

Cisco SecureX

Developing with the Next Generation Integration Platform

Ben Greenbaum, Technical Engineer, Security Integrations

@secintsight

DevNet Day DEVNET-SEC



June 2-3, 2020 | ciscolive.com/us

#CiscoLive





Agenda

- Introduction
 - What is SecureX?
 - SecureX Feature Highlights
- Developing with SecureX
 - The API model
 - SecureX threat response
 - SecureX orchestration
- Resources

Introduction

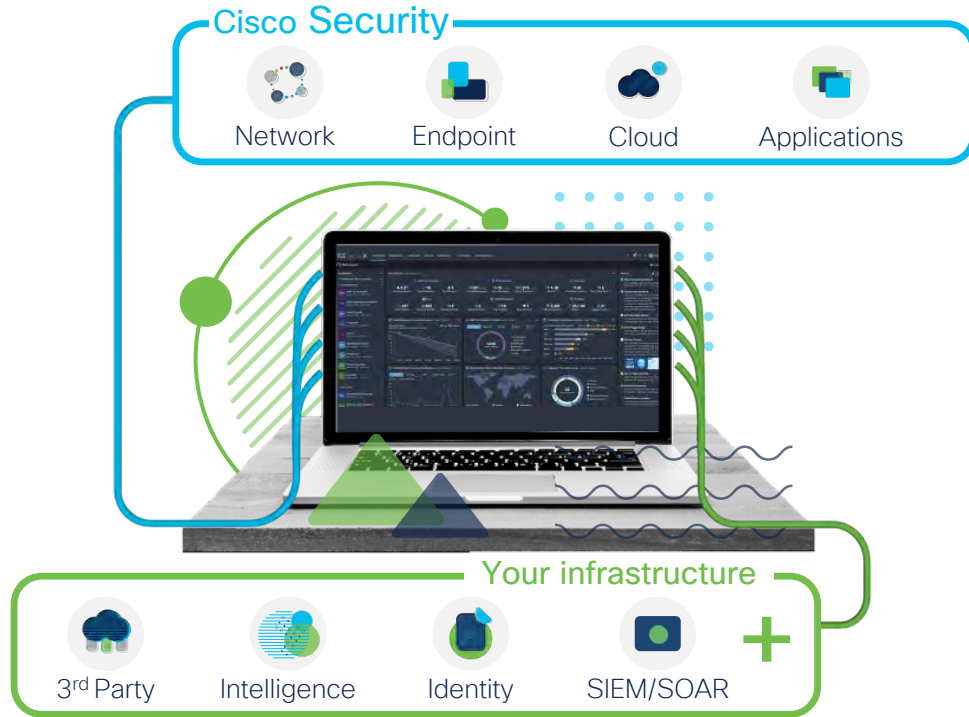
What is SecureX?

The Cisco SecureX platform is a **built-in** experience within our security portfolio



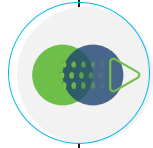
Unite all your
Cisco Security
products to
simplify your
approach and
maximize potential

That connects with your **entire** security infrastructure

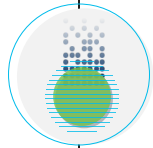


Integrate everything in your environment to unify visibility, enable automation, and strengthen security

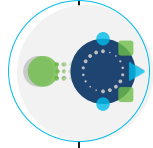
To unlock new value from your current investments



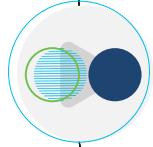
From partial awareness to **complete** and **actionable insights**



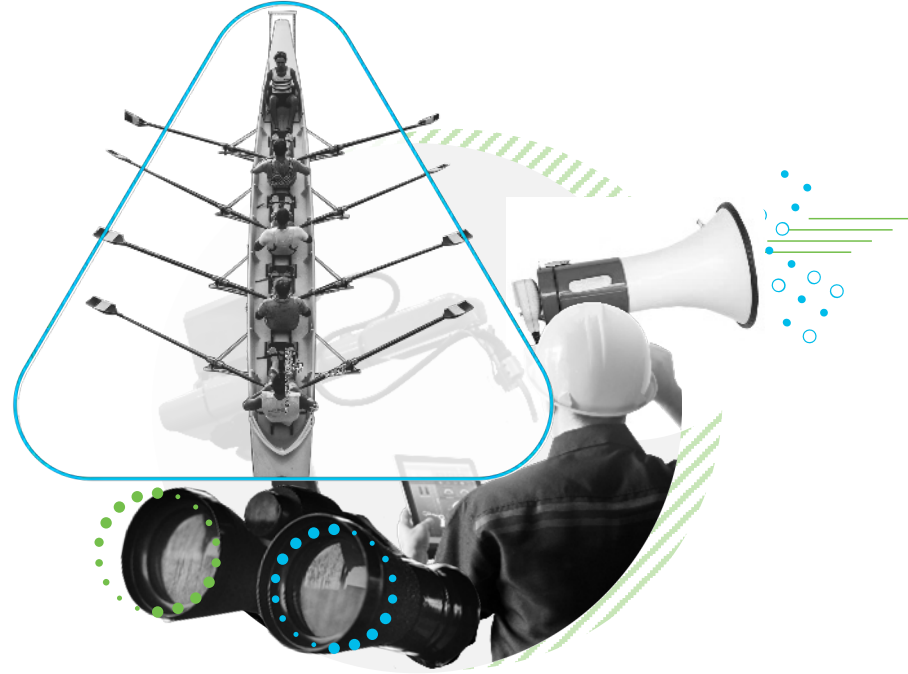
From inefficient workflows to the **strength of automation**



From siloed product usage to **shared context**



From complexity to **simplicity**



Feature highlights

SecureX capabilities and benefits

- **Threat response** for fast investigation and remediation
- **Playbook automation** to reduce manual workflows
- **3rd party integrations** for enhanced visibility into your environment
- **Secure sign-on** for seamless user experience
- **Customizable dashboard** to track detailed and important metrics
- **Ribbon** feature to share context between all teams and work across tools



SecureX threat response

- **Threat intelligence:** enrich your investigations with threat intelligence data from other Cisco Security products, Cisco Talos, 3rd party intelligence sources, and your own private intelligence to deliver quick answers when time is of the essence
- **Relations graph:** immediately visualize the threat and its organizational impact, and get an at-a-glance verdict for the observables you are investigating through a visually intuitive relations graph
- **Incident manager:** triage, prioritize, track, and respond to high-fidelity alerts through built-in manager
- **Response actions:** take rapid response actions across multiple security products: isolate hosts, block files and domains and block IPs – all from one convenient interface

SecureX orchestration

- **Low code approach**, high performance tool
- **Out-of-the box workflows** built by Cisco experts
- **Import / export workflows** from your trusted sources through convenient drag and drop interface
- **Create your own workflows** leveraging the intuitive interface and all the security tools you integrated
- **Event and intent based automation triggers**
- **Get the run time visibility** of workflows and status of their execution

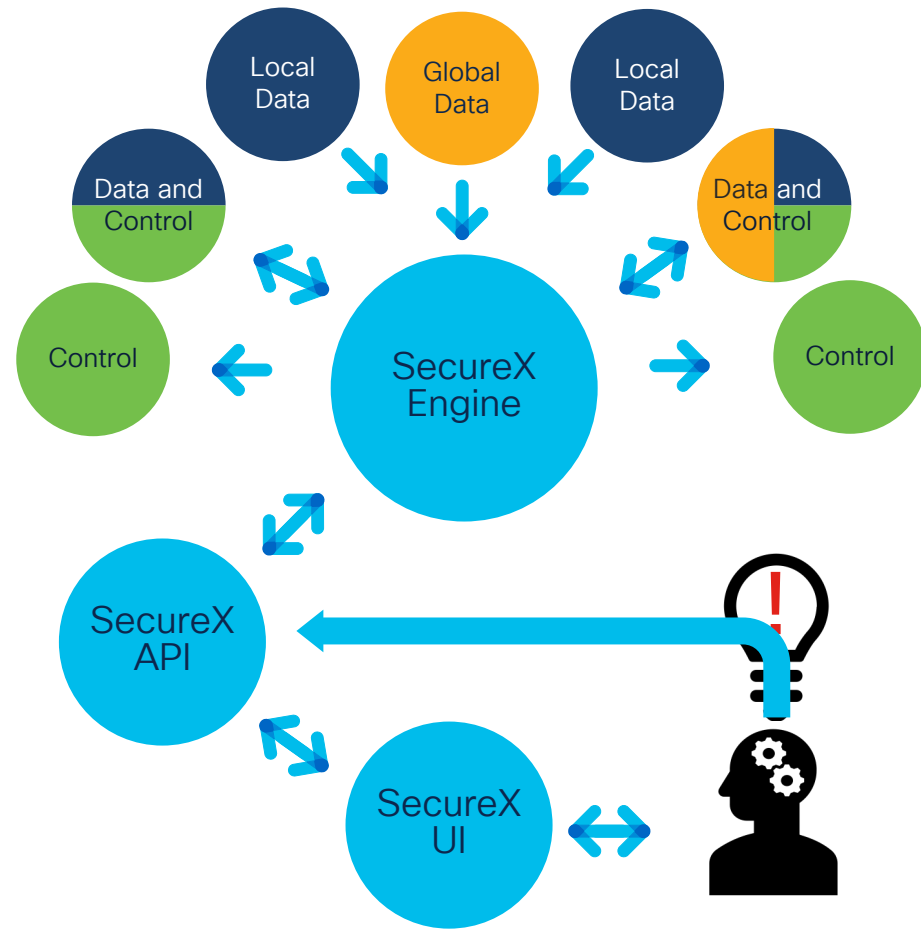
The SecureX Development Opportunity Space

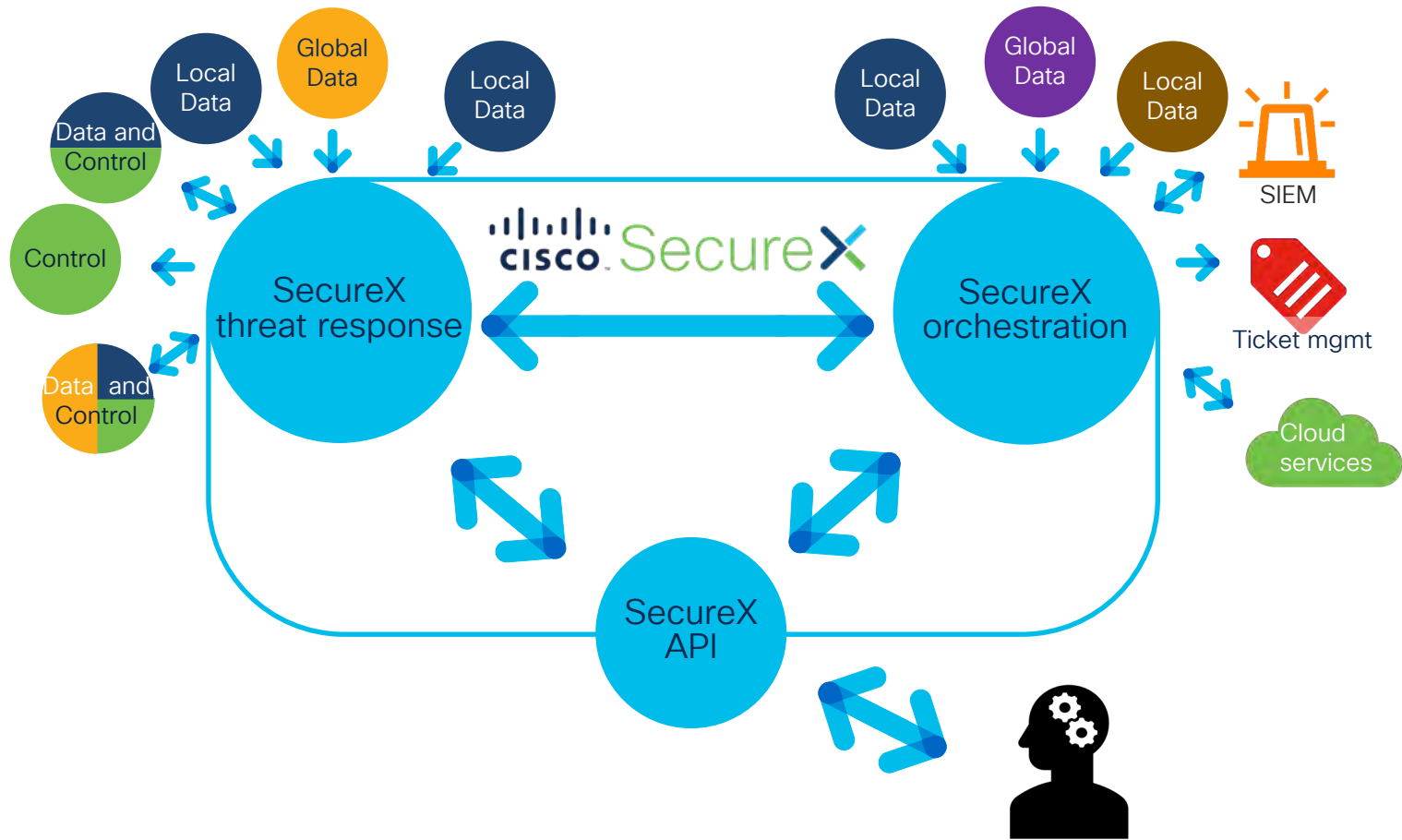
The API model

API aggregation at work



API relaying at work





SecureX threat response

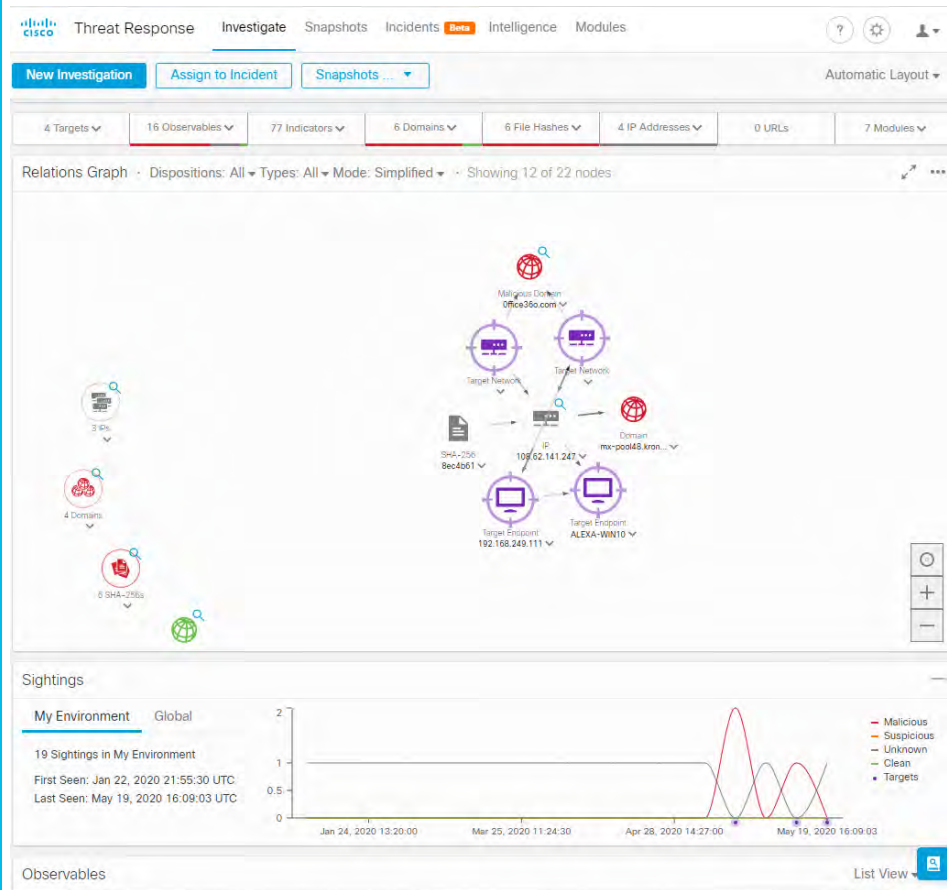
Use Cases

- Extract observables from text
- Quick reputation lookups
- Threat Hunting
- Create Incidents for Incident Manager
- Take response actions
- Add unsupported data sources!

DEMOS

- Script Demo
 - Find obsvs in text
 - Check reputations
 - Look for local sightings
 - Link to investigation
- Plugin Demo
 - Find obsvs in text
 - Quick reputation lookups
 - Find available responses
 - Take response actions

“Cisco Threat Response”



Modules

Pluggable code to talk to SecureX-capable intel, sensor, or control technologies



Relay Modules

Relay server translates from 3rd party data model and APIs to CTIM and SecureX APIs

- Currently implemented in AWS Lambda
- Write your own!
- Template on Github

Pulsedive	Farsight DNSDB
HIBP?	Google Chronicle
Abuse.ch IPDB	MS Graph Sec
Qualys IOC	ThreatInsight
CyberProtect	Spycloud
Shodan	Google SafeBrowsing
URLscan.io	MS Defender ATP

SecureX orchestration

Use Cases

- Incident & Ticket mgmt
- Automated Threat Hunting
- Phishing Investigations
- Manage Load Balancing
- Collect Threat Intelligence
- Find/Report Vulnerabilities
- Group Manual Responses
- Onboard New Users

DEMOS

- Show “Talos single blog post to Casebook”
- Walk through steps
- Show drag and drop
- Show threatgrid & SNOW

“Action Orchestrator”

The screenshot displays the Cisco Action Orchestrator web interface. At the top, a summary bar shows: 150 TOTAL, 15 INVALID, 69 VALIDATED, and 0 FAVORITE. Below this is a search bar and an 'IMPORT' button. A 'NEW WORKFLOW' button is located in the top right corner. The main area is a grid of workflow cards. Each card includes a title, a description, and validation details (e.g., 'Validated by Matt Vander H...', '05/19/20 04:50...'). The workflows are categorized by type: SECUREX, SECUREX-PLAYBOOK, ORBITAL, and FMC API. The interface also features a left-hand navigation menu with icons for various functions like search, settings, and notifications.

Workflow Name	Type	Validation Status	Validation Date
Talos RSS to CTR Casebook	SECUREX	Validated by Matt Vander H...	05/19/20 04:50...
CTR Workflow		Validated by Oxana Sanniko...	05/15/20 09:17...
Talos Single Blog Post to CTR Casebook	SECUREX-PLAYBOOK	Validated by Matt Vander H...	05/14/20 06:55...
Secure Remote Worker: VPN Capacity (No Duo)	SECUREX-PLAYBOOK	Validated by Matt Vander H...	05/13/20 08:34...
Secure Remote Worker: VPN Capacity (Duo)	SECUREX-PLAYBOOK	Validated by Naaslef Edross	05/11/20 06:07 am
CTR Enrich Observable osanniko		Validated by Oxana Sanniko...	05/08/20 12:52...
Office 365 Traffic Offload for ASA	SECUREX-PLAYBOOK	Validated by Matt Vander H...	05/08/20 07:26...
gacs-basic-wf		Validated by Gyorgy ACS	05/08/20 03:41 am
ServiceNow Trickery		Validated by Matt Vander H...	05/04/20 06:00...
Orbital Get Operating System	ORBITAL	Validated by Jamey Heary	05/02/20 12:29 pm
fmc create object group		Validated by Aditya Sankar	05/01/20 07:56 am
FMC API - POST FQDN object	FMC API +1	Validated by Aditya Sankar	05/01/20 07:40 am
Authenticate FMC API	FMC API		
FMC API - Get Network Object Details	FMC API +1		
FMC API - Get Network Group Objects	FMC API +1		

Arbitrary 3rd Party Integrations?

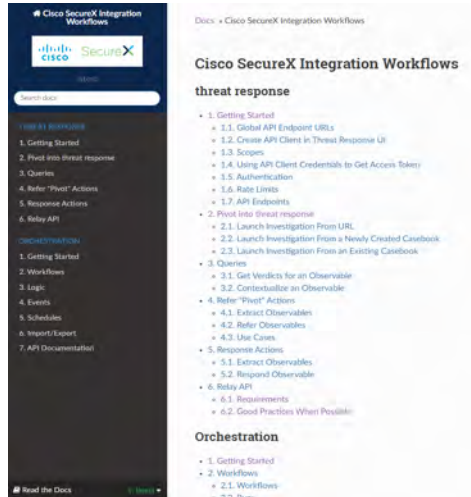
1. Create HTTP API target
2. Configure Account Keys
3. Use included Python Adapter to write Python script
4. Use HTTP adapter on Step 1 Target
5. Fetch data from Step 4 adapter, process response with Step 3 script.

Conclusion

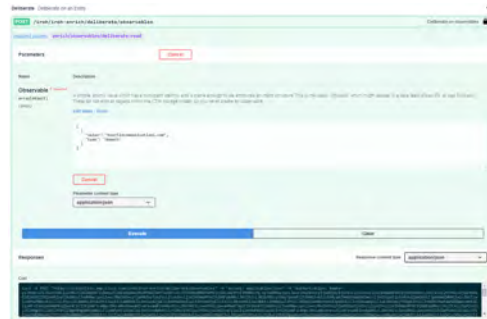
Resources

Integration documentation

cs.co/SecureX_integration_workflows



UI docs and proto tools



Github

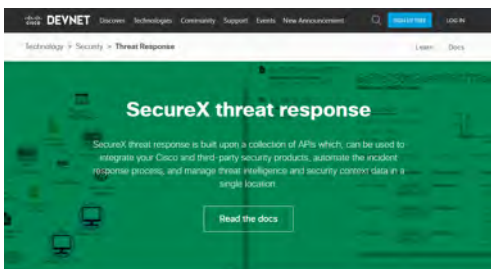
github.com/CiscoSecurity



SecureX threat response Resources

Devnet

developer.cisco.com/threat-response/

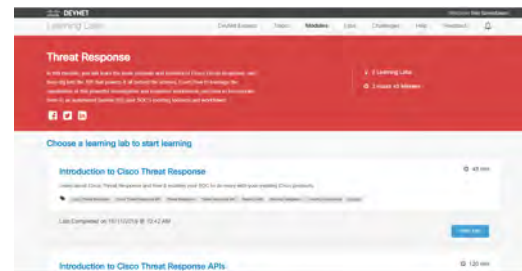


What can you do with SecureX threat response APIs?



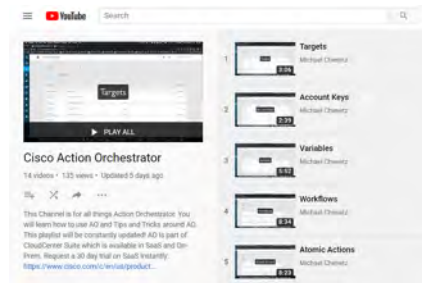
Devnet Learning Labs

cs.co/CTR-API-labs



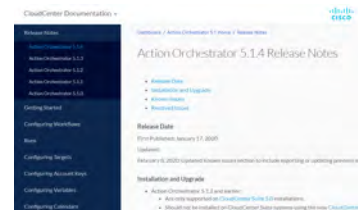
SecureX orchestration Resources

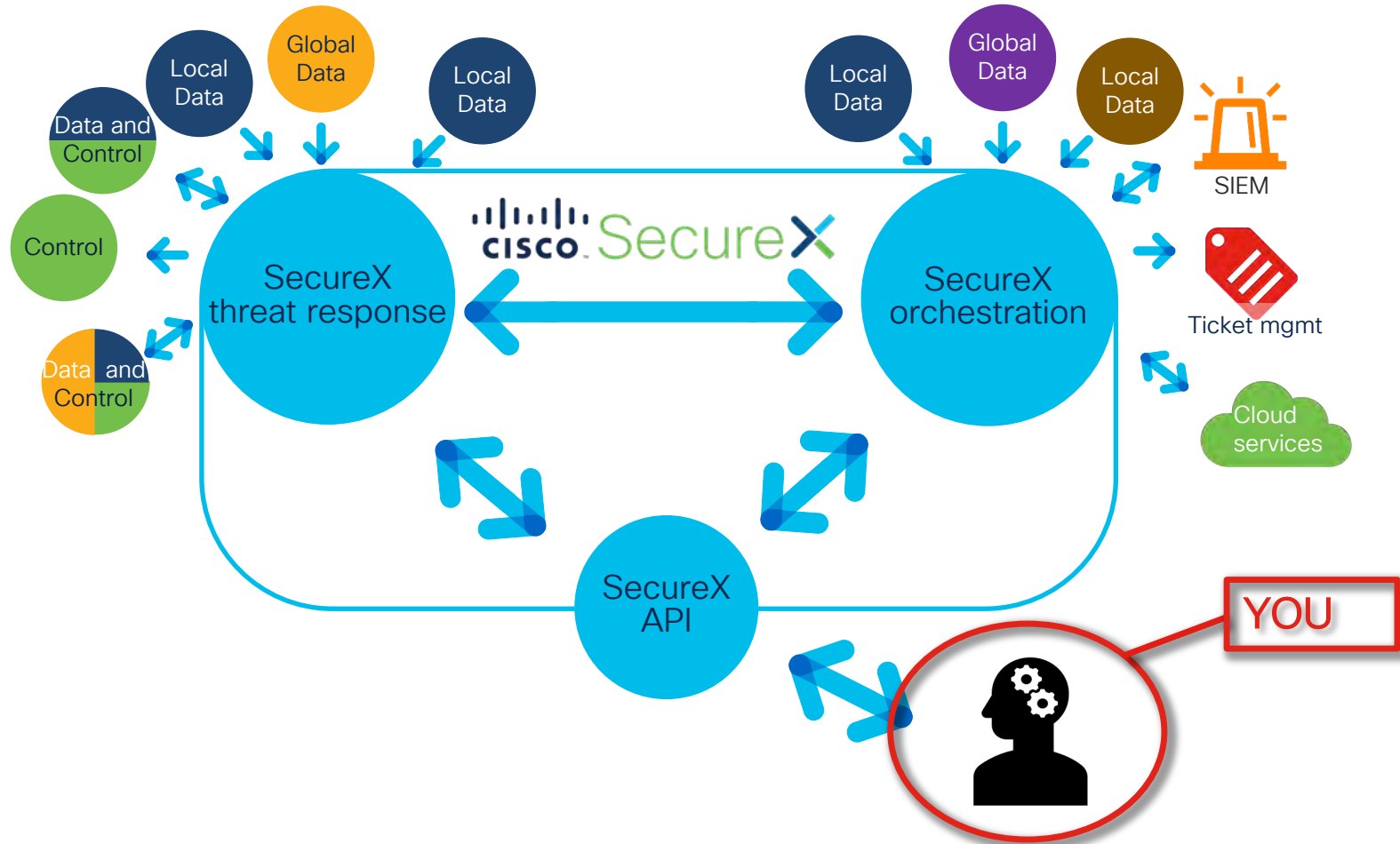
Action Orchestrator videos: cs.co/AOvideos



Action Orchestrator docs

<https://docs.cloudmgmt.cisco.com/display/ACTIONORCHESTRATOR51>





Thank you



Possibilities

#CiscoLive