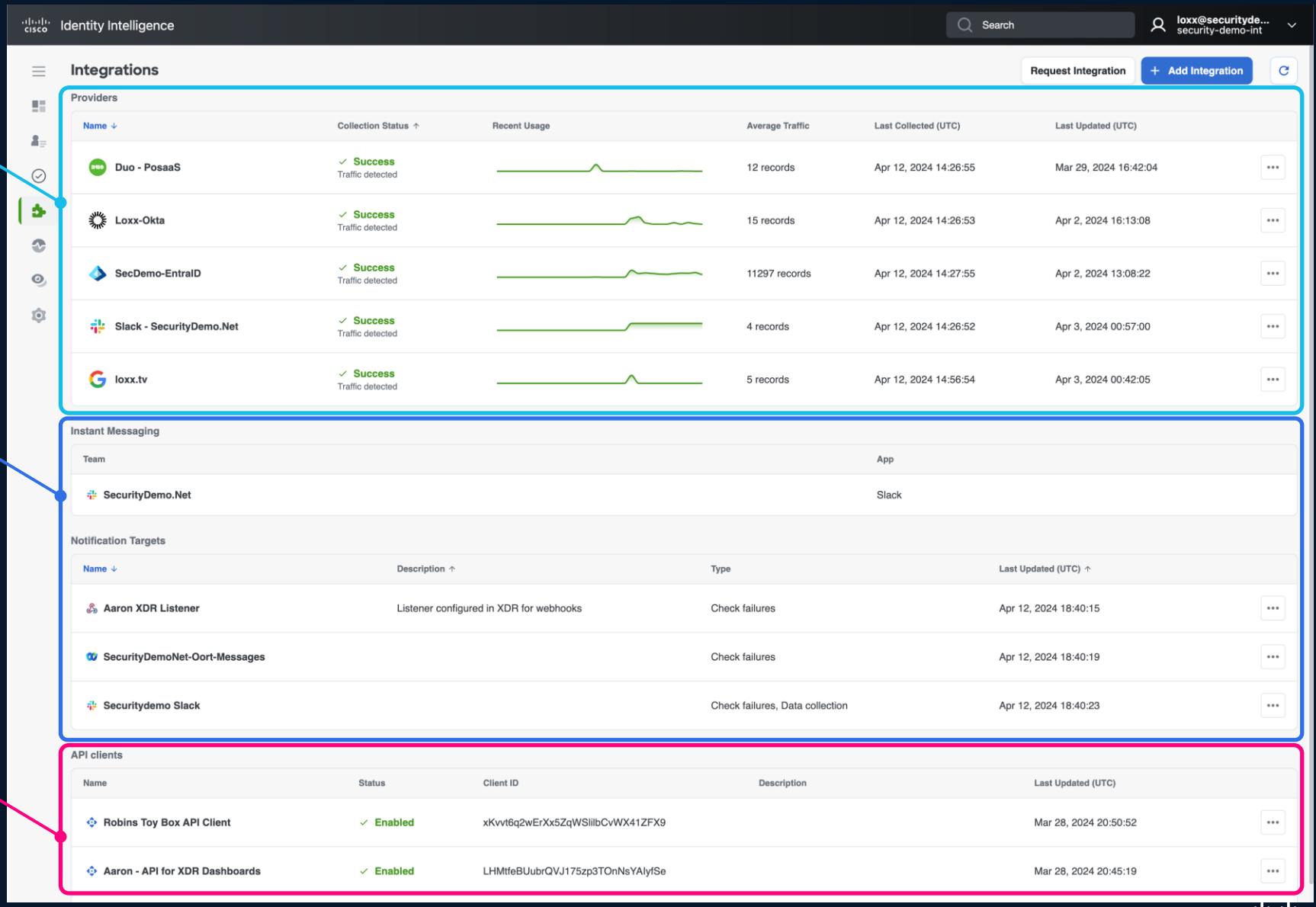
CII integrates w/ many key (cloud-based) ID sources already. These integrations are complex in nature.

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



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.

Wait... Why not just use the IDP?

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

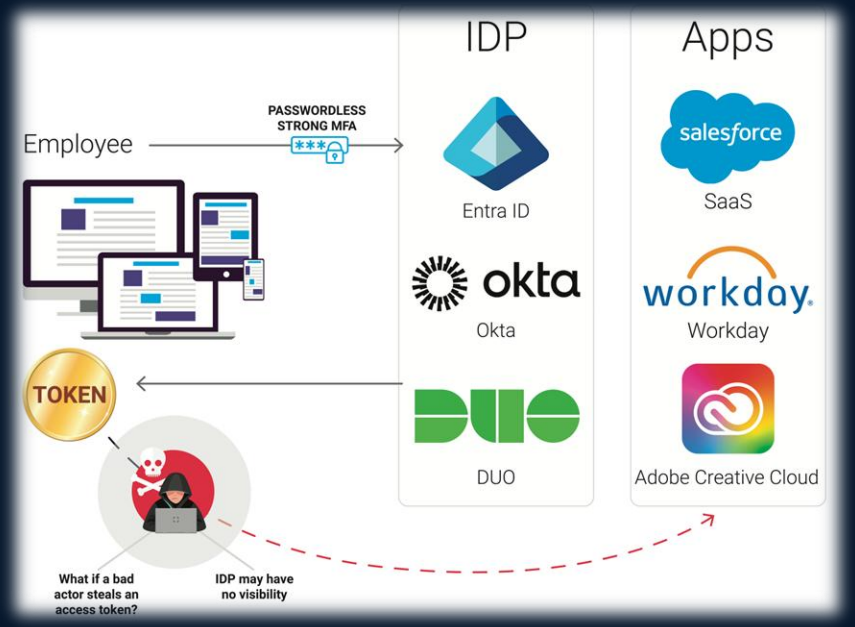
“CII gets great insights from Entra, and I cannot believe how bad Entra is at using their own alerts”
– Fortune 100 Manufacturing Co

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

Large MSP Business

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.

Rapid GTM motion with their MSSP customer base...



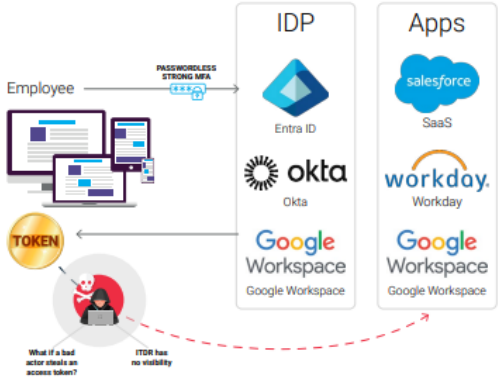
ConRes
IT SOLUTIONS

Strengthen your Identity Security with ConRes

Identity Intelligence enables organizations to adopt a proactive and comprehensive approach to identity security, effectively defending against evolving digital threats.

With 80% of security breaches involving identity vulnerabilities, threats like token theft and session hijacking have become increasingly common. Maintaining robust identity security is a critical part of operating in a complex business landscape, but the nature of security has changed. Remote and hybrid work has challenged the traditional attack surface, so organizations must make a shift.

ConRes Identity Intelligence offers a sophisticated solution that integrates with existing identity infrastructure to bolster security across platforms.



Key Features of Identity Intelligence

Comprehensive Analytics and Monitoring

Provides actionable insights and shifts organizations from reactive to proactive security strategies. It enhances visibility into your

Advanced Threat Detection

Utilizes sophisticated detection capabilities to monitor and alert security teams about threats like MFA fatigue attacks and Adversary-in-the-Middle (AiTM)

Rapid Response Integration

Seamlessly integrates with essential SOC tools, facilitating swift action through platforms you already have, like Webex, Slack, and Microsoft Teams.

Agenda

01 What is Cisco Identity Intelligence

02 Identity Security Posture

03 Monitoring Auth Factor Progression

04 Threat Detection & Response

05 User Trust Levels

06 Identity Security Assessments

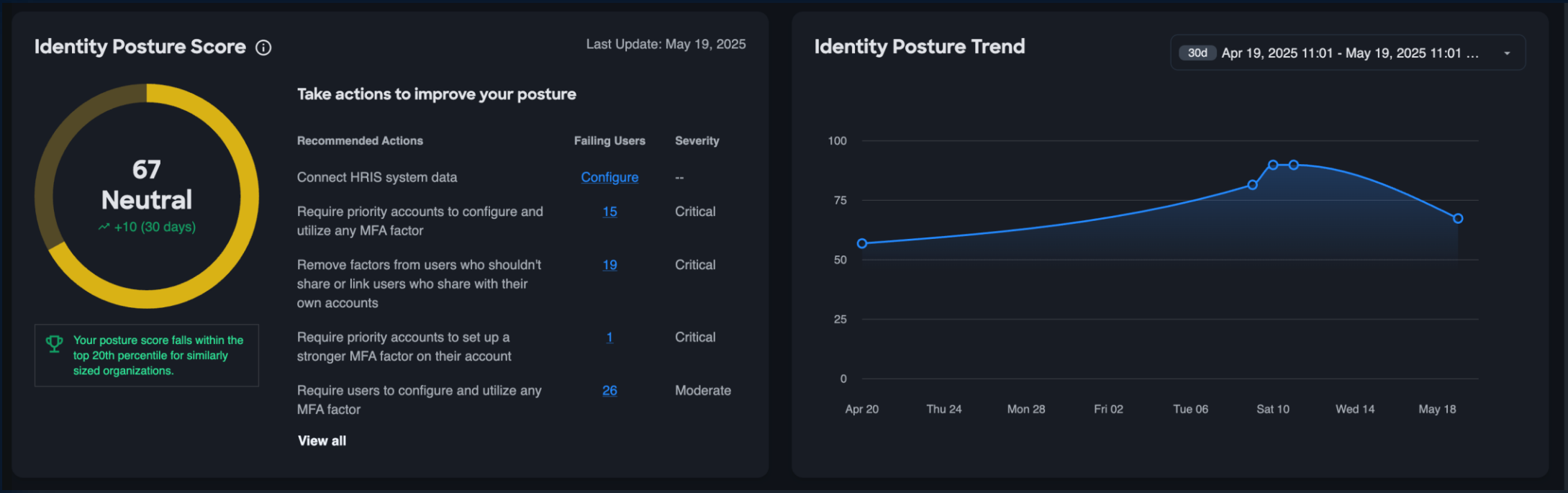
07 Putting the “R” in ITDR

08 Call to Action

Identity Security Posture Management (ISPM)

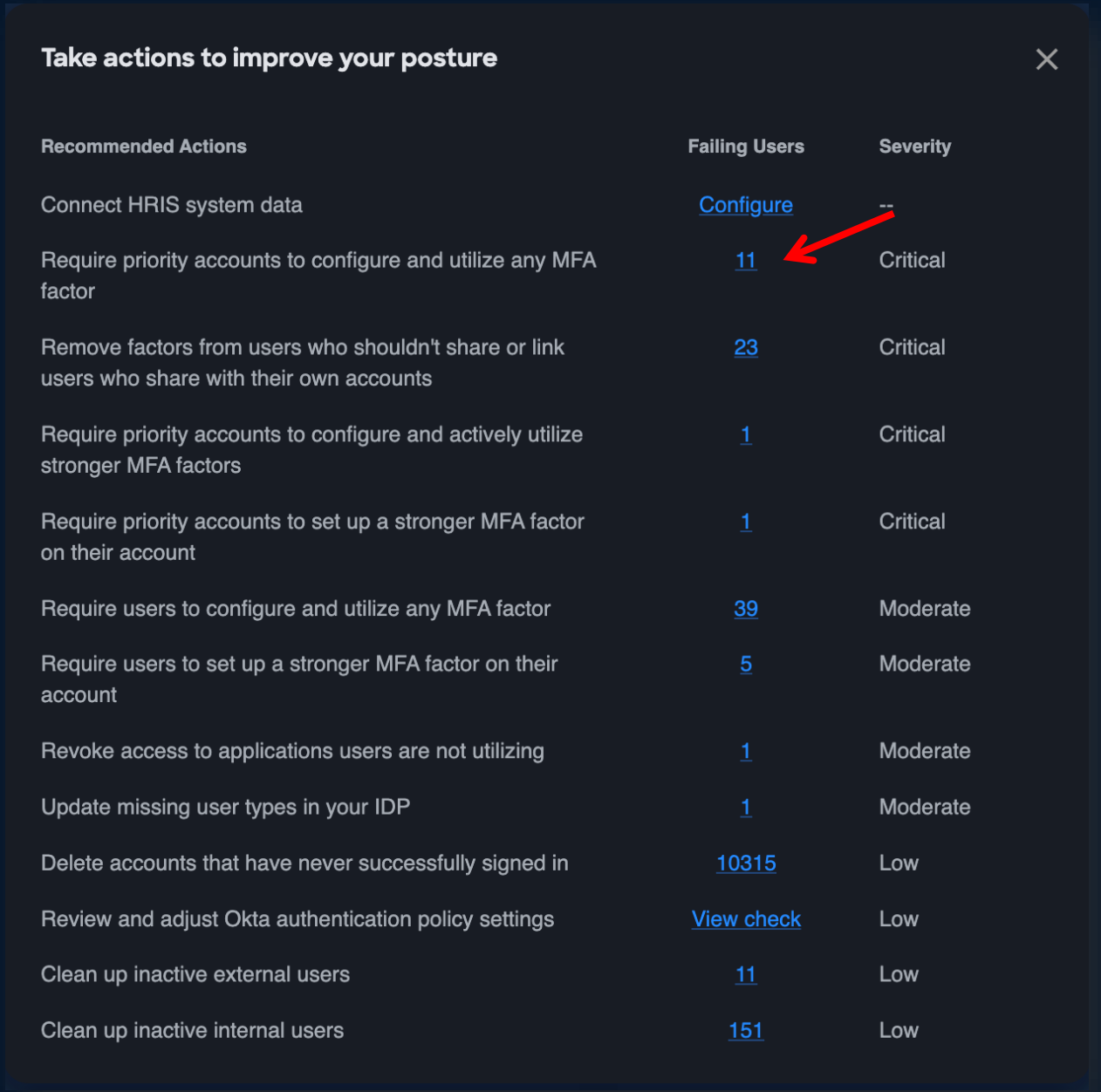
Identity Posture Score & Trend

- Your organization is given a posture score
  - It is compared to similar organizations, and the posture trend is tracked: in order to “nudge” you to improve



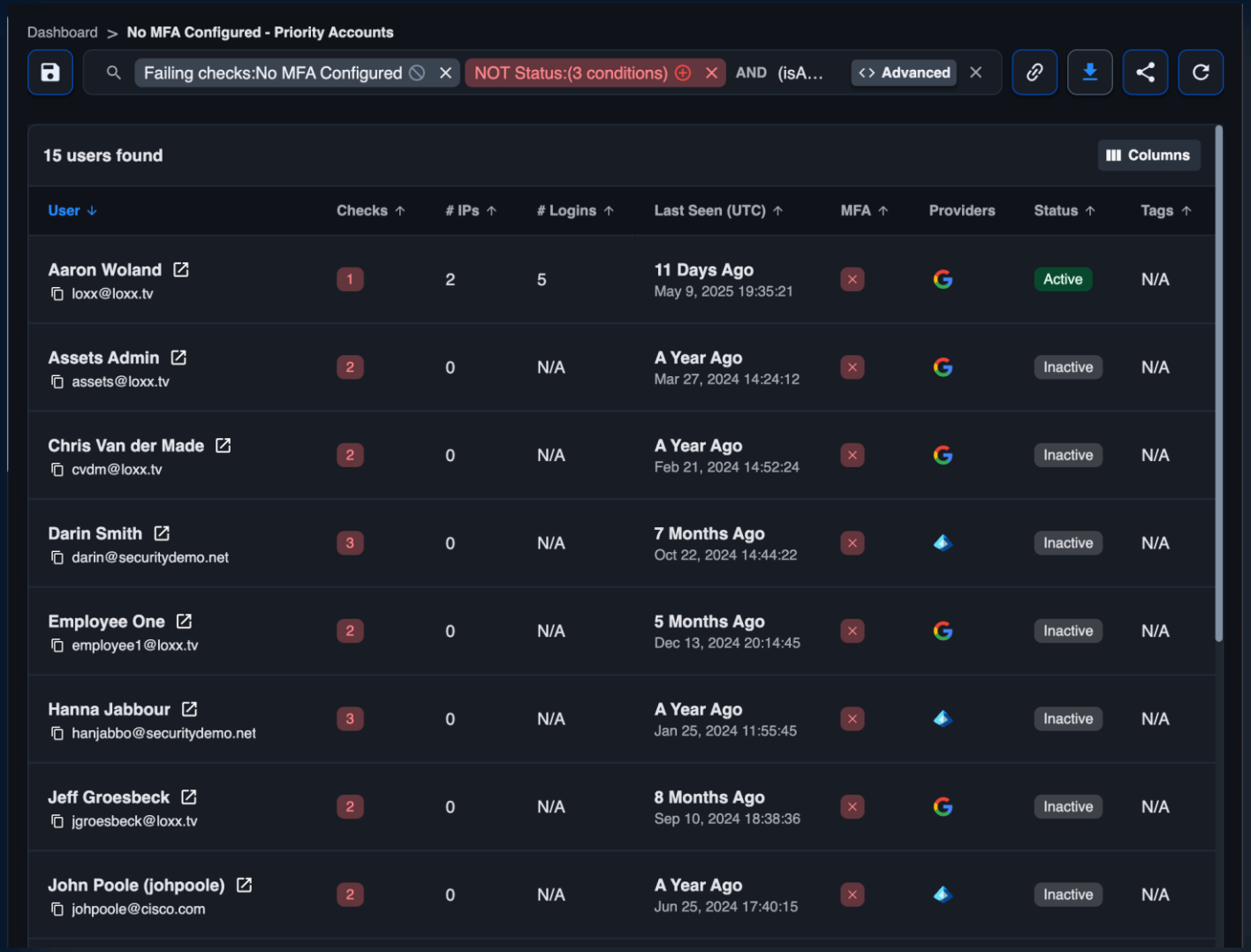
Identity Posture

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



Priority Accounts w/o MFA

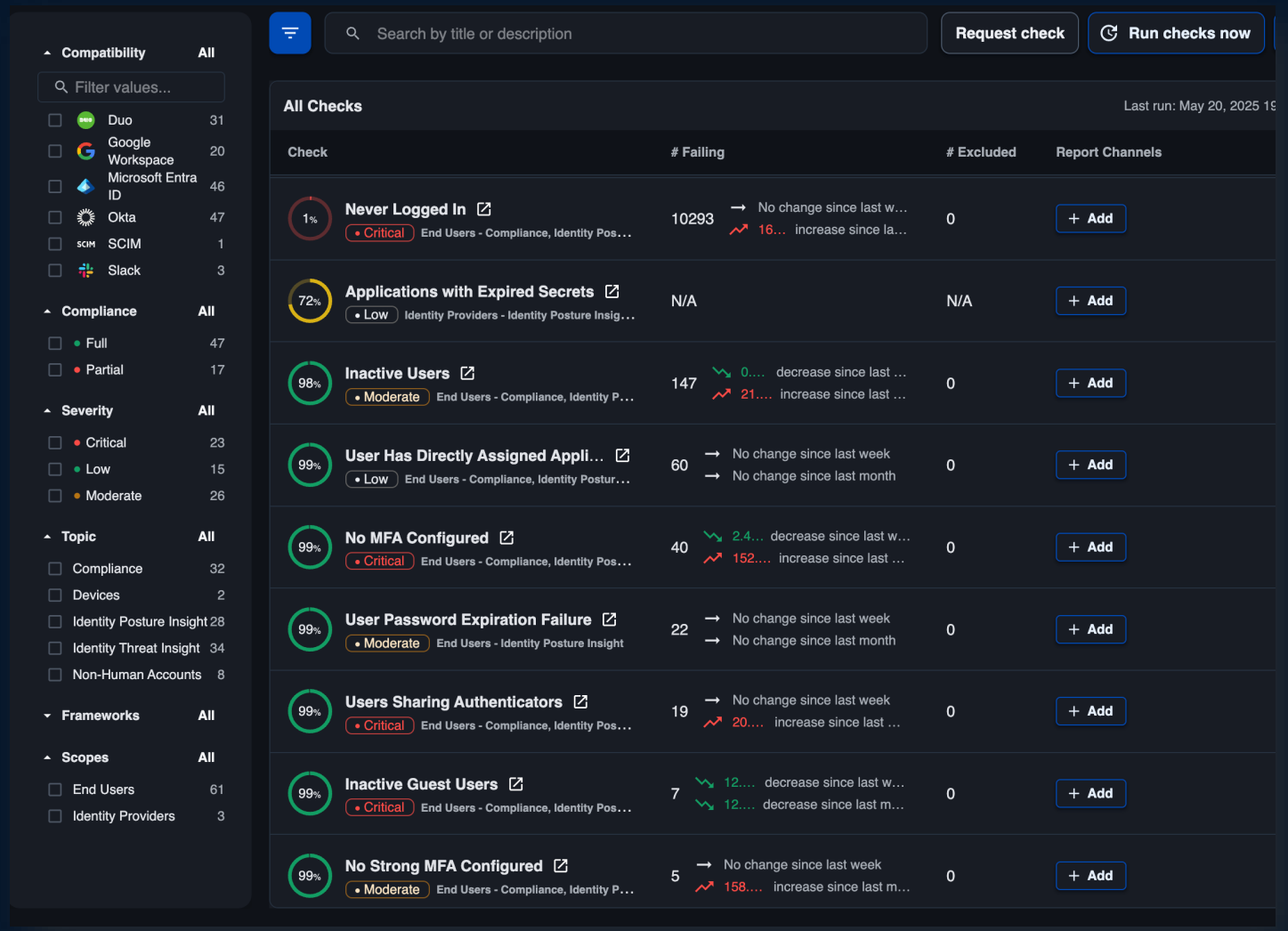
- Start with the low hanging fruit
  - These are admin accounts or other similar that do not have MFA in one or more IDPs
    - Determined by Failing the *No MFA Configured Check* AND (isAdmin:true OR isSpecialAccount:true)



Introducing.....
“Checks”

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

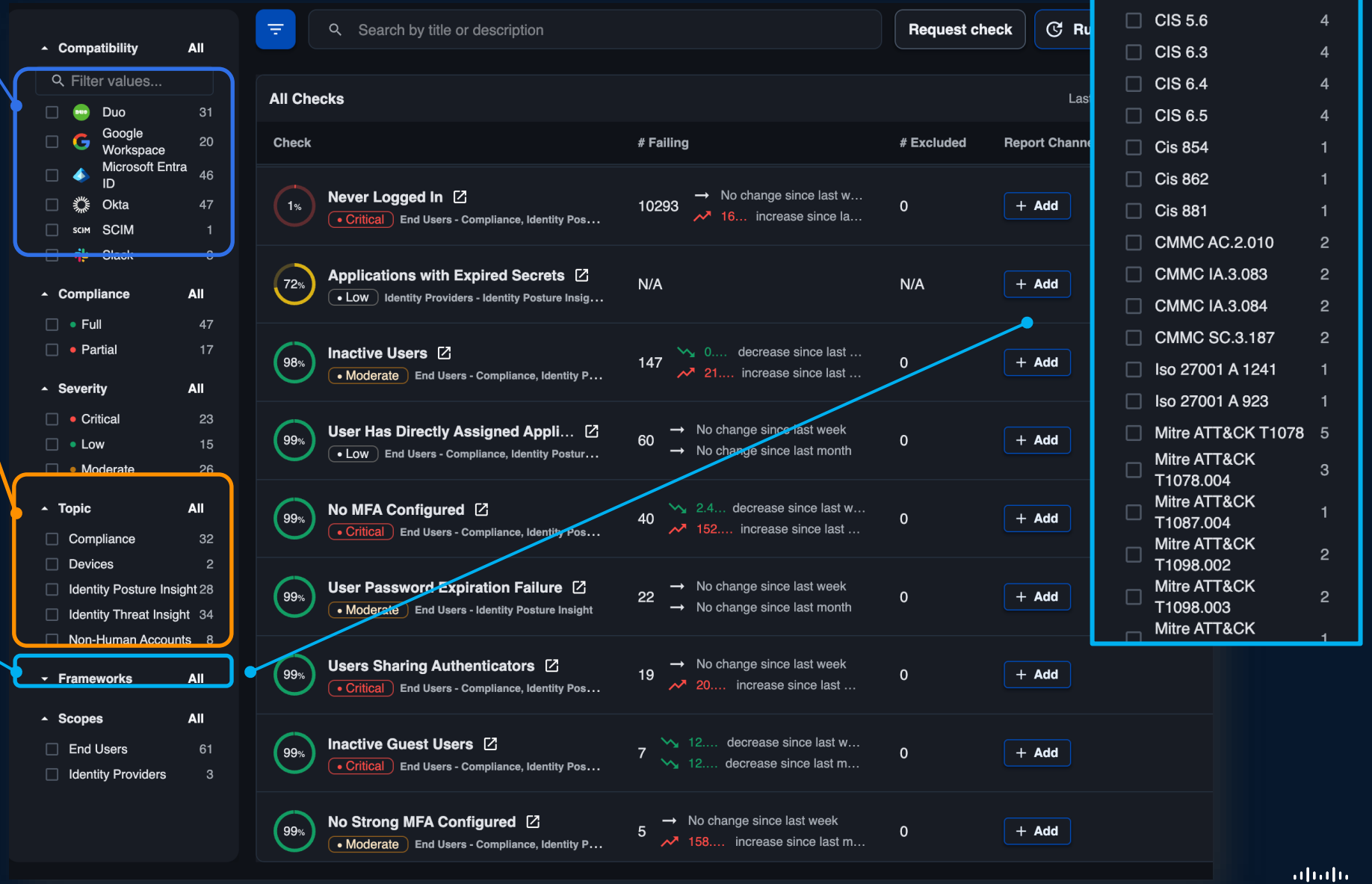
Not all checks are compatible with all providers / sources. You can filter the list of checks based on the IdP source

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.



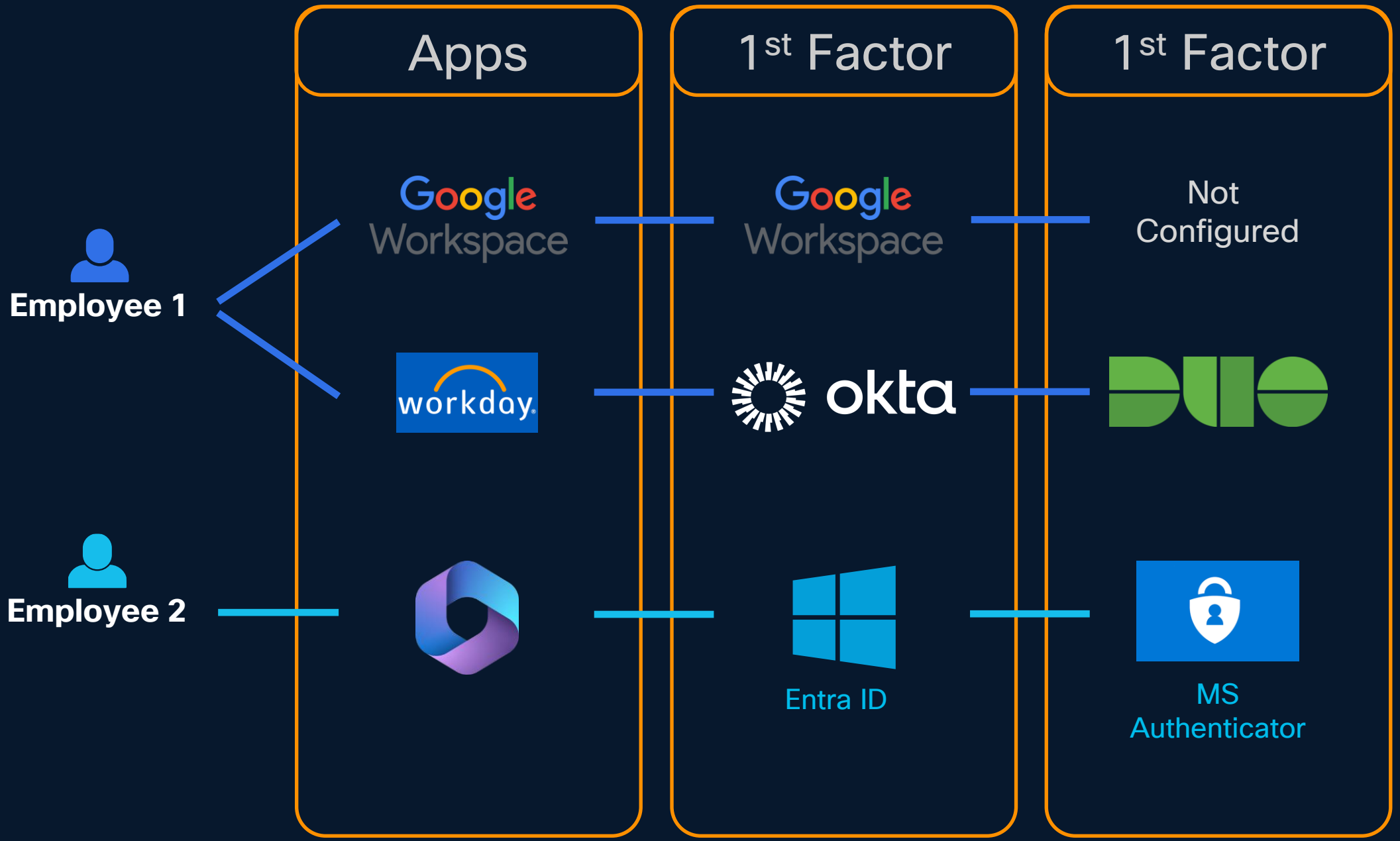
But my user does have MFA configured. Look! You can see that Duo MFA exists

– Many Customers

No MFA Configured Details

- Can be a little confusing because CII is reporting on the entire IDP Landscape.
- The user exists in One or more IDPs where there is no MFA configured
- Or no MFA seen in the authentication logs

Are you sure that strong MFA is configured everywhere?



Agenda

01 What is Cisco Identity Intelligence

02 Identity Security Posture

03 Monitoring Auth Factor Progression

04 Threat Detection & Response

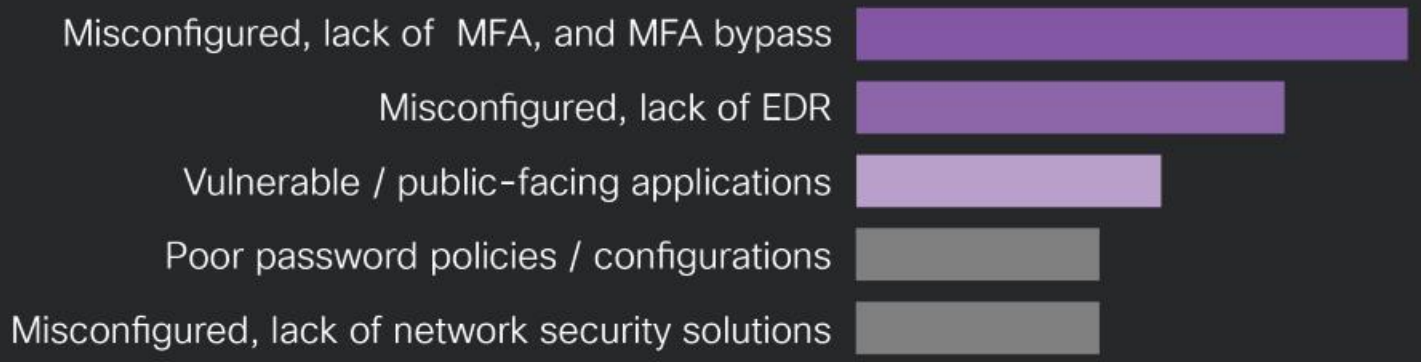
05 User Trust Levels

06 Identity Security Assessments

07 Putting the “R” in ITDR

08 Call to Action

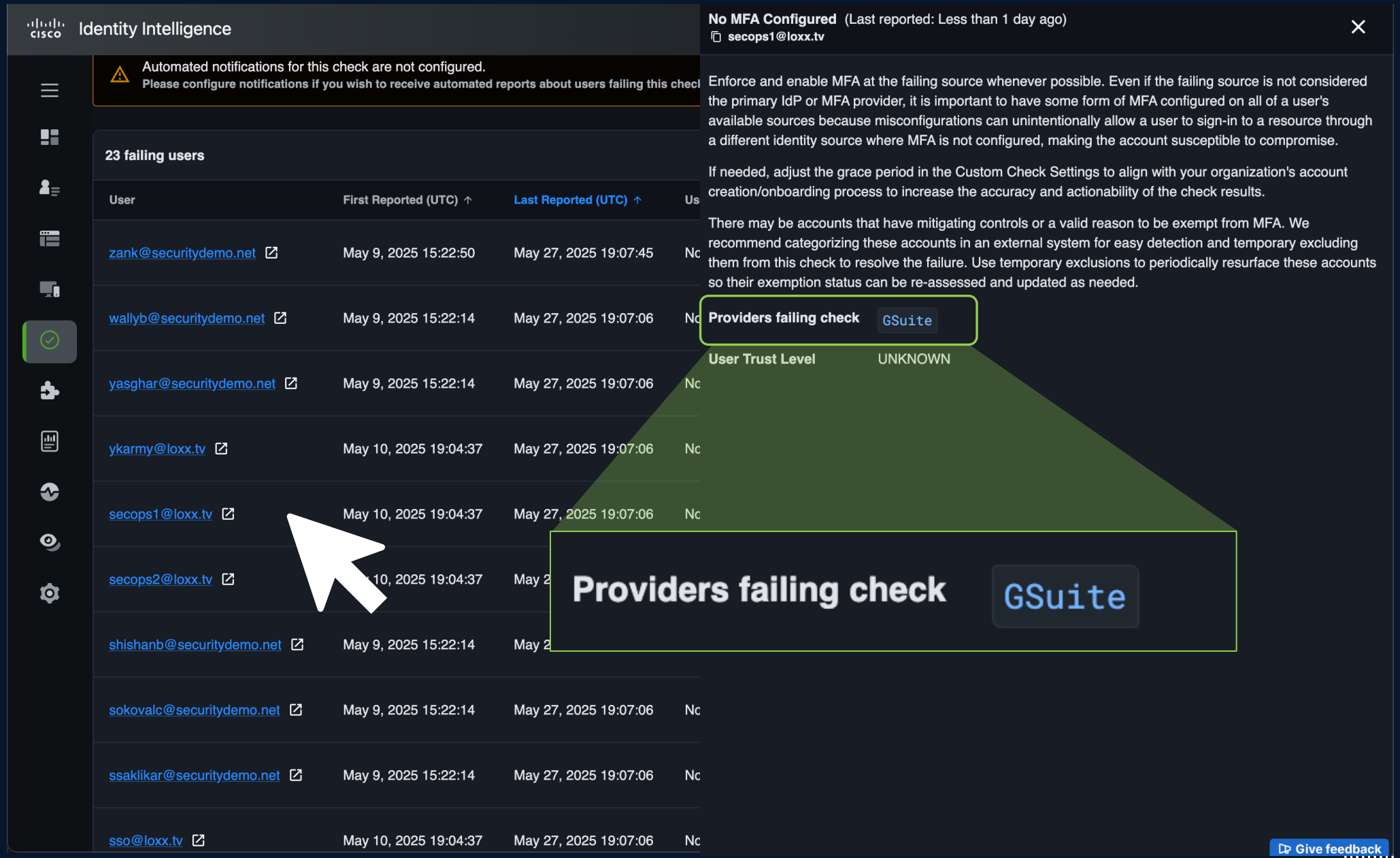
Lack of MFA was one of the top security weaknesses in Q3



CISCO TALOS

Click on user failing the “No MFA Configured” check.

Details are shown from the right-side & you can see which IDP(s) are applicable



Now, you can act! Go into that IDP and configure MFA

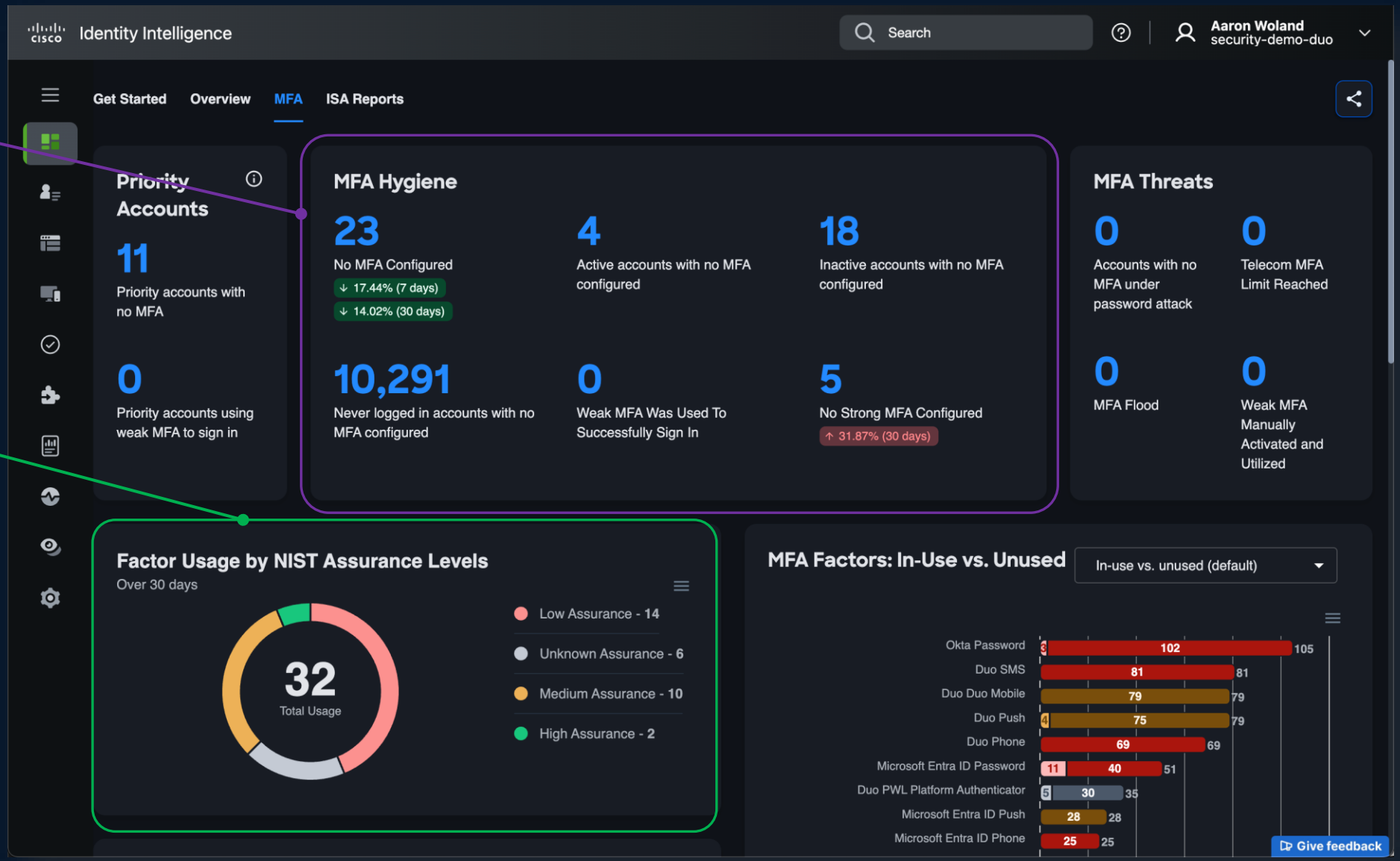
Leverage the MFA Dashboard to Keep Up

Overall MFA Hygiene

Use these to point out users without MFA configured, users who never logged in, etc.

Authentication Factors

Ensure you are using strong factors, like AAL3. Drill down into the lower assurance levels first.

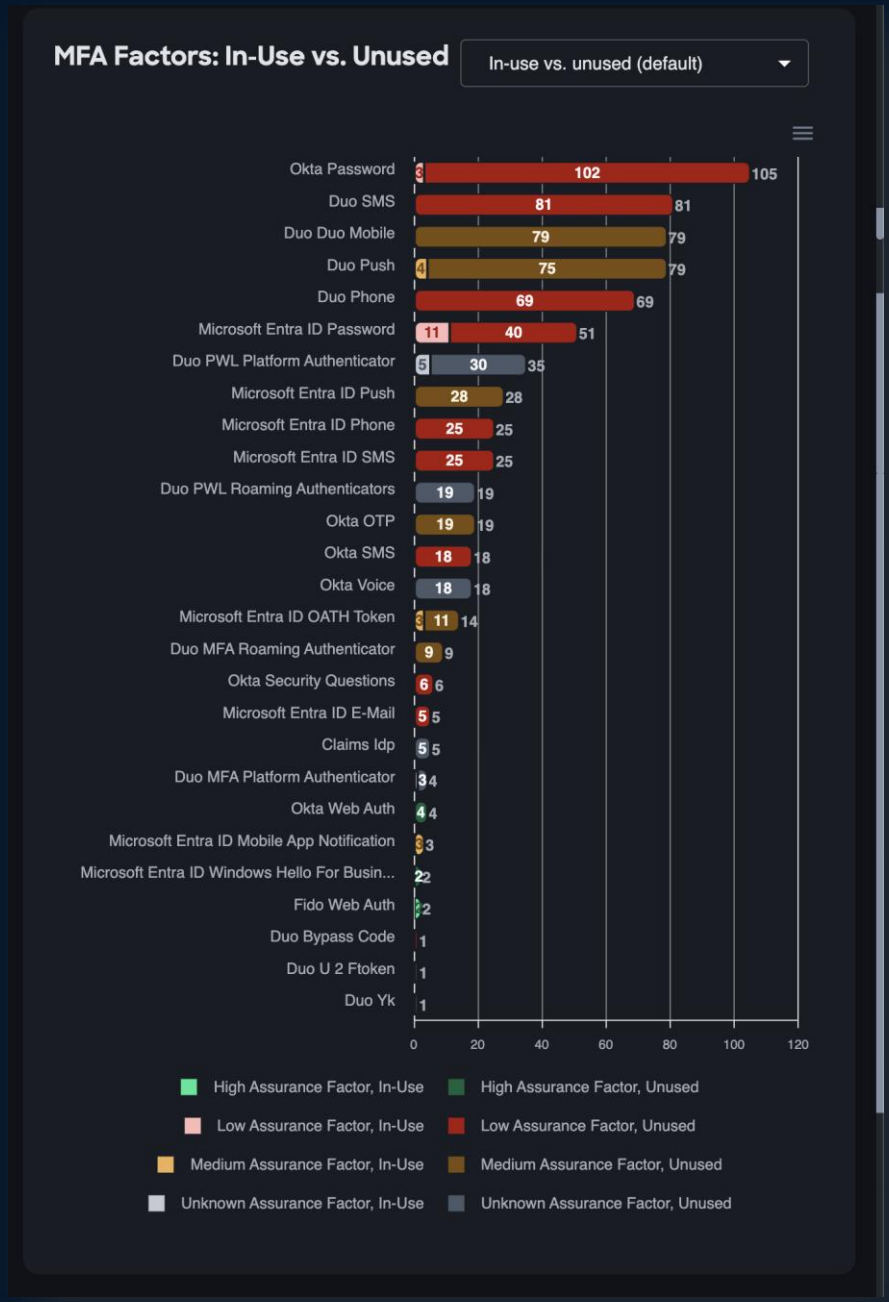


“I am certain that we removed all SMS & are only using AAL3 factors now”

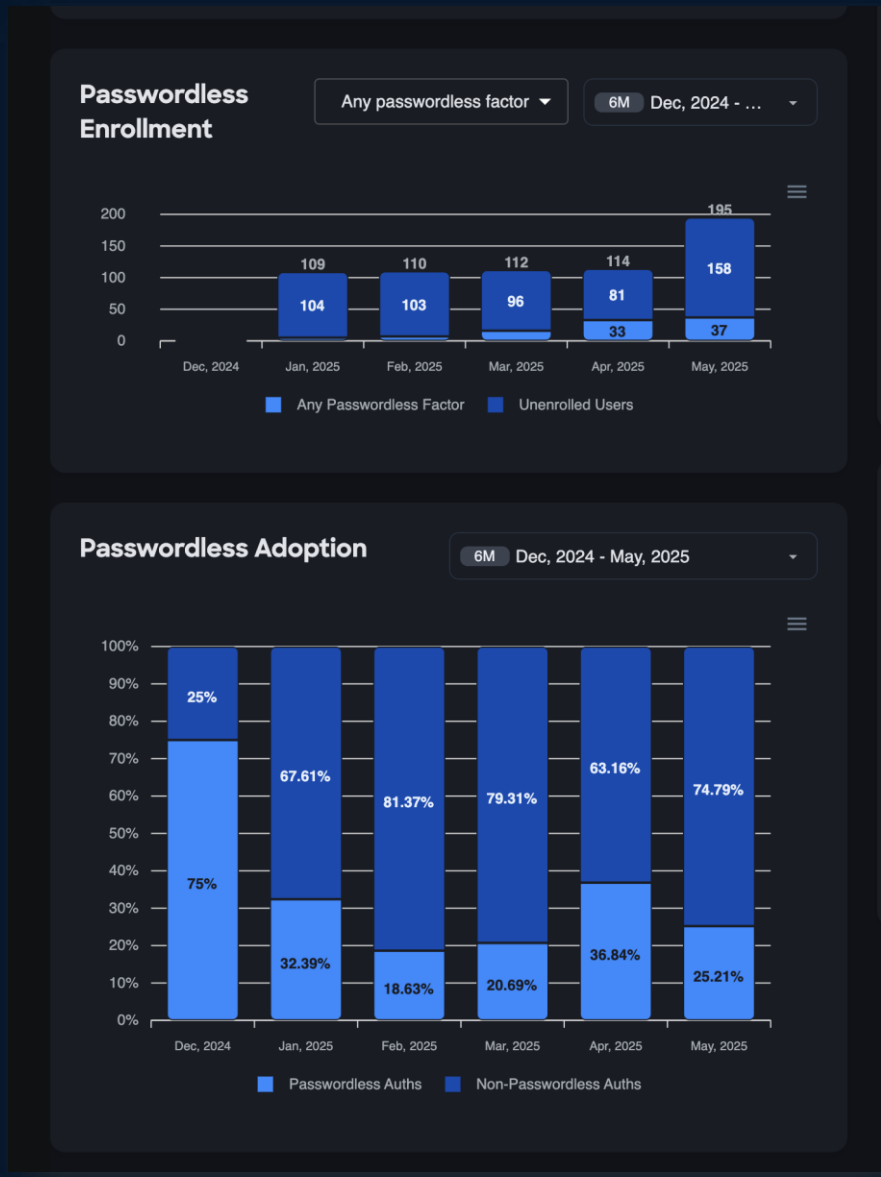
– Anonymous CISO that CII proved wrong

“We only use strong Authentication Factors!”

MFA Dashboard shows all the methods that are *actually* used.



Use the MFA Dashboard to monitor the progression towards passwordless!



Agenda

01 What is Cisco Identity Intelligence

02 Identity Security Posture

03 Monitoring Auth Factor Progression

04 Threat Detection & Response

05 User Trust Levels

06 Identity Security Assessments

07 Putting the “R” in ITDR

08 Call to Action

Reactive Security

Threat Detection & Response

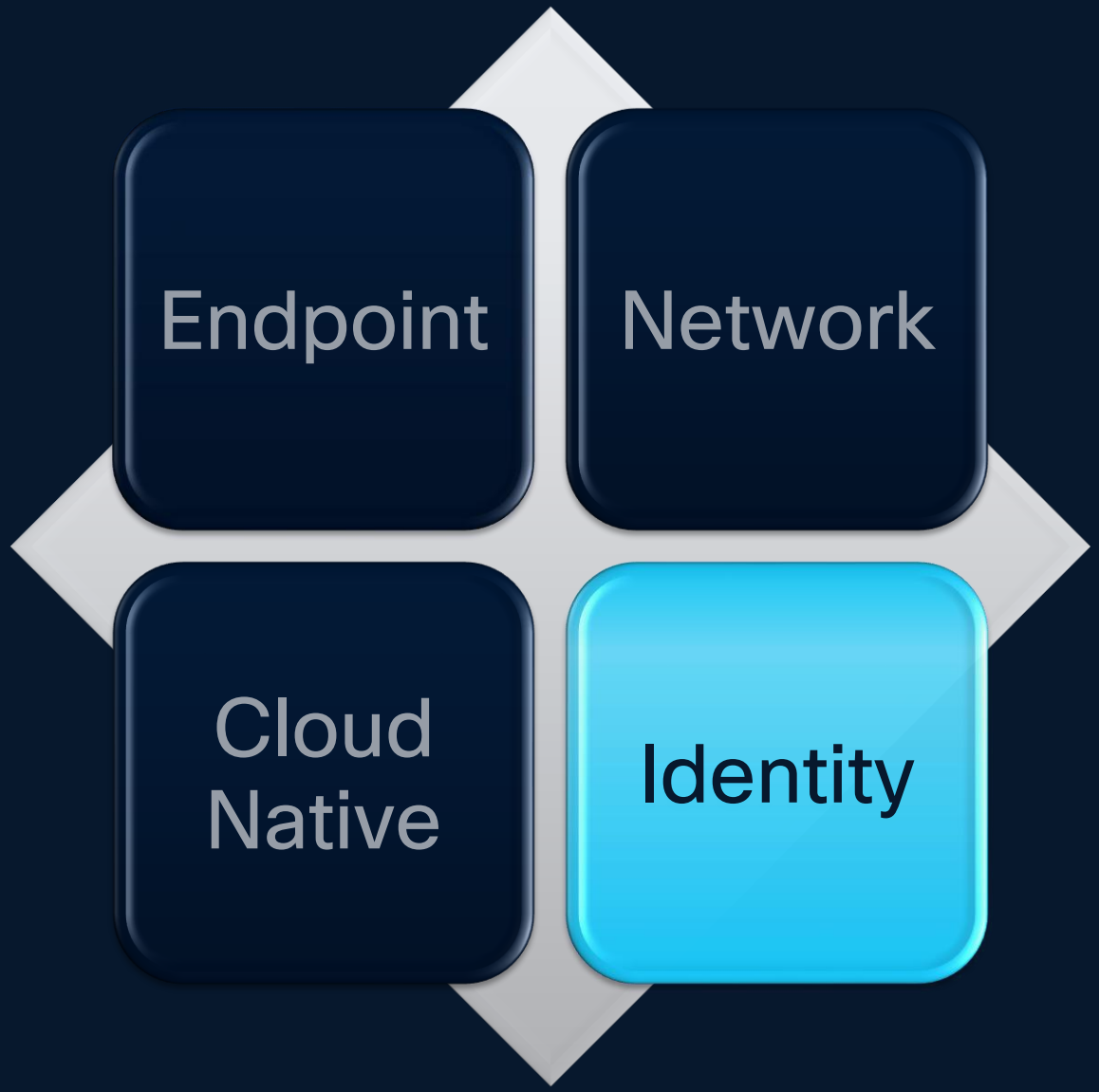
Prevention is not enough!

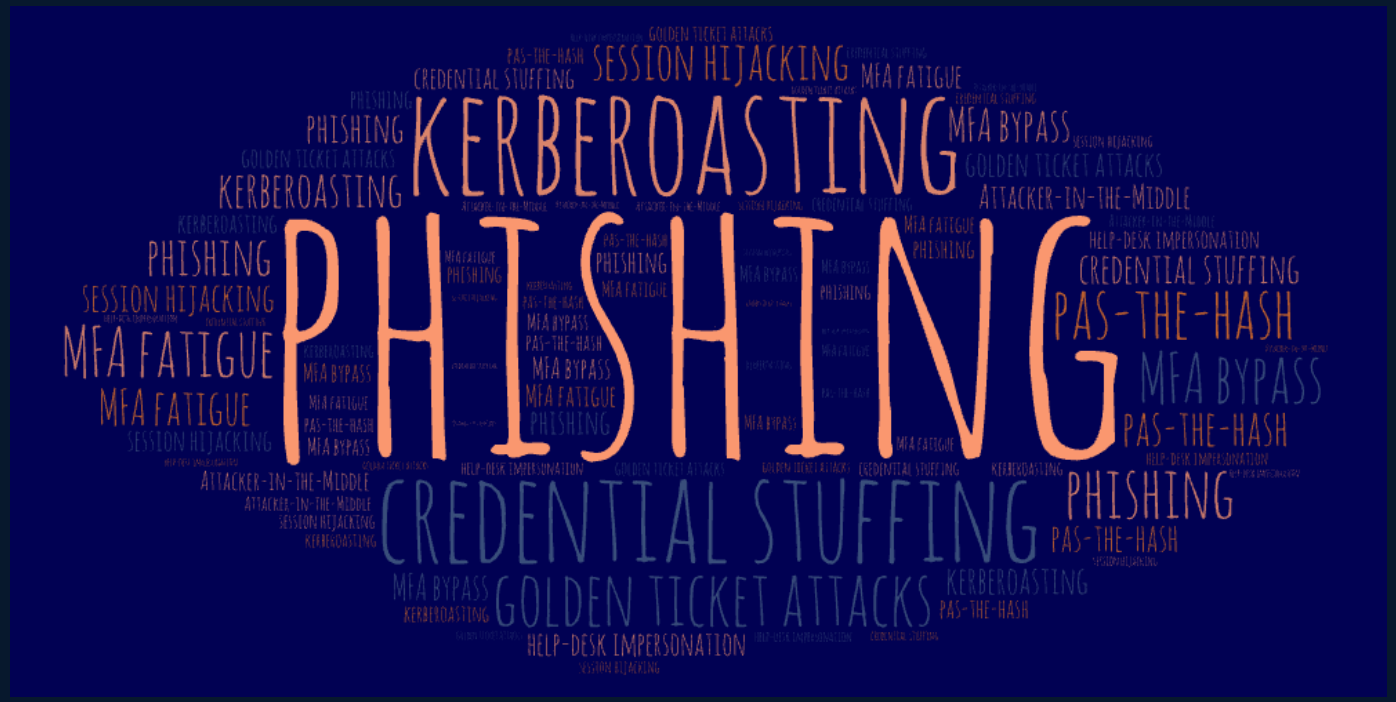
Endpoint Detection & Response

Network Detection & Response

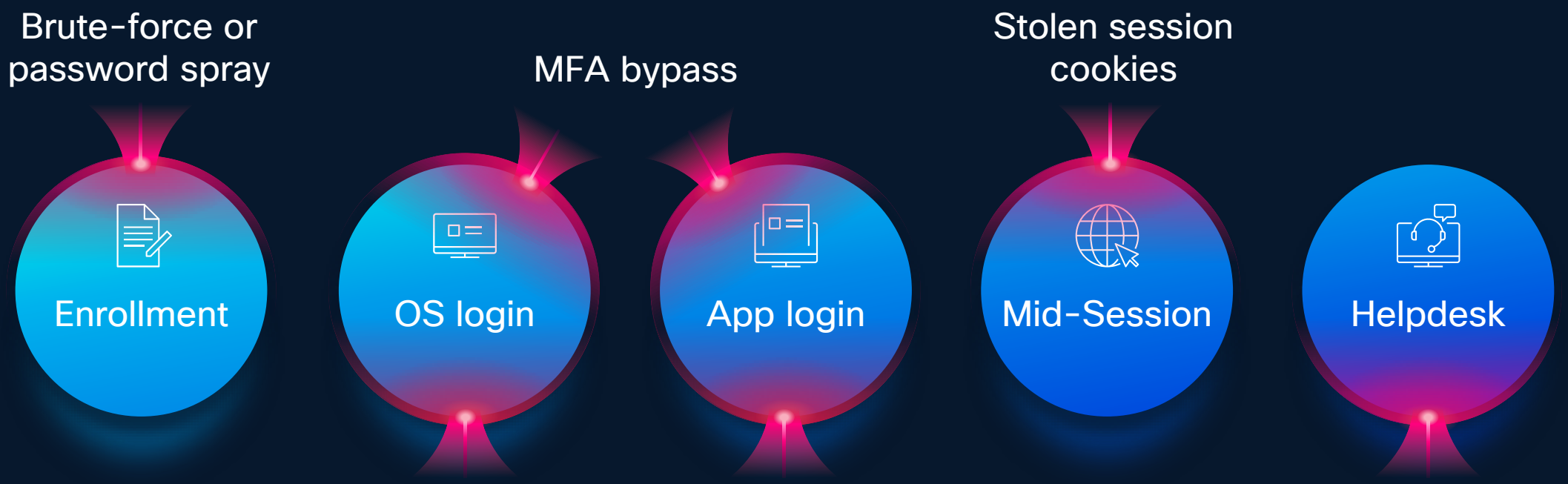
Cloud Native Detection & Response

Identity Threat Detection & Response





Attackers expect you to have MFA



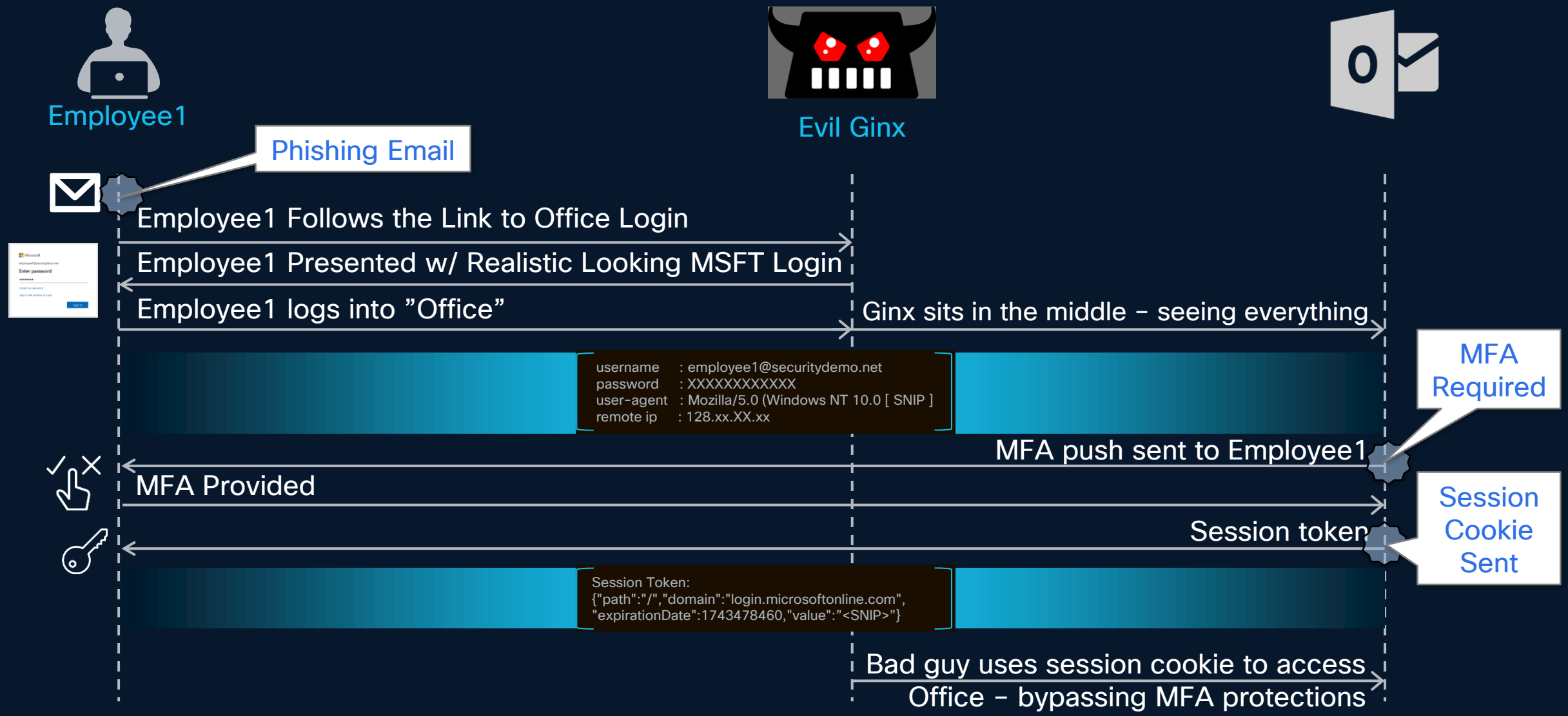
Session Hijacking Example


Actual login page
Hacker controlled proxy
Fake login page that looks normal

Session Hijacks are on the rise

- Can be accomplished with attacker-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)

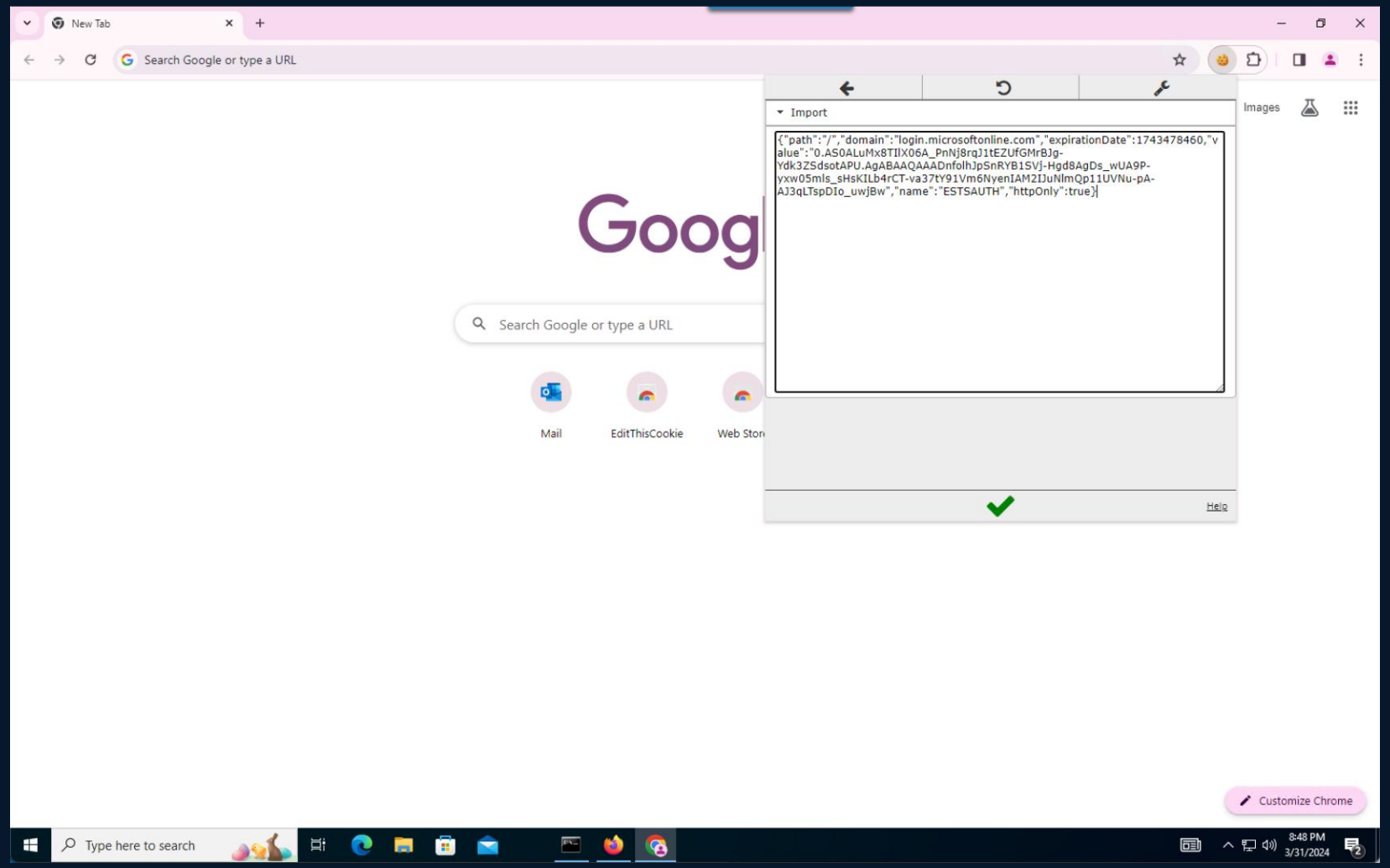
User follows the link & sees what looks exactly like the normal Microsoft Login flow

Bad Guy sees everything

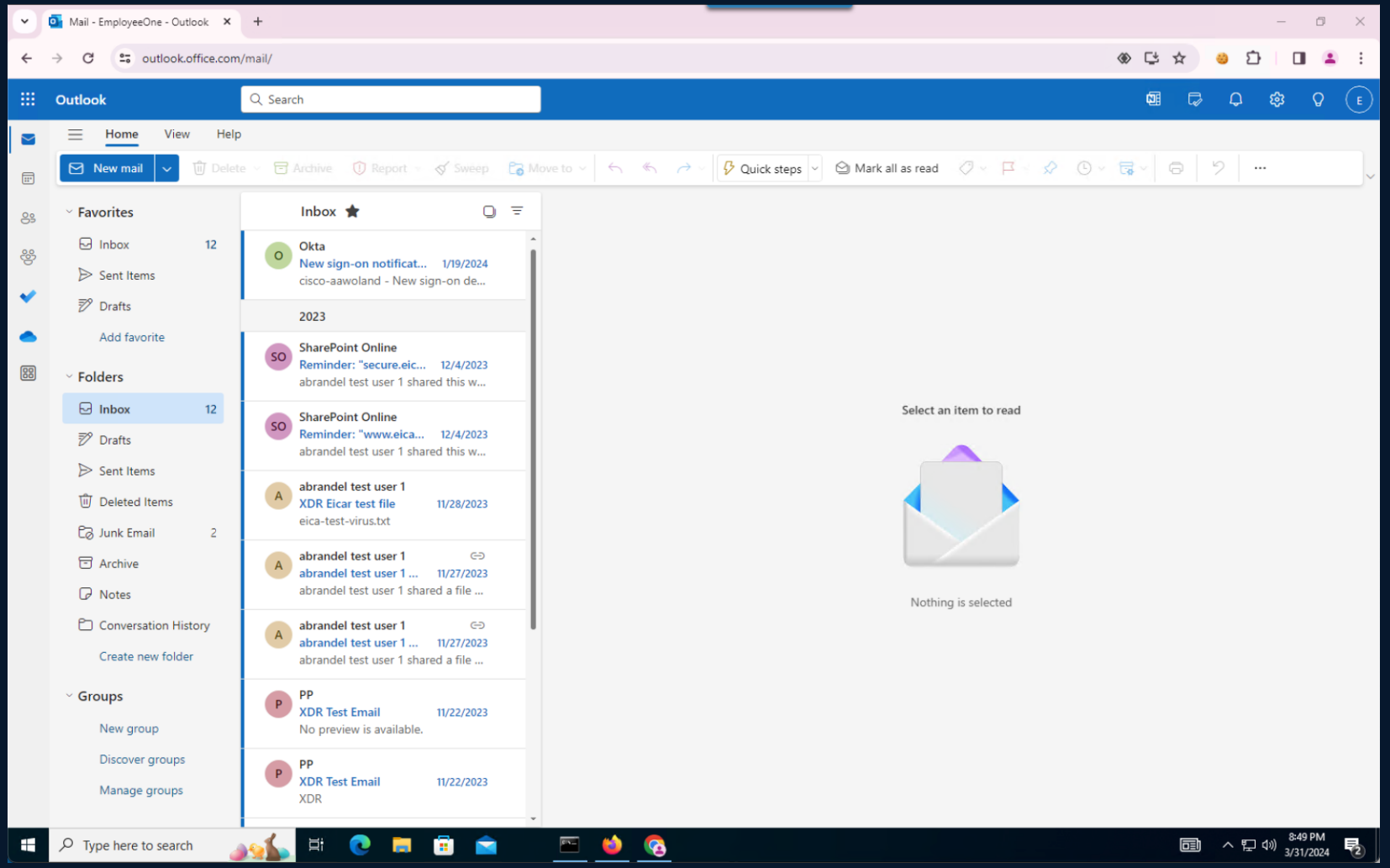
The bad guy is able to capture the username, password (most times) & more importantly the Session Info, including the cookie

```
| onelogin       | disabled | visible |
| outlook        | disabled | visible |
| paypal         | disabled | visible |
| protonmail     | disabled | visible |
| reddit         | disabled | visible |
| tiktok         | disabled | visible |
| twitter        | disabled | visible |
| twitter-mobile | disabled | visible |
| wordpress.org  | disabled | visible |
+----------------+----------+---------+

: lures

+----+----------+----------+-----------+------------+--------------+--------+------+
| id | phishlet | hostname |   path    | redirector | redirect_url | paused | og   |
+----+----------+----------+-----------+------------+--------------+--------+------+
| 0  | o365     |          | /spRqqIiF |            |              |        | ---- |
+----+----------+----------+-----------+------------+--------------+--------+------+

[03:09:25] [war] [o365] request to hidden phishlet: https://login.securitydemo.net/spRqqIiF (Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0) [128.107.78.71]
:
:
: phishlets unhide o365
[03:09:49] [inf] phishlet 'o365' is now reachable and visible from the outside
:
:
[03:10:03] [inf] [0] [o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0 (128.107.78.71)
[03:10:03] [inf] [0] [o365] landing URL: https://login.securitydemo.net/spRqqIiF
[03:10:54] [+++] [0] Username: [employee1@securitydemo.net]
[03:10:54] [+++] [0] Username: [employee1@securitydemo.net]
[03:10:54] [+++] [0] Password: [redacted]
[03:10:58] [+++] [0] all authorization tokens intercepted!
: phishlets hide o365
[03:11:49] [inf] phishlet 'o365' is now hidden and all requests to it will be redirected
:
:
[03:11:57] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [146.190.197.169]
[03:12:09] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [15.161.55.89]
[03:12:15] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [206.189.247.132]
[03:12:23] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [18.170.98.205]
: sessions

+----+----------+------------------+----------+----------+----------------+---------------------+
| id | phishlet |     username     | password |  tokens  |   remote ip    |        time         |
+----+----------+------------------+----------+----------+----------------+---------------------+
| 1  | o365     | employee1@s..... | Cisco123 | captured | 128.107.78.71  | 2024-04-01 03:10    |
+----+----------+------------------+----------+----------+----------------+---------------------+

:
```

Paste the Cookies into a plugin



Bam: Access as Employee1



Technical Nuggets

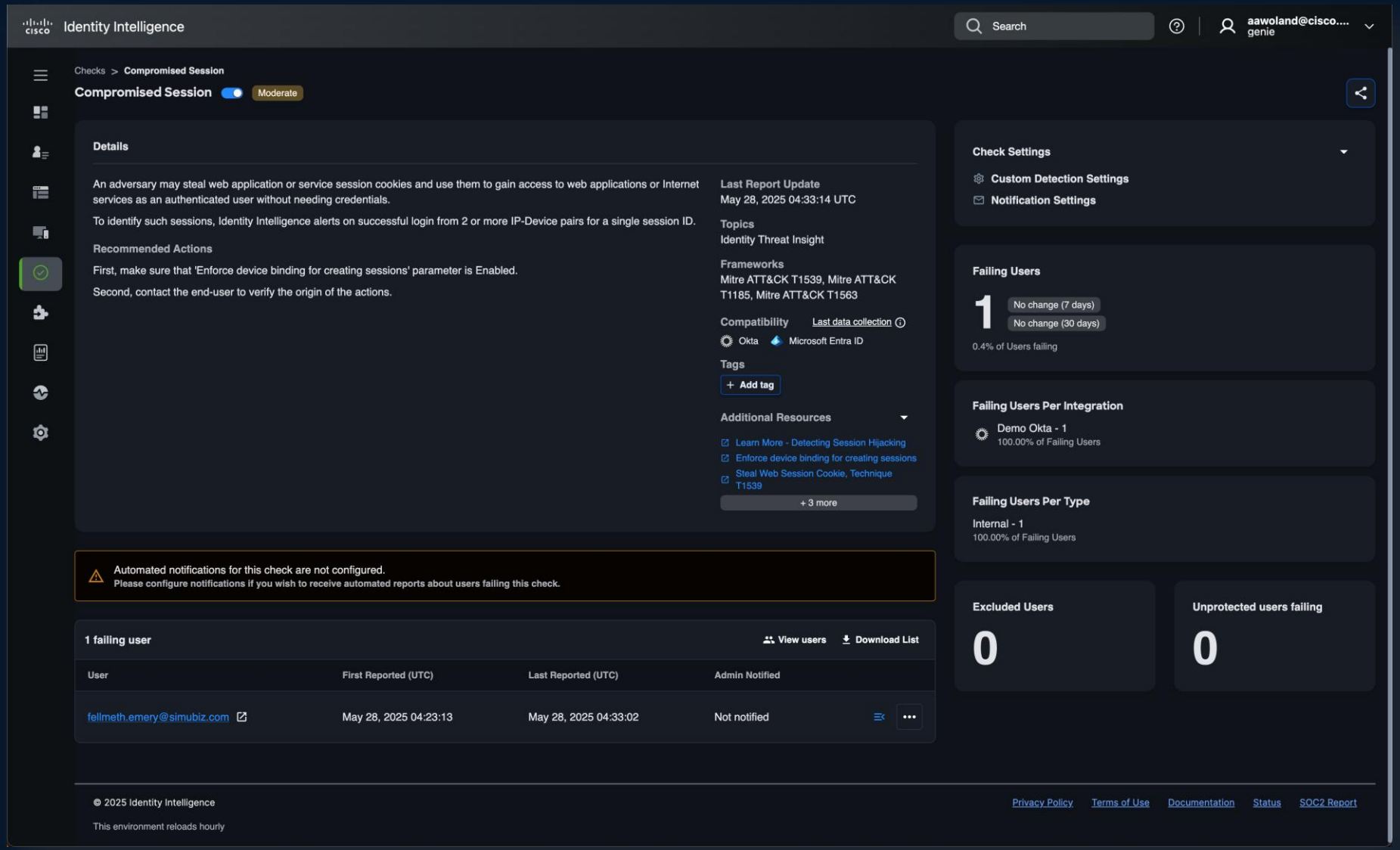
- With event-streaming, this gets detected much faster than Graph API sync
  - These signals from Entra fall into what are called “real-time checks”
  - Really near-real-time ☺
- Without event streaming it can take over 24 hours to detect this, if at all
- **Entra will label these as “Medium" criticality events**, even though it was a successful attack
  - Okta & Duo share the session info in their logs & makes it easier to detect
  - As of May 2025, Microsoft Entra’s IDP also maintains sessions and includes them in logs

...and CII can detect these

Compromised Sessions

Not all checks are compatible with all providers / sources.

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



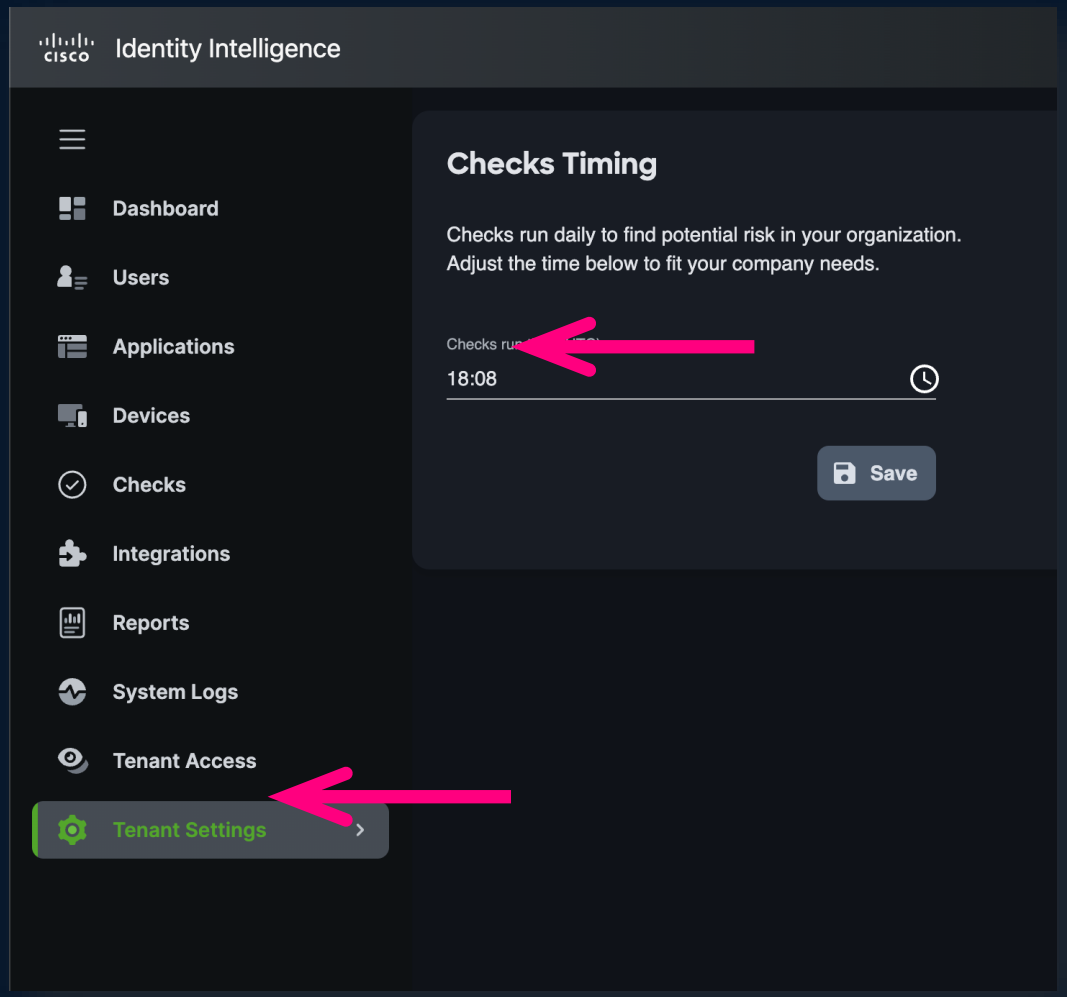
“But… CII Takes too Long to Detect”

– Rando person #3

Threat Discovery Mode (TDM) - High

Technical Nugget

- By default, CII runs it's checks once a day
  - Time configurable in Tenant Settings
  - But not the Frequency
- Called "Threat Discovery Mode" (TDM)
- Can be adjusted to once per hour
  - Threat Discovery Mode = High
- Pre-Requisites
  - 1+ more integrations above Duo
  - 1+ Notification Target (webhook) enabled
  - Streaming must be enabled (Duo, Okta, Entra)



https://docs.oort.io/how-to-guides/can-identity-intelligence-analyze-behavior-and-fail-checks-more-frequently

Agenda

01 What is Cisco Identity Intelligence

02 Identity Security Posture

03 Monitoring Auth Factor Progression

04 Threat Detection & Response

05 User Trust Levels

06 Identity Security Assessments

07 Putting the “R” in ITDR

08 Call to Action

User Trust Levels

User Trust Level

Who: Designed by 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 to be confused with RBA, it is more like a credit score than a real-time fraud detection service

Approach

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

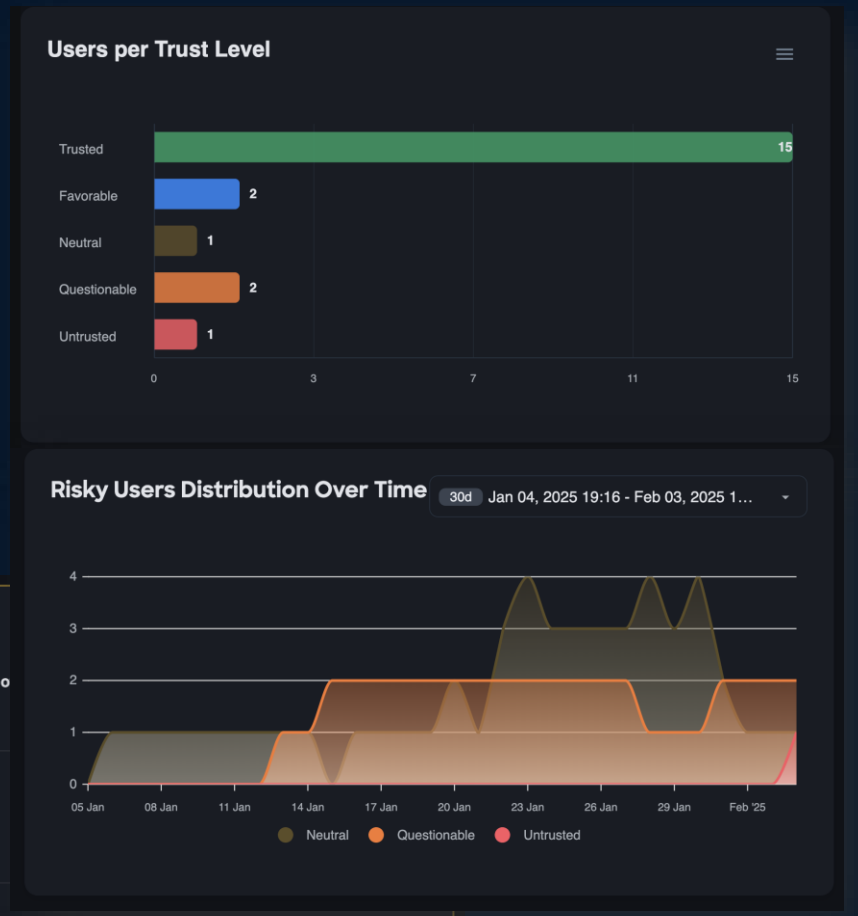
- Leverage the Score as a condition of the security policy
- Help limit access for untrustworthy users or at least require additional assurance
- Step-up authentication or require a managed device, too
- Secure Access & Secure Connect, ISE, Firewall, Meraki

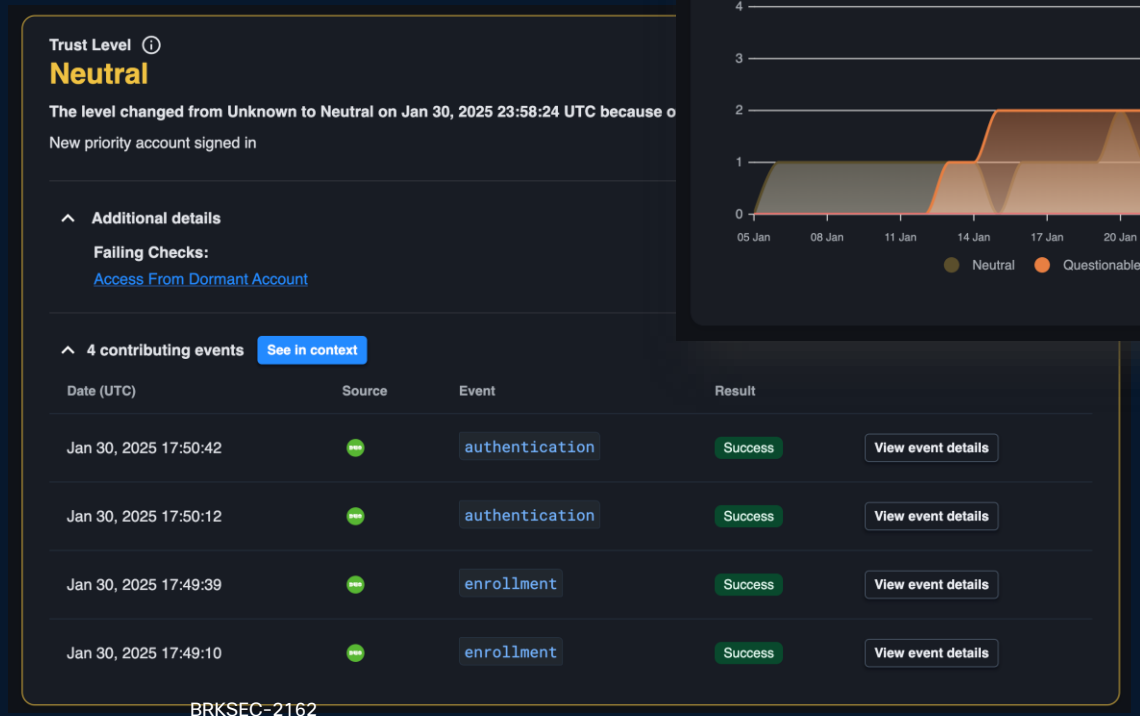
Threat Prioritization

- 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



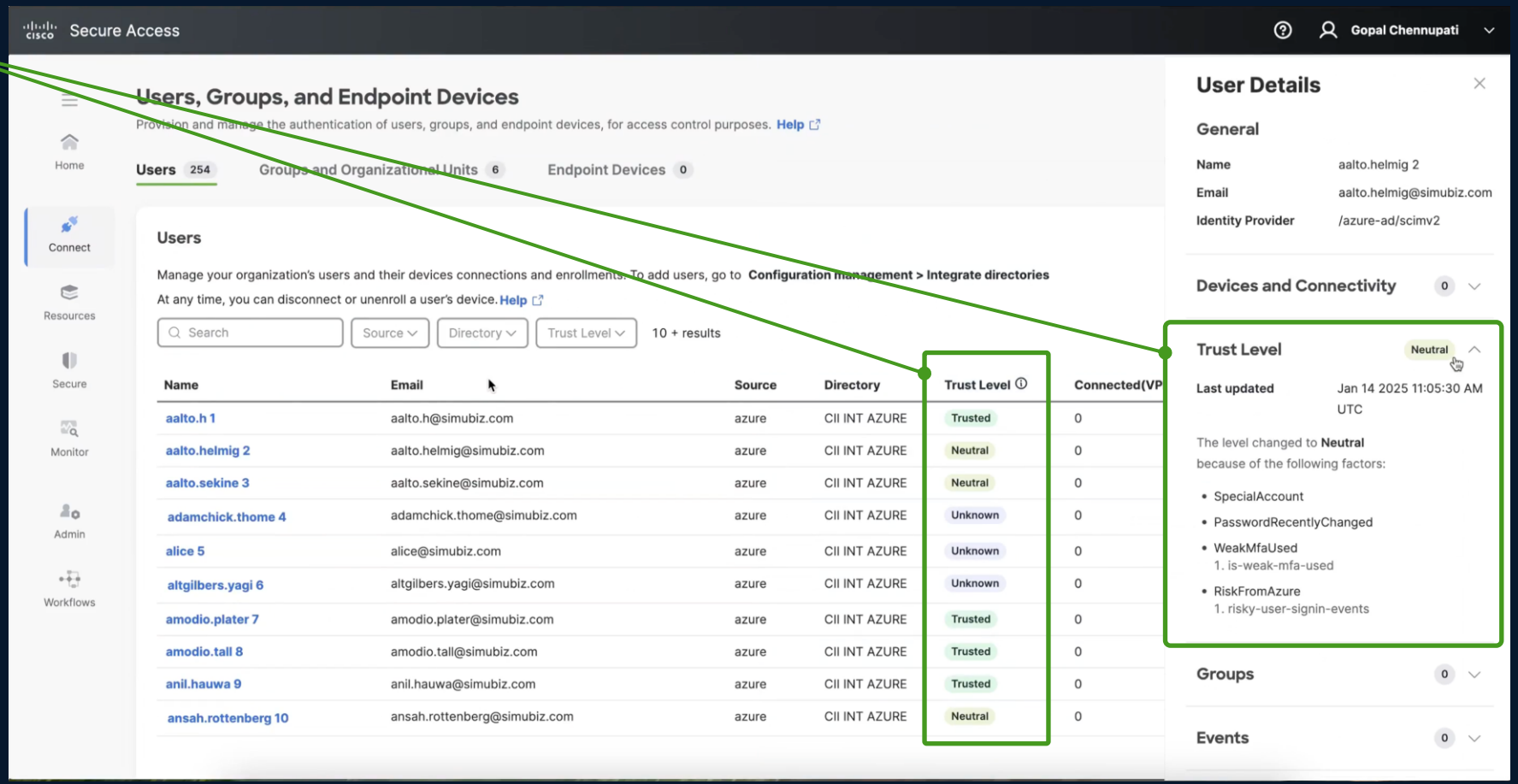


Users in Secure Access are flagged when risky

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.



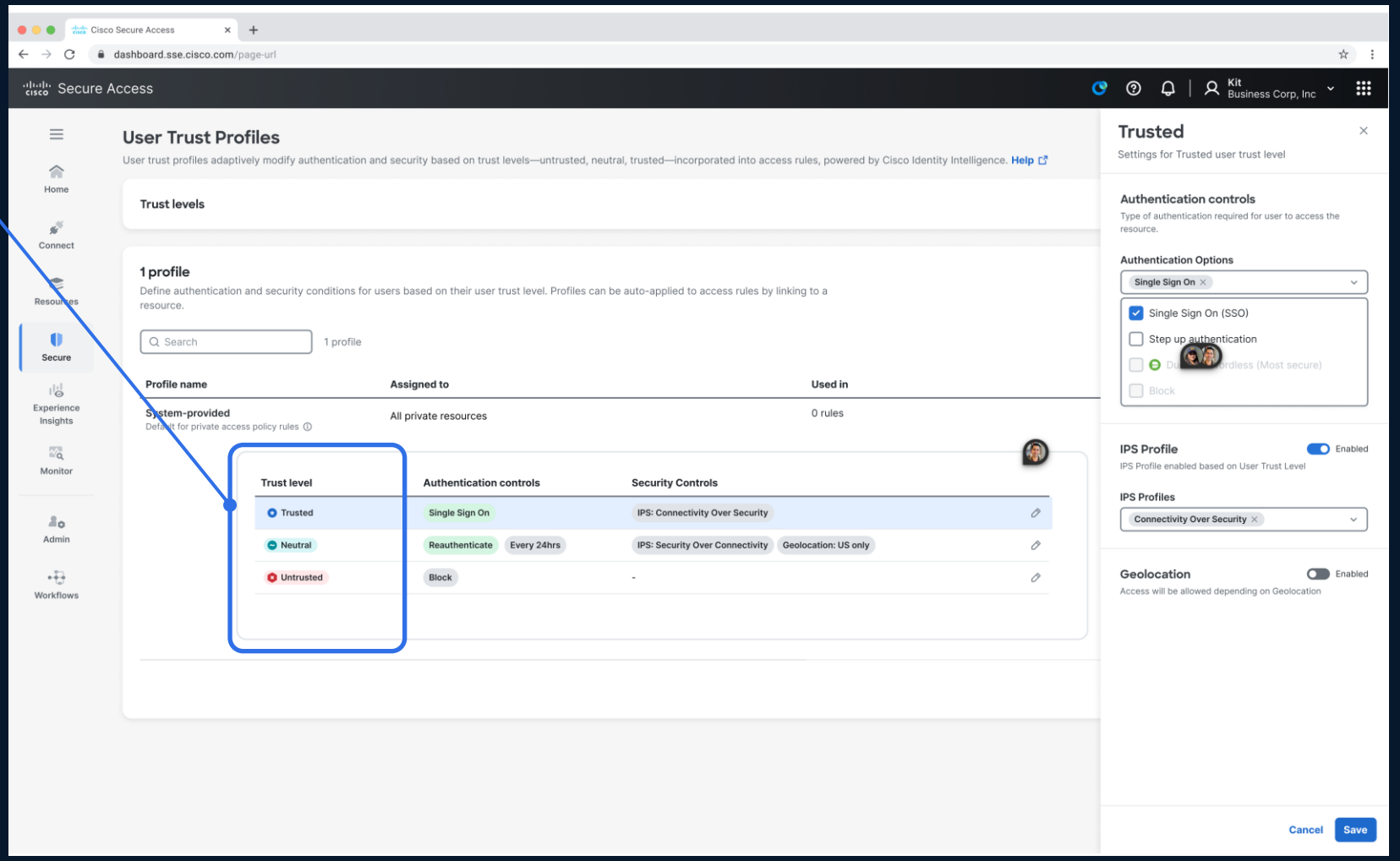
Example Wireframe: Secure Access

For Your Reference

Trust Levels

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

Note: this is not the final design



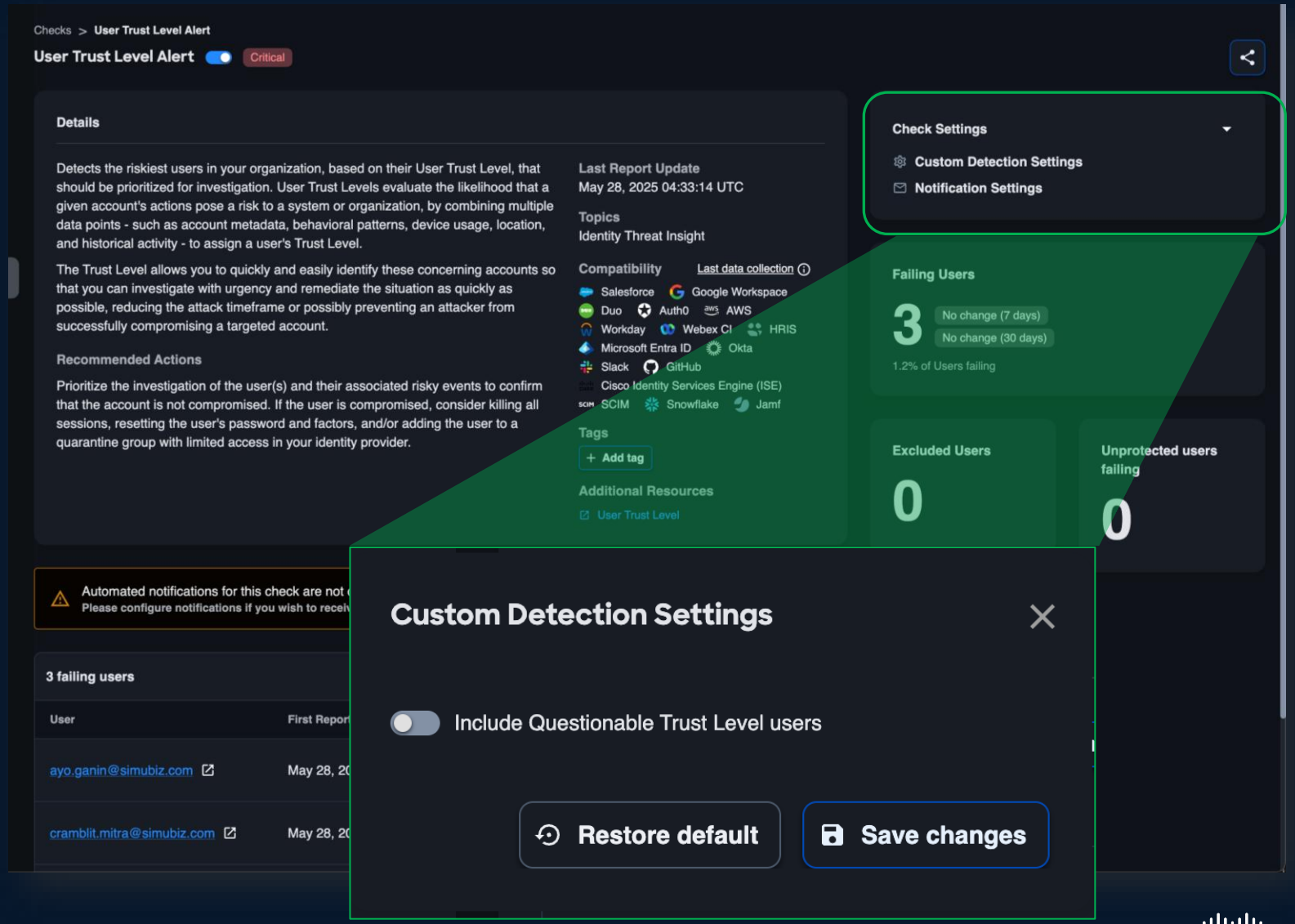
Users in Secure Access are flagged when risky

User Trust Level Alert

Will send alert to configured notification targets when a user is assigned to:

- Questionable (configurable)
- Untrusted (default)

Send those alerts to SIEM/SOAR/XDR or other automation tool to take action(s)



Agenda

01 What is Cisco Identity Intelligence

02 Identity Security Posture

03 Monitoring Auth Factor Progression

04 Threat Detection & Response

05 User Trust Levels

06 Identity Security Assessments

07 Putting the “R” in ITDR

08 Call to Action

Identity Security Assessment

ISA Report Automation

- All the most important elements learned from identity experts and their lessons learned
- Customizable
  - All widgets removable, and reorderable
  - Any saved searches can be added to the report
  - Each of the widgets allows for custom text to be added
- Report is exportable as PDF

Contains many very valuable security touch points

Agenda

01 What is Cisco Identity Intelligence

02 Identity Security Posture

03 Monitoring Auth Factor Progression

04 Threat Detection & Response

05 User Trust Levels

06 Identity Security Assessments

07 Putting the “R” in ITDR

08 Call to Action

The “R” in ITDR: Response

Taking Action(s)

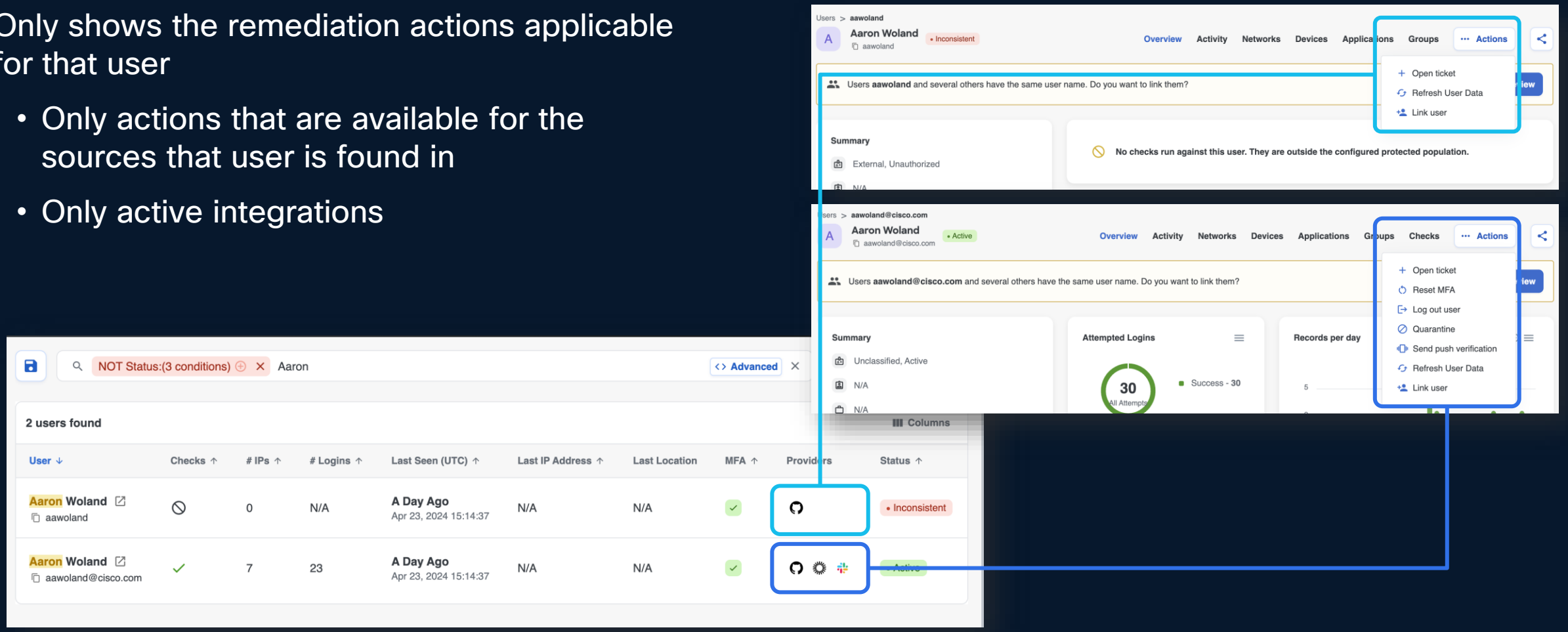
It is up to the customer to determine if direct remediation is right for the organization

- 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)

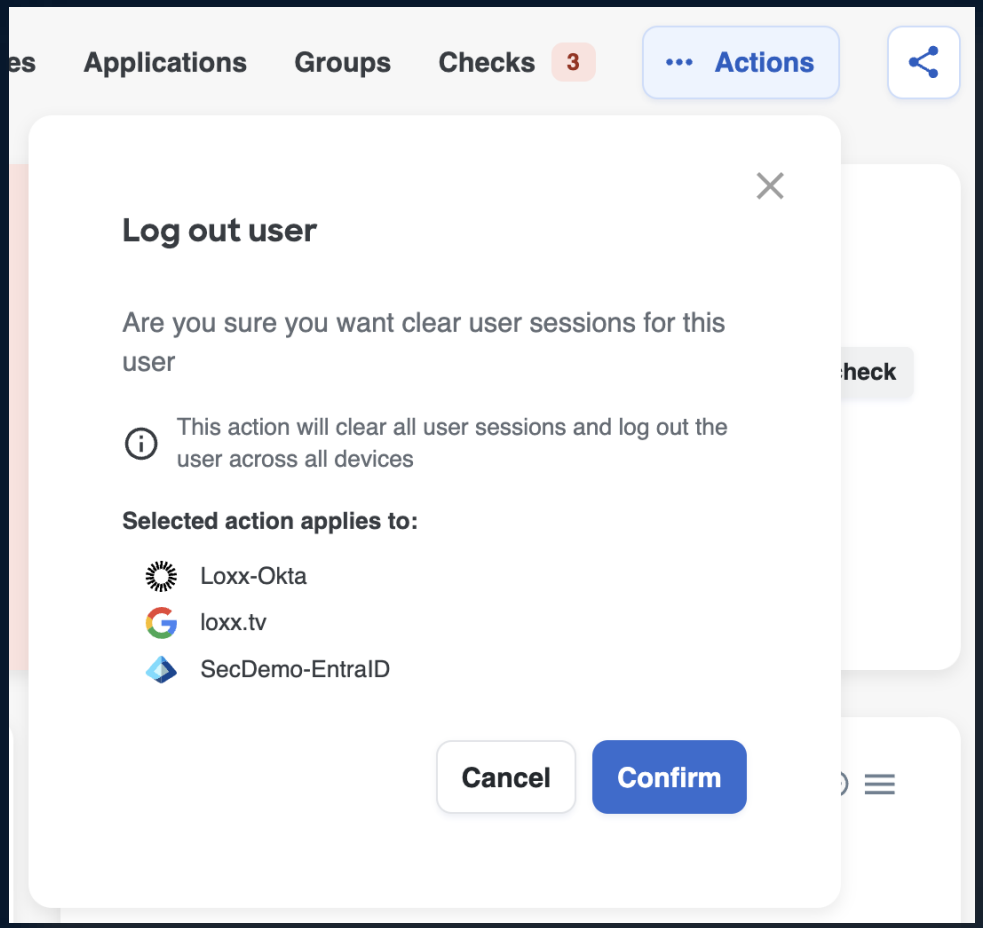
Context Specific Remediation Menu

- 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



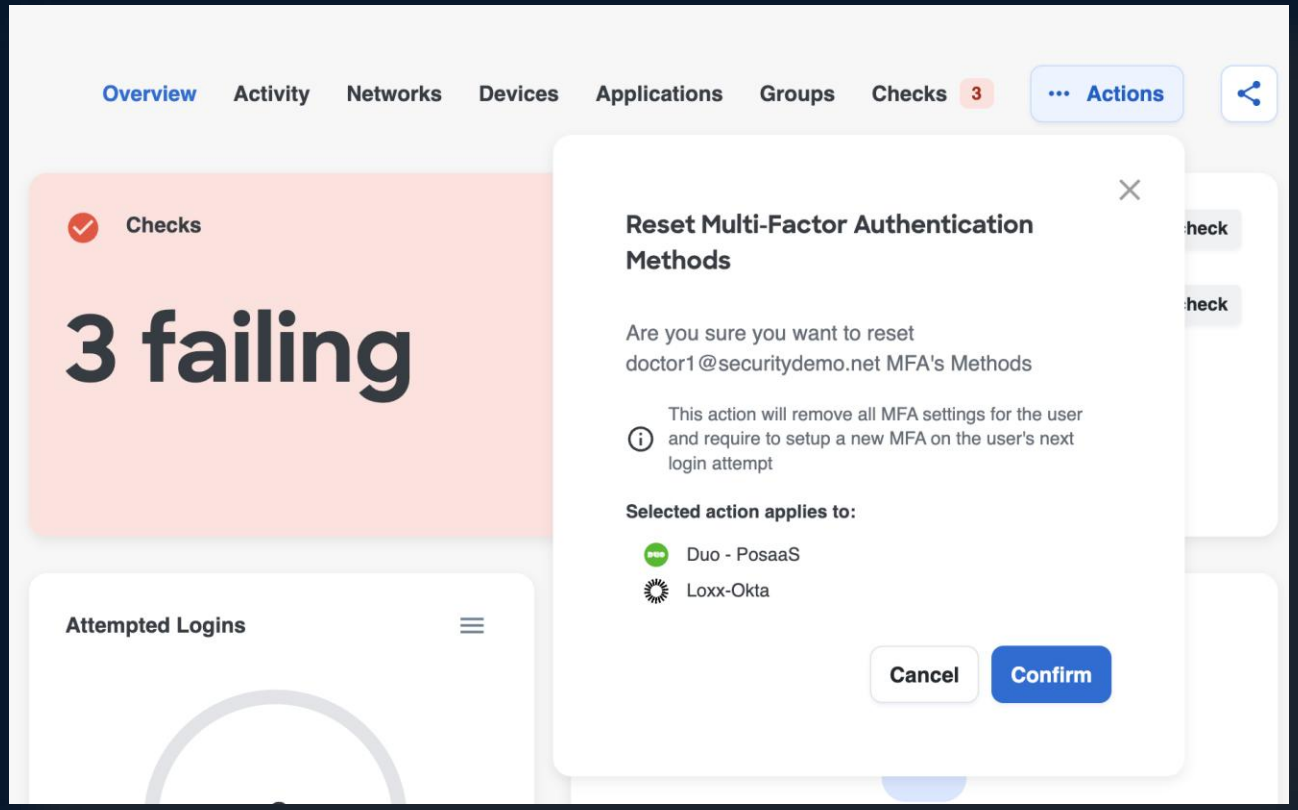
Log Out User

- Clears all user sessions
  - Logs out the user across the IDPs that support the function
- 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



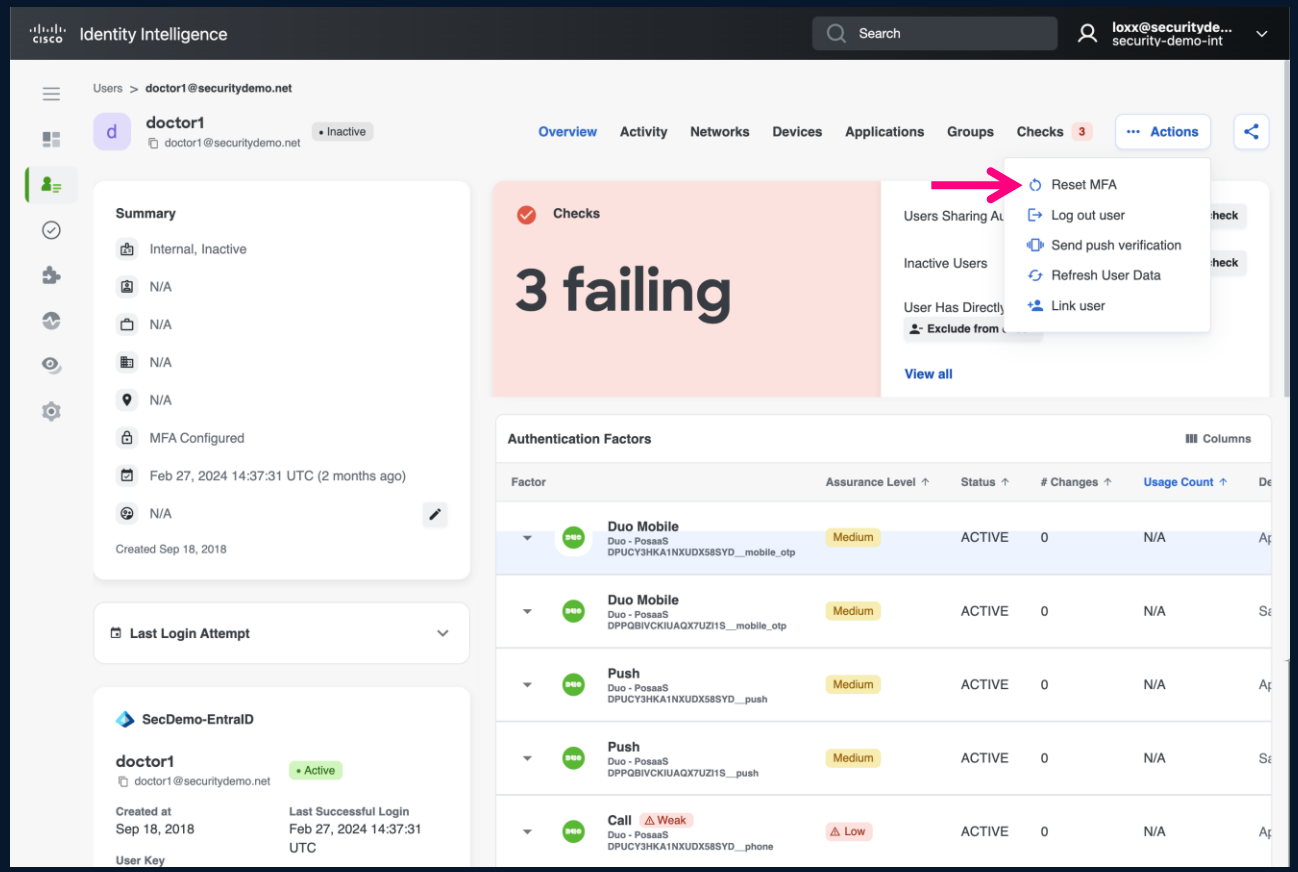
Reset MFA example w/ Duo

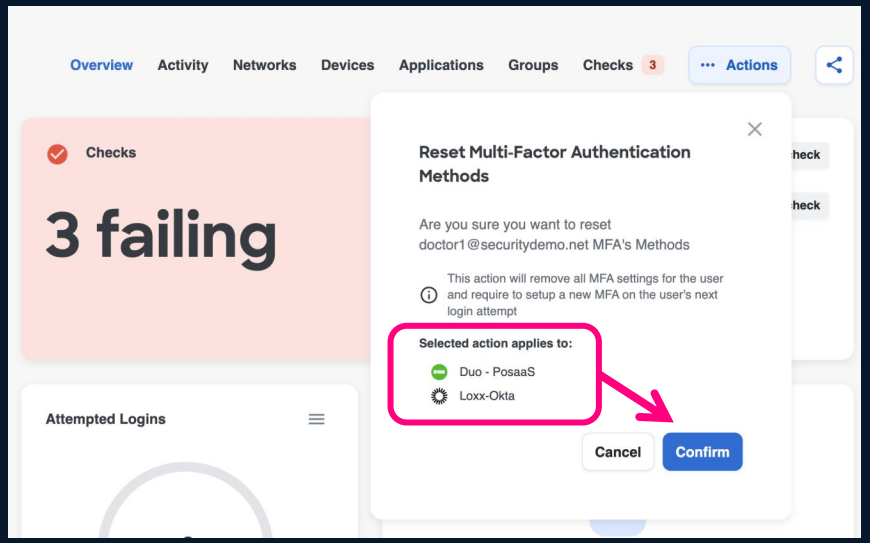
- CII queries the Duo Admin API
  - Learns all phones associated to user
  - Learns all hardware tokens for user
- CII Disassociates the user from the all their phones and tokens
  - User is as if they are brand-new
  - Have to setup MFA from scratch



Duo's Reset MFA

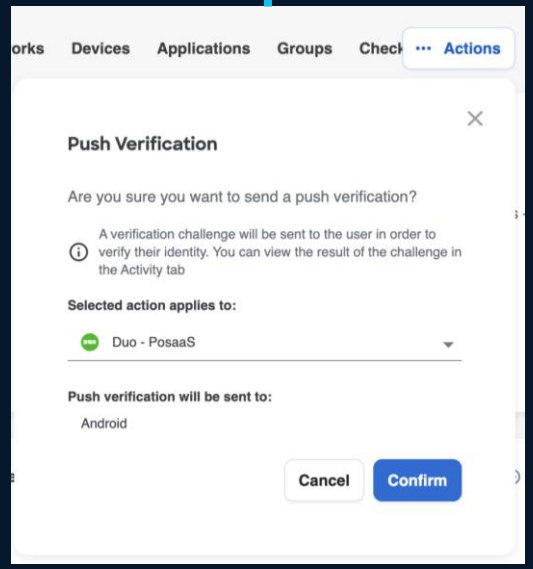
For Your Reference

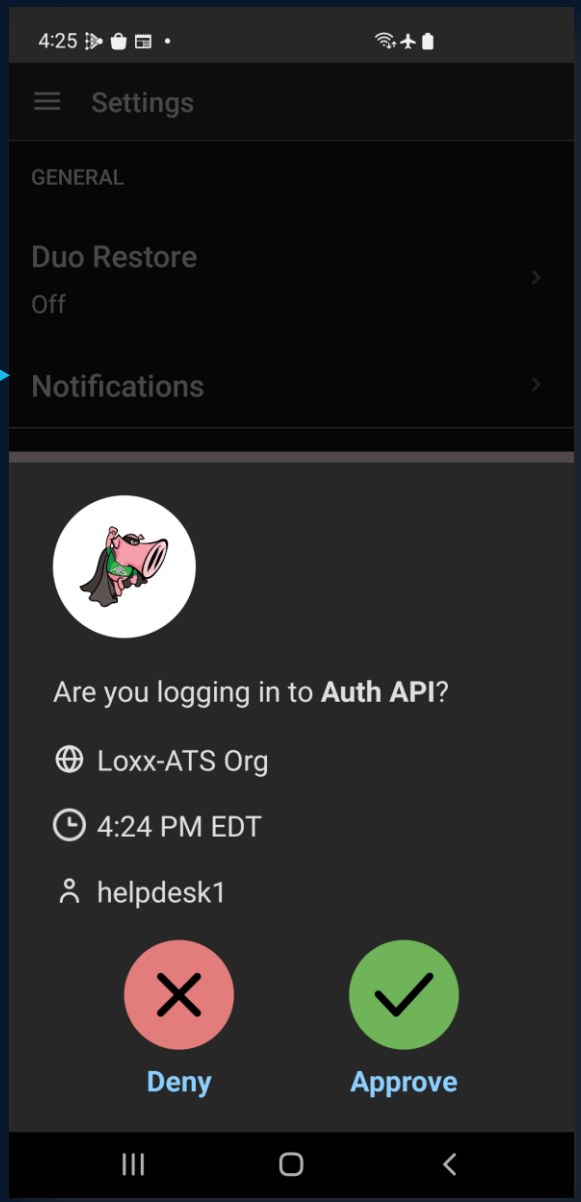




Send Push Notification

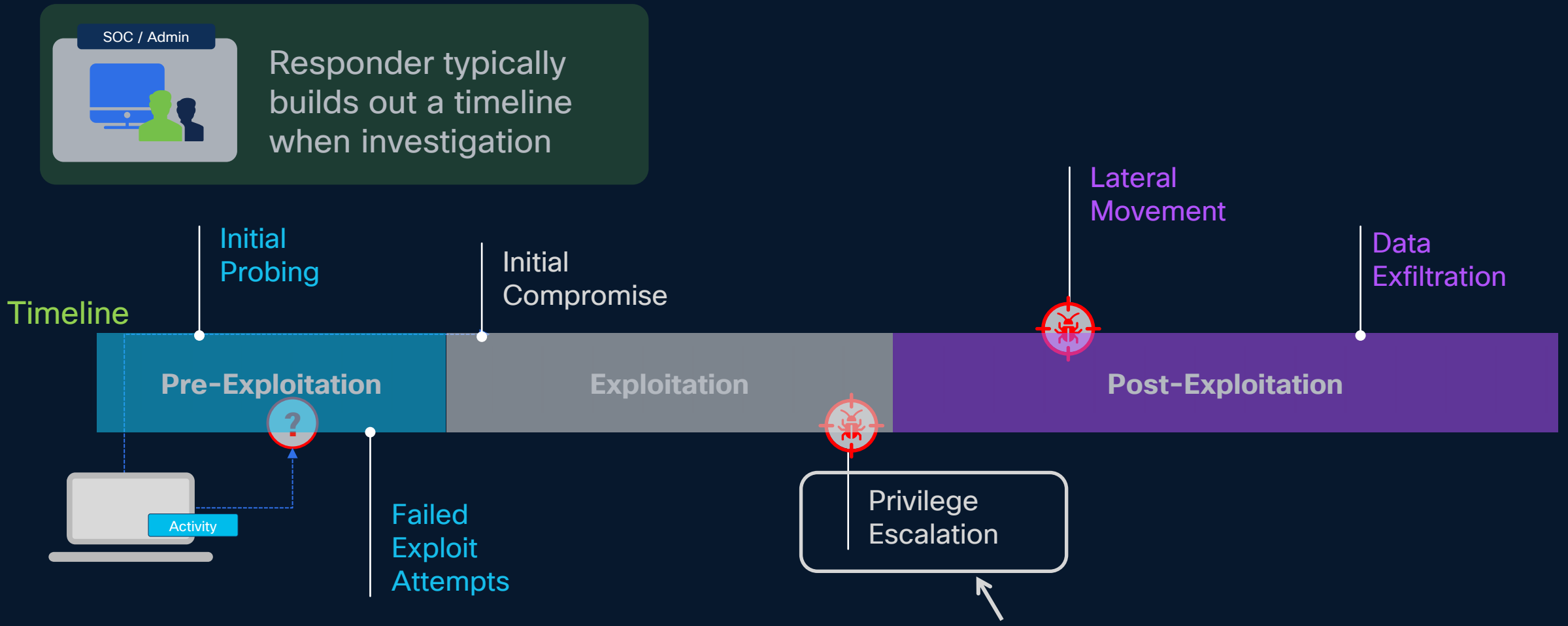
- To verify a user's identity
  - Send the user a one-time push notification to confirm they are who they say they are
  - Very helpful for help-desks to verify human calling them is indeed who they say they are
- Select the MFA provider
  - Click Confirm
  - Push notification is sent



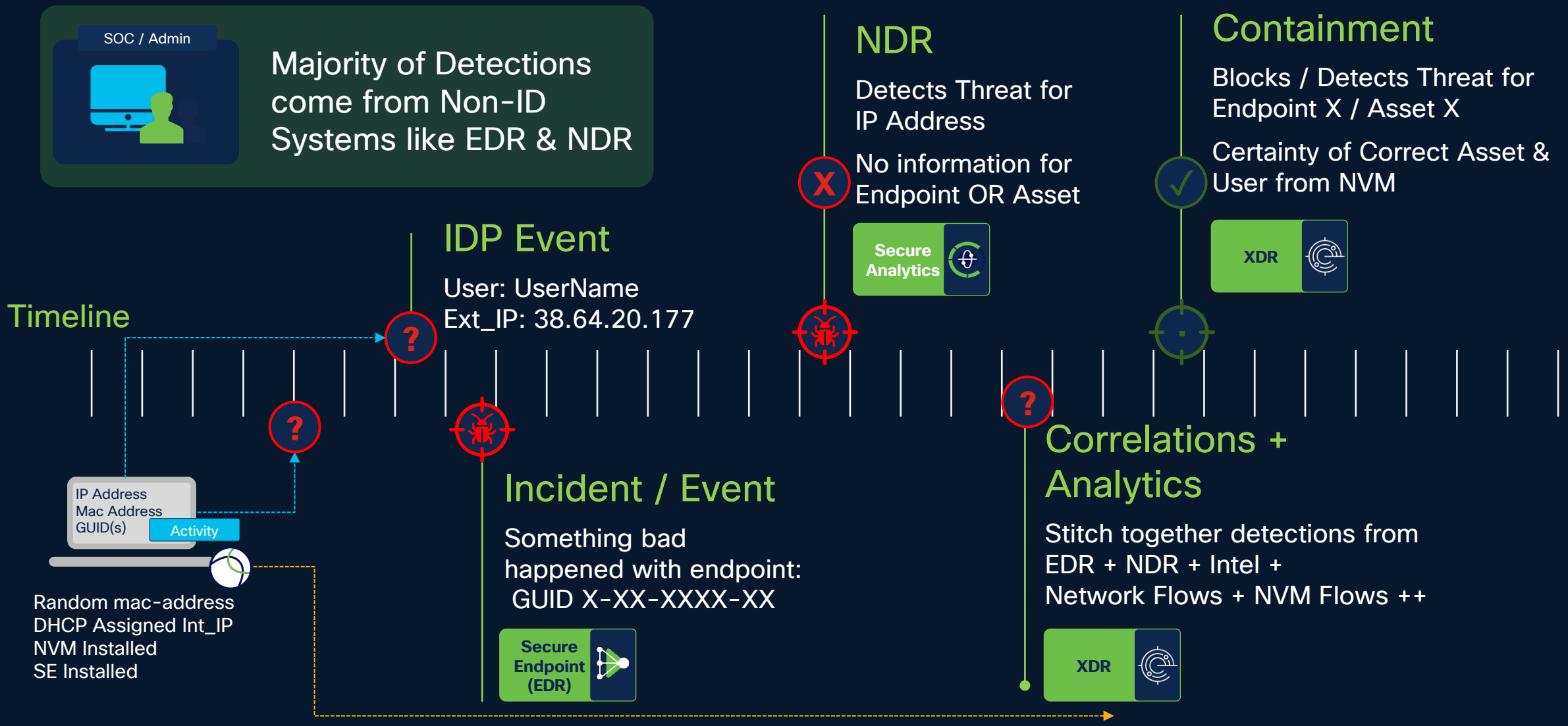


Leveraging Your Security Operations Center (SOC)

Investigation Timeline – what happened & when?

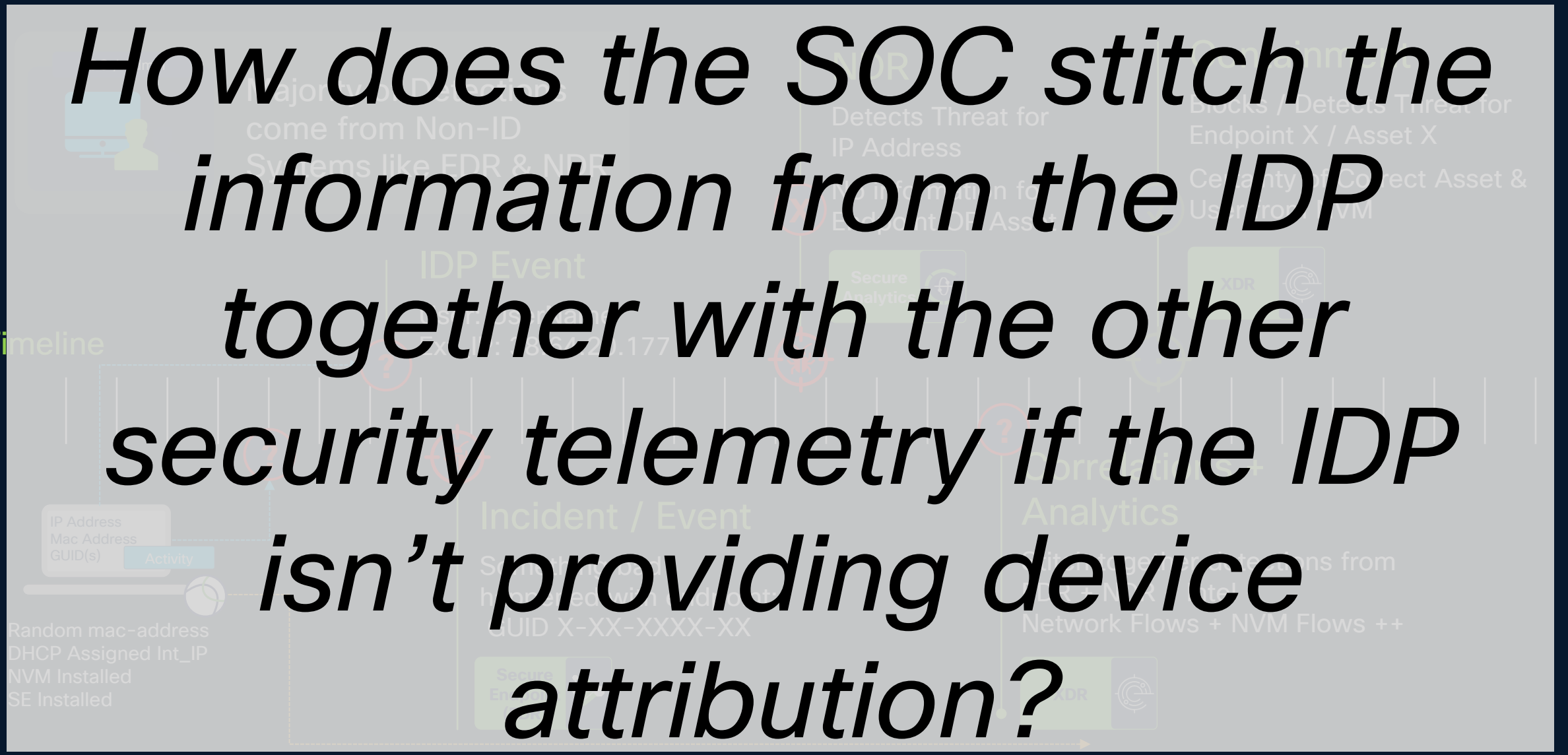


Investigation Timeline



Investigation Timeline

How does the SOC stitch the information from the IDP together with the other security telemetry if the IDP isn't providing device attribution?



Why Duo for the SOC

- With Duo Desktop, True binding of the User <> Device.
  - Critical to the SOC to stitch together the timeline of what has happened with the other security products.
- With IDP's, the Auth Logs include:
  - The external IP Address (which is often a NAT pool & often irrelevant to the investigation)
  - The userID (which is VERY relevant to the SOC),
  - The User Agent String (only mildly useful).
- Duo Desktop gets true cryptographic binding the unique endpoint and more!

MSFT IDP

"username": "Loxx"
"useragent": "Chrome"
"ip": "38.64.20.177"
"app": "Bloodhound"

Duo w/ Duo Desktop

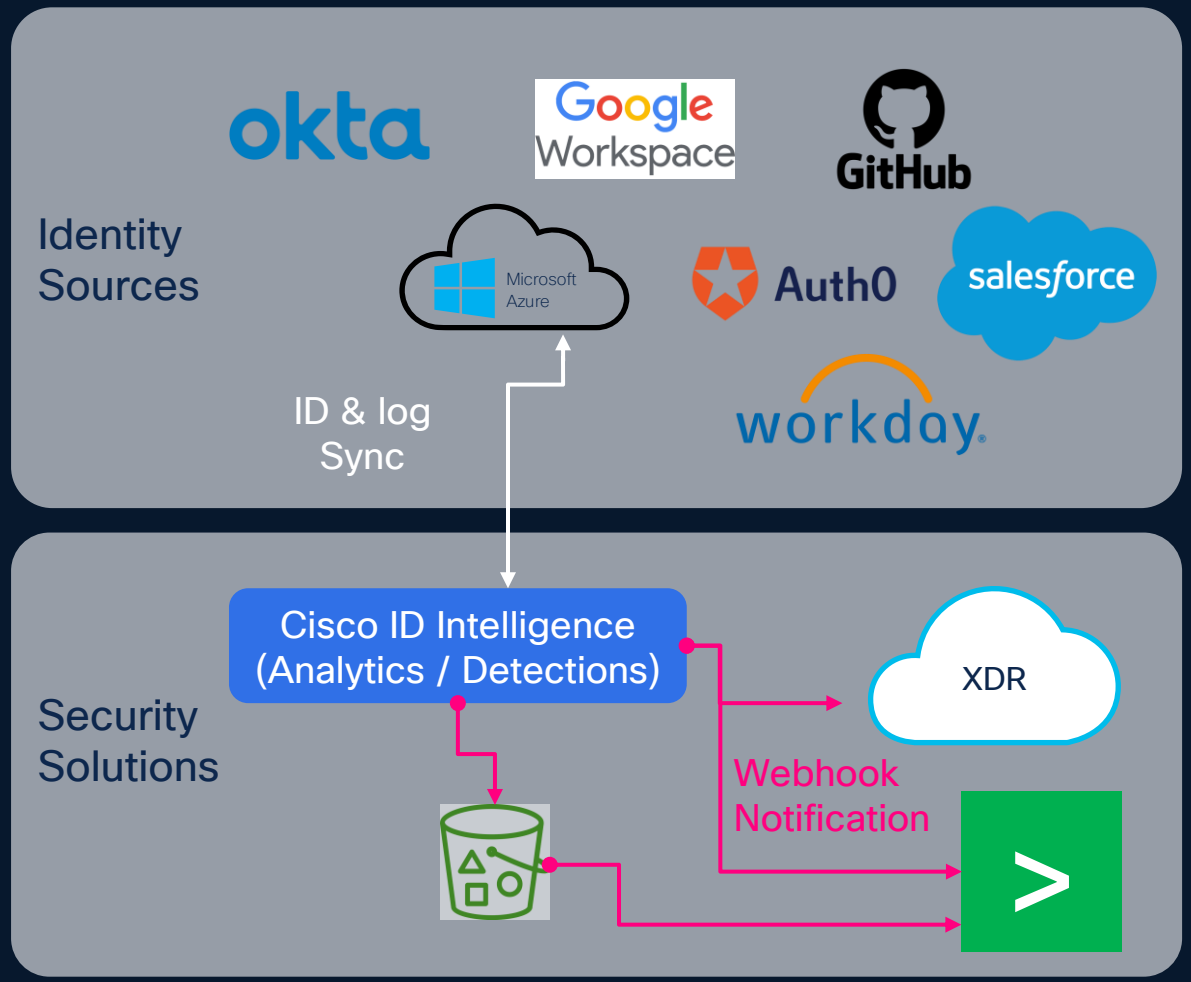
"browser": "Chrome",
"hostname": "ATW-WIN10-JUMP",
"ip": "38.64.20.177",
<Posture Details SNIP>

"machine_guid": "<SNIP>",

"location": {
"city": RTP,
"country": "United States",
"state": NC },
"adaptive_trust_assessments": {},
"alias": "unknown",
"application": {
"name": "Bloodhound"
},
"passport_assessment": {
"is_supported": false,
"reason": "unsigned_health_report"
},
"rbfs_triggered_attacks": null,
"reason": "user_approved",
"result": "success",
"trusted_endpoint_status": "not trusted",
"user": {
"groups": [
"oort_admins",
"LabUsers"
],
"name": "loxx"

Webhooks

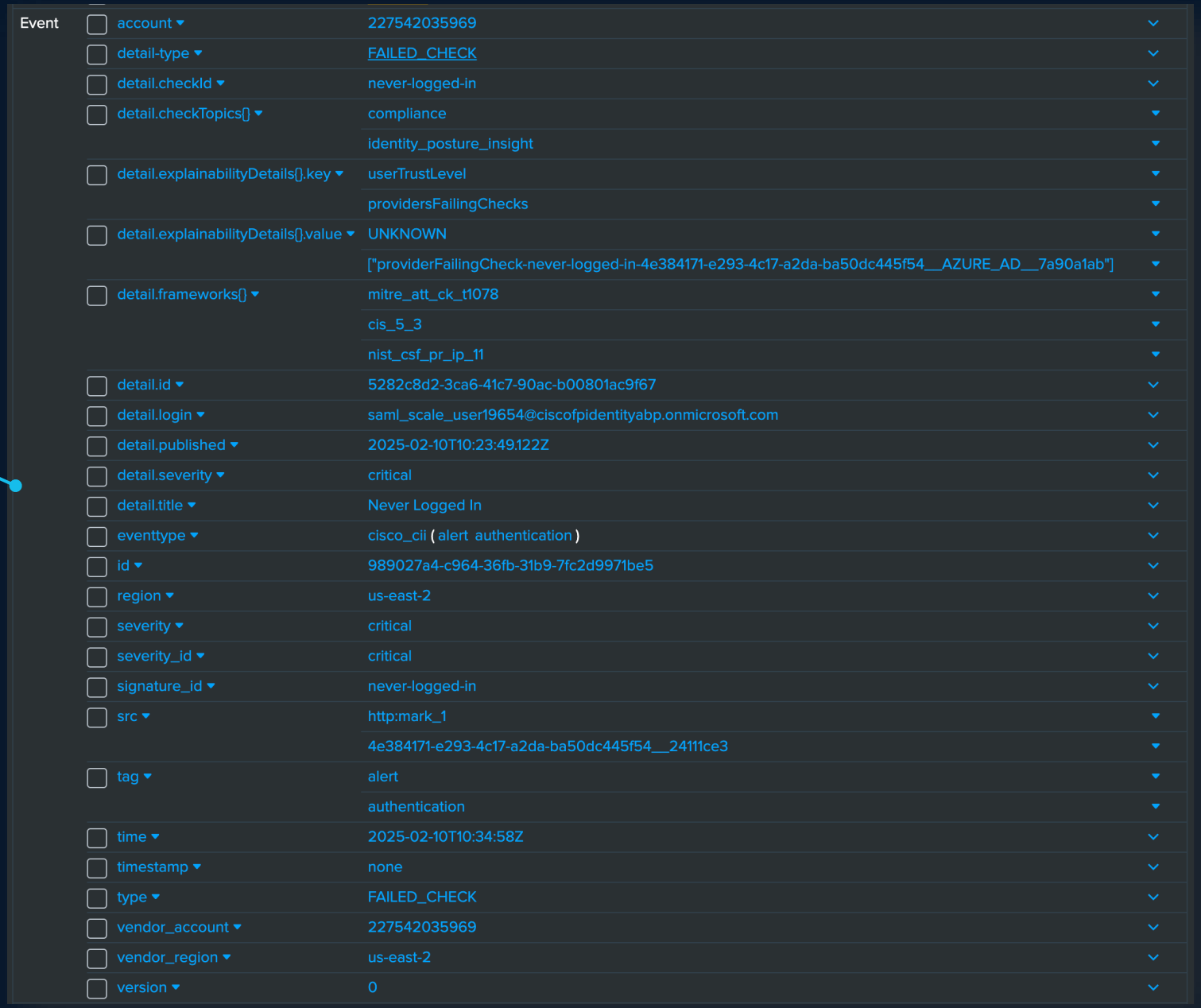
- A callback function that uses HTTP/S between two APIs based on events
  - Send small amounts of data, reactively after a check-fails
  - An example is CII sending a notice to Splunk SOAR or XDR of a check that failed
    - The automation playbook/workflow will extract the appropriate data and then proceed through the rest of the flow



What's in the Webhook?

Failed Checks

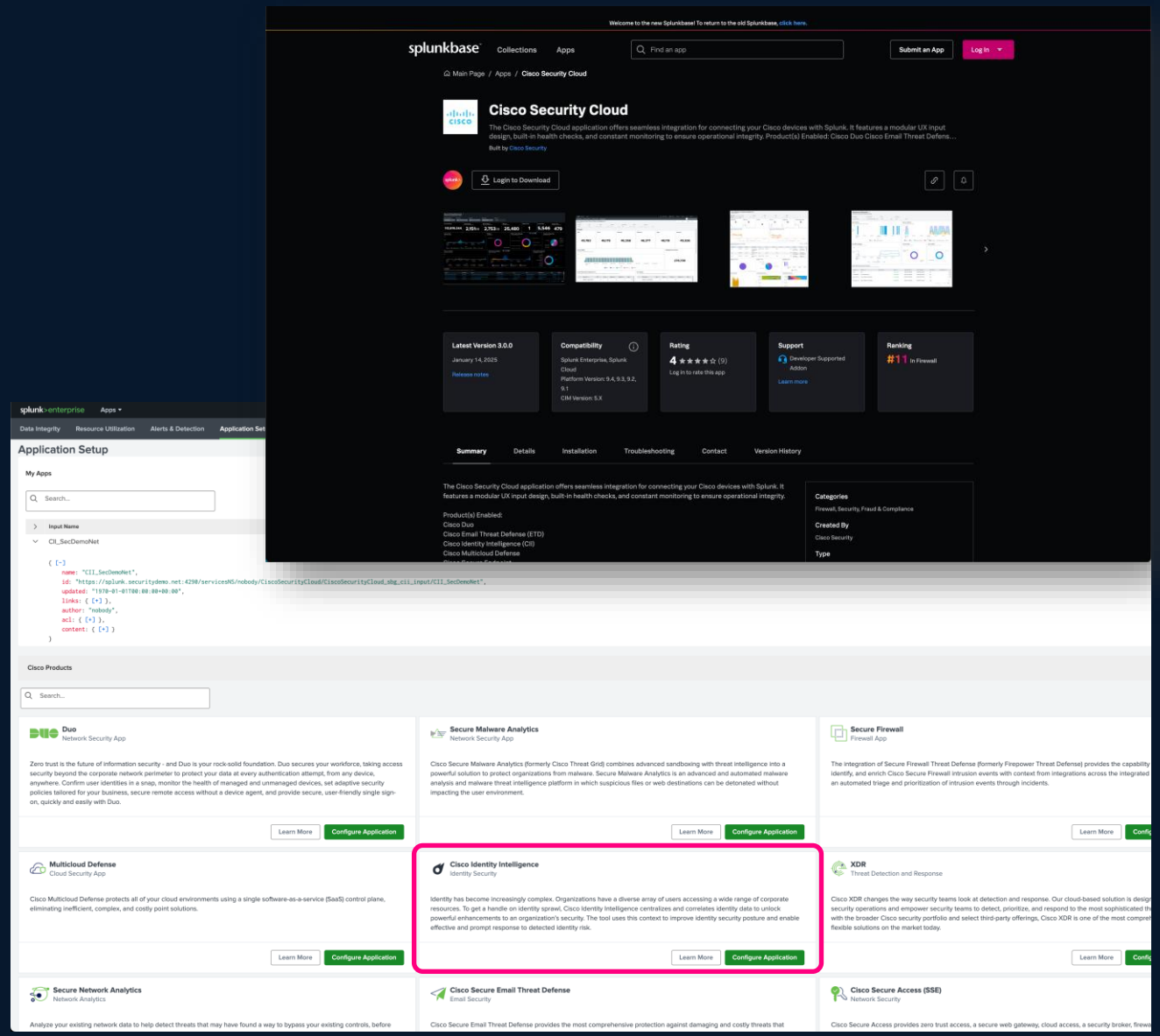
Ie.: A matched signature.
- Check Name
- Details
- ATT&CK Categorization
- Severity
- Tags
- Unique ID's



Event		
	account	227542035969
	detail-type	FAILED_CHECK
	detail.checkId	never-logged-in
	detail.checkTopics{}	compliance
		identity_posture_insight
	detail.explainabilityDetails{}.key	userTrustLevel
		providersFailingChecks
	detail.explainabilityDetails{}.value	UNKNOWN
		["providerFailingCheck-never-logged-in-4e384171-e293-4c17-a2da-ba50dc445f54__AZURE_AD__7a90a1ab"]
	detail.frameworks{}	mitre_att_ck_t1078
		cis_5_3
		nist_csf_pr_ip_11
	detail.id	5282c8d2-3ca6-41c7-90ac-b00801ac9f67
	detail.login	saml_scale_user19654@ciscofpidentityabp.onmicrosoft.com
	detail.published	2025-02-10T10:23:49.122Z
	detail.severity	critical
	detail.title	Never Logged In
	eventtype	cisco_cii (alert authentication)
	id	989027a4-c964-36fb-31b9-7fc2d9971be5
	region	us-east-2
	severity	critical
	severity_id	critical
	signature_id	never-logged-in
	src	http:mark_1
		4e384171-e293-4c17-a2da-ba50dc445f54__24111ce3
	tag	alert
		authentication
	time	2025-02-10T10:34:58Z
	timestamp	none
	type	FAILED_CHECK
	vendor_account	227542035969
	vendor_region	us-east-2
	version	0

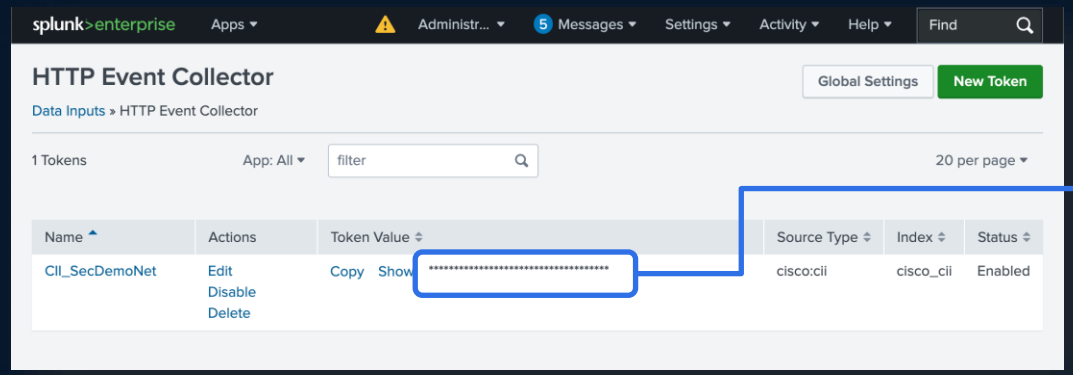
App (TA) in Splunk

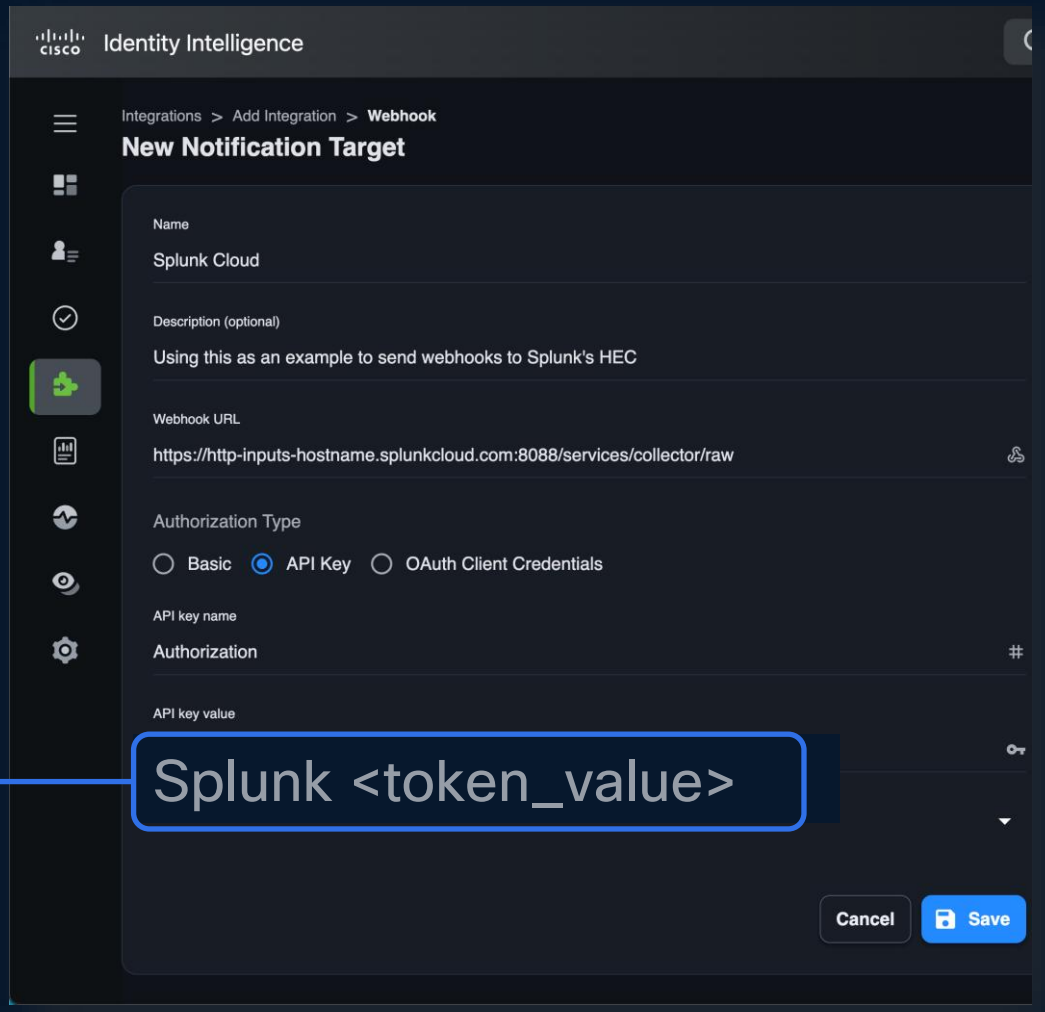
- Cisco Security Cloud App
  - Used for many Cisco Security Products, such as Duo, Firewall, etc.
  - Cisco Identity Intelligence is included.
  - Leverages an HTTP Event Collector (HEC) for Data input.
    - Must use a public signed certificate (today).



Cisco Security App (TA) in Splunk

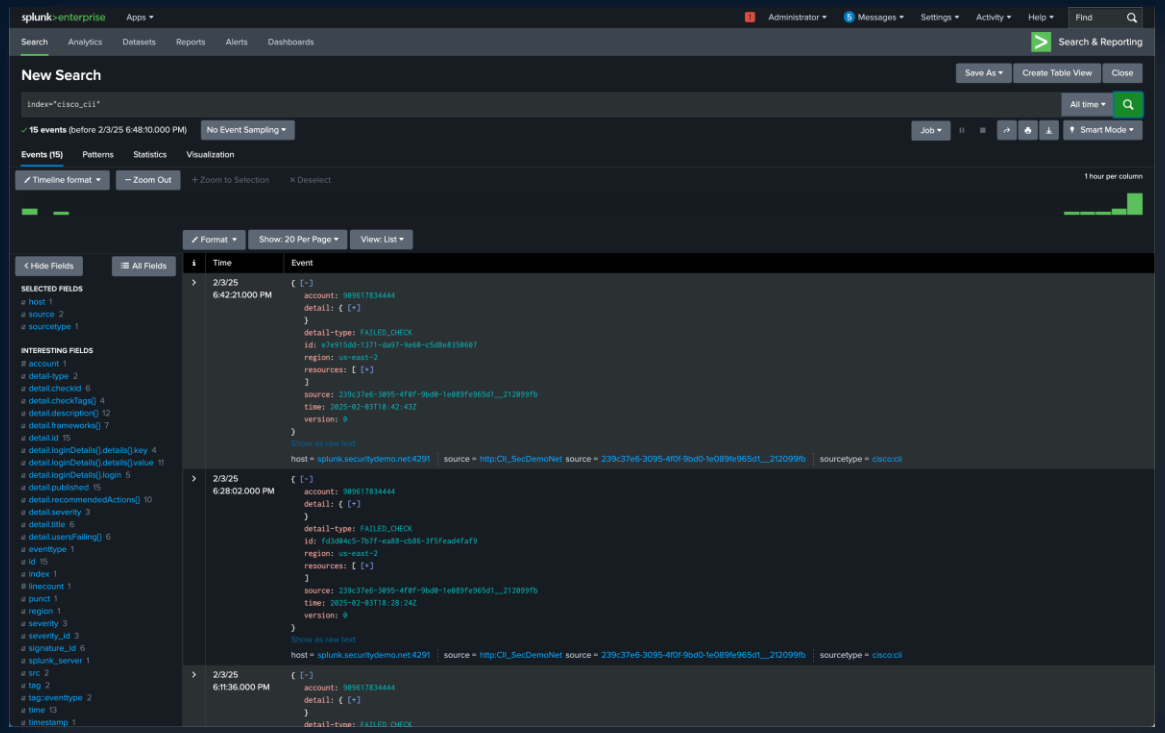
- Add webhook in CII for the HEC in Splunk
  - Ensure the URL includes “/services/collector/raw”
  - Authorization type = API Key
  - API Key value must be “Splunk” + a space, then the token value.

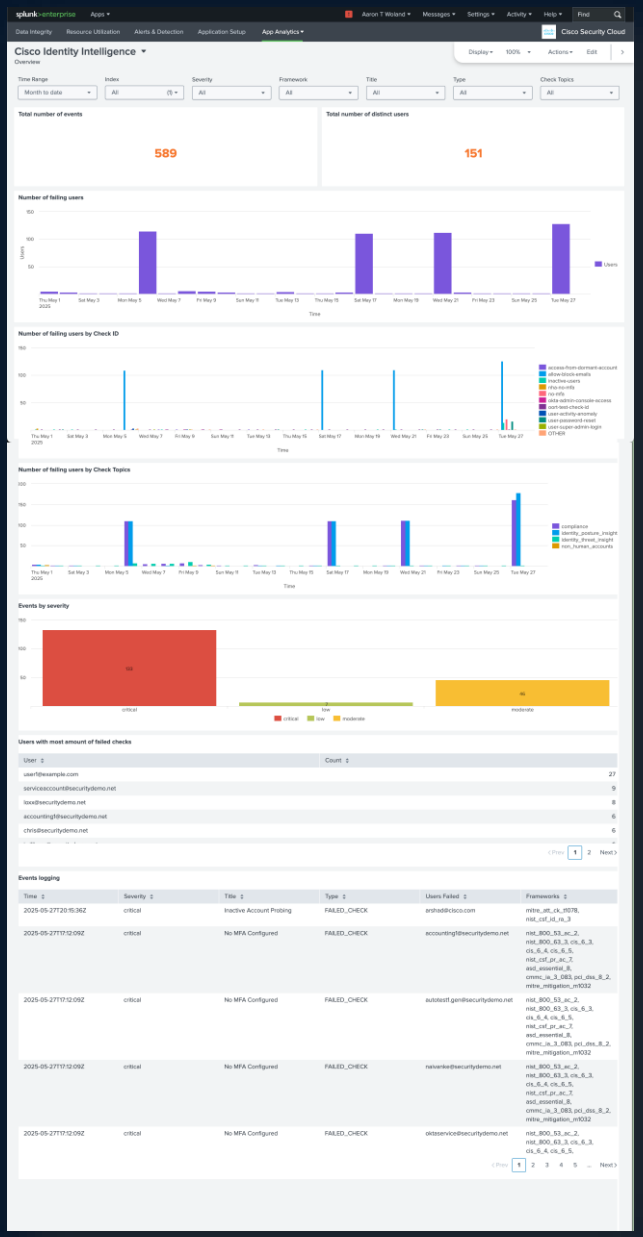




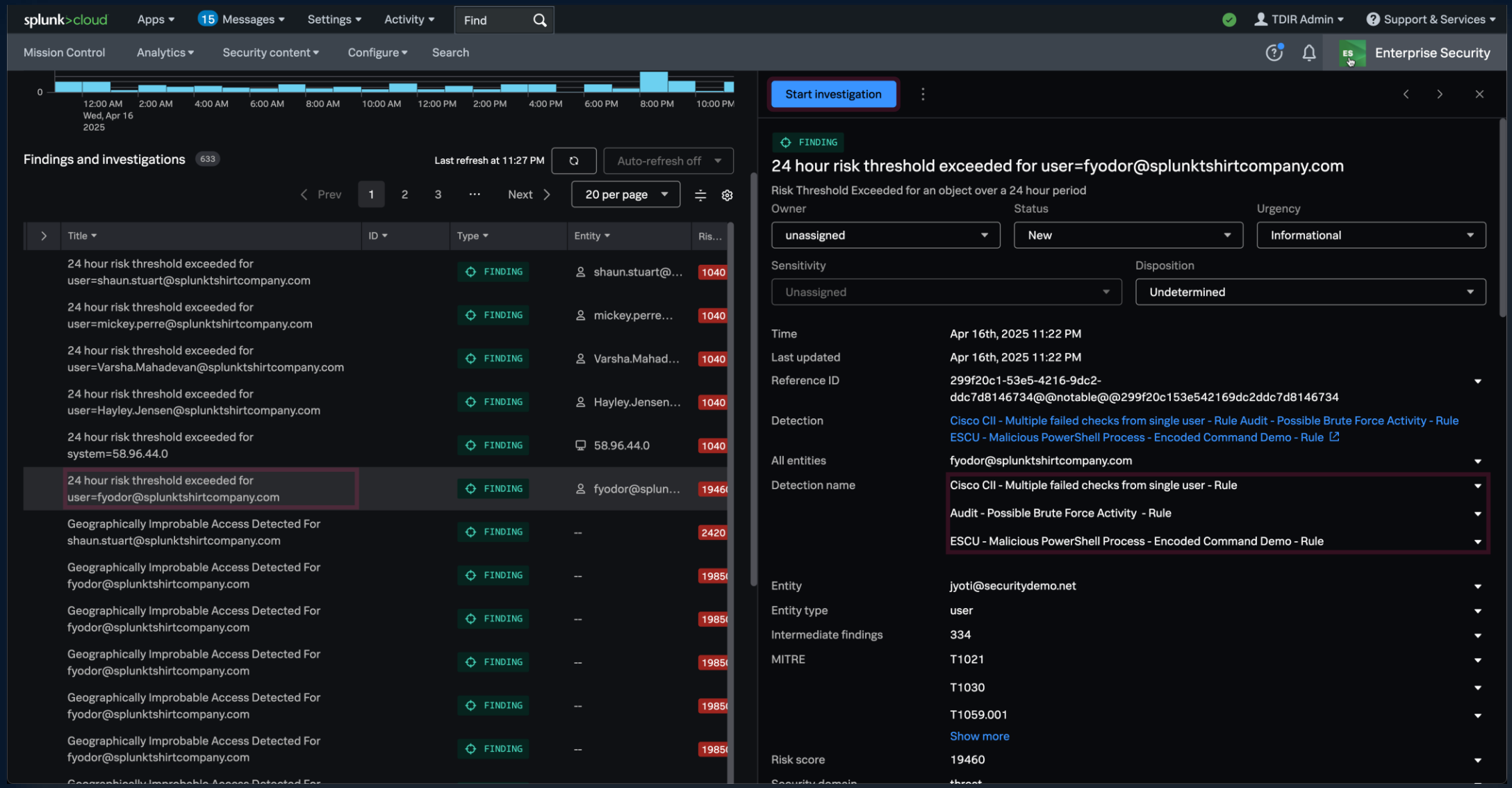
Cisco Security App (TA) in Splunk

- Cisco Identity Intelligence app has a dashboard
  - Creates the “cii_index"
  - Has a dashboard for the data



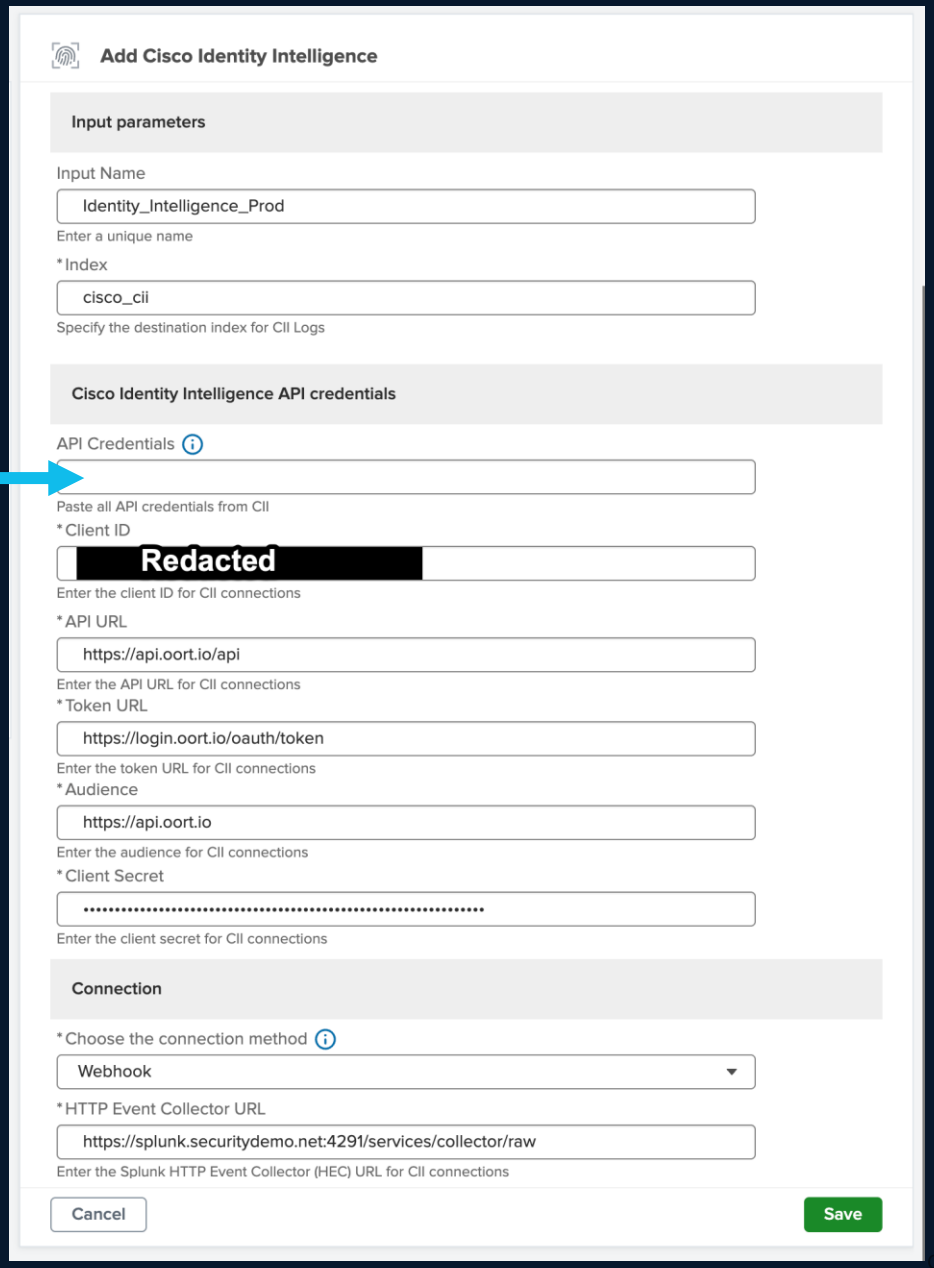


More can be done with Enterprise Security



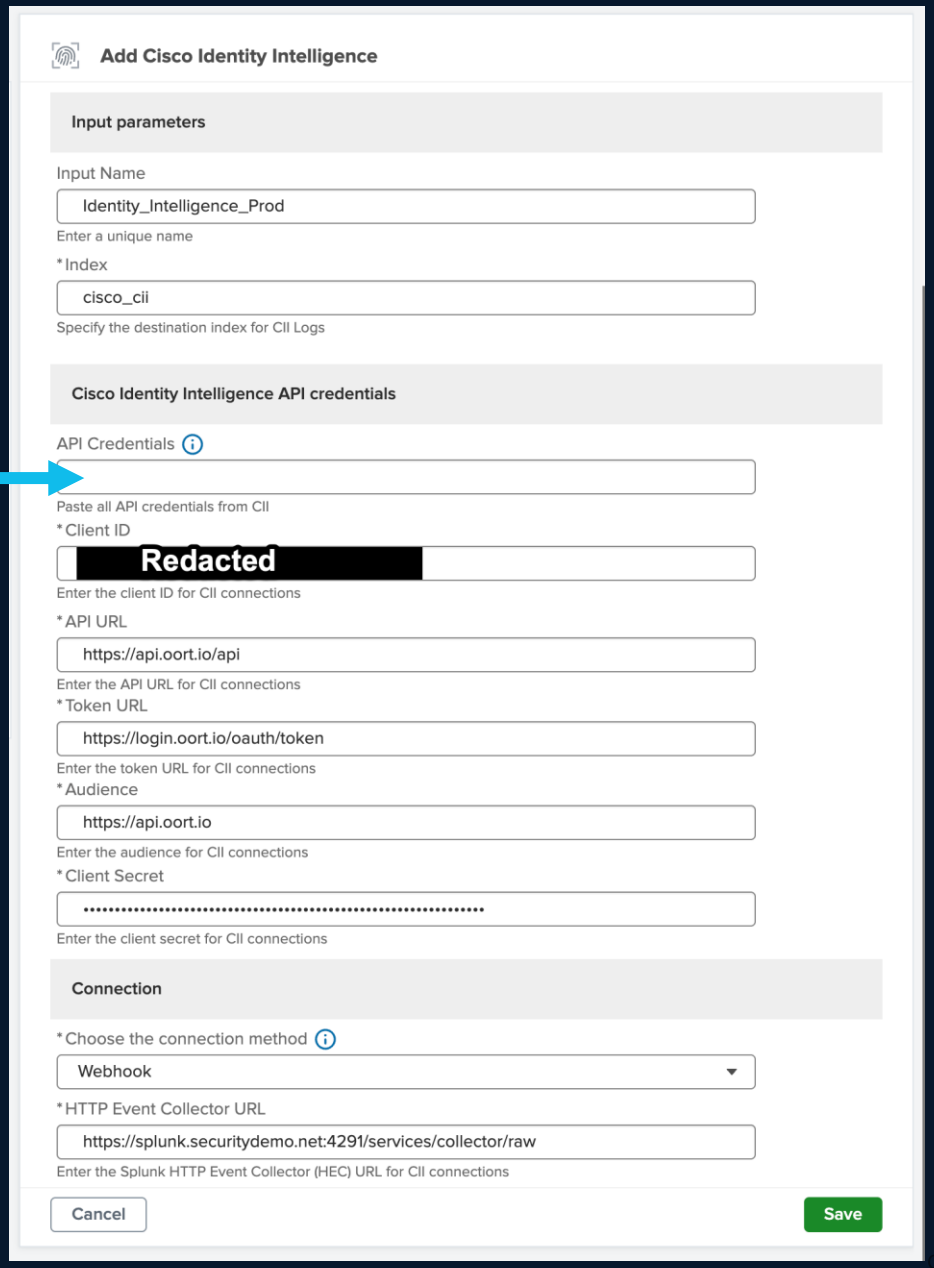
Splunk App <> CII Integration Configuration

- What was needed
  - Splunk requires an HTTP Event Collector (HEC) to receive the data from CII
  - Splunk requires an index to store the data in
  - Splunk Dashboards to display the data
  - CII requires a webhook target to be created for failed check notifications
  - CII checks must be configured to send notifications to the webhook
- What was delivered via the App:
  - Create an API key in CII
  - Paste the info into Splunk
  - The App creates everything needed on both sides!



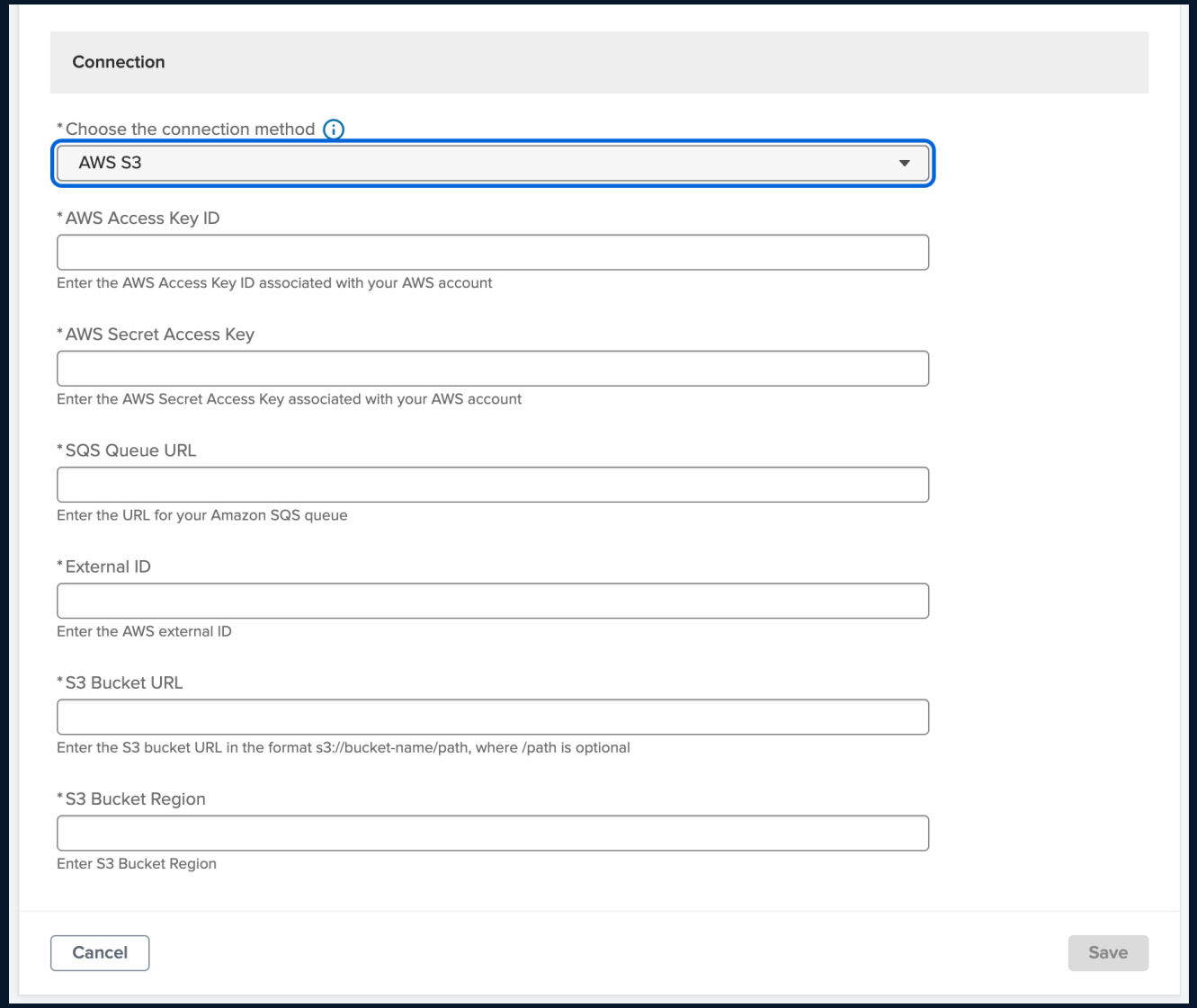
Splunk App <> CII Integration Configuration

- Paste the entire JSON into this field
  - The form fills out all fields with the available data
- Audience is no longer issued or needed by CII, but the Splunk TA still requires it
  - Use “http://api.oort.io”as the audience.
- HTTP Event Collector is Splunk’s Webhook Listener
  - Default port for collector is 8088
  - Splunk automatically defines a token to authenticate to the listener & configures CII to use that token



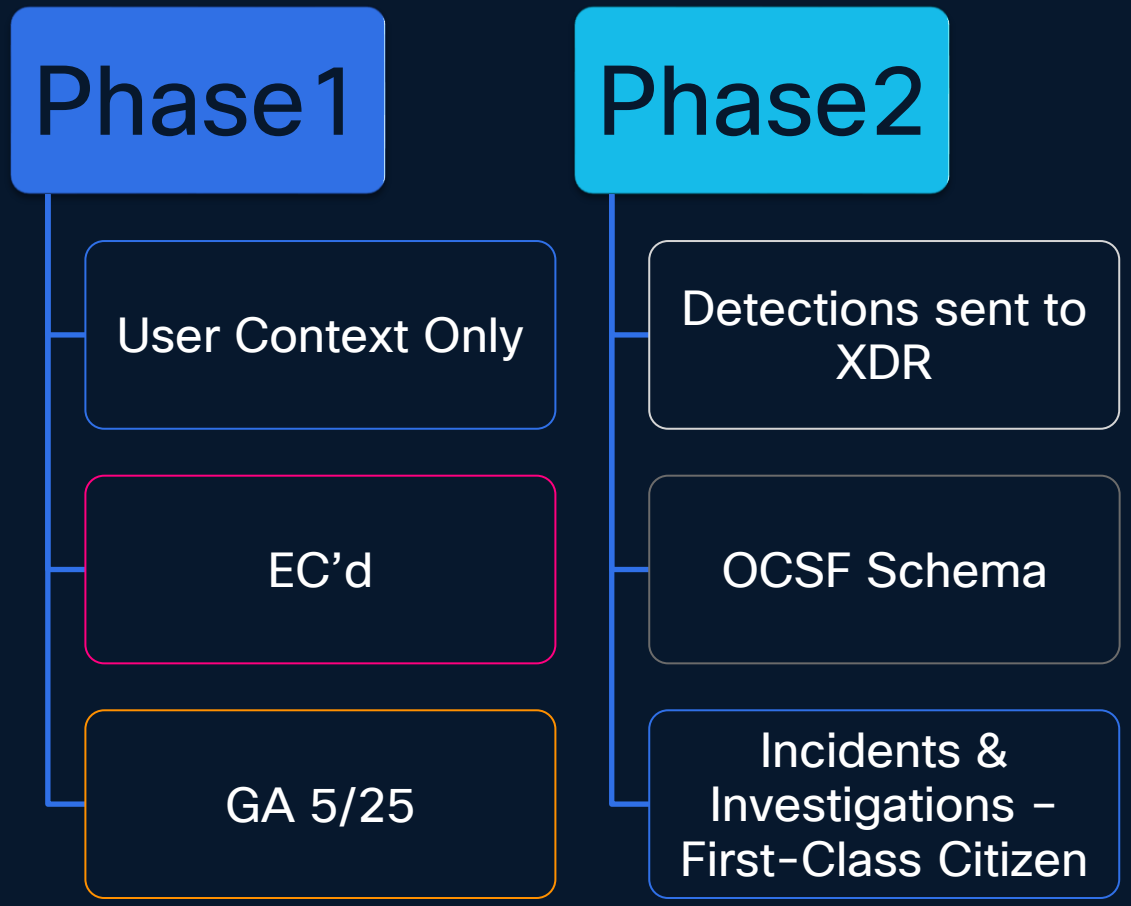
Alternative to HEC

- CII uses Amazon Event Bridge to send webhooks
  - Source IP from those webhooks could be one of hundreds of IP-ranges
    - Most customers not interested in opening their ACLs to the HEC to that many IP addresses.
  - Alternatively, the customer can provide CII w/ details for an S3 bucket.
    - The Splunk TA will collect from the bucket in a PULL instead of listening for the webhook.



Cisco XDR

Phased Integration



Phase 1
Released May 2025

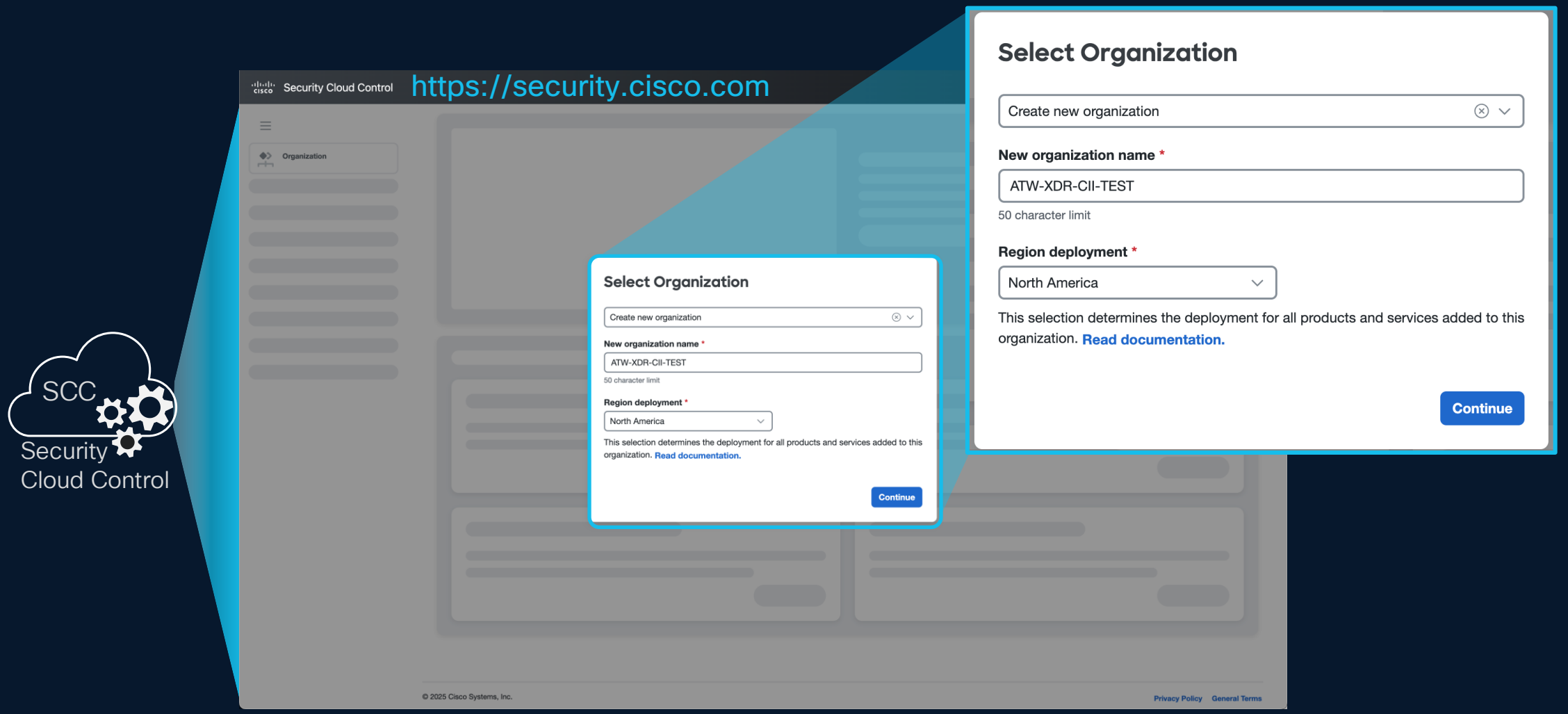
XDR Essentials+ Includes “Identity Intelligence Services”

- XDR is Threat Detection & Response product
  - Therefore, XDR plans to include a full ITDR experience within its own user interface
  - XDR has invested millions into the User Experience of the solution
  - Pivoting out of the XDR UI is deemed a non-starter
- As of May 2025, all XDR Customers are entitled to the Identity Intelligence Services
  - This is not the full Cisco Identity Intelligence product, which is available only via Duo Licenses
  - XDR is required to be attached to a Security Cloud Control (SCC) Enterprise

NOTE: This works the *SAME* way with Secure Access, which also include “Identity Intelligence Services”.

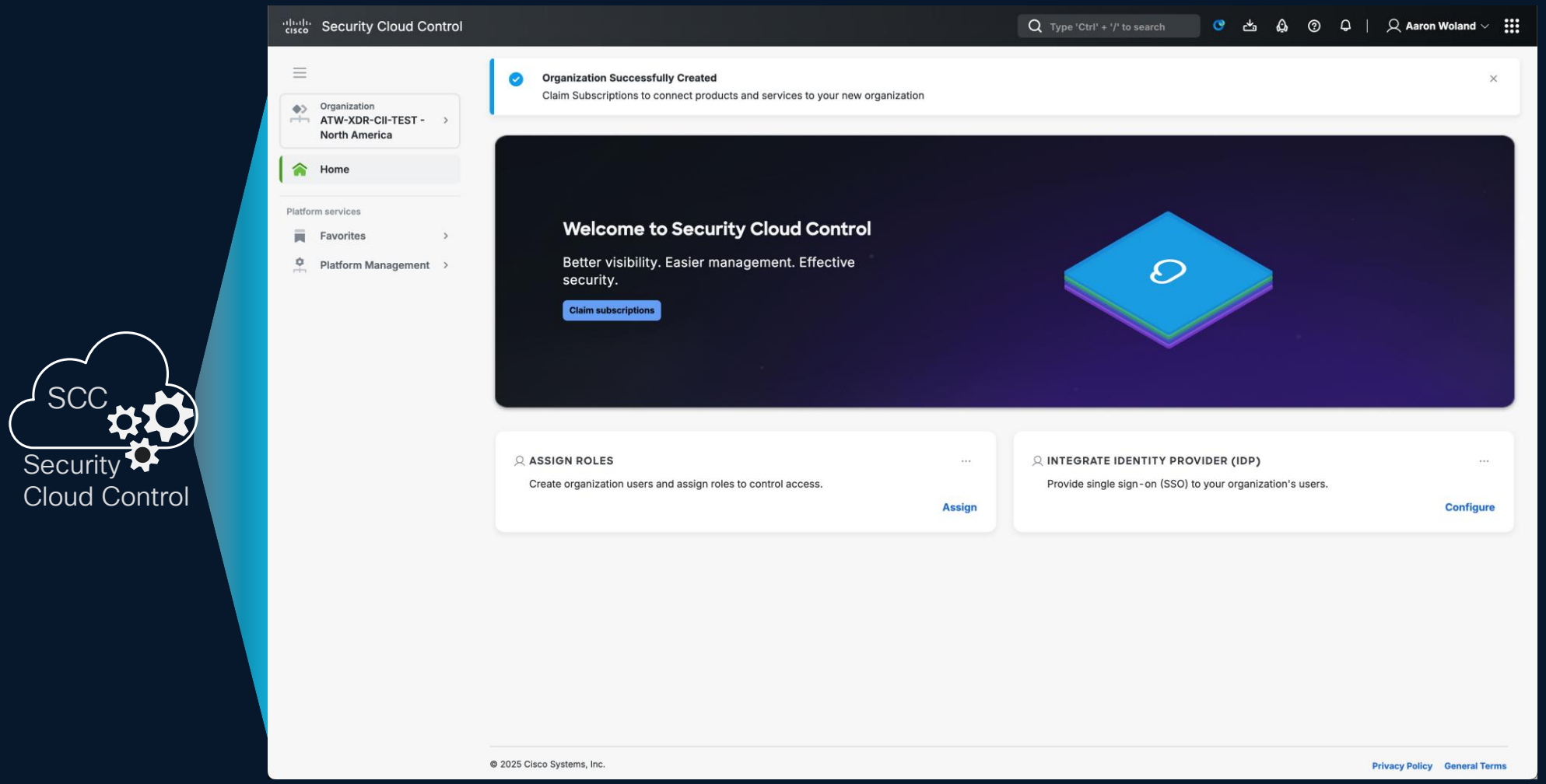
XDR leverages Security Cloud Control (SCC)

XDR Advantage+ (or suite) claim codes entered in SCC



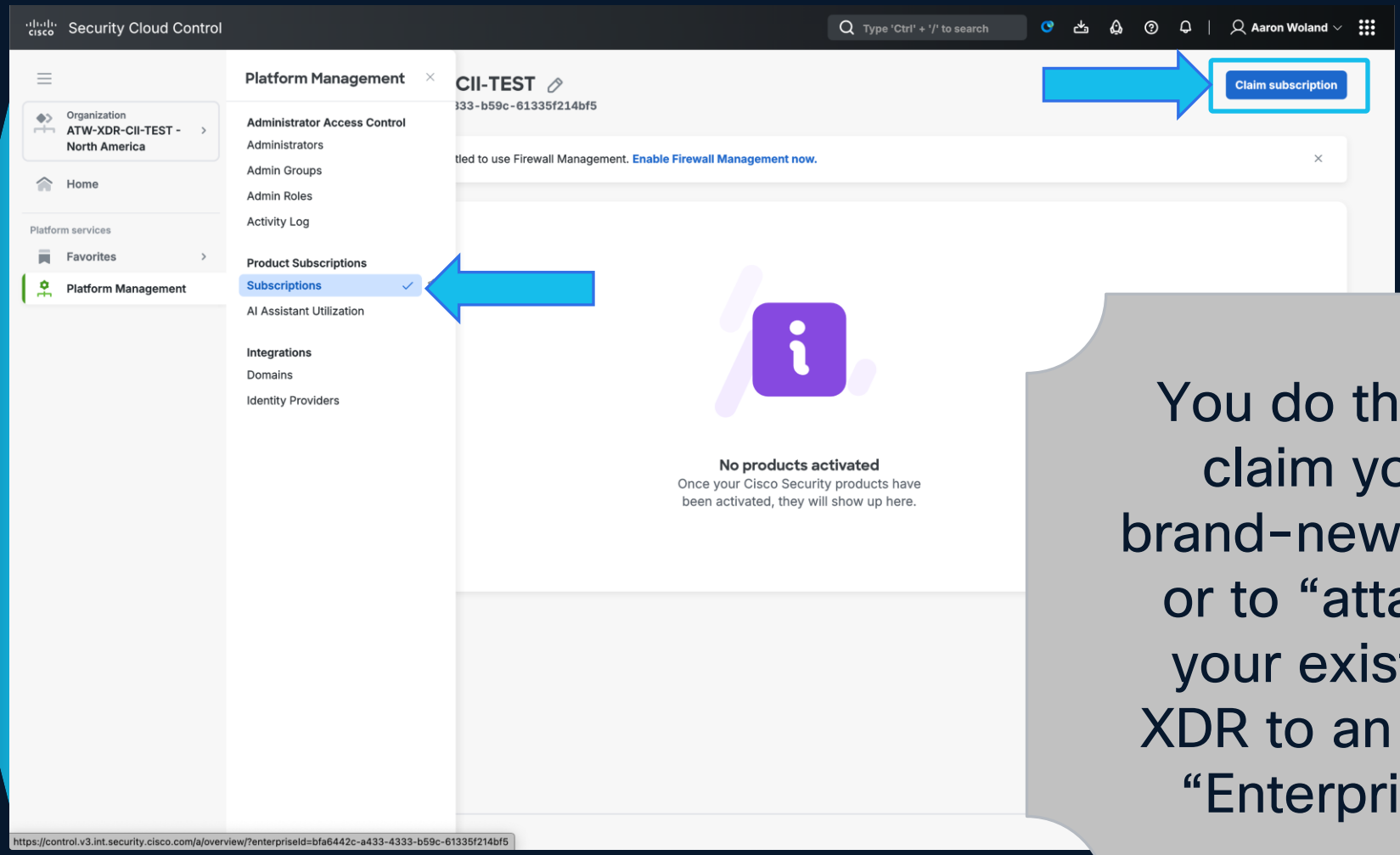
XDR leverages Security Cloud Control (SCC)

XDR Advantage+ (or suite) claim codes entered in SCC



XDR leverages Security Cloud Control (SCC)

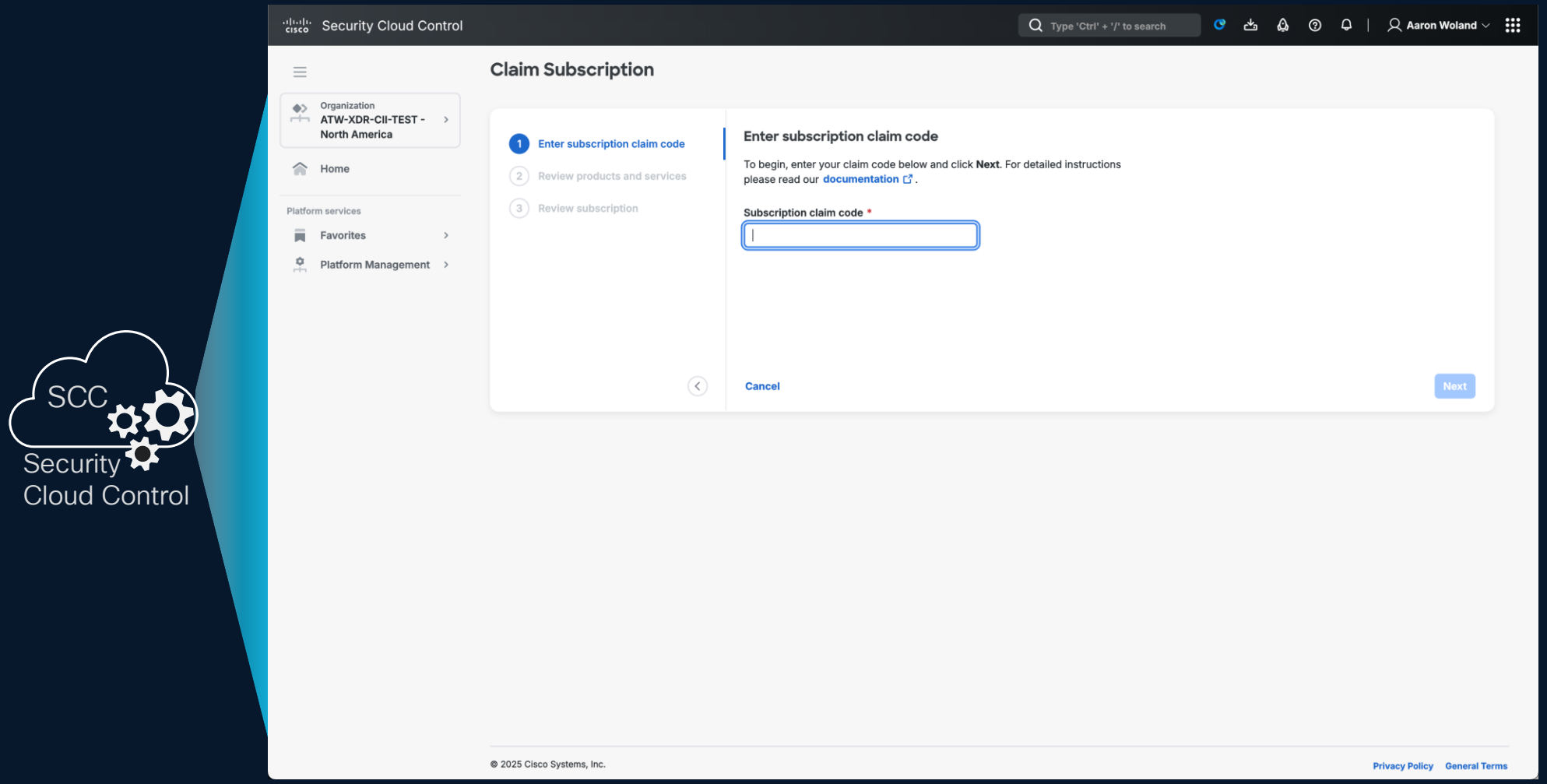
You must claim a subscription to attach/activate XDR



You do this to claim your brand-new XDR, or to “attach” your existing XDR to an SCC “Enterprise”

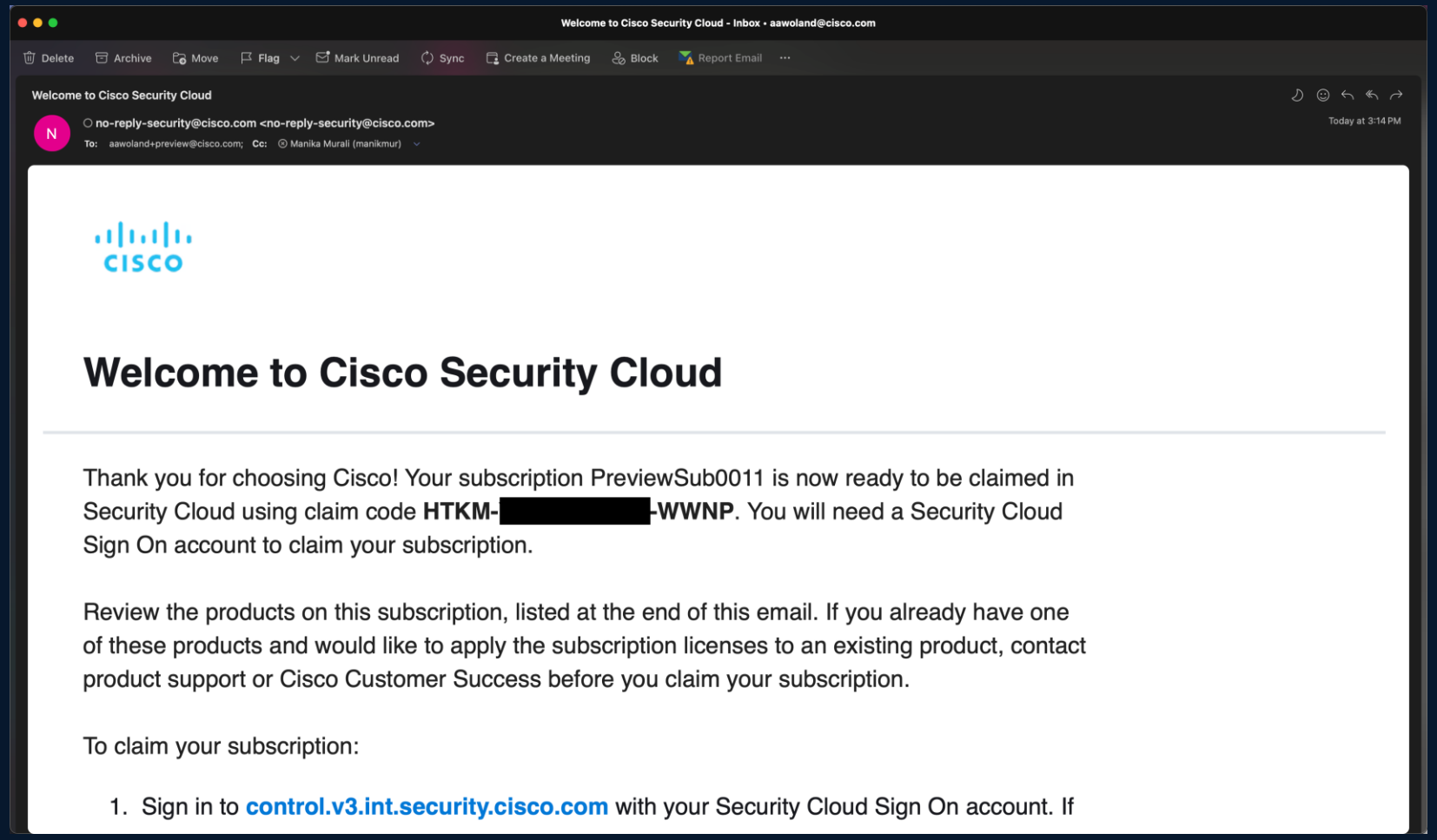
XDR leverages Security Cloud Control (SCC)

You paste the claim code, go check your email...



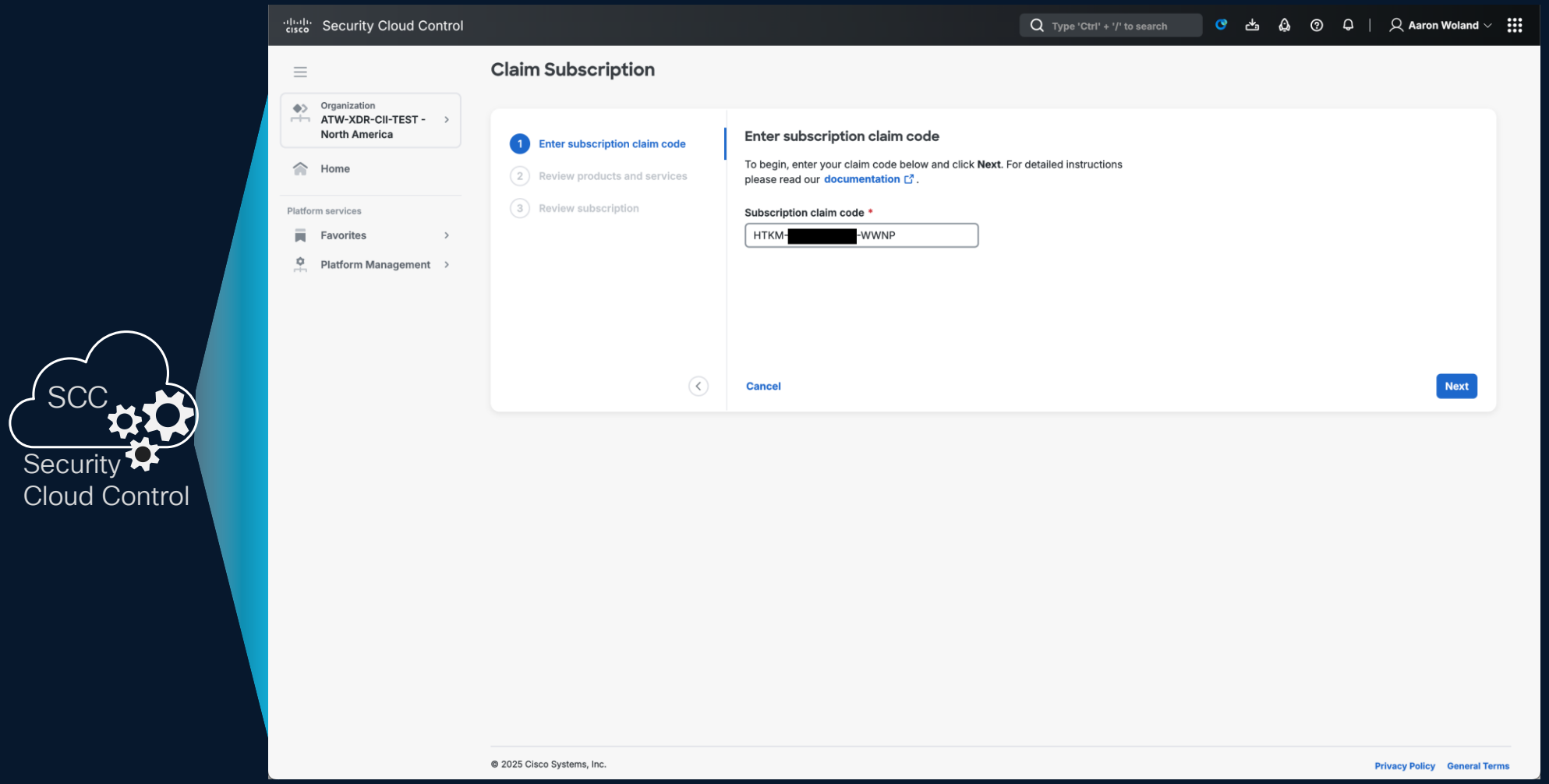
XDR leverages Security Cloud Control (SCC)

The claim code is in your email. Copy it.



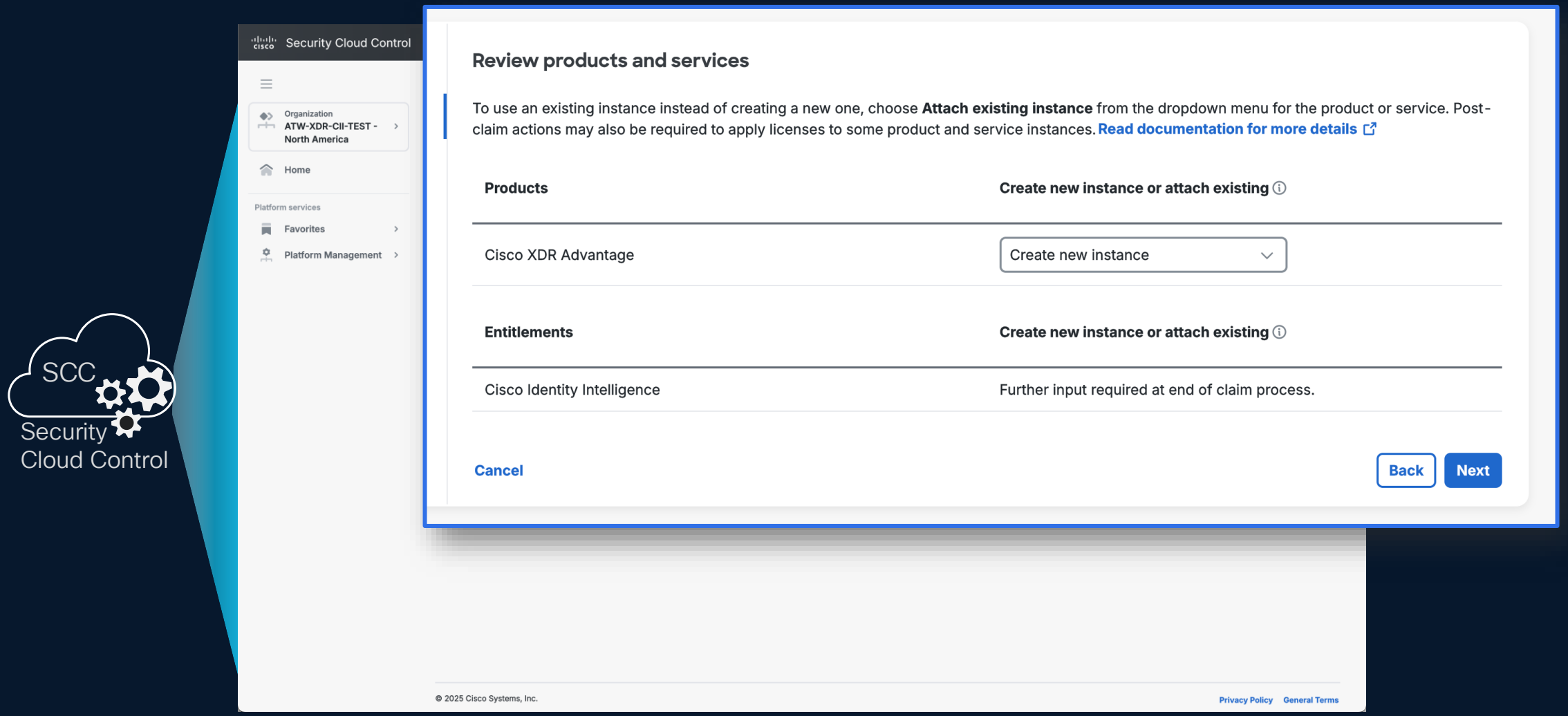
XDR leverages Security Cloud Control (SCC)

Paste the claim-code & click next



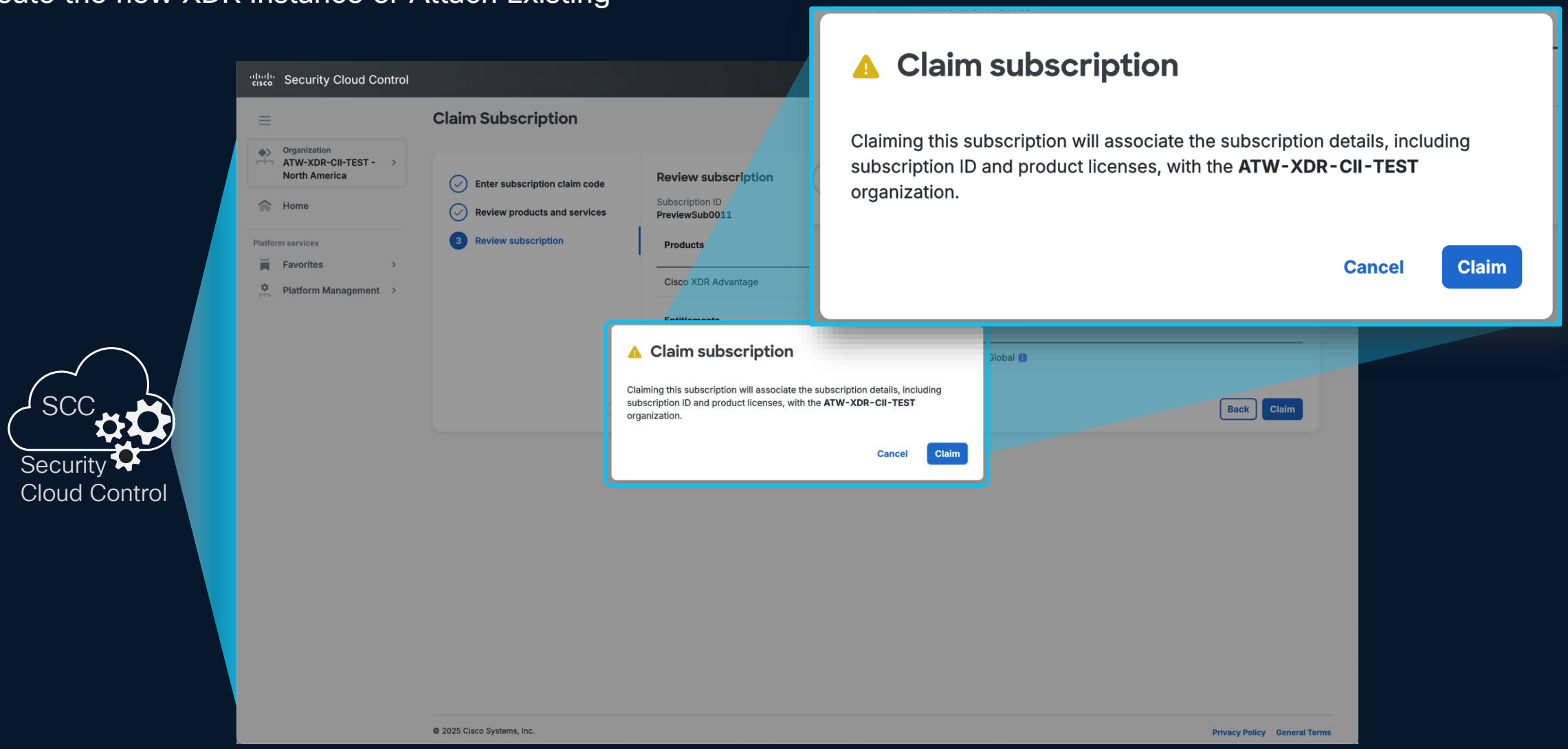
XDR leverages Security Cloud Control (SCC)

Create the new XDR Instance or Attach Existing



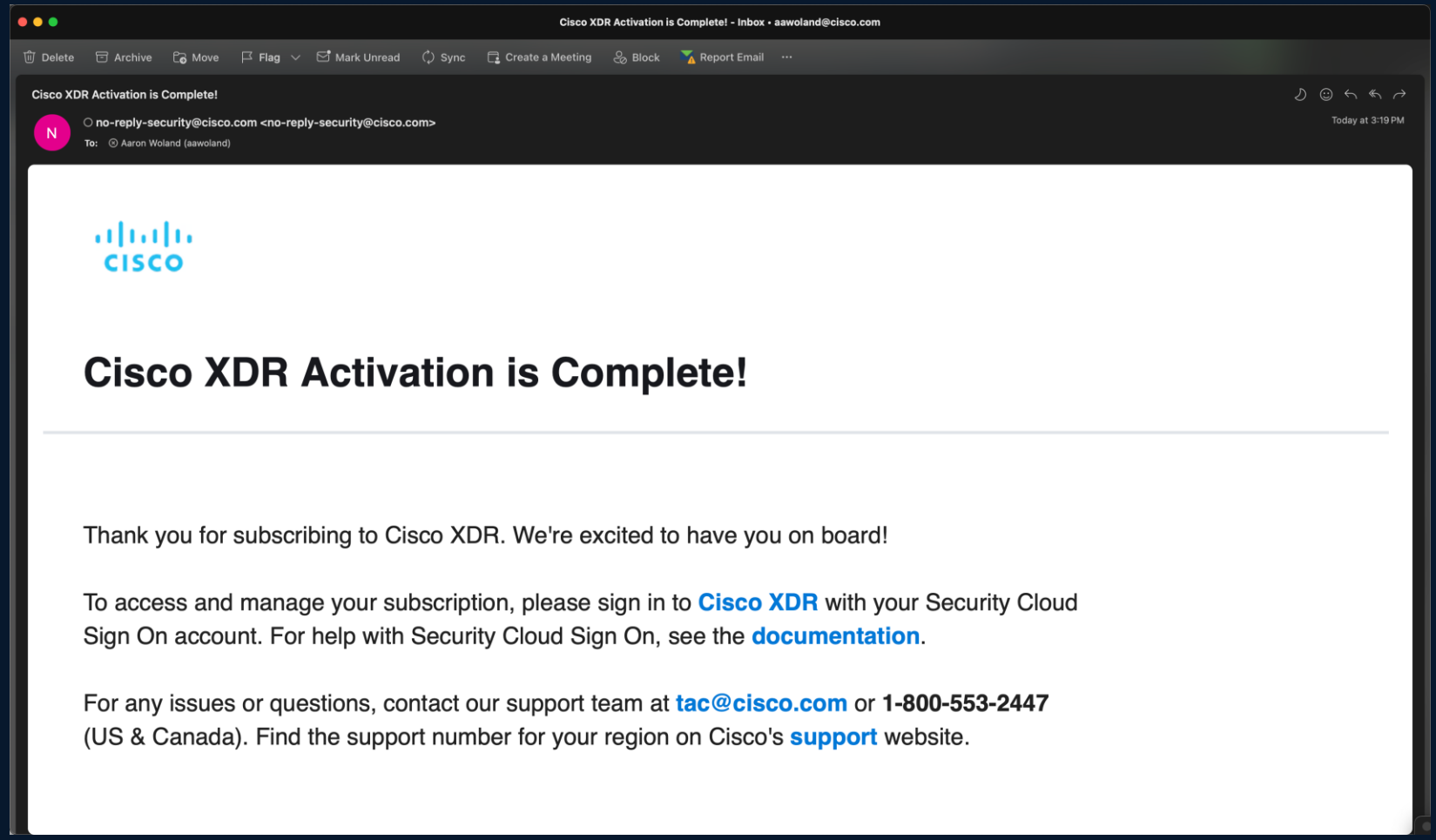
XDR leverages Security Cloud Control (SCC)

Create the new XDR Instance or Attach Existing



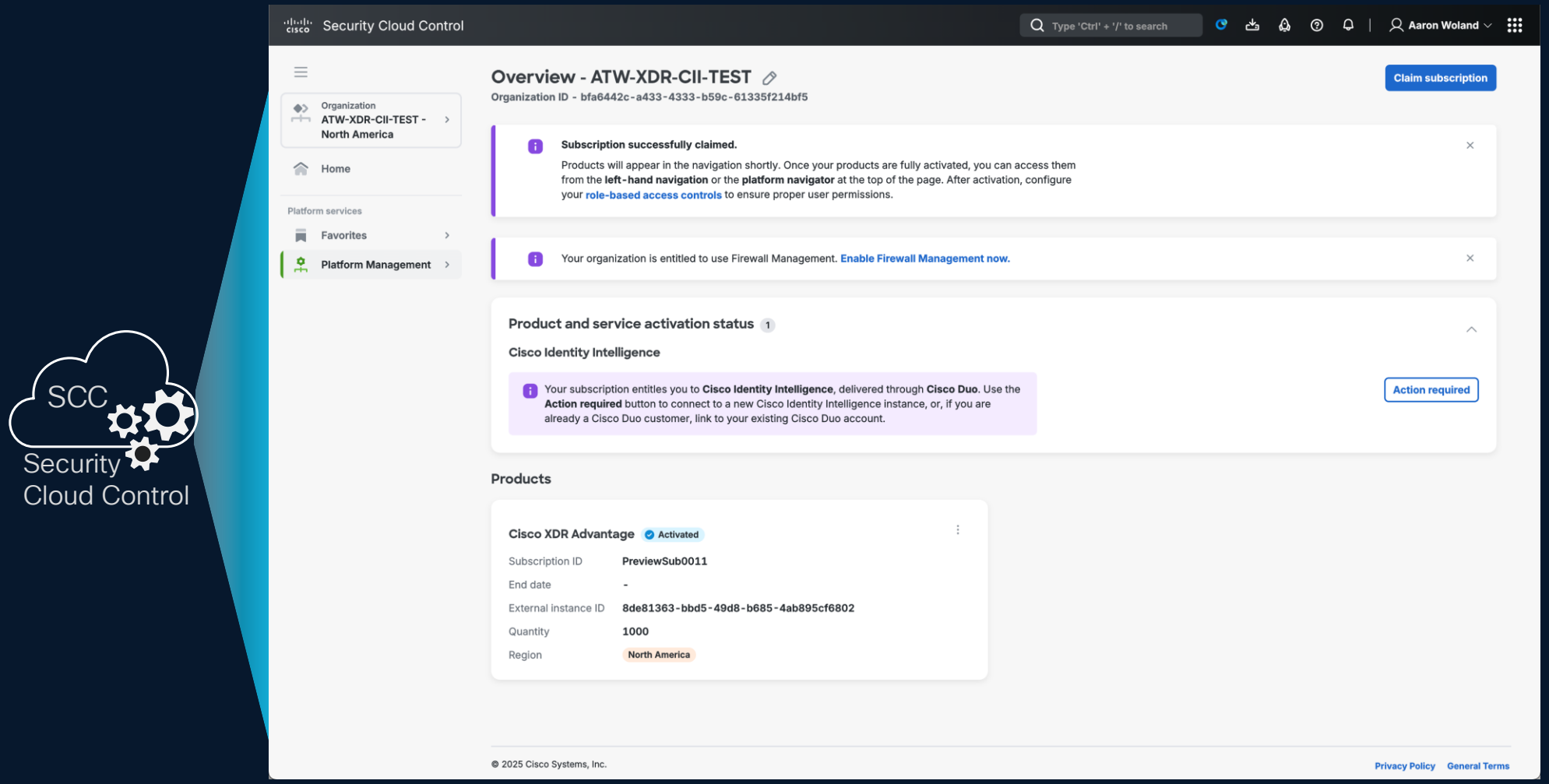
XDR leverages Security Cloud Control (SCC)

Email arrives that XDR is Activated



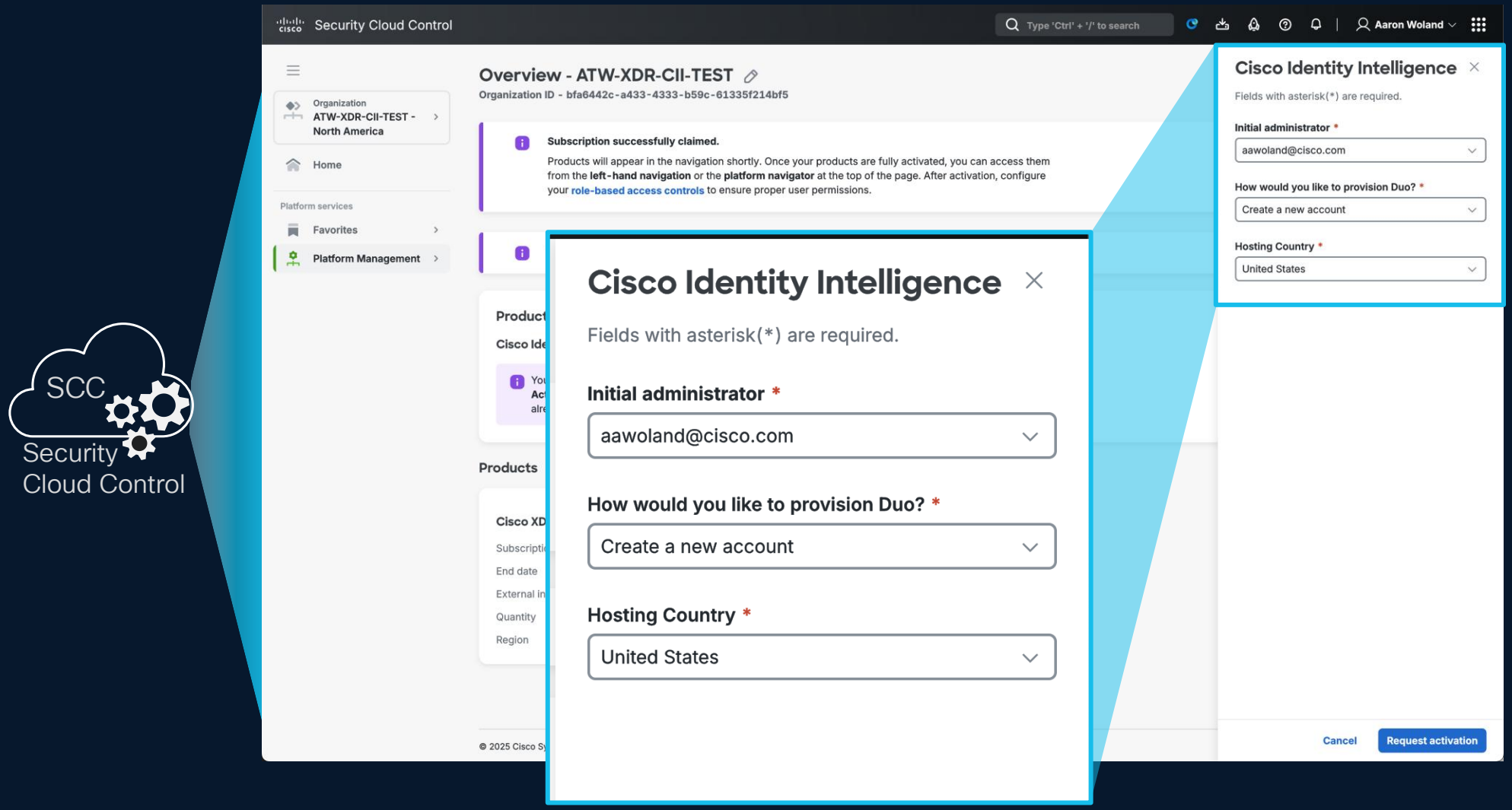
XDR leverages Security Cloud Control (SCC)

Now you need to activate Identity Intelligence



XDR leverages Security Cloud Control (SCC)

Define Initial Admin + Attach Duo or Create New One

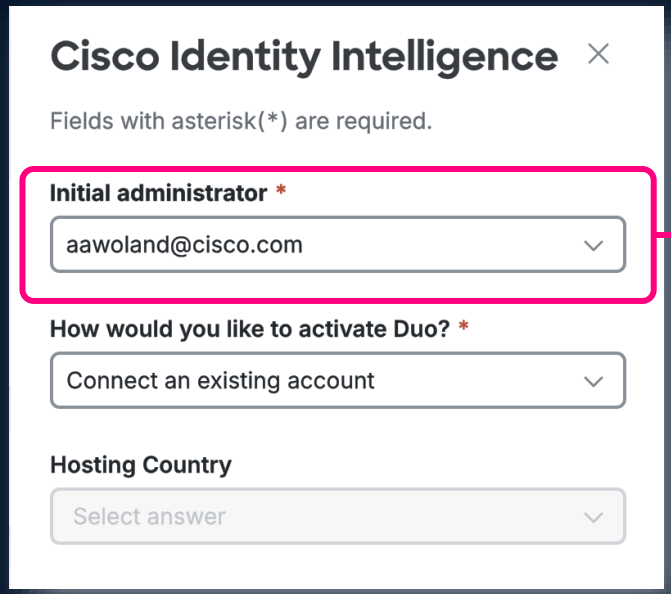


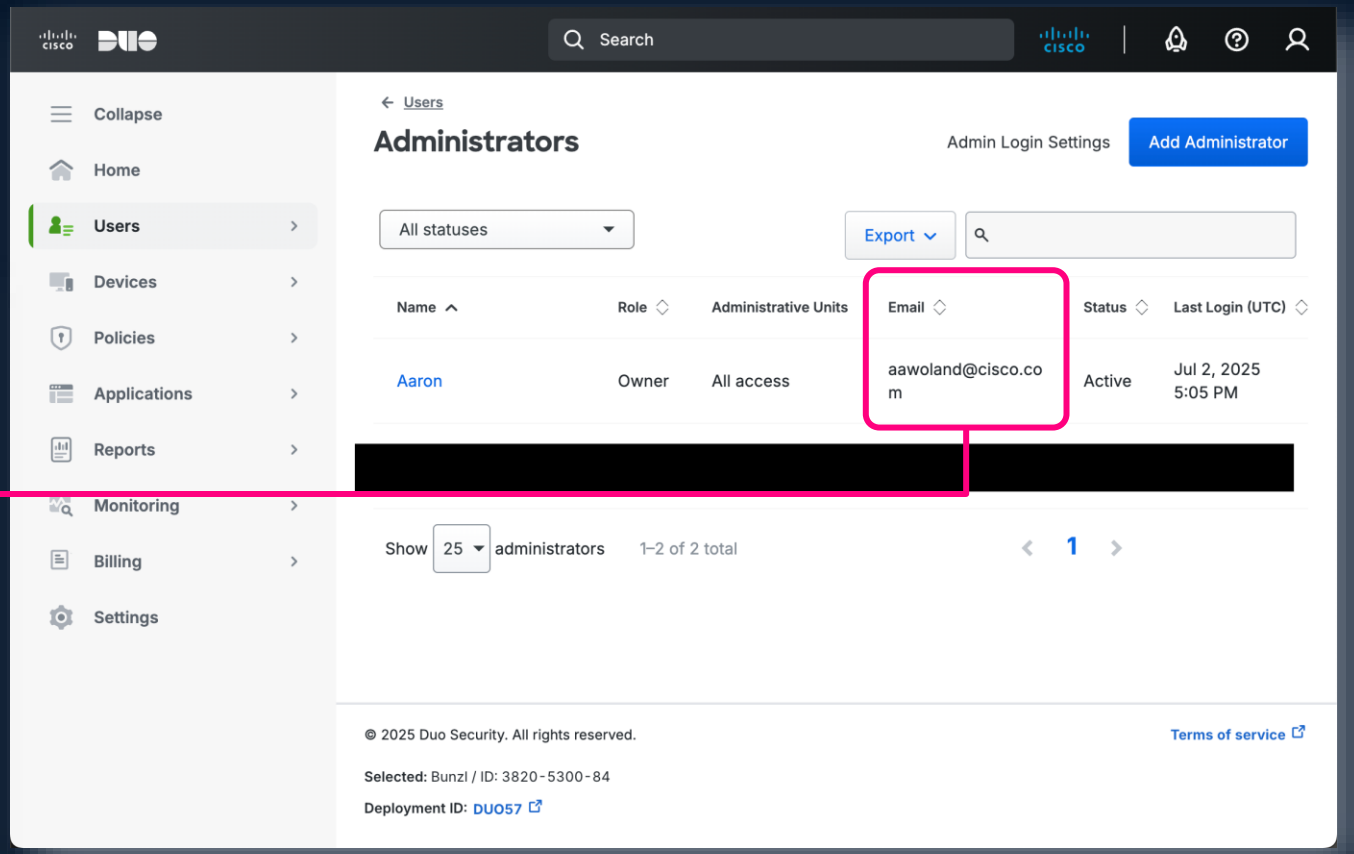
XDR leverages Security Cloud Control (SCC)

Existing Duo? Admin MUST be OWNER in Duo

Must be exact

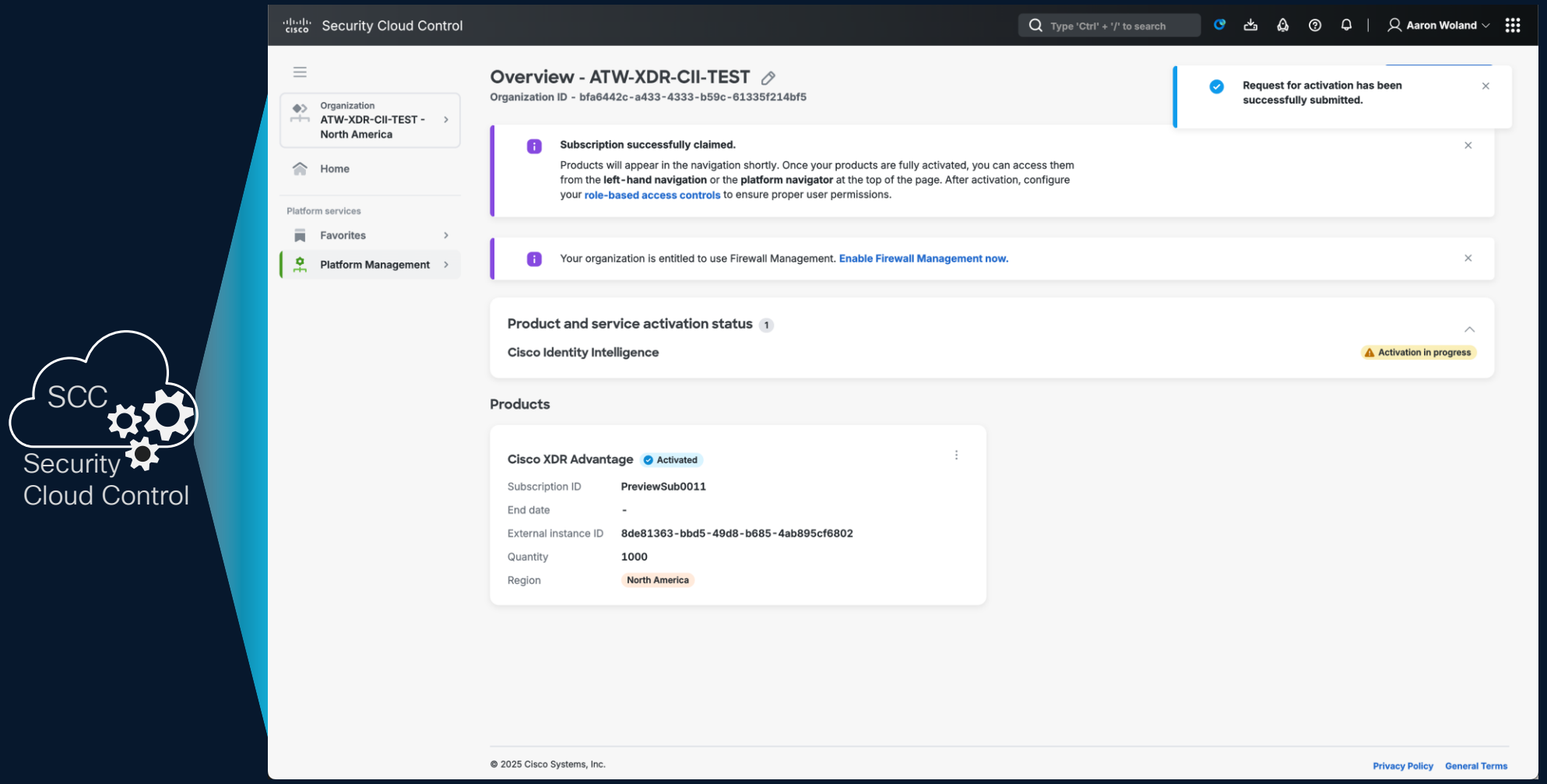
- The email address here, must be the exact email address in Duo.
- Administrator must be Owner





XDR leverages Security Cloud Control (SCC)

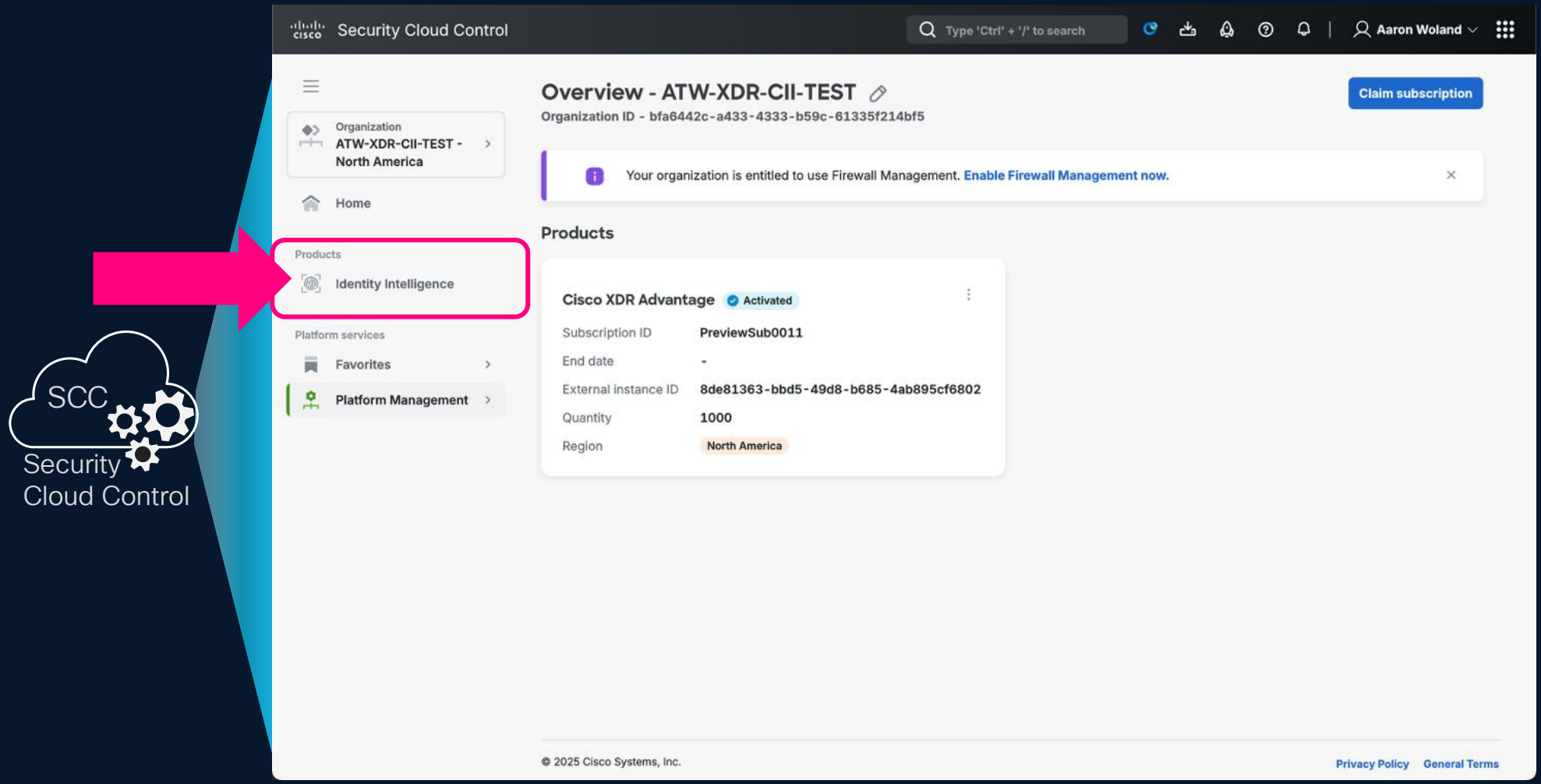
Provisioning of Headless Duo + CII Starts



Now... Wait

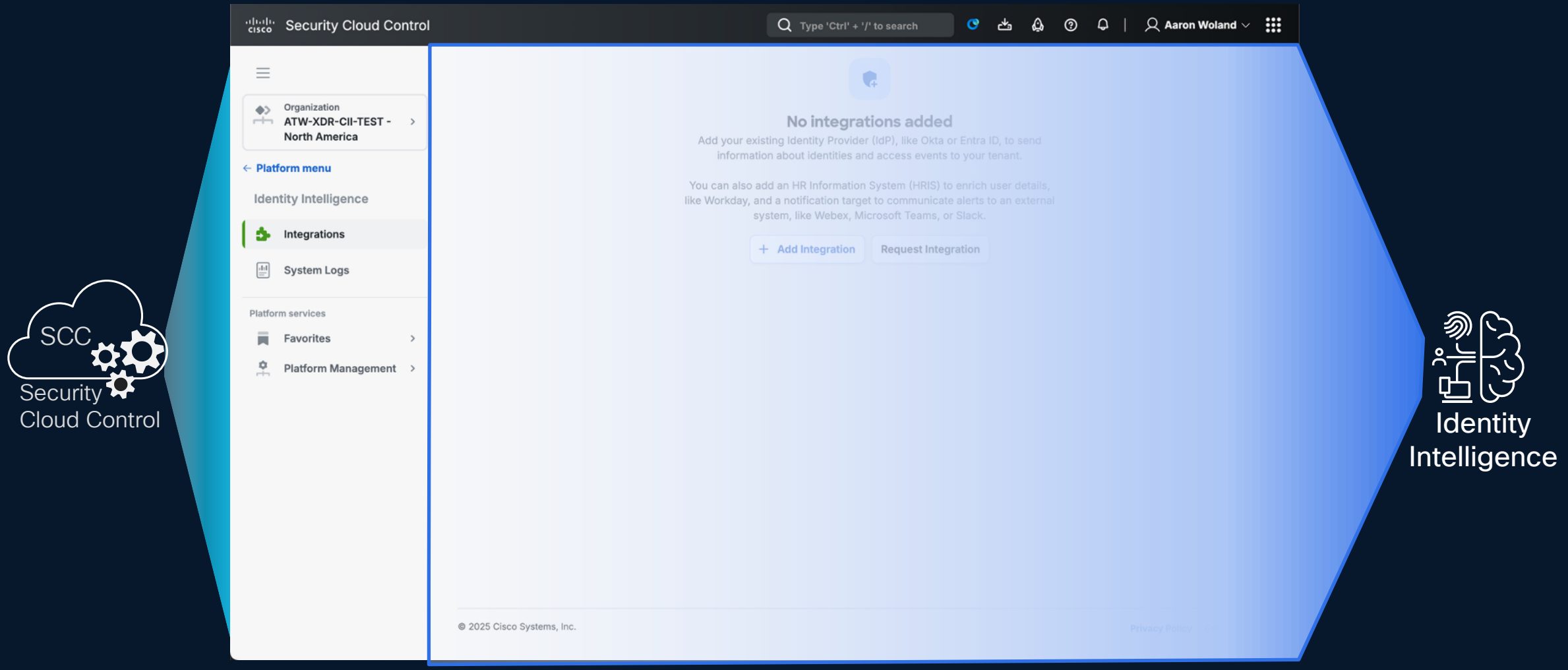
XDR leverages Security Cloud Control (SCC)

Provisioning of Headless Duo + CII Starts



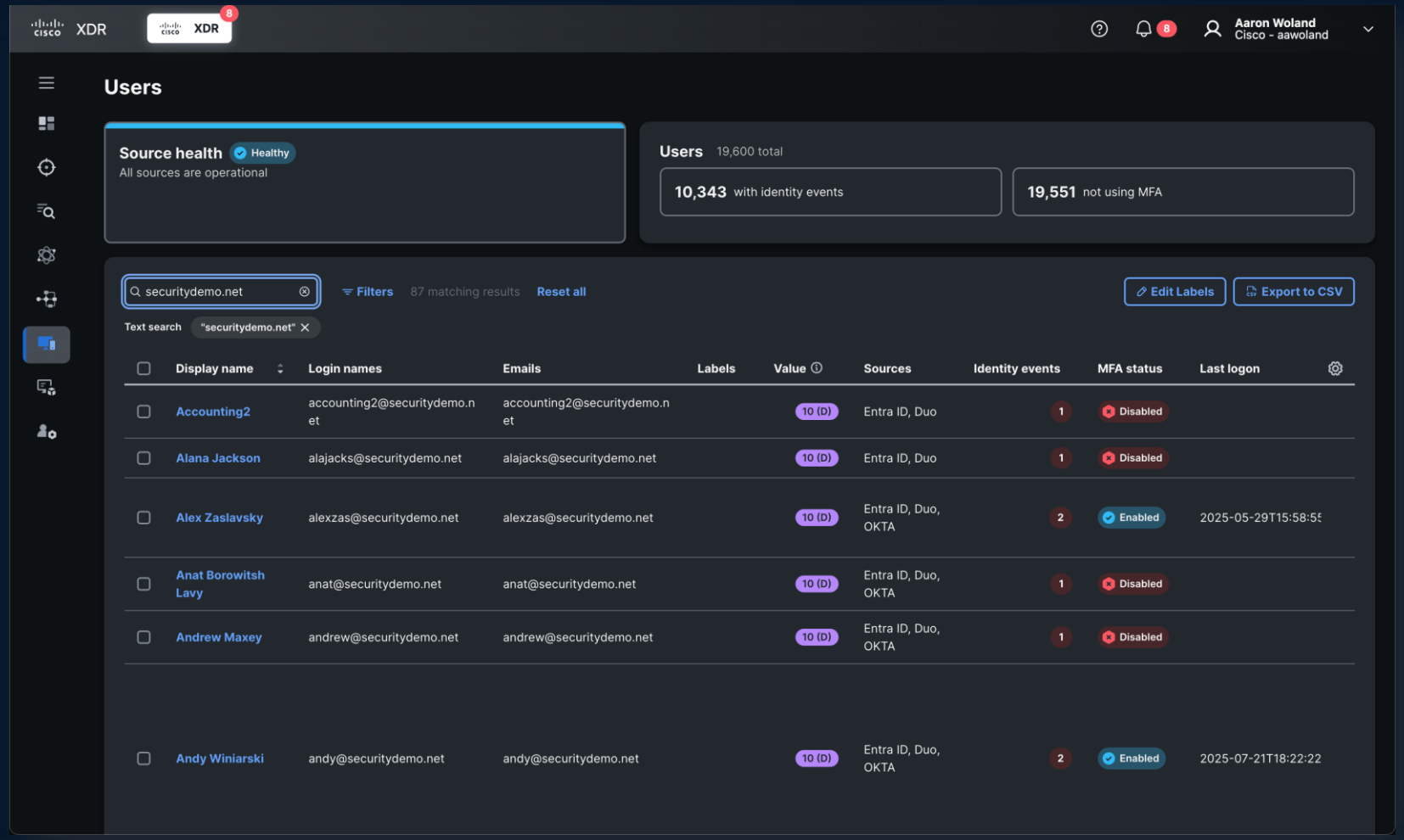
Security Cloud Control (SCC) uses Micro-Front Ends

Provisioning of Headless Duo + CII Starts



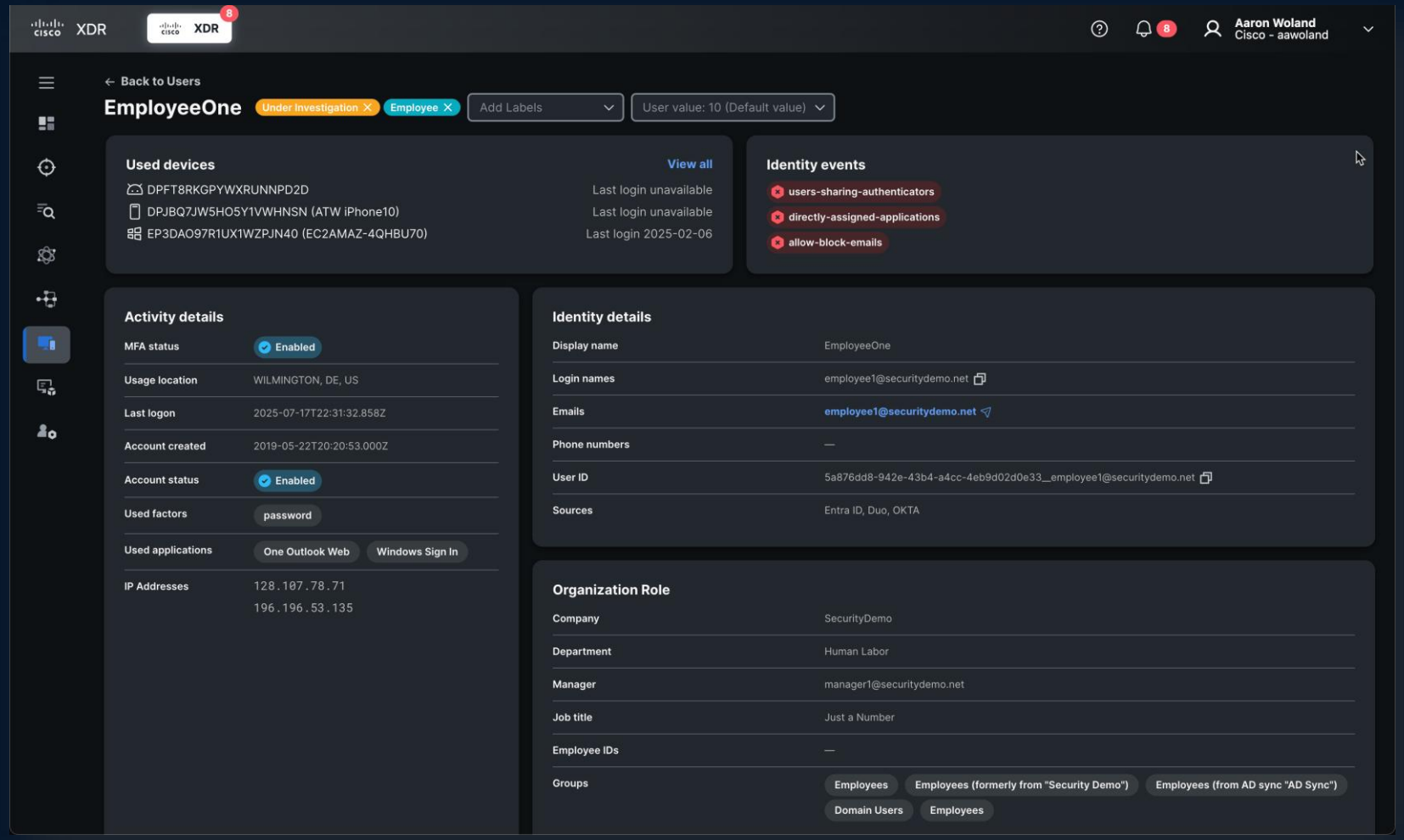
All Users are now in Assets > Users

Add more

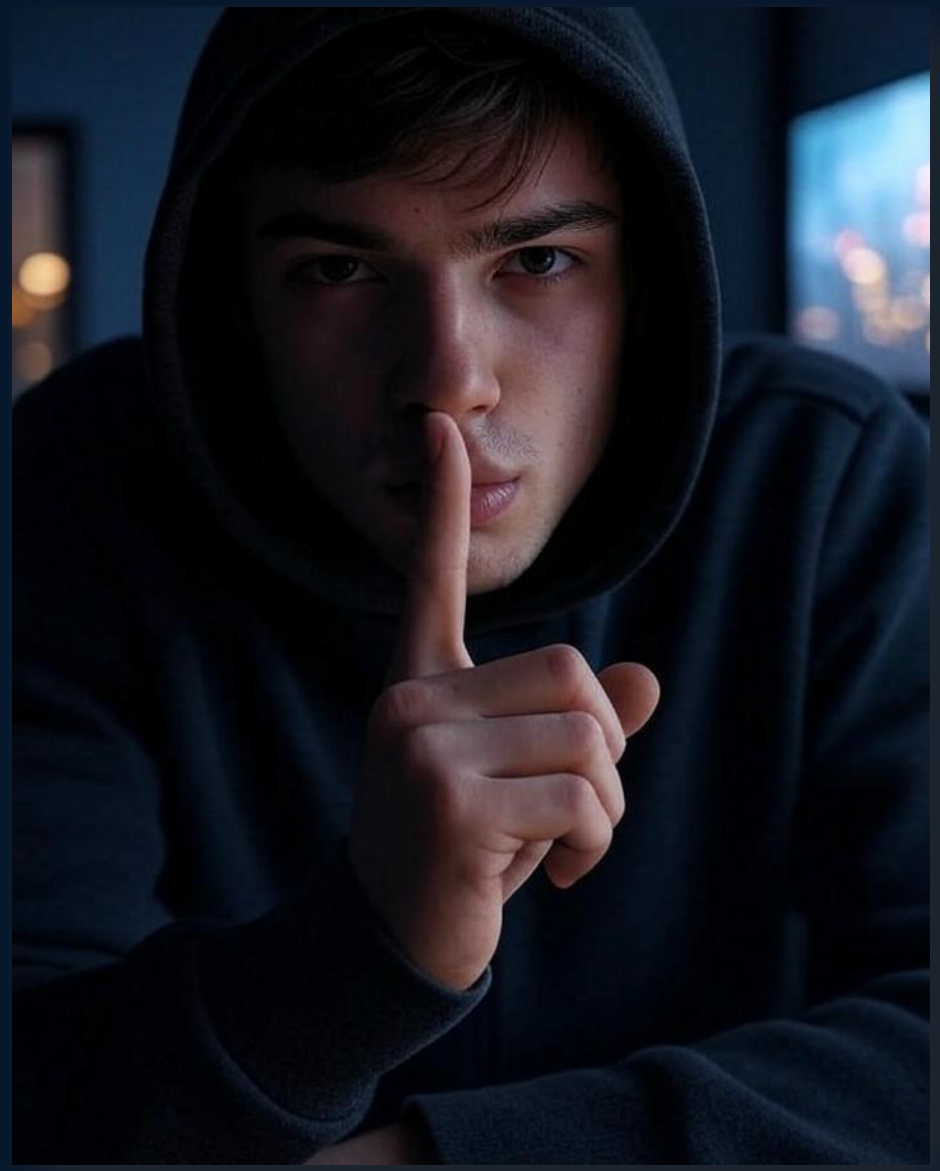


All Users are now in Assets > Users

Can add Labels and Change User Asset Value

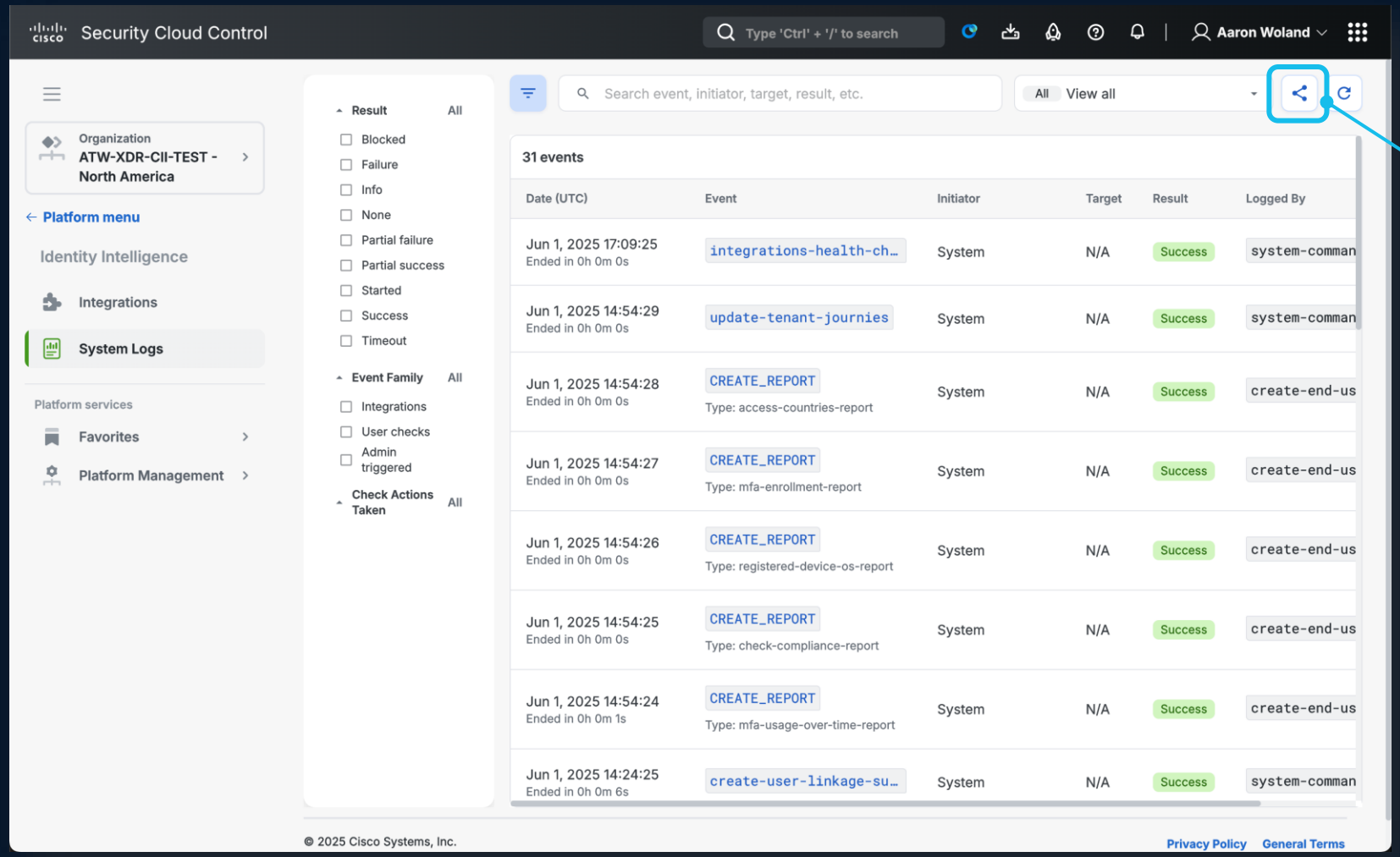


Sssssshhhhhhhhh!



XDR does not entitle users to the CII Console

But there's a way to do it.... SHHHH!!



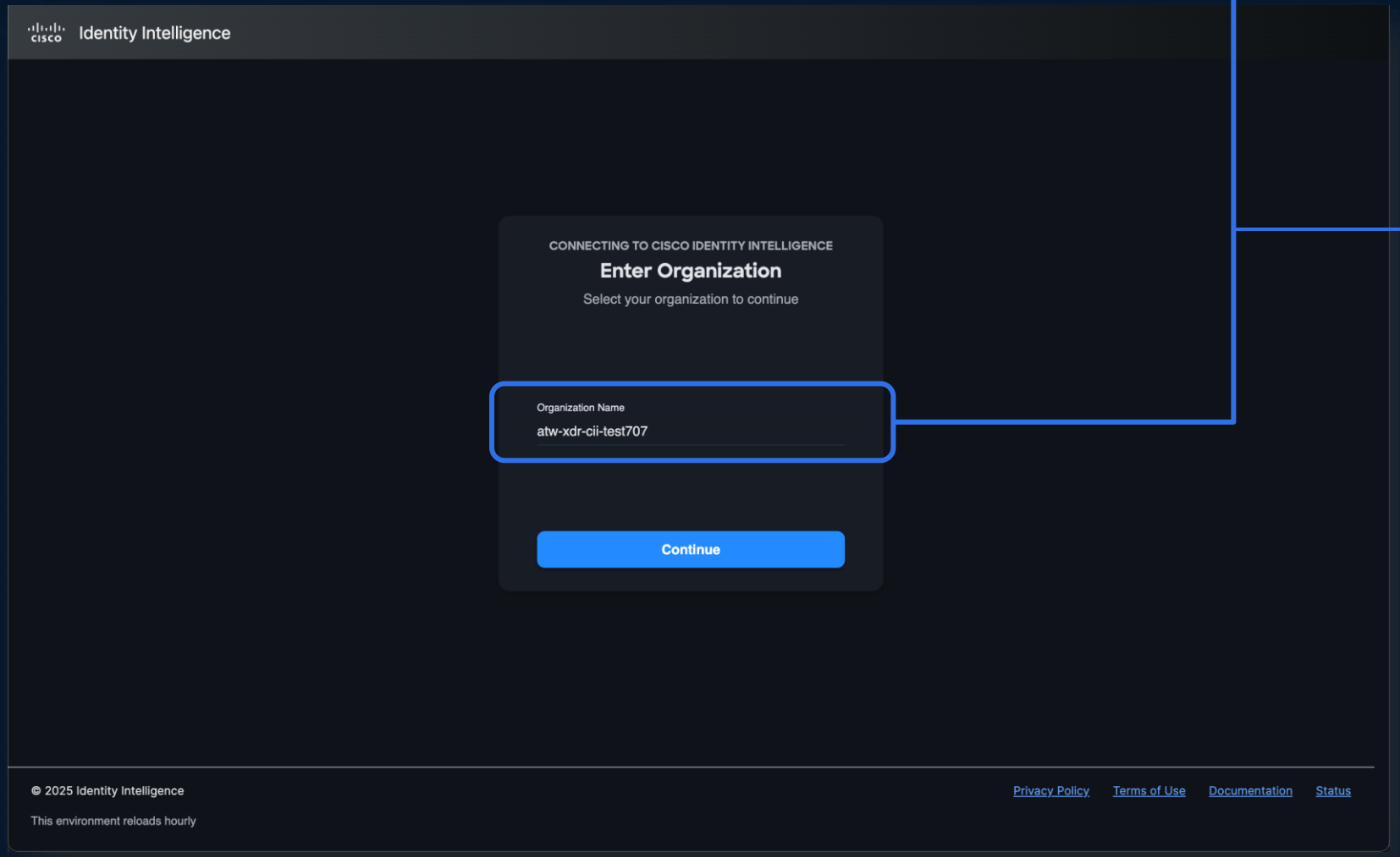
Copy direct link

Each CII page has an ability to copy a direct link, to make it easier to share out to others.

Copy that link

Grab the Slug text

https://control.v3.int.security.cisco.com/oort/go?slug=atw-xdr-cii-test707&type=system-logs



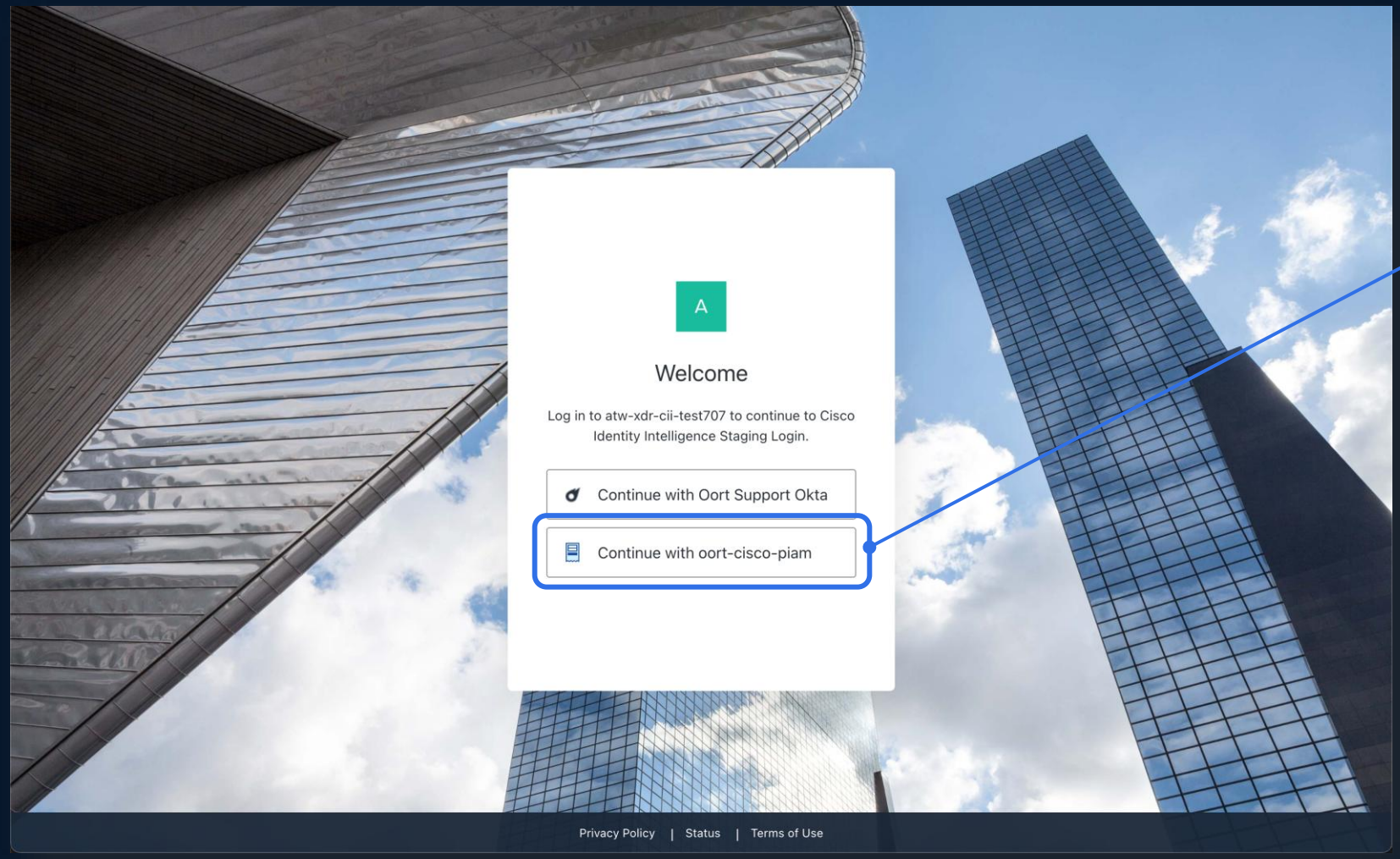
Copy direct link

Use the slug's string as the organization name on the login page for CII:

https://dashboard.[region].oort.io

CII's login screen will ask for IDP selection

Use the "oort-cisco-piam" IDP



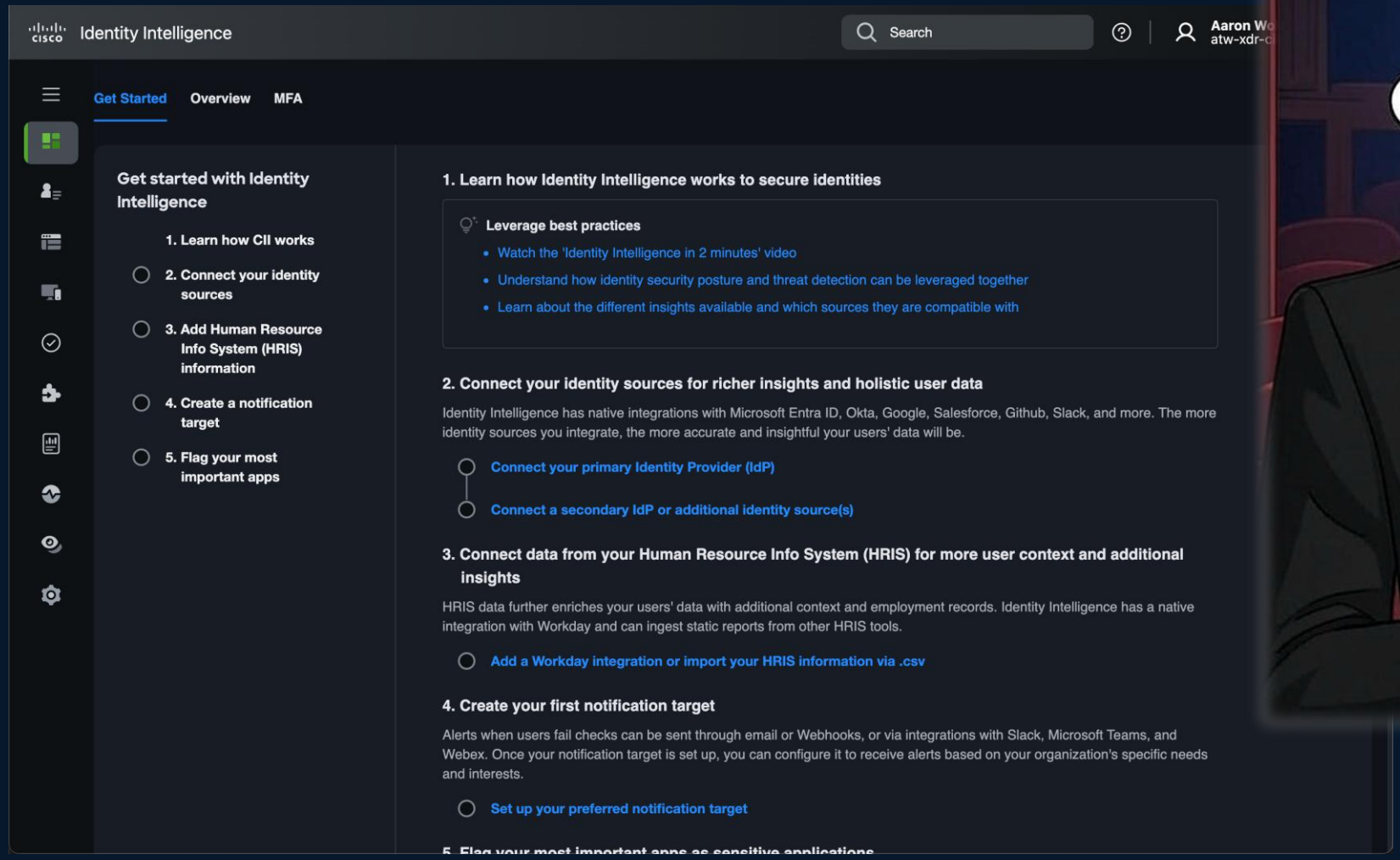
oort-cisco-piam

PIAM – Provisioning, Identity & Access Management. It is a part of SCC.

This connection is automatically created and leverages the admins configured in SCC as part of "Security Cloud Sign-on"

Voila... Magic!

Access to the CII User Interface



Webhooks w/ Cisco XDR

Webhook URL

XDR listener has specific requirements

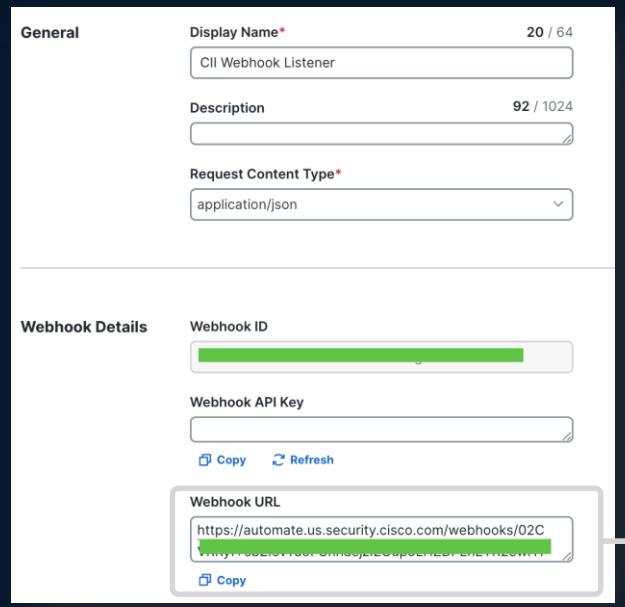
- API Key must be in the URL
- 2x Specific headers

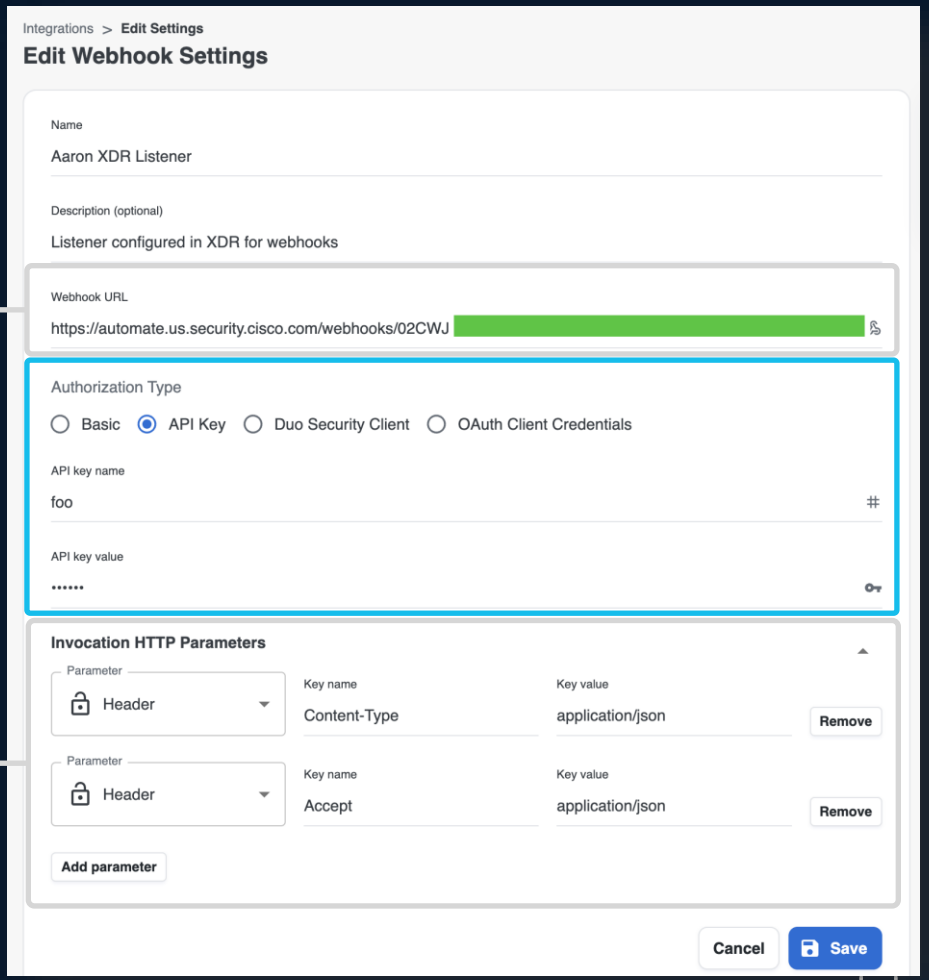
Authentication

- 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

Webhook URL

XDR listener has specific requirements

- API Key must be in the URL
- 2x Specific headers

Authentication

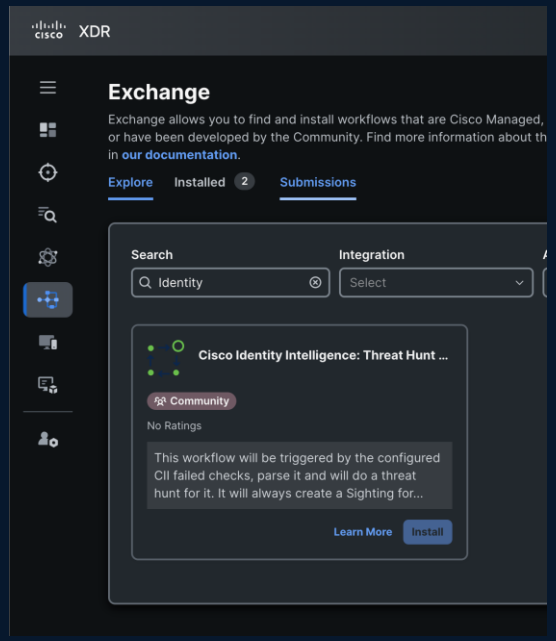
- CII webhooks require authentication
- But we can lie to it, as long as the key is in the URL
- Here, we lied to it w/ Foo & Fake password

Setup Guide

Published here at Aaron Woland's blog

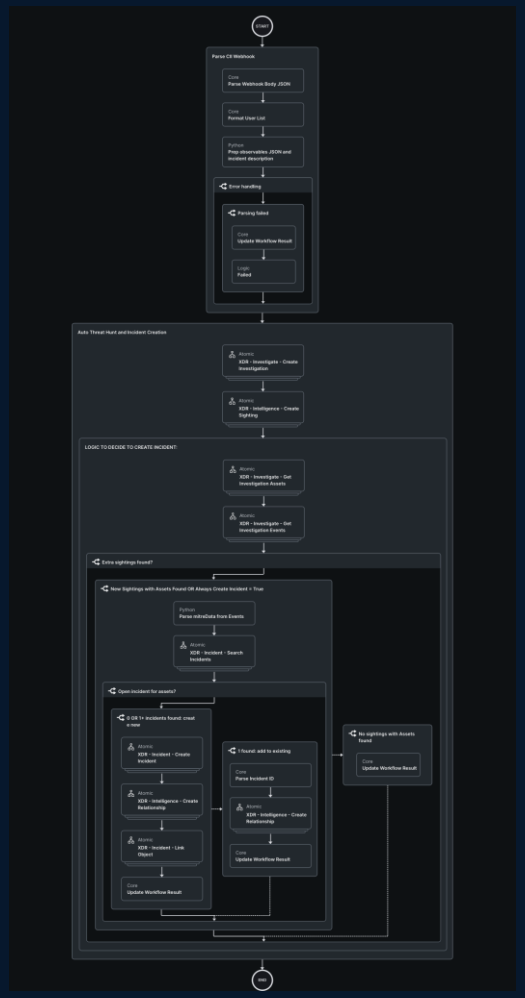
This is now automated in the latest versions of the published workflow

Webhooks w/ Cisco XDR



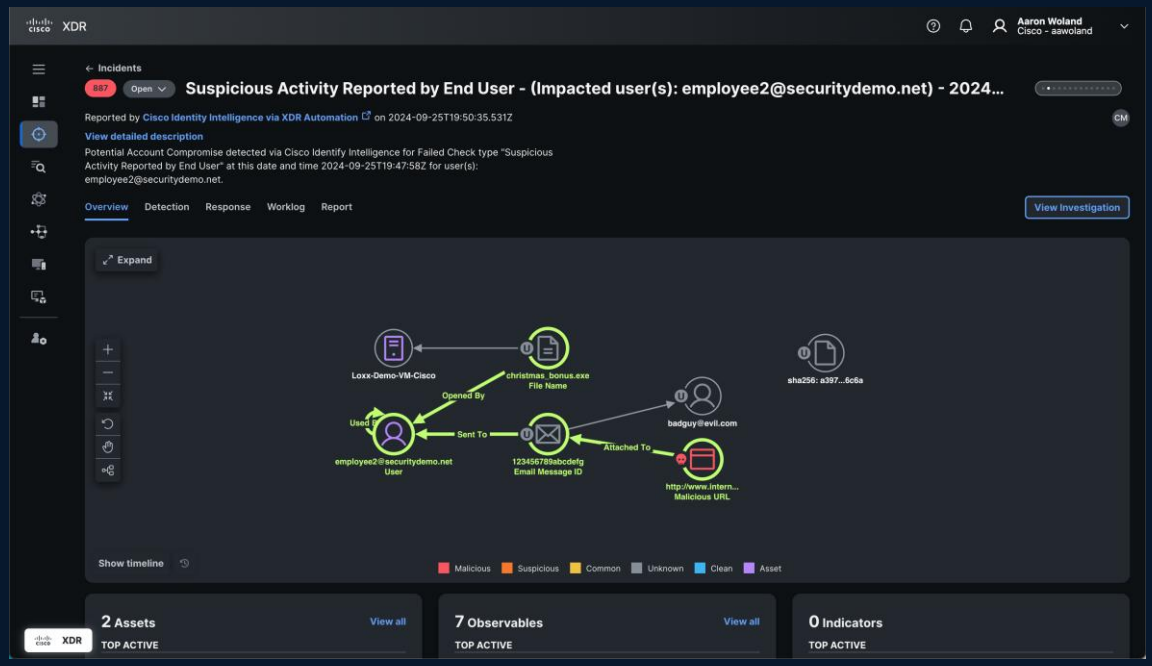
Published in Exchange

- 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

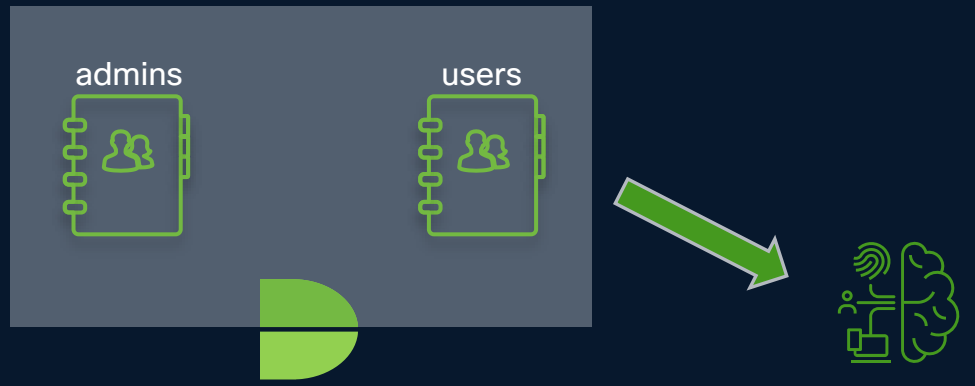
- The CII source events are correlated with the detections from other security products.
- The CII ITDR detection is now part of the attack graph & investigations



Logging into CII & RBAC

CII Requires Duo Single-Sign-on to login to the UI

- Duo maintains a separate directory for Admins than the end-users.
  - Logging into Duo Admin Panel, you must use an Admin Account.
  - Logging into CII UI, you must use a “user” account with the correct roles assigned to it.



Duo Groups:

- CII Admins
- CII Help Desk
- CII Read-only

Mapping

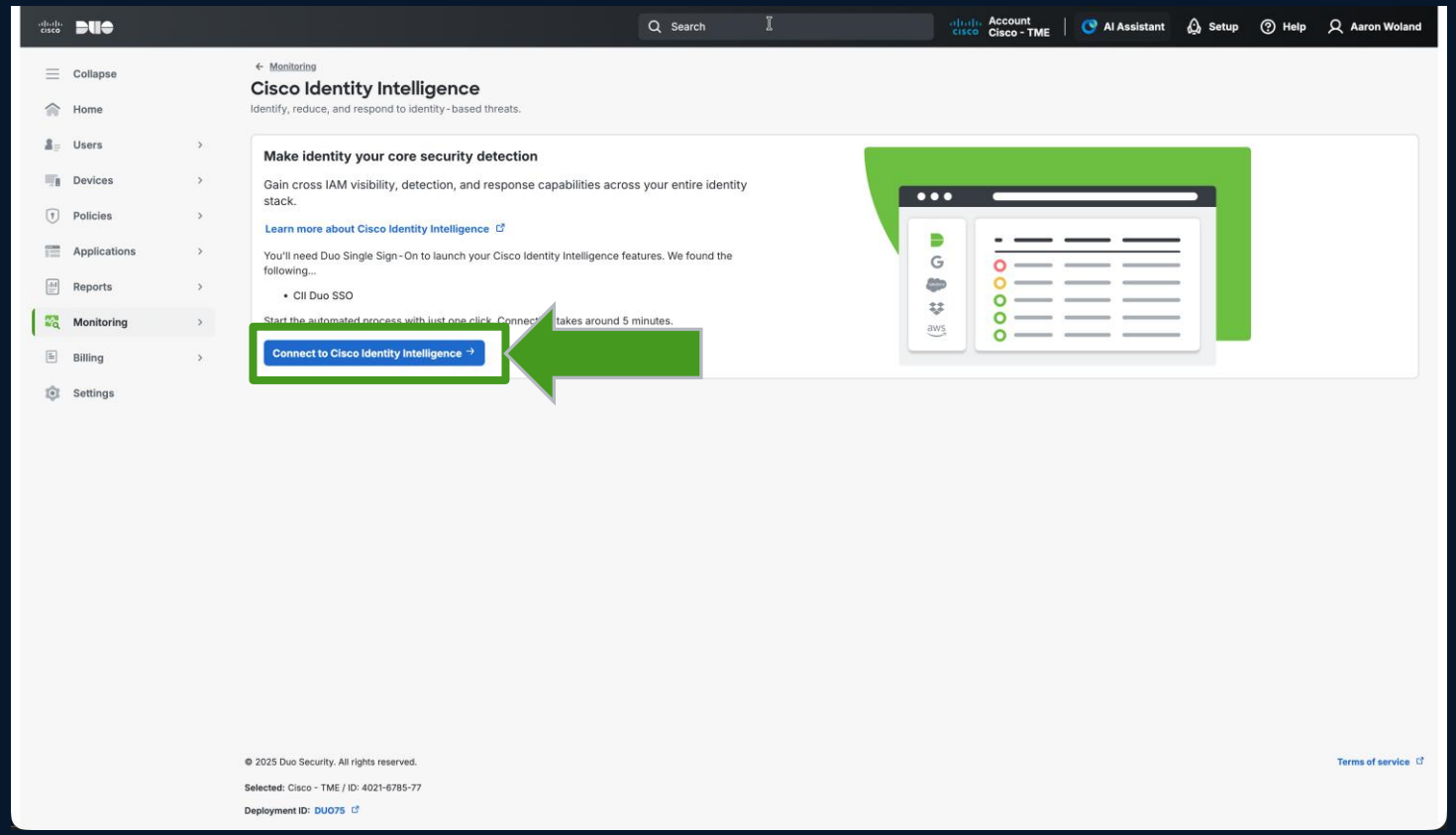
CII Roles:

- cii admins
- cii help desk
- cii read-only

The CII App is ”owned” and Protected by Duo

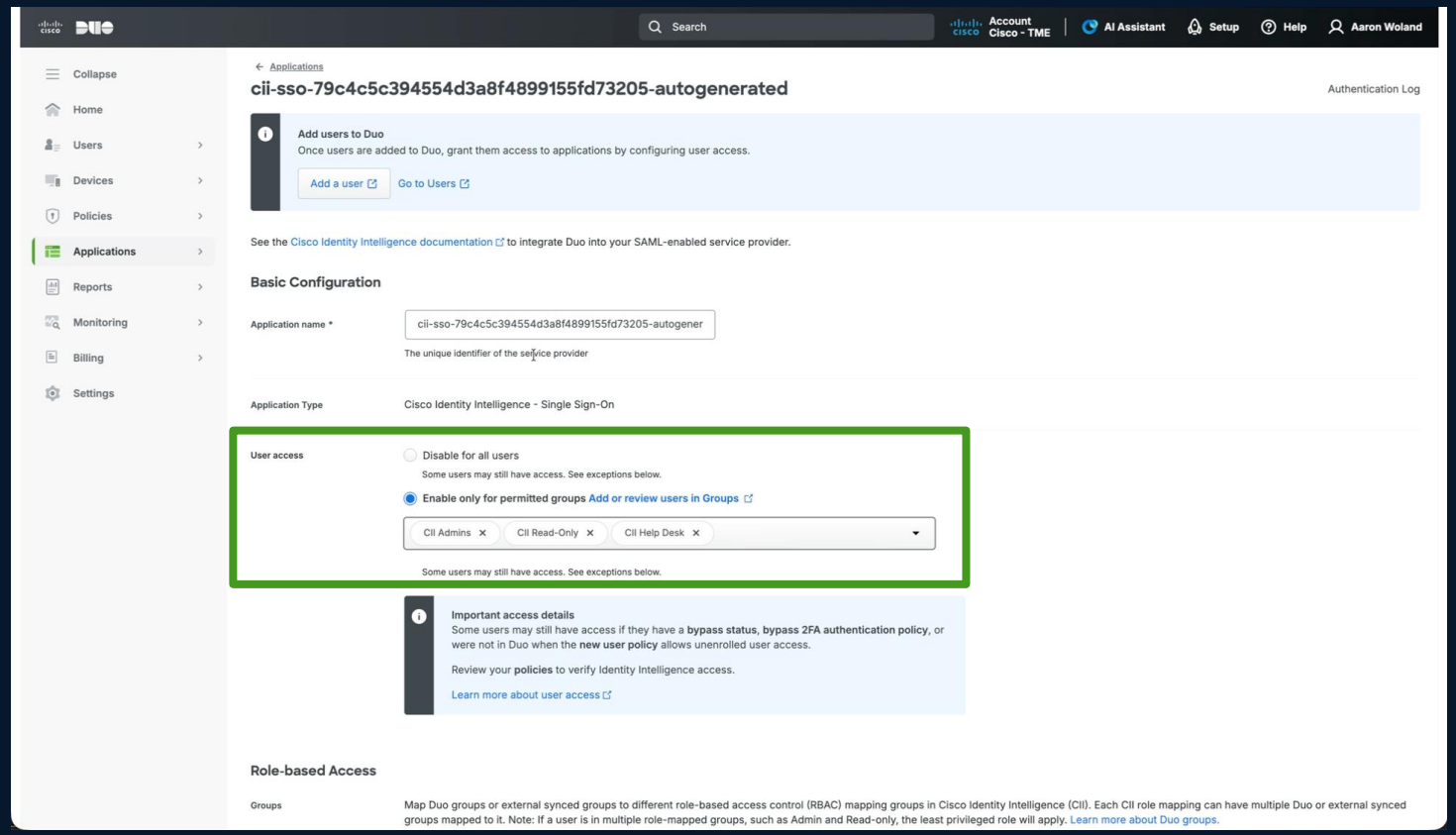
- You click to provision it
  - It is auto-provisioned if Duo is licensed at Advantage or above
  - So no need to do this step if you are licensed already.

Brand New Duo Tenant



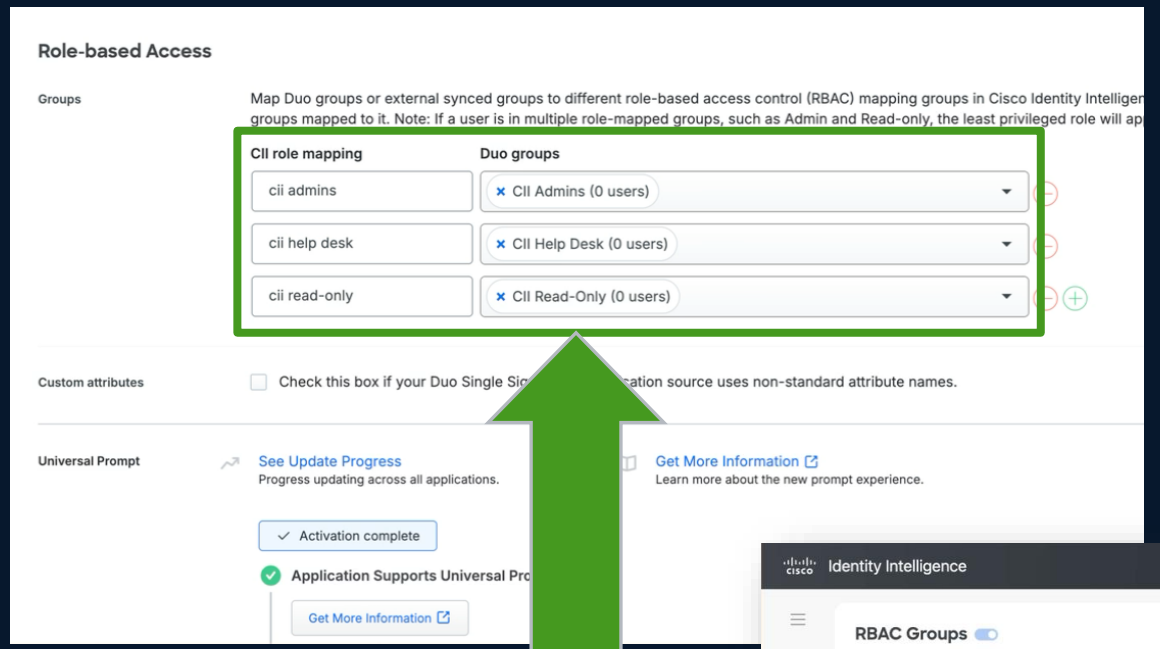
The CII App is ”owned” and Protected by Duo

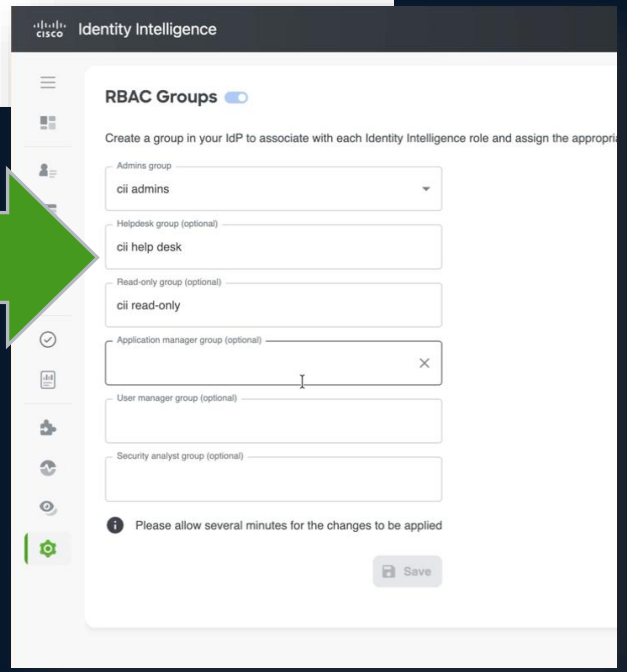
- App is protected by Duo SSO
  - Only members of the 3 pre-configured groups are allowed to AuthN to the CII app
  - Today: you cannot nest external users into internal Duo groups (hopefully will change in future)
  - You may add other groups, such as from external sources – like Active Directory
    - Users that are sync’ed into Duo via SCIM are considered local & therefore can be added to the internal Duo groups.
  - You MUST add the other groups to both Permitted Groups and Role-Based



Duo or External Groups map to CII “Roles”

- App is protected by Duo SSO
  - Duo Groups (or external groups) are mapped to the roles
  - These mappings are sent in the SAML Assertion – and provide the role to CII for the user





Common Mistake: Do not allow your users to be in more than one of these groups.

- CII uses LEAST-PRIV Access, and the user will get the lowest level group they are in

When user is a member of two groups for CII Roles

User: Crash Test Dummy

You can see this user is a member of two groups:

- CII Admins
- CII Read-Only

When user is a member of two groups for CII Roles

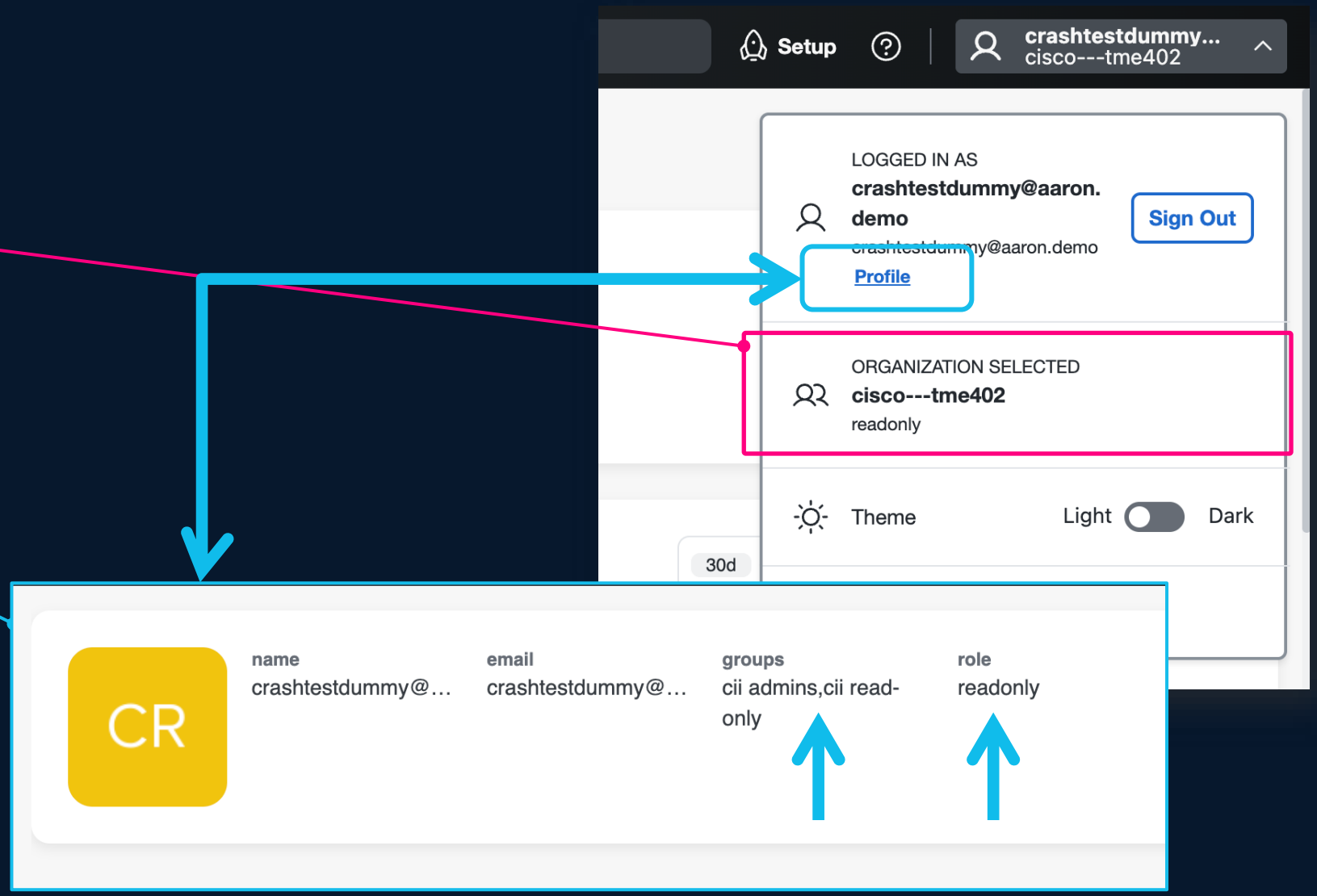
User: Crash Test Dummy

Logged into CII.
User is assigned readonly role?

Click on Profile

You can see user has both roles in the SAML Assertion.

CII follows Least-Privilege Access principle.

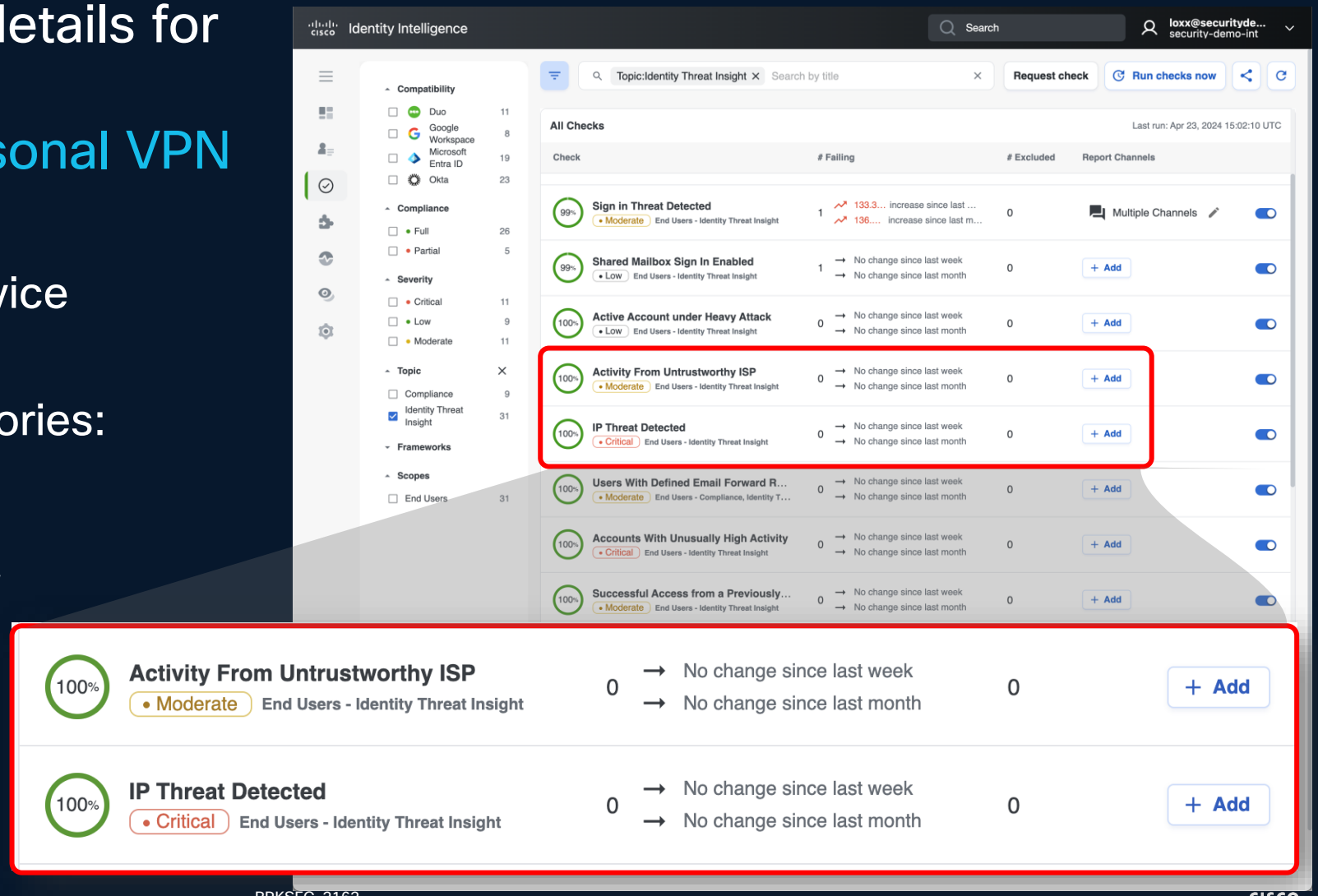


Miscellaneous Technical Info

Threat Intel Nuggets

For Your Reference

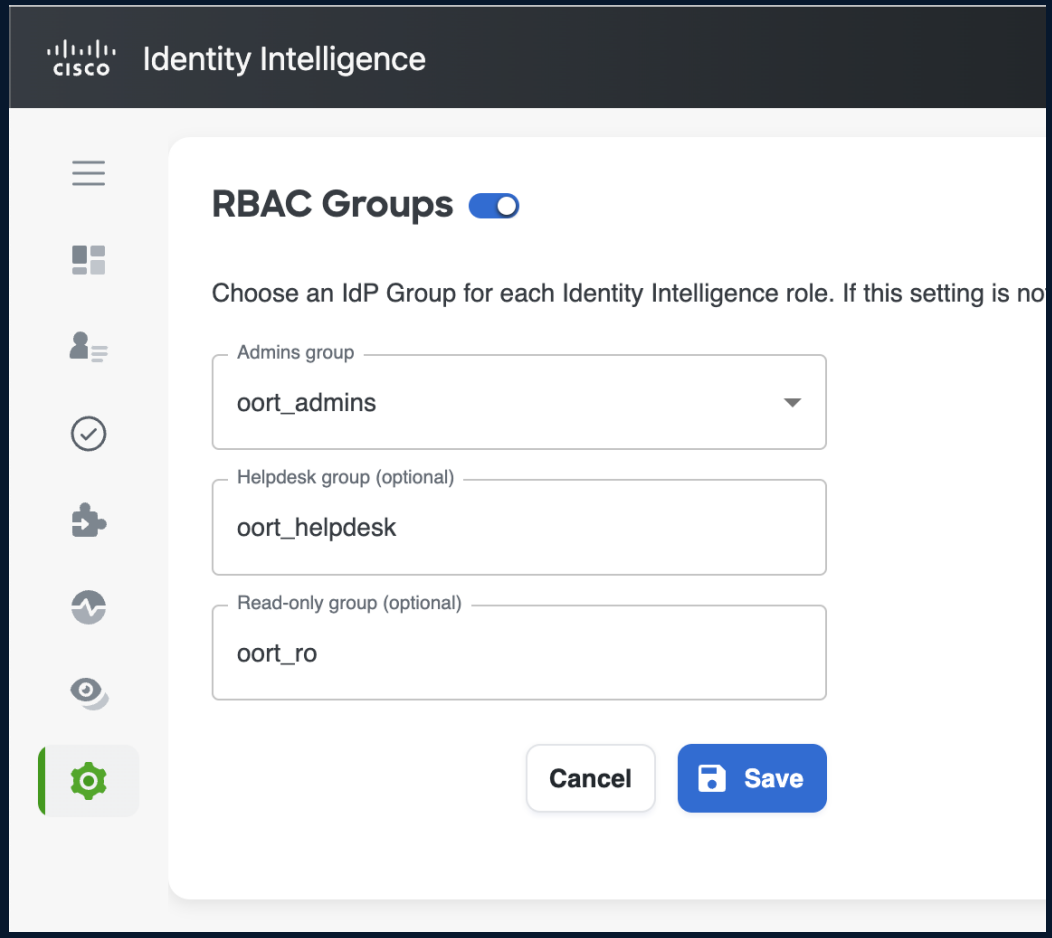
- How CII knows about ISP details for checks like “Activity From Untrustworthy ISP” & “Personal VPN Usage”:
  - CII is using the ASN of the service provider
  - Subscribe to IPInfo feed categories:
    - Hosting
    - Proxy
    - Tor
    - Vpn
    - Relay
    - Service
    - Malicious IP
    - Password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



Role Based Access Control

For Your Reference

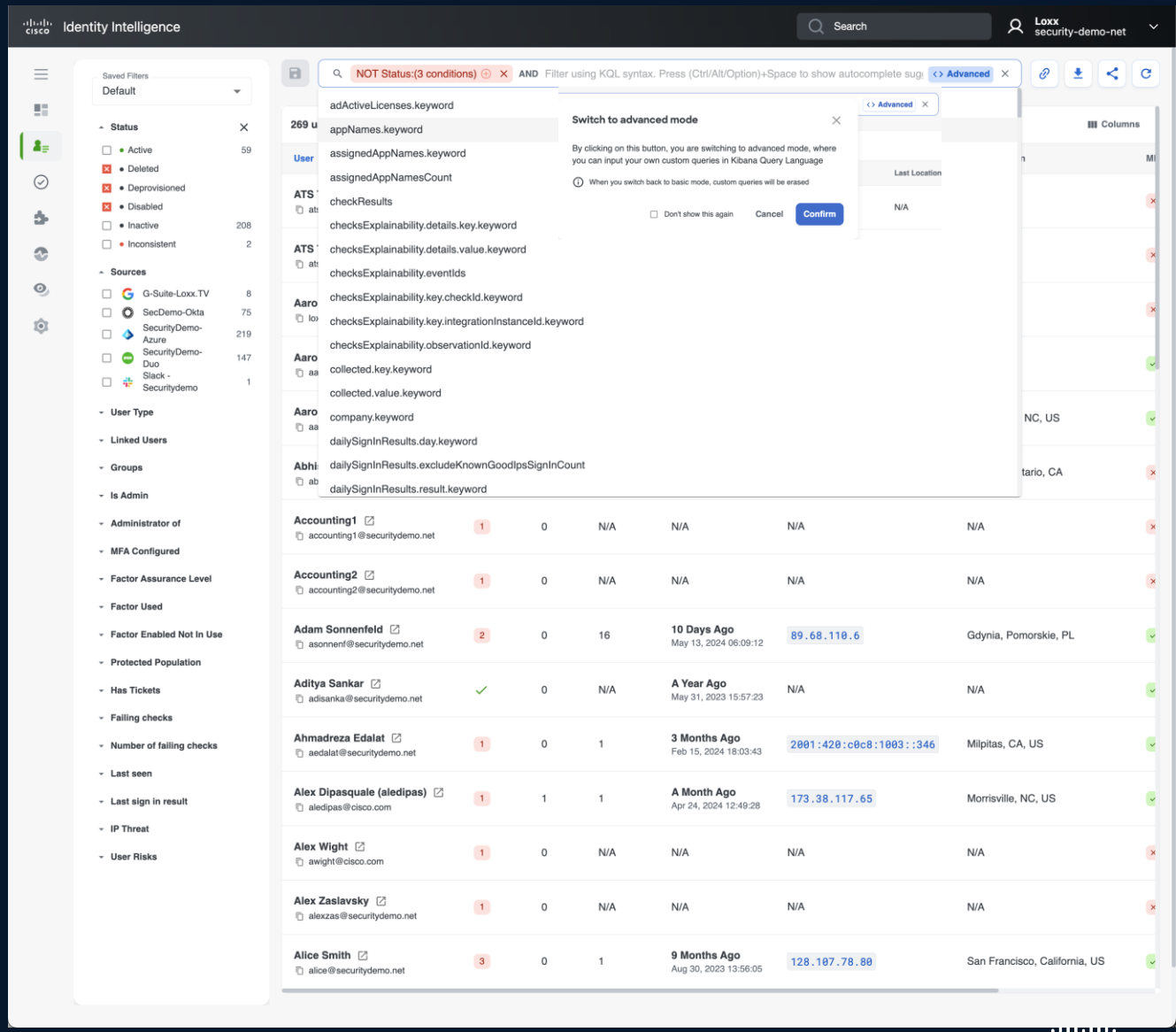
- Three built in Roles:
  - Admins (Full Administrator)
  - Helpdesk
  - Read-only
- Manage roles via groups in the IDP
- No local admin accounts – IDP only



Advanced Search

For Your Reference

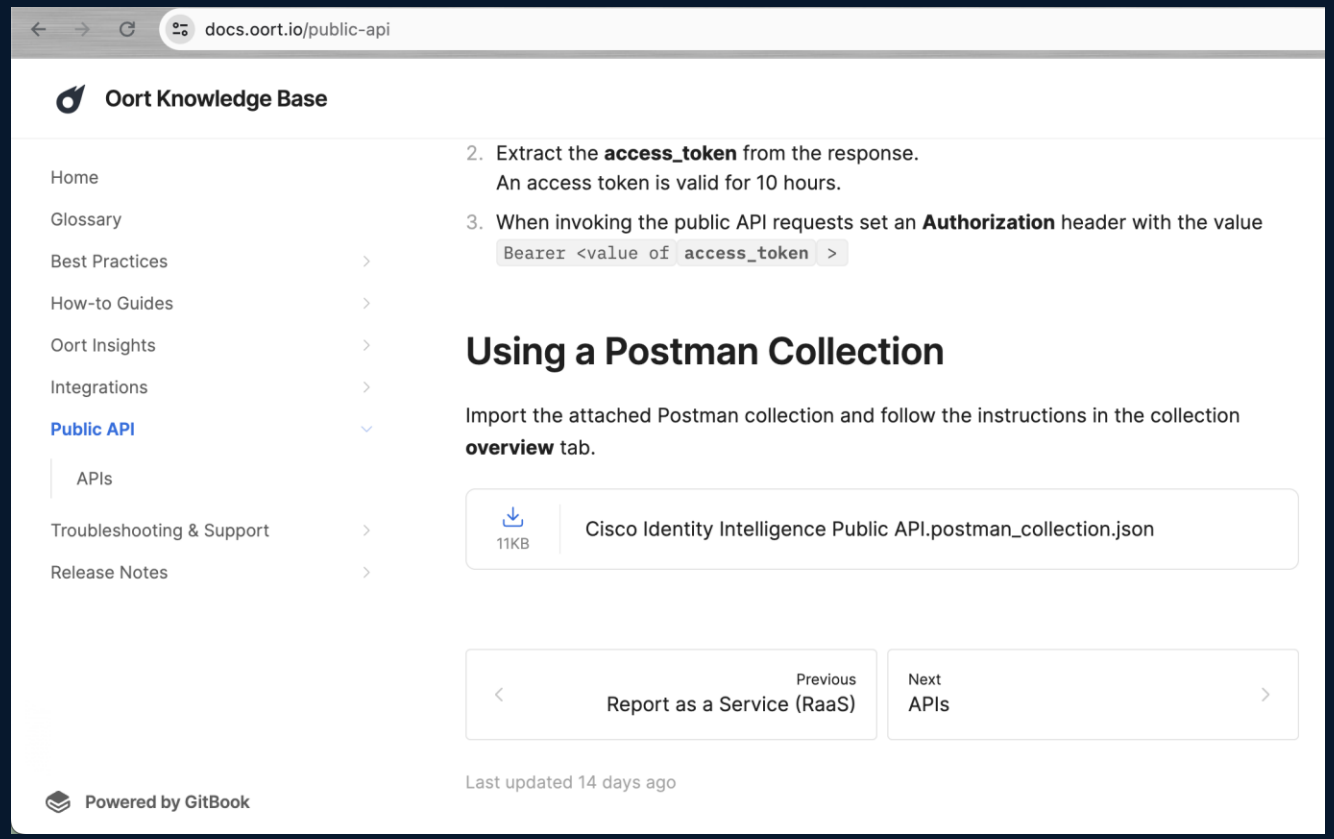
- Switch to advanced mode
  - Uses Kibana Query Language (KQL)
  - Provides search operators:
    - AND
    - OR
    - NOT
    - _exists_
    - !_exists_
  - Use **CTL + Space** to get list of advanced query attributes
  - Save your adv queries in the UI!



CII Public API

For Your Reference

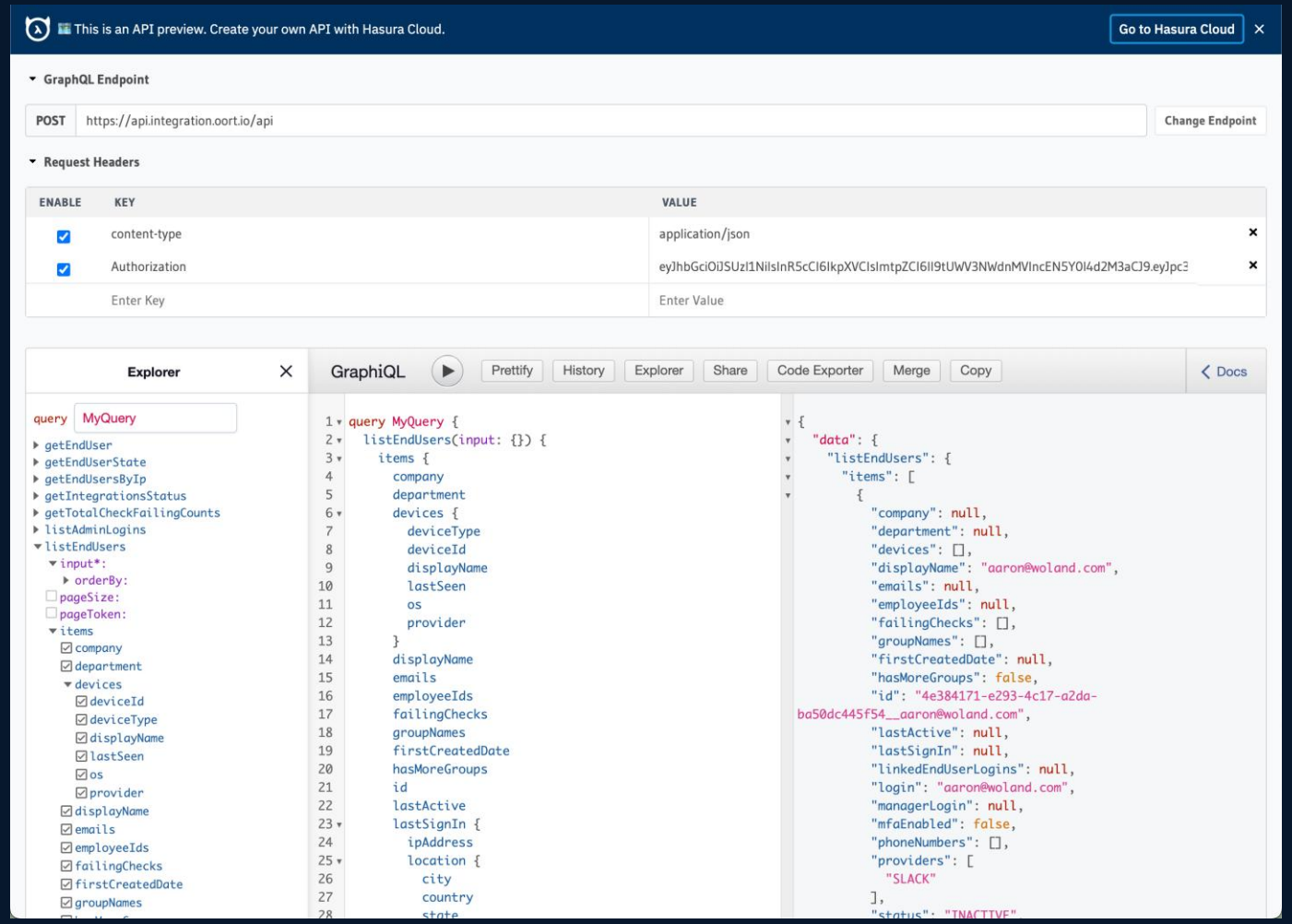
- https://docs.oort.io/public-api/apis
- GraphQL based API
  - Why graphQL – don't have to send EVERYTHING in the response..
  - Your request is structured as a query & CII sends only what you ask for.
- GraphQL self-documents its schema
- CII provides Postman collection, downloadable right from documentation



GraphQL Explorer Tools

For Your Reference

- 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]




For Your
Reference
Integrations Deep Dive
CISCO Live !

Identity sources and their methods

For Your Reference

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

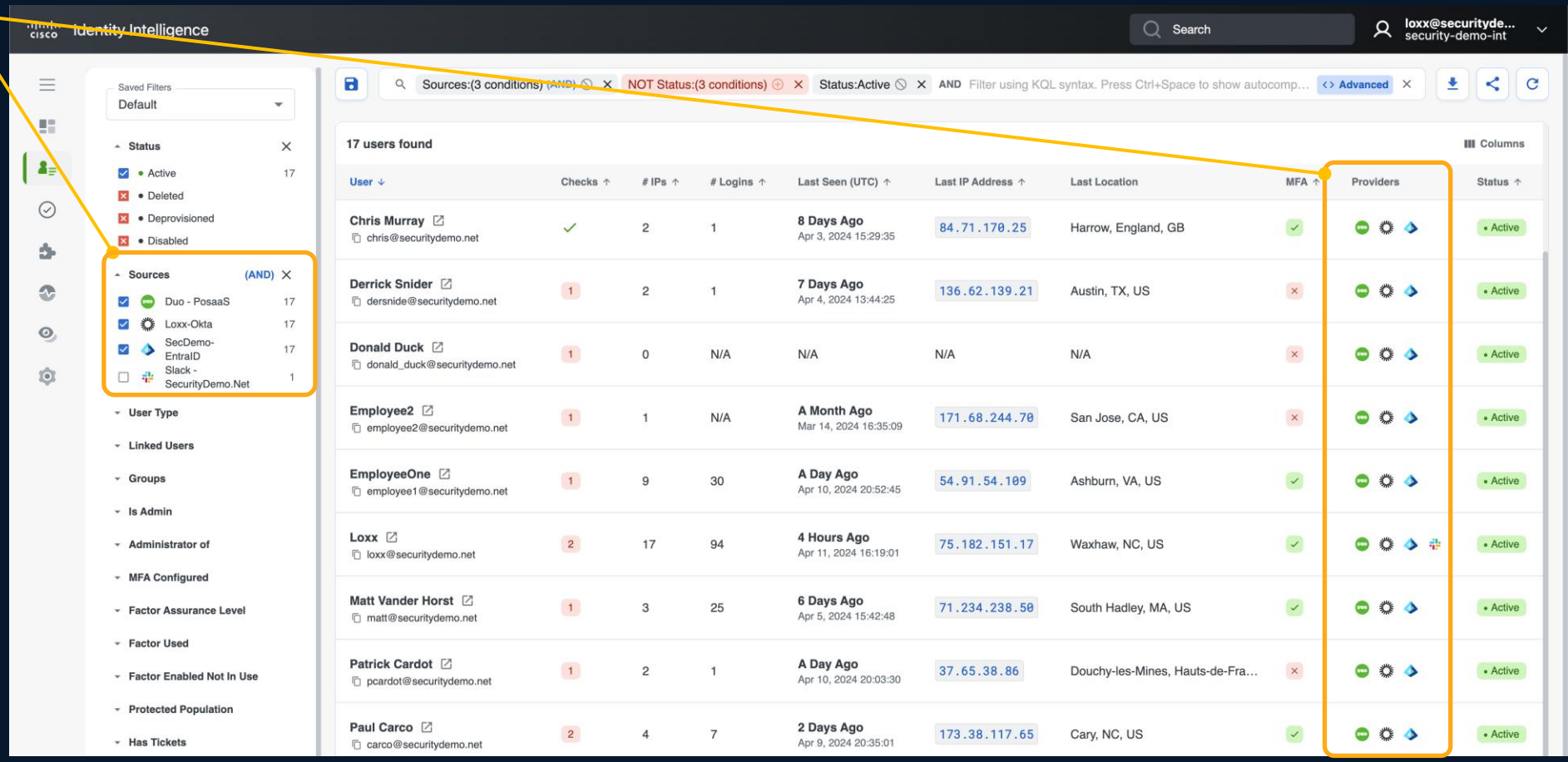
Merged view of users – combined from all sources

For Your Reference

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”

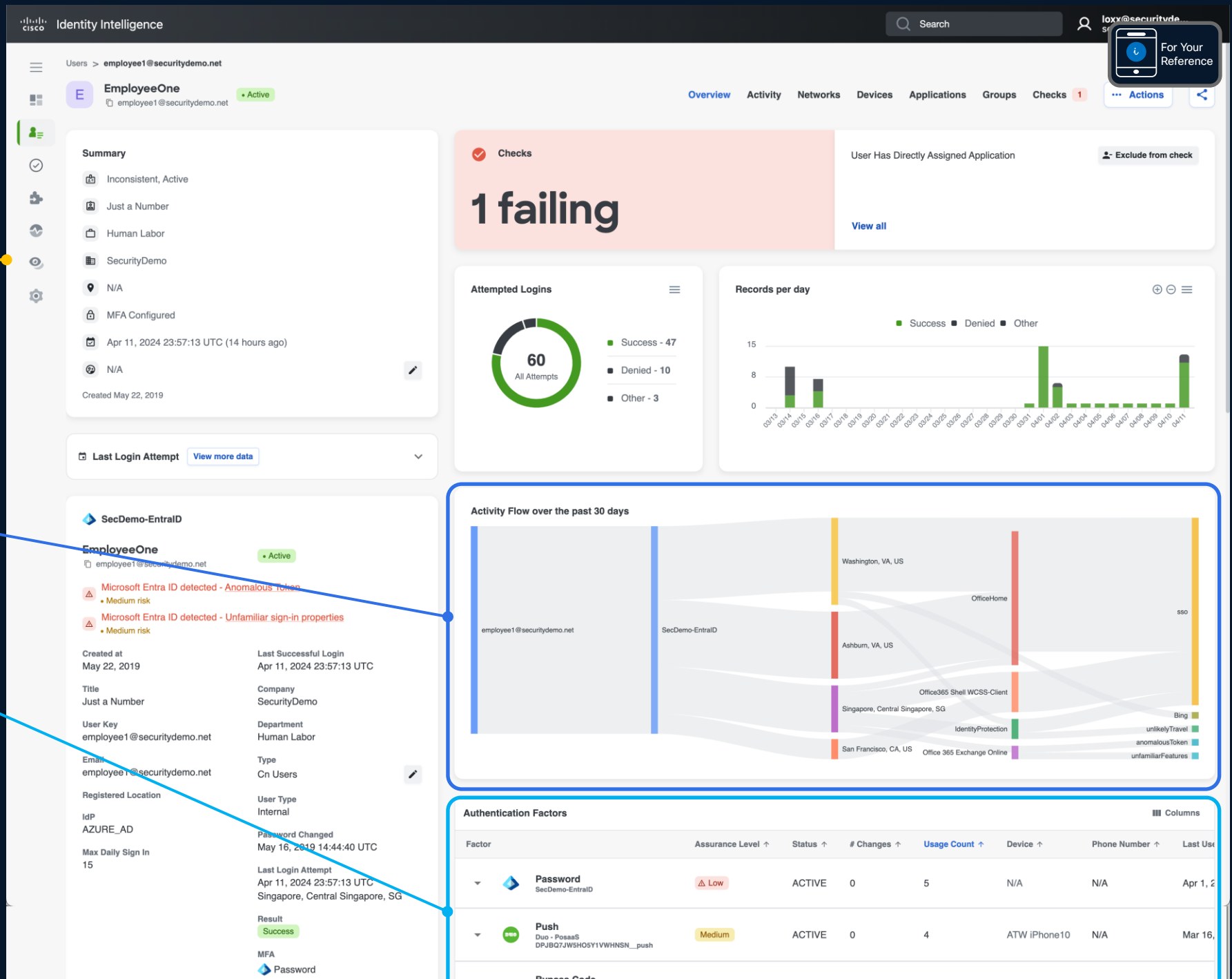
A true look at the user’s identity related security, activity and other important properties.

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



Activity

For Your Reference

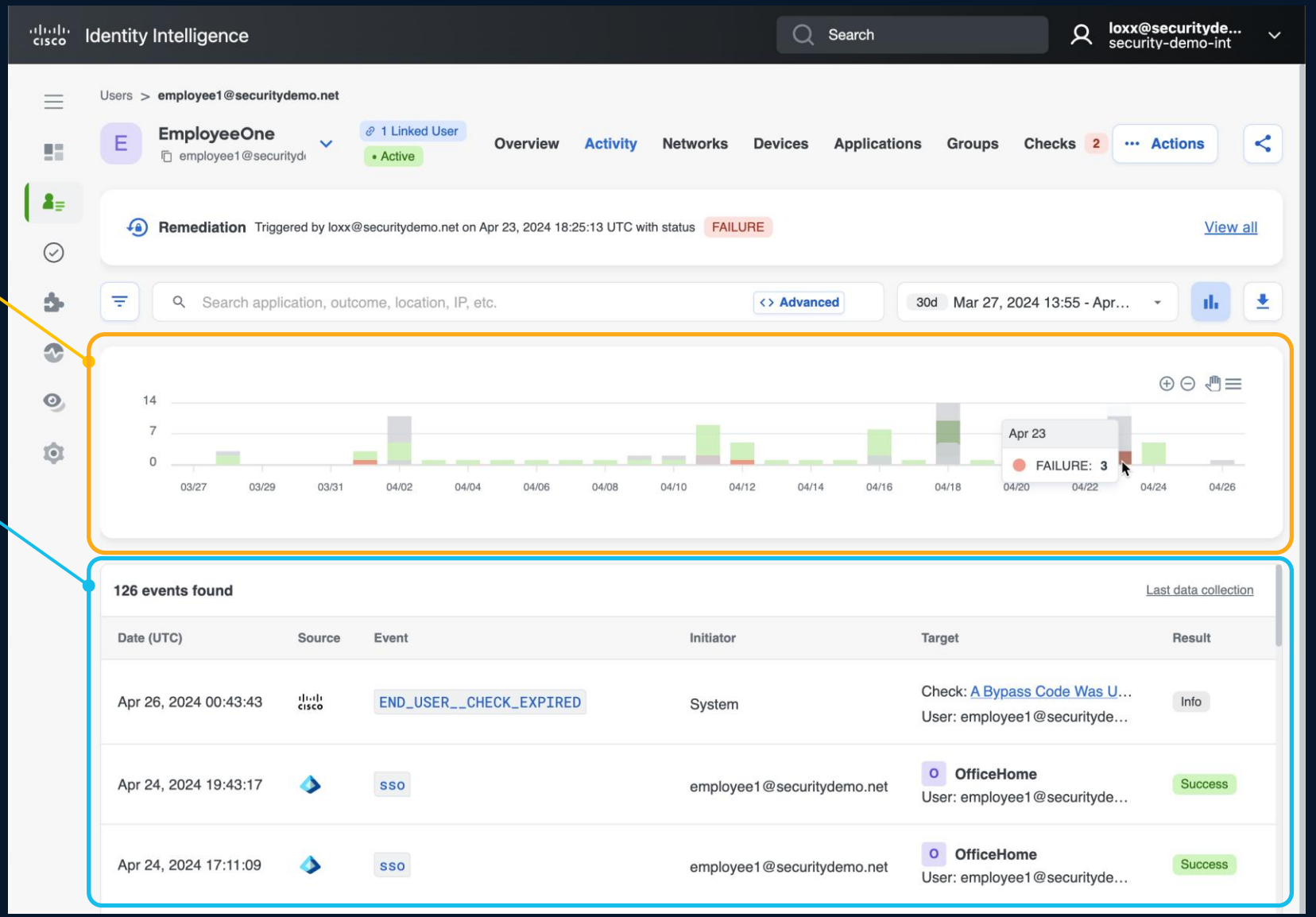
Activity Timeline

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

For Your Reference

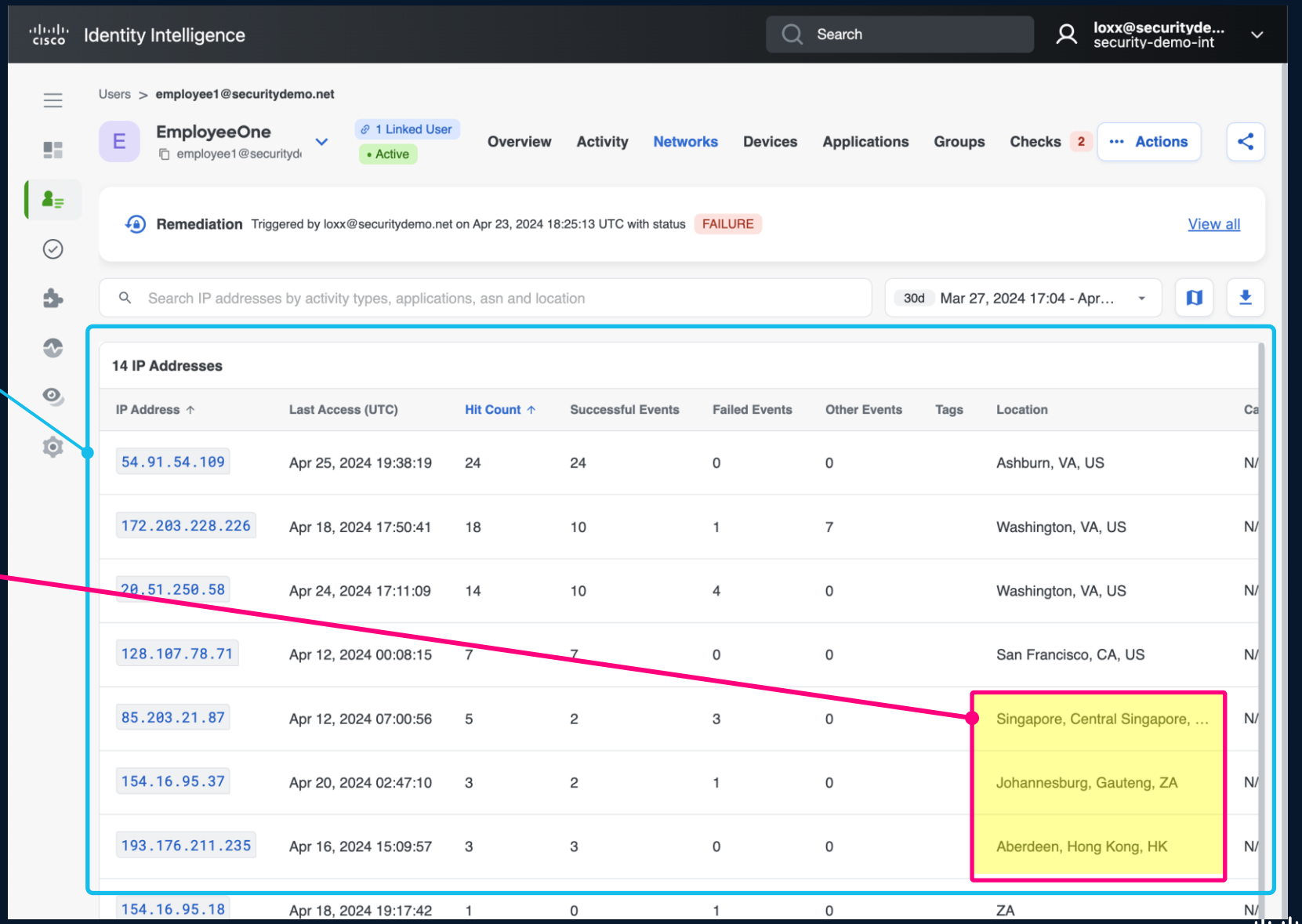
IP's recorded in IDP Logs

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

For Your Reference

Devices from IDPs

Not all IDPs are created equal with device information

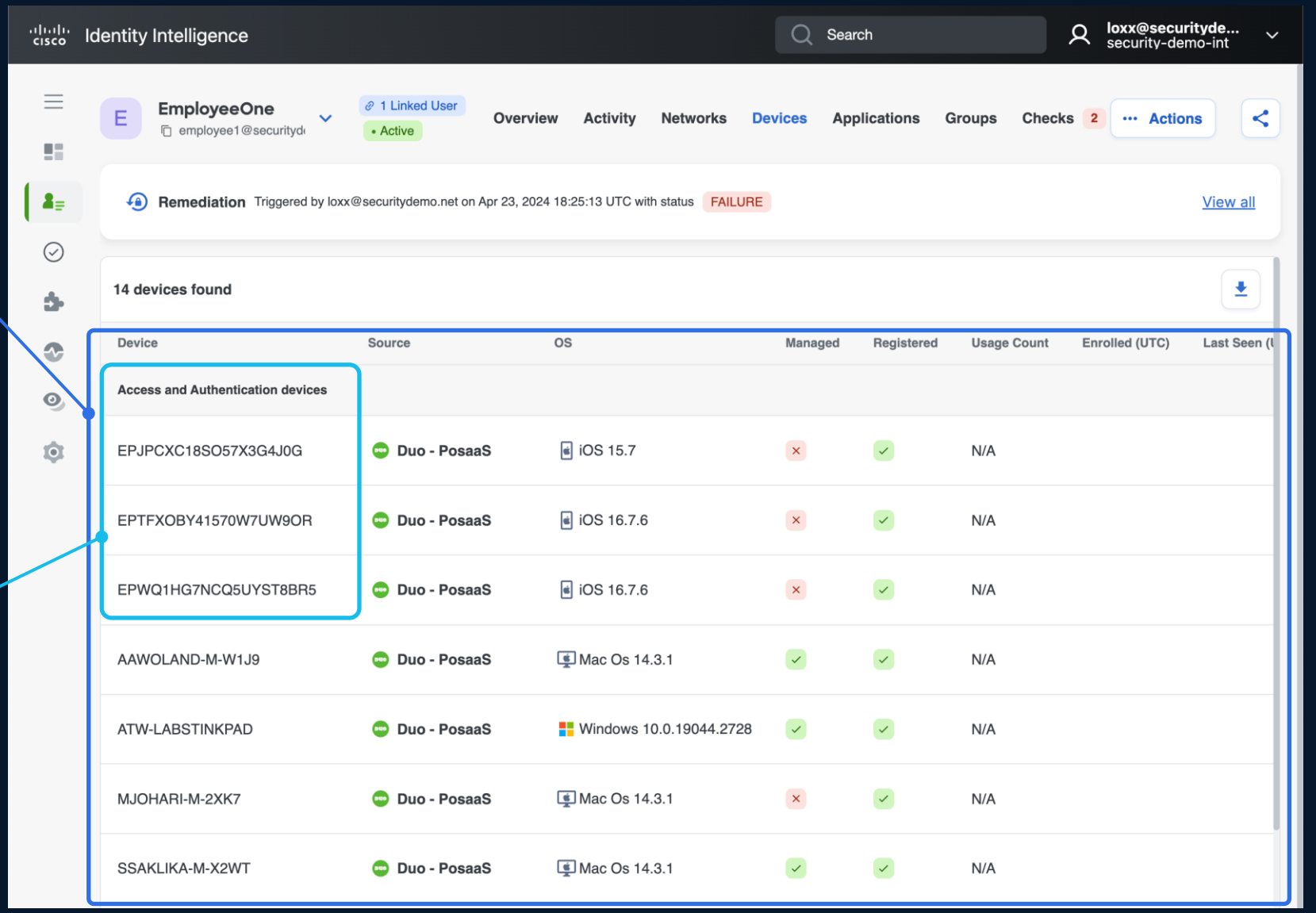
Duo is the best source for device data – when the Duo Auth includes the Health App.

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

For Your Reference

Usage Statistics

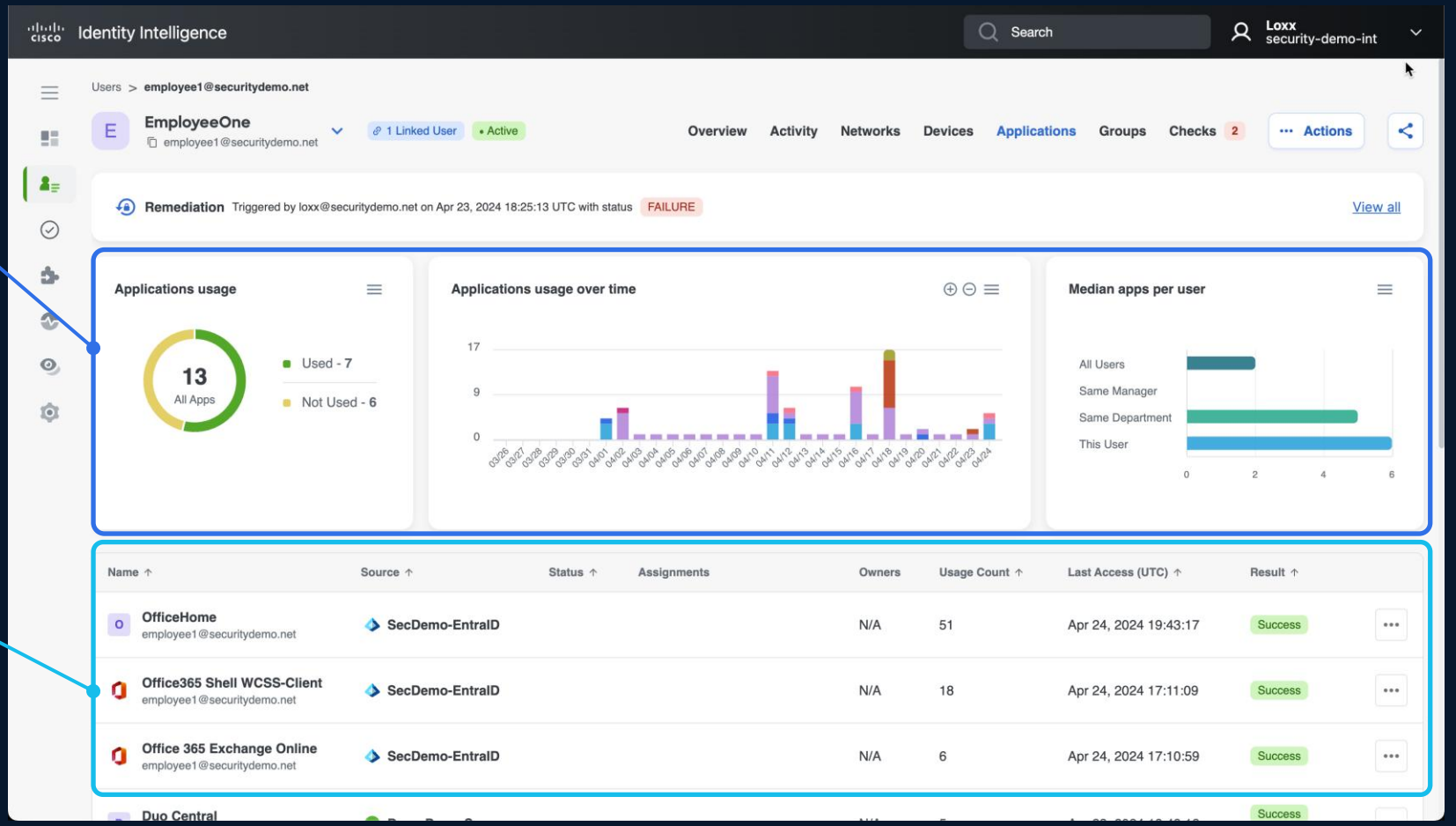
Quick overview of the apps used

Includes Apps not used

Application List

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

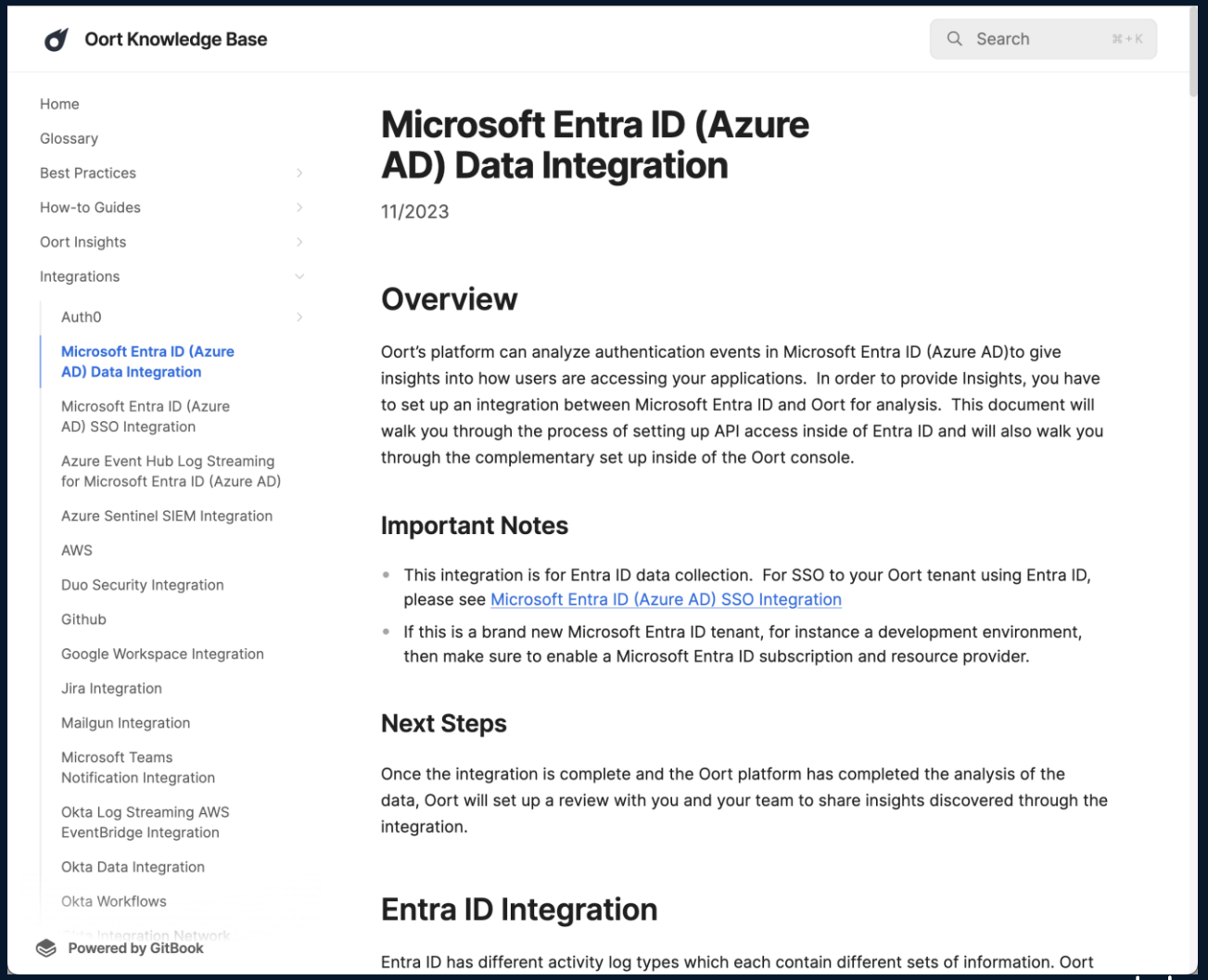
Which IDP reported the access & usage counts.



Excellent Documentation

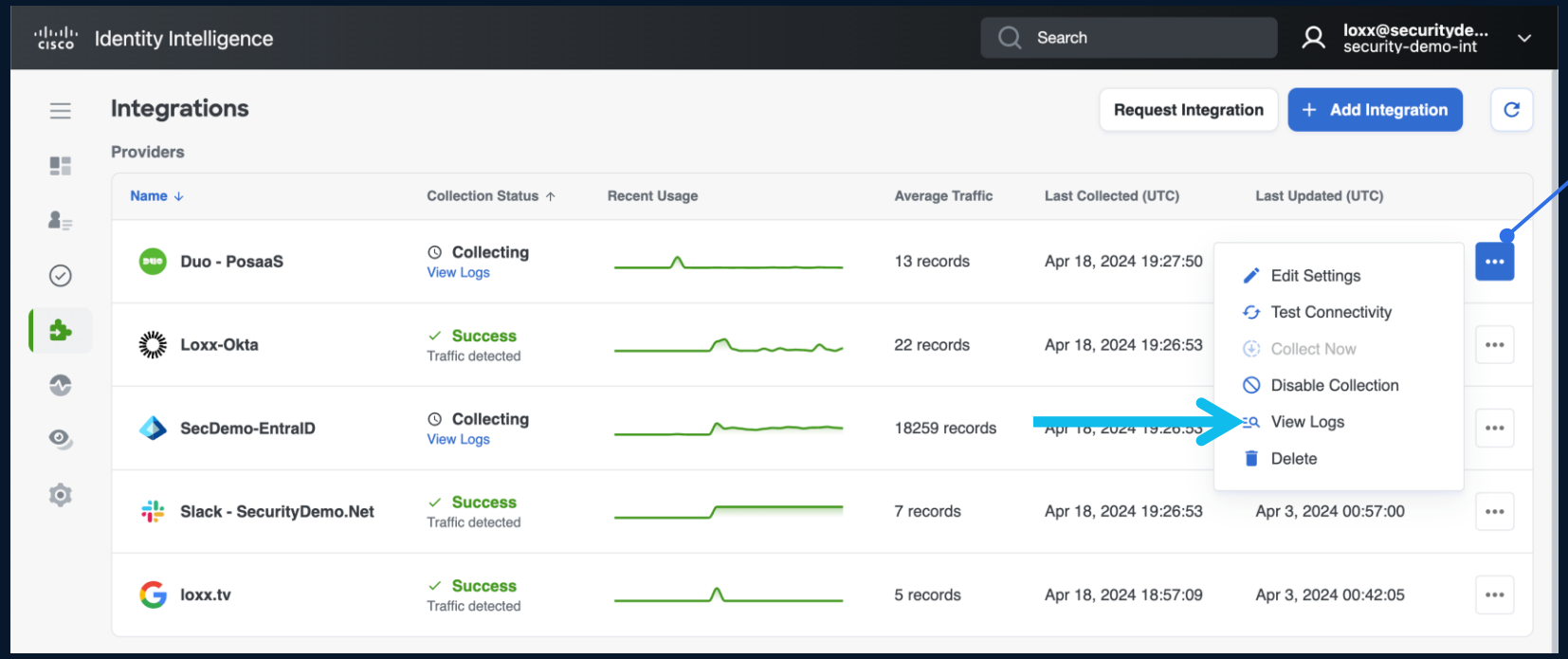
For Your Reference

- 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

For Your Reference



Ellipses (...)

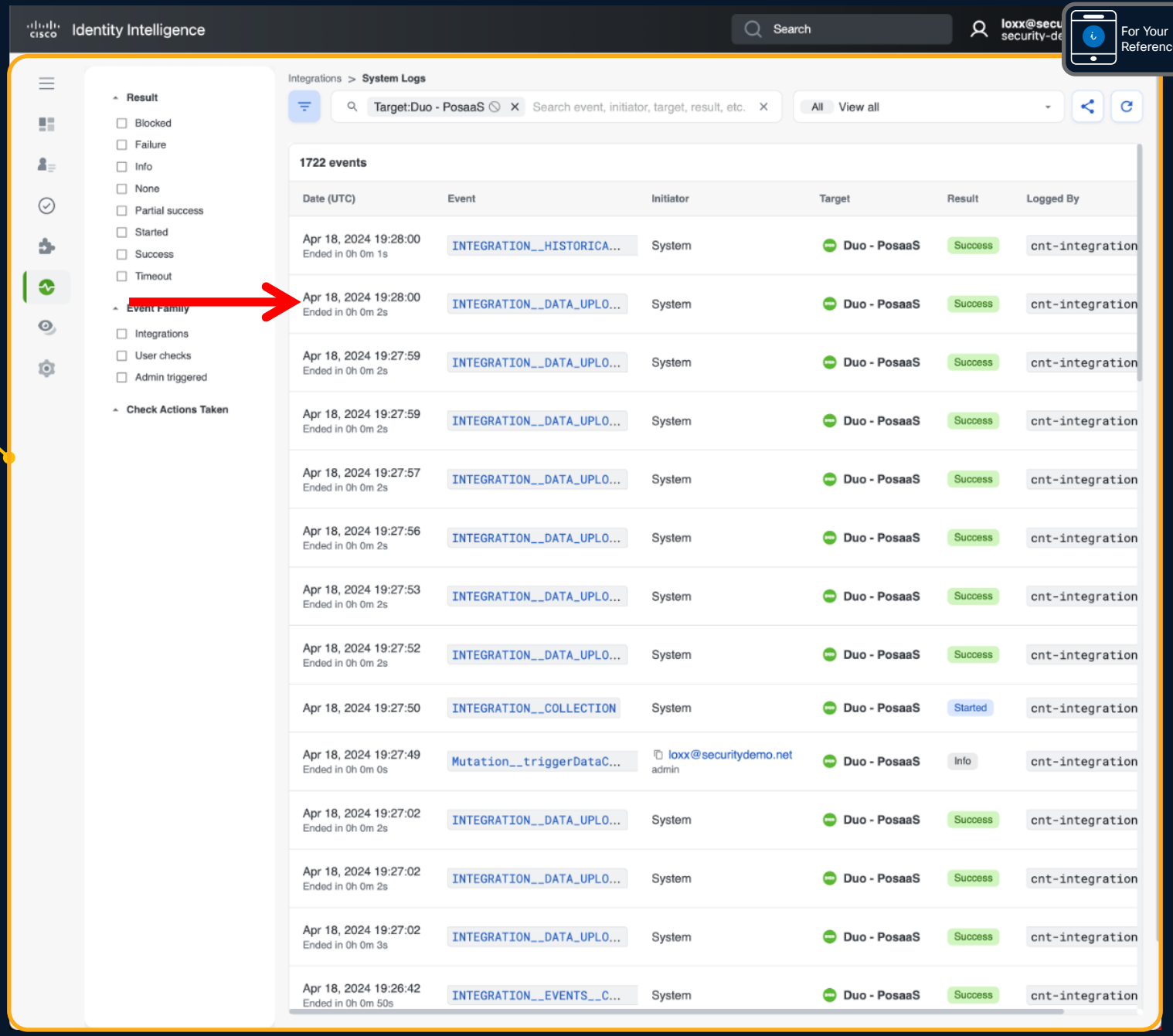
- Edit Settings
- Test connectivity – Terrific way to ensure the connection is working as expected
- Trigger collection (sync)
- Disable collection – use when there is an issue, and then enable again after that issue is resolved
- View Logs – see all logs related to the specific integration.
- Delete

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.



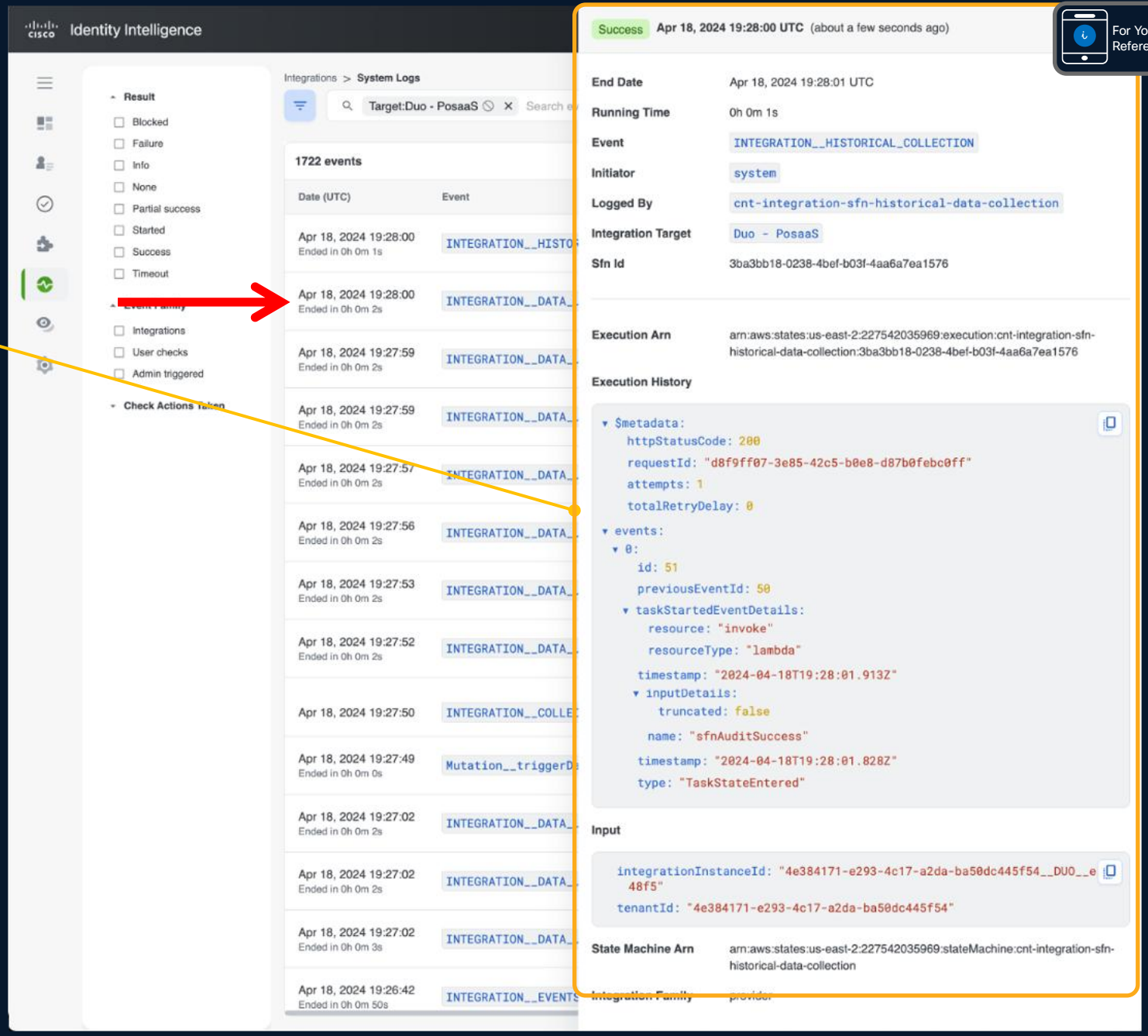
View Logs

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.

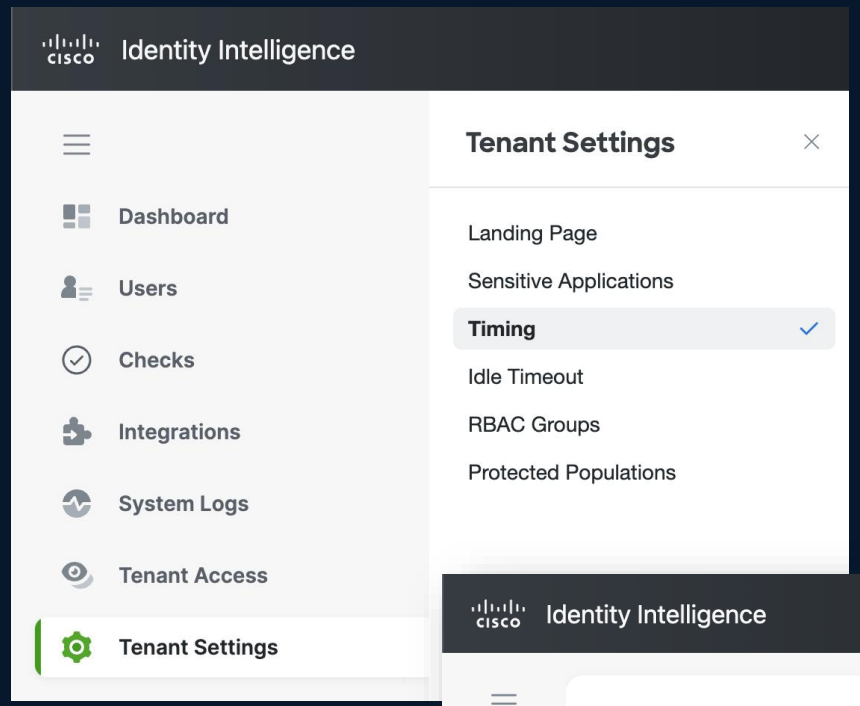
Aids tremendously when troubleshooting why information isn't getting sync'd across.

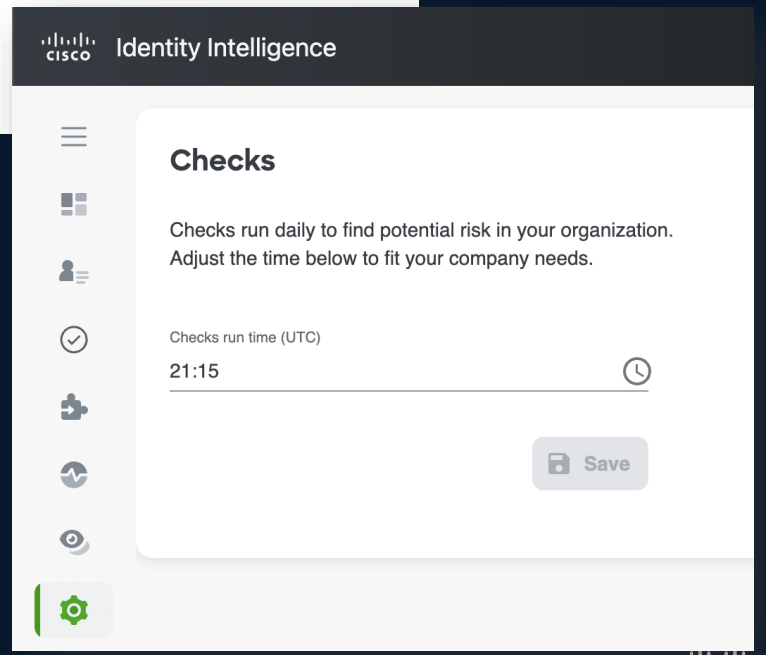


Sync Schedule

For Your Reference

- 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)

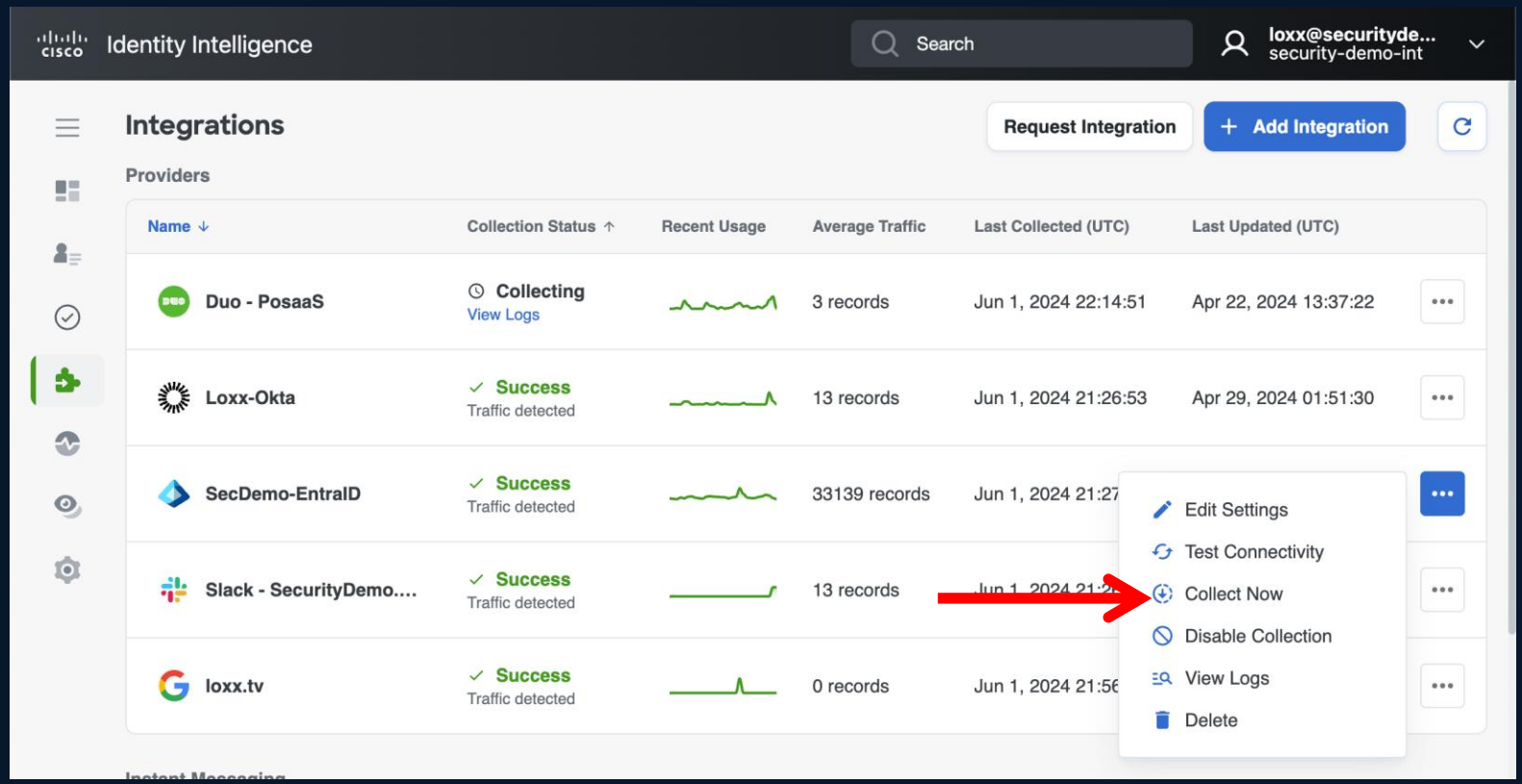




Sync Schedule

For Your Reference

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



For Your Reference

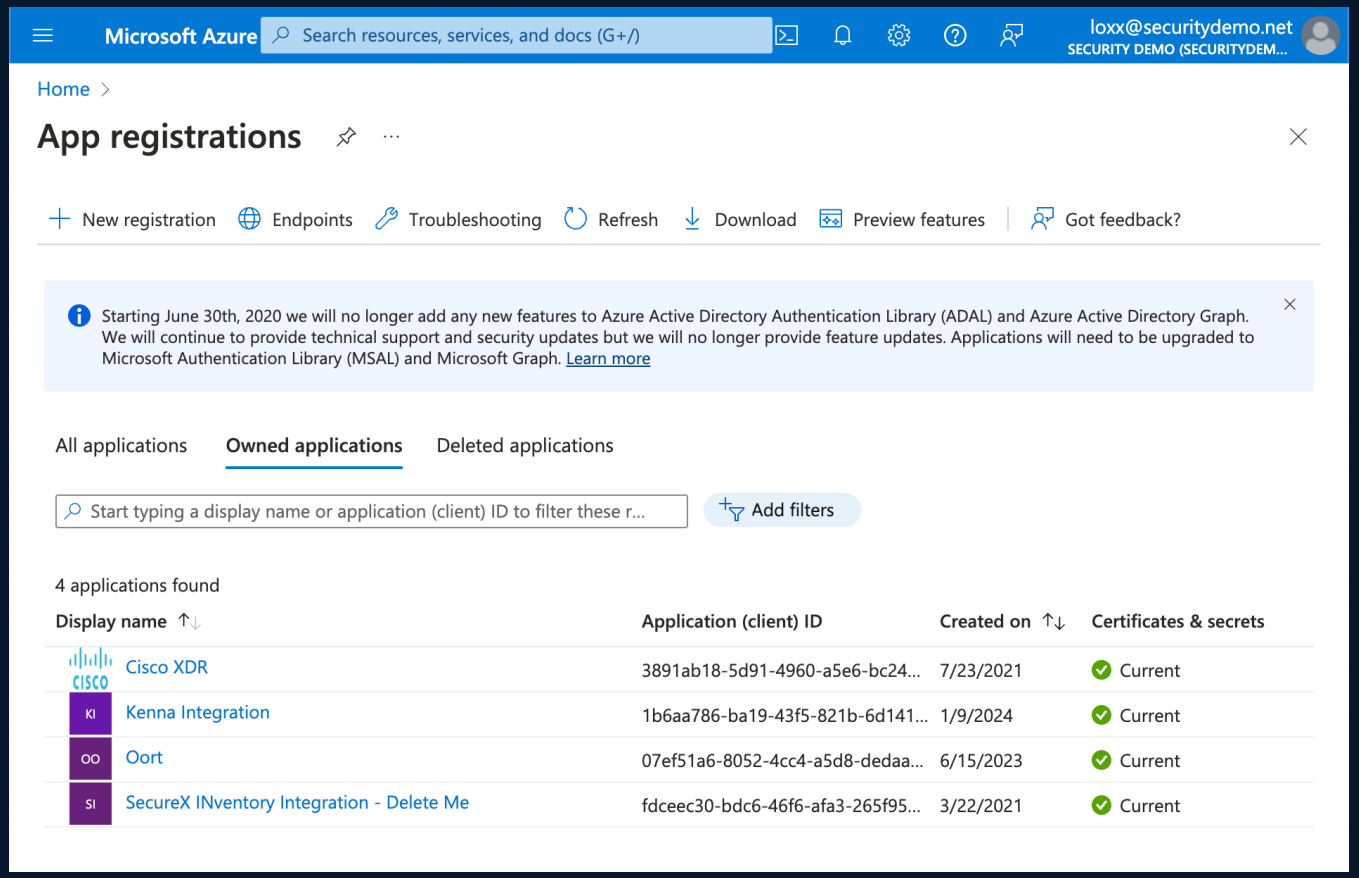
Microsoft Entra ID

Aka: Azure Active Directory (AAD)

MS Entra ID

For Your Reference

- 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

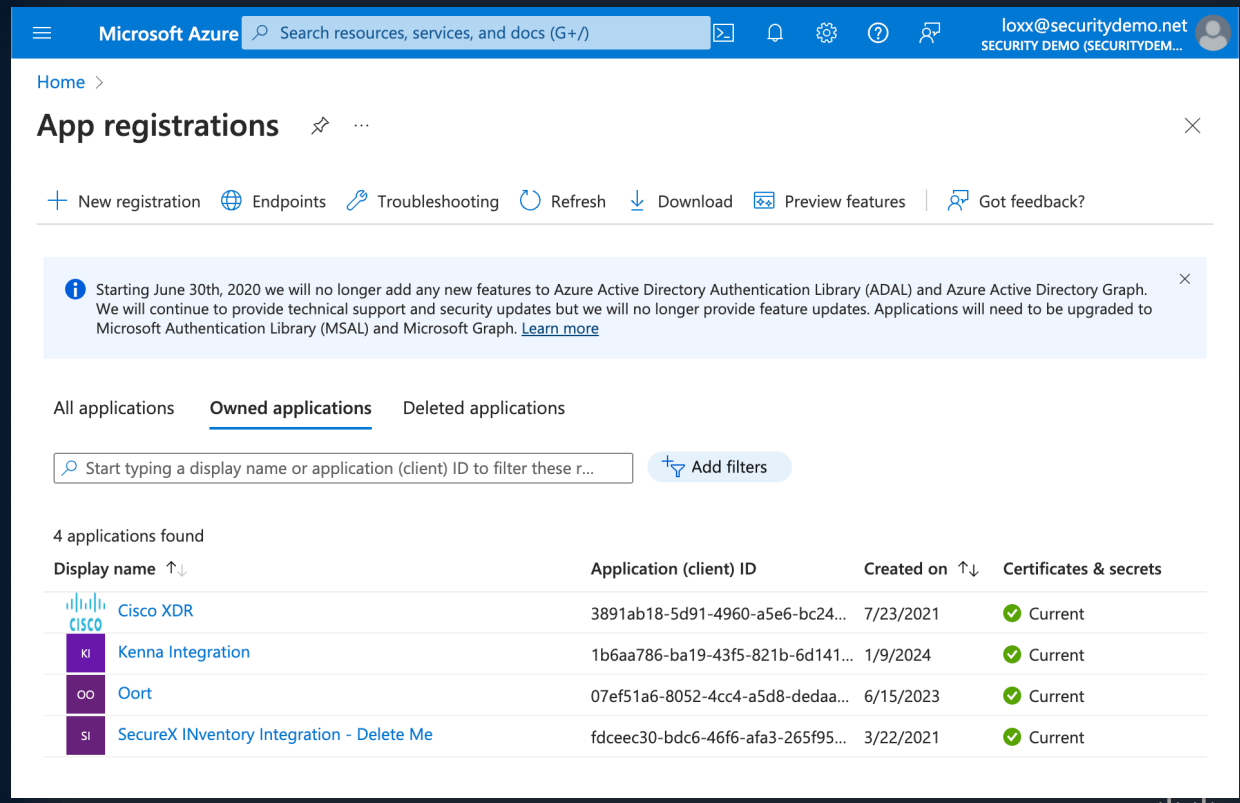


MS Entra ID

- 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

For Your Reference



MS Entra ID

General Settings

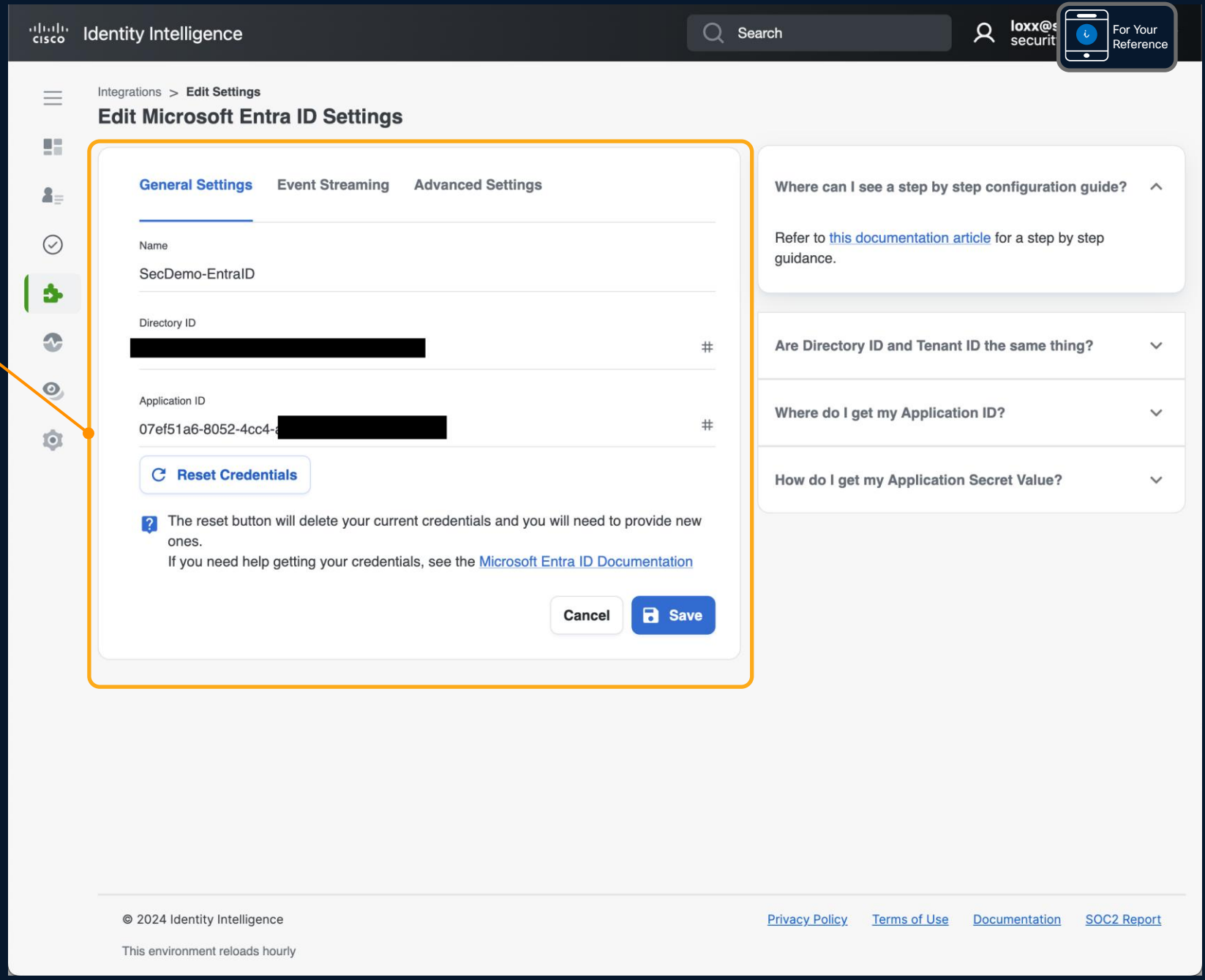
The credentials you obtained from the Azure “App” (ClientID, Secret Key, etc.)

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



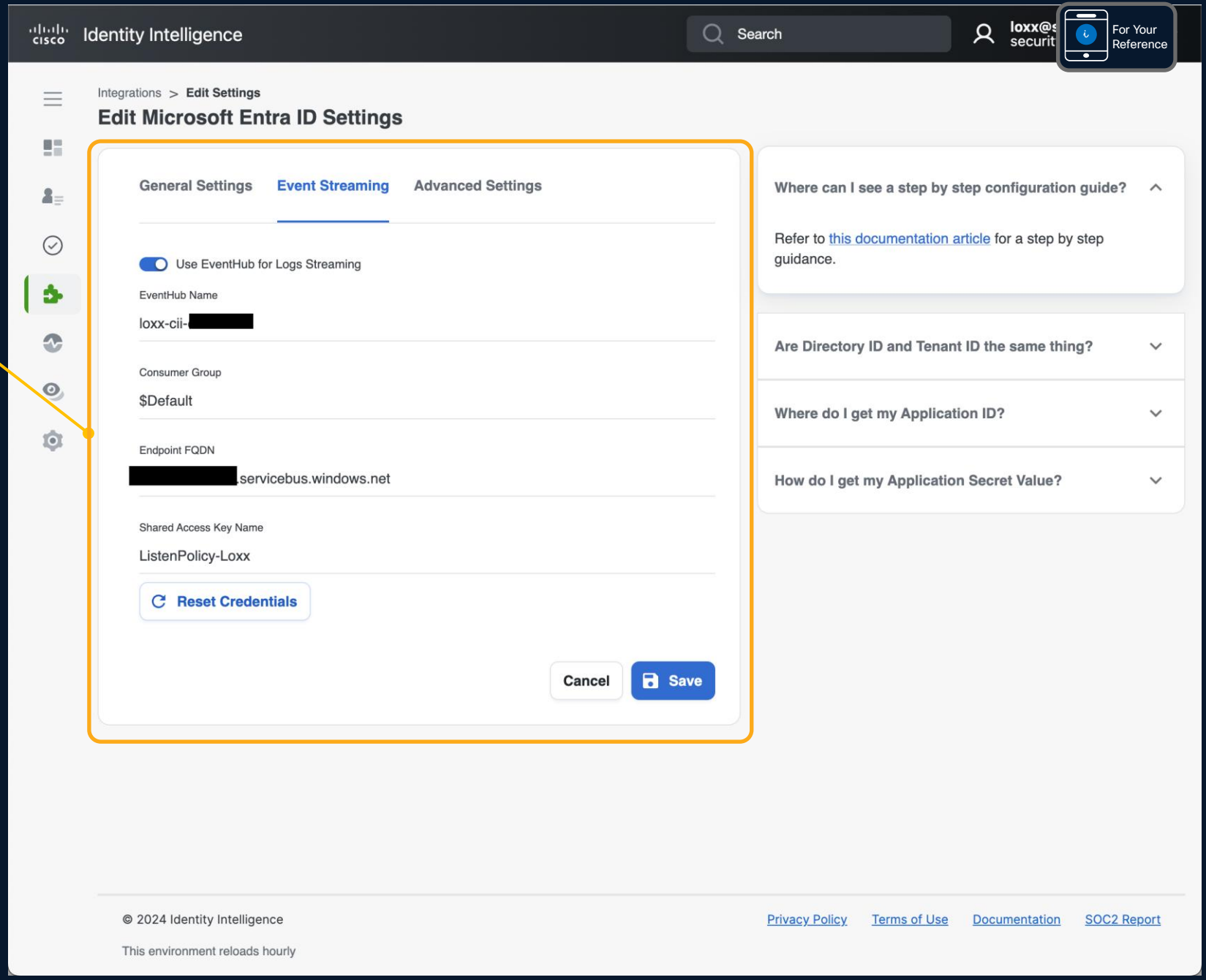
MS Entra ID

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)

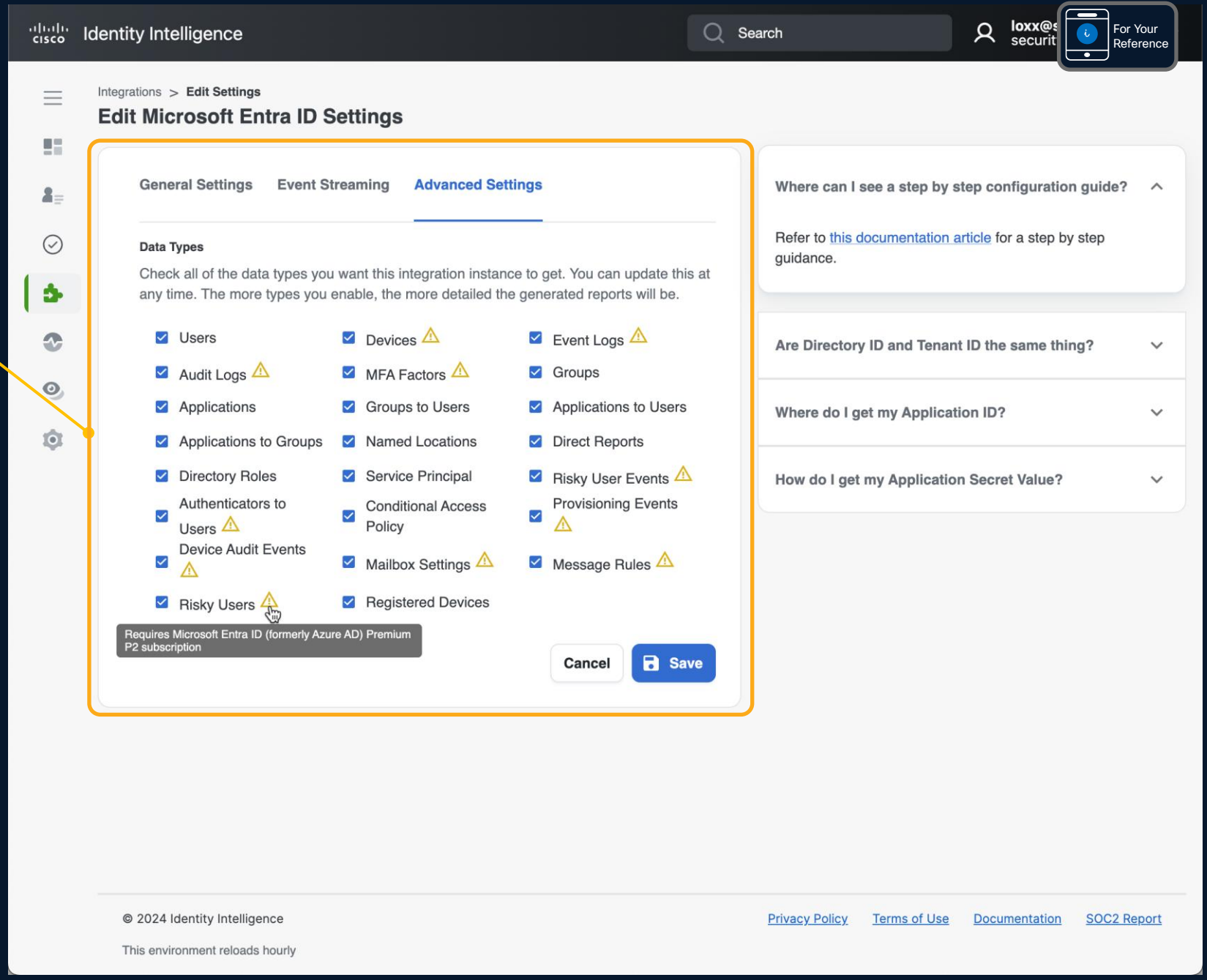


MS Entra ID

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.



For Your Reference

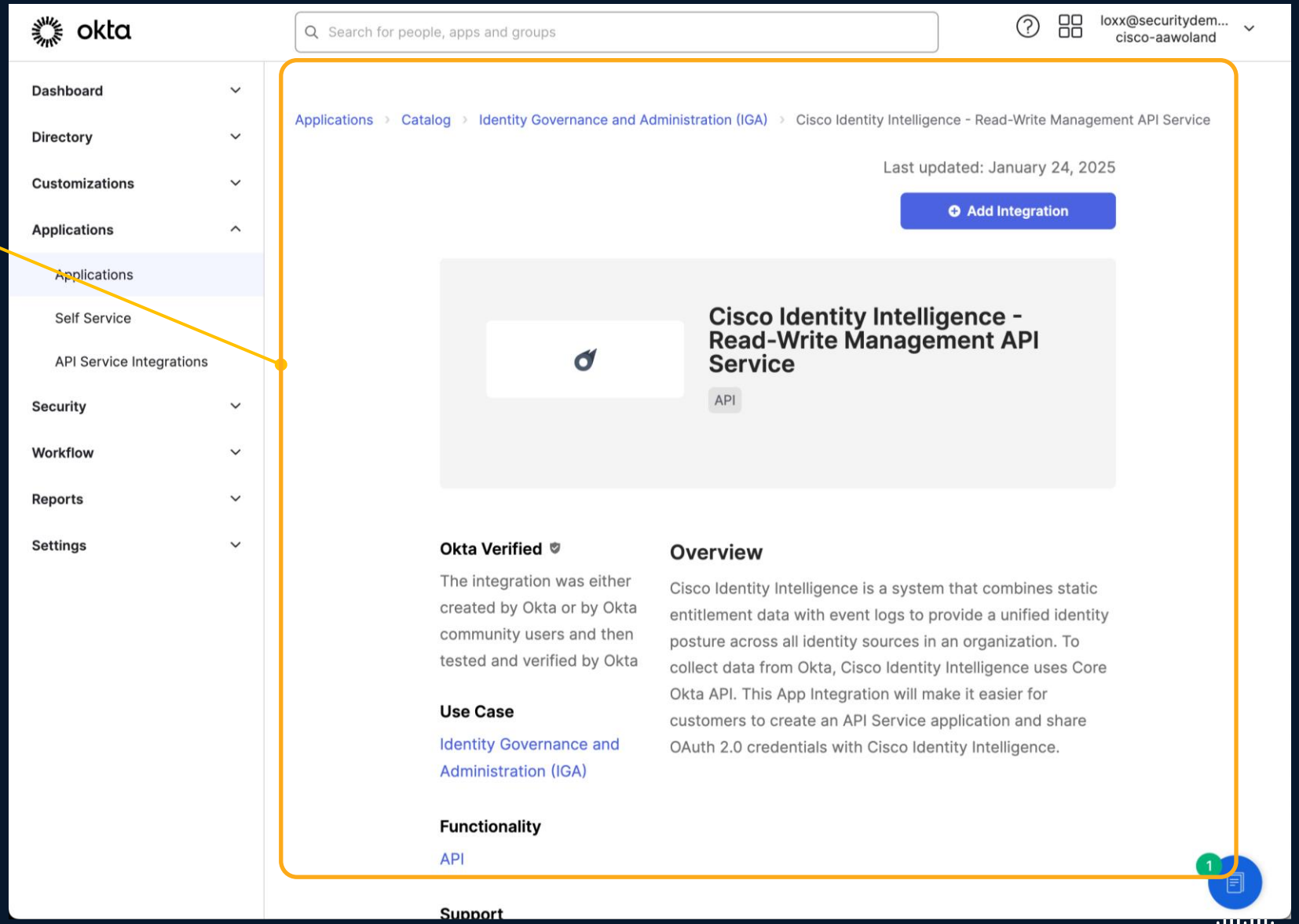
Okta Identity Engine

Okta

For Your Reference

App Catalog

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



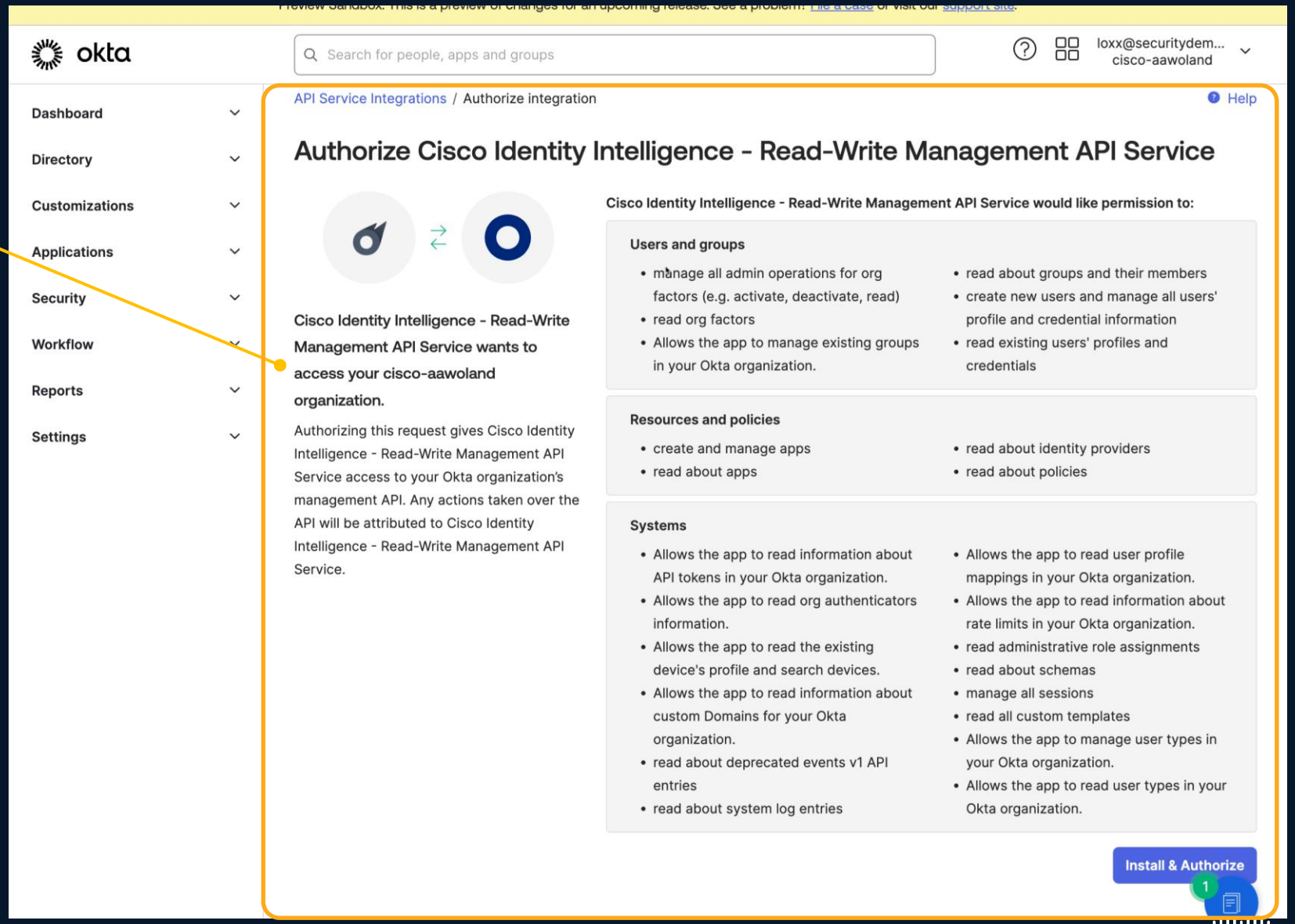
Okta

For Your Reference

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.



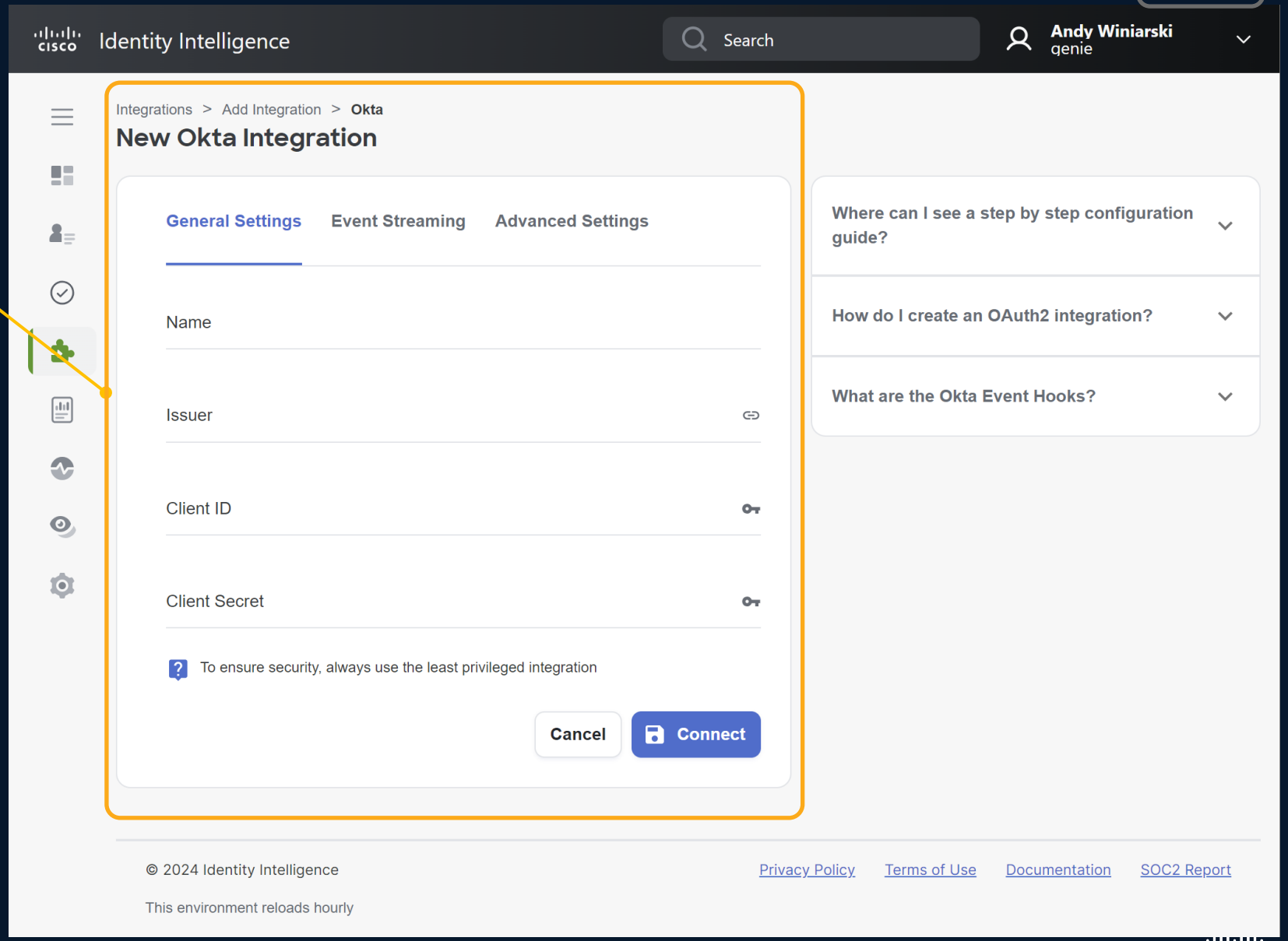
Okta

For Your Reference

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



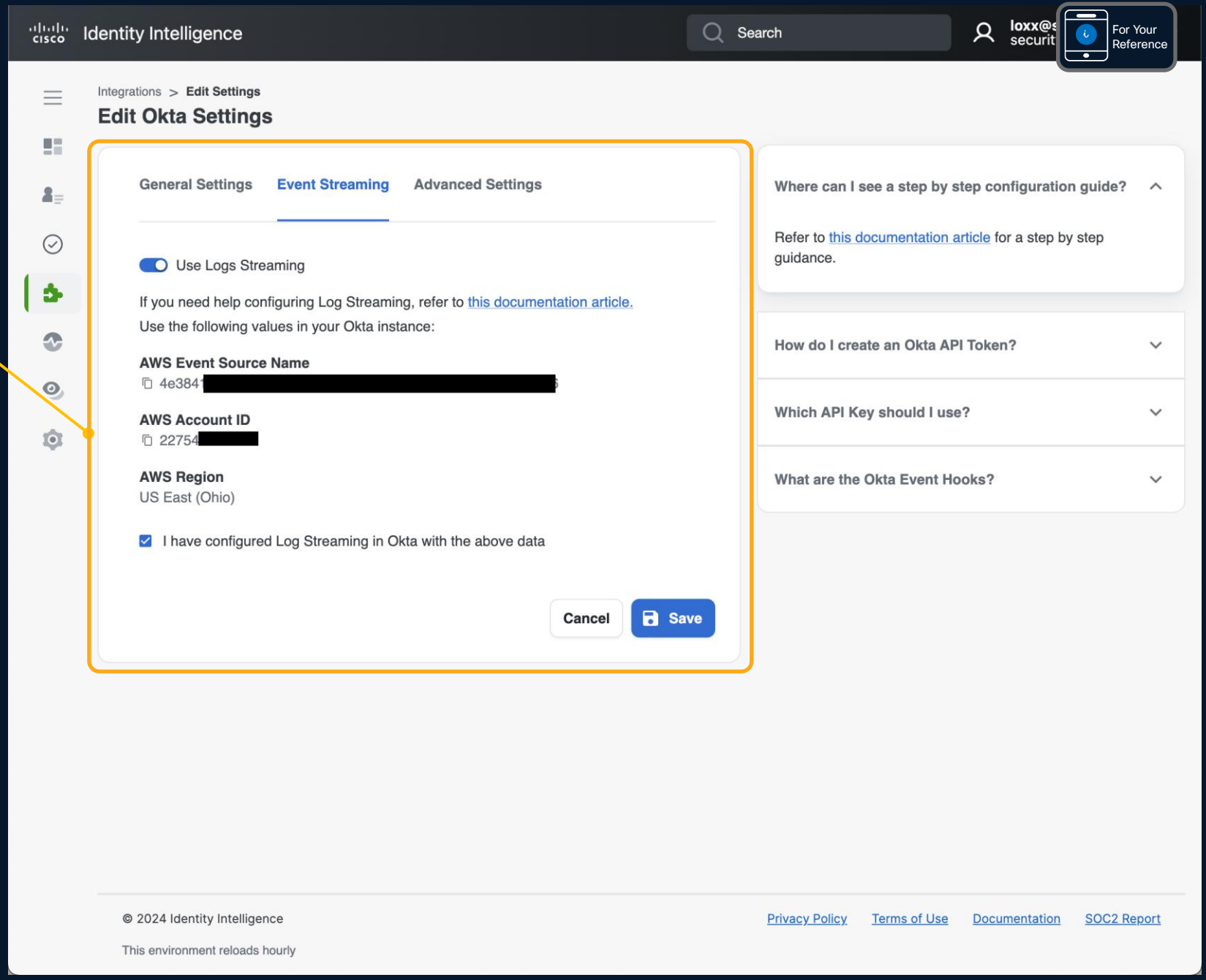
Okta

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

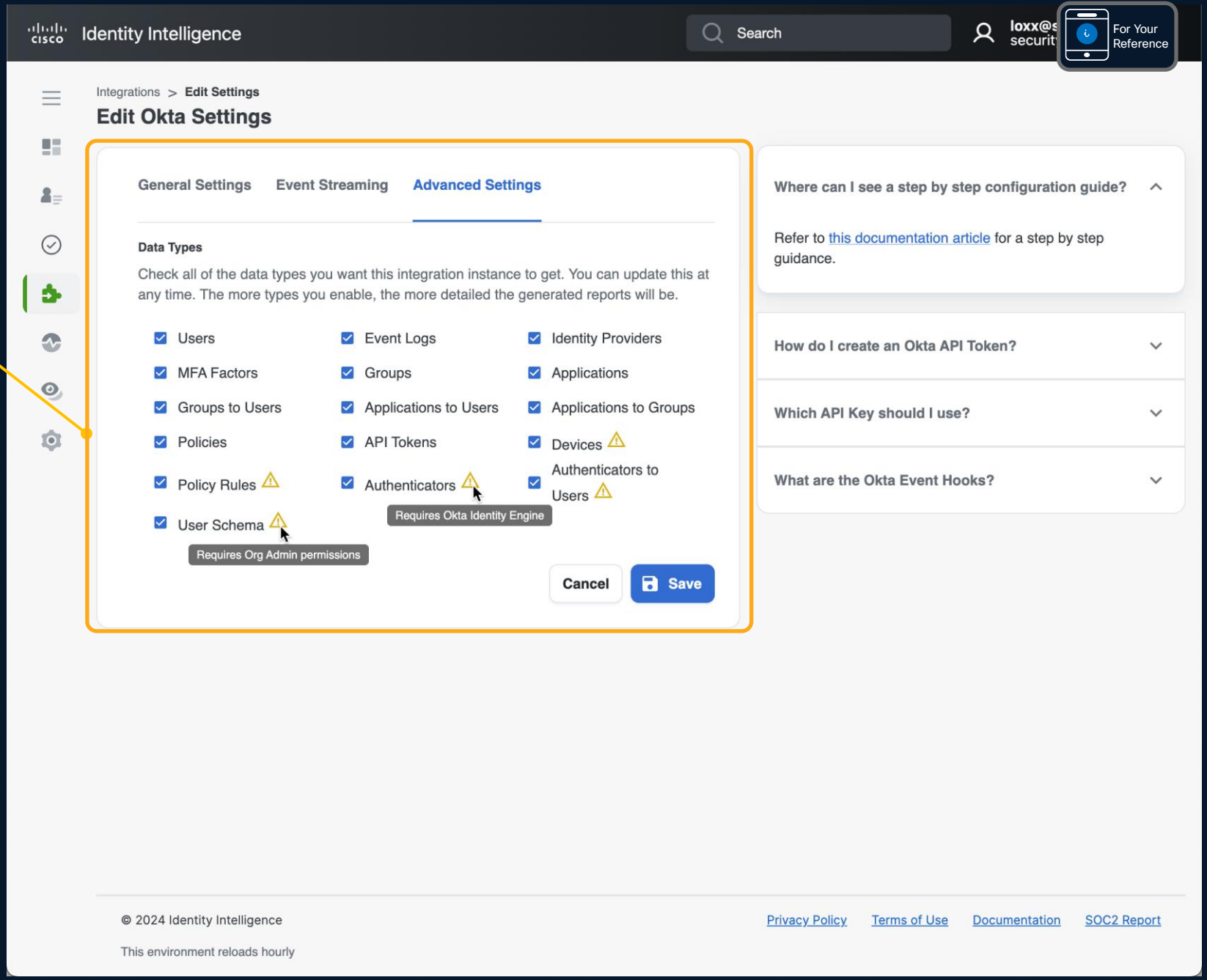
Advanced Settings

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

01 What is Cisco Identity Intelligence

02 Identity Security Posture

03 Monitoring Auth Factor Progression

04 Threat Detection & Response

05 User Trust Levels

06 Identity Security Assessments

07 Putting the “R” in ITDR

08 Call to Action

Please fill out the Survey

If there is anything we can improve, please let us know!

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

Continue your education

Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: Insert preferred comms method

Thank you


CISCO