



Identity Intelligence Demystified

Technical deep dive into CII (formerly Oort)

Aaron T Woland - CCIE #20113

Distinguished Engineer, Security

loxx@cisco.com |  @aaronwoland |  aaronwoland

BRKSEC-2162

CISCO *Live!*

\$ whoami



Cisco role: Distinguished Engineer, Security

Unofficial title:
“Cisco History Professor”

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

Fun fact 1: Father of 5 daughters

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

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

Sarcasm

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



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

Please fill out the survey



Drop your email in the comments – I WILL respond!

Cisco Webex App

Questions?

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

How

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

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

CISCO *Live!*

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



Agenda

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

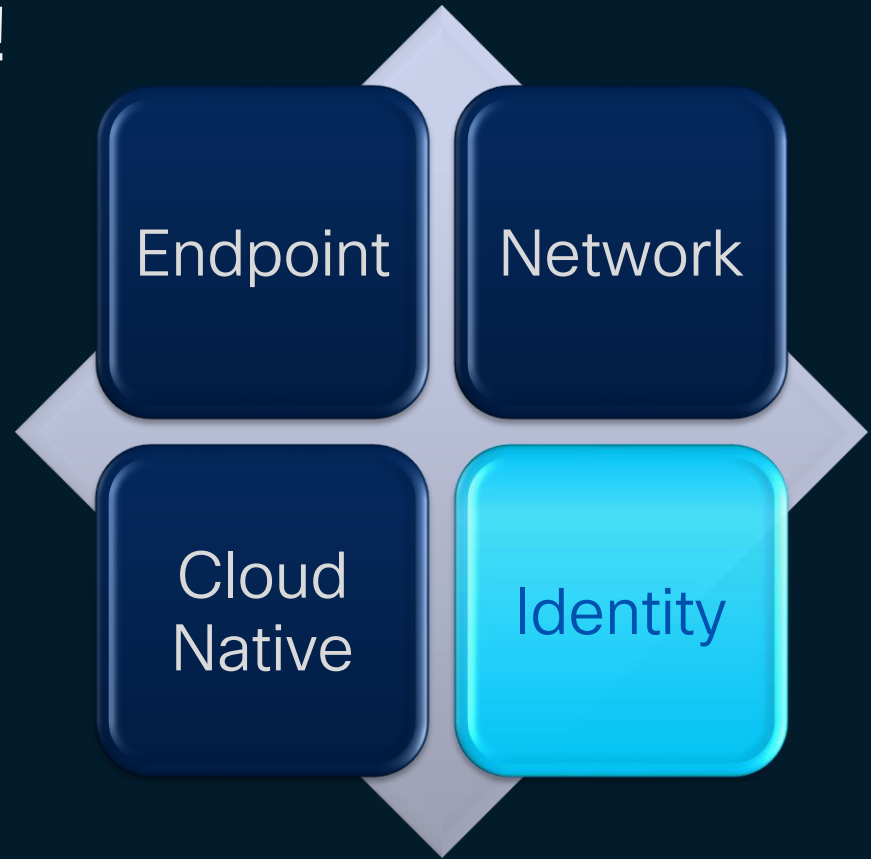
Prevention is not enough!

Endpoint Detection & Response

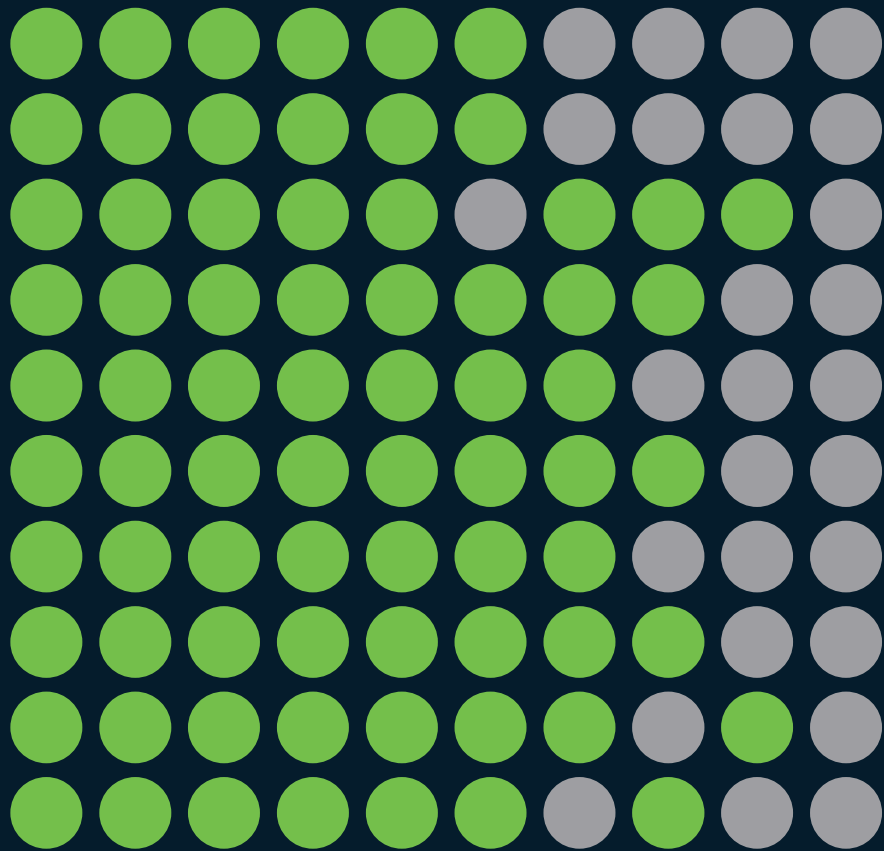
Network Detection & Response

Cloud Native Detection &
Response

Identity Threat Detection &
Response



*Identity has
become the
attack surface*



80%

of breaches leveraged
identity as a key component

Cisco Talos Incident Response Data 2023-2024

Breaches Occur: Fatigue with MFA “Nag”

Real Story

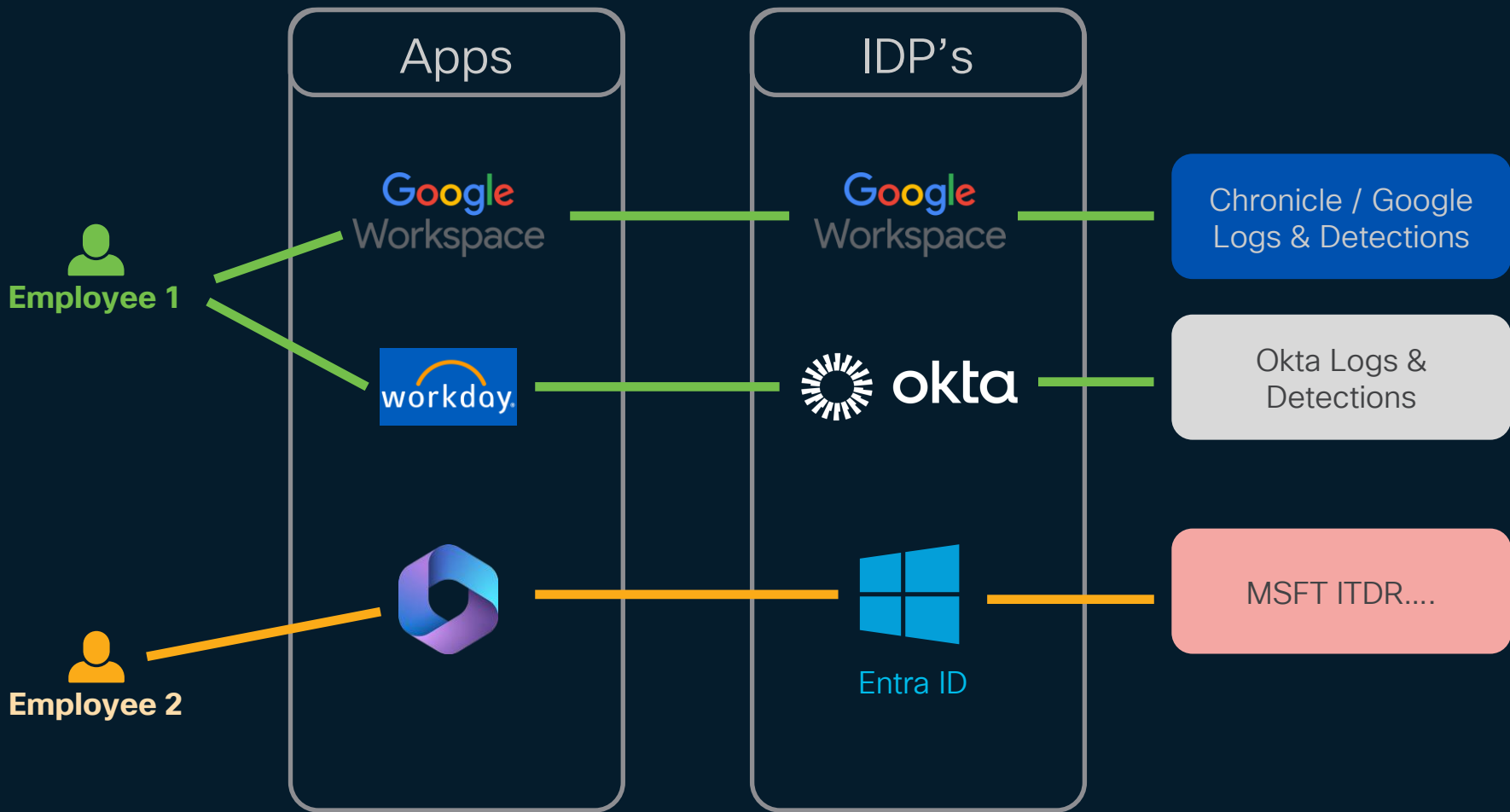
**Bypassed
My MFA**

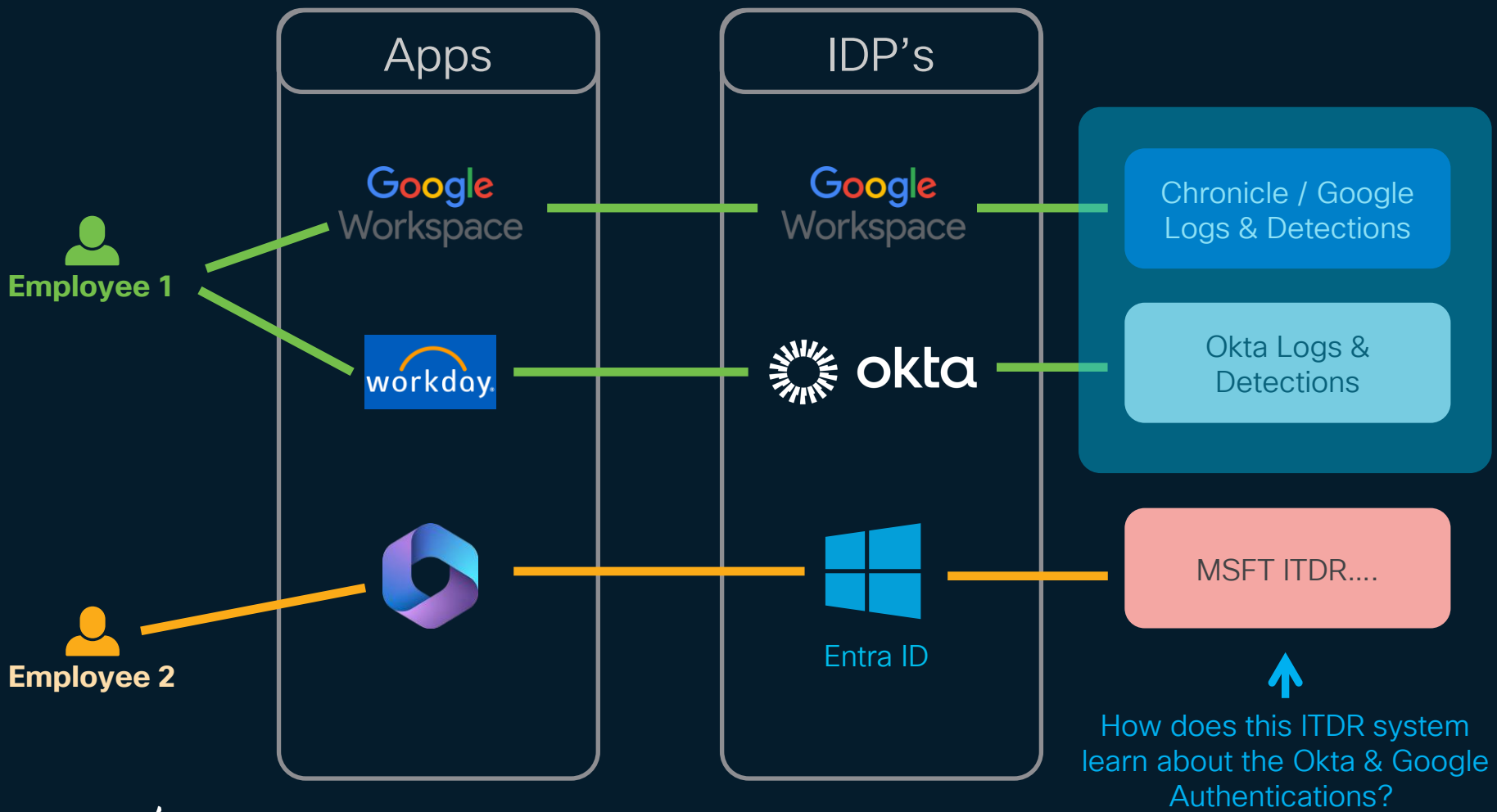
By Annoying Me!

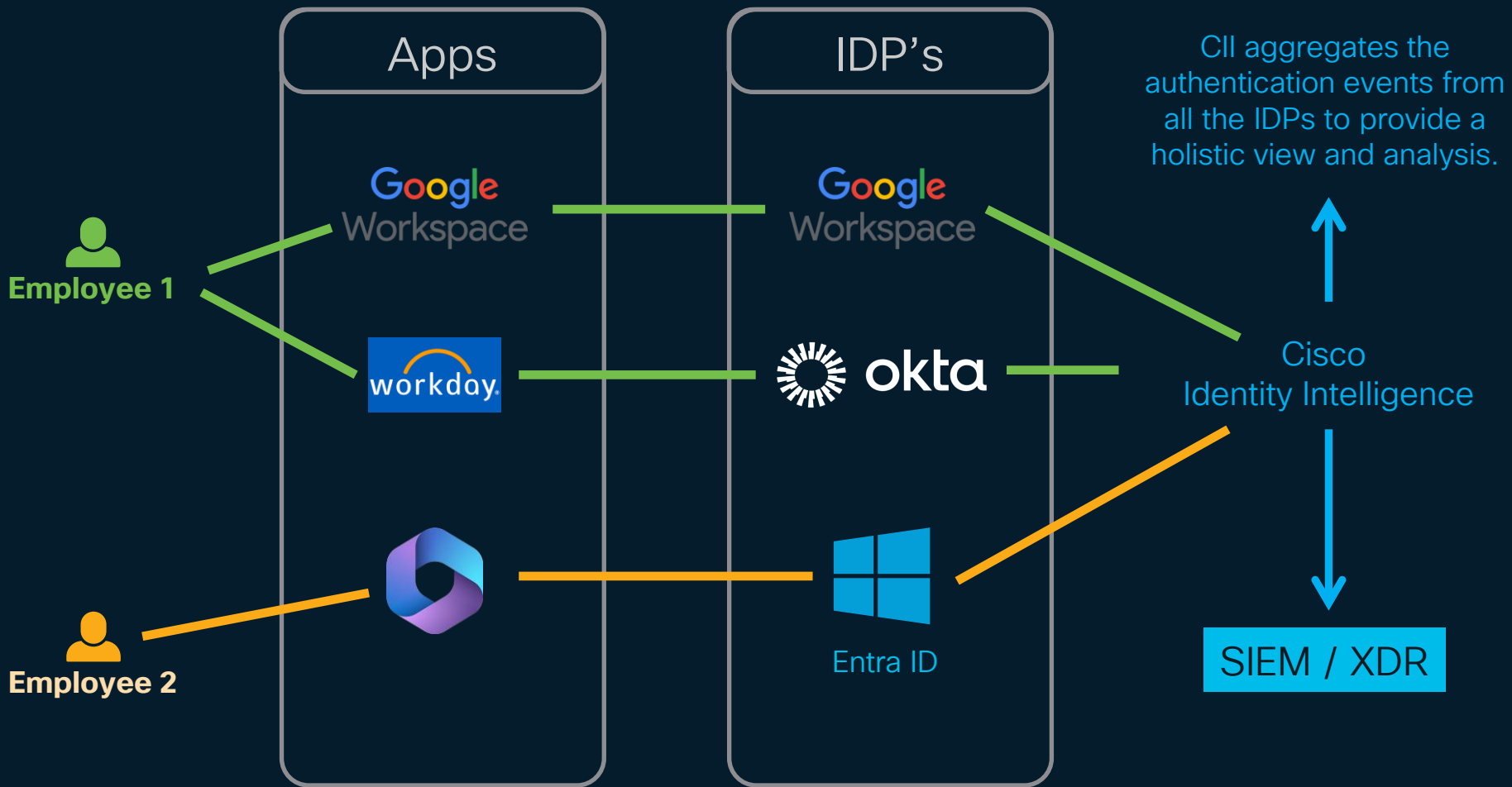


Credit: Wizer Security
<https://www.wizer-training.com>

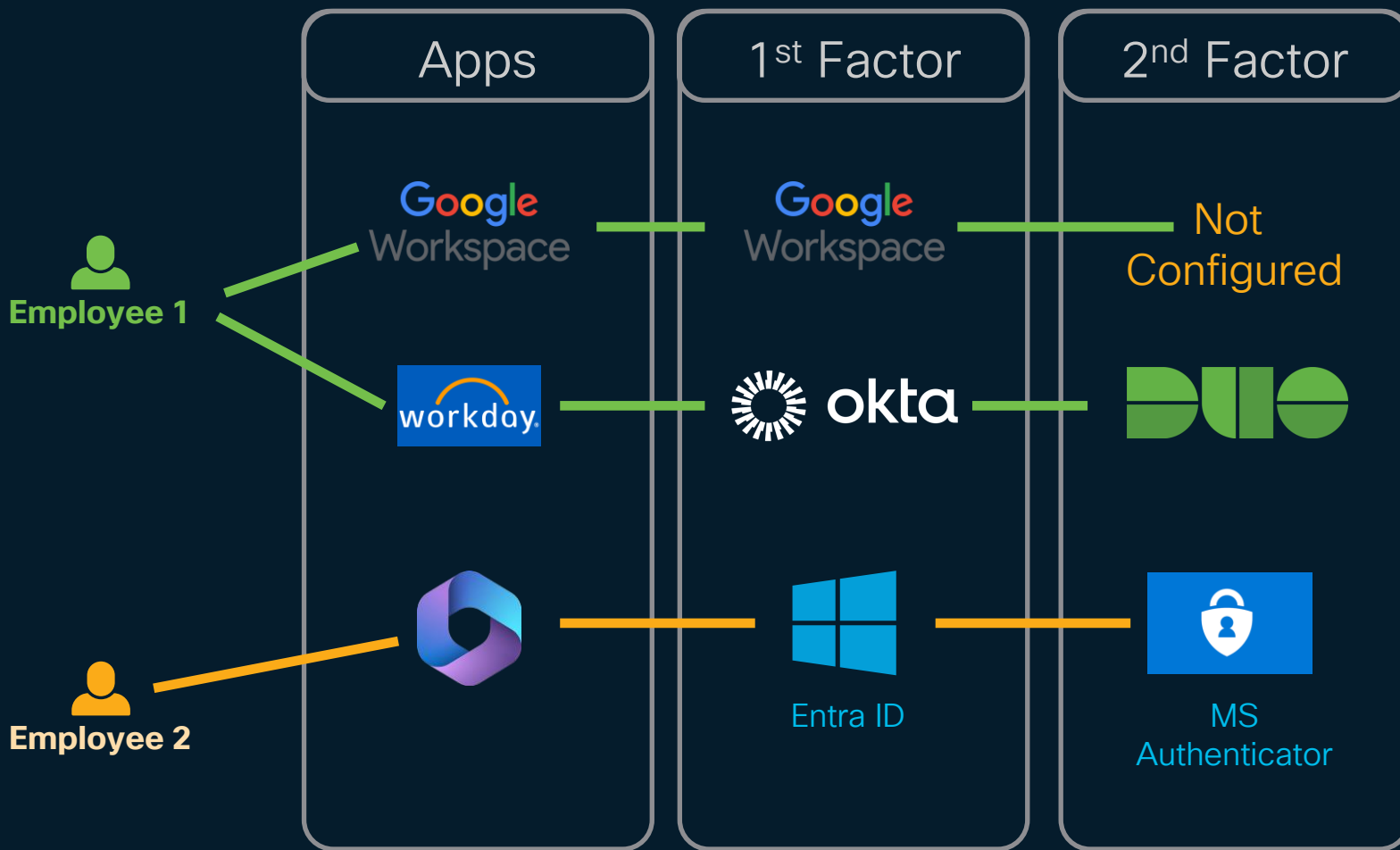
*You cannot
detect what
you cannot
see!*







*Are you sure
that strong
MFA is
configured
everywhere?*



We see
Environments
Like This
All the Time

Cisco Identity Intelligence



Users



Machines



Services



Apps



Data



Behaviors



Auth0

Workday

Okta

GitHub

Salesforce

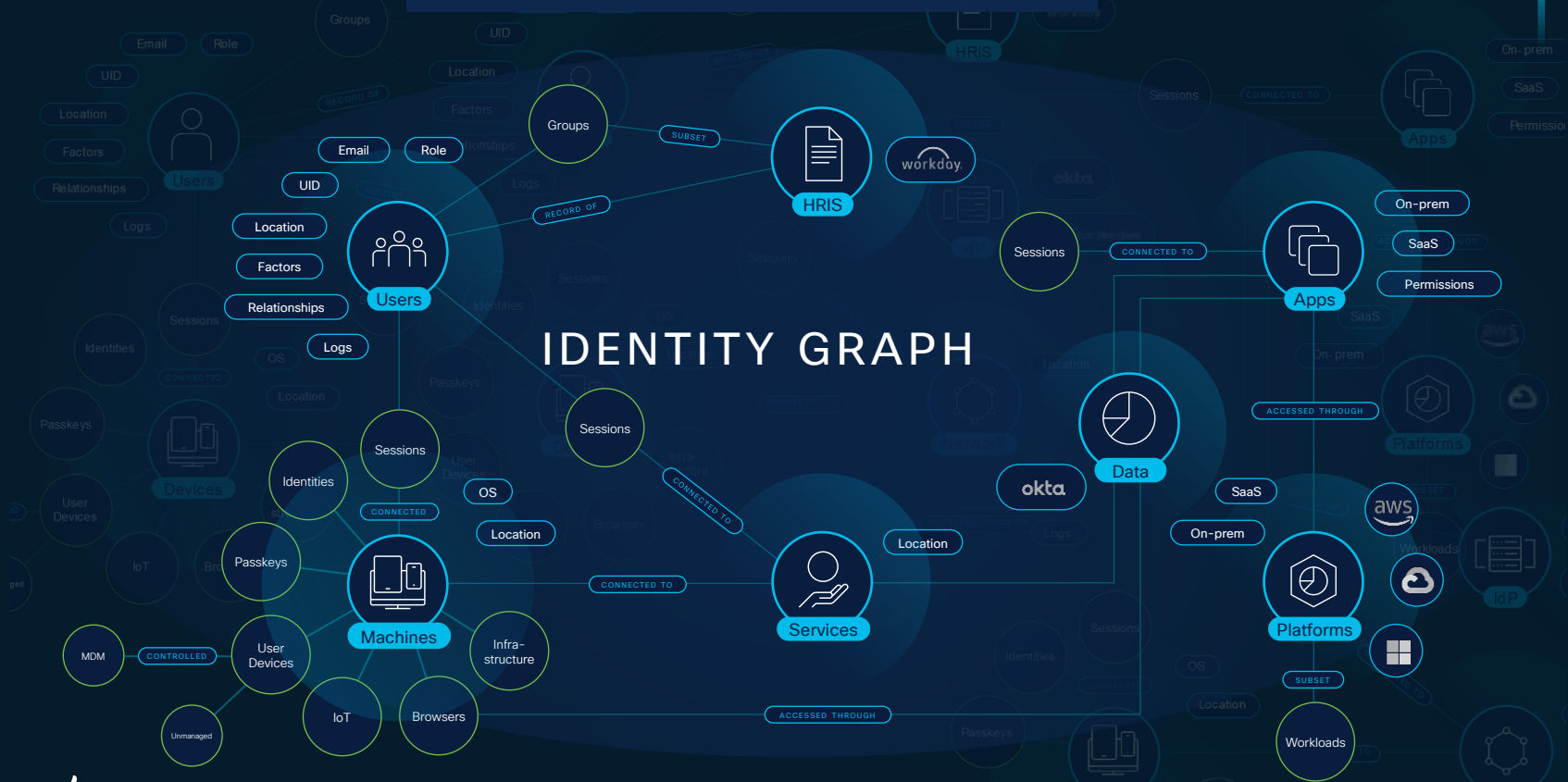
Microsoft



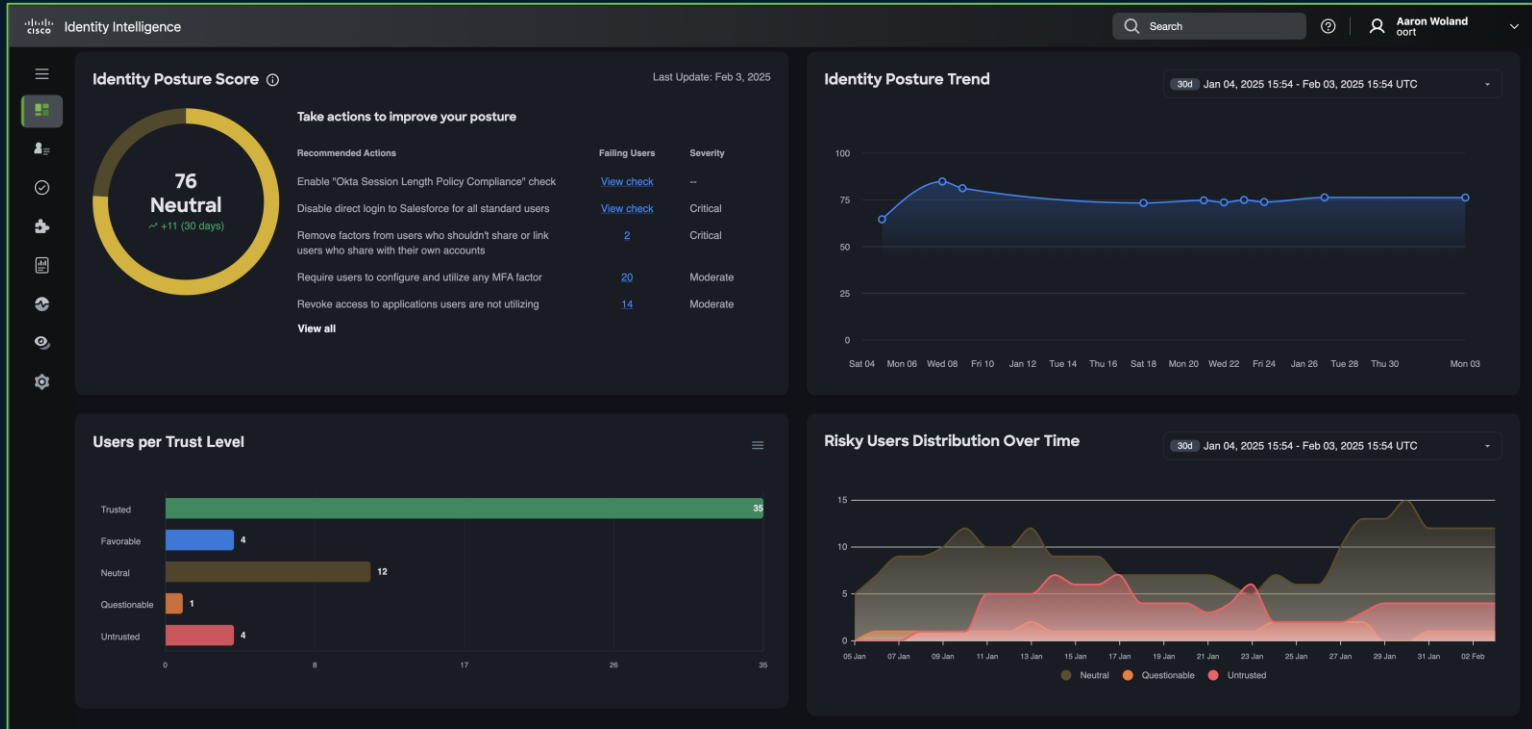
Google

Amazon

Identity Analytics

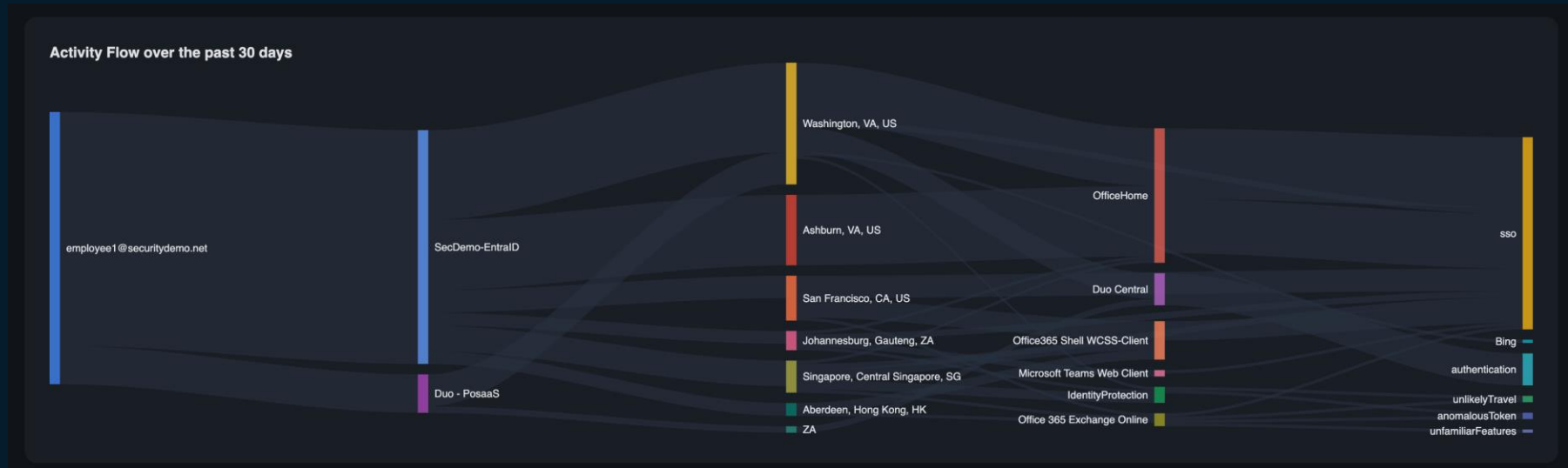


Provides information like this!



And this: Real life example of detection

Identity graph - Threat analysis based on probed account



Agenda

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

Integrations Overview

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-EntralID	✓ 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: SecurityDemo.Net, App: 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	xKvvt8q2wErXx5ZqWSlibGvWX41ZFX9		Mar 28, 2024 20:50:52
Aaron - API for XDR Dashboards	✓ Enabled	LHMtfeBUubrQVJ175zp3TONh5YAlyfSe		Mar 28, 2024 20:45:19

Integrations are “Life’s blood” for CII

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

Data collection methods

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

Identity sources and their methods

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

Wait... Why not just use the IDP?

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

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

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

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

- Large MSP Business

Merged view of users – combined from all sources

Merged Users

The user inventory is built out based on the users from each provider.

When the user is the same across multiple providers, those users are merged for a combined view.

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

The screenshot displays the Cisco Identity Intelligence user inventory interface. The left sidebar shows filter options for Status (Active, Deleted, Deprovisioned, Disabled) and Sources (Duo - PosaaS, Loox-Okta, SecDemo-EntraID, Slack - SecurityDemo.Net). The main table lists 17 users found, with columns for User, Checks, # IPs, # Logins, Last Seen (UTC), Last IP Address, Last Location, MFA, Providers, and Status. An orange box highlights the 'Providers' column, showing icons for different providers associated with each user.

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	✓	[Duo] [Okta]	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	✗	[Duo] [Okta]	Active
Donald Duck donald_duck@securitydemo.net	1	0	N/A	N/A	N/A	N/A	✗	[Duo] [Okta]	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	✗	[Duo] [Okta]	Active
EmployeeOne employee1@securitydemo.net	1	9	30	A Day Ago Apr 10, 2024 20:52:45	54.91.54.109	Ashburn, VA, US	✓	[Duo] [Okta]	Active
Loxx loxx@securitydemo.net	2	17	94	4 Hours Ago Apr 11, 2024 16:19:01	75.182.151.17	Waxhaw, NC, US	✓	[Duo] [Okta]	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	✓	[Duo] [Okta]	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...	✗	[Duo] [Okta]	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	✓	[Duo] [Okta]	Active

Users

User 360 View

The user details are 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

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

- Summary:** Lists user attributes such as "Inconsistent, Active", "Just a Number", "Human Labor", "SecurityDemo", "N/A", "MFA Configured", and "Apr 11, 2024 23:57:13 UTC (14 hours ago)". It also shows the user was created on May 22, 2019.
- Checks:** A prominent orange box indicates "1 failing" check: "User Has Directly Assigned Application".
- Attempted Logins:** A donut chart shows 60 total attempts, with 47 successful, 10 denied, and 3 other.
- Records per day:** A bar chart shows login activity over time, with a notable spike on April 11, 2024.
- Activity Flow:** A Sankey diagram shows the user's path from "SecDemo-EntralD" to various locations like "Washington, VA, US" and "Arlburn, VA, US", and through services like "OfficeHome" and "Office365 Shell WCSS-Client".
- Auth Log:** A table lists authentication events, including a "Last Successful Login" on April 11, 2024, and a "Last Login Attempt" on the same date from Singapore.
- Authentication Factors:** A table lists active factors: "Password" (Low assurance) and "Push" (Medium assurance).

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

The screenshot displays the Cisco Identity Intelligence interface for user **employee1@securitydemo.net**. The user is linked to **EmployeeOne** and is currently **Active**. A **Remediation** alert is shown, triggered by **loxx@securitydemo.net** on **Apr 23, 2024 18:25:13 UTC** with a status of **FAILURE**. Below the alert is a search bar and a bar chart showing activity trends from **03/27** to **04/26**. A tooltip for **Apr 23** indicates **FAILURE: 3**. Below the chart, a table lists **126 events found**. The table has columns for **Date (UTC)**, **Source**, **Event**, **Initiator**, **Target**, and **Result**.

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	User: employee1@securityde...	Success
Apr 24, 2024 17:11:09	OfficeHome	sso	employee1@securitydemo.net	User: employee1@securityde...	Success

Networks

The screenshot shows the Cisco Identity Intelligence interface for a user named EmployeeOne. The user is active and has a remediation status of FAILURE. Below this, there is a search bar for IP addresses and a table titled "14 IP Addresses". The table columns are IP Address, Last Access (UTC), Hit Count, Successful Events, Failed Events, Other Events, Tags, Location, and Ca. The IP addresses listed are 54.91.54.109, 172.203.228.226, 20.51.250.58, 128.107.78.71, 85.203.21.87, 154.16.95.37, 193.176.211.235, and 154.16.95.18. The location for the IP 85.203.21.87 is highlighted in yellow and includes "Singapore, Central Singapore, ...".

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

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.

The screenshot shows the Cisco Identity Intelligence interface for user EmployeeOne. The 'Devices' tab is active, displaying a list of 14 devices. A green box highlights the 'Access and Authentication devices' section, and a blue box highlights the first three rows of the table, which are Duo Epkeys.

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, 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:** 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 across various dates from 03/28 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-EntralD			N/A	51	Apr 24, 2024 19:43:17	Success
Office365 Shell WCSS-Client employee1@securitydemo.net	SecDemo-EntralD			N/A	18	Apr 24, 2024 17:11:09	Success
Office 365 Exchange Online employee1@securitydemo.net	SecDemo-EntralD			N/A	6	Apr 24, 2024 17:10:59	Success

Integrations Deep Dive

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

The screenshot shows the Oort Knowledge Base interface. The top navigation bar includes the Oort logo, the text 'Oort Knowledge Base', a search bar, and a user profile icon. A left sidebar menu lists various categories: Home, Glossary, Best Practices, How-to Guides, Oort Insights, Integrations (expanded), Auth0, Microsoft Entra ID (Azure AD) Data Integration (highlighted), Microsoft Entra ID (Azure AD) SSO Integration, Azure Event Hub Log Streaming for Microsoft Entra ID (Azure AD), Azure Sentinel SIEM Integration, AWS, Duo Security Integration, Github, Google Workspace Integration, Jira Integration, Mailgun Integration, Microsoft Teams Notification Integration, Okta Log Streaming AWS EventBridge Integration, Okta Data Integration, and Okta Workflows. The main content area features the title 'Microsoft Entra ID (Azure AD) Data Integration' with a date of '11/2023'. Below the title is an 'Overview' section stating that Oort's platform can analyze authentication events in Microsoft Entra ID (Azure AD) to provide insights into user access. An 'Important Notes' section contains two bullet points: one about SSO integration and another about enabling a Microsoft Entra ID subscription and resource provider in a development environment. A 'Next Steps' section indicates that once integration is complete, Oort will review the analysis with the user. The 'Entra ID Integration' section begins with the text 'Entra ID has different activity log types which each contain different sets of information. Oort'. At the bottom of the page, it says 'Powered by GitBook'.

View Logs

The screenshot shows the Cisco Identity Intelligence 'Integrations' page. At the top, there's a search bar and a user profile for 'loxx@securityde... security-demo-int'. Below the header, there are buttons for 'Request Integration', '+ Add Integration', and a refresh icon. The main content is a table titled 'Providers' with columns: Name, Collection Status, Recent Usage, Average Traffic, Last Collected (UTC), and Last Updated (UTC). The table lists several integrations: Duo - PosaaS (Collecting), Loxx-Okta (Success), SecDemo-EntralD (Collecting), Slack - SecurityDemo.Net (Success), and loxx.tv (Success). A blue arrow points to the 'View Logs' option in the dropdown menu for the 'SecDemo-EntralD' integration. A green line with an arrow points from the 'View Logs' option to the text 'Ellipses (...)' on the right.

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

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 shows the Cisco Identity Intelligence interface. The top navigation bar includes the Cisco logo, the text "Identity Intelligence", a search bar, and a user profile for "loxx@securityde... security-demo-int". The main content area is titled "Integrations > System Logs" and shows a search filter for "Target-Duo - PosaaS". A left sidebar contains a filter menu with categories like "Result", "Event Family", and "Check Actions Taken". A red arrow points from the "Event Family" section to the "Integration__DATA_UPLO..." entries in the log table.

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.

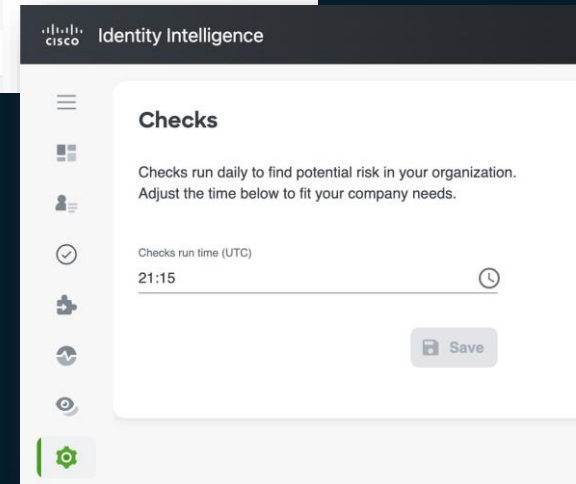
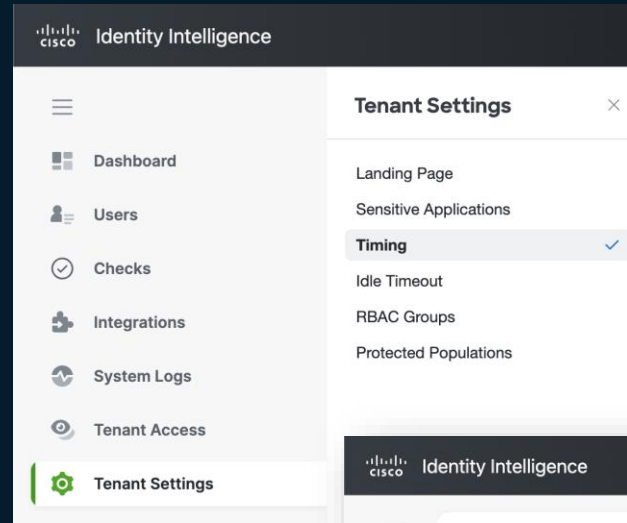
Aids tremendously when troubleshooting why information isn't getting sync'd across.

The screenshot displays the Cisco Identity Intelligence 'System Logs' interface. On the left, a sidebar contains a 'Result' filter menu with options like 'Blocked', 'Failure', 'Info', 'None', 'Partial success', 'Started', 'Success', and 'Timeout'. A red arrow points from the 'Success' filter to a specific log entry in the main table. The table lists events with columns for 'Date (UTC)' and 'Event'. The selected event is expanded to show a detailed view with the following information:

- End Date:** Apr 18, 2024 19:28:00 UTC
- Running Time:** 0h 0m 1s
- Event:** INTEGRATION__HISTORICAL_COLLECTION
- Initiator:** system
- Logged By:** cnt-integration-sfn-historical-data-collection
- Integration Target:** Duo - PosaaS
- Stn Id:** 3ba3bb18-0238-4bef-b03f-4aa6a7ea1576
- Execution Arn:** arn:aws:states-us-east-2:227542035969:execution:cnt-integration-sfn-historical-data-collection:3ba3bb18-0238-4bef-b03f-4aa6a7ea1576
- Execution History:**
 - Metadata:
 - statusCode: 200
 - requestId: "d8f9ff07-3e85-42c5-b0e8-d87b0f6bc0ff"
 - attempts: 1
 - totalRetryDelay: 0
 - events:
 - 0:
 - id: 51
 - previousEventId: 50
 - taskStartedEventDetails:
 - resource: "invoke"
 - resourceType: "lambda"
 - timestamp: "2024-04-18T19:28:01.913Z"
 - inputDetails:
 - truncated: false
 - name: "sfnAuditSuccess"
 - timestamp: "2024-04-18T19:28:01.828Z"
 - type: "TaskStateEntered"
- Input:**
 - integrationInstanceId: "4e384171-e293-4c17-a2da-ba50dc445f54__DUO_e48f5"
 - tenantId: "4e384171-e293-4c17-a2da-ba50dc445f54"
- State Machine Arn:** arn:aws:states-us-east-2:227542035969:stateMachine:cnt-integration-sfn-historical-data-collection

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 table lists several providers with their collection status, recent usage, average traffic, and last collected/updated times. A red arrow points to the 'Collect Now' option in the dropdown menu for the 'Slack - SecurityDemo...' provider.

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 21:27:15	Apr 29, 2024 01:51:30
Slack - SecurityDemo...	Success Traffic detected	[Line Graph]	13 records	Jun 1, 2024 21:56:15	Apr 29, 2024 01:51:30
loxx.tv	Success Traffic detected	[Line Graph]	0 records	Jun 1, 2024 21:56:15	Apr 29, 2024 01:51:30

Duo
a Cisco Company



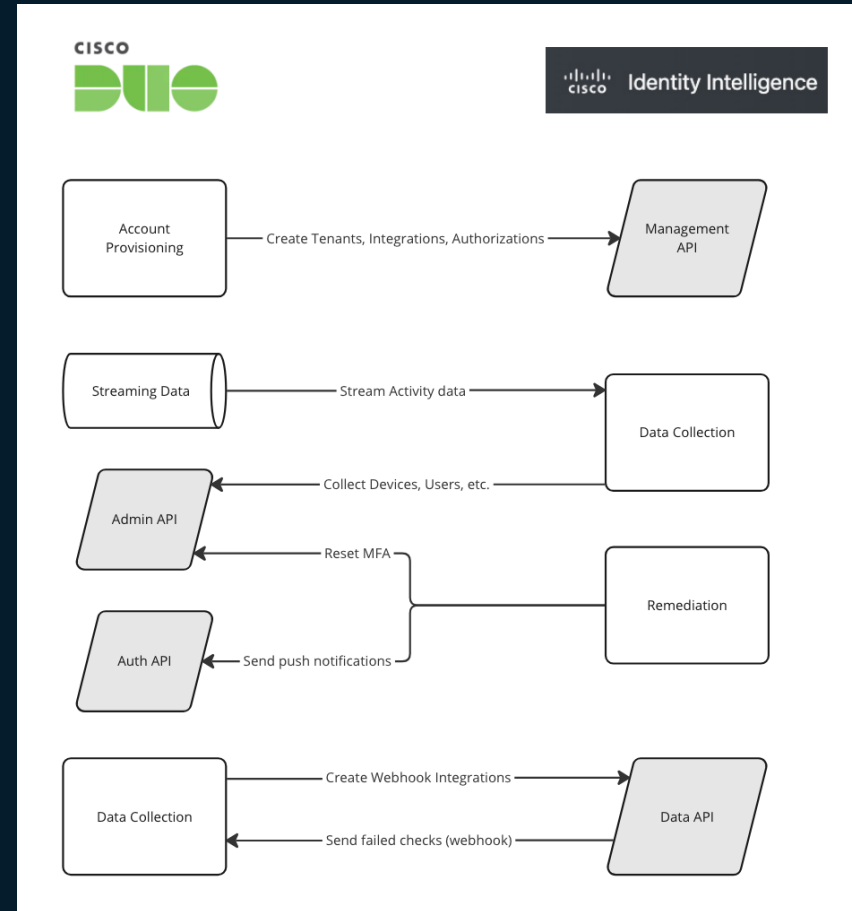
Duo <> CII Integration

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

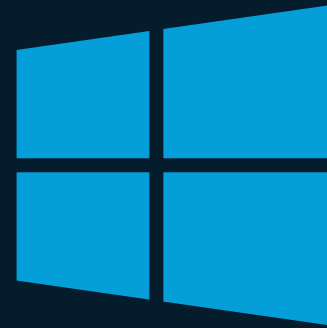
The screenshot displays the Cisco Identity Intelligence (CII) management interface. The top navigation bar includes the Cisco Duo logo, a search bar, and user information for 'Account Oort Inc' and 'Andy Winiarski'. The left sidebar contains a menu with categories like Dashboard, Device Insight, Policies, Applications, Single Sign-On, Users, Groups, Endpoints, 2FA Devices, Administrators, Trusted Endpoints, Monitoring (selected), Reports, and Settings. The main content area shows the 'Cisco Identity Intelligence' page with a breadcrumb trail: Dashboard > Monitoring > Cisco Identity Intelligence. Below the title, there's a description: 'Set up an organization to identify, reduce, and respond to identity-based threats.' The 'Organization details' section features a progress indicator with three steps: 'Create organization' (checked), 'Configure your organization' (checked), and 'Configure an identity provider' (checked). The 'Create organization' step is active, showing a form for 'Organization name' with the value 'andywduotest'. A note below the form states: 'Organization names must be in all lowercase. Only letters, numbers, underscores, and dashes may be used.' There are 'Back' and 'Next' buttons at the bottom right of the form. The footer contains copyright information: '© 2024 Duo Security. All rights reserved.', a 'Terms of service' link, and specific details: 'Selected: Oort Inc / ID: 3709-5886-11' and 'Deployment ID: DU072'.

Duo Integration Details

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



Microsoft Entra ID



Aka: Azure Active Directory (AAD)

MS Entra ID

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

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

The screenshot shows the 'Edit Microsoft Entra ID Settings' page in the Cisco Identity Intelligence interface. The 'General Settings' tab is selected, displaying the following configuration:

- Name:** SecDemo-EntraID
- Directory ID:** [Redacted]
- Application ID:** 07ef51a6-8052-4cc4-[Redacted]

A **Reset Credentials** button is present, accompanied by a warning: "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](#)".

On the right side of the page, there are several expandable sections:

- Where can I see a step by step configuration guide?** (Expanded): Refer to [this documentation article](#) for a step by step guidance.
- Are Directory ID and Tenant ID the same thing?** (Collapsed)
- Where do I get my Application ID?** (Collapsed)
- How do I get my Application Secret Value?** (Collapsed)

The footer of the page includes: © 2024 Identity Intelligence, This environment reloads hourly, [Privacy Policy](#), [Terms of Use](#), [Documentation](#), and [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 'Edit Microsoft Entra ID Settings' page in the Cisco Identity Intelligence interface. The 'Event Streaming' tab is active, showing the following configuration details:

- Use EventHub for Logs Streaming:** Enabled (toggle switch).
- 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 form, there is a 'Reset Credentials' button, a 'Cancel' button, and a 'Save' button.

On the right side of the page, there is a sidebar with several expandable sections:

- Where can I see a step by step configuration guide? (Expanded, showing a link to documentation)
- 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.

The screenshot shows the 'Edit Microsoft Entra ID Settings' page in Cisco Identity Intelligence. The 'Advanced Settings' tab is active, and the 'Data Types' section is highlighted with an orange box. This section contains a list of data types with checkboxes and warning icons (yellow triangles). A tooltip for 'Risky Users' indicates it requires a Microsoft Entra ID Premium P2 subscription. The page also includes a search bar, user profile, and a footer with copyright and links.

Advanced Settings

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?

Where do I get my Application ID?

How do I get my Application Secret Value?

© 2024 Identity Intelligence

This environment reloads hourly

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

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

Okta Identity Engine



okta

App Catalog

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

The screenshot displays the Okta Admin Console interface. On the left is a navigation sidebar with categories like Dashboard, Directory, Customizations, Applications, Security, Workflow, Reports, and Settings. The 'Applications' section is expanded, and the 'API Service Integrations' sub-section is selected. The main content area shows the details for the 'Cisco Identity Intelligence - Read-Write Management API Service'. At the top right of this section, it says 'Last updated: January 24, 2025' and includes a blue 'Add Integration' button. Below this is a large card with the Cisco logo and the service name. Further down, there are sections for 'Okta Verified' (stating the integration was either created by Okta or verified by Okta), 'Use Case' (linking to 'Identity Governance and Administration (IGA)'), and 'Functionality' (labeled as 'API'). A blue notification bubble with the number '1' is visible in the bottom right corner of the page.

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.

Preview 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 loxx@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](#)

Okta

General Settings

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

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

Identity Intelligence

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?

© 2024 Identity Intelligence

This environment reloads hourly

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

Okta

Event Streaming

Okta logs can be streamed to AWS Event Bridge

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

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

Identity Intelligence

Search

loxx@securityde... security-demo-int

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-██

AWS Account ID
22754-██

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

Privacy Policy Terms of Use Documentation SOC2 Report

This environment reloads hourly

Okta

Advanced Settings

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

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

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

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

Identity Intelligence

Search

loxx@securityde... security-demo-int

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

Privacy Policy Terms of Use Documentation SOC2 Report

This environment reloads hourly

Agenda

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

What are Checks?

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

The screenshot displays the Cisco Identity Intelligence dashboard. On the left is a navigation sidebar with categories like Compatibility, Compliance, Severity, Topic, Frameworks, and Scopes. The main area shows a table of 'All Checks' with columns for Check name, # Failing, # Excluded, and a 'Report' button. Each check includes a score, a trend indicator (up/down arrow), and a percentage change since the last week or month.

Check	# Failing	# Excluded	Report
Inactive Users 85% Moderate End Users - Compliance, Identity Posture Insight	95 18.99% increase since last week 22.42% increase since last month	0	+ A
User Has Directly Assigned Application 70% Low End Users - Compliance, Identity Posture Insight	81 31.55% increase since last week 43.62% increase since last month	0	+ A
Never Logged In 70% Critical End Users - Compliance, Identity Posture Insight	80 12.64% decrease since last week 13.67% decrease since last month	0	+ A
Applications with Expired Secrets 81% Low Identity Providers - Identity Posture Insight	N/A	N/A	+ A
No MFA Configured 96% Critical End Users - Compliance, Identity Posture Insight	36 63.64% increase since last week 98.38% increase since last month	0	+ A
Users Sharing Authenticators 92% End Users - Compliance, Identity Posture Insight	20 No change since last week 2.74% increase since last month	0	+ A
User Password Expiration Failure 95% Moderate End Users - Identity Posture Insight	13 28.17% increase since last week 37.32% increase since last month	0	+ A
Unmanaged Devices Access 99% Low End Users - Compliance, Devices, Identity Posture Insight	9 1.56% decrease since last week 9.76% increase since last month	0	+ A
Inactive Guest Users 98% Critical End Users - Compliance, Identity Posture Insight	5 105.88% increase since last week 127.27% increase since last month	0	+ A
No Strong MFA Configured 98% Moderate End Users - Compliance, Identity Posture Insight	4 No change since last week No change since last month	0	+ A
Allow/Block Email Logins 99% Critical End Users - Compliance, Identity Posture Insight	2 No change since last week 80% increase since last month	0	+ A
Microsoft Entra ID Admin Activity Anomaly 99% Low End Users - Identity Threat Insight	1 68.67% decrease since last week 44.44% decrease since last month	0	+ A
Weak MFA Was Used To Successfully Sign In 99% Critical End Users - Identity Posture Insight	1 250% increase since last week 30% increase since last month	0	+ A
Shared Mailbox Sign In Enabled 99% Low End Users - Identity Threat Insight	1 No change since last week No change since last month	0	+ A
Access from Denied Countries	1 No change since last week	0	+ A

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.

The screenshot displays the Cisco Identity Intelligence dashboard. On the left, there are three filter panels: Compatibility, Topics, and Frameworks. The Compatibility panel lists providers like Duo, Google Workspace, Microsoft Entra ID, Okta, and Slack. The Topics panel lists categories like Compliance, Devices, Identity Posture Insight, and Identity Threat Insight. The Frameworks panel lists risk frameworks like End Users and Identity Providers. The main area shows a table of 'All Checks' with columns for Check name, # Failing, and trend indicators. A blue box highlights the Frameworks filter and the 'Users Sharing Authenticators' check row. A blue line connects this check to a detailed list of frameworks on the right side of the image.

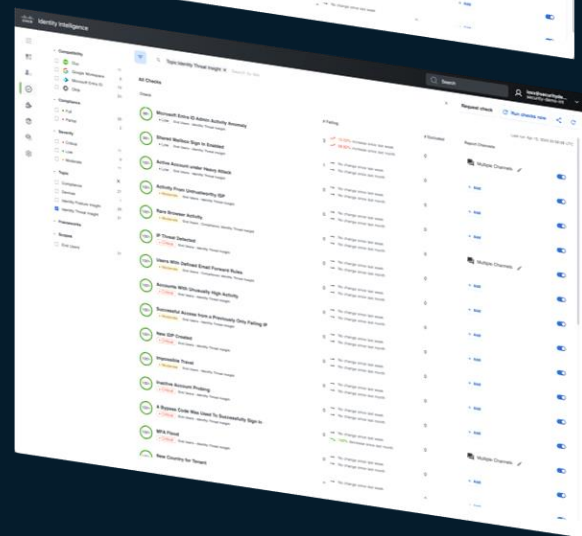
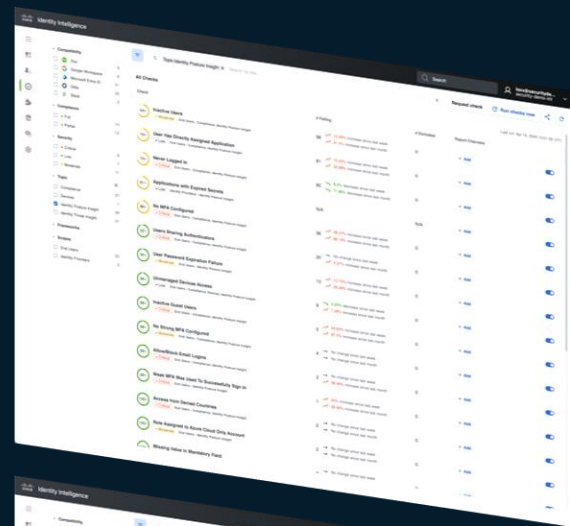
Check	# Failing	Trend
Inactive Users	95	18.96% increase since last week, 22.42% increase since last month
User Has Directly Assigned Application	81	31.55% increase since last week, 43.62% increase since last month
Never Logged In	80	12.01% decrease since last week, 13.67% decrease since last month
Applications with Expired Secrets	N/A	
No MFA Configured	36	63.64% increase since last week, 96.36% increase since last month
Users Sharing Authenticators	20	No change since last week, 2.74% increase since last month
User Password Expiration Failure	13	28.17% increase since last week, 37.32% increase since last month
Unmanaged Devices Access	9	1.56% decrease since last week, 9.76% increase since last month
Inactive Guest Users	5	105.88% increase since last week, 127.27% increase since last month
No Strong MFA Configured	4	No change since last week, No change since last month
Allow/Block Email Logins	2	No change since last week, 50% increase since last month

Frameworks

- ASD Essential 8 1
- ASD Level 3 2
- CIS 4.3 2
- CIS 5.3 3
- CIS 5.4 6
- CIS 5.5 1
- CIS 5.6 3
- CIS 6.3 3
- CIS 6.4 3
- CIS 6.5 3
- CMMC AC.2.010 2
- CMMC IA.3.083 1
- CMMC IA.3.084 2
- CMMC SC.3.187 2
- Mitre ATT&CK T1078 4
- Mitre ATT&CK T1078.004 1
- Mitre ATT&CK T1087.004 2
- Mitre Mitigation M1032 1
- Mitre Mitigation M1036 1
- NIST 800-63-3 2
- NIST CSF DE.CM-3 6
- NIST CSF PR.AC-7 1
- NIST CSF PR.IP-11 2
- PCI DSS 8.2 1
- SOX Section 302.2 1

Proactive vs. Reactive

- **Posture Checks are Proactive** – examining the authentications and account configurations – to reduce probability and blast radius
- **Threat Checks are Reactive** – examining the behavior of users and their authentications – to detect threats



Checks are Tunable

Check Settings

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

Custom Detection Settings

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

List Settings

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

Default was: Ignore Medium & Below

The screenshot displays the Cisco Identity Intelligence interface for the 'Sign in Threat Detected' check. The main view shows details, recommended actions, and tags. Three callout boxes highlight specific settings:

- Custom Detection Settings:** A modal window with a toggle for 'Exclude known good ips' (currently off), 'Restore default', and 'Save changes' buttons. It also features 'Test' buttons on the right side.
- Check Settings:** A panel on the right showing 'Custom Detection Settings' (with an 'Edit' button), 'Notification Settings' (with a 'Customize messages' button), and a list of notification recipients: 'Aaron XDR Listener', 'SecurityDemoNet-Oort-Messages', and 'Securitydemo Slack', each with a 'Test' button.
- List Settings:** A modal window for configuring the 'Ignore list'. It includes 'Cancel', 'Restore default', '+ Add', and 'Save' buttons. The list contains 5 items: 'hidden', 'low', 'medium', 'none', and 'unknownFutureValue'. A 'Delete item' button is positioned next to the 'low' item.

Outbound Notifications

Notifications

Notifications are configured per check.

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

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

Notifications Targets:

Notification Targets

- Email**: Email address to be used for Identity Intelligence notifications. Adding a different address as CC is supported. [+ Add Email Target](#)
- Microsoft Teams**: Install our bot in your Microsoft Teams to get all the latest updates in any public channel you choose. [+ Add MS Teams Target](#)
- Slack**: Install our app in your Slack Workspace to get all the latest updates directly or in any channel you choose. [+ Add Slack Target](#)
- Webhook**: Connect Identity Intelligence failed check notifications with your automated processes via webhooks. [+ Add Webhook Target](#)
- Webex**: Install our app in your Webex Workspace to get failed check notifications. [+ Add Webex Target](#)

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

Compatibility: Duo (20), Google Workspace (14), Microsoft Entra ID (40), Okta (43), Slack (2)

Compliance: Full (13), Partial (7)

Severity: Critical (11), Low (2), Moderate (7)

Topic: Compliance (9), Identity Posture Insight (9), Identity Threat Insight (11)

Frameworks: Scopes (End Users)

Check	# Failing	# Excluded	Report Channels
Inactive Users (Moderate) End Users - Compliance, Identity Posture Insight 64% 12.48% increase since last week, 21.4% increase since last month	98	0	+ Add
Never Logged In (Critical) End Users - Compliance, Identity Posture Insight 70% 8.2% decrease since last week, 11.66% decrease since last month	80	0	+ Add
No MFA Configured (Critical) End Users - Compliance, Identity Posture Insight 86% 28.57% increase since last week, 69.19% increase since last month	36	0	+ Add
Users Sharing Authenticators (Critical) End Users - Compliance, Identity Posture Insight 92% No change since last week, 2.27% increase since last month	20	0	+ Add
No Strong MFA Configured (Moderate) End Users - Compliance, Identity Posture Insight 98% No change since last week, No change since last month	4	0	+ Add

Notification Settings

Send failure reports to:

- Aaron XDR Listener | Test | + Add
- SecurityDemoNet-Oort-Messages | Test | + Add
- Securitydemo Slack | Test | + Add
- Multiple Channels | + Add

Direct User / Manager Notifications

Identity Intelligence

Checks > No MFA Configured

No MFA Configured Critical

Details

Detects users with no Multi-Factor Authentication (MFA) enabled. MFA requires users to provide something you know, like a password or PIN, or something you have, like an out-of-band device or a one-time password provider. All users should be using MFA to gain access to the system. Users will not fail this check if they fall within the grace period of 14 days. You can add known domains to either ignore or include list.

Learn More About the Risk

[How Multi Factor Authentication Can Save You](#)

Check Settings

Custom Detection Settings Edit

Grace period for new accounts (days): 14

Notification Settings Customize messages

Send failure reports to:

- Aaron XDR Listener Test
- SecurityDemoNet-Oort-Messages Test
- Securitydemo Slack Test

Send direct messages on failure: Send test message to me

Who should be messaged: User

Message channels: Email

Discard changes Save settings

List Settings Edit

Ignore list

Your don't have any items in your ignore list

49 failing users

User

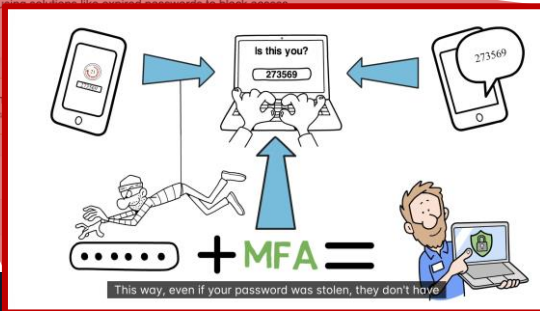
secops2@loxx.tv

Security Education

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

Educate the End-User

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



Chat Ops

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

The image shows a Cisco Identity Intelligence alert and its integration with Slack. The alert, titled "Microsoft Entra ID Admin Activity Anomaly", is displayed in a dark-themed interface. It includes a severity level of "Low", a count of "2 failing users", and a timestamp of "12 Apr 2024 15:01 GMT". The alert references "Identity Threat Insight | CIS 5.4 NIST CSF PR.AC-4 NIST CSF DE.CM-3 Mitre ATT&CK T1098.003". The alert text describes the detection of new administrative actions and provides context on how Identity Intelligence detects such actions. It also notes that adversaries may create or modify accounts to evade defenses. The alert lists two failing logins: "azita@securitydemo.net" and "prakasp3@cisco.com". Below the alert, there are three buttons: "Exclude from check", "Interesting", and "Normal behavior". The alert also shows the integration ID "SecDemo-EntraID" and the number of actions performed (59 and 13). The Slack interface on the right shows a message from "Oort Bot Integration" with the Slack logo and a message about the beginning of the direct message history. Below this, there is a message from "Oort Bot Integration" with the subject "Sign In Threat Detected" and a detailed description of the threat, including a severity level of "Moderate" and a count of "1 failing users". The Slack message also includes a "Go to report" button and a note that sending messages to the app has been turned off.

Chat Notification Targets

Today New

Oort Bot Integration APR 2:03 PM
No MFA Configured

Critical | Compliance, Identity Posture Insight | NIST 800-63-3, CIS 6.3, CIS 6.4, CIS 6.5, NIST CSF PR.AC-7, ASD Essential 8, CMMC IA.3.083, PCI DSS 8.2, Mitre Mitigation M1032

Your account is not using Multi-Factor Authentication. All users should be using Multi-Factor Authentication to access the system.

Learn More About the Risk
[How MFA Can Save You](#)

▶ **Free Security Awareness Training**
How Multi Factor Authentication Can Save You
Free Security Awareness Training • Simply Explained • Access Anywhere • Follow Progress (219 kB) ▾

Sending messages to this app has been turned off.

Oort
ANTI-spam Take Action: No MFA Configured
To: loxx@securitydemo.net

Inbox - Loxx@SecurityDemo.Net 2:01 PM

Identity Intelligence

No MFA Configured

critical | Compliance, Identity Posture Insight | NIST 800-63-3, CIS 6.3, CIS 6.4, CIS 6.5, NIST CSF PR.AC-7, ASD Essential 8, CMMC IA.3.083, PCI DSS 8.2, Mitre Mitigation M1032

Your account is not using Multi-Factor Authentication. All users should be using Multi-Factor Authentication to access the system.

Learn More About the Risk
[How MFA Can Save You](#)

Visit [Cisco Identity Intelligence](#)

©2024 Cisco Systems, Inc. | [Support center](#)

Agenda

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

Taking Action(s)

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

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

Remediations are source specific

- Not all sources support the same remediation.
- Reset MFA is applicable to Okta & Duo only (for example)

Remediation Nuggets:

- CII only allows one remediation action at a time.
- The provider must be configured to allow the actions (think “*write*” access)

Context Specific Remediation Menu

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

NOT Status:(3 conditions) Aaron

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.

Users > aawoland@cisco.com

Aaron Woland aawoland@cisco.com Active

Overview Activity Networks Devices Applications Groups 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

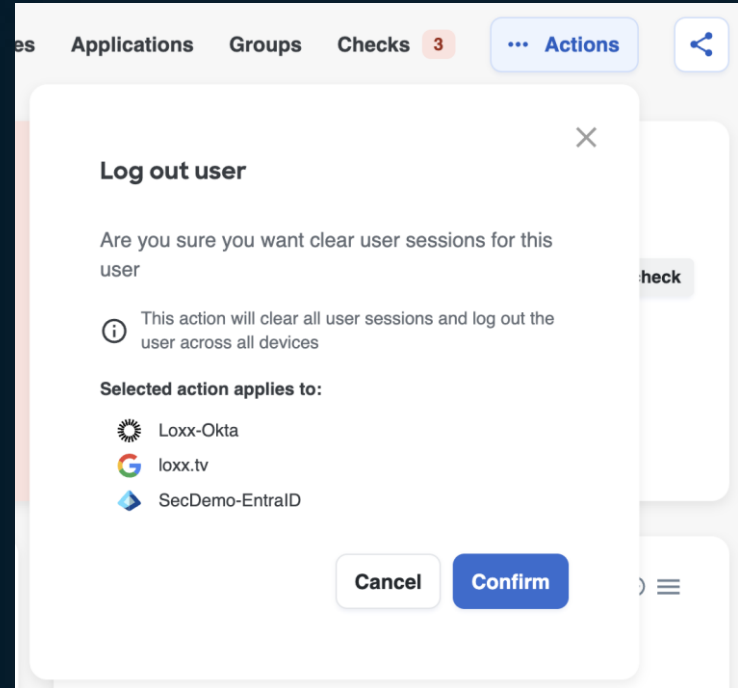
Records per day

30 All Attempts

Success - 30

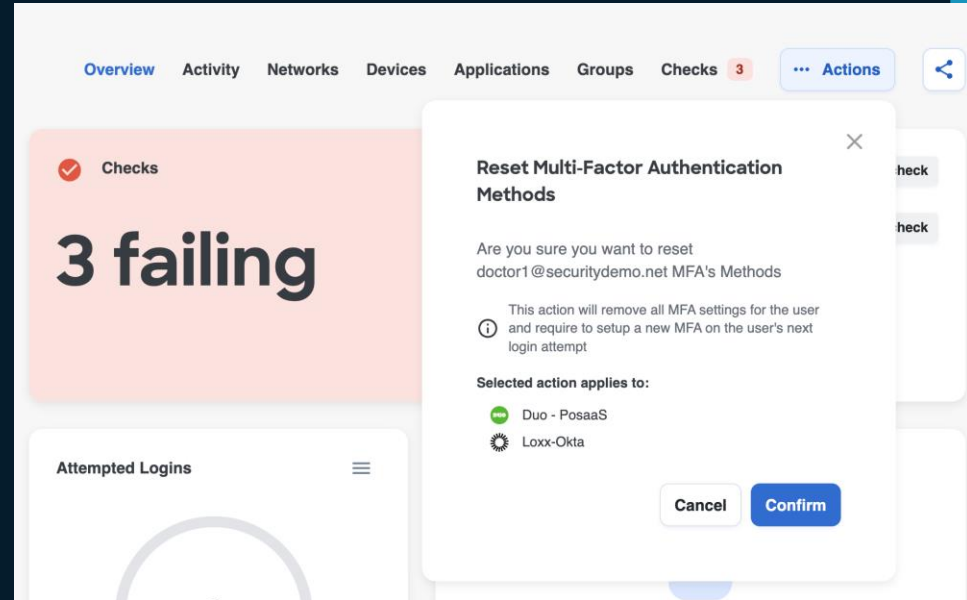
Log Out User

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



Reset MFA example w/ Duo

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



Duo's Reset MFA

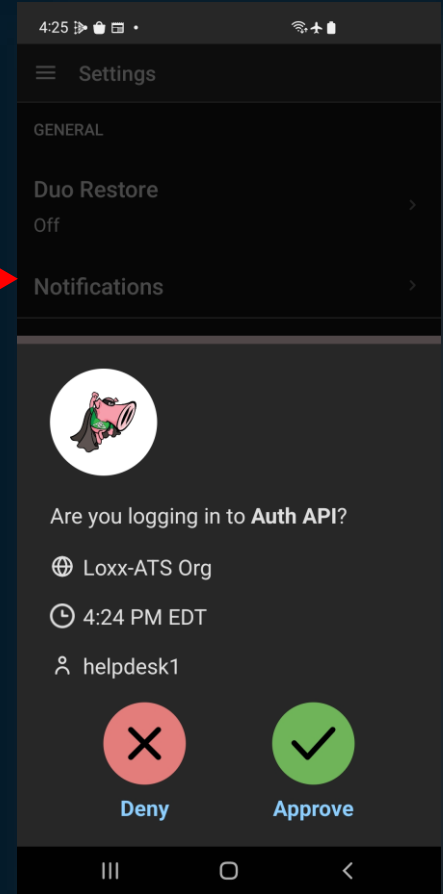
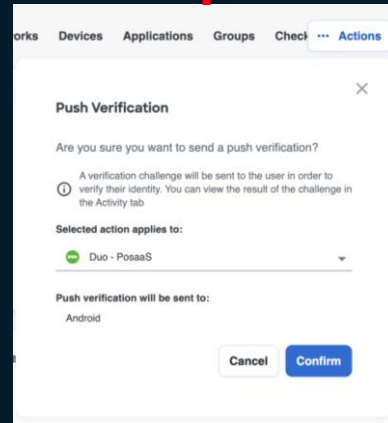
The screenshot shows the Cisco Identity Intelligence interface for user 'doctor1'. The 'Checks' section indicates '3 failing'. A dropdown menu is open, showing the 'Reset MFA' option highlighted with a purple arrow. Other options include 'Log out user', 'Send push verification', 'Refresh User Data', and 'Link user'.

Factor	Assurance Level	Status	# Changes	Usage Count	Device
Duo Mobile Duo - PosaaS DPUCT3HKA1NKU0X388YD__mobile_otp	Medium	ACTIVE	0	N/A	Af
Duo Mobile Duo - PosaaS DPUCT3HKA1NKU0X388YD__mobile_otp	Medium	ACTIVE	0	N/A	Sc
Push Duo - PosaaS DPUCT3HKA1NKU0X388YD__push	Medium	ACTIVE	0	N/A	Af
Push Duo - PosaaS DPUCT3HKA1NKU0X388YD__push	Medium	ACTIVE	0	N/A	Sc
Call Duo - PosaaS DPUCT3HKA1NKU0X388YD__phone	Low	ACTIVE	0	N/A	Af

The screenshot shows the 'Reset Multi-Factor Authentication Methods' dialog box. The dialog asks for confirmation to reset MFA settings for the user 'doctor1@securitydemo.net'. It lists the selected action as 'Duo - PosaaS' and 'Loxx-Okta'. The 'Confirm' button is highlighted with a purple arrow.

Send Push Notification

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



Leveraging Your Security Operations Center (SOC)



Cisco XDR



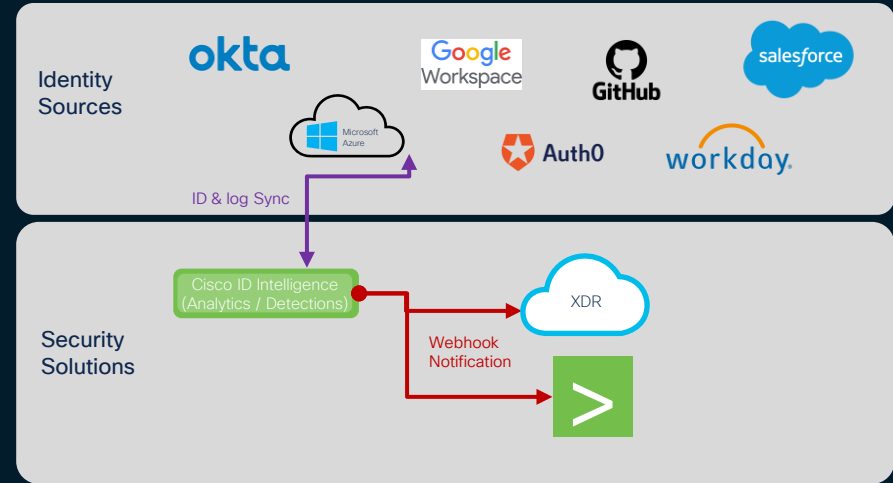
Splunk

...and other SOC Tools

Webhooks

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

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



What's in the Webhook?

Failed Checks

ie.: A matched signature.

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

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__2411fce3	▼
	<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	▼

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

Webhook API Key

Copy Refresh

Webhook URL
<https://automate.us.security.cisco.com/webhooks/02CWJ...>
Copy

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...>

Authorization Type
 Basic API Key Duo Security Client OAuth Client Credentials

API key name
foo

API key value

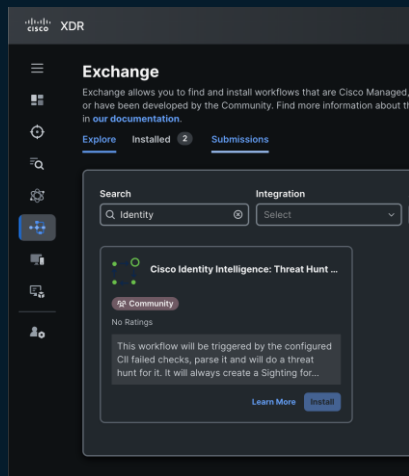
Invocation HTTP Parameters

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

Add parameter

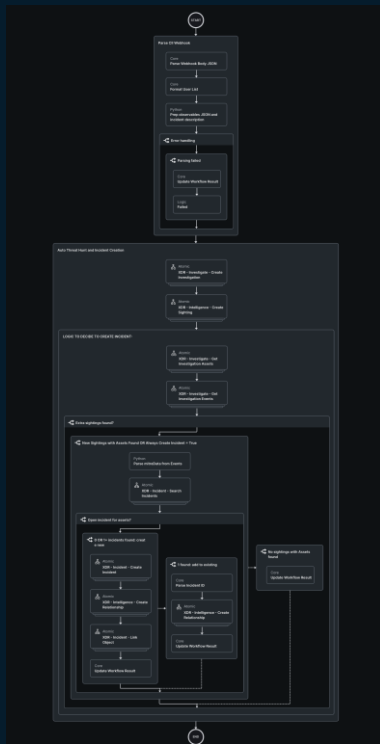
Cancel Save

Webhooks w/ Cisco XDR



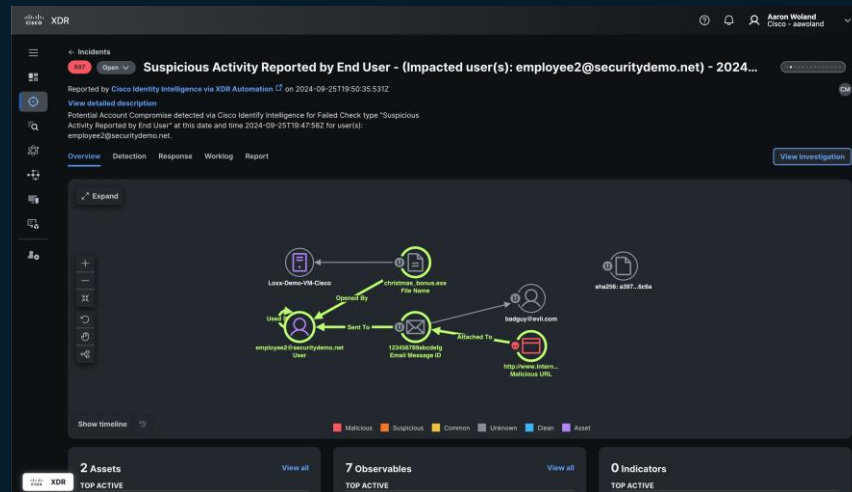
Published in Exchange

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



Merges with Incidents

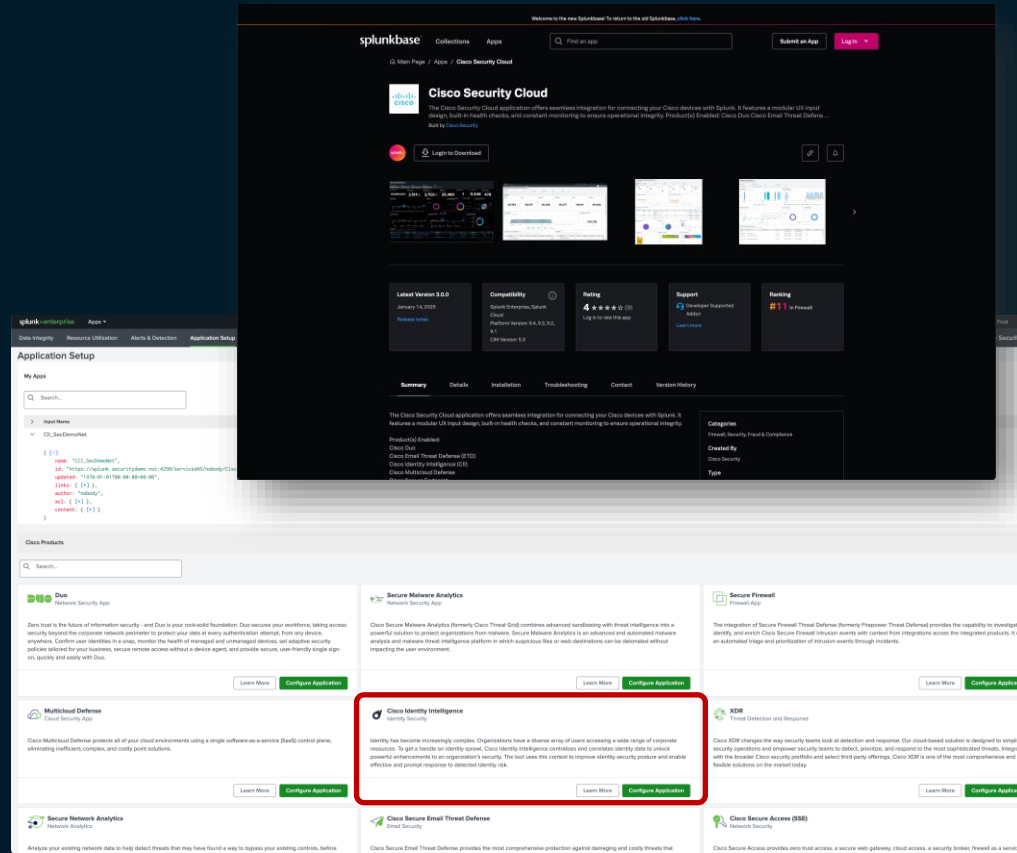
- The CII source events are correlated with the detections from other security products.
- The CII ITDR detection is now part of the attack graph & investigations



App (TA) in Splunk

Cisco Security Cloud App

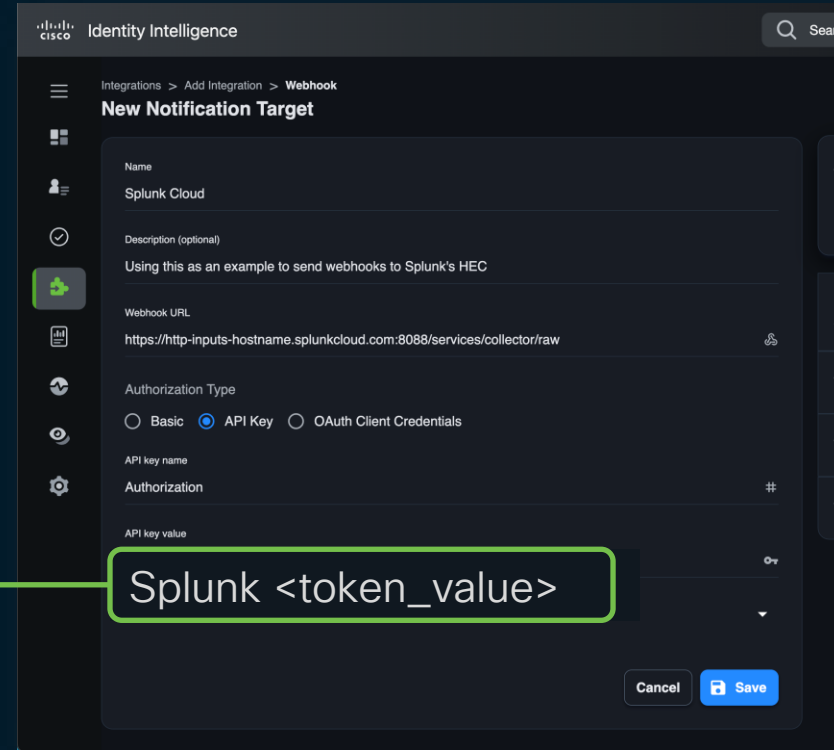
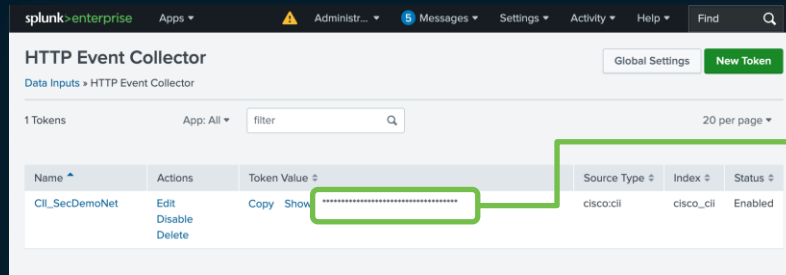
- Used for many Cisco Security Products, such as Duo, Firewall, etc.
- Cisco Identity Intelligence is included.
- Leverages an HTTP Event Collector (HEC) for Data input.
- Must use a public signed certificate (today).



Cisco Security App (TA) in Splunk

Add webhook in CII for the HEC in Splunk

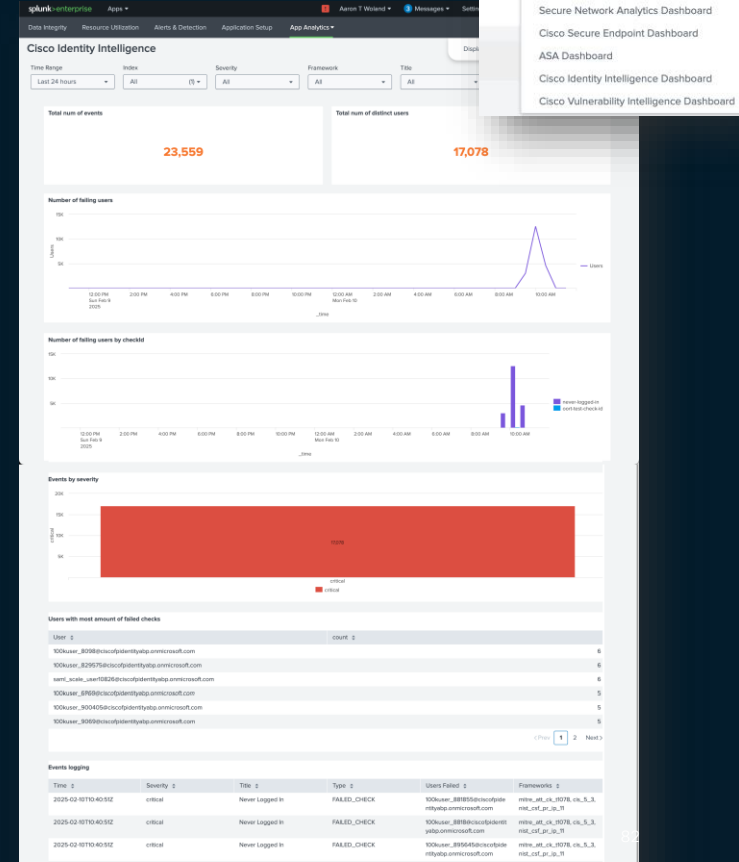
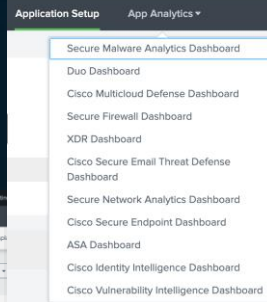
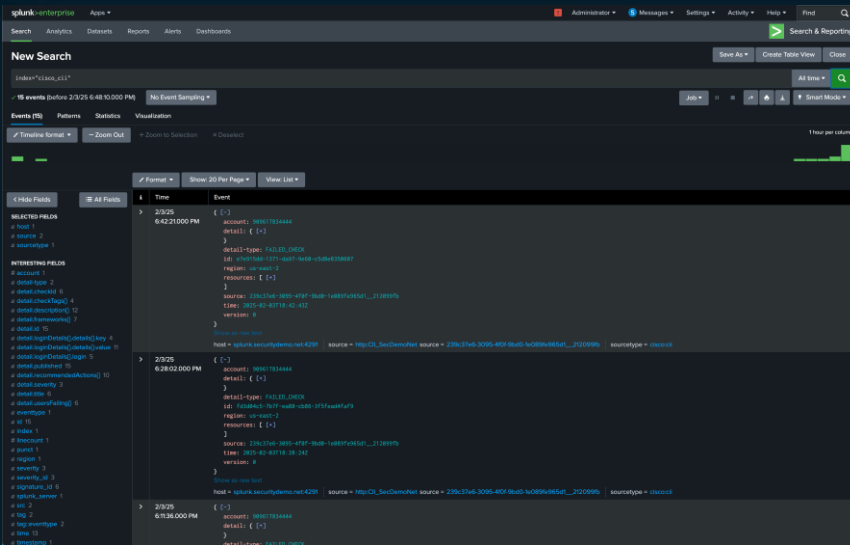
- Ensure the URL includes “/services/collector/raw”
- Authorization type = API Key
- API Key value must be “Splunk” + a space, then the token value.



Cisco Security App (TA) in Splunk

Cisco Identity Intelligence app has a dashboard

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



Agenda

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

Account Merges

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

The screenshot shows the Duo user management interface for a user named 'employee1'. The 'Username aliases' section contains two entries: 'Username alias 1' with the value '123456789' and 'Username alias 2' with the value 'employee1@securitydemo.net'. The 'Email' field at the bottom also contains 'employee1@securitydemo.net'. Red boxes highlight the 'Username alias 2' field and the 'Email' field, with red lines connecting them to the corresponding fields in the other screenshots.

The screenshot shows the Microsoft Azure AD user profile for 'EmployeeOne'. The 'Basic info' section displays the 'User principal name' as 'employee1@securitydemo.net', the 'Object ID' as '101e3689-1337-4df5-98f8-b5cbd46d1910', and the 'Created date time' as 'May 22, 2019, 4:20 PM'. A red box highlights the 'User principal name' field, with a red line connecting it to the 'Username' field in the Okta screenshot.

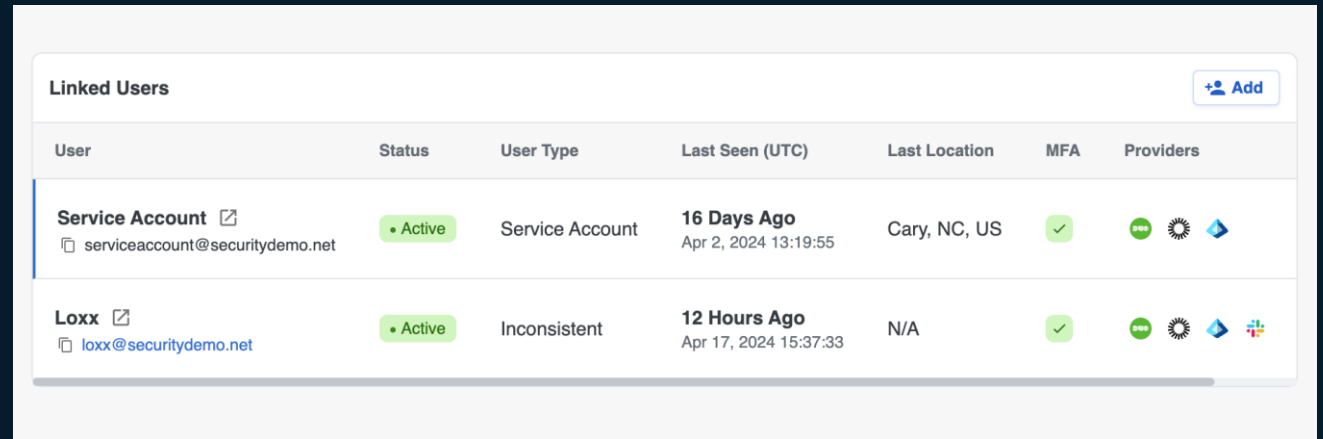
The screenshot shows the Okta user profile for 'Employee One'. The 'Attributes' section displays the 'Username' as 'employee1@securitydemo.net' and the 'login' attribute. A red box highlights the 'Username' field, with a red line connecting it to the 'User principal name' field in the Azure AD screenshot.









Linking Accounts

Not a merge, a linkage

For example, a privileged admin creates a service account.

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



User	Status	User Type	Last Seen (UTC)	Last Location	MFA	Providers
Service Account   serviceaccount@securitydemo.net	• Active	Service Account	16 Days Ago Apr 2, 2024 13:19:55	Cary, NC, US		
Loxx   loxx@securitydemo.net	• Active	Inconsistent	12 Hours Ago Apr 17, 2024 15:37:33	N/A		

Suggesting Linkages

Link Suggestions

CIl will merge accounts automatically.

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

Link Suggestions

I call this the "Google photos" feature..

Is this the same user?

- Link
- Reject
- Skip for now

The screenshot shows the Cisco Identity Intelligence user interface. At the top, the user is logged in as Aaron Woland. The main content area displays the profile for 'Users > aawoland@cisco.com'. A yellow box highlights a notification: 'Users aawoland@cisco.com and several others have the same user name. Do you want to link them?' with 'Dismiss' and 'Review' buttons. A modal dialog is open in the foreground with the title 'These accounts might belong to the same user'. The dialog contains the text: 'Review the following users that we identified with the same employee ID or similar usernames. Select users you would like to link with aawoland@cisco.com'. Below this, it says 'To add or remove existing linked users from this profile, go to the "Linked Users" table.' A table lists two accounts with the same username: 'Aaron Woland' (aawoland) and 'Aaron Woland' (aawoland@cisco.com). Each account has three radio buttons labeled 'Link', 'Reject', and 'Skip for now'. At the bottom of the dialog are 'Cancel' and 'Confirm Linkage' buttons.

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

The screenshot shows the Cisco Identity Intelligence (CII) interface. The left sidebar contains navigation options like Compatibility, Compliance, Severity, Topic, Frameworks, and Scopes. The main area displays a list of checks under the heading 'All Checks'. Two checks are highlighted with a red box:

Check	# Falling	# Excluded	Report Channels
Activity From Untrustworthy ISP • Moderate End Users - Identity Threat Insight	0	0	+ Add
IP Threat Detected • Critical End Users - Identity Threat Insight	0	0	+ Add

Below the screenshot, a detailed view of the two highlighted checks is shown:

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

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 sidebar on the left contains navigation icons: a hamburger menu, a grid, a person icon, a checkmark, a puzzle piece, a clock, an eye, and a gear. 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'. Three dropdown menus are visible: 'Admins group' with 'oort_admins' selected, 'Helpdesk group (optional)' with 'oort_helpdesk' selected, and 'Read-only group (optional)' with 'oort_ro' selected. At the bottom right of the form, there are 'Cancel' and 'Save' buttons.

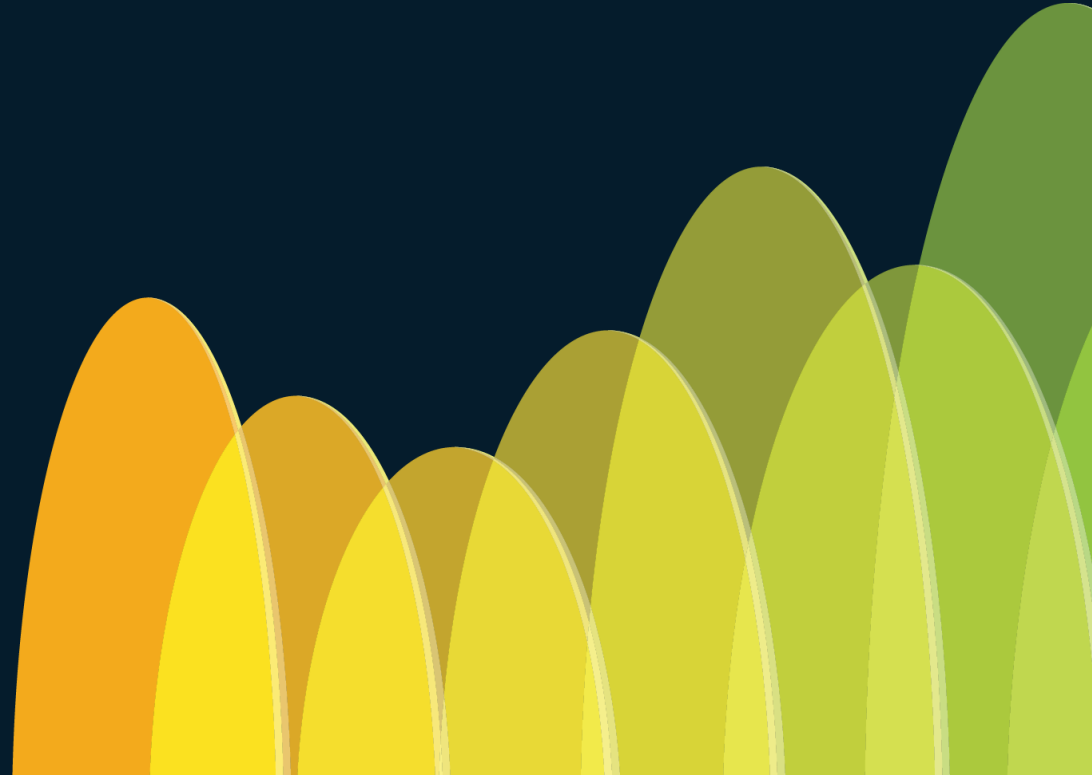
Advanced Search

- 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. The top navigation bar includes the Cisco logo, 'Identity Intelligence', a search bar, and the user profile 'Loxx security-demo-net'. The main content area is divided into several sections:

- Filters:** A sidebar on the left lists various filters such as Status (Active, Deleted, Deprovisioned, Inactive, Inconsistent), Sources (G-Suite, SecDemo, Azure, Stack), User Type, and Groups.
- Query Builder:** A central area shows a KQL query: `NOT Status:(3 conditions) AND ...`. A 'Switch to advanced mode' dialog box is open, explaining that clicking the button switches to advanced mode and that custom queries will be erased.
- Results Table:** A table displays search results for users. Each row includes a user name, email, and various attributes like 'Number of failing checks', 'Last seen', and 'Last sign in result'. The table also shows a list of checks associated with each user, such as 'adActiveLicenses.keyword' and 'appNames.keyword'.

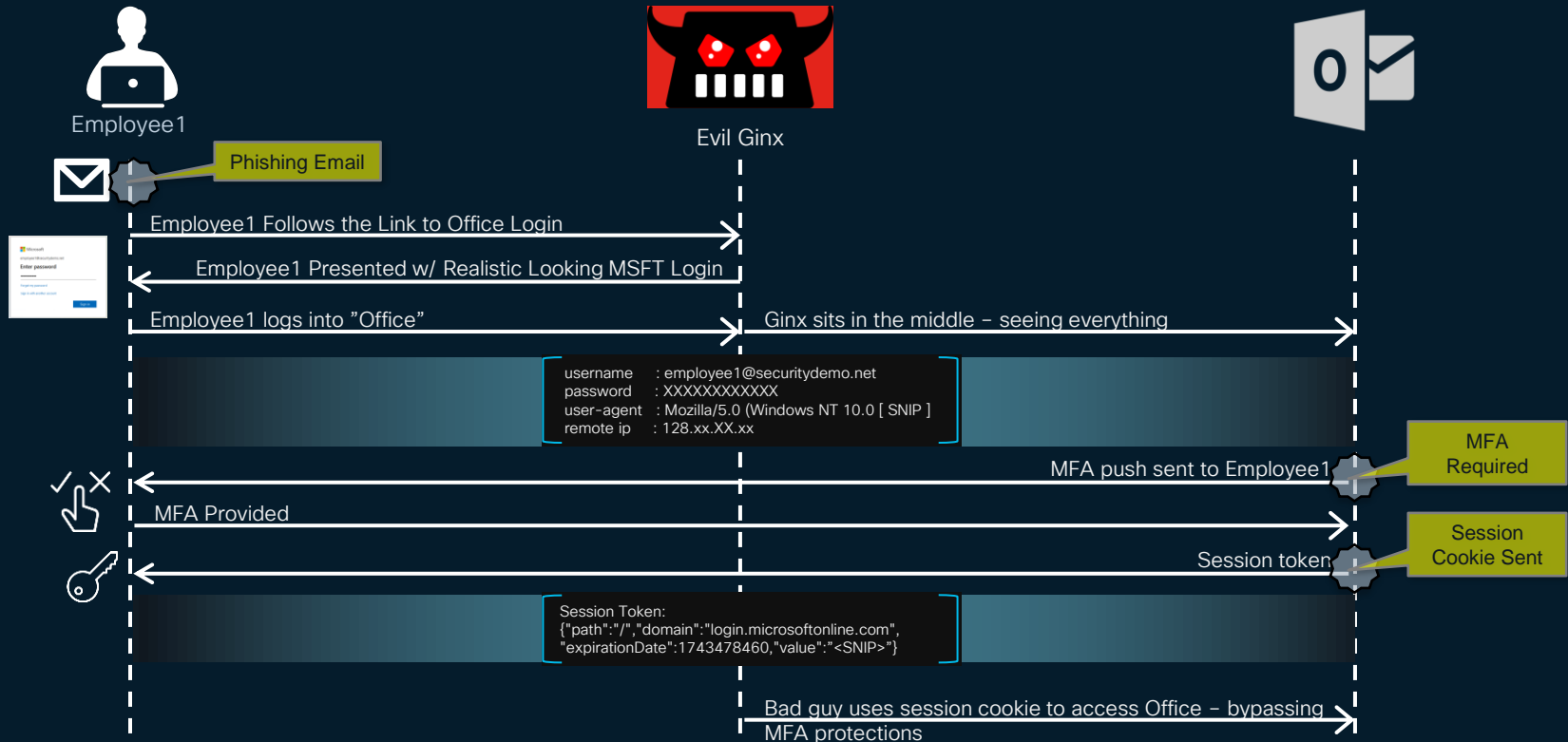
Session Hijacking Example



Session Hijacks are on the rise

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

Session Hijacking Example



What the Bad Actor sees

Lure them in

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

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

Bad Guy sees everything

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

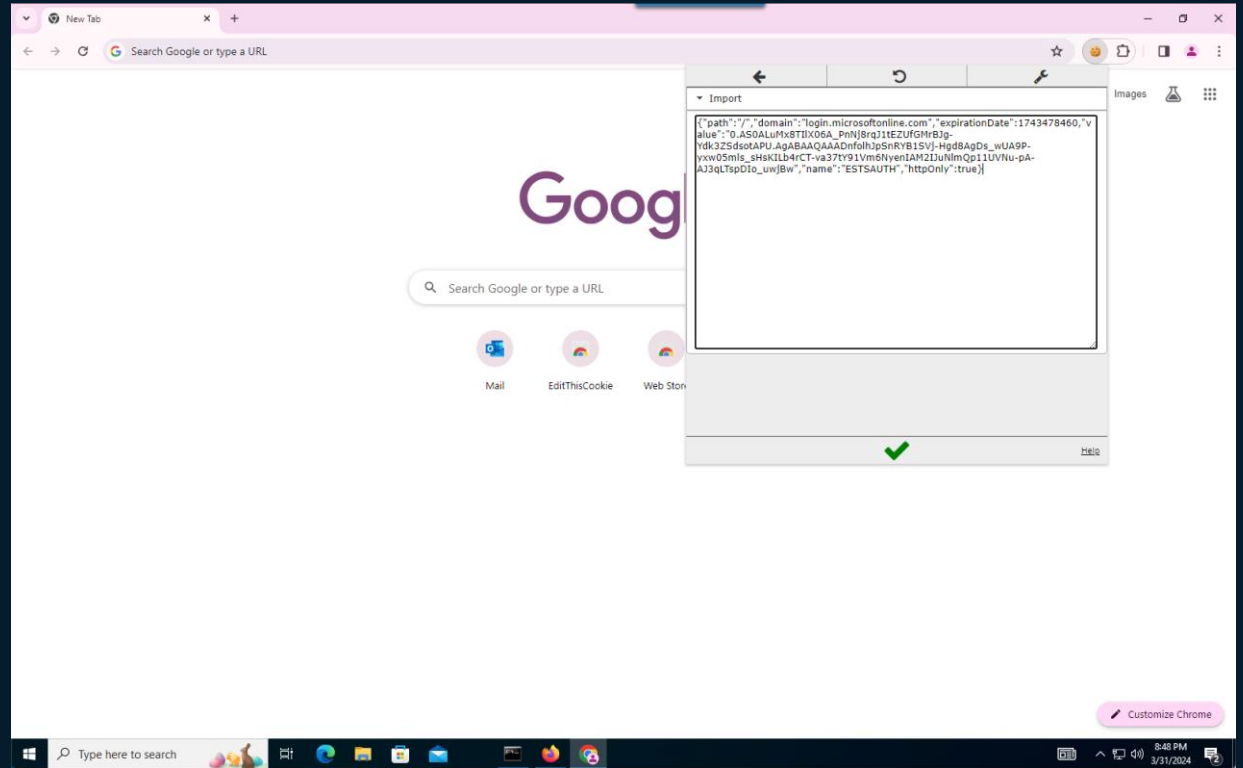
```
onelogin | disabled | visible |
outlook | disabled | visible |
paypal | disabled | visible |
protonmail | disabled | visible |
reddit | disabled | visible |
tiktok | disabled | visible |
twitter | disabled | visible |
twitter-mobile | disabled | visible |
wordpress.org | disabled | visible |

: lures
: sessions

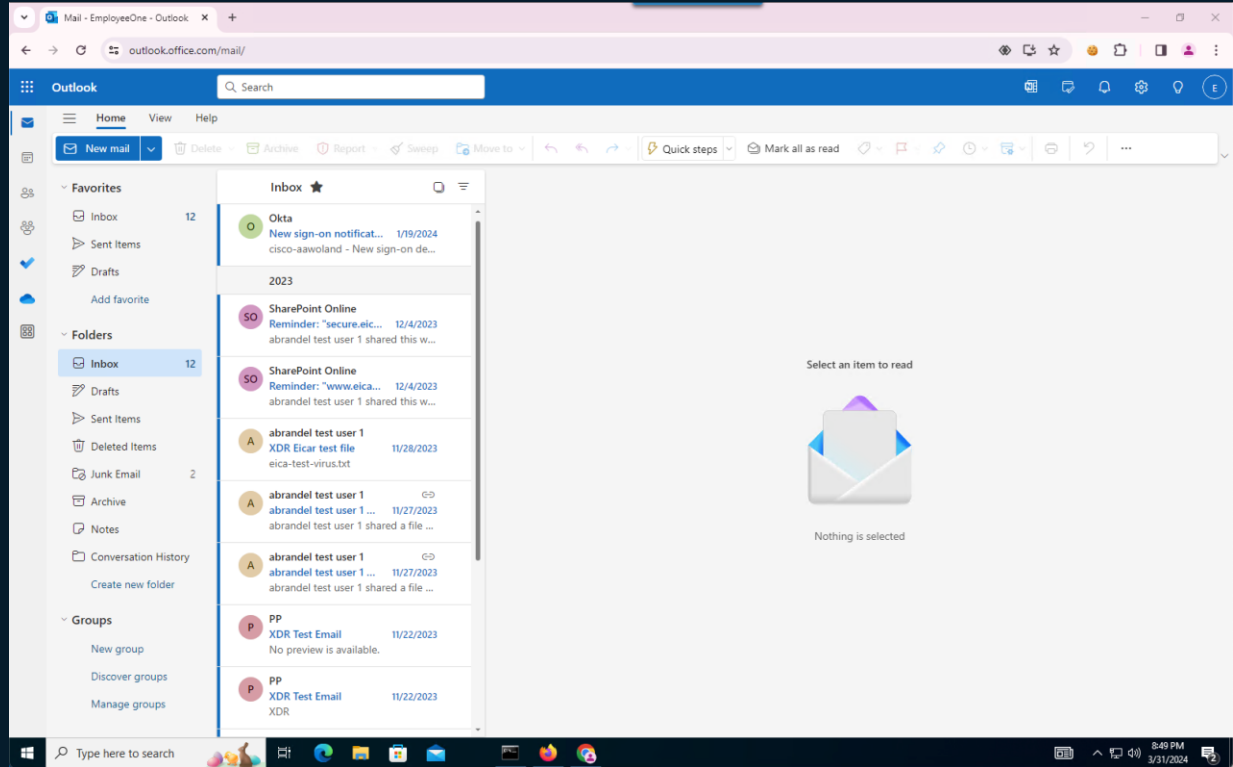
id | phishlet | hostname | path | redirector | redirect_url | paused | og |
---|---|---|---|---|---|---|---|
0 | o365 | | /spRqalIF | | | | |

[03:09:25] [war] [o365] request to hidden phishlet: https://Login.securitydemo.net/spRqalIF (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
:
:
[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/spRqalIF
[03:10:54] [inf] [0] [o365] Username: [employee1@securitydemo.net]
[03:10:54] [inf] [0] [o365] Password: [REDACTED]
[03:10:58] [inf] [0] [o365] all authorization tokens intercepted!
: phishlets hide o365
03:11:49] [inf] phishlet 'o365' is now hidden and all requests to it will be redirected
:
:
[03:11:57] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEwmm/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile DeviceUID: VendorUID: AppPkgID: ee.delfi.delfi) [146.190.197.169]
[03:12:09] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEwmm/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile DeviceUID: VendorUID: AppPkgID: ee.delfi.delfi) [15.161.55.89]
[03:12:15] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEwmm/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile DeviceUID: VendorUID: AppPkgID: ee.delfi.delfi) [206.189.247.132]
[03:12:23] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEwmm/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile DeviceUID: VendorUID: AppPkgID: ee.delfi.delfi) [18.170.98.205]
: sessions
:
id | phishlet | username | password | tokens | remote ip | time |
---|---|---|---|---|---|---|
1 | o365 | employee1@... | 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

Agenda

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

User Trust Level

Who: Cross-Functional Team

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

What it Is:

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

What it's Not:

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

Not a numeric value!

Trust Level Approach



Trusted
Favorable
Neutral
Questionable
Untrusted

Simplicity

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

Explainability

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

Use Cases

Authentication, Authorization & Access decisions

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

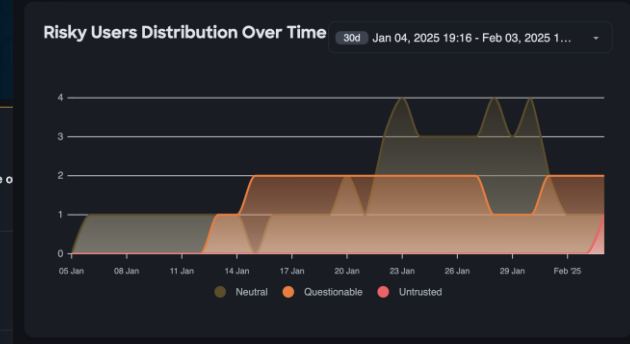
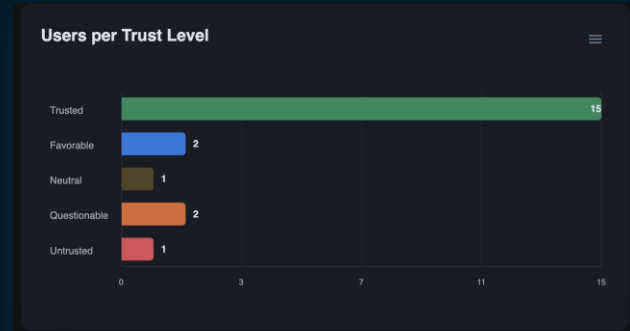
Threat Prioritization

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

Trust Level Nuggets

User is assigned a trust level based on activity.

- No activity = no level
- Explainability shows why a user has the assigned level



Trust Level ⓘ
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

Trust Level as Criteria in Security Policy

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



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

Example Wireframe: Secure Access

Trust Levels

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

Note: this is not the final design

The screenshot displays the Cisco Secure Access dashboard for User Trust Profiles. The main content area shows a table of trust levels and their associated controls. A yellow box highlights the 'Trust level' column, and a yellow arrow points from the 'Trust Levels' text on the left to this box. A 'Trusted' settings panel is open on the right side of the screen.

Profile name	Assigned to	Used in
System-provided	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 (SSO) [checked]
Step up authentication [unchecked]
Address (Most secure) [unchecked]
Block [unchecked]

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 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 console interface. The main content area shows a table of users with columns for Name, Email, Source, Directory, Trust Level, and Connected (VP). The 'Trust Level' column is highlighted with an orange box. A callout box on the right provides details for the user 'aalto.helmig 2', showing their Trust Level is 'Neutral' and listing factors such as 'SpecialAccount' and 'WeakMfaUsed'.

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

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

Identity Posture

The overall level for your organization

Provides a “guide” to gamify the cleanup of your ID environment & policies

Can use the trend to ensure your organization is going in the right direction



Identity Posture

The overall level for your organization

Provides a “guide” to gamify the cleanup of your ID environment & policies

Can use the trend to ensure your organization is going in the right direction

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

Agenda

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

CII Public API

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

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.

[Download](#) Cisco Identity Intelligence Public API.postman_collection.json (11KB)

[Previous](#) Report as a Service (Raas) [Next](#) APIs

Powered by GitBook

Last updated 14 days ago

GraphQL Explorer Tools

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

The screenshot displays the Hasura GraphQL Explorer interface. At the top, it shows the GraphQL Endpoint as `POST https://api.integration.oort.io/api`. Below this, the Request Headers section is visible, with a table containing the following data:

ENABLE	KEY	VALUE
<input checked="" type="checkbox"/>	content-type	application/json
<input checked="" type="checkbox"/>	Authorization	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsImtZCI6Ii9UWzV3NWdnMlVncENSY0I4d2M3aCJ9.ejpc3
	Enter Key	Enter Value

The main interface is divided into three panes. The left pane, titled "Explorer", shows a tree view of the schema with the following structure:

- query MyQuery
- getEndUser
- getEndUserState
- getEndUsersByIp
- getIntegrationsStatus
- getTotalCheckFailingCounts
- listAdminLogins
- listEndUsers
 - input*
 - orderBy:
 - pageSize:
 - pageToken:
 - items
 - company
 - department
 - devices
 - deviceId
 - deviceType
 - displayName
 - lastSeen
 - os
 - provider
 - displayName
 - emails
 - employeeIds
 - failingChecks
 - firstCreatedDate
 - groupNames

The middle pane shows the GraphQL query:

```
1 query MyQuery {
2   listEndUsers(input: {}) {
3     items {
4       company
5       department
6     }
7     devices {
8       deviceId
9       deviceType
10      displayName
11      lastSeen
12      os
13      provider
14    }
15    displayName
16    emails
17    employeeIds
18    failingChecks
19    groupNames
20    firstCreatedDate
21    hashMoreGroups
22    id
23    lastActive
24    lastSignIn {
25      ipAddress
26      location {
27        city
28        country
29        state
30      }
31    }
32  }
33 }
```

The right pane shows the JSON response:

```
{
  "data": {
    "listEndUsers": {
      "items": [
        {
          "company": null,
          "department": null,
          "devices": [],
          "displayName": "aaron@woland.com",
          "emails": null,
          "employeeIds": null,
          "failingChecks": [],
          "groupNames": [],
          "firstCreatedDate": null,
          "hasMoreGroups": false,
          "id": "4e384171-e293-4c17-a2da-ba50dc445f54_aaron@woland.com",
          "lastActive": null,
          "lastSignIn": null,
          "linkedEndUserLogins": null,
          "login": "aaron@woland.com",
          "managerLogin": null,
          "mfaEnabled": false,
          "phoneNumbers": [],
          "providers": [
            "SLACK"
          ],
          "status": "INACTIVE"
        }
      ]
    }
  }
}
```

Agenda

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

Call to Action

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

Q & A

CISCO *Live!*



Webex App

Questions?

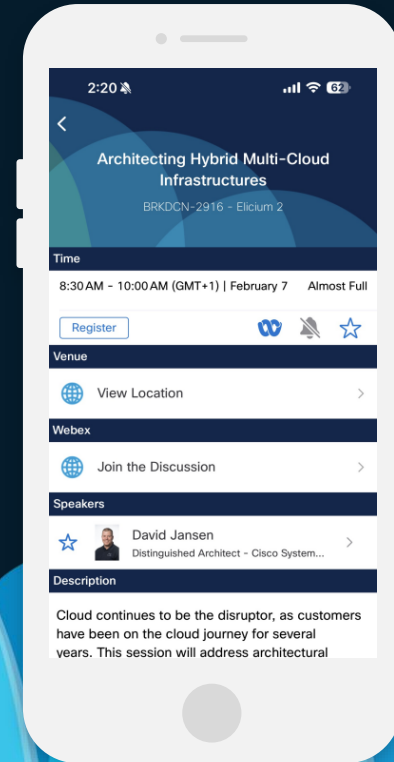
Use the Webex app to chat with the speaker after the session

How

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

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

CISCO *Live!*



Fill Out Your Session Surveys



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

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



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



Content Catalog

Continue your education

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



Thank you

CISCO *Live!*