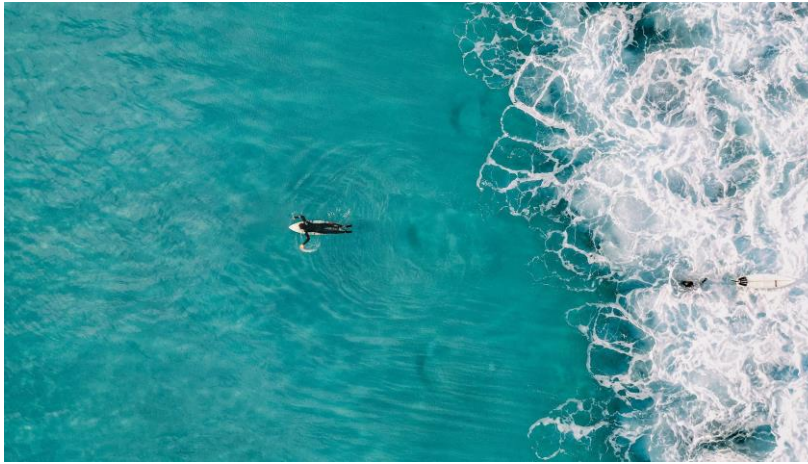
The bridge to possible

The Power of Customized Workflow Integration with SecureX

Pojchara Trainorapong (James), Systems Engineer

About Me



Cisco Webex App

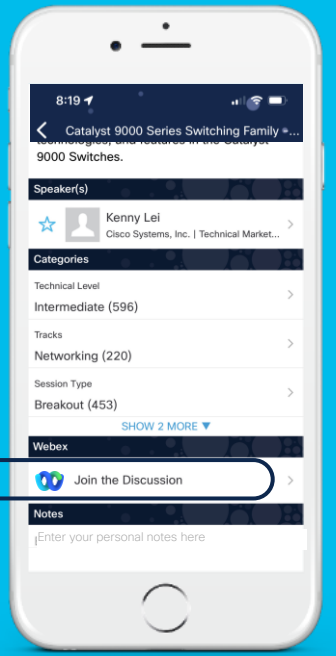
Questions?

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.



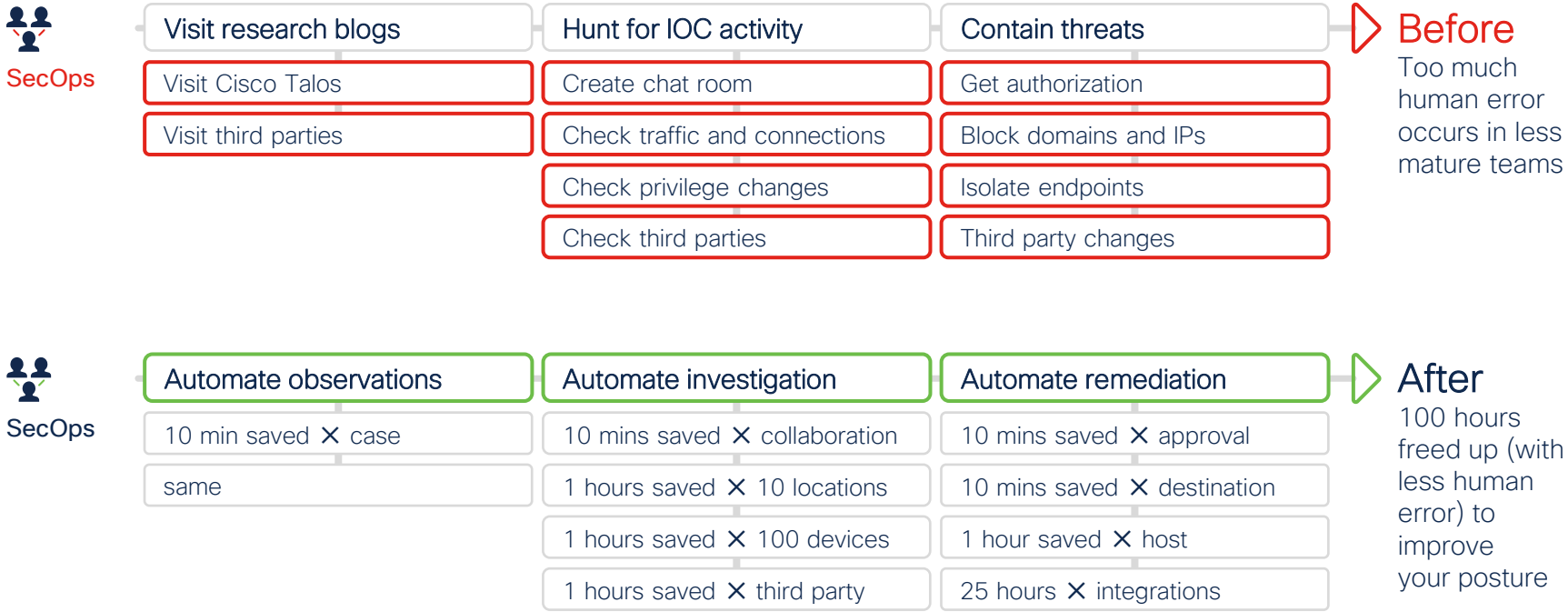
Agenda

- Introduction to SecureX
- Customized Orchestration Workflow
- Demo
- Conclusion

Introduction to SecureX

cisco Live!

Threat Hunting

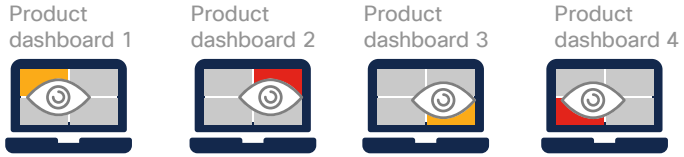


How true **simplicity** is experienced

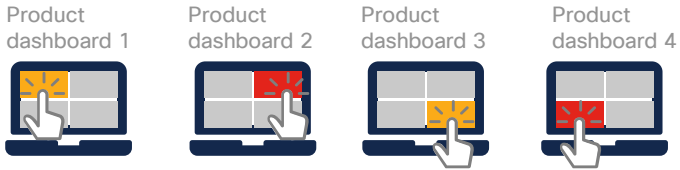
Before: 32 minutes

1. IOC/alert

2. Investigate incidents in multiple consoles



3. Remediate by coordinating multiple teams



After: 5 minutes

A platform approach that confidently tackles the most pressing security operation challenges

Simplicity

Integrate technology with true **turnkey interoperability**

Visibility

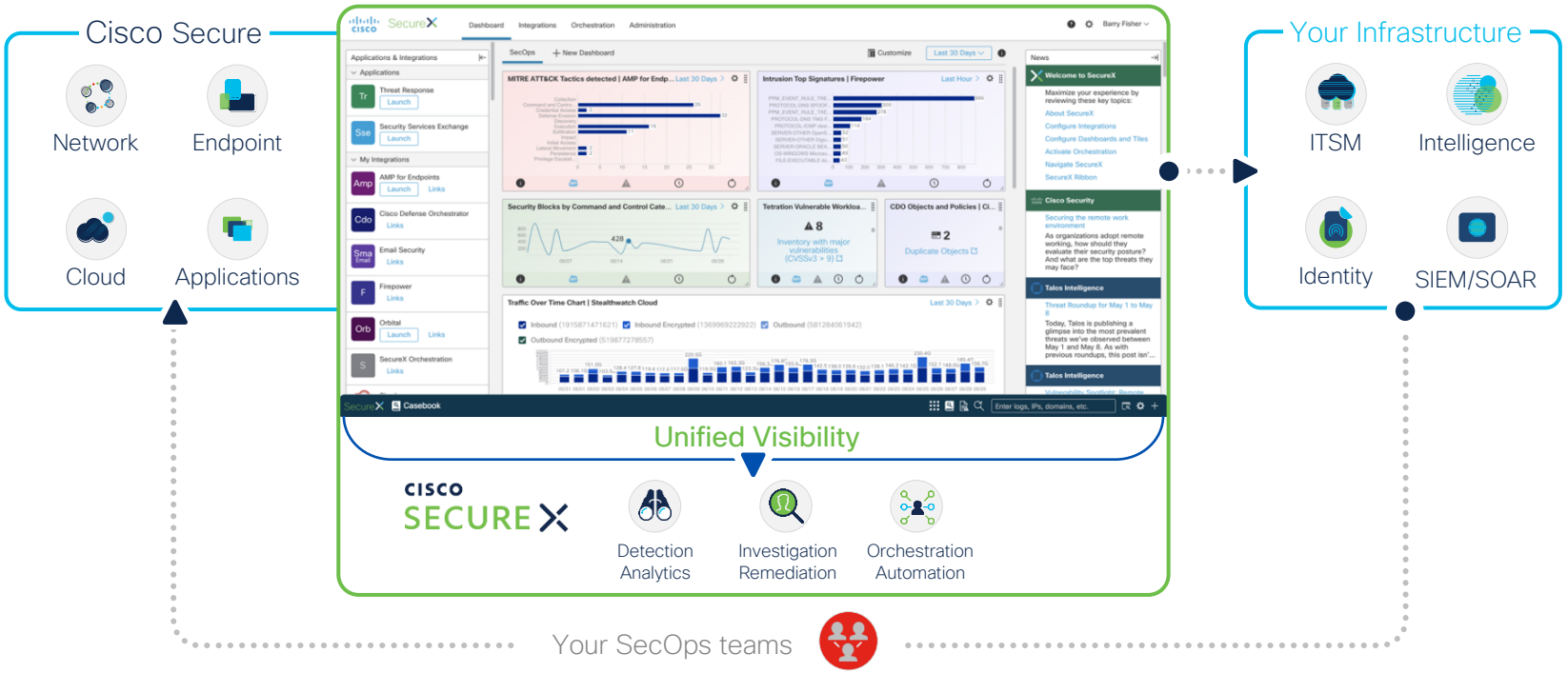
Accelerate **time to detect and investigate** threats and maintain contextual awareness

Efficiency

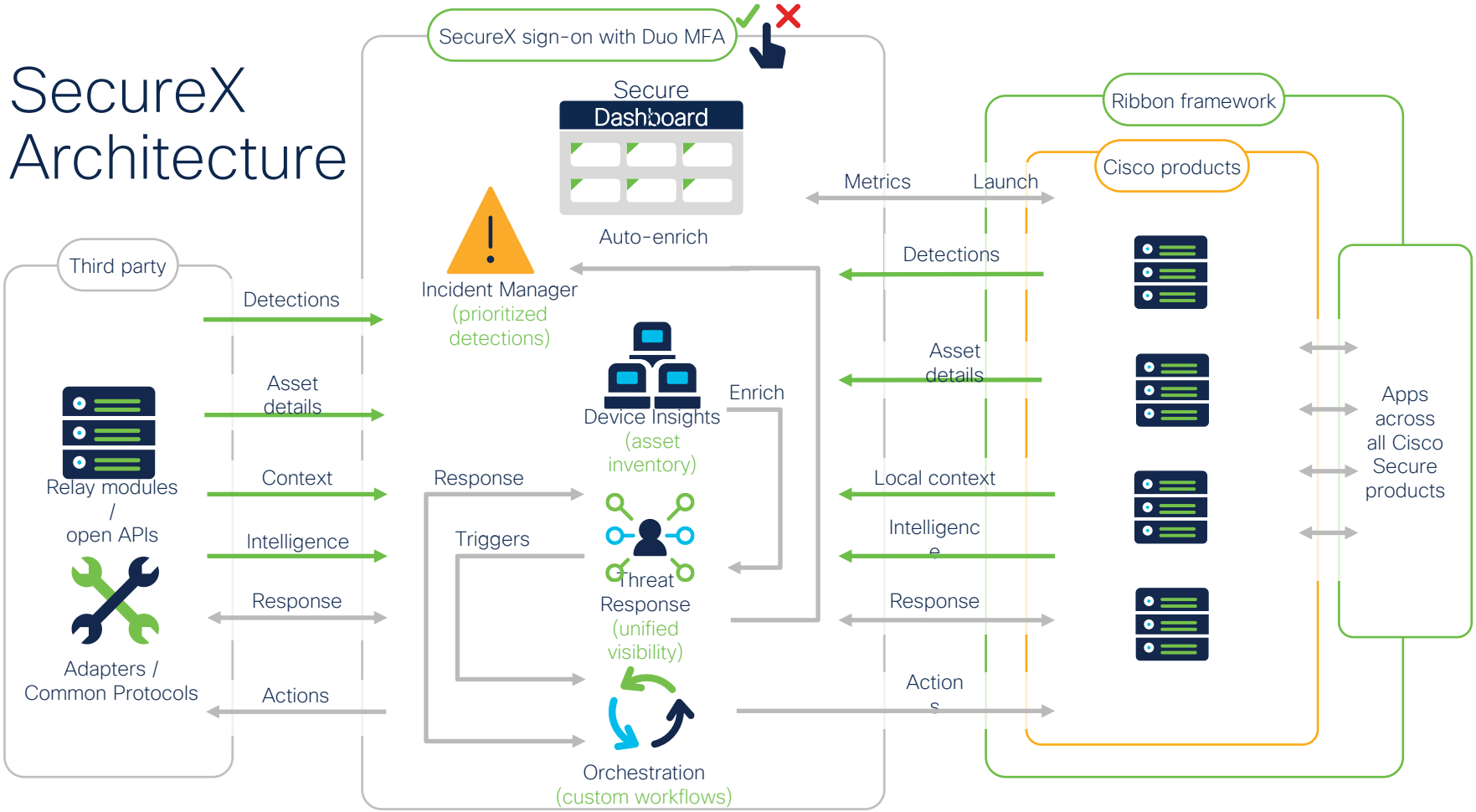
Accelerate **time to remediate** and automate workflows to lower costs and strengthen security

Cisco SecureX

A cloud-native, built-in platform experience within our portfolio



SecureX Architecture



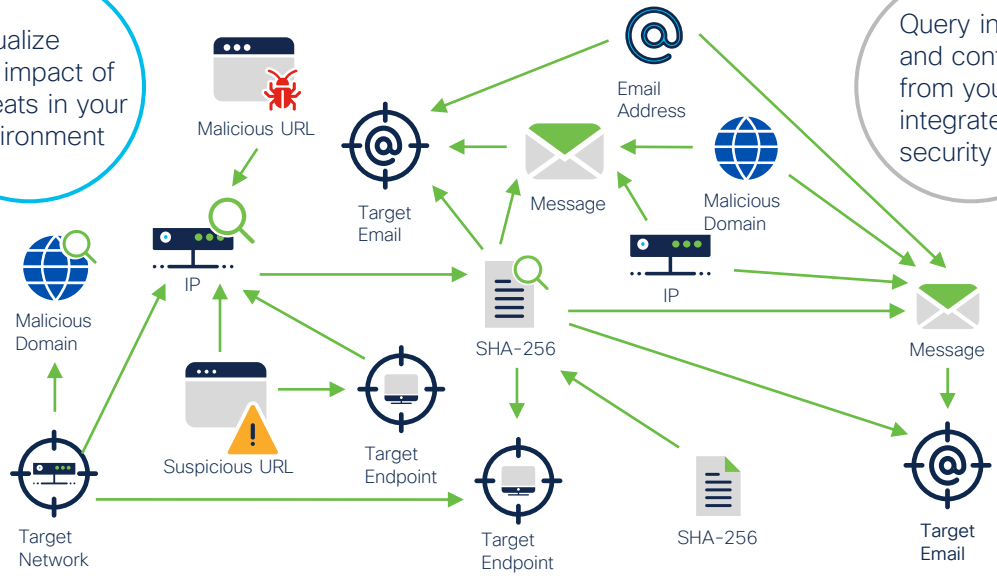
See and stop attacks in minutes with a few clicks

SecOps with SecureX Threat Response

Visualize the impact of threats in your environment

Extract observables from browser content with one click

- Security blogs
- Cisco interfaces
- Third-party interfaces



Query intel and context from your integrated security

85% reduction in time to respond and remediate to an attack

- Isolate hosts
- Block files
- Block destinations

Or eliminate the clicks, by automating this workflow

For Technical Reference

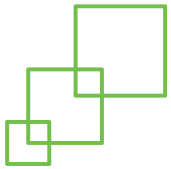
Searchable observables

SecureX Threat Response

amp_computer_guid
certificate_common_name
certificate_issuer
certificate_serial
cisco_mid
cisco_uc_id
device
domain
email
email_messageid
email_subject
file_name
file_path
hostname
imei
imsi
ip
ipv6
mac_address
md5

ms_machine_id
mutex
ngfw_id
ngfw_name
odns_identity
odns_identity_label
orbital_node_id
pki_serial
process_name
registry_key
registy_name
registry_path
s1_agent_id
serial_number
sha1
sha256
swc_device_id
url
user
user_agent

Simplifying SOC Operations with SecureX



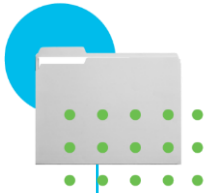
Integration Modules

APIs

Orchestration

Automation vs. Orchestration

Automation
The ability to perform individual, repetitive tasks.



Orchestration
The arrangement and coordination of automated and non-automated tasks, ultimately resulting in a consolidated process or workflow.

Why do customers want to Automate?

"I need to deploy new services quicker; customer demand is drowning me."

"I have repetitive tasks we are doing manually – I need to free up people to do other value-added work"

"I need a way to do more with less" (shrinking budgets)

"I have an aging workforce that I can't replace with experienced network operators – I need to capture that IP into automated workflows."

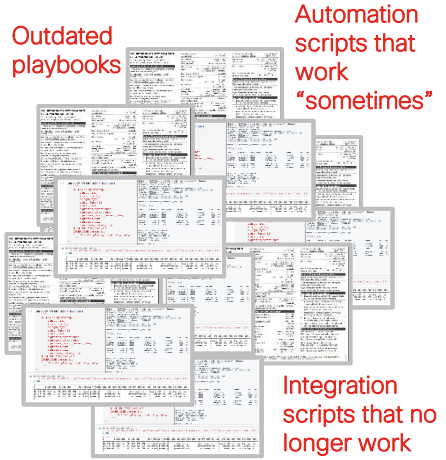
Why do customers want to Orchestrate?

"I want to glue my systems together to achieve an end-to-end workflow that reflects our service life-cycle request, implementation, sustainment, modification, decommissioning."

"Vendors offer many management tools – some do provisioning of services, others do monitoring – why can't they be tied together as a single solution?"

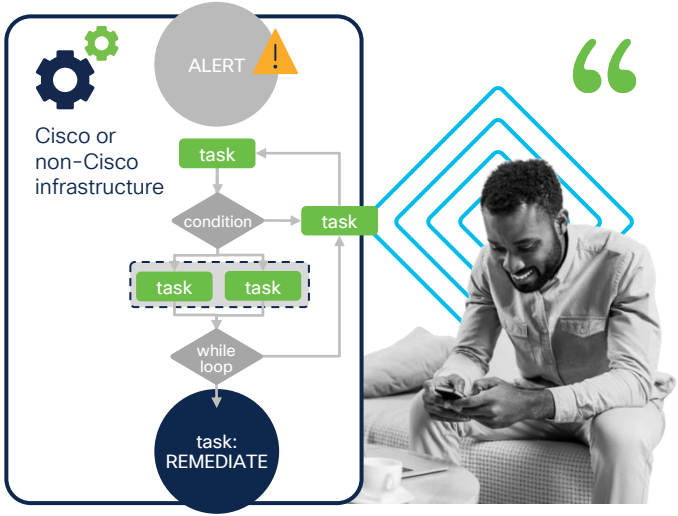
Maximizing operational efficiency

Before: Repetitive, human-powered tasks



Solution: Orchestrating security across the full lifecycle

Pre-built or customizable workflows



After: I combined **nine tasks** across three security tools, two infrastructure systems, and three teams in **one keystroke!**

"I make automated playbook changes in minutes with a drag-drop interface

We have never communicated faster: Our approvals are automated

My top five most frustrating tasks have all been automated

SecureX Orchestration

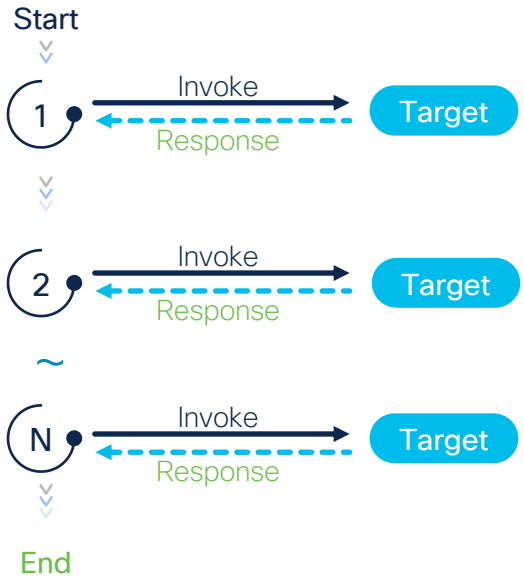
Cloud-Native, microservice architecture

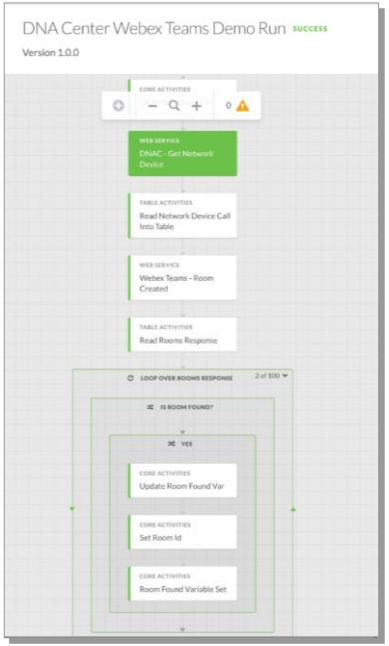
- Highly Performant, Scalable and Secure
- Reusable and Embeddable

Intuitive drag-drop UI with **visual workflows**

Combine flexible out of the box atomics and workflows to **create new integrations**

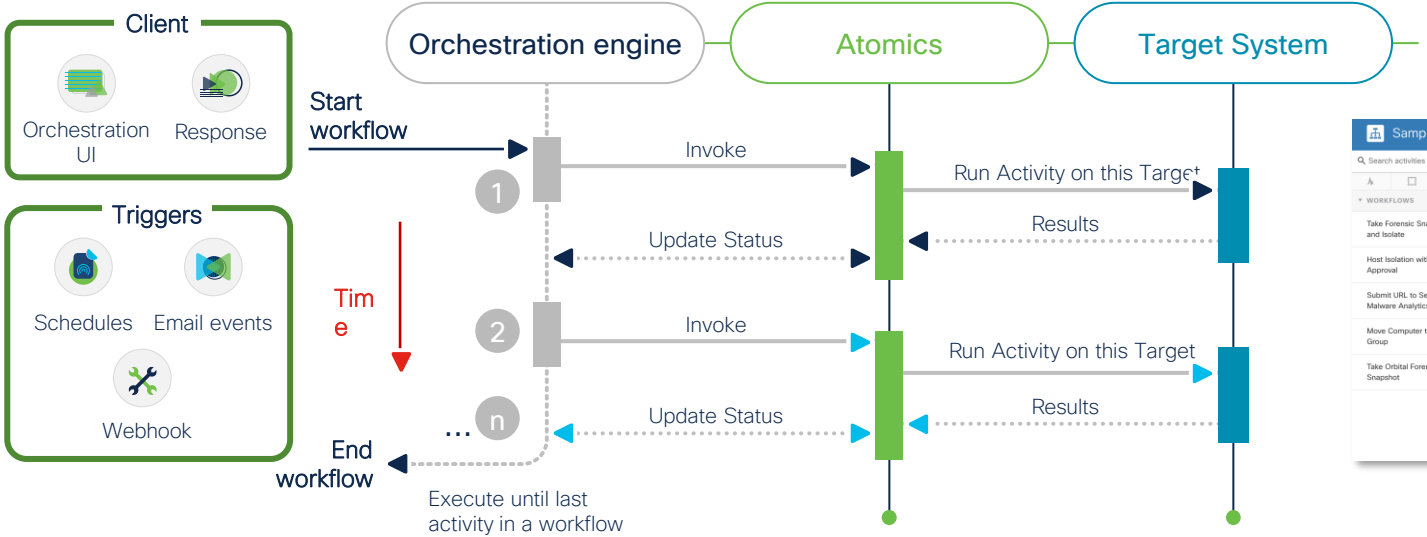
- Automate tasks according to schedules or external events such as email events

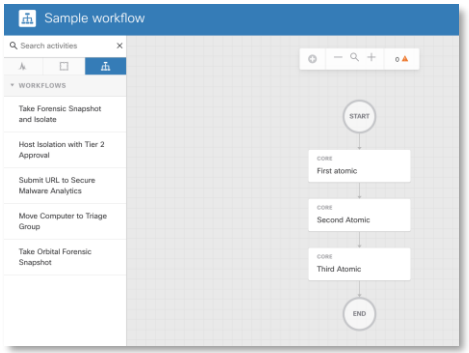




SecureX Orchestration workflow sequence

The orchestration engine runs workflows to execute atomics on the target systems, which returns results and status, then the next step in the workflow begins.

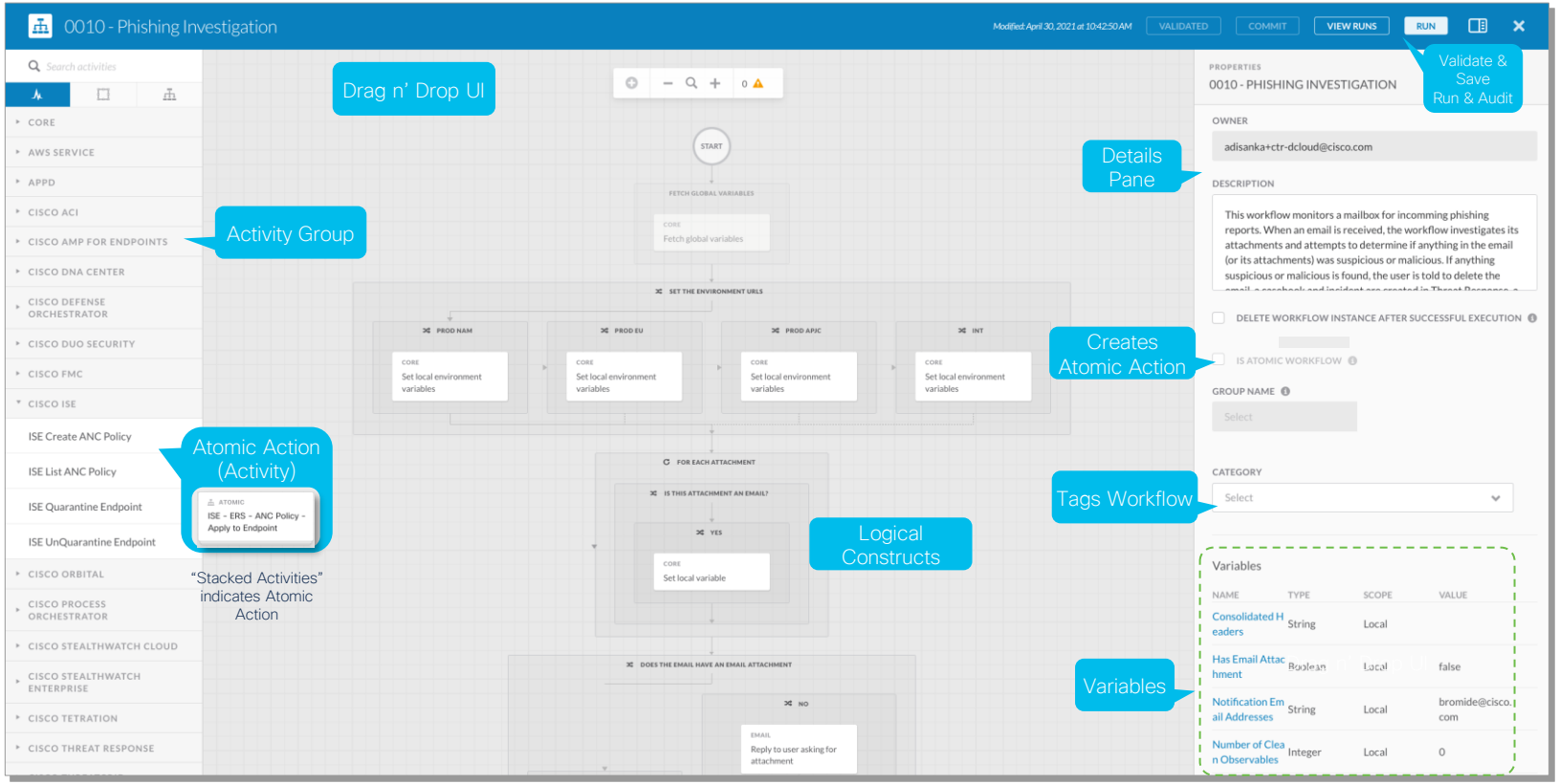




Atomic:
REST call, Run terminal, Send email … etc..

Target System:
The host/endpoint that executes an activity

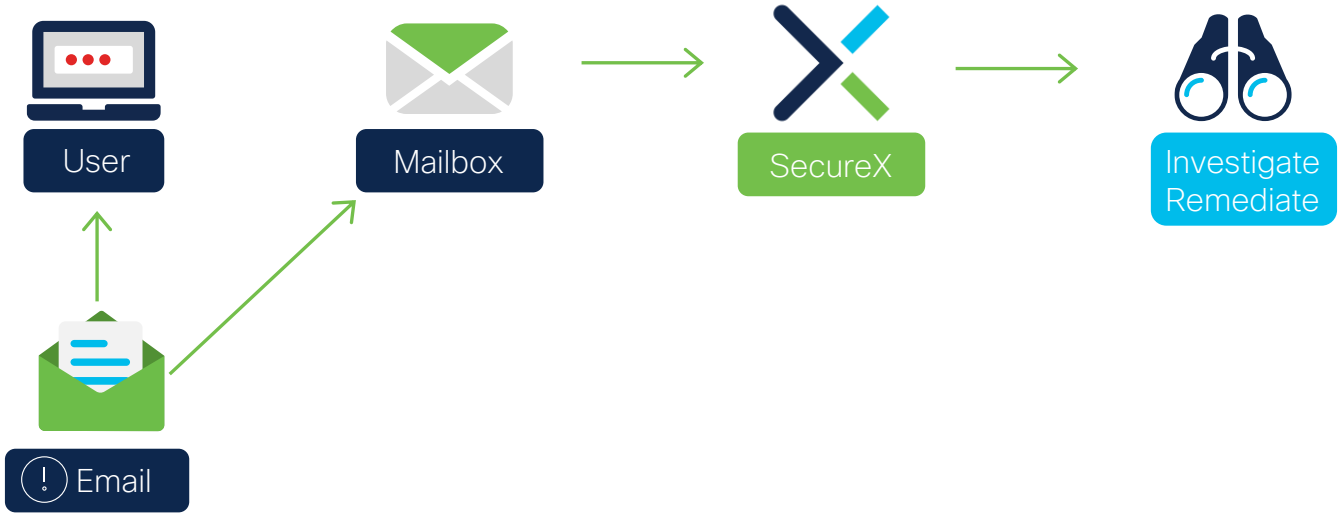
SecureX Orchestration canvas overview



Phishing Investigation Orchestration

cisco Live!

Suspected Phishing Email



Key Components

SecureX

Secure Email

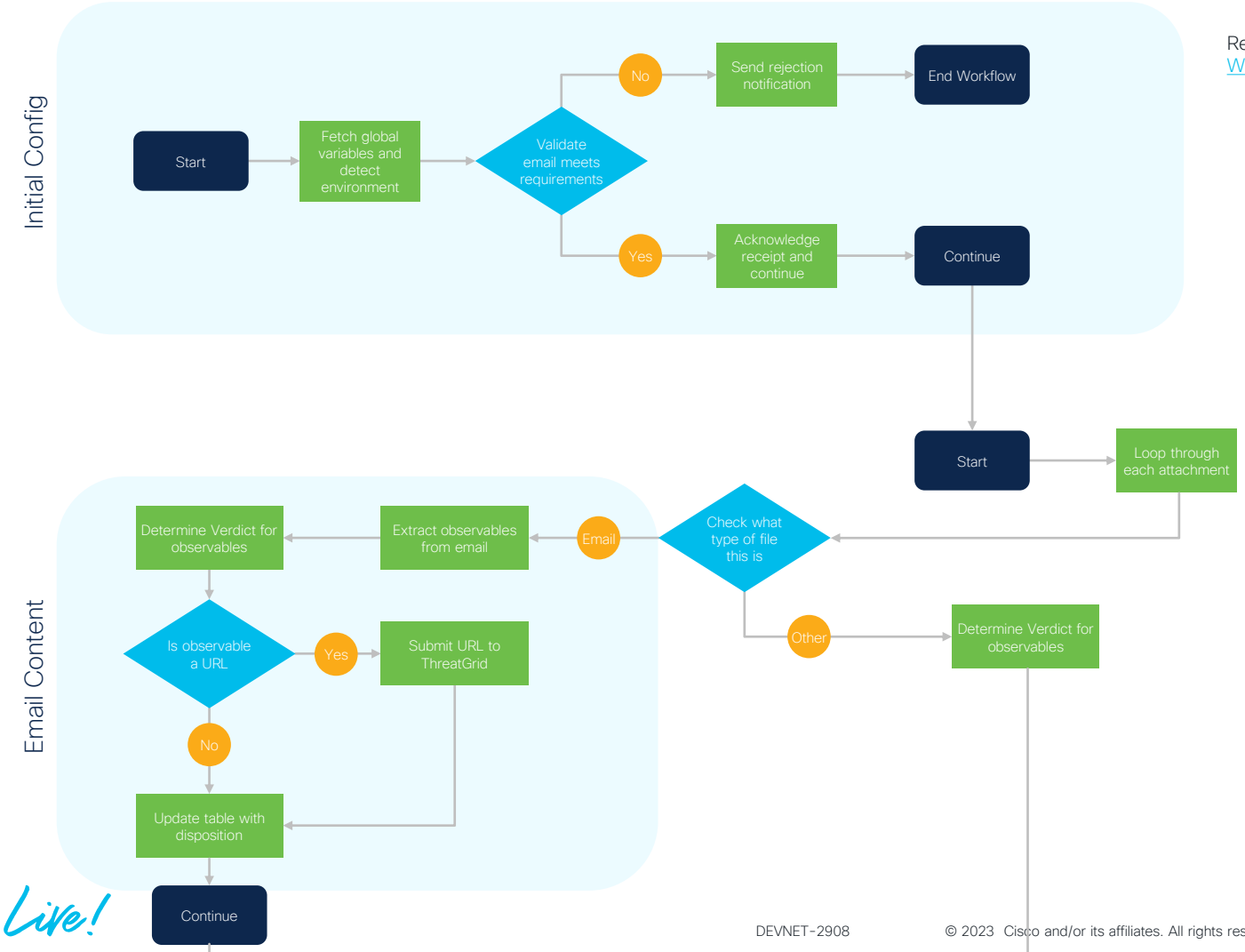
Umbrella

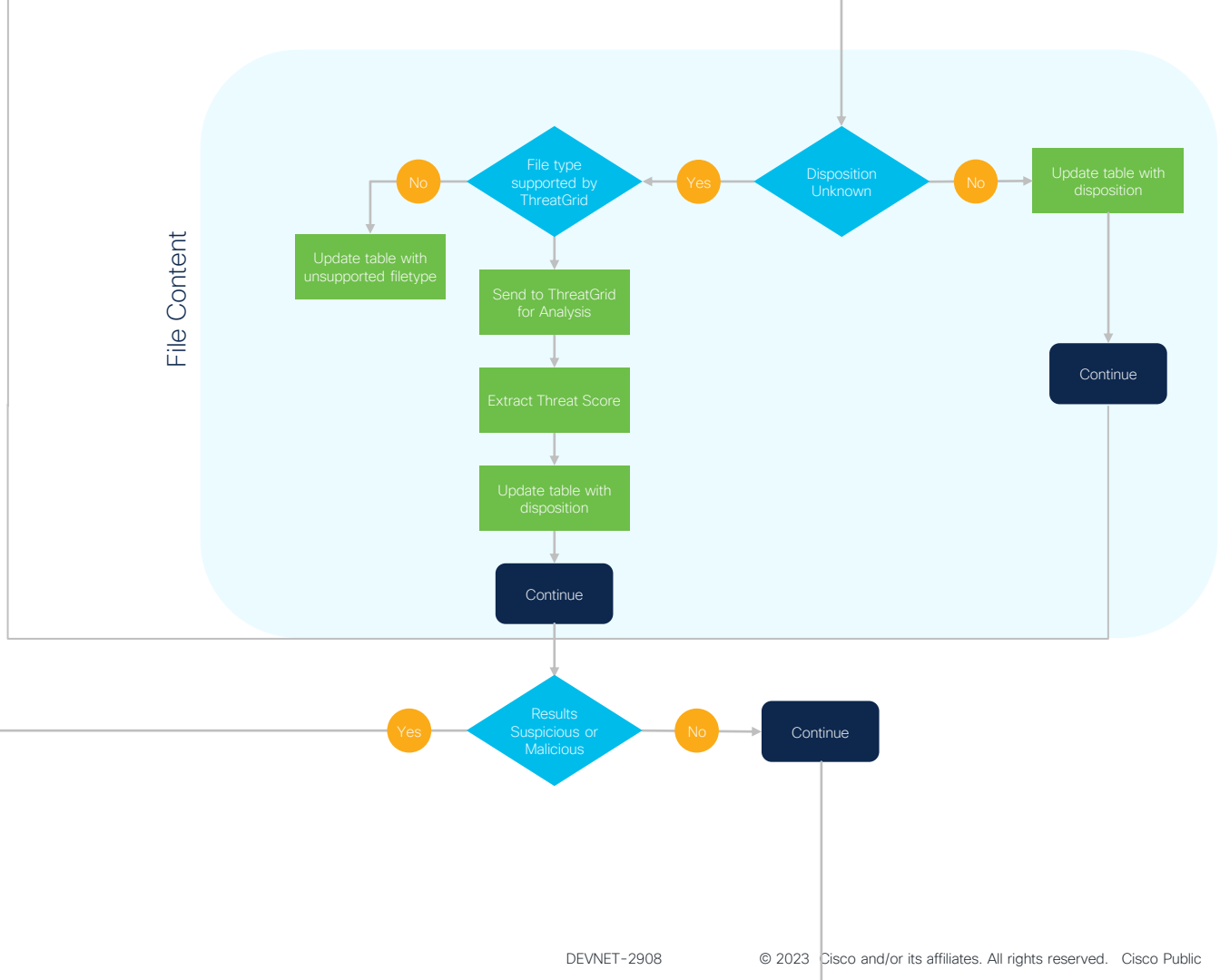
Threat Grid

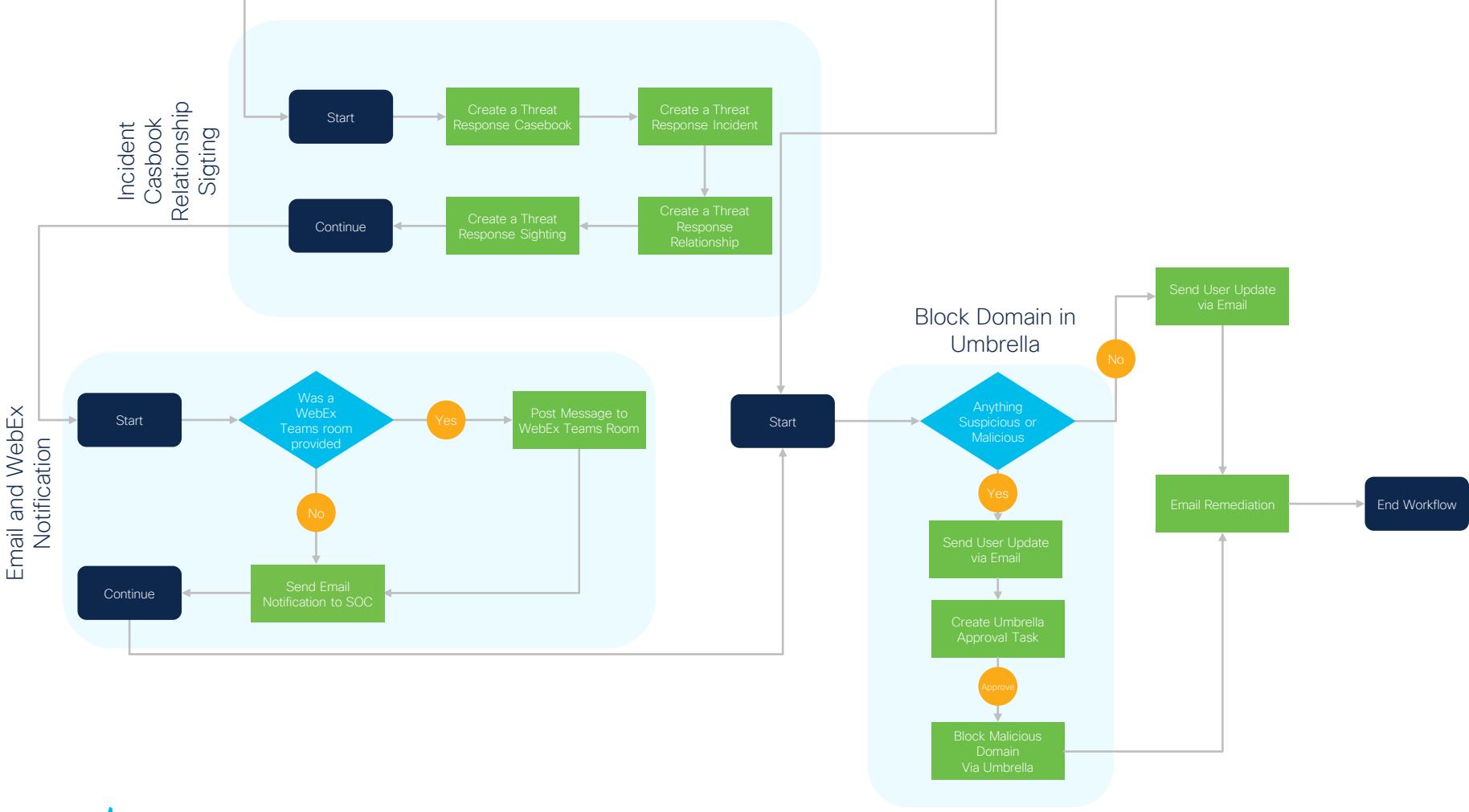
WebEx

Phishing Investigation Workflow

Reference: Phishing Investigation Workflow







Demo

Simplifying SOC operation with SecureX Orchestration

Resources

- SecureX GitHub Repository
  https://cs.co/SXO_repo
- SecureX Documentation
  https://cs.co/SXO_docs
- SecureX Video Playlist
  https://cs.co/SXO_videos
- Cisco DevNet
  https://developer.cisco.com/
- SecureX Orchestration Announcement room
  https://eurl.io/#l3vMZGcQ1

Call to Action

- Try out SecureX Orchestration for yourself
- Lots of integrations and pre-built workflow already there!
- Explore the power of integrating SecureX Orchestration with other Cisco solutions or 3rd party solutions via API

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- 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