

Identity Intelligence Demystified

Technical deep dive into CII (formerly Oort)

Aaron T. Woland, CCIE #20113

Distinguished Engineer, Identity Security | loxx@cisco.com | [X @aaronwoland](https://twitter.com/aaronwoland) | [in aaronwoland](https://www.linkedin.com/in/aaronwoland)

CISCO Live !

Cisco Webex App

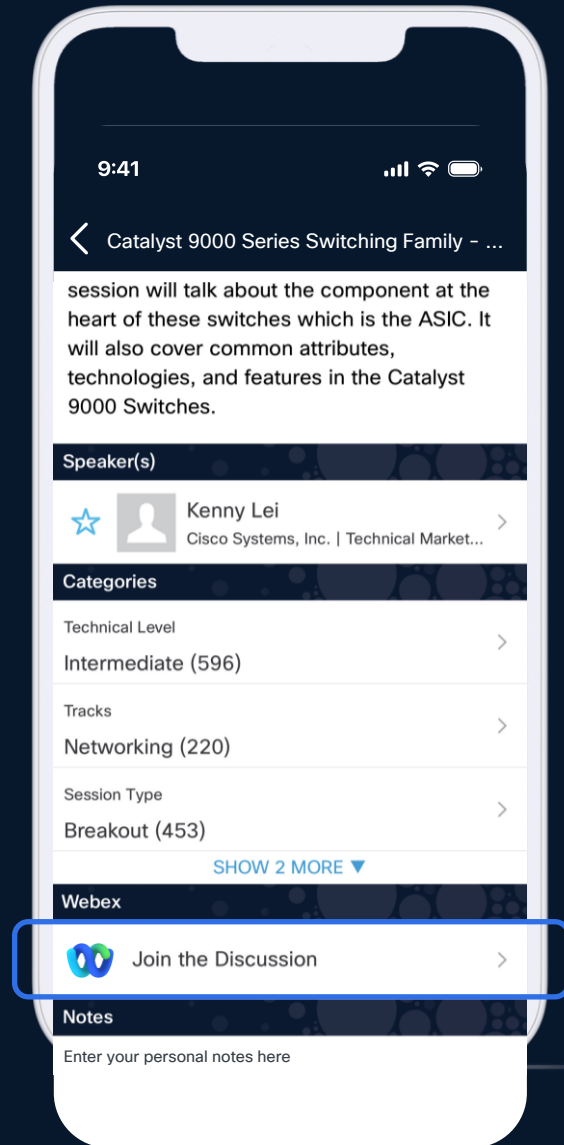
Questions?

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



For Your
Reference

- 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?



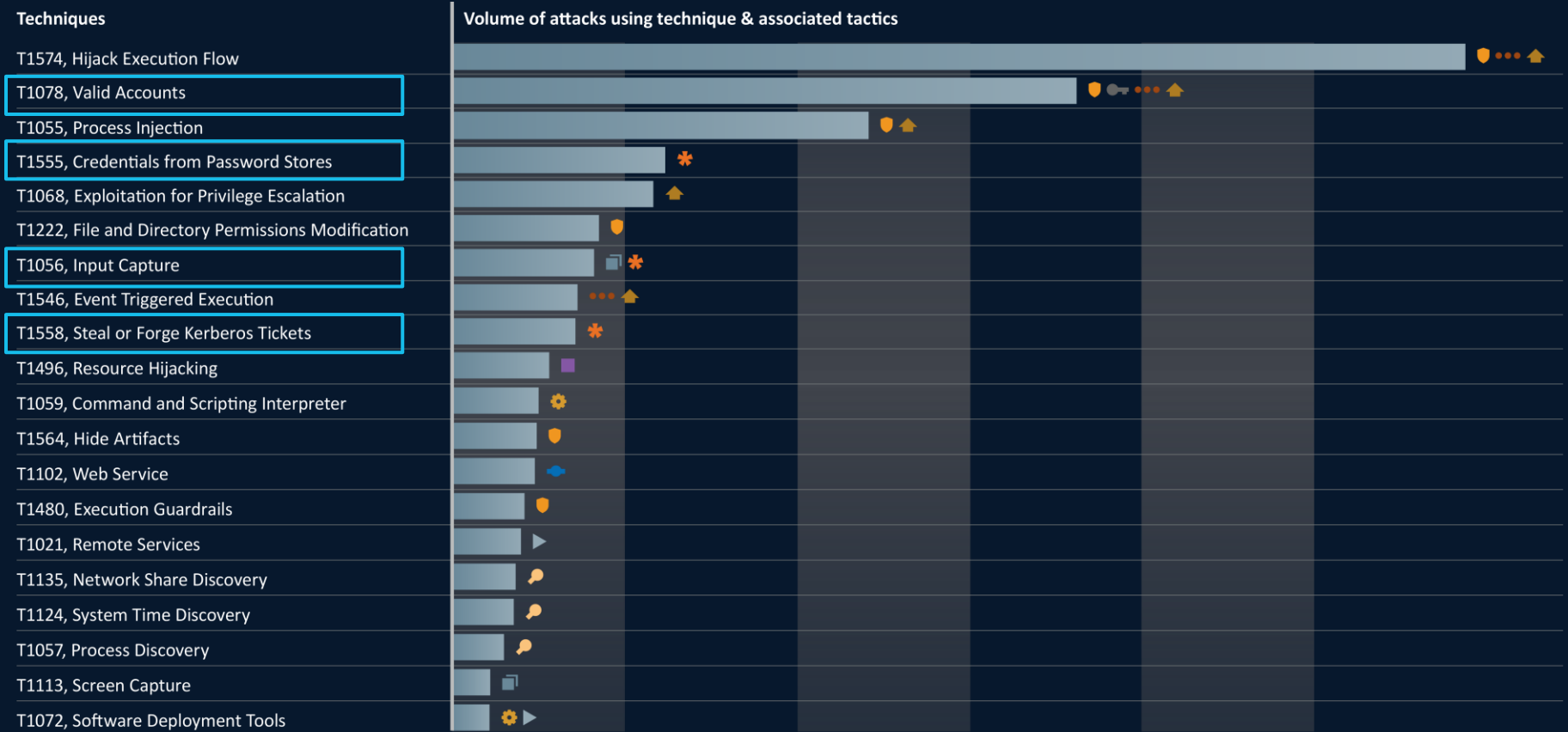
...a security discipline that encompasses threat intelligence, best practices, a knowledge base, tools, and processes to protect identity systems. It works by implementing **detection mechanisms, investigating suspicious posture changes and activities, and responding to attacks** to restore the integrity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

Gartner

Top MITRE ATT&CK techniques



Volume of attacks using technique and associated tactics



TACTIC KEY

- Collection
- Command and control
- Credential access
- Defense evasion
- Discovery
- Execution
- Impact
- Initial access
- Lateral movement
- Persistence
- Privilege escalation

Source: Cisco Secure Endpoint

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2162



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?



60
percent

of breaches
leveraged identity
as a key component

Cisco Talos Incident Response | Year in Review 2024

Breaches Occur: Fatigue with MFA “Nag”

Real Story

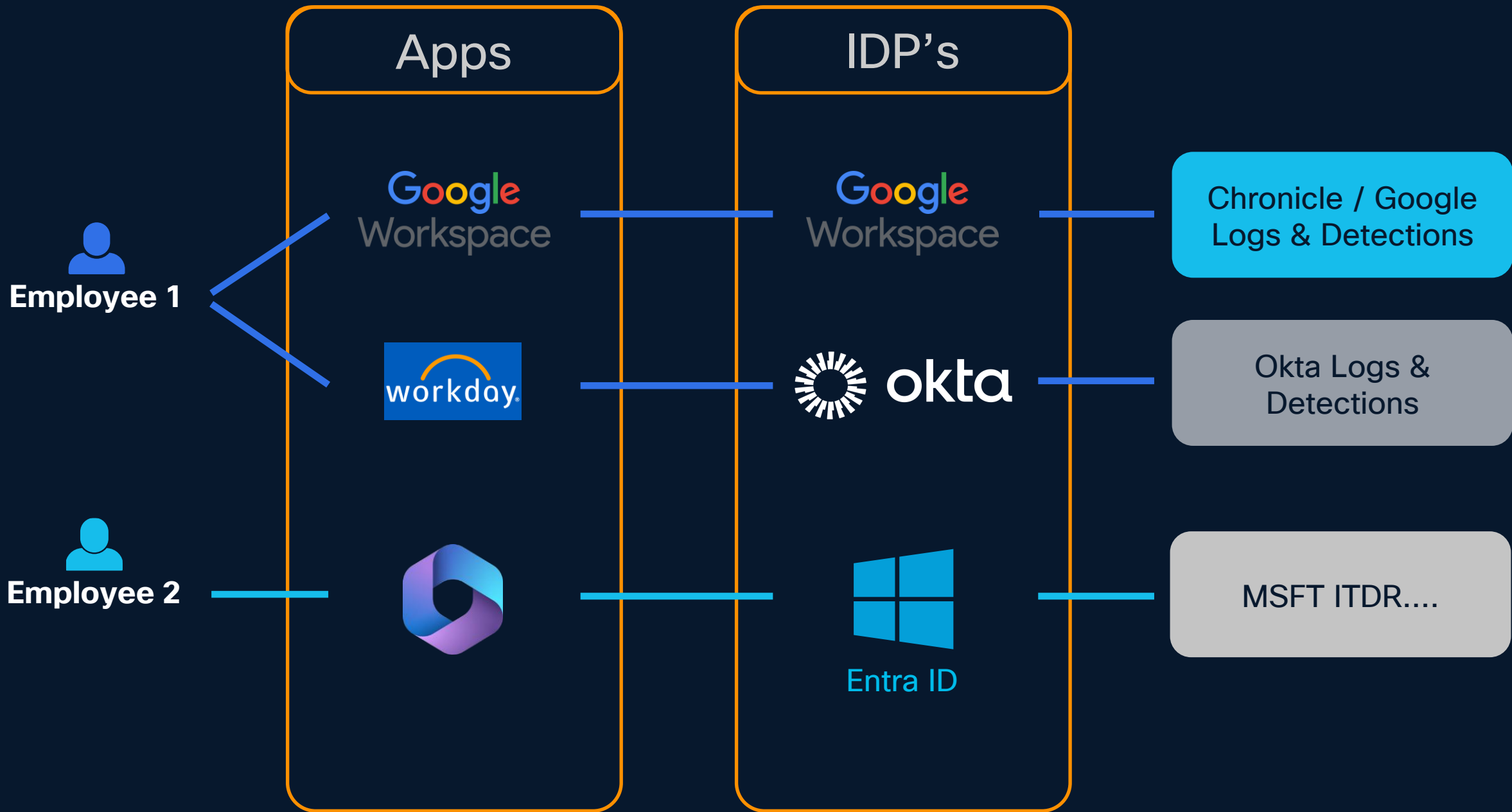
**Bypassed
My MFA**

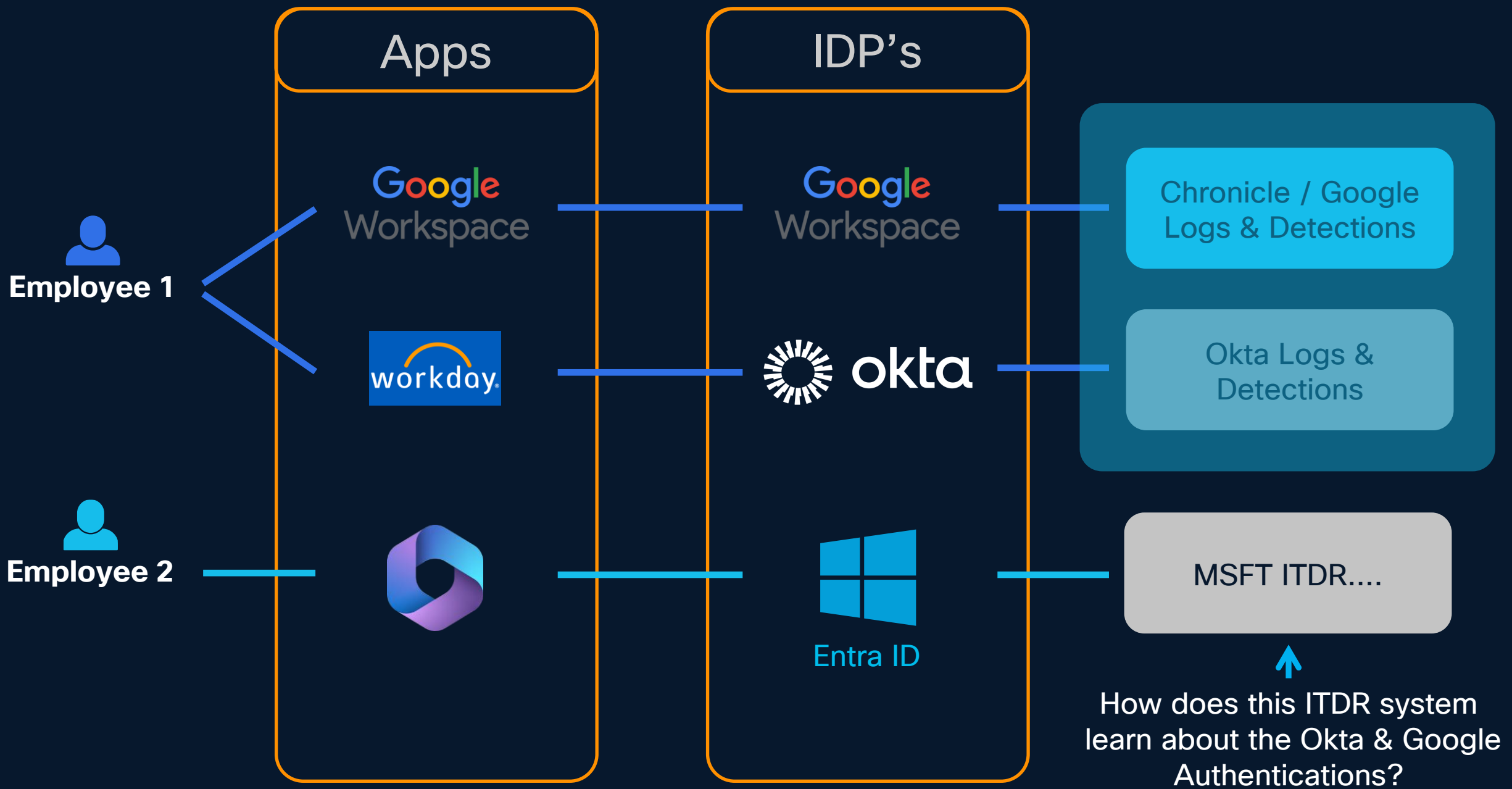
By Annoying Me!



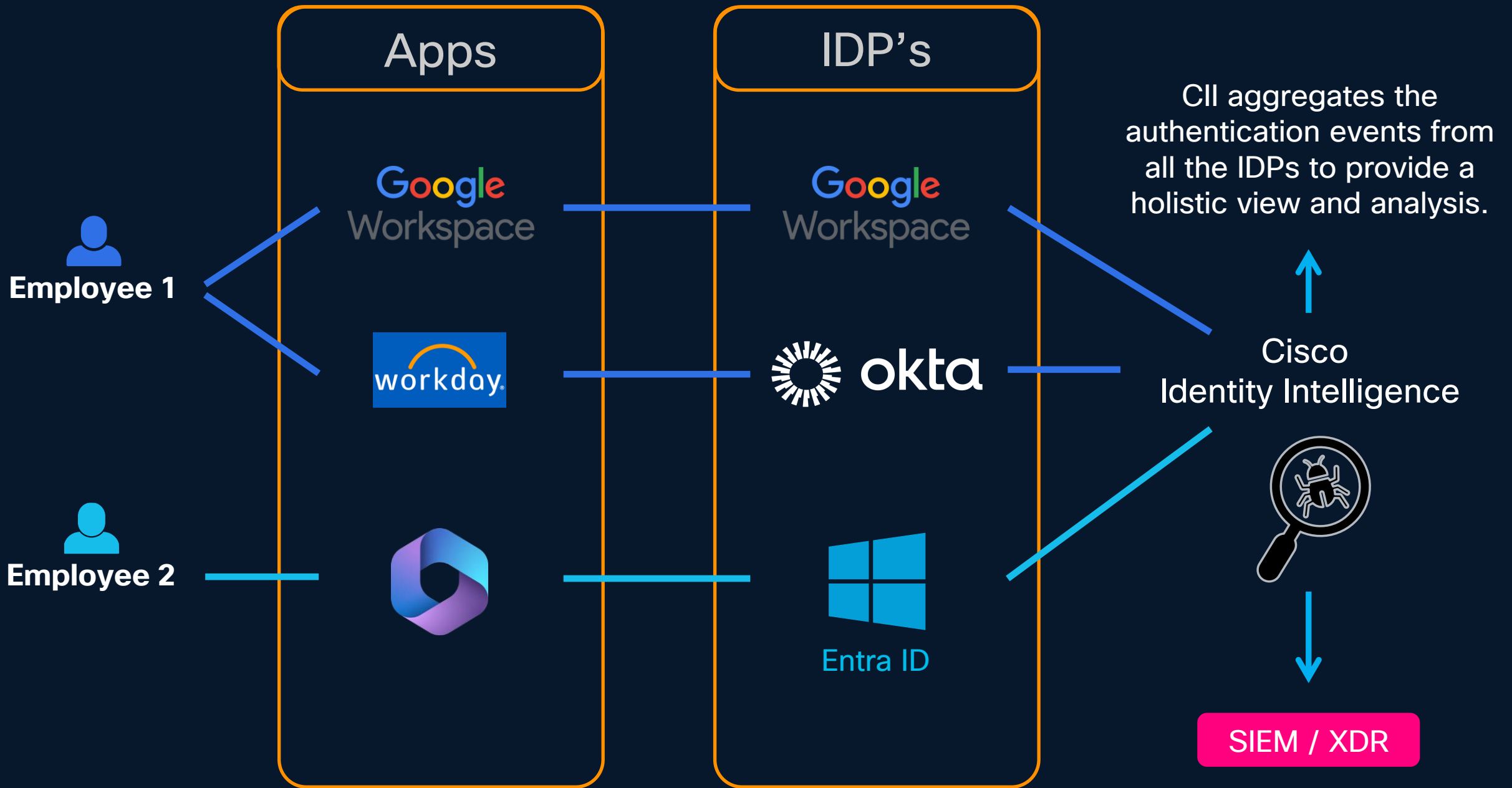
Credit: Wizer Security
<https://www.wizer-training.com>

**You cannot detect
what you cannot see!**





**“But I send all of this
to my SIEM...”**

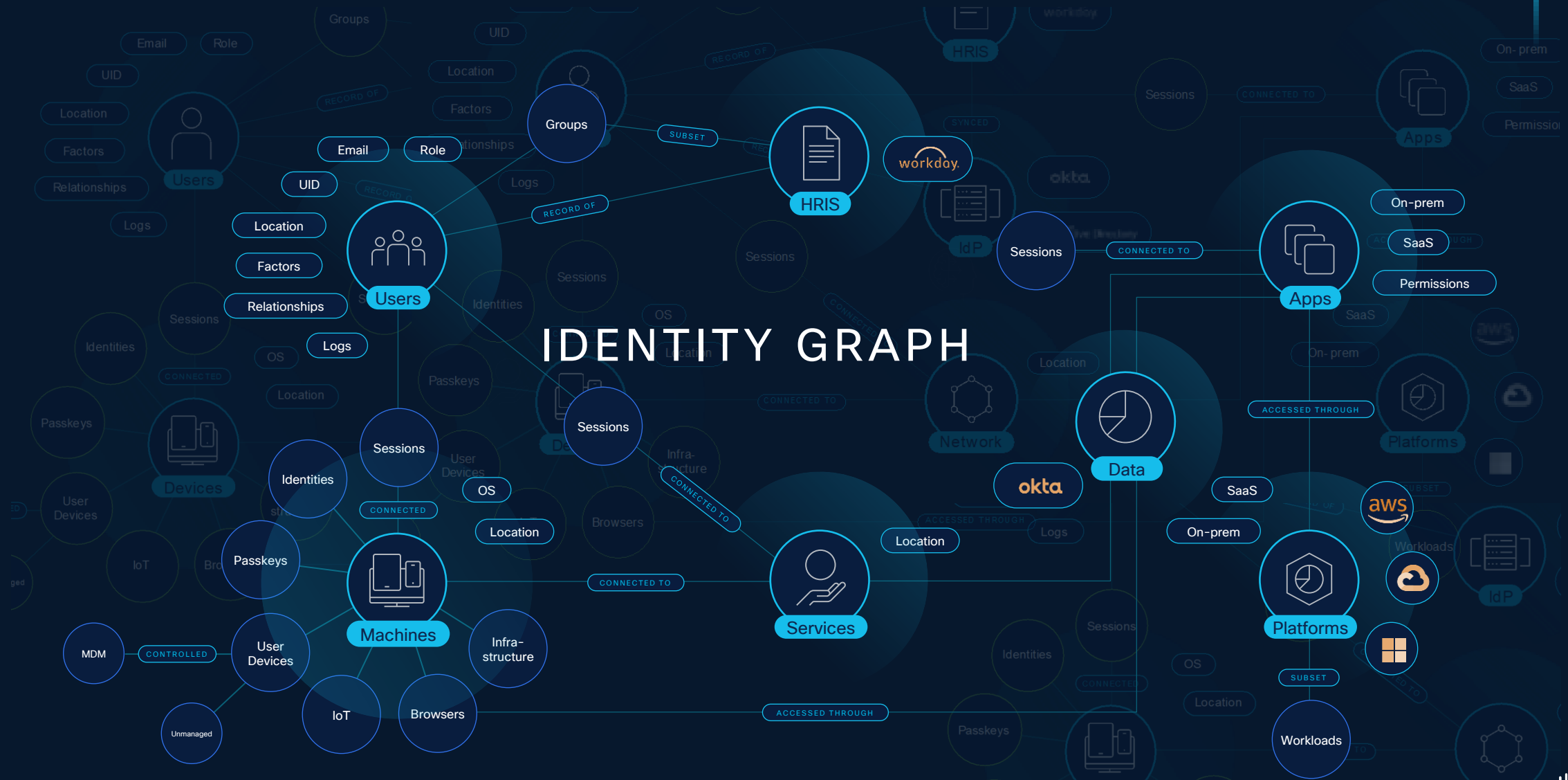


Cisco Acquires

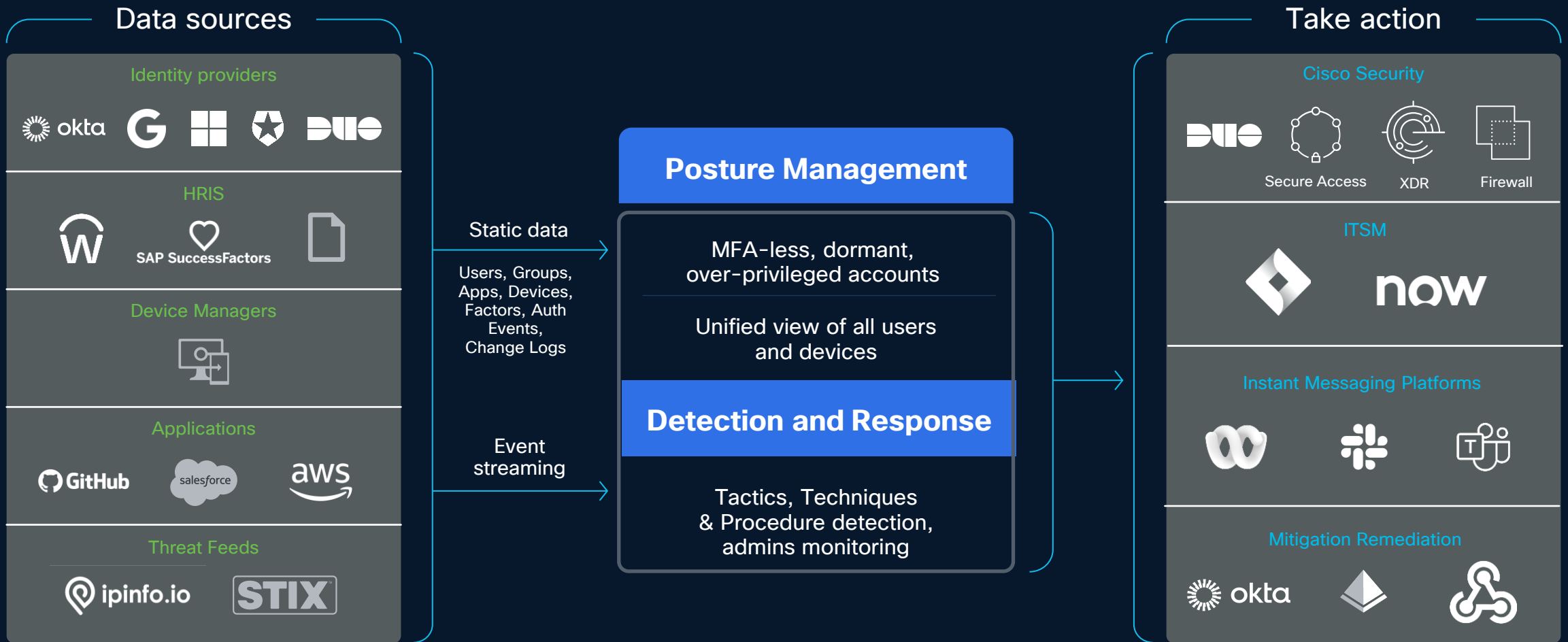
DOORT

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

Providers

Name	Collection Status	Recent Usage	Average Traffic	Last Collected (UTC)	Last Updated (UTC)
Duo - PosaaS	✓ Success Traffic detected		12 records	Apr 12, 2024 14:26:55	Mar 29, 2024 16:42:04
Loxx-Okta	✓ Success Traffic detected		15 records	Apr 12, 2024 14:26:53	Apr 2, 2024 16:13:08
SecDemo-EntraID	✓ Success Traffic detected		11297 records	Apr 12, 2024 14:27:55	Apr 2, 2024 13:08:22
Slack - SecurityDemo.Net	✓ Success Traffic detected		4 records	Apr 12, 2024 14:26:52	Apr 3, 2024 00:57:00
loxx.tv	✓ Success Traffic detected		5 records	Apr 12, 2024 14:56:54	Apr 3, 2024 00:42:05

Instant Messaging

Team	App
SecurityDemo.Net	Slack

Notification Targets

Name	Description	Type	Last Updated (UTC)
Aaron XDR Listener	Listener configured in XDR for webhooks	Check failures	Apr 12, 2024 18:40:15
SecurityDemoNet-Oort-Messages		Check failures	Apr 12, 2024 18:40:19
Securitydemo Slack		Check failures, Data collection	Apr 12, 2024 18:40:23

API clients

Name	Status	Client ID	Description	Last Updated (UTC)
Robins Toy Box API Client	✓ Enabled	xKwvt6q2wErXx5ZqWSlibCvWX41ZFX9		Mar 28, 2024 20:50:52
Aaron - API for XDR Dashboards	✓ Enabled	LHMtfeBUubrQVJ175zp3TOmNsYAlfSe		Mar 28, 2024 20:45:19

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

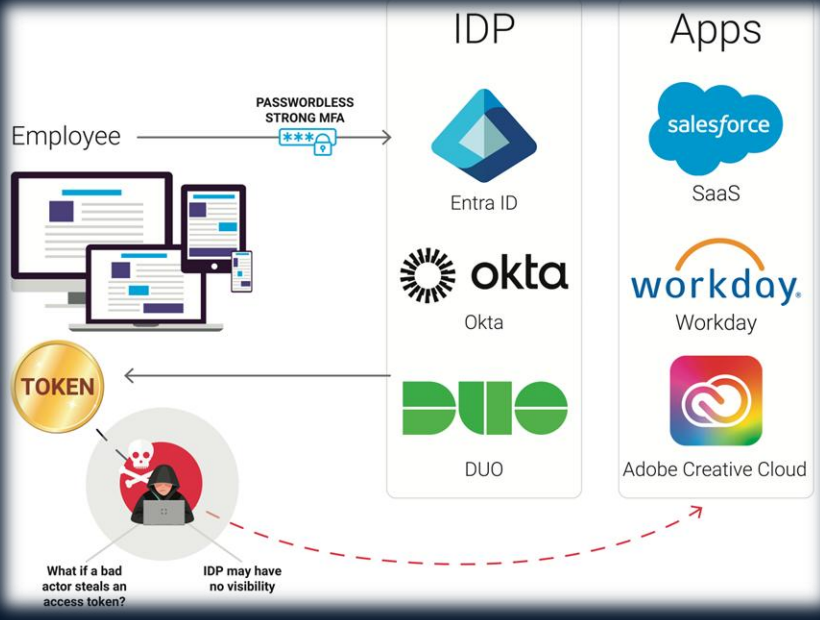


"I cannot believe how quickly we were able to find out about this attempted login from this unusual location"

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...

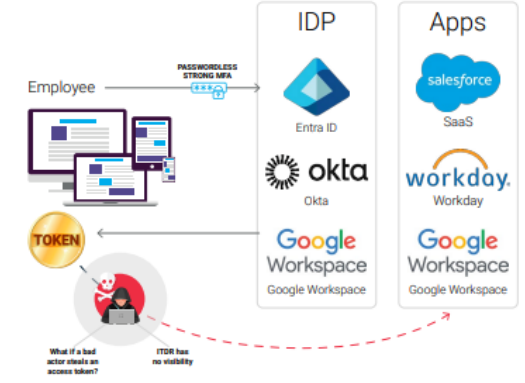


Strengthen your Identity Security with ConRes

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

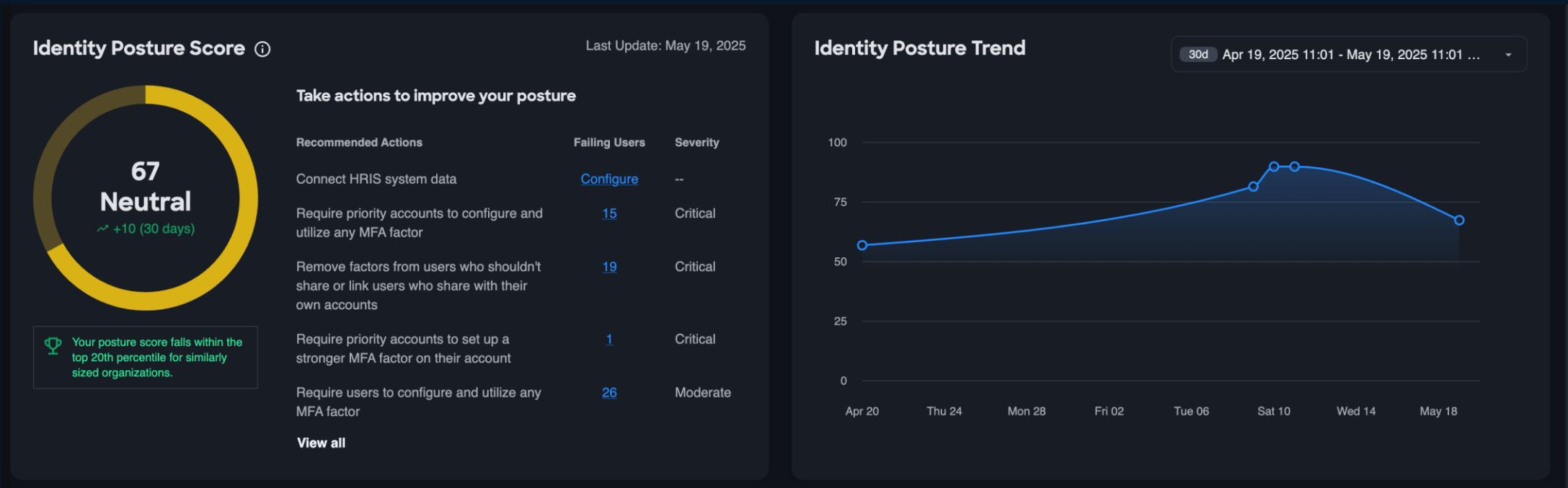
- 01 What is Cisco Identity Intelligence
- 02 Identity Security Posture
- 03 Monitoring Auth Factor Progression
- 04 Threat Detection & Response
- 05 User Trust Levels
- 06 Identity Security Assessments
- 07 Putting the “R” in ITDR
- 08 Call to Action

Proactive Security

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

Take actions to improve your posture

Recommended Actions	Failing Users	Severity
Connect HRIS system data	Configure	--
Require priority accounts to configure and utilize any MFA factor	11	Critical
Remove factors from users who shouldn't share or link users who share with their own accounts	23	Critical
Require priority accounts to configure and actively utilize stronger MFA factors	1	Critical
Require priority accounts to set up a stronger MFA factor on their account	1	Critical
Require users to configure and utilize any MFA factor	39	Moderate
Require users to set up a stronger MFA factor on their account	5	Moderate
Revoke access to applications users are not utilizing	1	Moderate
Update missing user types in your IDP	1	Moderate
Delete accounts that have never successfully signed in	10315	Low
Review and adjust Okta authentication policy settings	View check	Low
Clean up inactive external users	11	Low
Clean up inactive internal users	151	Low

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*)

Dashboard > No MFA Configured - Priority Accounts

🔍 Failing checks:No MFA Configured × NOT Status:(3 conditions) × AND (isA... <> Advanced × 🔗 ⬇️ ⬅️ ↻

15 users found Columns

User ↓	Checks ↑	# IPs ↑	# Logins ↑	Last Seen (UTC) ↑	MFA ↑	Providers	Status ↑	Tags ↑
Aaron Woland 🔗 loxx@loxx.tv	1	2	5	11 Days Ago May 9, 2025 19:35:21	×		Active	N/A
Assets Admin 🔗 assets@loxx.tv	2	0	N/A	A Year Ago Mar 27, 2024 14:24:12	×		Inactive	N/A
Chris Van der Made 🔗 cvdm@loxx.tv	2	0	N/A	A Year Ago Feb 21, 2024 14:52:24	×		Inactive	N/A
Darin Smith 🔗 darin@securitydemo.net	3	0	N/A	7 Months Ago Oct 22, 2024 14:44:22	×		Inactive	N/A
Employee One 🔗 employee1@loxx.tv	2	0	N/A	5 Months Ago Dec 13, 2024 20:14:45	×		Inactive	N/A
Hanna Jabbour 🔗 hanjabbo@securitydemo.net	3	0	N/A	A Year Ago Jan 25, 2024 11:55:45	×		Inactive	N/A
Jeff Groesbeck 🔗 jgroesbeck@loxx.tv	2	0	N/A	8 Months Ago Sep 10, 2024 18:38:36	×		Inactive	N/A
John Poole (johpoole) 🔗 johpoole@cisco.com	2	0	N/A	A Year Ago Jun 25, 2024 17:40:15	×		Inactive	N/A

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.

Search by title or description

Request check Run checks now

All Checks Last run: May 20, 2025 19

Check	# Failing	# Excluded	Report Channels
1% Never Logged In Critical End Users - Compliance, Identity Pos...	10293 → No change since last w... ↗ 16... increase since la...	0	+ Add
72% Applications with Expired Secrets Low Identity Providers - Identity Posture Insig...	N/A	N/A	+ Add
98% Inactive Users Moderate End Users - Compliance, Identity P...	147 ↘ 0... decrease since last ... ↗ 21... increase since last ...	0	+ Add
99% User Has Directly Assigned Appli... Low End Users - Compliance, Identity Postur...	60 → No change since last week → No change since last month	0	+ Add
99% No MFA Configured Critical End Users - Compliance, Identity Pos...	40 ↘ 2.4... decrease since last w... ↗ 152... increase since last ...	0	+ Add
99% User Password Expiration Failure Moderate End Users - Identity Posture Insight	22 → No change since last week → No change since last month	0	+ Add
99% Users Sharing Authenticators Critical End Users - Compliance, Identity Pos...	19 → No change since last week ↗ 20... increase since last ...	0	+ Add
99% Inactive Guest Users Critical End Users - Compliance, Identity Pos...	7 ↘ 12... decrease since last w... ↘ 12... decrease since last m...	0	+ Add
99% No Strong MFA Configured Moderate End Users - Compliance, Identity P...	5 → No change since last week ↗ 158... increase since last m...	0	+ Add

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.

Compatibility All

- Duo 31
- Google Workspace 20
- Microsoft Entra ID 46
- Okta 47
- SCIM 1
- Slack 8

Compliance All

- Full 47
- Partial 17

Severity All

- Critical 23
- Low 15
- Moderate 26

Topic All

- Compliance 32
- Devices 2
- Identity Posture Insight 28
- Identity Threat Insight 34
- Non-Human Accounts 8

Frameworks All

- End Users 61
- Identity Providers 3

All Checks

Check	# Failing	# Excluded	Report Channel
Never Logged In (Critical) End Users - Compliance, Identity Pos... 1% 10293 → No change since last w... ↑ 16... increase since la...	10293	0	+ Add
Applications with Expired Secrets (Low) Identity Providers - Identity Posture Insig... 72% N/A	N/A	N/A	+ Add
Inactive Users (Moderate) End Users - Compliance, Identity P... 98% 147 ↓ 0... decrease since last ... ↑ 21... increase since last ...	147	0	+ Add
User Has Directly Assigned Appli... (Low) End Users - Compliance, Identity Postur... 99% 60 → No change since last week → No change since last month	60	0	+ Add
No MFA Configured (Critical) End Users - Compliance, Identity Pos... 99% 40 ↓ 2.4... decrease since last w... ↑ 152... increase since last ...	40	0	+ Add
User Password Expiration Failure (Moderate) End Users - Identity Posture Insight 99% 22 → No change since last week → No change since last month	22	0	+ Add
Users Sharing Authenticators (Critical) End Users - Compliance, Identity Pos... 99% 19 → No change since last week ↑ 20... increase since last ...	19	0	+ Add
Inactive Guest Users (Critical) End Users - Compliance, Identity Pos... 99% 7 ↓ 12... decrease since last w... ↓ 12... decrease since last m...	7	0	+ Add
No Strong MFA Configured (Moderate) End Users - Compliance, Identity P... 99% 5 → No change since last week ↑ 158... increase since last m...	5	0	+ Add

Frameworks

- CIS 5.3 3
- CIS 5.4 6
- CIS 5.5 1
- CIS 5.6 4
- CIS 6.3 4
- CIS 6.4 4
- CIS 6.5 4
- Cis 854 1
- Cis 862 1
- Cis 881 1
- CMMC AC.2.010 2
- CMMC IA.3.083 2
- CMMC IA.3.084 2
- CMMC SC.3.187 2
- Iso 27001 A 1241 1
- Iso 27001 A 923 1
- Mitre ATT&CK T1078 5
- Mitre ATT&CK T1078.004 3
- Mitre ATT&CK T1087.004 1
- Mitre ATT&CK T1098.002 2
- Mitre ATT&CK T1098.003 2
- Mitre ATT&CK 1



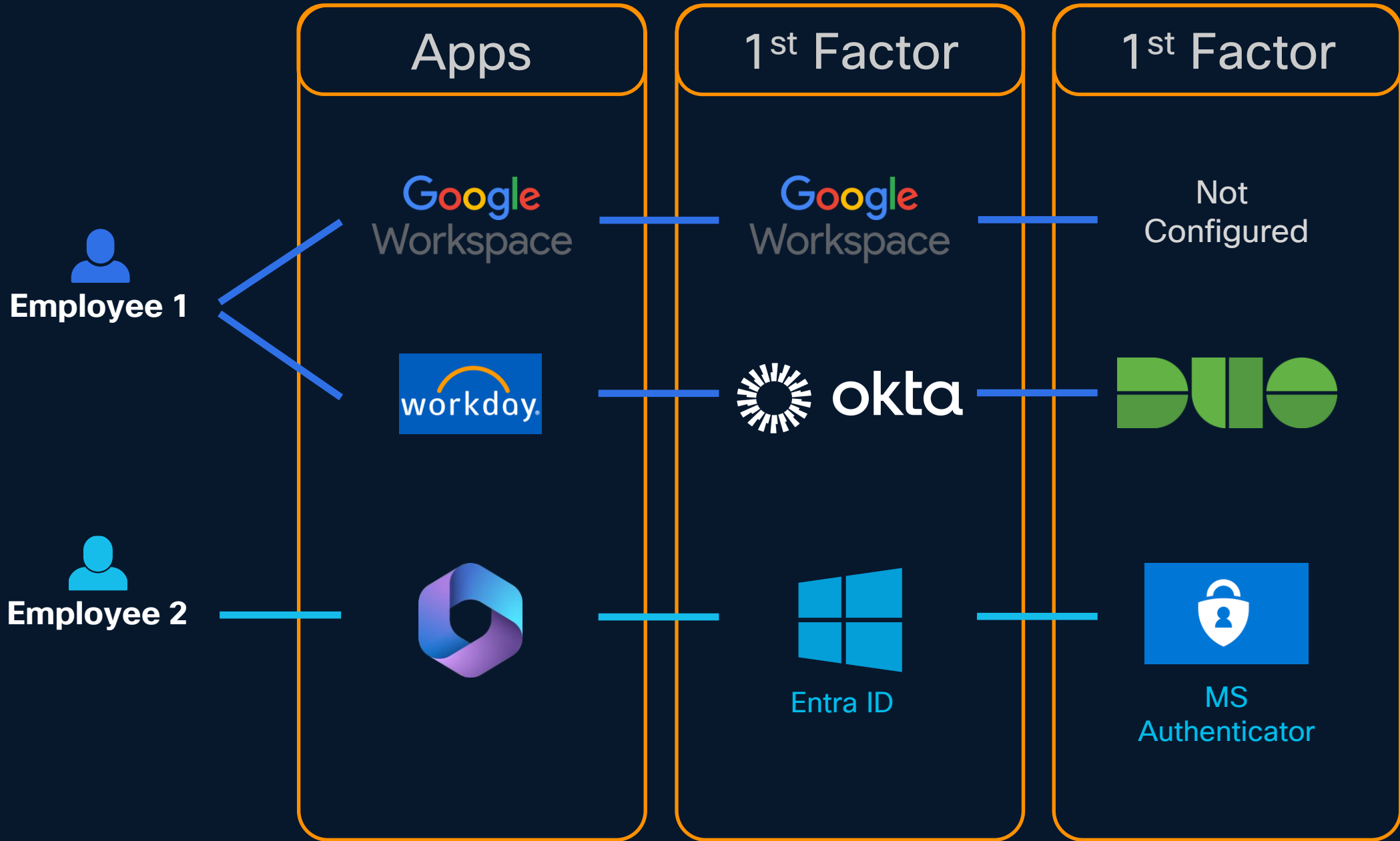
But my user **does** have MFA
configured. Look! You can see that
Duo MFA exists

- 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?**



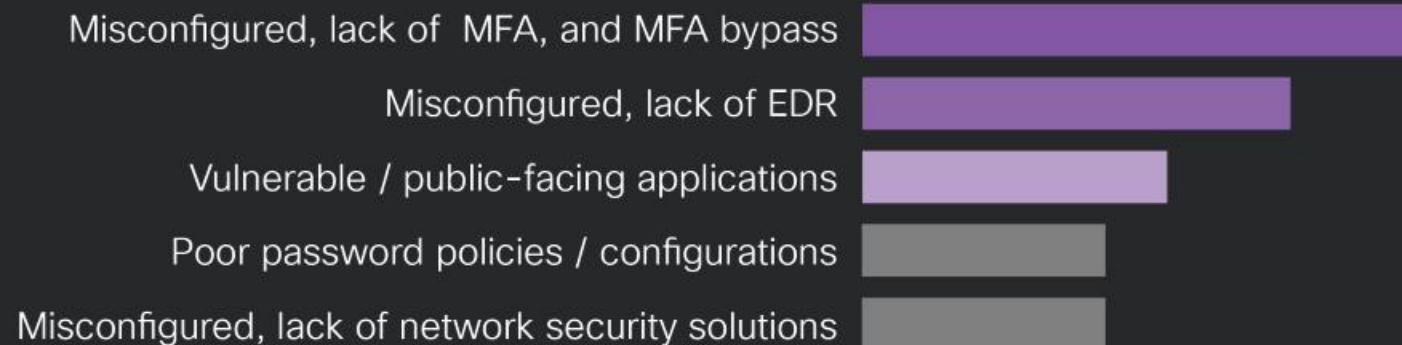
We see
Environments
Like This
All the Time

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



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

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

Identity Intelligence No MFA Configured (Last reported: Less than 1 day ago)
secops1@loxx.tv

Automated notifications for this check are not configured. Please configure notifications if you wish to receive automated reports about users failing this check.

23 failing users

User	First Reported (UTC) ↑	Last Reported (UTC) ↑	Us
zank@securitydemo.net	May 9, 2025 15:22:50	May 27, 2025 19:07:45	Nc
wallyb@securitydemo.net	May 9, 2025 15:22:14	May 27, 2025 19:07:06	Nc
yasghar@securitydemo.net	May 9, 2025 15:22:14	May 27, 2025 19:07:06	Nc
ykarmy@loxx.tv	May 10, 2025 19:04:37	May 27, 2025 19:07:06	Nc
secops1@loxx.tv	May 10, 2025 19:04:37	May 27, 2025 19:07:06	Nc
secops2@loxx.tv	May 10, 2025 19:04:37	May 27, 2025 19:07:06	Nc
shishanb@securitydemo.net	May 9, 2025 15:22:14	May 27, 2025 19:07:06	Nc
sokovalc@securitydemo.net	May 9, 2025 15:22:14	May 27, 2025 19:07:06	Nc
ssaklikar@securitydemo.net	May 9, 2025 15:22:14	May 27, 2025 19:07:06	Nc
sso@loxx.tv	May 10, 2025 19:04:37	May 27, 2025 19:07:06	Nc

Enforce and enable MFA at the failing source whenever possible. Even if the failing source is not considered the primary IdP or MFA provider, it is important to have some form of MFA configured on all of a user's available sources because misconfigurations can unintentionally allow a user to sign-in to a resource through a different identity source where MFA is not configured, making the account susceptible to compromise.

If needed, adjust the grace period in the Custom Check Settings to align with your organization's account creation/onboarding process to increase the accuracy and actionability of the check results.

There may be accounts that have mitigating controls or a valid reason to be exempt from MFA. We recommend categorizing these accounts in an external system for easy detection and temporary excluding them from this check to resolve the failure. Use temporary exclusions to periodically resurface these accounts so their exemption status can be re-assessed and updated as needed.

Providers failing check GSuite

User Trust Level UNKNOWN

Providers failing check GSuite

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

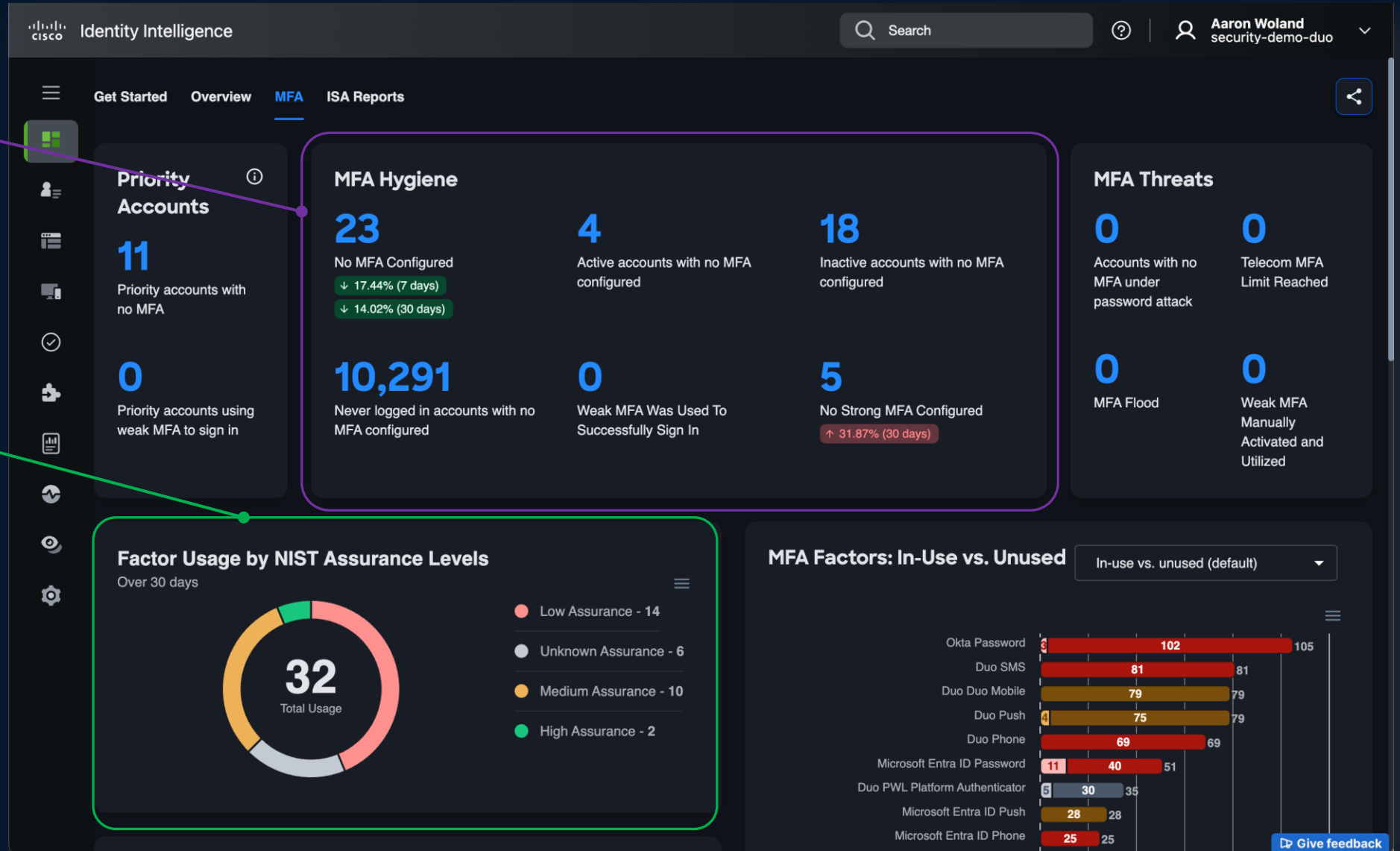
Leverage the MFA Dashboard to Keep Up

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.

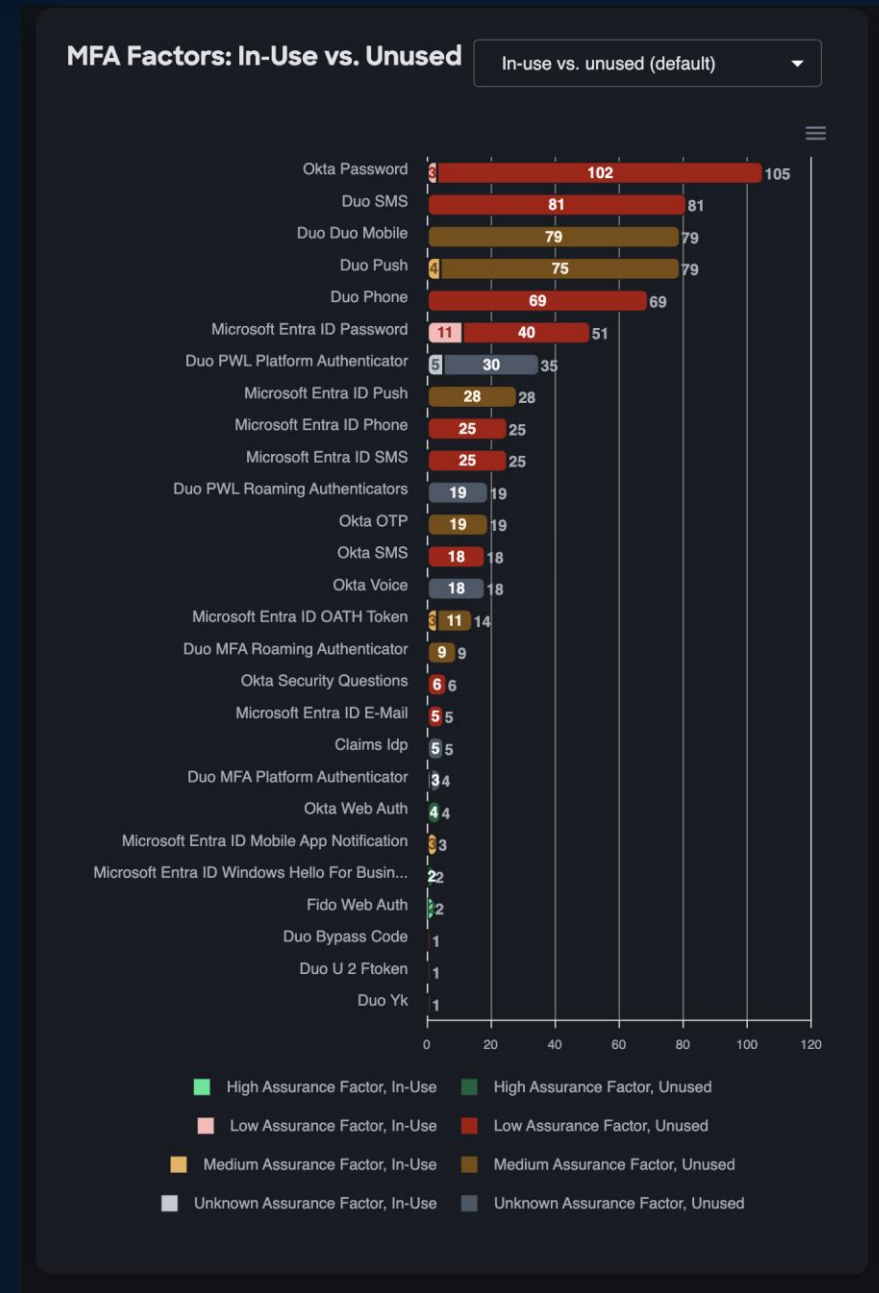


“I am certain that we removed all SMS & are only using AAL3 factors now”

- Anonymous CISO that CII proved wrong

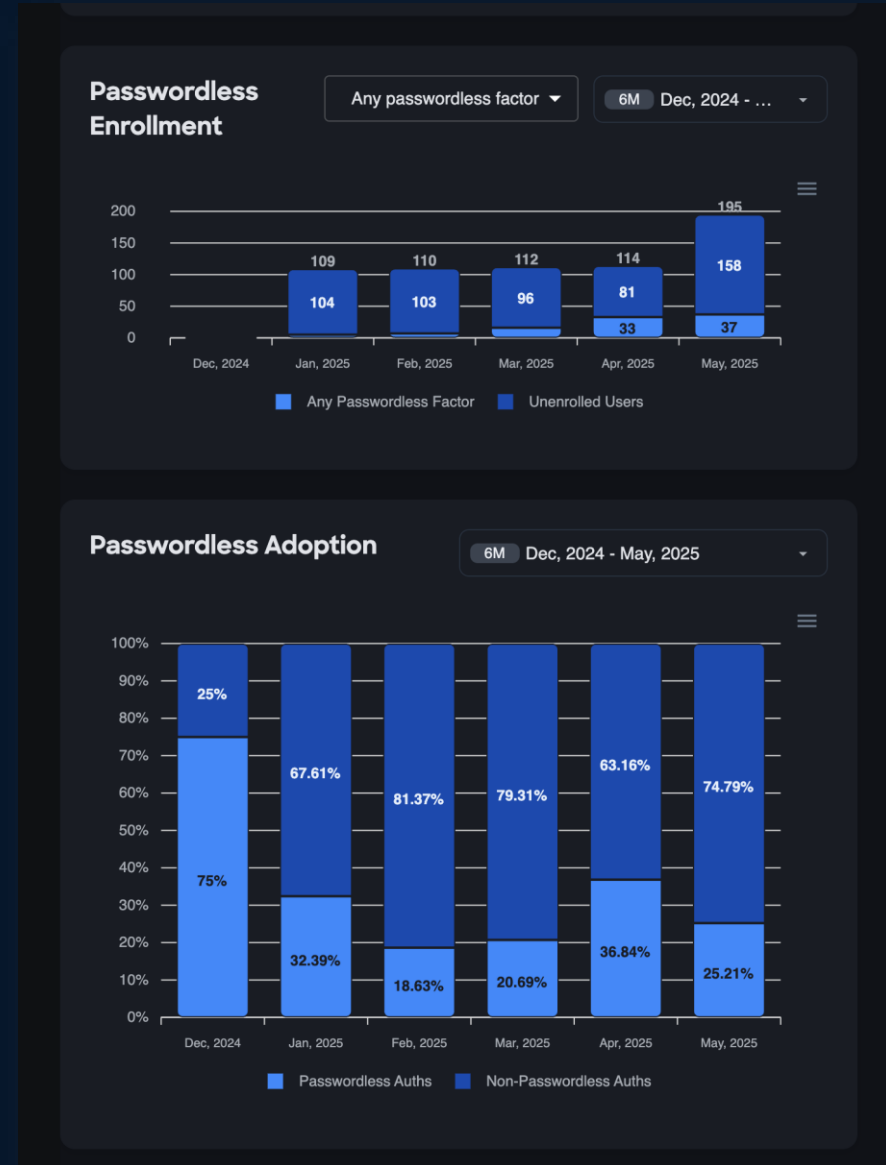
“We only use strong Authentication Factors!”

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



How is our Passwordless Rollout Going?

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

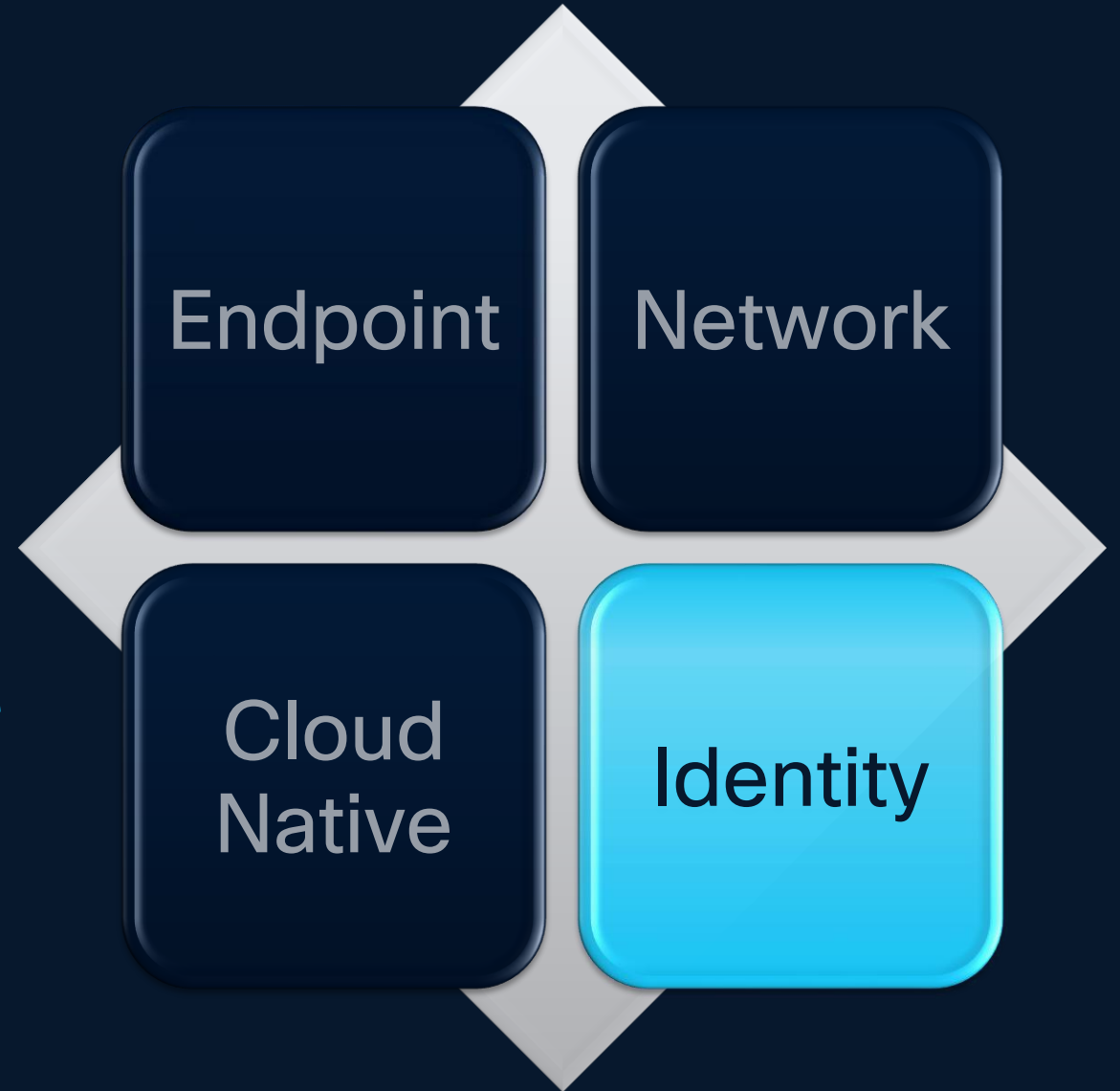
Prevention is not enough!

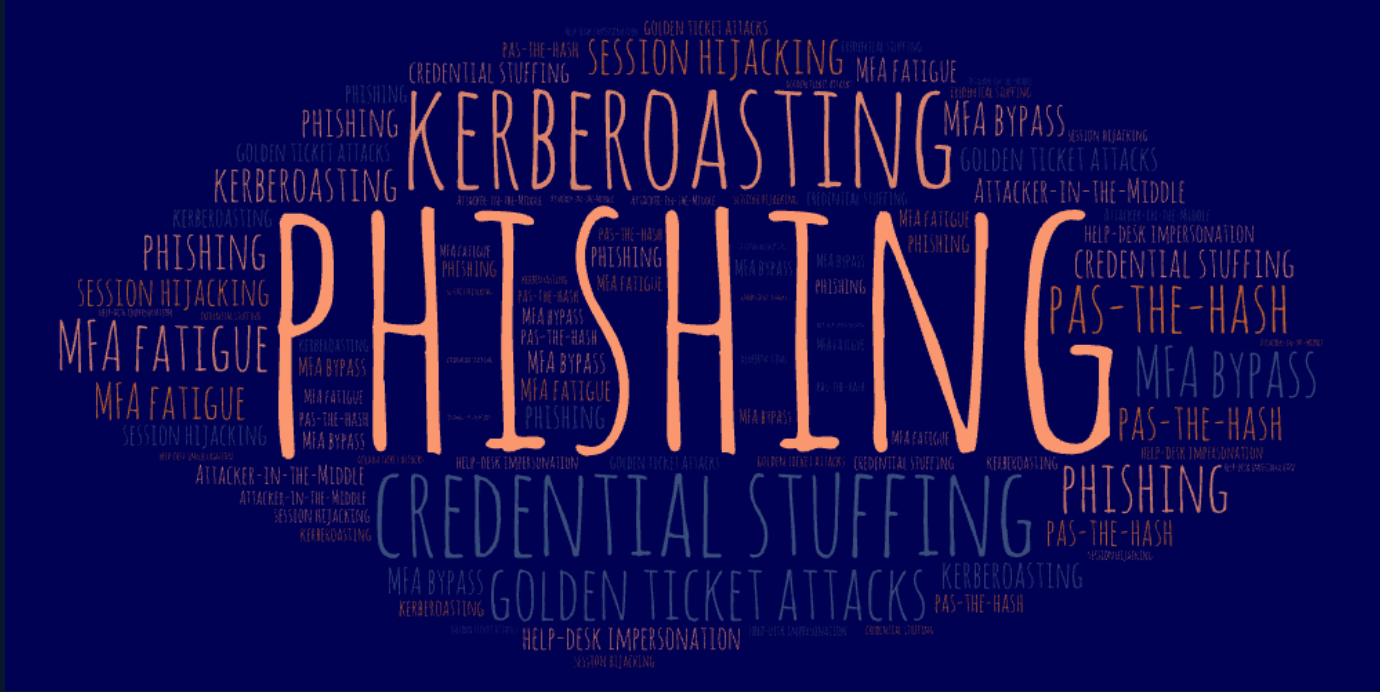
Endpoint Detection & Response

Network Detection & Response

Cloud Native Detection & Response

Identity Threat Detection & Response







Identity-based threats

Identity attacks dominated the threat landscape in 2024

Identity was a common through line in 2024 across much of the data we looked at for this report. From initial access vectors to operational techniques further down the attack chain, threat actors relied heavily on identity-based attacks to power their operations. Adversaries are increasingly opting to compromise networks and accounts by simply logging in, rather than using more complex methods like exploiting vulnerabilities or deploying malware.

2024
YEAR IN REVIEW

Attackers expect you to have MFA

Brute-force or password spray



MFA bypass

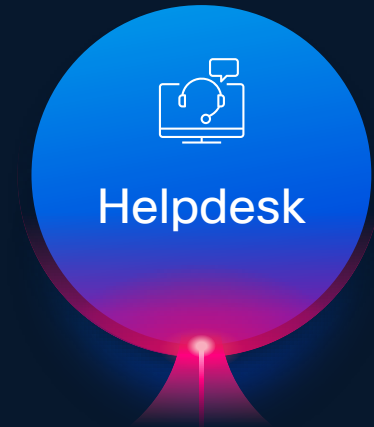


Physical access to device



Fallback to less secure MFA method

Stolen session cookies



Deepfake social engineering at help desk

Session Hijacking Example



Actual login page

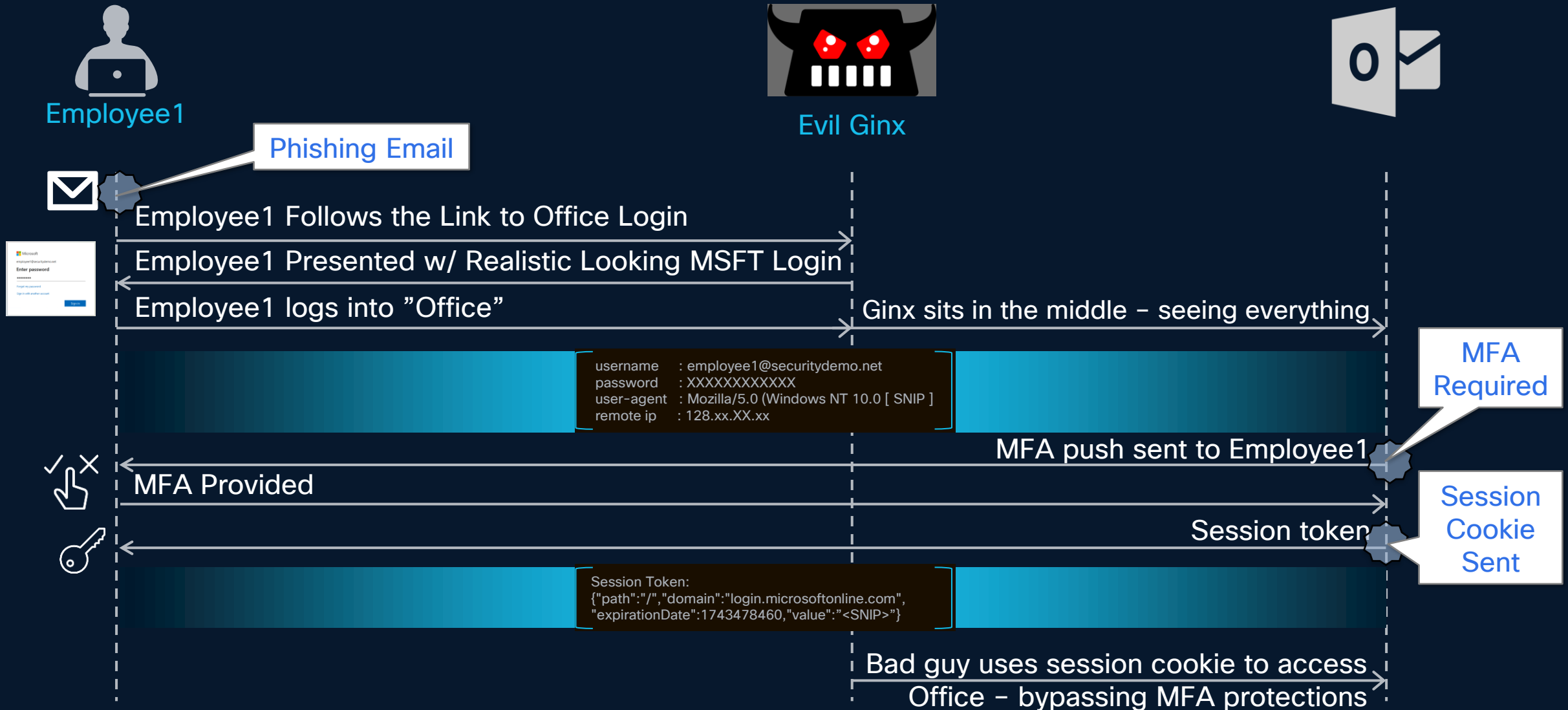
Hacker controlled proxy

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 | sessions
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

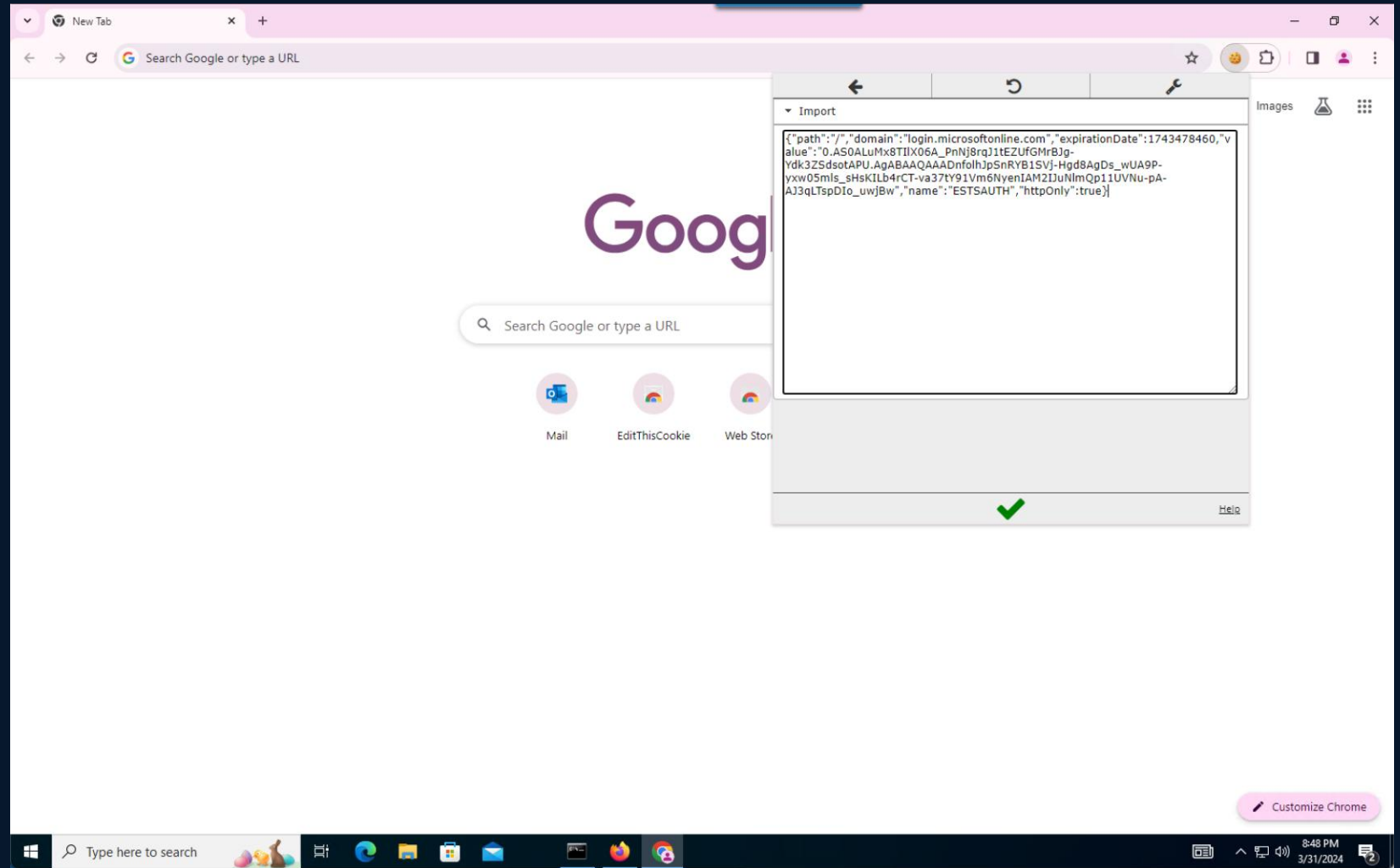
Getting started
: lures
: sessions

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

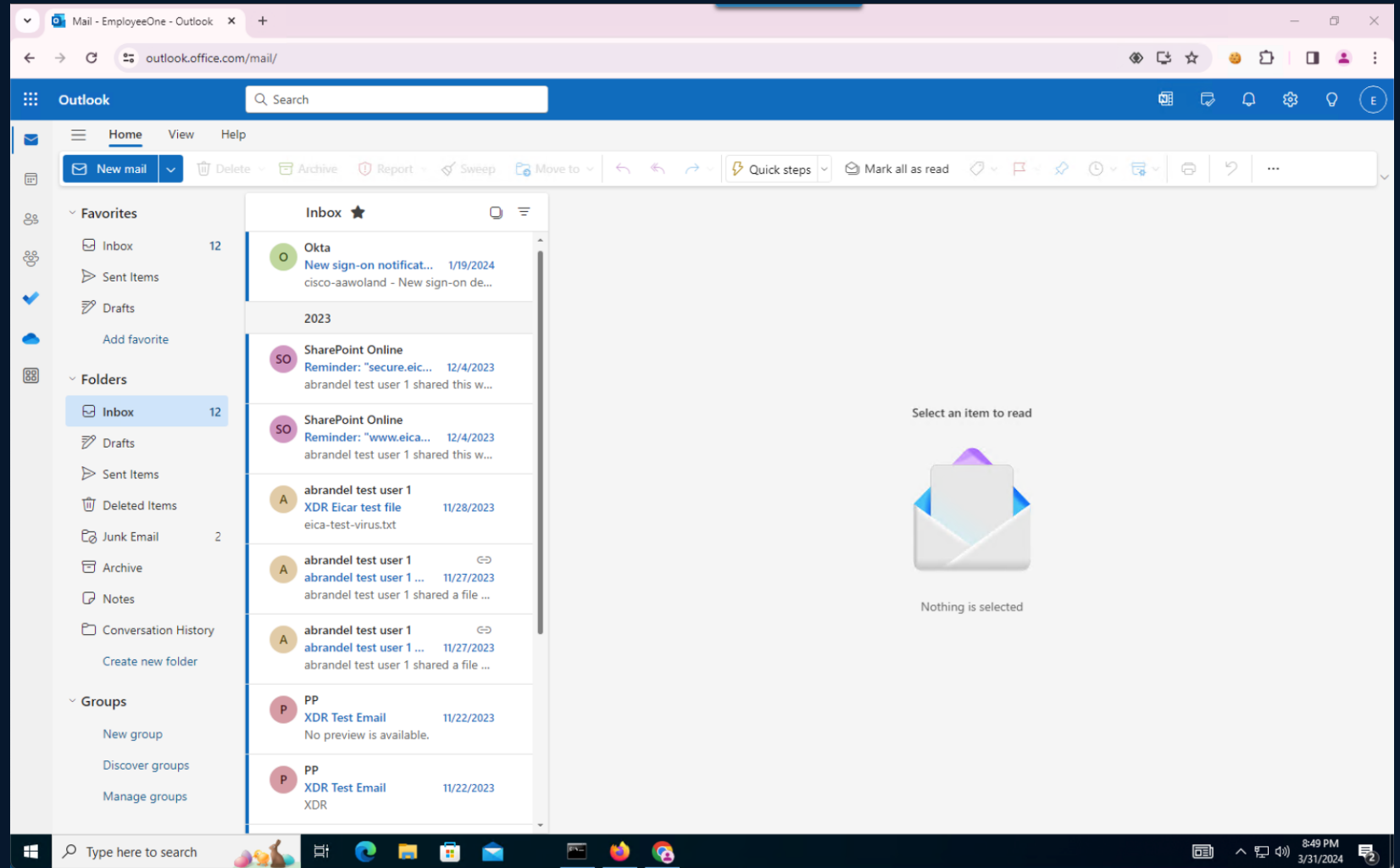
[03:09:25] [war] [o365] request to hidden phishlet: https://login.securitydemo.net/spRqQIIF (Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0) [128.107.78.71]
: phishlets
: phishlets unhide o365
[03:09:49] [inf] phishlet 'o365' is now reachable and visible from the outside
: Redirectors
[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
: sessions
[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 DeviceID: 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 DeviceID: 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 DeviceID: 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 DeviceID: VendorUID: AppPkgID: ee.delfi.delfi) [18.170.98.205]
: sessions

id | phishlet | username | password | tokens | remote ip | time
---|---|---|---|---|---|---
1 | o365 | employee1@... | 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

Identity Intelligence | Search | aawoland@cisco...
Checks > **Compromised Session** [Moderate]

Details

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials.

To identify such sessions, Identity Intelligence alerts on successful login from 2 or more IP-Device pairs for a single session ID.

Recommended Actions

First, make sure that 'Enforce device binding for creating sessions' parameter is Enabled.
Second, contact the end-user to verify the origin of the actions.

Last Report Update
May 28, 2025 04:33:14 UTC

Topics
Identity Threat Insight

Frameworks
Mitre ATT&CK T1539, Mitre ATT&CK T1185, Mitre ATT&CK T1563

Compatibility | Last data collection
Okta | Microsoft Entra ID

Tags
+ Add tag

Additional Resources

- Learn More - Detecting Session Hijacking
- Enforce device binding for creating sessions
- Steal Web Session Cookie, Technique T1539

+ 3 more

Check Settings
Custom Detection Settings
Notification Settings

Failing Users

1 No change (7 days)
No change (30 days)
0.4% of Users failing

Failing Users Per Integration

Demo Okta - 1
100.00% of Failing Users

Failing Users Per Type

Internal - 1
100.00% of Failing Users

Excluded Users 0 | **Unprotected users failing** 0

Automated notifications for this check are not configured.
Please configure notifications if you wish to receive automated reports about users failing this check.

1 failing user | View users | Download List

User	First Reported (UTC)	Last Reported (UTC)	Admin Notified
fellmeth.emery@simubiz.com	May 28, 2025 04:23:13	May 28, 2025 04:33:02	Not notified

© 2025 Identity Intelligence
This environment reloads hourly

Privacy Policy | Terms of Use | Documentation | Status | SOC2 Report

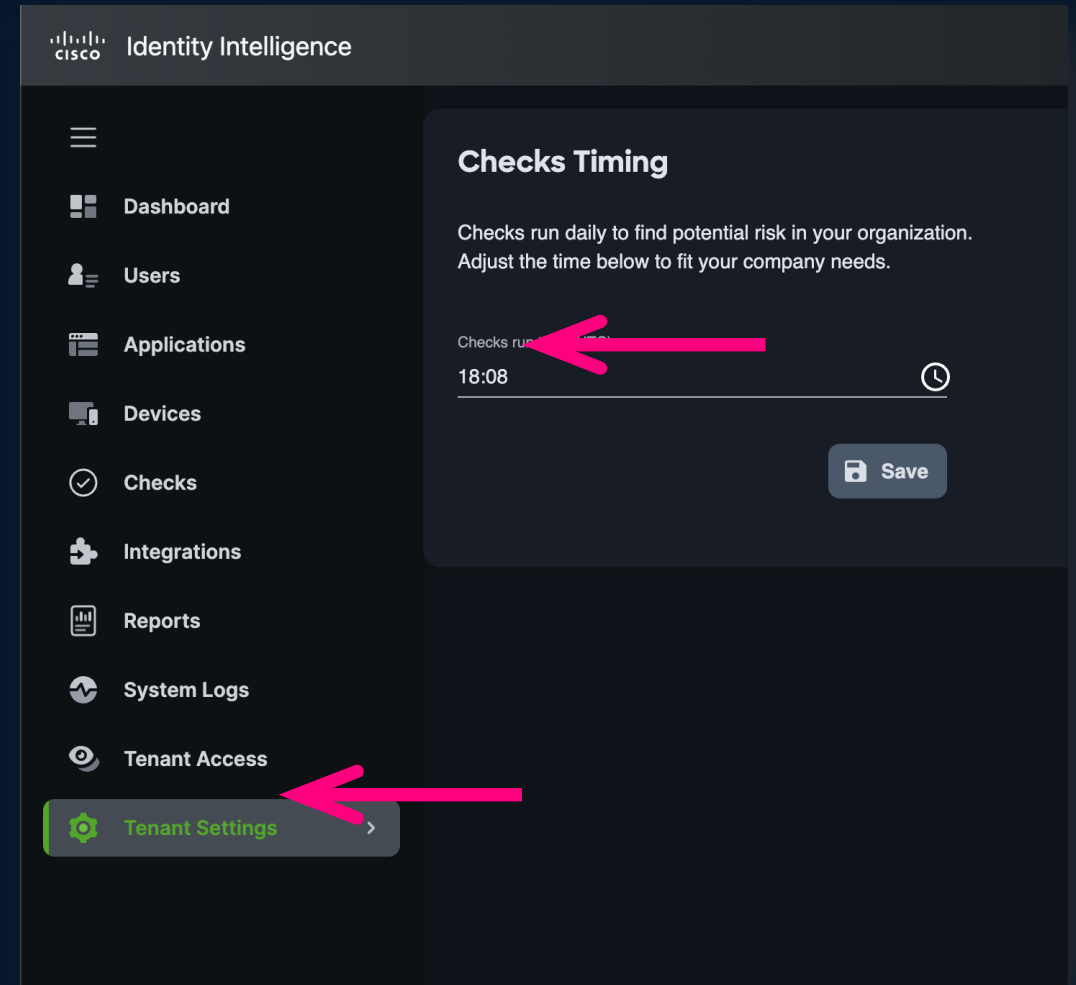
*“But... CII Takes
too Long to Detect”*

- Rando person #3

Threat Discovery Mode (TDM) - High

Technical Nugget

- By default, CII runs its 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-Requirements
 - 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

Trust Level ⓘ
Neutral

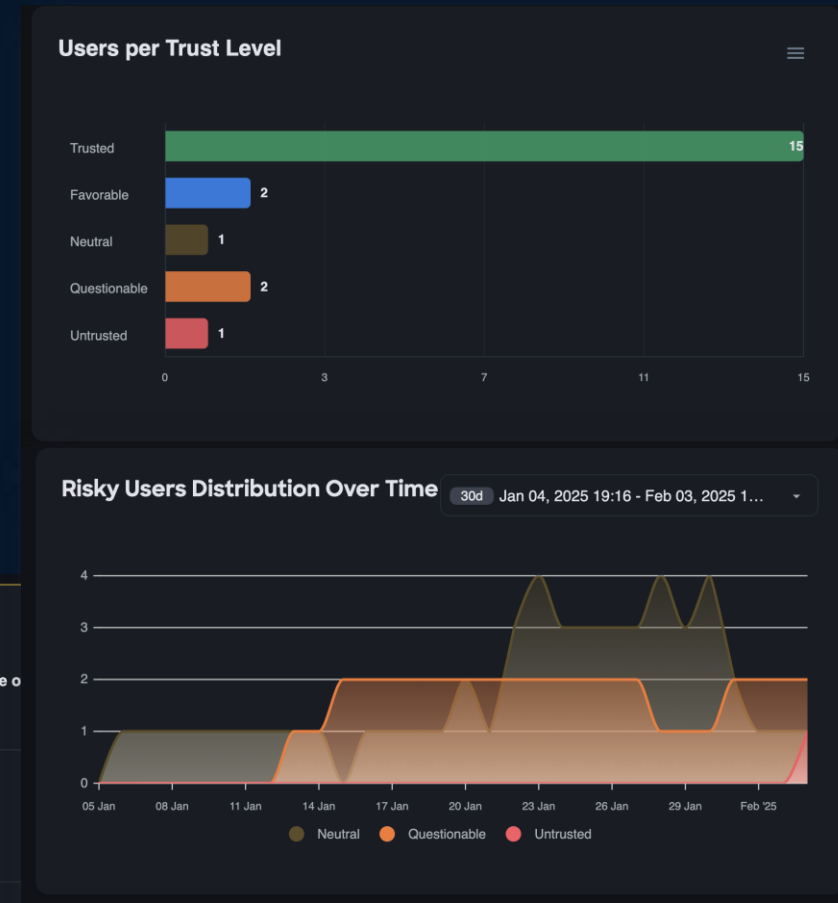
The level changed from Unknown to Neutral on Jan 30, 2025 23:58:24 UTC because of New priority account signed in

^ Additional details

Failing Checks:
[Access From Dormant Account](#)

^ 4 contributing events [See in context](#)

Date (UTC)	Source	Event	Result	
Jan 30, 2025 17:50:42	🟢	authentication	Success	View event details
Jan 30, 2025 17:50:12	🟢	authentication	Success	View event details
Jan 30, 2025 17:49:39	🟢	enrollment	Success	View event details
Jan 30, 2025 17:49:10	🟢	enrollment	Success	View event details



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.

The screenshot displays the Cisco Secure Access management interface. The main section shows a table of users with columns for Name, Email, Source, Directory, Trust Level, and Connected(VP). The Trust Level column is highlighted with a green box, showing values like 'Trusted', 'Neutral', and 'Unknown'. A detailed view on the right, also highlighted with a green box, shows the 'Trust Level' for a user, indicating it is 'Neutral' and listing factors such as 'SpecialAccount', 'PasswordRecentlyChanged', 'WeakMfaUsed', and 'RiskFromAzure'.

Name	Email	Source	Directory	Trust Level	Connected(VP)
aalto.h 1	aalto.h@simubiz.com	azure	CII INT AZURE	Trusted	0
aalto.helmig 2	aalto.helmig@simubiz.com	azure	CII INT AZURE	Neutral	0
aalto.sekine 3	aalto.sekine@simubiz.com	azure	CII INT AZURE	Neutral	0
adamchick.thome 4	adamchick.thome@simubiz.com	azure	CII INT AZURE	Unknown	0
alice 5	alice@simubiz.com	azure	CII INT AZURE	Unknown	0
altgilbers.yagi 6	altgilbers.yagi@simubiz.com	azure	CII INT AZURE	Unknown	0
amodio.plater 7	amodio.plater@simubiz.com	azure	CII INT AZURE	Trusted	0
amodio.tall 8	amodio.tall@simubiz.com	azure	CII INT AZURE	Trusted	0
anil.hauwa 9	anil.hauwa@simubiz.com	azure	CII INT AZURE	Trusted	0
ansah.rottenberg 10	ansah.rottenberg@simubiz.com	azure	CII INT AZURE	Neutral	0

User Details: Trust Level
Trust Level: Neutral
Last updated: Jan 14 2025 11:05:30 AM UTC
The level changed to **Neutral** because of the following factors:

- SpecialAccount
- PasswordRecentlyChanged
- WeakMfaUsed
 - 1. is-weak-mfa-used
- RiskFromAzure
 - 1. risky-user-signin-events

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

User Trust Profiles
User trust profiles adaptively modify authentication and security based on trust levels—untrusted, neutral, trusted—incorporated into access rules, powered by Cisco Identity Intelligence. [Help](#)

Trust levels

1 profile

Search 1 profile

Profile name	Assigned to	Used in
System-provided Default for private access policy rules	All private resources	0 rules

Trust level	Authentication controls	Security Controls
Trusted	Single Sign On	IPS: Connectivity Over Security
Neutral	Reauthenticate Every 24hrs	IPS: Security Over Connectivity Geolocation: US only
Untrusted	Block	-

Trusted
Settings for Trusted user trust level

Authentication controls
Type of authentication required for user to access the resource.

Authentication Options

Single Sign On

Single Sign On (SSO)

Step up authentication

Duo Push (Most secure)

Block

IPS Profile Enabled
IPS Profile enabled based on User Trust Level

IPS Profiles

Connectivity Over Security

Geolocation Enabled
Access will be allowed depending on Geolocation

Cancel Save

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)

Checks > User Trust Level Alert

User Trust Level Alert 🔴 Critical

Details

Detects the riskiest users in your organization, based on their User Trust Level, that should be prioritized for investigation. User Trust Levels evaluate the likelihood that a given account's actions pose a risk to a system or organization, by combining multiple data points - such as account metadata, behavioral patterns, device usage, location, and historical activity - to assign a user's Trust Level.

The Trust Level allows you to quickly and easily identify these concerning accounts so that you can investigate with urgency and remediate the situation as quickly as possible, reducing the attack timeframe or possibly preventing an attacker from successfully compromising a targeted account.

Recommended Actions

Prioritize the investigation of the user(s) and their associated risky events to confirm that the account is not compromised. If the user is compromised, consider killing all sessions, resetting the user's password and factors, and/or adding the user to a quarantine group with limited access in your identity provider.

Last Report Update
May 28, 2025 04:33:14 UTC

Topics
Identity Threat Insight

Compatibility Last data collection

Salesforce Google Workspace
Duo Auth0 AWS
Workday Webex CI HRIS
Microsoft Entra ID Okta
Slack GitHub
Cisco Identity Services Engine (ISE)
SCIM Snowflake Jamf

Tags
[+ Add tag](#)

Additional Resources
[User Trust Level](#)

Check Settings

- ⚙️ Custom Detection Settings
- 📧 Notification Settings

Failing Users

3 No change (7 days)
No change (30 days)

1.2% of Users failing

Excluded Users **0**

Unprotected users failing **0**

Automated notifications for this check are not configured. Please configure notifications if you wish to receive alerts.

3 failing users

User	First Report
ayo.ganin@simubiz.com	May 28, 2025
cramblit.mitra@simubiz.com	May 28, 2025

Custom Detection Settings

Include Questionable Trust Level users

[↺ Restore default](#) [💾 Save changes](#)

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

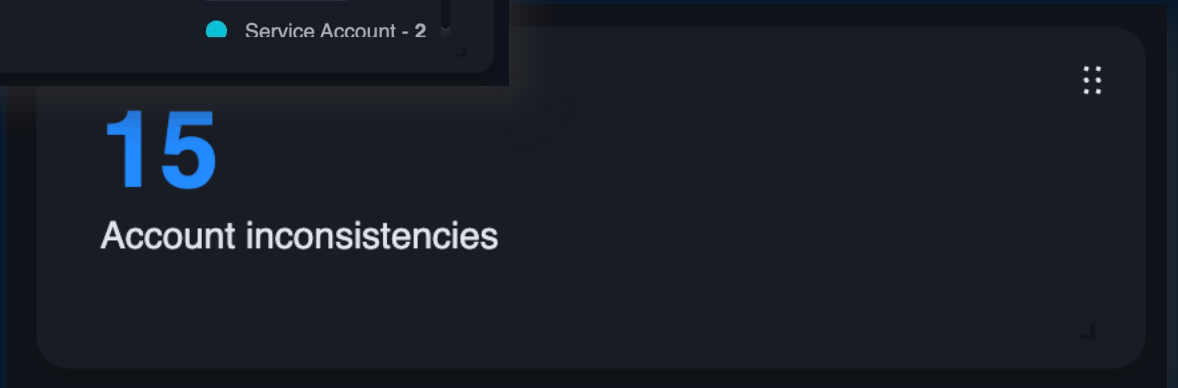
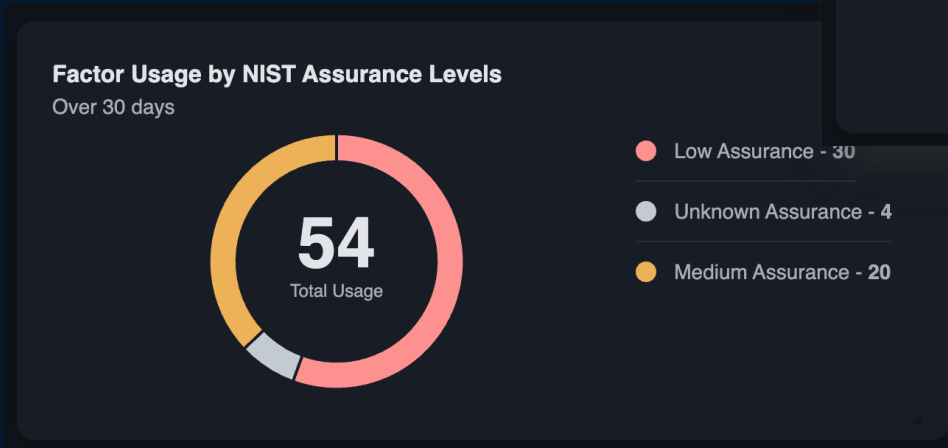
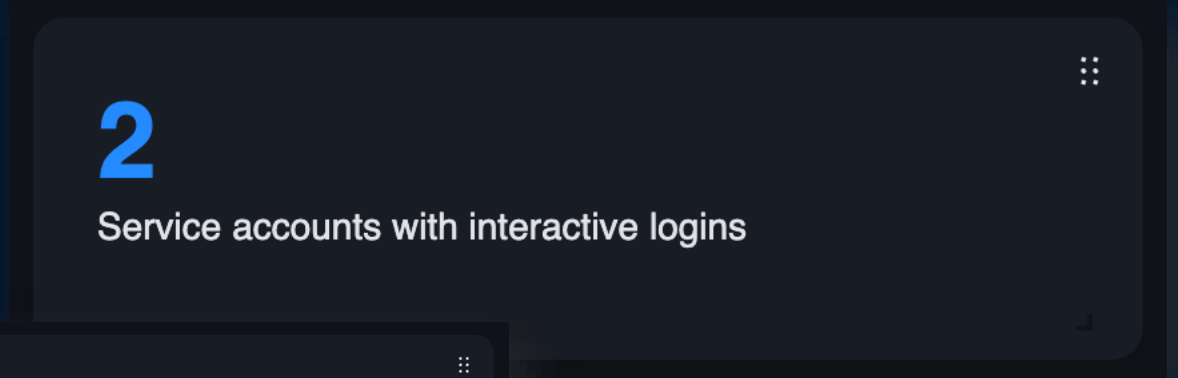
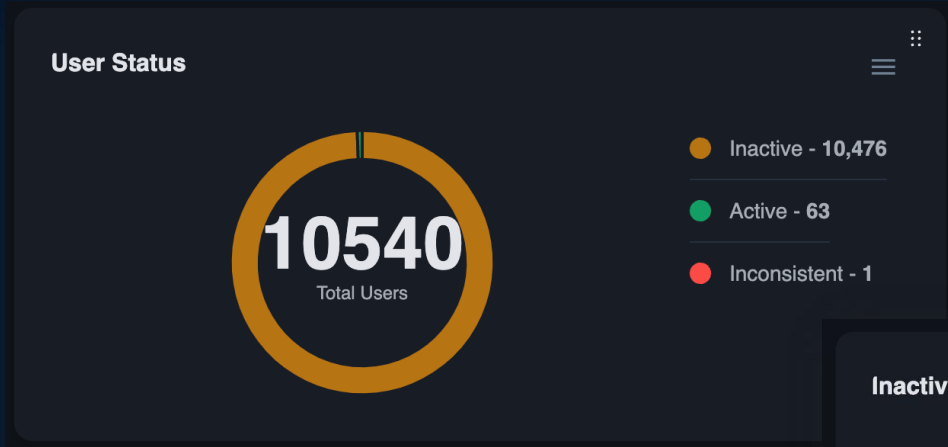
Identity Security Assessment

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

NOT Status:(3 conditions) X Aaron <> Advanced X

2 users found

User	Checks	# IPs	# Logins	Last Seen (UTC)	Last IP Address	Last Location	MFA	Providers	Status
Aaron Woland aawoland	⊘	0	N/A	A Day Ago Apr 23, 2024 15:14:37	N/A	N/A	✓	🔄	Inconsistent
Aaron Woland aawoland@cisco.com	✓	7	23	A Day Ago Apr 23, 2024 15:14:37	N/A	N/A	✓	🔄 ⚙️ 🌐	Active

Users > aawoland

Aaron Woland
aawoland Inconsistent

Overview Activity Networks Devices Applications Groups Actions

Users aawoland and several others have the same user name. Do you want to link them?

Summary

External, Unauthorized

No checks run against this user. They are outside the configured protected population.

Actions menu:

- + Open ticket
- Refresh User Data
- Link user

Users > aawoland@cisco.com

Aaron Woland
aawoland@cisco.com Active

Overview Activity Networks Devices Applications Checks Actions

Users aawoland@cisco.com and several others have the same user name. Do you want to link them?

Summary

Unclassified, Active

Attempted Logins: 30 (All Attempts)

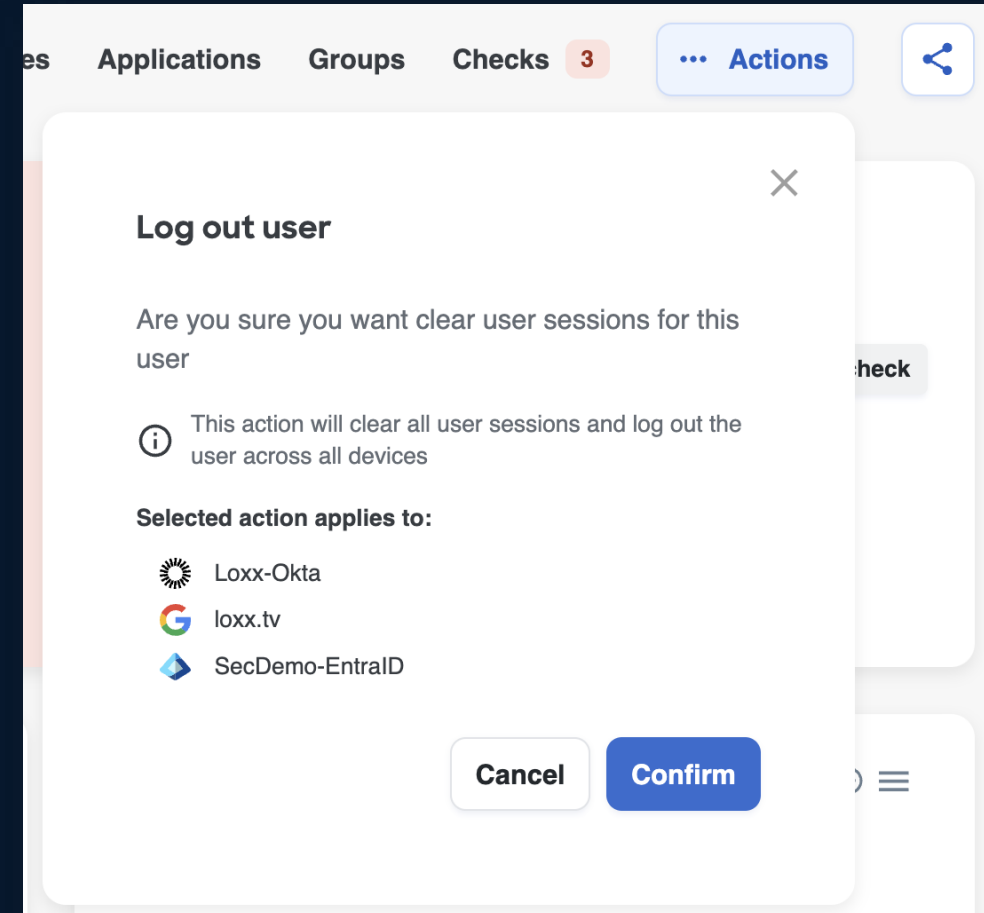
Records per day: 5

Actions menu:

- + Open ticket
- Reset MFA
- Log out user
- Quarantine
- Send push verification
- Refresh User Data
- Link user

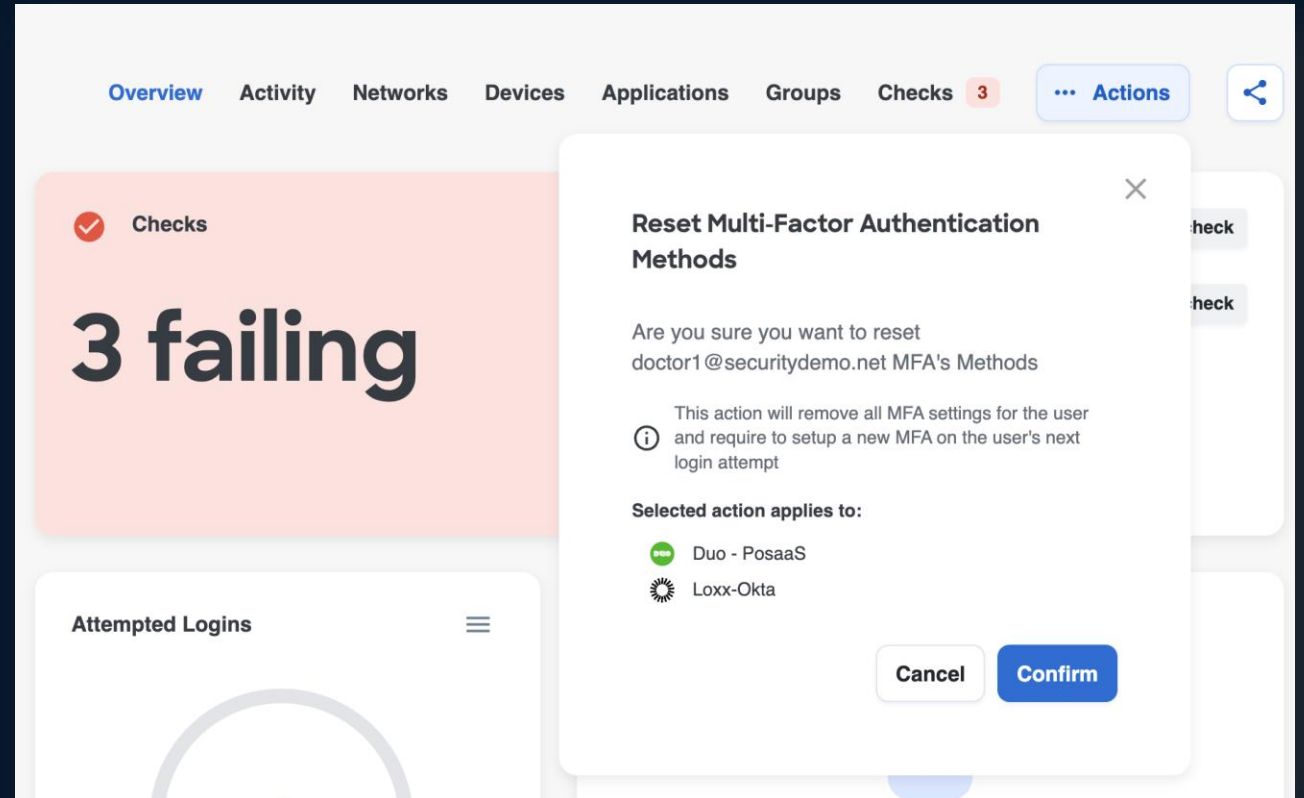
Log Out User

- 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



Identity Intelligence

Users > doctor1@securitydemo.net

doctor1
doctor1@securitydemo.net Inactive

Overview Activity Networks Devices Applications Groups Checks 3 Actions

3 failing

- Reset MFA
- Log out user
- Send push verification
- Refresh User Data
- Link user
- Exclude from

Authentication Factors

Factor	Assurance Level	Status	# Changes	Usage Count
Duo Mobile Duo - PosaaS DPUCY3HKA1NXUDX58SYD__mobile_otp	Medium	ACTIVE	0	N/A
Duo Mobile Duo - PosaaS DPPQBIVCKIUAGX7UZ1S__mobile_otp	Medium	ACTIVE	0	N/A
Push Duo - PosaaS DPUCY3HKA1NXUDX58SYD__push	Medium	ACTIVE	0	N/A
Push Duo - PosaaS DPPQBIVCKIUAGX7UZ1S__push	Medium	ACTIVE	0	N/A
Call Weak Duo - PosaaS DPUCY3HKA1NXUDX58SYD__phone	Low	ACTIVE	0	N/A

Overview Activity Networks Devices Applications Groups Checks 3 Actions

3 failing

Reset Multi-Factor Authentication Methods

Are you sure you want to reset doctor1@securitydemo.net MFA's Methods

This action will remove all MFA settings for the user and require to setup a new MFA on the user's next login attempt

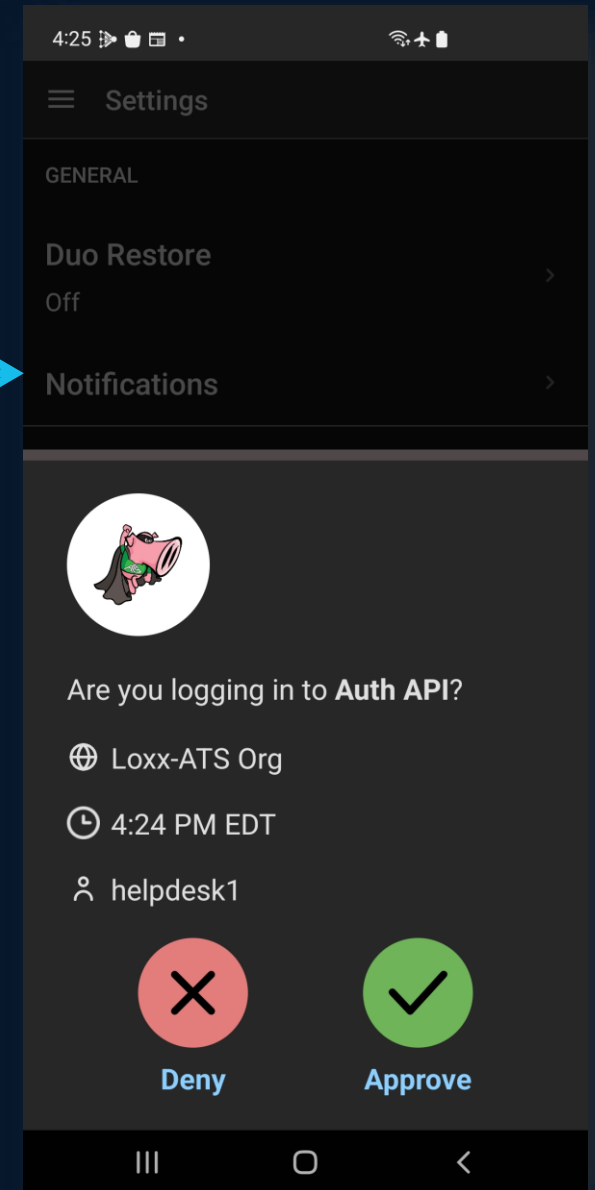
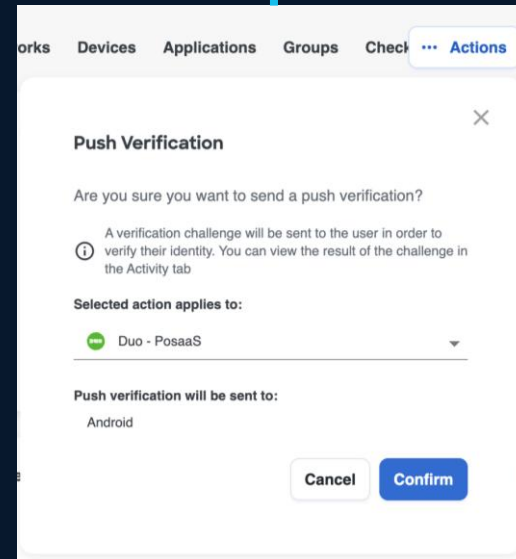
Selected action applies to:

- Duo - PosaaS
- Loxx-Okta

Cancel Confirm

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?

SOC / Admin




Responder typically builds out a timeline when investigation



Starting Here, look forward & backwards for correlation to build the timeline / attack graph of “what happened”

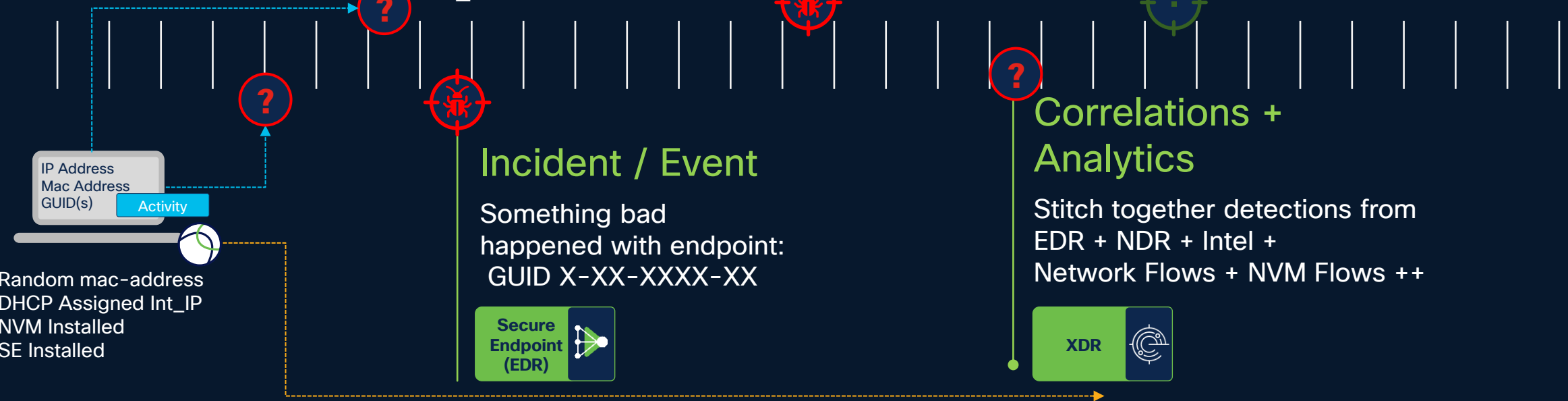
Investigation Timeline

SOC / Admin



Majority of Detections come from Non-ID Systems like EDR & NDR

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"
```

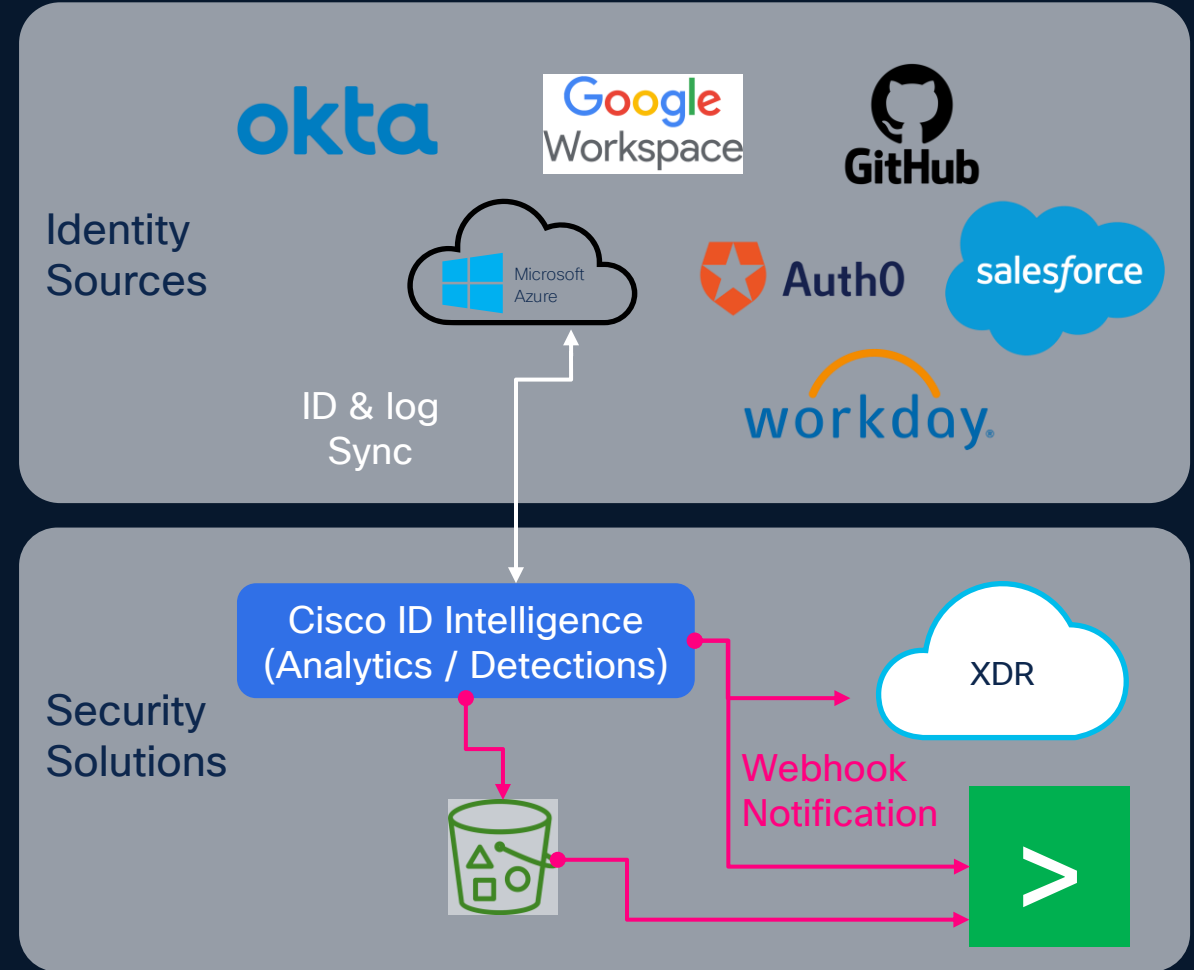


Duo w/
Duo Desktop

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



splunk >

a CISCO company

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).

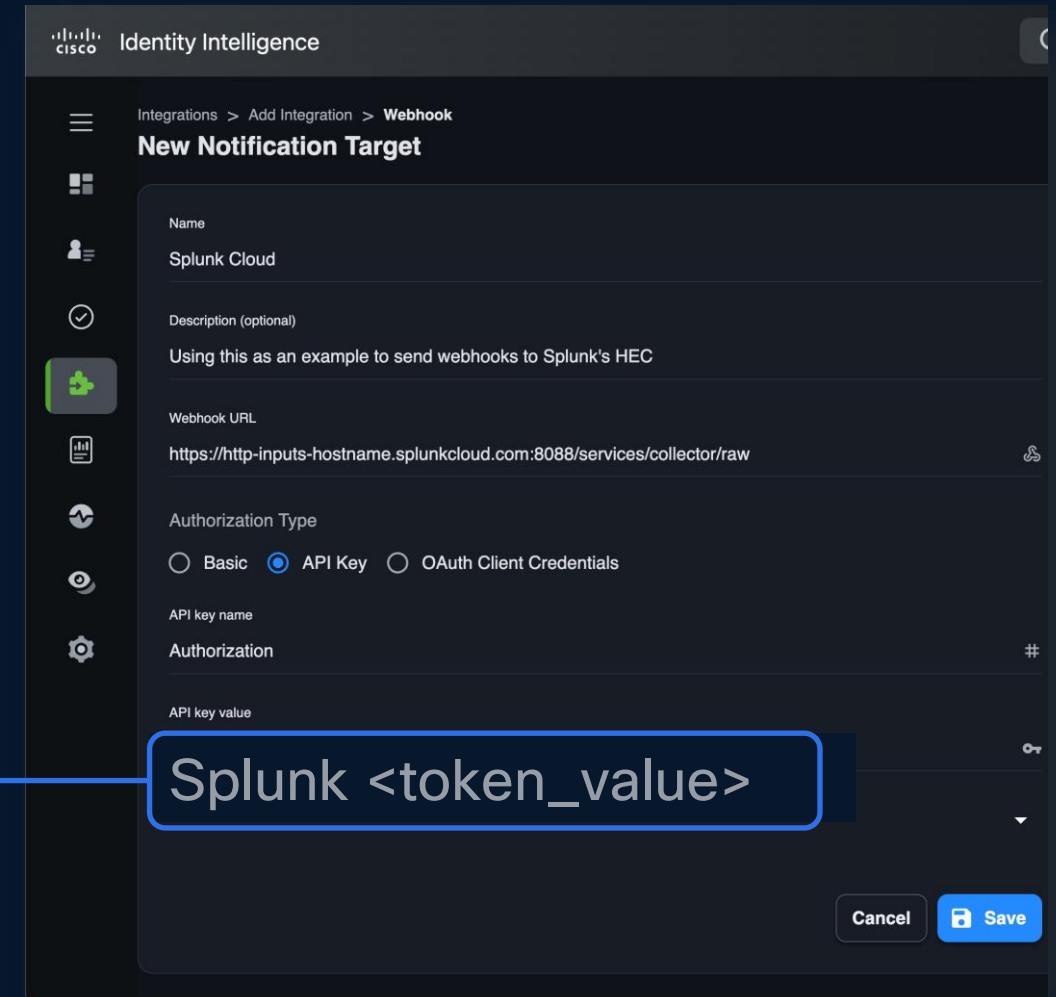
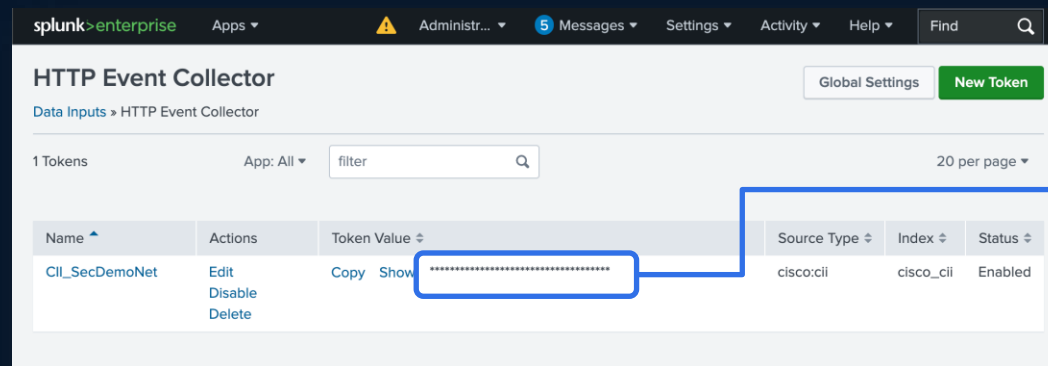
The image shows two screenshots related to the Cisco Security Cloud app in Splunk. The top screenshot is the Splunkbase app page for 'Cisco Security Cloud'. It features a search bar, a 'Login to Download' button, and several informational cards: 'Latest Version 3.0.0' (January 14, 2025), 'Compatibility' (Splunk Enterprise, Splunk Cloud, Platform Versions 9.4, 9.3, 9.2, 9.1, CIM Version: 5.8), 'Rating' (4 stars), 'Support' (Developer Supported Add-on), and 'Ranking' (#1 in Firewall). Below these are tabs for 'Summary', 'Details', 'Installation', 'Troubleshooting', 'Contact', and 'Version History'. The 'Summary' tab is active, showing a description of the app and a list of 'Product(s) Enabled': Cisco Duo, Cisco Email Threat Defense (ETD), Cisco Identity Intelligence (CI), and Cisco Multicloud Defense. The bottom screenshot shows the 'Application Setup' interface in Splunk Enterprise. It has a search bar and a 'My Apps' section with a search input. Under 'My Apps', there is an entry for 'CII_SecDemoNet' with a configuration block:

```
{ name: "CII_SecDemoNet", id: "https://splunk_securitydemo_net-4298/service/6/nobody/CiscoSecurityCloud/CiscoSecurityCloud_cii_input/CII_SecDemoNet", updated: "1979-01-01T00:00:00-08:00", links: { }, author: "nobody", acl: { }, content: { } }
```

 Below this is a 'Cisco Products' section with a search bar and a grid of product cards. The 'Cisco Identity Intelligence' card is highlighted with a red box. Other cards include Duo, Secure Malware Analytics, Secure Firewall, Multicloud Defense, Secure Network Analytics, Cisco Secure Email Threat Defense, XDR, and Cisco Secure Access (SSA).

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

The screenshot shows the Splunk search interface. A search for 'Index="cii_index"' has been performed, resulting in 15 events. The interface includes a search bar, filters, and a table of search results. The table columns are Time and Event. The event details are as follows:

Time	Event
2/3/25 6:42:21.000 PM	<pre>{ [-] account: 98917934444 detail: { [-] } detail-type: FAILED_CHECK id: #7491664-1371-6497-9e48-c3d8e3358697 region: us-east-2 resources: [[+]] source: 239:3746-3095-418f-9d08-1e889f6955d1_212099fb time: 2025-02-03T18:42:43Z version: 0 }</pre>
2/3/25 6:28:02.000 PM	<pre>{ [-] account: 98917934444 detail: { [-] } detail-type: FAILED_CHECK id: #103462-2977-e248-c348-3f3fe4dfaf9 region: us-east-2 resources: [[+]] source: 239:3746-3095-418f-9d08-1e889f6955d1_212099fb time: 2025-02-03T18:28:34Z version: 0 }</pre>
2/3/25 6:11:36.000 PM	<pre>{ [-] account: 98917934444 detail: { [-] } detail-type: FAILED_CHECK</pre>

The screenshot shows the Cisco Identity Intelligence dashboard. It features several charts and tables:

- Total number of events:** 589
- Total number of distinct users:** 151
- Number of failing users:** A bar chart showing the number of failing users over time.
- Number of failing users by Check ID:** A bar chart showing the number of failing users for different check IDs.
- Number of failing users by Check Topic:** A bar chart showing the number of failing users for different check topics.
- Events by severity:** A horizontal bar chart showing the number of events for different severity levels: critical, error, and info.
- Users with most amount of failed checks:** A table listing users and their count of failed checks.
- Events logging:** A table listing events with columns for Time, Severity, Title, Type, Users Failed, and Frameworks.

More can be done with Enterprise Security

The screenshot displays the Splunk Enterprise Security interface. At the top, there's a navigation bar with 'splunk>cloud', 'Apps', '15 Messages', 'Settings', 'Activity', and a search bar. Below this is a secondary navigation bar with 'Mission Control', 'Analytics', 'Security content', 'Configure', and 'Search'. The main content area is divided into two panels. The left panel, titled 'Findings and investigations', shows a list of findings. The right panel, titled 'Start investigation', provides a detailed view of a specific finding.

Findings and investigations

Title	ID	Type	Entity	Ris...
24 hour risk threshold exceeded for user=shaun.stuart@splunktshirtcompany.com		FINDING	shaun.stuart@...	1040
24 hour risk threshold exceeded for user=mickey.perre@splunktshirtcompany.com		FINDING	mickey.perre...	1040
24 hour risk threshold exceeded for user=Varsha.Mahadevan@splunktshirtcompany.com		FINDING	Varsha.Mahad...	1040
24 hour risk threshold exceeded for user=Hayley.Jensen@splunktshirtcompany.com		FINDING	Hayley.Jensen...	1040
24 hour risk threshold exceeded for system=58.96.44.0		FINDING	58.96.44.0	1040
24 hour risk threshold exceeded for user=fyodor@splunktshirtcompany.com		FINDING	fyodor@splun...	1946
Geographically Improbable Access Detected For shaun.stuart@splunktshirtcompany.com		FINDING	--	2420
Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	1985
Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	1985
Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	1985
Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	1985
Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	1985

Start investigation

FINDING

24 hour risk threshold exceeded for user=fyodor@splunktshirtcompany.com

Risk Threshold Exceeded for an object over a 24 hour period

Owner: unassigned | Status: New | Urgency: Informational

Sensitivity: Unassigned | Disposition: Undetermined

Time: Apr 16th, 2025 11:22 PM
Last updated: Apr 16th, 2025 11:22 PM
Reference ID: 299f20c1-53e5-4216-9dc2-ddc7d8146734@@notable@@299f20c153e542169dc2ddc7d8146734

Detection: Cisco CII - Multiple failed checks from single user - Rule Audit - Possible Brute Force Activity - Rule ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule

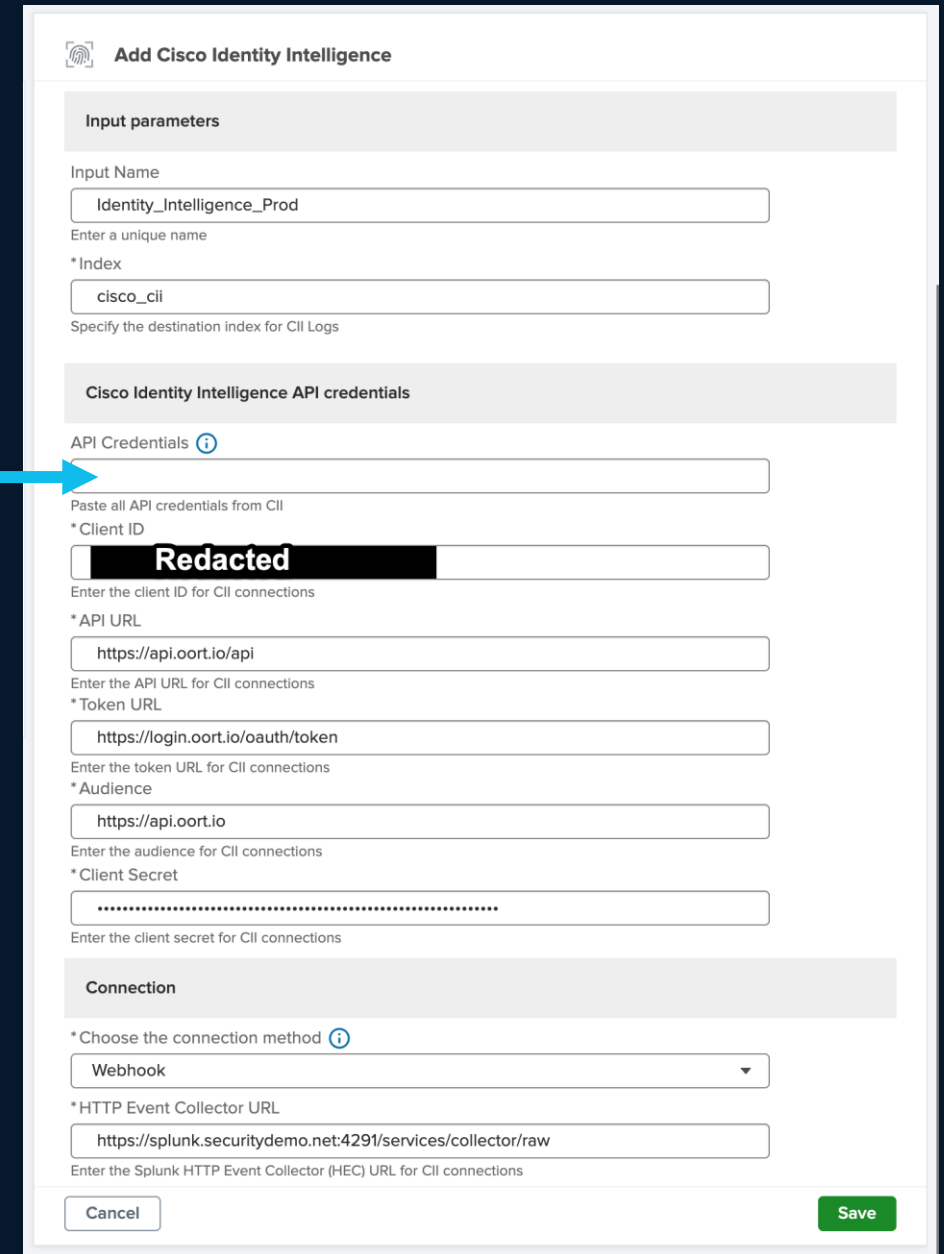
All entities: fyodor@splunktshirtcompany.com

Detection name: Cisco CII - Multiple failed checks from single user - Rule Audit - Possible Brute Force Activity - Rule ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule

Entity: jyoti@securitydemo.net
Entity type: user
Intermediate findings: 334
MITRE: T1021, T1030, T1059.001
Risk score: 19460
Security domain: threat

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!



Add Cisco Identity Intelligence

Input parameters

Input Name

Enter a unique name

* Index

Specify the destination index for CII Logs

Cisco Identity Intelligence API credentials

API Credentials ⓘ

Paste all API credentials from CII

* Client ID

Enter the client ID for CII connections

* API URL

Enter the API URL for CII connections

* Token URL

Enter the token URL for CII connections

* Audience

Enter the audience for CII connections

* Client Secret

Enter the client secret for CII connections

Connection

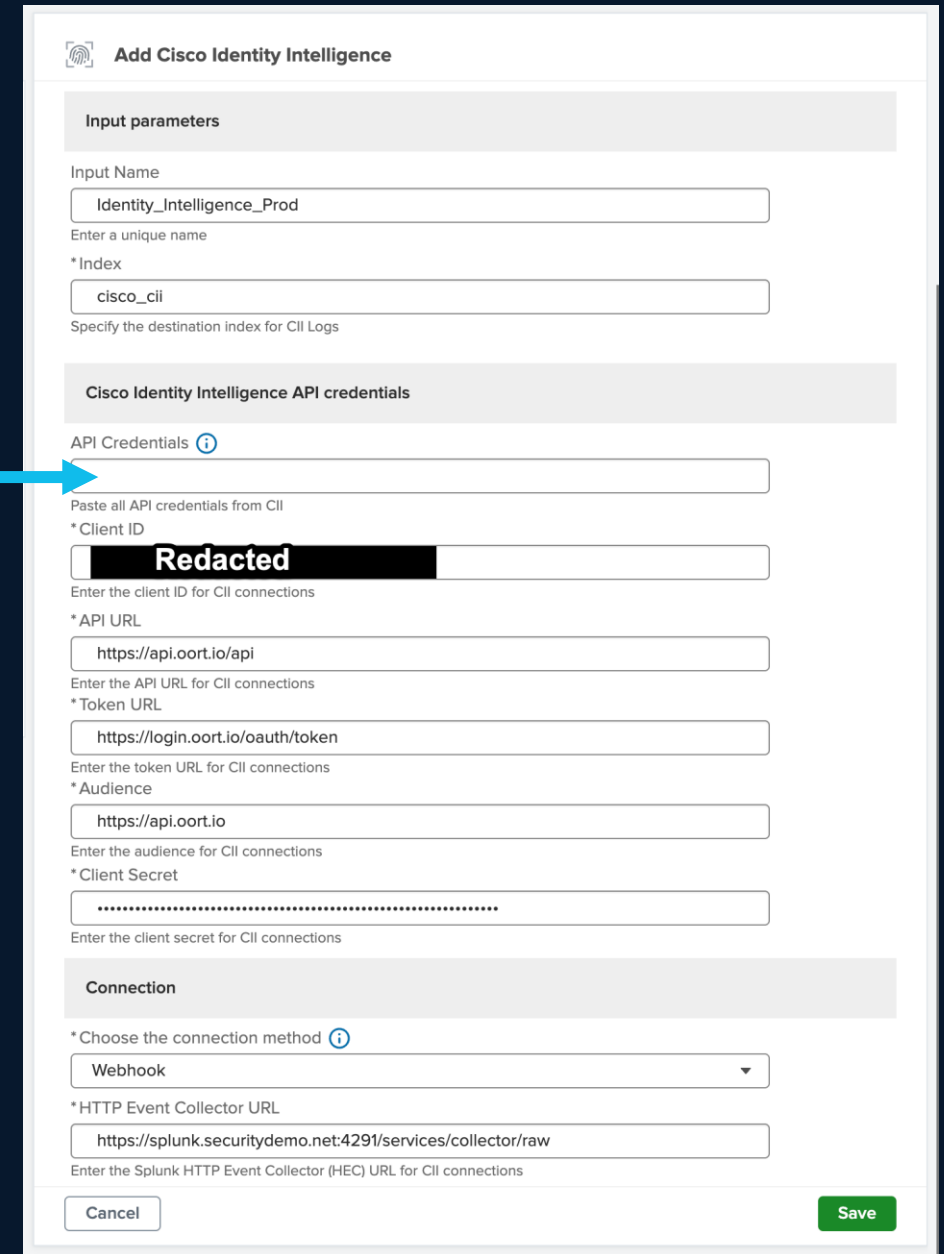
* Choose the connection method ⓘ

* HTTP Event Collector URL

Enter the Splunk HTTP Event Collector (HEC) URL for CII connections

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



Add Cisco Identity Intelligence

Input parameters

Input Name
Identity_Intelligence_Prod
Enter a unique name

* Index
cisco_cii
Specify the destination index for CII Logs

Cisco Identity Intelligence API credentials

API Credentials ⓘ
Paste all API credentials from CII

* Client ID
Redacted
Enter the client ID for CII connections

* API URL
https://api.oort.io/api
Enter the API URL for CII connections

* Token URL
https://login.oort.io/oauth/token
Enter the token URL for CII connections

* Audience
https://api.oort.io
Enter the audience for CII connections

* Client Secret
.....
Enter the client secret for CII connections

Connection

* Choose the connection method ⓘ
Webhook

* HTTP Event Collector URL
https://splunk.securitydemo.net:4291/services/collector/raw
Enter the Splunk HTTP Event Collector (HEC) URL for CII connections

Cancel Save

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.

Connection

* Choose the connection method [i](#)

AWS S3

* AWS Access Key ID

Enter the AWS Access Key ID associated with your AWS account

* AWS Secret Access Key

Enter the AWS Secret Access Key associated with your AWS account

* SQS Queue URL

Enter the URL for your Amazon SQS queue

* External ID

Enter the AWS external ID

* S3 Bucket URL

Enter the S3 bucket URL in the format s3://bucket-name/path, where /path is optional

* S3 Bucket Region

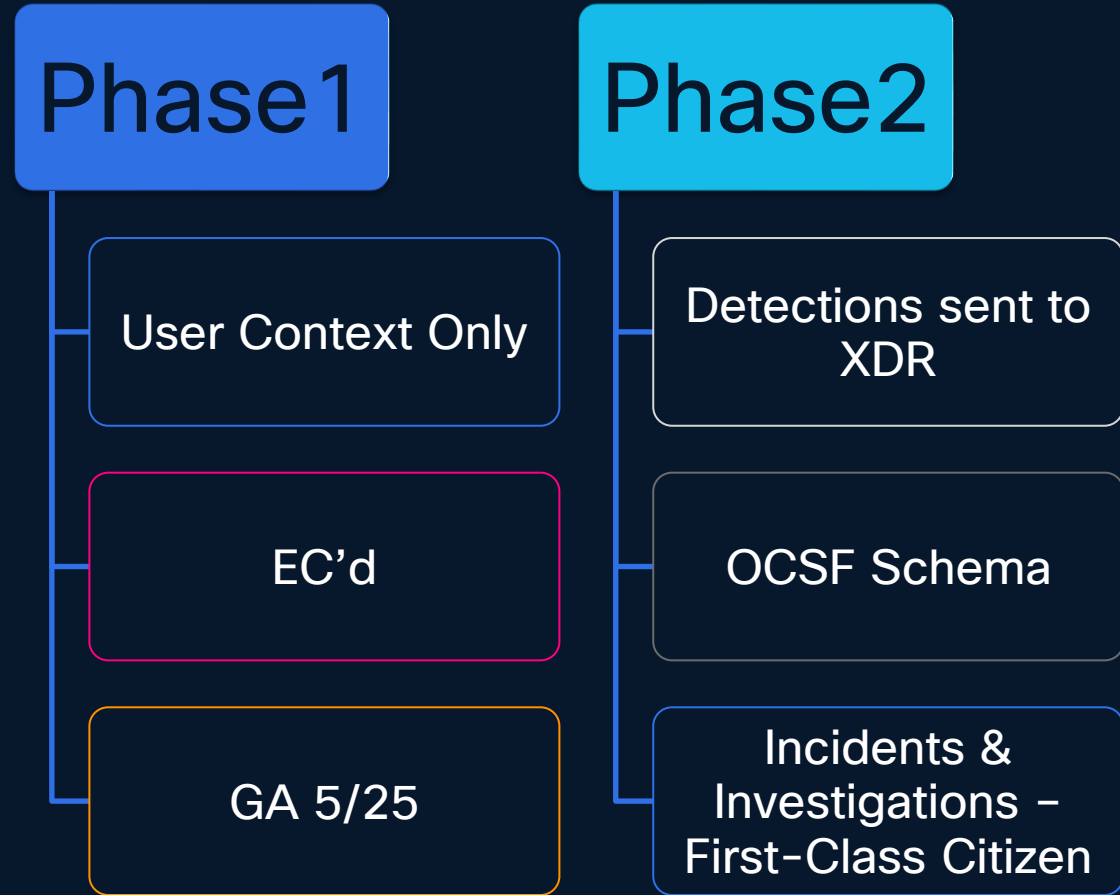
Enter S3 Bucket Region

Cancel Save



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

A screenshot of the Security Cloud Control (SCC) web interface. The browser address bar shows 'https://security.cisco.com'. The page title is 'Security Cloud Control'. The main content area is titled 'Organization'. A modal window titled 'Select Organization' is open, showing a form with the following fields: 'Create new organization' (a dropdown menu), 'New organization name *' (a text input field containing 'ATW-XDR-CII-TEST' with a '50 character limit' note below it), and 'Region deployment *' (a dropdown menu showing 'North America'). Below the form, there is explanatory text: 'This selection determines the deployment for all products and services added to this organization. [Read documentation.](#)' and a blue 'Continue' button. A larger, semi-transparent version of this modal is overlaid on the right side of the screenshot for emphasis.

XDR leverages Security Cloud Control (SCC)

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



A screenshot of the Security Cloud Control (SCC) web interface. The top navigation bar includes the Cisco logo, the text 'Security Cloud Control', a search bar with the placeholder 'Type \"/>

XDR leverages Security Cloud Control (SCC)

You must claim a subscription to attach/activate XDR



A screenshot of the Cisco Security Cloud Control (SCC) web interface. The page title is 'Platform Management' for the organization 'CII-TEST'. The left sidebar shows a navigation menu with 'Platform Management' selected. The main content area displays a 'No products activated' message with a purple information icon. A blue arrow points to the 'Subscriptions' link in the left sidebar, and another blue arrow points to a 'Claim subscription' button in the top right corner of the main content area. The URL at the bottom of the browser window is 'https://control.v3.int.security.cisco.com/a/overview?enterpriseid=bfa6442c-a433-4333-b59c-61335f214bf5'.

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)

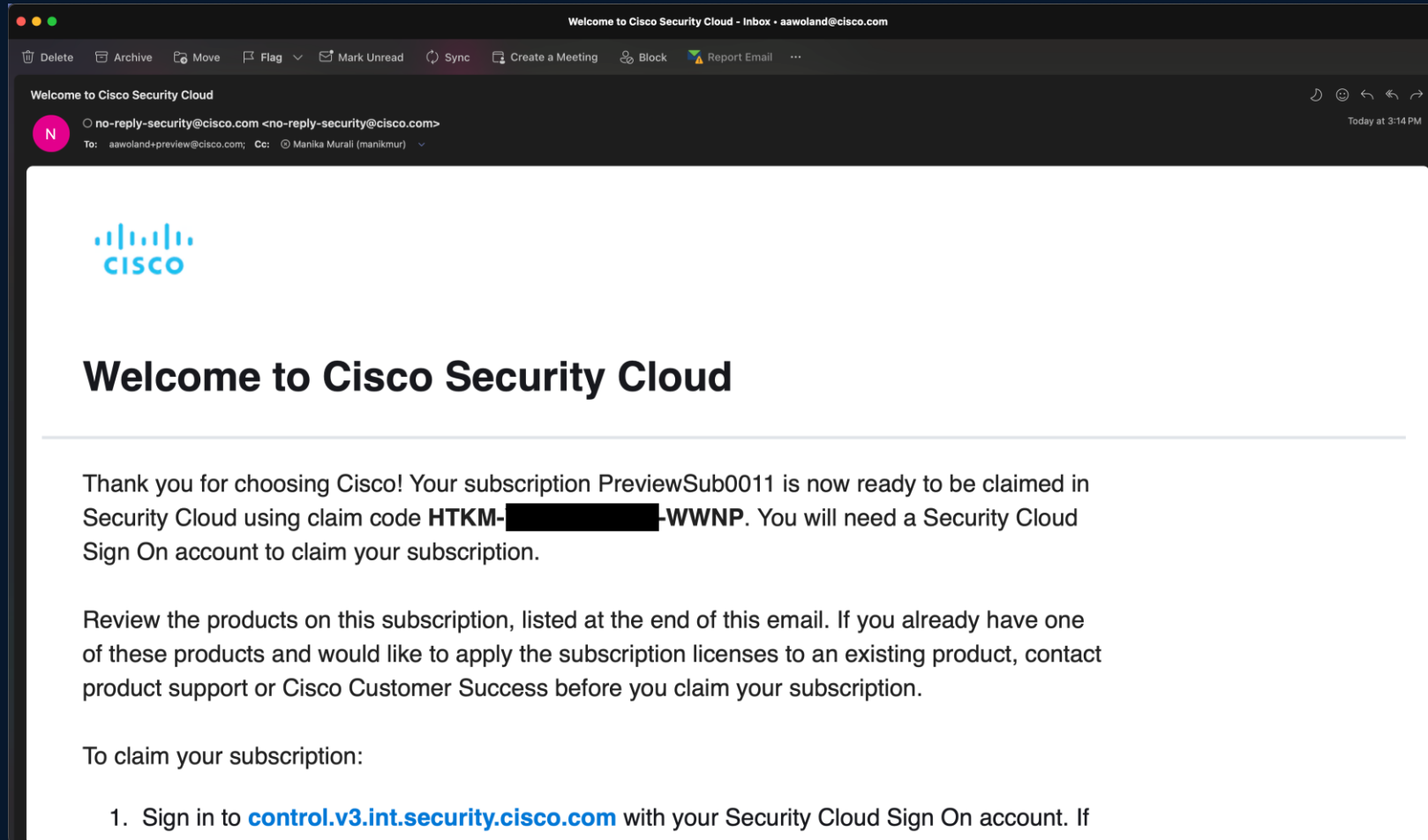
You paste the claim code, go check your email...



A screenshot of the Cisco Security Cloud Control (SCC) web interface. The page title is 'Claim Subscription'. On the left is a navigation sidebar with a menu icon, an organization dropdown (ATW-XDR-CII-TEST - North America), and links for Home, Platform services, Favorites, and Platform Management. The main content area shows a three-step process: 1. Enter subscription claim code (active), 2. Review products and services, and 3. Review subscription. The active step contains instructions to enter a claim code and click 'Next', with a 'documentation' link. Below the text is a text input field labeled 'Subscription claim code *'. At the bottom of the main area are 'Cancel' and 'Next' buttons. The footer includes '© 2025 Cisco Systems, Inc.' and links for 'Privacy Policy' and 'General Terms'.

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

A screenshot of the Cisco Security Cloud Control (SCC) web interface. The page title is "Claim Subscription". On the left, there is a navigation sidebar with a menu icon at the top, followed by "Organization ATW-XDR-CII-TEST - North America", "Home", "Platform services", "Favorites", and "Platform Management". The main content area shows a progress indicator with three steps: "1 Enter subscription claim code" (active), "2 Review products and services", and "3 Review subscription". The active step is titled "Enter subscription claim code" and contains instructions: "To begin, enter your claim code below and click **Next**. For detailed instructions please read our [documentation](#)." Below the instructions is a text input field labeled "Subscription claim code" with a red asterisk indicating it is required. The field contains the text "HTKM-[REDACTED]-WWNP". At the bottom of the form are "Cancel" and "Next" buttons. The footer of the page includes "© 2025 Cisco Systems, Inc." and links for "Privacy Policy" and "General Terms".

XDR leverages Security Cloud Control (SCC)

Create the new XDR Instance or Attach Existing



A screenshot of the Cisco Security Cloud Control (SCC) web interface. The left sidebar shows the organization 'ATW-XDR-CII-TEST - North America' and navigation options like 'Home', 'Favorites', and 'Platform Management'. The main content area is titled 'Review products and services' and contains instructions on how to create or attach an instance. It lists two categories: 'Products' and 'Entitlements'. Under 'Products', 'Cisco XDR Advantage' is shown with a dropdown menu set to 'Create new instance'. Under 'Entitlements', 'Cisco Identity Intelligence' is shown with the note 'Further input required at end of claim process.' At the bottom, there are 'Cancel', 'Back', and 'Next' buttons. The footer includes the copyright notice '© 2025 Cisco Systems, Inc.' and links for 'Privacy Policy' and 'General Terms'.

XDR leverages Security Cloud Control (SCC)

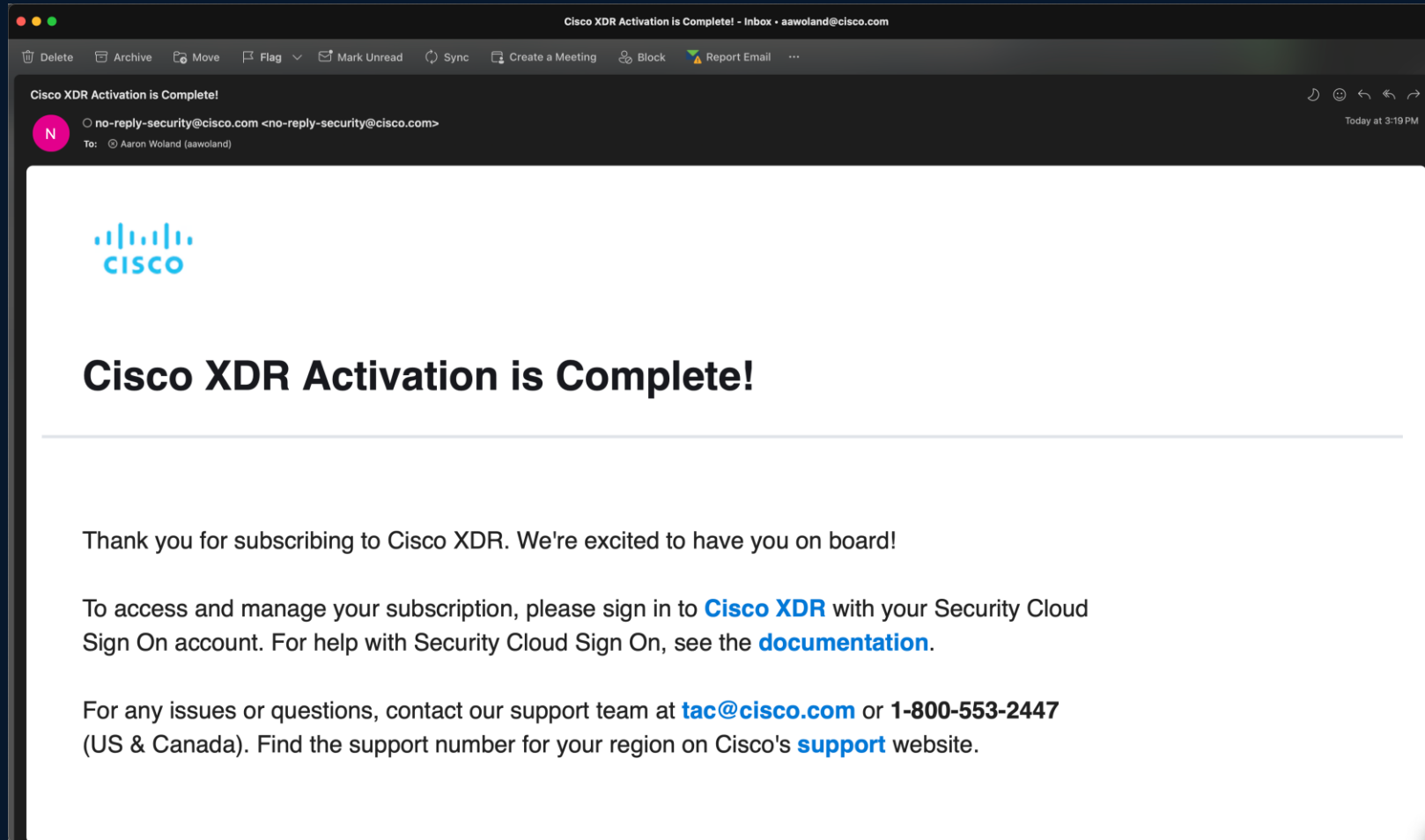
Create the new XDR Instance or Attach Existing



A screenshot of the Cisco Security Cloud Control (SCC) web interface. The main page is titled 'Claim Subscription' and shows a progress bar with three steps: 'Enter subscription claim code', 'Review products and services', and 'Review subscription' (the current step). The 'Review subscription' section displays 'Subscription ID: PreviewSub0011' and 'Products: Cisco XDR Advantage'. Two callout boxes are overlaid on the interface. The top callout box, titled 'Claim subscription' with a warning icon, contains the text: 'Claiming this subscription will associate the subscription details, including subscription ID and product licenses, with the ATW-XDR-CII-TEST organization.' and has 'Cancel' and 'Claim' buttons. The bottom callout box, also titled 'Claim subscription' with a warning icon, contains the same text and has 'Cancel' and 'Claim' buttons. The background interface is dimmed. At the bottom of the page, there is a copyright notice '© 2025 Cisco Systems, Inc.' and links for 'Privacy Policy' and 'General Terms'.

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



The screenshot shows the SCC web interface for an organization named 'ATW-XDR-CII-TEST - North America'. The page title is 'Overview - ATW-XDR-CII-TEST'. A search bar at the top right contains the text 'Type \'Ctrl\' + \'/\' to search'. The user's name 'Aaron Woland' is visible in the top right corner. The left sidebar contains navigation options: 'Home', 'Platform services', 'Favorites', and 'Platform Management'. The main content area displays several notification cards. The first card states 'Subscription successfully claimed.' and provides instructions on where to find products and how to configure role-based access controls. The second card indicates that the organization is entitled to use Firewall Management and provides a link to 'Enable Firewall Management now.'. Below these notifications is a section titled 'Product and service activation status' with a notification icon. Under this section, 'Cisco Identity Intelligence' is listed with an information icon and a message stating that the subscription entitles the user to Cisco Identity Intelligence, delivered through Cisco Duo. An 'Action required' button is present next to this message. The 'Products' section below shows 'Cisco XDR Advantage' as 'Activated'. A table provides details for this product: Subscription ID (PreviewSub0011), End date (-), External Instance ID (8de81363-bbd5-49d8-b685-4ab895cf6802), Quantity (1000), and Region (North America). The footer of the page includes the copyright notice '© 2025 Cisco Systems, Inc.' and links for 'Privacy Policy' and 'General Terms'.

XDR leverages Security Cloud Control (SCC)

Define Initial Admin + Attach Duo or Create New One



The screenshot displays the Cisco Security Cloud Control (SCC) web interface. The main content area shows the "Overview - ATW-XDR-CII-TEST" page for an organization with ID "bfa6442c-a433-4333-b59c-61335f214bf5". A notification states "Subscription successfully claimed." Below this, a modal window titled "Cisco Identity Intelligence" is open, allowing for configuration. The modal includes a message "Fields with asterisk(*) are required." and three required fields: "Initial administrator *" (set to "aawoland@cisco.com"), "How would you like to provision Duo? *" (set to "Create a new account"), and "Hosting Country *" (set to "United States"). At the bottom of the modal are "Cancel" and "Request activation" buttons. The background interface shows a sidebar with navigation options like "Home", "Favorites", and "Platform Management".

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

Cisco Identity Intelligence

Fields with asterisk(*) are required.

Initial administrator *

aawoland@cisco.com

How would you like to activate Duo? *

Connect an existing account

Hosting Country

Select answer

The screenshot shows the Duo Admin console interface. On the left is a navigation sidebar with options like Home, Users, Devices, Policies, Applications, Reports, Monitoring, Billing, and Settings. The main content area is titled 'Administrators' and includes a search bar, a filter for 'All statuses', and an 'Export' button. Below this is a table of administrators:

Name	Role	Administrative Units	Email	Status	Last Login (UTC)
Aaron	Owner	All access	aawoland@cisco.com	Active	Jul 2, 2025 5:05 PM

At the bottom of the console, there is a footer with copyright information: © 2025 Duo Security. All rights reserved. It also shows 'Selected: Bunzl / ID: 3820-5300-84' and 'Deployment ID: DU057'.

XDR leverages Security Cloud Control (SCC)

Provisioning of Headless Duo + CII Starts



The screenshot displays the SCC web interface. At the top, the Cisco logo and 'Security Cloud Control' are visible. A search bar contains the text 'Type 'Ctrl' + '/' to search'. The user 'Aaron Woland' is logged in. The left sidebar shows navigation options: Organization (ATW-XDR-CII-TEST - North America), Home, Platform services, Favorites, and Platform Management. The main content area is titled 'Overview - ATW-XDR-CII-TEST' with Organization ID 'bfa6442c-a433-4333-b59c-61335f214bf5'. A notification banner at the top right states 'Request for activation has been successfully submitted.' Below this, a message indicates 'Subscription successfully claimed.' and provides instructions on where to find products and how to configure role-based access controls. Another notification states 'Your organization is entitled to use Firewall Management. Enable Firewall Management now.' The 'Product and service activation status' section shows 'Cisco Identity Intelligence' with a yellow 'Activation in progress' warning. The 'Products' section lists 'Cisco XDR Advantage' as 'Activated' with the following details:

Subscription ID	PreviewSub0011
End date	-
External Instance ID	8de81363-bbd5-49d8-b685-4ab895cf6802
Quantity	1000
Region	North America

At the bottom of the page, there is a copyright notice '© 2025 Cisco Systems, Inc.' and links for 'Privacy Policy' and 'General Terms'.

Now... Wait



XDR leverages Security Cloud Control (SCC)

Provisioning of Headless Duo + CII Starts



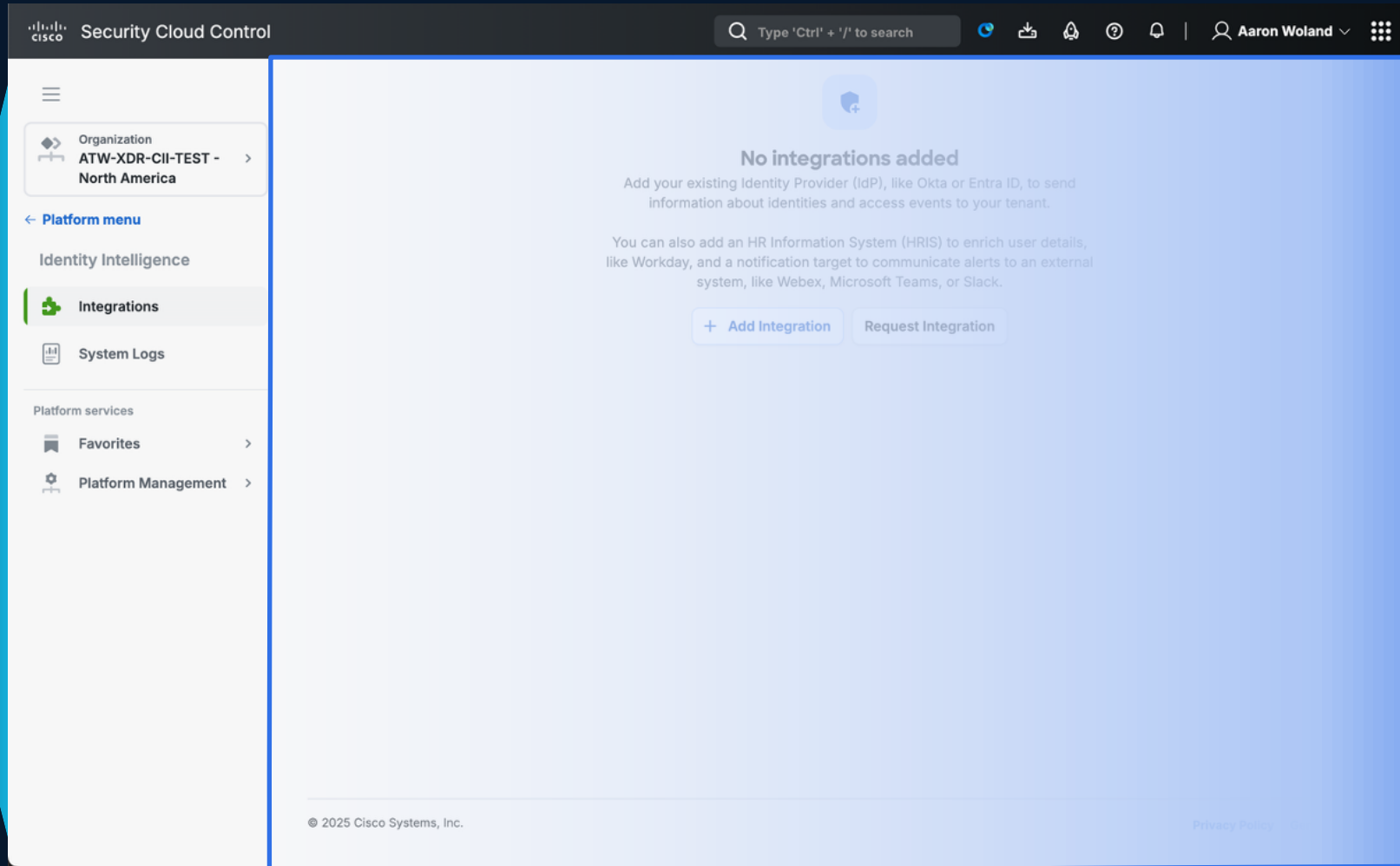
The screenshot shows the Cisco Security Cloud Control (SCC) interface. The top navigation bar includes the Cisco logo, the text 'Security Cloud Control', a search bar with the placeholder 'Type 'Ctrl' + '/' to search', and user information for 'Aaron Woland'. The main content area is titled 'Overview - ATW-XDR-CII-TEST' and includes a 'Claim subscription' button. Below the title, the organization ID is listed as 'bfa6442c-a433-4333-b59c-61335f214bf5'. A notification banner states: 'Your organization is entitled to use Firewall Management. Enable Firewall Management now.' The 'Products' section shows 'Cisco XDR Advantage' as 'Activated'. Below this, a table lists subscription details:

Subscription ID	PreviewSub0011
End date	-
External instance ID	8de81363-bbd5-49d8-b685-4ab895cf6802
Quantity	1000
Region	North America

The left-hand navigation pane contains several menu items: 'Organization ATW-XDR-CII-TEST - North America', 'Home', 'Products' (with 'Identity Intelligence' highlighted by a pink box and a pink arrow), 'Platform services', 'Favorites', and 'Platform Management'. The footer of the interface includes the copyright notice '© 2025 Cisco Systems, Inc.' and links for 'Privacy Policy' and 'General Terms'.

Security Cloud Control (SCC) uses Micro-Front Ends

Provisioning of Headless Duo + CII Starts



All Users are now in Assets > Users

Add more

The screenshot shows the Cisco XDR 'Users' page. At the top, there's a navigation bar with 'XDR' and a user profile for 'Aaron Woland'. Below the navigation, the 'Users' section is active. A 'Source health' indicator shows 'Healthy' with 'All sources are operational'. Summary statistics show '19,600 total' users, with '10,343 with identity events' and '19,551 not using MFA'. A search bar contains 'securitydemo.net', resulting in 87 matching users. A table lists several users with columns for display name, login names, emails, labels, value, sources, identity events, MFA status, and last logon.

Display name	Login names	Emails	Labels	Value	Sources	Identity events	MFA status	Last logon
Accounting2	accounting2@securitydemo.net	accounting2@securitydemo.net	10 (D)	10 (D)	Entra ID, Duo	1	Disabled	
Alana Jackson	alajacks@securitydemo.net	alajacks@securitydemo.net	10 (D)	10 (D)	Entra ID, Duo	1	Disabled	
Alex Zaslavsky	alexzas@securitydemo.net	alexzas@securitydemo.net	10 (D)	10 (D)	Entra ID, Duo, OKTA	2	Enabled	2025-05-29T15:58:55
Anat Borowitsh Lavy	anat@securitydemo.net	anat@securitydemo.net	10 (D)	10 (D)	Entra ID, Duo, OKTA	1	Disabled	
Andrew Maxey	andrew@securitydemo.net	andrew@securitydemo.net	10 (D)	10 (D)	Entra ID, Duo, OKTA	1	Disabled	
Andy Winiarski	andy@securitydemo.net	andy@securitydemo.net	10 (D)	10 (D)	Entra ID, Duo, OKTA	2	Enabled	2025-07-21T18:22:22

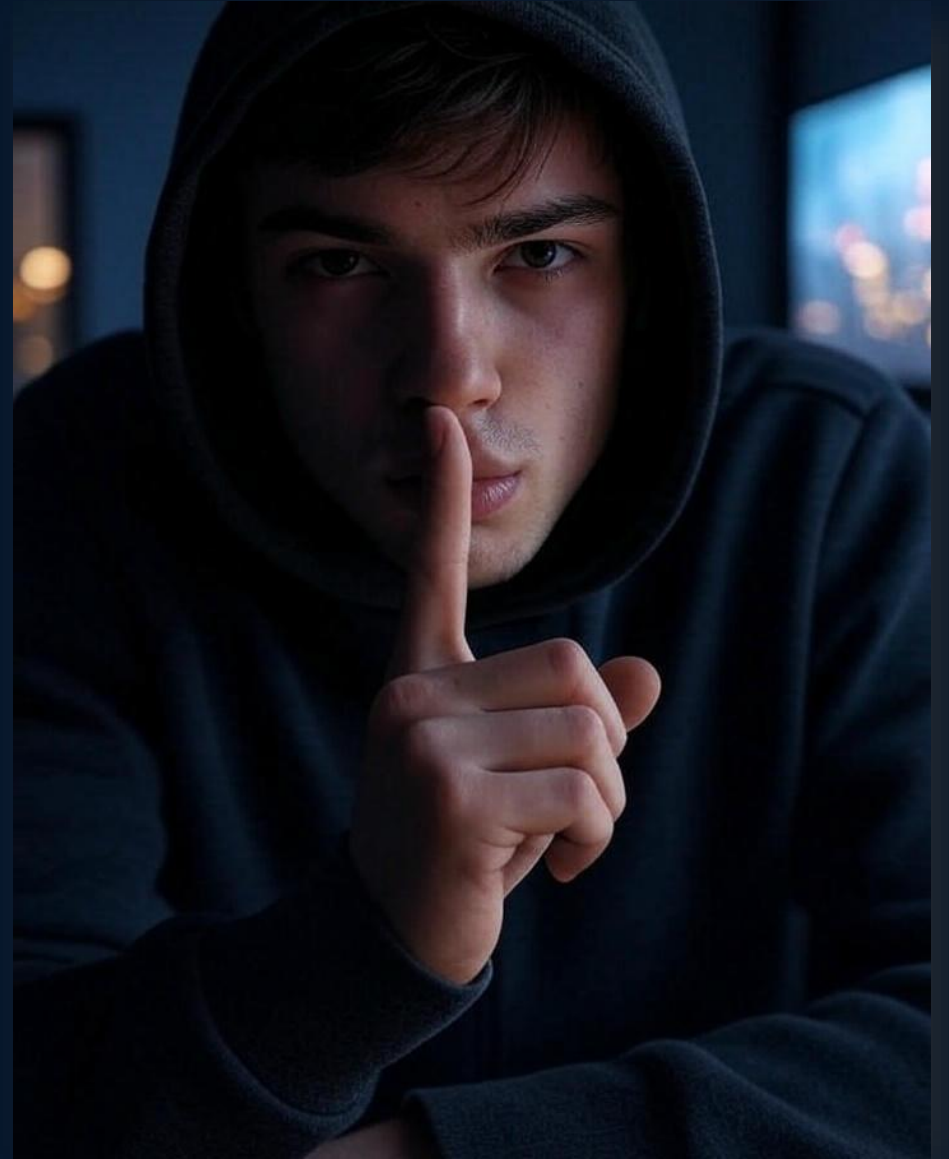
All Users are now in Assets > Users

Can add Labels and Change User Asset Value

The screenshot shows the Cisco XDR user profile for 'EmployeeOne'. The interface includes a navigation sidebar on the left, a top header with the user's name 'Aaron Woland' and a notification bell, and a main content area with several sections:

- Header:** 'EmployeeOne' with labels 'Under Investigation' and 'Employee'. Includes 'Add Labels' and 'User value: 10 (Default value)'.
- Used devices:** Lists three devices with their last login status.
- Identity events:** Lists events such as 'users-sharing-authenticators', 'directly-assigned-applications', and 'allow-block-emails'.
- Activity details:** Shows MFA status (Enabled), usage location (WILMINGTON, DE, US), last logon time, account creation date, account status (Enabled), used factors (password), and used applications (One Outlook Web, Windows Sign In).
- IP Addresses:** Lists two IP addresses: 128.107.78.71 and 196.196.53.135.
- Identity details:** Shows display name (EmployeeOne), login names, emails, phone numbers, user ID, and sources (Entra ID, Duo, OKTA).
- Organization Role:** Shows company (SecurityDemo), department (Human Labor), manager, job title, employee IDs, and groups (Employees, Domain Users, etc.).

Sssshhhhhhhh!



XDR does not entitle users to the CII Console

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

The screenshot shows the Cisco Security Cloud Control interface. On the left is a navigation menu with sections like 'Platform menu', 'Identity Intelligence', 'Integrations', 'System Logs', 'Platform services', 'Favorites', and 'Platform Management'. The main area displays a list of 31 events. The table has columns for Date (UTC), Event, Initiator, Target, Result, and Logged By. A red box highlights the share icon in the top right corner of the event list.

Date (UTC)	Event	Initiator	Target	Result	Logged By
Jun 1, 2025 17:09:25 Ended in 0h 0m 0s	integrations-health-ch...	System	N/A	Success	system-comman
Jun 1, 2025 14:54:29 Ended in 0h 0m 0s	update-tenant-journies	System	N/A	Success	system-comman
Jun 1, 2025 14:54:28 Ended in 0h 0m 0s	CREATE_REPORT Type: access-countries-report	System	N/A	Success	create-end-us
Jun 1, 2025 14:54:27 Ended in 0h 0m 0s	CREATE_REPORT Type: mfa-enrollment-report	System	N/A	Success	create-end-us
Jun 1, 2025 14:54:26 Ended in 0h 0m 0s	CREATE_REPORT Type: registered-device-os-report	System	N/A	Success	create-end-us
Jun 1, 2025 14:54:25 Ended in 0h 0m 0s	CREATE_REPORT Type: check-compliance-report	System	N/A	Success	create-end-us
Jun 1, 2025 14:54:24 Ended in 0h 0m 1s	CREATE_REPORT Type: mfa-usage-over-time-report	System	N/A	Success	create-end-us
Jun 1, 2025 14:24:25 Ended in 0h 0m 6s	create-user-linkage-su...	System	N/A	Success	system-comman

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>

Identity Intelligence

CONNECTING TO CISCO IDENTITY INTELLIGENCE

Enter Organization

Select your organization to continue

Organization Name
atw-xdr-cii-test707

Continue

© 2025 Identity Intelligence
This environment reloads hourly

[Privacy Policy](#) [Terms of Use](#) [Documentation](#) [Status](#)

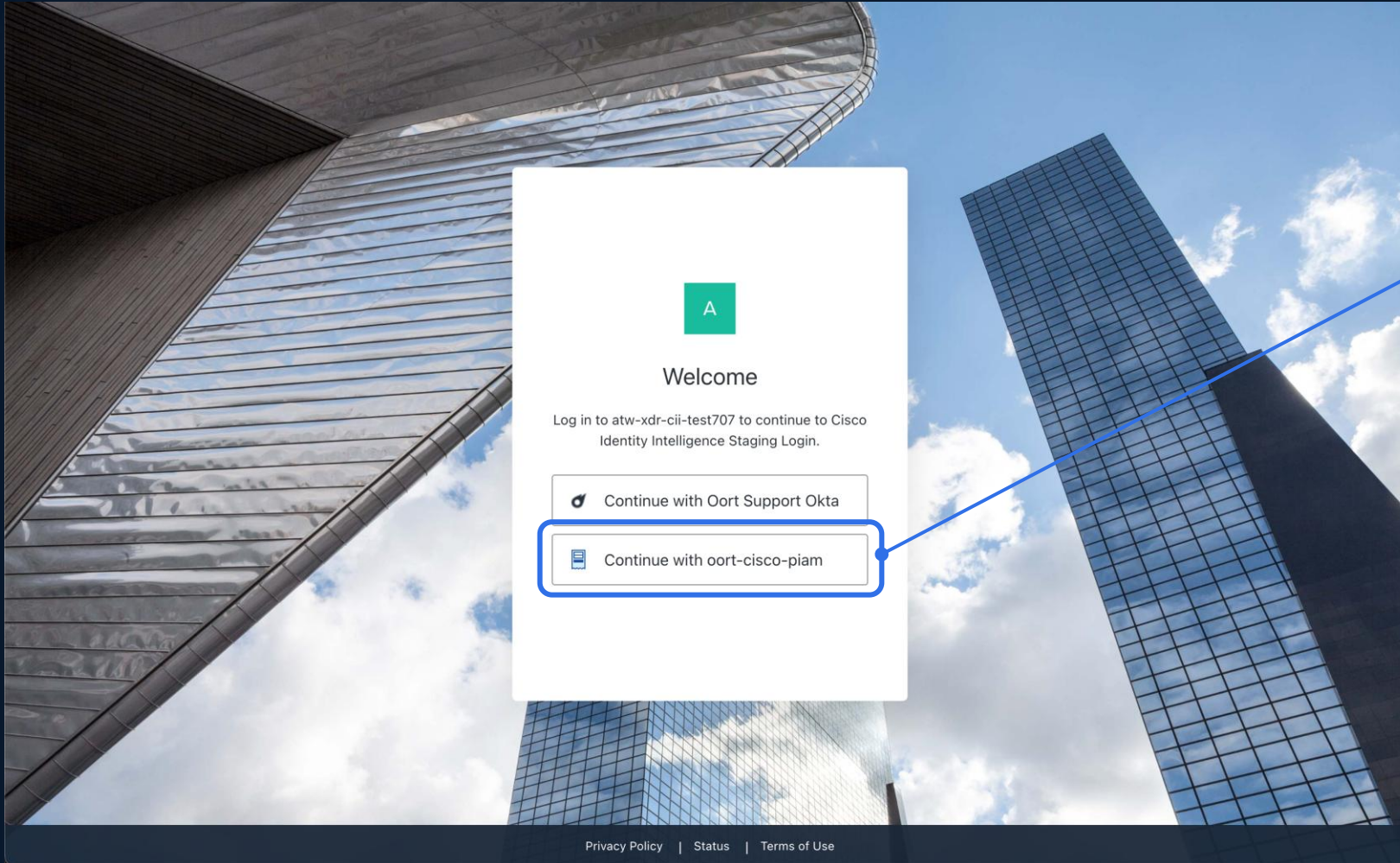
Copy direct link

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

[https://dashboard.\[region\].oort.io](https://dashboard.[region].oort.io)

CI'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

Identity Intelligence

Search

Aaron We atw-xdr-c

Get Started Overview MFA

Get started with Identity Intelligence

1. Learn how CII works
2. Connect your identity sources
3. Add Human Resource Info System (HRIS) information
4. Create a notification target
5. Flag your most important apps

1. Learn how Identity Intelligence works to secure identities

Leverage best practices

- Watch the 'Identity Intelligence in 2 minutes' video
- Understand how identity security posture and threat detection can be leveraged together
- Learn about the different insights available and which sources they are compatible with

2. Connect your identity sources for richer insights and holistic user data

Identity Intelligence has native integrations with Microsoft Entra ID, Okta, Google, Salesforce, Github, Slack, and more. The more identity sources you integrate, the more accurate and insightful your users' data will be.

- [Connect your primary Identity Provider \(IdP\)](#)
- [Connect a secondary IdP or additional identity source\(s\)](#)

3. Connect data from your Human Resource Info System (HRIS) for more user context and additional insights

HRIS data further enriches your users' data with additional context and employment records. Identity Intelligence has a native integration with Workday and can ingest static reports from other HRIS tools.

- [Add a Workday integration or import your HRIS information via .csv](#)

4. Create your first notification target

Alerts when users fail checks can be sent through email or Webhooks, or via integrations with Slack, Microsoft Teams, and Webex. Once your notification target is set up, you can configure it to receive alerts based on your organization's specific needs and interests.

- [Set up your preferred notification target](#)

5. Flag your most important apps as sensitive applications



AI generated image

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](#)



General

Display Name* 20 / 64
CII Webhook Listener

Description 92 / 1024

Request Content Type*
application/json

Webhook Details

Webhook ID
[Redacted]

Webhook API Key
[Redacted]

Webhook URL
https://automate.us.security.cisco.com/webhooks/02C [Redacted]

Integrations > Edit Settings
Edit Webhook Settings

Name
Aaron XDR Listener

Description (optional)
Listener configured in XDR for webhooks

Webhook URL
https://automate.us.security.cisco.com/webhooks/02CWJ [Redacted]

Authorization Type
 Basic API Key Duo Security Client OAuth Client Credentials

API key name
foo #

API key value

Invocation HTTP Parameters

Parameter	Key name	Key value	
Header	Content-Type	application/json	Remove
Header	Accept	application/json	Remove

Add parameter

Cancel Save

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

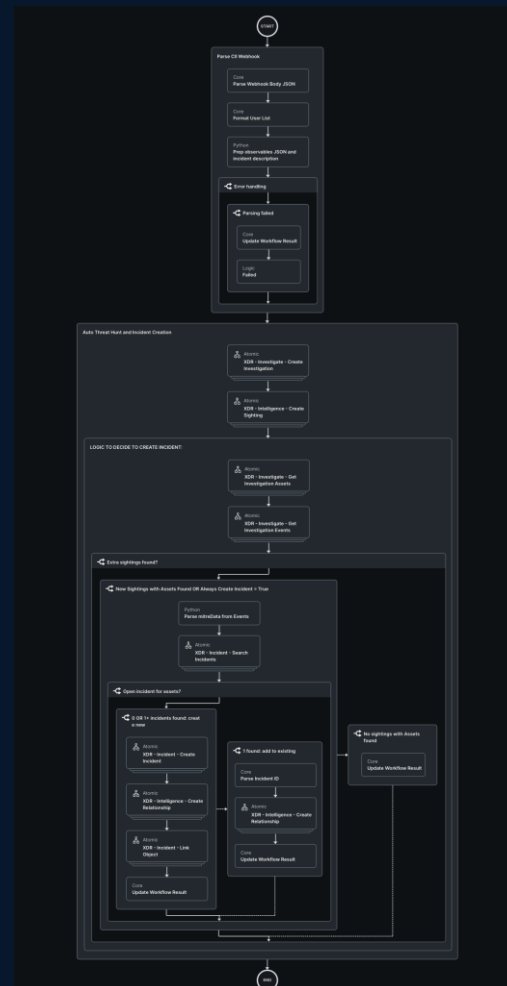
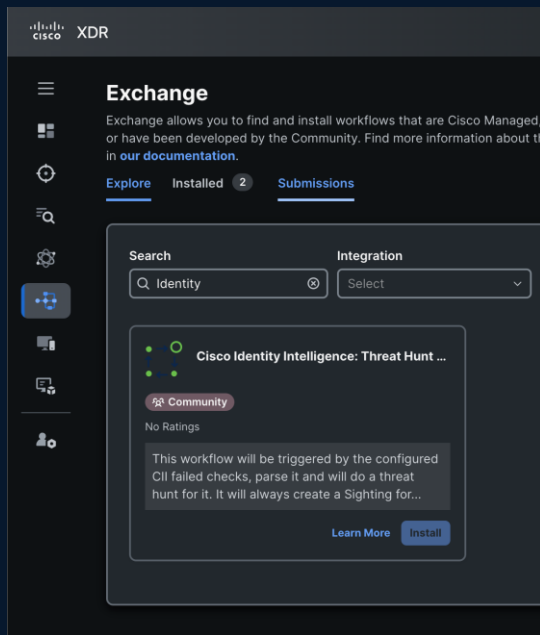
Setup Guide

Published [here at Aaron Woland's blog](#)

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

Webhooks w/ Cisco XDR

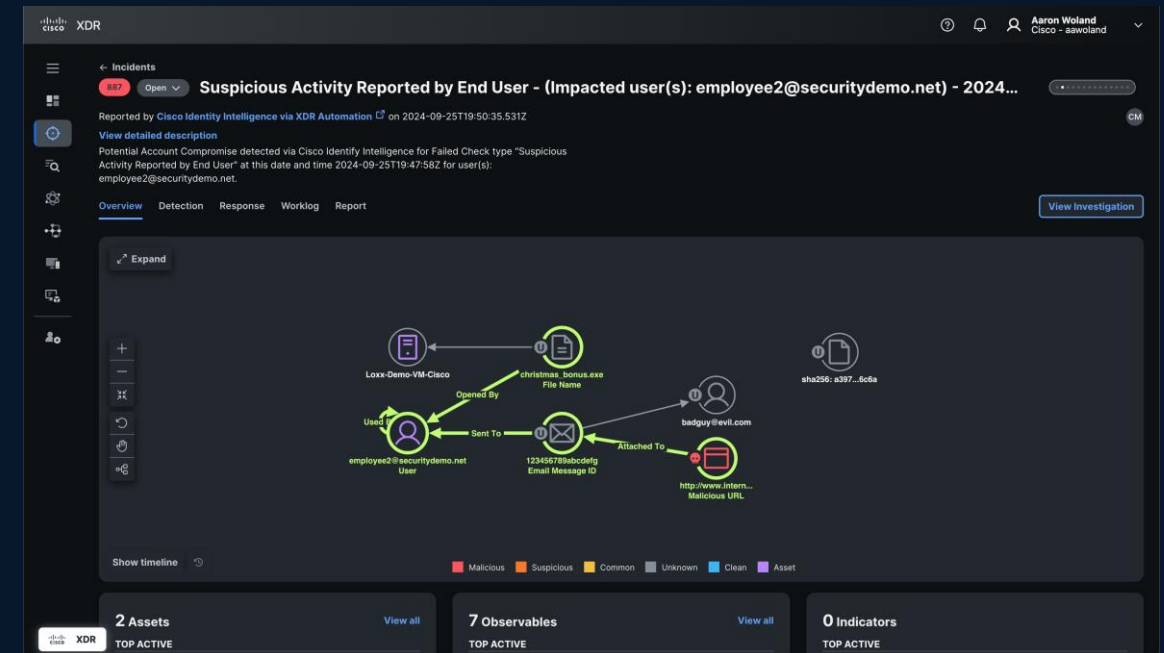
Merges with Incidents



- 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

Published in Exchange

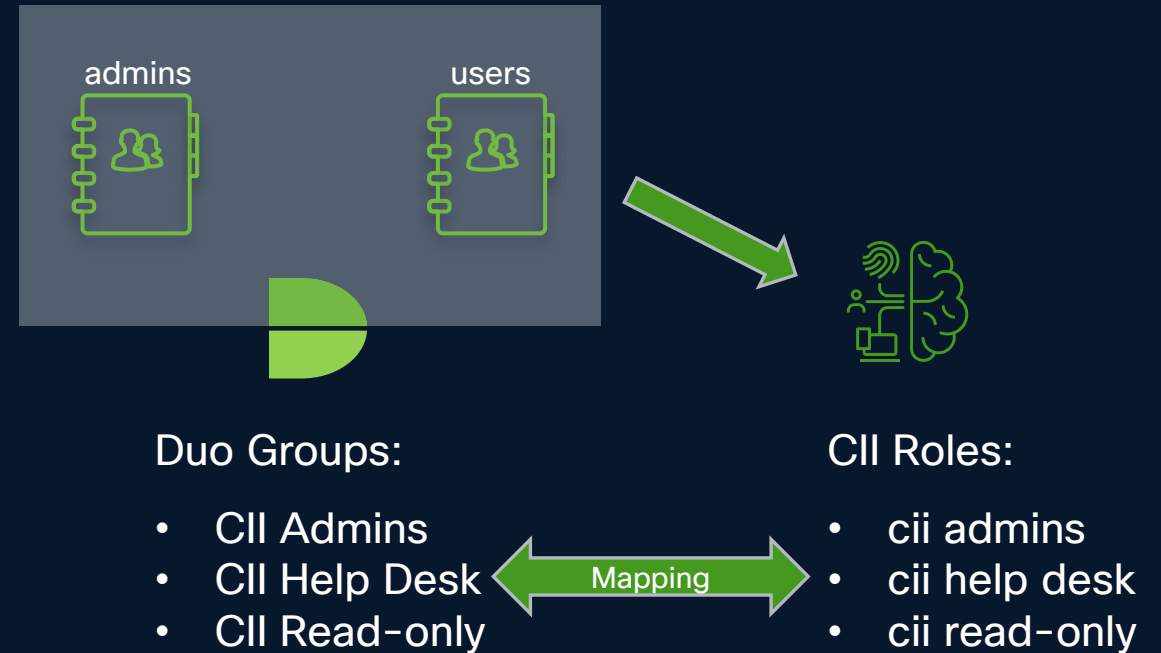
- A community-maintained XDR workflow.
- Takes the CII Webhook & parses it.
- Will enrich existing incidents, or none exist will create a new incident.



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.



The CII App is "owned" and Protected by Duo

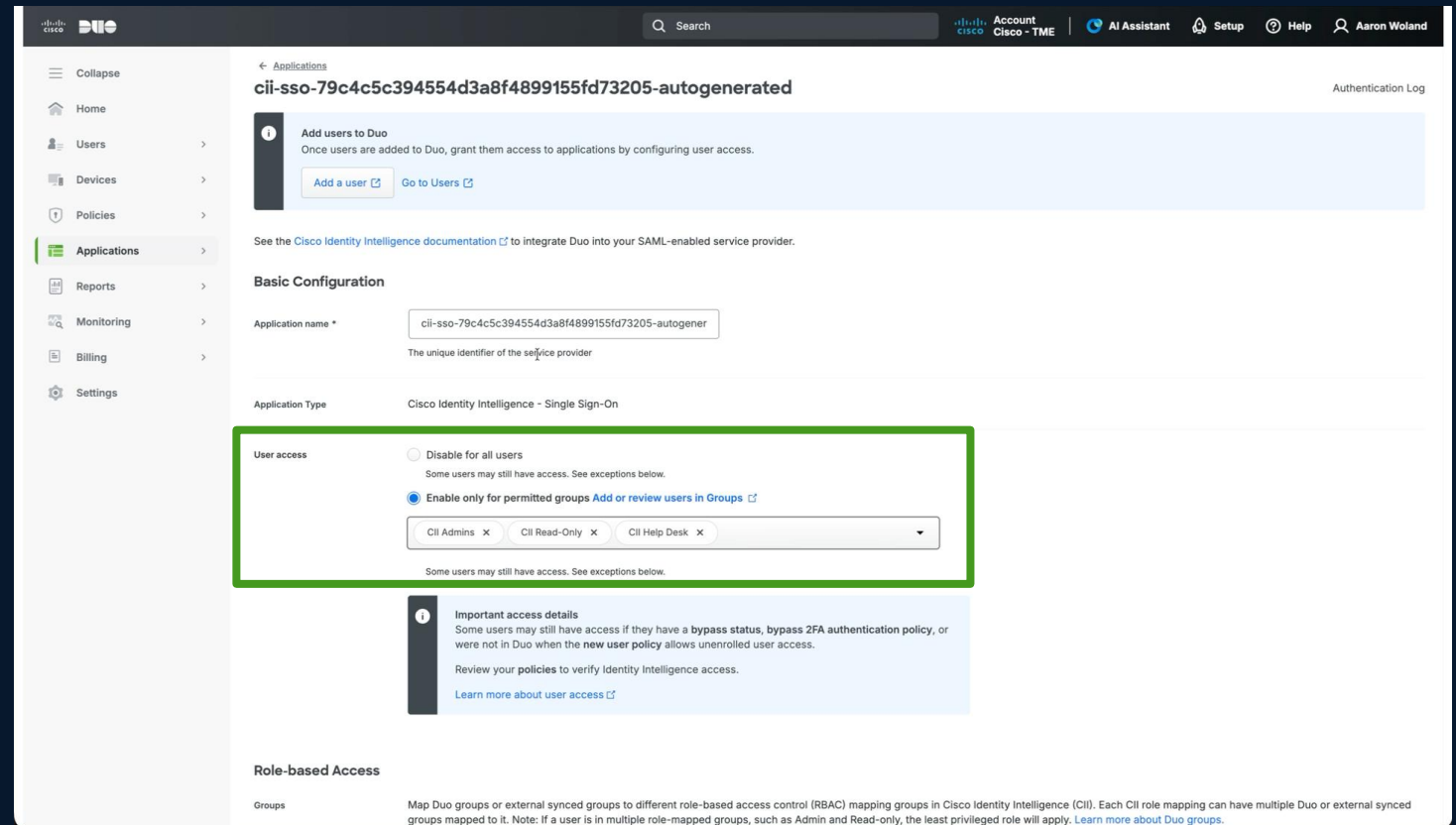
- You click to provision it
 - It is auto-provisioned if Duo is licensed at Advantage or above
 - So no need to do this step if you are licensed already.

Brand New Duo Tenant

The screenshot shows the Cisco Duo tenant dashboard. The top navigation bar includes the Cisco Duo logo, a search bar, and user information for Aaron Woland. The left sidebar contains navigation links: Collapse, Home, Users, Devices, Policies, Applications, Reports, Monitoring (highlighted), Billing, and Settings. The main content area is titled 'Monitoring' and 'Cisco Identity Intelligence'. It features a section titled 'Make identity your core security detection' with a description and a 'Learn more about Cisco Identity Intelligence' link. Below this, it states 'You'll need Duo Single Sign-On to launch your Cisco Identity Intelligence features. We found the following...' and lists 'CII Duo SSO'. A green box highlights the 'Connect to Cisco Identity Intelligence' button, with a green arrow pointing to it from the right. The footer contains copyright information and a 'Terms of service' link.

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



The screenshot displays the Cisco Duo console interface for configuring an application. The main content area is titled "Applications" and shows the configuration for "cii-sso-79c4c5c394554d3a8f4899155fd73205-autogenerated".

Key sections visible include:

- Add users to Duo:** A section with a blue background and a white box containing the text "Add users to Duo" and "Once users are added to Duo, grant them access to applications by configuring user access." Below this are two buttons: "Add a user" and "Go to Users".
- Basic Configuration:** A section with a white background and a light blue border. It contains the following fields:
 - Application name:** "cii-sso-79c4c5c394554d3a8f4899155fd73205-autogener" (The unique identifier of the service provider)
 - Application Type:** "Cisco Identity Intelligence - Single Sign-On"
- User access:** A section with a white background and a light blue border, highlighted with a green box. It contains the following options:
 - Disable for all users (Some users may still have access. See exceptions below.)
 - Enable only for permitted groups (Add or review users in Groups)Below these options is a dropdown menu showing "CII Admins", "CII Read-Only", and "CII Help Desk".
- Important access details:** A section with a blue background and a white box containing the text "Some users may still have access if they have a bypass status, bypass 2FA authentication policy, or were not in Duo when the new user policy allows unenrolled user access. Review your policies to verify Identity Intelligence access. Learn more about user access"
- Role-based Access:** A section with a white background and a light blue border. It contains the text "Map Duo groups or external synced groups to different role-based access control (RBAC) mapping groups in Cisco Identity Intelligence (CII). Each CII role mapping can have multiple Duo or external synced groups mapped to it. Note: If a user is in multiple role-mapped groups, such as Admin and Read-only, the least privileged role will apply. Learn more about Duo groups."

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

Role-based Access

Map Duo groups or external synced groups to different role-based access control (RBAC) mapping groups in Cisco Identity Intelligence. Note: If a user is in multiple role-mapped groups, such as Admin and Read-only, the least privileged role will apply.

CII role mapping	Duo groups
cii admins	CII Admins (0 users)
cii help desk	CII Help Desk (0 users)
cii read-only	CII Read-Only (0 users)

Custom attributes: Check this box if your Duo Single Sign-On configuration source uses non-standard attribute names.

Universal Prompt: [See Update Progress](#) (Progress updating across all applications.) [Get More Information](#) (Learn more about the new prompt experience.)

Activation complete. Application Supports Universal Prompt. [Get More Information](#)

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

Identity Intelligence

RBAC Groups

Create a group in your IdP to associate with each Identity Intelligence role and assign the appropriate permissions.

Admins group: cii admins

Helpdesk group (optional): cii help desk

Read-only group (optional): cii read-only

Application manager group (optional):

User manager group (optional):

Security analyst group (optional):

Please allow several minutes for the changes to be applied.

Save

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

The screenshot shows the user profile for 'crashtestdummy' in the Cisco Duo interface. The user is enrolled and has the following details:

- Device enrollment: ✔ Enrolled
- Username: crashtestdummy
- Display Name: Crash Test Dummy
- Email Address: crashtestdummy@aaron.demo
- Groups: CII Admins, CII Read-Only

A red box highlights the 'Groups' section, and a red line connects it to the text on the left. Below the groups, there is a note: 'Groups can be used for management, reporting, and policy. [Learn more about groups](#)'.

When user is a member of two groups for CII Roles

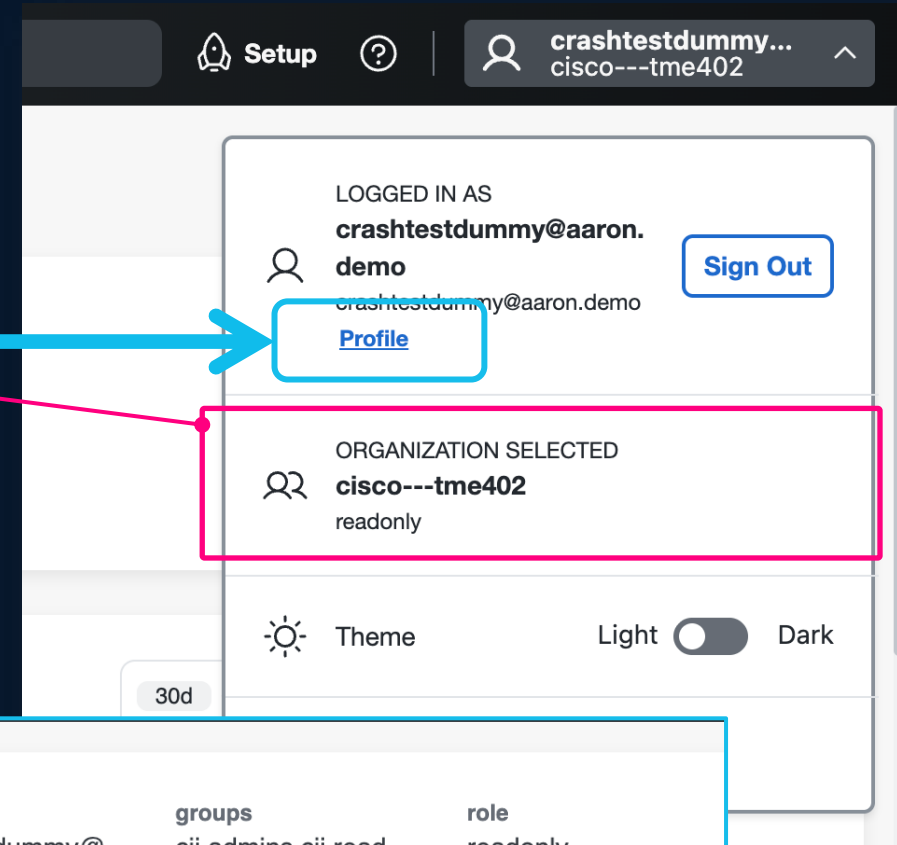
User: Crash Test Dummy


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.



	name crashtestdummy@...	email crashtestdummy@...	groups cii admins,cii read-only	role readonly
---	-----------------------------------	------------------------------------	---	-------------------------



Miscellaneous Technical Info

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

Check	# Falling	# Excluded	Report Channels
99% Sign in Threat Detected • Moderate End Users - Identity Threat Insight	1 133.3... increase since last ... 136... increase since last m...	0	Multiple Channels
99% Shared Mailbox Sign In Enabled • Low End Users - Identity Threat Insight	1 No change since last week No change since last month	0	+ Add
100% Active Account under Heavy Attack • Low End Users - Identity Threat Insight	0 No change since last week No change since last month	0	+ Add
100% Activity From Untrustworthy ISP • Moderate End Users - Identity Threat Insight	0 No change since last week No change since last month	0	+ Add
100% IP Threat Detected • Critical End Users - Identity Threat Insight	0 No change since last week No change since last month	0	+ Add
100% Users With Defined Email Forward R... • Moderate End Users - Compliance, Identity T...	0 No change since last week No change since last month	0	+ Add
100% Accounts With Unusually High Activity • Critical End Users - Identity Threat Insight	0 No change since last week No change since last month	0	+ Add
100% Successful Access from a Previously... • Moderate End Users - Identity Threat Insight	0 No change since last week No change since last month	0	+ Add

100% Activity From Untrustworthy ISP • Moderate End Users - Identity Threat Insight	0 No change since last week No change since last month	0	+ Add
100% IP Threat Detected • Critical End Users - Identity Threat Insight	0 No change since last week No change since last month	0	+ Add

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

The screenshot shows the 'Identity Intelligence' configuration interface. At the top, the Cisco logo and 'Identity Intelligence' are displayed. A left-hand navigation menu contains icons for home, dashboard, users, status, groups, and settings. The main content area is titled 'RBAC Groups' with a toggle switch that is turned on. Below the title, there is a descriptive text: 'Choose an IdP Group for each Identity Intelligence role. If this setting is no...'. There are three dropdown menus for selecting groups: 'Admins group' (selected: oort_admins), 'Helpdesk group (optional)' (selected: oort_helpdesk), and 'Read-only group (optional)' (selected: oort_ro). At the bottom right of the form are 'Cancel' and 'Save' buttons.

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!

The screenshot displays the Cisco Identity Intelligence Advanced Search interface. On the left, there are filters for Status (Active, Deleted, Deprovisioned, Disabled, Inactive, Inconsistent) and Sources (G-Suite-Loxx-TV, SecDemo-Okta, SecurityDemo-Azure, SecurityDemo-Slack, Securitydemo). The main area shows a list of users with columns for Name, Status, and Location. A modal window titled "Switch to advanced mode" is open, providing instructions on using Kibana Query Language (KQL) and a "Confirm" button. Below the modal, a table lists users with their status and location details.

Name	Status	Location
Accounting1	1	N/A
Accounting2	1	N/A
Adam Sonnenfeld	2	Gdynia, Pomorskie, PL
Aditya Sankar	✓	N/A
Ahmadreza Edalat	1	Milpitas, CA, US
Alex Dipasquale (aledipas)	1	Morrisville, NC, US
Alex Wight	1	N/A
Alex Zaslavsky	1	N/A
Alice Smith	3	San Francisco, California, US

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

The screenshot shows the Oort Knowledge Base documentation page for the Public API. The page is titled "Oort Knowledge Base" and has a navigation menu on the left with items: Home, Glossary, Best Practices, How-to Guides, Oort Insights, Integrations, Public API (selected), APIs, Troubleshooting & Support, and Release Notes. The main content area includes a list of instructions for using the API, a section titled "Using a Postman Collection" with a download button for "Cisco Identity Intelligence Public API.postman_collection.json" (11KB), and navigation links for "Report as a Service (RaaS)" and "Next APIs". The page is powered by GitBook and was last updated 14 days ago.

docs.oort.io/public-api

Oort Knowledge Base

Home
Glossary
Best Practices >
How-to Guides >
Oort Insights >
Integrations >
Public API >
APIs
Troubleshooting & Support >
Release Notes >

2. Extract the **access_token** from the response.
An access token is valid for 10 hours.
3. When invoking the public API requests set an **Authorization** header with the value
`Bearer <value of access_token >`

Using a Postman Collection

Import the attached Postman collection and follow the instructions in the collection **overview** tab.

11KB Cisco Identity Intelligence Public API.postman_collection.json

Previous
Report as a Service (RaaS) Next
APIs

Powered by GitBook

Last updated 14 days ago



Integrations Deep Dive

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	✗	✓	✓
Github	✗	✓	✓
AWS	✗	✓	✓
Google Workspace	✗	✓	✓
Workday	✗	✓	✗
Salesforce	✗	✓	partial
Auth0 (acquired by Okta)	✓	✓	✗
Manual Upload (CSV/JSON)	✗	✗	✗

¹ listed as notification, but also an identity source

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.

The screenshot displays the Cisco Identity Intelligence interface. On the left, a sidebar contains filter options: Status (Active, Deleted, Deprovisioned, Disabled), Sources (Duo - PosaaS, Loxx-Okta, SecDemo-EntraID, Slack - SecurityDemo.Net), User Type, Linked Users, Groups, Is Admin, Administrator of, MFA Configured, Factor Assurance Level, Factor Used, Factor Enabled Not In Use, Protected Population, and Has Tickets. The main area shows a search bar with filters: Sources:(3 conditions) AND, NOT Status:(3 conditions), Status:Active, and AND. Below the search bar, a table lists 17 users found. The table columns are: User, Checks, # IPs, # Logins, Last Seen (UTC), Last IP Address, Last Location, MFA, Providers, and Status. The Providers column is highlighted with an orange box, showing icons for various providers like Duo, Okta, and EntraID. The Status column shows 'Active' for all users.

User	Checks	# IPs	# Logins	Last Seen (UTC)	Last IP Address	Last Location	MFA	Providers	Status
Chris Murray chris@securitydemo.net	✓	2	1	8 Days Ago Apr 3, 2024 15:29:35	84.71.170.25	Harrow, England, GB	✓	🔌 ⚙️ 🔑	Active
Derrick Snider dersnide@securitydemo.net	1	2	1	7 Days Ago Apr 4, 2024 13:44:25	136.62.139.21	Austin, TX, US	✗	🔌 ⚙️ 🔑	Active
Donald Duck donald_duck@securitydemo.net	1	0	N/A	N/A	N/A	N/A	✗	🔌 ⚙️ 🔑	Active
Employee2 employee2@securitydemo.net	1	1	N/A	A Month Ago Mar 14, 2024 16:35:09	171.68.244.70	San Jose, CA, US	✗	🔌 ⚙️ 🔑	Active
EmployeeOne employee1@securitydemo.net	1	9	30	A Day Ago Apr 10, 2024 20:52:45	54.91.54.109	Ashburn, VA, US	✓	🔌 ⚙️ 🔑	Active
Loxx loxx@securitydemo.net	2	17	94	4 Hours Ago Apr 11, 2024 16:19:01	75.182.151.17	Waxhaw, NC, US	✓	🔌 ⚙️ 🔑 🌐	Active
Matt Vander Horst matt@securitydemo.net	1	3	25	6 Days Ago Apr 5, 2024 15:42:48	71.234.238.50	South Hadley, MA, US	✓	🔌 ⚙️ 🔑	Active
Patrick Cardot pcardot@securitydemo.net	1	2	1	A Day Ago Apr 10, 2024 20:03:30	37.65.38.86	Douchy-les-Mines, Hauts-de-Fra...	✗	🔌 ⚙️ 🔑	Active
Paul Carco carco@securitydemo.net	2	4	7	2 Days Ago Apr 9, 2024 20:35:01	173.38.117.65	Cary, NC, US	✓	🔌 ⚙️ 🔑	Active

Users

Summary

- Inconsistent, Active
- Just a Number
- Human Labor
- SecurityDemo
- N/A
- MFA Configured
- Apr 11, 2024 23:57:13 UTC (14 hours ago)
- N/A

Created May 22, 2019

Checks

1 failing

User Has Directly Assigned Application

Attempted Logins

60 All Attempts

- Success - 47
- Denied - 10
- Other - 3

Records per day

Success Denied Other

Activity Flow over the past 30 days

employee1@securitydemo.net

SecDemo-EntralD

Washington, VA, US

Ashburn, VA, US

Singapore, Central Singapore, SG

San Francisco, CA, US

OfficeHome

Office365 Shell WCSS-Client

IdentityProtection

Office 365 Exchange Online

SSO

Bing

unlikelyTravel

anomalousToken

unfamiliarFeatures

Authentication Factors

Factor	Assurance Level	Status	# Changes	Usage Count	Device	Phone Number	Last Used
Password SecDemo-EntralD	Low	ACTIVE	0	5	N/A	N/A	Apr 11, 2024
Push Duo - PosasS DPJBG7.WSHOSY1VWHNSN_push	Medium	ACTIVE	0	4	ATW iPhone10	N/A	Mar 16, 2024

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



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

Identity Intelligence | Search | loxx@securitydemo.net | security-demo-int

Users > **employee1@securitydemo.net**

EmployeeOne | 1 Linked User | Active | Overview | **Activity** | Networks | Devices | Applications | Groups | Checks 2 | Actions

Remediation Triggered by loxx@securitydemo.net on Apr 23, 2024 18:25:13 UTC with status **FAILURE** | View all

Search application, outcome, location, IP, etc. | <> Advanced | 30d Mar 27, 2024 13:55 - Apr...

Activity Timeline: A bar chart showing activity from 03/27 to 04/26. A tooltip for Apr 23 shows **FAILURE: 3**.

126 events found | Last data collection

Date (UTC)	Source	Event	Initiator	Target	Result
Apr 26, 2024 00:43:43	Cisco	END_USER__CHECK_EXPIRED	System	Check: A Bypass Code Was U... User: employee1@securityde...	Info
Apr 24, 2024 19:43:17	OfficeHome	sso	employee1@securitydemo.net	OfficeHome User: employee1@securityde...	Success
Apr 24, 2024 17:11:09	OfficeHome	sso	employee1@securitydemo.net	OfficeHome User: employee1@securityde...	Success

Networks



The screenshot shows the Cisco Identity Intelligence interface for user **EmployeeOne** (employee1@securitydemo.net). A remediation alert is visible, triggered on Apr 23, 2024, with a status of **FAILURE**. Below the alert is a search bar for IP addresses and a table titled "14 IP Addresses".

IP Address	Last Access (UTC)	Hit Count	Successful Events	Failed Events	Other Events	Tags	Location
54.91.54.109	Apr 25, 2024 19:38:19	24	24	0	0		Ashburn, VA, US
172.203.228.226	Apr 18, 2024 17:50:41	18	10	1	7		Washington, VA, US
20.51.250.58	Apr 24, 2024 17:11:09	14	10	4	0		Washington, VA, US
128.107.78.71	Apr 12, 2024 00:08:15	7	7	0	0		San Francisco, CA, US
85.203.21.87	Apr 12, 2024 07:00:56	5	2	3	0		Singapore, Central Singapore, ...
154.16.95.37	Apr 20, 2024 02:47:10	3	2	1	0		Johannesburg, Gauteng, ZA
193.176.211.235	Apr 16, 2024 15:09:57	3	3	0	0		Aberdeen, Hong Kong, HK
154.16.95.18	Apr 18, 2024 19:17:42	1	0	1	0		ZA

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.

Identity Intelligence

EmployeeOne (1 Linked User) - Active

Remediation: Triggered by loxx@securitydemo.net on Apr 23, 2024 18:25:13 UTC with status FAILURE

14 devices found

Device	Source	OS	Managed	Registered	Usage Count	Enrolled (UTC)	Last Seen (t
Access and Authentication devices							
EPJPCXC18SO57X3G4J0G	Duo - PosaaS	iOS 15.7	✗	✓	N/A		
EPTFXOBY41570W7UW9OR	Duo - PosaaS	iOS 16.7.6	✗	✓	N/A		
EPWQ1HG7NCQ5UYST8BR5	Duo - PosaaS	iOS 16.7.6	✗	✓	N/A		
AAWOLAND-M-W1J9	Duo - PosaaS	Mac Os 14.3.1	✓	✓	N/A		
ATW-LABSTINKPAD	Duo - PosaaS	Windows 10.0.19044.2728	✓	✓	N/A		
MJOHARI-M-2XK7	Duo - PosaaS	Mac Os 14.3.1	✗	✓	N/A		
SSAKLIKA-M-X2WT	Duo - PosaaS	Mac Os 14.3.1	✓	✓	N/A		

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.

The screenshot displays the Cisco Identity Intelligence interface for a user named 'EmployeeOne'. The page is divided into several sections:

- Header:** Cisco Identity Intelligence, search bar, and user profile 'Loxx security-demo-int'.
- User Profile:** 'EmployeeOne' (employee1@securitydemo.net), 1 Linked User, Active status. Navigation tabs: Overview, Activity, Networks, Devices, Applications (selected), Groups, Checks (2), Actions.
- Remediation:** A notification triggered by loxx@securitydemo.net on Apr 23, 2024 18:25:13 UTC with status FAILURE.
- Applications usage:** A donut chart showing 13 All Apps, with 7 Used (green) and 6 Not Used (yellow).
- Applications usage over time:** A bar chart showing usage counts from 03/26 to 04/24.
- Median apps per user:** A horizontal bar chart comparing 'All Users' (median ~2), 'Same Manager' (median ~4), 'Same Department' (median ~5), and 'This User' (median ~6).
- Application List Table:**

Name	Source	Status	Assignments	Owners	Usage Count	Last Access (UTC)	Result
OfficeHome employee1@securitydemo.net	SecDemo-EntralID			N/A	51	Apr 24, 2024 19:43:17	Success
Office365 Shell WCSS-Client employee1@securitydemo.net	SecDemo-EntralID			N/A	18	Apr 24, 2024 17:11:09	Success
Office 365 Exchange Online employee1@securitydemo.net	SecDemo-EntralID			N/A	6	Apr 24, 2024 17:10:59	Success
Duo Central							Success

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 ownership of that portion on the vendor directly

A screenshot of the Oort Knowledge Base website. The page title is "Microsoft Entra ID (Azure AD) Data Integration" with a date of "11/2023". The left sidebar contains a navigation menu with categories like Home, Glossary, Best Practices, How-to Guides, Oort Insights, and Integrations. Under Integrations, "Microsoft Entra ID (Azure AD) Data Integration" is highlighted. The main content area has an "Overview" section explaining that Oort's platform can analyze authentication events in Microsoft Entra ID (Azure AD) to provide insights. It also includes an "Important Notes" section with two bullet points: one about SSO integration and another about enabling a subscription for new tenants. A "Next Steps" section mentions a review process. The "Entr ID Integration" section is partially visible at the bottom. The footer of the page includes "Powered by GitBook" and "Cisco Integration Network".

View Logs



Identity Intelligence

Search

loxx@securityde... security-demo-int

Integrations

Request Integration + Add Integration

Providers

Name ↓	Collection Status ↑	Recent Usage	Average Traffic	Last Collected (UTC)	Last Updated (UTC)
Duo - PosaaS	Collecting View Logs		13 records	Apr 18, 2024 19:27:50	
Loxx-Okta	Success Traffic detected		22 records	Apr 18, 2024 19:26:53	
SecDemo-EntralD	Collecting View Logs		18259 records	Apr 18, 2024 19:26:53	
Slack - SecurityDemo.Net	Success Traffic detected		7 records	Apr 18, 2024 19:26:53	Apr 3, 2024 00:57:00
loxx.tv	Success Traffic detected		5 records	Apr 18, 2024 18:57:09	Apr 3, 2024 00:42:05

Menu for SecDemo-EntralD:

- Edit Settings
- Test Connectivity
- Collect Now
- Disable Collection
- View Logs
- Delete

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.

The screenshot displays the Cisco Identity Intelligence interface for viewing system logs. The top navigation bar includes the Cisco logo, the text "Identity Intelligence", a search bar, and a user profile for "loxx@secu security-de". A "For Your Reference" icon is visible in the top right corner.

The main content area is titled "Integrations > System Logs" and features a search bar with the query "Target:Duo - PosaaS" and a "View all" button. Below this, a table lists 1722 events. The table columns are: Date (UTC), Event, Initiator, Target, Result, and Logged By. A red arrow points to the "Event Family" filter in the left sidebar, which is currently set to "Integrations".

Date (UTC)	Event	Initiator	Target	Result	Logged By
Apr 18, 2024 19:28:00 Ended in 0h 0m 1s	INTEGRATION__HISTORICA...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:28:00 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:59 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:59 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:57 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:56 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:53 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:52 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:50	INTEGRATION__COLLECTION	System	Duo - PosaaS	Started	cnt-integration
Apr 18, 2024 19:27:49 Ended in 0h 0m 0s	Mutation__triggerDataC...	loxx@securitydemo.net admin	Duo - PosaaS	Info	cnt-integration
Apr 18, 2024 19:27:02 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:02 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:02 Ended in 0h 0m 3s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:26:42 Ended in 0h 0m 50s	INTEGRATION__EVENTS__C...	System	Duo - PosaaS	Success	cnt-integration

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.

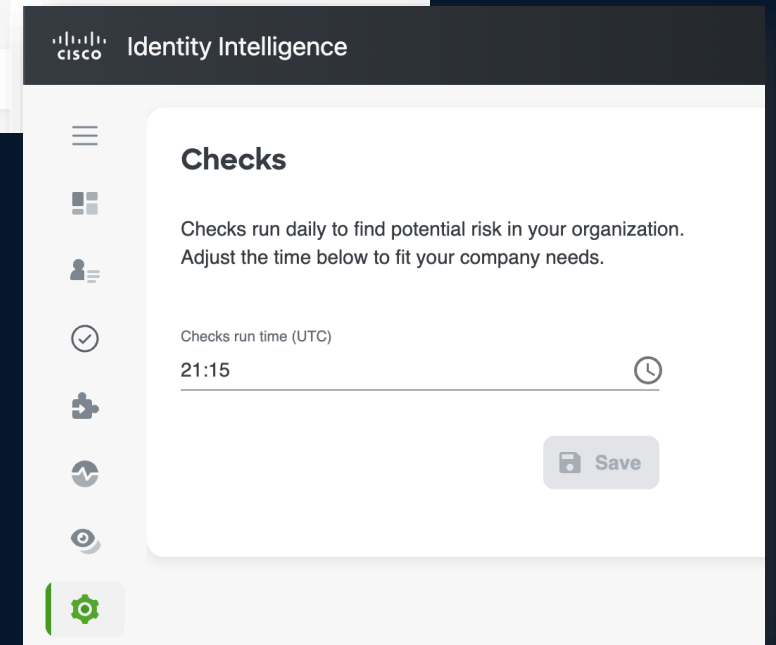
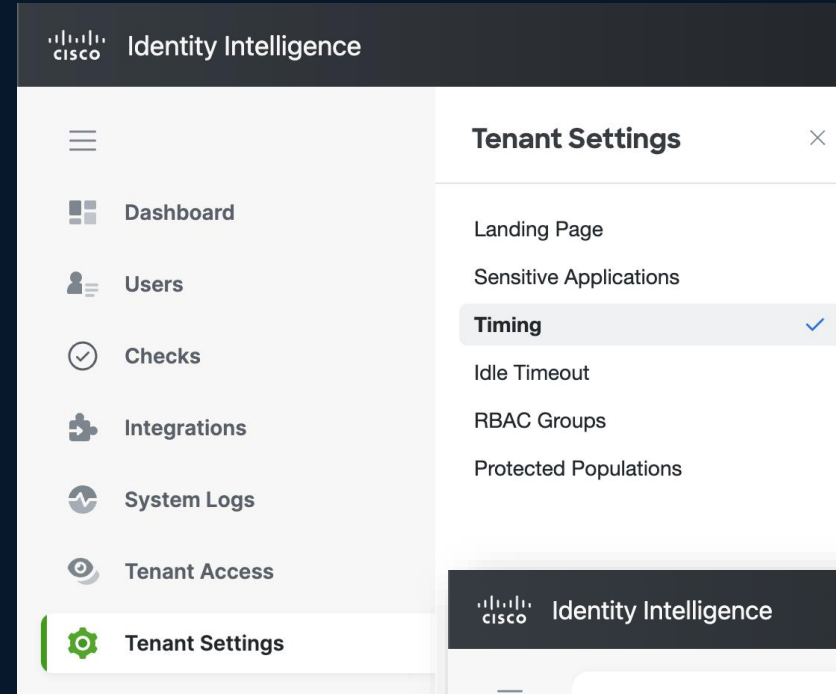
You can click in & leverage progressive disclosure to view the raw log, too.

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

The screenshot displays the Cisco Identity Intelligence 'System Logs' interface. On the left, a sidebar contains a filter menu with categories like 'Result' (Blocked, Failure, Info, None, Partial success, Started, Success, Timeout), 'Event Family' (Integrations, User checks, Admin triggered), and 'Check Actions Taken'. A red arrow points from the 'Event Family' section to the main log list. The main area shows a table of 1722 events with columns for Date (UTC) and Event. A yellow arrow points from the 'Event' column to a detailed view on the right. This view shows a successful event from Apr 18, 2024, 19:28:00 UTC. The event details include: End Date, Running Time (0h 0m 1s), Event (INTEGRATION__HISTORICAL_COLLECTION), Initiator (system), Logged By (cnt-integration-sfn-historical-data-collection), Integration Target (Duo - PosaaS), Sfn Id (3ba3bb18-0238-4bef-b03f-4aa6a7ea1576), Execution Arn, and Execution History. The Execution History section is expanded to show metadata (httpStatusCode: 200, requestId, attempts: 1, totalRetryDelay: 0) and event details (id: 51, previousEventId: 50, taskStartedEventDetails, inputDetails). The input details show integrationInstanceId and tenantId. A 'For Your Reference' icon is visible in the top right corner.

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

The screenshot shows the Cisco Identity Intelligence 'Integrations' page. The 'Providers' section contains a table with the following data:

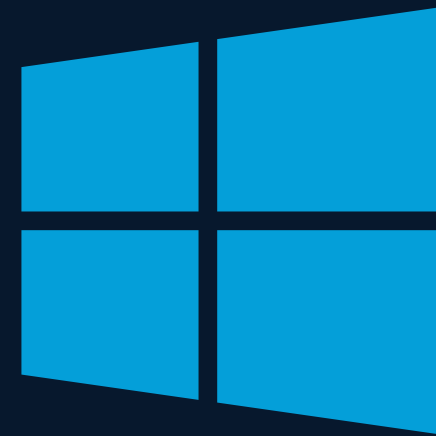
Name	Collection Status	Recent Usage	Average Traffic	Last Collected (UTC)	Last Updated (UTC)
Duo - PosaaS	Collecting	[Line graph]	3 records	Jun 1, 2024 22:14:51	Apr 22, 2024 13:37:22
Loxx-Okta	Success Traffic detected	[Line graph]	13 records	Jun 1, 2024 21:26:53	Apr 29, 2024 01:51:30
SecDemo-EntraID	Success Traffic detected	[Line graph]	33139 records	Jun 1, 2024 21:27:...	
Slack - SecurityDemo...	Success Traffic detected	[Line graph]	13 records	Jun 1, 2024 21:24:...	
loxx.tv	Success Traffic detected	[Line graph]	0 records	Jun 1, 2024 21:56:...	

A dropdown menu is open for the 'Slack - SecurityDemo...' integration, showing the following options:

- Edit Settings
- Test Connectivity
- Collect Now (highlighted with a red arrow)
- Disable Collection
- View Logs
- Delete



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

Microsoft Azure Search resources, services, and docs (G+)

Home > App registrations





+ New registration Endpoints Troubleshooting Refresh Download Preview features Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications **Owned applications** Deleted applications

Start typing a display name or application (client) ID to filter these r... Add filters

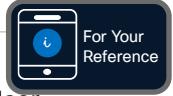
4 applications found

Display name ↑↓	Application (client) ID	Created on ↑↓	Certificates & secrets
 Cisco XDR	3891ab18-5d91-4960-a5e6-bc24...	7/23/2021	✓ Current
 Kenna Integration	1b6aa786-ba19-43f5-821b-6d141...	1/9/2024	✓ Current
 Oort	07ef51a6-8052-4cc4-a5d8-dedaa...	6/15/2023	✓ Current
 SecureX INventory Integration - Delete Me	fdceec30-bdc6-46f6-afa3-265f95...	3/22/2021	✓ Current

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



Microsoft Azure Search resources, services, and docs (G+)

Home > App registrations





+ New registration | Endpoints | Troubleshooting | Refresh | Download | Preview features | Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications | **Owned applications** | Deleted applications

Start typing a display name or application (client) ID to filter these r... Add filters

4 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
 Cisco XDR	3891ab18-5d91-4960-a5e6-bc24...	7/23/2021	Current
 Kenna Integration	1b6aa786-ba19-43f5-821b-6d141...	1/9/2024	Current
 Oort	07ef51a6-8052-4cc4-a5d8-dedaa...	6/15/2023	Current
 SecureX INventory Integration - Delete Me	fdceec30-bdc6-46f6-afa3-265f95...	3/22/2021	Current

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

Identity Intelligence

Search

loxx@ security For Your Reference

Integrations > Edit Settings

Edit Microsoft Entra ID Settings

General Settings | Event Streaming | Advanced Settings

Name
SecDemo-EntraID

Directory ID
[REDACTED] #

Application ID
07ef51a6-8052-4cc4-4-[REDACTED] #

[Reset Credentials](#)

? The reset button will delete your current credentials and you will need to provide new ones.
If you need help getting your credentials, see the [Microsoft Entra ID Documentation](#)

[Cancel](#) [Save](#)

Where can I see a step by step configuration guide? ^

Refer to [this documentation article](#) for a step by step guidance.

Are Directory ID and Tenant ID the same thing? v

Where do I get my Application ID? v

How do I get my Application Secret Value? v

© 2024 Identity Intelligence

This environment reloads hourly

[Privacy Policy](#) [Terms of Use](#) [Documentation](#) [SOC2 Report](#)

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)

The screenshot displays the Cisco Identity Intelligence (CII) interface for editing Microsoft Entra ID settings. The main content area is titled "Edit Microsoft Entra ID Settings" and is divided into three tabs: "General Settings", "Event Streaming" (which is selected and highlighted with a yellow border), and "Advanced Settings".

Under the "Event Streaming" tab, the following configuration options are visible:

- Use EventHub for Logs Streaming
- EventHub Name: loxx-cii-[REDACTED]
- Consumer Group: \$Default
- Endpoint FQDN: [REDACTED].servicebus.windows.net
- Shared Access Key Name: ListenPolicy-Loxx

At the bottom of the configuration area, there is a "Reset Credentials" button and "Cancel" and "Save" buttons.

On the right side of the interface, there is a "Where can I see a step by step configuration guide?" section with a dropdown arrow. Below it, there is a "Refer to [this documentation article](#) for a step by step guidance." section. Further down, there are three more dropdown menus with the following text:

- Are Directory ID and Tenant ID the same thing?
- Where do I get my Application ID?
- How do I get my Application Secret Value?

The footer of the page includes the copyright notice "© 2024 Identity Intelligence", the text "This environment reloads hourly", and links for "Privacy Policy", "Terms of Use", "Documentation", and "SOC2 Report".

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.

Identity Intelligence

Search

loxx@ security For Your Reference

Integrations > Edit Settings

Edit Microsoft Entra ID Settings

General Settings Event Streaming **Advanced Settings**

Data Types

Check all of the data types you want this integration instance to get. You can update this at any time. The more types you enable, the more detailed the generated reports will be.

<input checked="" type="checkbox"/> Users	<input checked="" type="checkbox"/> Devices ⚠	<input checked="" type="checkbox"/> Event Logs ⚠
<input checked="" type="checkbox"/> Audit Logs ⚠	<input checked="" type="checkbox"/> MFA Factors ⚠	<input checked="" type="checkbox"/> Groups
<input checked="" type="checkbox"/> Applications	<input checked="" type="checkbox"/> Groups to Users	<input checked="" type="checkbox"/> Applications to Users
<input checked="" type="checkbox"/> Applications to Groups	<input checked="" type="checkbox"/> Named Locations	<input checked="" type="checkbox"/> Direct Reports
<input checked="" type="checkbox"/> Directory Roles	<input checked="" type="checkbox"/> Service Principal	<input checked="" type="checkbox"/> Risky User Events ⚠
<input checked="" type="checkbox"/> Authenticators to Users ⚠	<input checked="" type="checkbox"/> Conditional Access Policy	<input checked="" type="checkbox"/> Provisioning Events ⚠
<input checked="" type="checkbox"/> Device Audit Events ⚠	<input checked="" type="checkbox"/> Mailbox Settings ⚠	<input checked="" type="checkbox"/> Message Rules ⚠
<input checked="" type="checkbox"/> Risky Users ⚠	<input checked="" type="checkbox"/> Registered Devices	

Requires Microsoft Entra ID (formerly Azure AD) Premium P2 subscription

Cancel Save

Where can I see a step by step configuration guide? ^

Refer to [this documentation article](#) for a step by step guidance.

Are Directory ID and Tenant ID the same thing? v

Where do I get my Application ID? v

How do I get my Application Secret Value? v

© 2024 Identity Intelligence

This environment reloads hourly

[Privacy Policy](#) [Terms of Use](#) [Documentation](#) [SOC2 Report](#)



Okta Identity Engine

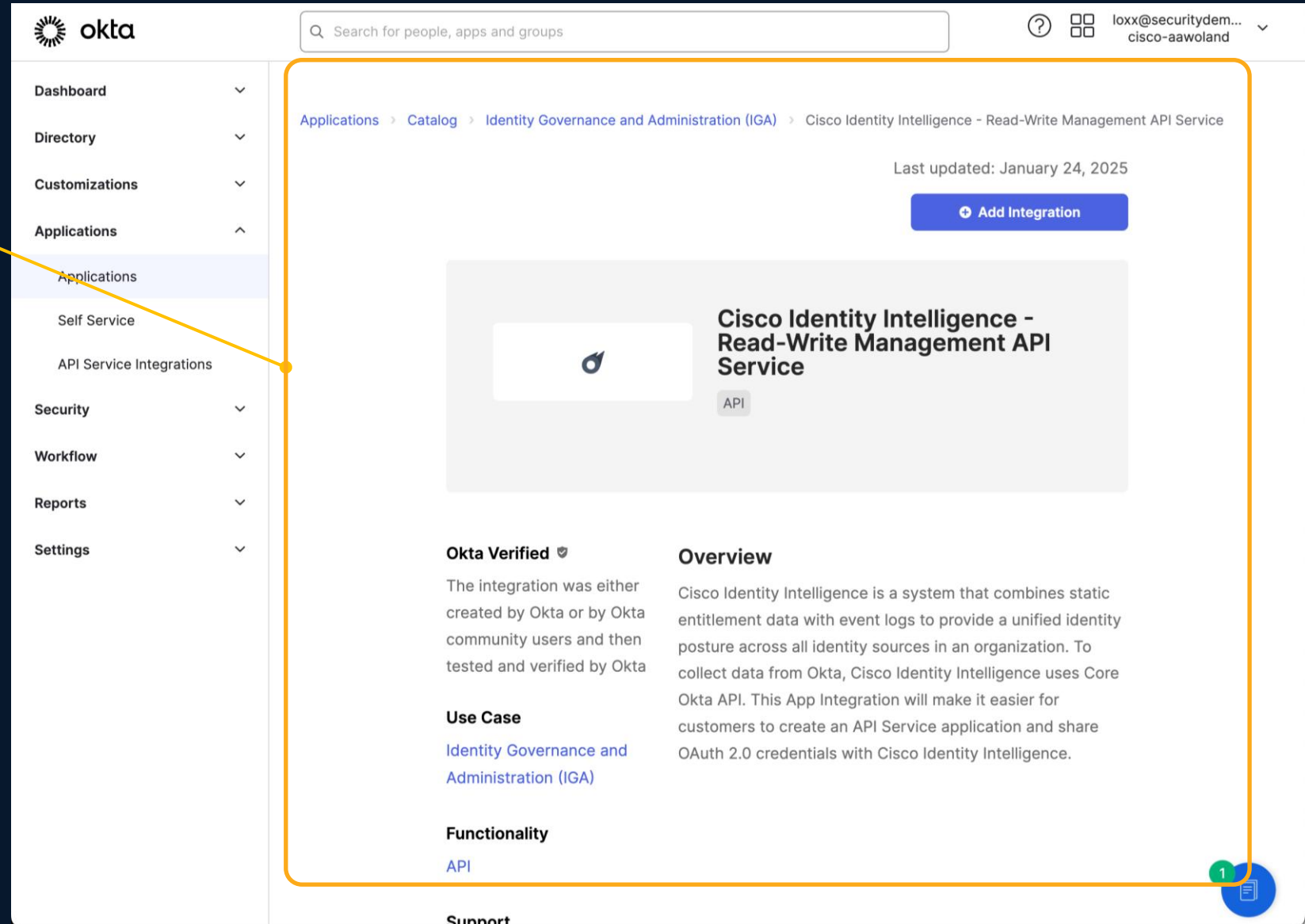


okta

App Catalog

CII is an app in the Okta Catalog

- Sets up all the permissions
- Makes the integration dead-simple



okta


Search for people, apps and groups

loxx@securitydem...
cisco-aawoland


Applications > Catalog > Identity Governance and Administration (IGA) > Cisco Identity Intelligence - Read-Write Management API Service

Last updated: January 24, 2025

[+ Add Integration](#)

 **Cisco Identity Intelligence - Read-Write Management API Service**

API

Okta Verified 

The integration was either created by Okta or by Okta community users and then tested and verified by Okta

Use Case

[Identity Governance and Administration \(IGA\)](#)

Functionality

[API](#)

Overview

Cisco Identity Intelligence is a system that combines static entitlement data with event logs to provide a unified identity posture across all identity sources in an organization. To collect data from Okta, Cisco Identity Intelligence uses Core Okta API. This App Integration will make it easier for customers to create an API Service application and share OAuth 2.0 credentials with Cisco Identity Intelligence.

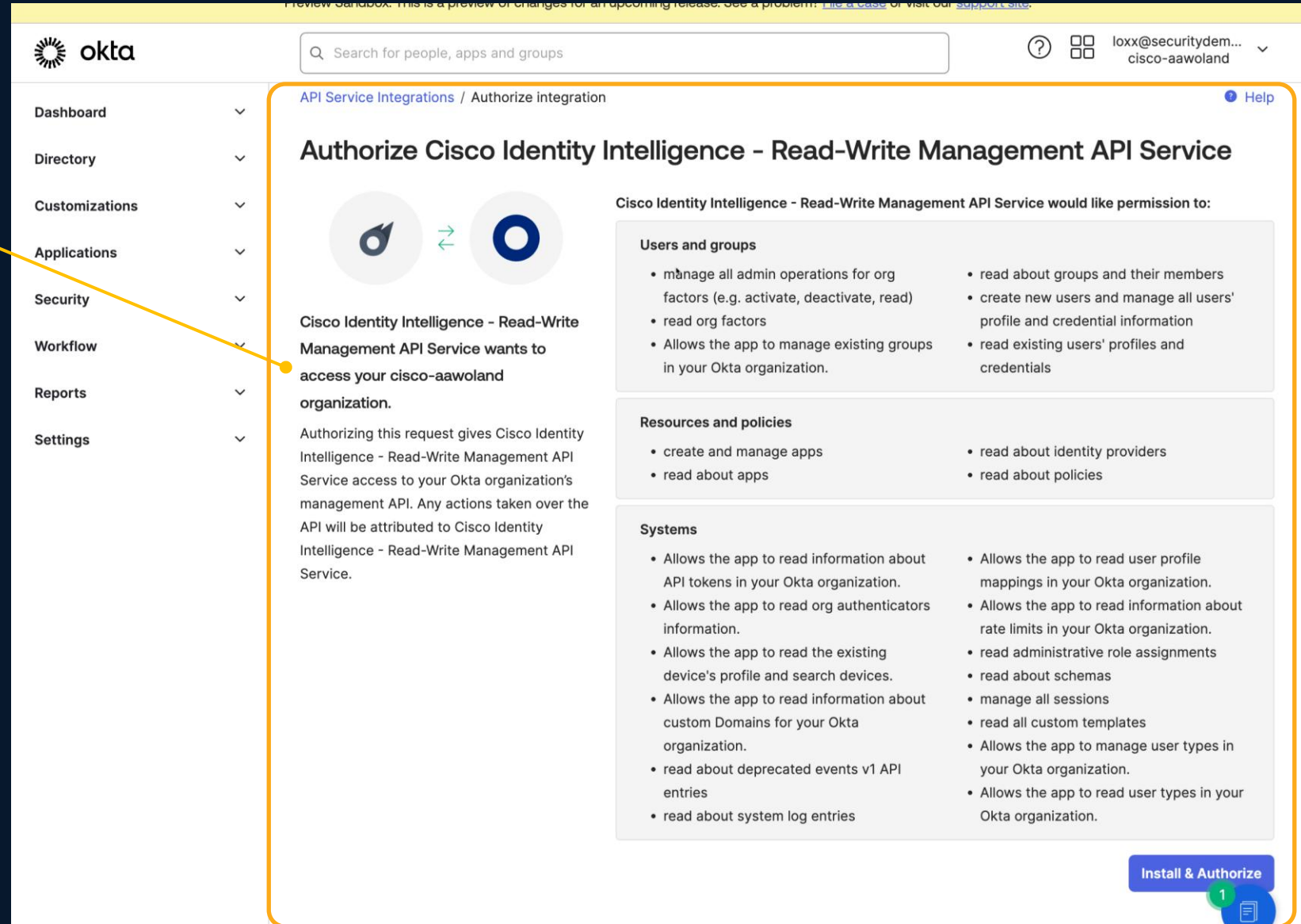
Support

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.



Review Sandbox: This is a preview of changes for an upcoming release. See a problem? [File a case](#) or visit our [support site](#).

okta Search for people, apps and groups iolxx@securitydem... cisco-aawoland

API Service Integrations / Authorize integration Help

Authorize Cisco Identity Intelligence - Read-Write Management API Service

Cisco Identity Intelligence - Read-Write Management API Service wants to access your cisco-aawoland organization.

Authorizing this request gives Cisco Identity Intelligence - Read-Write Management API Service access to your Okta organization's management API. Any actions taken over the API will be attributed to Cisco Identity Intelligence - Read-Write Management API Service.

Cisco Identity Intelligence - Read-Write Management API Service would like permission to:

- Users and groups**
 - manage all admin operations for org factors (e.g. activate, deactivate, read)
 - read org factors
 - Allows the app to manage existing groups in your Okta organization.
 - read about groups and their members
 - create new users and manage all users' profile and credential information
 - read existing users' profiles and credentials
- Resources and policies**
 - create and manage apps
 - read about apps
 - read about identity providers
 - read about policies
- Systems**
 - Allows the app to read information about API tokens in your Okta organization.
 - Allows the app to read org authenticators information.
 - Allows the app to read the existing device's profile and search devices.
 - Allows the app to read information about custom Domains for your Okta organization.
 - read about deprecated events v1 API entries
 - read about system log entries
 - Allows the app to read user profile mappings in your Okta organization.
 - Allows the app to read information about rate limits in your Okta organization.
 - read administrative role assignments
 - read about schemas
 - manage all sessions
 - read all custom templates
 - Allows the app to manage user types in your Okta organization.
 - Allows the app to read user types in your Okta organization.

Install & Authorize 1

Integrations > Add Integration > Okta
New Okta Integration


General Settings Event Streaming Advanced Settings

Name

Issuer

Client ID

Client Secret


 To ensure security, always use the least privileged integration

Cancel

 Connect

Where can I see a step by step configuration guide? 

How do I create an OAuth2 integration? 

What are the Okta Event Hooks? 

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

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

Identity Intelligence

Search

loxx@security For Your Reference

Integrations > Edit Settings

Edit Okta Settings

General Settings **Event Streaming** Advanced Settings

Use Logs Streaming

If you need help configuring Log Streaming, refer to [this documentation article](#).
Use the following values in your Okta instance:

AWS Event Source Name
4e384 [REDACTED]

AWS Account ID
22754 [REDACTED]

AWS Region
US East (Ohio)

I have configured Log Streaming in Okta with the above data

Cancel Save

Where can I see a step by step configuration guide? ^

Refer to [this documentation article](#) for a step by step guidance.

How do I create an Okta API Token? v

Which API Key should I use? v

What are the Okta Event Hooks? v

© 2024 Identity Intelligence

This environment reloads hourly

[Privacy Policy](#) [Terms of Use](#) [Documentation](#) [SOC2 Report](#)

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.

Identity Intelligence

Search

loxx@ security For Your Reference

Integrations > Edit Settings

Edit Okta Settings

General Settings Event Streaming **Advanced Settings**

Data Types

Check all of the data types you want this integration instance to get. You can update this at any time. The more types you enable, the more detailed the generated reports will be.

<input checked="" type="checkbox"/> Users	<input checked="" type="checkbox"/> Event Logs	<input checked="" type="checkbox"/> Identity Providers
<input checked="" type="checkbox"/> MFA Factors	<input checked="" type="checkbox"/> Groups	<input checked="" type="checkbox"/> Applications
<input checked="" type="checkbox"/> Groups to Users	<input checked="" type="checkbox"/> Applications to Users	<input checked="" type="checkbox"/> Applications to Groups
<input checked="" type="checkbox"/> Policies	<input checked="" type="checkbox"/> API Tokens	<input checked="" type="checkbox"/> Devices ⚠
<input checked="" type="checkbox"/> Policy Rules ⚠	<input checked="" type="checkbox"/> Authenticators ⚠	<input checked="" type="checkbox"/> Authenticators to Users ⚠
<input checked="" type="checkbox"/> User Schema ⚠	Requires Okta Identity Engine	

Requires Org Admin permissions

Cancel Save

Where can I see a step by step configuration guide? ^

Refer to [this documentation article](#) for a step by step guidance.

How do I create an Okta API Token? v

Which API Key should I use? v

What are the Okta Event Hooks? v

© 2024 Identity Intelligence

This environment reloads hourly

[Privacy Policy](#) [Terms of Use](#) [Documentation](#) [SOC2 Report](#)

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 Live !

