The bridge to possible

Security Automation

Developing with SecureX

Matt Vander Horst
Technical Leader

Cisco Webex App

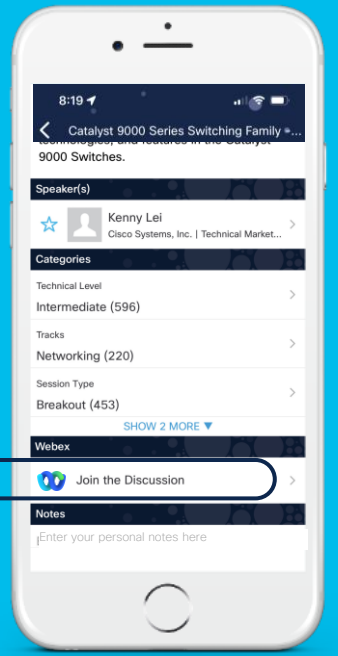
Questions?

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 until February 24, 2023.



Agenda

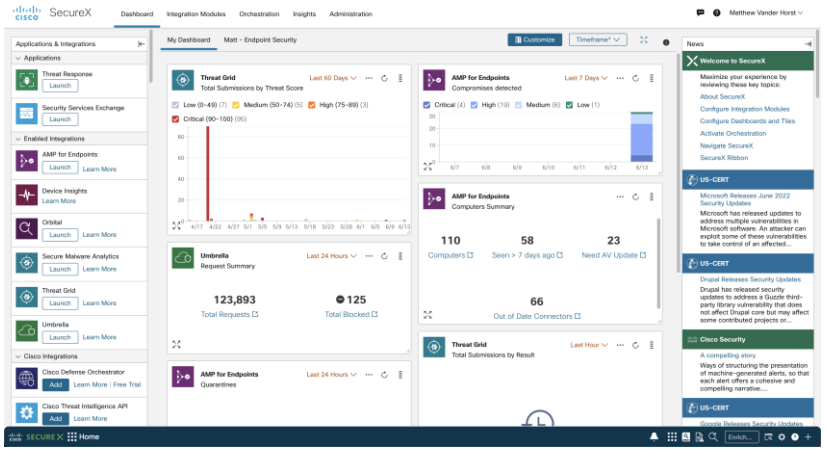
- Integration Modules
- APIs
- SecureX Orchestration
- Resources

Matt Vander Horst

- 8 years at a Fortune 100 insurance company
  - Network engineering
  - Cisco ISE
  - Software/DevOps
- 3 years at Cisco
  - SecureX
  - Automation and orchestration

What is SecureX?

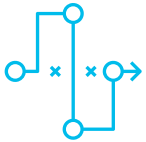
- Platform for centralized visibility and actionability across the Cisco Secure portfolio
- Integrates with both Cisco and third-party products
- Features include:
  - Dashboard
  - Threat Response
  - Orchestration
  - Device Insights
  - Cisco Secure Client



Developing with SecureX

Integration Modules

APIs



Orchestration

SecureX

Integration Modules

- Allow SecureX to communicate with other products
  - Both Cisco and Third Party
- Uses the Cisco Threat Intelligence Model (CTIM) to represent data
- Available by:
  - Enabling in SecureX
  - Browsing Cisco's GitHub
  - Writing your own

Secure X

Integration Modules

- Module Capabilities:
  - Observe
    - Provides a summary of data for an observable
      - Indicators
      - Verdicts
      - Judgements
      - Sightings
      - and more…
  - Deliberate
    - Provides verdicts with a disposition
      - Clean, Unknown, Malicious, Suspicious

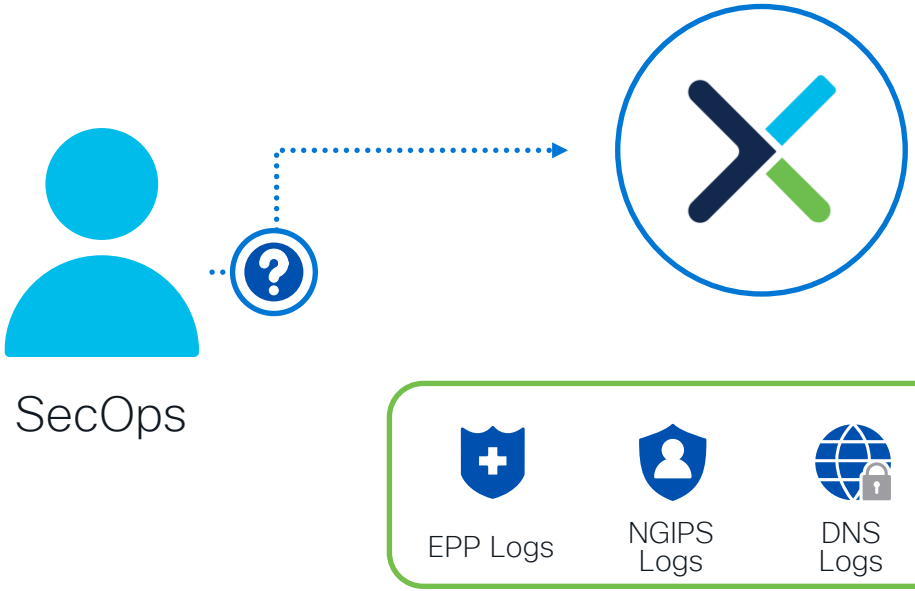
SecureX

Integration Modules

- Module Capabilities:
  - Respond
    - Provides response actions (these appear primarily in pivot menus)
  - Refer
    - Provides links to other resources or tools
  - Dashboard
    - Provides dashboard tiles and their data

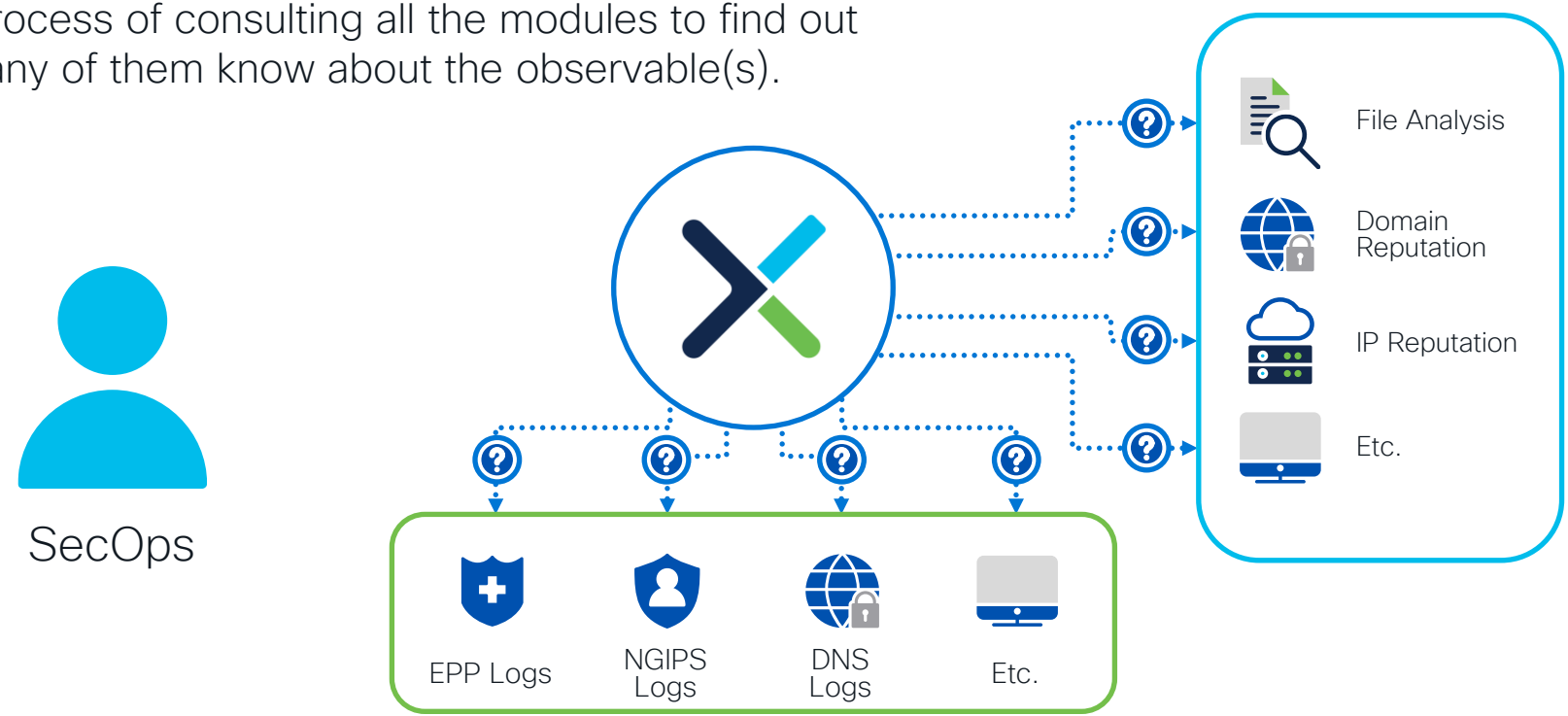
Enrichment Demo

The process of consulting all the modules to find out what any of them know about the observable(s).



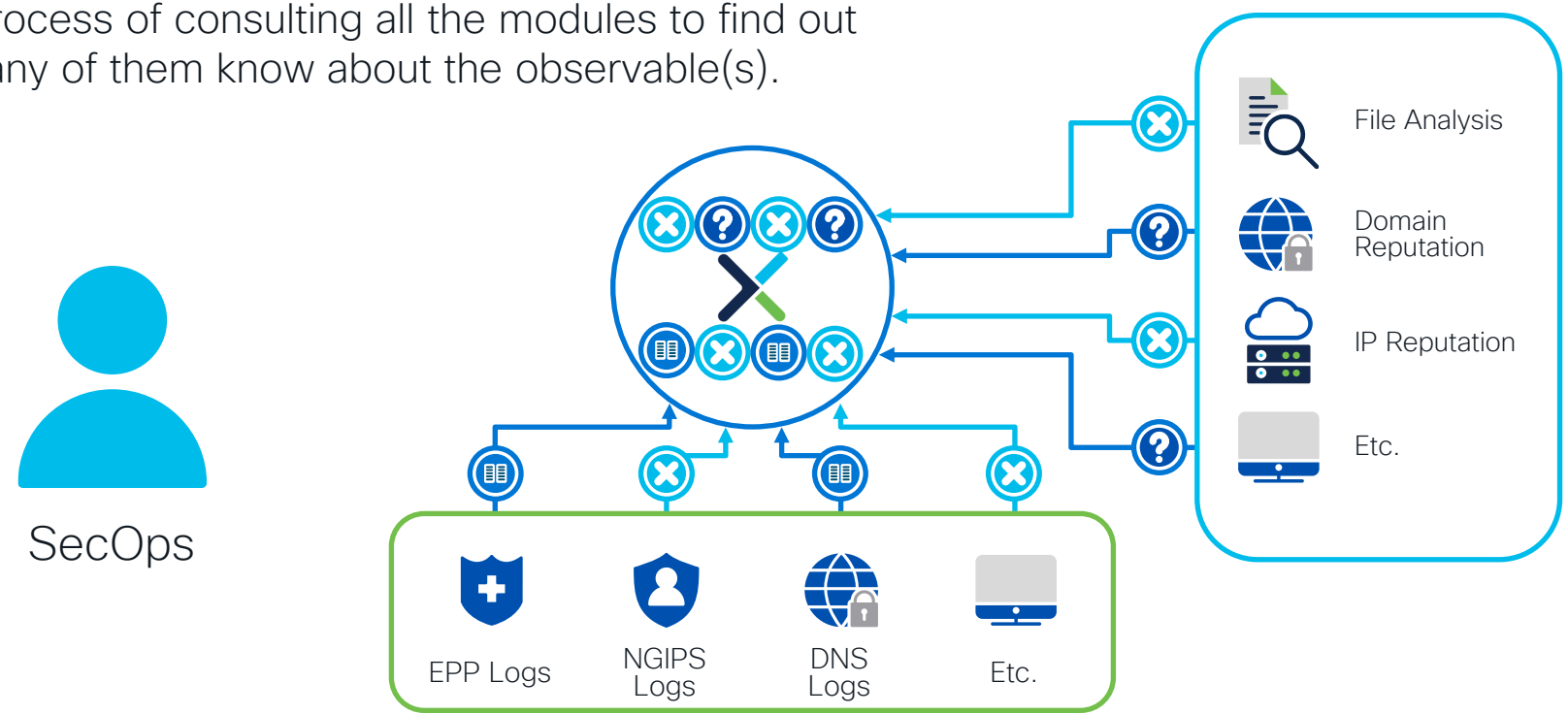
Enrichment Demo

The process of consulting all the modules to find out what any of them know about the observable(s).



Enrichment Demo

The process of consulting all the modules to find out what any of them know about the observable(s).



Sample Integrations

Cisco

Duo Security

Secure Endpoint

Secure Malware Analytics

Secure Cloud Analytics

Umbrella

Secure Email

Third Party

Splunk

Microsoft Graph Security API

Farsight DNSDB

Gigamon

Exabeam

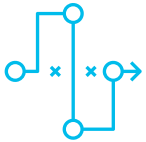
ServiceNow

More: http://cs.co/threatresponseintegrations

Developing with SecureX

Integration Modules

APIs



Orchestration

SecureX

APIs

- SecureX has multiple different APIs
- Provide unique functionality to SecureX
  - For example: inspecting content for observables
- Provide a conduit to integration modules and their aggregated data
- Require an API key generated in SecureX with the appropriate scopes

SecureX

APIs: Private Intelligence

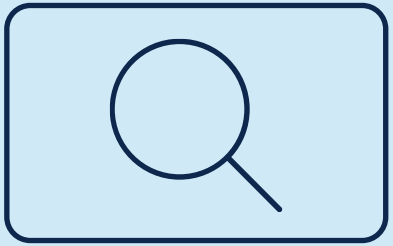
- Uses the Cisco Threat Intelligence Model (CTIM) to represent data
- APIs for:
  - Casebooks
  - Incidents
  - Indicators
  - Judgements
  - Sightings
  - Verdicts

SecureX

APIs: Threat Response

- Uses the Cisco Threat Intelligence Model (CTIM) to represent data
- APIs for:
  - Inspect
  - Observe
  - Deliberate
  - Refer
  - Respond

What can we do with these APIs?

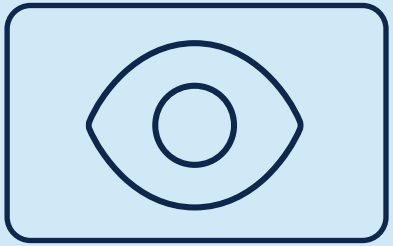


Inspect

- Extract observables from a body of text

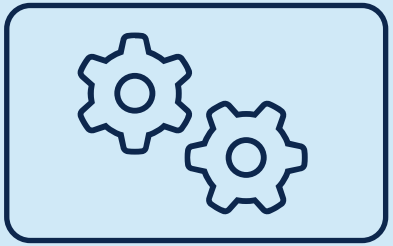
Deliberate

- Get dispositions for observables:
  - Clean
  - Unknown
  - Malicious
  - Suspicious



Observe

- Ask each SecureX module if a given observable was seen in the environment



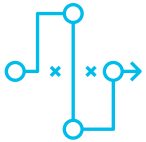
Respond

- Take action against an observable through a SecureX module
- Includes SecureX Orchestration

Developing with SecureX

Integration Modules

APIs



Orchestration

What is SecureX Orchestration?

Process **automation made simple** with a no/low-code drag-drop interface

Investigate

Reduce research and response times with workflows and playbooks that execute at machine speed

Automate

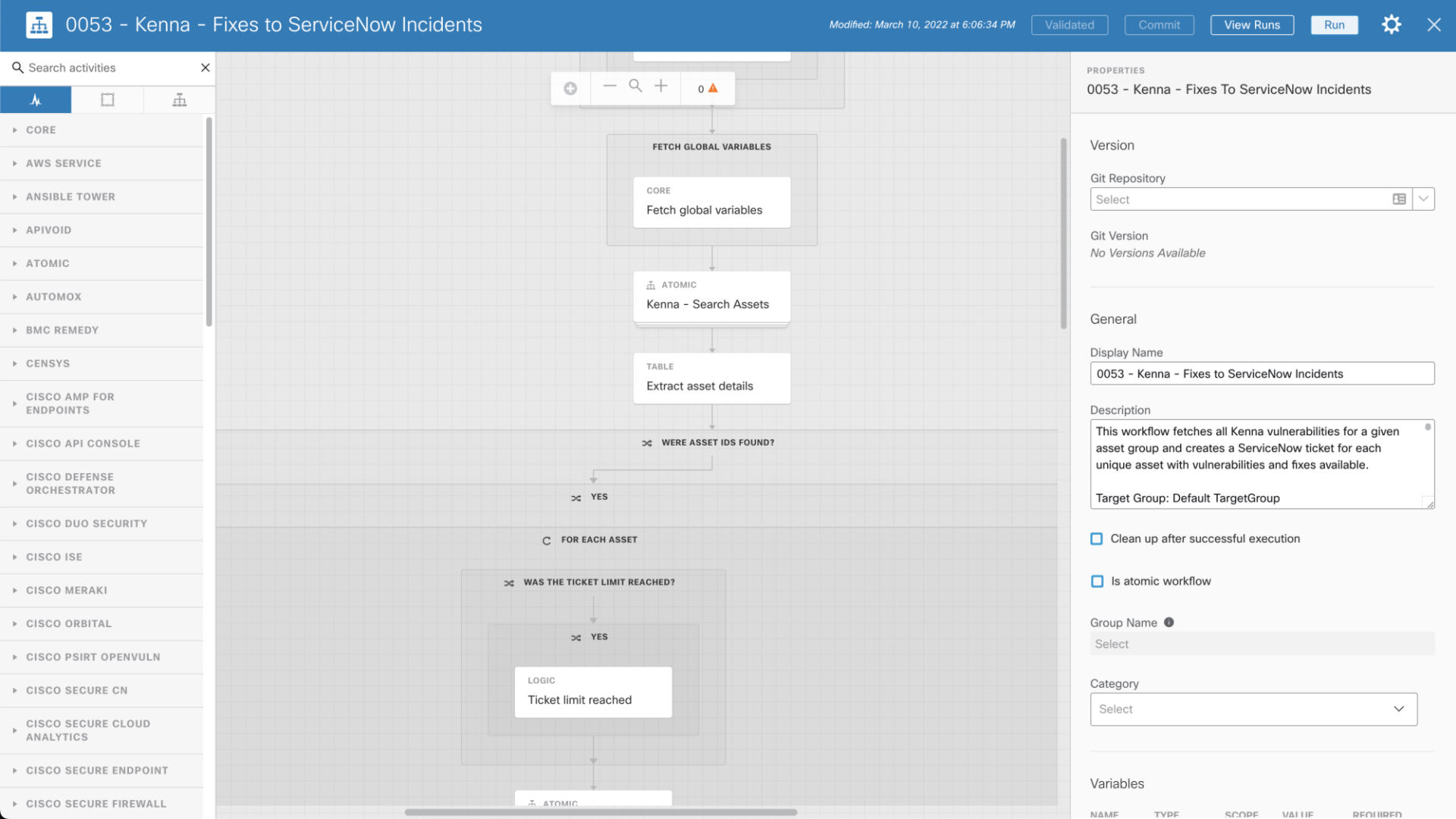
Eliminate repetitive tasks and reduce MTTR to increase productivity and focus on mission-critical projects

Integrate

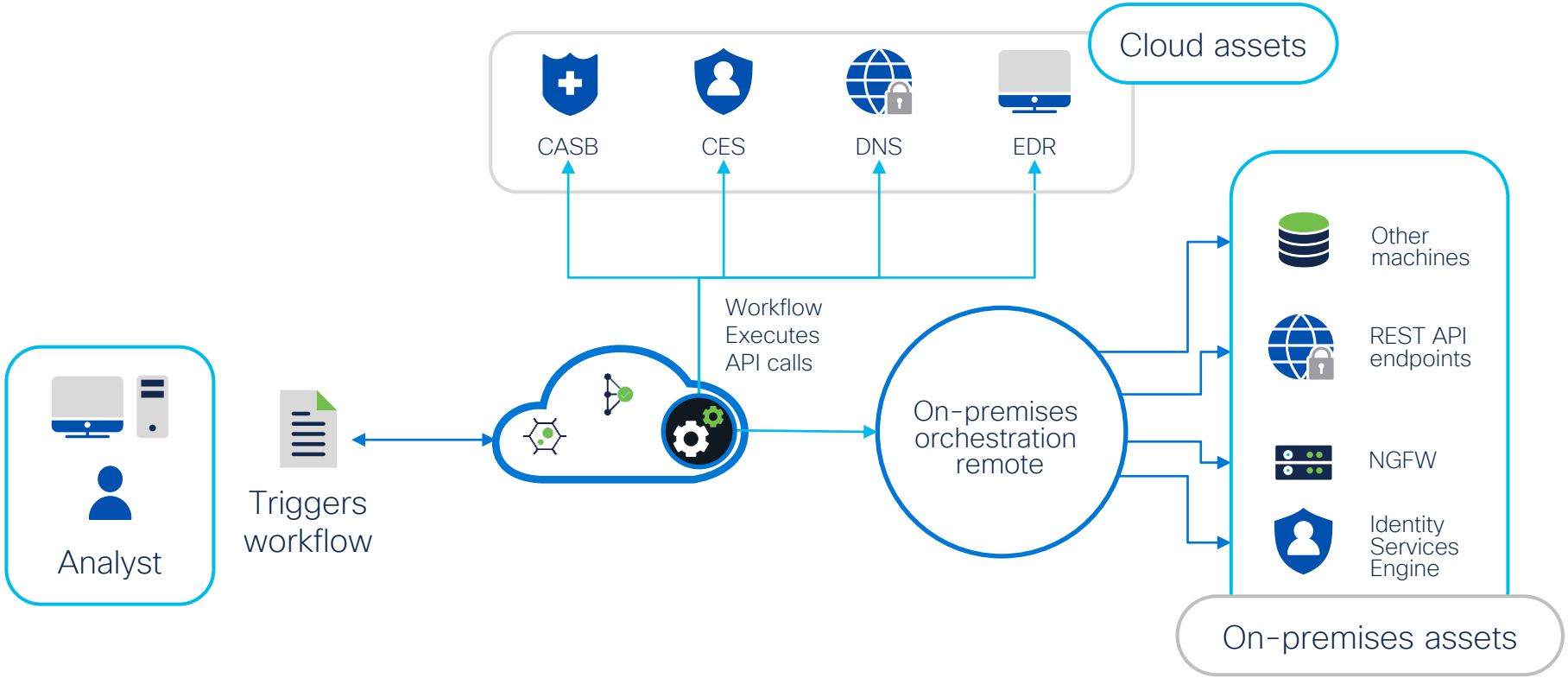
Unique turnkey approach to quickly integrate with other systems and solutions to expand your toolbox

Scale

Automation that scales infinitely and never takes a day off, delivering the same SLA around the clock


0053 - Kenna - Fixes to ServiceNow Incidents
Modified: March 10, 2022 at 6:06:34 PM
Validated
Commit
View Runs
Run
Search activities
CORE
AWS SERVICE
ANSIBLE TOWER
APIVOID
ATOMIC
AUTOMOX
BMC REMEDY
CENSYS
CISCO AMP FOR ENDPOINTS
CISCO API CONSOLE
CISCO DEFENSE ORCHESTRATOR
CISCO DUO SECURITY
CISCO ISE
CISCO MERAKI
CISCO ORBITAL
CISCO PSIRT OPENVULN
CISCO SECURE CN
CISCO SECURE CLOUD ANALYTICS
CISCO SECURE ENDPOINT
CISCO SECURE FIREWALL
0
FETCH GLOBAL VARIABLES
CORE
Fetch global variables
ATOMIC
Kenna - Search Assets
TABLE
Extract asset details
WERE ASSET IDS FOUND?
YES
FOR EACH ASSET
WAS THE TICKET LIMIT REACHED?
YES
LOGIC
Ticket limit reached
ATOMIC
PROPERTIES
0053 - Kenna - Fixes To ServiceNow Incidents
Version
Git Repository
Select
Git Version
No Versions Available
General
Display Name
0053 - Kenna - Fixes to ServiceNow Incidents
Description
This workflow fetches all Kenna vulnerabilities for a given asset group and creates a ServiceNow ticket for each unique asset with vulnerabilities and fixes available.
Target Group: Default TargetGroup
Clean up after successful execution
Is atomic workflow
Group Name
Select
Category
Select
Variables
NAME
TYPE
SCOPE
VALUE
REQUIRED

SecureX Orchestration



Demo

SecureX Module Resources

GitHub Repository

https://github.com/CiscoSecurity/

Module Maker

https://ciscosecurity.github.io/tr-05-module-maker/

Cisco Threat Intelligence Model (CTIM)

https://github.com/threatgrid/ctim/

SecureX API Resources

Inspect API

https://visibility.amp.cisco.com/iroh/iroh-inspect/

Enrich API

https://visibility.amp.cisco.com/iroh/iroh-enrich/

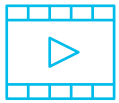
Response API

https://visibility.amp.cisco.com/iroh/iroh-response/

Private Intelligence

https://private.intel.amp.cisco.com/

SecureX Orchestration Resources



Videos

https://cs.co/SXO_videos

Documentation

https://cs.co/SXO_docs

GitHub Repository

https://cs.co/SXO_repo

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

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


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN