The bridge to possible

Development opportunities with SecureX

How to build onto the industry's broadest security platform

Ben Greenbaum, Sr. Product Manager, SecureX
@secintsight

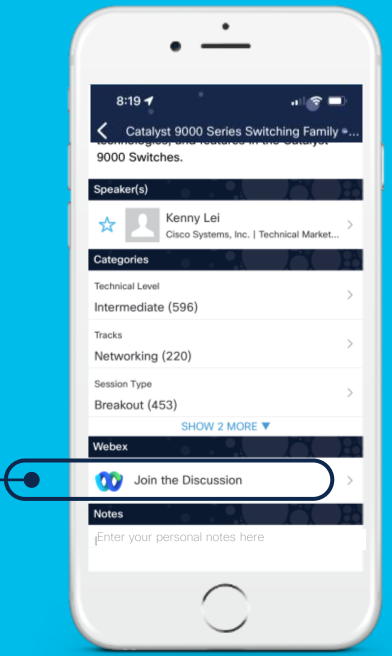
Cisco Webex App

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



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Webex spaces will be moderated until February 24, 2023.

Agenda

- Introduction
  - What is SecureX?
  - SecureX Feature Highlights
- The SecureX Development Opportunity
  - The API model
  - SecureX threat response
  - SecureX orchestration
- Conclusion & Resources

Objectives

Overview

- Understand SecureX purpose and application
- Understand integration use cases (why integrate?)

Threat Response

- Understand Modules and Relays

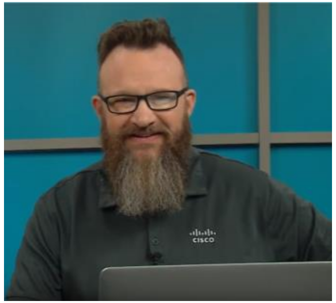
Orchestration

- Understand Workflows and Targets

Ben Greenbaum

Professional life

- 25 years experience
- Engineering roles at
  - SecurityFocus
  - Symantec
  - SOC/Engineering roles at Financial Services
  - PayPal
  - Hedge Fund
- 5 years at Cisco



Personal life

- Interests
  - Travel
  - Poorly advised motorsports
- Life
  - Rural Arizona
  - With:
    - Wife
    - 4 cats
    - Many broken cars

Introduction to SecureX

What is SecureX?

What is SecureX?

SecureX is
platfor ss
th
I
a to 3rd
par services
as w

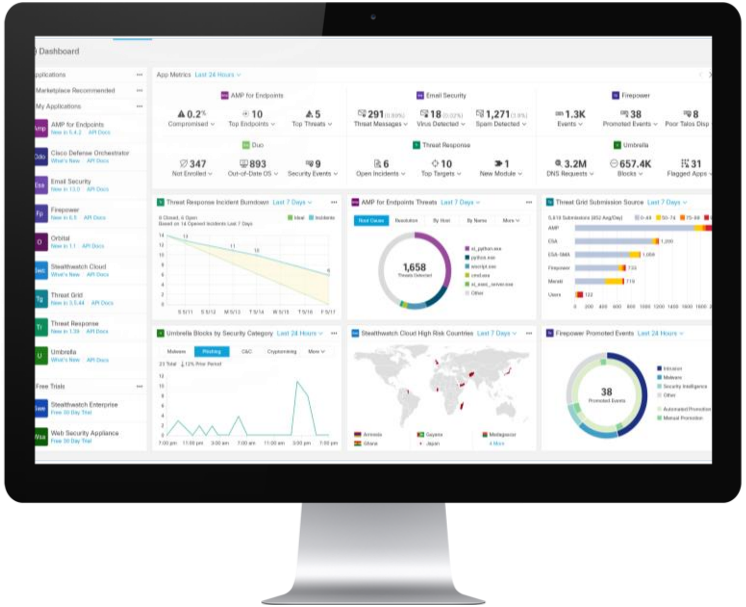
AKA
XDR

The real power of SecureX is the combined power of all the connected technologies, multiplied by the efficiency gains from automation…

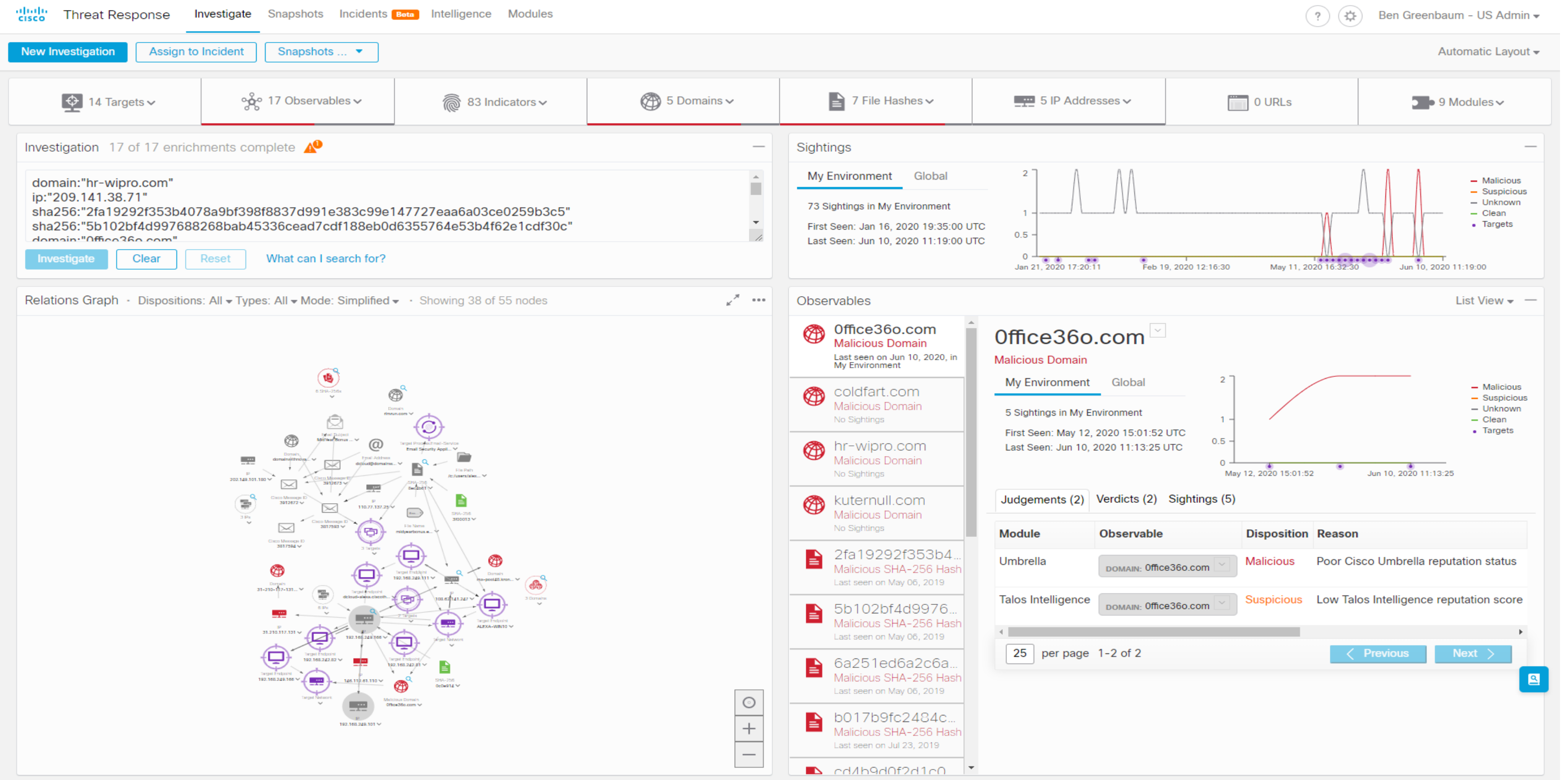
SecureX Features

SecureX capabilities and benefits

- **Threat response** for fast investigation and remediation
- **Orchestration** to reduce manual workflows
- **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



Investigation 17 of 17 enrichments complete

```
domain:"hr-wipro.com"
ip:"209.141.38.71"
sha256:"2fa19292f353b4078a9bf398f8837d991e383c99e147727eaa6a03ce0259b3c5"
sha256:"5b102bf4d997688268bab45336cead7cdf188eb0d6355764e53b4f62e1cdf30c"
domain:"0ffice36o.com"
```

Sightings

73 Sightings in My Environment

First Seen: Jan 16, 2020 19:35:00 UTC
Last Seen: Jun 10, 2020 11:19:00 UTC

Relations Graph · Dispositions: All · Types: All · Mode: Simplified · Showing 38 of 55 nodes

Observables

0ffice36o.com
Malicious Domain
Last seen on Jun 10, 2020, in My Environment

coldfart.com
Malicious Domain
No Sightings

hr-wipro.com
Malicious Domain
No Sightings

kuternull.com
Malicious Domain
No Sightings

2fa19292f353b4...
Malicious SHA-256 Hash
Last seen on May 06, 2019

5b102bf4d9976...
Malicious SHA-256 Hash
Last seen on May 06, 2019

6a251ed6a2c6a...
Malicious SHA-256 Hash
Last seen on May 06, 2019

b017b9fc2484c...
Malicious SHA-256 Hash
Last seen on Jul 23, 2019

cd4b9d0f2d1c0

0ffice36o.com
Malicious Domain

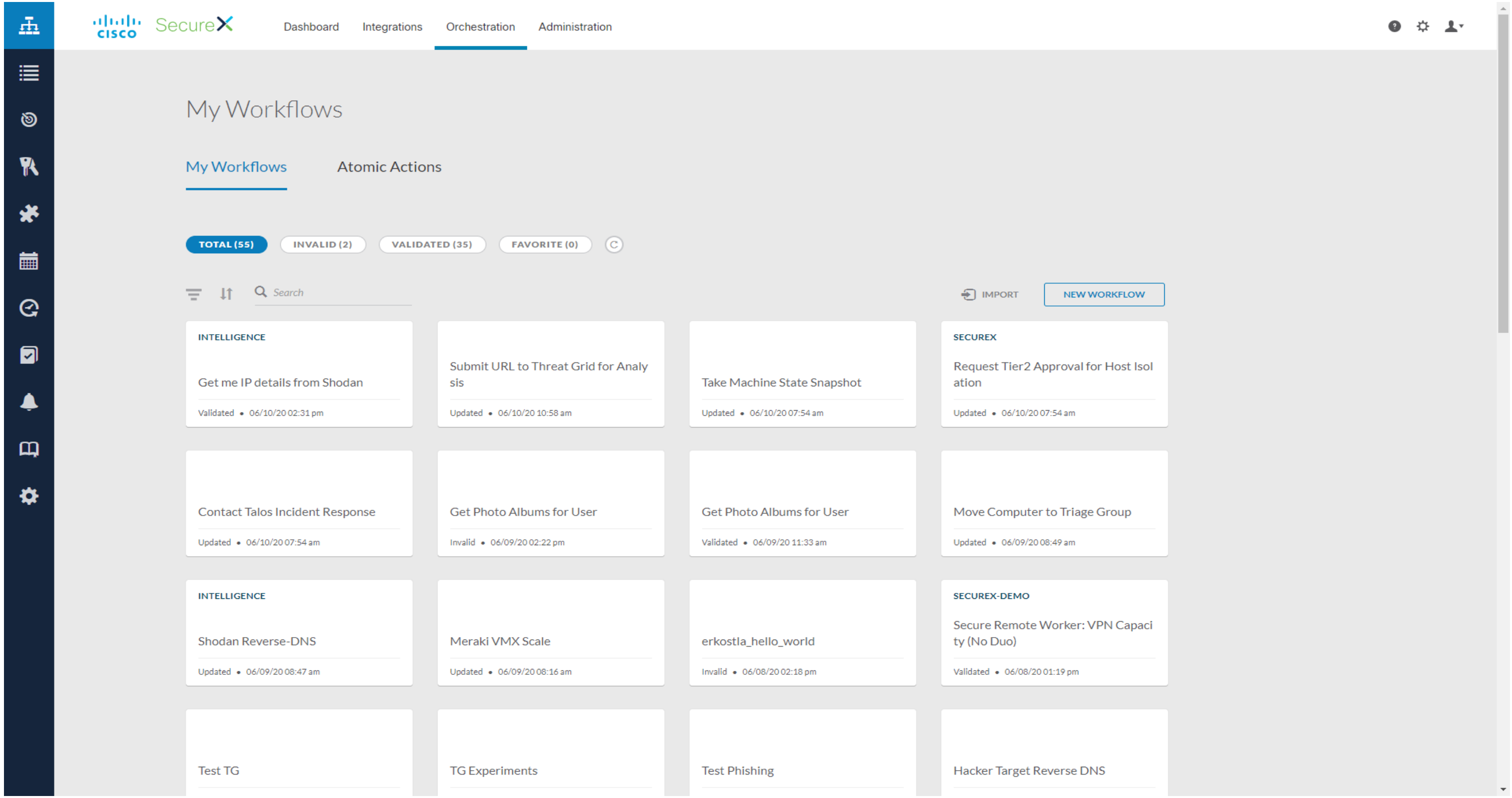
5 Sightings in My Environment

First Seen: May 12, 2020 15:01:52 UTC
Last Seen: Jun 10, 2020 11:13:25 UTC

Module	Observable	Disposition	Reason
Umbrella	DOMAIN: 0ffice36o.com	Malicious	Poor Cisco Umbrella reputation status
Talos Intelligence	DOMAIN: 0ffice36o.com	Suspicious	Low Talos Intelligence reputation score

25 per page 1-2 of 2

SecureX orchestration



My Workflows

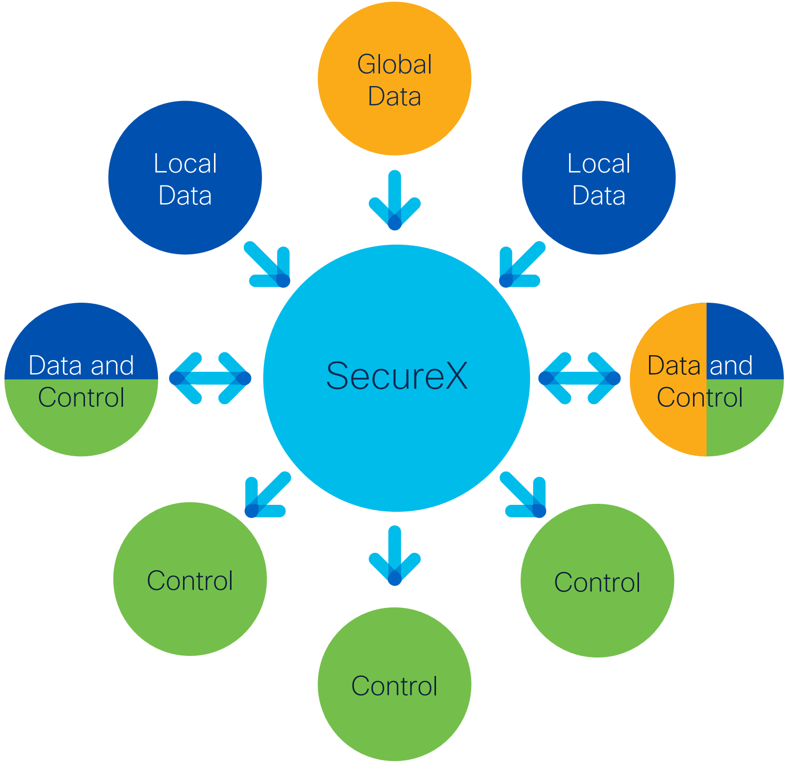
My Workflows | Atomic Actions

INTELLIGENCE Get me IP details from Shodan Validated • 06/10/20 02:31 pm	Submit URL to Threat Grid for Analysis Updated • 06/10/20 10:58 am	Take Machine State Snapshot Updated • 06/10/20 07:54 am	SECUREX Request Tier2 Approval for Host Isolation Updated • 06/10/20 07:54 am
Contact Talos Incident Response Updated • 06/10/20 07:54 am	Get Photo Albums for User Invalid • 06/09/20 02:22 pm	Get Photo Albums for User Validated • 06/09/20 11:33 am	Move Computer to Triage Group Updated • 06/09/20 08:49 am
INTELLIGENCE Shodan Reverse-DNS Updated • 06/09/20 08:47 am	Meraki VMX Scale Updated • 06/09/20 08:16 am	erkostla_hello_world Invalid • 06/08/20 02:18 pm	SECUREX-DEMO Secure Remote Worker: VPN Capacity (No Duo) Validated • 06/08/20 01:19 pm
Test TG	TG Experiments	Test Phishing	Hacker Target Reverse DNS

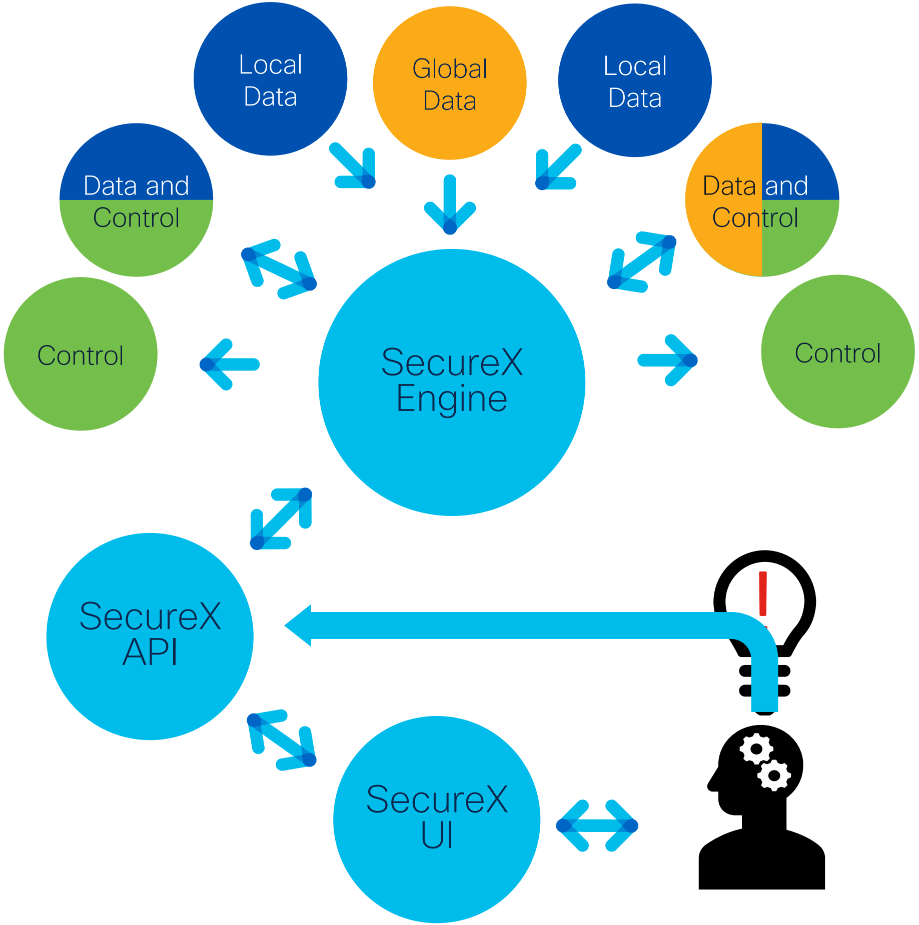
The SecureX Development Opportunity Advantage

The SecureX API Model

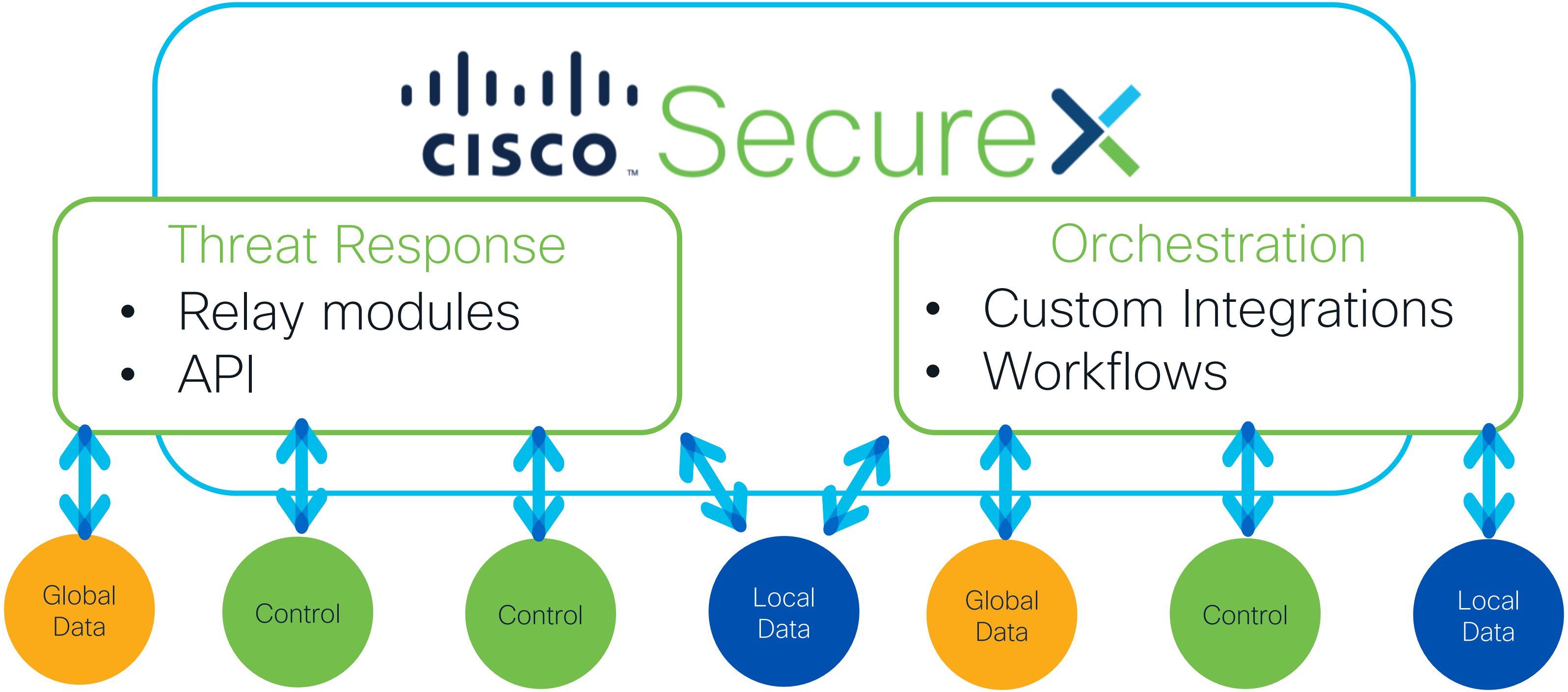
API aggregation at work



API proxying at work



Hooks and Integration Points

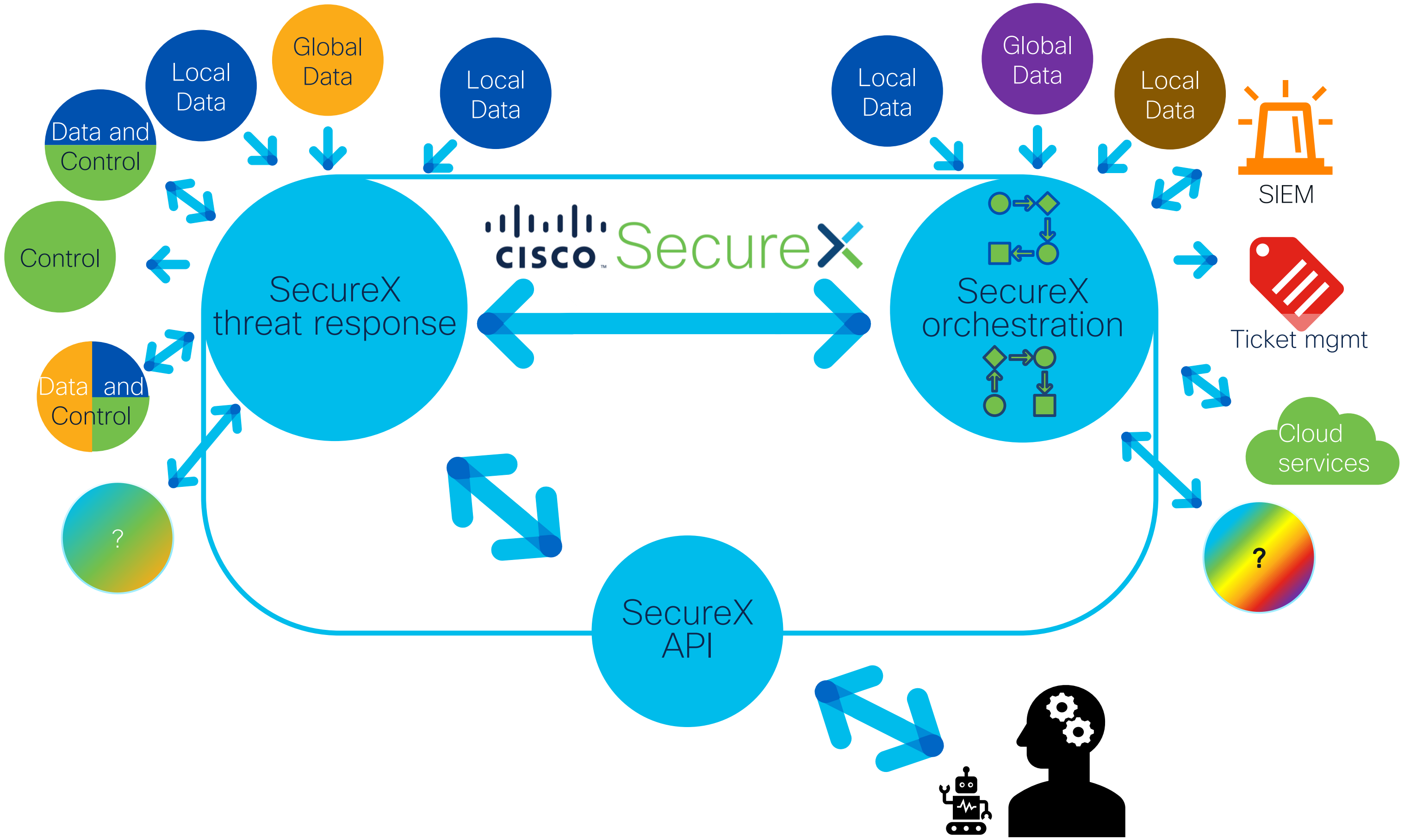


Threat Response

- Relay modules
- API

Orchestration

- Custom Integrations
- Workflows



Local Data

Global Data

Local Data

Data and Control

Control

Data and Control

?

cisco SecureX

SecureX threat response

SecureX orchestration

SecureX API

Local Data

Global Data

Local Data

SIEM

Ticket mgmt

Cloud services

?

SecureX threat response

SecureX threat response Integration Use Cases

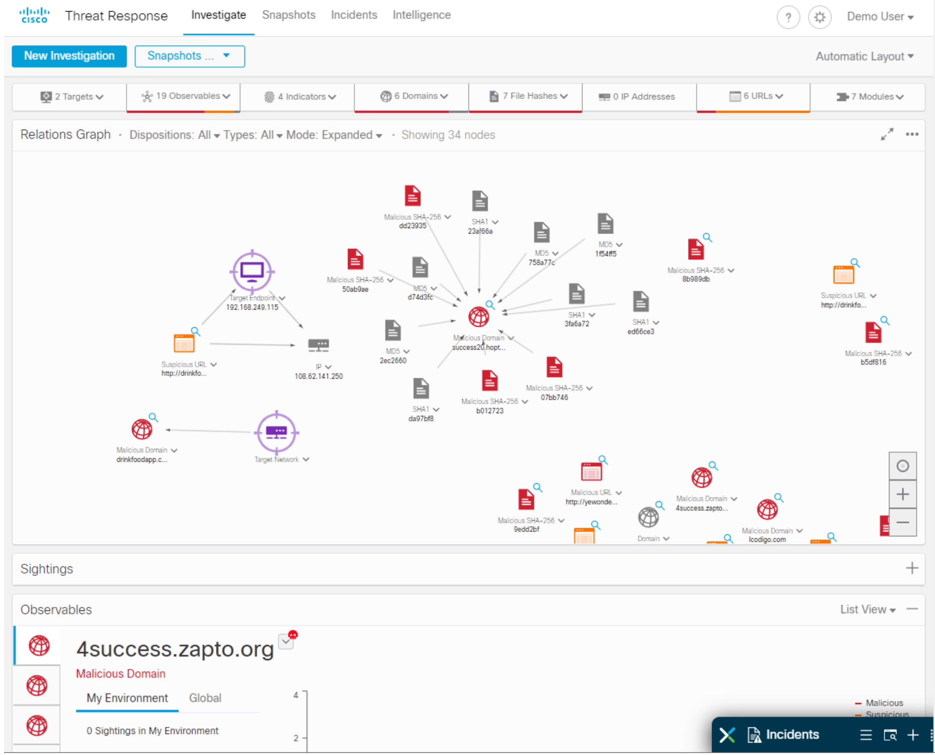
- 3rd Party Program Using SecureX:
  - Extract observables from text
  - Quick reputation lookups
  - Threat Hunting
  - Create Incidents for Incident Manager
  - Take response actions

SecureX threat response Integration Use Cases

- SecureX using the 3rd Party Program:
  - Add arbitrary data/response sources!
    - Enrichment data
    - Take response actions

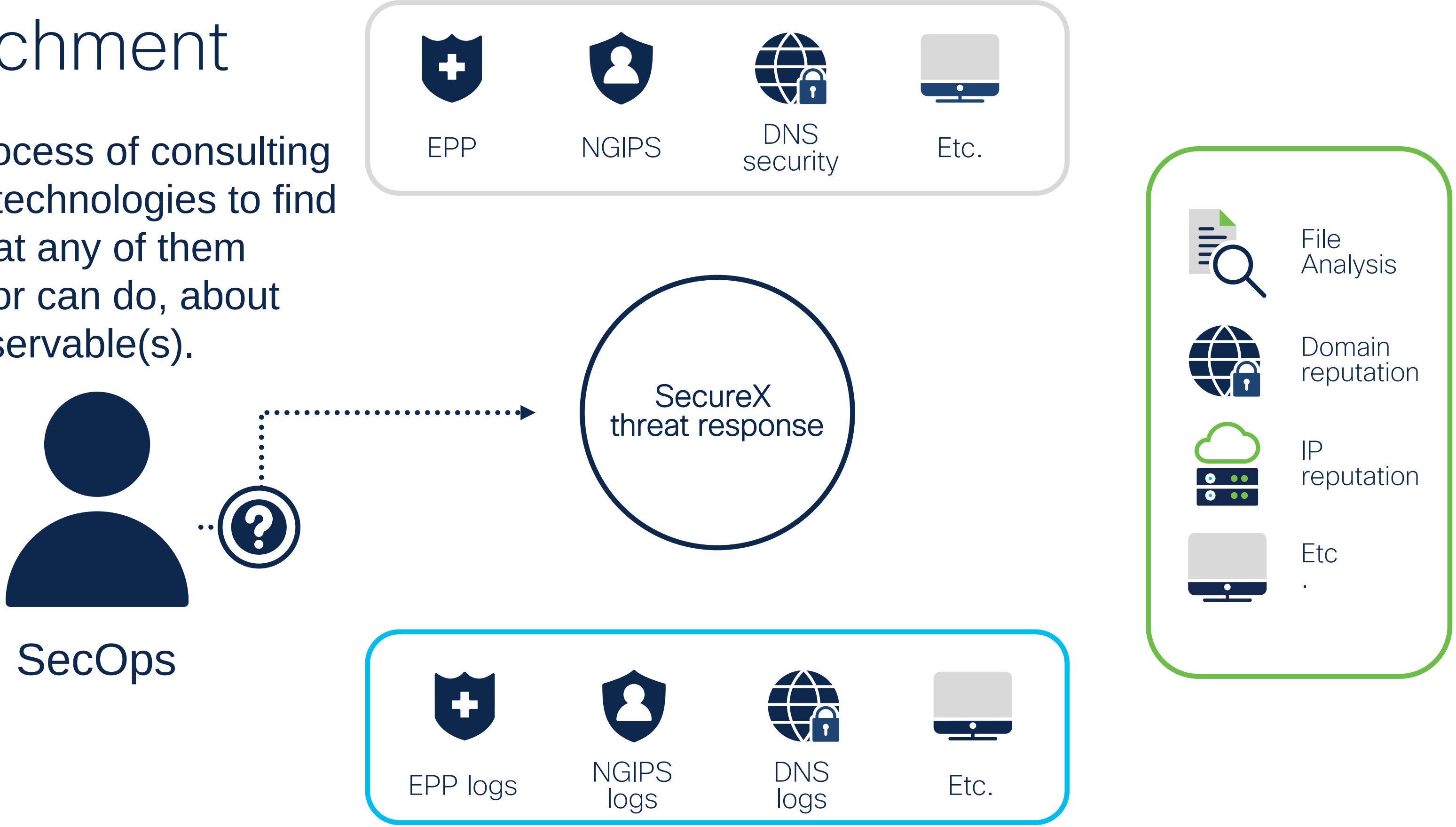
SecureX threat response

- Products host their own APIs
- SecureX threat response makes requests
  - “Do you know anything about this observable?”
  - “Have you seen this observable?”
  - “What can you do about it?”
  - “Do that to/with this observable”

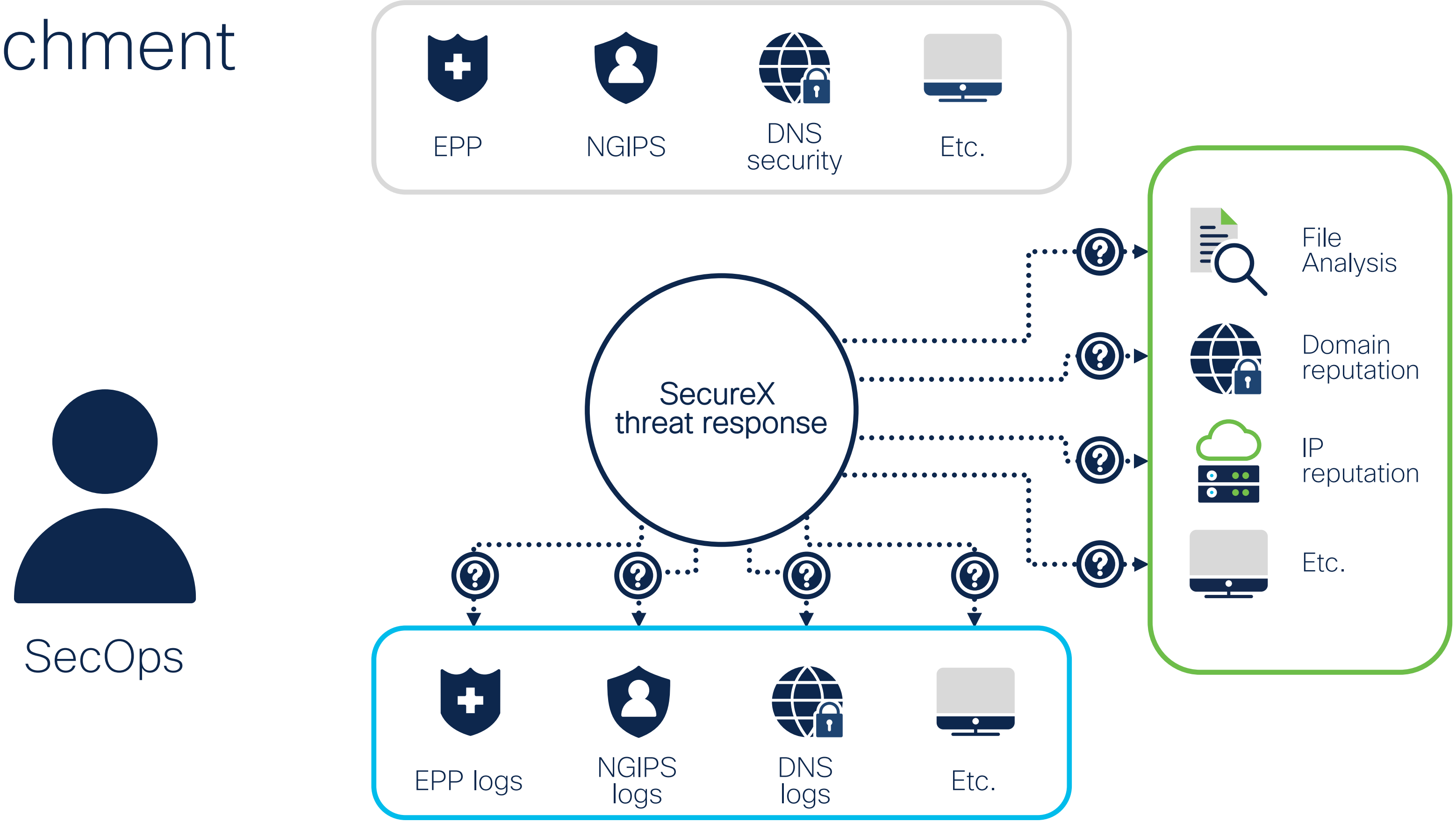


Enrichment

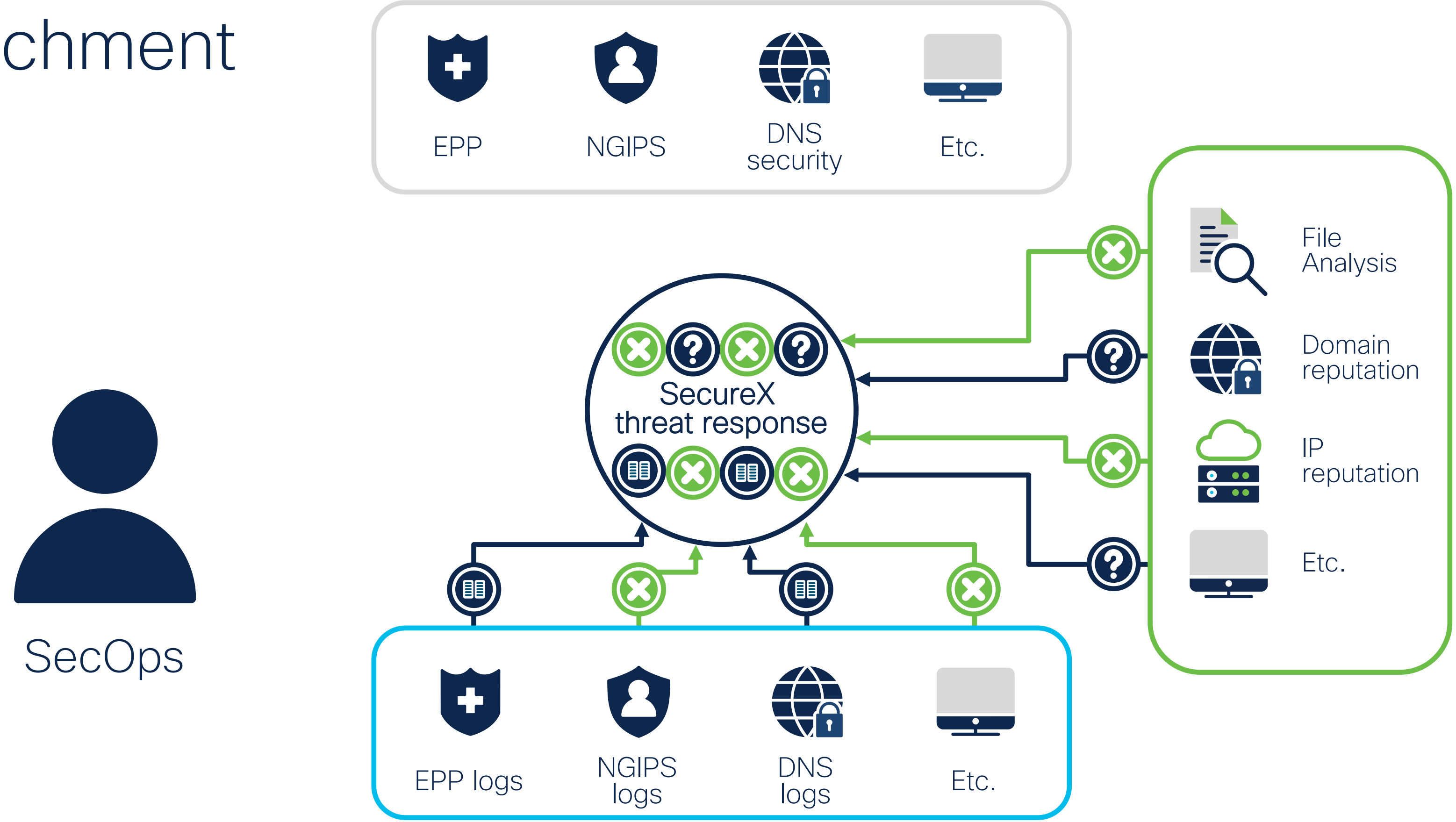
The process of consulting all the technologies to find out what any of them know, or can do, about the observable(s).



Enrichment

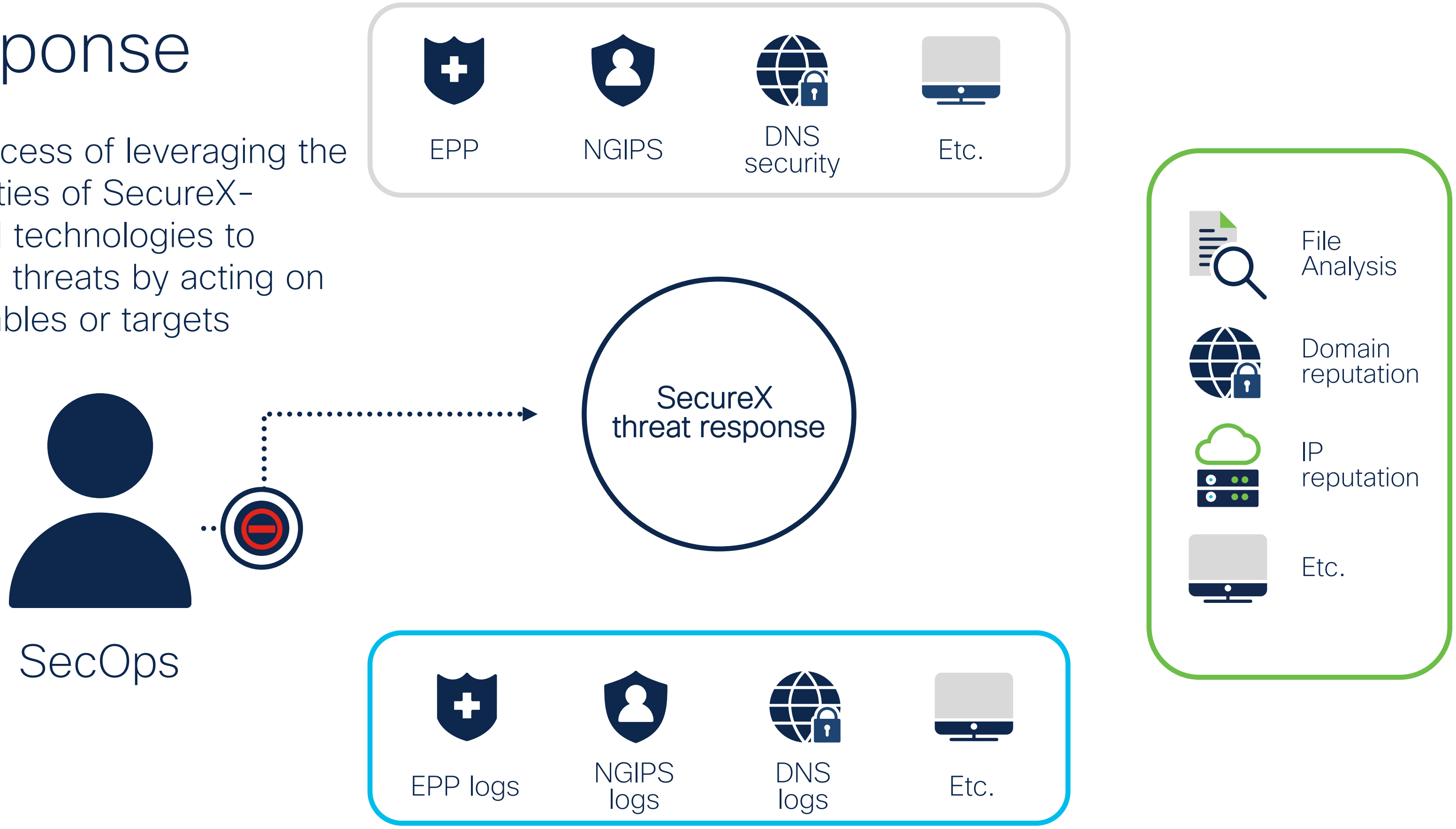

EPP
NGIPS
DNS security
Etc.
SecureX threat response
File Analysis
Domain reputation
IP reputation
Etc.
EPP logs
NGIPS logs
DNS logs
Etc.
SecOps

Enrichment

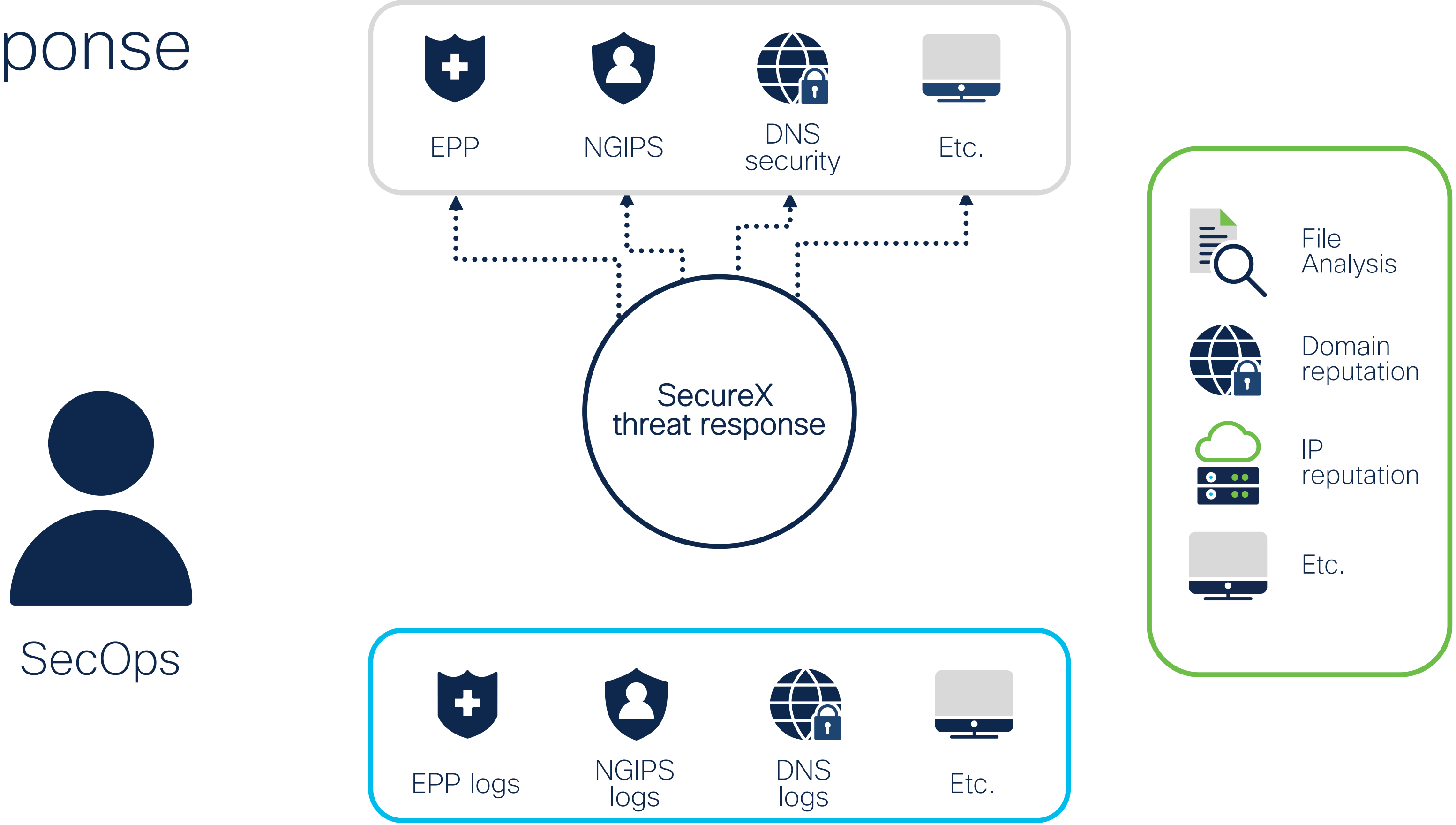

EPP
NGIPS
DNS security
Etc.
SecOps
SecureX threat response
File Analysis
Domain reputation
IP reputation
Etc.
EPP logs
NGIPS logs
DNS logs
Etc.

Response

The process of leveraging the capabilities of SecureX-enabled technologies to mitigate threats by acting on observables or targets

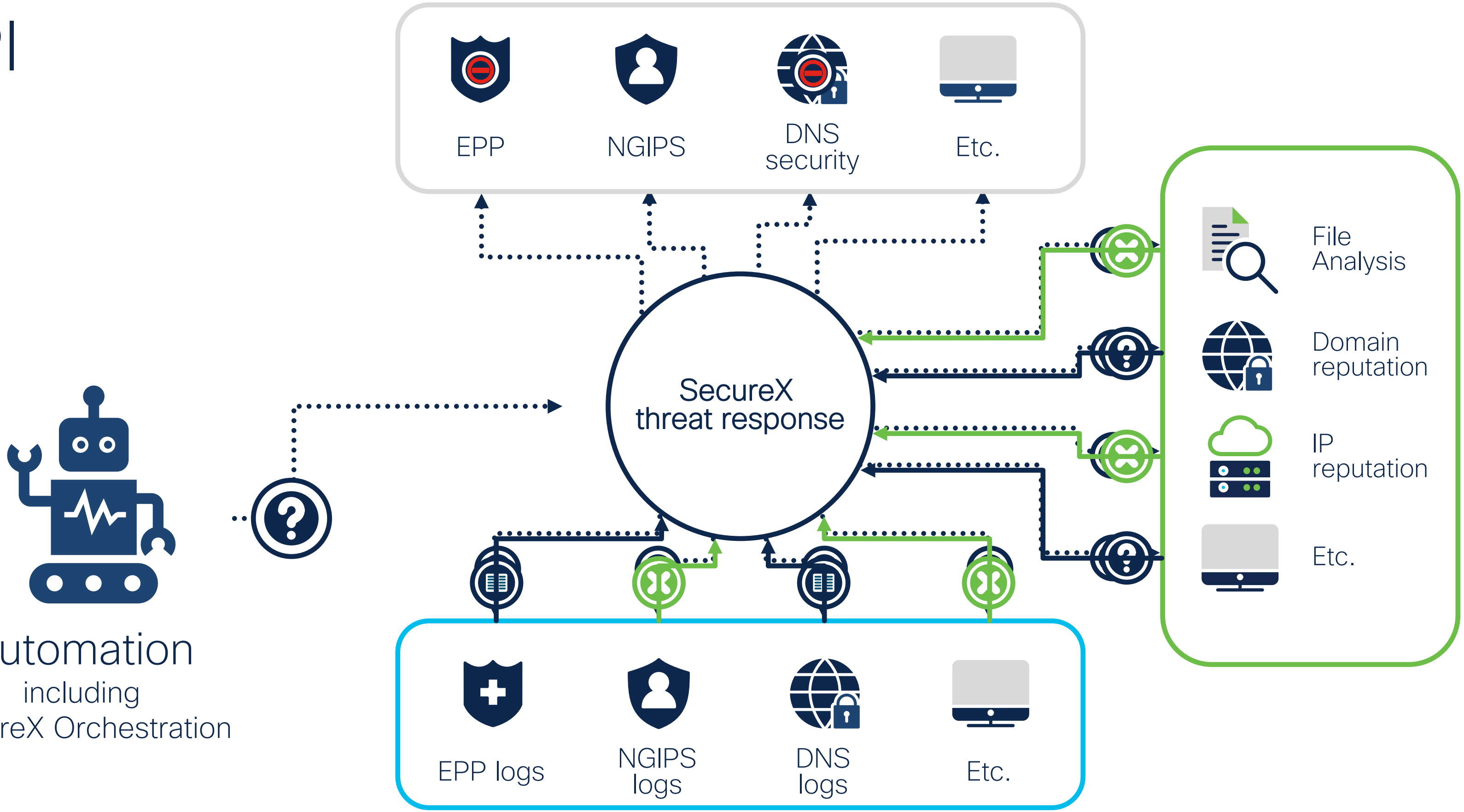


Response



EPP
NGIPS
DNS security
Etc.
SecureX threat response
File Analysis
Domain reputation
IP reputation
Etc.
SecOps
EPP logs
NGIPS logs
DNS logs
Etc.

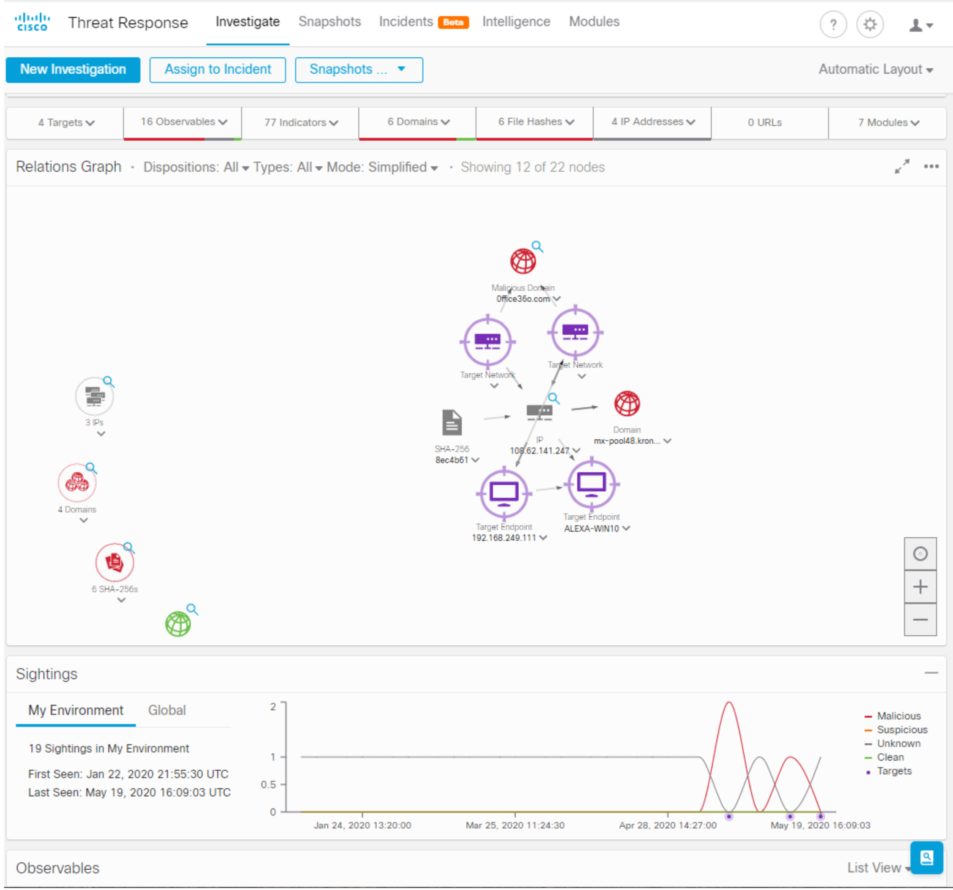
API


EPP
NGIPS
DNS security
Etc.
File Analysis
Domain reputation
IP reputation
Etc.
SecureX threat response
Automation
including
SecureX Orchestration
EPP logs
NGIPS logs
DNS logs
Etc.

Concepts

- “Cisco Threat Response”
- Observables
- Sightings & Targets
- Judgements & Verdicts
- Modules
  - Relay modules
- Data storage
  - Snapshots
  - Casebooks
  - Incidents

“Cisco Threat Response”



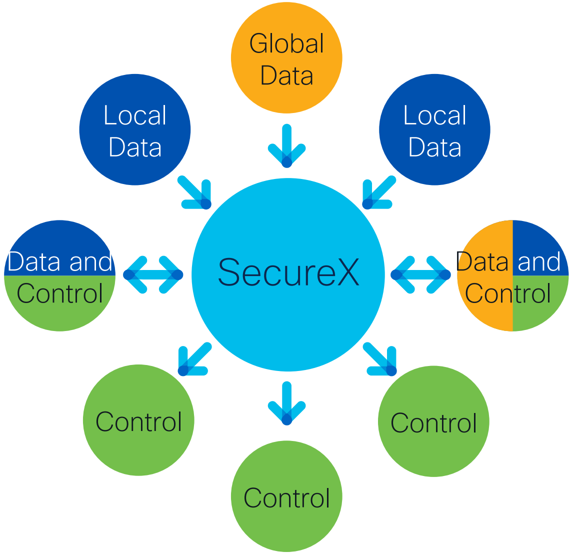
19 Sightings in My Environment

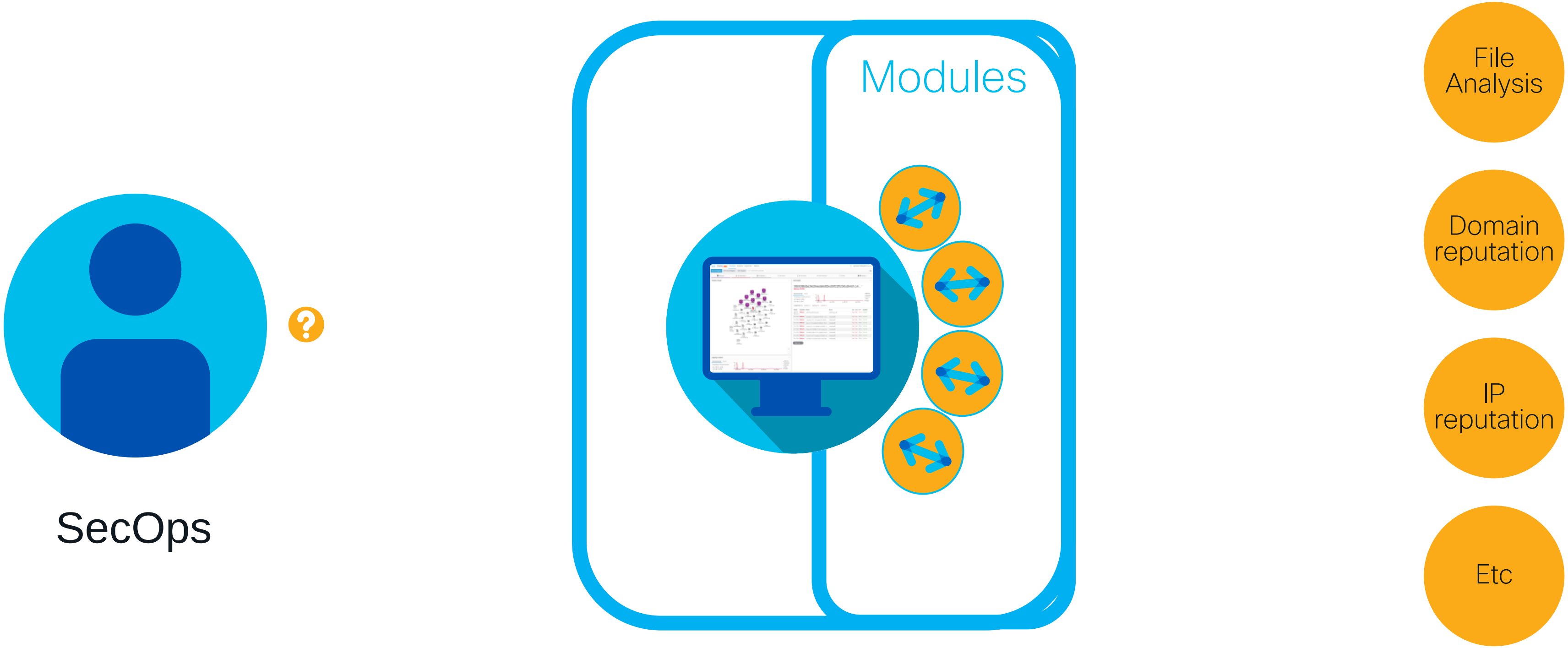
First Seen: Jan 22, 2020 21:55:30 UTC

Last Seen: May 19, 2020 16:09:03 UTC

Modules

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





SecOps

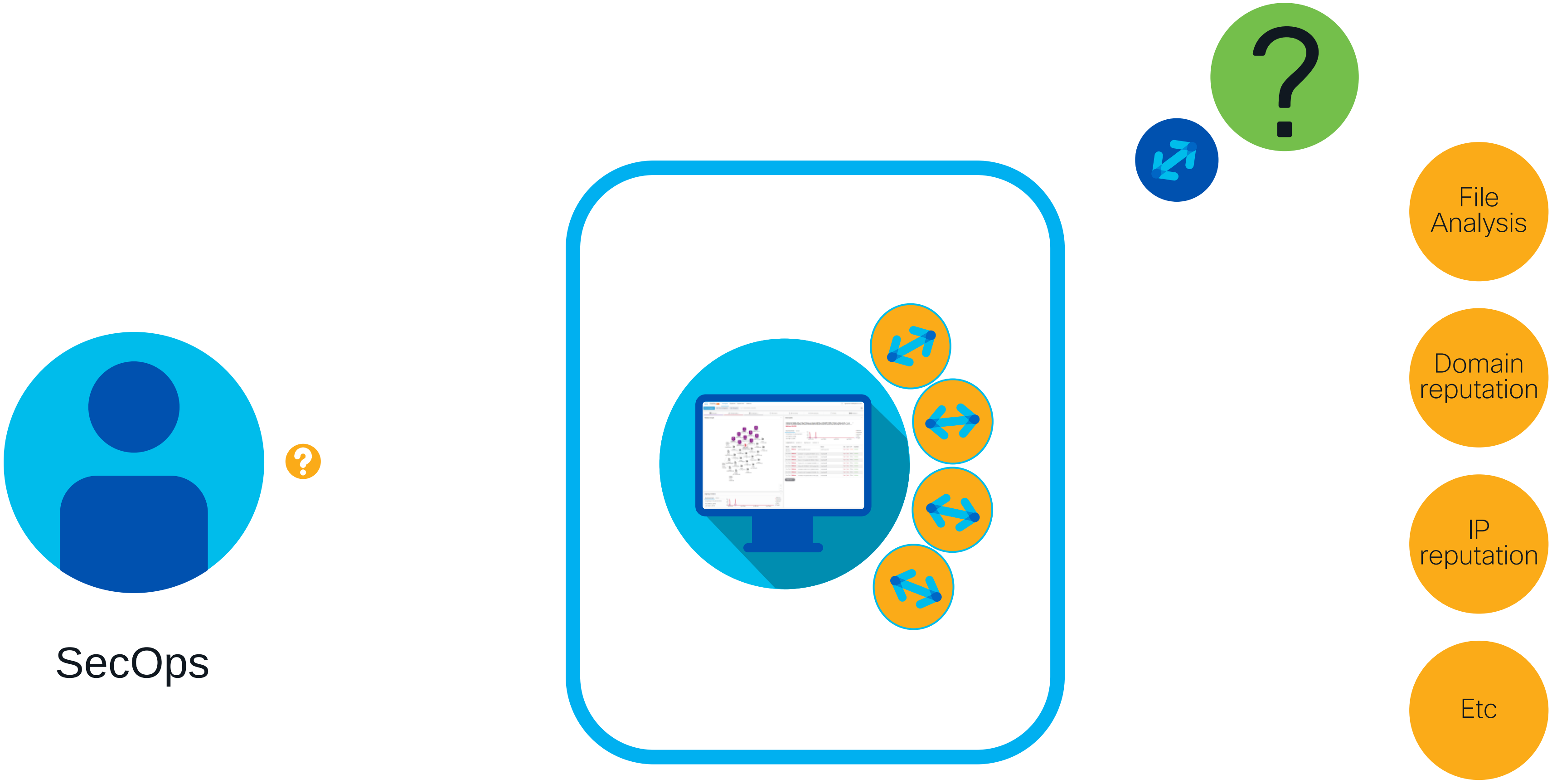
Modules

File Analysis

Domain reputation

IP reputation

Etc



SecOps

File Analysis

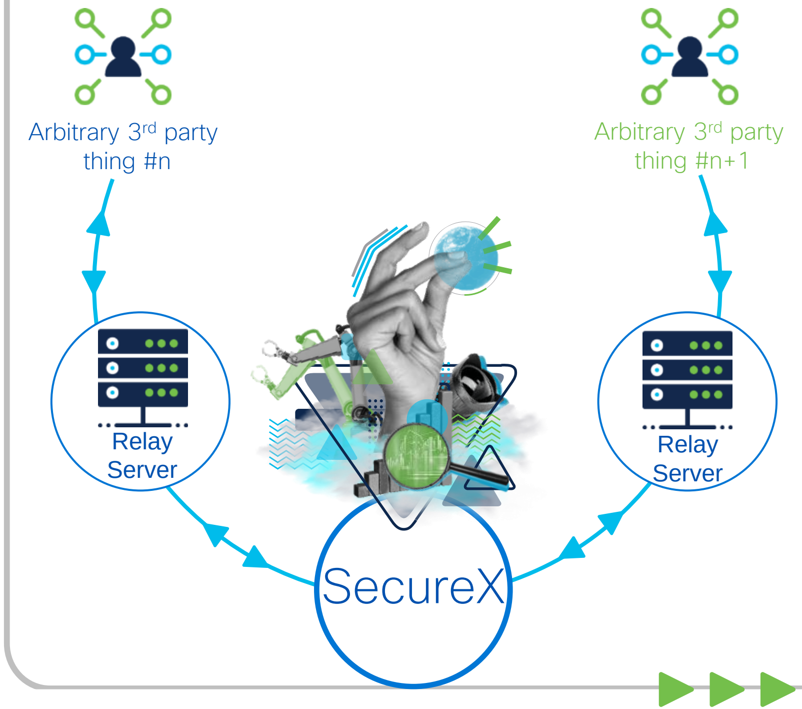
Domain reputation

IP reputation

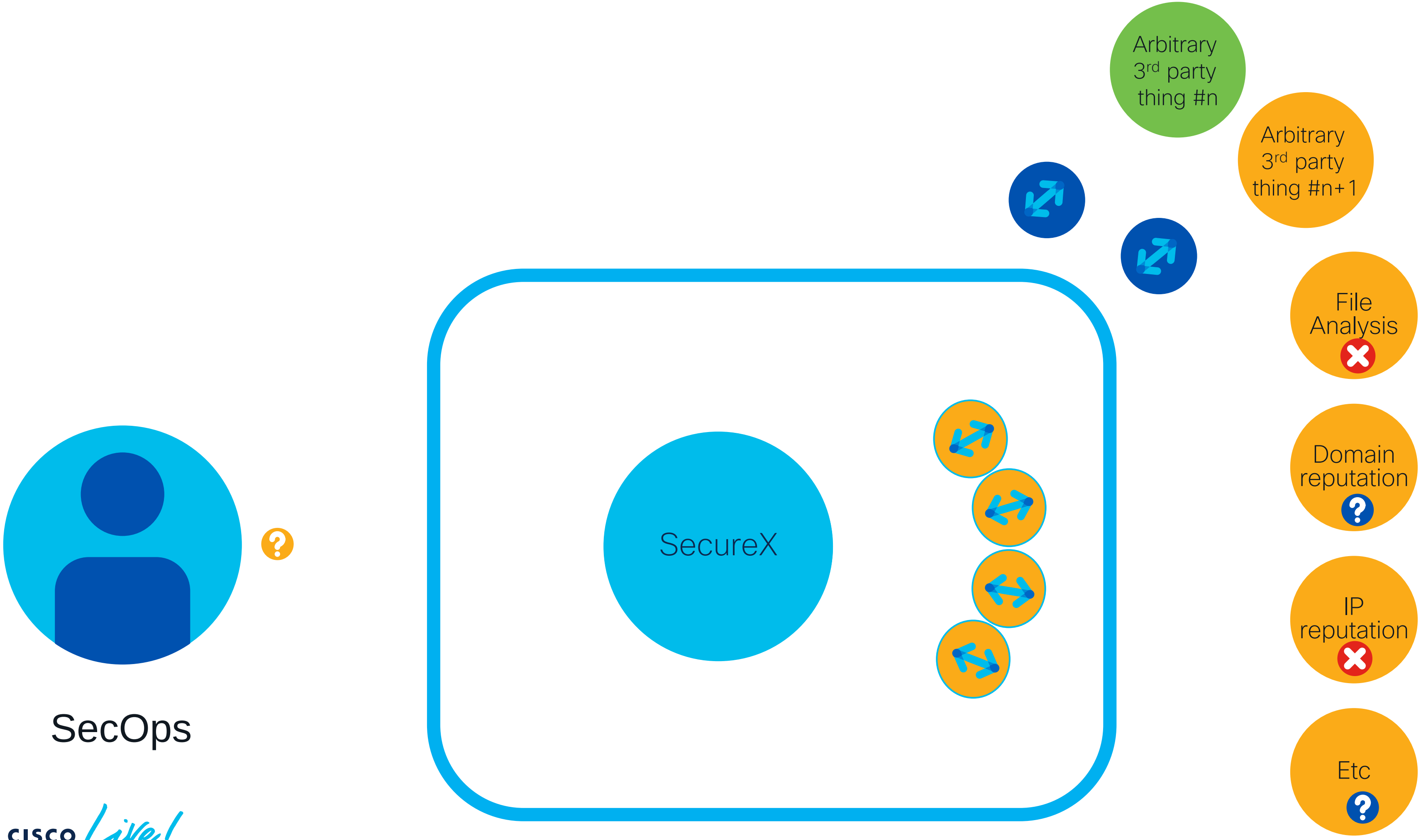
Etc

Relay modules

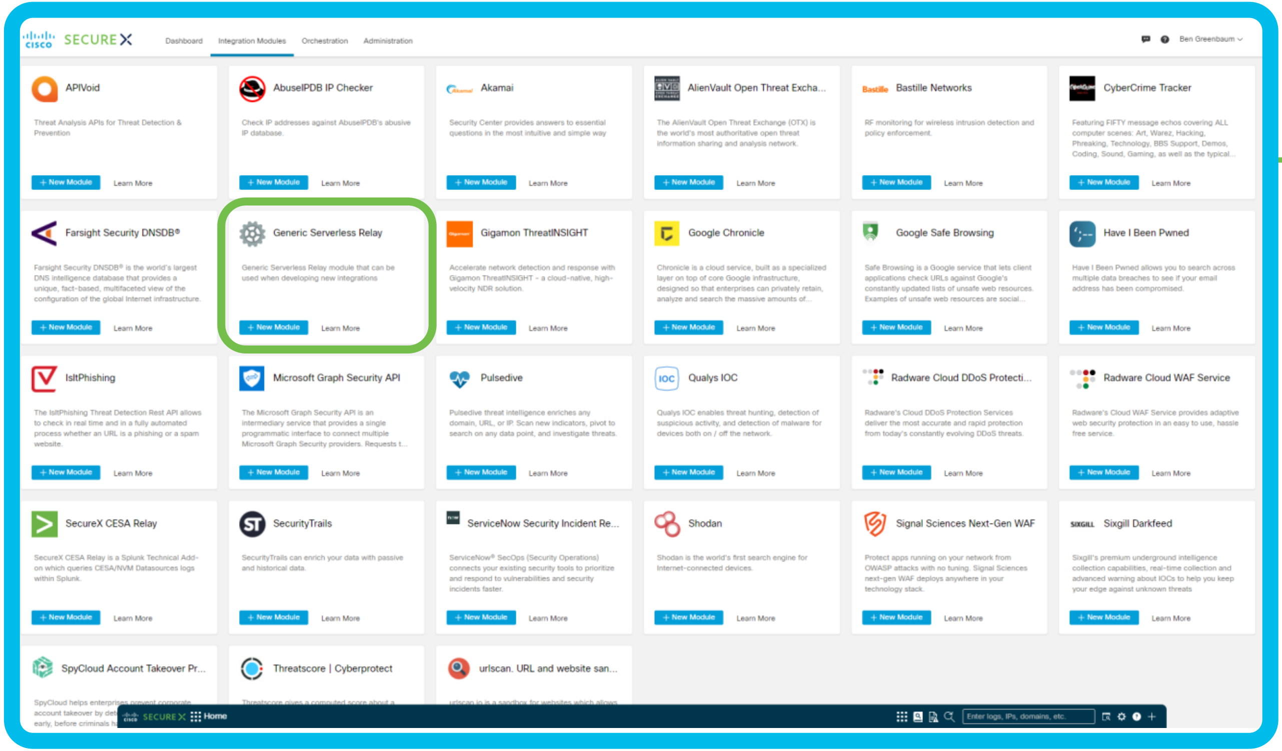
Relay server translates from 3rd party data model and APIs to Cisco Threat Intelligence Model and SecureX APIs



cisco Live!


Arbitrary 3rd party thing #n
Arbitrary 3rd party thing #n+1
File Analysis
Domain reputation
IP reputation
Etc
SecureX
SecOps

Relay modules



APIVoid
Threat Analysis APIs for Threat Detection & Prevention

AbuseIPDB IP Checker
Check IP addresses against AbuseIPDB's abusive IP database.

Akamai
Security Center provides answers to essential questions in the most intuitive and simple way

AlienVault Open Threat Excha...
The AlienVault Open Threat Exchange (OTX) is the world's most authoritative open threat information sharing and analysis network.

Bastille Networks
RF monitoring for wireless intrusion detection and policy enforcement.

CyberCrime Tracker
Featuring FIFTY message echos covering ALL computer scenes: Art, Warez, Hacking, Phreaking, Technology, BBS Support, Demos, Coding, Sound, Gaming, as well as the typical...

Farsight Security DNSDB®
Farsight Security DNSDB® is the world's largest DNS intelligence database that provides a unique, fact-based, multifaceted view of the configuration of the global Internet infrastructure.

Generic Serverless Relay
Generic Serverless Relay module that can be used when developing new integrations

Gigamon ThreatINSIGHT
Accelerate network detection and response with Gigamon ThreatINSIGHT - a cloud-native, high-velocity NDR solution.

Google Chronicle
Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed so that enterprises can privately retain, analyze and search the massive amounts of...

Google Safe Browsing
Safe Browsing is a Google service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources. Examples of unsafe web resources are social...

Have I Been Pwned
Have I Been Pwned allows you to search across multiple data breaches to see if your email address has been compromised.

IsItPhishing
The IsItPhishing Threat Detection Rest API allows to check in real time and in a fully automated process whether an URL is a phishing or a spam website.

Microsoft Graph Security API
The Microsoft Graph Security API is an intermediary service that provides a single programmatic interface to connect multiple Microsoft Graph Security providers. Requests t...

Pulsedive
Pulsedive threat intelligence enriches any domain, URL, or IP. Scan new indicators, pivot to search on any data point, and investigate threats.

Qualys IOC
Qualys IOC enables threat hunting, detection of suspicious activity, and detection of malware for devices both on / off the network.

Radware Cloud DDoS Protecti...
Radware's Cloud DDoS Protection Services deliver the most accurate and rapid protection from today's constantly evolving DDoS threats.

Radware Cloud WAF Service
Radware's Cloud WAF Service provides adaptive web security protection in an easy to use, hassle free service.

SecureX CESA Relay
SecureX CESA Relay is a Splunk Technical Add-on which queries CESA/NVM Datasources logs within Splunk.

SecurityTrails
SecurityTrails can enrich your data with passive and historical data.

ServiceNow Security Incident Re...
ServiceNow® SecOps (Security Operations) connects your existing security tools to prioritize and respond to vulnerabilities and security incidents faster.

Shodan
Shodan is the world's first search engine for Internet-connected devices.

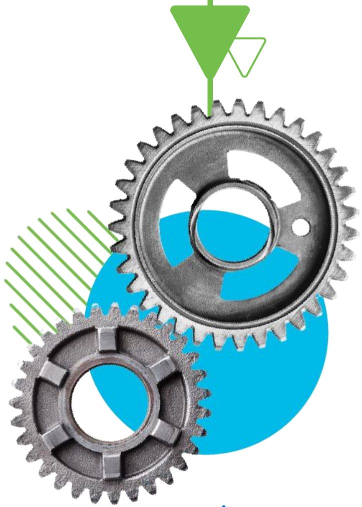
Signal Sciences Next-Gen WAF
Protect apps running on your network from OWASP attacks with no tuning. Signal Sciences next-gen WAF deploys anywhere in your technology stack.

Sixgill Darkfeed
Sixgill's premium underground intelligence collection capabilities, real-time collection and advanced warning about IOCs to help you keep your edge against unknown threats

SpyCloud Account Takeover Pr...
SpyCloud helps enterprises prevent corporate account takeover by det
early, before criminals h

Threatscore | Cyberprotect
Threatscore gives a computed score about a

urlscan. URL and website san...
urlscan.io is a sandbox for websites which allows



Threat Response: Relays and Relay Modules

Relays can be used to provide to SecureX and via SecureX, any of the following supported functions from any technology capable of providing them

- Reputations (malicious, suspicious, etc)
- Sightings (local or global)
- Response/Enforcement (block or quarantine etc on observable)
- Reference Links (search for this observable in external UI)

Observables

Anything that can be observed…

- IP
- Domain
- URL
- File hash
- Email address
- User Identity
- User Agent
- Etc
- …

Sightings

An observable being… observed.

- Firewall alert
- AMP file activity
- Threat Grid file submission
- ESA email logs
- WSA proxy logs
- SWE alarm
- Umbrella DNS request
- Etc
- …

Targets

A local asset involved in a sighting

- Endpoint
- Email address
- IP address
- Server
- Process
- User Identity
- Etc
- …

Judgements & Verdicts

Reputations and opinions on observables

- Malicious
- Suspicious
- Unknown
- Clean

Judgements	Verdicts
Multiple per module	One per module
Points of info	Holistic rendering

Data storage

Snapshot

- Point in time record of investigation
- User-created
- URL accessible

Casebook

- Set of observables
- User-created
- User notes
- Pivot Menus and actions
- Available across products

Incident

- Security Event
- System or user created
- System triaged
- User-managed

Cisco Threat Intelligence Model

CTIM is closely based on STIX with a few simplifications

The primary focus of CTIM is the decomposition, storage, and retrieval of vast quantities of existing threat intelligence.

Data Model examples:

- Actor
- Attack Pattern
- Campaign
- Course of Action
- Feedback
- Incident
- Indicator
- Judgement
- Malware
- Relationship
- Casebook
- Sighting
- IdentityAssertion
- Tool
- Verdict
- Weakness

Threat Response: Relays and Relay Modules

Relays can be used to provide to SecureX and via SecureX, any of the following supported functions from any technology capable of providing them

- Reputations (malicious, suspicious, etc)
- Sightings (local or global)
- Response/Enforcement (block or quarantine etc on observable)
- Reference Links (search for this observable in external UI)

Demo #1 – Browser Plugin

Threat Response Recap

SecureX Threat Response can help you

- Hunt for threats
- Defend proactively against threats
- Remediate discovered attacks
- Investigate and manage incidents

You can extend Threat Response via Relays to leverage additional sources of

- Threat Intelligence
- Local Security Context
- Response and enforcement
- External references and lookups

You can leverage all capabilities of Threat Response over the API

- Tie them into existing tools
- Standalone automation scripts

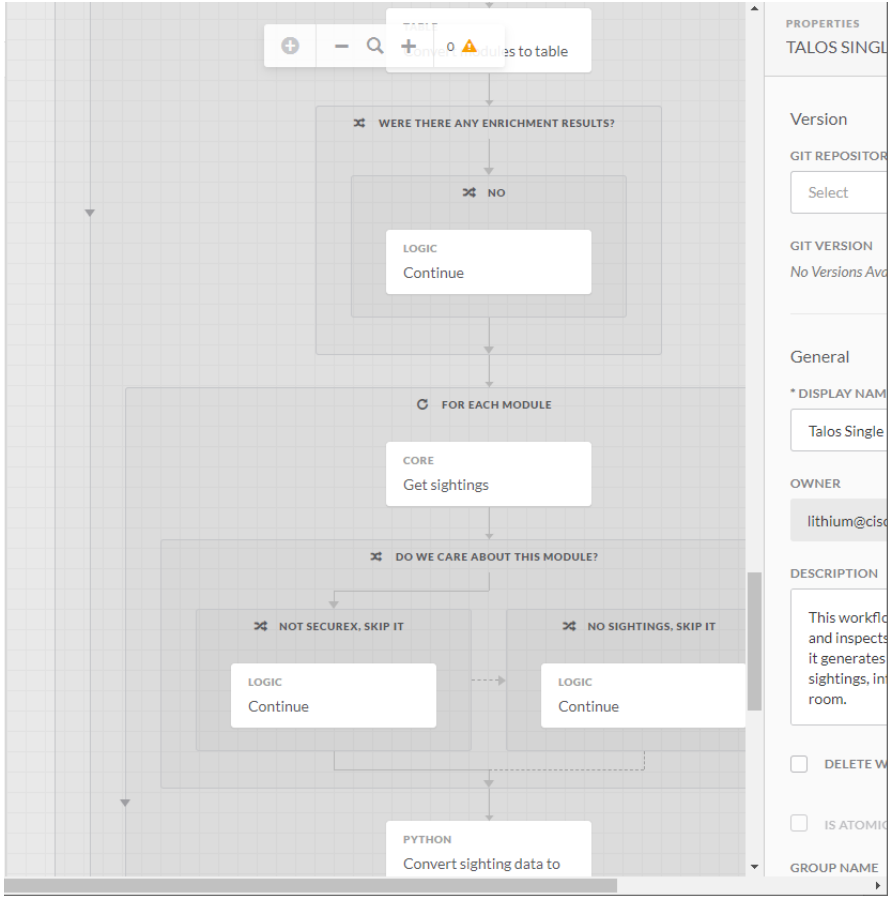
SecureX orchestration

Integration Use Cases for SecureX orchestration

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

SecureX orchestration

- Workflows run in an interpreter
- Products/Services host their own APIs
- SecureX orchestration makes requests
  - Nature of requests is… wide open
  - “tell me about this observable”
  - “spin up another VPN head end”
  - “analyze this URL”
  - “ask for approval via Duo”
  - “record an incident / open a ticket”
  - “Post a chat in the Teams Space”
- SecureX orchestration can respond and react to results, and pass results between steps in the workflow



PROPERTIES
TALOS SINGL

Version
GIT REPOSITOR
Select
GIT VERSION
No Versions Ava

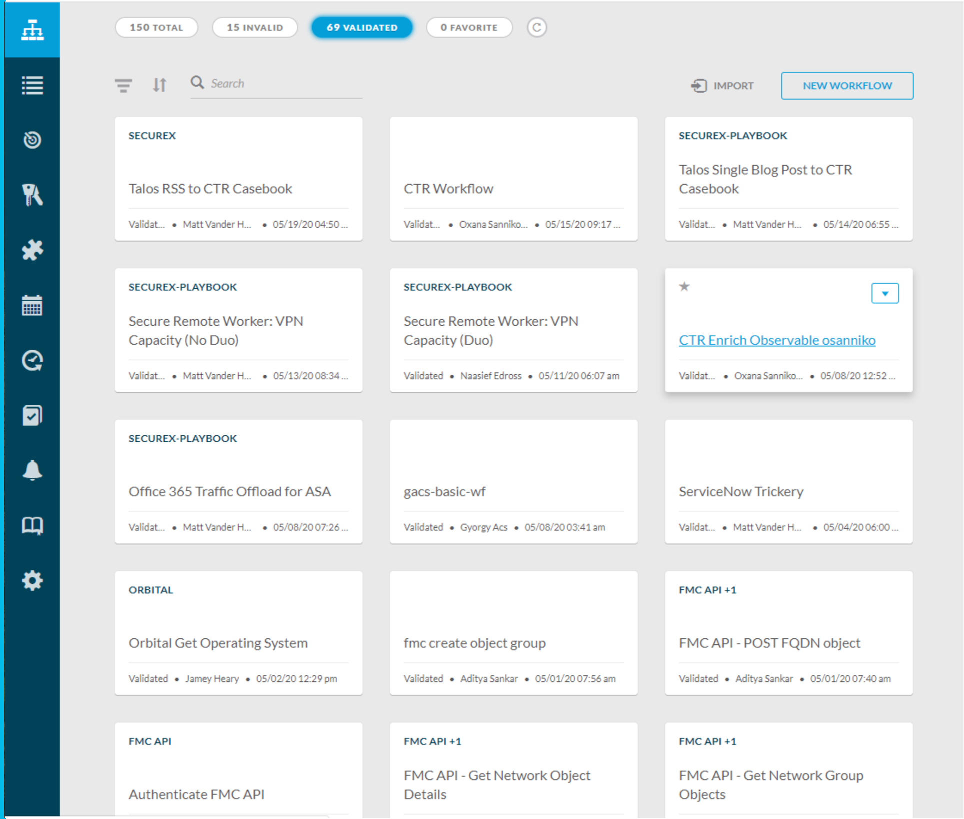
General
* DISPLAY NAM
Talos Single
OWNER
lithium@cisc
DESCRIPTION
This workflo
and inspects
it generates
sightings, in
room.

□ DELETE W
□ IS ATOMIC
GROUP NAME

Concepts

- “Action Orchestrator”
- Adapter
- Workflow
- Applicable programming concepts
  - Flow Control
  - Variables

“Action Orchestrator”



SECUREX
Talos RSS to CTR Casebook
Validat... • Matt Vander H... • 05/19/20 04:50 ...

CTR Workflow
Validat... • Oxana Sanniko... • 05/15/20 09:17 ...

SECUREX-PLAYBOOK
Talos Single Blog Post to CTR Casebook
Validat... • Matt Vander H... • 05/14/20 06:55 ...

SECUREX-PLAYBOOK
Secure Remote Worker: VPN Capacity (No Duo)
Validat... • Matt Vander H... • 05/13/20 08:34 ...

SECUREX-PLAYBOOK
Secure Remote Worker: VPN Capacity (Duo)
Validated • Naasief Edross • 05/11/20 06:07 am

★
CTR Enrich Observable osanniko
Validat... • Oxana Sanniko... • 05/08/20 12:52 ...

SECUREX-PLAYBOOK
Office 365 Traffic Offload for ASA
Validat... • Matt Vander H... • 05/08/20 07:26 ...

gacs-basic-wf
Validated • Gyorgy Acs • 05/08/20 03:41 am

ServiceNow Trickery
Validat... • Matt Vander H... • 05/04/20 06:00 ...

ORBITAL
Orbital Get Operating System
Validated • Jamey Heary • 05/02/20 12:29 pm

fmc create object group
Validated • Aditya Sankar • 05/01/20 07:56 am

FMC API +1
FMC API - POST FQDN object
Validated • Aditya Sankar • 05/01/20 07:40 am

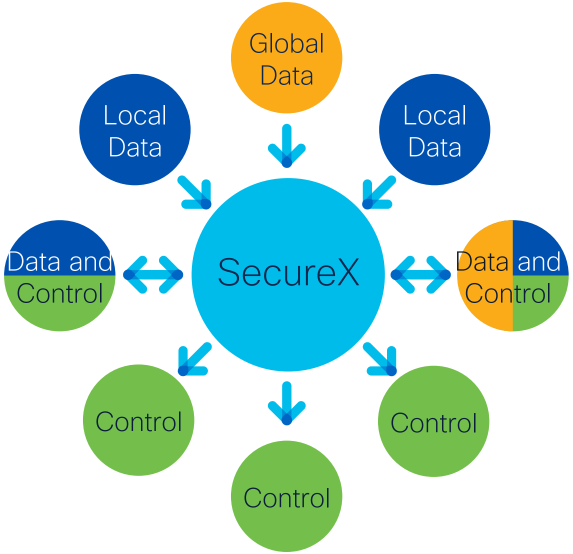
FMC API
Authenticate FMC API

FMC API +1
FMC API - Get Network Object Details

FMC API +1
FMC API - Get Network Group Objects

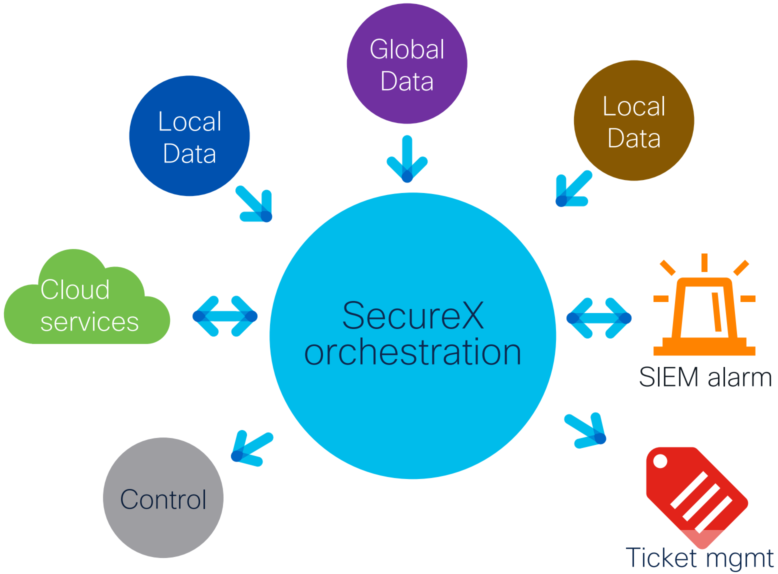
Adapters

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



Adapters

Pluggable code to talk to any arbitrary technologies



Custom

Adapters

Arbitrary 3rd Party Integrations?

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

If REST Then YES

Multiple Generic Protocol Adapters

- HTTP
- FTP
- JDBC
- SMTP
- SNMP
- SSH

Workflow

- A series of steps to follow
- A “program”
- Created by:
  - Cisco
  - User
  - Community

Programming Concepts

- No specific language experience required
- Familiarity a plus with ideas like
  - Flow Control
    - Conditionals
    - Loops
  - Variables

cisco Live!

Workflow Triggers

- Manually
  - In the Orchestration UI
- Email
  - to configured IMAP inbox
- From SecureX threat response
  - Via pivot menu item
  - For workflows that take one input observable
- Calendar/schedule
  - "Every day at 2:42"
  - "Every *n* minutes"
  - AKA pull/poll to external flag, SXtr API, etc

Demo #1 – Workflow editor

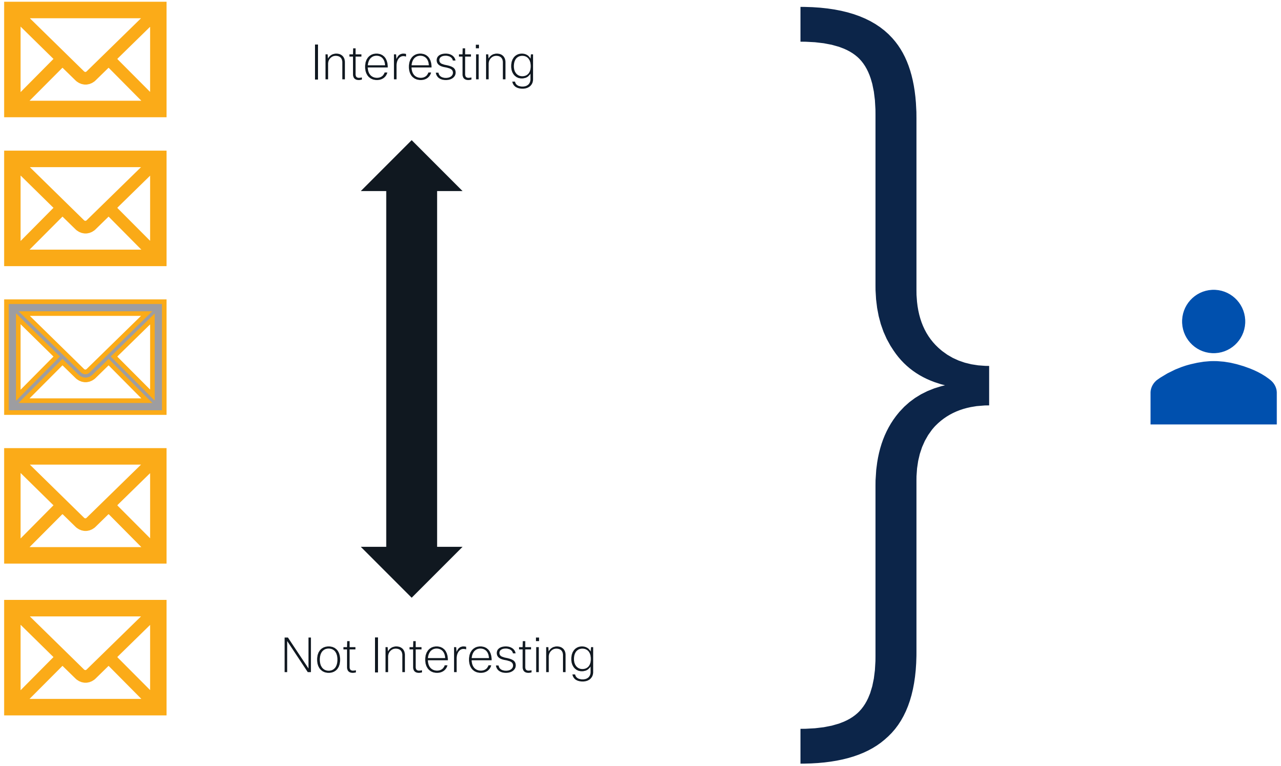
Workflow Example:
Phishing Investigation

Phishing Investigation Workflow

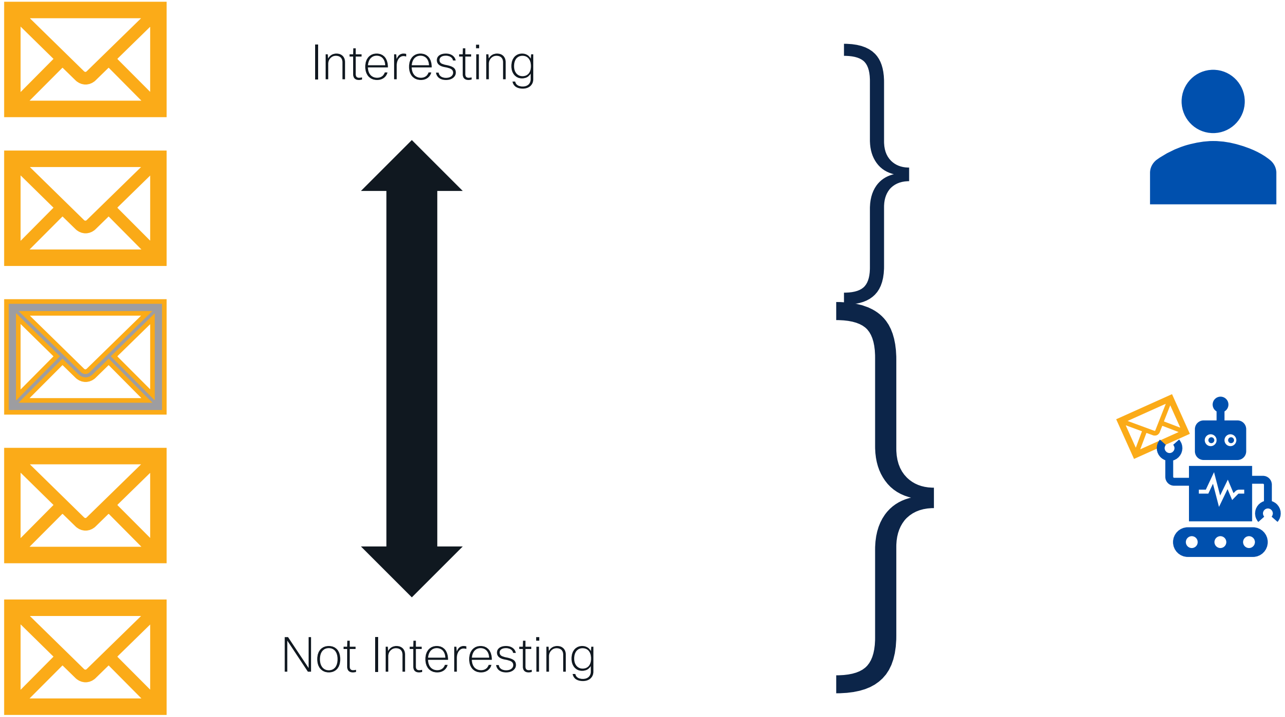
Phishing Investigation Workflow

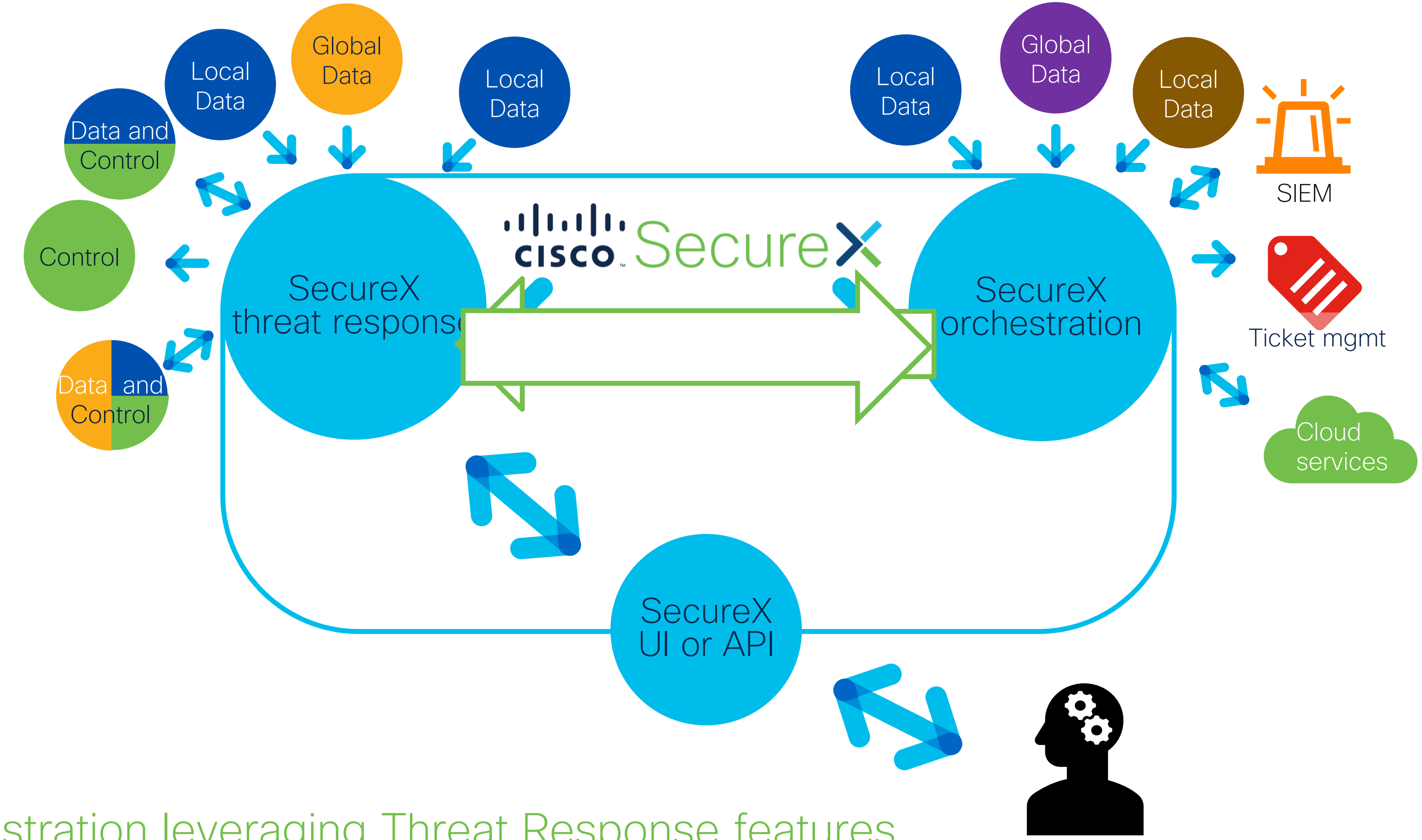
- Receive Email
- Process Attachment(s)
- Inspect headers and body for Observables (email addresses, domains, files, etc)
- Check Observables Dispositions (malicious, suspicious, unknown, clean)
- Analyze unknown Observables (if supported, e.g. files / URLs)
- Make verdict based on all dispositions
  - If Malicious, alert user and SOC and create SecureX Incident
  - If Suspicious or Unknown alert SOC to continue investigation

Phishing Investigation Workflow



Phishing Investigation Workflow

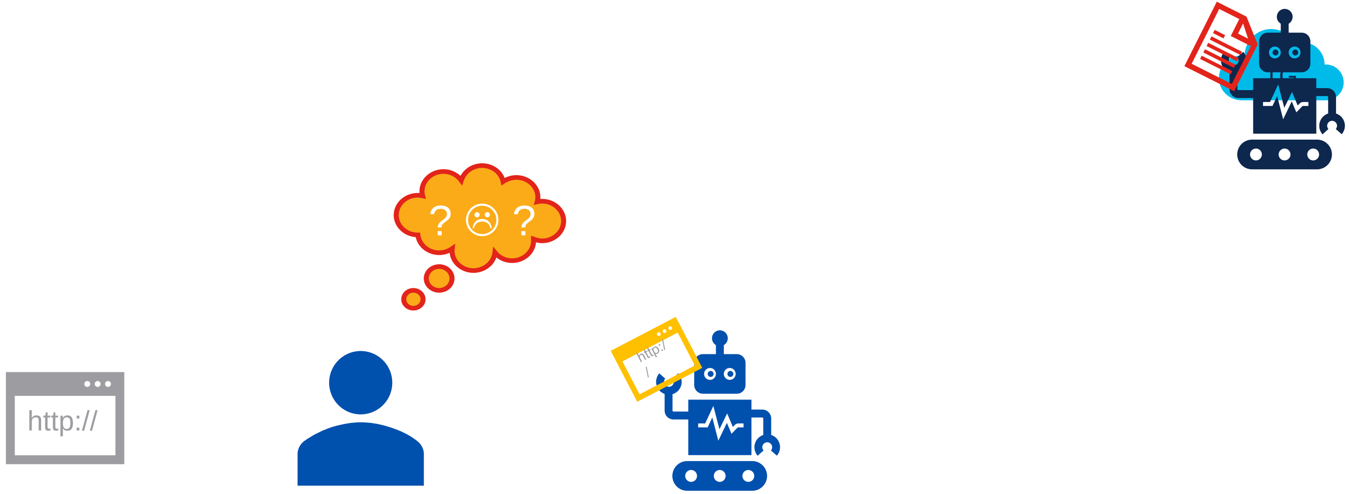




Orchestration leveraging Threat Response features

Workflow Example:
Submit URL to ThreatGrid

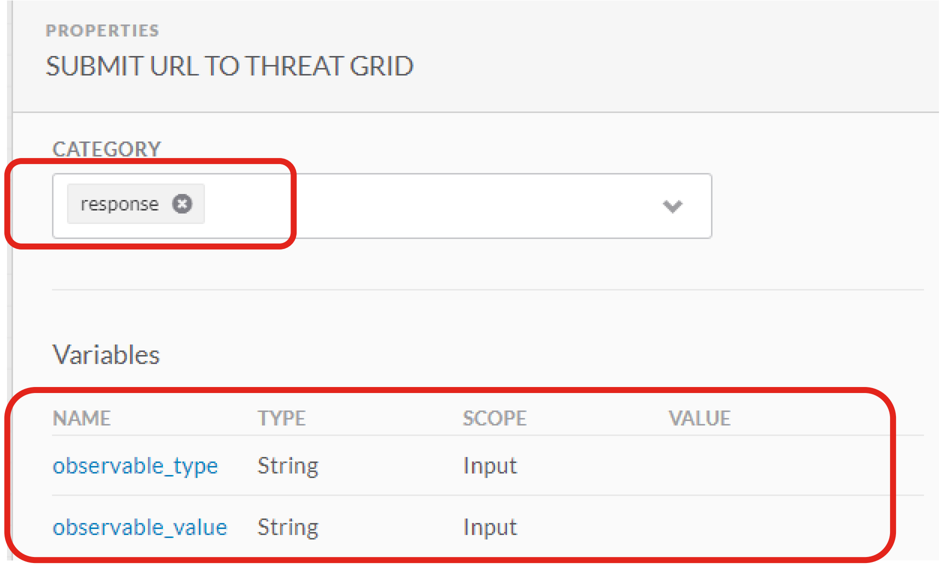
“URL to ThreatGrid” Workflow



Submit URL to ThreatGrid Workflow

- Verify URL
- Submit to ThreatGrid via ThreatGrid API
- Provide report link to analyst

Add a Workflow to Threat Response Menus



PROPERTIES

SUBMIT URL TO THREAT GRID

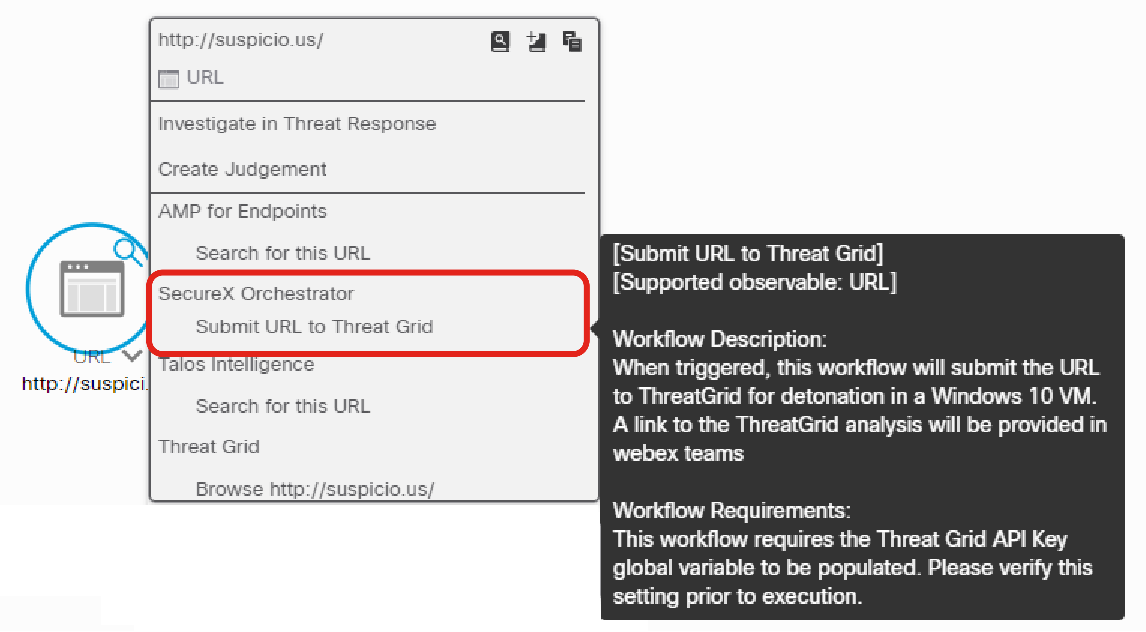
CATEGORY

response

Variables

NAME	TYPE	SCOPE	VALUE
observable_type	String	Input	
observable_value	String	Input	

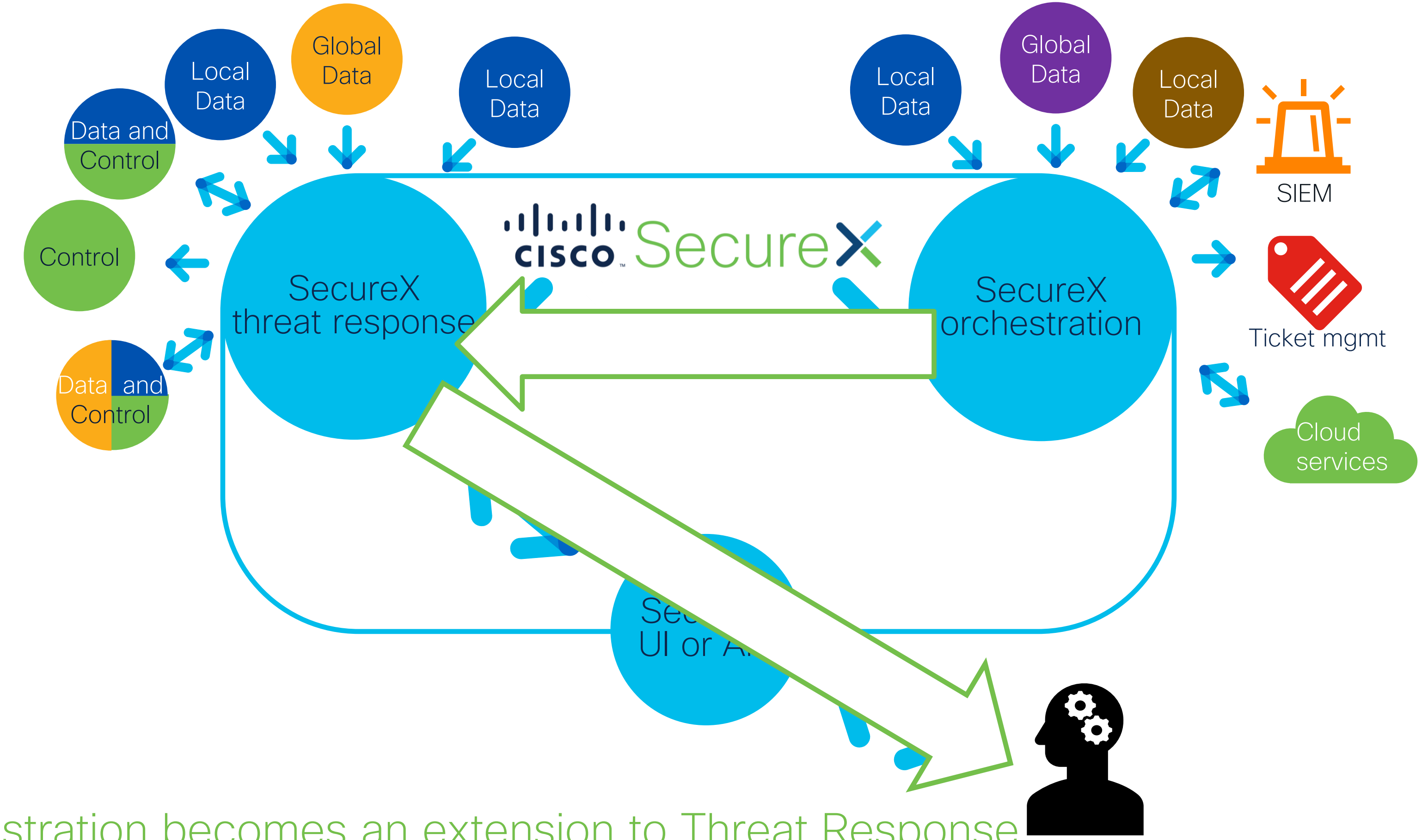
Add a Workflow to Threat Response Menus



[Submit URL to Threat Grid]
[Supported observable: URL]

Workflow Description:
When triggered, this workflow will submit the URL to ThreatGrid for detonation in a Windows 10 VM. A link to the ThreatGrid analysis will be provided in webex teams

Workflow Requirements:
This workflow requires the Threat Grid API Key global variable to be populated. Please verify this setting prior to execution.



Orchestration becomes an extension to Threat Response

Need response capability from a 3rd party RESTful API for which there is no Module or Relay Module?

- No Problem!
- “if REST then yes”
- Create a workflow that uses the API
- Enable that workflow for the Threat Response menu
- Done!
- *(or, write a Relay Module)*

Orchestration Recap

SecureX orchestration can help you

- Secure your assets more efficiently
- Reduce human error
- Reduce human lag
- Adhere to documented policies

You can extend Orchestration via protocol-based adapters to leverage additional services from any software that supports:

- HTTP, FTP, SMTP, SNMP, SSH, etc

You can leverage all capabilities of Orchestration as Threat Response menu actions for use in

- SecureX console
- Threat Response API scripts

Conclusion & Resources

Recap

- SecureX Brings together
  - Local security context
  - Threat intelligence
  - Response capabilities
  - Automation & Orchestration
- SecureX reduces operational complexity
- SecureX is API-driven
- SecureX Threat Response
  - Fully leverageable over API
  - Can include arbitrary technologies via Custom Relays
  - Can include custom response actions via Orchestration Workflows
- SecureX Orchestration
  - IS a dev environment
  - Workflows are triggerable externally via email, remote flags, etc
  - Can leverage arbitrary technologies over multiple built in protocols

The Bottom Line:

- SecureX is heavily extensible to accommodate multiple
  - Organization security needs
  - Existing technologies already in your SOC
  - Future technologies you may add, Cisco or not
- SecureX is forward-compatible to drive
  - Progress up the maturity model ladder
  - Increased visibility, efficiency, and security

Resources

Development References to continue learning …

General SecureX Programmability

- developer.cisco.com/SecureX
- cs.co/SecureX_integration_workflows
- cs.co/spoton_series
- Product Documentation
- github.com/CiscoSecurity

threat response

- Self paced API labs: cs.co/CTR-API-labs
- CTIM: cs.co/CTIM_docs
- Code: cs.co/SXtr_repo

orchestration

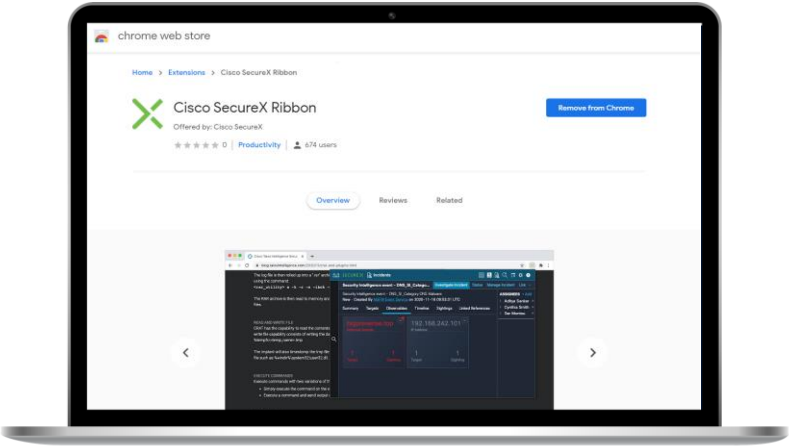
- Tutorials and demos: cs.co/SXO_Videos
- Documentation: cs.co/SXO_docs
- Code: cs.co/SXO_repo

General SecureX Resources

- SecureX introduction:
  - cisco.com/go/securex
- Watch and save SecureX playlist
  - cs.co/SecureX_videos
- SecureX FAQ:
  - cs.co/SecureX_faq
- SecureX content at prior Cisco Lives
  - cs.co/SecureX_CiscoLive
- Get Started!
  - security.cisco.com

SecureX Browser Plugins

cs.co/SecureX_Chrome



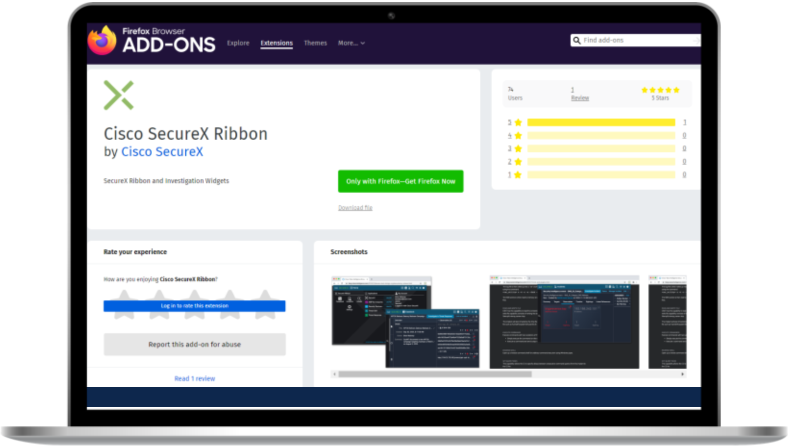
chrome web store

Home > Extensions > Cisco SecureX Ribbon

Cisco SecureX Ribbon

Offered by: Cisco SecureX

★★★★★ 0 | Productivity | 674 users



Firefox Browser ADD-ONS

Explore
Extensions
Themes
More...
Find add-ons

Cisco SecureX Ribbon

by Cisco SecureX

SecureX Ribbon and Investigation Widgets

74 Users	1 Review	★★★★★ 5 Stars

5 ★	1
4 ★	0
3 ★	0
2 ★	0
1 ★	0

Only with Firefox—Get Firefox Now
Download file

Rate your experience

How are you enjoying Cisco SecureX Ribbon?

Log in to rate this extension
Report this add-on for abuse
Read 1 review
Screenshots

cs.co/SecureX_Firefox

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.

Continue your Education

SecureX CL AMS 23 Learning Map

https://www.ciscolive.com/emea/learn/sessions/session-catalog.html?search.learningmap=1614366204738006MRIo#/

Objectives

Overview

- Understand SecureX purpose and application
- Understand integration use cases (why integrate?)

Threat Response

- Understand Modules and Relays

Orchestration

- Understand Workflows and Targets

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

Questions?

The bridge to possible

Thank you

cisco Live!

ALL IN