

ALL
IN

CISCO *Live!*

DevNet Zone



The bridge to possible

SecureX All The Things

With Hosted and Remote Relays

Matt Vander Horst
Technical Leader, SecureX
DEVNET-1483



DevNet Zone

#CiscoLiveAPJC

Cisco Webex App

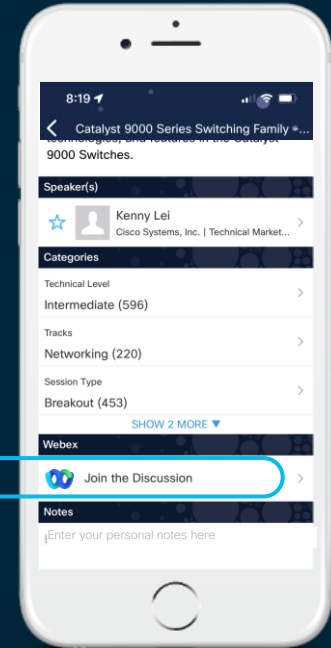
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until Thursday 22 December, 2022.





Agenda

- Introduction
- SecureX Tour
- Relays, Modules, and Relay Modules
- Demo
- Conclusion

Introduction



Matt Vander Horst

- 8 years at a Fortune 100 insurance company
 - Network engineering
 - Cisco ISE
 - DevOps
- 2.5 years at Cisco
 - SecureX
 - Automation and orchestration



SecureX Tour



Security Operations challenges

- Overwhelmed with alerts from disparate security products
- SOC's are understaffed
- Unable to keep pace with current threats



65% of organizations
report a shortage of cybersecurity staff



1.3 million
positions unfulfilled*

The security industry isn't making it any easier

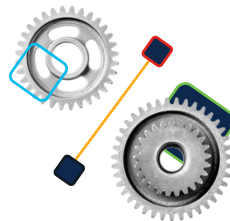
CISCO *Live!*

DevNet Zone



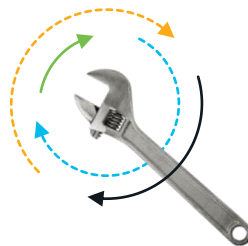
Vast security market

3,000+ Cybersecurity vendors¹



Siloed solution sets

75 security tools on average²

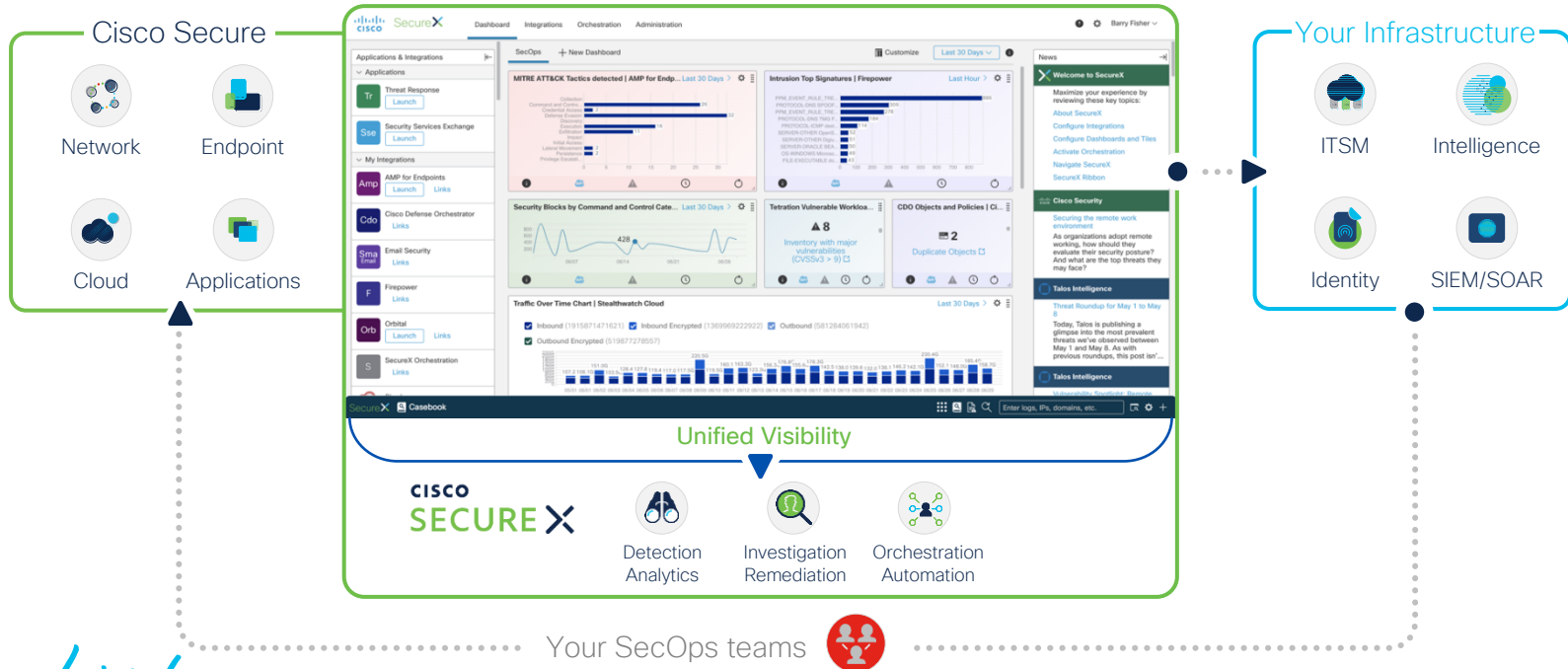


Reduced effectiveness

79% of CISOs say it's difficult to orchestrate alerts³

Introducing Cisco SecureX

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



SecureX is a **cloud-native** security platform



Integrated
and open for
simplicity



Unified in one
location for
visibility



Maximized
operational
efficiency



integrations
built-in, pre-built
or custom

ribbon
never leaves you
maintains context

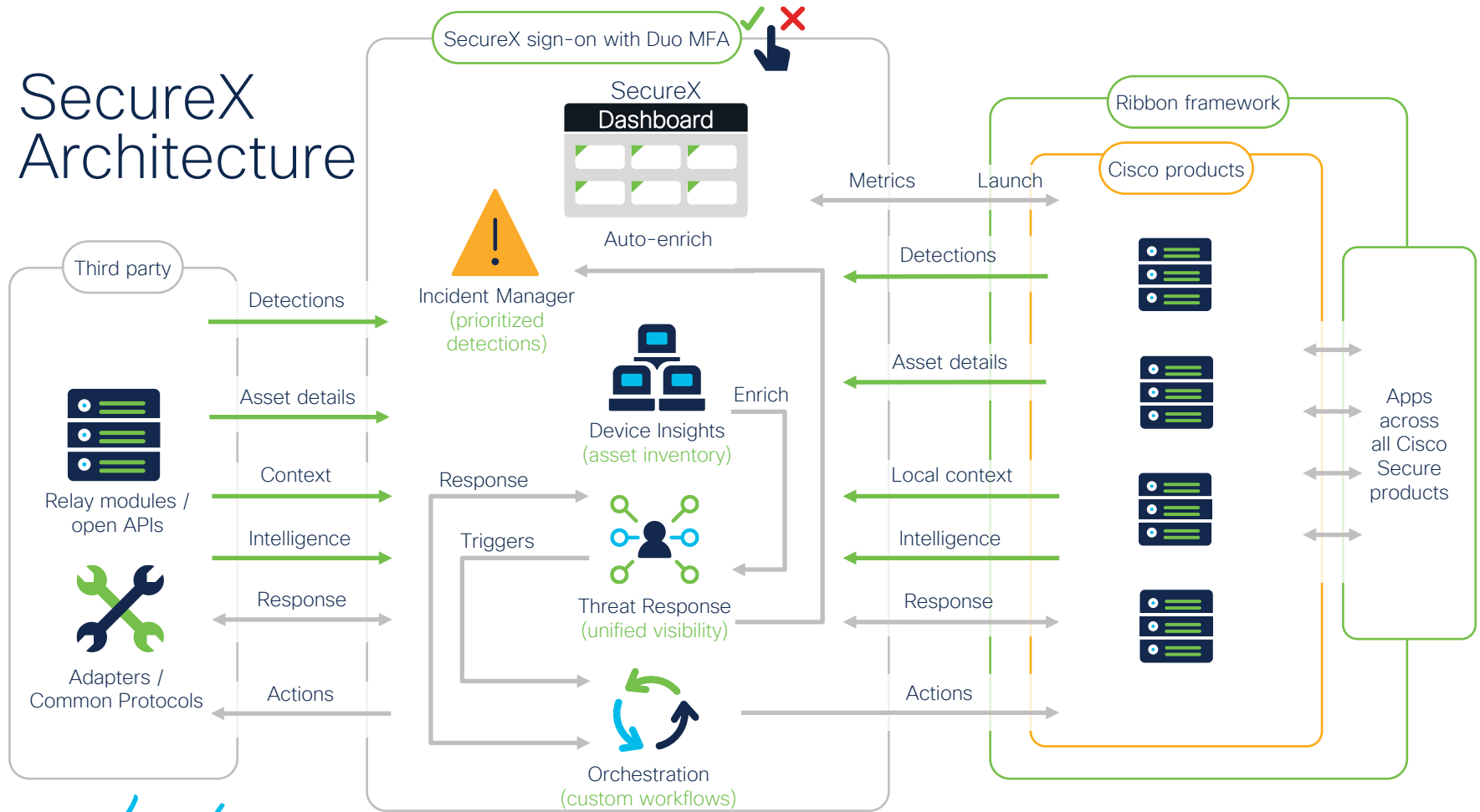
dashboard
customizable for what
matters to you

threat response
is at the core
of the platform

orchestration
drag-drop GUI
for no/low code

insights
device inventory with
contextual awareness

SecureX Architecture



How does it work?

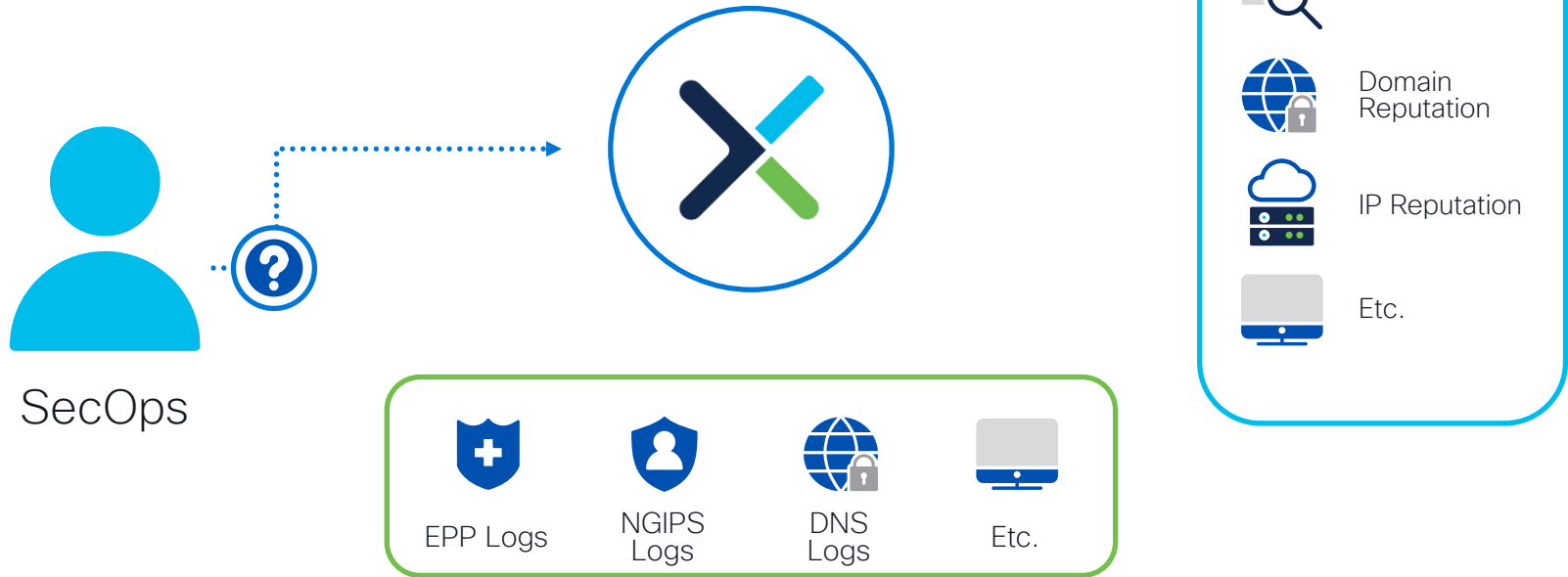


ALL THE APIs!

- SecureX aggregates information from the APIs of integrated products
- Most of this is done in real time
 - We're not a SIEM
- Every product speaks a different language, but we speak CTIM
 - Cisco Threat Intelligence Model
 - Relays handle translation

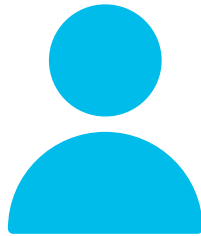
Enrichment Demo

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

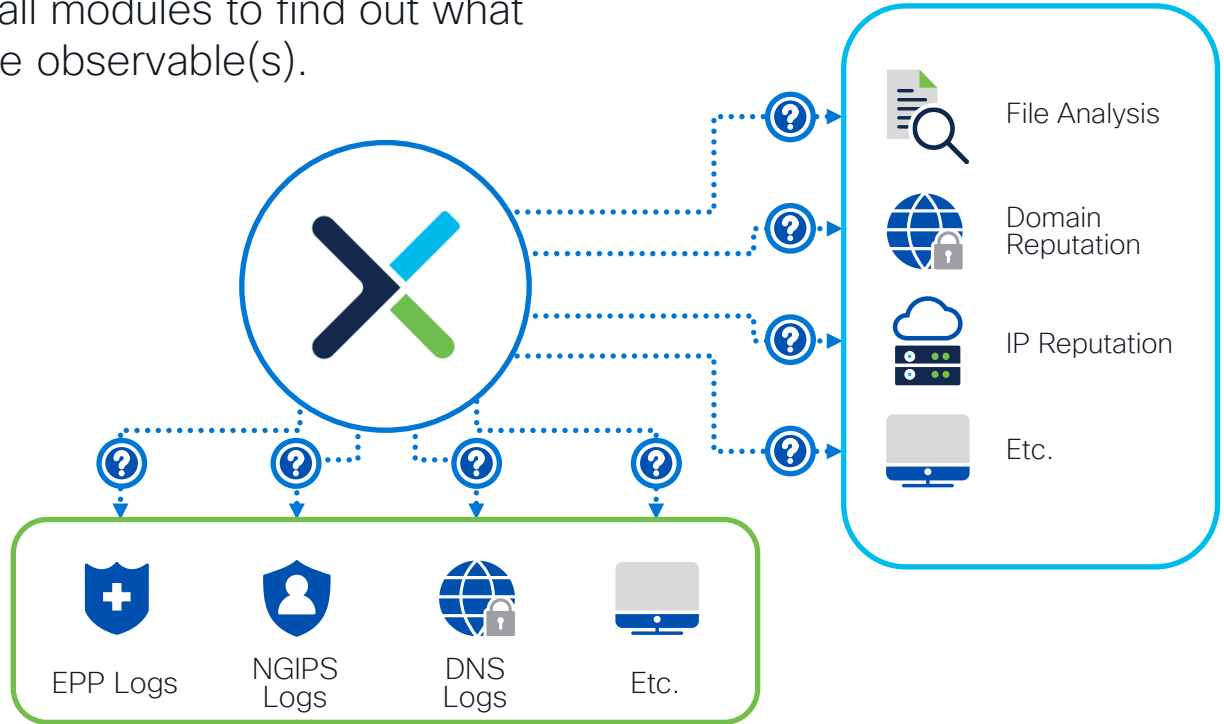


Enrichment Demo

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

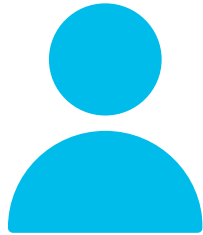


SecOps

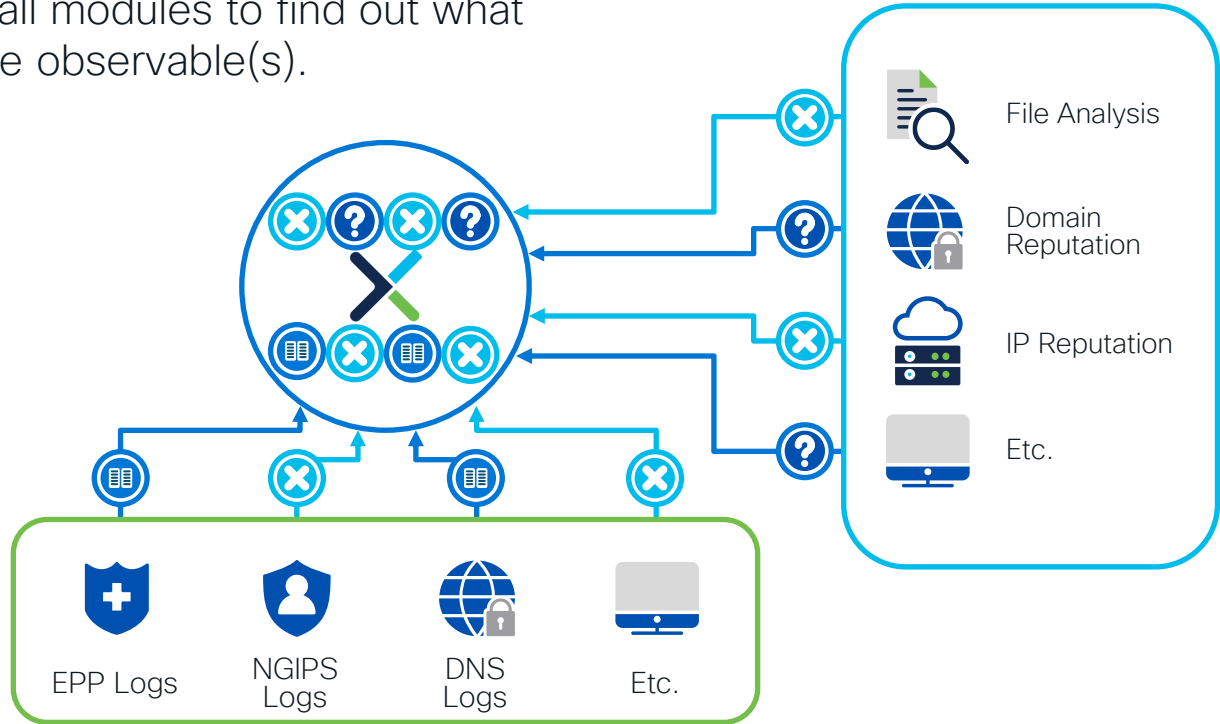


Enrichment Demo

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

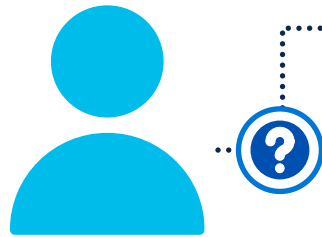


SecOps



Response

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



SecOps



EPP



NGIPS



DNS
security



Etc.



EPP Logs



NGIPS
Logs



DNS
Logs



Etc.



File Analysis



Domain
Reputation



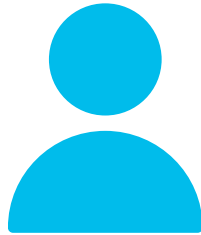
IP Reputation



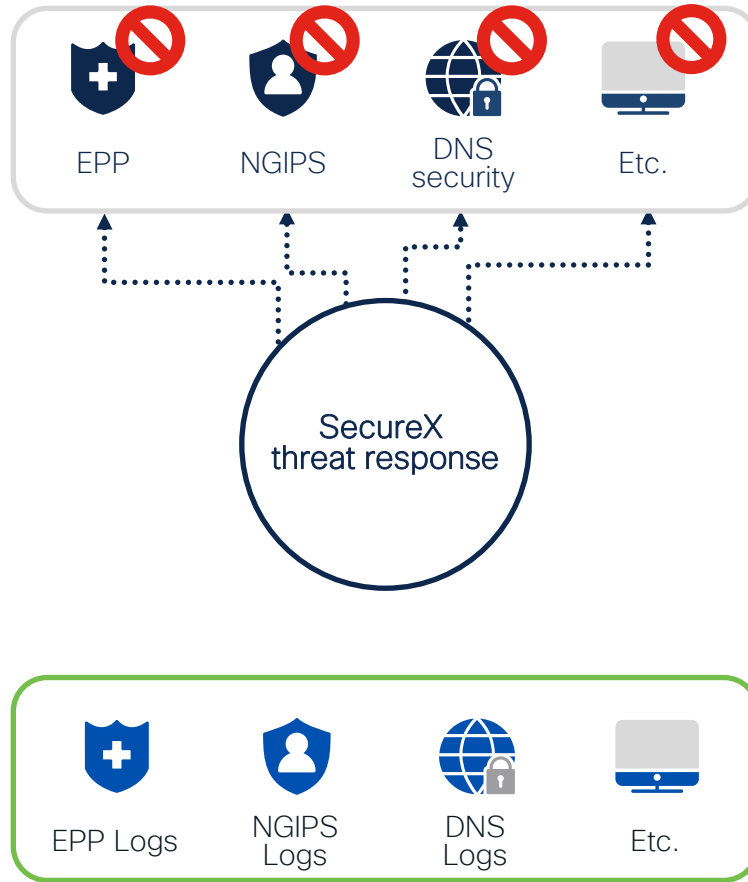
Etc.

Response

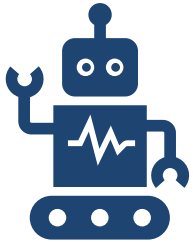
The process of leveraging the capabilities of SecureX-enabled technologies to mitigate threats by acting on observables or targets.

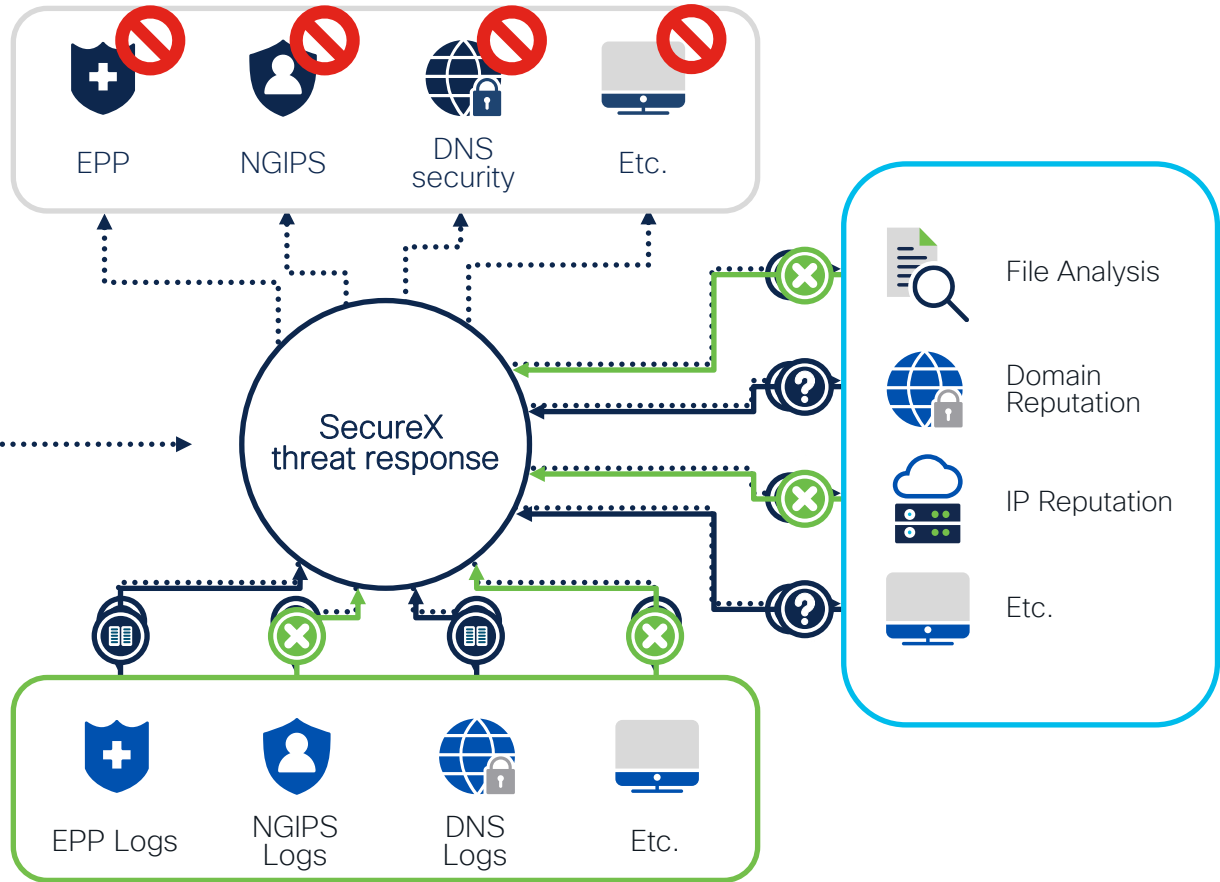


SecOps

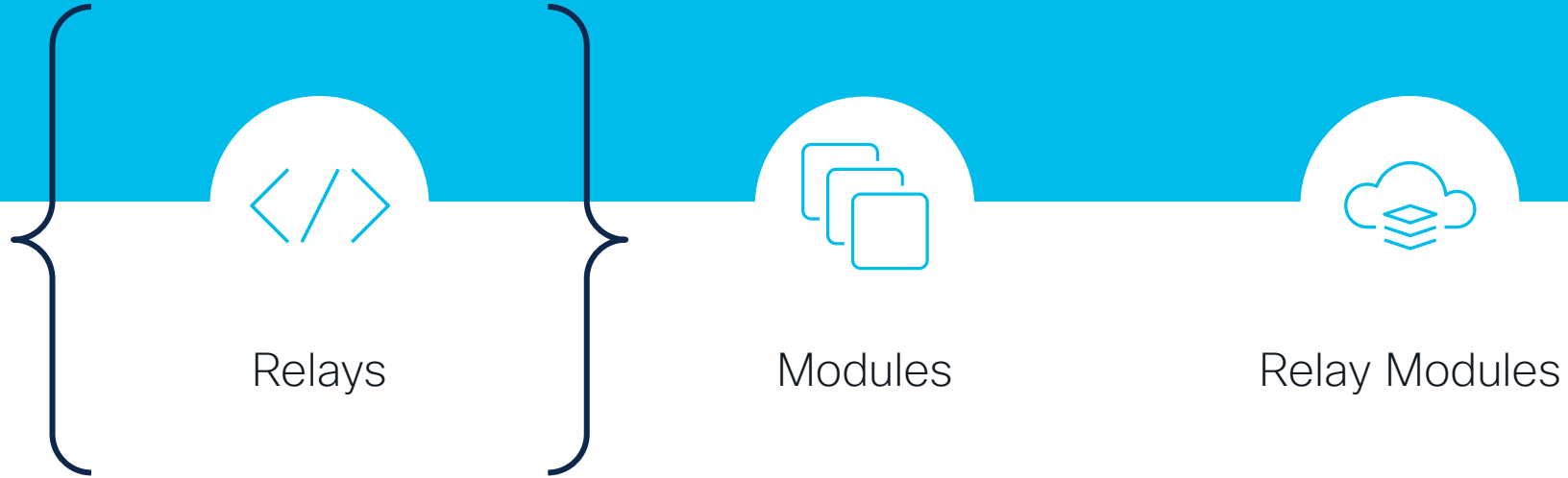


Using APIs


Automation
including
SecureX Orchestration



What enables SecureX integrations?



Relays

- HTTP-based APIs that can translate between CTIM and another product
 - Reminder: Cisco Threat Intelligence Model
- Allow integrated products to be asked questions they can understand
- Allow SecureX to understand the responses it receives

Relays

*This capability can't be used by non-Cisco-published modules



- A relay API's capabilities can include:
 - Dashboard
 - Deliberation
 - Device Insights*
 - Enrichment
 - Health Check
 - Reference Links
 - Response Actions
- These must match what the module is configured for (more on that later)

Side by Side

Umbrella API

```
[
  {
    "amazon.com": {
      "status": 1,
      "security_categories": [],
      "content_categories": [ 8 ]
    }
  }
]
```

Cisco Threat Intelligence Model

```
{
  "type": "verdict",
  "disposition": 1,
  "observable": {
    "value": "amazon.com",
    "type": "domain"
  },
  "disposition_name": "Clean",
  "valid_time": ...
}
```


Who can create relays?



Cisco



Customers
Partners
Third-Parties
You??

Yes, you can write your own relays!

[Dashboard](#)[Integration Modules](#)[Orchestration](#)[Administration](#)[My Integration Modules](#)[Available Integration Modules](#)

Integration Modules

SecureX uses integration modules to integrate with other Cisco security products and third-party solutions. [Click here to view all the available integration modules.](#)

Your Configurations



Add New Integration Module



Threat Grid
Threat Grid

✓ Integrated

Cisco Threat Grid combines advanced sandboxing with threat intelligence into a powerful solution to protect organizations from malware.

[Edit](#)[Learn More](#)

Unsupported 3rd Party Thing ✓ Integrated
Generic Serverless Relay

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

[Edit](#)[Learn More](#)

Where can relay APIs live?



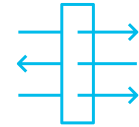
Within SecureX's
Infrastructure
aka "Hosted"



Public Cloud



Customer Cloud



Customer DMZ

"Remote"

*Need to be accessible via the internet!

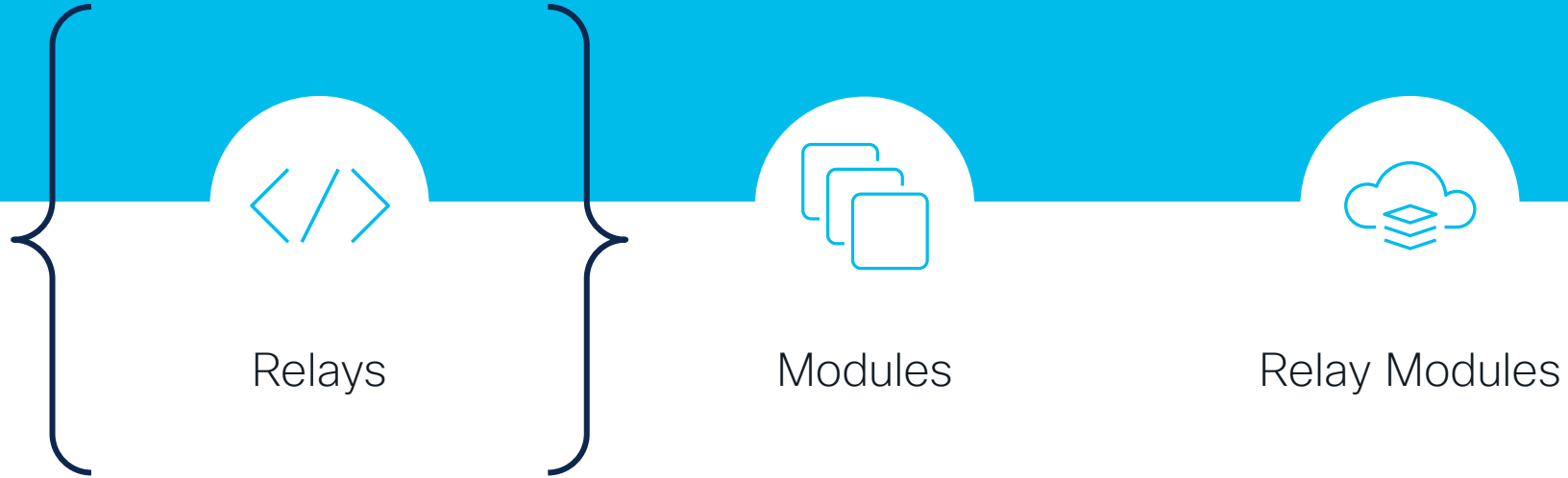
What can relay APIs be?

- An AWS Lambda or other serverless resource
- A part of your product's own API
 - If you add API endpoints that speak CTIM, SecureX can communicate directly with your product
- Java/PHP/Python/Ruby/etc. running on a normal web server
 - Remember, relay APIs are just HTTP using a specific data model
- Regardless of what you choose, remember that you'll need to handle validation of the token SecureX provides to the relay

Sample relay API endpoints

- /deliberate/observable
- /health
- /observe/observables
- /refer/observables
- /respond/observables
- /respond/trigger
- /tiles
- /tiles/tile
- /tiles/tile-data
- /version

What enables SecureX integrations?



Modules

- Tell SecureX how the integration works
- Includes information like:
 - Product information
 - Product logo
 - Relay API location
 - Relay API capabilities
 - Authentication requirements
 - Configuration requirements

Modules

*This capability can't be used
by non-Cisco modules



- A module's capabilities can include:
 - Dashboard
 - Deliberation
 - Device Insights*
 - Enrichment
 - Health Check
 - Reference Links
 - Response Actions
- These must match what the relay API is capable of

Modules

- Created by default for all the integrations available in the SecureX integrations catalog
 - The integration catalog is actually a list of modules
- Can be created yourself using the Module Maker in GitHub and the SecureX API
 - <https://visibility.amp.cisco.com/iroh/iroh-int/>

What enables SecureX integrations?



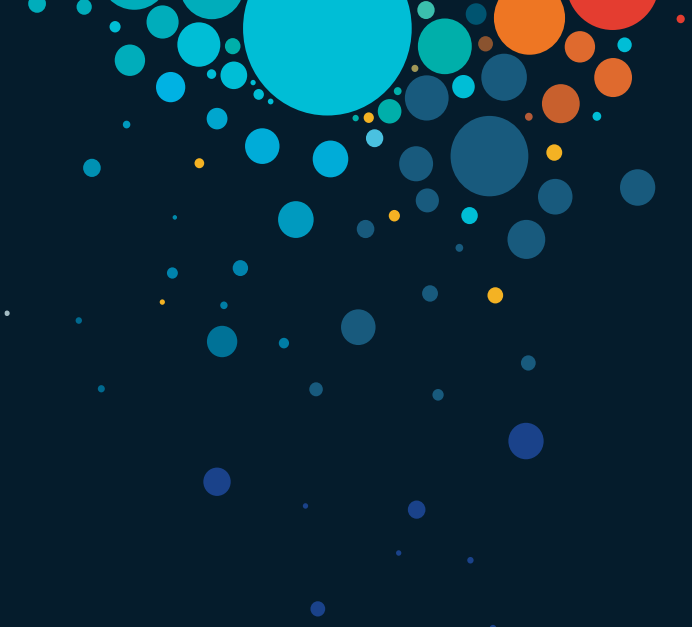
Relays



Modules



Relay Modules



Relays + Modules = “Relay Modules”

Relay Modules

- Amazon GuardDuty
- APIVoid
- Cisco Defense Orchestrator
- Cisco Firepower
- Cisco Orbital
- Cisco Secure Cloud Analytics
- Cisco Secure Cloud Insights
- Cisco Secure Email Appliance
- Cisco Secure Endpoint
- Cisco Secure Malware Analytics
- Cisco Secure Network Analytics
- Cisco Secure Web Appliance
- Duo Security
- Exabeam
- Farsight Security DNSDB®
- Gigamon ThreatINSIGHT

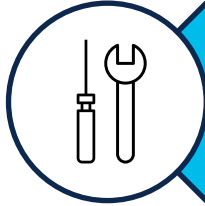
Relay Modules

- Jamf Pro
- LogRhythm
- Meraki Systems Manager
- Microsoft Graph Security API
- Microsoft Intune
- MISP
- ServiceNow Security Incident Response | ServiceNow Threat Intelligence
- Shodan
- Sumo Logic Cloud SIEM
- Talos Intelligence
- Umbrella
- urlscan.io
- VirusTotal
- VMWare Workspace ONE UEM

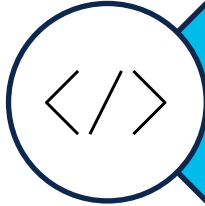


Okay, but now what...

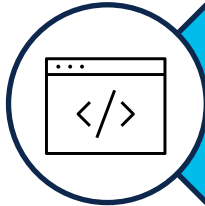
Building an integration



Build a relay API that can speak CTIM with SecureX and supports the capabilities you want. Examples are published in GitHub to help get you started



Use the module maker to generate the module definition you need to add to SecureX. This will be a JSON-formatted representation of the module



POST the module definition to the “/iroh-int/module-type” SecureX API endpoint (you’ll need a SecureX API client with the “Integration” scope)

Demo

Demo Outline

1

API Endpoint
Overview

2

Module Definition
JSON

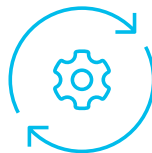
3

Module in Action

Conclusion



We believe
security solutions
should **empower**
people to
investigate and
respond to
threats faster




Automation should
reduce the burden
on the SOC



Security products and
threat intel should all
work together



Make it **easier and faster**
to investigate threats



*“I am able to visualize threats within
my environment and take action in
half the time it used to take me.”*

Security Engineer

Large Financial Services Company

Module and Relay Resources



GitHub Repository

<https://github.com/CiscoSecurity/>



Module Maker

<https://ciscosecurity.github.io/tr-05-module-maker/>



Cisco Threat Intelligence Model (CTIM)

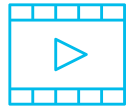
<https://github.com/threatgrid/ctim/>

Module and Relay Resources



Integration Catalog

<https://cs.co/threatresponseintegrations>



Video Playlist

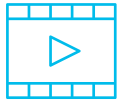
https://cs.co/SecureX_third_party_videos



Cisco Secure Technical Alliance

<https://cs.co/CSTA>

Orchestration Resources



Videos

https://cs.co/SXO_videos



Documentation

https://cs.co/SXO_docs



GitHub Repository

https://cs.co/SXO_repo

SecureX API Resources



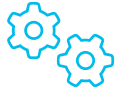
Inspect API

<https://visibility.amp.cisco.com/iroh/iroh-inspect/>



Enrich API

<https://visibility.amp.cisco.com/iroh/iroh-enrich/>



Response API

<https://visibility.amp.cisco.com/iroh/iroh-response/>



Private Intelligence

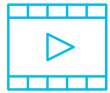
<https://private.intel.amp.cisco.com/>

SecureX Resources



Homepage

<https://cisco.com/go/securex>



Video Playlist

https://cs.co/SecureX_videos



Frequently Asked Questions

https://cs.co/SecureX_faq



Get Started!

<https://security.cisco.com>

Session Surveys

We would love to know your feedback on this session!

- Complete the session surveys in the Cisco Events mobile app. You'll earn some points in the Cisco Live Game and potentially win a prize.
- Complete a minimum of four session and the overall event surveys to claim a Cisco Live cable bag.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



Learn

Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals





The bridge to possible

Thank you

CISCO *Live!*

DevNet Zone

#CiscoLiveAPJC

CISCO *Live!*



#CiscoLiveAPJC