



Cisco Tech Club Days



Detekce, diagnostika a analýza bezpečnostních incidentů pro SoC a I&R týmy

Jiří Tesař

Technical Solution Architect - Security

2.9. 2020

What we need to support

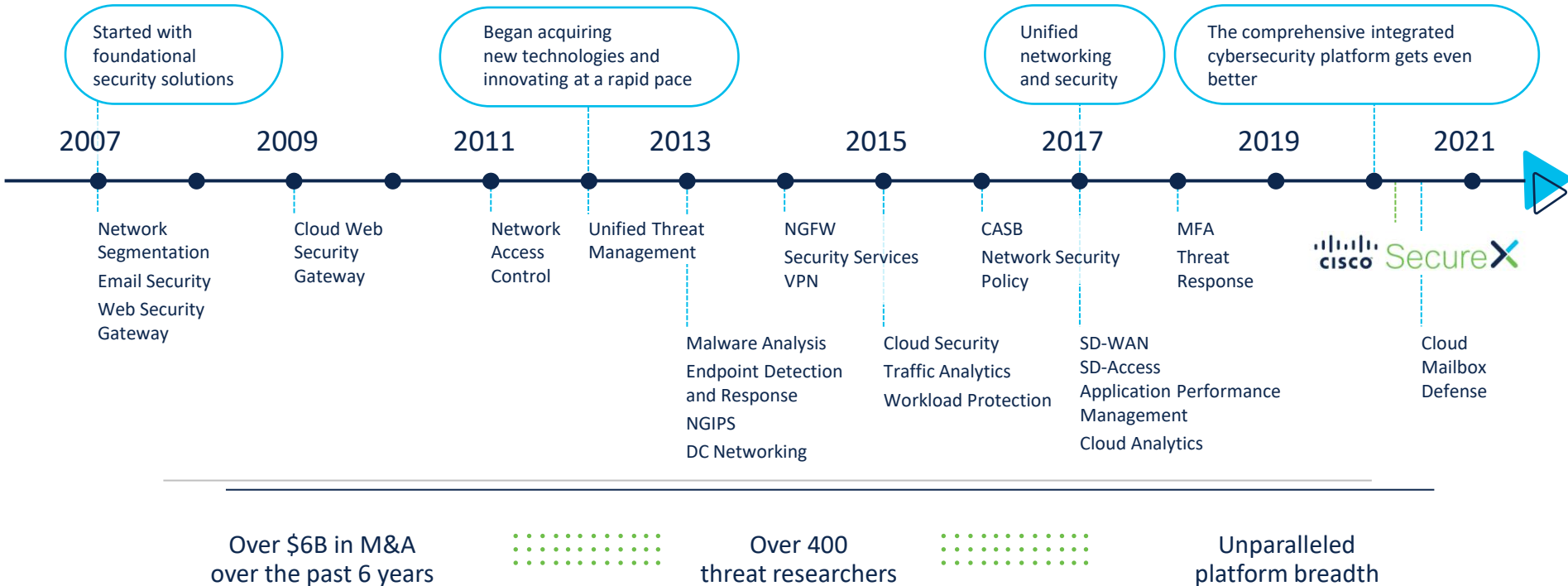
- 1 Trusted Security Architecture** Provides pervasive network visibility and control - reduce complexity and increase protection
- 2 Rich and Innovative Products** Addresses any organization size and needs
- 3 Context Awareness and Security Intelligence** Discovers and protects against next generation of threats using industry unique capabilities
- 4 Consistent Policy Enforcement** Secures the borderless experience with context-aware policy
- 5 Network Integration** Enables security data gathering and enforcement across devices, the network and data center



A platform approach confidently tackles the most pressing security operation challenges



Building a platform takes time and engineering talent



Introducing SecureX

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



SecureX **unlocks value** for your organization



Integrated and open for
simplicity



Unified in one location for
visibility



Maximized operational
efficiency

Included with every Cisco Secure product

In 15 minutes, you achieve real benefits using what you already have as it's cloud-native

In half the time, customers say they visualize threats within their environment¹

Save 100 hours by unifying visibility and automating your workflows

85% reduction in time to respond and remediate to an attack²

[1] Source: TechValidate

[2] Source: Based on internal simulation

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

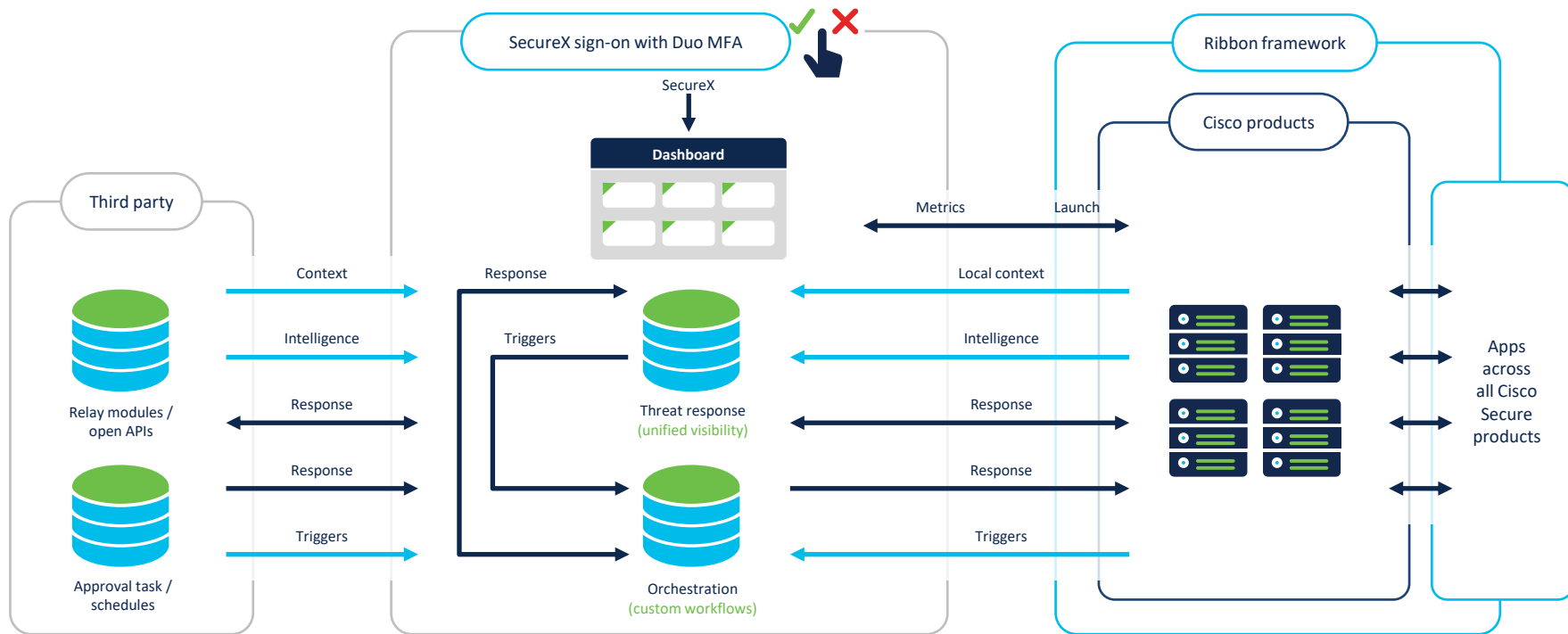
ribbon & sign-on
never leaves you
maintains context

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



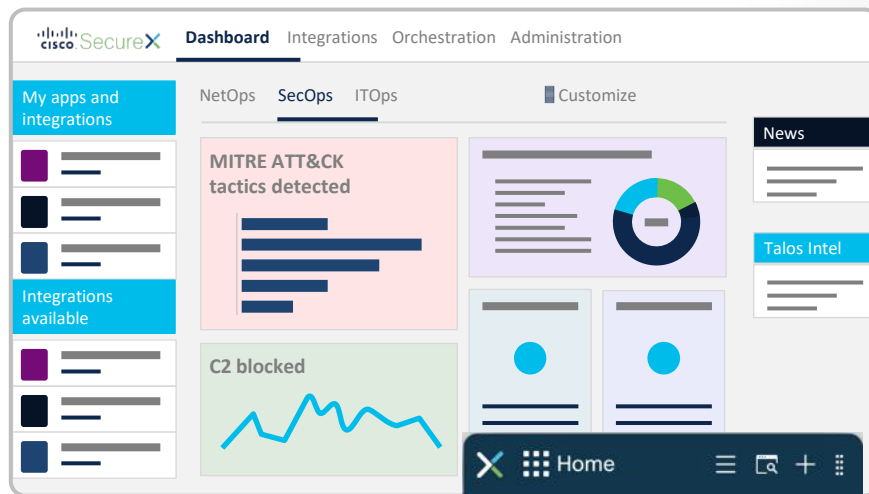
What unified **visibility** looks like



BEFORE: “We swivel our chair to see many views”



AFTER: “We instantly see what matters to us in one view”



“We can view ROI metrics and operational measures across many products in **one or more customizable dashboards**”

“We **never lose context** as the ribbon follows us everywhere when we use the Cisco Secure portfolio”

“We can try other platform integrations **with a click** before we buy”

“Our **SOC knows latest intel** from the largest threat research team on the planet”

SecureX sign-on

Adaptive, layered and simplified authentication

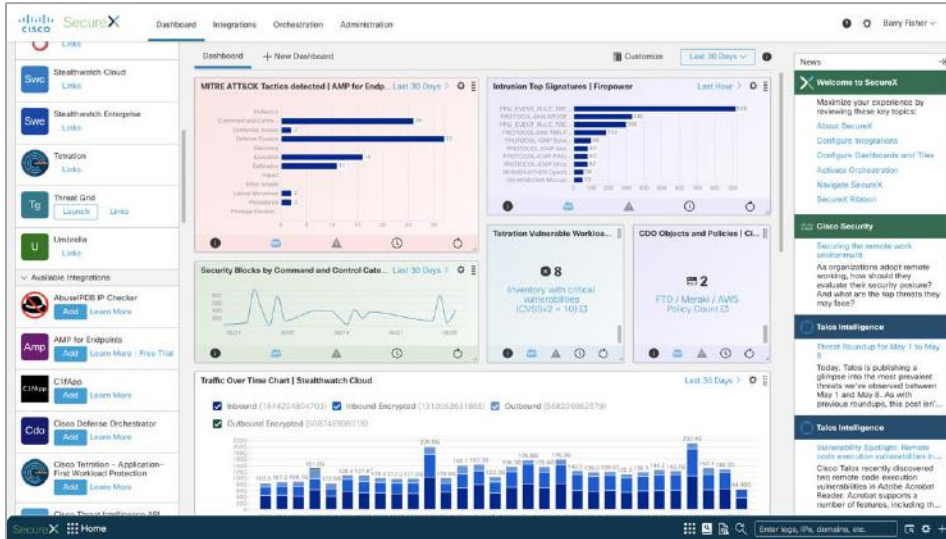
Duo's Multi-Factor Authentication (MFA) integration with SecureX sign-on means one push notification and one tap away from instant access

Easily manage and invite users to your organization



SecureX Dashboard Demo

A new level of visibility with SecureX dashboard



Applications (left)

View, launch or trial the integrated products



Tiles (middle)

Presents metrics and operational measures from the integrated products



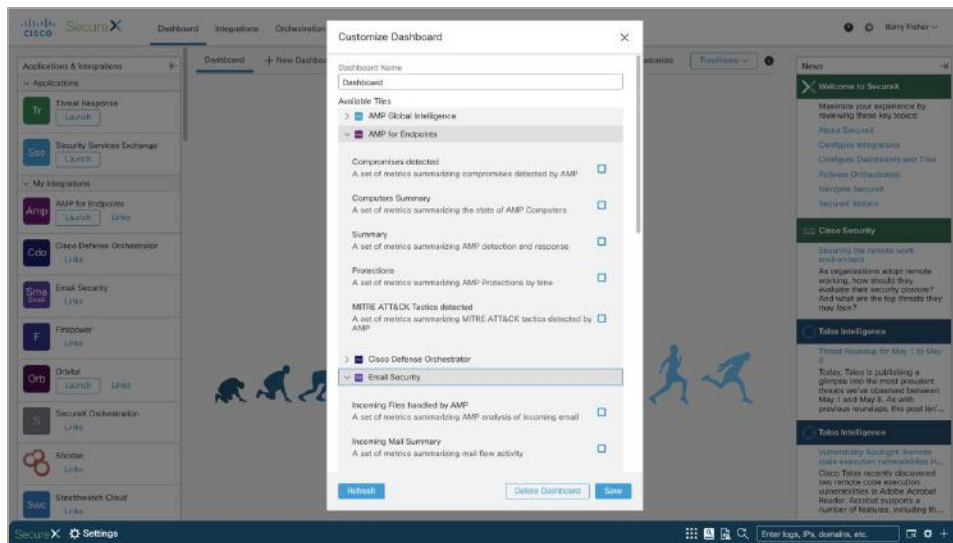
News (right)

Product updates, industry news, and blog posts

Understand what matters in one view across your security infrastructure



Have it your way with customizable dashboards



Up to 5 customizable dashboards per user



60+ color-coded tiles available across 12+ Cisco Secure product families



Customize tiles by layout, size, timeframe, scale, etc.

Accelerate investigations in SecureX

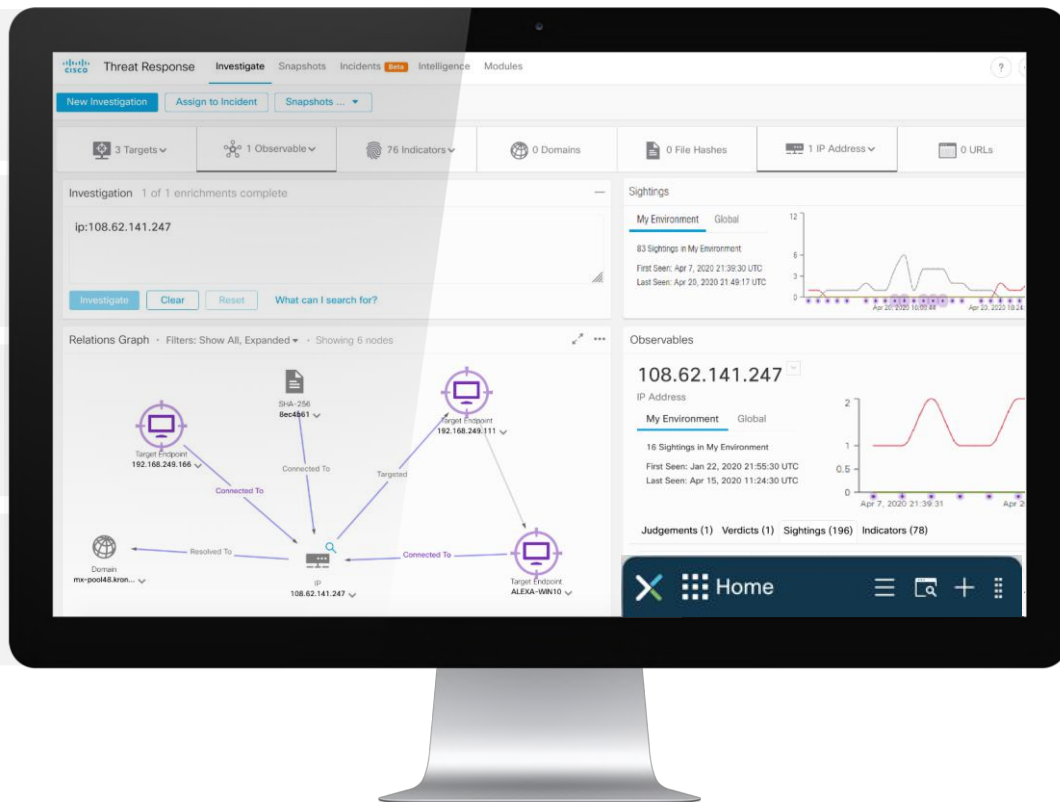
SecureX threat response

Aggregate and query global intel and local context in one view

Visualize the impact of threats across your environment

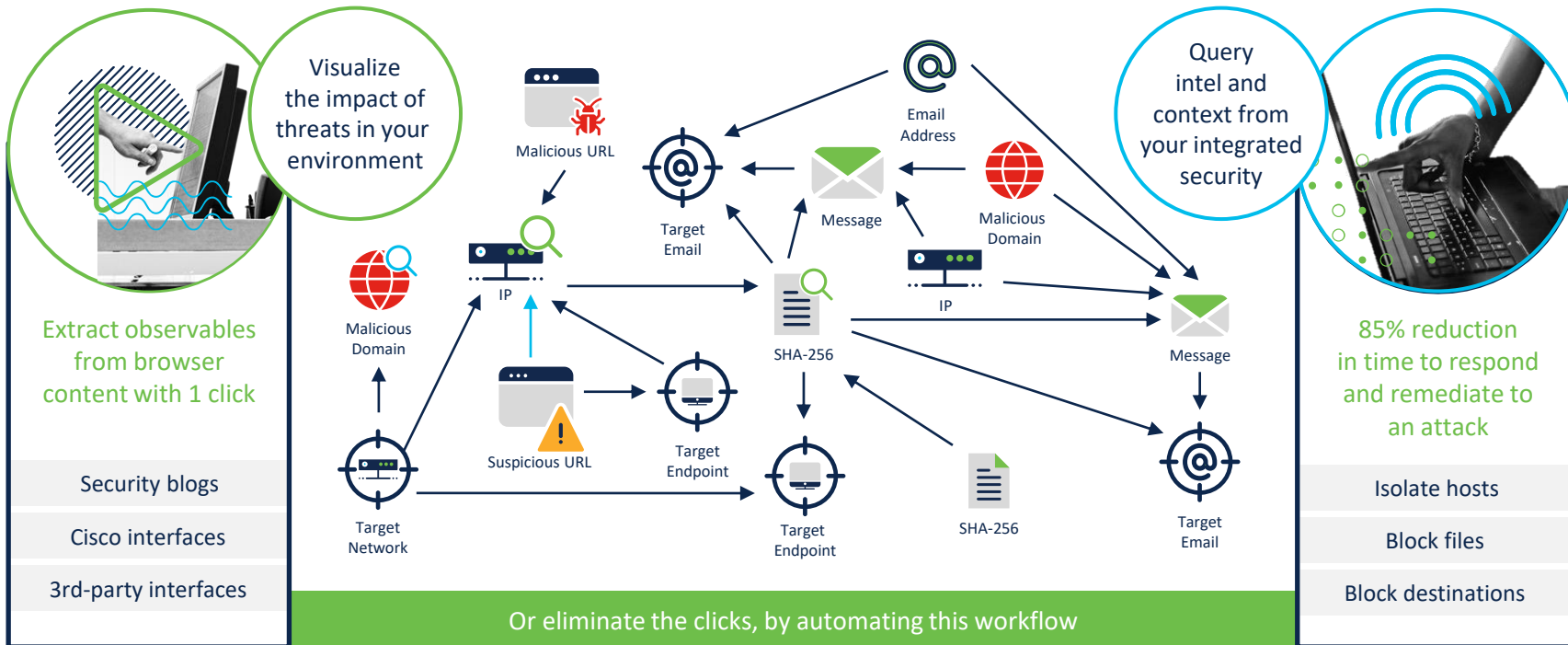
Take immediate action to isolate hosts and block destinations or files

Automate workflows with approval actions for better collaboration



In minutes, see and stop attacks with a few clicks

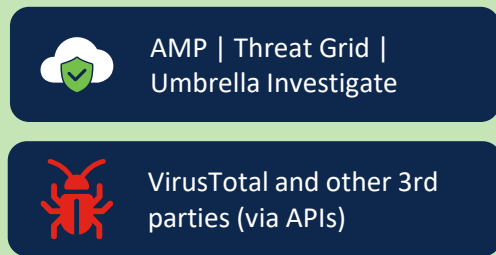
Your SecOps with SecureX threat response



Investigate with intelligence, context and response

SecureX threat response

Intelligence



Are these observables suspicious or malicious?

Observables:

- File hash
- IP address
- Domain
- URL
- Email addresses
- Etc.

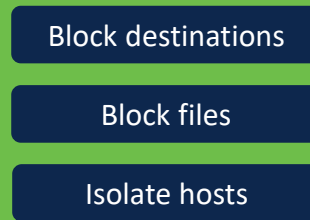
Local security context



Have we seen these observables? Where?

Which endpoints connected to the domain/URL?

Response actions



What can I do about it right now?

Never lose context with SecureX ribbon

Home Casebook Query endpoints Find observables on page

Incidents Search Settings

SecureX Incidents

Enter logs, IPs, domains, etc.

Max/Min

Incidents

Investigate in Threat Response Change Status View in Incident Manager

ASSIGNEES · Add

No one is assigned - [assign yourself](#)

Search... X ↓

Assigned to others - (359) < >

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
NGFW Event Service Jun 29, 2020

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

Summary Targets **Observables** Timeline Sightings Indicators

Casebooks Snapshots

192.168.250.173 >
IP Address

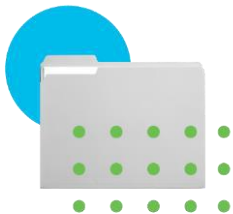
146.112.61.107 >
IP Address

1 1
Target Sighting

1 1
Target Sighting

SecureX ribbon

Applications available in SecureX ribbon at launch:



Casebook

gather observables in groups, assign the case a name and a description, take and save notes on the case, add other observables at any time, immediately **see verdicts and take actions**, share cases between staff.



Incident manager

single list for security Incidents across all supported products; assign, open, close and work tickets through the lifecycle; quick pivots into investigations and response actions; **automated triage** saves time and human cycles

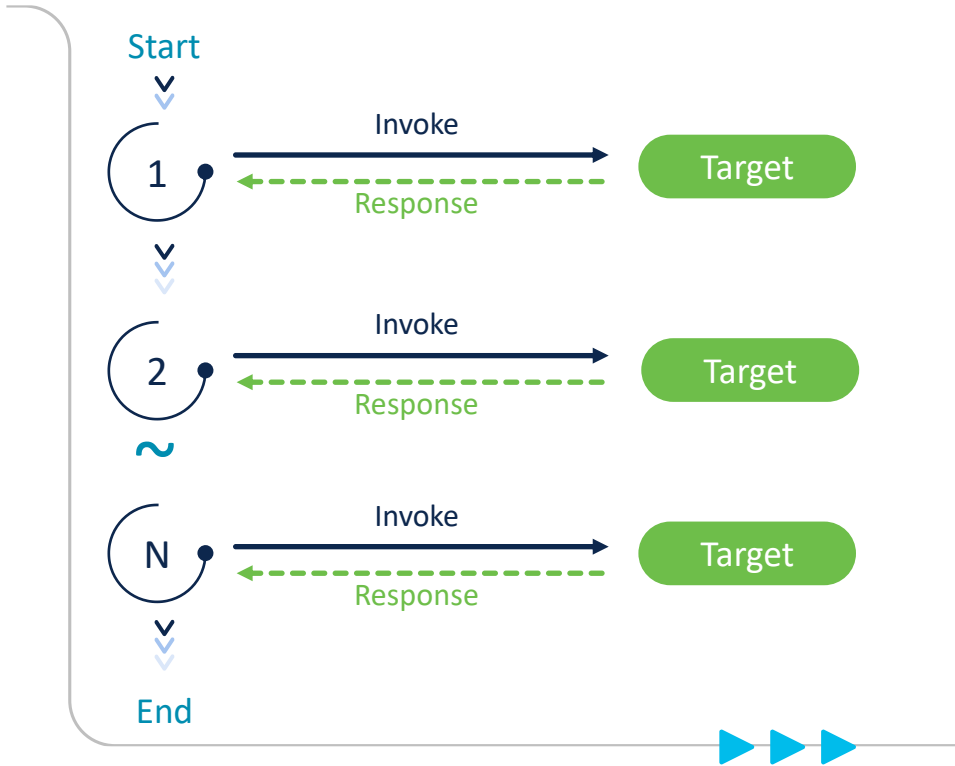


Orbital advance search

detailed **endpoint visibility** in a familiar SQL format, with an **intuitive graphical interface** and a catalog of pre-built queries for threat hunting and incident response.

... more apps coming to bring additional functionality in the future

Benefits:



SecureX Orchestration Demo

SecureX orchestration notes

Beta release

Focused on response workflows

Supported event triggers:
Approval task event,
time-based schedule

5 response workflows packaged with release 1.51:



Move Computer to AMP Triage group



Submit URL to Threat Grid



Take Orbital forensic snapshot

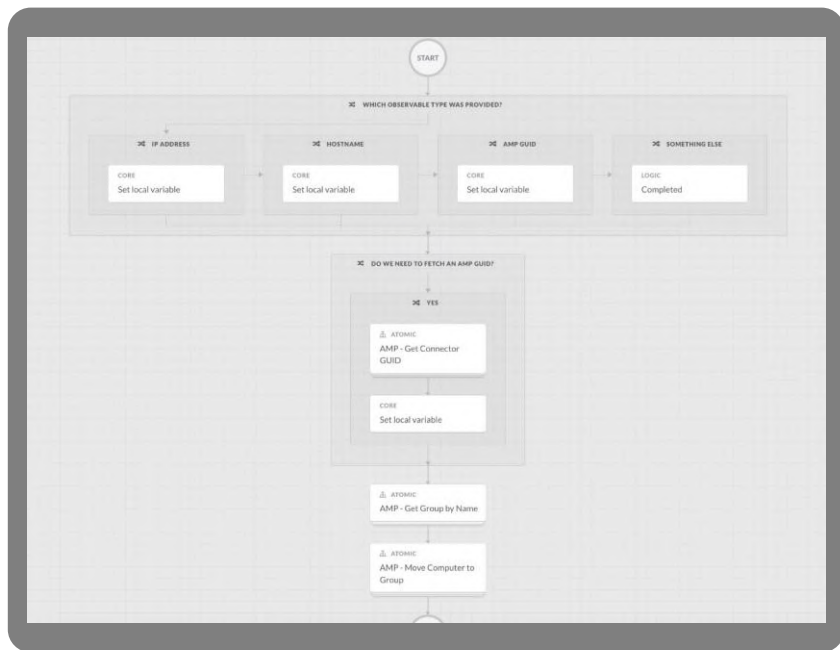


Take forensic snapshot and isolate



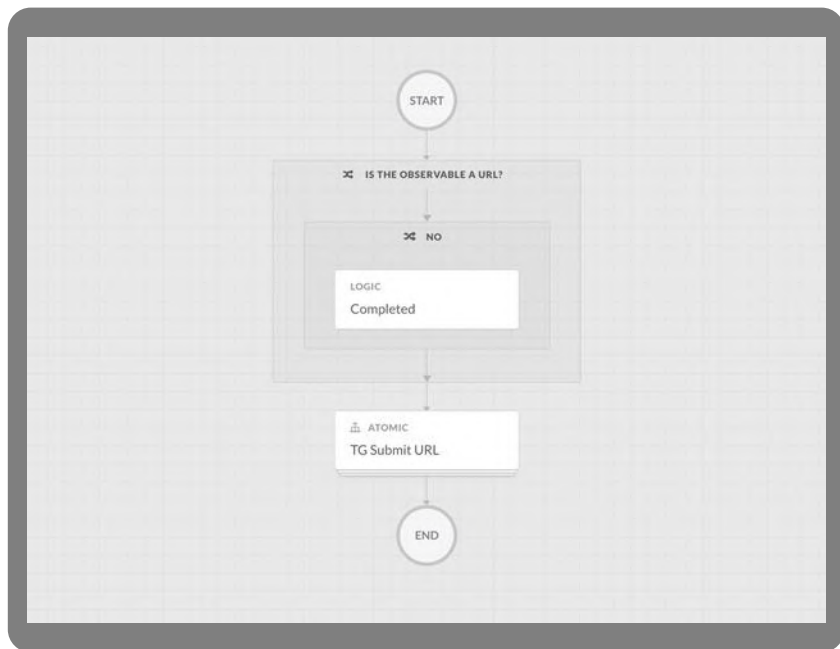
AMP host isolation with tier 2 approval

SecureX workflow: Move Computer to AMP Triage group



- ▶ The Move Computer to AMP Triage group workflow takes an IP address, hostname, or AMP Computer GUID and moves the corresponding endpoint to a triage group. The name of the triage group is configurable using a local variable inside the workflow.
- ▶ If an IP address or hostname of the device are provided, it attempts to convert them to an AMP Computer GUID.

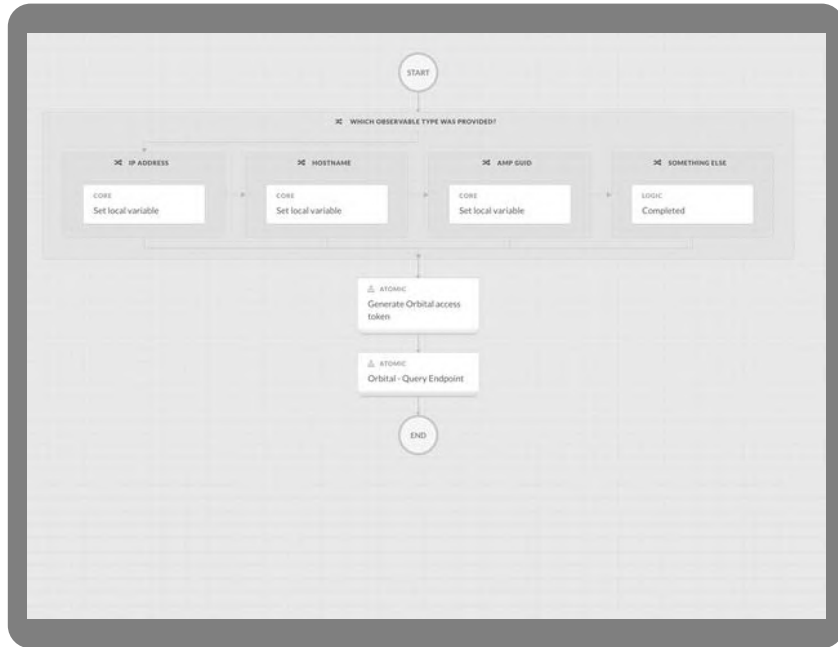
SecureX workflow: Submit URL to Threat Grid



▶ The Submit URL to Threat Grid workflow takes a URL and submits it to Threat Grid for analysis.

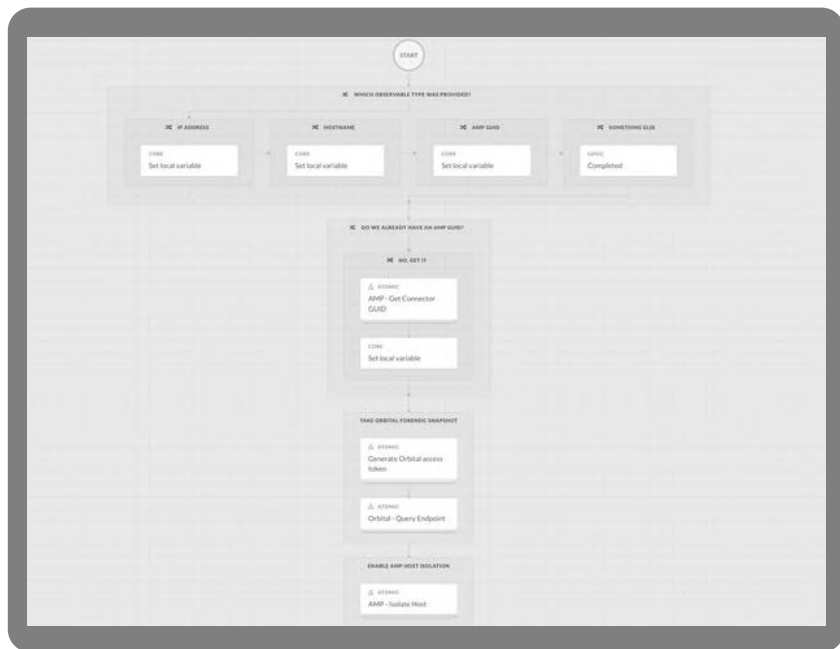
The result of the submission can be viewed from the Threat Grid console.

SecureX workflow: Take Orbital forensic snapshot



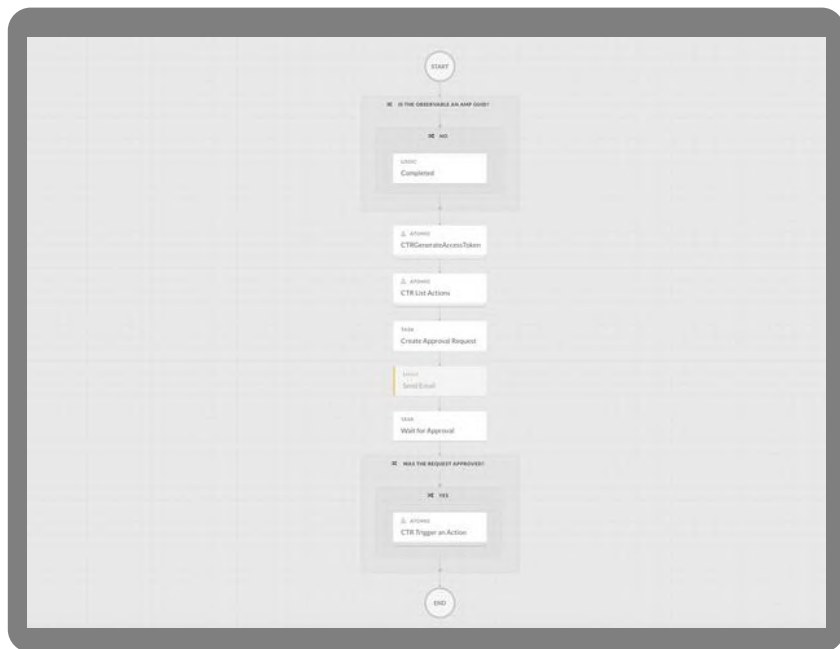
The Take Orbital forensic snapshot workflow takes an IP address, hostname, or AMP computer GUID and initiates an Orbital forensic snapshot for the corresponding endpoint.

SecureX workflow: Take forensic snapshot and isolate



- ▶ The Take forensic snapshot and Isolate workflow takes an IP address, hostname, or AMP computer GUID, requests an Orbital forensic snapshot for the endpoint, and then enables AMP host isolation using the response action.
- ▶ The forensic snapshot can be viewed in the Orbital console.

SecureX workflow: AMP host isolation with tier 2 approval



The AMP host isolation with tier 2 approval workflow takes an AMP computer GUID and requests approval to enable host isolation for the corresponding endpoint using the response action for AMP host isolation from SecureX threat response.

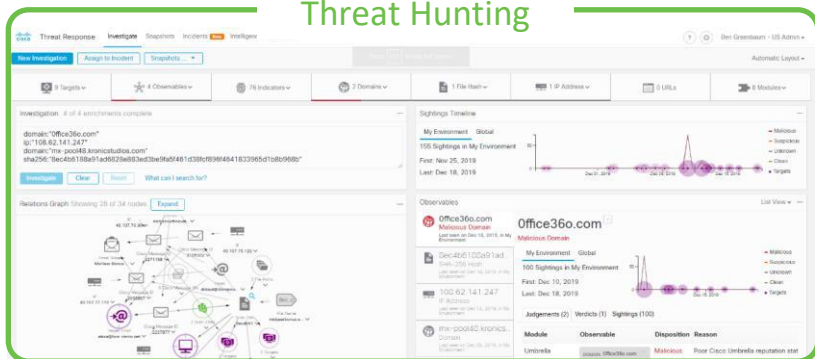
If approved, isolation is enabled. If rejected or expired, no action is taken.

This workflow is an inspirational workflow showing how approvals can be used with the response actions from SecureX threat response. To stop isolation of the the endpoint, use the AMP end isolation action from SecureX threat response.

Use cases

SecureX threat response

Threat Hunting



Incident Response

Title	Status	Confidence	Description	Source	Modified	Actions
Intrusion event 1:100000...	New	Medium	MALWARE CNC SIGNAL ...	ngfw_ips_event_service	Dec 18, 2019	...
Data Exfiltration	New	Low	Tracks inside and outsid...	Cisco Stealthwatch Enterprise	Dec 18, 2019	...
Security Intelligence eve...	New	High	Security Intelligence eve...	ngfw_event_service	Dec 17, 2019	...
Security Intelligence eve...	New	High	Security Intelligence eve...	ngfw_event_service	Dec 17, 2019	...

Protect your organization against

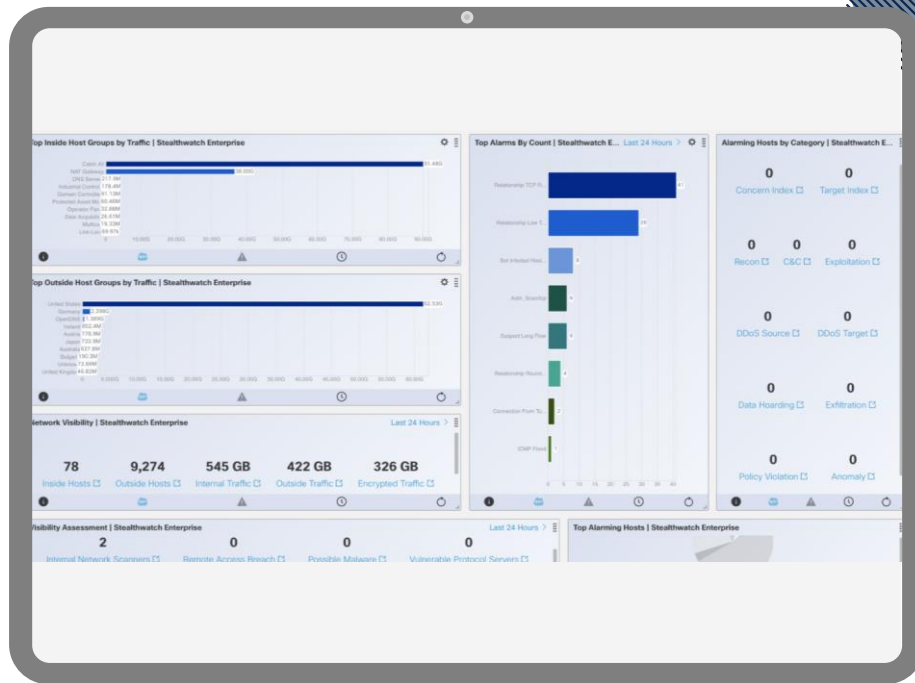
- Ransomware
- Server-based attacks
- File-less malware
- Cryptomining
- Phishing attacks
- Corporate espionage
- IoT attacks
- Data breaches

SecureX
Threat Hunting
Demo

Stealthwatch Enterprise

Dashboard

- Alarming hosts by category
- Top outside host groups by traffic
- Network visibility
- Top inside host groups by traffic
- Visibility assessment
- Top alarms by count
- Top alarming hosts



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

SecureX integrations with third parties

Farsight Security
Gigamon ThreatINSIGHT
Google Chronicle
Google Safe Browsing
VirusTotal
IBM QRadar
Microsoft Defender ATP
Microsoft Graph Security
Polarity Data Awareness
Qualys IOC
Radware DDoS
Radware WAF
SecurityTrails
ServiceNow Security Operations
Shodan
Signal Sciences
Splunk Enterprise
Splunk Phantom
SpyCloud
Swimlane
ThreatQ

AlienVault OTX
Abuse IPDB
APIVoid
Auth0 Signals
C1fApp
Cybercrime Tracker
Cyberprotect
Have I Been Pwned
Pulsedive
The Hive Project
urlscan.io

Resources

Integration documentation

cs.co/SecureX_integration_workflows

The screenshot shows the Cisco SecureX Integration Workflows documentation page. The header includes the Cisco logo and 'SecureX Integration Workflows'. A search bar is present. The main content is organized into two primary sections: 'threat response' and 'Orchestration'. Each section contains a numbered list of articles.

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

UI docs and proto tools

The screenshot displays a web interface for a Threat Response UI. It features a 'Parameters' section with a 'Submit' button. Below this is an 'Observable' field with a 'Submit' button and a dropdown menu for 'Observable context type' set to 'application/json'. An 'Execute' button is also visible. The bottom of the interface shows a 'Responses' section with a 'Refresh context type' dropdown and a 'Clear' button. A terminal window at the bottom displays a list of JSON objects representing threat response data.

Github

github.com/CiscoSecurity

The screenshot shows the GitHub repository page for Cisco Security. The page title is 'Cisco Security' and the description is 'Collection of example scripts for Cisco Security APIs'. The page lists several pinned repositories:

- tr-05-gigamon-threatinsight**: Threat Response Serverless Relay for Gigamon ThreatINSIGHT. Languages: python, flask, aws, relay, lambda, serverless, zapppa. Updated 9 hours ago.
- tr-05-serverless-farsight-dnsdb**: Threat Response Serverless Relay for Farsight DNSDB. Languages: serverless, threat-response. Updated 10 hours ago.
- tr-05-serverless-shodan**: Threat Response Serverless Relay for Shodan. Languages: serverless, threat-response.

SecureX threat response resources

Devnet

developer.cisco.com/threat-response/



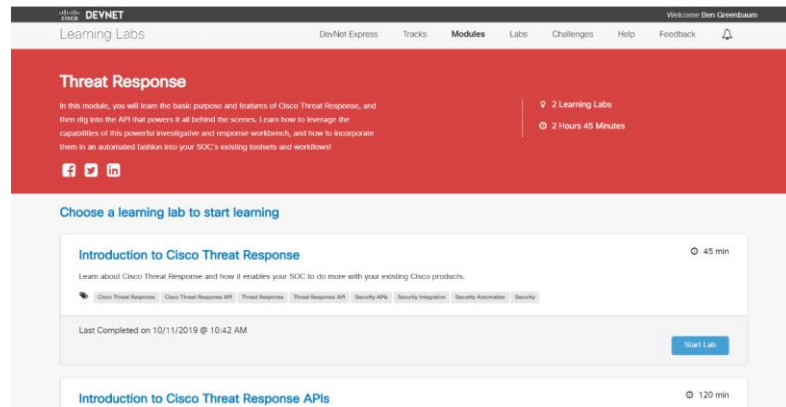
The screenshot shows the Cisco DevNet page for SecureX threat response. The header includes the DevNet logo and navigation links like Discover, Technologies, Community, Support, Events, and New Announcement. The main content area features a green background with the title "SecureX threat response" and a sub-header "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." A "Read the docs" button is visible at the bottom of the main content area.

What can you do with SecureX threat response APIs?



Devnet learning labs

cs.co/CTR-API-labs

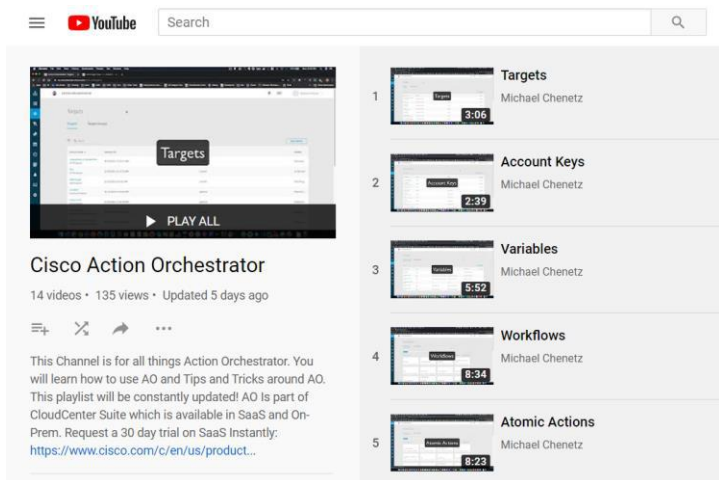


The screenshot shows the Cisco DevNet Learning Labs page for Threat Response. The header includes the DevNet logo and navigation links like DevNet Express, Tracks, Modules, Labs, Challenges, Help, Feedback, and a user profile. The main content area features a red background with the title "Threat Response" and a sub-header "In this module, you will learn the basic purpose and features of Cisco Threat Response, and then dig into the APIs 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 workflow!" A "Start Lab" button is visible at the bottom of the main content area. Below the main content area, there is a section titled "Choose a learning lab to start learning" with a list of labs. The first lab is "Introduction to Cisco Threat Response" with a duration of 45 min. The second lab is "Introduction to Cisco Threat Response APIs" with a duration of 120 min.

SecureX orchestration resources

Videos

cs.co/AOvideos



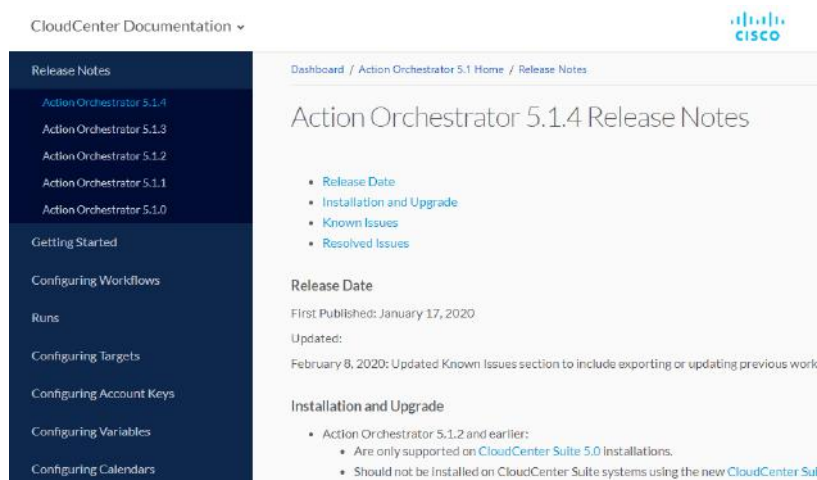
The screenshot shows a YouTube search results page for the playlist "Cisco Action Orchestrator" by Michael Chenetz. The playlist contains five videos:

1. Targets (3:06)
2. Account Keys (2:39)
3. Variables (5:52)
4. Workflows (8:34)
5. Atomic Actions (8:23)

The video description reads: "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...>"

Docs

<https://docs.cloudmgmt.cisco.com/display/ACTIONORCHESTRATOR52>



The screenshot shows the Cisco CloudCenter Documentation page for Action Orchestrator 5.1.4 Release Notes. The page includes a navigation menu on the left with the following items:

- 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

The main content area shows the "Action Orchestrator 5.1.4 Release Notes" page. The "Release Date" section indicates it was first published on January 17, 2020, and updated on February 8, 2020. The "Installation and Upgrade" section lists the following items:

- 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 Suite...

