Practice for Asset

Product Version	3.0.64C and above
Document Version	v1.0
Released on	2023-05-08

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

Intended Audience

This document is intended for:

- Pre-sales
- FAE

Note Icons

English Icon	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
2023-05-08	This is the first release of this document.

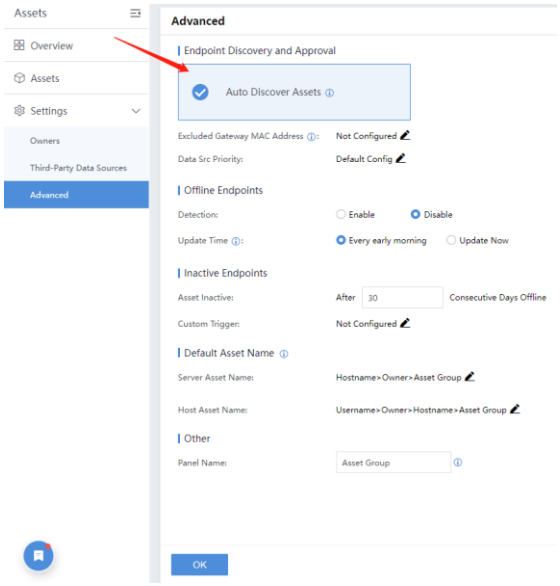
Contents

1 Underlying Concepts

1.1 Asset Auto-Discovery Mechanism

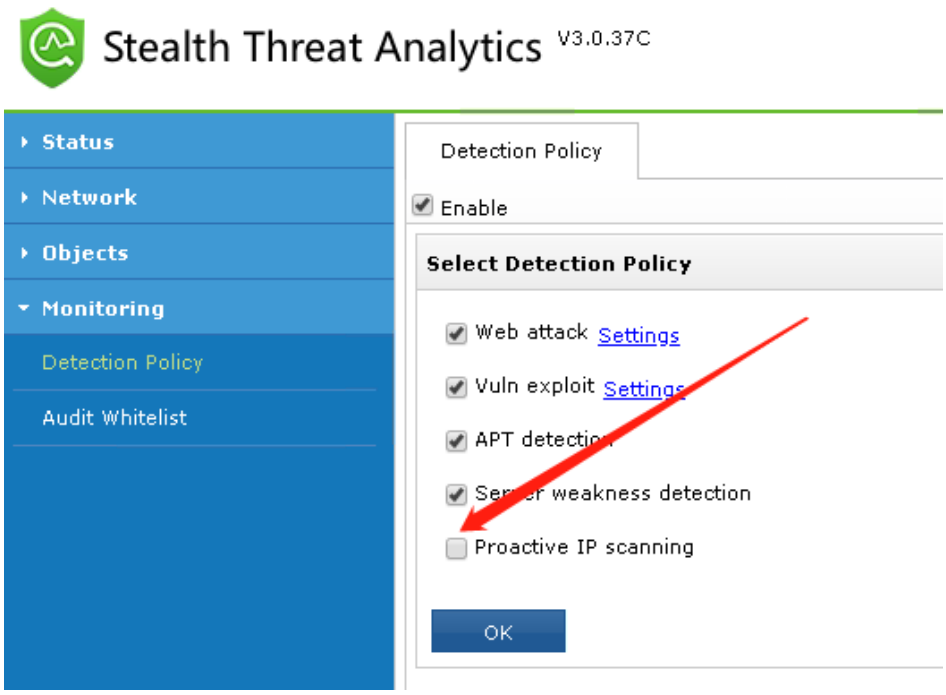
1.1.1 Passive Asset Identification in CC

The type of identification is obtained by hitting various logs. When the protocol audit log matches some built-in asset type fingerprints (for example: destination port, access frequency...etc), corresponding types of assets will be generated. These fingerprints are black box functions and cannot be configured and edited in Web GUI, but there is a switch which can control turn it on or off(see as below). Basically, the vast majority of auto-identified assets in the asset list are identified in this way.



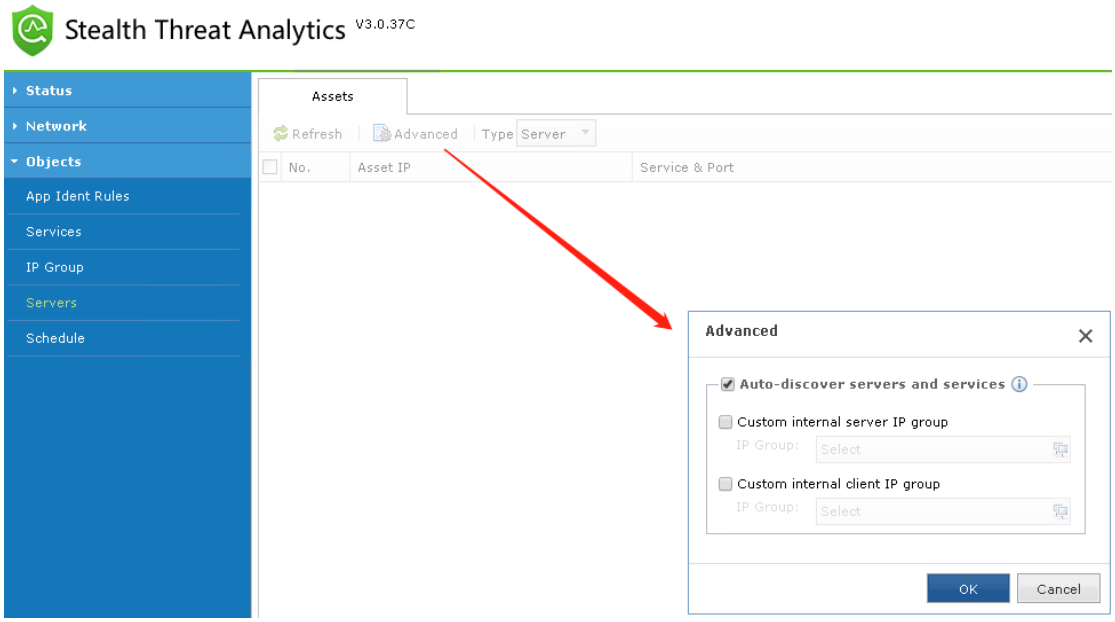
1.1.2 Proactive Asset Identification in STA

On **Monitoring->Detection Policy** the Page, and in most circumstance, don't select it as it can have side effects.



1.1.3 Passive Asset Identification in STA

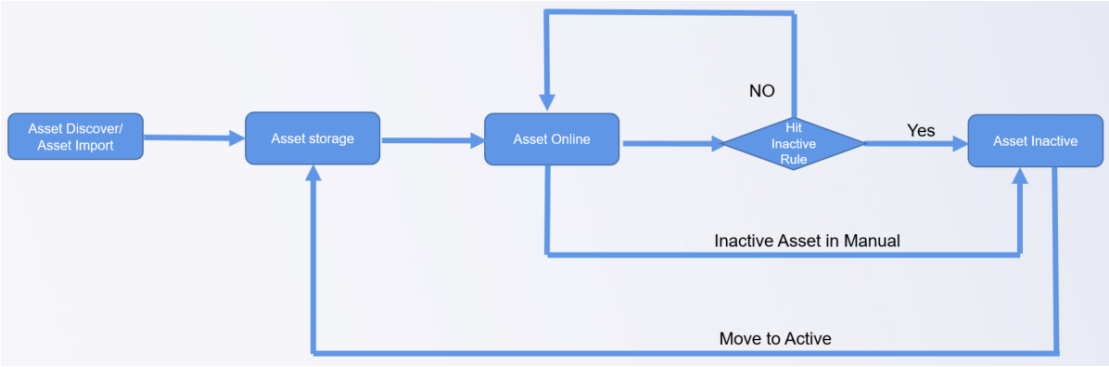
On **Objects->Servers->Assets->Advanced** the page, make sure **Auto-discover servers and services** has been selected which is also the default setting and never unselect it.



1.2 Asset Life Cycle

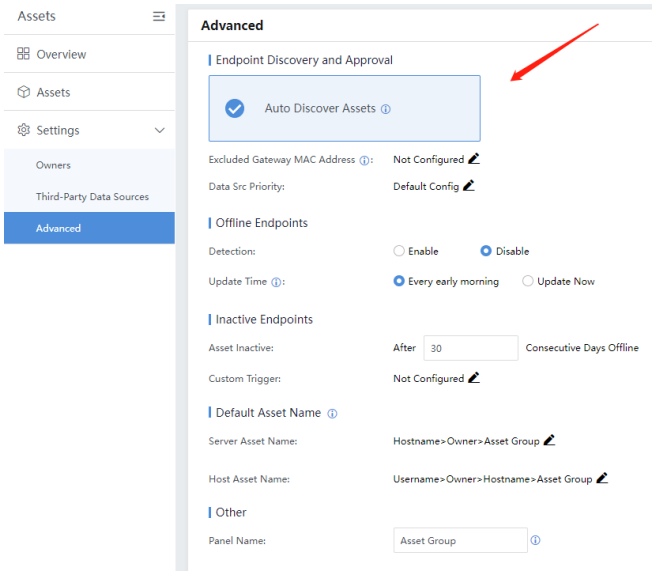
Asset life cycle management mainly contain several status, such as asset discover、asset import、asset storage、asset online、and asset inactive. The

entire process is shown in the diagram below.



1.2.1 Auto-Discover Asset

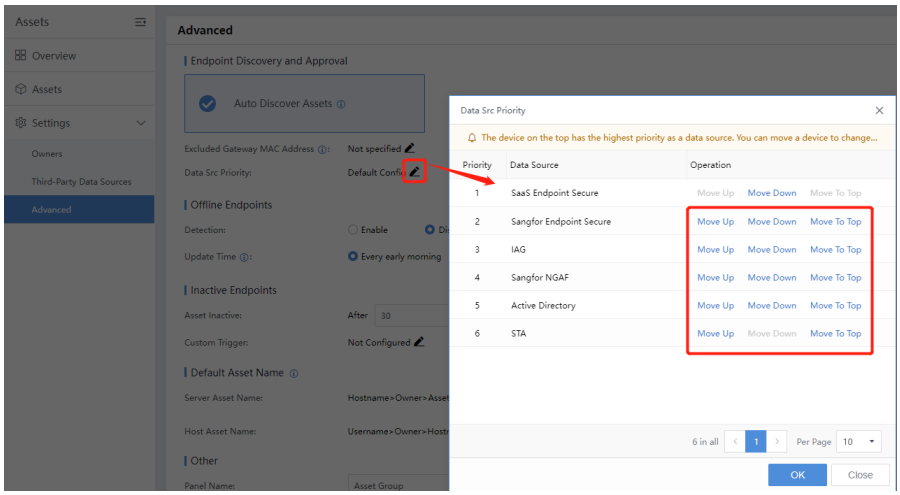
By default, CC platform has enabled the function of auto-discover asset, and will automatically replenish assets that are not in the IP range. If it is turned off, assets will be automatically identified and stored. If it is turned off, assets will not be automatically identified and stored. The function switch is located on Assets->Setting->Advanced



multiple data source

There are multiple data sources for the same asset, such as NGAF, STA, and ES devices connected at the same time. At this time, the same asset may be recognized by multiple devices. It is necessary to determine which data source is recommended. CC has the default data source priority, under special circumstances, it can be manually adjusted when the default order is found to be inconsistent with the actual business environment, as shown in the

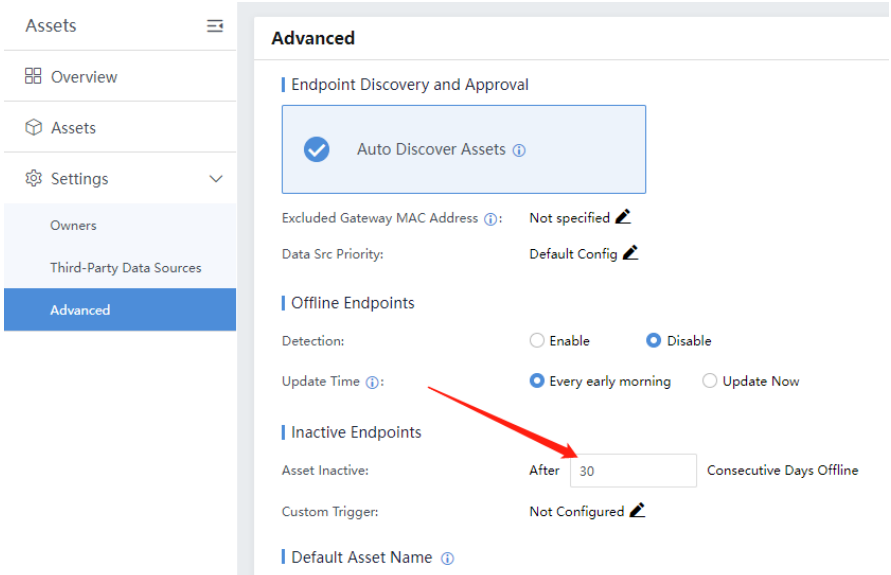
figure below.



1.2.2 Asset Inactive

Note: Inactive Asset only takes effect for auto-discover assets, and will not affect assets imported in manual.

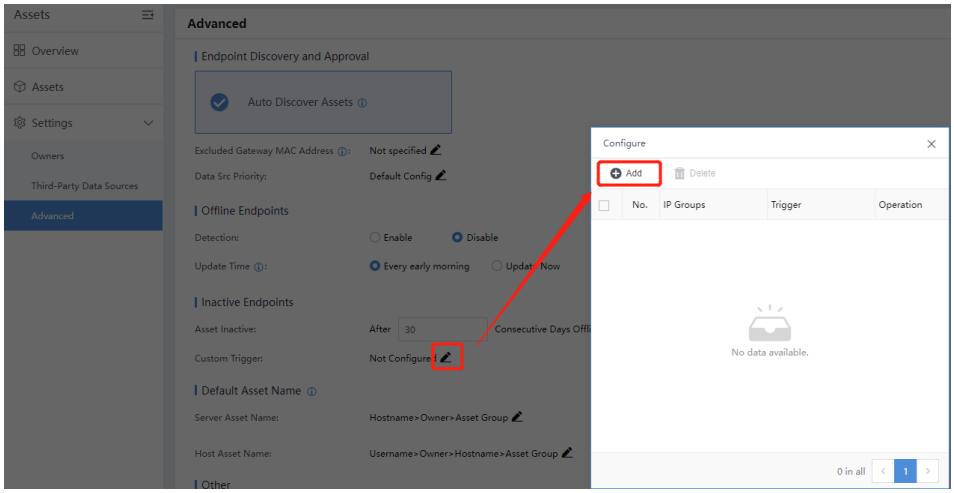
Asset inactive is to abandon assets that have expired or have no value or have been inactive for long period in order to maintain the accuracy and stable amount of asset. Zombie assets can be identified during security governance. The specific asset groups that need to be abandoned and the time range should be based on the fact and be discussed with customers, such as the asset group of the dynamic IP network segment, the asset inactive time range can refer to the DHCP lease cycle.



Generally speaking, asset inactive is usually for general assets, rather than critical assets, for example, it is not proper to configure business server

assets inactive. It is recommended that different assets group can be configured in different time range.

- In principle, the assets of the DHCP network can be set asset inactive;
- Guest mobile terminals asset group under the WLAN network can be set asset inactive
- Server-type assets are usually not set asset inactive.



1.3 Some Indicator Specification

- The maximum of asset groups is 3000 that contains all subgroups, and which cover the cascade scenario reported asset groups by the lower level.
- The maximum of asset group hierarchy depth is 15;
- The maximum number of assets imported at a time is 20,000;
- The maximum number of assets exported at a time is 10,000;

2 Asset group and Asset Allocation

At present, there are totally 3 methods to allocate asset groups, they can be used in different scenarios.

2.1 Group by IP Range

Applied in most scenarios, all asset groups do not have the same address range, the network segment is clear, and can be set according to the asset

group and the matching network segment.

2.2 Group by Device Source

In some special scenarios, asset group based on device source is used. For example, in the headquarters-branch scenario, STA is deployed in each branch, CC is deployed in the headquarters, and many network segments are duplicated between branches. It is a wise choice to set group by device source.

This mode will lead to an obvious disadvantage, that is, all addresses both private IP address and public IP address audited by the STA's traffic will be written into the asset table which is not expected.

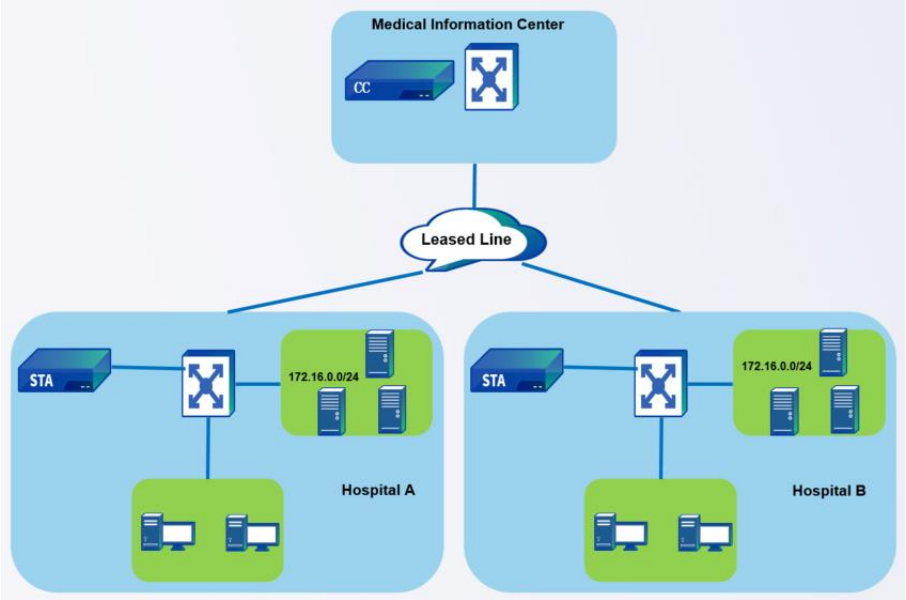
2.3 Group by Source Device or IP Range

There is almost no space and scenario for such mode since the relationship between source and IP rangge is "or" , rather than "and". According to pruduct line version releasing plan, the next version of CC will modify such mode completely then it can support many comprehensive scenarios and make CC more valuable.

2.4 Case Study

2.4.1 Case Description

Two hospitals, A and B, are connected to the medical leased line network. Hospital A and hospital B have deployed STA and connected to CC which is deployed in the medical information center. Two asset groups are created on CC representing hospital A and B assets respectively, However there is a duplicate network segment 172.16.0.0/24 between hospital A and hospital B.

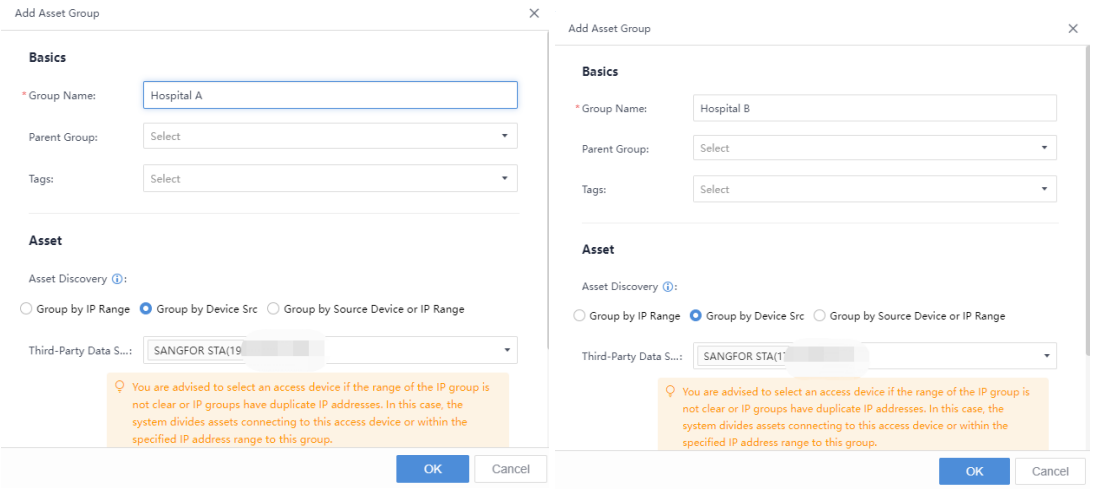


2.4.2 Issues Confronted

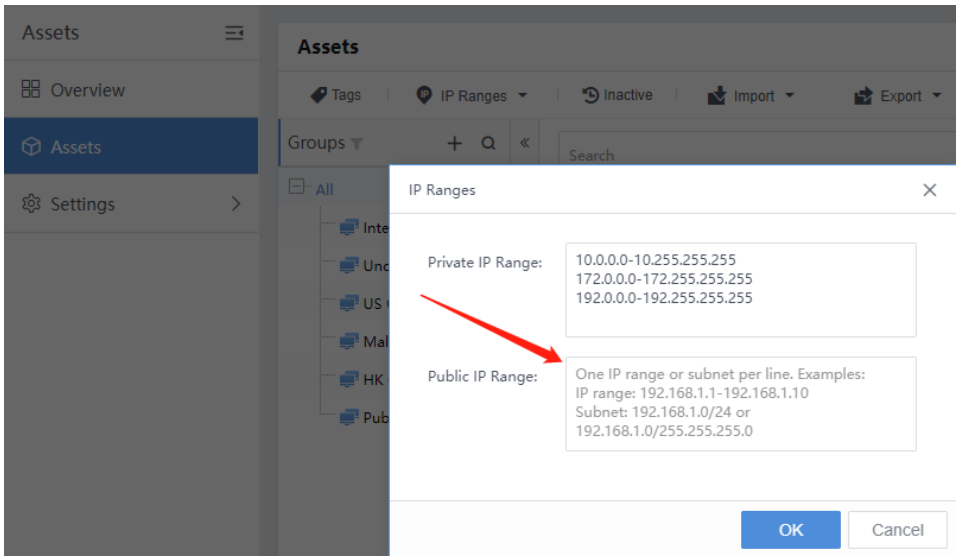
It is impossible to create two asset groups by IP rangge if the IP range is confilict between them.

2.4.3 Recommended Solution

- Step 1: Create two asset groups by device source mode



- Step 2: Add public IP address assets into public IP range in manual.



3 Asset Management

How to manage large-scale assets, such as tens of thousands of assets?

● Asset Stratification

No matter how large the assets scale is, there will contains 2 layers when it comes to assets importance, that is critial, general and indifferent assets.

What sorts of assets are critical in common sense?

1. Business servers(Database, Middleware, Backup, Syalog.etc)
2. Public servers (Mail, ERP, FTP, DHCP/AD/DNS, SNMP.etc)
3. Network Devices(Switches, Routers, Cloud Platform Radius.etc)
4. Security Devices (AF, WAF, IPS/IDS, VPN, Proxy, Loadblance, Anti-virus.etc)

What sorts of assets are general?

Destop, Laptop, PC, Workstation, Public printer.etc.

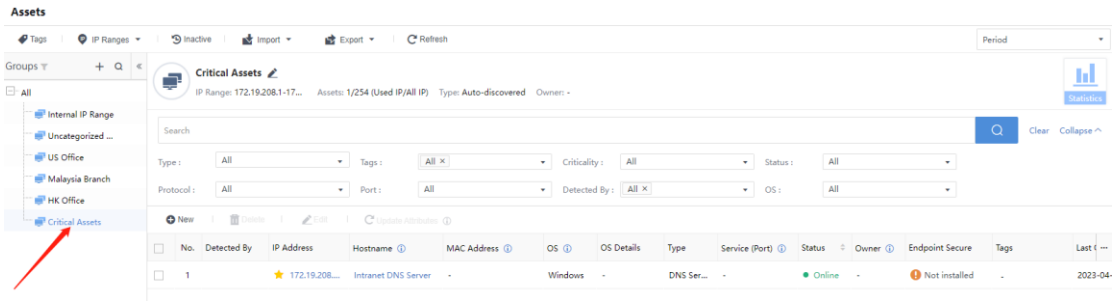
What sorts of assets are indifferent?

Visitors' mobile terminals when they access WLAN.

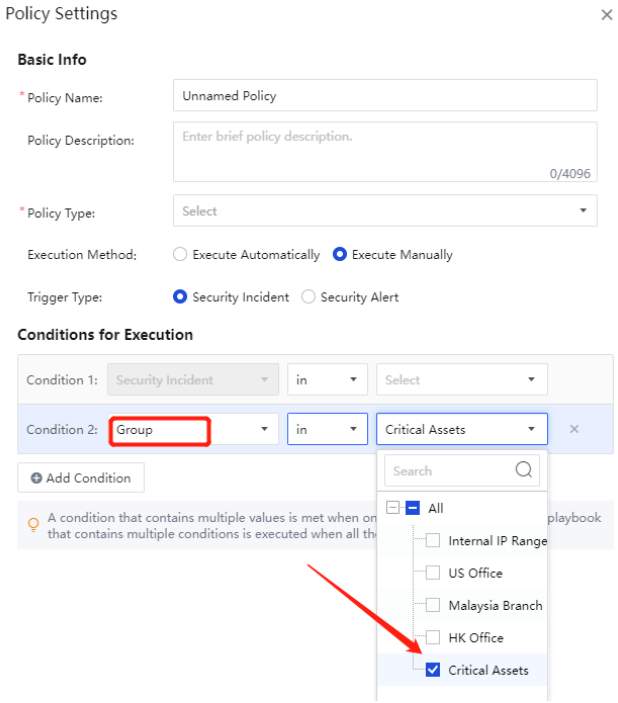
● Critical Assets

Generally speaking, creating asset groups should be consistent with the business organization structure, but in large-scale assets scenario, we

suggest that pick out the critical assets at the begining and label them as critical assets.



If we distinguish the critical and general assets, there will be flexible when we create differernt automatic response policy.



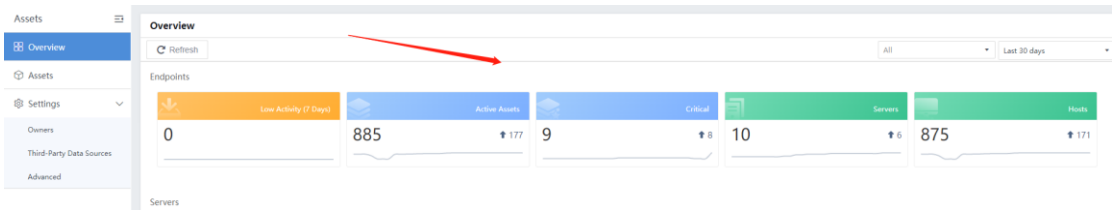
NOTE

Generally speaking, automatic response policy are mainly aimed at assets of general importance, rather than critical assets.

● Asset Quantity Fluctuations

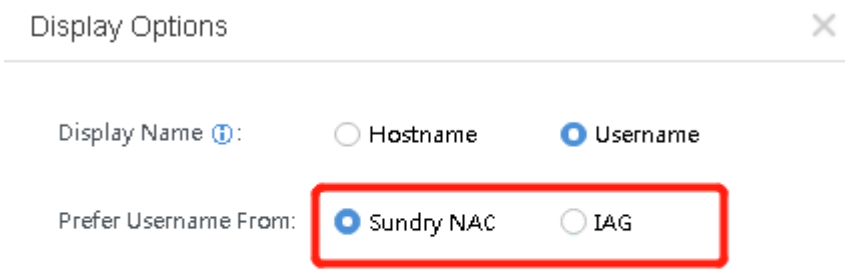
In daily security operations, it is necessary to pay attention to the fluctuation of the number of assets every day. If there is a sudden increase

or decrease, it is necessary to check whether there are other external causes, such as: network changes, artificial deletion.etc.

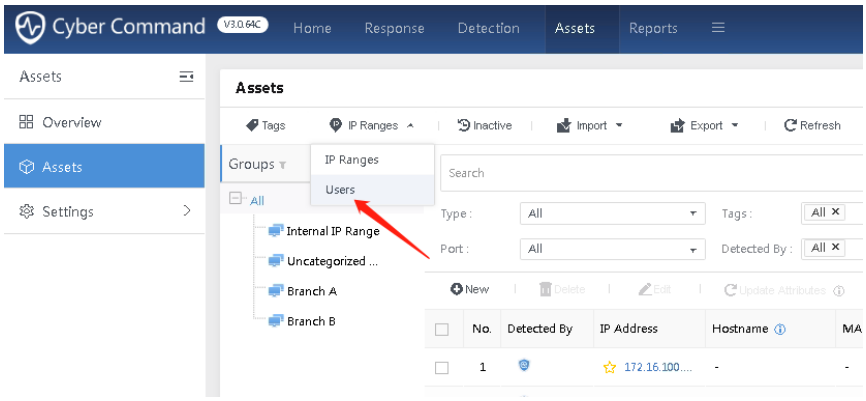


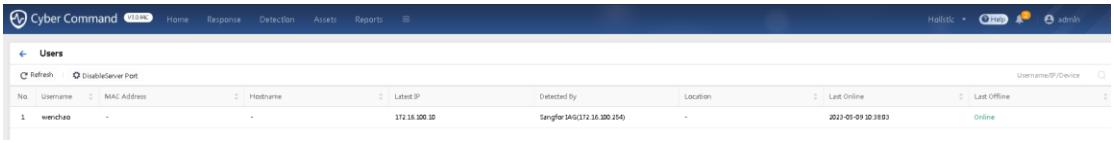
4 DHCP Network Scenario

In the DHCP network environment, IP addresses are unreliable, so other factors, such as MAC addresses or usernames, can be considered in the analysis of threat source tracing. However, CC cannot perform playbook policy based on MAC addresses, tracing risky usernames becomes a priority in such scenario. There are some prerequisites for getting the terminal username, at present CC can obtain these by some authentication system, such as Sundry NAC or IAG.

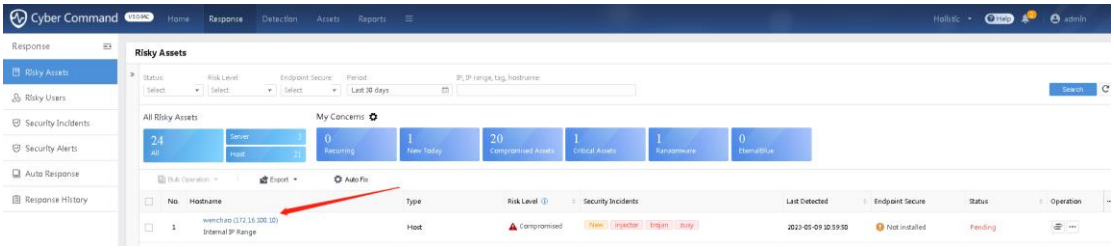


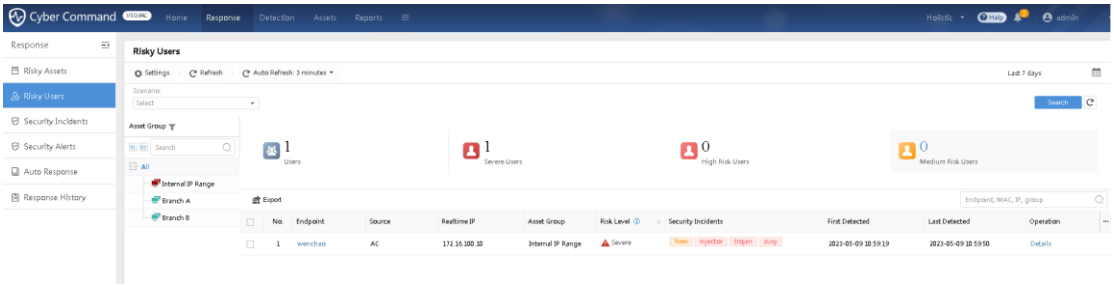
All usernames can be found on **Asset->Asset->Users** page.



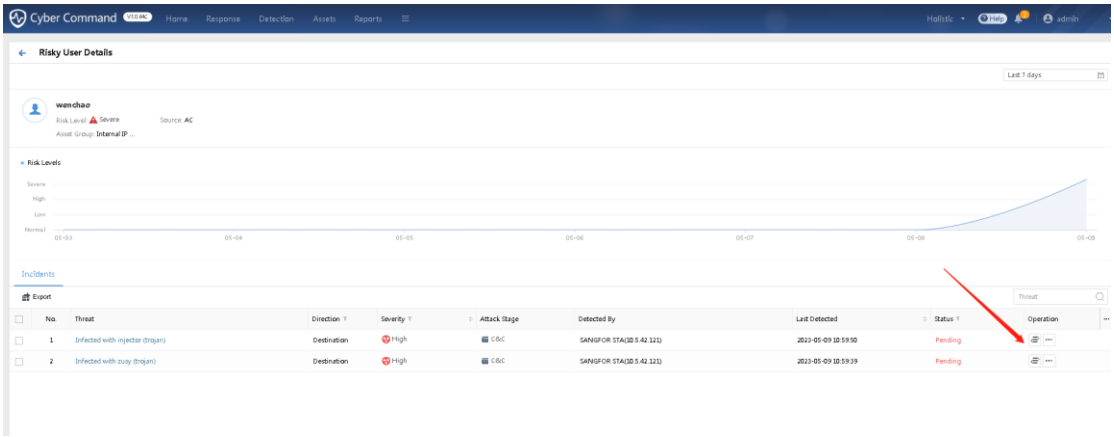


If some of these usernames are correlated with security incidents, you can see the risky users on the **Response->Risky Users** page.





Click the username to view the detail and you can disposal relative incidents by palybook policies.



5 Scenarios without a Solution

1. At present, CC cannot perform playbook policy based on MAC address.

2. A device has multiple network ports and is configured with multiple IP addresses. The traffic of these network ports is mirrored by STA and identified as assets. In the CC asset module, you can actually see several

assets, one for each network por,rather than only one asset.