

TALOS

Threat Intelligence Use in Cybersecurity Operation

Rich Yim, CCIE R&S, CCIE SP #37710

Systems Architect, Cisco

Date: Dec 2022



Talos continues to support Ukraine. Read our newest research [here](#) and see all our other resources [here](#).

Reputation Lookup

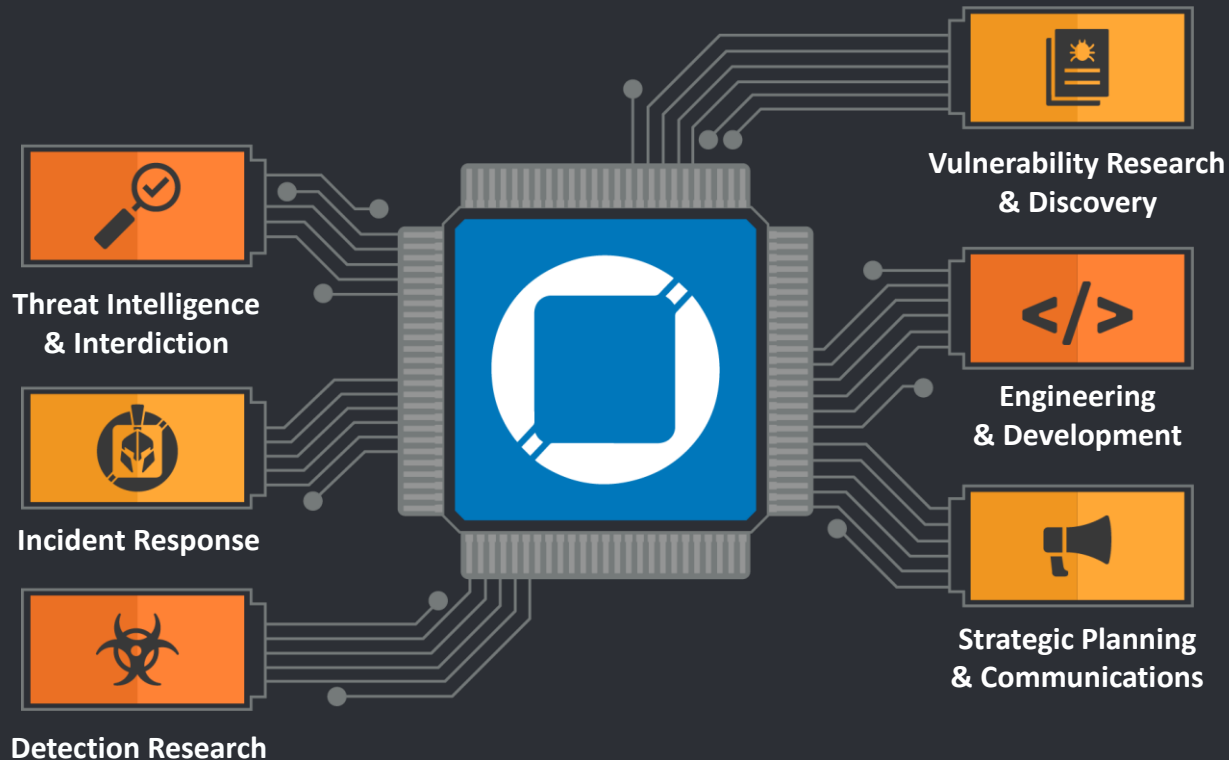


Query by IP, domain, or network owner for real-time threat data.

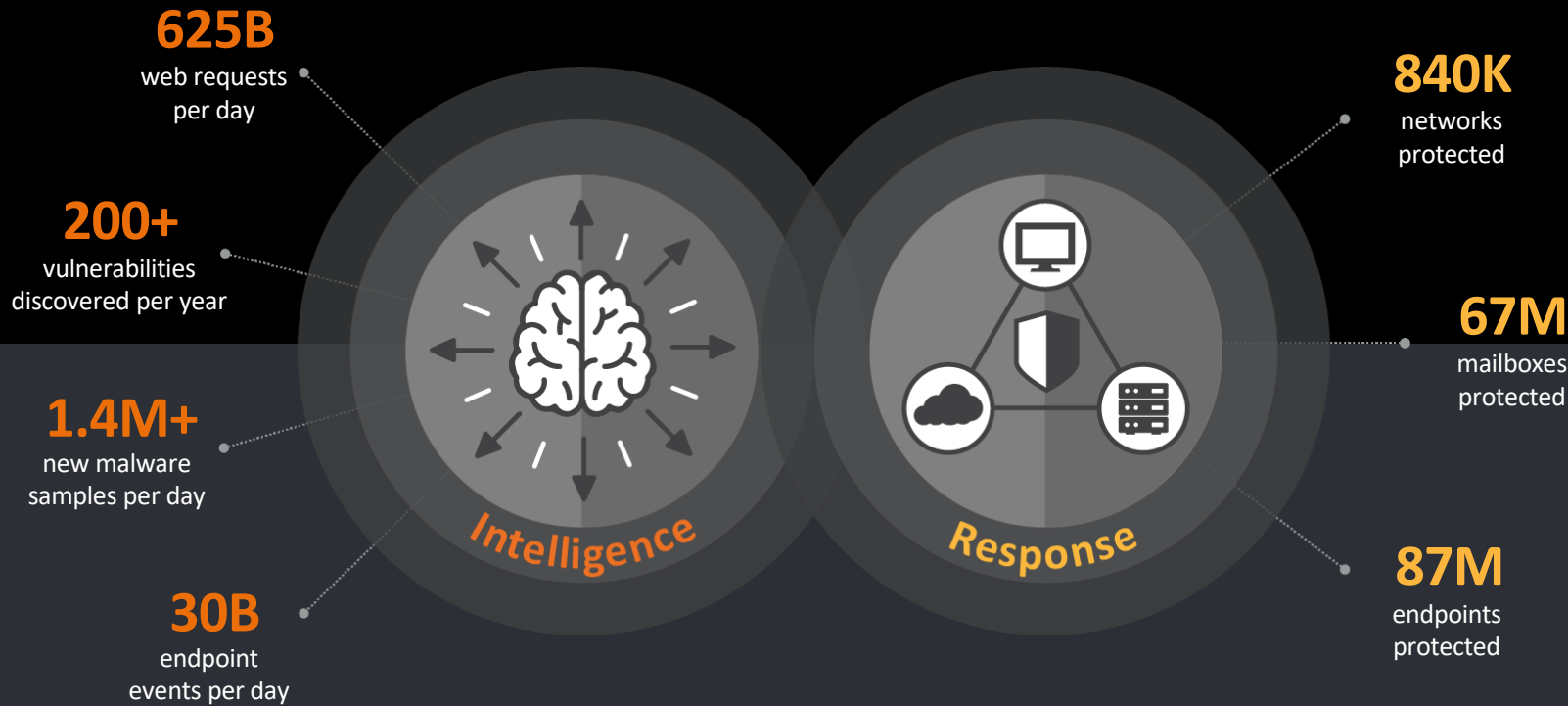


Talos job is protecting your network

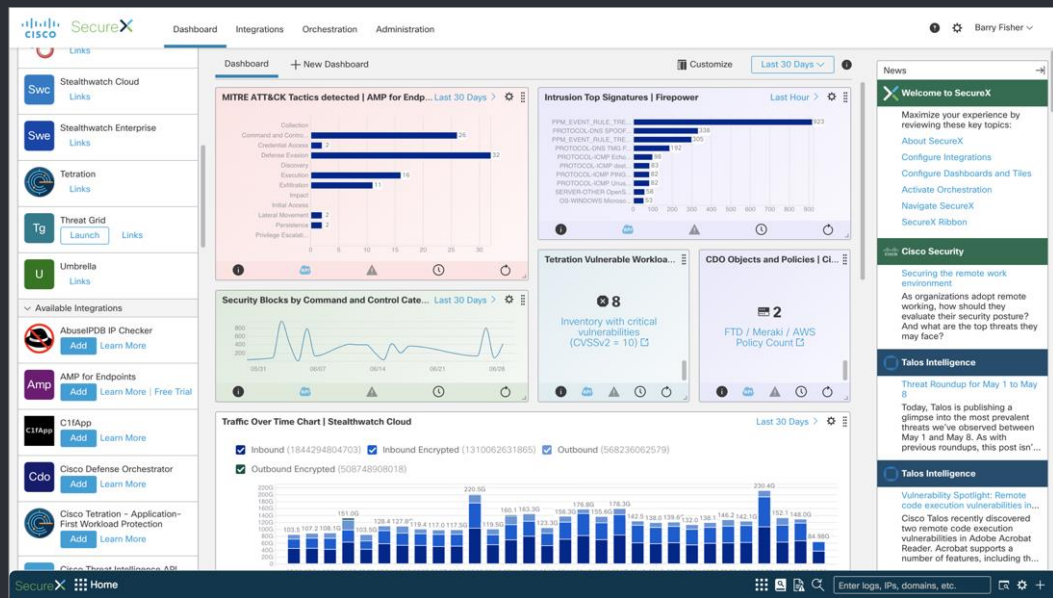
Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.



World-class breadth and depth of Cisco Talos



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

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

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



Cloud security



Network firewall



Web security

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.

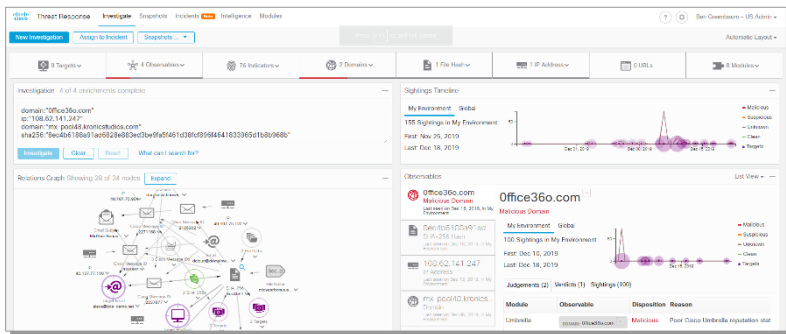
SecOps with SecureX threat response



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 API

The screenshot displays the Cisco SecureX web interface. The top navigation bar includes 'Dashboard', 'Integration Modules', 'Orchestration', and 'Administration' (highlighted with a red box). The left sidebar contains a 'Help' section with links to 'Release Notes', 'What's New', and a list of modules including 'Getting Started', 'Ribbon', 'Ribbon Extension', 'Casebook App', 'Incidents App', 'Orbital App', 'Dashboard', 'Integration Modules', 'Orchestration', 'Administration', 'Roles', 'Pivot Menu', 'SecureX APIs' (highlighted with a red box), 'System Status and Upda...', 'Glossary', 'Resources', 'Terms and Privacy', 'User Feedback', and 'Contact Support'. The main content area is titled 'SecureX API Integration' and contains a paragraph about the API collection, a bulleted list of capabilities, and a link to 'Cisco DEVNET' (highlighted with a red box). Below this is the 'API Clients' section, which includes a note about the beta status and instructions on generating API client credentials. A 'Creating an API Client' section follows with two numbered steps. At the bottom, a modal window titled 'Add New Client' is open, showing fields for 'Client Name*' and 'Client Preset', with 'API Clients' selected as the client type.

Administration

SecureX API Integration

Cisco SecureX 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. With SecureX, you can:

- **Enrich** an IP address, or file hash.
- Load threat intelligence into your [Private Intel Store](#)
- Manage your [casebooks](#) and [investigation](#) snapshots
- Automate [response](#) actions
- Provide a link for users to click and Investigate an alert or observable

For more information using the APIs, see [Cisco DEVNET](#).

API Clients

Note: The API Client feature is subject to change while in beta.

Users can generate API Client credentials, which can be used to access the SecureX APIs programmatically.

Creating an API Client

1. In SecureX, click the **Administration** tab and choose **API Clients** in the navigation pane.
2. On the **API Clients** page, click **Generate API Client** to open the **Add New Client** form.

Add New Client

Client Name*

Client Preset

☒ API Clients ☐ OAuth Code Clients

SecureX API's

- Build on top of **OpenAPI**, which is an open-source suite of API developer tools, enabling development across the entire API lifecycle, from design and documentation, to test and deployment.
- Uses **OAuth 2.0** to do authentication.
- The authentication flow is as follows:
 1. Use your ClientID and Password to obtain a token.
 2. Use the token to access the APIs for all other functions.
 3. When the token expires, request a new token with your API ClientID and API Secret.
 4. Use the new token to continue using the APIs for all other functions, until it expires.
 5. Repeat steps 3-4 as needed.

SecureX API's

- SecureX API, broken out by a logical separation of functions:
 - **Inspect** – pull observables out of formatted or unformatted text.
 - **Enrich** – search for additional information about those observables. Also contains Refer endpoint for pivoting into other products.
 - **Response** – take actions on observables (for example, add to blocklist).
 - **Settings** – configure Threat Response.
 - **OAuth** – use credentials and get access tokens.
 - **Global intel** – read global threat intelligence (CTIA).
 - **Private intel** – read and write user-provided threat intelligence (CTIA).
 - Used by the Incident Manager and Casebook.
 - This API could be used to add 3rd Party data in Threat Response.
 - **More endpoints!**

Create an API Client

Use the smallest scope needed!

Make sure you rotate API keys according to defined Security Policy and audit methods!

Add New Client

Client Name*

MY API CLIENT

Scopes* · [Select None](#)

☒ Casebook

Access and modify your casebooks.

☒ Enrich

Query your configured modules for threat intelligence - Read Only

☒ Inspect

Extract Observables and data from text - Read Only

☒ Global Intelligence

Access AMP Global Intelligence - Read Only

☒ Private Intelligence

Access AMP Private Intelligence

☒ Response

List and execute response actions using configured modules.

Description

THIS IS HOW YOU CREATE AN API CLIENT

Add New Client

Close

Test out the API's using the Swagger Framework.

In this case: the Inspect API...

Inspect Inspect related routes

INSPECT

POST /iroh/iroh-inspect/inspect return extracted observables from some raw text

[required_scopes: inspect:read](#)

Parameters Cancel

Name	Description
StrContent * required (body)	<div>Edit Value Model</div> <div><pre>{ "content": "internetbadguys.com 1.2.3.4 foo bar blaps bloops https://moreinternetbadguys.com"}</pre></div> <div>Cancel</div>

Parameter content type
application/json

Execute

Responses Response content type application/json

See the results!

What is this API used for in the GUI?

[illegible]

Investigation

Upload Snapshot

internetbadguys.com 1.2.3.4 foo bar blaps bloops https://moreinternetbadguys.com

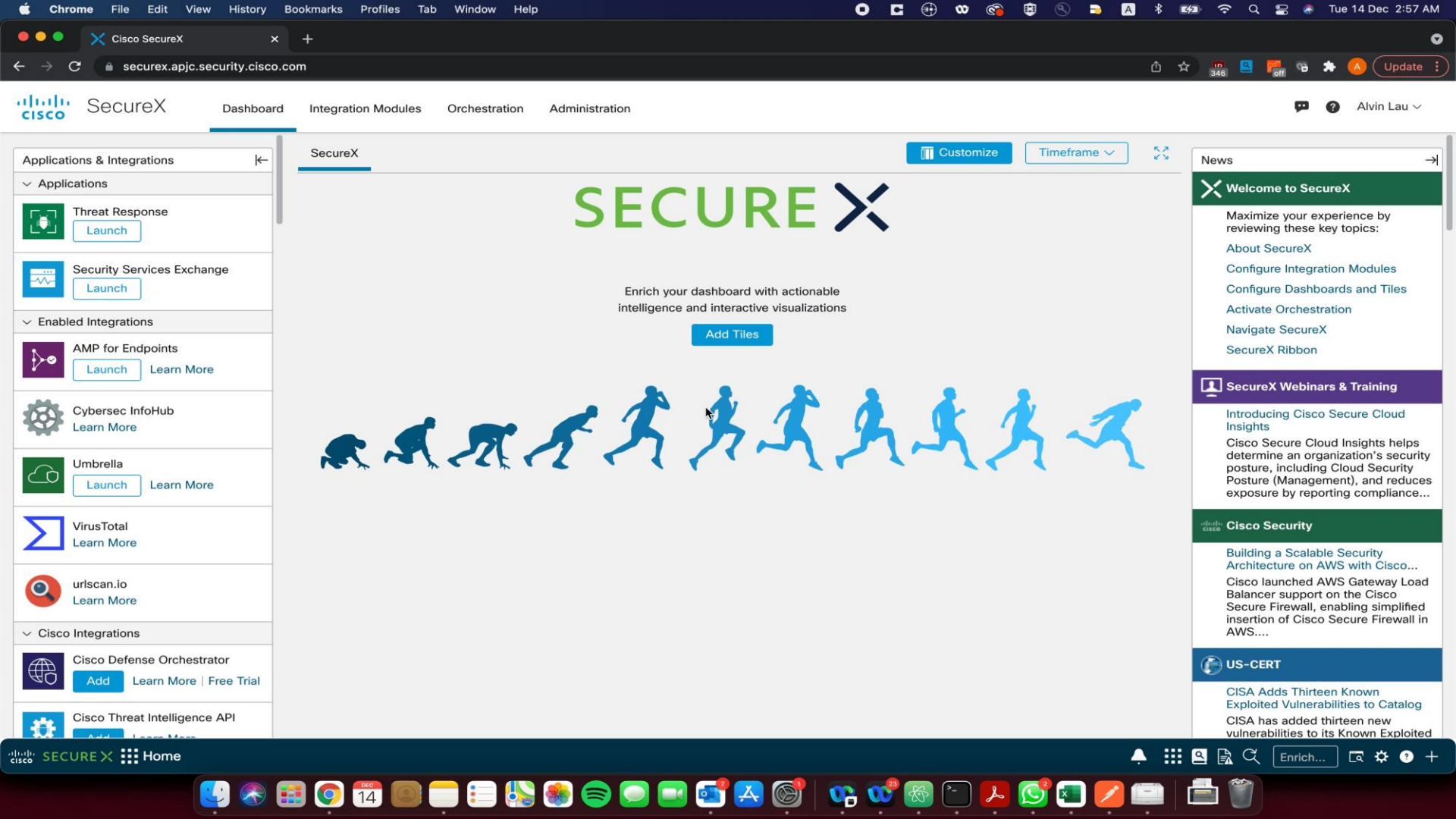
Investigate

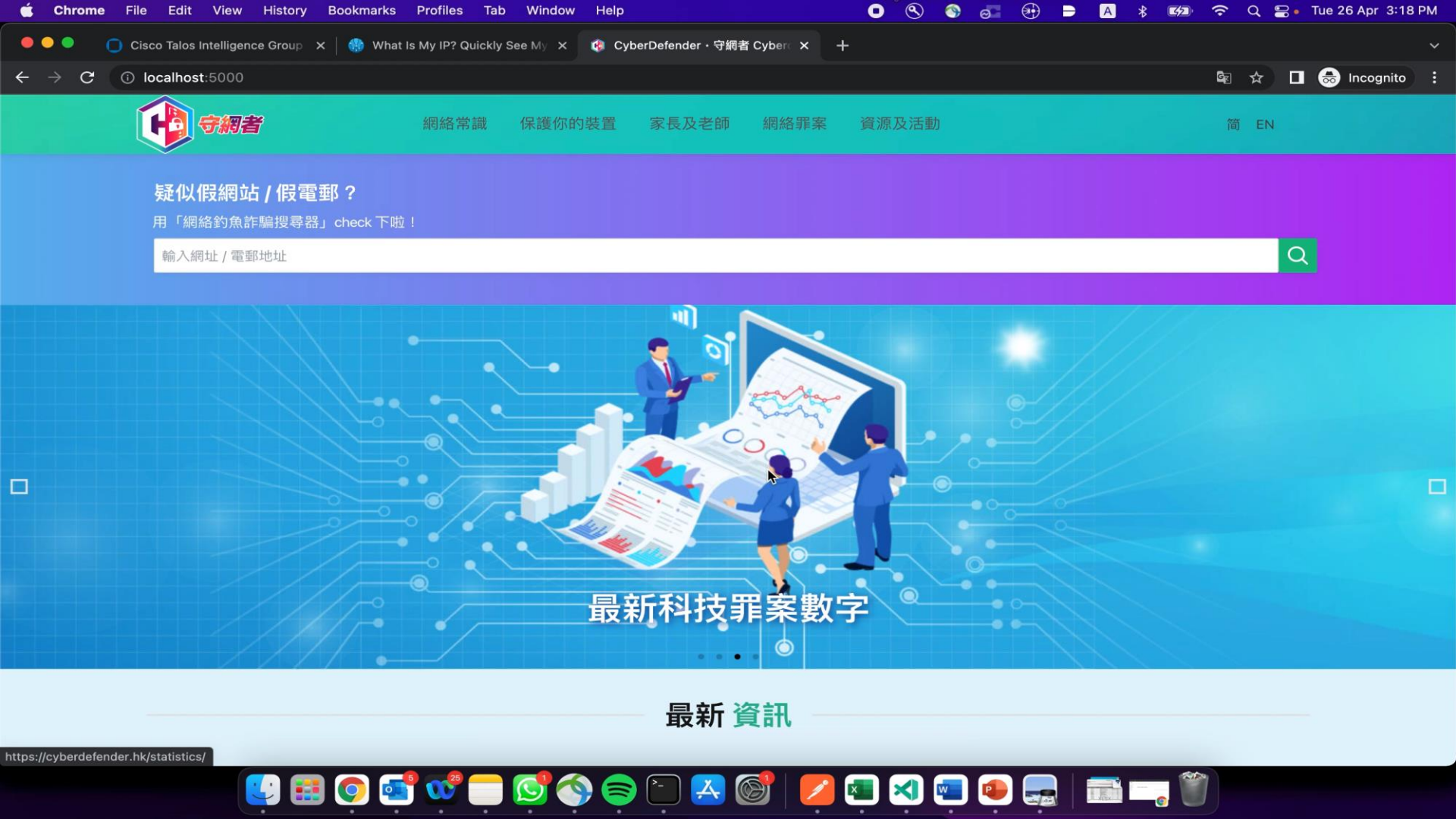
Clear

Reset

What can I search for?

```
strict-transport-security: max-age=31536000; includeSubDomains
vary: Accept-Encoding, User-Agent
x-content-type-options: nosniff
x-ctim-version: 1.0.12
x-iroh-config: 960872ab24f23d6e9af6bd1770cac8c8dd78a4d2
x-iroh-version: 245caa75b0c3527ba8d94ee85bd1988be78f8e8e
```





The SxTR SDK

threatresponse 0.10.0

```
pip install threatresponse
```



Threat Response API Module

Navigation

 Project description

 Release history

 Download files

Project description

[gitter](#) [join chat](#) [build](#) [passing](#) [pypi](#) [v0.10.0](#) [python](#) [2.6](#) | [2.7](#) | [3.5](#) | [3.6](#) | [3.7](#) | [3.8](#)

Threat Response API Module

Python API Module for Threat Response APIs.



Join the security developer community

The DevNet developer security community has been redesigned and reorganized around developers writing integrations and automations including SecureX Orchestration

Join the Community



BLOG

Get Ready To Try the Umbrella Cloud Security Sandbox

BLOG

Outsourcing Security Operations with Cisco Secure Endpoint

BLOG

Get to Know Cisco SecureX

Getting started



Threat Hunting with Cisco Security APIs



Enrich and remediate your security events



automation

I'm looking for information about...

developer.cisco.com/security

Chat with Us!



Technology & Support



For Partners



Customer Connection



Webex



Events



Members & Recognition

[Cisco Community](#) / [Technology and Support](#) / [For Developers](#) / [Developer Security](#)

```
{
  "Forums": {
    "Application Security": {
      "Technologies": ["Secure Workload (Tetration)", "AppDynamics"]},
    "Cloud Edge": {
      "Technologies": ["Cisco Umbrella"]},
    "Network Security": {
      "Technologies": ["Threat Defense (FTD)", "Threat Defense Manager (FMC)", "CDO", "ASA", "ISE", "Secure Network Analytics (Stealthwatch)"]},
    "SecureX": {
      "Technologies": ["SecureX Threat Response", "SecureX Orchestration"]},
    "User and Endpoint Protection": {
      "Technologies": ["Cisco Secure Access by Duo", "Secure Endpoint (AMP)"]},
```

