



The bridge to possible

Meet Cisco Secure X

Luis Silva, Customer Success Specialist, CCIE Security #36825
January 2022

What's coming up?



Spotlight Awards



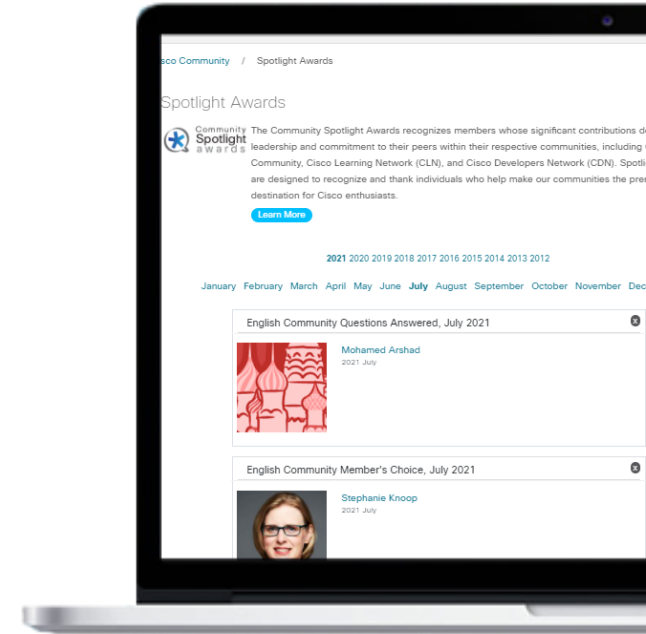
Get recognized by the Cisco Community
New Awardees every month!

First winners in 2022: cs.co/6016KBIA8

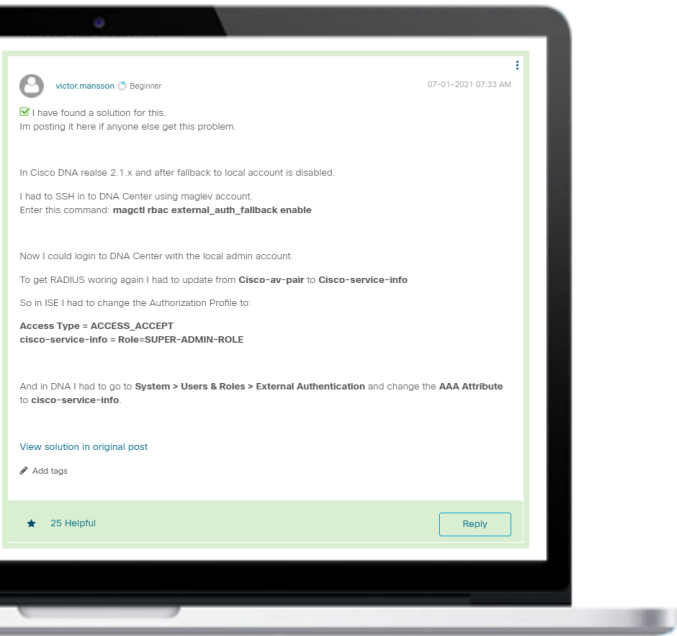
Stand out for your effort and commitment helping other members. Spotlight Awards highlight outstanding members. Be the next recipient!

Now you can also nominate a candidate!

[Click here](#)



Connect, Engage, Collaborate!



When you ask a Question and receive a correct Answer, **accept it as a solution!**

That helps other users find correct answers.

Accept as Solution

We all are sensitive to be highlighted.

Helpful votes motivate enthusiastic members by giving them a **token of recognition!**



25 Helpful

Our Expert



Luis Silva
Presenter



Scott Nishimura
Question Manager



Download the Presentation!

Polling Question 1

Do you know Cisco SecureX

- A. Yes
- B. No

SecureX

Click to add text



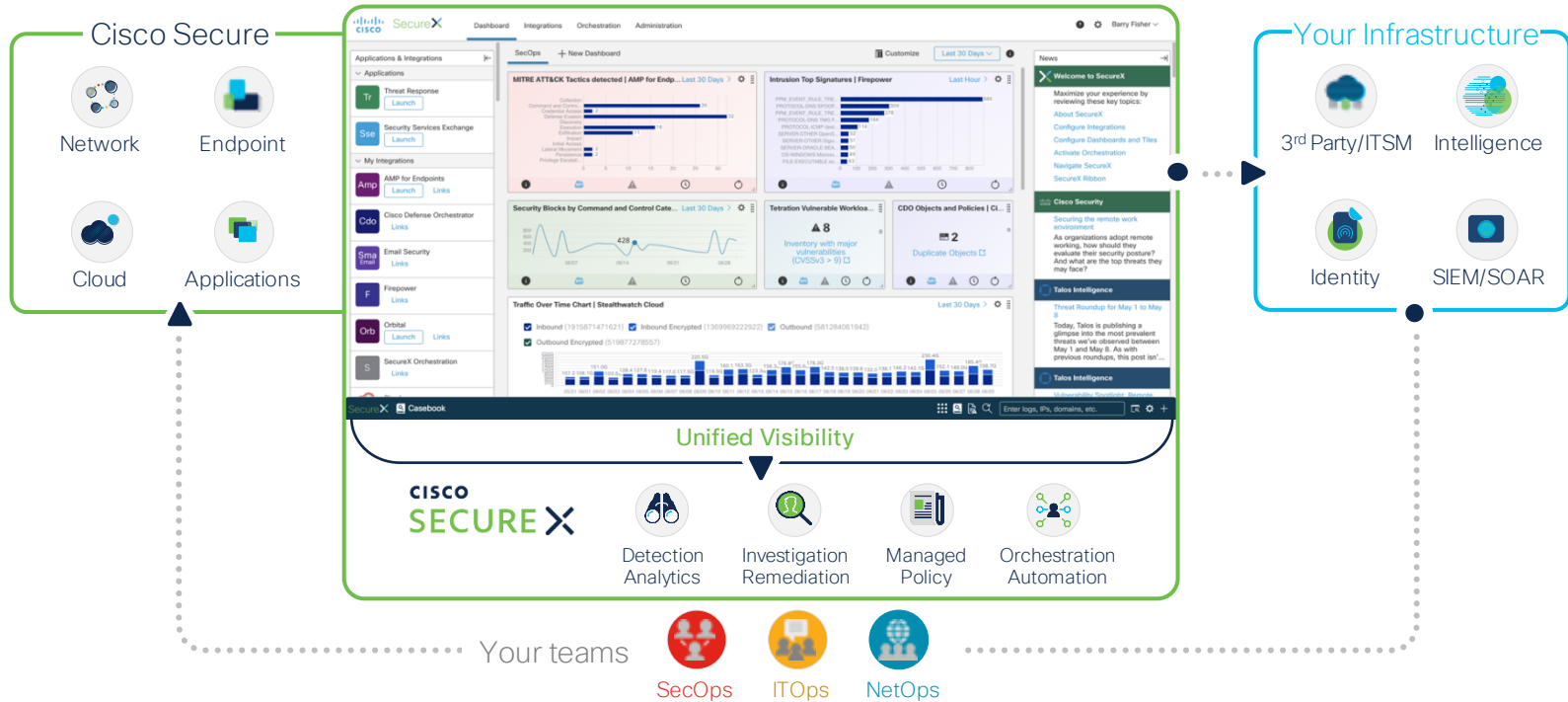
Luis Silva
Customer Success Specialist

Agenda

- 1 **SecureX overview**
- 2 Unify visibility with SecureX dashboard
- 3 Never lose context with SecureX ribbon
- 4 Experience simplicity with SecureX threat response
- 5 Maximize efficiency with SecureX orchestration

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 workflows²



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

Agenda

- 1 SecureX overview
- 2 Unify visibility with SecureX dashboard
- 3 Never lose context with SecureX ribbon
- 4 Experience simplicity with SecureX threat response
- 5 Maximize efficiency with SecureX orchestration

SecureX **sign-on**

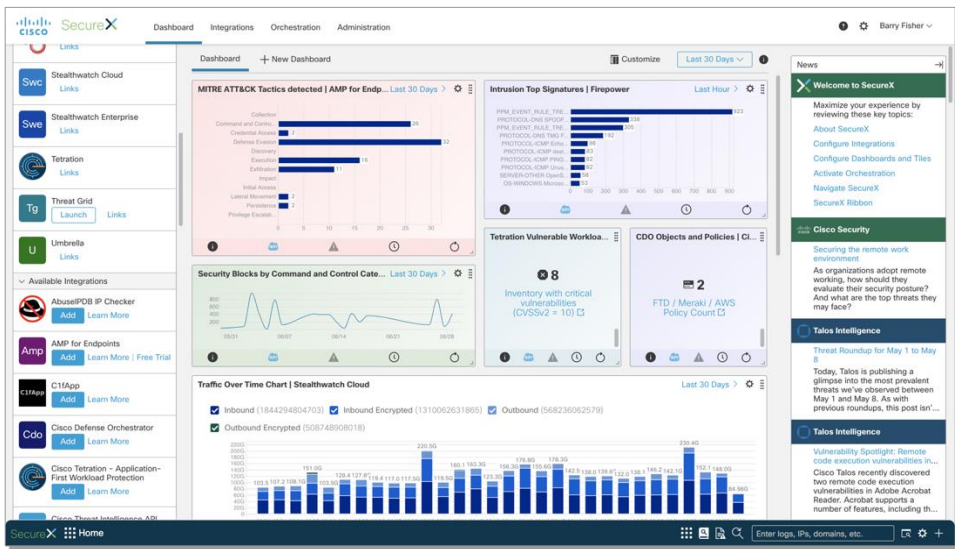
▼ **Adaptive**, layered and simplified authentication

▼ 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



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

Modules

SecureX threat response uses integration modules to integrate with Cisco Secure products and third-party tools.

Integration modules can provide enrichment and response capabilities.

The screenshot displays the Cisco SecureX Integration Modules dashboard. At the top, there are navigation tabs for Dashboard, Integration Modules (selected), Orchestration, and Administration. Below the navigation, there are two tabs: My Integration Modules and Available Integration Modules. The main content area is titled "Integration Modules" and includes a link to view all available modules. Under "Your Configurations", there are several module cards:

- AMP for Endpoints**: Integrated. Description: AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints. Buttons: Edit, Learn More.
- SecureX Orchestration**: Integrated. Description: The SecureX Orchestrator module provides the capability to automate security processes to strengthen SOC operational efficiency and precision. Buttons: Edit, Learn More.
- Stealthwatch Cloud**: Integrated. Description: Gain the visibility and continuous threat detection needed to secure your public cloud, private network, and hybrid environments. Buttons: Edit, Learn More.
- Farsight Security DNSDB**: Integrated. Description: 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... Buttons: Edit, Learn More.
- Gigamon ThreatINSIGHT**: Error. Description: Accelerate network detection and response with Gigamon ThreatINSIGHT - a cloud-native, high-velocity NDR solution. Buttons: Edit, Learn More.

Below this section is "Built in Integration Modules":

- AMP File Reputation**: Description: AMP File Reputation is the database that powers AMP file hash lookups. Button: Learn More.
- AMP Global Intelligence**: Description: AMP Global Intelligence is a repository of Cisco and third-party intelligence curated by Cisco engineers and researchers. Button: Learn More.
- Private Intelligence**: Description: Private Intelligence is a data storage facility built into CTR, to store the incidents that display in the Threat Response Incident Manager, Casebooks, Snapshots, and... Button: Learn More.
- Talos Intelligence**: Description: Talos is Cisco's industry-leading threat intelligence team that protects your organization's people, data and infrastructure from active adversaries. Button: Learn More.

At the bottom of the dashboard, there is a "Casebook" link.

Polling Question 2

Which security product do you use in your enterprise?

- A. Email security
- B. Firewalls
- C. Endpoints
- D. Cloud Security



SecureX integrations with Cisco Secure portfolio

Secure Endpoints

- Orbital
- Malware analytics

Umbrella

Secure Firewall

- Defense Orchestrator

Secure Email Appliance

Secure Web Appliance

Secure Cloud Analytics

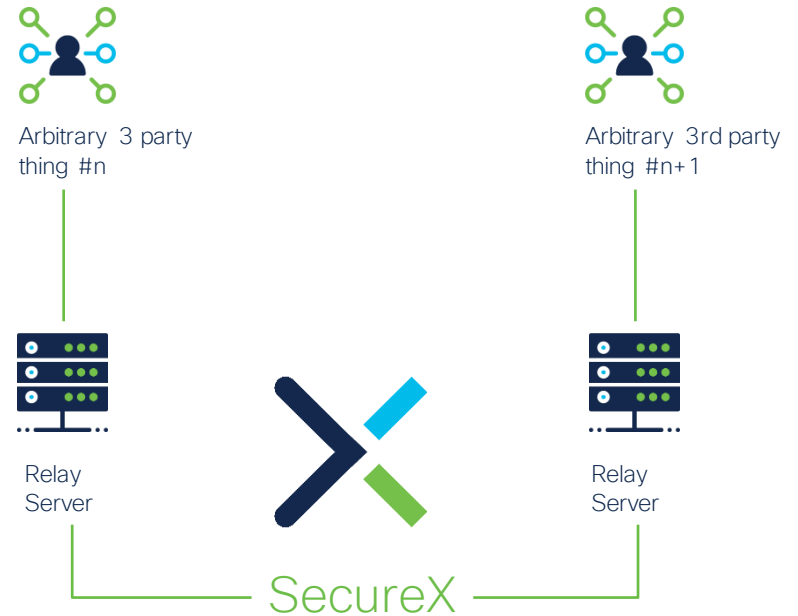
Secure Network Analytics

Secure Workload

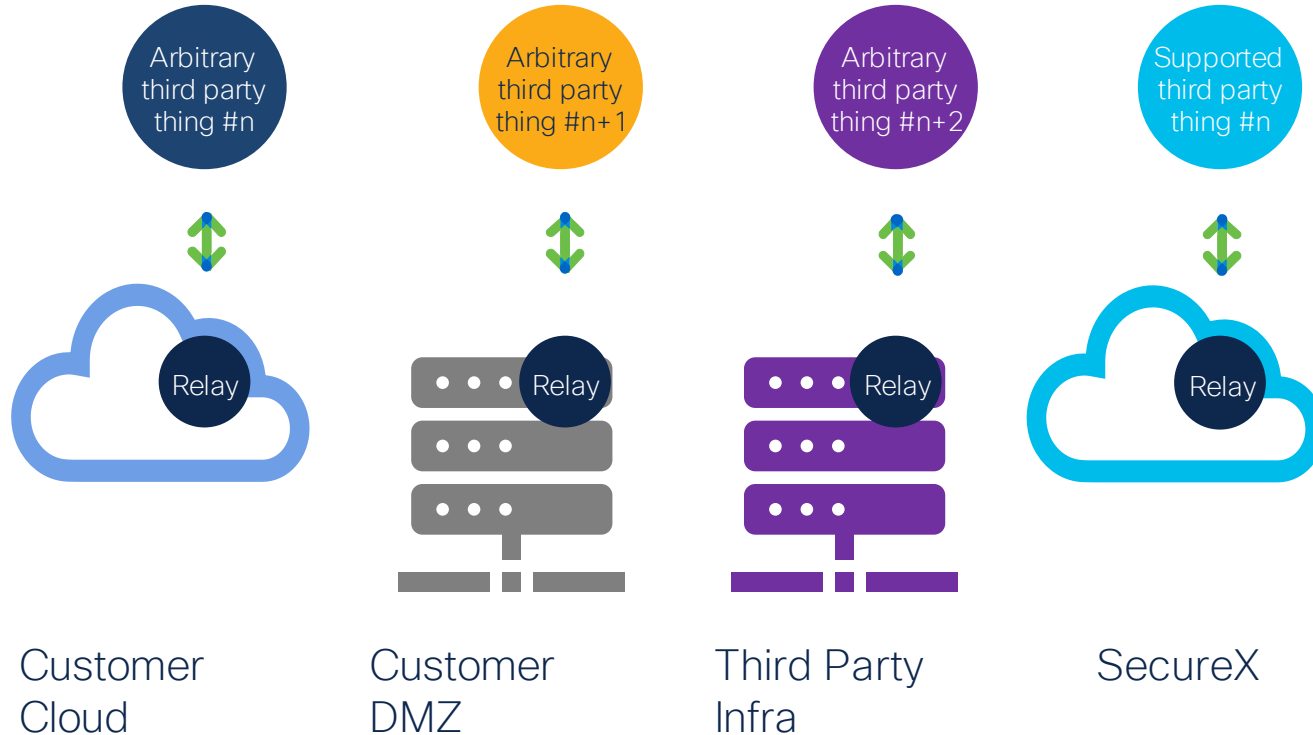


SecureX threat response: Relay modules

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



Where do the relay servers live?



SecureX threat response Relay modules



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

- ▶ [Many available by default \(examples below\)](#)
- ▶ [Write your own!](#)
- ▶ [Templates and examples available on Github](#)

- Abuse IPDB*
- APIVoid*
- CyberCrime Tracker*
- Cyberprotect Threatscore*
- Farsight Security
- Google Chronicle
- Google Safe Browsing
- Google VirusTotal*
- Have I Been Pwned*
- Microsoft Graph Security
- Pulsedive*
- SecurityTrails
- See One Feed App*
- SpyCloud
- urlscan.io*
- Gigamon ThreatINSIGHT
- Qualys IOC
- Radware WAF and DDoS
- Signal Sciences ▶▶▶
- AlienVault OTX*

Meaningful integrations with your investments not just a simple syslog data dump

Third-party security

Operational tools, intelligence sources, infrastructure protections and visibility

Cisco infrastructure

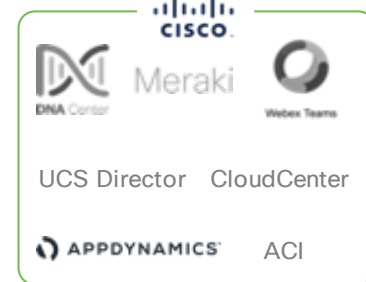
Networking, collaboration, server/app, and multicloud management platforms

Third-party infrastructure

IT service management, and cloud/virtual and DevOp platforms

General infrastructure

Scripting/dev tools, system interfaces, data exchanges, and messaging protocols



HTTP SMTP SNMP

...and more!

Agenda

- 1 SecureX overview
- 2 Unify visibility with SecureX dashboard
- 3 **Never lose context with SecureX ribbon**
- 4 Experience simplicity with SecureX threat response
- 5 Maximize efficiency with SecureX orchestration

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



Never lose **context** with SecureX ribbon



The screenshot displays the Cisco SecureX interface. The top navigation bar includes 'Incidents', 'New Incident', and 'Investigate Incident'. The main content area shows details for 'Intrusion event 1-48764-1', including a summary, observables, and targets. A sidebar on the left lists various incidents, and a right sidebar shows assignees and key properties.

Incidents	Assigned to me - Open (10)	Assigned to me - New (5)
Phishing Investigation for "FW: 2020 Tax... securex-orchestration Mar 16, 2021	Intrusion event 122-1-1 NGFW Event Service Mar 10, 2021	Intrusion event 1-48764-1 NGFW Event Service Mar 02, 2021
Security Intelligence event - DNS_SI_Ca... NGFW Event Service Nov 16, 2020	Security Intelligence event - IP_Reputati... NGFW Event Service Aug 13, 2020	Assigned to others - (143,007)

Intrusion event 1-48764-1
MALWARE-CNC Win.Trojan.Zebrocy variant outbound connection
New · Created By NGFW Event Service on 2021-03-02 23:02:37 UTC

Summary | **Observables** | Timeline | Sightings | Linked References (1)

Targets (1) · Investigate these Targets

- 192.168.243.116
IP · Targeted by 2 unique observables, 2 times in the last 2 months
IP Address · 192.168.243.116
First: 2021-03-02T22:54:41.000Z · Last: 2021-03-02T22:54:41.000Z

Incident Observables (3) · Investigate these Observables

- mta2.tixamail.com
Malicious Domain · 0 Targets · 0 Sightings
- 89.37.226.148
Malicious IP Address · 1 Target · 1 Sighting
First: 2021-03-02T22:54:41.000Z · Last: 2021-03-02T22:54:41.000Z

Info

Assignees · Add

- Aditya Sankar
- Eric Howard SSO
- Eric Howard
- Jamey Heary
- Jamey Heary

Key Properties

- Categories: Select ...
- Disc. Method: NIPS
- Intend. Effect: Select ...
- Confidence: Medium
- TLP: Amber

Agenda

- 1 SecureX overview
- 2 Unify visibility with SecureX dashboard
- 3 Never lose context with SecureX ribbon
- 4 Experience simplicity with SecureX threat response
- 5 Maximize efficiency with SecureX orchestration
- 6 Get contextual awareness with SecureX device insights
- 7 Next step and resources
- 8 Appendix

How true **simplicity** is experienced

Before: 32 minutes

1. IOC/alert



2. Investigate incidents in multiple consoles

Product dashboard 1



Product dashboard 2



Product dashboard 3



Product dashboard 4



3. Remediate by coordinating multiple teams

Product dashboard 1



Product dashboard 2



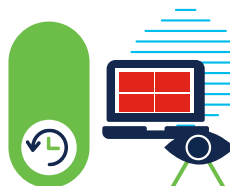
Product dashboard 3



Product dashboard 4

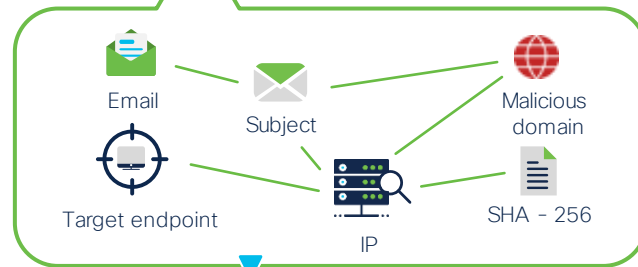


After: 5 minutes



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

Metrics Bar

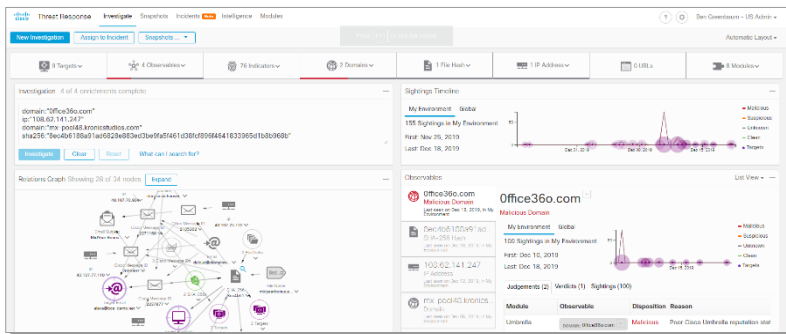
Investigation Timeline

Observable Details Panel

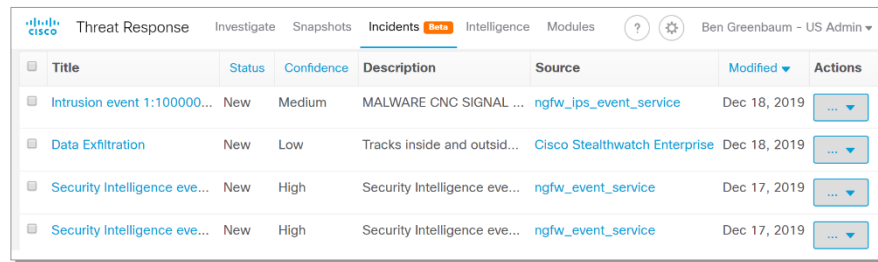
Use cases

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

Investigate with intelligence, context and response

SecureX threat response

Intelligence



Endpoint security
Malware intelligence
Internet intelligence



VirusTotal and
other 3rd parties

Are these observables
suspicious or malicious?

Local security context



Endpoint security



Email security



Analytics



Cloud security



Network firewall



Secure Web
Appliance

Have we seen these observables? Where?
Which endpoints connected to the domain/URL?

Response actions

Block destinations

Block files

Isolate hosts

What can I do about
it right now?

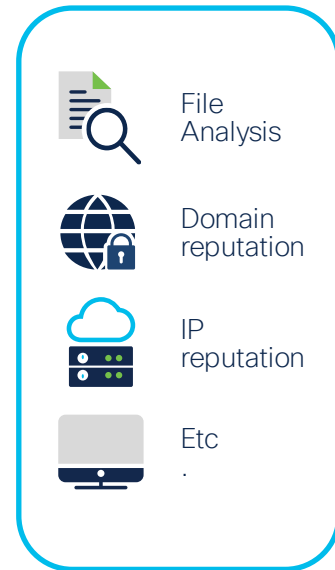
Observables: 1) File hash, 2) IP address, 3) Domain, 4) URL, 5) Email addresses, etc..

Enrichment

The process of consulting all the modules to find out what any of them know about the observable(s).



SecOps

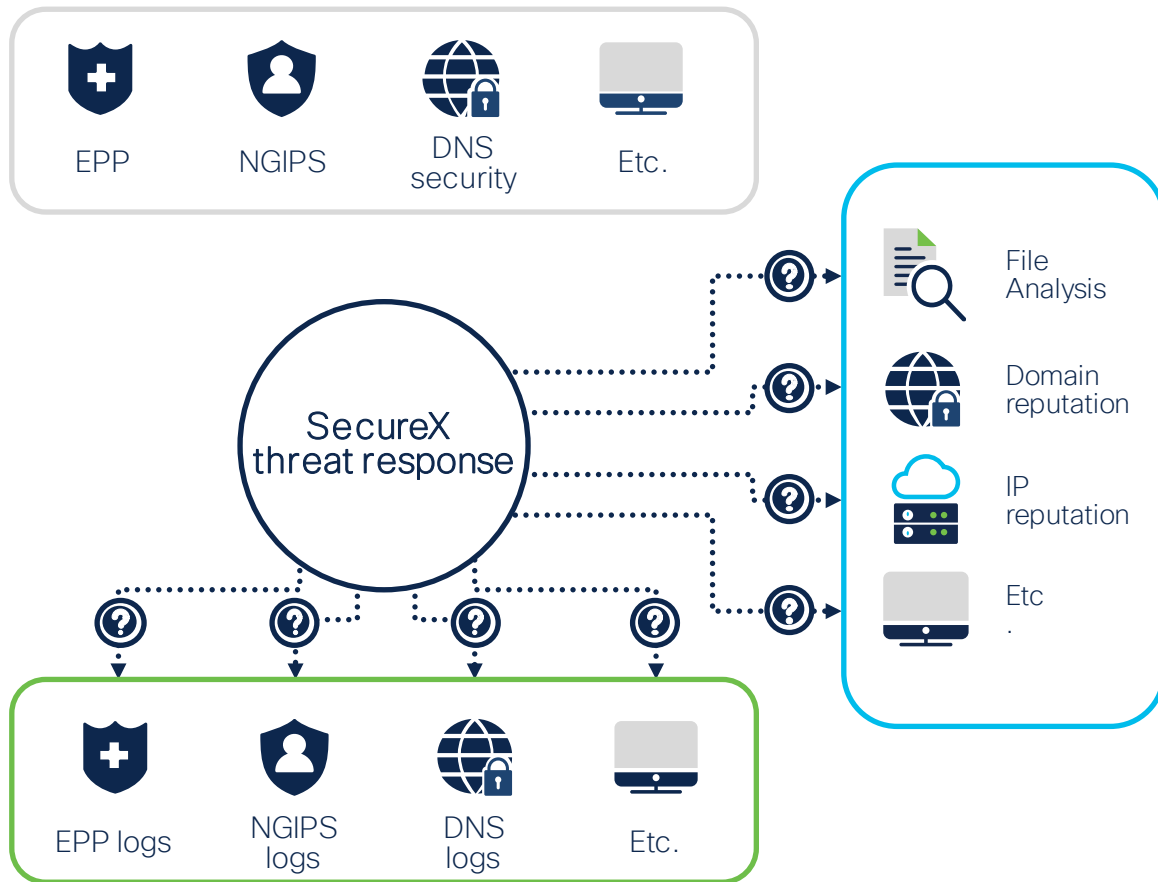


Enrichment

The process of consulting all the modules to find out what any of them know about the observable(s).



SecOps

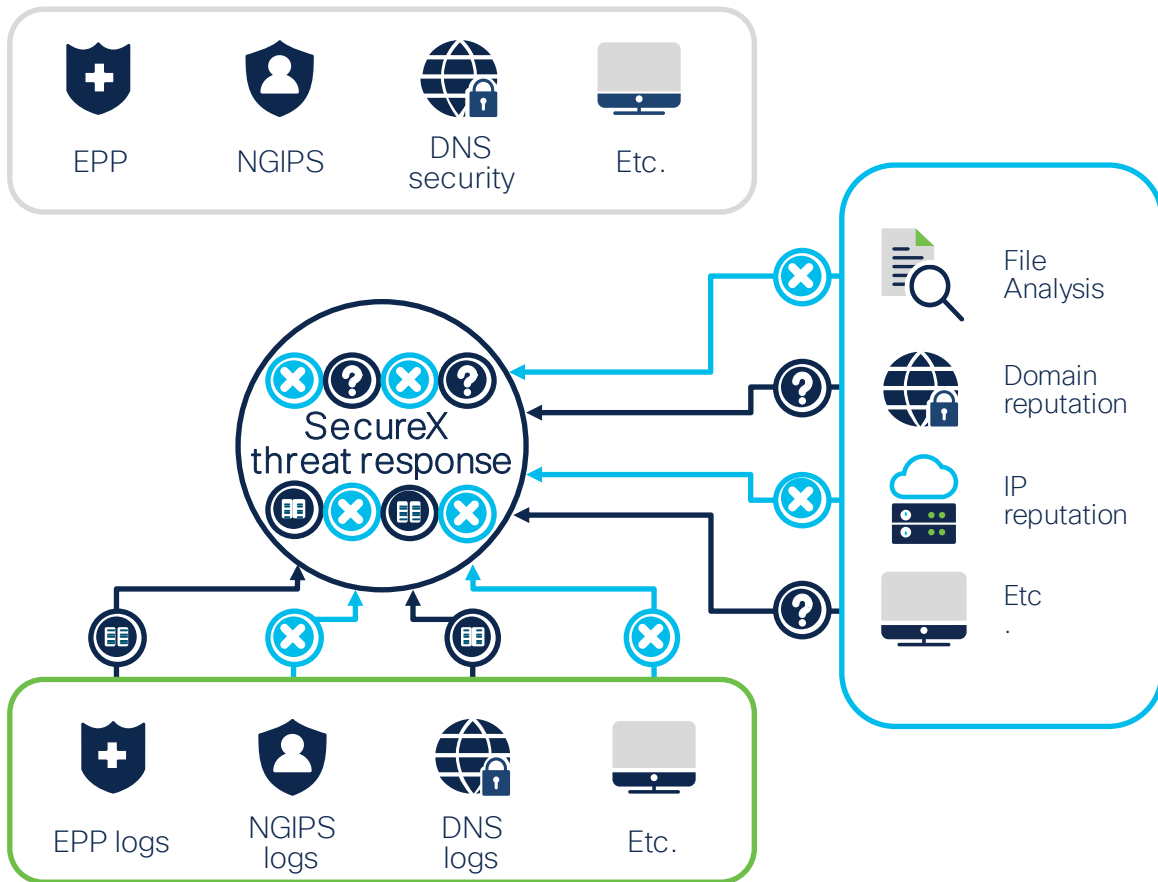


Enrichment

The process of consulting all the modules to find out what any of them know about the observable(s).

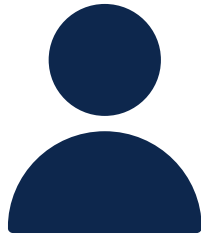


SecOps

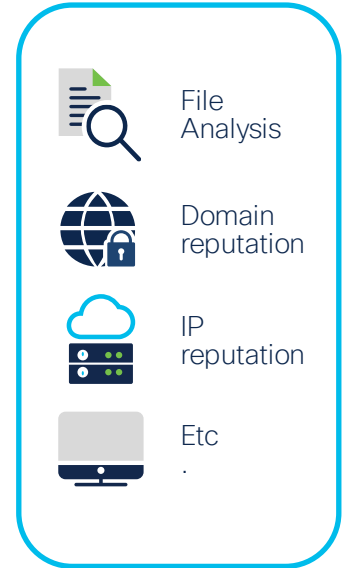


Response

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



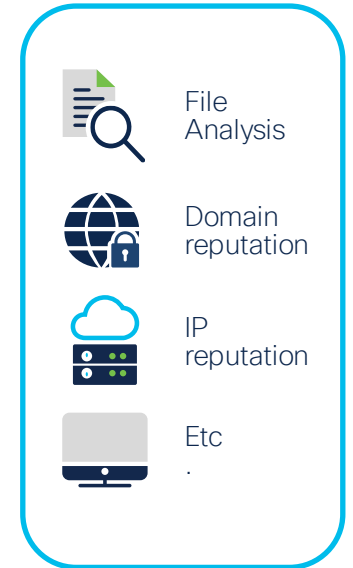
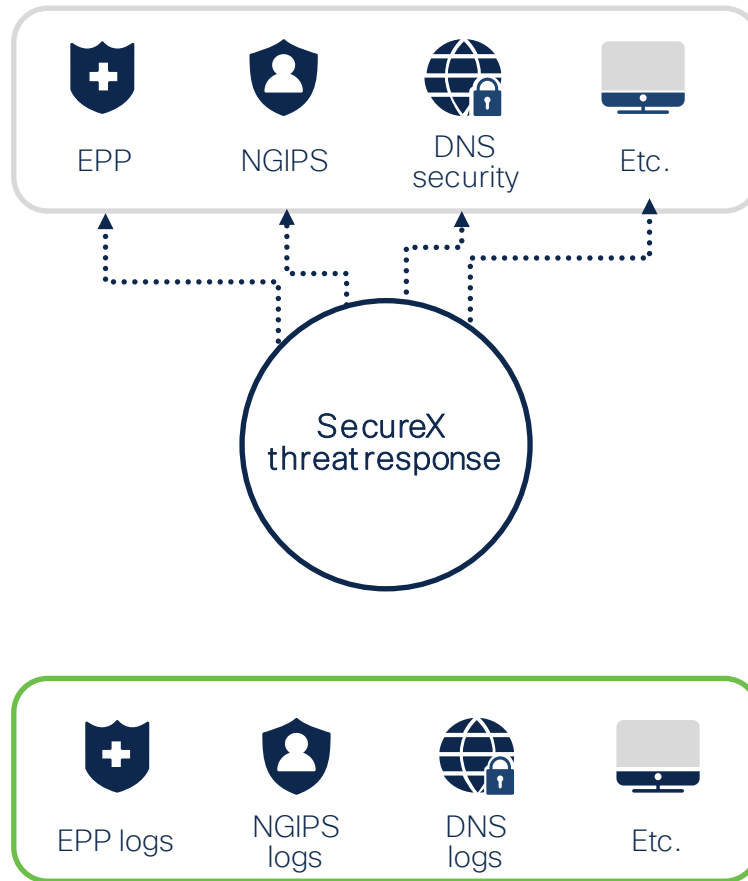
SecOps



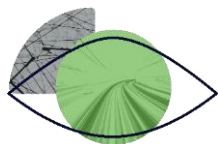
Response



SecOps



Record-keeping



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

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

Polling Question 3

Are you familiar with SecureX
Orchestration ?

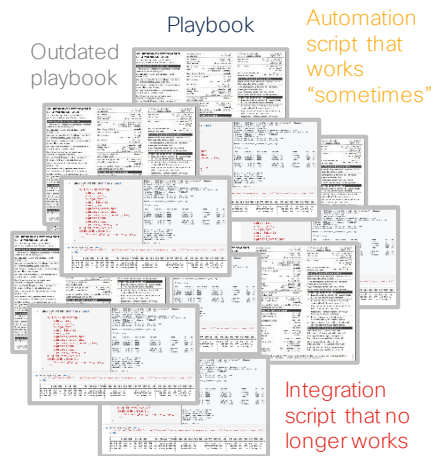
- A. Yes
- B. No

Agenda

- 1 SecureX overview
- 2 Unify visibility with SecureX dashboard
- 3 Never lose context with SecureX ribbon
- 4 Experience simplicity with SecureX threat response
- 5 **Maximize efficiency with SecureX orchestration**

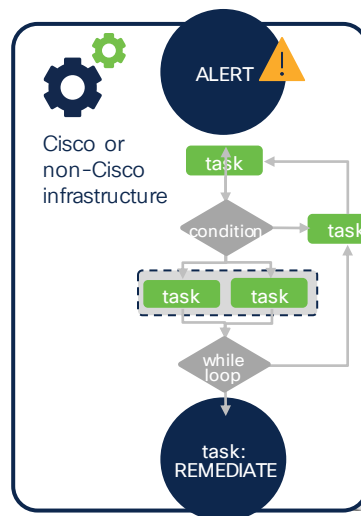
Maximizing operational **efficiency**

Before: Repetitive, human-powered tasks



Solution: Orchestrating security across the full lifecycle

Pre-built or customizable workflows



After: I combined **9 tasks** across 3 security tools, 2 infrastructure systems, and 3 teams in **one keystroke!**

“

I make automated playbook changes in minutes with a drag-drop interface

We have never communicated faster: Our approvals are automated

My top 5 most frustrating tasks have all be automated



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

The screenshot displays the SecureX orchestration interface for a workflow titled "Move Computer to AMP Triage Group". The workflow is visualized as a flowchart on a grid background. It starts with a decision diamond: "WHICH OBSERVABLE TYPE WAS PROVIDED?". This leads to four parallel paths: "IP ADDRESS", "HOSTNAME", "AMP GUID", and "SOMETHING ELSE". Each path contains a "CORE Set local variable" task. These paths converge into a second decision diamond: "DO WE NEED TO FETCH AN AMP GUID?". The "YES" path leads to an "ATOMIC AMP - Get Connector GUID" task, followed by a "CORE Set local variable" task. The "NO" path bypasses this. Both paths then lead to an "ATOMIC AMP - Get Group by Name" task, followed by an "ATOMIC AMP - Move Computer to Group" task, and finally an "END" node. The interface includes a left-hand navigation menu with categories like "CORE", "AWS SERVICE", "APPD", and various Cisco products. The top right shows workflow status: "Modified April 6, 2021 at 11:11:44 AM", "VALIDATED", "COMMIT", "VIEW RUNS", "RUN", and "X". The right-hand panel shows the workflow's properties, including version, git repository, and description.



Automation vs orchestration



Automation

The ability to perform individual, repetitive tasks.

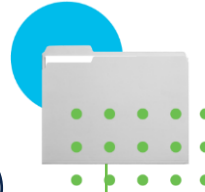
Why do customers want to automate?

“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.”

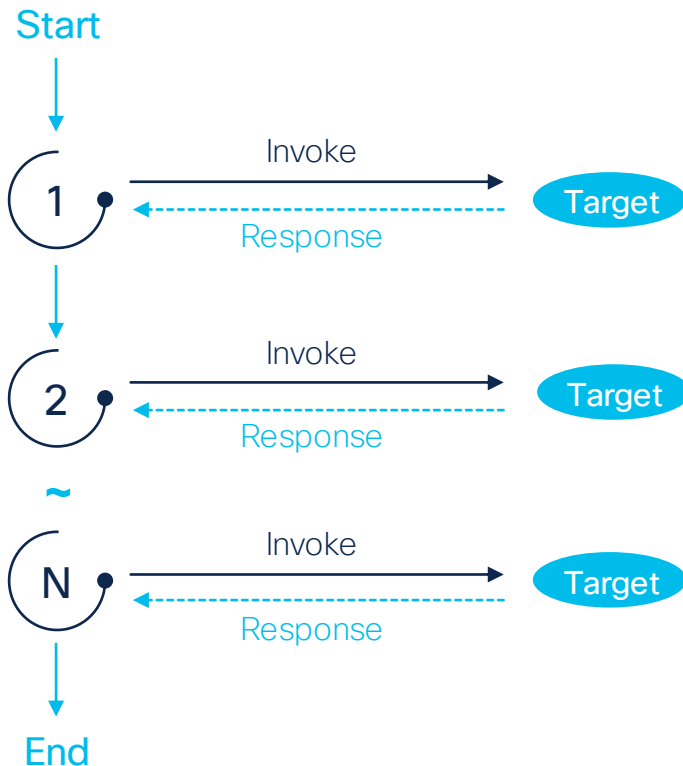
“Vendors offer many management tools – some do provisioning of services, others do monitoring – why can’t they be tied together as a solution?”

SecureX orchestration Remote

Available with SecureX release 1.73

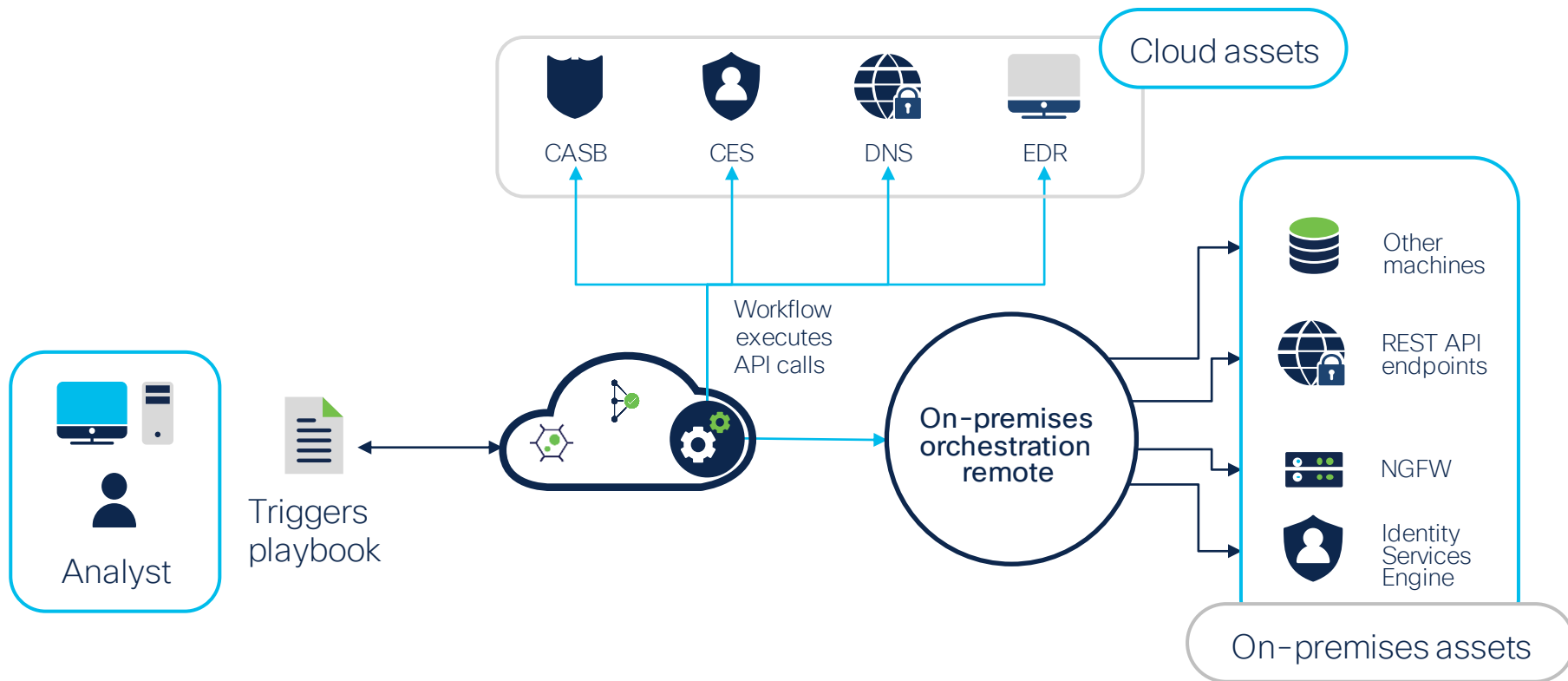
- Orchestration remote extends SaaS delivered functionality to your on-premise infrastructure
- Downloadable OVF deployment runs on VMware ESXi 5.5+
- Communicates with SecureX Orchestration over TCPS port 8883 – regional presence
- Use included atomics & workflows
... or create custom ones!

Benefits: Using orchestration remote the power of SecureX orchestration is extended to your on-premise infrastructure



* HTTP / REST Targets are supported at this time with more to be added in the future

SecureX orchestration



References to continue learning

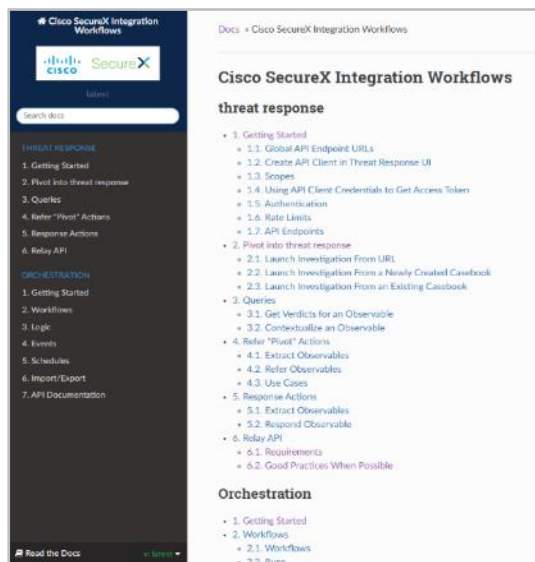
- cisco.com/go/securex
- cs.co/SecureX_videos
- SecureX session at CiscoLive on-demand: cs.co/SecureX_CiscoLive
- SecureX Academy: <https://learnsecurex.cisco.com>



Resources

Integration documentation

cs.co/SecureX_integration_workflows



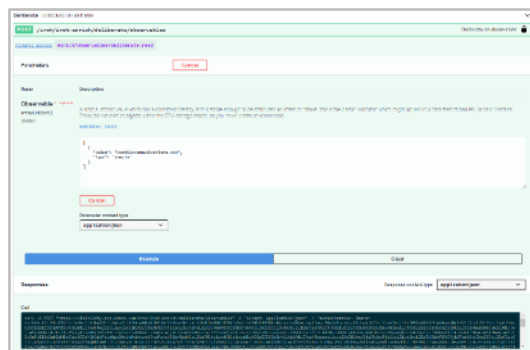
The screenshot shows the Cisco SecureX Integration Workflows documentation page. The page is titled "Cisco SecureX Integration Workflows" and is categorized under "threat response". The main content is a list of articles organized into three sections: "Threat Response", "Orchestration", and "Relay API".

- 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. Inq
 - 4. Events
 - 5. Schedules
 - 6. Import / Export
 - 7. API Documentation
- Relay API**
 - 1. Getting Started
 - 2. Create API Client in Threat Response UI
 - 3. Scopes
 - 4. Using API Client: Credentials to Get Access Token
 - 5. Authentication
 - 6. Rate Limits
 - 7. API Endpoints

The page also includes a search bar and a "Read the Docs" button at the bottom left.

UI docs and proto tools

github.com/threatgrid/ctim/tree/master/doc



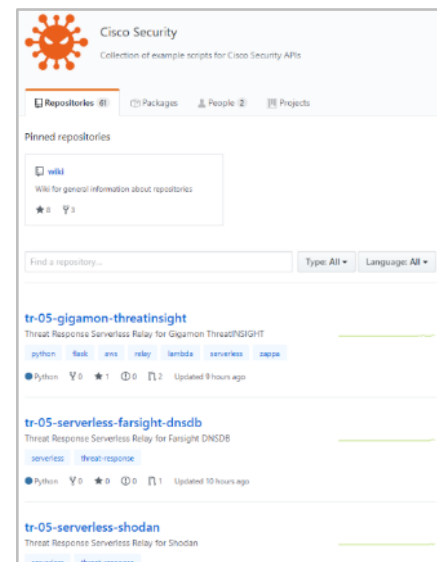
The screenshot shows the Threat Response UI documentation page. The page is titled "Threat Response UI" and is categorized under "UI docs and proto tools". The main content is a list of articles organized into three sections: "Threat Response", "Orchestration", and "Relay API".

- Threat Response**
 - 1. Getting Started
 - 2. Create API Client in Threat Response UI
 - 3. Scopes
 - 4. Using API Client: Credentials to Get Access Token
 - 5. Authentication
 - 6. Rate Limits
 - 7. API Endpoints
- Orchestration**
 - 1. Getting Started
 - 2. Workflows
 - 3. Inq
 - 4. Events
 - 5. Schedules
 - 6. Import / Export
 - 7. API Documentation
- Relay API**
 - 1. Getting Started
 - 2. Create API Client in Threat Response UI
 - 3. Scopes
 - 4. Using API Client: Credentials to Get Access Token
 - 5. Authentication
 - 6. Rate Limits
 - 7. API Endpoints

The page also includes a search bar and a "Read the Docs" button at the bottom left.

GitHub

github.com/CiscoSecurity



The screenshot shows the Cisco Security GitHub repository page. The page is titled "Cisco Security" and is categorized under "GitHub". The main content is a list of repositories organized into three sections: "Threat Response", "Orchestration", and "Relay API".

- Threat Response**
 - 1. Getting Started
 - 2. Create API Client in Threat Response UI
 - 3. Scopes
 - 4. Using API Client: Credentials to Get Access Token
 - 5. Authentication
 - 6. Rate Limits
 - 7. API Endpoints
- Orchestration**
 - 1. Getting Started
 - 2. Workflows
 - 3. Inq
 - 4. Events
 - 5. Schedules
 - 6. Import / Export
 - 7. API Documentation
- Relay API**
 - 1. Getting Started
 - 2. Create API Client in Threat Response UI
 - 3. Scopes
 - 4. Using API Client: Credentials to Get Access Token
 - 5. Authentication
 - 6. Rate Limits
 - 7. API Endpoints

The page also includes a search bar and a "Read the Docs" button at the bottom left.

SecureX threat response resources

DevNet

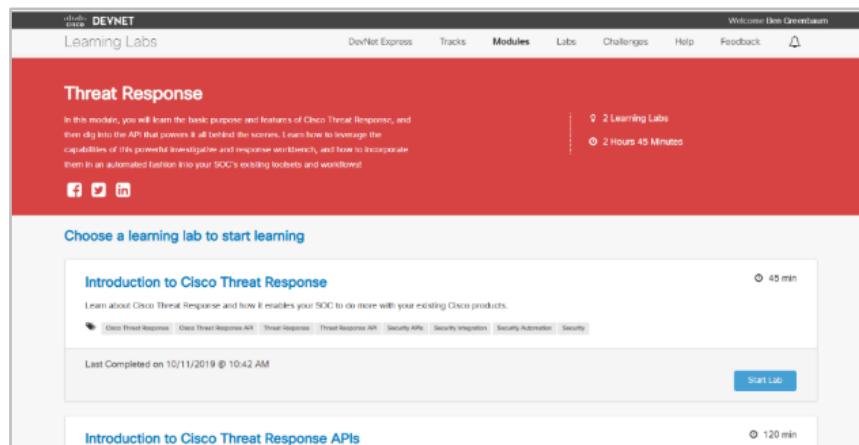
- developer.cisco.com/threat-response/
- cs.co/SecureX_integration_workflows



The screenshot shows the DevNet website 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 large heading 'SecureX threat response' and a sub-heading 'Cisco's 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.' Below this is a 'Read the docs' button. At the bottom, there are three cards: 'BLOG: Harvesting Threat Intelligence with the SecureX Threat...', 'BLOG: SecureX Threat Response Ecosystem', and 'NEW LEARNING TRACK: Introduction to SecureX'. A question 'What can you do with SecureX threat response APIs?' is displayed at the bottom of the page.

DevNet learning labs

- cs.co/CTR-API-labs



The screenshot shows the 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 'Notifications'. The main content area features a large heading 'Threat Response' and a sub-heading 'In this module, you will learn the basic purpose and features of Cisco Threat Response, and even dig into the API that powers it. All behind the scenes. Learn how to leverage the capabilities of its powerful intelligence and response workflows, and how to incorporate them in an automated fashion into your SOC's existing toolsets and workflow.' Below this is a 'Choose a learning lab to start learning' section with two lab cards: 'Introduction to Cisco Threat Response' (45 min) and 'Introduction to Cisco Threat Response APIs' (120 min). The 'Introduction to Cisco Threat Response' card shows a progress bar and a 'Start Lab' button.

SecureX orchestration resources

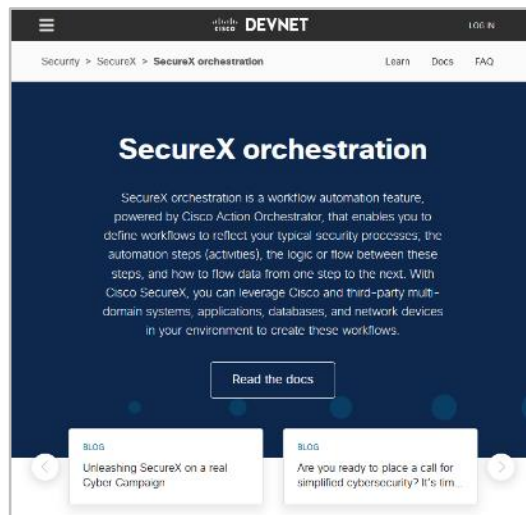
Videos

cs.co/SXO_videos



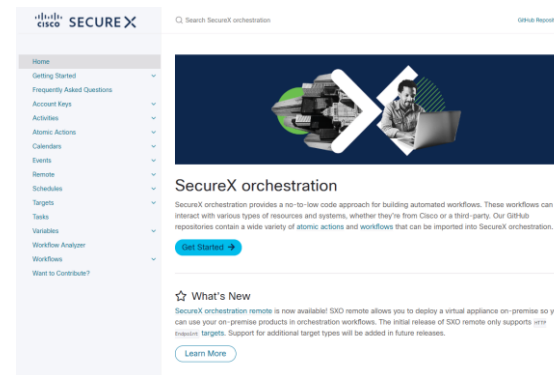
DevNet

developer.cisco.com/securex/orchestration



GitHub

cs.co/SXO_docs





THANK YOU

Submit Your
Questions Now!



Use the Q&A panel to submit your questions,
our expert will respond

Ask Me Anything following the event

Now through Friday
January 28th, 2022

With
Luis Silva

<https://bit.ly/ama-securex>



Luis Silva

Customer Success Specialist
CCIE #36825



A low-angle photograph of a man in a light-colored checkered shirt and tie, looking down at a tablet computer. He is standing in an urban environment with a large stone archway on the left, a classical fountain in the foreground, and modern buildings in the background under a bright sky with lens flare.

Do you have any Comments?

Take our Survey!



The bridge to possible