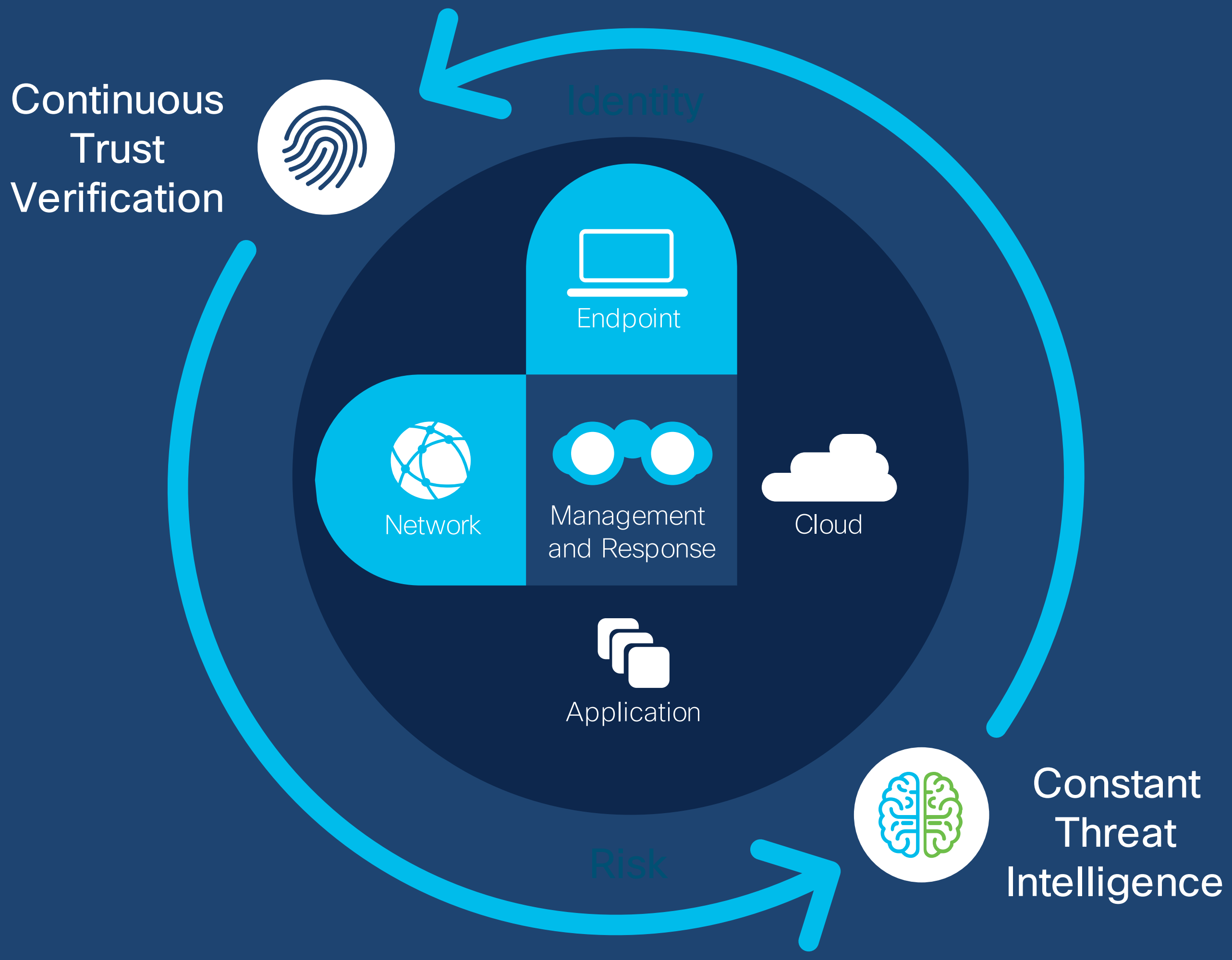
cisco SECURE X

Cisco SecureX

Martin Rulec – mrulec@cisco.com
GVE Technical Solutions Architect
January 2021

Protect your business with the strongest security team on the planet



The Cisco Security Platform

cisco SECURE

cisco SECURE X

Cisco Secure Platform

Network Security

- Secure Network Analytics
  Formerly Stealthwatch
- Secure Firewall
  Formerly Next-Generation Firewall (NGFW)
- Identity Services Engine

Cloud Edge

- Umbrella

User and Endpoint Protection

- Secure Endpoint
  Formerly Advanced Malware Protection (AMP) for Endpoints
- Secure Email
  Formerly Email Security
- Secure Access by Duo

Application Security

- Secure Workload
  Formerly Tetration

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

Simplicity

Integrate technology together with true **turnkey interoperability**

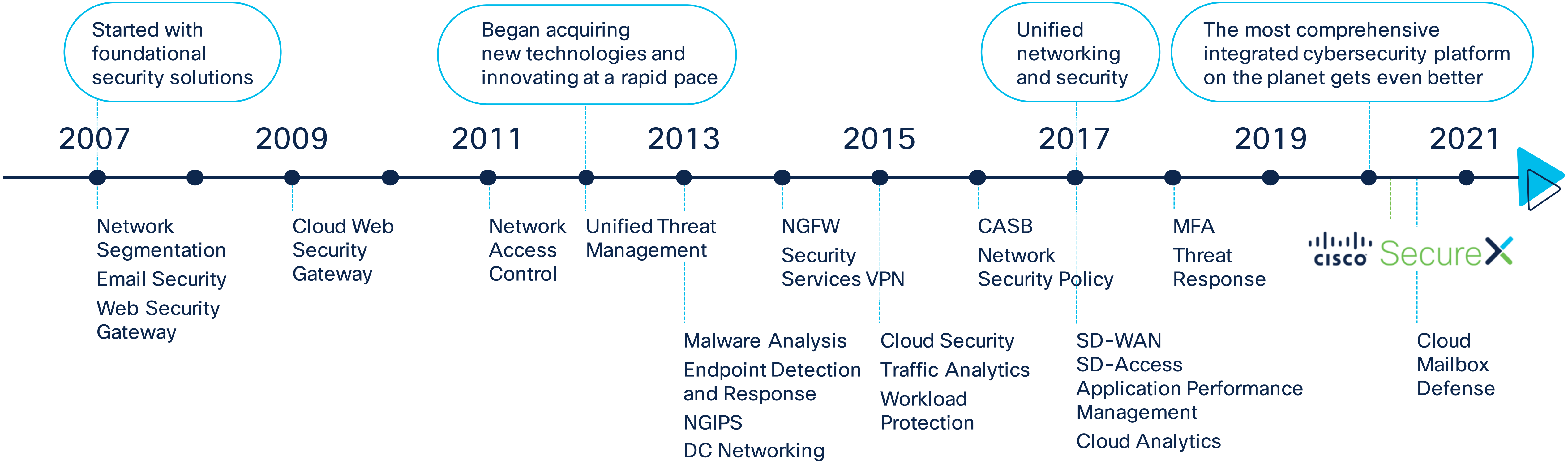
Visibility

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

Building a platform takes time and engineering talent



Started with foundational security solutions

Began acquiring new technologies and innovating at a rapid pace

Unified networking and security

The most comprehensive integrated cybersecurity platform on the planet gets even better

2007

- Network Segmentation
- Email Security
- Web Security Gateway

2009

- Cloud Web Security Gateway

2011

- Network Access Control
- Unified Threat Management

2013

- Malware Analysis
- Endpoint Detection and Response
- NGIPS
- DC Networking
- NGFW
- Security Services VPN

2015

- Cloud Security
- Traffic Analytics
- Workload Protection
- CASB
- Network Security Policy

2017

- SD-WAN
- SD-Access
- Application Performance Management
- Cloud Analytics
- MFA
- Threat Response

2019

- cisco SecureX
- Cloud Mailbox Defense

2021

Over $6B in M&A over the past 6 years

Over 400 threat researchers

Unparalleled platform breadth

Introducing SecureX

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

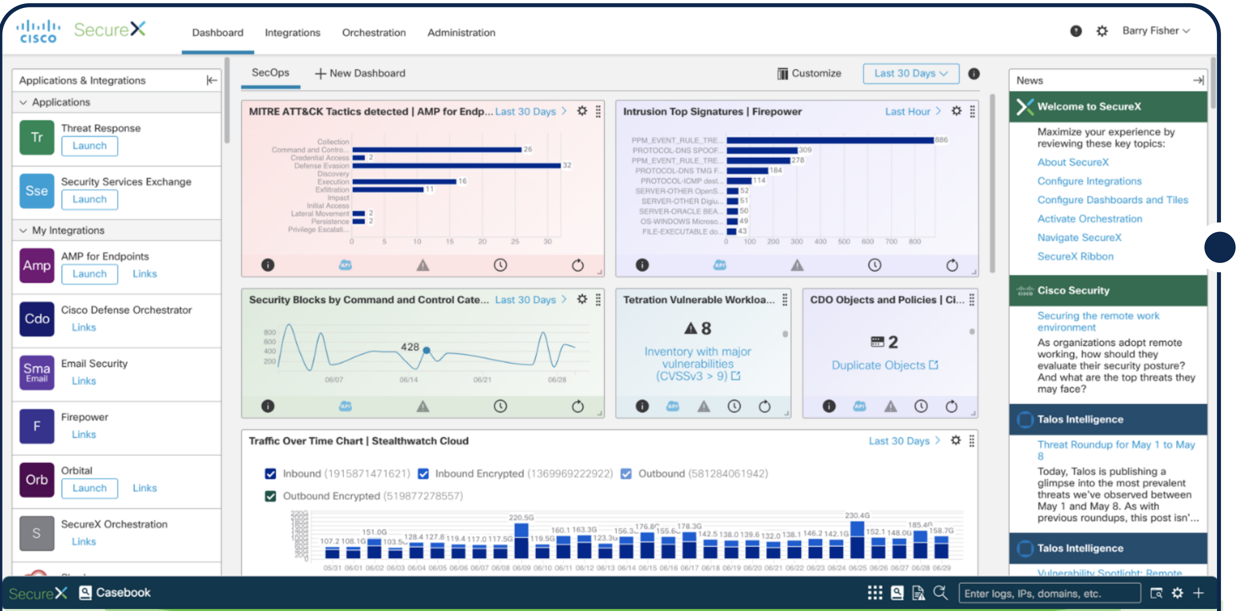
Cisco Secure

Network

Endpoint

Cloud

Applications


cisco SecureX
Dashboard
Integrations
Orchestration
Administration
Barry Fisher
Applications & Integrations
Applications
Tr Threat Response Launch
Sse Security Services Exchange Launch
My Integrations
Amp AMP for Endpoints Launch Links
Cdo Cisco Defense Orchestrator Links
Sma Email Email Security Links
F Firepower Links
Orb Orbital Launch Links
S SecureX Orchestration Links
SecOps
+ New Dashboard
Customize
Last 30 Days
MITRE ATT&CK Tactics detected | AMP for Endp... Last 30 Days
Collection
Command and Contro... 26
Credential Access 2
Defense Evasion 32
Discovery
Execution 16
Exfiltration 11
Impact
Initial Access
Lateral Movement 2
Persistence 2
Privilege Escalati...
0 5 10 15 20 25 30
Intrusion Top Signatures | Firepower Last Hour
PPM_EVENT_RULE_TRE... 886
PROTOCOL-DNS SPOOF... 309
PPM_EVENT_RULE_TRE... 278
PROTOCOL-DNS TMG F... 184
PROTOCOL-ICMP dest... 114
SERVER-OTHER OpenS... 52
SERVER-OTHER Digiu... 51
SERVER-ORACLE BEA... 50
OS-WINDOWS Microso... 49
FILE-EXECUTABLE do... 43
0 100 200 300 400 500 600 700 800
Security Blocks by Command and Control Cate... Last 30 Days
800 600 400 200
428
06/07 06/14 06/21 06/28
Tetration Vulnerable Workloa...
8
Inventory with major vulnerabilities (CVSSv3 > 9)
CDO Objects and Policies | Ci...
2
Duplicate Objects
Traffic Over Time Chart | Stealthwatch Cloud Last 30 Days
☑ Inbound (1915871471621) ☑ Inbound Encrypted (1369969222922) ☑ Outbound (581284061942)
☑ Outbound Encrypted (519877278557)
107.2 108.1G 151.0G 103.5G 128.4 127.8 119.4 117.0 117.5G 220.5G 119.5G 160.1 163.3G 123.3G 156.3G 176.8G 155.6G 178.3G 142.5 138.0 139.6 132.0 138.1 146.2 142.1G 230.4G 152.1 148.0G 185.4G 158.7G
05/31 06/01 06/02 06/03 06/04 06/05 06/06 06/07 06/08 06/09 06/10 06/11 06/12 06/13 06/14 06/15 06/16 06/17 06/18 06/19 06/20 06/21 06/22 06/23 06/24 06/25 06/26 06/27 06/28 06/29
News
Welcome to SecureX
About SecureX
Configure Integrations
Configure Dashboards and Tiles
Activate Orchestration
Navigate SecureX
SecureX Ribbon
Cisco Security
Securing the remote work environment
Talos Intelligence
Threat Roundup for May 1 to May 8
Talos Intelligence
Vulnerability Spotlight: Remote
SecureX Casebook
Enter logs, IPs, domains, etc.

Maximize your experience by reviewing these key topics:

As organizations adopt remote working, how should they evaluate their security posture? And what are the top threats they may face?

Today, Talos is publishing a glimpse into the most prevalent threats we've observed between May 1 and May 8. As with previous roundups, this post isn'...

Your Infrastructure

3rd Party/ITSM

Intelligence

Identity

SIEM/SOAR

Unified Visibility

SecureX

Detection Analytics

Investigation Remediation

Managed Policy

Orchestration Automation

Your teams

SecOps

ITOps

NetOps

cisco SECURE X

The broadest, most integrated set of XDR capabilities on the market

Broadest XDR capabilities through …

Built-in eXtensions – Simplify breach defense by natively connecting detection to response with capabilities integrated within each other products' consoles across the broadest portfolio.

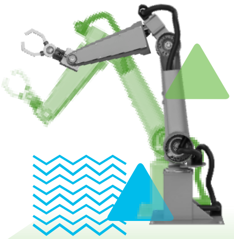
Intelligent Detections – Identify malicious intent and risk exposure more accurately by connecting machine learning-enhanced analytics across the most data sources.

Confident Responses – Reduce threat dwell times by pinpointing root causes with visual investigations and by connecting playbook-driven automation across the most control points.

SecureX is a cloud-native security platform

Integrated and open for **simplicity**

Unified in one location for **visibility**



Maximized operational **efficiency**

SecureX

integrations
built-in, pre-built
or custom

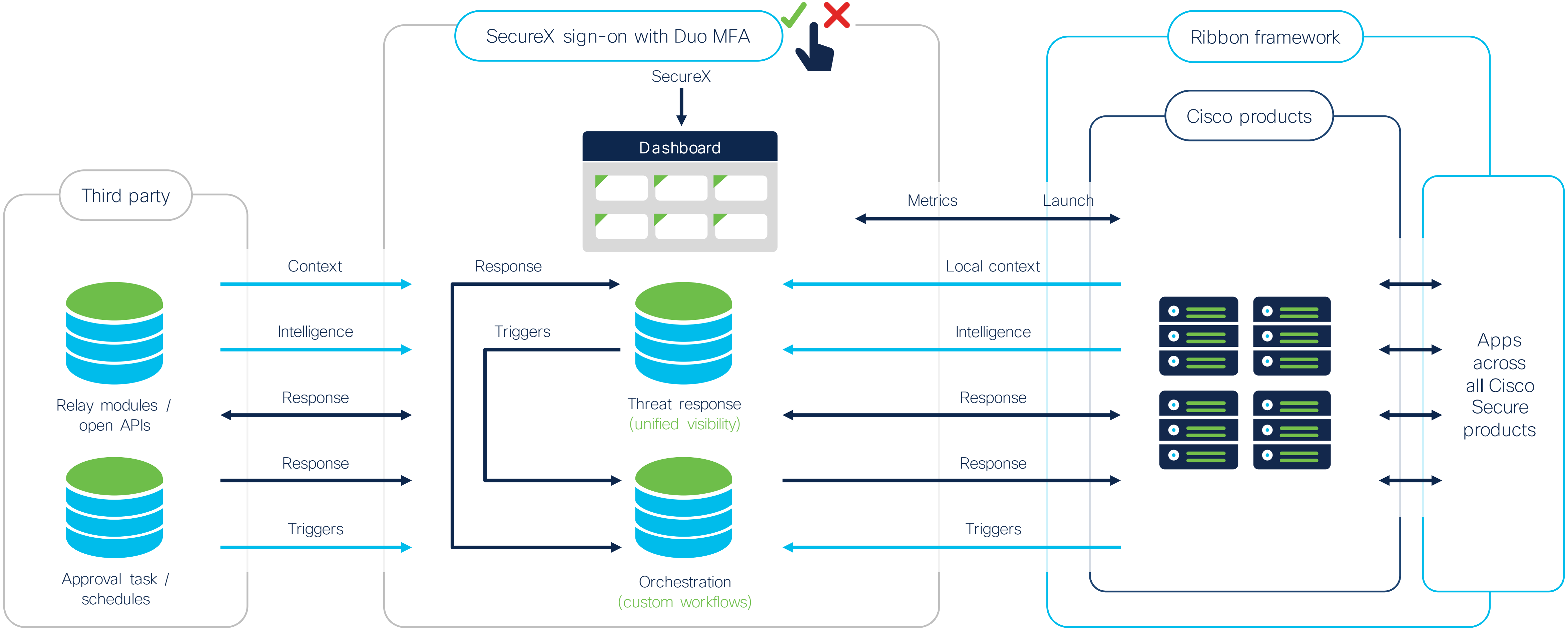
ribbon & sign-on
never leaves you
maintains context

dashboard
customizable for what
matters to you

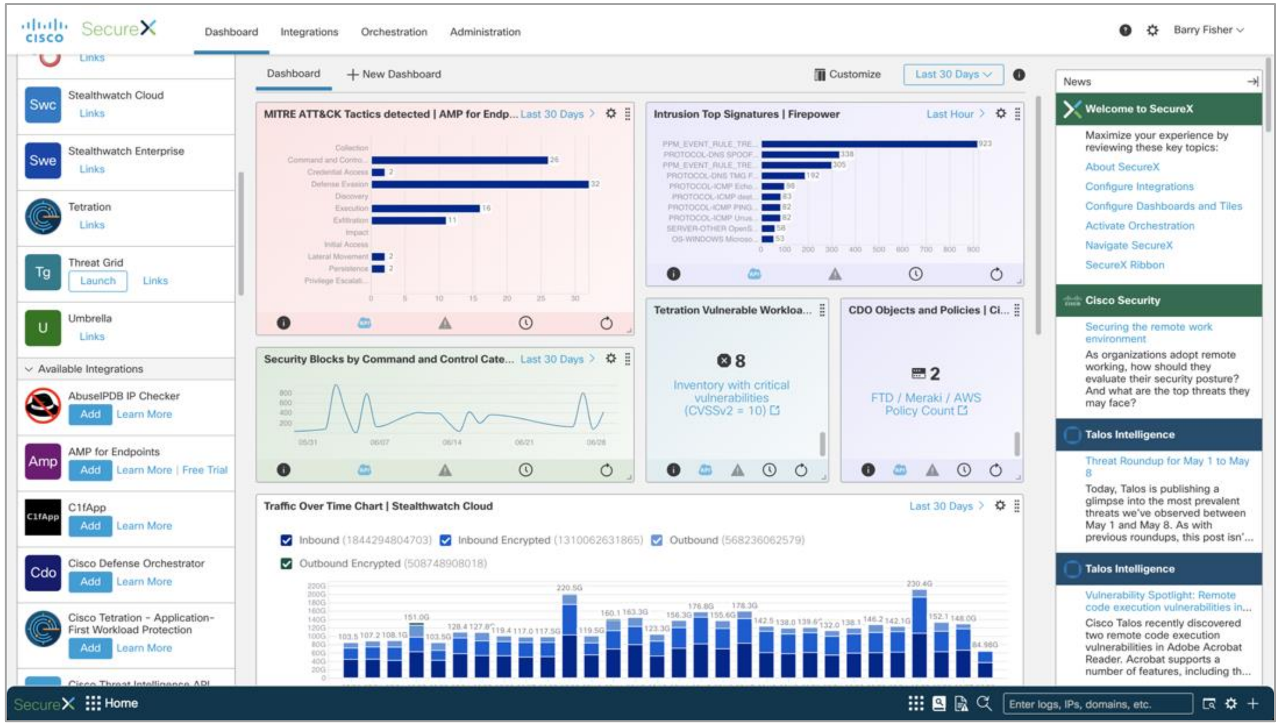
threat response
is at the core
of the platform

orchestration
drag-drop GUI
for no/low code

SecureX architecture



A new level of **visibility** with SecureX dashboard


SecureX
Dashboard
Integrations
Orchestration
Administration
Barry Fisher
Stealthwatch Cloud
Links
Stealthwatch Enterprise
Tetration
Threat Grid
Launch
Umbrella
Available Integrations
AbuseIPDB IP Checker
Add
Learn More
AMP for Endpoints
Free Trial
C1fApp
Cisco Defense Orchestrator
Cisco Tetration - Application-First Workload Protection
Cisco Threat Intelligence API
New Dashboard
Customize
Last 30 Days
MITRE ATT&CK Tactics detected | AMP for Endp...
Intrusion Top Signatures | Firepower
Last Hour
Security Blocks by Command and Control Cate...
Tetration Vulnerable Workloa...
8
Inventory with critical vulnerabilities (CVSSv2 = 10)
CDO Objects and Policies | Ci...
2
FTD / Meraki / AWS Policy Count
Traffic Over Time Chart | Stealthwatch Cloud
Inbound
Inbound Encrypted
Outbound
Outbound Encrypted
Home
Enter logs, IPs, domains, etc.
News

Welcome to SecureX

Maximize your experience by reviewing these key topics:

About SecureX

Configure Integrations

Configure Dashboards and Tiles

Activate Orchestration

Navigate SecureX

SecureX Ribbon

Cisco Security

Securing the remote work environment

As organizations adopt remote working, how should they evaluate their security posture? And what are the top threats they may face?

Talos Intelligence

Threat Roundup for May 1 to May 8

Today, Talos is publishing a glimpse into the most prevalent threats we've observed between May 1 and May 8. As with previous roundups, this post isn'...

Talos Intelligence

Vulnerability Spotlight: Remote code execution vulnerabilities in...

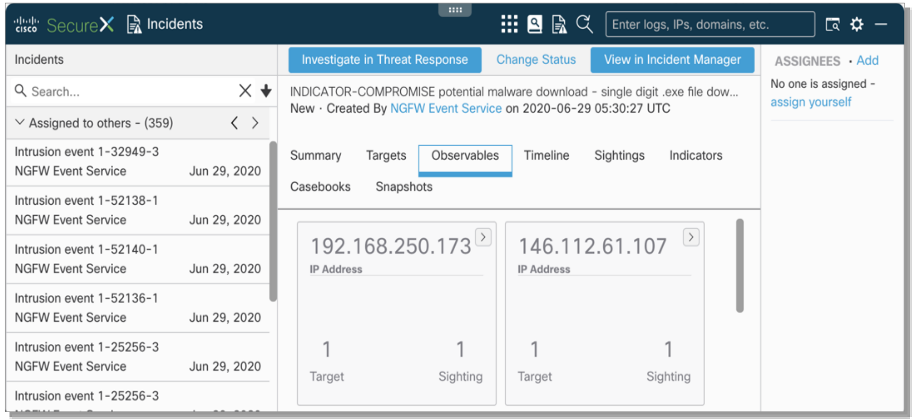
Cisco Talos recently discovered two remote code execution vulnerabilities in Adobe Acrobat Reader. Acrobat supports a number of features, including th...

- **Applications (left)**
  View, launch or trial the integrated products
- **Tiles (middle)**
  Presents metrics and operational measures from the integrated products
- **News (right)**
  Product updates, industry news, and blog posts

Understand what matters in one view across your security infrastructure

SecureX ribbon

- **SecureX ribbon** allows you to carry the most relevant security context and threat intelligence with you across all products
- **Transport framework** for functionality: Take the capabilities of SecureX and your integrated products with you when you go to any other product console. Have all your best tools handy
- **Ties products together** and provides unified experience and broad response capabilities across all the products
- **Cross-launch capability:** Pivot into any other products from the ribbon
- **Ribbon apps:** Brokered by SecureX, provided by SecureX and other products



Intrusion event 1-32949-3
NGFW Event Service Jun 29, 2020

Intrusion event 1-52138-1
NGFW Event Service Jun 29, 2020

Intrusion event 1-52140-1
NGFW Event Service Jun 29, 2020

Intrusion event 1-52136-1
NGFW Event Service Jun 29, 2020

Intrusion event 1-25256-3
NGFW Event Service Jun 29, 2020

Intrusion event 1-25256-3

INDICATOR-COMPROMISE potential malware download - single digit .exe file dow...
New · Created By NGFW Event Service on 2020-06-29 05:30:27 UTC

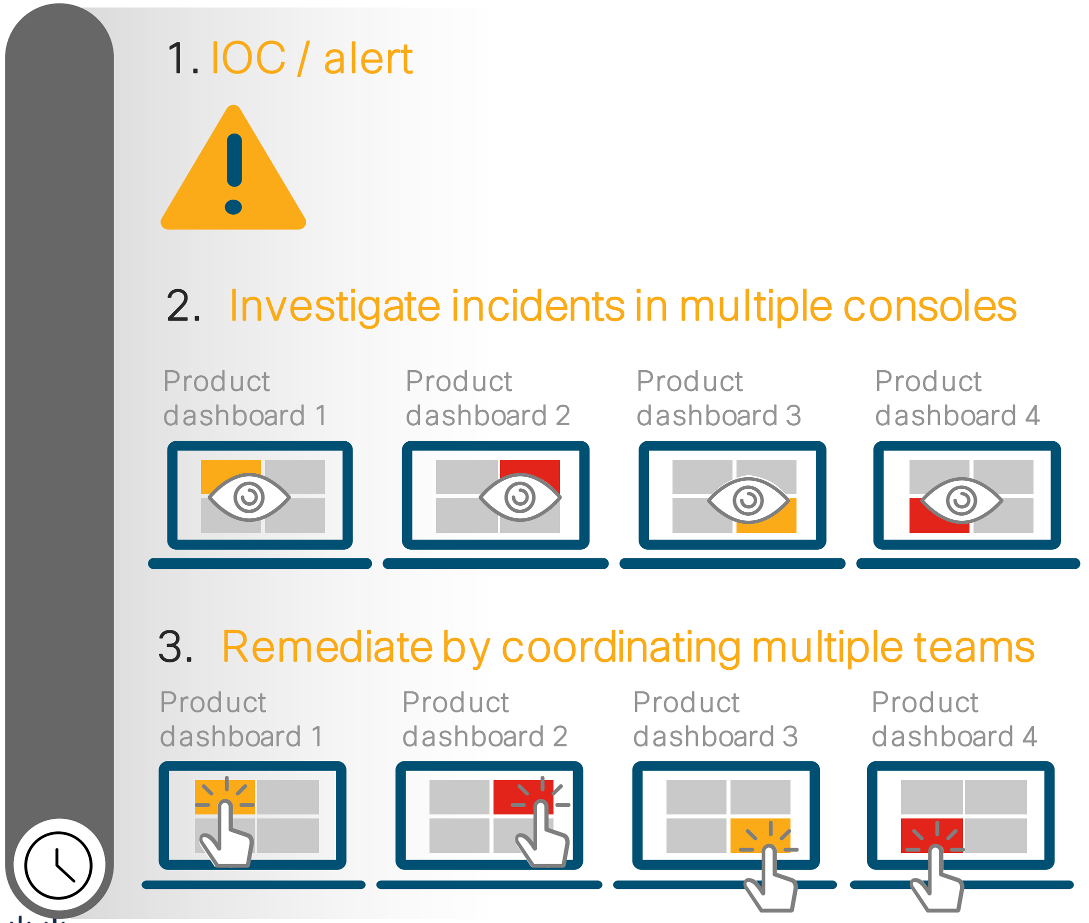
No one is assigned - assign yourself

192.168.250.173
IP Address
1 Target 1 Sighting

146.112.61.107
IP Address
1 Target 1 Sighting

How true simplicity is experienced

BEFORE: 32 minutes .....or months☺

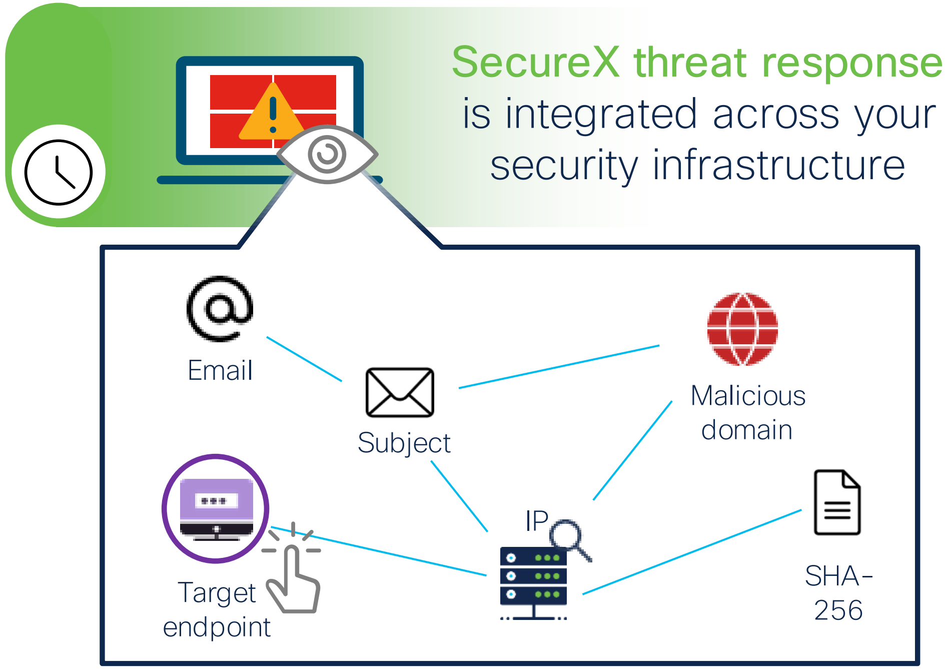


1. IOC / alert

2. Investigate incidents in multiple consoles

3. Remediate by coordinating multiple teams

AFTER: 5 minutes



SecureX threat response is integrated across your security infrastructure

In one view: Query intel and telemetry from multiple integrated products

Quickly visualize the threat impact in your environment

Remediate directly from one UI

Accelerate investigations in SecureX

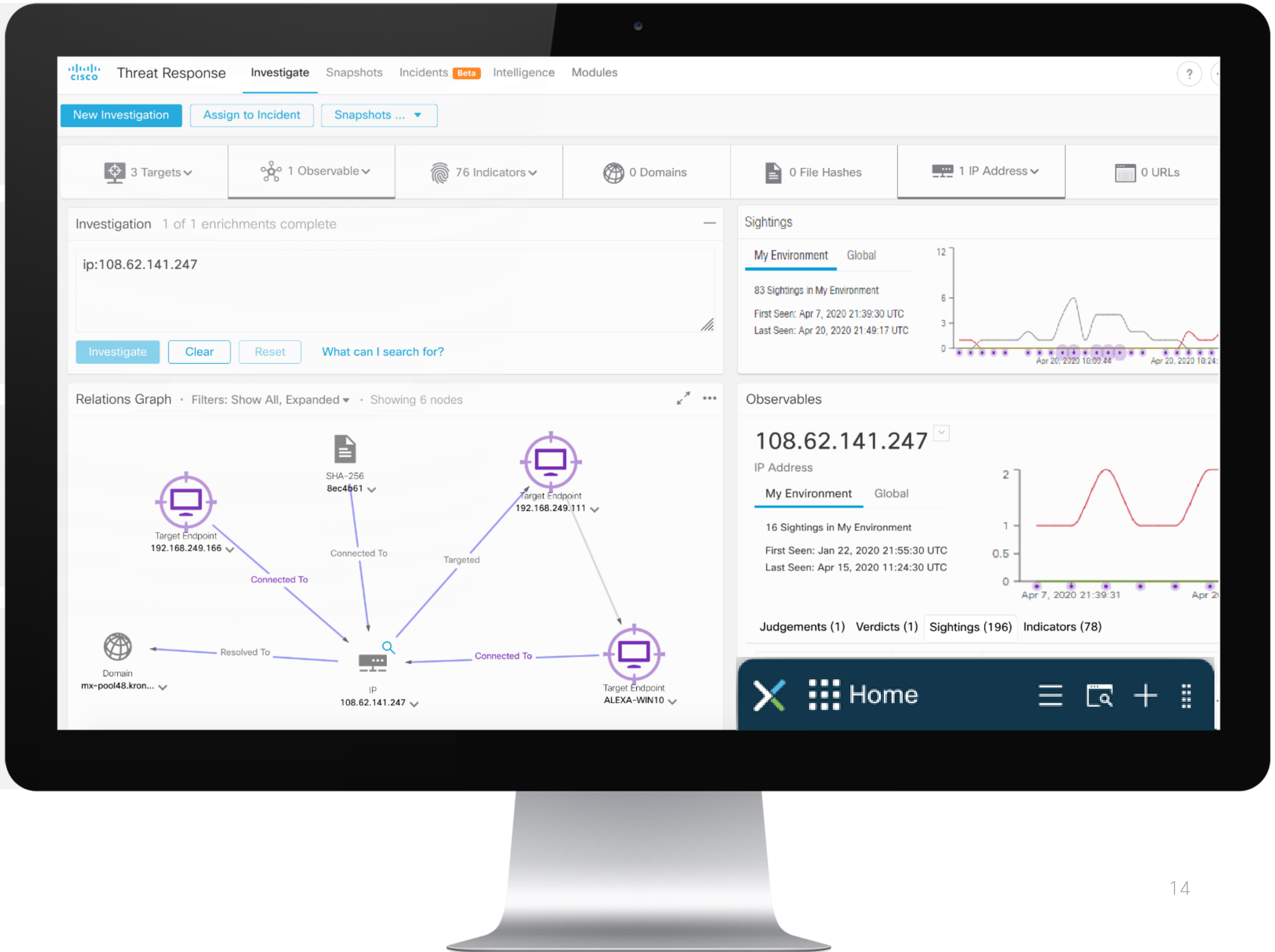
SecureX threat response

Aggregate and query global intel and local context in one view

Visualize the impact of threats across your environment

Take immediate action to isolate hosts and block destinations or files

Automate workflows with approval actions for better collaboration



Investigation 1 of 1 enrichments complete

ip:108.62.141.247

83 Sightings in My Environment

First Seen: Apr 7, 2020 21:39:30 UTC
Last Seen: Apr 20, 2020 21:49:17 UTC

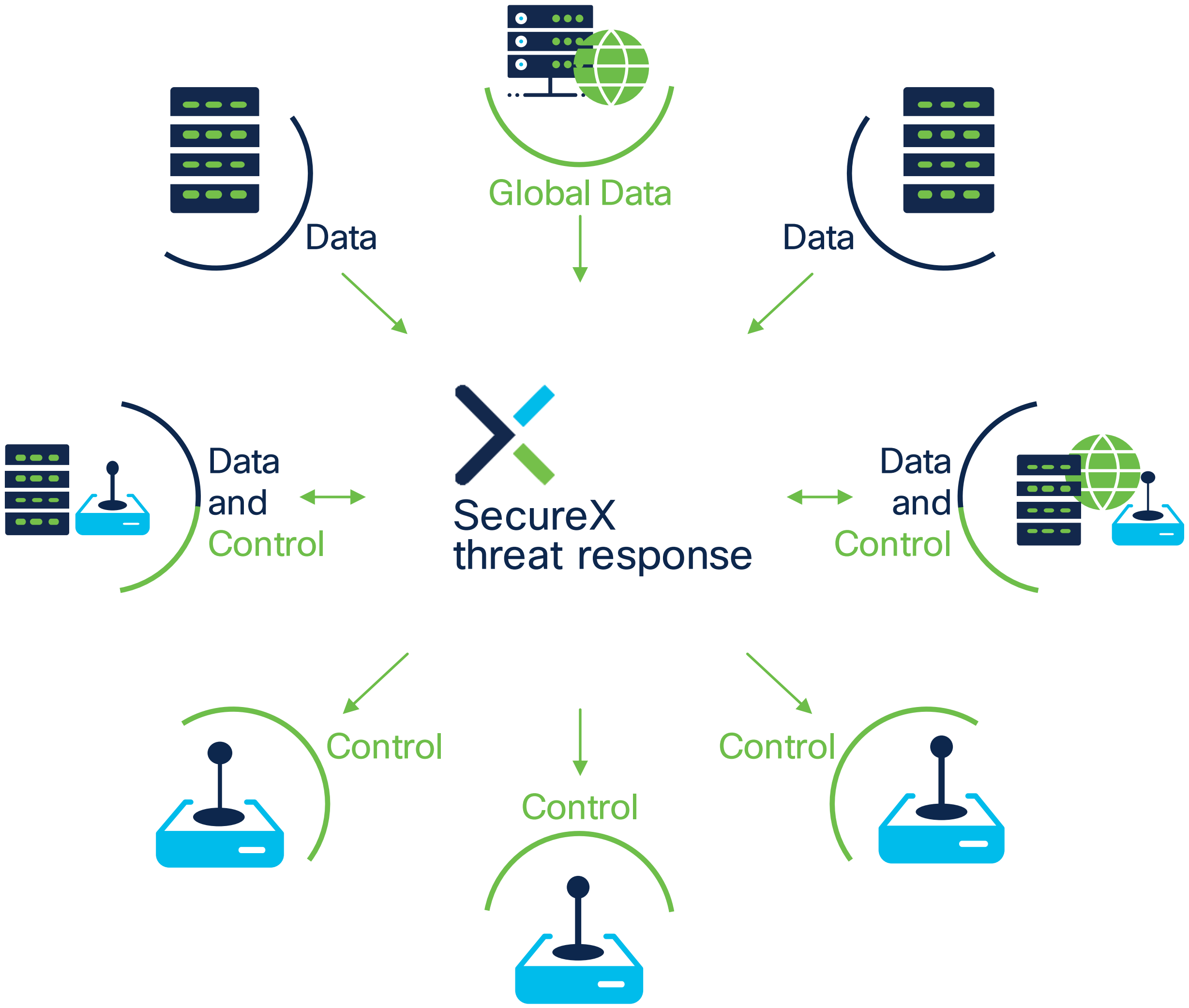
108.62.141.247
IP Address

16 Sightings in My Environment

First Seen: Jan 22, 2020 21:55:30 UTC
Last Seen: Apr 15, 2020 11:24:30 UTC

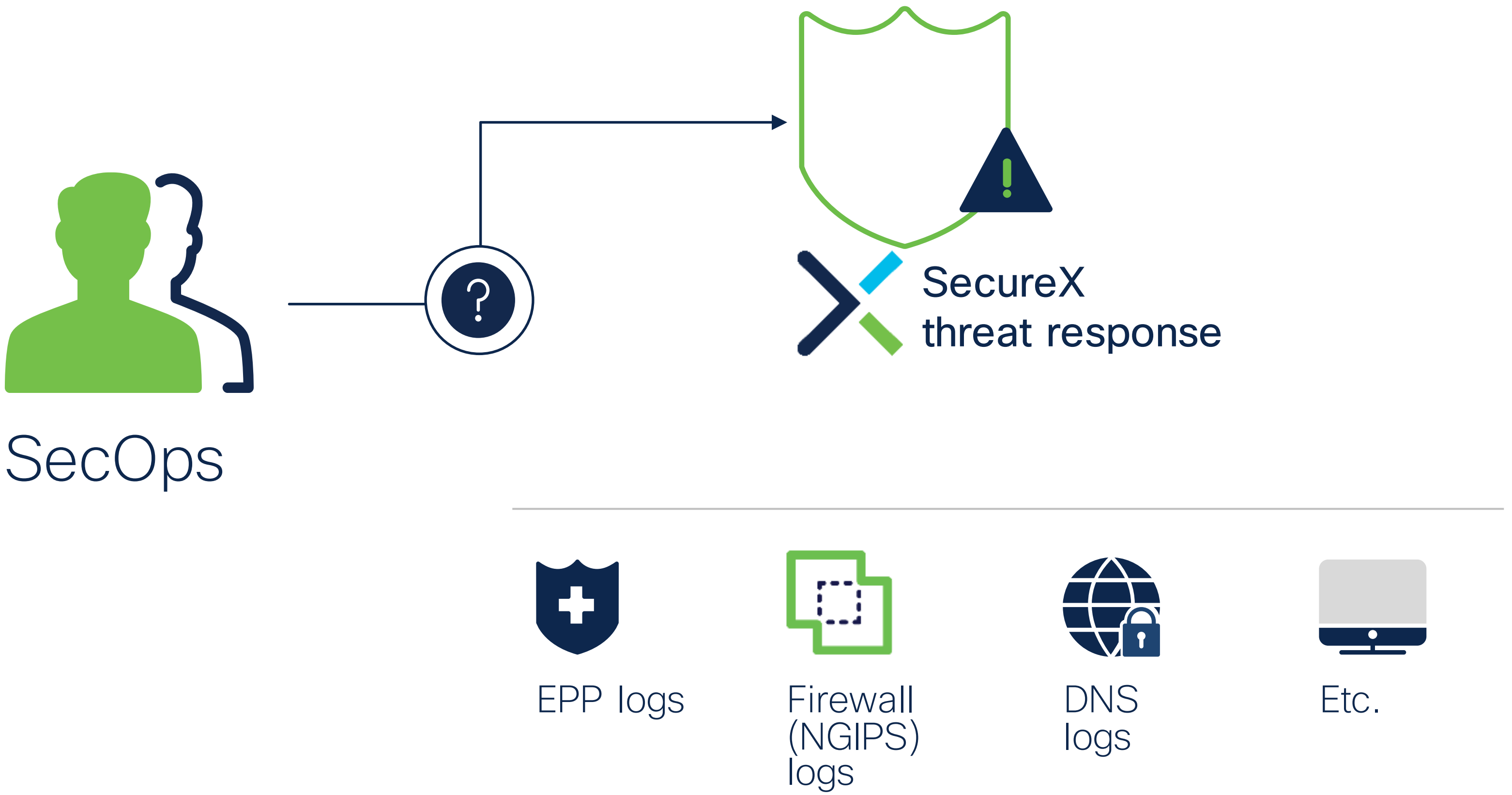
Judgements (1) Verdicts (1) Sightings (196) Indicators (78)

API aggregation at work



Enrichment

The process of consulting all the modules to find out what is known about the observable(s).



SecOps

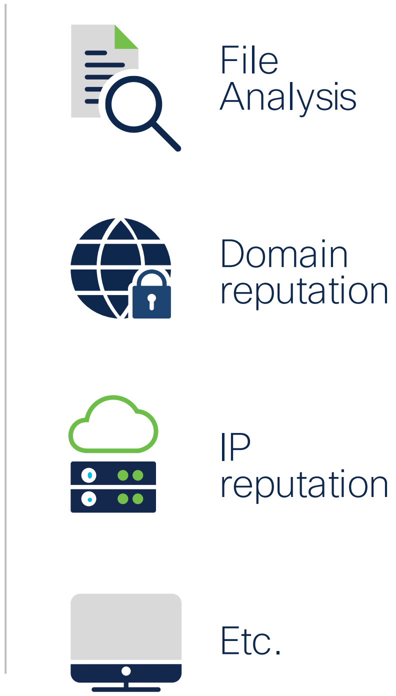
SecureX threat response

EPP logs

Firewall (NGIPS) logs

DNS logs

Etc.



File Analysis

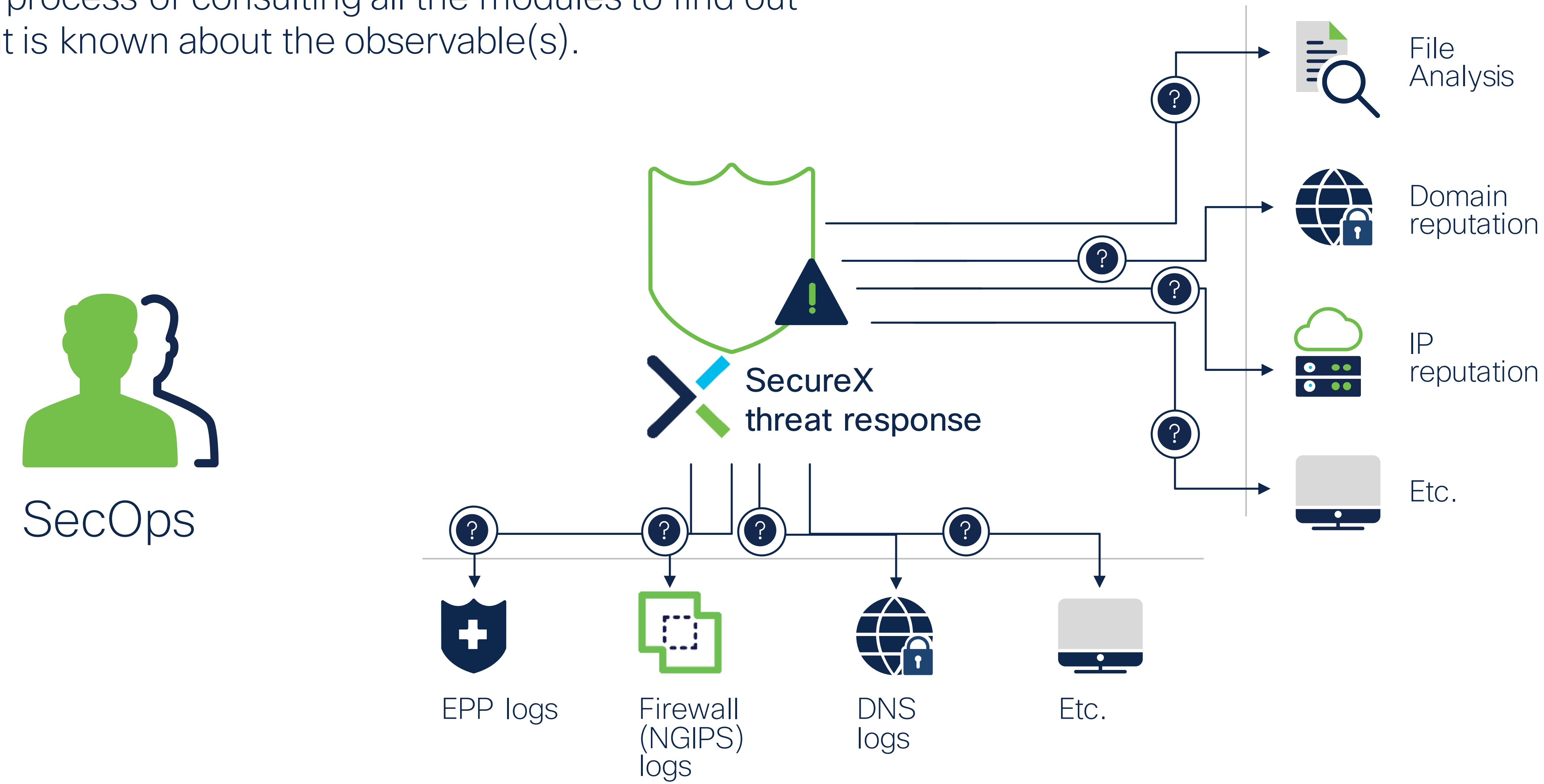
Domain reputation

IP reputation

Etc.

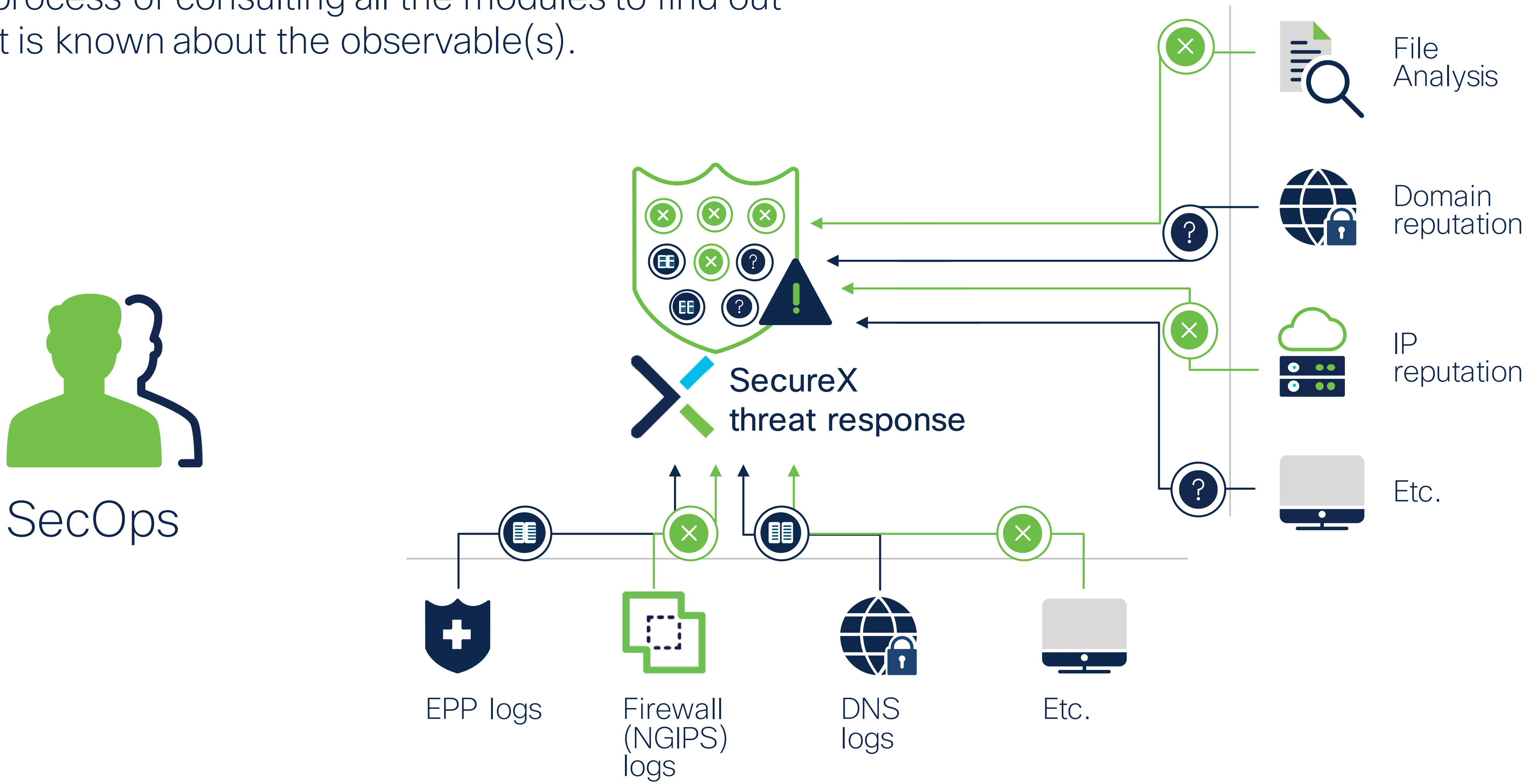
Enrichment

The process of consulting all the modules to find out what is known about the observable(s).

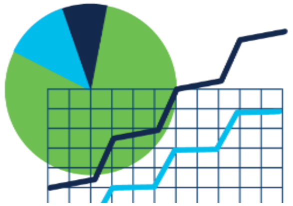


Enrichment

The process of consulting all the modules to find out what is known about the observable(s).



Record-keeping: Snapshots, Casebooks, and Incidents

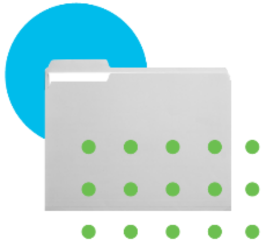


Snapshot

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

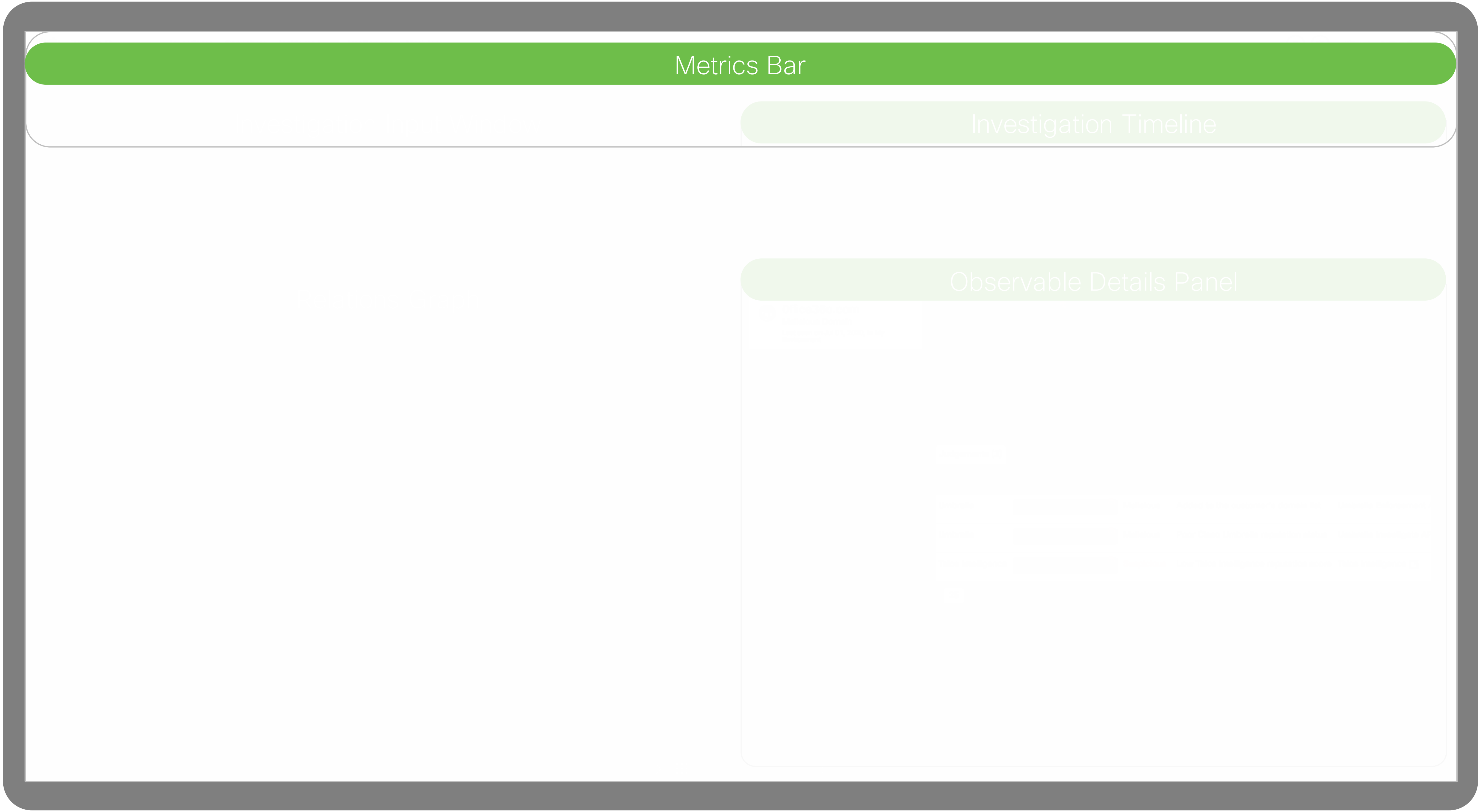
Incident

Security event

System created

System triaged

User-managed

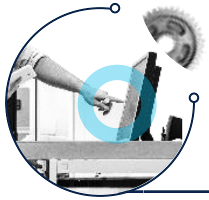


Metrics Bar

Investigation Timeline

Observable Details Panel

Automation vs orchestration



Automation

The ability to perform individual, repetitive tasks.

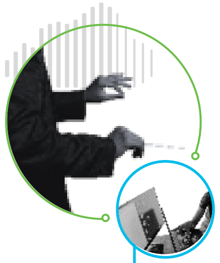
Why do customers want to automate?

“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.



Orchestration

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

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 solution?”

Introducing 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

SecureX orchestration

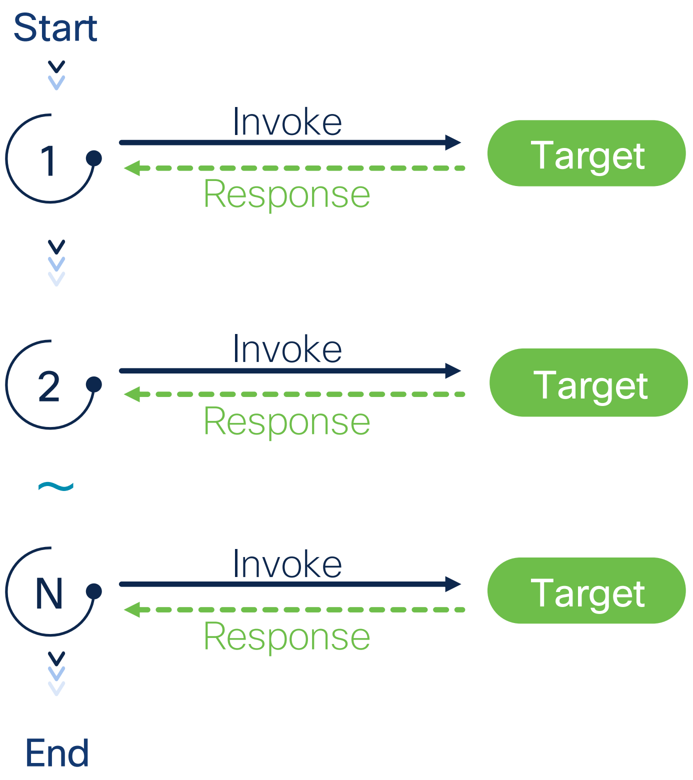
Cloud-Native, microservice architecture with “API-first” design

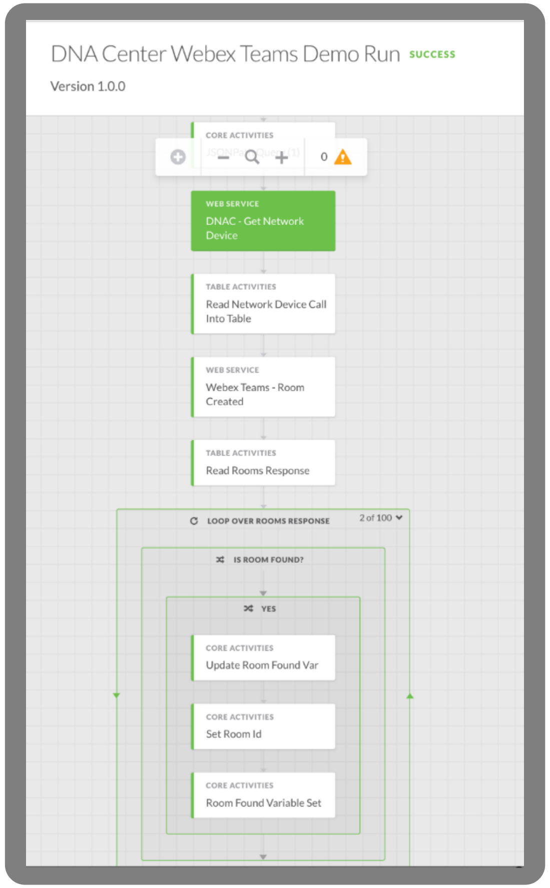
- Highly Performant, Scalable and Secure
- Reusable and Embeddable

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

Combine flexible out of the box adapters to **create new integrations**

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

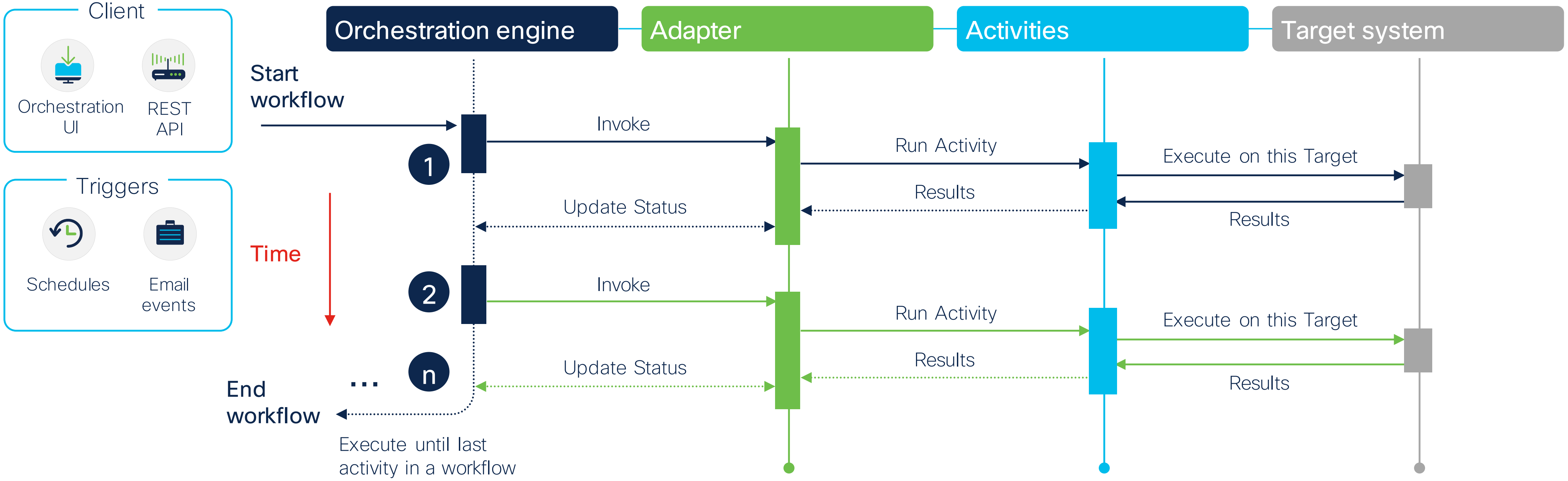



DNA Center Webex Teams Demo Run SUCCESS

Version 1.0.0

SecureX orchestration workflow sequence

The orchestration engine invokes **adapters** to execute **activities** on the **target systems**, which returns results and **status**, then the next step in the workflow begins.



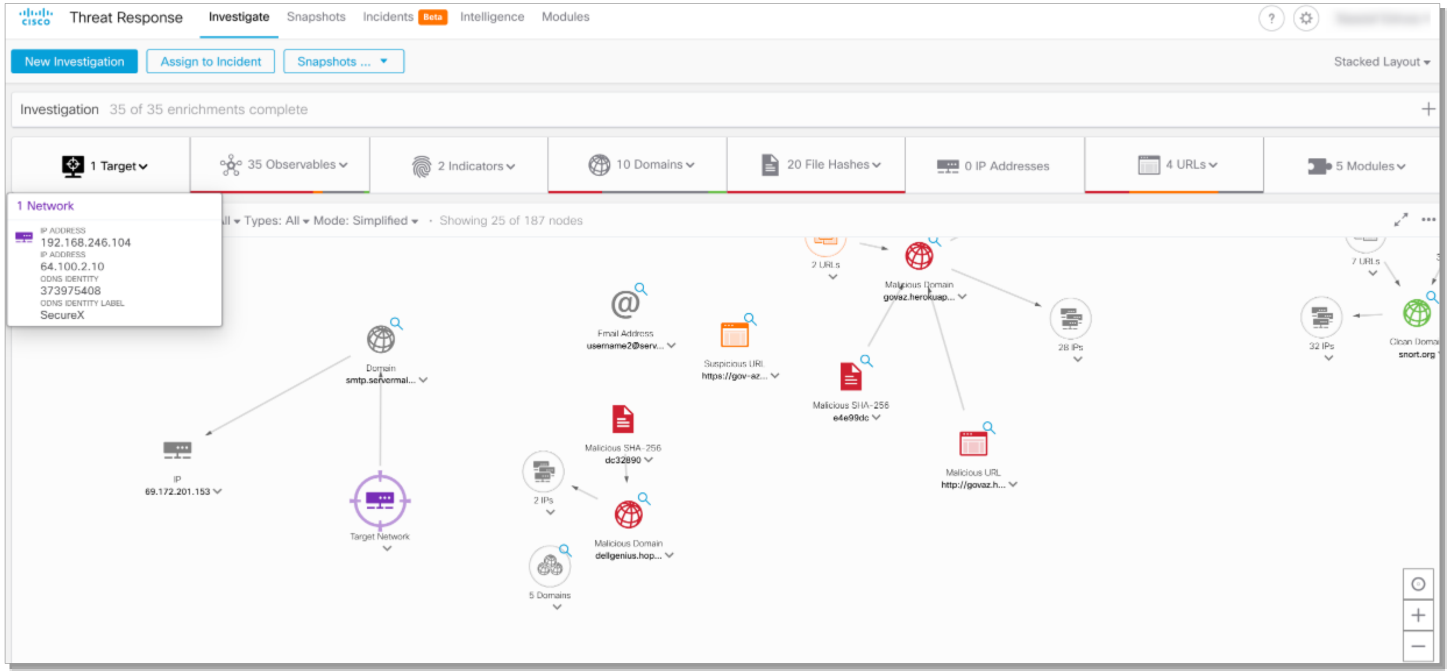
Adapter: Integration with a target system, provides activities to perform task automation

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

Target System: The host/endpoint that executes an activity

Threat hunting before SecureX

Customers receive an email notification of blog updates. Using the threat response browser extension, SOC personnel are conducting investigations to extract observables associated with Talos intelligence blogs.



Investigation 35 of 35 enrichments complete

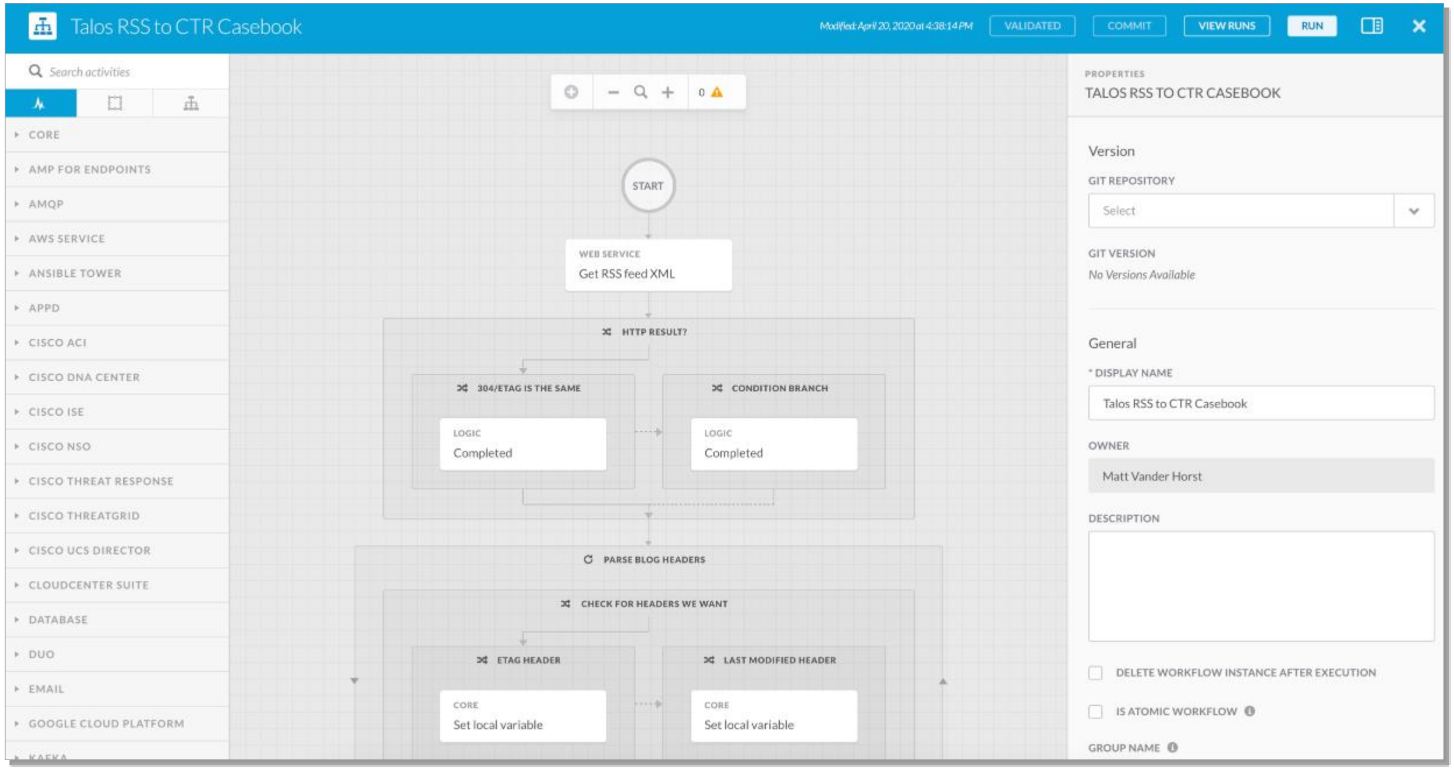
Showing 25 of 187 nodes

1 Network

IP ADDRESS
192.168.246.104
IP ADDRESS
64.100.2.10
ODNS IDENTITY
373975408
ODNS IDENTITY LABEL
SecureX

With SecureX

A playbook runs periodically to query the RSS feed for Talos intelligence blogs. Threat response casebooks are created with any observables. If a target is found based on a blog entry, the SOC is notified in a Webex Teams room.



Talos RSS to CTR Casebook

Modified: April 20, 2020 at 4:38:14 PM

PROPERTIES

TALOS RSS TO CTR CASEBOOK

Version

GIT REPOSITORY: Select

GIT VERSION: *No Versions Available*

General

* DISPLAY NAME: Talos RSS to CTR Casebook

OWNER: Matt Vander Horst

DESCRIPTION:

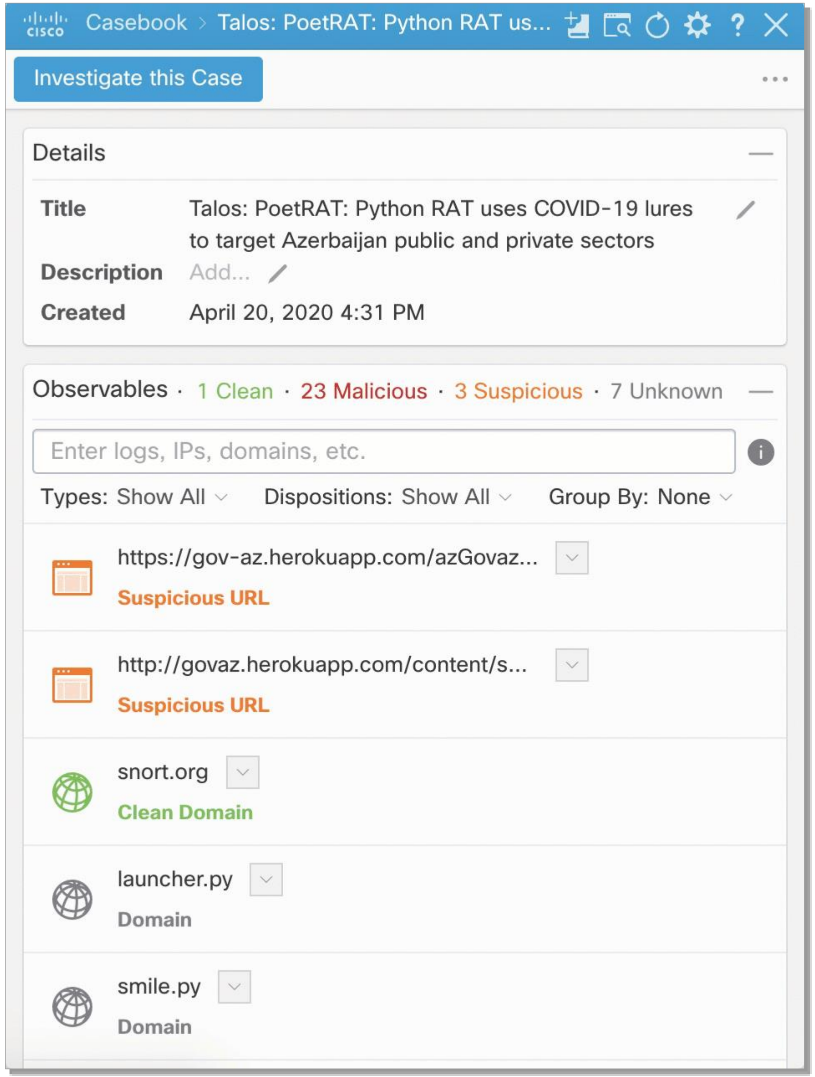
□ DELETE WORKFLOW INSTANCE AFTER EXECUTION

□ IS ATOMIC WORKFLOW

GROUP NAME

With SecureX

A playbook runs periodically to query the RSS feed for Talos intelligence blogs. Threat response casebooks are created with any observables. If a target is found based on a blog entry, the SOC is notified in a Webex Teams room.



Casebook › Talos: PoetRAT: Python RAT us...

Details

Title Talos: PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors

Description Add...

Created April 20, 2020 4:31 PM

Observables · 1 Clean · 23 Malicious · 3 Suspicious · 7 Unknown

Enter logs, IPs, domains, etc.

Types: Show All   Dispositions: Show All   Group By: None

https://gov-az.herokuapp.com/azGovaz...
Suspicious URL

http://govaz.herokuapp.com/content/s...
Suspicious URL

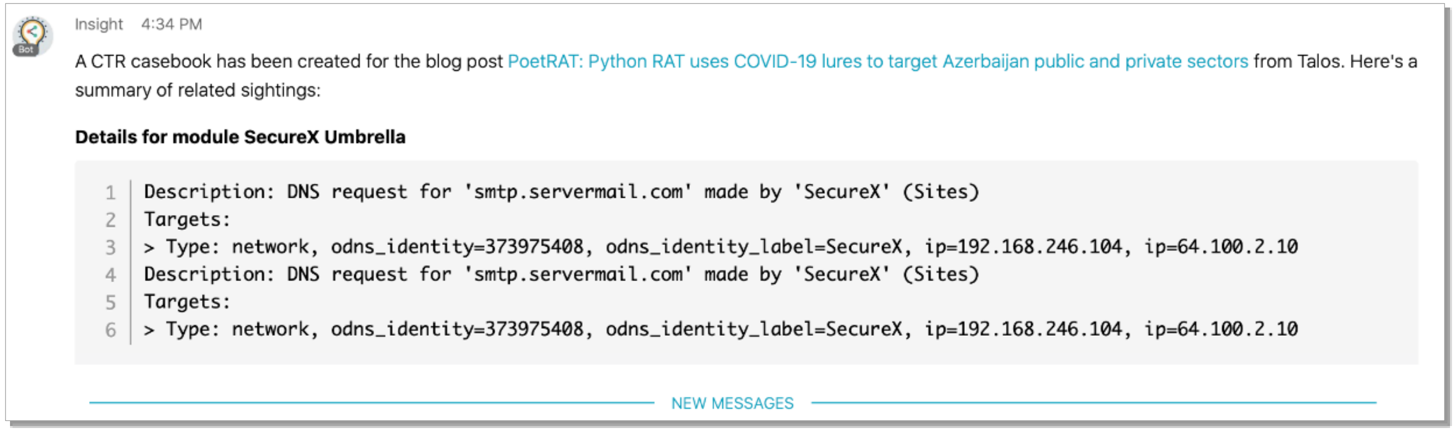
snort.org
Clean Domain

launcher.py
Domain

smile.py
Domain

With SecureX

A playbook runs periodically to query the RSS feed for Talos intelligence blogs. Threat response casebooks are created with any observables. If a target is found based on a blog entry, the SOC is notified in a Webex Teams room.



Insight 4:34 PM

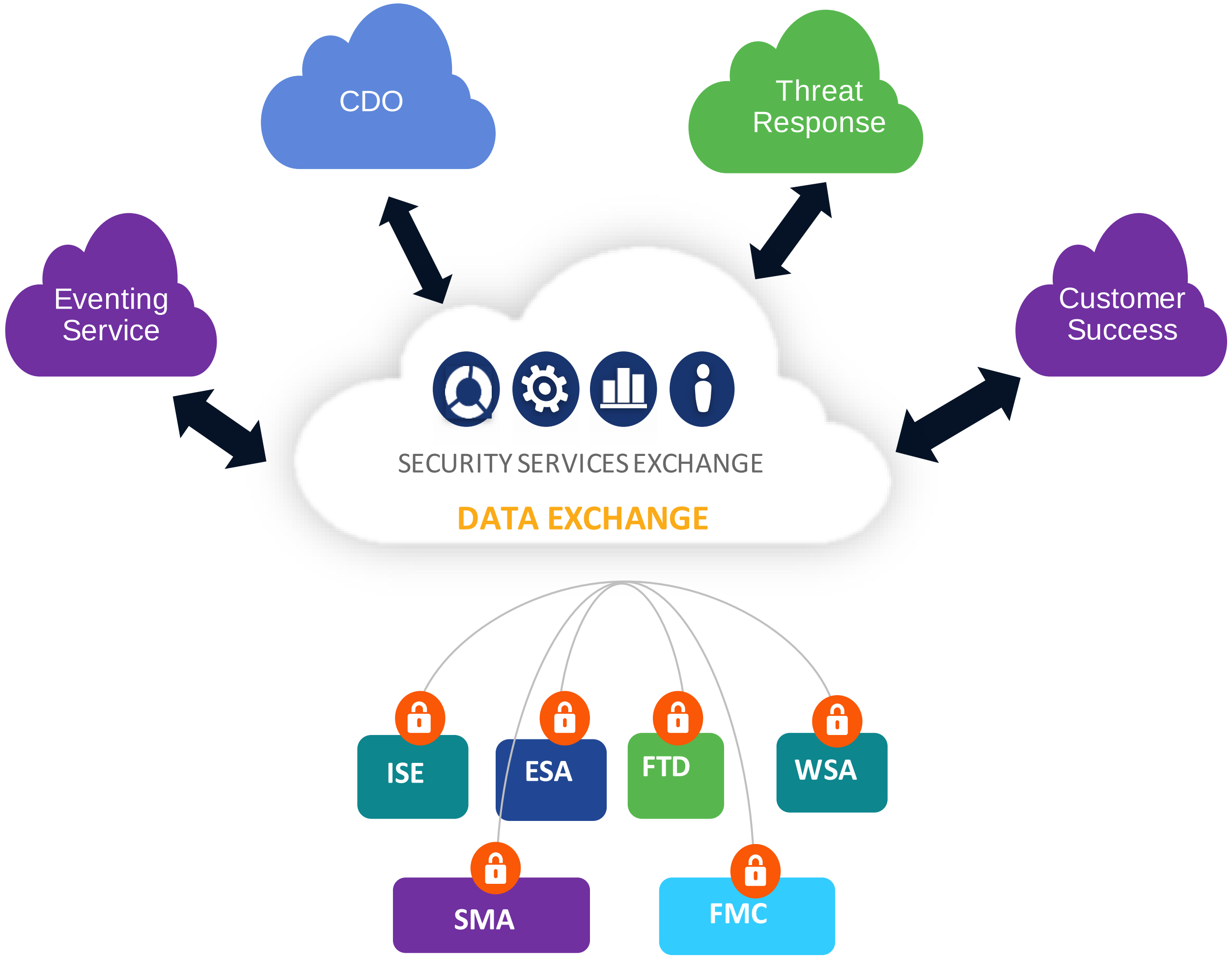
A CTR casebook has been created for the blog post PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors from Talos. Here's a summary of related sightings:

Details for module SecureX Umbrella

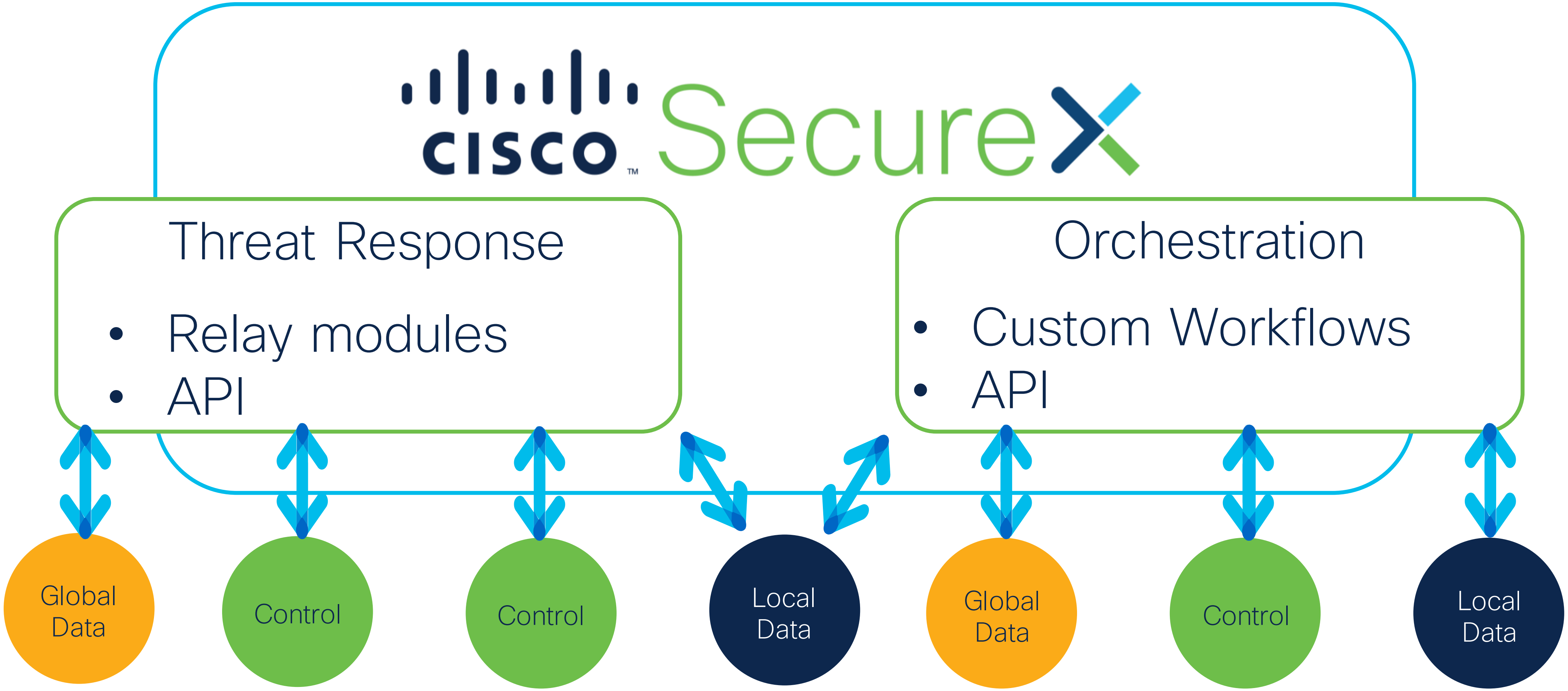
```
Description: DNS request for 'smtp.servermail.com' made by 'SecureX' (Sites)
Targets:
> Type: network, odns_identity=373975408, odns_identity_label=SecureX, ip=192.168.246.104, ip=64.100.2.10
Description: DNS request for 'smtp.servermail.com' made by 'SecureX' (Sites)
Targets:
> Type: network, odns_identity=373975408, odns_identity_label=SecureX, ip=192.168.246.104, ip=64.100.2.10
```

Why do I need SSE?

- Security Services Exchange is required to receive / enumerate events from on-premises infrastructure.
- These events can be consumed by SecureX, Threat Response, Security Analytics and Logging, etc.
- SSE is not needed for SecureX if only integrating Cloud systems (Umbrella, SWC, AMP, etc).



Hooks and Integration Points



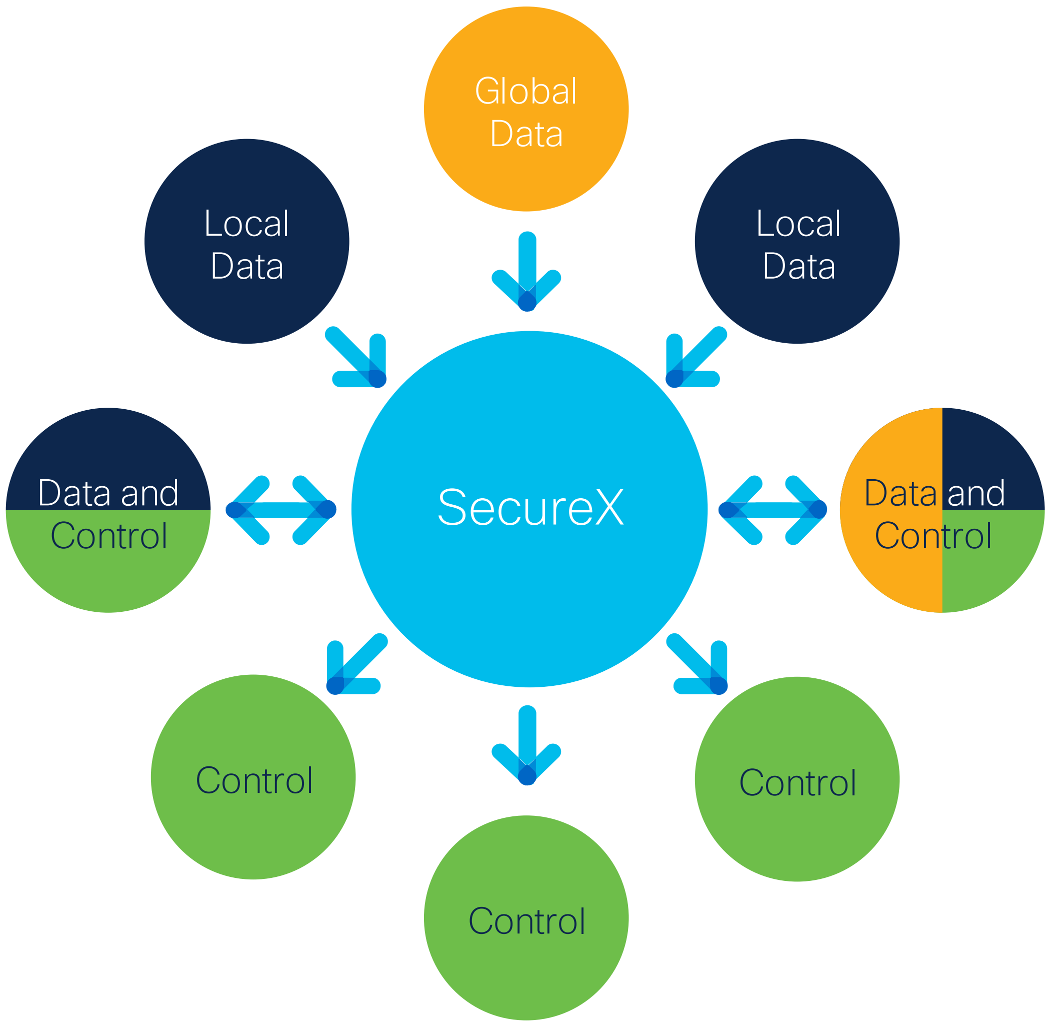
Threat Response

- Relay modules
- API

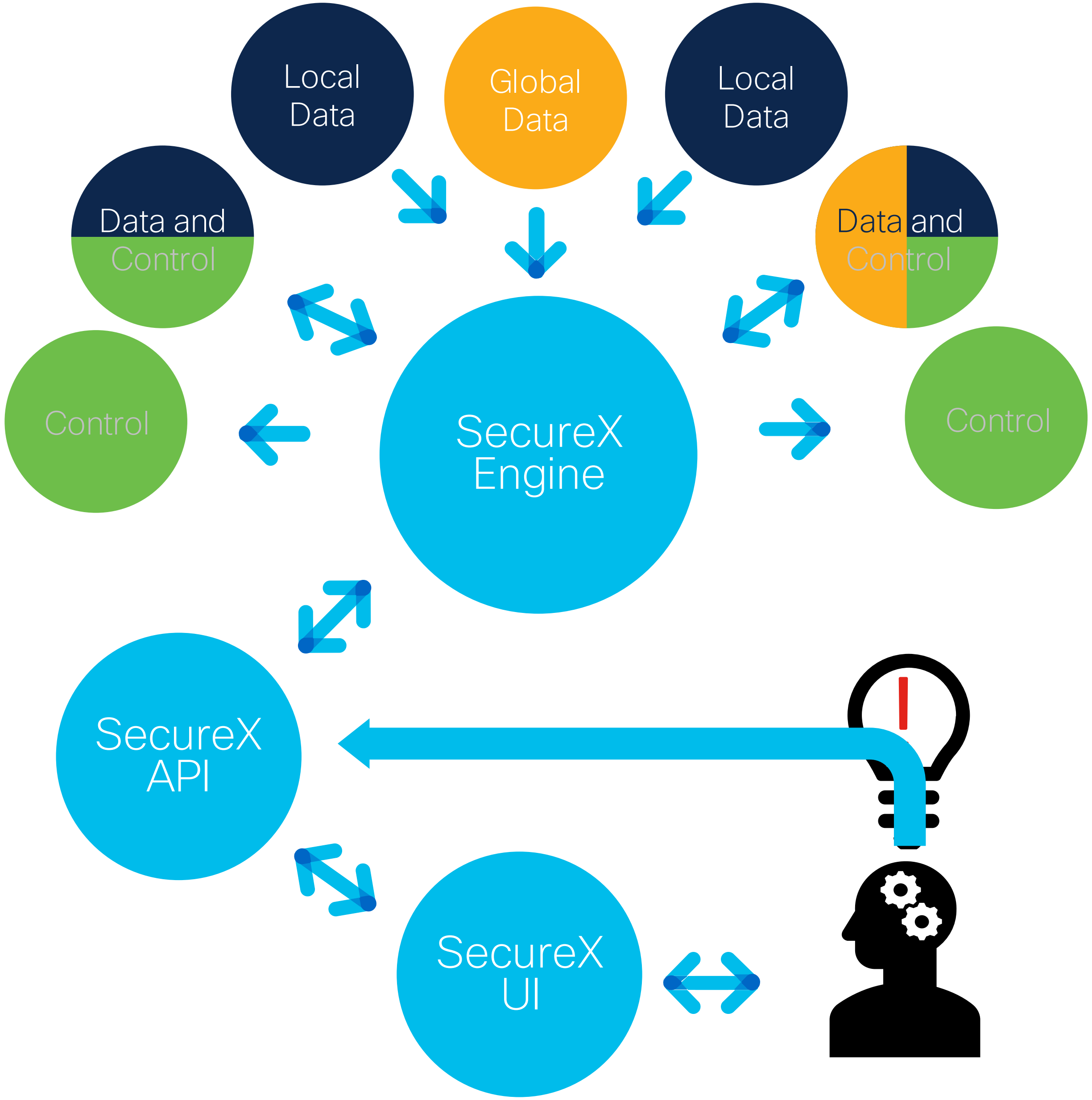
Orchestration

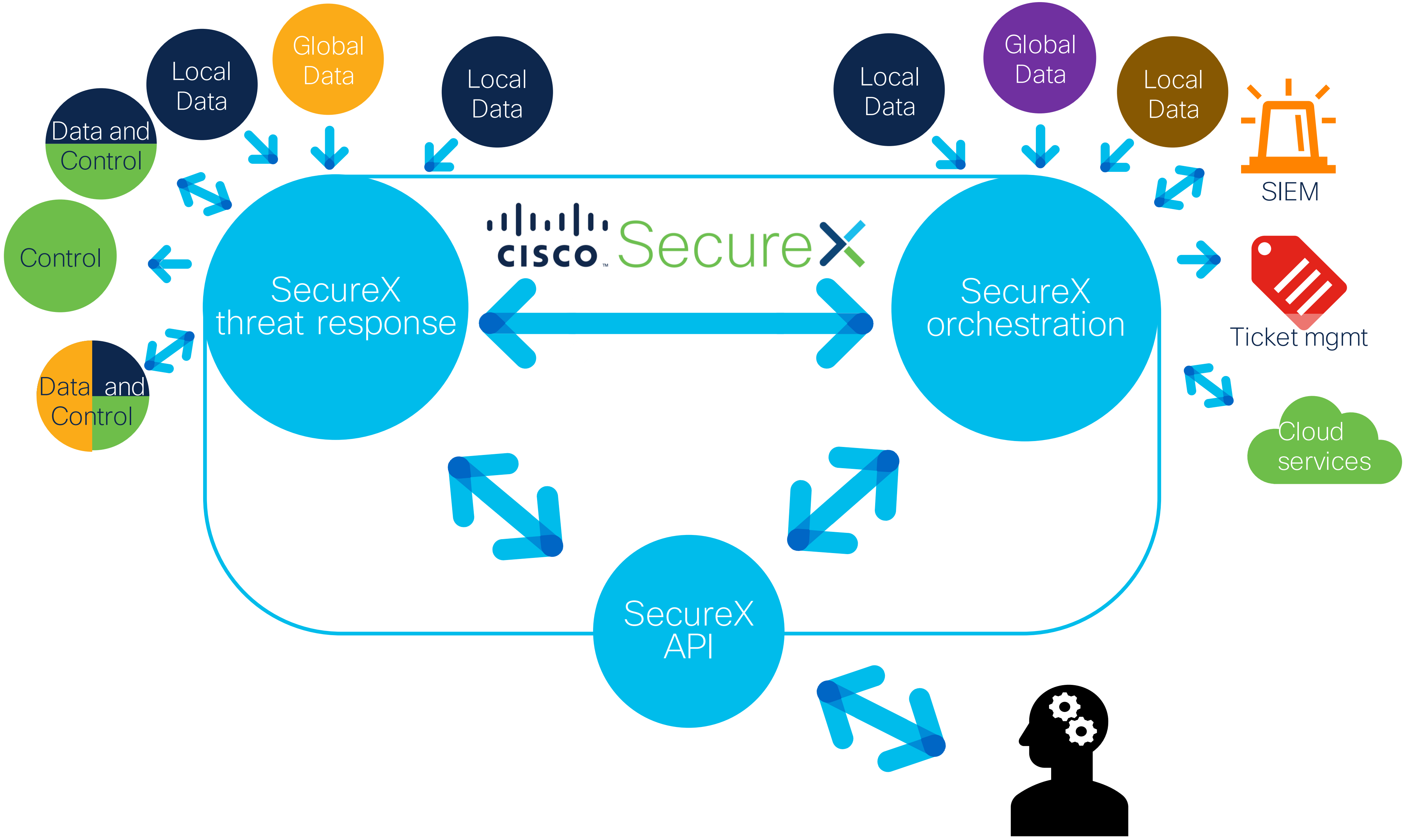
- Custom Workflows
- API

API aggregation at work



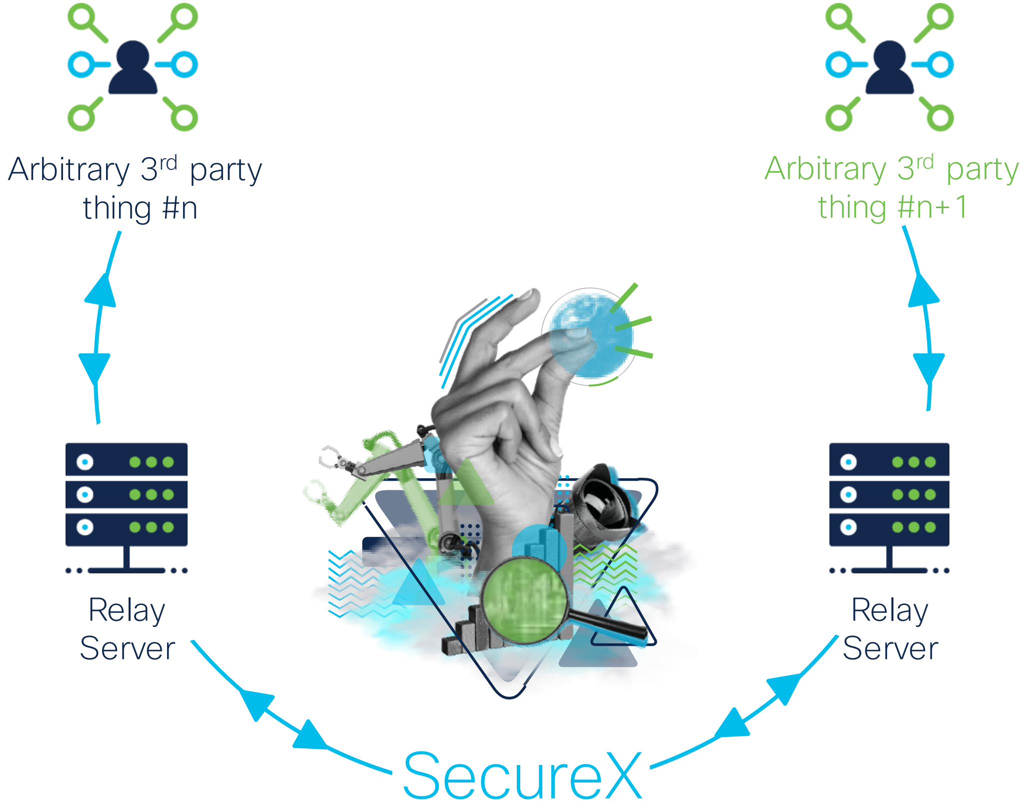
API relaying at work




Data and Control
Local Data
Global Data
Local Data
Control
Data and Control
cisco SecureX
SecureX threat response
SecureX orchestration
SecureX API
Local Data
Global Data
Local Data
SIEM
Ticket mgmt
Cloud services

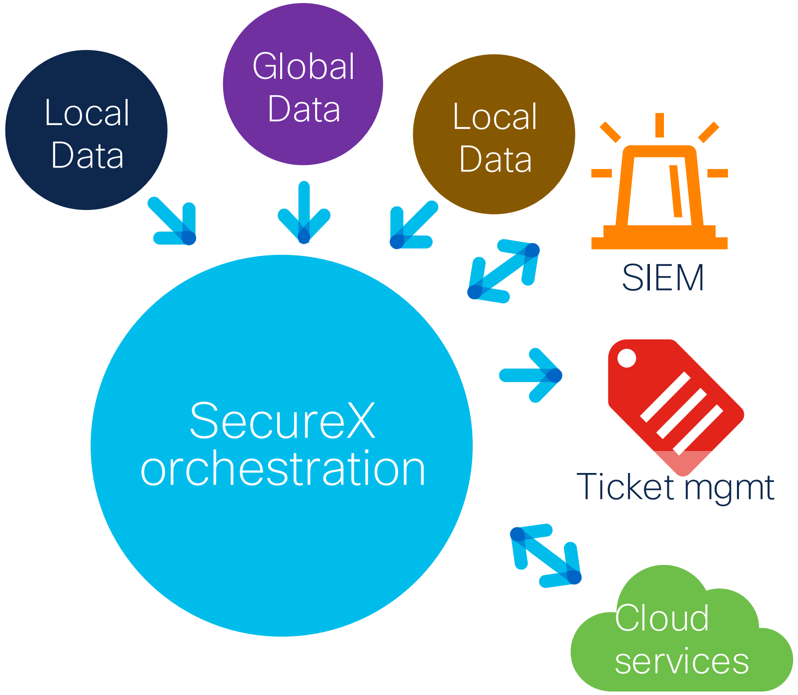
Relay modules

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



Adapters

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

I’m a Cisco Secure customer with SecureX threat response

My team can:

Answer questions faster about observables.

Block and unblock domains from threat response.

Block and unblock file executions from threat response

Isolate Hosts

Hunt for an observable associated with a known actor and immediately see organizational impact.

Save a point in time **snapshot** of our investigations for further analysis.

Document our analysis in a cloud casebook from all integrated or web-accessible tools, via an API.

Integrate threat response easily into existing processes and custom tools

Store our own threat intel in threat response private intel for use in investigations

See Incidents all in one place

Proven platform with 11,000+ customers unlocking new value today with SecureX threat response

98%
found the unified view enables rapid threat response

95%
say that our security platform helps them take action and remediate

91%
find that our security platform helps their teams collaborate more

> ***"I am able to visualize threats within my environment and take action in half the time it used to take me."***
>
> *–Security Engineer,*
> *Large Enterprise Banking Company*

In Summary…

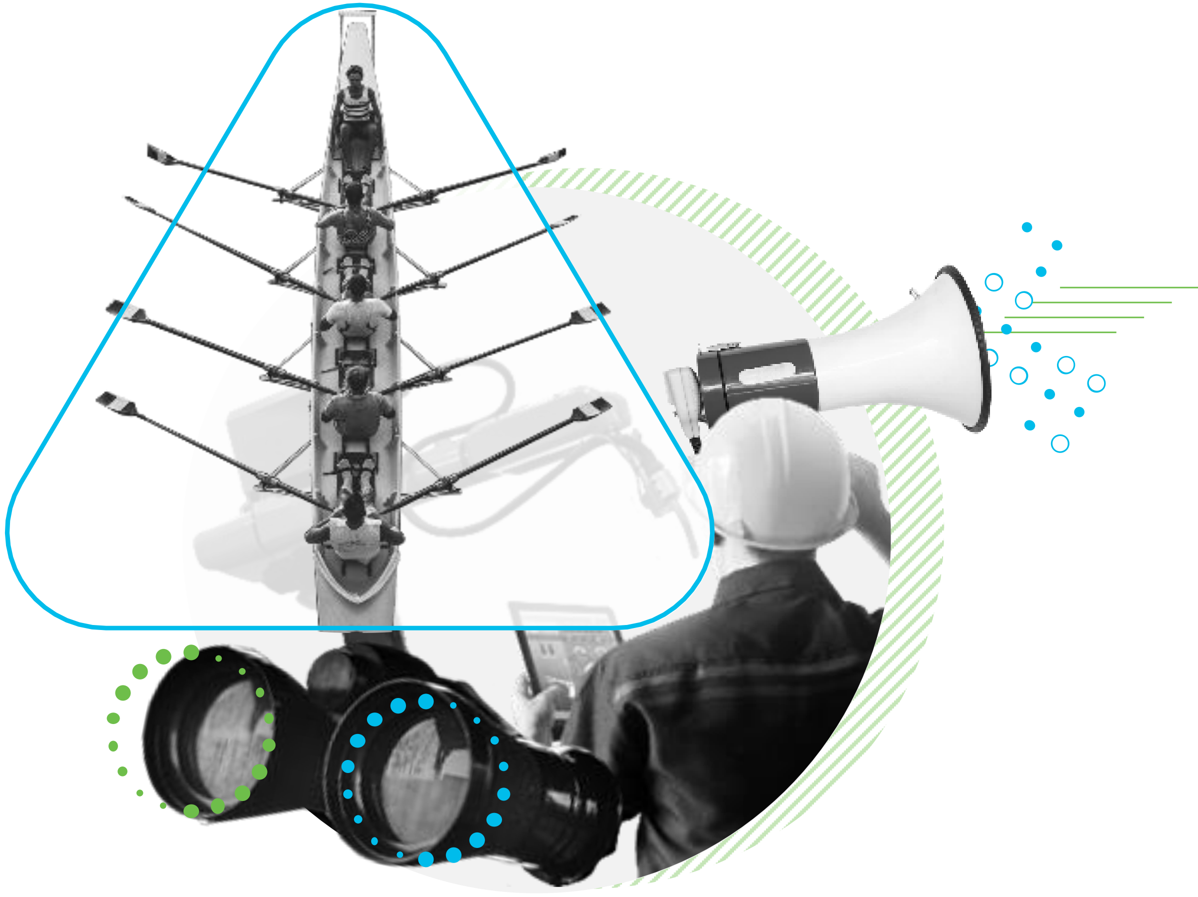
Unlock new value from your current investments

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**



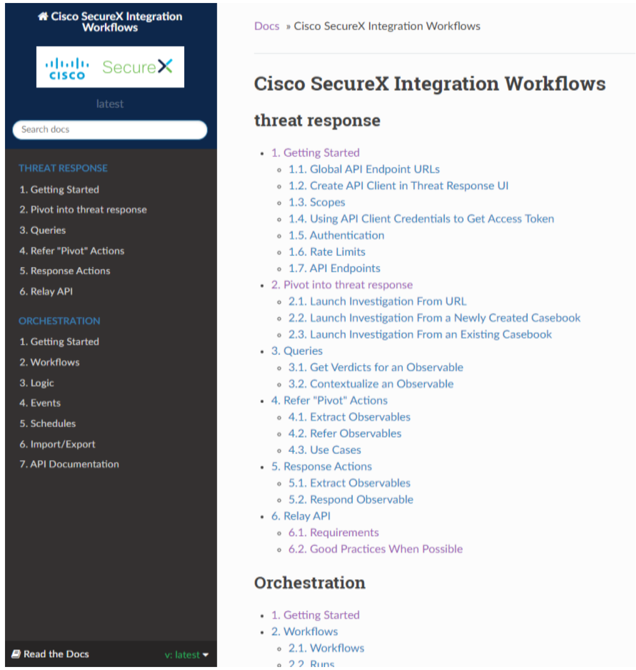
DEMO Time

THANK YOU

Resources

Integration documentation

cs.co/SecureX_integration_workflows



Cisco SecureX Integration Workflows

latest

Search docs

THREAT RESPONSE

1. Getting Started
2. Pivot into threat response
3. Queries
4. Refer "Pivot" Actions
5. Response Actions
6. Relay API

ORCHESTRATION

1. Getting Started
2. Workflows
3. Logic
4. Events
5. Schedules
6. Import/Export
7. API Documentation

Read the Docs v: latest

Docs » Cisco SecureX Integration Workflows

Cisco SecureX Integration Workflows

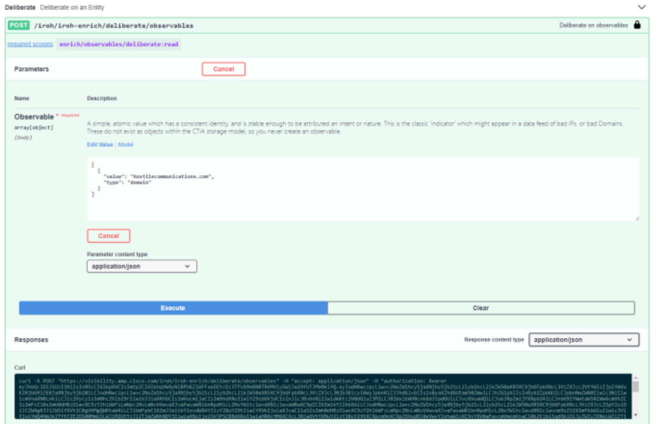
threat response

- 1. Getting Started
  - 1.1. Global API Endpoint URLs
  - 1.2. Create API Client in Threat Response UI
  - 1.3. Scopes
  - 1.4. Using API Client Credentials to Get Access Token
  - 1.5. Authentication
  - 1.6. Rate Limits
  - 1.7. API Endpoints
- 2. Pivot into threat response
  - 2.1. Launch Investigation From URL
  - 2.2. Launch Investigation From a Newly Created Casebook
  - 2.3. Launch Investigation From an Existing Casebook
- 3. Queries
  - 3.1. Get Verdicts for an Observable
  - 3.2. Contextualize an Observable
- 4. Refer "Pivot" Actions
  - 4.1. Extract Observables
  - 4.2. Refer Observables
  - 4.3. Use Cases
- 5. Response Actions
  - 5.1. Extract Observables
  - 5.2. Respond Observable
- 6. Relay API
  - 6.1. Requirements
  - 6.2. Good Practices When Possible

Orchestration

- 1. Getting Started
- 2. Workflows
  - 2.1. Workflows
  - 2.2. Runs

UI docs and proto tools



Deliberate Deliberate on an Entity

POST /iroh/iroh-enrich/deliberate/observables — Deliberate on observables

required scopes: enrich/observables/deliberate:read

Parameters

Name: Observable * required — array[object] (body)

Description: A simple, atomic value which has a consistent identity, and is stable enough to be attributed an intent or nature. This is the classic 'indicator' which might appear in a data feed of bad IPs, or bad Domains. These do not exist as objects within the CTIA storage model, so you never create an observable.

```
[
  {
    "value": "hostilecommunications.com",
    "type": "domain"
  }
]
```

Parameter content type: application/json

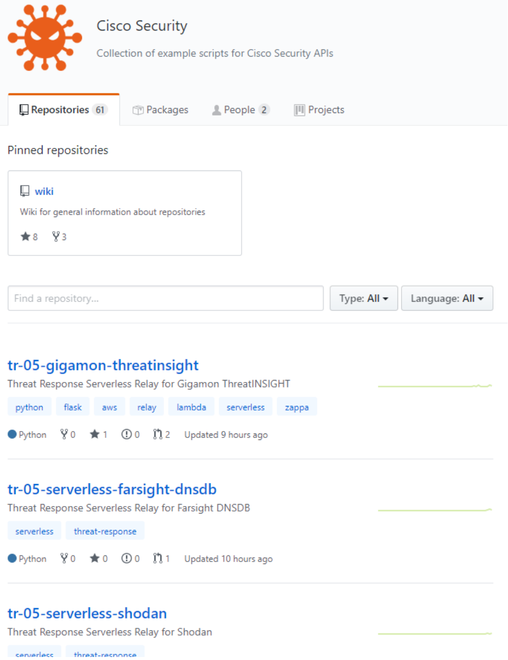
Responses — Response content type: application/json

Curl

```
curl -X POST "https://visibility.amp.cisco.com/iroh/iroh-enrich/deliberate/observables" -H "accept: application/json" -H "authorization: Bearer
[illegible]
```

Github

github.com/CiscoSecurity



Cisco Security

Collection of example scripts for Cisco Security APIs

Pinned repositories

wiki — Wiki for general information about repositories — ★ 8, forks 3

tr-05-gigamon-threatinsight
Threat Response Serverless Relay for Gigamon ThreatINSIGHT
python flask aws relay lambda serverless zappa
Python, forks 0, ★ 1, issues 0, pull requests 2, Updated 9 hours ago

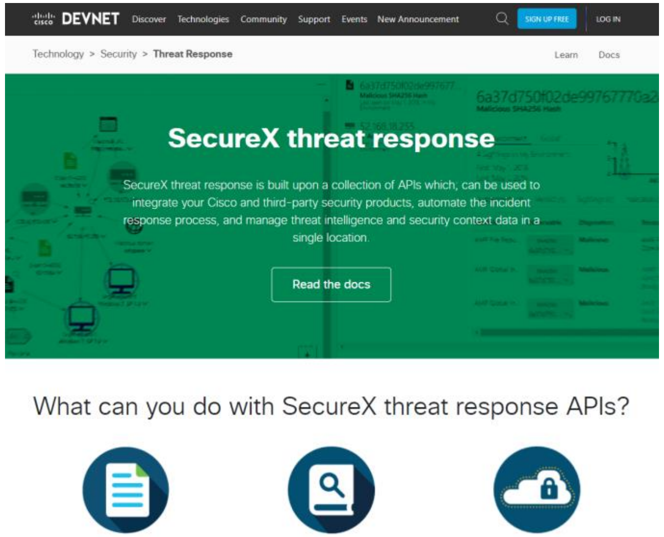
tr-05-serverless-farsight-dnsdb
Threat Response Serverless Relay for Farsight DNSDB
serverless threat-response
Python, forks 0, ★ 0, issues 0, pull requests 1, Updated 10 hours ago

tr-05-serverless-shodan
Threat Response Serverless Relay for Shodan
serverless threat-response

SecureX threat response Resources

Devnet

developer.cisco.com/threat-response/



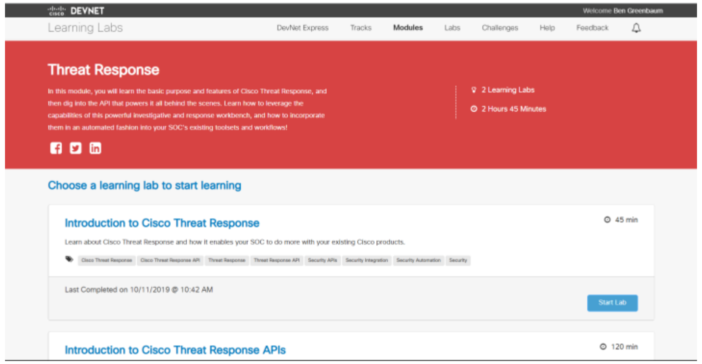
SecureX threat response

SecureX threat response is built upon a collection of APIs which; can be used to integrate your Cisco and third-party security products, automate the incident response process, and manage threat intelligence and security context data in a single location.

What can you do with SecureX threat response APIs?

Devnet Learning Labs

learninglabs.cisco.com/labs/tags/Cisco Threat Response



Threat Response

In this module, you will learn the basic purpose and features of Cisco Threat Response, and then dig into the API that powers it all behind the scenes. Learn how to leverage the capabilities of this powerful investigative and response workbench, and how to incorporate them in an automated fashion into your SOC's existing toolsets and workflows!

2 Learning Labs

2 Hours 45 Minutes

Choose a learning lab to start learning

Introduction to Cisco Threat Response — 45 min

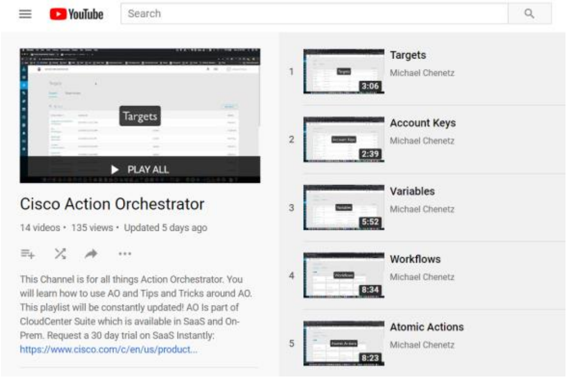
Learn about Cisco Threat Response and how it enables your SOC to do more with your existing Cisco products.

Last Completed on 10/11/2019 @ 10:42 AM

Introduction to Cisco Threat Response APIs — 120 min

SecureX orchestration Resources

Action Orchestrator videos: cs.co/AOvideos



Cisco Action Orchestrator

14 videos • 135 views • Updated 5 days ago

This Channel is for all things Action Orchestrator. You will learn how to use AO and Tips and Tricks around AO. This playlist will be constantly updated! AO Is part of CloudCenter Suite which is available in SaaS and On-Prem. Request a 30 day trial on SaaS Instantly: https://www.cisco.com/c/en/us/product...

1 Targets – Michael Chenetz – 3:06

2 Account Keys – Michael Chenetz – 2:39

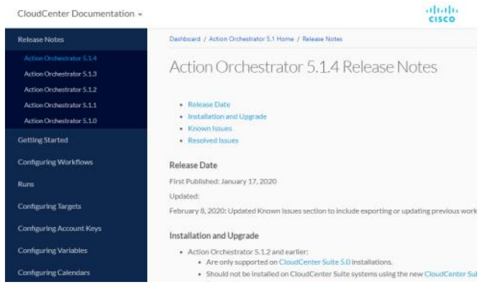
3 Variables – Michael Chenetz – 5:52

4 Workflows – Michael Chenetz – 8:34

5 Atomic Actions – Michael Chenetz – 8:23

Action Orchestrator docs

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



CloudCenter Documentation
Release Notes
Action Orchestrator 5.1.4
Action Orchestrator 5.1.3
Action Orchestrator 5.1.2
Action Orchestrator 5.1.1
Action Orchestrator 5.1.0
Getting Started
Configuring Workflows
Runs
Configuring Targets
Configuring Account Keys
Configuring Variables
Configuring Calendars
Dashboard / Action Orchestrator 5.1 Home / Release Notes

Action Orchestrator 5.1.4 Release Notes

- Release Date
- Installation and Upgrade
- Known Issues
- Resolved Issues

Release Date

First Published: January 17, 2020

Updated:

February 8, 2020: Updated Known Issues section to include exporting or updating previous work

Installation and Upgrade

- Action Orchestrator 5.1.2 and earlier:
  - Are only supported on CloudCenter Suite 5.0 installations.
  - Should not be installed on CloudCenter Suite systems using the new CloudCenter Sui