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

Simplicity

Integrate technology together with true turnkey interoperability

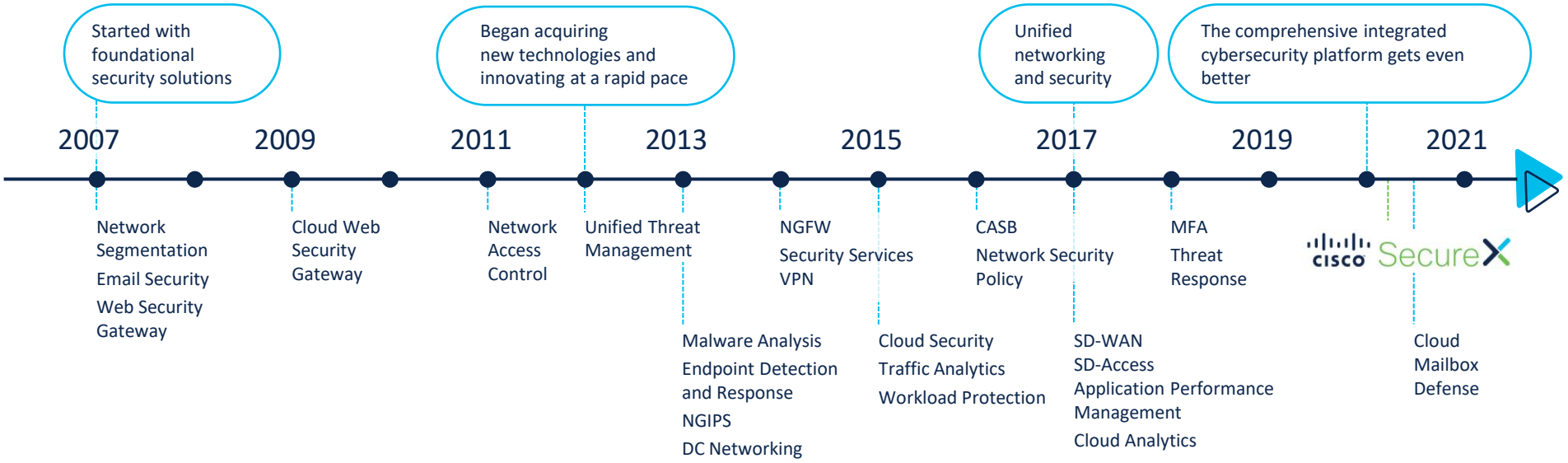
Visibility

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



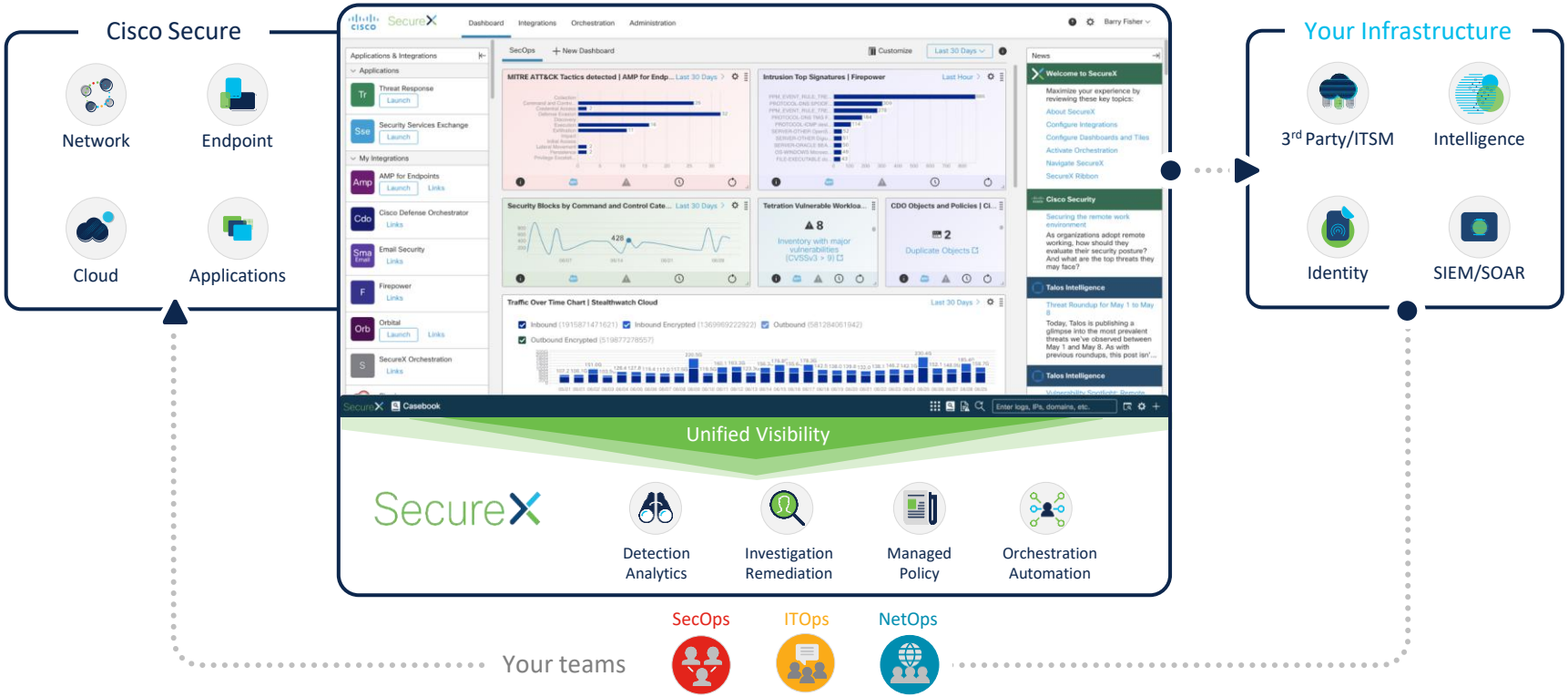
Over $6B in M&A over the past 6 years

Over 400 threat researchers

Unparalleled platform breadth

Introducing SecureX

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



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 environment[1]

Save 100 hours
by unifying visibility and automating your workflows

85% reduction
in time to respond and remediate to an attack[2]

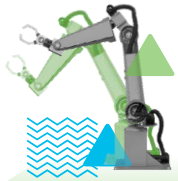
[1] Source: TechValidate

[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

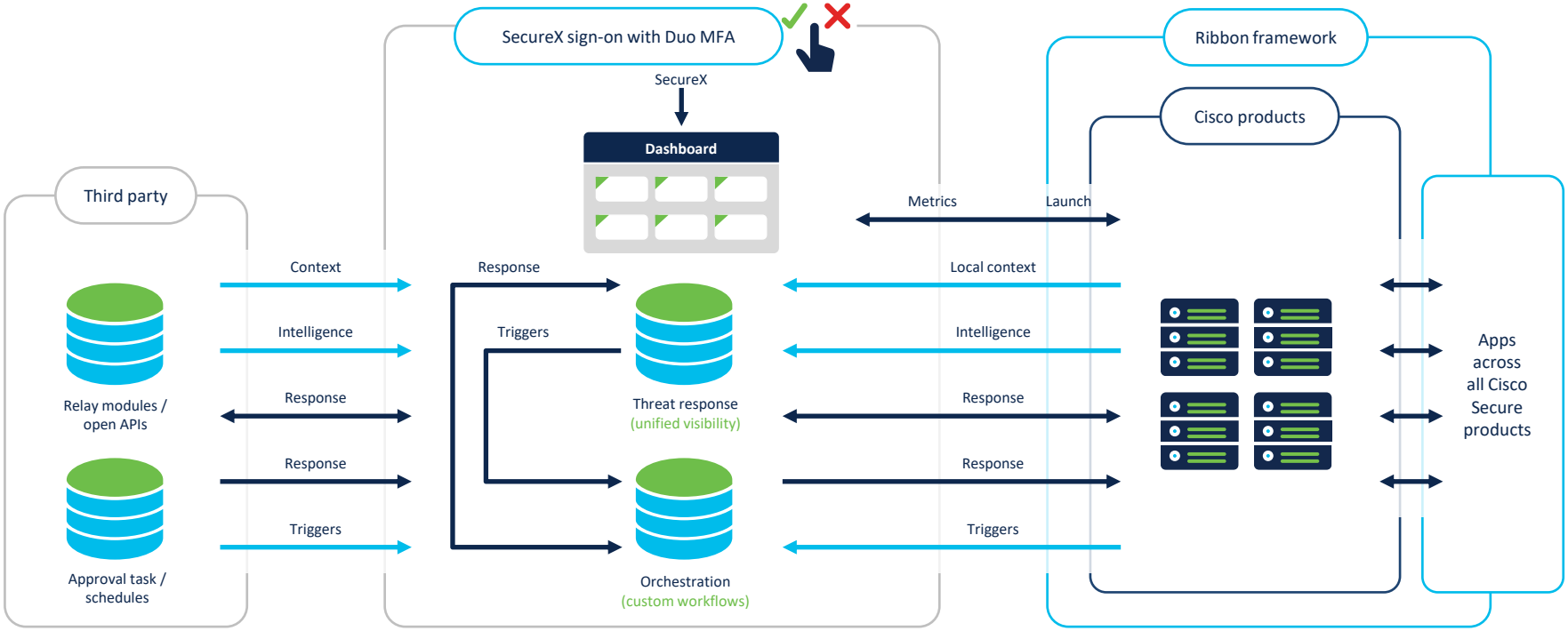
ribbon & sign-on
never leaves you maintains context

dashboard
customizable for what matters to you

threat response
is at the core of the platform

orchestration
drag-drop GUI for no/low code

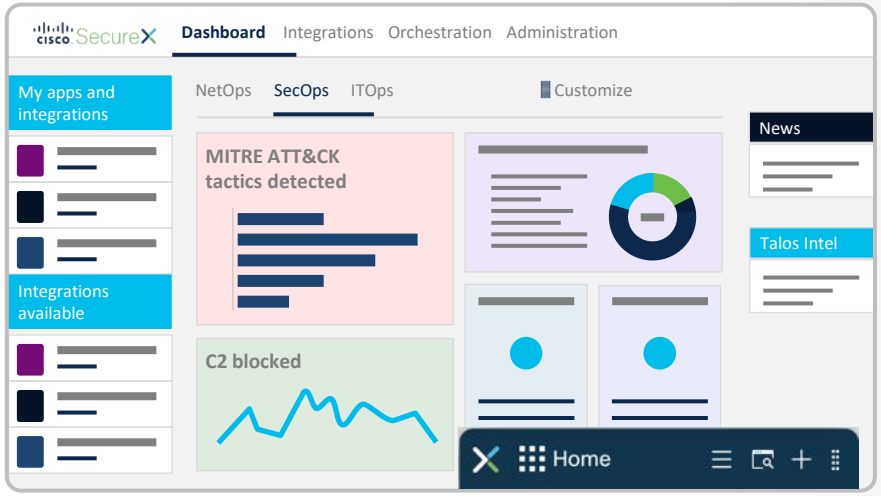
SecureX architecture



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”

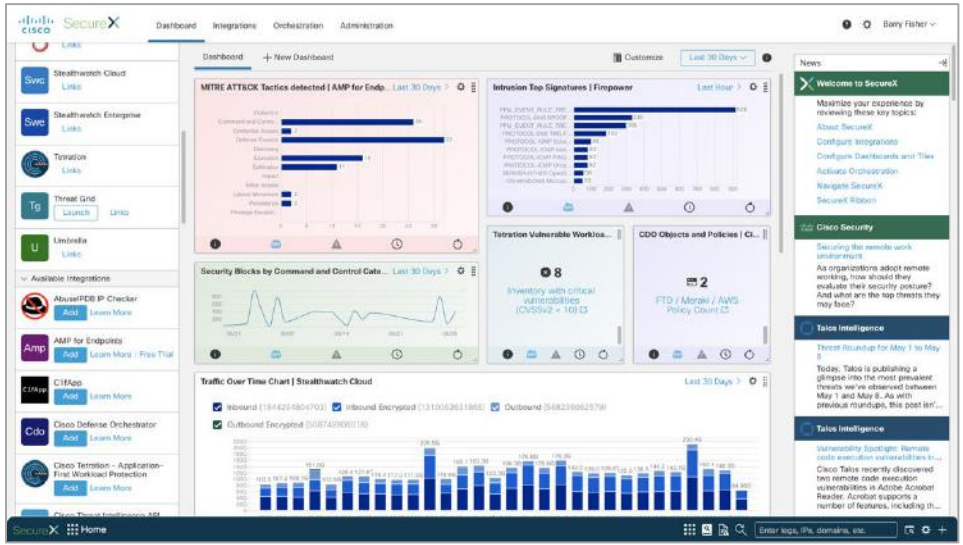
“Our SOC knows latest intel from the largest threat research team on the planet”

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



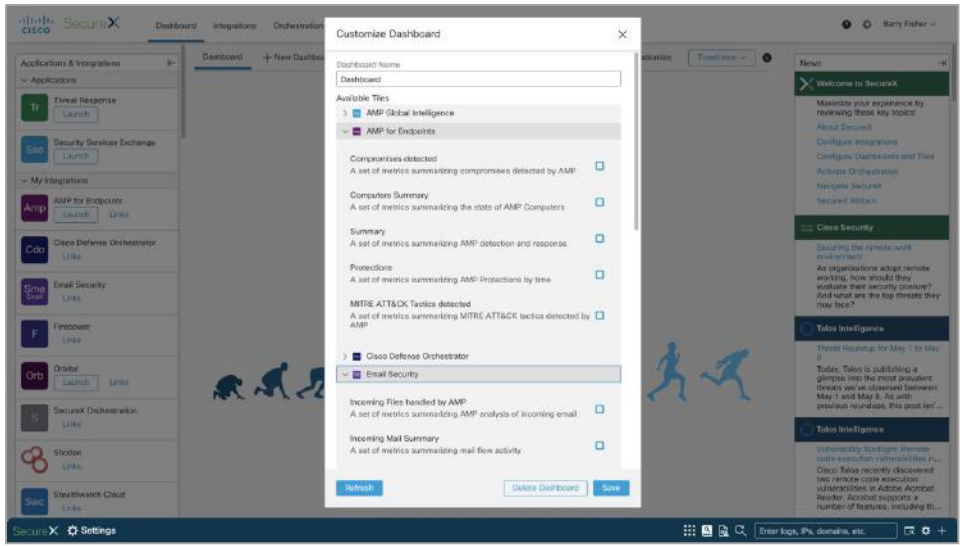
Applications (left)
View, launch or trial the integrated products

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

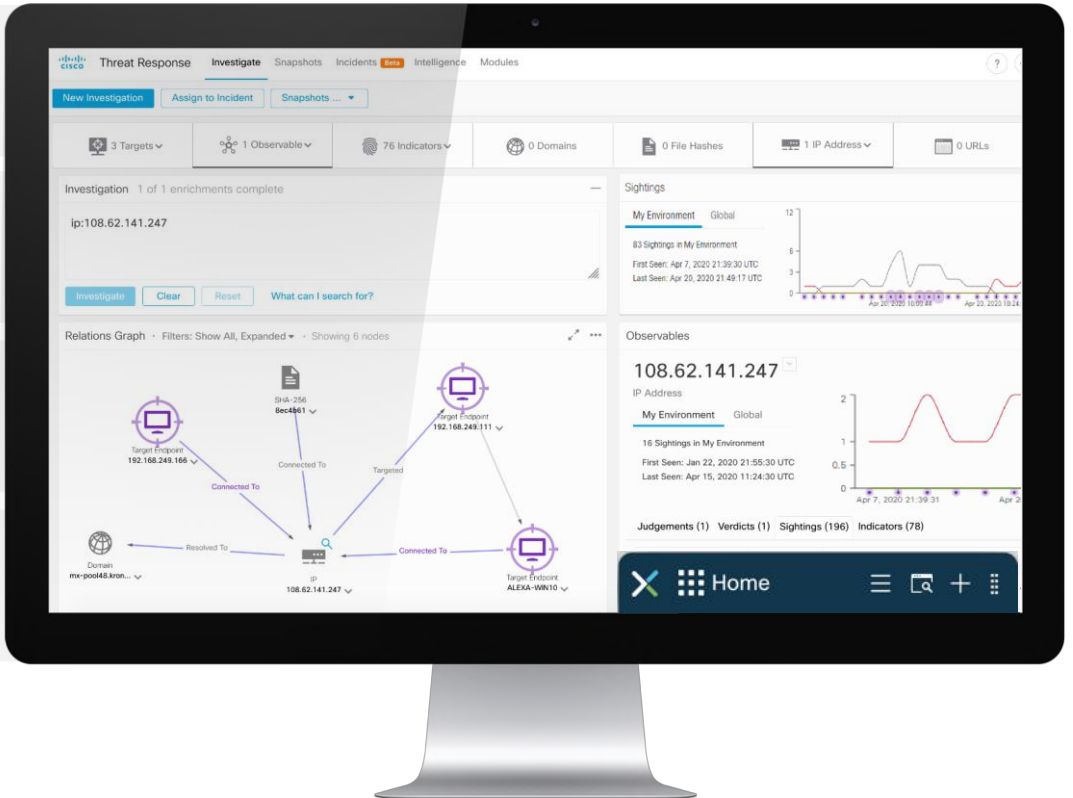
SecureX threat response

Aggregate and query global intel and local context in one view

Visualize the impact of threats across your environment

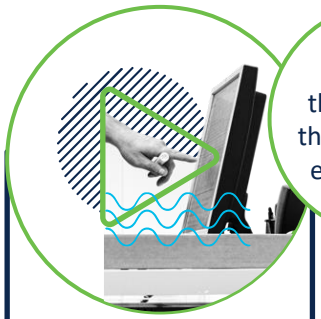
Take immediate action to isolate hosts and block destinations or files

Automate workflows with approval actions for better collaboration



In minutes, see and stop attacks with a few clicks

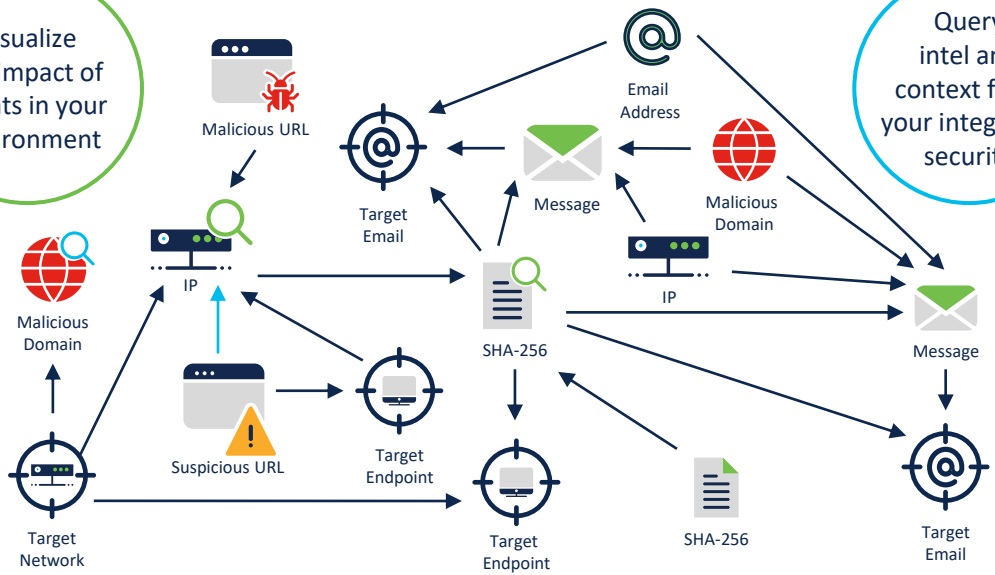
Your SecOps with SecureX threat response



Visualize the impact of threats in your environment

Extract observables from browser content with 1 click

- Security blogs
- Cisco interfaces
- 3rd-party interfaces



Query intel and context from your integrated security

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

- Isolate hosts
- Block files
- Block destinations

Or eliminate the clicks, by automating this workflow

Investigate with intelligence, context and response

SecureX threat response

Are these observables suspicious or malicious?

Have we seen these observables? Where?

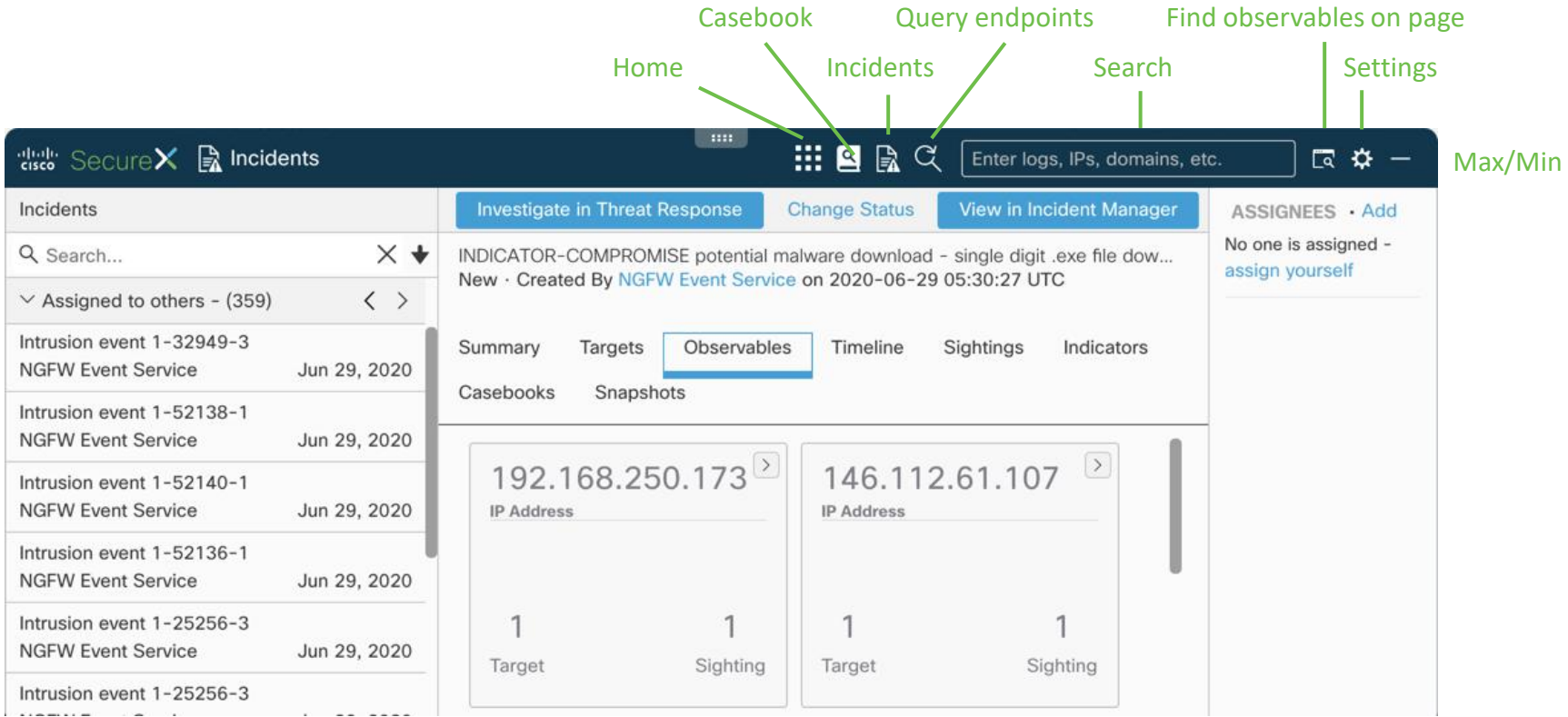
Which endpoints connected to the domain/URL?

What can I do about it right now?

Observables:

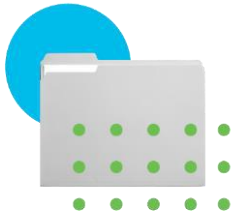
- File hash
- IP address
- Domain
- URL
- Email addresses
- Etc.

Never lose context with SecureX ribbon



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

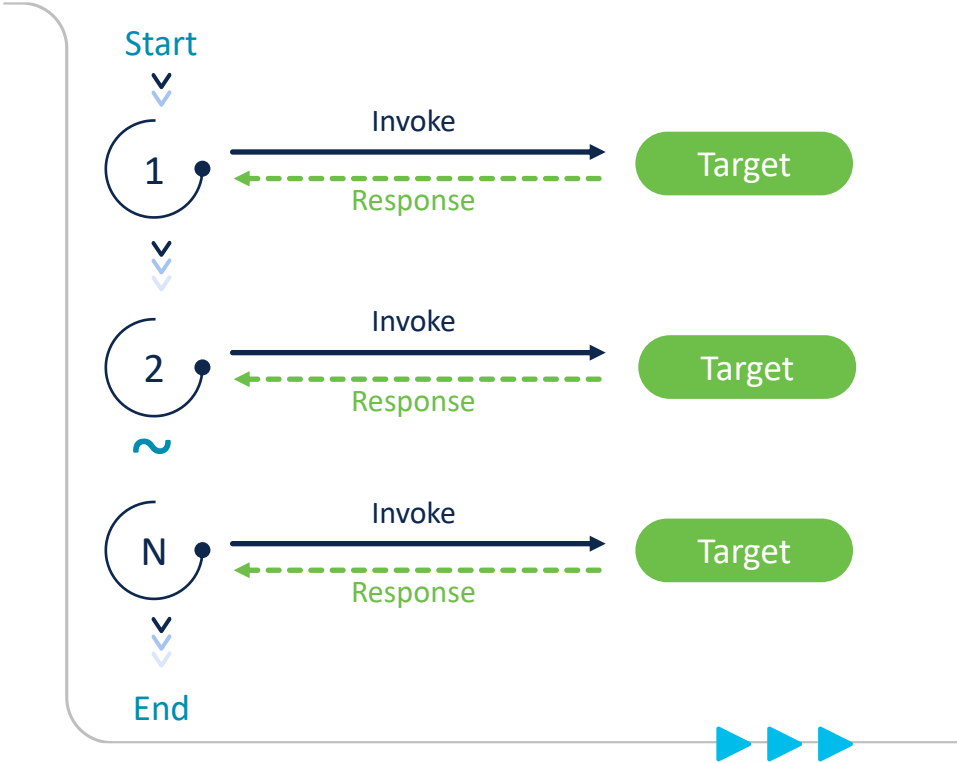
single list for security Incidents across all supported products; assign, open, close and work tickets through the lifecycle; quick pivots into investigations and response actions; **automated triage** saves time and human cycles

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:


Start
Invoke
1
Target
Response
Invoke
2
Target
Response
Invoke
N
Target
Response
End

SecureX
Orchestration Demo

SecureX orchestration notes

Beta release

Focused on response workflows

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

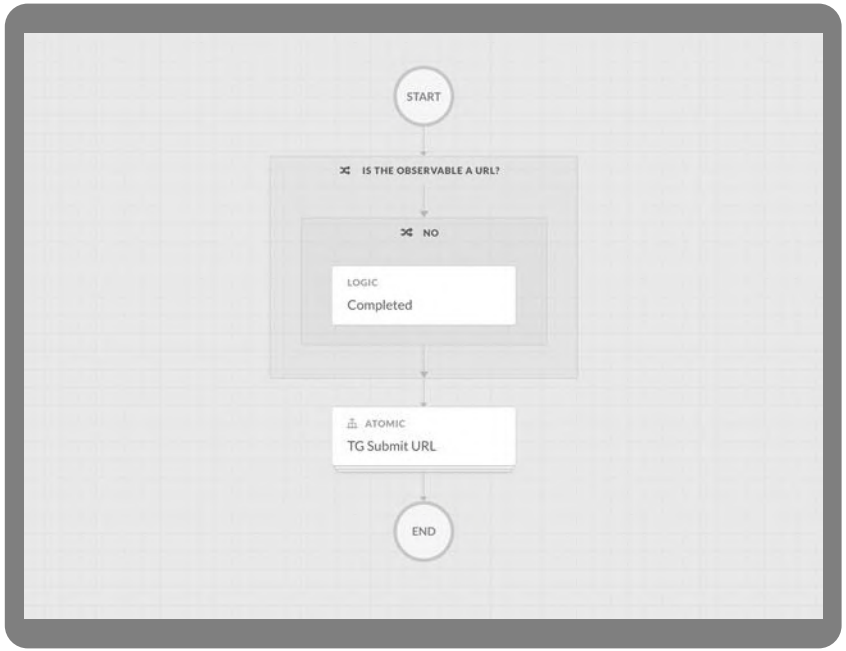
5 response workflows packaged with release 1.51:

- 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

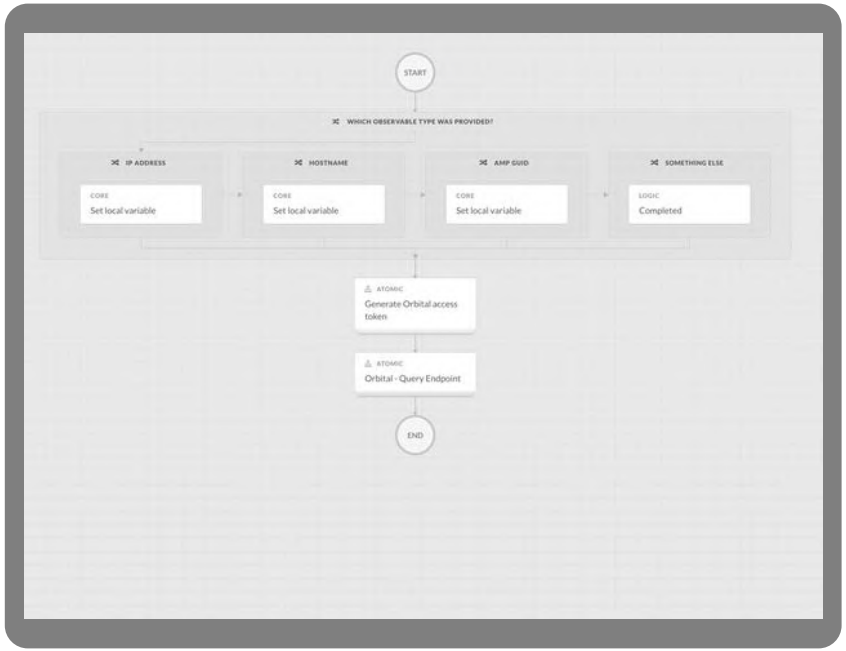
- The Move Computer to AMP Triage group workflow takes an IP address, hostname, or AMP Computer GUID and moves the corresponding endpoint to a triage group.
- The name of the triage group is configurable using a local variable inside the workflow.
- If an IP address or hostname of the device are provided,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

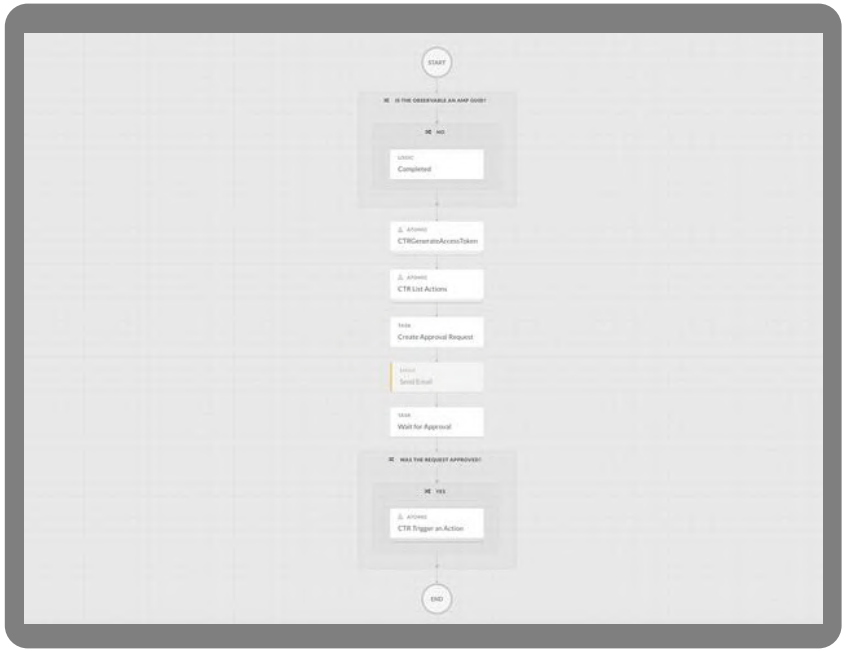


- The Take Orbital forensic snapshot workflow takes an IP address, hostname, or AMP computer GUID and initiates an Orbital forensic snapshot for the corresponding endpoint.

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

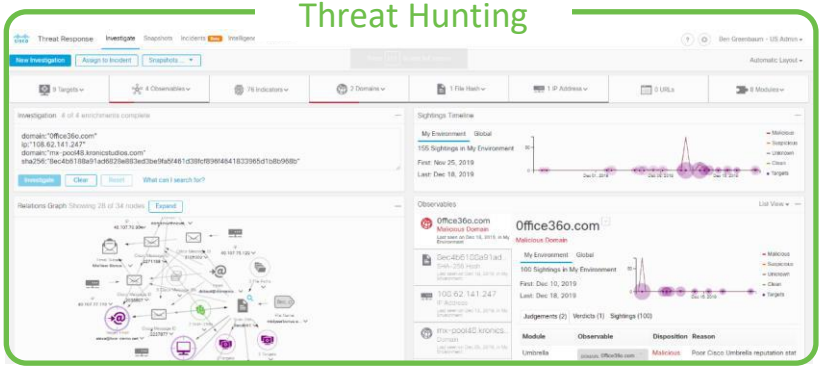


- The AMP host isolation with tier 2 approval workflow takes an AMP computer GUID and requests approval to enable host isolation for the corresponding endpoint using the response action for AMP host isolation from SecureX threat response**.**
- If approved, isolation is enabled. If rejected or expired, 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.

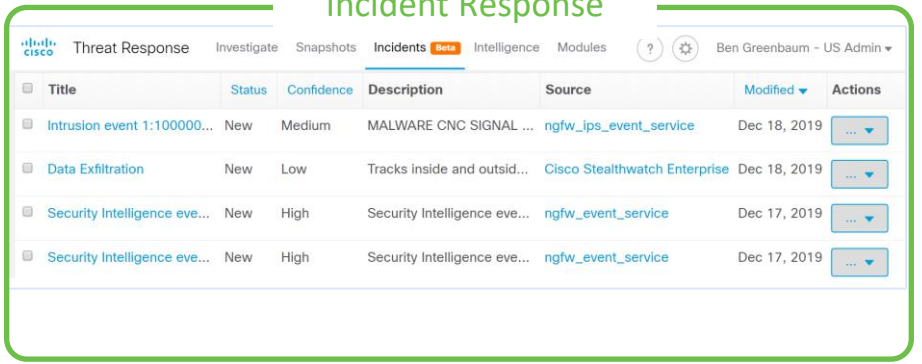
Use cases

SecureX threat response

Threat Hunting



Incident Response



Protect your organization against

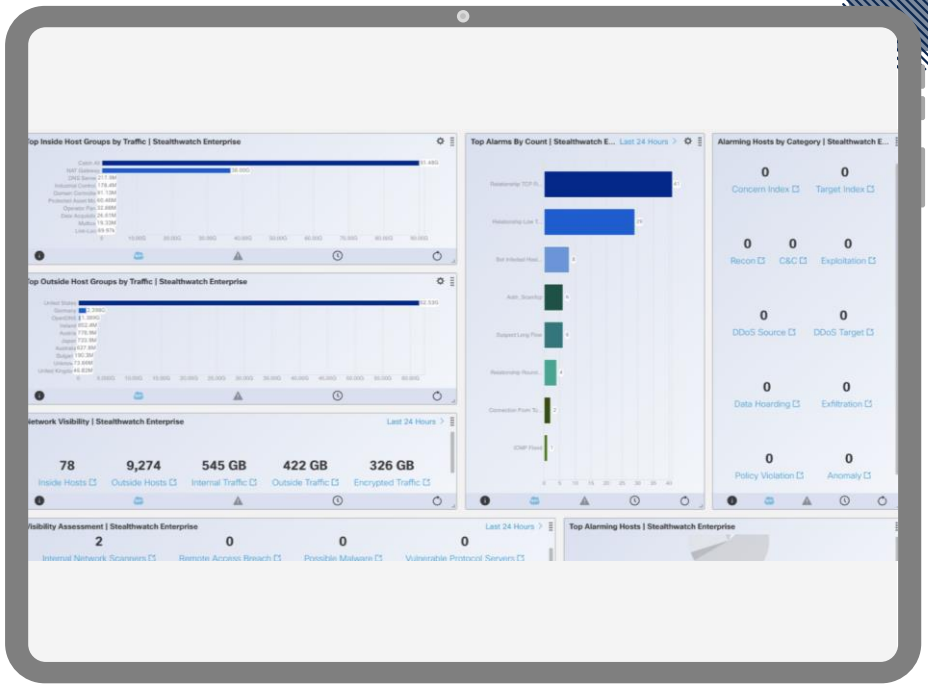
- Ransomware
- Server-based attacks
- File-less malware
- Cryptomining
- Phishing attacks
- Corporate espionage
- IoT attacks
- Data breaches

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

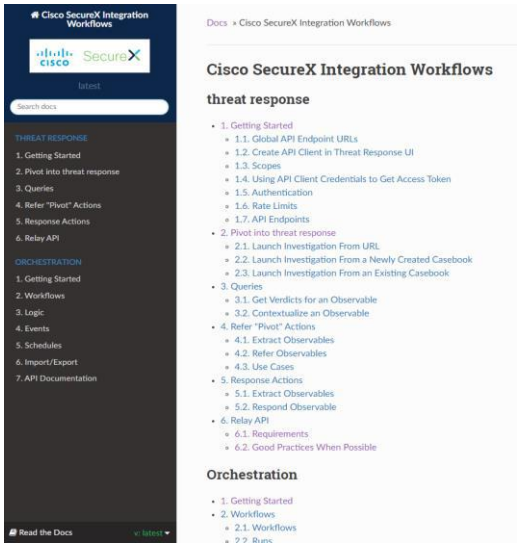
Farsight Security
Gigamon ThreatINSIGHT
Google Chronicle
Google Safe Browsing
VirusTotal
IBM QRadar
Microsoft Defender ATP
Microsoft Graph Security
Polarity Data Awareness
Qualys IOC
Radware DDoS
Radware WAF
SecurityTrails
ServiceNow Security Operations
Shodan
Signal Sciences
Splunk Enterprise
Splunk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

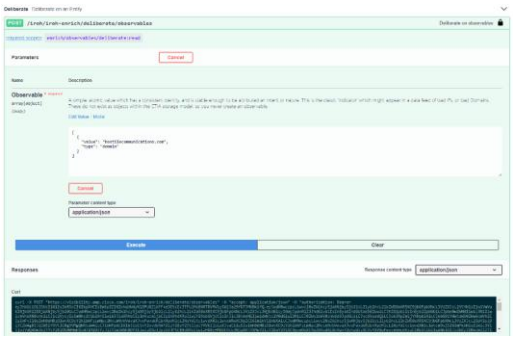
Resources

Integration documentation

cs.co/SecureX_integration_workflows

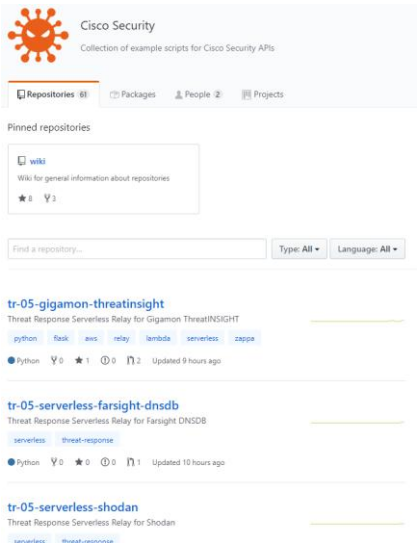


UI docs and proto tools



Github

github.com/CiscoSecurity



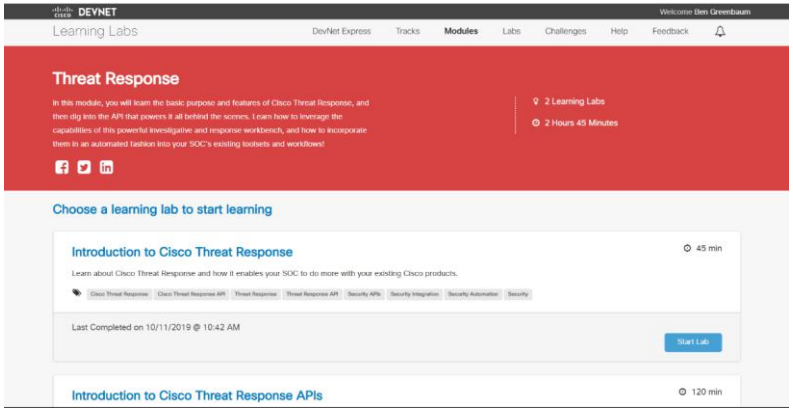
SecureX threat response resources

Devnet

developer.cisco.com/threat-response/

Devnet learning labs

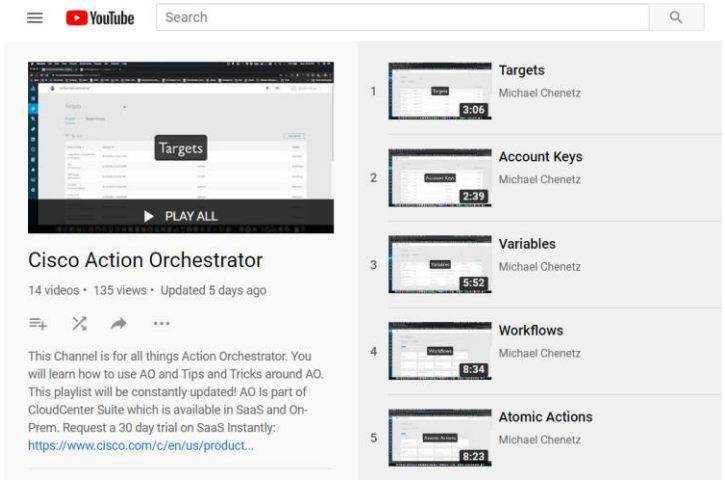
cs.co/CTR-API-labs



SecureX orchestration resources

Videos

cs.co/AOvideos



Docs

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