



Sangfor Cyber Command

User Manual

Product Version	3.0.92
Document Version	01
Released on	May 30, 2024

Copyright © Sangfor Technologies Inc. 2023. All rights reserved.

Unless otherwise stated or authorized, Sangfor Technologies Inc. (hereinafter referred to as "Sangfor") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, and trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of Sangfor, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

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.

About This Document

This document is the user manual of Sangfor Cyber Command.

Intended Audience

This document is intended for:

- Network design engineers
- O&M personnel

Note Icons

The symbols that may be found in this document are defined as follows.

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
May 30, 2024	This is the first release of this document.

Contents

- Technical Support 2
- Change Log 3
- 1 Installation Guide 7
 - 1.1 Environment Requirement 7
 - 1.2 Power Supply 7
 - 1.3 Product Interface Description 7
 - 1.4 Configuration and Management 9
 - 1.5 Wiring Method for Devices 9
- 2 Usage of Console 10
 - 2.1 Logging into Web UI Configuration Interface 10
 - 2.1.1 Configuration and Management 10
 - 2.1.2 Login to the Console 11
 - 2.2 Configuration and Usage 12
 - 2.2.1 Configuration and Usage of Cyber Command Console 12
- 3 Features 14
 - 3.1 Home 14
 - 3.1.1 Overview 14
 - 3.1.2 Monitor 18
 - 3.1.3 Data Center 22
 - 3.1.4 ATT&CK Capabilities 22
 - 3.2 Response 26
 - 3.2.1 Risky Assets 26
 - 3.3 Risky Users 35
 - 3.4 Security Incidents 37
 - 3.4.1 Security Incidents filtering 37
 - 3.4.2 Incidents 39

- 3.4.3 View Incidents 39
 - 3.4.4 Incident Details 42
 - 3.4.5 Incident Operation 46
- 3.5 Security Alerts 50
 - 3.5.1 Alert Filtering 50
 - 3.5.2 View Alerts 53
 - 3.5.3 Details 55
 - 3.5.4 Manual Response 57
 - 3.5.5 HCI Integration 61
- 3.6 Response Policies 61
 - 3.6.1 Policies Classification 62
 - 3.6.2 Policies Settings 64
 - 3.6.3 Add the Node 67
 - 3.6.4 Response History 69
- 3.7 Detection 71
 - 3.7.1 Logs 71
 - 3.7.2 Threats 73
 - 3.7.3 Traffic 83
 - 3.7.4 Anomalies 86
 - 3.7.5 Unauthorized Access 88
 - 3.7.6 Lateral Access 92
 - 3.7.7 Outbound Server Access 96
 - 3.7.8 Telemetry Hub 99
- 3.8 Assets 103
 - 3.8.1 Assets 103
 - 3.8.2 Weaknesses 110
- 3.9 Reports 120
 - 3.9.1 Security Risk Reports 120

- 3.9.2 Notification 123
 - 3.9.3 Security Incidents Database 124
 - 3.9.4 Data Sharing 125
- 3.10 Navigation 125
- 3.11 Other Settings 126
 - 3.11.1 Threat Intelligence 126
 - 3.11.2 System 127
 - 3.11.3 Security Capabilities 174
- 4 Attachments 192
 - 4.1 Attachment 192
 - 4.1.1 DNS Environment 192
 - 4.1.2 HCI Environment 194
 - 4.1.3 DHCP Environment 194

1 Installation Guide

This part mainly introduces the hardware installation of Cyber Command devices. After successful installation, Cyber Command can be configured and debugged.

1.1 Environment Requirement

Cyber Command shall be used in the following environment:

Model	CC-1000	CC-2000	CC-3000
Maximum power:	550W	550W	550W
Temperature:	10-35°C	10-35°C	10-35°C
Humidity:	35%-80%	20%-80%	35%-80%
Size (length*width*height)	735mm*447mm*88mm	735mm*447mm*88mm	735mm*447mm*88mm

Table 1: Environment Requirement

To ensure the system's long-term and stable running, please ensure that the power supply is well-grounded, dust-proof measures are taken, the working environment is well-ventilated, and the indoor temperature is stable. This product complies with the design requirements on environmental protection. The placement, usage, and discard of the product shall comply with relevant national laws and regulations where it is applied.

1.2 Power Supply

The Cyber Command series are supplied with 110V - 230V AC power. Before turning on the power, make sure that proper grounding measures are taken.

1.3 Product Interface Description

Cyber Command:



Device name	No.	Network interface No.	Network interface type
CC-1000-A600	1	ETH1	Gigabit electrical interface
	2	ETH2	Gigabit electrical interface
	3	ETH3	Gigabit electrical interface
	4	ETH4	Gigabit electrical interface
	5	ETH5	Gigabit electrical interface
	6	ETH6	Gigabit electrical interface

Table 2: Description of Interface



1. The picture is for reference only. Please refer to the actual product for the appearance of different models.
 2. The CONSOLE interface is for development, testing, and debugging only. A network interface shall access the device.
-

1.4 Configuration and Management

Before configuring the Cyber Command device, make sure that you have a computer whose browser (such as Chrome or Firefox) works well. The Cyber Command device shall be configured in the same LAN as the computer.

The management interface of the Cyber Command device is MANAGE (ETH0), and its factory default IP address is 10.251.251.252/24. When logging into the device for the first time, connect the MANAGE (ETH0) interface to the LAN using a network cable or directly to the computer.

1.5 Wiring Method for Devices

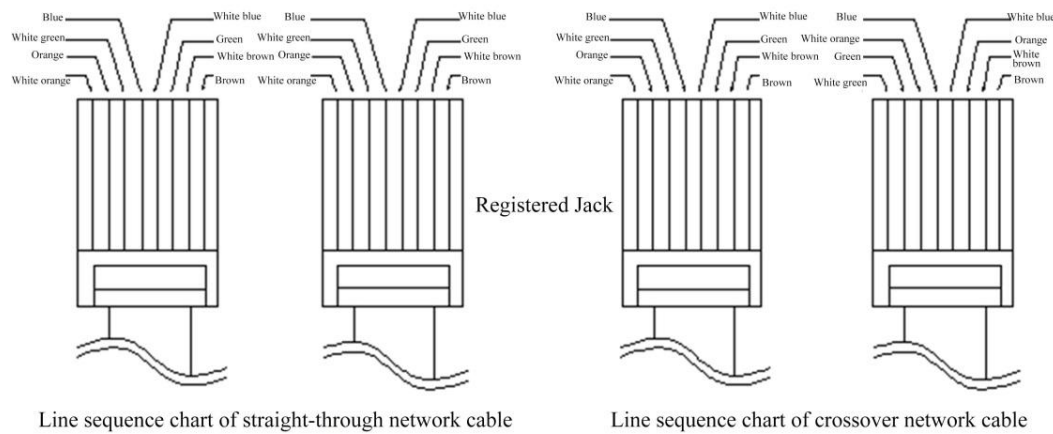
Plug the power cable into the device's rear panel, then turn on the power supply. At this time, the power indicator (green) and alert indicator (red) in the front panel will be on. The alert indicator will go out in one or two minutes, indicating the gateway is working.

Connect the MANAGE (ETH0) to the internal LAN using a standard RJ-45 ethernet cable, and then configure the Cyber Command and STA Devices.

After logging into the control panel, perform configuration and wiring according to the network environment and deployment requirements.

1. When the device is working, the POWER indicator and LINK indicator of the data interface for wiring stays on. The ACT indicator constantly blinks when there is data traffic. The ALERT indicator keeps red (for about one minute) only when the system is loading after startup and goes out when the system is working. If the indicator keeps red during installation, please switch off the power supply and reboot the device. If it still keeps on after a reboot, please contact us.
2. The network interface connects the modem with the switch via straight-through cables while connecting to the router with the computer via crossover cables. When the indicator is in normal status and the

connection is not working, please check whether the cables are being used correctly. The difference between the straight-through network cable and the crossover network cable lies in the wire sequence at both ends of the cables as follows:



2 Usage of Console

This part mainly introduces the products and hardware installation of Cyber Command. After successful installation, Cyber Command can be configured and debugged.

2.1 Logging into Web UI Configuration Interface

2.1.1 Configuration and Management

The factory default IP address of the device is shown in the table below:

Interface	IP Address
ETH0	10.251.251.252/24

Table 3: Default IP

The Cyber Command device only supports secure HTTPS login, adopting its standard port (port 443) of HTTPS protocol.



The Chrome and Firefox browser are recommended for logging in to the Cyber Command platform.

设置格式[SXF-zyl]: 非突出显示

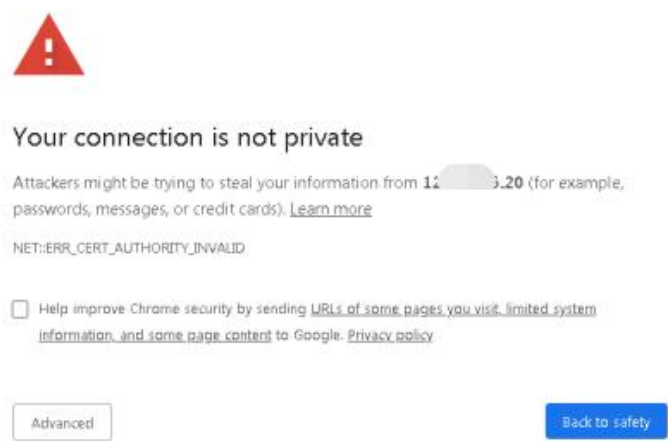
设置格式[SXF-zyl]: 非突出显示

设置格式[SXF-zyl]: 非突出显示

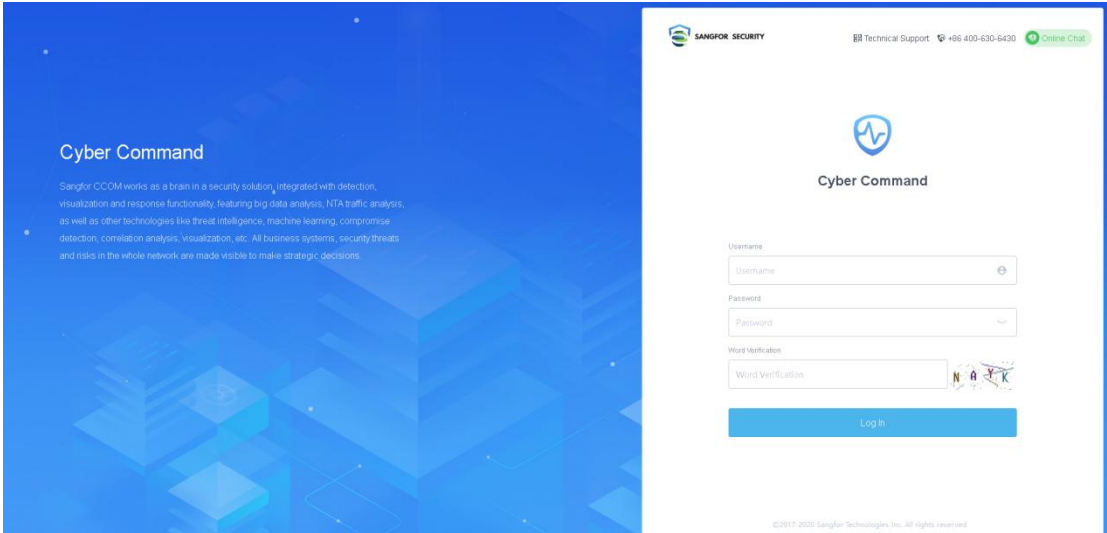
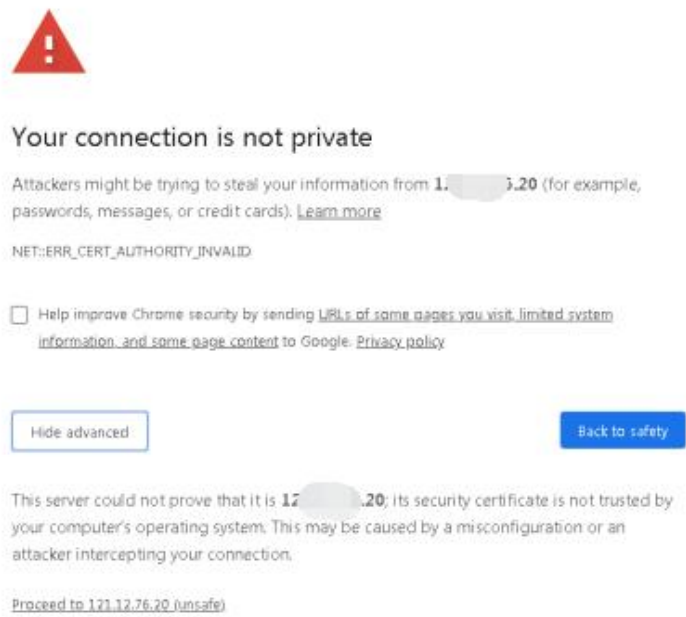
2.1.2 Login to the Console

Connect the computer network card and Cyber Command device ETH0 port to the same layer 2 Gigabit Switch, or connect the ETH0 port directly to the computer network card via network cable. Configure Cyber Command on the web interface. The method is as follows:

Firstly, configure an IP of network segment 10.251.251.X for the local unit (such as IP address: 10.251.251.100, netmask: 255.255.255.0), and then enter the default login IP address and port: https://10.251.251.252 of Cyber Command in the Chrome browser. A security prompt is shown below:



Click **Advanced > Proceed** to 10.251.251.252 (unsafe)



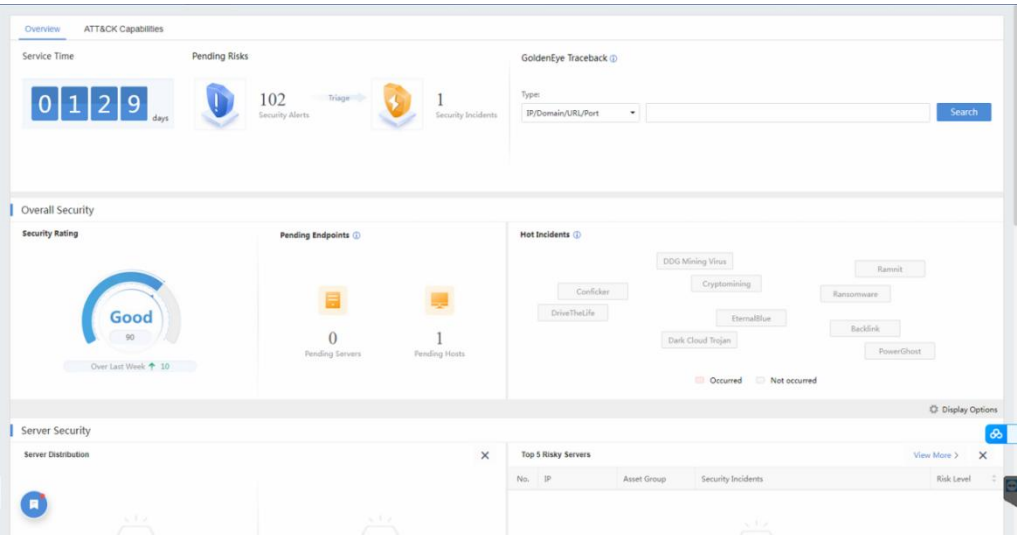
Enter the **Username** and **Password**, and click the **Login** button to log into the Cyber Command device for configuration. The username/password by default is **admin/admin**.

2.2 Configuration and Usage

2.2.1 Configuration and Usage of Cyber Command Console

Log into the Web UI configuration page, and the following configuration modules can be seen: **Home, Response, Analytics, Assets, Reports, More,**

Navigation, and Holistic.



Holistic: Used for unfolding branch information.

All ⓘ icons on the configuration page can display a brief description of the current configuration item when the mouse cursor is placed on this icon.

 NOTE

The holistic module is only displayed after the branch is configured.

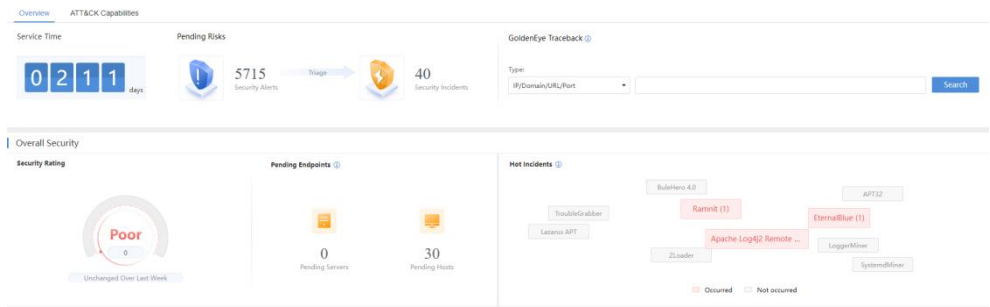
3 Features

3.1 Home

3.1.1 Overview

Comprehensive Security Intelligence

The comprehensive security intelligence displays the general and current situation of Cyber Command, including new events (30 days), fixed and unfixed events, **Security Rating**, **Pending Endpoints**, **GoldenEye Traceback**, and **Hot Incidents**. You can set the display of the overview module in the **Display Options** at the bottom right corner of the interface.

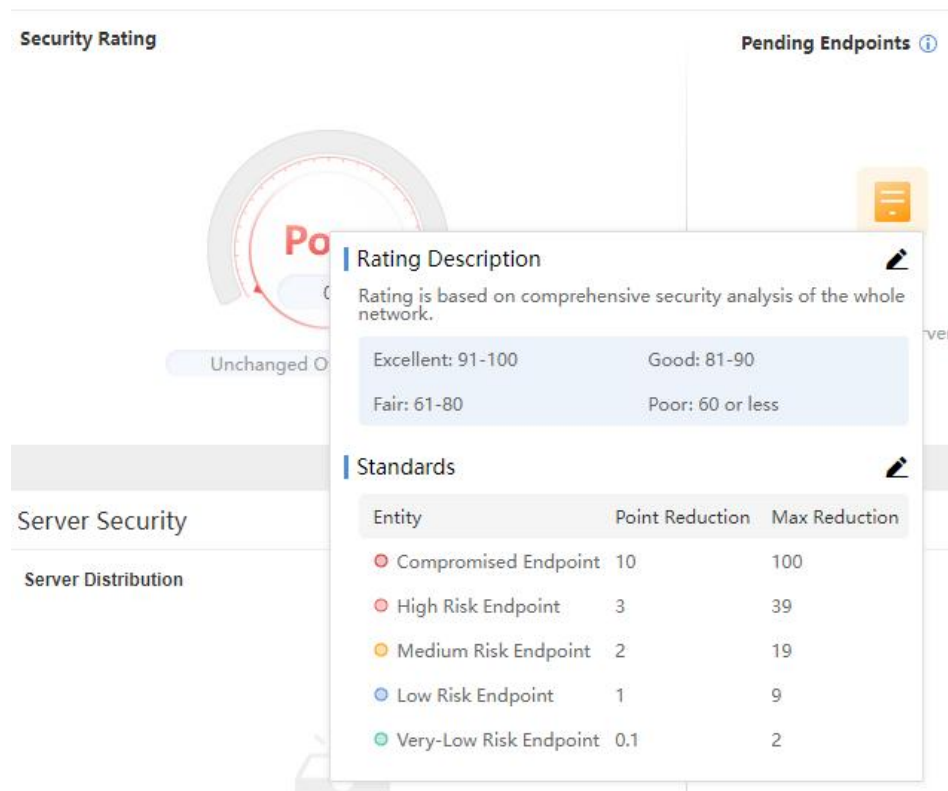


Security Rating: Display the current network rating by giving a score (maximum 100). It includes excellent (91-100), good (81-90), fair (61-80), and poor (60 or less) levels. The rating standard by default is shown in the following table:

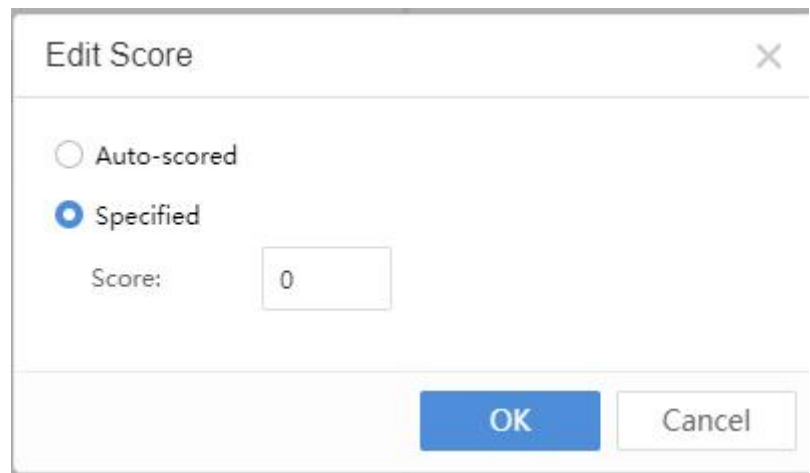
Entity	Point Reduction	Max Reduction
Compromised Endpoint	10	100
High Risk Endpoint	3	39
Middle Risk Endpoint	2	19
Low Risk Endpoint	1	9
Very-Low Risk Endpoint	0.1	2

Table 4: Security Rating

You can customize the security rating standard. When the cursor is placed on the rating, a window shown in the following figure appears.



Click the Edit icon next to the **Rating Description** to select **Auto-scored** or **Specified**, as shown below:



Click the Edit icon next to the **Standards** to modify the rating standard, and click **OK** to submit, as shown below:

Edit Standards

Entity	Point Reduction	Max Reduction	
Compromised Endpoint	10	100	
High Risk Endpoint	3	39	
Medium Risk Endpoint	2	19	
Low Risk Endpoint	1	9	
Very-Low Risk Endpoint	0.1	2	

Restore

Close

- **Pending Endpoints:** Statistically display existing compromised, high-risk, and middle-risk hosts, not low-risk and vulnerable hosts.
- **GoldenEye Tracebacks:** A search and tracking tool integrating access relation, UEBA, and host overview. It can perform a search when finding risky hosts or malicious domains. See chapter 3.1.3 for details.
- **Host Incidents:** Display recent hot incidents in the cyber security industry and rapidly perceive whether they affect the network.
- **Display Options:** Customize contents displayed in the overview.

Display Options

25

Compromised 11

High 9

Medium 5

Low 1

Server Distribution

100

Server Name

IP Address

Score

Top 5 Risky Servers

36

Compromised 11

High 9

Medium 5

Low 1

Host Distribution

100

Host Name

IP Address

Score

Top 5 Risky Hosts

8

User Name

IP Address

Score

User Security

Restore

☒ Select All (8 selected)

OK

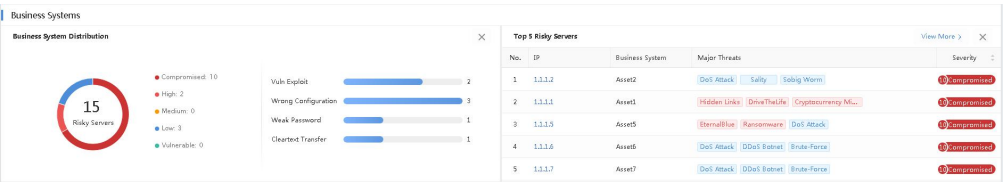
Cancel

Server Security

It statistically displays the distribution of business system security, including compromised, high-severity, middle-severity situations, and TOP 5 risky servers.

Version 01 (May 30, 2024)

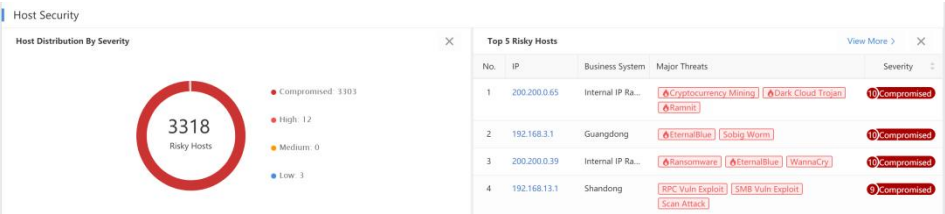
16



- **Server Distribution:** Count the number of compromised, high-severity, middle-severity, low-severity, and vulnerable hosts in the current network, as well as the vulnerability situation of risky servers, including vulnerability, configuration risks, weak password, and cleartext transfer.
- **Top 5 Risky Servers:** Rank the top 5 risky servers by risk level. The hosts with risk levels after the Top 5 will be ranked randomly. Click **View More** to go to **Response > Risky Assets**.

Host Security

It statistically displays the distribution of host security status, including Compromised, High, Medium, Low, and TOP 5 risky hosts.



- **Host Distribution Severity:** Count the number of compromised, high, medium, and low-severity hosts in the current network.
- **Top 5 Risky Hosts:** Rank the Top 5 risky endpoints by risk level. The endpoints with risk levels after the Top 5 will be ranked in random order. Click **View More** to go to **Response > Risky Assets**.

Assets

It statistically displays discovered servers and endpoints in the network.

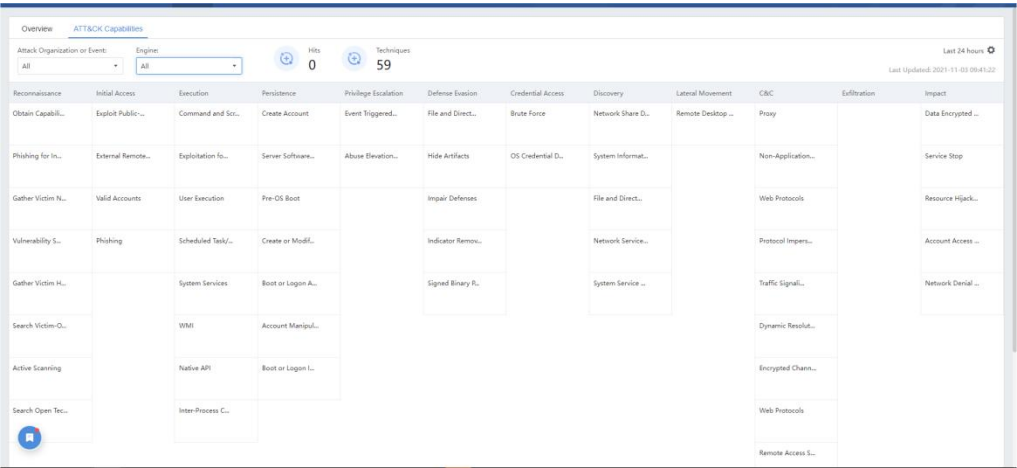


- **Assets:** Display the quantity of servers, the **Server Distribution By Criticality** (the server level shall be defined first), and the **Top 5 Open Ports By Servers**.

ATT&CK Capabilities

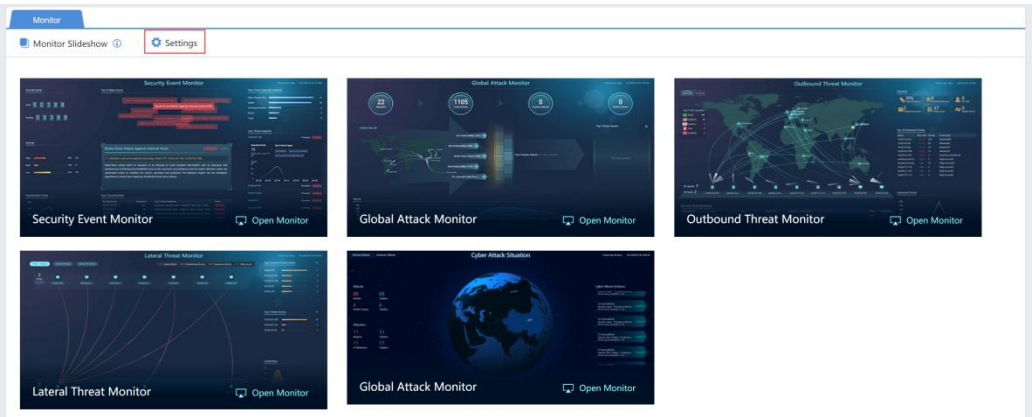
The full name of ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), the framework was first proposed by MITRE in 2013. It is a knowledge base and model used to describe attack behavior.

The Cyber Command has a built-in ATT&CK security framework in this version. The maps display the threats detected within the organization according to **Hits** and **Technique**.



3.1.2 Monitor

Go to **Home > Monitor**. It visually displays the security situation of the whole network from multiple dimensions.



Click **Settings** in the upper-left corner to configure relevant settings, as shown in the

following figure.

Settings

You have configured 3 Groups. [View Details](#)

Basics

Security Event Monitor

Global Attack Monitor

Outbound Threat Monitor

Lateral Threat Monitor

Period:

Last 24 hours

Last 7 days

Last 30 days

Groups:

Select

All

Location:

Johor

Threats:

All

Realtime Alert:

Enable

Settings

Disable

* Slideshow Interval:

30

(second)

Logo:

Show

Hide

Set Display Order

OK

Cancel

- **Basics:** Define configuration for all interfaces, such as data statistics cycle including the last 24 hours, the last 7 days, or 30 days. Decide whether to enable the real-time alert and select the unit's physical location and time interval of large screen rotation.

Settings

Basics

Security Event Monitor

Global Attack Monitor

Outbound Threat Monitor

Lateral Threat Monitor

Enable

* Subject:

Security Event Monitor

* Confidence:

Compromised

High

Low

* Severity:

High

Medium

Low

Set Display Order

OK

Cancel

- **Security Incidents Monitor:** Display a comprehensive security situation of the whole network, and the title name can be customized.

Security Incidents Monitor

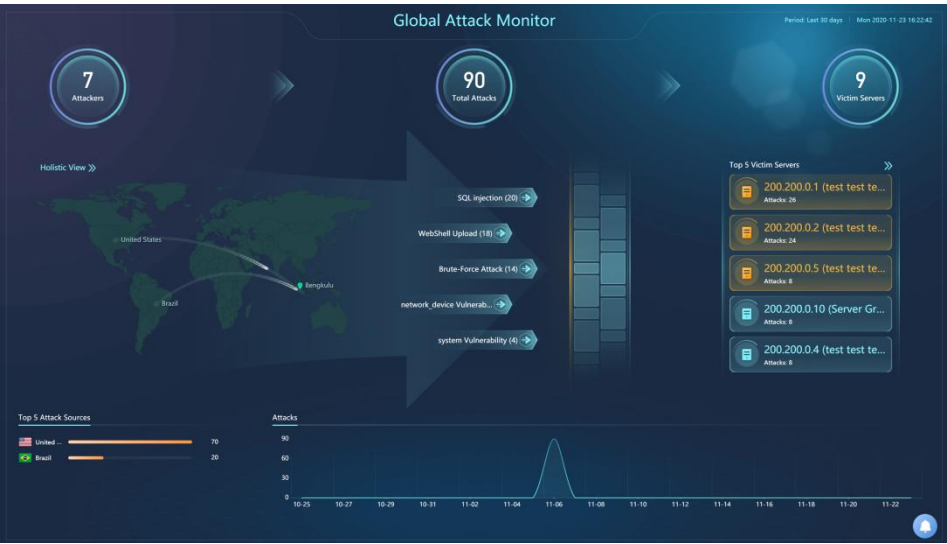
It monitors Security Incidents in LAN and recent hot events of cyber security in real-time to perceive LAN's security situation rapidly.



Global Attack Monitor

It monitors attacks from the outside and visually displays global attacks and threats confronted by LAN. The physical location of attack sources, attack methods, and attack services are displayed clearly.

2D Monitor



3D Monitor



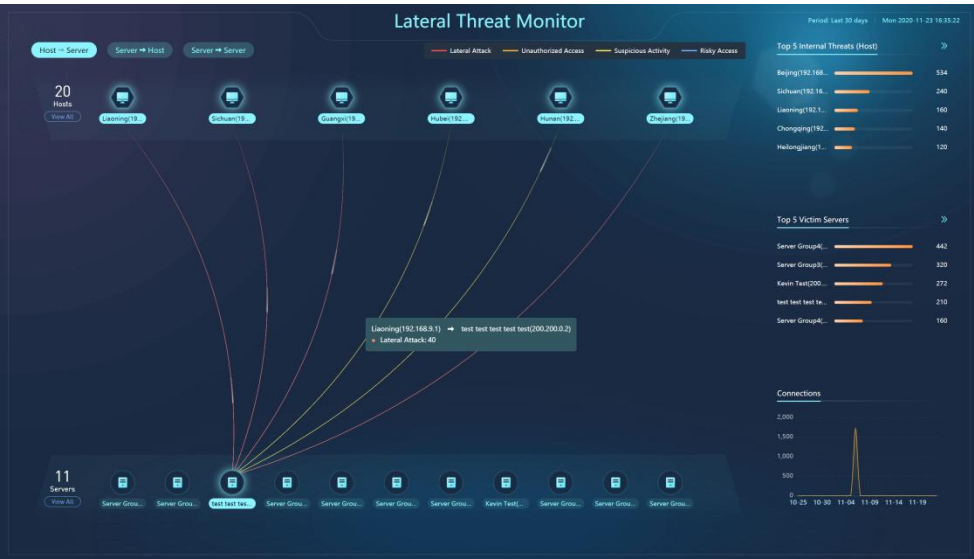
Outbound Threat Monitor

It monitors the risky external connection of services, attacks and C&C communications, and illegal access initiated by the business systems to the outside.



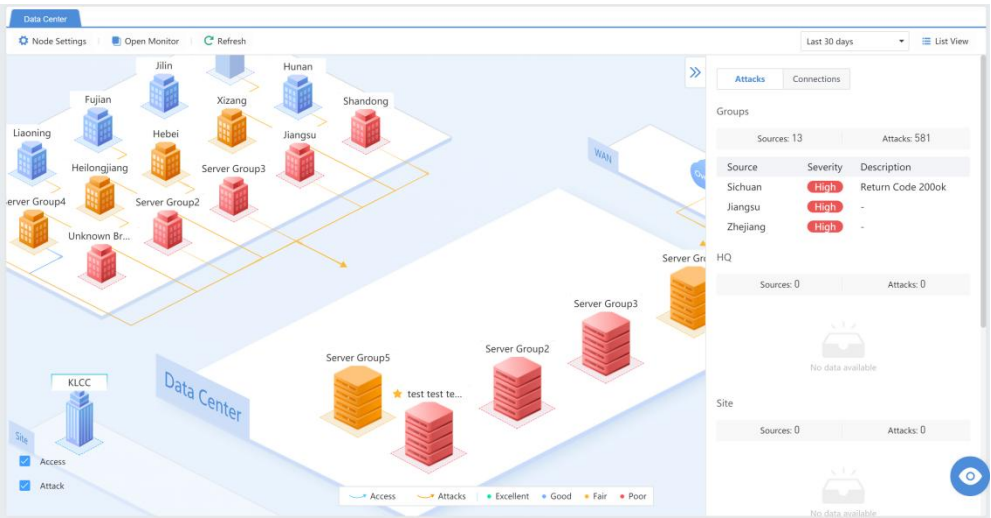
Lateral Threat Monitor

It monitors internal and lateral threats. The internal threats are displayed clearly, including Lateral Attacks, Unauthorized Access, Suspicious Activity, and Risky Access.



3.1.3 Data Center

Administrators can visually check the security status of server assets and support filtering based on the time range.

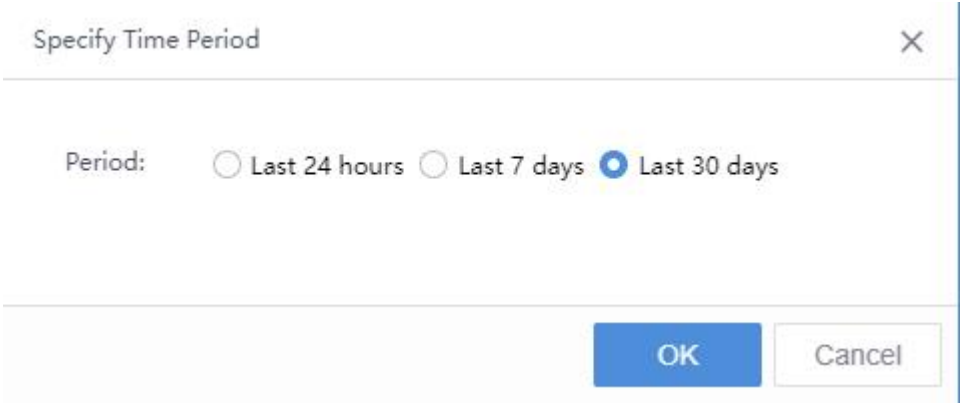


3.1.4 ATT&CK Capabilities

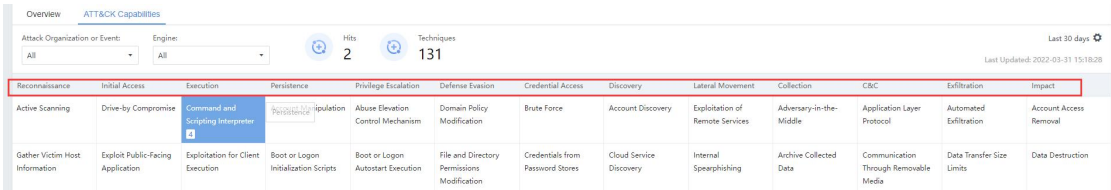
The ATT&CK model mainly integrates historical hacking organizations and attacks and uses attack strategies as clues to link attack technologies and software corresponding to different attack strategies. It provides an executable model of intermediate abstraction for information security practitioners. The ATT&CK Capability Map maps the current state of intranet security to the various stages of the model, as shown in the figure below.

OverviewATTACK Capabilities												
Attack Organization or Event:		Engine:		Hits		Techniques		Last 30 days				
All		All		2		131		Last Updated: 2022-03-31 15:18:28				
Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	C&C	Exfiltration	Impact
Active Scanning	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Domain Policy Modification	Brute Force	Account Discovery	Exploitation of Remote Services	Adversary In-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	File and Directory Permissions Modification	Credentials from Password Stores	Cloud Service Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Network Information	Hardware Additions	Inter-Process Communication	Browser Extensions	Event Triggered Execution	Hide Artifacts	Exploitation for Credential Access	Domain Trust Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Org Information	Phishing	Native API	Create Account	Exploitation for Privilege Escalation	Impair Defenses	Forced Authentication	File and Directory Discovery	Remote Services	Clipboard Data	Dynamic Resolution	Exfiltration Over C2 Channel	Endpoint Denial of Service
Obtain Capabilities	Supply Chain Compromise	System Services	Create or Modify System Process	Scheduled Task/Job	Indicator Removal on Host	Modify Authentication Process	Network Service Scanning	Replication Through Removable Media	Data Staged	Encrypted Channel	Exfiltration Over Other Network Medium	Initial System Recovery
Phishing for Information		User Execution	External Remote Services		Modify Registry	OS Credential Dumping	Network Share Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Physical Medium	Network Denial of Service
Search Open Technical Databases		Windows Management Instrumentation	Office Application Startup		Obfuscated Files or Information	Steal Application Access Token	Network Sniffing	Taint Shared Content	Data from Information Repositories	Ingress Tool Transfer	Exfiltration Over Web Service	Resource Hijacking
Steal User-Owned Data			Pre-OS Boot		Rogue Domain Controller	Steal Web Session Cookie	Password Policy Discovery	Use Alternate Authentication Material		Multi-Stage Channels	Scheduled Transfer	Service Stop

- **Attack Organizations or Incident:** Famous hacking organizations or attacks in the past, such as APT32, APT28, DarkVishnya, Kinsing, etc.
- **Engine:** It includes five major detection engines of Cyber Command: Rule Engine, Threat Intelligence Engine, File Analytics Engine, Attack Analytics Engine, and Abnormal Behavior Analytics Engine.
- **Hits**
- **Techniques**
- **Specify Time Period:** The data of the last 24 hours is displayed by default, and the data display of the last 7 days and the last 30 days is also supported, which can be adjusted by clicking ⚙️, as shown in the figure below.



- **ATT&CK model phase:** It includes reconnaissance, initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command control(C&C), exfiltration, and impact, as shown in the following figure.

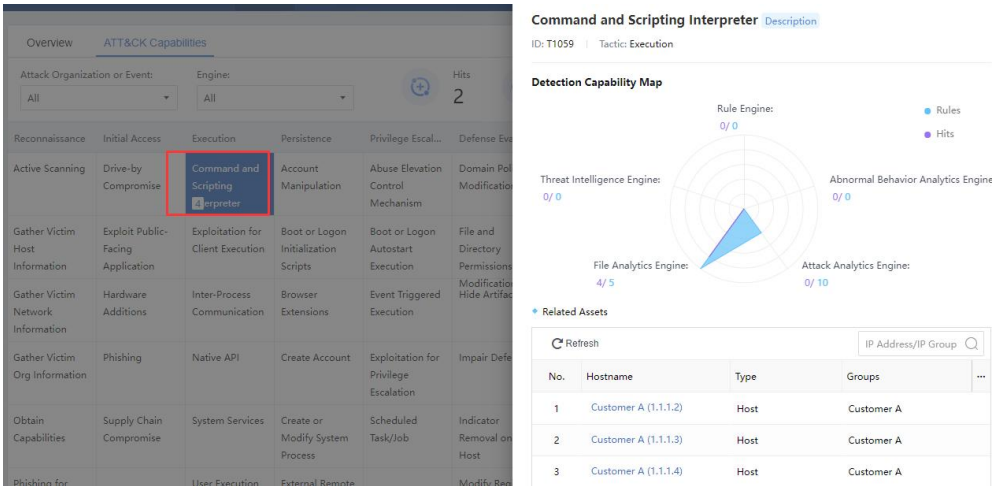


- **Detection technology cell:** ATT&CK capability spectrum below each stage of detection technology. When the color is dark blue, it indicates that the detection technology is currently hit. When the color is white but has a specific detection technology name, it means that the phase Cyber Command has a corresponding detection technology but has not been hit. Null indicates that the detection technology is empty, as shown in the figure below.



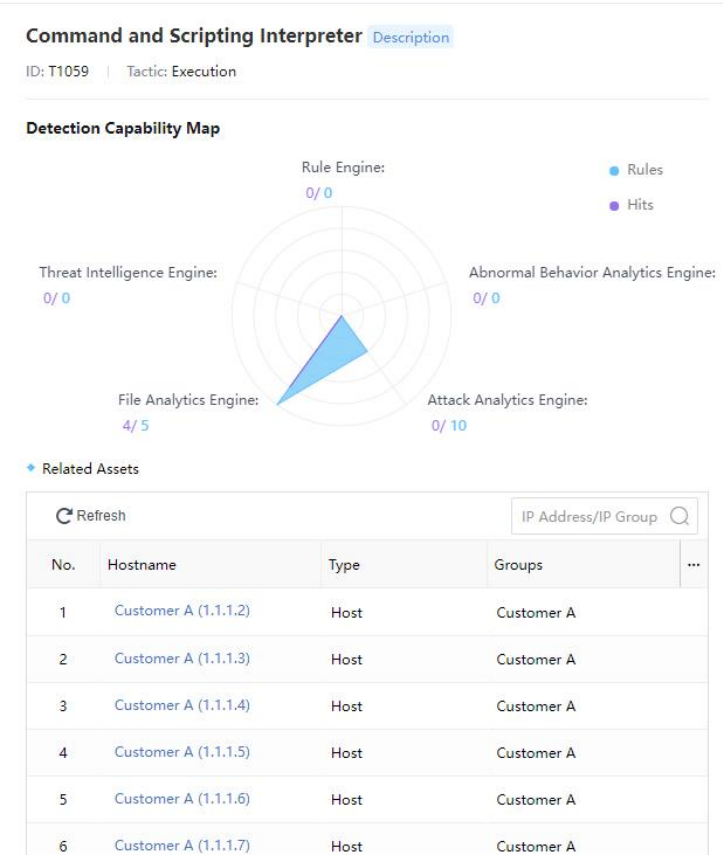
The color distribution and detection technology distribution of the ATT&CK capability map will change as the version evolves, the time of Cyber Command deployment in the intranet, and changes in abnormal traffic such as attacks.

At each stage of the ATT&CK graph, several detection technologies of Cyber Command will be matched. Click on the right side of the detection technology desktop to pop up the instructions page, as shown in the figure below.

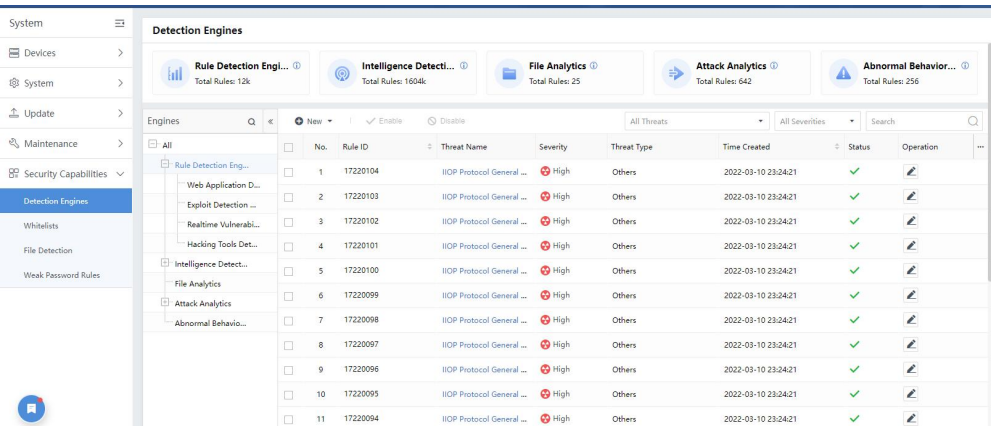


The detection engines include **File Analytics Engine, Threat Intelligence Engine, Attack Analytics Engine, Abnormal Behavior Analytics Engine, and Rule Engine**. The blue number represents the number of rules for this engine

type, and the purple number represents the number of rules currently hit, as shown in the figure below.



Clicking the number will automatically jump to the **System > Security Capability > Detection Engine** page, as shown in the figure below.



ATT&CK and Security Alert are two independent modules. Logically, there is no dependency between the two. The rule's properties include both ATT&CK-related words and security alert-related columns.

3.2 Response

Cyber Command collects log information by accessing devices such as STA and NGAF. It discovers Security Incidents in the corresponding services or endpoints based on big data analysis. You can find risky services and endpoints and view, analyze, and handle corresponding Security Incidents in **Response**.

3.2.1 Risky Assets

Cyber Command can classify and display risky assets according to risk level, status, etc so that administrators can screen and respond to the risky assets.

Risk Asset Filtering

Administrators logging in to Cyber Command can support filtering in the following ways under the **Response > Risk Assets** page:

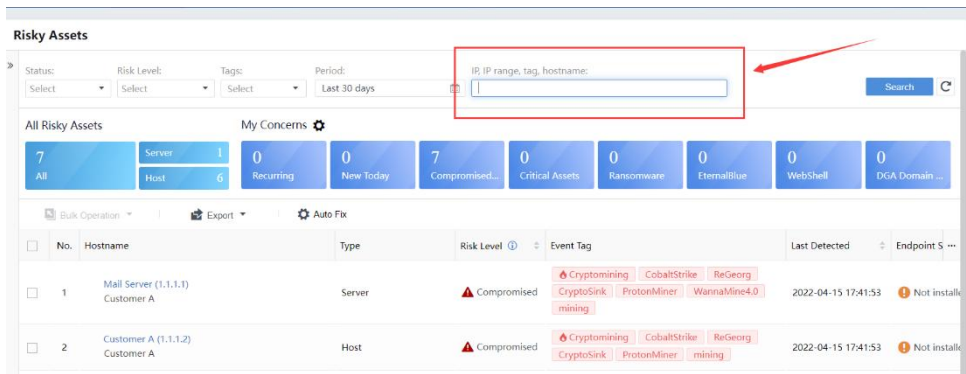
1. Filter the **details of risk assets under** the specified **asset group** through the asset group in the left column;
2. Status filters risk assets in the same **Status** to facilitate batch fixed, including **All**, **Pending**, **Suspended**, **Fixing**, and **Fixed**.
3. All risky assets with the same risk level are screened by **Risk Level**, including **All**, **Compromised** and **High Risk**. When the risk level of the risky asset is **Compromised** or **High**, the administrator needs to fix it promptly to avoid business interruption caused by the spread of risk.



Compromised events occurred in the following attack stages: C&C, propagation, and impact. The endpoint has been or is about to be controlled. Please fix it as soon as possible.

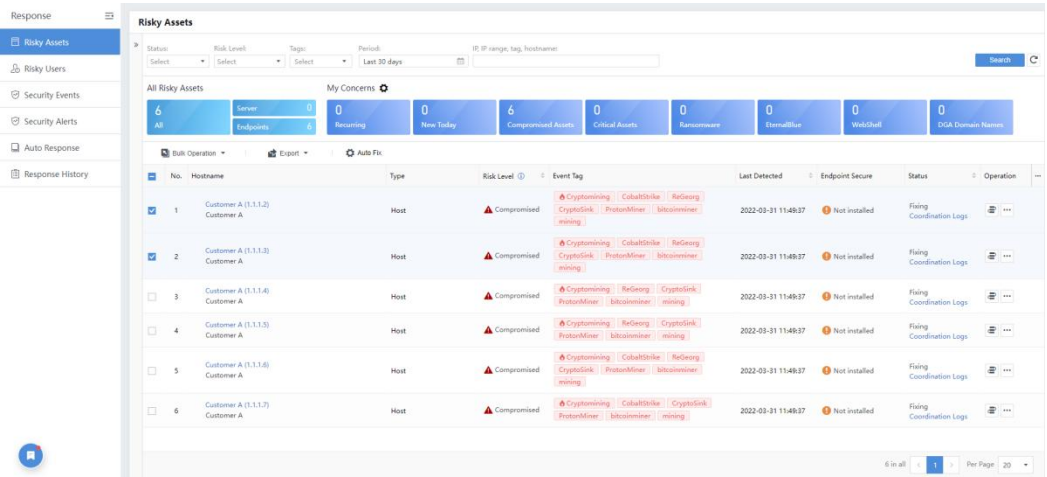
Events occurred in the following attack stages: weaknesses found, reconnaissance, and exploitation. Please fix it as soon as possible.

- 4. Filter all risk assets of the same Security Incidents through **event tags**, including **All, DNS Tunnel, Phishing, Eternal Blue, Blast, FTP Scan, Micro Quarantine, Web Command Injection**, etc. All event tags are built into the platform.
- 5. Filter all risk assets within a specified date by a **Period** so that administrators can view and handle the risk details within a specified date. The time range includes the **last 30 days, last 7 days, last 24 hours**, and **custom**.
- 6. Cyber Command supports filtering by **IP, IP range, tag, and hostname**.



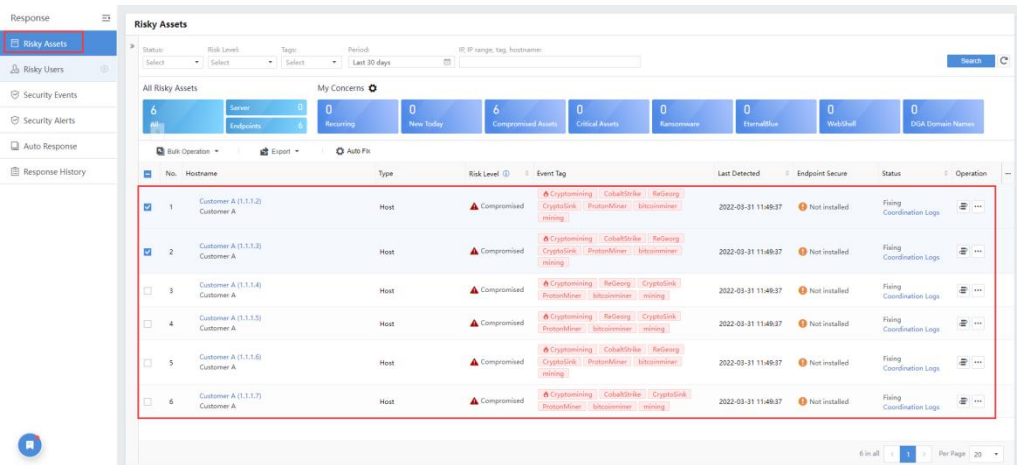
- 7. Module filtering is also supported. For example, if you click **Server**, all risk assets with the asset type of server will be displayed in the list.

Filtering in one or more ways is convenient for administrators to locate the location of risk assets accurately and respond to risk assets by analyzing the details of risk assets in multiple dimensions. For example, the filter will also filter the asset group and list data, as shown below. At the same time, the filter box will remember the last selected state, so you don't have to select it again.



View Risky Assets

On the **Risky Assets** page, administrators can view the asset organization structure of the current platform, an overview of all risky assets, details of the asset risks of **My Concerns**, and a list of risky assets, as shown in the following figure.

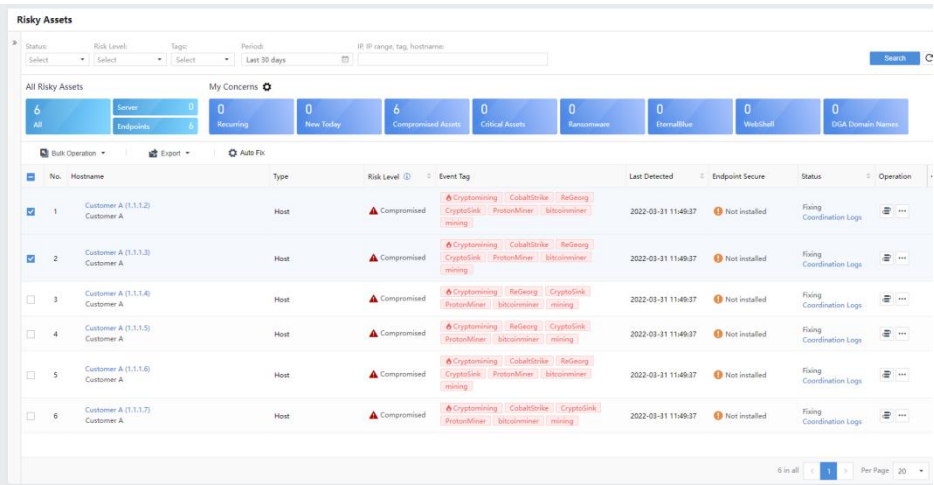


All Risky Assets

By default, the platform displays all the risky assets in the last month, identified as risky hosts and risky servers. It can be filtered according to requirements. The filter will filter the asset group, my concern, and the list of data. Click the hostname to view the corresponding risk asset details in the asset list.

My Concerns

The administrator can specify the content to follow by clicking the item under **My Concerns**. You can display the filtered content and click  again to cancel the filter.

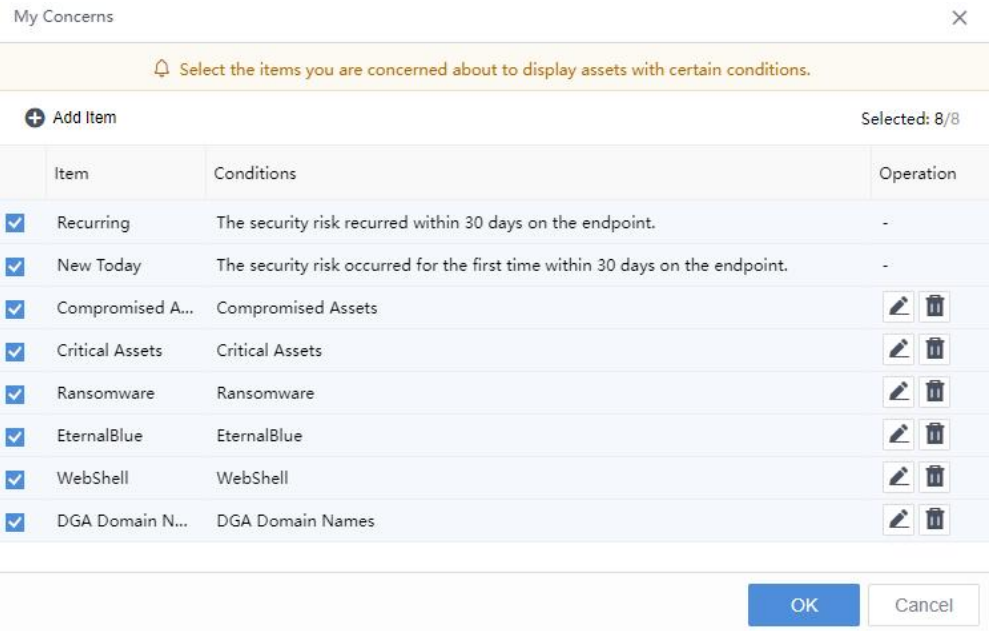


Configure My Concerns

- Click the configuration button  to configure **My Concerns**, as shown in the following figure.

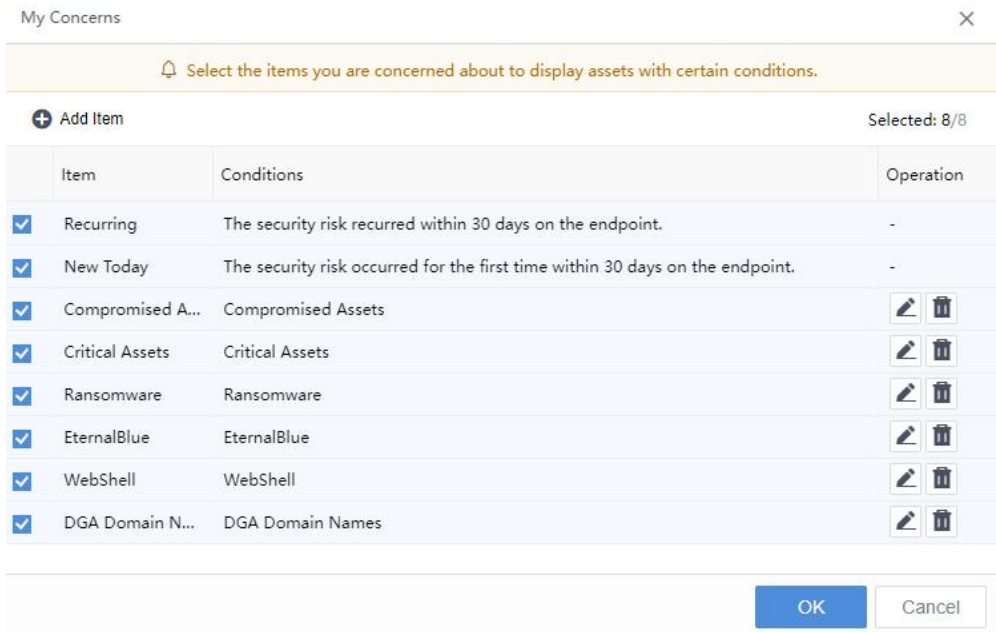


- You can customize **My Concerns**. By default, it will show **Recurring**, **New Today**, **Compromised Assets**, **Critical Assets**, **Ransomware**, **EternalBlue**, **WebShell**, and **DGA Domain Names**. You can uncheck the specific checkbox if you do not want to show it.

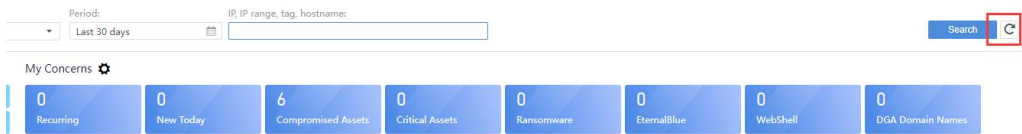


- You can also add a new **My Concern** group, configure the content, and check the checkbox to display it. Take the example of configuring the **Item**

type of the Conditions group. For the groups you follow, you can also edit them by clicking the Edit icon.

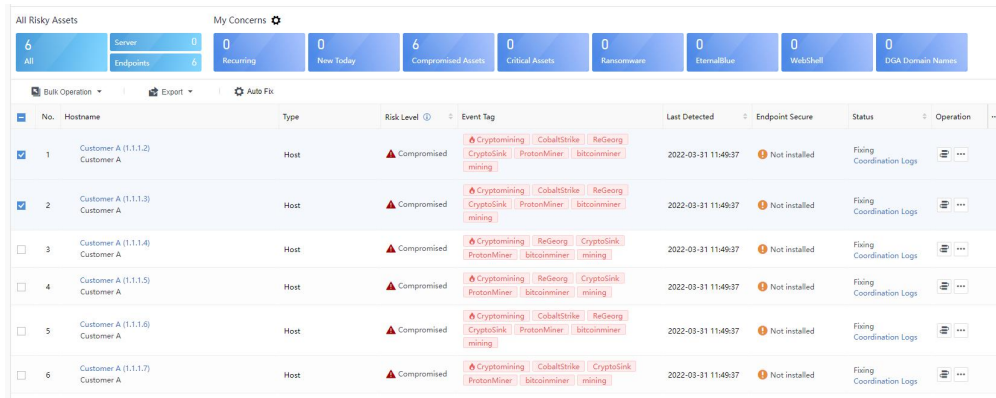


- Click the Refresh icon to view the newest content in **My Concern** on Display, as shown in the image below.



1. Risky Assets

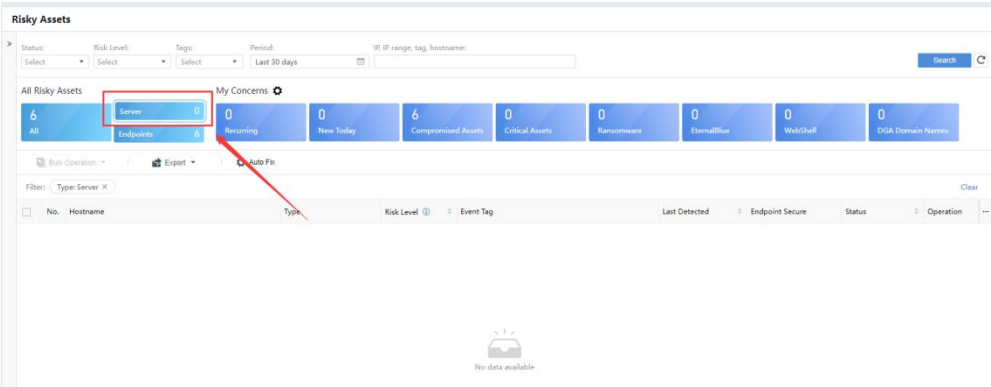
In the list, administrators can view the **Hostname**, **Risk Level**, **Type**, **Security Incidents**, **Last Detected**, **Endpoint Secure**, etc.



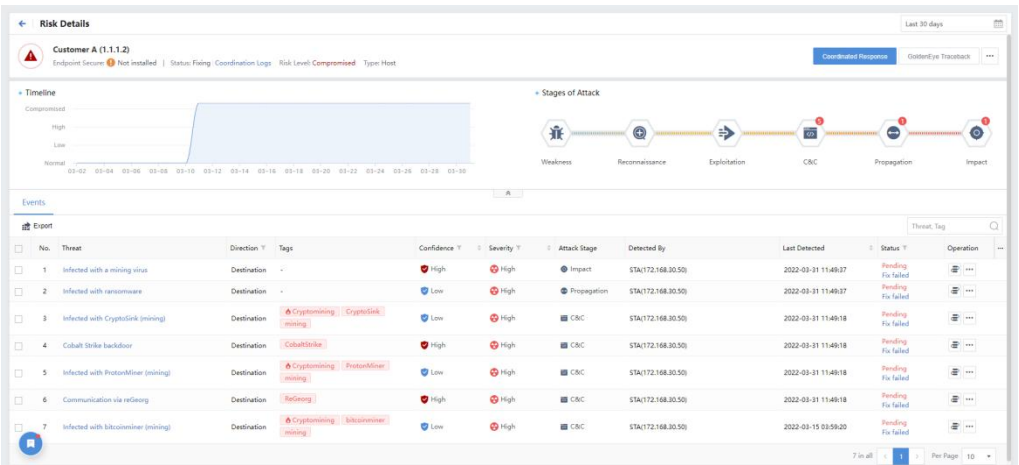
Click to handle the corresponding event:

- by **Server**

Under All risk assets, click **Server**, and the list displays all risk assets whose assets are the server.



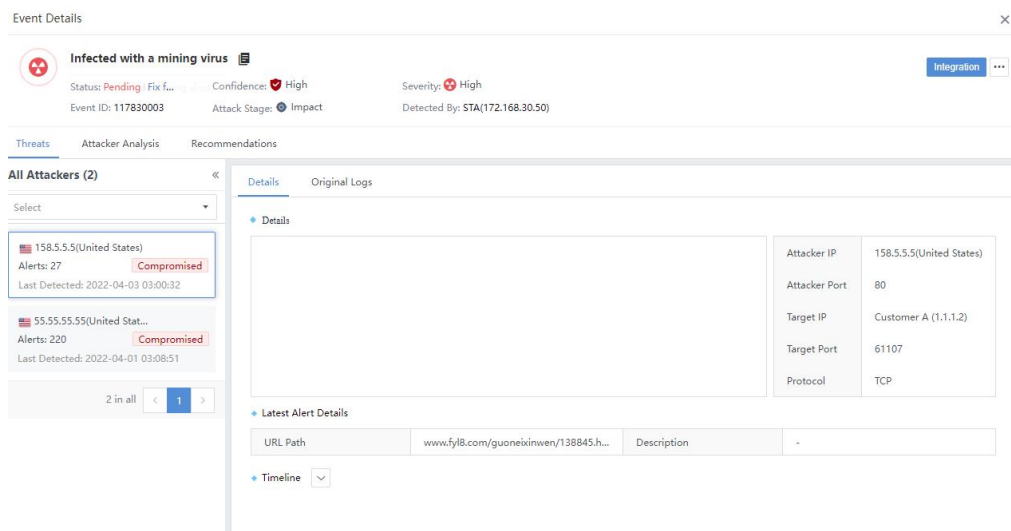
Click the listed **Hostname** to view the details of the risk server, displaying data statistics, Security Incidents, event perspectives, and threat entities, as shown in the following figure.



The **Timeline** and **Stages of Attack** distribution are displayed by default under the statistics column, as shown in the following figure.

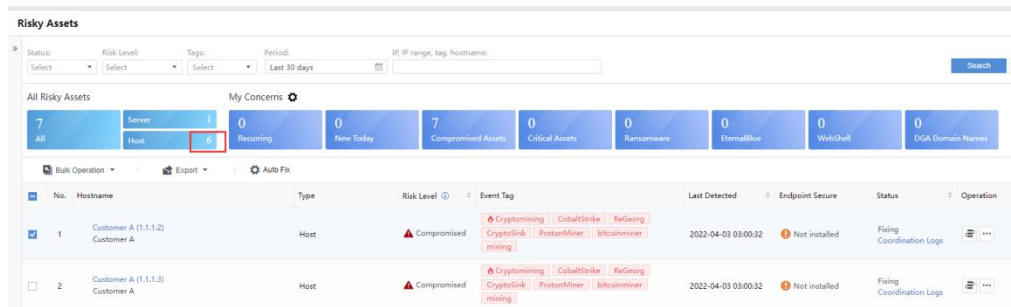


Click the **Threat name** to view detailed information such as **Threats**, **Attacker Analysis**, **Recommendations**, and the risk of specific Security Incidents, as shown in the following figure.

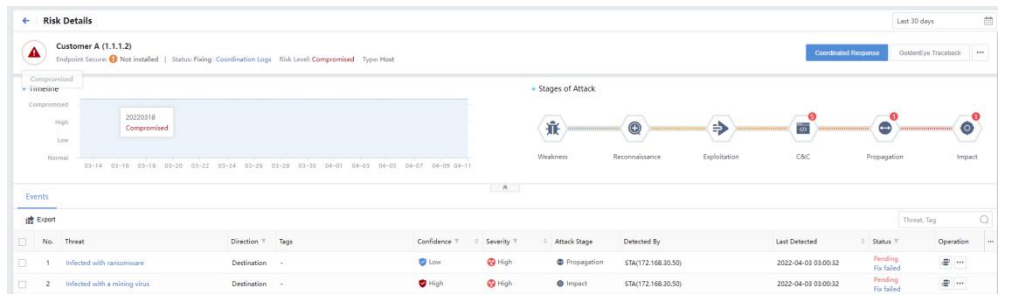


- by **Host**

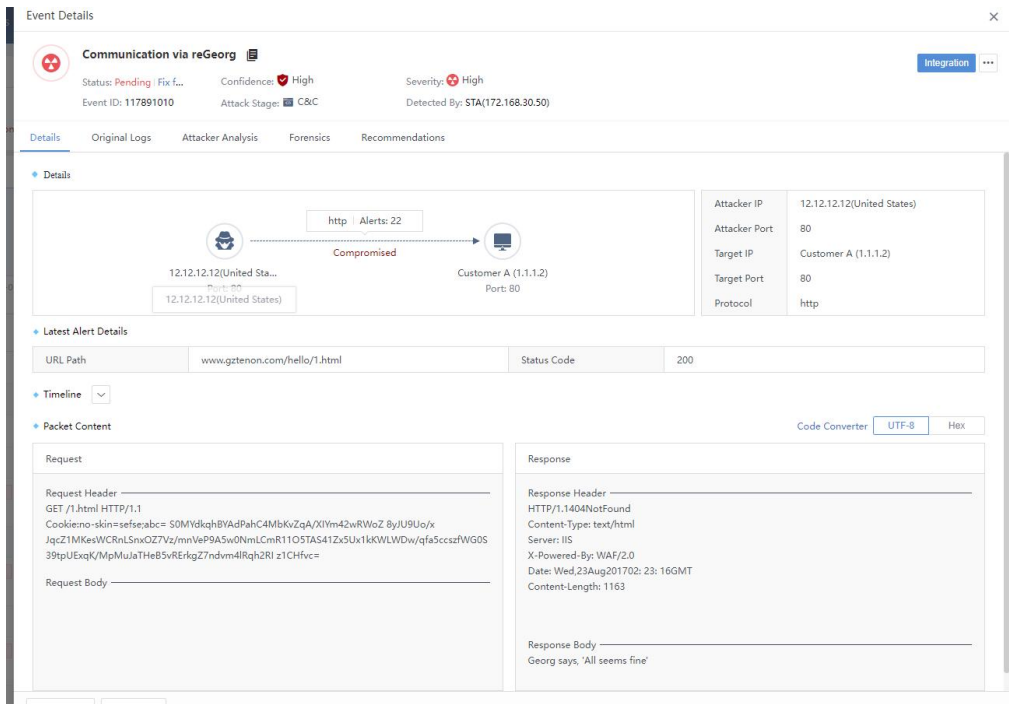
Under All risk assets, click **Host**, and the list displays all risk assets whose assets are the host.



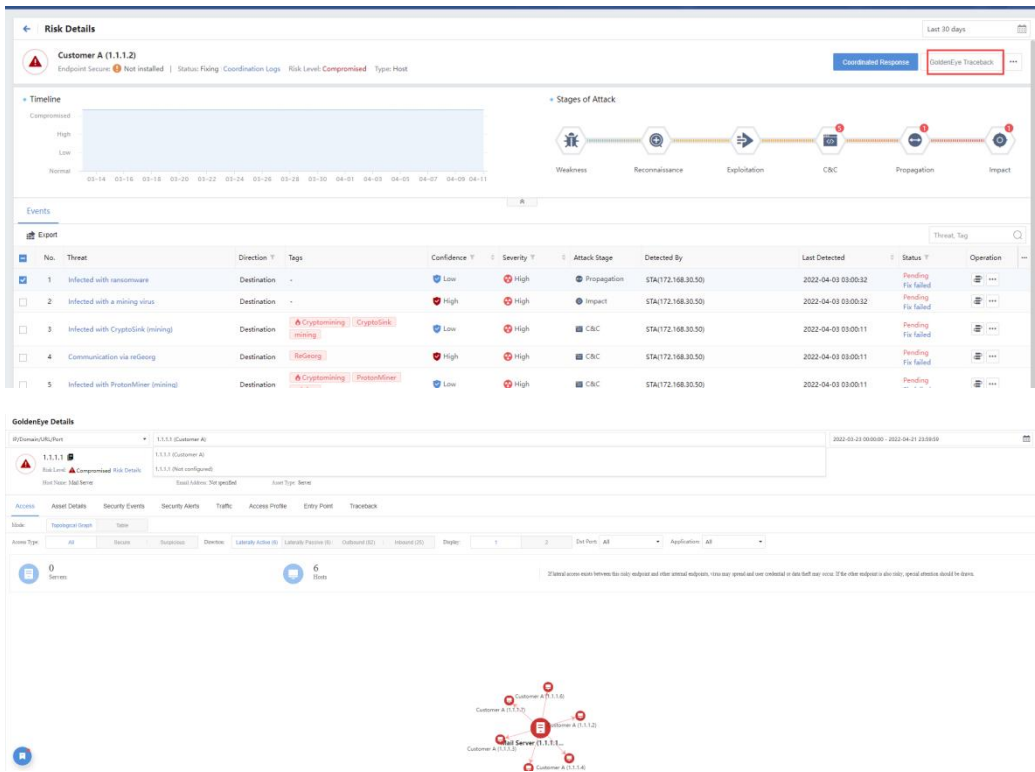
Click to view the risk details of the risky host, showing the asset level event, stage of attack, incidents, threat entities, etc., as shown in the following figure.

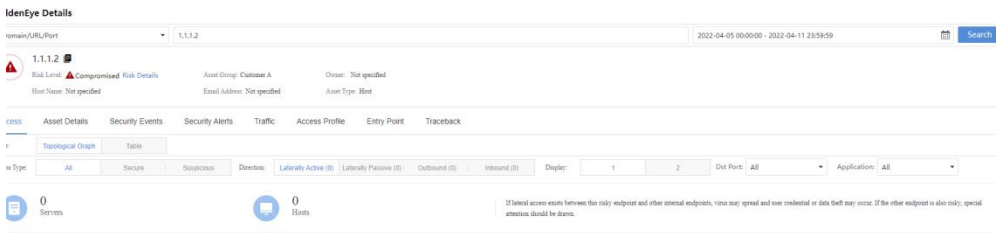
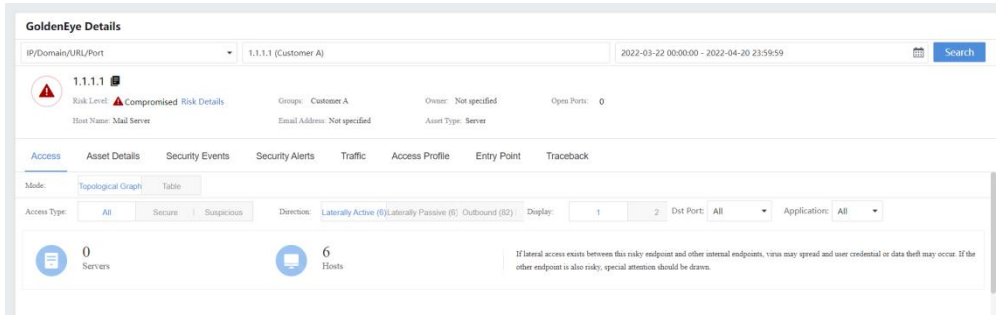


Click a specific event to view the detailed information, original log, attack analysis, recommendations, and risk Impact of the Events, as shown in the following figure.



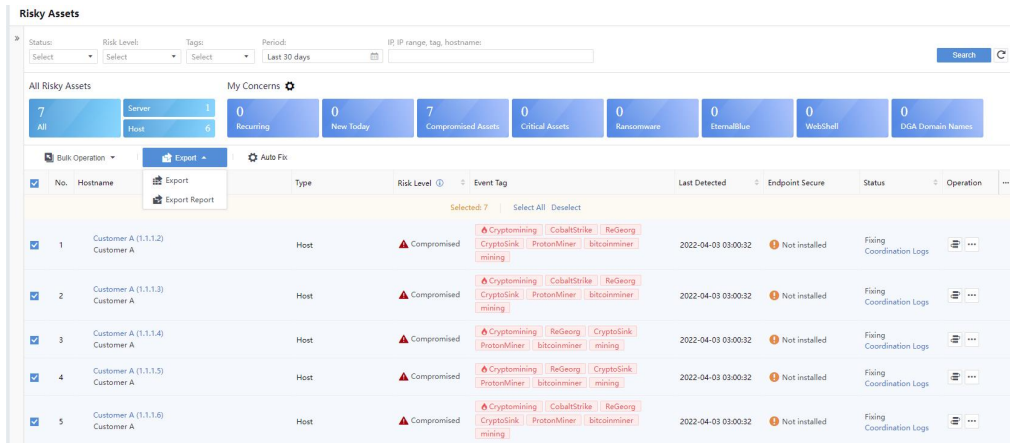
Click the Risk **Details** page to jump to the risk detail investigation page to show **GoldenEye Traceback**. You can view the **Access**, **Access Details**, **Security Incidents**, **Security Incidents**, **Traceback**, etc., as shown below.





2. Export the risky assets

You can export the list and risk report on the **Risk Assets** page. Click  **Export** to export all the current page data by default, and the file format is **.xlsx**. At the same time, click a specific risk asset IP to jump to the Risk Detail page. On the **Risk Details** page, you can export the list of Security Incidents.



Click **Export** to configure the report as required, such as **Period**, **Asset Group**, **Format**, **Report Name**, and **Items**, as shown below.

Export Endpoint Security

Period:

Last 7 days

Asset Group:

All

Format:

.pdf

Report Name:

Default

Custom

* Items

Latent Threat

Weakness

Export

Cancel

3. Edit Endpoint Secure Forensics

After ES accesses the Cyber Command platform, the risk endpoint on the ES side synchronizes the botnet logs to the platform. Cyber Command can display the process and file information of accessing malicious domain names to help users conduct research and judgment. Hover the mouse over the operation

column and click  to obtain the forensic information.

Coordinated Response Details

systemExecuted Action: Push Down Virus Scan Task (Before 8minutes)

Executed

system Executed Action: View Virus Scan Results (Remaining Latency -1000Milliseconds)

Waiting for Execution

Automatically Executed Policies: Auto Scan Endpoints

systemExecuted Action: Push Down Virus Scan Task (Before 13minutes)

Executed

systemExecuted Action: View Virus Scan Results (Before 5minutes)

Executed

systemExecuted Action: Isolated Hosts (Before 5minutes)

...

Automatically Executed Policies: Auto Scan Endpoints

systemExecuted Action: Push Down Virus Scan Task (Before 17minutes)

Executed

systemExecuted Action: View Virus Scan Results (Before 9minutes)

Executed

systemExecuted Action: Isolated Hosts (Before 9minutes)

...

Automatically Executed Policies: Auto Scan Endpoints

2022-04-21 15:36:22

2022-04-21 15:32:07

2022-04-21 15:26:18

Cancel

3.3 Risky Users

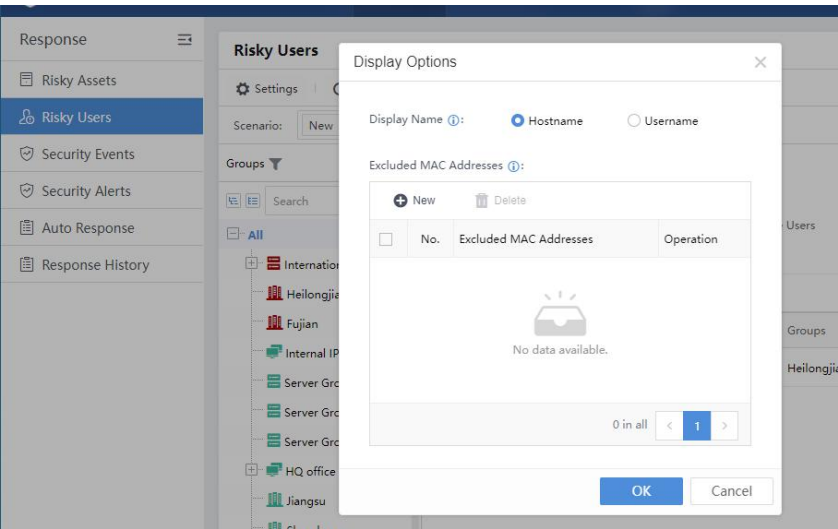
Version 01 (May 30, 2024)

35

User's Source

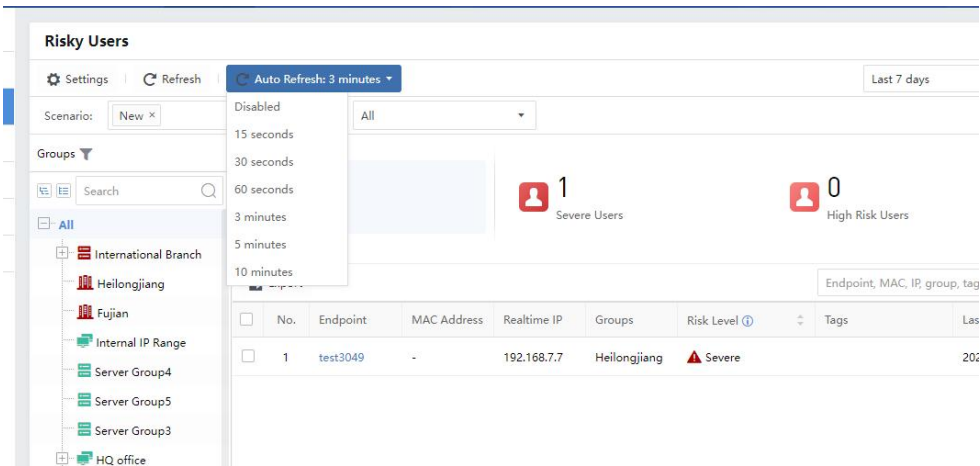
It is required to correlate with IAG, SVPN, and WAC to use their user authentication information. The discovered risky endpoints can be directly viewed in **Risky Users**.

Go to **Response > Risky Users**, and click **Settings** to select the display name: **Hostname** or **Username**.

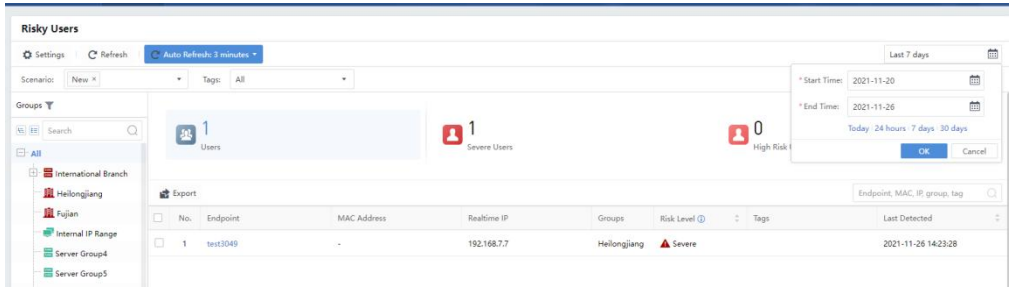


View Risky Users

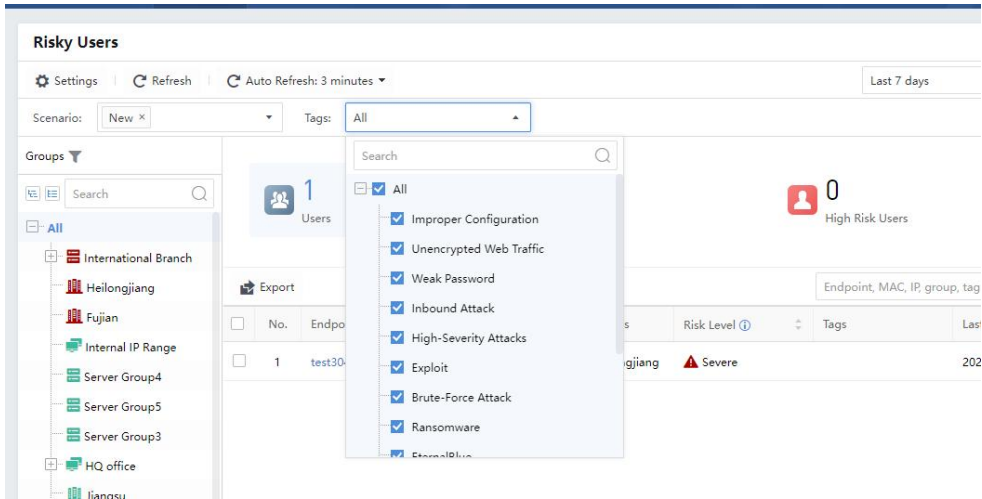
The default **Auto Refresh** time of the Risky Users is 3 minutes for data synchronization. You can manually select other time frequencies, as shown in the figure below.



There are two scenarios for risky users: **All** in Groups and **Today**. If risk users who only pay attention to the day's increment use the **Today** scenario, you can select a maximum of **30 days**, as shown below.



Risky users' time can also be retrieved based on threat event **Tags**, as shown below.



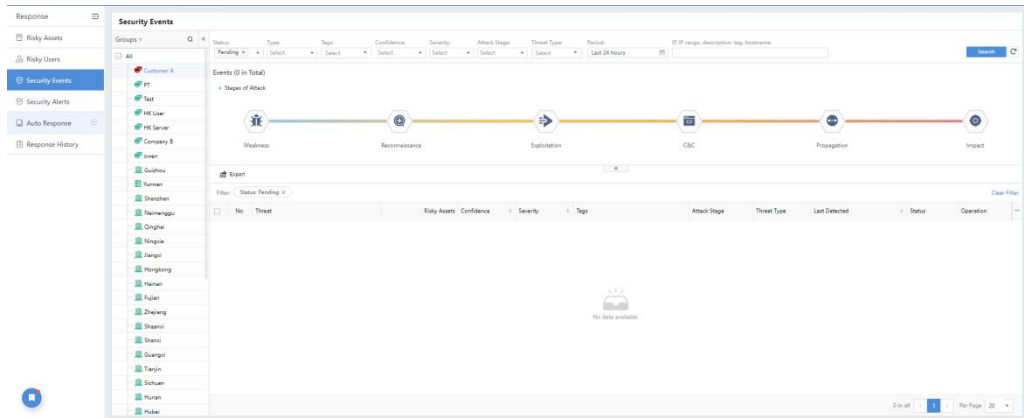
3.4 Security Incidents

Security Incidents

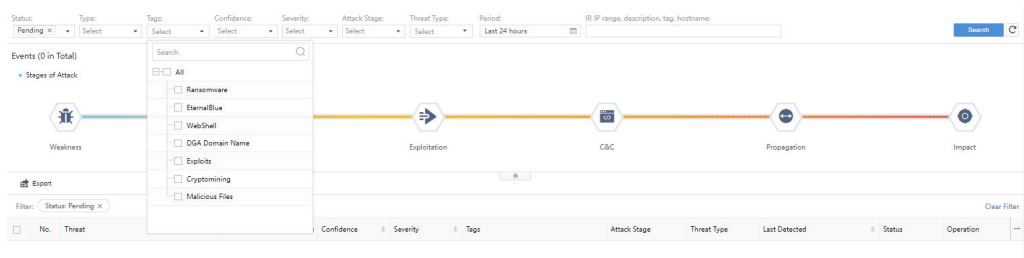
The threat perspective mainly provides queries, statistics, traceability, and proof of Security Incidents and Security Alerts. Security Incidents are obtained by correlating multiple dimensions such as high reliability, high threat, and successful attack Security Alerts based on Security Alerts and matching them through a special built-in algorithm.

3.4.1 Security Incidents filtering

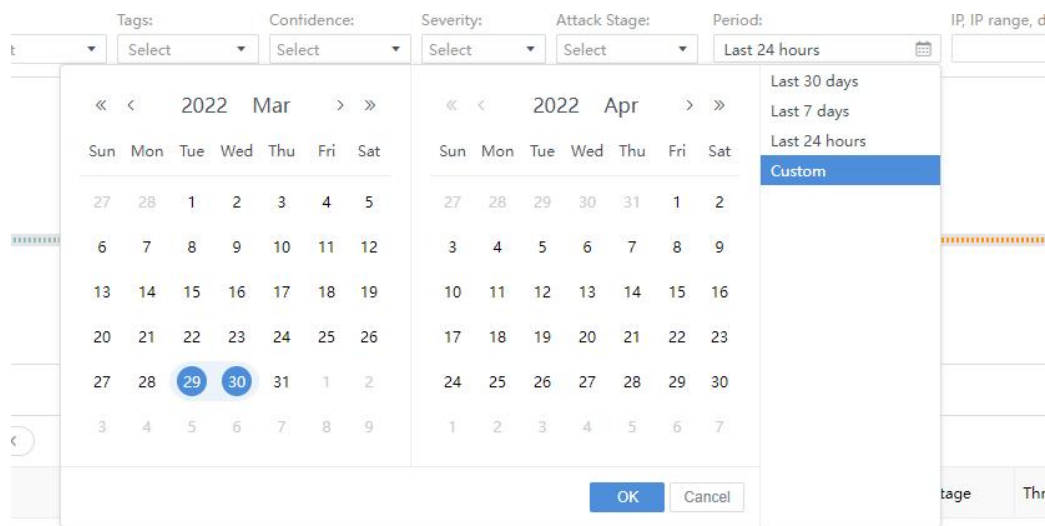
On the **Response > Security Incidents** page, you can see the distribution of Security Incidents, which can be filtered according to your need, as shown in the following figure.



- **Status:** All, Suspended, Pending, Fixing, Fixed.
- **Type:** All, Server, Host.
- **Tags:** Tags were mainly extracted from a hot event or name in the industry, such as Ransomware, WebShell, EternalBlue, etc., as shown in the following figure.



- **Severity:** According to the comprehensive assessment of the impact scope and depth of Security Incidents, divided into **All**, **High**, **Medium**, and **Low**.
- **Attack Stage:** Stage matching of Security Incidents based on industry-standard attack chain models, divided into **All**, **Weakness**, **Reconnaissance**, **Exploitation**, **C&C**, **Propagation**, and **Impact**.
- **Threat Type:** Includes Low, Medium, and High.
- **Period:** Filter for the Security Incidents based on period. You can choose **Last 30 days**, **Last 7 days**, **Last 24 hours**, or **Custom**. Choose **Custom** to filter the Security Incidents beyond 30 days, as shown in the following figure.



- **Search:** You can search the Security Incidents based on IP, IP range, description, or hostname.

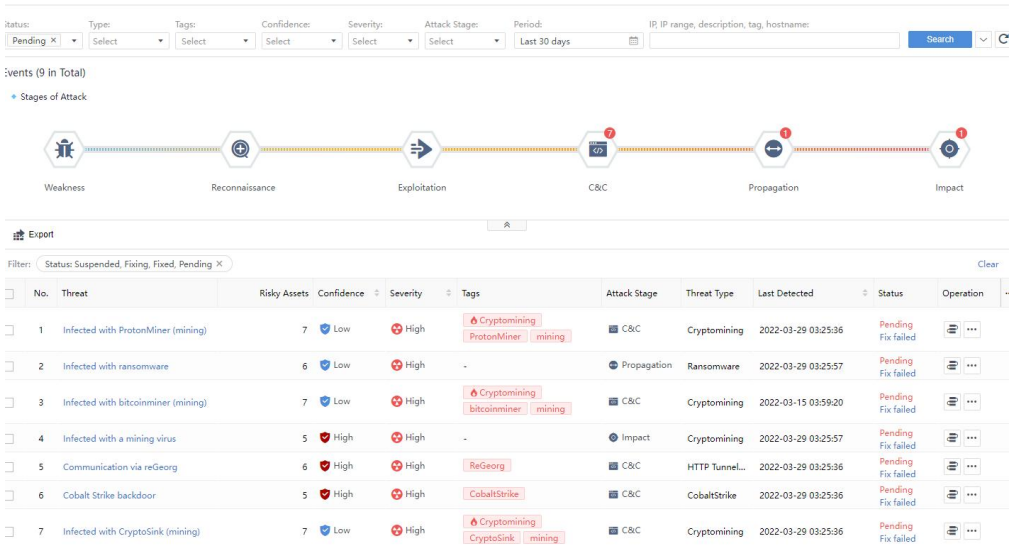
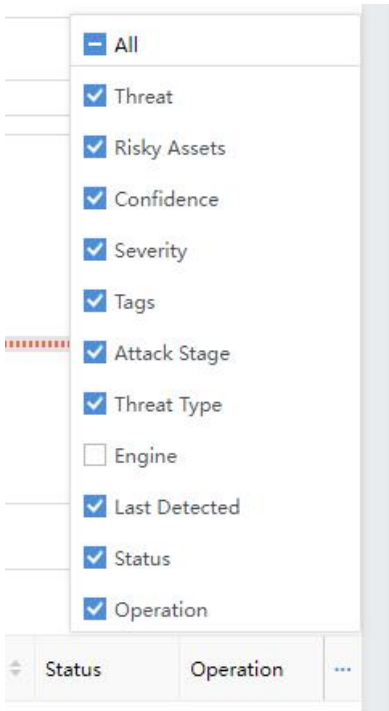
3.4.2 Incidents

In the middle section of the **Security Incidents** page, you can see the **Events** statistics, divided into several sections according to the event attributes: **Weakness**, **Reconnaissance**, **Exploitation**, **C&C**, **Propagation**, and **Impact**. Each section has specific quantitative statistics. The total number of incident attribute categories is the same as the number of incident attribute categories, as shown in the following figure.



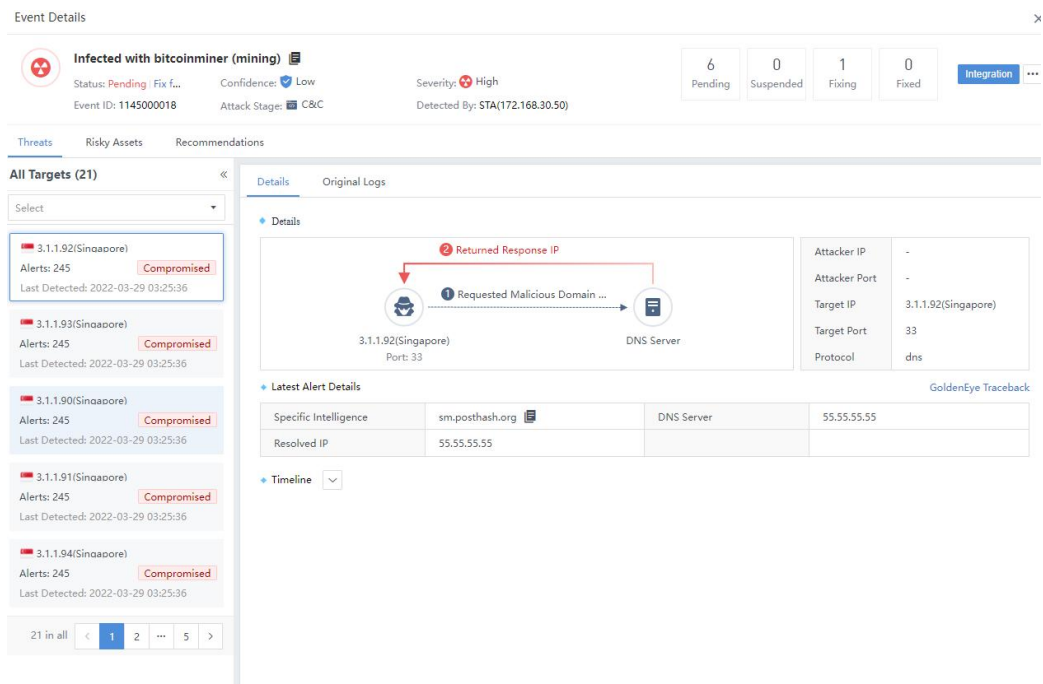
3.4.3 View Incidents

Perform search based on the above conditions to see a list of specific Security Incidents. The dimensions of each Security incident include **Threat**, **Risky Assets**, **Confidence**, **Severity**, **Tags**, **Attack Stage**, **Threat Type**, **Engine**, **Last Detected**, **Status**, and **Operation**, as shown in the following figure.

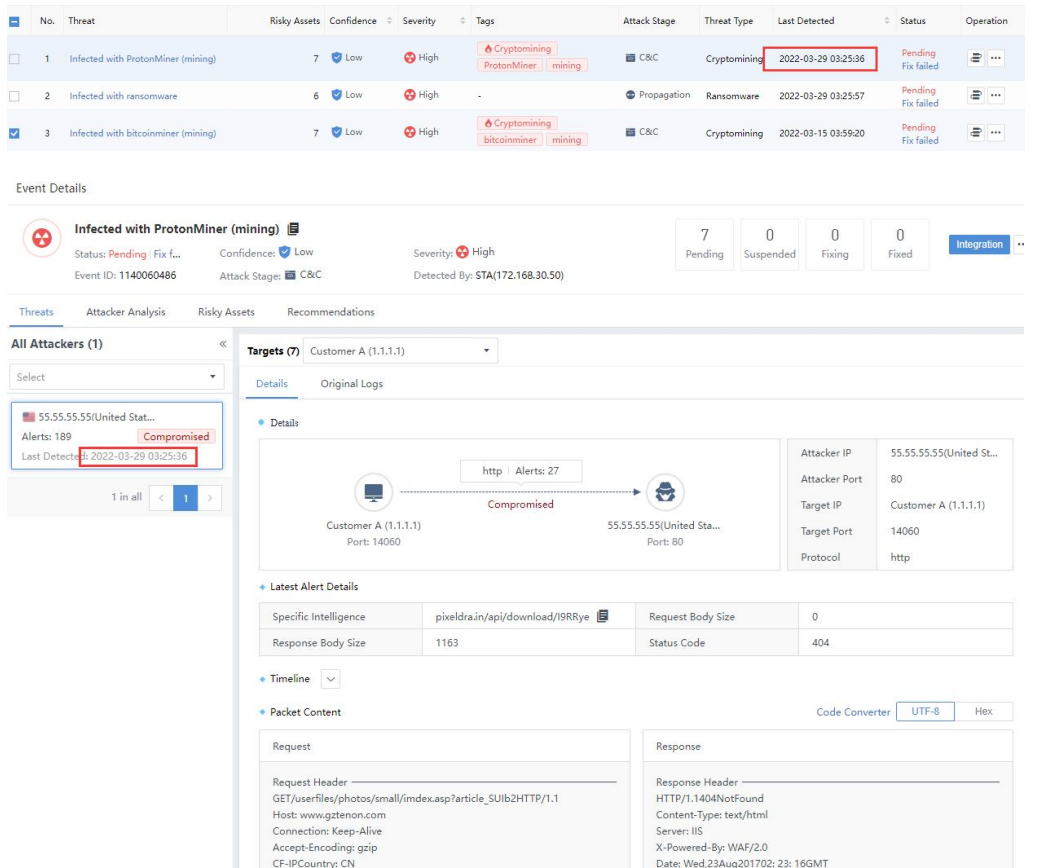


- **The number of Risky Assets:** Represents the risk assets associated with the Security Incidents. You can click the Security Incidents and select the **Risky Assets** sub-page on the event details page to view it, as shown in the following figure.

No.	Threat	Risky Assets	Confidence	Severity	Tags	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Infected with ProtonMiner (mining)	7	Low	High	Cryptomining, ProtonMiner, mining	C&C	Cryptomining	2022-03-29 03:25:36	Pending Fix failed	...
2	Infected with ransomware	6	Low	High	-	Propagation	Ransomware	2022-03-29 03:25:57	Pending Fix failed	...
3	Infected with bitcoinminer (mining)	7	Low	High	Cryptomining, bitcoinminer, mining	C&C	Cryptomining	2022-03-15 03:59:20	Pending Fix failed	...
4	Infected with a mining virus	5	High	High	-	Impact	Cryptomining	2022-03-29 03:25:57	Pending Fix failed	...
5	Communication via reGeorg	6	High	High	ReGeorg	C&C	HTTP Tunnel...	2022-03-29 03:25:36	Pending Fix failed	...



- **The Status is divided into** Pending, Suspended, Fixing, and Fixed.
- **Last Detected:** It represents the time of the most recent entry in the alert log associated with all risky assets within the change event, as shown in the following figure.



- **Status:** Represents the safety status of a risky asset. If there are multiple risky assets and all of the risky assets are fixed, it will display **Fixed**. If there are **unfixed** risky assets, it will display **Pending**, as shown in the following figure.

export

Filter: Status: Suspended, Fixing, Fixed, Pending X Clear

No.	Threat	Risky Assets	Confidence	Severity	Tags	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Infected with ProtonMiner (mining)	7	Low	High	Cryptomining ProtonMiner mining	C&C	Cryptomining	2022-03-29 03:25:36	Fixed Fix failed	
2	Infected with ransomware	6	Low	High	-	Propagation	Ransomware	2022-03-29 03:25:57	Pending Fix failed	
3	Infected with bitcoinminer (mining)	7	Low	High	Cryptomining bitcoinminer mining	C&C	Cryptomining	2022-03-15 03:59:20	Pending Fix failed	
4	Infected with a mining virus	5	High	High	-	Impact	Cryptomining	2022-03-29 03:25:57	Pending Fix failed	
5	Communication via reGeorg	6	High	High	ReGeorg	C&C	HTTP Tunneling	2022-03-29 03:25:36	Pending Fix failed	

3.4.4 Incident Details

Select security incident and enter the incident details page. The number on the **All Targets** represents the number of attackers associated with the Security Incidents, as shown in the following figure.

Incident Details

General system command injection attack

Status: Pending

Threat Type: System Command Injection

Severity: High

Mark as Fixed

Detected By: SANGFOR STA(192.168.20.1...

Attack Stage: Propagation

Incident ID: 117980007

Threats

Hit Rules

Attacker Analysis

Risky Assets

Recommendations

All Attackers (8)

Select

Internal IP Range (10.32...)

Attacks: 240

Succeed

Last Detected: 2023-03-06 16:03:37

Internal IP Range (10.67...)

Attacks: 465

Succeed

Last Detected: 2023-03-06 16:03:27

Internal IP Range (192.1...)

Attacks: 126

Succeed

Last Detected: 2023-03-06 15:26:16

Internal IP Range (10.25...)

Attacks: 319

Attempted

Last Detected: 2023-03-06 16:00:08

Internal IP Range (10.25...)

Attacks: 36

Attempted

Last Detected: 2023-03-06 15:21:08

8 in all

All attacker

Attacker	Victim	Attack Result	Last Detected
Internal IP Range (10.32.36.181)	Internal IP Range (10.90.26.41)	Succeed	2023-03-06 15:51:06

Details

Original Logs

Details

Host

10.32.36.181

Internal IP Range

Port: 58716

Attacks: 240

Attack Result: Attempted

Protocol: http

Server

10.90.26.41

Internal IP Range

Port: 80

Latest Attack Details

url	10.128.156.18/shell.jsp?i=whoami	status_code	0
-----	----------------------------------	-------------	---

Result Offered by Platform

Business may be invalid.

Timeline

Data Packet

Request

Request Header

GET /shell.jsp?i=whoami HTTP/1.1

Host: 10.128.156.18

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116

Response

Response Header

-

Response Body

Code Converter

Download

UTF-8

Hex

1 in all

1

Per Page

10

The total number of attackers and the number of risky assets in the **Hit Rules** are two different things, not necessarily equal, as shown in the following figure.

Incident Details

General system command injection attack

Status: Pending

Threat Type: System Command Injection

Severity: High

Detected By: SANGFOR STA(192.168.20.1...

Attack Stage: Propagation

Incident ID: 117980007

Mark as Fixed

Threats

Hit Rules

Attacker Analysis

Risky Assets

Recommendations

No.	Rule ID	Rule Name	Detection Engine	Threat Type	Severity	ATT&CK Attack Technique
1	13010197	OS Cmd Injection netstat com...	Web Application Detection Dat...	Code Injection	High	Exploit Public-Facing Application
2	13010450	Apache Struts OGNL Expressio...	Web Application Detection Dat...	Code Injection	High	Exploit Public-Facing Application

Incident Details

[Behinder(Godzilla)] JSP communication

Status: Pending

Threat Type: WebShell Access

Severity: High

Detected By: SANGFOR STA(192.168.20.1...

Attack Stage: Propagation

Incident ID: 117891064

Mark as Fixed

Threats

Hit Rules

Risky Assets

Recommendations

No.	Rule ID	Rule Name	Detection Engine	Threat Type	Severity	ATT&CK Attack Technique
1	17891064	[Behinder(Godzilla)] JSP commu...	Backdoor Communication Dete...	Web Backdoor	High	Server Software Component

The number of **Attacks** on the **Incident details** subpage represents the total number of **Original Logs** hit by the corresponding IP as an attack launched by an attacker, consistent with the number of alerts in the **Details** subpage.

Incident Details

General system command injection attack

Status: Pending

Threat Type: System Command Injection

Severity: High

Detected By: SANGFOR STA(192.168.20.1...

Attack Stage: Propagation

Incident ID: 117980007

Mark as Fixed

Threats

Hit Rules

Attacker Analysis

Risky Assets

Recommendations

All Attackers (8)

Select

Internal IP Range (10.32.36.181)

Attacks: 200

Succeed

Last Detected: 2023-03-10 10:16:12

Internal IP Range (10.67...)

Attacks: 405

Succeed

Last Detected: 2023-03-10 10:15:32

Internal IP Range (192.1...)

Attacks: 118

Succeed

Last Detected: 2023-03-10 10:07:30

Internal IP Range (10.25...)

Attacks: 258

Attempted

Last Detected: 2023-03-10 10:15:32

2.0.1.19(France)

Attacks: 6

Attempted

Last Detected: 2023-03-10 10:10:41

8 in all

1

2

Attacker

Victim

Attack Result

Last Detected

Internal IP Range (10.32.36.181)	Internal IP Range (10.90.26.41)	Succeed	2023-03-10 10:05:28
----------------------------------	---------------------------------	---------	---------------------

Details

Original Logs

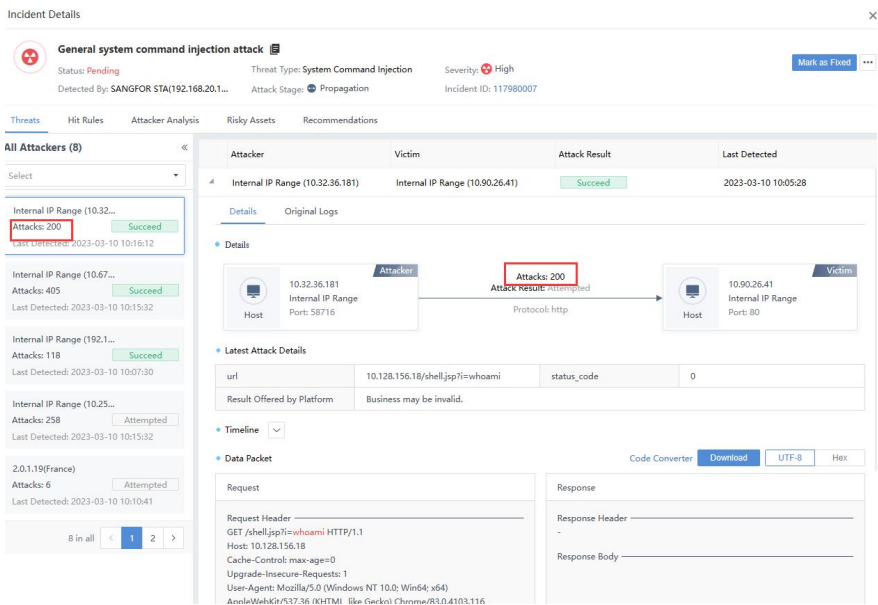
Logs: 201

Go to Logs

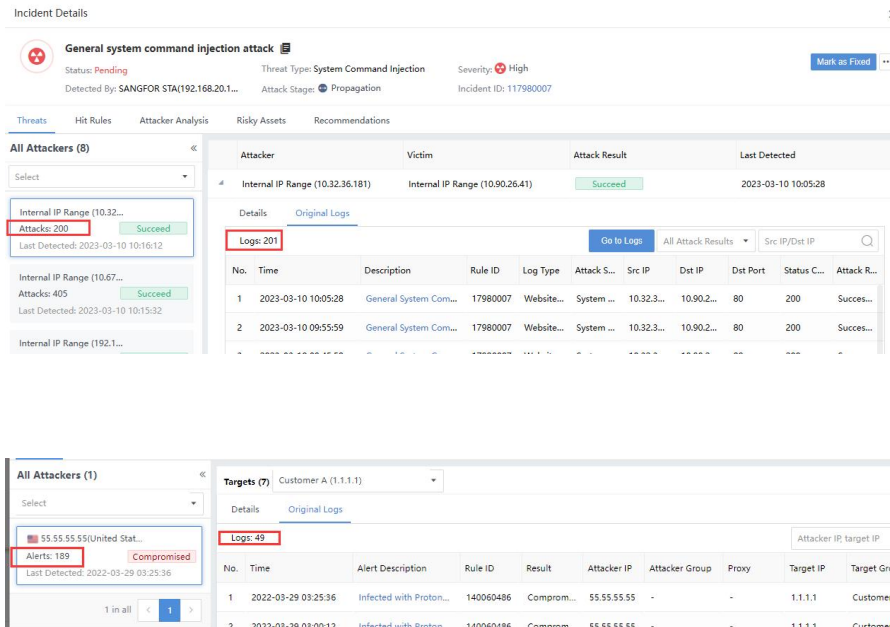
All Attack Results

Src IP/Dst IP

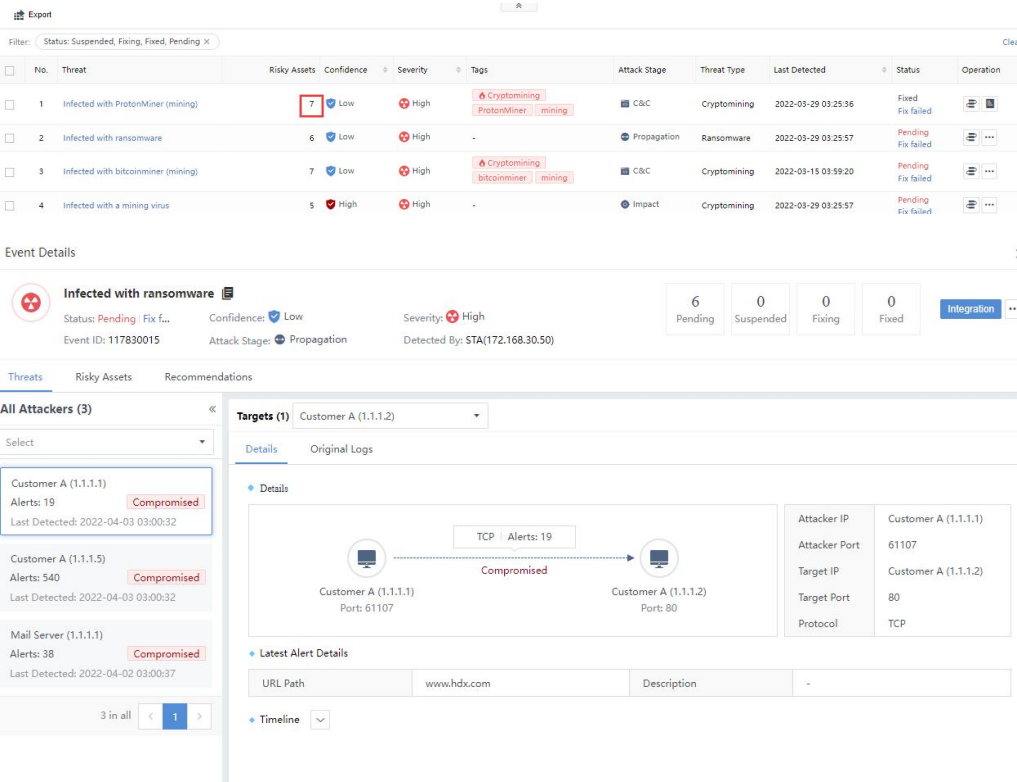
No.	Time	Description	Rule ID	Log Type	Attack S...	Src IP	Dst IP	Dst Port	Status C...	Attack R...
1	2023-03-10 10:05:28	General System Com...	17980007	Website...	System ...	10.32.3...	10.90.2...	80	200	Succes...
2	2023-03-10 09:55:59	General System Com...	17980007	Website...	System ...	10.32.3...	10.90.2...	80	200	Succes...
3	2023-03-10 09:45:58	General System Com...	17980007	Website...	System ...	10.32.3...	10.90.2...	80	200	Succes...
4	2023-03-10 09:42:51	General System Com...	17980007	Website...	System ...	10.32.3...	10.90.2...	80	200	Succes...
5	2023-03-10 09:23:54	General System Com...	17980007	Website...	System ...	10.32.3...	10.90.2...	80	200	Succes...
6	2023-03-10 09:08:21	General System Com...	17980007	Website...	System ...	10.32.3...	10.90.2...	80	200	Succes...
7	2023-03-10 08:58:20	General System Com...	17980007	Website...	System ...	10.32.3...	10.90.2...	80	200	Succes...
8	2023-03-10 08:45:00	General System Com...	17980007	Website...	System ...	10.32.3...	10.90.2...	80	200	Succes...
9	2023-03-10 08:41:52	General System Com...	17980007	Website...	System ...	10.32.3...	10.90.2...	80	200	Succes...
10	2023-03-10 08:15:20	General System Com...	17980007	Website...	System ...	10.32.3...	10.90.2...	80	200	Succes...



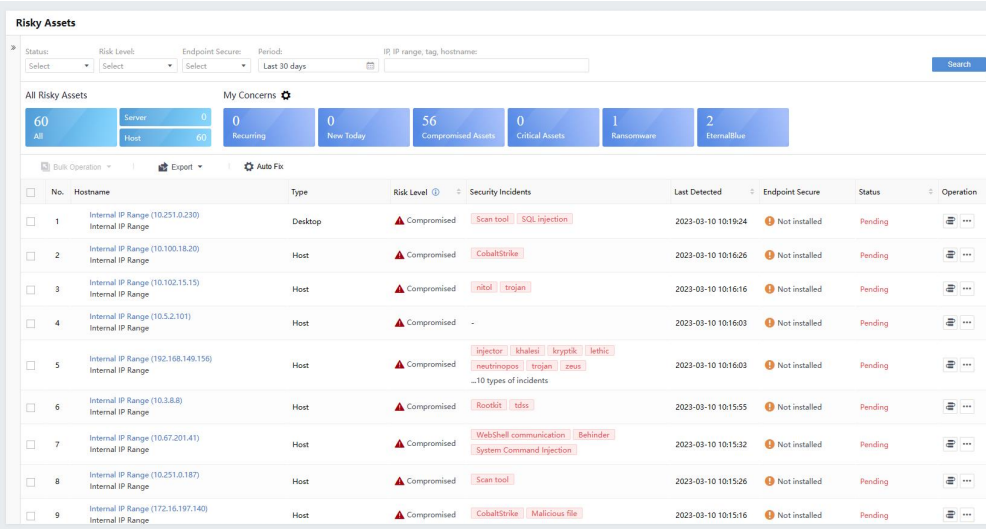
There are multiple victims when the number of attacks on the left pane is inconsistent with the original logs list on the right. The sum of the number of logs hit by multiple victims on the right is equal to the number of attacks on the left, as shown in the following figure.

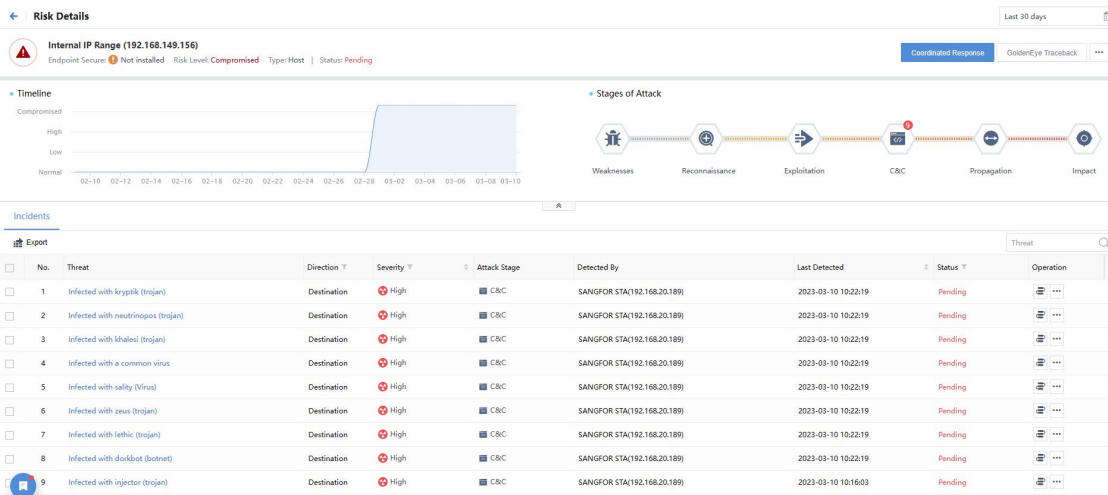


Risky Assets represent the number of risk assets associated with Security Incidents. You can click the Security Incidents and select the **Threats** sub-page on the incident details page to view it, as shown in the following figure.



The number of attacks consistent with the number of victims on the **Threat** page equals the corresponding number of original logs in the risk assets list, as shown in the following figure.



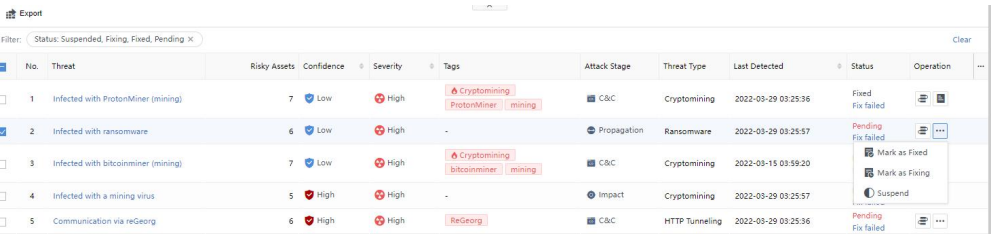


3.4.5 Incident Operation

Security Incidents can be handled manually or by integration. The status after manual response includes: **Fixed**, **Fixing**, **Suspended** and **Pending**. Correlate response is based on scripts or actions.

Response Manually

On the **Response > Security Incidents** page, select a specific Security Incidents and click the More icon in the **Operation** column, as shown in the following figure.



Click the **Mark as Fixed**, fill in remarks in the pop-up box, and upload pictures as proof if necessary. The status will change to **Fixed**, as shown in the following figure.

Fixed

It may take some time to change the status of all alerts associat...

Remarks (optional)

Upload Image

OK

Cancel

You can enter the risky asset of Security Incidents and respond manually, as shown in the following figure.

Filter: Status: Suspended, Fixing, Fixed, Pending X Clear

No.	Threat	Risky Assets	Confidence	Severity	Tags	Attack Stage	Threat Type	Last Detected	Status	Operation
☐	1 Infected with ProtonMiner (mining)		7 Low	High	Cryptomining ProtonMiner mining	C&C	Cryptomining	2022-03-29 03:25:36	Fixed	Fix failed
☒	2 Infected with ransomware		6 Low	High	-	Propagation	Ransomware	2022-03-29 03:25:57	Pending	Fix failed
☐	3 Infected with bitcoinminer (mining)		7 Low	High	Cryptomining bitcoinminer mining	C&C	Cryptomining	2022-03-15 03:59:20	Pending	Fix failed
☐	4 Infected with a mining virus		5 High	High	-	Impact	Cryptomining	2022-03-29 03:25:57	Pending	Fix failed

Coordinated Response

On the **Response > Security Incidents** page, click the  icon to bring up the integration action dialog. You can respond based on the policies' execution or the execution action. The matching and the enabled policies will be displayed in a pop-up box when you follow the policies, as shown in the following figure.

☒	2	Infected with ransomware	6	Low	High	-	Propagation	Ransomware	2022-03-29 03:25:57	Pending	Fix failed	...
☐	3	Infected with bitcoinminer (mining)	7	Low	High	Cryptomining bitcoinminer mining	C&C	Cryptomining	2022-03-15 03:59:20	Pending	Fix failed	Coordinated Response

Coordinated Response

Refresh

All Event Types

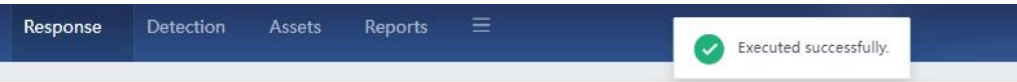
Name, device, IP, policy type

No.	Name	Hit Event	Device	IP Address	Policy Type	
☒	Threat Scan - Predefined Start a full/quick scan and block/trust detected malicious files.	Event-SQL Injection Event-Remote File Incl. 275 Event Types	Sangfor Endpoint S... Sangfor Cyber Com...	Cyber Command (...)	Built-in Strategy	
☐	Block Endpoint - Predefined Block the endpoint for N days. During this period, the endpoint cannot communicate with the...	Event-SQL Injection Event-Remote File Incl. 275 Event Types	Sangfor Endpoint S... Sangfor NGAF (v8.0... 4 Applications	af_54.83.49.40 (54...	Built-in Strategy	
☐	Access Control - Predefined Prevent an endpoint from accessing specified IP addresses and ports to block abnormal and attack...	Event-SQL Injection Event-Remote File Incl. 275 Event Types	Sangfor NGAF (v8.0... Sangfor Endpoint S... 4 Applications	af_54.83.49.40 (54...	Built-in Strategy	
☐	Block Domain Name/URL - Predefined - Event Block Attacker Domain Name/URL - N Days.	Event-SQL Injection Event-Remote File Incl. 275 Event Types	Sangfor NGAF (v8.0... Sangfor NGAF (v8.0... 3 Applications	af_172.168.30.44 (...)	Built-in Strategy	
☐	Account Lockout - Predefined Block communication between infected endpoints and the Internet.	Event-SQL Injection Event-Remote File Incl. 275 Event Types	Sangfor IAM Sangfor IAG 3 Applications	ac_218.253.76.106...	Built-in Strategy	
☐	Endpoint Lockout - Predefined If you use a Sunday AP or Sunday switch for authentication, you can perform lockout by using...	Event-SQL Injection Event-Remote File Incl. 275 Event Types	Sangfor Network C... Sangfor Cyber Com...	Cyber Command (...)	Built-in Strategy	
☐	Browsing Risk Notification - Predefined Users will be notified of endpoint risks when they surf the Internet with a browser	Event-SQL Injection Event-Remote File Incl. 275 Event Types	Sangfor IAM Sangfor IAG	ac_218.253.76.106...	Built-in Strategy	

Per Page: 207 in all<1>

Add PolicyNextCancel

Select the policy and execute it. The pop-up box displays the execution status, as shown in the following figure.



You can also perform actions. Select from the Select Action option drop-down list, where you can select by filter **By App** or **By Action**, and click **OK**.

Parameter Settings

* Node Name:

AF-T1-Add Access Control

* Action:

Add Access Control

By AppBy Action

App Name

All Types

Sophos Firewall

Sangfor NGAF (v8.0.35 and above)

Sangfor Network Controller

Sangfor NGAF (v8.0.8 to v8.0.34)

Sangfor IAG

Sangfor IAM

Sangfor Cyber Command

Host Security App

Sangfor Endpoint Secure

* Device IP:

OKCancel

Parameter Settings

* Node Name:

AF-T1-Add Access Control

* Action:

Add Access Control

By AppBy Action

Name

All Types

Remediation

Add Correlated Block

Remove Correlated Block

Add Block IP

Delete Block IP

Disable Device

Enable Device

Create Isolate Endpoint Task

Restore Endpoint From Isolation

App Name

FortiGate

Sangfor NGAF (...)

* Device IP:

OKCancel

Parameter Settings

* Node Name:

Add Correlated Block

* Action:

Add Correlated Block

* Block Direction:

Enter/Select Parameter

* Object Type to Block:

Enter/Select Parameter

* Object to Block:

Enter/Select Parameter

* Block Duration:

Enter/Select Parameter

* Block Duration Unit:

Enter/Select Parameter

* Device IP:

Device IP

Advanced

This field is required.

Delayed Execution:

Select the corresponding instance resource and execute it, and you can see the task delivery status, as shown in the following figure.



On the **Response > Response History > Auto Response History** page, you can check the **Execution Status, Start Time, End Time, Application, Operation**, etc. You can also click **Execute Again** for the failed response, as shown in the figure below.

Risky Assets

Security Events

Security Alerts

Auto Response History

Coordinated Actions

All Categories

All Statuses

Asset IP: policy name, security event, fixed by

No.	Running Policy	Asset IP	Policy Type	Application	Security Events	End Time	Executed By	Execution Status	Coordinated Action	Operation
1	Auto Response	1.1.1.3	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-11 14:31:31	admin	Failed ⓘ	View	Execute Again
2	Auto Response	1.1.1.3	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
3	Auto Response	1.1.1.5	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
4	Auto Response	1.1.1.6	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
5	Auto Response	1.1.1.6	Advanced	Sangfor Cyber Comma...	Event-CobaltStrike	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
6	Auto Response	1.1.1.7	Advanced	Sangfor Cyber Comma...	Event-CobaltStrike	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
7	Auto Response	1.1.1.3	Advanced	Sangfor Cyber Comma...	Event-CobaltStrike	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
8	Auto Response	1.1.1.2	Advanced	Sangfor Cyber Comma...	Event-CobaltStrike	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
9	Auto Response	1.1.1.1	Advanced	Sangfor Cyber Comma...	Event-CobaltStrike	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
10	Auto Response	1.1.1.4	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
11	Auto Response	1.1.1.2	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
12	Auto Response	1.1.1.1	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
13	Auto Response	1.1.1.7	Advanced	Sangfor Cyber Comma...	Event-Cryptomining	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
14	Auto Response	1.1.1.6	Advanced	Sangfor Cyber Comma...	Event-Cryptomining	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
15	Auto Response	1.1.1.5	Advanced	Sangfor Cyber Comma...	Event-Cryptomining	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
16	Auto Response	1.1.1.4	Advanced	Sangfor Cyber Comma...	Event-Cryptomining	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
17	Auto Response	1.1.1.3	Advanced	Sangfor Cyber Comma...	Event-Cryptomining	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again

Displaying 1 - 20 of 1644 Per Page 20 1644 in all 1 2 3 4 5 6 ... 82

Risky Assets

Security Events

Security Alerts

Auto Response History

Coordinated Actions

All Categories

All Statuses

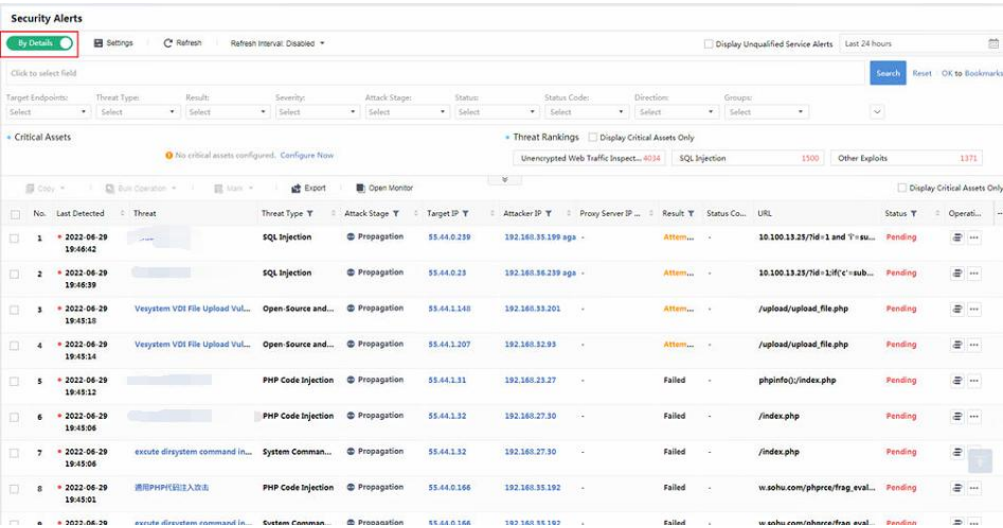
Asset IP: policy name, security event, fixed by

No.	Running Policy	Asset IP	Policy Type	Application	Security Events	End Time	Executed By	Execution Status	Coordinated Action	Operation
1	Auto Response	1.1.1.3	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-11 14:31:31	admin	Failed ⓘ	View	Execute Again
2	Auto Response	1.1.1.3	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
3	Auto Response	1.1.1.5	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
4	Auto Response	1.1.1.6	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
5	Auto Response	1.1.1.6	Advanced	Sangfor Cyber Comma...	Event-CobaltStrike	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
6	Auto Response	1.1.1.7	Advanced	Sangfor Cyber Comma...	Event-CobaltStrike	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
7	Auto Response	1.1.1.3	Advanced	Sangfor Cyber Comma...	Event-CobaltStrike	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
8	Auto Response	1.1.1.2	Advanced	Sangfor Cyber Comma...	Event-CobaltStrike	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
9	Auto Response	1.1.1.1	Advanced	Sangfor Cyber Comma...	Event-CobaltStrike	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
10	Auto Response	1.1.1.4	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
11	Auto Response	1.1.1.2	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:25	system	Failed ⓘ	View	Execute Again
12	Auto Response	1.1.1.1	Advanced	Sangfor Cyber Comma...	Event-HTTP Tunneling	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
13	Auto Response	1.1.1.7	Advanced	Sangfor Cyber Comma...	Event-Cryptomining	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
14	Auto Response	1.1.1.6	Advanced	Sangfor Cyber Comma...	Event-Cryptomining	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
15	Auto Response	1.1.1.5	Advanced	Sangfor Cyber Comma...	Event-Cryptomining	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
16	Auto Response	1.1.1.4	Advanced	Sangfor Cyber Comma...	Event-Cryptomining	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again
17	Auto Response	1.1.1.3	Advanced	Sangfor Cyber Comma...	Event-Cryptomining	2022-04-03 04:11:24	system	Failed ⓘ	View	Execute Again

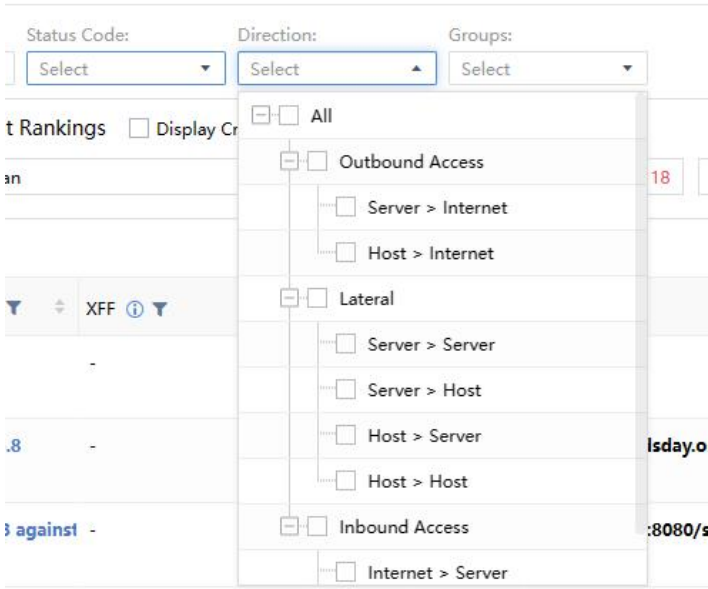
3.5 Security Alerts

3.5.1 Alert Filtering

On the **Response > Security Alerts** page, you can see the distribution of security alerts, which you can filter by **Status, Type, Groups, Direction, Confidence, Severity, Attack Stage, Result, Threat Type**, etc., as shown in the following figure.

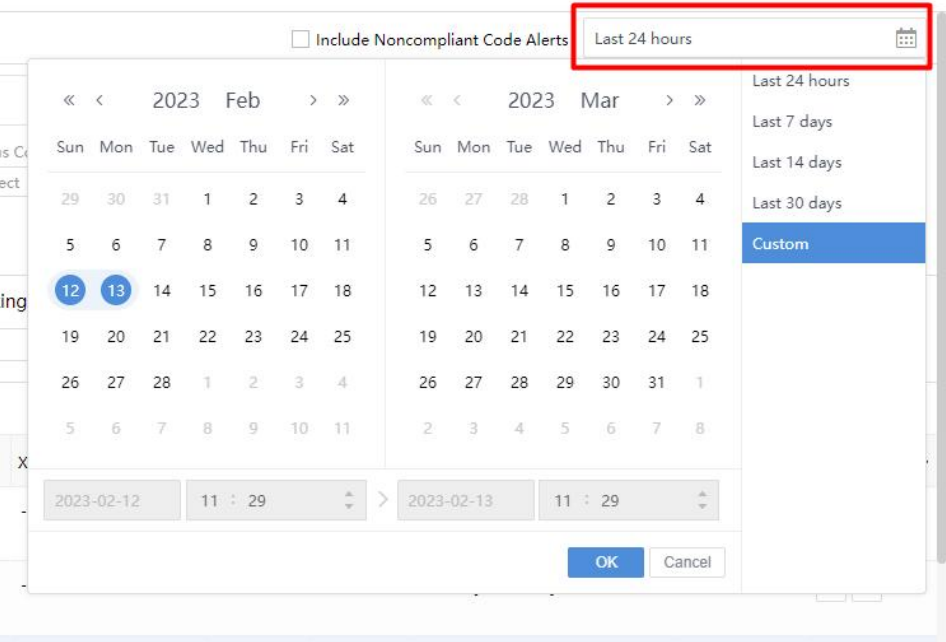


- **Status:** All, Pending, Suspended, Fixing, Fixed.
- **Target Endpoints:** All, Server, Host.
- **Groups:** A drop-down list for you to select different asset groups.
- **Direction:** Represents the direction of the **Security Alerts** traffic, including All, outbound access, Lateral and inbound access. etc., as shown in the following figure.

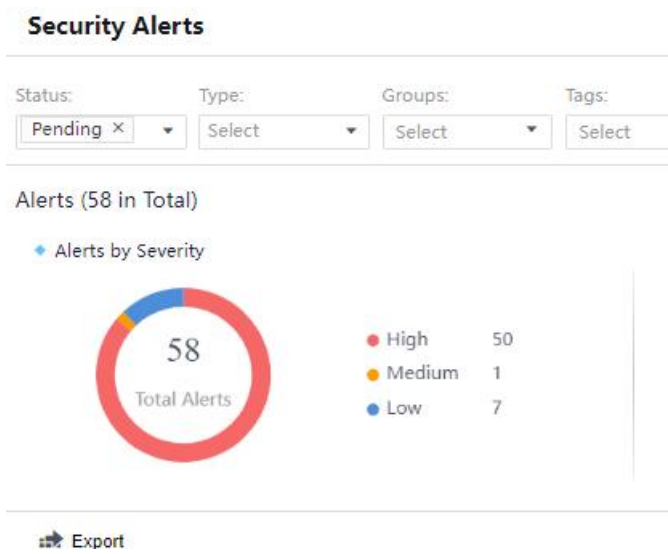


- **Severity:** According to the comprehensive assessment of the impact scope and depth of Security Incidents, divided into **All**, **High**, **Medium**, and **Low**.
- **Attack Stage:** Stage matching of Security Incidents based on industry-standard attack chain models, divided into **All**, **Weakness**, **Reconnaissance**, **Exploitation**, **C&C**, **Propagation**, and **Impact**.

- **Threat Type:** High, Medium, and Low.
- **Period:** Filter for the Security Incidents based on period. You can choose **Last 30 days**, **Last 7 days**, **Last 24 hours**, or **Custom**. Choose **Custom** to filter the Security Incidents beyond 30 days, as shown in the following figure.



- **Search:** You can search the Security Incidents based on IP, IP segment, description, tag, or hostname.
- **Severity:** You can see the event statistics in the middle section of the **Security Alerts** page, showing three alert level: **High**, **Medium**, and **Low**. Each section has specific quantitative statistics, as shown in the following figure.



Security Incidents are quantified and matched according to the attack stage. As a result, the total number is consistent with the number of event attribute classifications, as shown in the following figure.



3.5.2 View Alerts

You can see the specific Security Alert list according to the above conditions. The dimensions of each Security incident, including **Threat, Severity, Attack Stage, Threat Type, Status, Operation, etc.**, are shown in the following figure.

Result	Status Co...	URL	Status	Operati...	...
Succeed	-	-	Per		
Attem...	-	-	Per		
Succeed	-	-	Per		
Attem...	-	10.251.0.105/nicedit/	Per		
Failed	404	10.251.0.231/never_could_exi...	Per		
Succeed	404	192.168.180.222/zabbix/api_j...	Per		
Compr...	-	-	Per		
Attem...	-	prcp.mygoodsday.org/addrec...	Per		
Attem...	200	172.20.64.50:8080/struts2-sh...	Per		

All

☐Severity

☒Target IP

☐Target Group

☒Attacker IP

☐Asset of Attacker

☒XFF

☒Result

☒Status Code

☐Attacks

☒URL

☐Threat Intelligence

☐Sensor Device

☐Platform

☒Status

☒Operation

Export

Filter: Status: Pending X

Clear

☐	No.	Threat	Direction	Risky Assets	Severity	Tags	Attack Stage	Last Detected	Status	Operation
☐	1	Infected with bitcoinminer (mining)	Inbound	7	High	bitcoinminer, mining	C&C	2022-03-15 03:59:20	Pending	
☐	2	Infected with coinminer (mining)	Inbound	2	High	coinminer, mining	C&C	2022-03-15 03:59:20	Pending	
☐	3	Infected with coinminer (mining)	Lateral	1	High	coinminer, mining	C&C	2022-03-15 03:59:20	Pending	
☐	4	Infected with drivelfe (mining)	Lateral	1	High	drivelfe, mining	C&C	2022-03-15 03:59:20	Pending	
☐	5	Plaintext transmission of the username and password for...	Outbound	1	High	Web	Weaknesses	2022-03-27 03:01:06	Pending	
☐	6	Weak IMAP password	Inbound	7	Low	IMAP	Weaknesses	2022-03-28 10:06:13	Pending	
☐	7	Weak Web password	Inbound	7	Low	Web	Weaknesses	2022-03-28 10:06:13	Pending	
☐	8	Weak POP3 password	Inbound	7	Low	POP3	Weaknesses	2022-03-28 10:06:13	Pending	
☐	9	Malicious file found in the file sharing directory	Outbound	1	High	Intelligent File Analytics Engine	Exploitation	2022-03-28 10:06:13	Pending	
☐	10	Malicious file found in the file sharing directory	Lateral	1	High	Intelligent File Analytics Engine	Propagation	2022-03-28 10:06:13	Pending	

- The number of risky assets:** Represents the number of risky assets associated with the Security Alerts. You can click the Security Incidents and select the **Risky Assets-Target** subpage on the alert details page to view it, as shown in the following figure.

Filter: Status: Pending X

Clear

☐	No.	Threat	Direction	Risky Assets	Severity	Tags	Attack Stage	Last Detected	Status	Operation
☐	1	Infected with bitcoinminer (mining)	Inbound	7	High	bitcoinminer, mining	C&C	2022-03-15 03:59:20	Pending	
☐	2	Infected with coinminer (mining)	Inbound	2	High	coinminer, mining	C&C	2022-03-15 03:59:20	Pending	
☐	3	Infected with coinminer (mining)	Lateral	1	High	coinminer, mining	C&C	2022-03-15 03:59:20	Pending	
☐	4	Infected with drivelfe (mining)	Lateral	1	High	drivelfe, mining	C&C	2022-03-15 03:59:20	Pending	
☐	5	Plaintext transmission of the username and password for...	Outbound	1	High	Web	Weaknesses	2022-03-27 03:01:06	Pending	

Details

Close

Infected with bitcoinminer (mining)

Status: Pending Confidence: High Severity: High Hits: 1 Attack Stage: C&C Detected By: STA(172.168.30.50)

6 Pending

0 Suspended

1 Fixing

0 Fixed

Mark as Fixed

Threats

Risky Assets-Target

Recommendations

Bulk Operation

Export

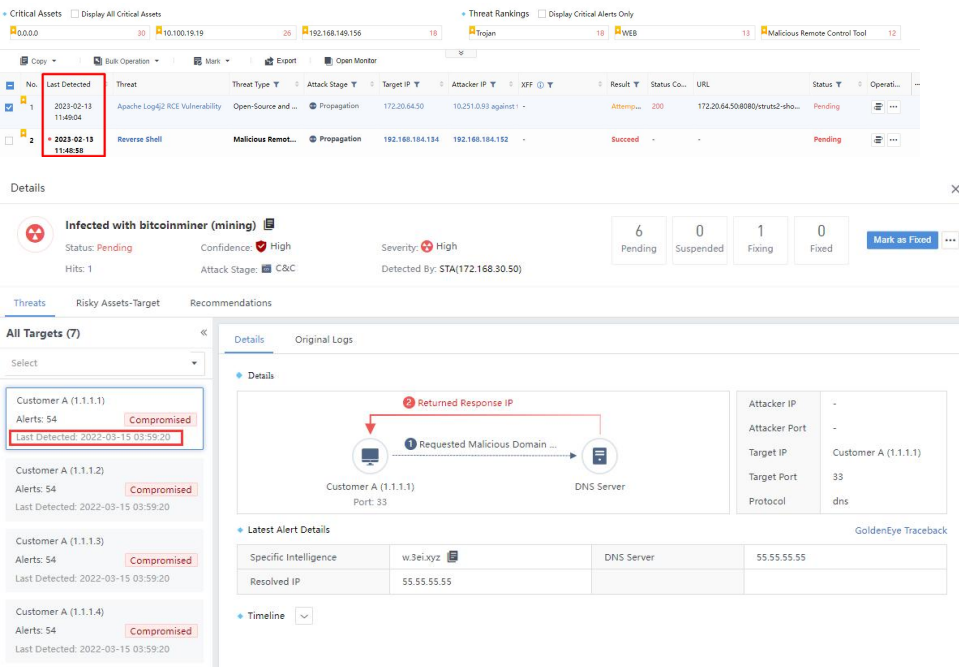
All Statuses

☐	No.	Risky Assets	Type	Threat Detections	Last Detected	Status	Operation
☐	1	Customer A (1.1.1.1) Customer A	Server	5	2022-03-15 03:59:20	Pending	
☐	2	Customer A (1.1.1.2) Customer A	Host	5	2022-03-15 03:59:20	Pending	
☐	3	Customer A (1.1.1.3) Customer A	Host	5	2022-03-15 03:59:20	Pending	
☐	4	Customer A (1.1.1.4) Customer A	Host	5	2022-03-15 03:59:20	Pending	
☐	5	Customer A (1.1.1.5) Customer A	Host	5	2022-03-15 03:59:20	Fixing	
☐	6	Customer A (1.1.1.6) Customer A	Host	5	2022-03-15 03:59:20	Pending	
☐	7	Customer A (1.1.1.7) Customer A	Host	5	2022-03-15 03:59:20	Pending	

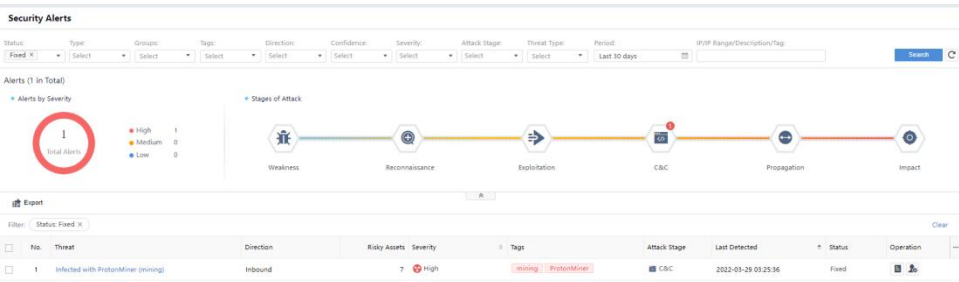
- Direction:** Represents the direction of the Security Alert traffic, including: undirected (multiple locally generated alerts), inbound (such as externally initiated attacks), literal (such as horizontal), and outbound (such as malicious, accidental connection), etc., as shown in the following figure.

☒	No.	Threat	Direction	Risky Assets	Severity	Tags	Attack Stage	Last Detected	Status	Operation
☒	1	Infected with bitcoinminer (mining)	Inbound	7	High	bitcoinminer, mining	C&C	2022-03-15 03:59:20	Pending	
☐	2	Infected with coinminer (mining)	Inbound	2	High	coinminer, mining	C&C	2022-03-15 03:59:20	Pending	
☐	3	Infected with coinminer (mining)	Lateral	1	High	coinminer, mining	C&C	2022-03-15 03:59:20	Pending	
☐	4	Infected with drivelfe (mining)	Lateral	1	High	drivelfe, mining	C&C	2022-03-15 03:59:20	Pending	
☐	5	Plaintext transmission of the username and password for...	Outbound	1	High	Web	Weaknesses	2022-03-27 03:01:06	Pending	
☐	6	Weak IMAP password	Inbound	7	Low	IMAP	Weaknesses	2022-03-28 10:06:13	Pending	
☐	7	Weak Web password	Inbound	7	Low	Web	Weaknesses	2022-03-28 10:06:13	Pending	
☐	8	Weak POP3 password	Inbound	7	Low	POP3	Weaknesses	2022-03-28 10:06:13	Pending	
☐	9	Malicious file found in the file sharing directory	Outbound	1	High	Intelligent File Analytics Engine	Exploitation	2022-03-28 10:06:13	Pending	

- **Status:** Pending, Suspended, Fixing, and Fixed.
- **Last detected:** Represents the time of the latest alert log associated with all risk assets within the alert, as shown in the following figure.

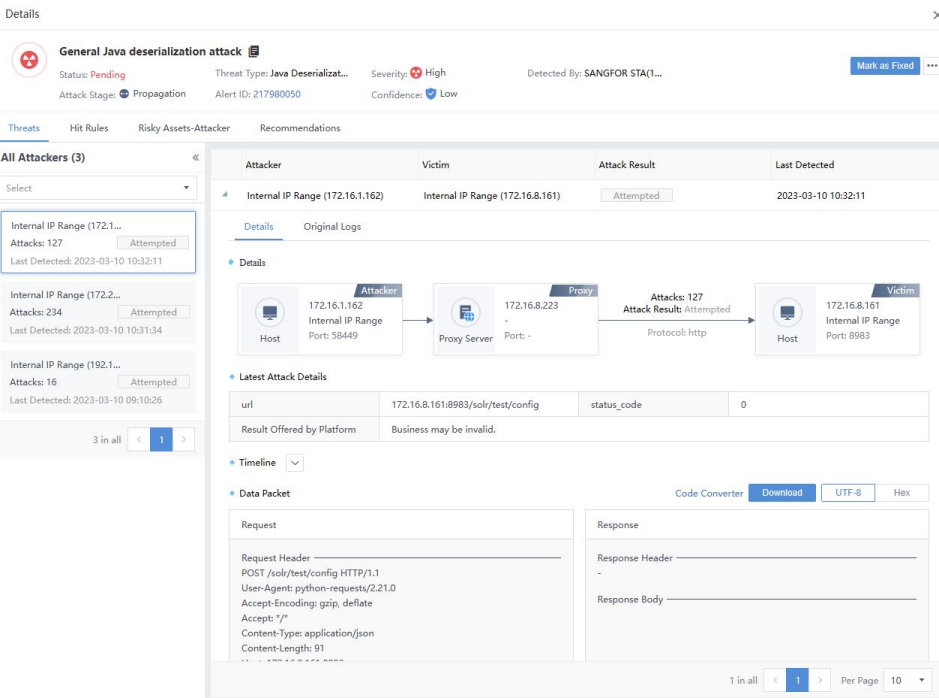


- **Status:** Represents the response status of a risky asset. If there are multiple risky assets and all of them are fixed, it will display **Fixed**. If there are no fixed risky assets, it will display **Pending**, as shown in the figure below.

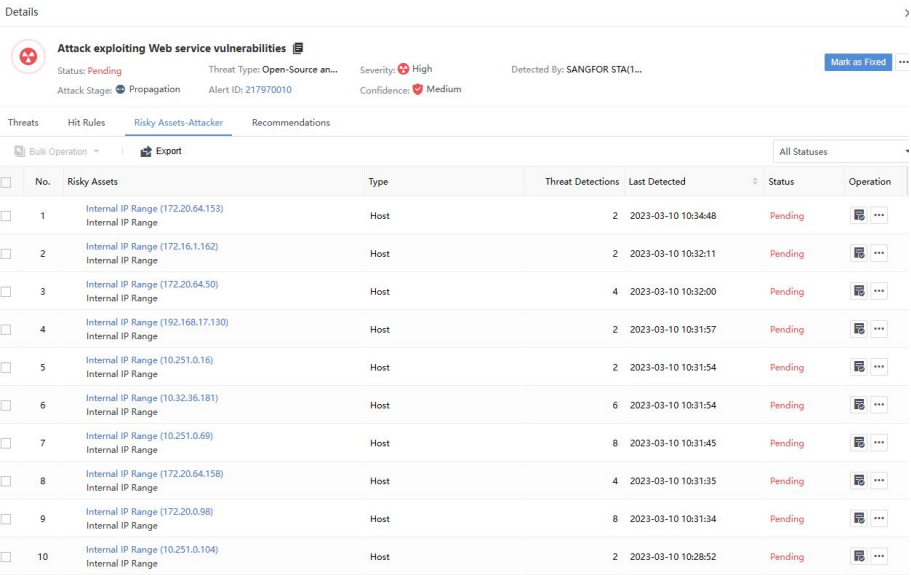


3.5.3 Details

Click a specific threat to enter the **Details** page, and you can view the number of attacks as shown in the following figure.



Risky Assets-attacker represents the number of risky assets associated with the Security Incidents, which can be viewed by selecting the **Risky Assets-attacker** subpage on the alert details page, as shown in the following figure.



A **Recommendation** represents a macro-guidance statement for responding to this type of Security Incident according to the industry's best practices, as shown in the figure below.

Details

Infected with bitcoinminer (mining)

Status: Pending Confidence: High Severity: High Detected By: STA(172.168.30.50)

Hits: 1 Pending Suspended Fixing Fixed [Mark as Fixed](#)

[Threats](#) [Risky Assets-Target](#) [Recommendations](#)

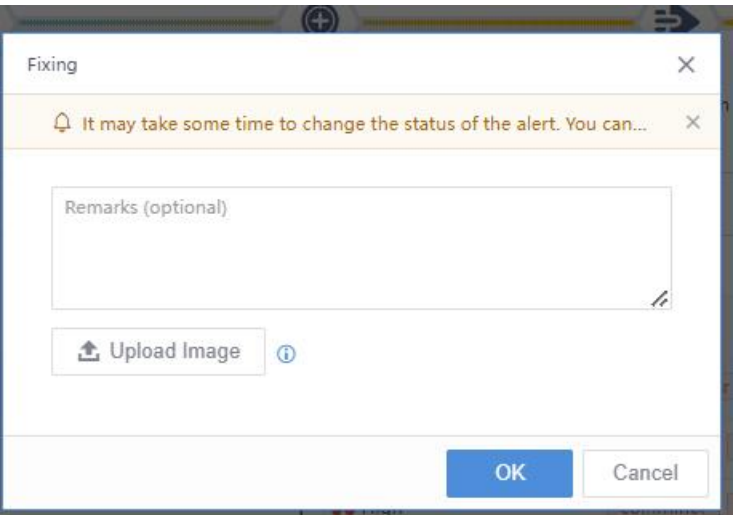
All Targets (7)

Select

- Customer A (1.1.1.1)
Alerts: 54 Compromised
Last Detected: 2022-03-15 03:59:20
- Customer A (1.1.1.2)
Alerts: 54 Compromised
Last Detected: 2022-03-15 03:59:20
- Customer A (1.1.1.3)
Alerts: 54 Compromised
Last Detected: 2022-03-15 03:59:20
- Customer A (1.1.1.4)
Alerts: 54 Compromised
Last Detected: 2022-03-15 03:59:20
- Customer A (1.1.1.5)
Alerts: 54 Compromised
Last Detected: 2022-03-15 03:59:20

7 in all < 1 >

Version 01 (May 30, 2024)

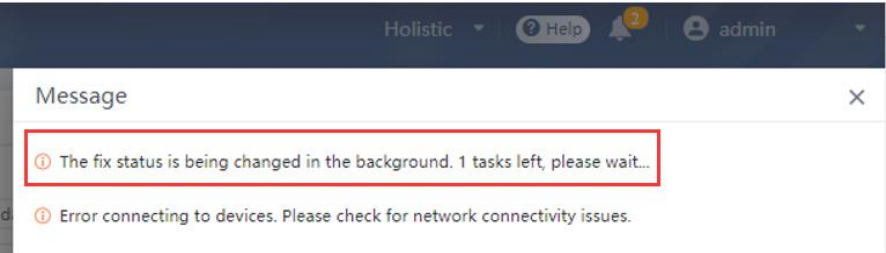


The page is updated after the status changes, as shown in the image below.

Filter: Status Fixed x Clear										
☐	No.	Threat	Direction	Risky Assets	Severity	Tags	Attack Stage	Last Detected	Status	Operation
☐	1	Infected with ProtonMiner (mining)	Inbound		High	mining ProtonMiner	C&C	2022-03-29 03:25:36	Fixed	

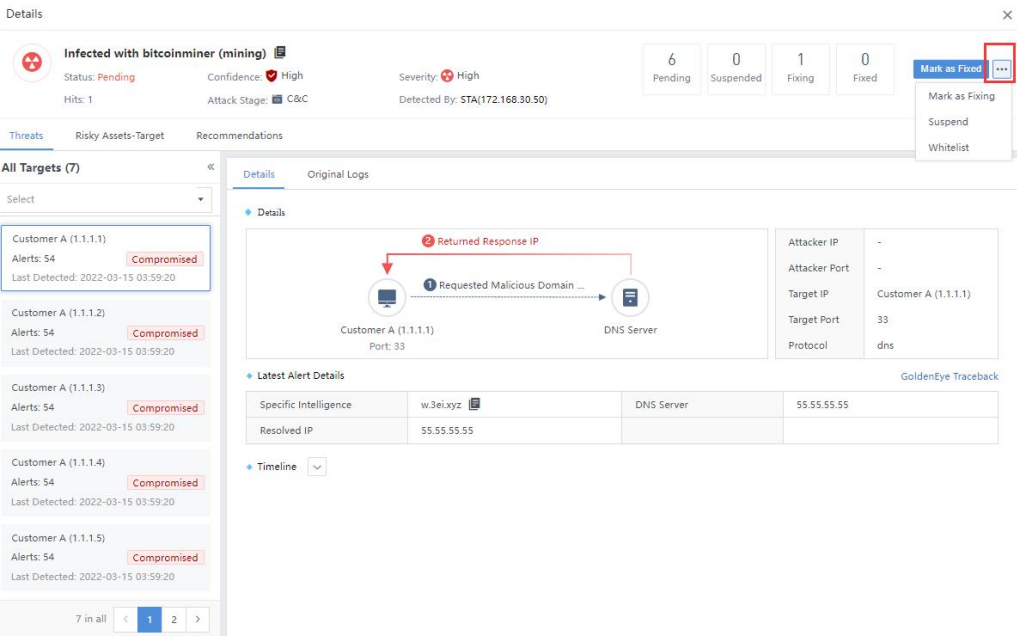


When issuing the response action, the small bell in the upper right corner of the page will prompt the task progress to ensure the normal execution of the task, as shown in the following figure.



Method Two: Response on the Alert Details Page

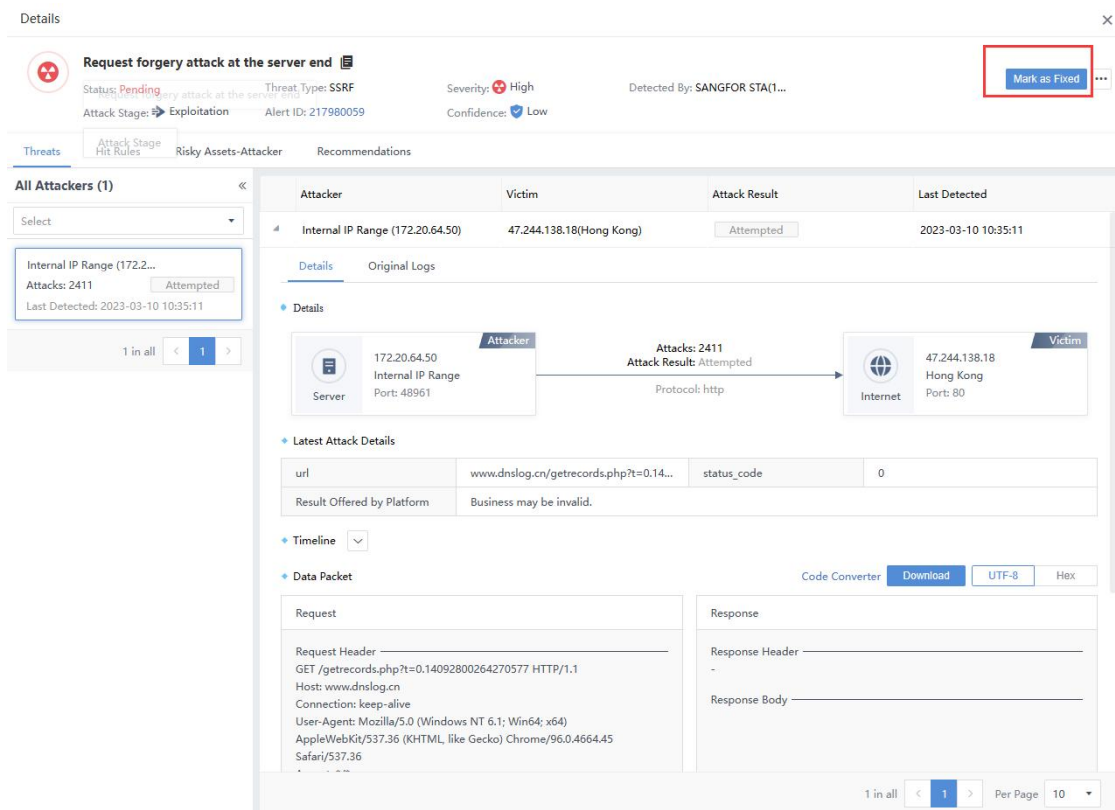
Select a specific threat on the **Security Alert** page to enter its details page. Then, click the More icon in the upper-right corner of the page, as shown in the following figure.



The above two methods have the same effect, and both operate on all risk assets of a single Security Alert.

• **Response of individual risk assets in alert**

Select a specific threat on the **Security Alert** page to enter its details page.
Then, select the **Risky Assets-Target** subtab to see the associated risk assets.
Select the risky assets you want to respond to and click **Mark as fixed**. After you respond, you can see the response's status in the upper right corner of the event details page, as shown in the following figure.



Whitelist

In addition to manual handling of Security Alerts, you can also manually whitelist the security alert. Select the threat, click the  icon, and click **Whitelist**. The **Add Security Alert Whitelist** pop-up box will automatically pop up. The Src IP, Dst IP, etc., are filled in by default. You need to specify the Apply To and **Schedule**, etc.

No.	Threat	Direction	Risky Assets	Severity	Tags	Attack Stage	Last Detected	Status	Operation
1	Infected with bitcoinminer (mining)	Inbound	7	High	bitcoinminer mining	C&C	2022-03-15 09:59:20	Pending	
2	Infected with coinminer (mining)	Inbound	2	High	coinminer mining	C&C	2022-03-15 09:59:20	Pending	
3	Infected with coinminer (mining)	Lateral	1	High	coinminer mining	C&C	2022-03-15 09:59:20	Pending	
4	Infected with drivelfile (mining)	Lateral	1	High	drivelfile mining	C&C	2022-03-15 09:59:20	Pending	

Add Security Alert Whitelist

Notes:

1. If multiple conditions are specified, the whitelist entry will take effect only when all the conditions are met.
2. After the whitelist entry is added, no alert will be triggered for the logs hitting this entry.

*Threat Type:

Malicious Remote ...

☒ Rule ID:

17139169

☒ Src IP:

192.168.184.152

☐ Src Type:

Internal IP Range

☒ Dst IP:

192.168.184.134

☐ Dst Type:

Internal IP Range

☐ Dst Port:

Separate ports with cor

☐ Domain Name/URL:

*Apply To:

All x

*Schedule:

Never Expire

Remarks:

OK

Cancel

3.5.5 HCI Integration

You can go to **Response > Response History > Auto Response History**, to check the execution status, end time, etc. You can also click **Execute Again** to execute the failed running policy, as shown in the figure below.

Response

Risky Assets

Risky Users

Security Events

Security Alerts

Auto Response

Response History

Risky Assets

Security Events

Security Alerts

Auto Response History

Coordinated Actions

All Categories

All Statuses

Asset IP policy name, security event, fixed by

No.	Running Policy	Asset IP	Policy Type	Application	Security Events	End Time	Executed By	Execution Status	Coordinated Action	Operation
1	Threat Scan - Prefixed	1.1.1.1,1.1.1.1,1.1.1.1,1.1.1.1	Butlin Strategy	Sangfor Endpoint Secure...	Event-Ransomware	2022-01-30 10:58:22	admin	Failed	View	Execute Again
2	Auto Response	1.1.1.6	Advanced	Sangfor Cyber Command...	Event-Ransomware	2022-01-29 03:27:56	system	Failed	View	Execute Again
3	Auto Response	1.1.1.7	Advanced	Sangfor Cyber Command...	Event-Ransomware	2022-01-29 03:27:56	system	Failed	View	Execute Again
4	Auto Response	1.1.1.5	Advanced	Sangfor Cyber Command...	Event-Ransomware	2022-01-29 03:27:56	system	Failed	View	Execute Again
5	Auto Response	1.1.1.4	Advanced	Sangfor Cyber Command...	Event-Ransomware	2022-01-29 03:27:56	system	Failed	View	Execute Again
6	Auto Response	1.1.1.3	Advanced	Sangfor Cyber Command...	Event-Ransomware	2022-01-29 03:27:56	system	Failed	View	Execute Again
7	Auto Response	1.1.1.2	Advanced	Sangfor Cyber Command...	Event-Ransomware	2022-01-29 03:27:56	system	Failed	View	Execute Again
8	Auto Response	1.1.1.5	Advanced	Sangfor Cyber Command...	Event-Cryptomining	2022-01-29 03:27:56	system	Failed	View	Execute Again
9	Auto Response	1.1.1.4	Advanced	Sangfor Cyber Command...	Event-Cryptomining	2022-01-29 03:27:56	system	Failed	View	Execute Again
10	Auto Response	1.1.1.3	Advanced	Sangfor Cyber Command...	Event-Cryptomining	2022-01-29 03:27:56	system	Failed	View	Execute Again
11	Auto Response	1.1.1.2	Advanced	Sangfor Cyber Command...	Event-Cryptomining	2022-01-29 03:27:55	system	Failed	View	Execute Again

Response

Risky Assets

Risky Users

Security Events

Security Alerts

Auto Response

Response History

Risky Assets

Security Events

Security Alerts

Auto Response History

Coordinated Actions

Execution Time

All Actions

All Apps

All Execution Results

Asset IP resource, fixed by

No.	Coordinated Action	Asset IP	Action Parameter	Application	Resource	End Time	Executed By	Execution Result	Details
1	-	1.1.1.1,1.1.1.1,1.1.1.1,1.1.1.1	Sangfor Endpoint Secure...	-	-	2022-01-30 10:58:22	admin	Failed	Execute Again
2	Change Risky Endpoint Status	1.1.1.1,1.1.1.1,1.1.1.1,1.1.1.1	Sangfor Cyber Command...	Sangfor Cyber Command	Cyber Command	2022-01-30 10:58:22	admin	Executed	View
3	-	1.1.1.3	Sangfor Endpoint Secure	-	-	2022-01-29 03:27:56	Trigger Policy system	Failed	Execute Again
4	-	1.1.1.4	Sangfor Endpoint Secure	-	-	2022-01-29 03:27:56	Trigger Policy system	Failed	Execute Again
5	-	1.1.1.7	Sangfor Endpoint Secure	-	-	2022-01-29 03:27:56	Trigger Policy system	Failed	Execute Again
6	-	1.1.1.6	Sangfor Endpoint Secure	-	-	2022-01-29 03:27:56	Trigger Policy system	Failed	Execute Again
7	-	1.1.1.6	Sangfor Endpoint Secure	-	-	2022-01-29 03:27:56	Trigger Policy system	Failed	Execute Again
8	-	1.1.1.5	Sangfor Endpoint Secure	-	-	2022-01-29 03:27:56	Trigger Policy system	Failed	Execute Again
9	-	1.1.1.7	Sangfor Endpoint Secure	-	-	2022-01-29 03:27:56	Trigger Policy system	Failed	Execute Again
10	-	1.1.1.5	Sangfor Endpoint Secure	-	-	2022-01-29 03:27:56	Trigger Policy system	Failed	Execute Again
11	-	1.1.1.3	Sangfor Endpoint Secure	-	-	2022-01-29 03:27:56	Trigger Policy system	Failed	Execute Again

3.6 Response Policies

Policies management is to connect various devices or platforms through SOAR tools.

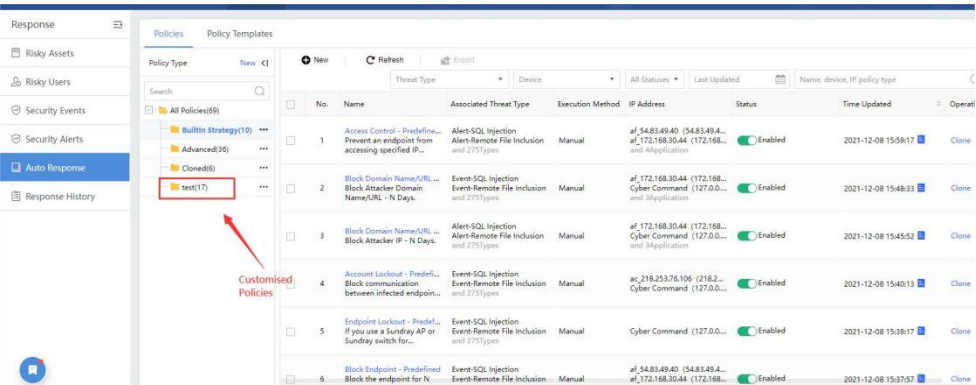
Version 01 (May 30, 2024)

61

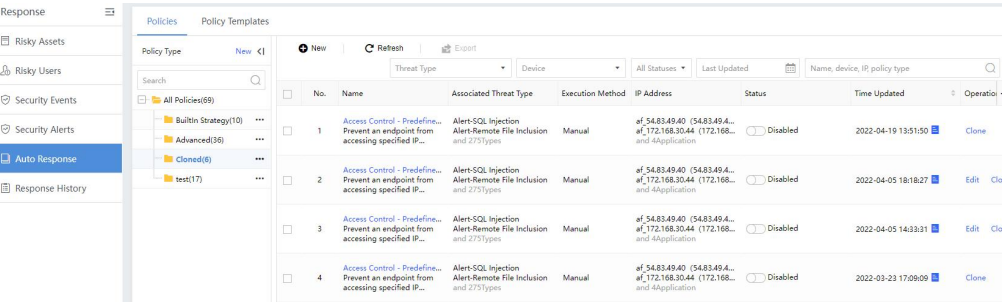
It helps customers build a standard handling process for security alerts/incidents, accelerate security threat response, respond to various security attacks in a timely and effective manner, build a security defense system, and reduce security operating costs. Policies management includes policies classification, policies addition, policies editing, etc.

3.6.1 Policies Classification

The system default types include **BuiltIn Strategy**, **Advanced**, **Cloned**, and you may custom-create a policy type, as shown in the figure below.

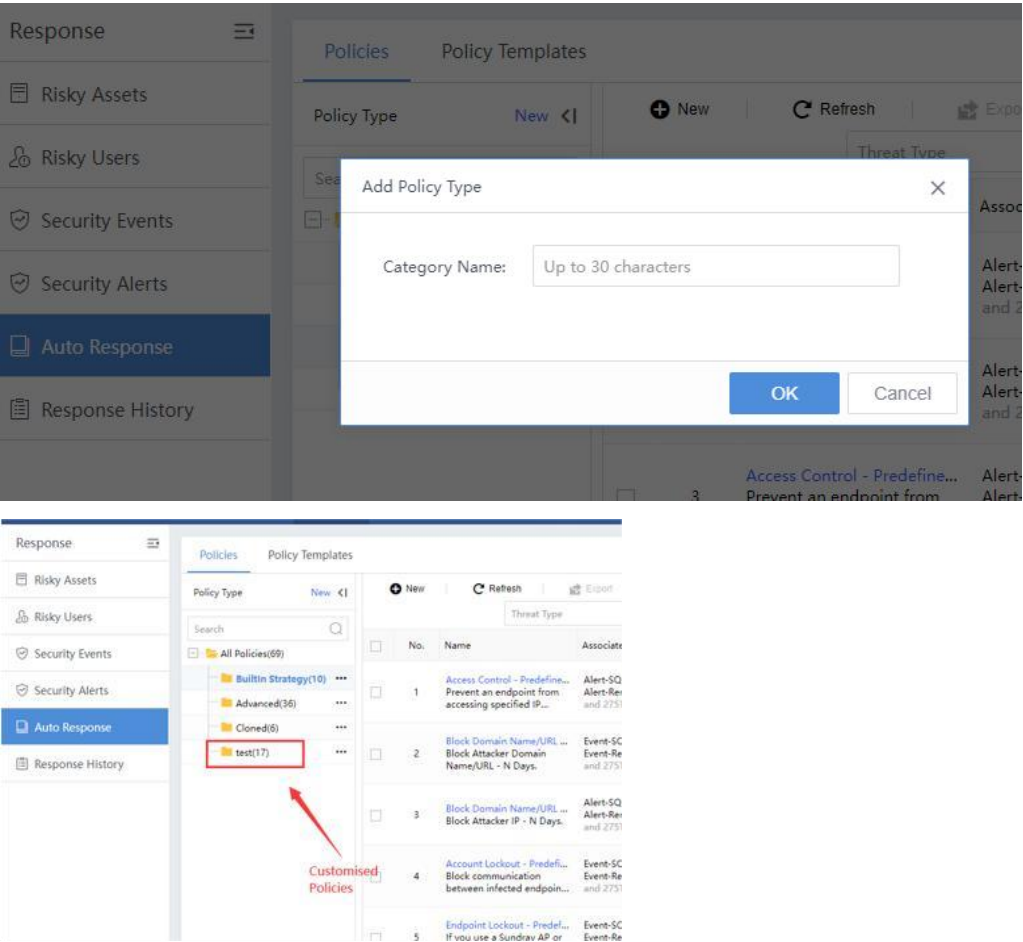


- **BuiltIn Strategy:** The policies were developed from the SOAR tool production line and synchronized to Cyber Command.
- **Advanced:** Refer to the default automatic response policies of the previous version (not including customization). After the upgraded version, it will be smoothly upgraded and translated into Response Strategy Conversion Script, as shown in the figure below.
- **Cloned:** After cloning **Builtin Strategy** or **Advanced** policies, it will be automatically added to the cloned policies. Edit and save the policies here. After copying, the policies name will default to **original policies name-copy Unix timestamp at time-copy** format, as shown in the figure below.

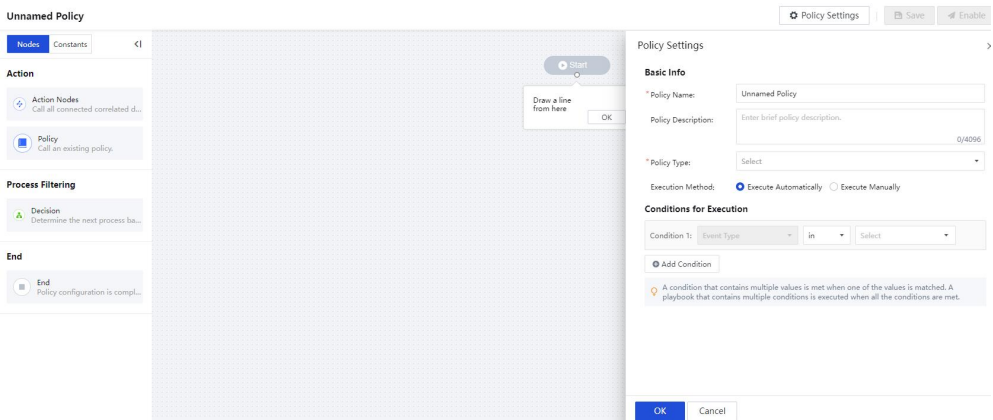


You can click the copied policies to edit it.

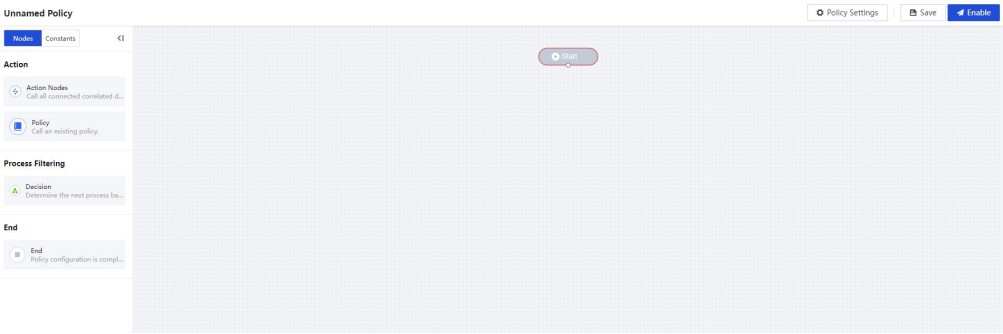
- **Custom:** Customize the catalog and add new policies here. In the **Response > Auto Response > Policies**, click **New** beside **Policy Type** to create a custom category, as shown in the figure below.



Add New Policies



On the **Response > Auto Response** page, click **New** to enter the policies layout canvas, as shown in the figure below.



The left navigation pane includes the **Nodes** and **Constants** library. The function description is shown below.

Category	Name	Function Description
Node	Action Nodes	Response actions corresponding to applications are different for different applications.
	Policies	Refers to the entire response process, including execution nodes, process filtering nodes, end nodes, etc.
	Decision	When logical judgments are needed between nodes, decision-makers will be introduced, and common judgment conditions such as if-else judgments, etc.
	End	Identifies the node where the entire policies flow ends.
Constant		Mark the parameters as constants. For example, mark a specific IP address/network segment as a business group/organization name as a constant, which can be quickly and intuitively identified and called in the policies layout. In addition to network IP resources, other resource types can be defined.

3.6.2 Policies Settings

Fill in the **Policy Name**, **Policy Description**, **Policy Type**, **Trigger Type**, and set **Condition for Execution** in the Policy setting pop-up box, as shown in the figure below.

Policy Settings

×

Basic Info

* Policy Name:

Unnamed Policy

Policy Description:

Enter brief policy description.

0/4096

* Policy Type:

Select

Execution Method:

☒ Execute Automatically

☐ Execute Manually

Trigger Type:

☒ Security Incident

☐ Security Alert

Conditions for Execution

Condition 1:

Security Incident

in

Select

+

Add Condition

💡

A condition that contains multiple values is met when one of the values is matched. A playbook that contains multiple conditions is executed when all the conditions are met.

- **Policy Name:** required field, custom name.
- **Policy Description:** optional, filled in according to the actual situation.
- **Policies Type:** Divided into Cloned, Advanced, and and custom policies, as shown in the figure below.

* Policy Type:

Select

Execution Method:

Cloned

Trigger Type:

Advanced

JH_Test

- **Execution Method:** It is divided into two methods: **Execute Automatically** and **Execute Manually**. Scripts under **Execute Automatically** mode will automatically match the conditions after the corresponding event and then automatically execute the corresponding integration processing. If set to manual execution mode, the policies will not be executed automatically, and you need to manually select manual execution in the corresponding response policy;

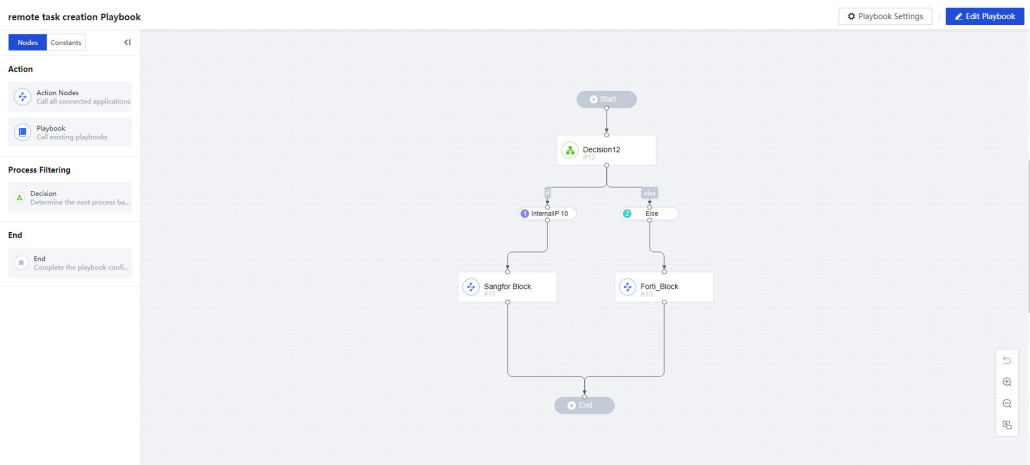
- **Condition for Execution:** mainly to delineate the scope of application of the policies through multiple dimensions. The dimensions are divided into **Asset Type, Group, Time Detected, IP, Rule ID, and Security Incident**. Only one condition can be configured each time. The relationship between them is **"and"** when there are multiple conditions. When there are various values in a single condition, the relationship between the value and the value is **"or"**. At least one condition must be chosen by default, as shown below.

Conditions for Execution

Condition 1:	Event Type	in	Select
Condition 2:	Select	in	Select
Condition 3:	Select	in	Select
Condition 4:	Select	in	Select
Condition 5:	Select	in	Select

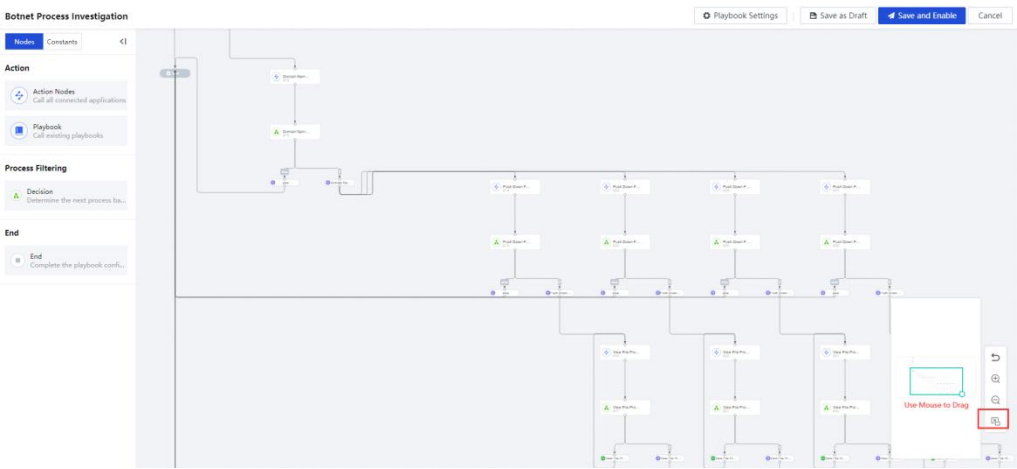
[+ Add Condition](#)

As shown in the figure above, the condition of the event type must exist by default and cannot be changed. Each dimension can only be referenced by one condition. When the condition has full with all attributes, the **Add Condition** button will be set at this time. Gray, non-editable status. After the policies are set, click **OK** to enter the canvas, and you can perform operations such as **Save Draft** and **Update Online** on the policies, as shown in the figure below.



In the above figure, click the canvas to undo the policies layout to the previous

action, click  to zoom in on the canvas, click  to zoom out, and click  to display thumbnails. Use the mouse to drag and adjust, as shown in the figure below.

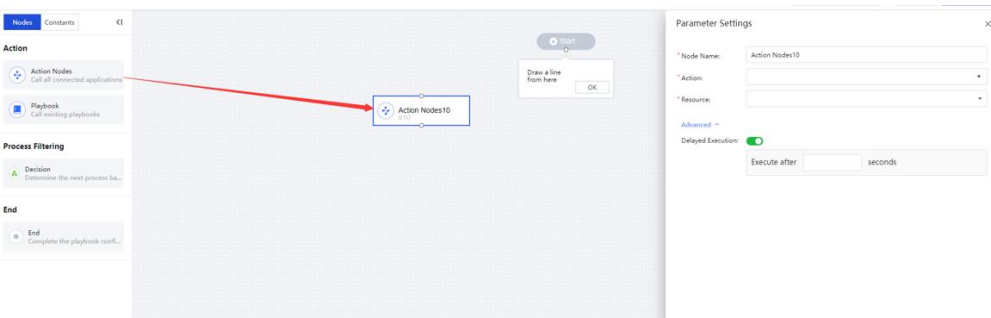


3.6.3 Add the Node

On the **Auto Response** page, under a policies category, click **Add** to enter the canvas interface and drag the **Action Nodes** icon in the left navigation bar to the middle canvas area.

Action Nodes

Drag the action node to the canvas and double-click to enter the Parameter Settings box, enter the **Node Name**, **Action**, **Device IP**, and click **Advanced** to turn on or off the **Delayed Execution** manually.



- **Action:** You can choose according to the application/action. There are differences in actions between different applications. You can choose visually **By App** or **By Action** according to the navigation of the pop-up box classification. You can also perform a fuzzy search for applications/motions based on keywords, as shown in the figure below.

Parameter Settings

* Node Name:

Action Nodes10

* Action:

* Resource:

By App

By Action

Advanced ^

Delayed Execution:

App Name

All Types

Network Security App

Sangfor Network Controller

Sangfor Cyber Command

Sangfor IAG

FortiGate

Paloalto

Macmon NAC

Bitdefender

Cisco ASA Firewall

OK

Cancel

Parameter Settings

* Node Name:

Action Nodes10

* Action:

* Resource:

By App

By Action

Advanced ^

Delayed Execution:

Name

All Types

Fix

Add Host Freeze

Modify Host Lockout

Remove Host Lockout

Query Host Lockout Status

Add Browsing Risk Notification

Add Account Lockout

Modify Account Lockout

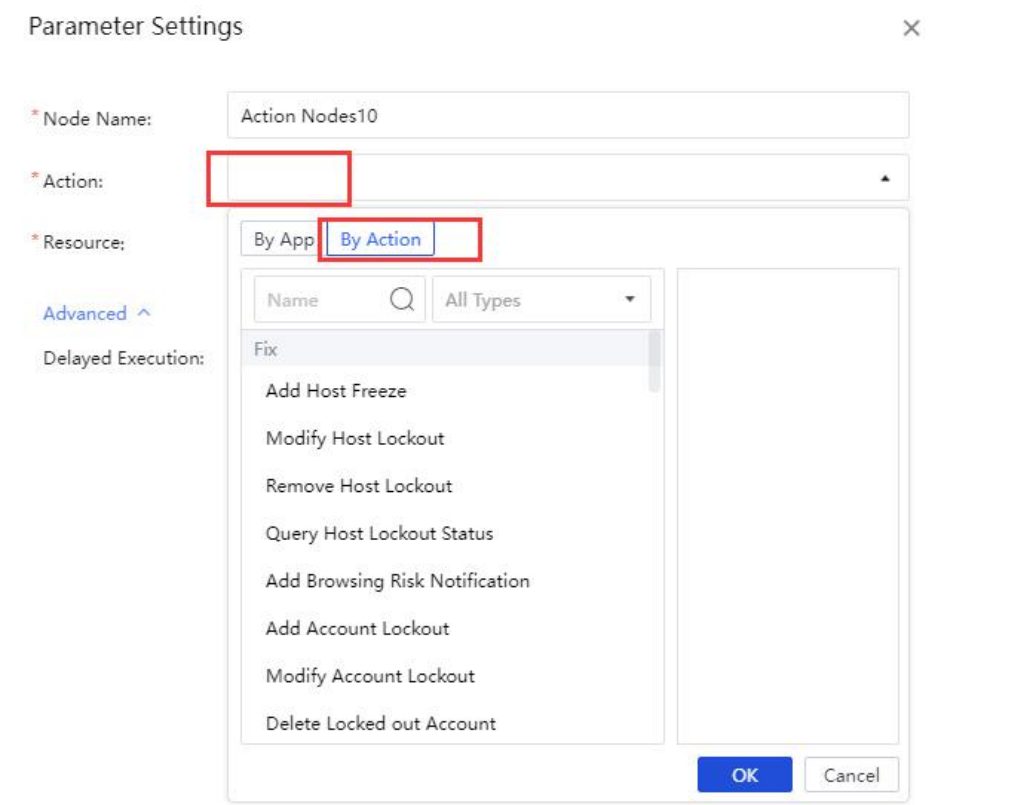
Delete Locked out Account

OK

Cancel

Action Node-policies

You can call an existing policy for nested action when adding a new policy. Drag **Action Nodes** directly to the canvas, double-click to configure, fill in the **Node Name**, select **By Action** for **Action**, the Delayed Execution is not enabled by default, then click **OK**, as shown in the figure below.



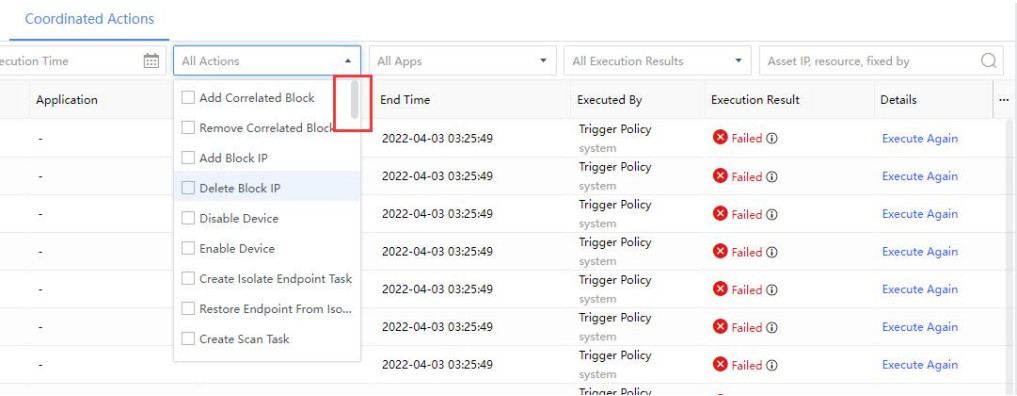
3.6.4 Response History

Go to **Response > Response History > Coordinated Actions**.

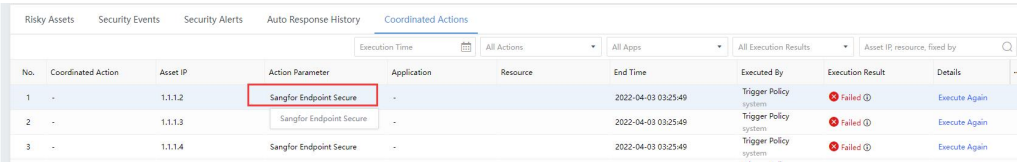
Action execution history mainly records action-level records, as shown in the following figure.

Coordinated Actions									
Execution Time									
No.	Coordinated Action	Asset IP	Action Parameter	Application	Resource	End Time	Executed By	Execution Result	Details
1	-	1.1.1.2	Sangfor Endpoint Secure	-	-	2022-04-03 03:25:49	Trigger Policy system	Failed (i)	Execute Again
2	-	1.1.1.3	Sangfor Endpoint Secure	-	-	2022-04-03 03:25:49	Trigger Policy system	Failed (i)	Execute Again

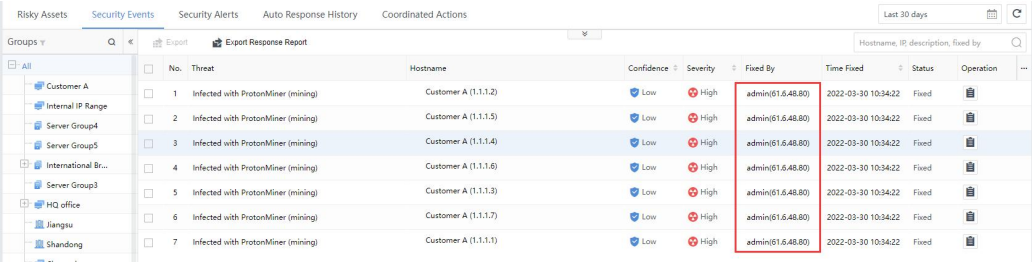
- **All Action:** All response actions supported by the Cyber Command platform, as shown in the following figure.



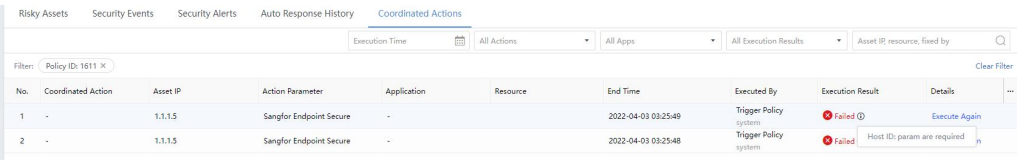
- **Action Parameter:** A collection of action-related properties, including calling application, calling resource, endpoint ID, file ID, file MD5, response method, event type, and risk level to be fixed. You can see it at the end of each successful action line, as shown in the following figure.



- **Fixed By:** The role that invokes the policies, including manual execution by Cyber Command platform users (for example, admin) and script triggering method (system creation automatic execution), as shown in the following figure.



- **Execution Result:** If it is the result of execution failure, the ⓘ icon will show the cause of the failure, as shown in the following figure.



- **All Execution Results:** If the execution is successful, you can click to view the details. If the execution fails, you can correct it according to the failure cause and click **Execute Again**, as shown in the following figure.

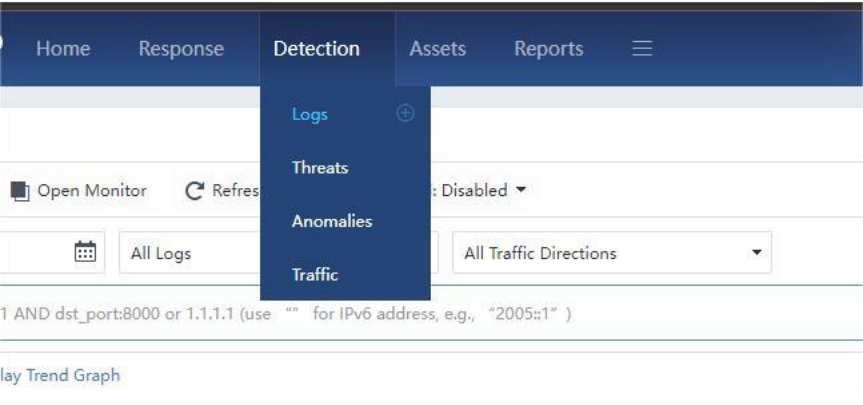
Coordinated Actions									
Execution Time: [Calendar Icon] All Actions All Apps Failed Asset IP resource, fixed by [Search Icon]									
Filter: Policy ID: 1611 X Clear Filter									
No.	Coordinated Action	Asset IP	Action Parameter	Application	Resource	End Time	Executed By	Execution Result	Details
1	-	1.1.1.5	Sangfor Endpoint Secure	-	-	2022-04-03 03:25:49	Trigger Policy system	Failed ⓘ	Execute Again
2	-	1.1.1.5	Sangfor Endpoint Secure	-	-	2022-04-03 03:25:48	Trigger Policy system	Failed ⓘ	Execute Again

3.7 Detection

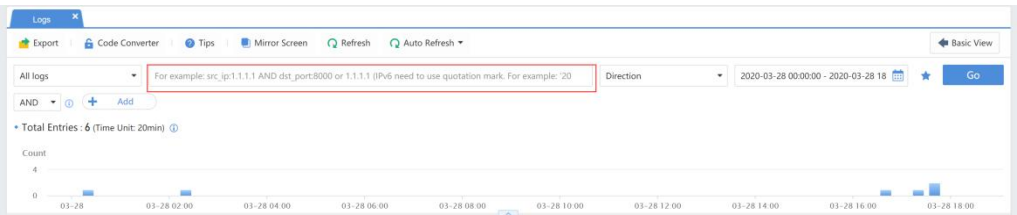
Certain experience is needed for further analysis of Security Incidents or risky hosts, normally this is used for the security professional personnel to do the analysis on the Security Incident and Security Events.

3.7.1 Logs

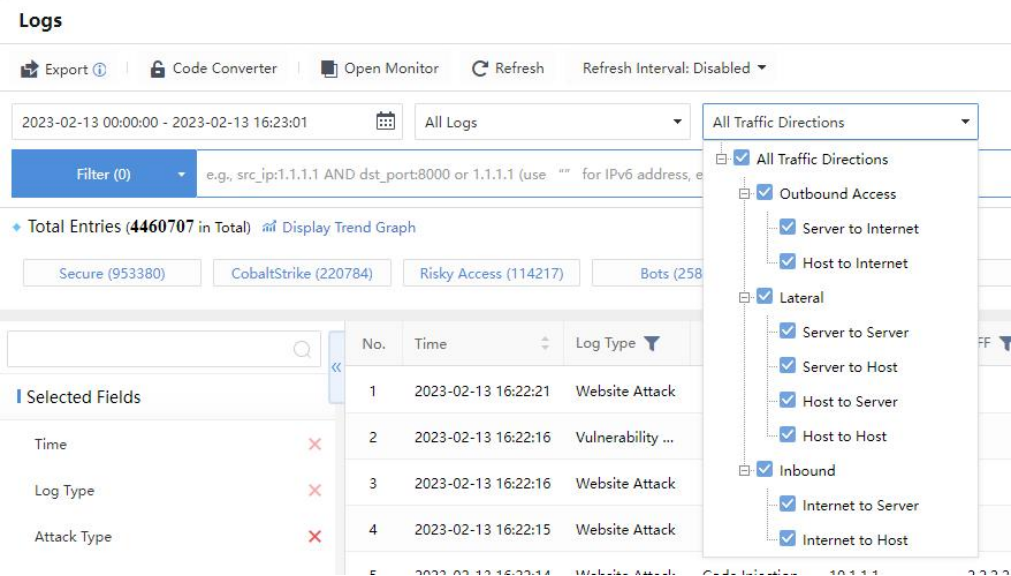
Retrieve security logs and audit logs. There are certain security analysis requirements, which are used when the security issues need further analysis.



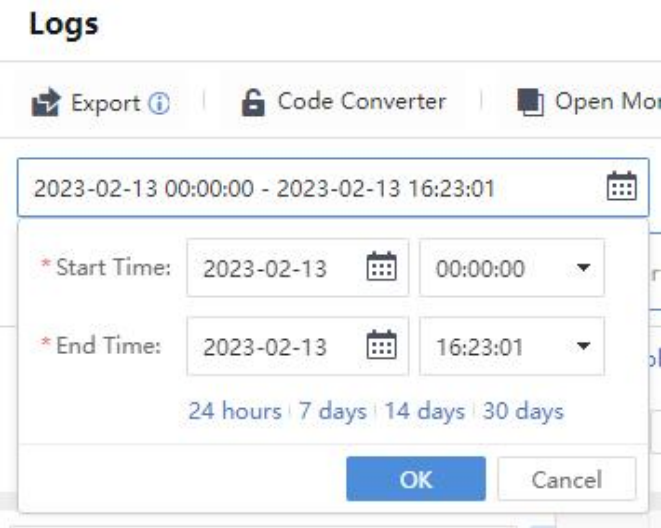
- **All Logs:** Divided into **Security Logs** and **Audit Logs**. You can view more detailed log types in each category.



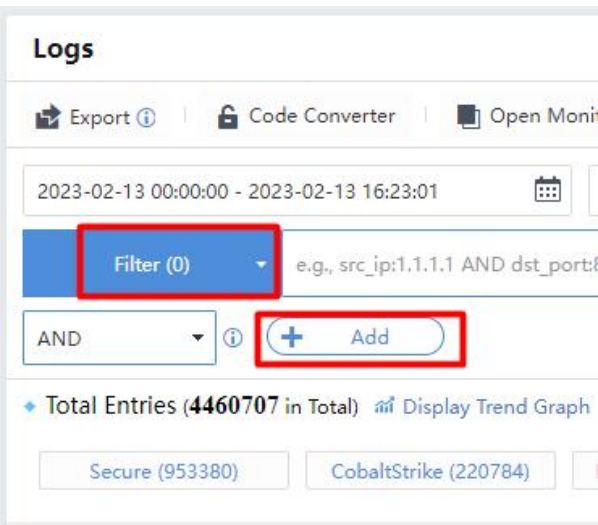
Click **Traffic Direction** to select the access direction of the log to be queried, as shown below:



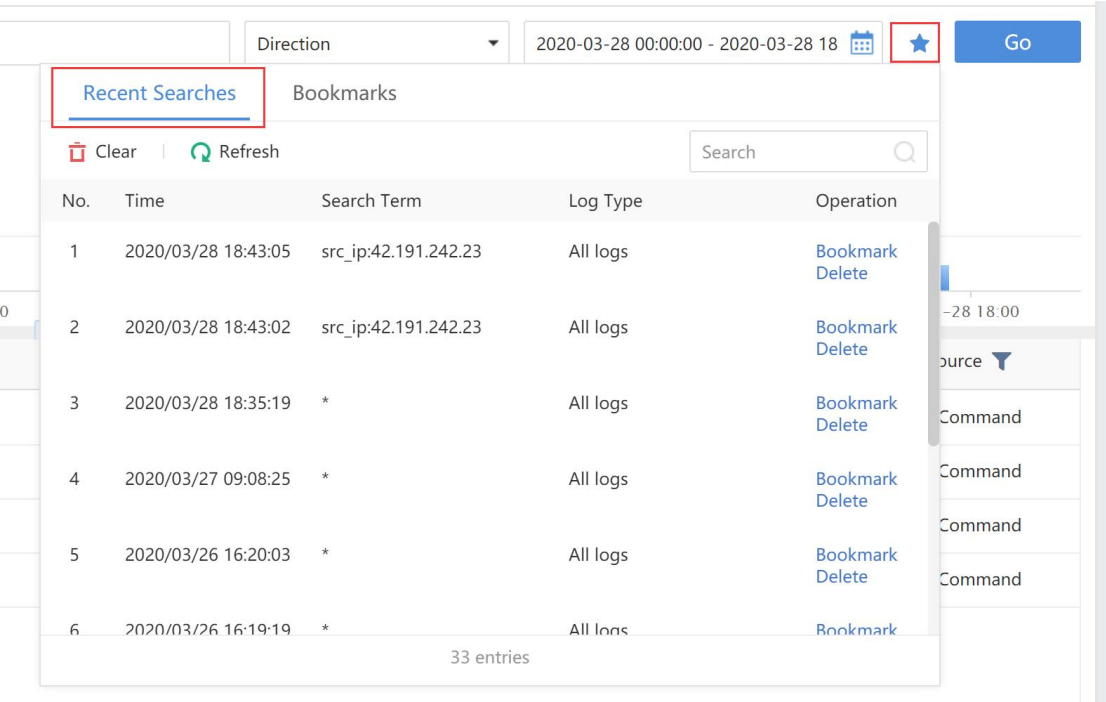
Click the time range to select the range of query time.



Click **Filter** > **Add** to query multiple conditions simultaneously.



Click  to query historical search records, and add the common search records to the favorites for later use.



- **Time:** Refer to the generation time of logs.
- **Search Term:** Refer to the attacks on hosts.
- **Log Type:** Refer to the types of logs.
- **Operation:** Bookmark the record.

3.7.2 Threats

Through the threat analysis module, Cyber Command can perform detailed analysis on threats such as **Ransomware, Cryptomining, File Threats, Inbound Attacks and Evasive Attacks.**

Ransomware

The ransomware risk analysis page focuses on displaying and managing ransom-themed Security Incidents. This part of the data mainly comes from ES and AF integration equipment. The traffic/process of relevant ransom behavior characteristics is found through traffic learning or endpoint security monitoring, and a small part of the data comes from Cyber Command.

Currently, the ransomware attack methods are:

RDP Brute-Force Attack, Ransomware Infection, Ransomware Attack, Commonly-Exploited Vuln, Commonly-Used Port, and C&C Communication

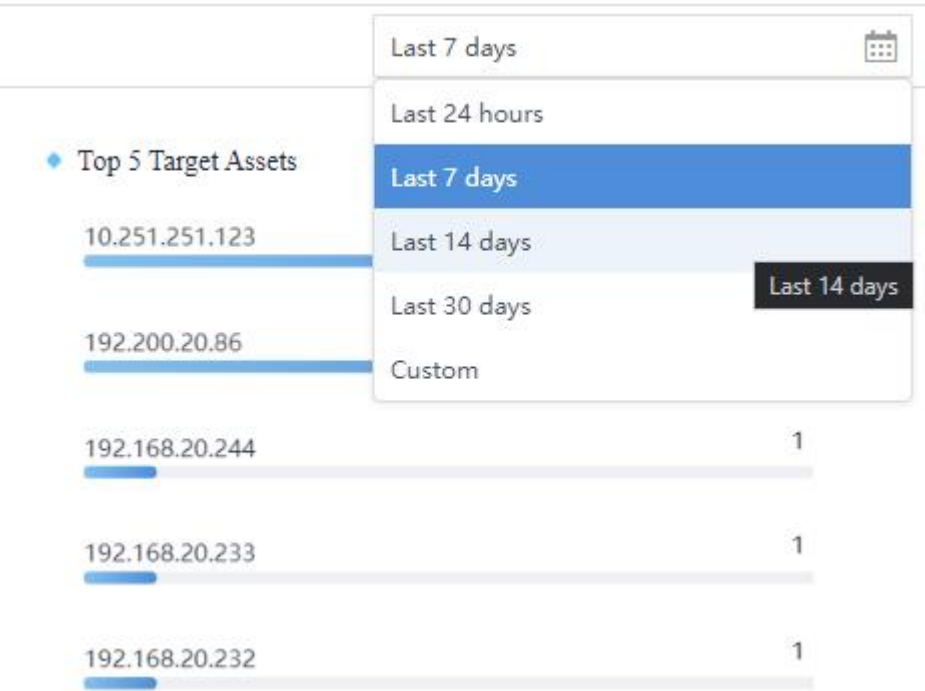
Threat presentation

On the **Ransomware** page, there are several parts, including **Time Selection**, **Detection**, **Top 5 Target Assets**, etc.

No.	Last Detected	Threat Description	Cryptomining Stage	Attack Stage	Severity	Target IP	Target Type	Attacker IP	Attacks	Result	Status	Operation
1	2022-04-18 17:41:32	Infected with Pygma (mining)	C&C Communication	C&C	High	8.1.1.7	Internet	-	9	Compromised	Pending	Coordinated Response
2	2022-04-18 17:41:32	Infected with bitcoinstminer (mining)	C&C Communication	C&C	High	8.1.1.88	Internet	-	48	Compromised	Pending	

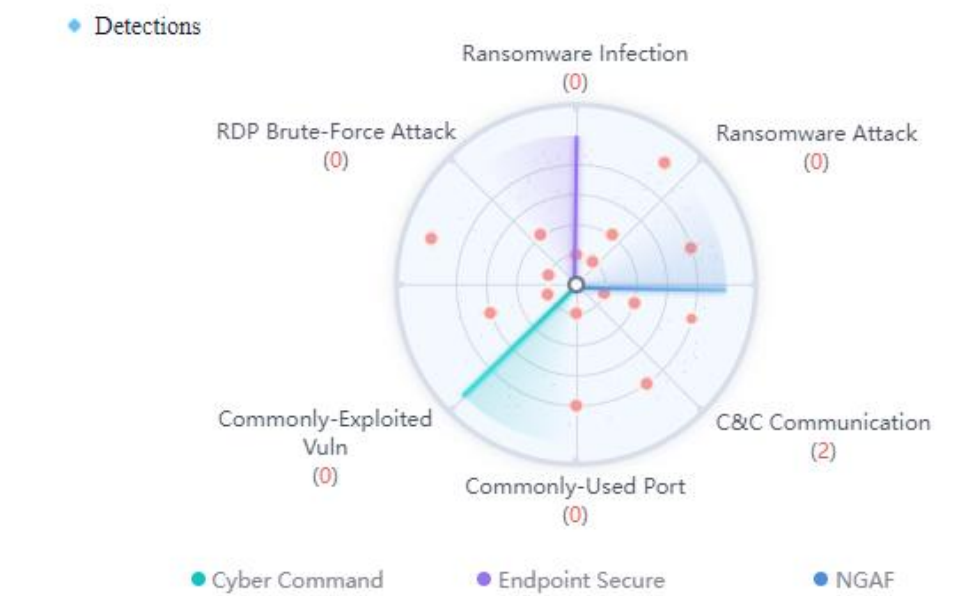
Time selection:

You can choose **Last 30 days**, **Last 7 days**, **Last 24 hours**, or **Custom** from the drop-down list (not only limited to 1 month, it can be customized), as shown in the figure below.



Detection

The sources of detection include Cyber Command, Endpoint Secure, and NGAF. The data are classified into the ransomware infection route/method, including **RDP Brute-Force Attack, Ransomware Infection, Ransomware Attack, Commonly-Exploited Vuln, Commonly-Used Port**, and **C&C Communication**, as shown in the figure below.



The red number represents the frequency of all ransomware risk assets that this method hits. The source device displays blue under normal conditions and gray when abnormal, and the associated 3-pointers are blue under normal conditions and will detect periodically.

Target Assets

Target assets are divided into four levels: High, Medium, Low, and Compromised. Click each severity level to see a list of related target assets.

No.	Last Detected	Threat Description	Risk	Attack Stage	Severity	Target IP	Target Type	Attacker IP	Attacks	Result	Status	Operation
1	2022-04-15 17:41:51	Infected with ransomware	C&C Communication	Impact	High	1.1.1.2, etc.	Host	1.1.1.1	76	Compromised	Pending	...
2	2022-04-15 17:41:52	Infected with ransomware	C&C Communication	Impact	High	1.1.1.1, etc.	Internet	1.1.1.1	80	Compromised	Pending	...
3	2022-04-08 09:00:32	Infected with ransomware	C&C Communication	Impact	High	1.1.1.2, etc.	Host	1.1.1.1	19	Compromised	Pending	...
4	2022-04-02 09:00:32	Infected with ransomware	C&C Communication	Impact	High	1.1.1.1, etc.	Internet	1.1.1.1	40	Compromised	Pending	...
5	2022-04-02 09:00:37	Infected with ransomware	C&C Communication	Impact	High	1.1.1.2, etc.	Host	1.1.1.1	19	Compromised	Pending	...
6	2022-04-02 09:00:37	Infected with ransomware	C&C Communication	Impact	High	1.1.1.1, etc.	Internet	1.1.1.1	20	Compromised	Pending	...

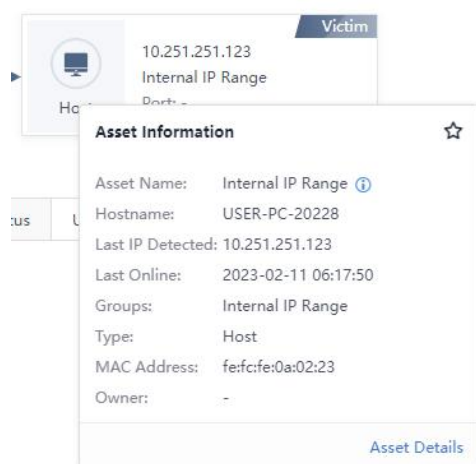
List view

The list of ransom risk assets includes **Last detection, Threat Description, Risk, Attack Stage, Severity, Target IP, Target Type, Attacker IP, Attacks, Result, Status, Operation**, etc.

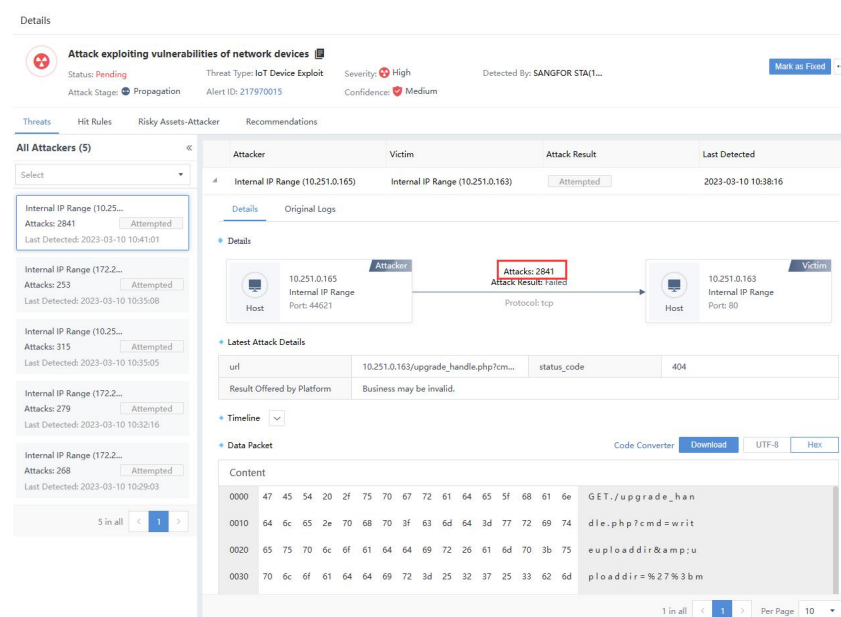
No.	Last Detected	Threat Description	Risk	Attack Stage	Severity	Target IP	Target Type	Attacker IP	Attacks	Result	Status	Operation
1	2022-04-15 17:41:51	Infected with ransomware	C&C Communication	Impact	High	1.1.1.2, etc.	Host	1.1.1.1	76	Compromised	Pending	...
2	2022-04-15 17:41:52	Infected with ransomware	C&C Communication	Impact	High	1.1.1.1, etc.	Internet	1.1.1.1	80	Compromised	Pending	...
3	2022-04-08 09:00:32	Infected with ransomware	C&C Communication	Impact	High	1.1.1.2, etc.	Host	1.1.1.1	19	Compromised	Pending	...
4	2022-04-02 09:00:32	Infected with ransomware	C&C Communication	Impact	High	1.1.1.1, etc.	Internet	1.1.1.1	40	Compromised	Pending	...
5	2022-04-02 09:00:37	Infected with ransomware	C&C Communication	Impact	High	1.1.1.2, etc.	Host	1.1.1.1	19	Compromised	Pending	...

Single view

Click the specific name in the **Threat Description** column to go to the **Details** page. The risk summary displays the **Asset Name, Hostname, Groups, Owner**, etc.



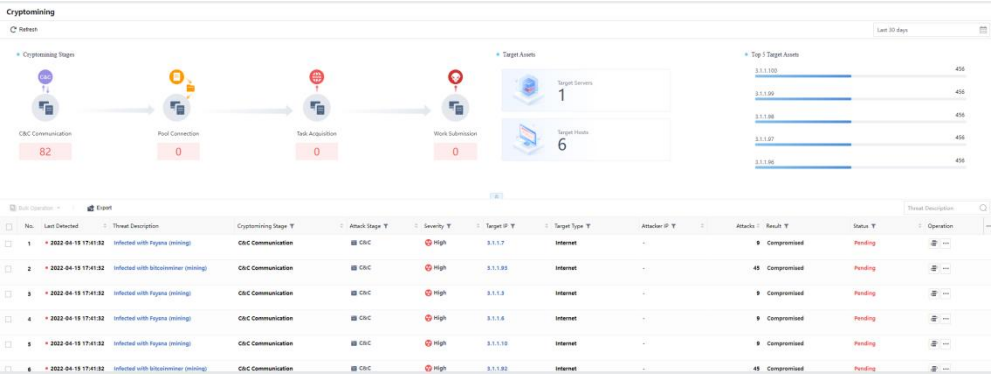
The risk details section mainly includes security alerts and ransomware exposure. Click the specific name of the **risk name** field in the list to enter the vulnerability details page.



Cryptomining

The **Cryptomining** special detection function can analyze the intranet mining events detected by the platform.

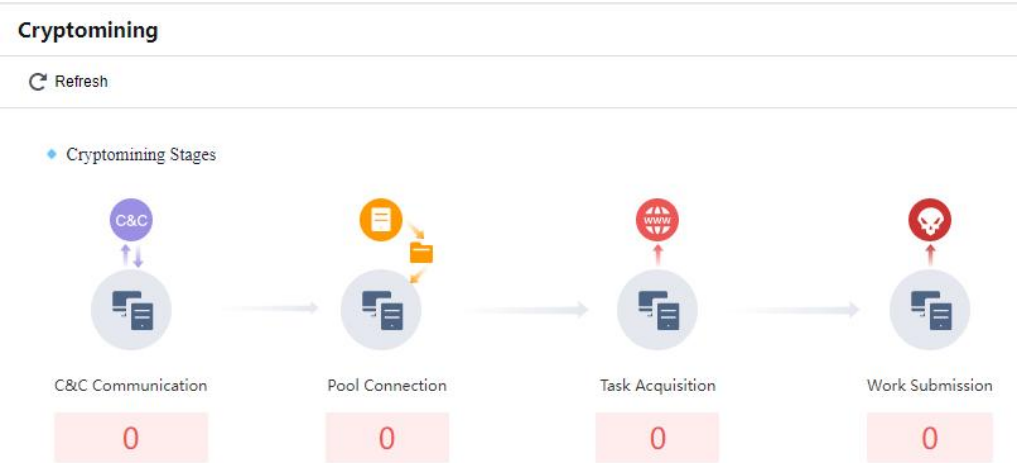
It displays the **Cryptomining Stages**, **Target Assets**, and **Top 5 Target Assets**, as shown below.



Click the listed **threat description** to jump to the security knowledge base in the help document to view detailed instructions for mining and suggestions. At the same time, click the typical mining case shown on the right to view the details of the case.

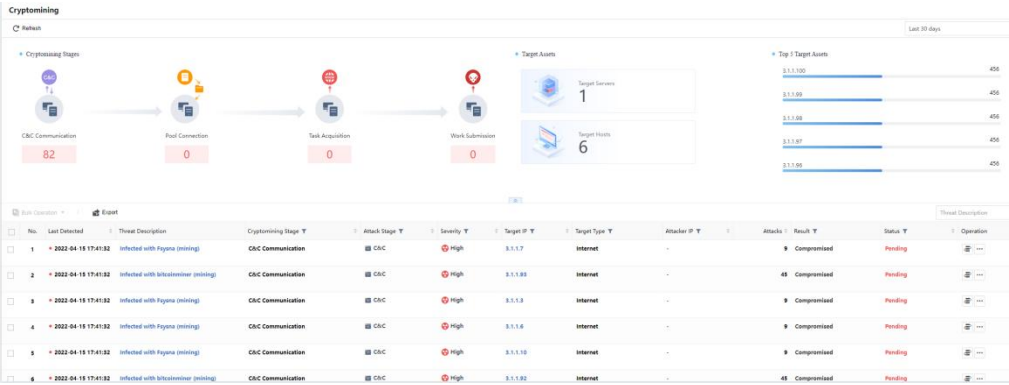
Cryptomining Stages

Under the **Cryptomining Stages**, you can analyze and display the affected hosts at different stages. Mining is divided into **C&C Communication**, **Pool Connection**, **Task Acquisition**, and **Work Submission**, as shown below.



Distribution of Cryptomining (number of infected hosts)

You can analyze and display the infected hosts. You can view the number of infected hosts for each stage and the risk trend of the number of mining events per day, as shown below.



Target Hosts

You can click the **Target Hosts** tab to view the hosts currently affected by the mining virus. Click **IP address** to view detailed Security Incidents information, and you can search through fields such as the mining stage. The page is shown in the figure below.



Mining Host Retrieval

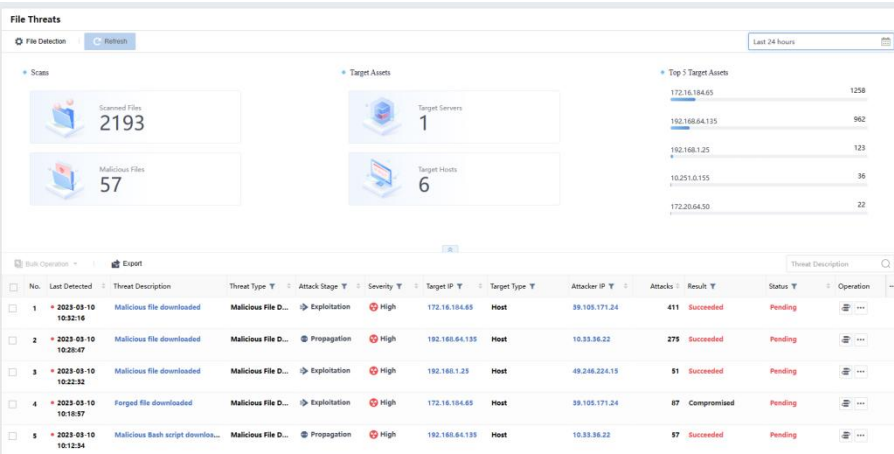
You can search according to the mining stage and keywords fuzzy search. The mining stage includes **C&C communication, Pool connection, Task acquisition, Work submission**, etc., as shown in the figure below.

No.	Last Detected	Threat Description	Cryptomining Stage	Attack Stage	Severity	Target IP	Target Type	Attacker IP	Attacks	Result	Status	Operation
1	2022-03-28 10:13:01	Infected with Cryptolink (mining)	C&C Communication	C&C	High	1.1.1.3	Host	-	38	Compromised	Pending	...
2	2022-03-28 10:13:01	Infected with Cryptolink (mining)	C&C Communication	C&C	High	1.1.1.6	Host	-	38	Compromised	Pending	...
3	2022-03-28 10:13:01	Infected with Cryptolink (mining)	C&C Communication	C&C	High	1.1.1.2	Host	-	38	Compromised	Pending	...
4	2022-03-28 10:13:01	Infected with Cryptolink (mining)	C&C Communication	C&C	High	1.1.1.8	Host	-	38	Compromised	Pending	...
5	2022-03-28 10:13:01	Infected with Cryptolink (mining)	C&C Communication	C&C	High	1.1.1.7	Host	-	38	Compromised	Pending	...
6	2022-03-28 10:13:01	Infected with Wannakr4st.0 (mining)	C&C Communication	C&C	High	1.1.1.2	Host	-	19	Compromised	Pending	...
7	2022-03-28 10:13:01	Infected with Protonminer (mining)	C&C Communication	C&C	High	1.1.1.4	Host	55.55.55.55, etc.	10	Compromised	Fixed	...
8	2022-03-28 10:13:01	Infected with Protonminer (mining)	C&C Communication	C&C	High	1.1.1.5	Host	55.55.55.55, etc.	10	Compromised	Fixed	...
9	2022-03-28 10:13:01	Infected with Protonminer (mining)	C&C Communication	C&C	High	1.1.1.2	Host	55.55.55.55, etc.	10	Compromised	Fixed	...
10	2022-03-28 10:13:01	Infected with Protonminer (mining)	C&C Communication	C&C	High	1.1.1.7	Host	55.55.55.55, etc.	10	Compromised	Fixed	...

File Threats

The file threat intrudes LAN hosts by spreading virus files. After the malicious file is executed in a user's host, it can control the host and disclose sensitive data. Thus, it is an important entry point in the attack chain.

You can view the statistics by selecting **Last 7 days**, **Last 30 days**, **Last 24 hours**, **Last 14 days**, or **Custom**.



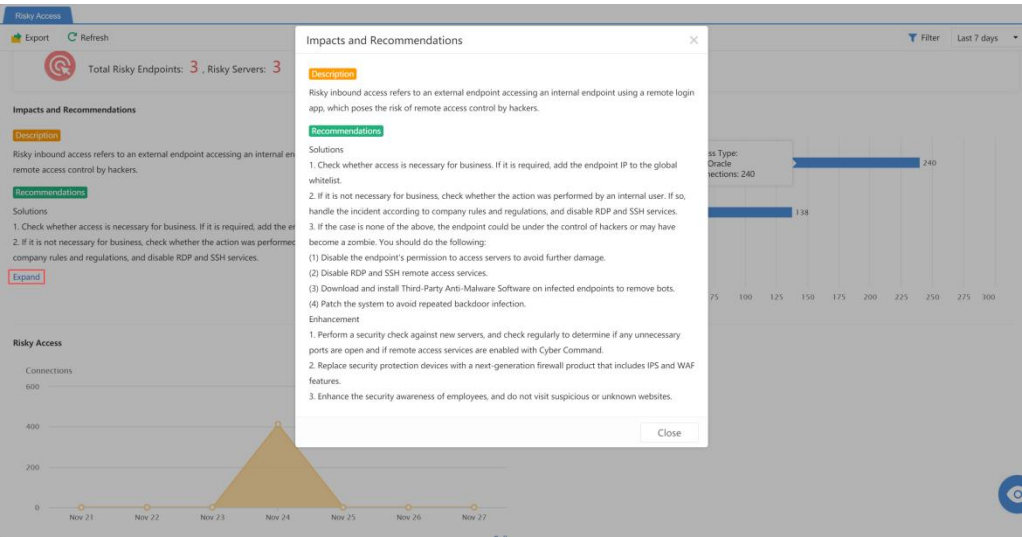
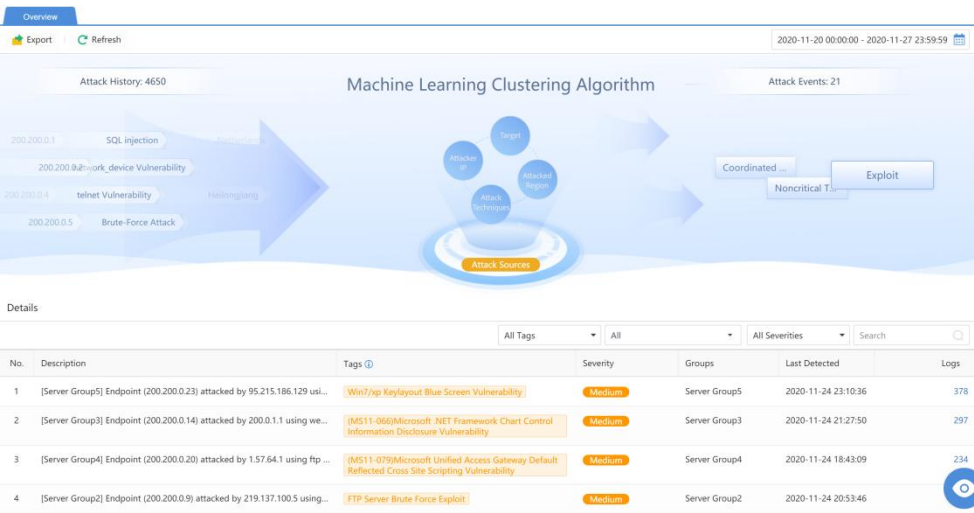
Click **Export** to export all file threats in the Excel format, as shown below:

File Threat Alerts												
Filter												
Period:	2023-02-14 11:37:02 - 2023-02-15 11:37:02											
Result												
No.	Last Detected	Threat Description	Threat Type	Attack Stage	Severity	Target IP	Target Type	Attacker IP	Attacks	Result	Status	
1	2023-02-15 11:34:32	Malicious file download	Malicious File Download	Exploitation	High	172.16.184.65	Host	39.105.171.24	431	Succeeded	Pending	
2	2023-02-15 11:33:51	Forged file download	Malicious File Download	Exploitation	High	172.16.184.65	Host	39.105.171.24	61	Compromised	Pending	
3	2023-02-15 11:13:31	Malicious file download	Malicious File Download	Propagation	High	192.168.64.135	Host	10.33.36.22	285	Succeeded	Pending	
4	2023-02-15 11:04:18	Malicious file download	Malicious File Download	Exploitation	High	192.168.1.25	Host	49.246.224.15	59	Succeeded	Pending	
5	2023-02-15 11:00:53	Download malicious Java	Malicious File Download	Propagation	Medium	172.20.64.50	Host	10.251.0.93	10	Succeeded	Pending	
6	2023-02-15 04:01:22	Download files as forged	Malicious File Download	Propagation	Medium	192.168.64.135	Host	10.33.36.22	6	Succeeded	Pending	
7	2023-02-15 03:13:20	Malicious file download	Malicious File Download	Propagation	High	172.16.197.133	Host	172.16.197.140	1	Succeeded	Pending	
8	2023-02-15 00:00:14	Webshell file(endpoint Sa	Webshell Access	Impact	High	-	Internet	10.231.30.13	4	Attempted	Pending	
9	2023-02-14 23:58:20	Malicious file download	Malicious File Download	Exploitation	High	172.16.184.65	Host	39.105.171.24	667	Succeeded	Pending	
10	2023-02-14 23:39:37	Forged file download	Malicious File Download	Exploitation	High	172.16.184.65	Host	39.105.171.24	152	Compromised	Pending	
11	2023-02-14 23:37:02	Malicious file download	Malicious File Download	Exploitation	High	192.168.1.25	Host	49.246.224.15	141	Succeeded	Pending	
12	2023-02-14 23:31:05	Malicious file download	Malicious File Download	Propagation	High	192.168.64.135	Host	10.33.36.22	522	Succeeded	Pending	
13	2023-02-14 23:13:11	Download malicious Java	Malicious File Download	Propagation	Medium	172.20.64.50	Host	10.251.0.93	18	Succeeded	Pending	

Last Detection Time: Refer to the recent time when Cyber Command detects malicious emails.

Inbound Attacks

Cyber Command can perform a **Machine Learning Clustering Algorithm** for attacks over some time to provide an overview of outbound attack clustering. As shown below:



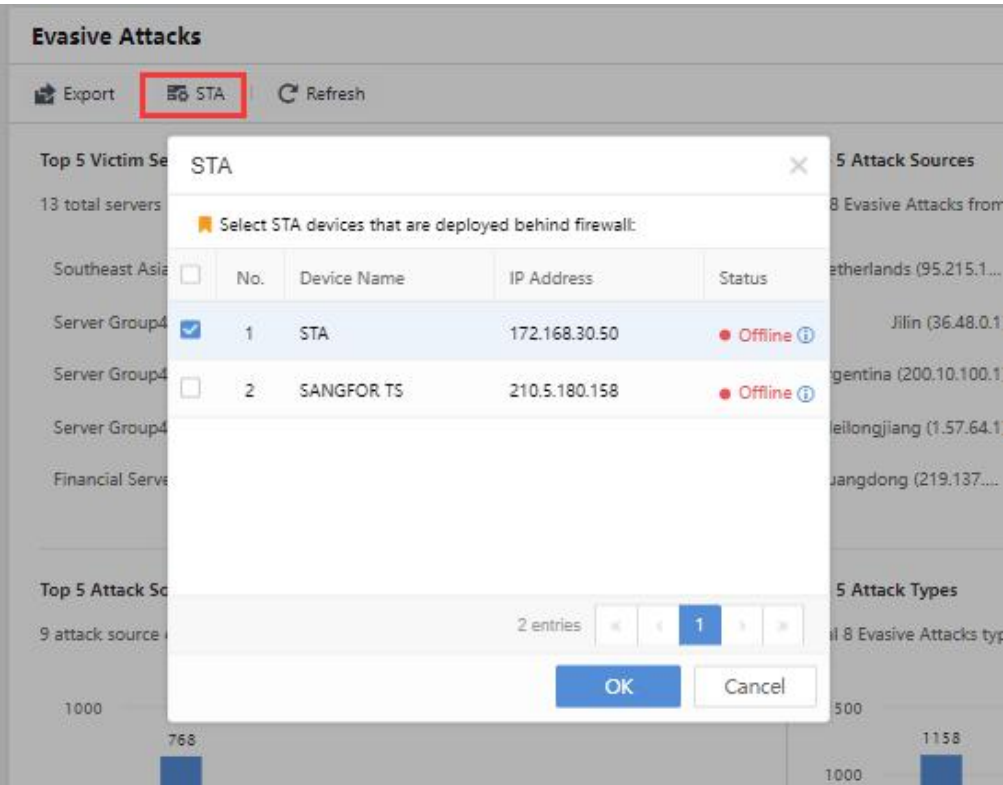
Evasive Attack

Evasive attacks refer to attacks detected by STA deployed behind the defense system. Such attacks indicate that the defense capabilities of the corresponding defense equipment need to be upgraded, or the defense policy has omissions and needs further reinforcement.

Definition of STA

To ensure accurate analysis of Evasive attacks, it is necessary to manually define the probes deployed behind the firewall. When the STA detects the external network attack behavior, the attack behavior is an evasive attack. The administrator can click **STA** to configure the STA behind the firewall on the **Detection > Threats > Evasive**

Attacks page.



Overall Display

On the **Detection > Threats > Evasive Attacks** page, the administrator can view the following TOP5 data:

- **Top 5 Target Servers by Attacks:** The top five servers have suffered the most evasive attacks.
- **Top 5 Attack Sources:** You can click **View More** to view all attack sources and export the data.
- **Top 5 Attack Source Regions:** The top five countries or regions have launched the most attacks.
- **TOP 5 Attack Types:** You can click **View More** to view detailed information, such as the victim's IP address corresponding to the attack type, and export the data.

You may also view the statistics based on the time range by selecting **Last 7 days**, **Last 30 days**, **Last 24 hours**, or **Today**. At the same time, you can click **Filter** to filter the **Attacker Geolocation** and **Attack Type**, as shown below:

Details

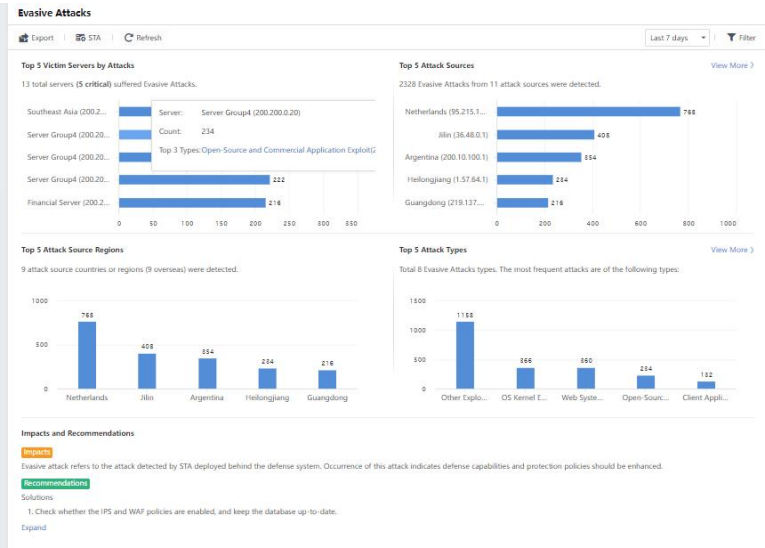
Select

Search

No.	Attacker IP	Attacker Geolocation	Detected By	Target	Target Asset Group	Attack Type	Time Attacked	Logs
1	219.137.100.5	Guangdong	STA(172.168.30.50)	Mail Server (3.3.3.3)	Customer-A	IoT Device Exploit(141), Web Framework Exploit(113), OS Kernel Exploit(2)	2022-03-28 10:09:21 - 2022-04-15 17:41:53	299
2	95.55.55.55	United States	STA(172.168.30.50)	Mail Server (3.3.3.3)	Customer-A	Code Injection(150), OS Kernel Exploit(115), Web Framework Exploit(46)	2022-03-28 10:09:24 - 2022-04-15 17:41:53	299
3	118.56.0.1	Beijing	STA(172.168.30.50)	Mail Server (3.3.3.3)	Customer-A	Web Framework Exploit(113), Code Injection(46)	2022-03-28 10:09:21 - 2022-04-15 17:41:53	161
4	222.144.0.1	Hubei	STA(172.168.30.50)	Mail Server (3.3.3.3)	Customer-A	Penetration Framework(115), OS Kernel Exploit(40)	2022-03-28 10:09:21 - 2022-04-15 17:41:53	161
5	200.10.100.1	Argentina	STA(172.168.30.50)	Mail Server (3.3.3.3)	Customer-A	Penetration Framework(138)	2022-03-28 10:09:21 - 2022-04-15 17:41:53	168
6	14.1.1.0.1	Malaysia	STA(172.168.30.50)	Mail Server (3.3.3.3)	Customer-A	OS Kernel Exploit(30)	2022-03-28 10:09:21 - 2022-04-15 17:41:53	92
7	161.157.0.1		STA(172.168.30.50)	Mail Server (3.3.3.3)	Customer-A	Penetration Framework(100)	2022-03-28 10:09:21 - 2022-04-15 17:41:53	49

7 entries

Administrators can click **Export** at the upper left corner of the page to export all evasive attacks as an excel sheet.



Top 5 Attack Source Regions

9 attack source countries or regions (9 overseas) were detected.

Netherlands

768

Jilin

408

Argentina

334

Heilongjiang

234

Guangdong

218

Top 5 Attack Types

Total 8 Evasive Attacks types. The most frequent attacks are of the following types:

Other Exploits(228)

1158

OS Kernel Exploits(22)

168

Web Spies(8)

890

Open-Source and Commercial Application Exploits(234)

234

Client Applications(112)

112

Impacts and Recommendations

Impacts

Evasive attack refers to the attack detected by STA deployed behind the defense system. Occurrence of this attack indicates defense capabilities and protection policies should be enhanced.

Recommendations

Solutions

1. Check whether the IPS and WAF policies are enabled, and keep the database up-to-date.

Expand

Detailed Analysis

On the **Detection > Threats > Evasive Attacks** tab, the administrator can view the attack details, including the **Attacker IP, Attacker Geolocation, Detected By, Attack Type, Time Attacked**, etc., as shown below.

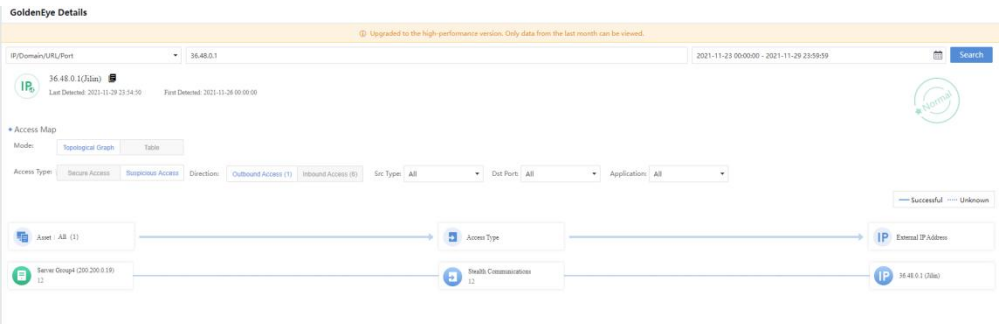
Details

All

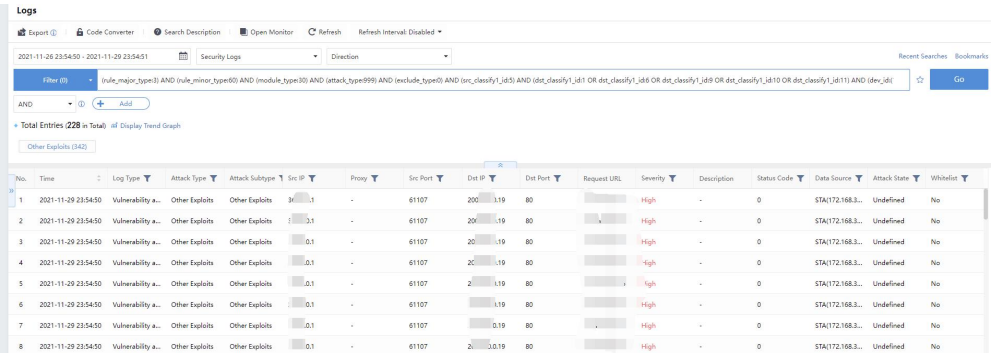
Search

No.	Attacker IP	Attacker Geolocation	Detected By	Victim	Victim Asset Group	Attack Type	Time Attacked	Logs
1	1.57.64.1	Heilongjiang	STA(172.168.30.50)	Server Group4 (200.200.0.20)	Server Group4	Open-Source and Commercial Application Exploit(234)	2021-11-26 18:43:09 - 2021-11-29 18:43:09	234
2	36.48.0.1	Jilin	STA(172.168.30.50)	Server Group4 (200.200.0.19)	Server Group4	Other Exploits(228)	2021-11-26 23:54:50 - 2021-11-29 23:54:50	228
3	95.215.186.129	Netherlands	STA(172.168.30.50)	Server Group4 (200.200.0.18)	Server Group4	Other Exploits(222)	2021-11-26 13:02:46 - 2021-11-29 13:02:46	222

Click a specific **Attacker IP**, and it will jump to the **GoldenEye Details** page to display the risk of the IP, as shown in the figure below.

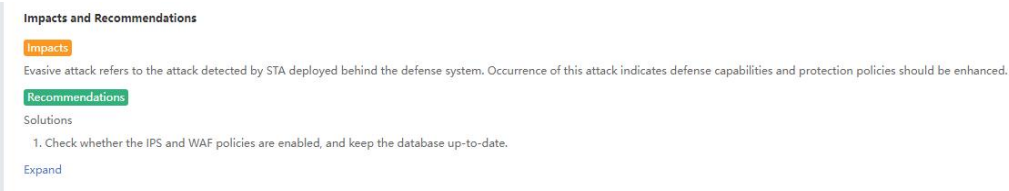


Click the **Attack Type** or the **number of logs** will jump to the **Detection > Logs** page to display the detailed log information of the attack type, as shown in the figure below.



Impact and Response Advice

Under the **Detection > Threats > Evasive Attacks** tab, the administrator can view the **Impacts and Recommendations**. You can click **Expand** to view the complete suggestions, as shown in the figure below.



3.7.3 Traffic

View the lateral access relationship of internal hosts and the external connection access relationship from the LAN host to the Internet.

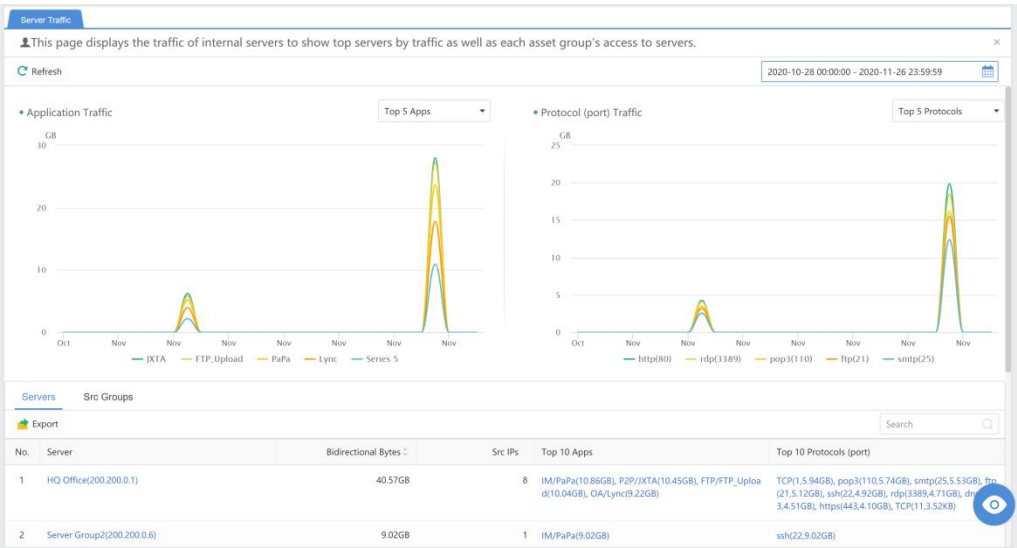
Lateral Traffic

Go to **Detection > Traffic > Lateral Traffic** page. It displays the traffic of internal servers to show top servers by traffic and each asset group’s access to servers,

including:

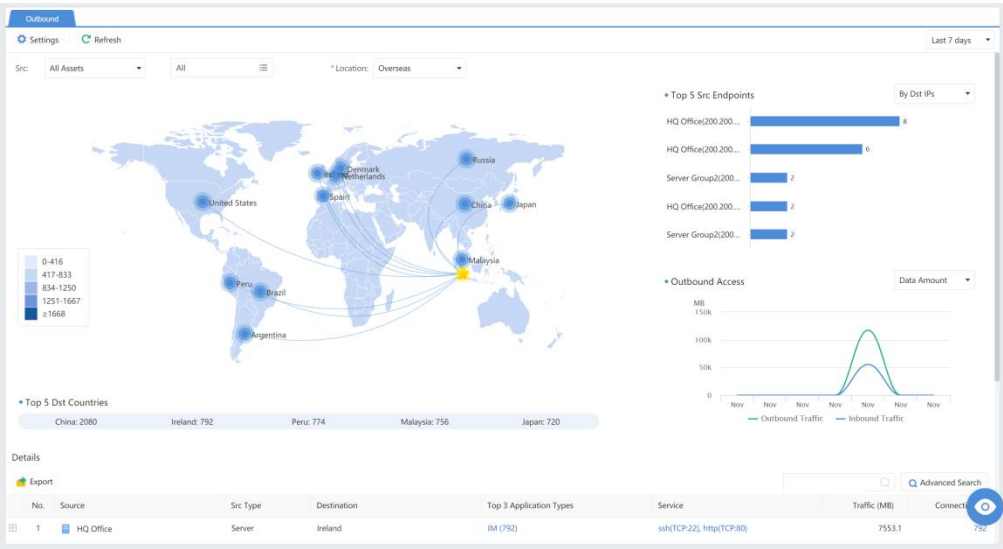
- The total number of servers and endpoints that initiated lateral threats and the total number of servers that suffered lateral attacks;
- The application traffic and protocol traffic.

At the same time, you can view the statistics of a time range by selecting **Last 7 days**, **Last 30 days**, **Last 14 days**, and **24 hours**, as shown below.

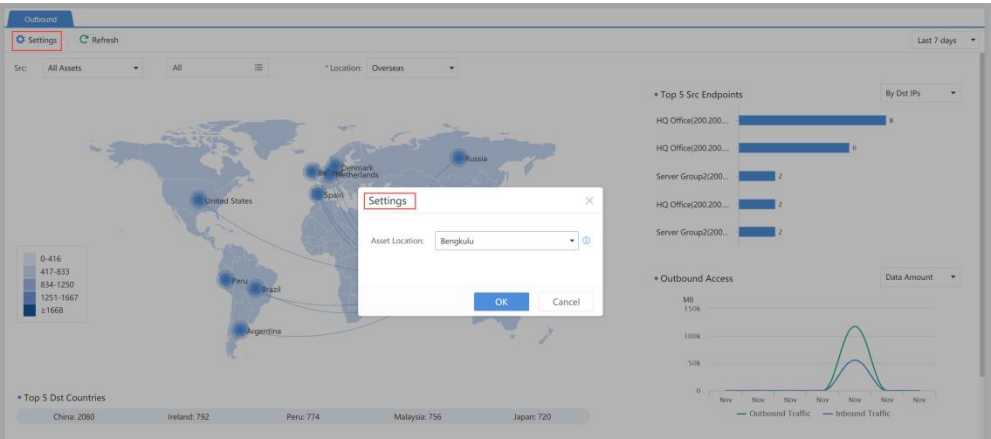


Outbound Traffic

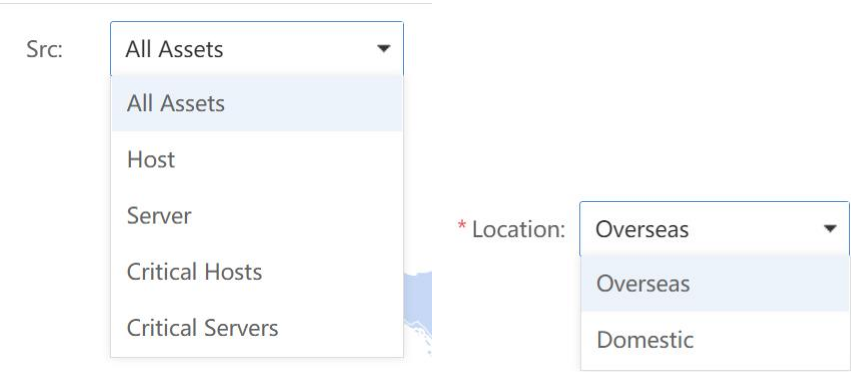
Outbound access is an access relationship between the endpoint or server and the Internet. You can change the data time range for outbound access data by selecting **Last 24 hours** or **Last 7 days** in the upper right corner.



Click **Settings** to change the **Asset location**. Select one point on the map to represent the user’s location.

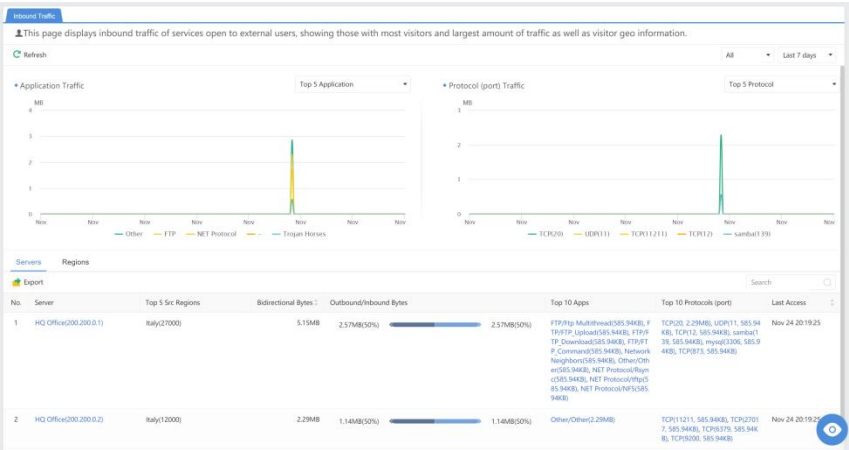


Select **Src** and **location** (Domestic or Overseas) to view the outbound access situations.



Inbound Traffic

This page displays inbound traffic of services open to external users, showing those with the most visitors and the largest amount of traffic and visitor geoinformation.



Risky Registration Regions

+ New

✖ Delete

🔄 Refresh

Search

☐	No.	Registration Region	Remarks	Operation
☐	1	 Samoa	No diplomatic relations with China,...	Delete
☐	2	 Russia	Countries with Active Hackers	Delete
☐	3	 Palau	No diplomatic relations with China,...	Delete
☐	4	 Mozambique	No diplomatic relations with China,...	Delete

8 entries

«

<

1

2

>

»

Close

3.7.4 Anomalies

Abnormal behavior analysis is mainly based on access direction and includes submodules such as **Unauthorized Access**, **Lateral Access**, and **Outbound Server Access**, etc.

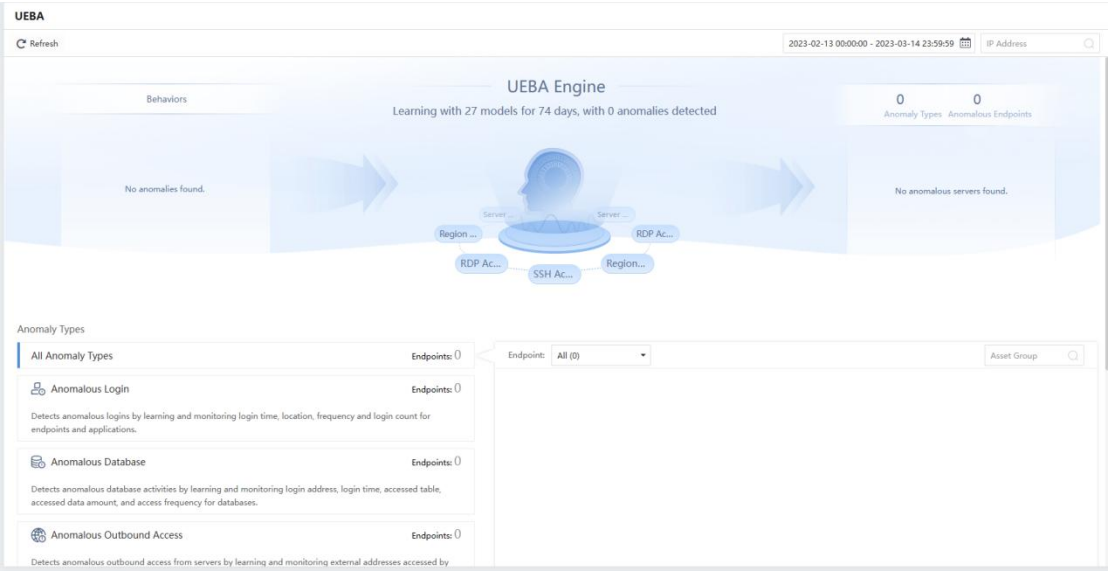
UEBA

The behavior analysis module can use the **UEBA(User and Entity Behavior Analytics)** engine to analyze the host (server/endpoint) operation’s abnormal behavior and display the behavior according to different risk scenarios. Under the **UEBA** page, the administrator can overview the number of days of continuous behavior study, risk scenarios/abnormal hosts/abnormal behaviors, and further view for different anomaly types.

At least 96 GB memory is required to display this UEBA module.

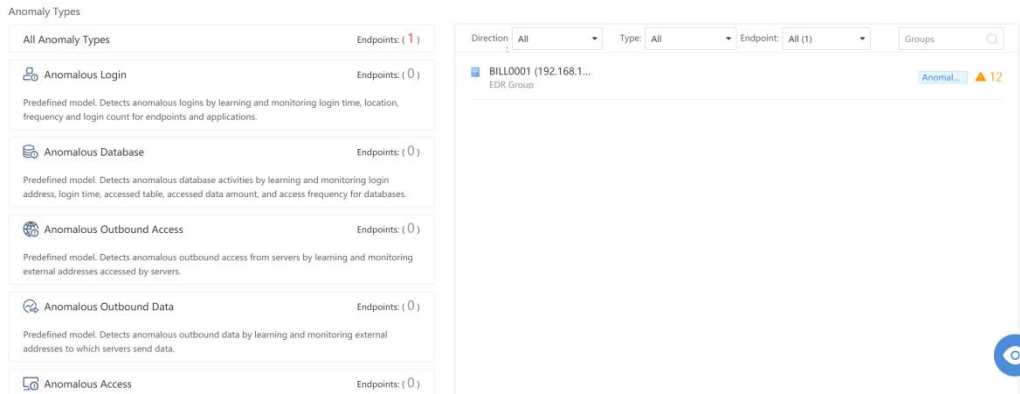
Overview

The administrator can search for abnormal behaviors according to **Time Range** or **IP Address**.

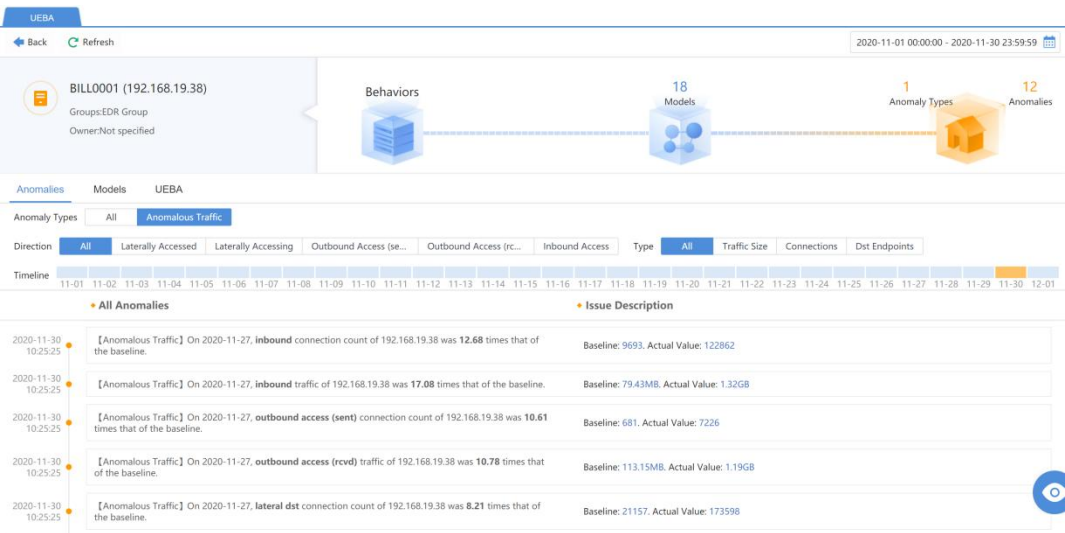


- All Anomaly Types

All anomaly types include **Anomalous Login, Anomalous Database, Anomalous Outbound Access, Anomalous Outbound Data, Anomalous Access, and Anomalous Traffic.**



Administrators can click specific Anomaly behaviors to view detailed **Anomalies, Models, and UEBA.**



3.7.5 Unauthorized Access

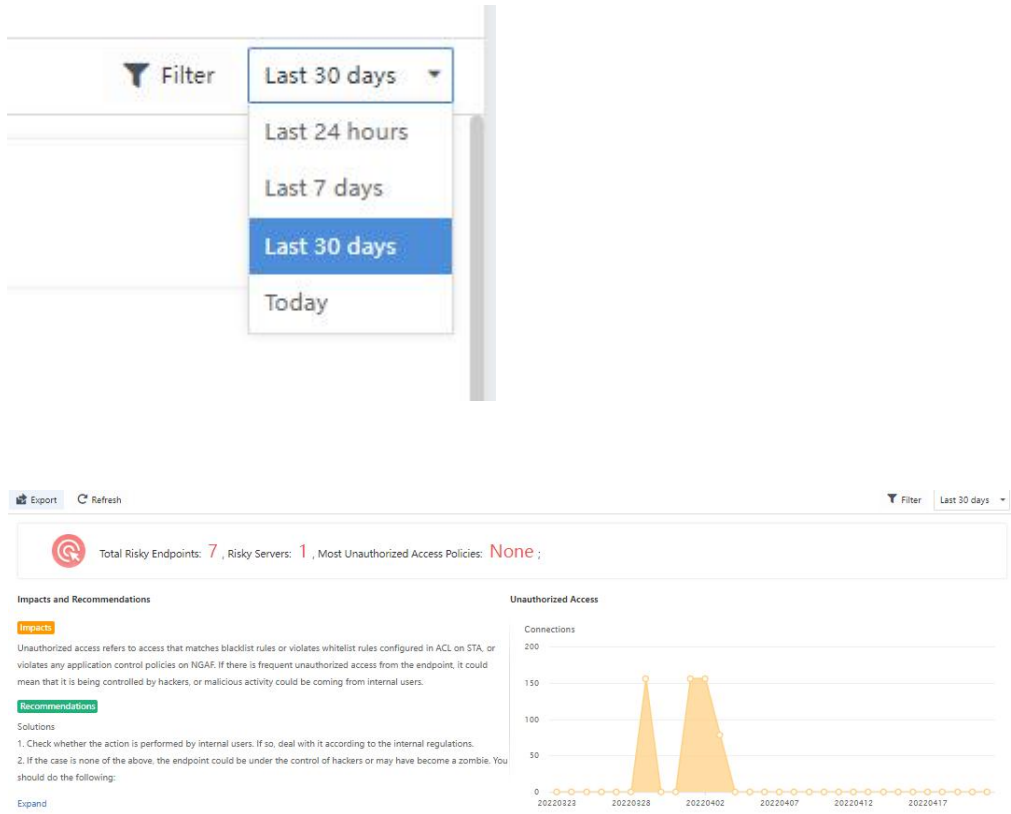
Unauthorized access mainly refers to the access behavior that matches the STA's illegal access policy blacklist or whitelist or the behavior that violates the application control policy in the next-generation firewall. When a host is frequently accessed in violation, the host may be controlled by a hacker or a violation by an intranet user. The Cyber Command platform displays the overall situation of illegal access for administrators on the **Detection > Anomalies > Unauthorized Access** page and guides specific analysis and corresponding handling.

Overall Display

Under the **Detection > Anomalies > Unauthorized Access** page, administrators can summarize the following overall data:

- **Lateral Threat:** Shows out all Lateral Threat
- **Outbound Threat:** Show out all outbound threat

In addition, you can view statistics of a specific time frame by selecting **Last 7 days**, **Last 30 days**, **Today**, or **Last 24 hours**.



The administrator can click the **Export** button in the top left corner of the page to export the data in the Excel format.

Detailed Analysis

Administrators can view unauthorized **Source** and **Destination** by category on the **Unauthorized Access** page.

Sources

Administrators can view the Src IP, Src Type, Groups, Destinations, Dst Type, Top 3 Policy Breaches, and Logs, as shown in the following figure.

Sources		Destinations							
All (0)		Server to Server (0)	Host to Server (0)	Host to Host (0)	Server to Host (0)	☐ Critical Servers Only		IP address, Asset Group	
No.	Src IP	Src Type	Asset Group	Destinations	Dst Type	Top 3 Policy Breaches		Logs	
No data available									

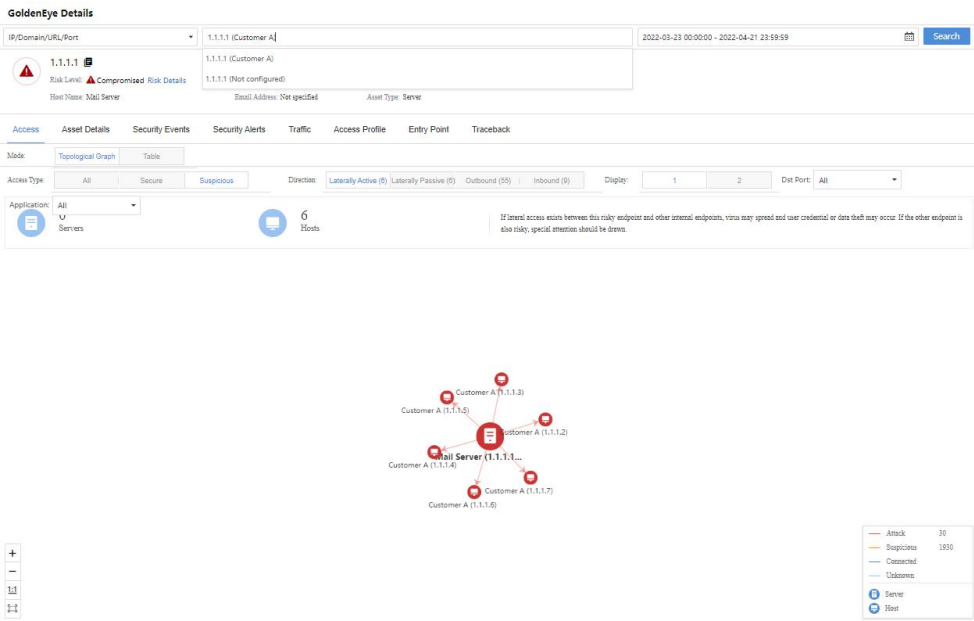
You can filter by **All**, **Server to Server**, **Host to Host**, **Host to Server**, or **Server to Host**. You can also directly search for the IP address/asset organization through the search box on the right side and check the **Critical Servers Only** checkbox. The list will display the details of the critical server only.

Sources		Destinations					
All (7)		Server to Server (0)		Host to Server (6)		Host to Host (0)	
						Server to Host (1)	
						☐ Critical Servers Only	
						IP address, Asset Group	
No.	Src IP	Src Type	Asset Group	Destinations	Dst Type	Top 3 Policy Breaches	Logs
1	Customer A (1.1.1.1)	Server	Customer A	6	Host	None(294)	294
2	Customer A (1.1.1.2)	Host	Customer A	1	Server	None(42)	42
3	Customer A (1.1.1.3)	Host	Customer A	1	Server	None(42)	42
4	Customer A (1.1.1.4)	Host	Customer A	1	Server	None(42)	42
5	Customer A (1.1.1.5)	Host	Customer A	1	Server	None(42)	42
6	Customer A (1.1.1.6)	Host	Customer A	1	Server	None(42)	42
7	Customer A (1.1.1.7)	Host	Customer A	1	Server	None(42)	42
7 entries							



The illegal access policy needs to be configured on the STA in advance. For the configuration method, see the STA security policy configuration section.

Administrators can click the specific IP/internal target number to jump to the corresponding **GoldenEye Details** page for further details, as shown in the following figure.



The administrator can click the specific **policy breaches** to jump to the corresponding **Detection > Logs** to automatically filter the corresponding logs, as shown below.

Logs

Export

Code Converter

Open Monitor

Refresh

Refresh Interval: Disabled

2022-03-23 00:00:00 - 2022-04-21 23:59:59

Traffic

Direction

Recent Searches

Bookmarks

Filter (0)

(rule_major_type=40) AND (src_ip=1.1.1.1) AND (src_asset_id=680) AND (src_branch_id=50) AND (dst_ip=1.1.1.4) AND (dst_asset_id=587) AND (dst_branch_id=50) AND (rule_major_type=1) AND (exclude_type=0) AND (NOT serv_cnc3595)

AND

Add

Total Entries (35 in Total)

all

Display Trend Graph

Unauthorized Accesses

No.	Time	Log Type	Src IP	Src Port	Dst IP	Dst Port	Access Type	Description	App Type	App Name	Data Source	Action
1	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
2	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
3	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
4	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
5	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
6	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
7	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
8	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
9	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
10	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
11	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
12	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
13	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
14	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
15	2022-04-15 17:34:43	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
16	2022-04-15 17:34:43	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
17	2022-04-15 17:34:43	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
18	2022-04-15 17:34:43	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
19	2022-04-15 17:34:43	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow

Destinations

On the **Destinations** page, administrators can view the **Src IP, Src Type, Groups, Destinations, Dst Type, Top 3 Risky Access Types**, and **Logs**, as shown in the following figure.

SourcesDestinations

All (8)

Server (0)

Host (8)

Critical Servers Only

IP address, Groups

No.	Dst IP	Dst Type	Groups	Sources	Top 3 Risky Access Types	Logs
-----	--------	----------	--------	---------	--------------------------	------

You can filter by **All, Server**, and **Host**, and support searching and filtering by IP/asset organization; if you check the **Critical Servers Only** checkbox, the list only displays the data details of critical servers.

SourcesDestinations

All (0)

Server (0)

Host (0)

Critical Servers Only

IP address, Groups

No.	Dst IP	Dst Type	Groups	Sources	Top 3 Policy Breaches	Logs
-----	--------	----------	--------	---------	-----------------------	------

The administrator can click the **specific Top 3 Risky Access Types** and jump to the corresponding **Detection > Logs** to automatically filter the corresponding logs, as shown in the figure below.

Logs

Export

Code Converter

Open Monitor

Refresh

Refresh Interval: Disabled

2022-03-23 00:00:00 - 2022-04-21 23:59:59

Traffic

Direction

Recent Searches

Bookmarks

Filter (0)

(rule_minor_type=0) AND (src_ip=1.1.1.1) AND (src_asset_id=680) AND (src_branch_id=50) AND (dst_ip=1.1.1.4) AND (dst_asset_id=587) AND (dst_branch_id=50) AND (rule_major_type=1) AND (exclude_type=0) AND (NOT serv_cnc1506)

Search

AND

+

Add

Total Entries (35 in Total)

all

Display Trend Graph

Unauthorized Accesses

No.	Time	Log Type	Src IP	Src Port	Dst IP	Dst Port	Access Type	Description	App Type	App Name	Data Source	Action
1	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
2	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
3	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
4	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
5	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
6	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
7	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
8	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
9	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
10	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
11	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
12	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
13	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
14	2022-04-15 17:38:03	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
15	2022-04-15 17:34:43	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
16	2022-04-15 17:34:43	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
17	2022-04-15 17:34:43	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
18	2022-04-15 17:34:43	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow
	2022-04-15 17:34:43	Traffic	1.1.1.1	1	1.1.1.4	1	-	None	-	-	STA(172.168.30.50)	Allow

3.7.6 Lateral Access

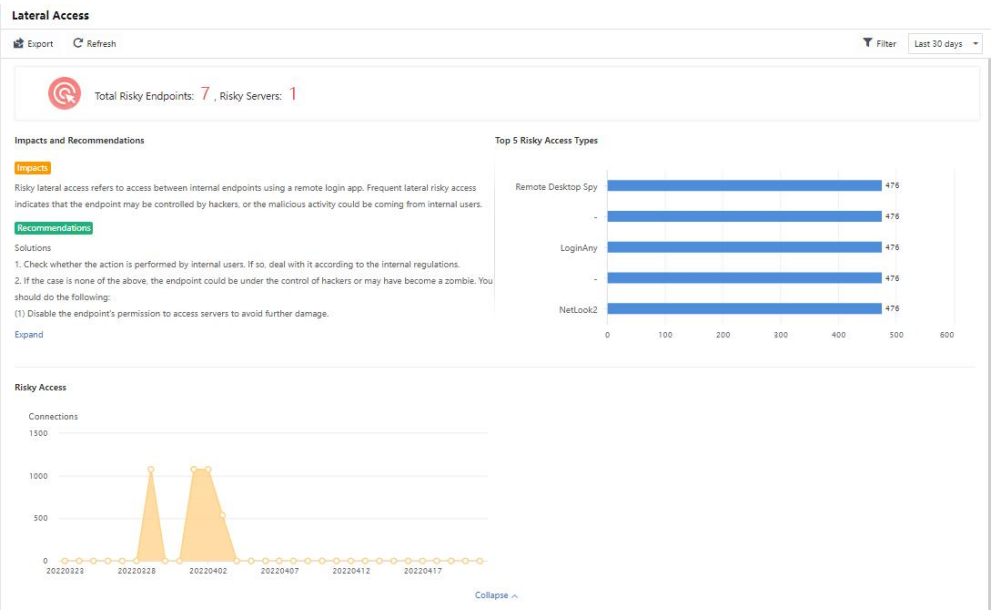
Lateral attacks mainly refer to attacks by internal endpoints on other internal endpoints. Hackers may control the endpoint to become a springboard to control more other endpoints on the intranet or malicious acts by intranet users, which significantly impact the customer's intranet security. On the **Lateral Access** page, the Cyber Command platform displays the overall situation of Lateral attacks for administrators and guides specific analysis and corresponding solutions.

Overall Display

Under the **Lateral Access** page, the administrator can overview the following overall data:

- The number of **Risky Endpoints** and **Risky Servers**.
- **Risky Access:** Record the number of insider attacks that occur every day over some time.
- **Impacts and Recommendations:** Includes hazard description and safety recommendations. Click **Expand** to view the complete recommendations.

You can view the statistics of a specific time range by selecting **Last 7 days**, **Last 30 days**, **Today**, and **Last 24 hours**. At the same time, you can click **Filter** to customize the **Period** and **Application**, as shown in the following figure.



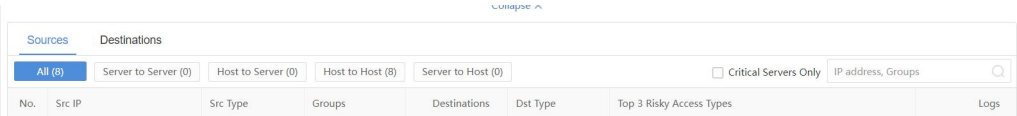
The administrator can click **Export** to export the data into an excel sheet.

Detailed Analysis

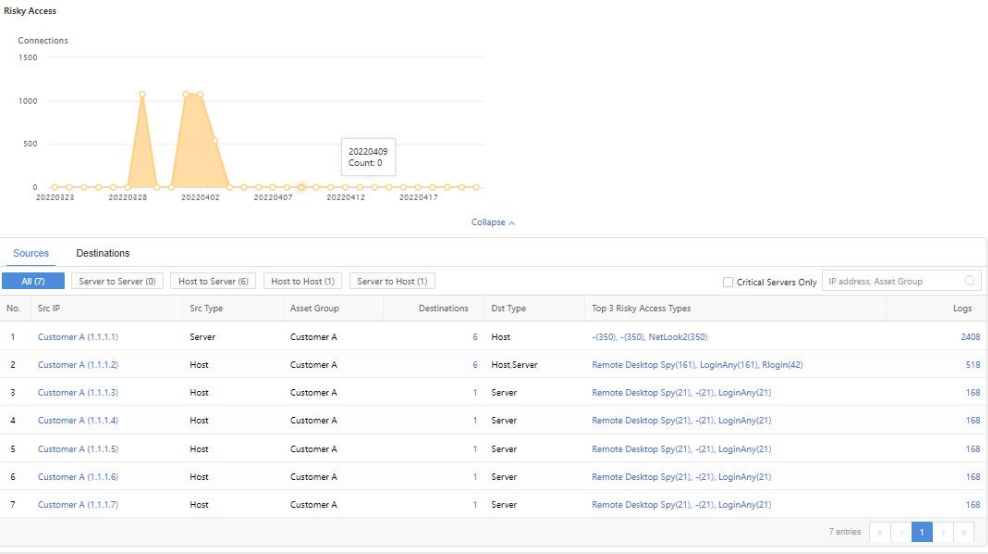
Under the **Lateral Access** tab, the administrator can see the **Source** and **Destination** columns.

Source

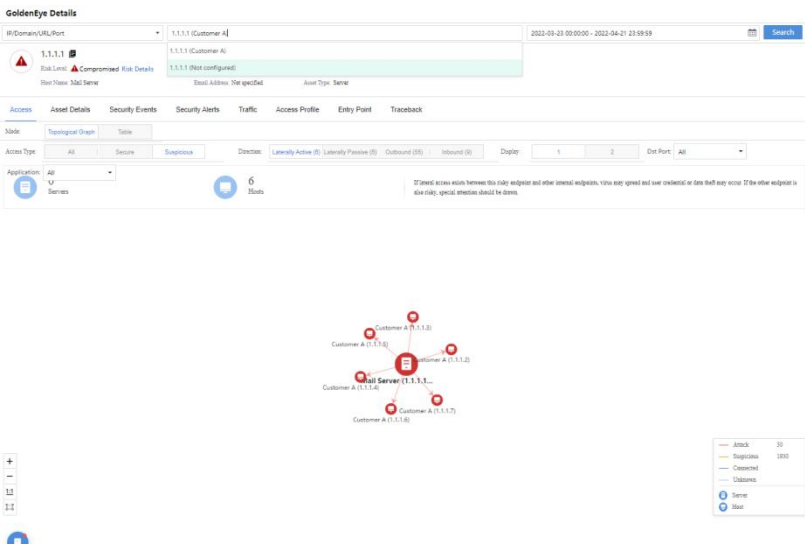
On the **Sources** page, administrators can view the Src IP, Src Type, Groups, Destinations, Dst Type, Top 3 Policy Breaches, and Logs, as shown in the following figure.



You can filter through **All**, **Server to Server**, **Host to Server**, **Host to Host**, **Server to Host**, or directly search the **IP address/Asset Group** through the search box.



Administrators can click the specific Source IP/number of Destinations to jump to the corresponding **GoldenEye Details** page to further display detailed information, as shown in the following figure.



The administrator can click the **specific Top 3 Risky Access Types**, jump to the corresponding **Detection > Logs** page and automatically filter the corresponding logs, as shown in the following figure.

Logs

Export

Code Converter

Open Monitor

Refresh

Refresh Interval: Disabled

2022-03-23 00:00:00 - 2022-04-21 23:59:59

Traffic

Direction

Recent Searches

Bookmarks

Filter (0)

(rule_major_type:1) AND (rule_minor_type:30) AND (exclude_type:0) AND (src_ip:1.1.1.1) AND (src_branch_id:50) AND (src_classify_id:1 OR src_classify_id:2 OR src_classify_id:6 OR src_classify_id:7 OR src_classify_id:8 OR src_

AND

+

Add

Search

Total Entries (1150) in Total

Display Trend Graph

Risky Access (150)

No.	Time	Log Type	Src IP	Src Port	Dst IP	Dst Port	Access Type	Description	App Type	App Name	Data Source	Action
1	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.3	1	-	Remote access via...	-	NetLook2	STA(172.168.30.50)	Allow
2	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.3	1	-	Remote access via...	-	NetLook2	STA(172.168.30.50)	Allow
3	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.5	1	-	Remote access via...	-	NetLook2	STA(172.168.30.50)	Allow
4	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.6	1	-	Remote access via...	-	NetLook2	STA(172.168.30.50)	Allow
5	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.6	1	-	Remote access via...	-	NetLook2	STA(172.168.30.50)	Allow
6	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.7	1	-	Remote access via...	-	NetLook2	STA(172.168.30.50)	Allow
7	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.3	1	-	Remote access via...	-	NetLook2	STA(172.168.30.50)	Allow
8	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.6	1	-	Remote access via...	-	NetLook2	STA(172.168.30.50)	Allow
9	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.2	1	-	Remote access via...	-	NetLook2	STA(172.168.30.50)	Allow
10	2022-04-15 17:41:53	Traffic	1.1.1.1	1	1.1.1.2	1	-	Remote access via...	-	NetLook2	STA(172.168.30.50)	Allow

Destinations

On the **Destinations** page, administrators can view the victim IP/type (server/host), asset organization, number of internal attackers, TOP3 attack types, and log number information, as shown in the following figure.

Sources

Destinations

All (8)

Server (0)

Host (8)

Critical Servers Only

IP address, Groups

No.	Dst IP	Dst Type	Groups	Sources	Top 3 Risky Access Types	Logs
-----	--------	----------	--------	---------	--------------------------	------

Internal victims can filter by **All**, **Servers**, and **Hosts**, and check the **Critical Server Only** checkbox to display the details of core servers in the list. At the same time, **IP address** or **Asset Group** search is supported.

Sources

Destinations

All (7)

Server (1)

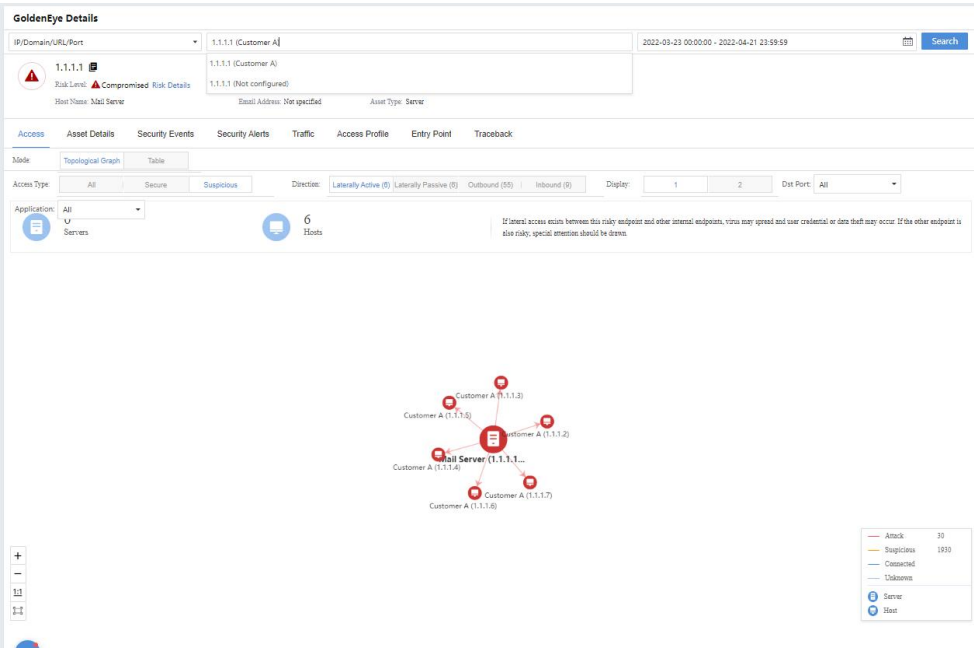
Host (6)

Critical Servers Only

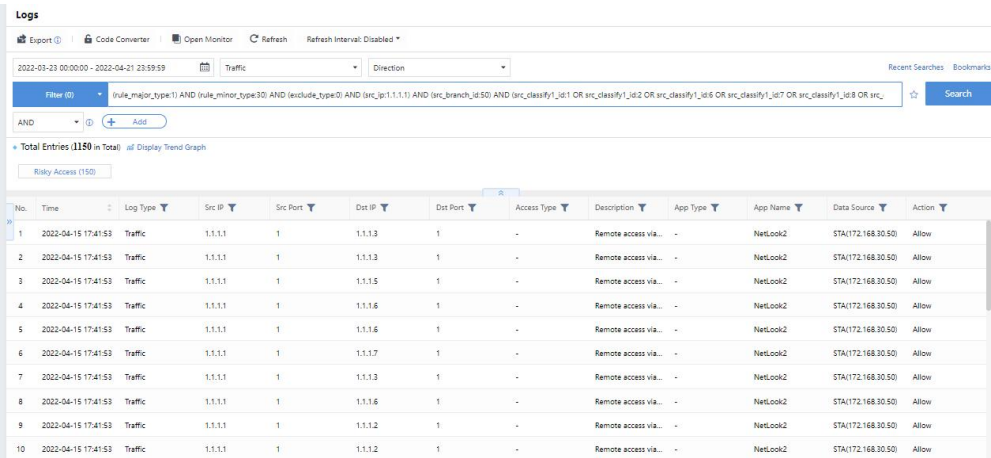
IP address, Asset Group

No.	Dst IP	Dst Type	Asset Group	Sources	Top 3 Risky Access Types	Logs
1	Customer A (1.1.1.1)	Server	Customer A	6	Remote Desktop Spy(126), ~(126), LoginAny(126)	1008
2	Customer A (1.1.1.3)	Host	Customer A	2	Remote Desktop Spy(63), ~(63), LoginAny(63)	490
3	Customer A (1.1.1.4)	Host	Customer A	2	Remote Desktop Spy(63), ~(63), LoginAny(63)	490
4	Customer A (1.1.1.5)	Host	Customer A	2	Remote Desktop Spy(63), ~(63), LoginAny(63)	490
5	Customer A (1.1.1.6)	Host	Customer A	2	Remote Desktop Spy(63), ~(63), LoginAny(63)	490
6	Customer A (1.1.1.7)	Host	Customer A	2	Remote Desktop Spy(63), ~(63), LoginAny(63)	490
7	Customer A (1.1.1.2)	Host	Customer A	1	Remote Desktop Spy(35), ~(35), LoginAny(35)	308

Administrators can click the specific IP/number of sources to jump to the **GoldenEye Details** page to further display detailed information, as shown in the following figure.



The administrator can click the specific **Top 3 Risky Access Types** and jump to the **Detection > Logs** to automatically filter the corresponding logs, as shown in the following figure.



3.7.7 Outbound Server Access

Overall Display

Under the **Detection > Abnormalities > Outbound Server Access** page, administrators can visually view the external connection from the server's perspective and pay timely attention to the access connections of businesses that do

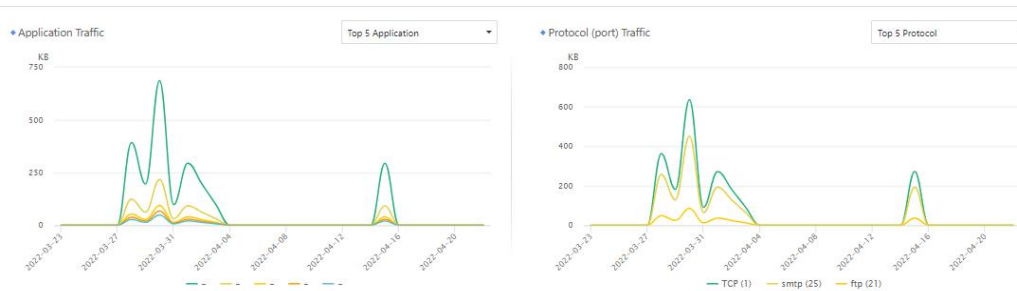
not need access to foreign countries. At the same time, the administrator can specify the server, region, and period. The overall display information mainly includes:

- **Application Traffic:** By default, the trend displays the top 5 application traffic of the server. The administrator can switch to the application traffic in the upper right corner of the corresponding page.
- **Protocol (port) Traffic:** The trend displays the server's top 5 protocol port traffic by default. Administrators can switch to the protocol traffic in the upper right corner of the corresponding page.



Specify the server scope to include all servers, core servers, upstream traffic greater than downstream, and overnight connections (can be customized by clicking the settings button on the right) categories for further filtering by the administrator.

The TOP 5 application and protocol trends are shown in the figure below.



Detailed Analysis

Administrators can view specific server connection details from a **Regions** or **Servers** perspective.

Regions

From a regional perspective, it mainly includes **Region, Src IPs, Bidirectional Bytes, Outbound/Inbound Bytes, Top 10 Apps, Top 10 Protocols (port), and Last Access**. Administrators can search for keywords through the search bar or click **Export** upper left corner to export.

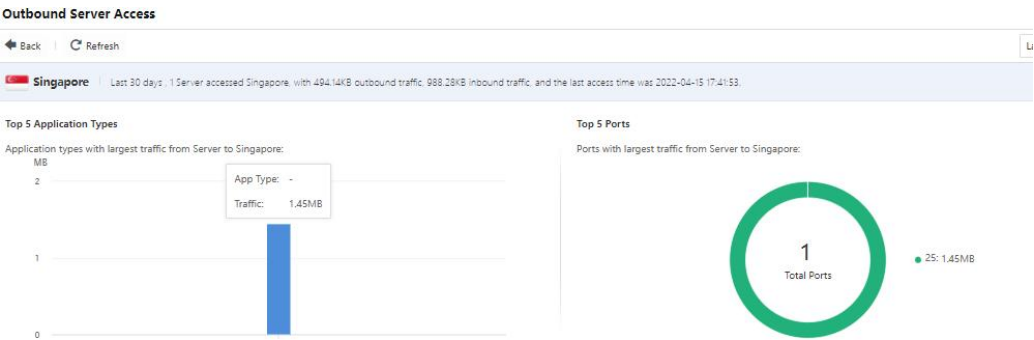
RegionsServers

Export

Search

No.	Region	Src IPs	Bidirectional Bytes	Outbound/Inbound Bytes	Top 10 Apps	Top 10 Protocols (port)	Last Access
1	Singapore	2	1.45MB	494.14KB(33.33%) 988.28KB(66.67%)	- (808.59KB), Google Picasa (673.83KB)	smtp (25, 1.45MB)	2022-04-15 17:41:53
2	Peru	2	323.44KB	107.81KB(33.33%) 215.62KB(66.67%)	- (107.81KB), Uber (94.34KB), - (53.91KB), - (40.43KB), - (26.95KB)	TCP (1, 323.44KB)	2022-04-15 17:41:53
3	Australia	2	283.01KB	94.34KB(33.33%) 188.67KB(66.67%)	- (141.50KB), - (121.29KB), - (20.21KB)	ftp (21, 283.01KB)	2022-04-15 17:41:53
4	Denmark	2	256.05KB	85.35KB(33.33%) 170.70KB(66.67%)	Uber (107.81KB), - (67.38KB), Agoda (53.91KB), - (26.95KB)	TCP (1, 256.05KB)	2022-04-15 17:41:53
5	Ireland	2	242.58KB	80.86KB(33.33%) 161.72KB(66.67%)	- (94.34KB), - (67.38KB), WebSocket (67.38KB), - (13.48KB)	TCP (1, 242.58KB)	2022-04-15 17:41:53
6	United States	2	229.10KB	76.37KB(33.33%) 152.73KB(66.67%)	SOAP (80.86KB), - (80.86KB), - (26.95KB), OCSP (26.95KB), - (13.48KB)	TCP (1, 229.10KB)	2022-04-15 17:41:53
7	China	2	215.62KB	71.88KB(33.33%) 143.75KB(66.67%)	Atom (107.81KB), - (53.91KB), WebSocket (53.91KB)	TCP (1, 215.62KB)	2022-04-15 17:41:53
8	Argentina	2	202.15KB	67.38KB(33.33%) 134.77KB(66.67%)	- (94.34KB), SOAP (67.38KB), - (26.95KB), Google News (13.48KB)	TCP (1, 202.15KB)	2022-04-15 17:41:53

When you click a specific **Region**, **Top 10 Apps**, or **Top 10 Protocols (port)**, it will jump to the page corresponding to the region to display information such as **Top 5 applications Types**, **Top 5 Ports**, and **Outbound AccessServerList**, as shown in the following figure.



Server

From the server's perspective, it mainly includes information such as **Server**, **Top 5 Dst Regions**, **Bidirectional Bytes**, **Outbound/Inbound Bytes**, **Top 10 Apps**, **Top 10 Protocols (port)**, and **Last Access**. Administrators can search for keywords through the search bar. You may also click the **Export** in the upper left corner for batch export operations, as shown in the figure below.

RegionsServers

Export

Search

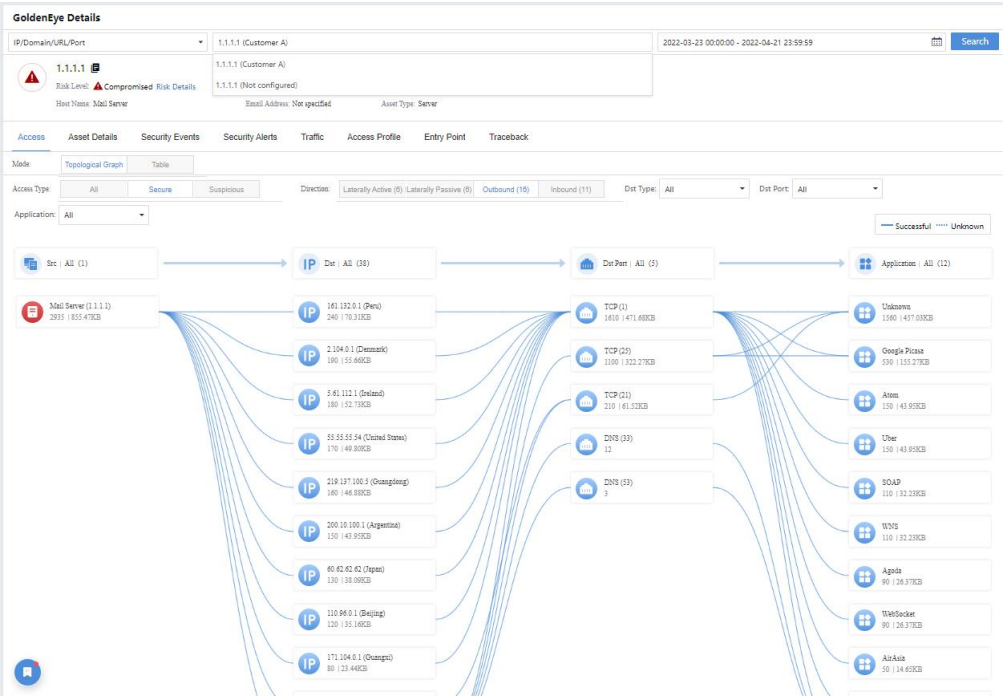
No.	Server	Top 5 Dst Regions	Bidirectional Bytes	Outbound/Inbound Bytes	Top 10 Apps	Top 10 Protocols (port)	Last Access
1	Customer A (1.1...)	Singapore(3960), Peru(864), Australia(756), Denmark(684), Ireland(648)	2.95MB	1005.47KB(33.33%) 1.96MB(66.67%)	- (748.83KB), Google Picasa (558.98KB), - (174.02KB), - (158.20KB), Atom (158.20KB), Uber (158.20KB), - (126.56KB), WNS (116.02KB), SOAP (116.02KB), - (110.74KB)	TCP (1, 1.60MB), smtp (25, 1.13MB), ftp (21, 221.48KB)	2022-04-03 03:00:32
2	Mail Server (1.1...)	Singapore(1100), Peru(240), Australia(210), Denmark(190), Ireland(180)	897.89KB	279.30KB(33.33%) 558.59KB(66.67%)	- (208.01KB), Google Picasa (155.27KB), - (48.34KB), - (43.95KB), Atom (43.95KB), Uber (43.95KB), - (35.16KB), WNS (32.23KB), SOAP (32.23KB), - (30.76KB)	TCP (1, 454.10KB), smtp (25, 322.27KB), ftp (21, 61.52KB)	2022-04-15 17:41:53

2 entries

1

Per Page 10

When you click the specific **Server**, **Top 10 Apps**, or **Top 10 Protocols (port)**, you will be redirected to the **GoldenEye Details** page for further details.



3.7.8 Telemetry Hub



Telemetry Hub will take effect relying on the valid license as well as larger than 96GB size memory to Cyber Command.



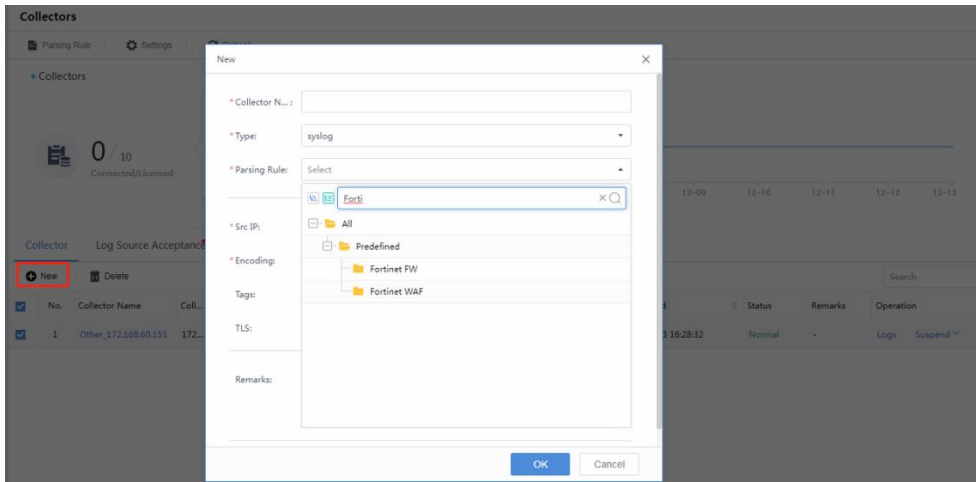
In addition, if the current Cyber Command 3.0.81 version is upgraded from a lower version and oriented to Telemetry Hub, you have to update the license as well.

Telemetry Hub mainly focuses on collecting third-party vendor's logs to Cyber Command to centralized management and certain types of logs even can be further analyzed and aggregated into security alerts in Cyber Command.

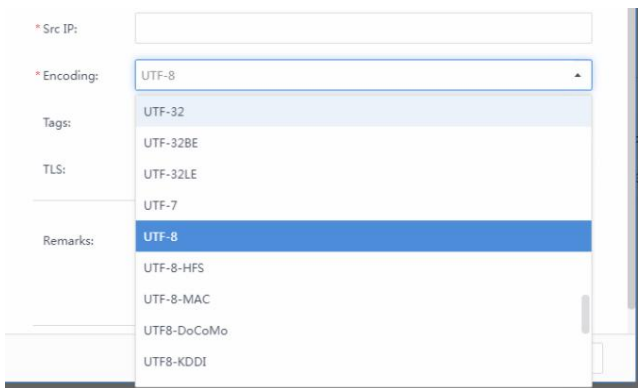
Collectors

Telemetry Hub feature supports current prevail data sending methods, including **Database, FTP, Kafka, SNMP, SNMP Trap, Syslog, webservice, winlogbeat**, and **WMI**. You can select the corresponding method, and among these methods, **syslog** type is the most frequently used.

1. Go to **Detection > Telemetry Hub > Collector** page, and click **New** to add a new data source. When the type is syslog, you need to pull down **Parsing Rules** and search for what exactly you need. Since there are a large number of rules which has been imported in Cyber Command, you can search for a precise rule by matching keywords. In this example, search for "Fortinet's FW", as shown in the following figure.



- **Src IP:** Fill in the source vendor IP;
- **Encoding:** Confirm with third-party vendor encoding types.



- **TLS:** Usually there is no need for TLS, while it depends on customer's requirement, if it transmits with TLS, need to be generated and installed on the collector.

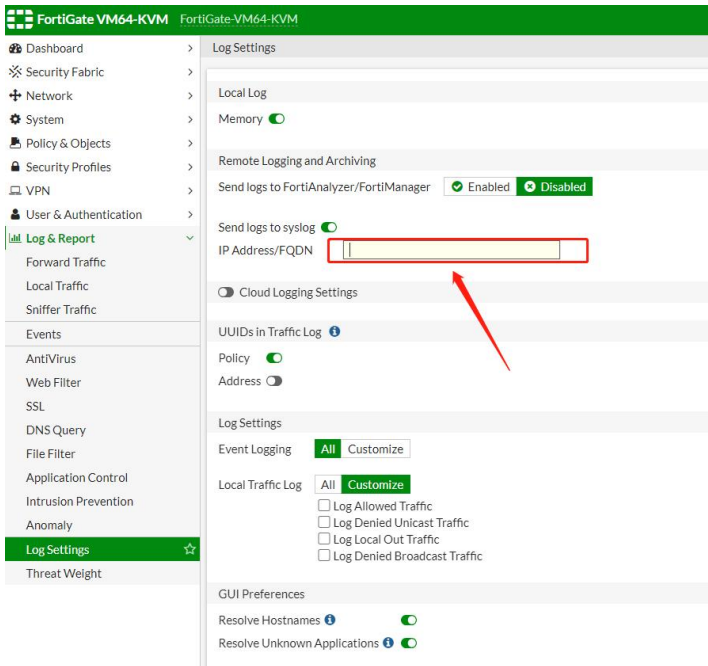
Tags:

TLS: ☒ Enable

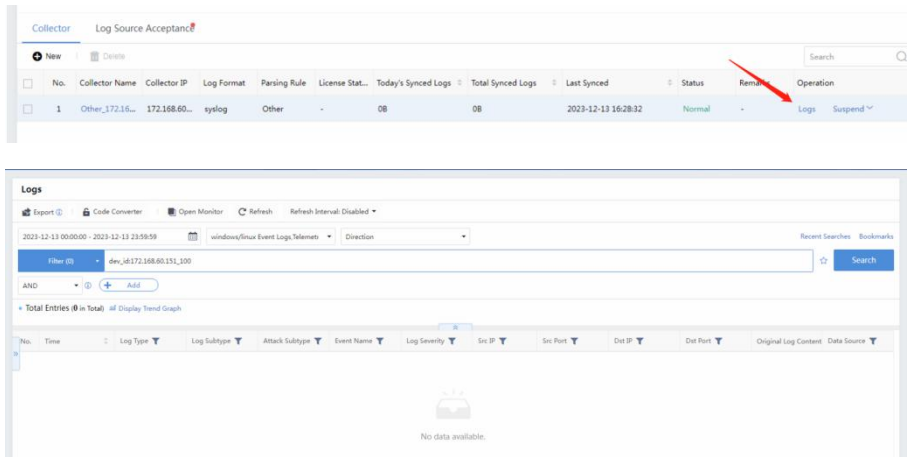
Client Certificate (installed on the collector): [Download Certificate](#)

Remarks:

2. Configure syslog sending in third-party vendor side, for example below is Fortigate.

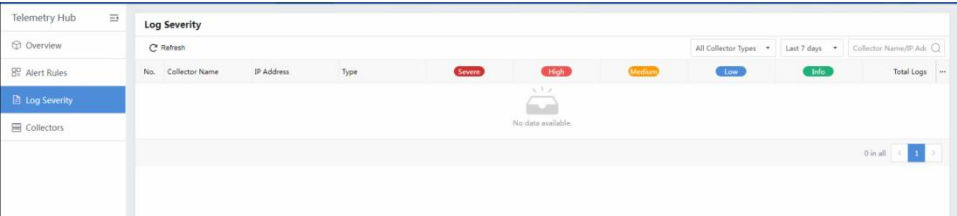


3. When the data source is configured correctly, you can select a specific collector and search the logs it sends, which will be redirected to the **Logs** page.



Log Severity

Specific logs that are received and parsed correctly are displayed on the **Log Severity** page. Logs with different severity levels are displayed.

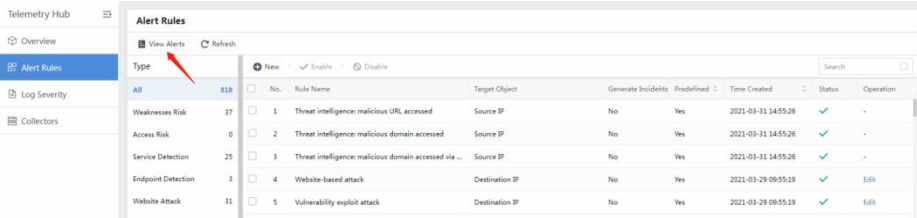


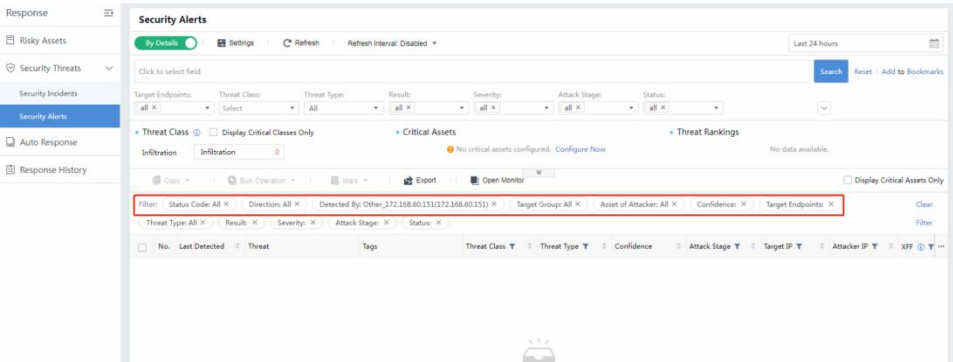
Alert Rule

An alert rule is mainly oriented to correlate third-party logs into security alerts. In the **Alert Rule** module, there are many built-in alert rules already as follows.

Alert Rules									
View Alerts Refresh									
Type	No.	Rule Name	Target Object	Generate Incidents	Predefined	Time Created	Status	Operation	
All	319								
Weaknesses Risk	37	1 Threat intelligence: malicious URL accessed	Source IP	No	Yes	2021-03-31 14:55:26	✓	-	
Access Risk	0	2 Threat intelligence: malicious domain accessed	Source IP	No	Yes	2021-03-31 14:55:26	✓	-	
Service Detection	25	3 Threat intelligence: malicious domain accessed via ...	Source IP	No	Yes	2021-03-31 14:55:26	✓	-	
Endpoint Detection	3	4 Website-based attack	Destination IP	No	Yes	2021-03-29 09:55:19	✓	Edit	
Website Attack	31	5 Vulnerability exploit attack	Destination IP	No	Yes	2021-03-29 09:55:19	✓	Edit	
Backdoor Communication	17	6 Brute-force attack on the SSL VPN administrator ac...	Destination IP	No	Yes	2021-03-29 09:55:19	✓	Edit	
Account Attack	35	7 Communication via chopper	Destination IP	Yes	Yes	2021-03-29 09:55:19	✓	Edit	
Attack and Exploit	2	8 Brute-force attack	Destination IP	No	Yes	2021-03-29 09:55:19	✓	Edit	
Email Attack	4	9 SSL VPN user account locked	Destination IP	No	Yes	2021-03-29 09:55:19	✓	-	
DoS attack	7	10 SSL VPN administrator account logged in during u...	Destination IP	No	Yes	2021-03-29 09:55:19	✓	Edit	
Backlink	0	11 Brute-force attack on common SSL VPN user accou...	Destination IP	No	Yes	2021-03-29 09:55:19	✓	Edit	
Vulnerability and Exploit	23	12 Attack exploiting DedeCMS vulnerabilities	Destination IP	No	Yes	2021-03-29 09:55:19	✓	Edit	
Hacking Tools	18	13 Attack exploiting Struts 2 vulnerabilities	Destination IP	No	Yes	2021-03-29 09:55:19	✓	-	
Database Attack Exploit	0	14 phpStudy backdoor code injection attack	Destination IP	No	Yes	2021-03-29 09:55:19	✓	Edit	
Malicious File Access	6	15 Attack exploiting Joomla vulnerabilities	Destination IP	No	Yes	2021-03-29 09:55:19	✓	Edit	
Malicious File Infection	18	16 Attack exploiting ECShop vulnerabilities	Destination IP	No	Yes	2021-03-29 09:55:19	✓	Edit	
Abnormal Endpoint	77								
319 Entries									

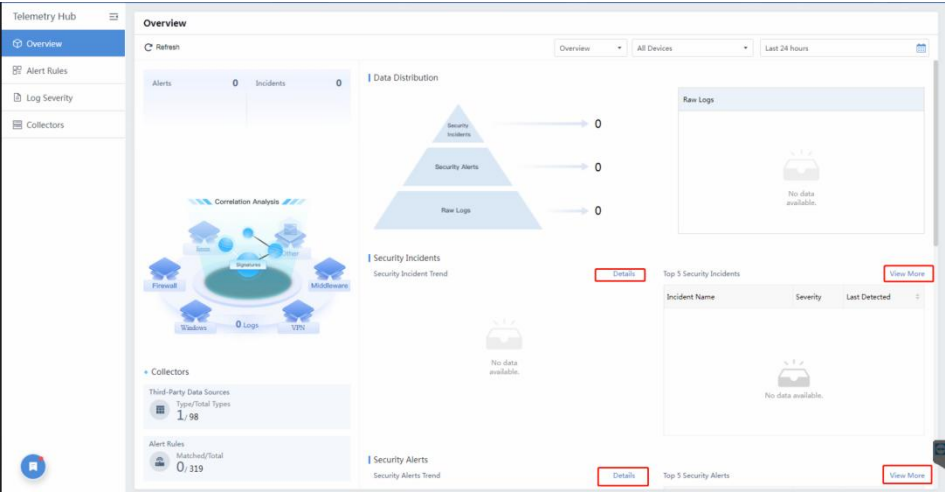
Click **View Alerts**, and the **Security Alerts** page appears





Overview

The **Overview** page can provide general dashboard about Telemetry Hub module, you can click **Details** or **View More** for further data.



3.8 Assets

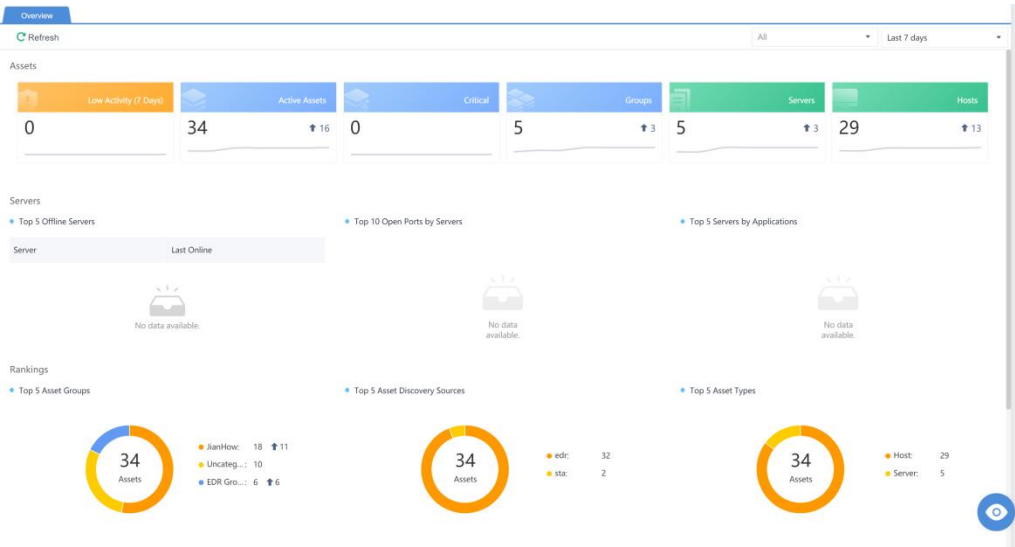
The asset center includes **Assets** and **Weaknesses**. In **Assets**, you can discover and define LAN's endpoint, server, and asset group. You can find vulnerabilities, weak passwords, unencrypted web traffic, and improper configuration of assets in **Weakness**.

3.8.1 Assets

In **Assets**, you can discover and define LAN's endpoint, server, and business system. Branches also can be configured in a multi-branch scenario.

Overview

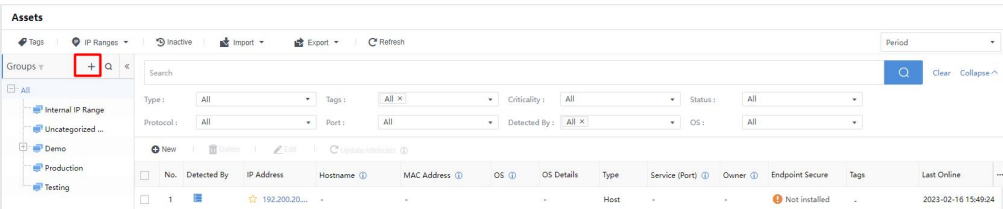
A panel to display all assets, as shown below:



Assets

The Business Systems/Server displays automatically identified servers or manually added servers or asset groups. A server can be automatically discovered, whereas **Asset Group** shall be manually added.

Click the plus (+) icon to add an asset group manually.



Add Asset Group

Basics

* Group Name:

Required

Parent Group:

Select

Tags:

Select

Asset

Asset Discovery

Group by IP Range

Group by Device Src

Group by Source Device or IP Range

Type:

Auto-discovered

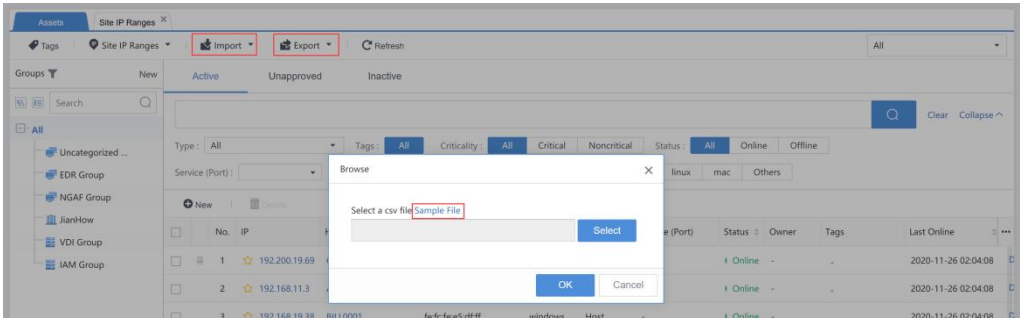
IP Range:

IP ranges or subnets
It can overlap with private IP ranges. The specified subnet is prioritized.

OK

Cancel

- **Group Name:** Add a group name information of the asset.
- **Parent Group:** Select a Parent Group.
- **Tags:** Tags are divided into **Business System**, **Branch**, **Security Domains**, **IP Groups**, and **Headquarter**.
- **Type:** Refer to the type of asset. It is mainly divided into **Auto-discovered**, **Server**, and **Host**.
- **IP Range:** It can overlap with private IP ranges. The specified subnet is prioritized.



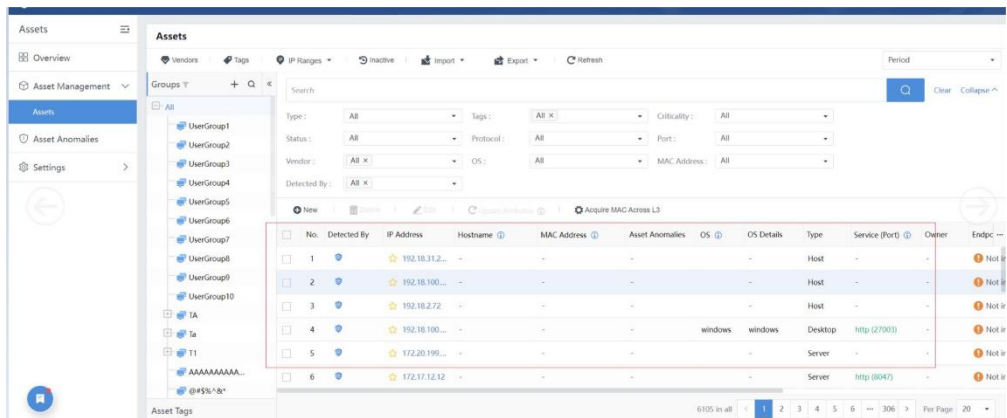
You can manually **Import** and **Export** the asset information.

IOMT Asset Identification

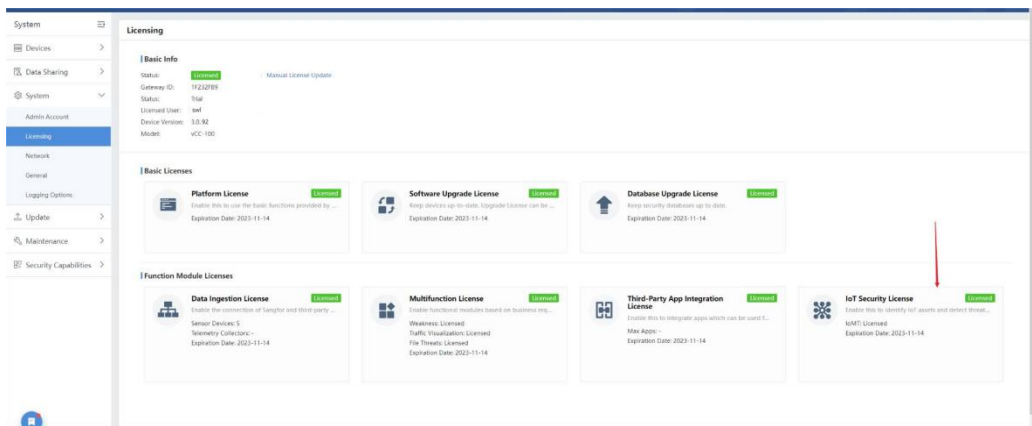
Cyber Command provides the Internet of Medical Things (IOMT) asset identification feature that can precisely identify IOMT assets. This facilitates tracing, management, and maintenance of IOMT assets.

The following content describes how to use this feature.

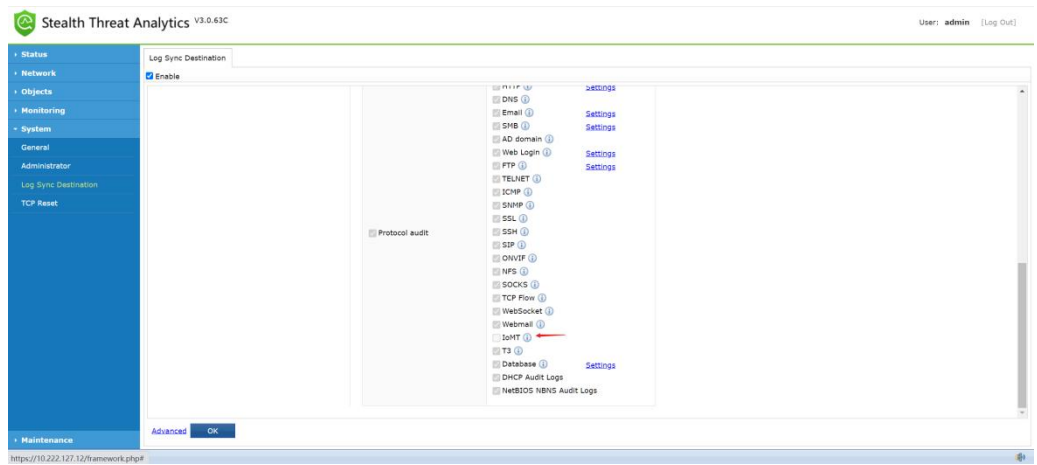
- 1. If the IOMT asset identification feature is disabled, IOMT assets cannot be identified and are marked as hosts and servers, as shown in the following figure.



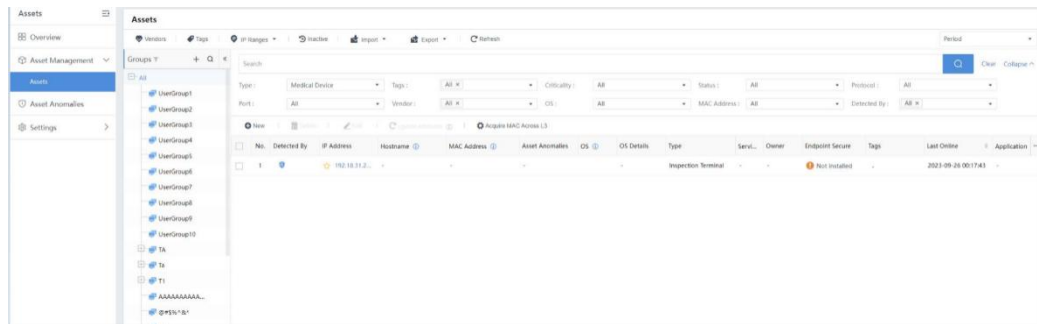
- 2. Enable IoT Security License. To do this, log in to the Cyber Command console, move the pointer over the user avatar, and select **System**. Then, go to **System > System > Licensing**, and make sure that **IoT Security License** is in the **Licensed** state, as shown in the following figure.



- 3. Enable **IoMT** in the Stealth Threat Analytics (STA) console of v3.0.63 or later. To do this, log in to the STA console, go to **System > Log Sync Destination**, and select **IoMT**, as shown in the following figure.



4. In the Cyber Command console, go to **Assets > Assets > Asset Management > Assets** to view that the IoT asset can be precisely identified. In this example, the IoT asset is precisely identified as **Inspection Terminal** in the **Type** column, as shown in the following figure.

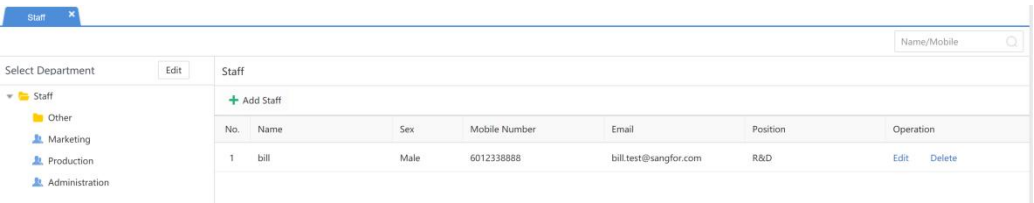


Usage Notes

- Make sure that **IoT** is enabled on the **Log Sync Destination** page in the STA console of v3.0.63 or later.
- Make sure that **IoT Security License** is in the **Licensed** state in the Cyber Command console.

Staff

Go to **Assets > Assets > Settings > Owners**, and you can view the staff information such as **Name, Gender, Mobile Number, Email, and Job Title**.



Advanced

The following are the basic settings of some Assets, as shown below:

The screenshot shows the 'Advanced' settings panel for Assets. On the left is a sidebar with navigation options: Assets, Overview, Assets, Settings, Owners, and Advanced (highlighted). The main panel is titled 'Advanced' and contains several sections:

- Endpoint Discovery and Approval:** Includes a toggle for 'Auto Discover Assets' (checked).
- Excluded Gateway MAC Address:** A field showing 'Not Configured' with an edit icon.
- Offline Endpoints:** Includes a 'Detection' section with radio buttons for 'Enable' and 'Disable' (selected). Below it is an 'Update Time' section with radio buttons for 'Every early morning' (selected) and 'Update Now'.
- Inactive Endpoints:** Includes an 'Asset Inactive' section with a field 'After' set to '30' and a label 'Consecutive Days Offline'. Below it is a 'Custom Trigger' field set to 'Not Configured' with an edit icon.
- Default Asset Name:** Includes a 'Server Asset Name' field set to 'Hostname>Owner>Asset Group' and a 'Host Asset Name' field set to 'Username>Owner>Asset Group>Hostname', both with edit icons.
- Other:** Includes a 'Panel Name' field set to 'Asset Group' with an information icon.

At the bottom of the panel is an 'OK' button.

- **Asset Discovery and Approval:** Cyber Command can auto-discover assets. If you tick **Auto Discover Assets**, adding asset information requires administrator approval.
- **Excluded Gateway MAC Address:** Exclude the useless MAC address to avoid interruption.
- **Offline Endpoints:** Assets without traffic for a certain period will be automatically offline.
- **Update Time:** Cyber Command will update asset information at a specific time. If you choose **Update Now** may cause performance issues. Updating **Every early morning** is recommended.
- **Inactive Endpoints:** Assets will become inactive after being offline for a certain period.
- **Default Asset Name:** When an asset name is added to the platform, if no asset name is configured, the default asset name will be displayed based on the priority in **Server Asset Name** and **Host Asset Name**.

Third-Party Data Sources

Third-Party Data Sources support to sync the Domain user and display the domain username inside the Security Incident and Security Alert.

Go to **Assets > Assets > Settings > Third-Party Data Sources** and click the **Add Device** in the upper-right corner to add the domain controller.

Third-Party Data Sources

Enable

Disable

Sync Now

Refresh

IP Address

Q

Active Directory

Enabled

Devices: 1

Assets: 13/17 (Online/All)

Add Device

IP Address	Protocol	Status	Remarks	Operation
192.168.20.89	WMI	Enabled	-	Delete Disable Test Connectivity

1 in all1Per Page10

Add Domain Controller

X

* IP Address:

* Protocol:

WMI

* Domain Account:

* Password:

* Event ID:

4624

i

Test Connectivity

Remarks:

Save and Add

OK

Cancel

- **IP address:** IP address of the AD domain
- **Protocol:** WMI is the default protocol.
- **Domain Account:** Administrator of AD domain account.
- **Password:** Password of AD domain account.
- **Event ID:** Separate multiple event IDs with a comma. Event ID 4624 is specified by default.

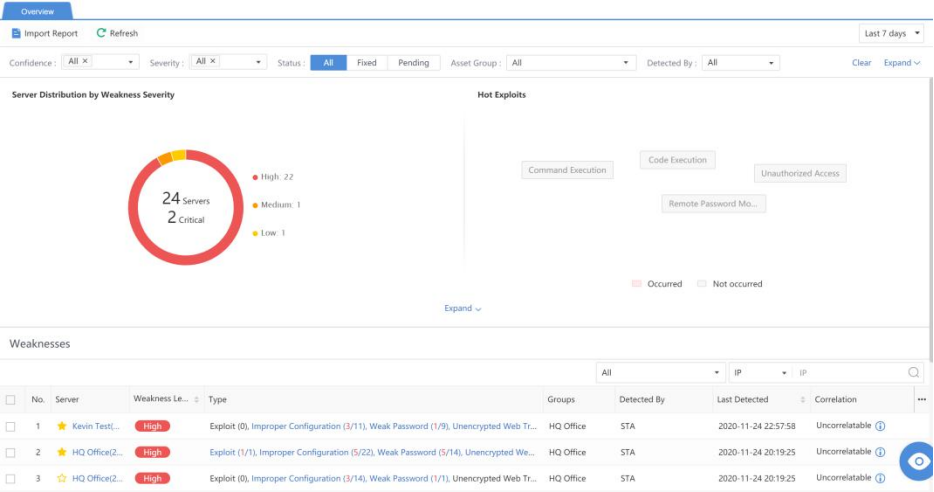
- **Remark:** Remark of the AD Domain.

3.8.2 Weaknesses

The server weakness refers to the server vulnerability in the server. Since all threats could cause harm to the server by attacking certain vulnerabilities of the server, the identification and processing of server weaknesses are essential to prevent the threats effectively.

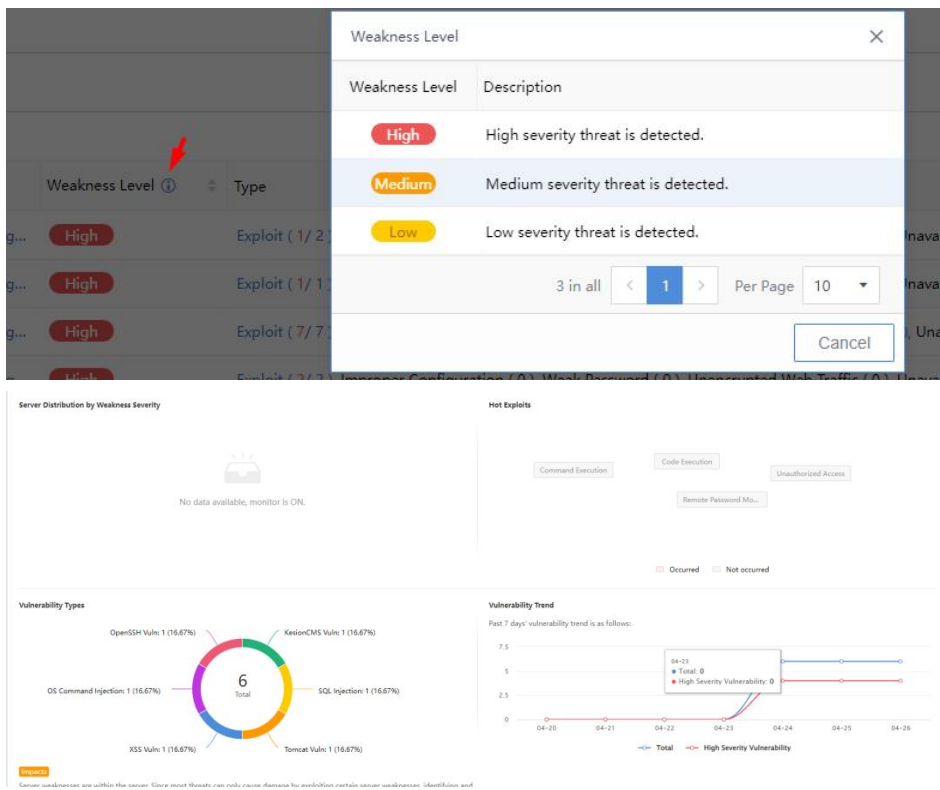
Overview

You can filter the time by **Last 30 days**, **Last 7 days**, or **Last 24 hours**.



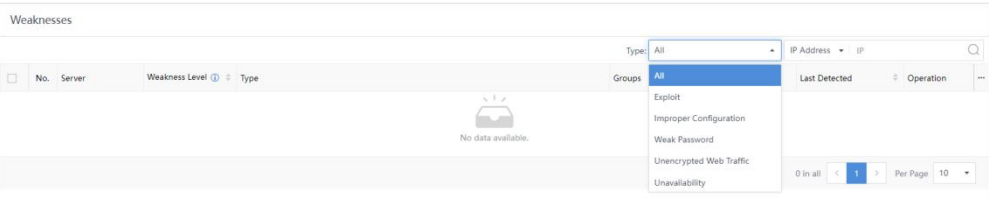
- **Weakness Level:** Display the weakness level as **High**, **Medium**, and **Low**.

Click  to view the definition and description, as shown below:



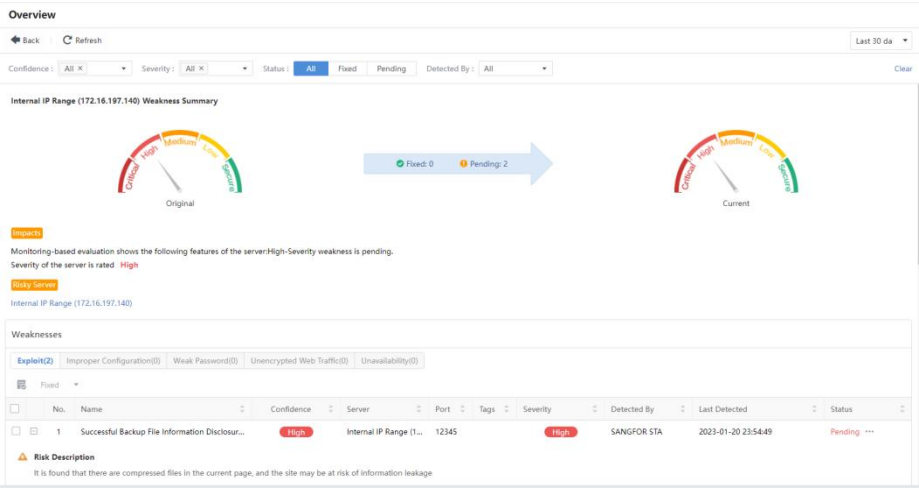
- **Hot Exploits:** Refer to common vulnerabilities in which the vulnerabilities in red exist in the network.
- **Vulnerability Types:** Count and display the types and quantity of discovered vulnerability types.
- **Vulnerability Trend:** Display the trend of the total number of discovered vulnerabilities and the number of high-severity vulnerabilities in a timeline.

Select the type of weaknesses from the **Type** drop-down list, including **Exploit**, **Improper Configuration**, **Weak Password**, **Unencrypted Web Traffic**, and **Unavailability**.



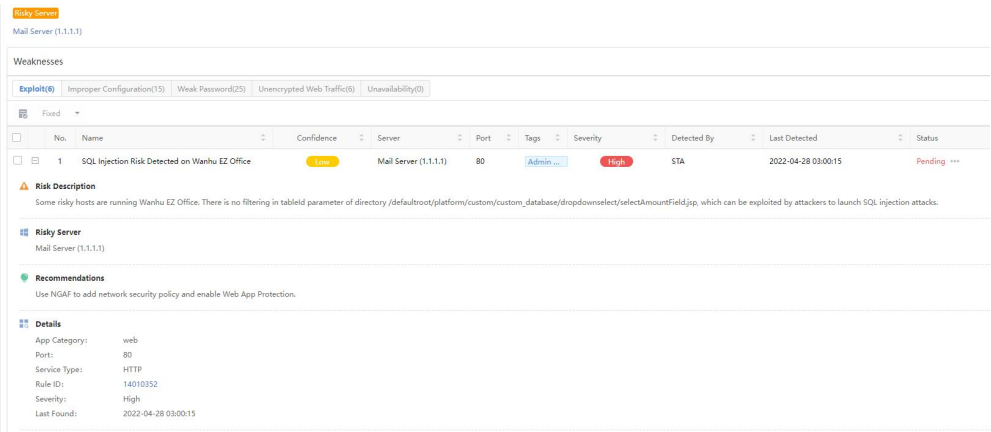
- **Last Detected:** Refer to the time the weakness in the business system was last detected.

Click the **Server** to view the weakness details situations of this IP address in the last 30 days, last 7 days, or last 24 hours.



Describe the severity of vulnerability in the host, and provide security recommendations and descriptions.

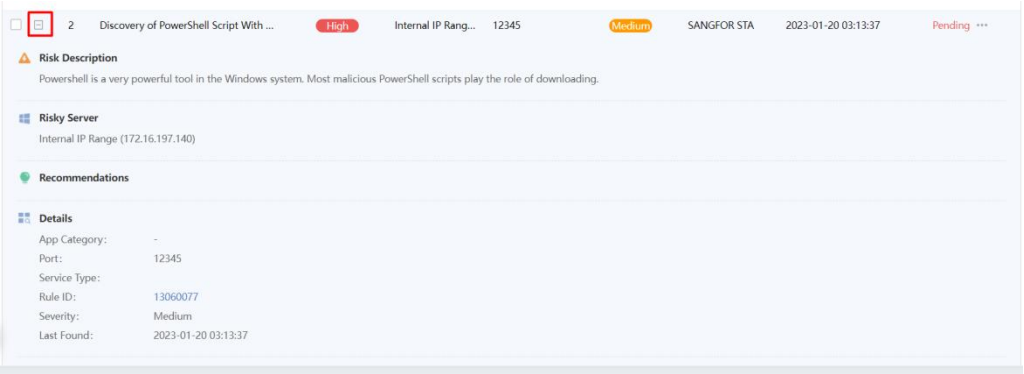
The weakness details are divided into five types: **Exploit, Improper Configuration, Weak Password, Unencrypted Web Traffic,** and **Unavailability.**



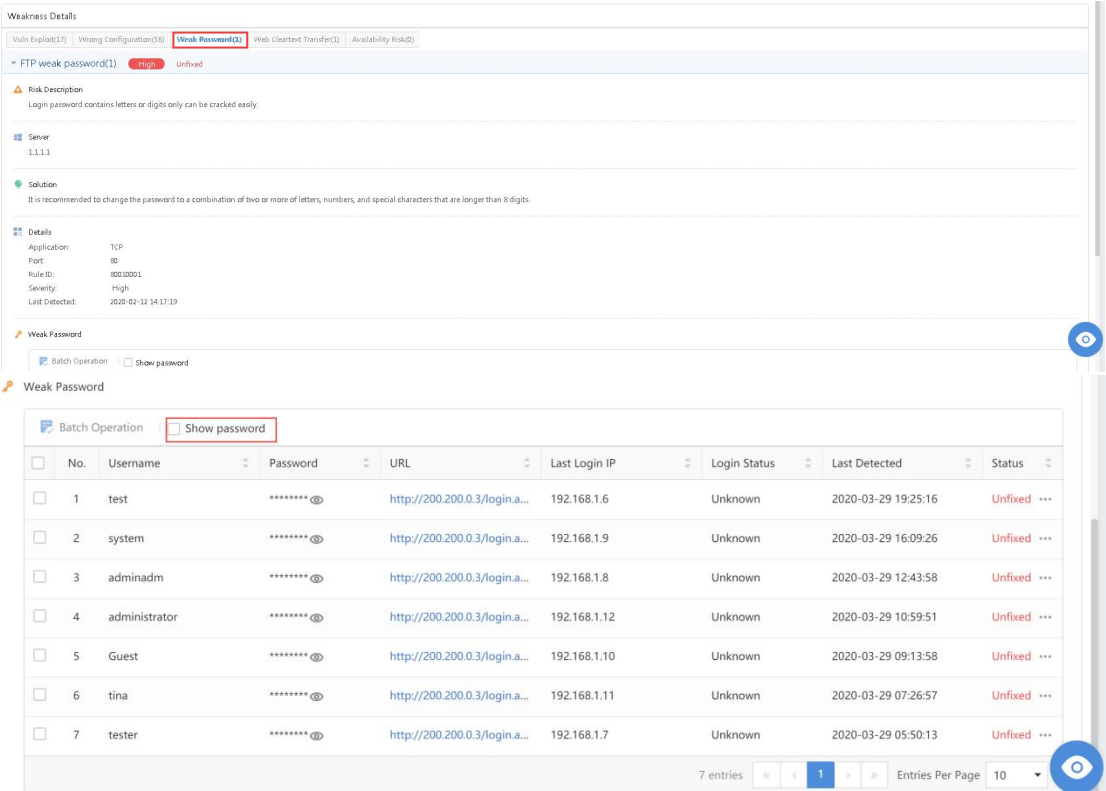
- **Name:** Refer to the name and CVE information of the vulnerability.
- **Server:** Refer to the IP address information of the server.
- **Port:** Refer to the port with the vulnerability.
- **Tags:** Refer to tag information of the vulnerability.
- **Severity:** Refer to the severity of the vulnerability.
- **Last Detected:** Refer to the time when this vulnerability was discovered.
- **Status:** Refer to whether the vulnerability is fixed, and this status shall be manually marked.

Click the plus (+) icon on the left side of the vulnerability to unfold the detailed description of this vulnerability, including **Risk Description, Risky Server, Recommendations, Details,** and **Vulnerability Proof.**

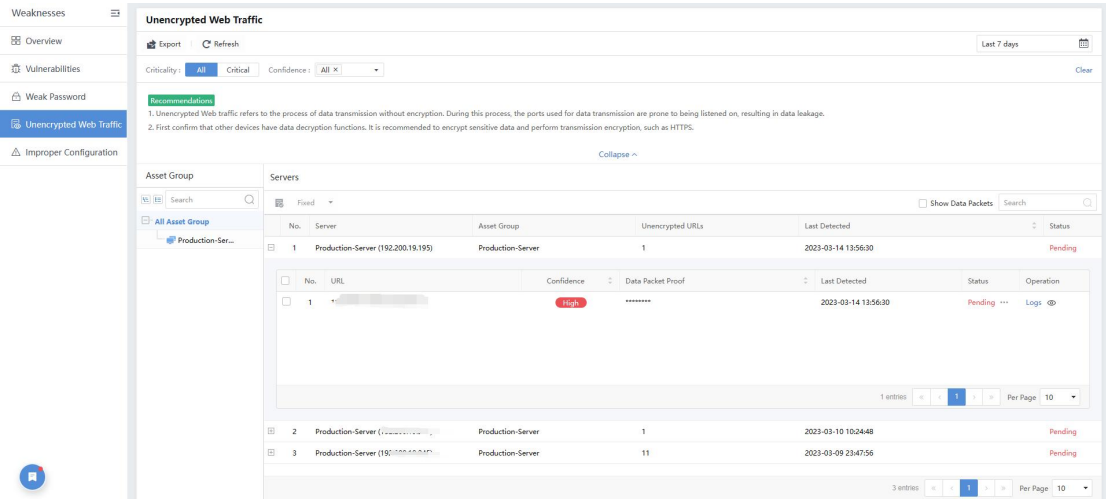
Click the plus (+) icon on the left side of the vulnerability to unfold the detailed description of this vulnerability, including **Risk Description**, **Server**, **Solution**, **Details**, and **Vulnerability Proof**.



Click **Weak Password** to view **Risk Description**, **Server**, **Solution**, **Details**, and **Weak Password Account**.

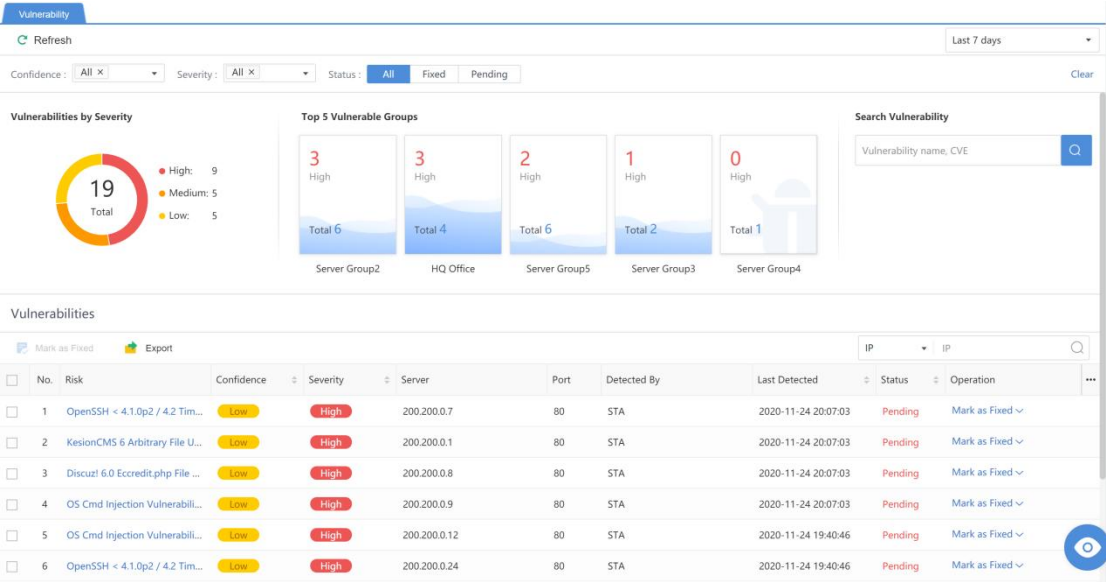


Click **Web Unencrypted web traffic** to view **URL**, **Confidence**, **Data Packet proof**, **last detected**, **status** and **operation**.



Vulnerabilities

Administrators can view **vulnerabilities by Severity**, **TOP5 Vulnerable Groups**, and vulnerability detection list from the vulnerability perspective. At the same time, you can search the vulnerability by **Vulnerability name** or **CVE** through the search bar. The administrator can specify the time range (**Last 24 hours**, **Last 7 days**, **Last 30 days**, or **Custom**). At the same time, further filter by keywords such as **Confidence**, **Severity**, **Status**, etc., as shown below.



- **Vulnerabilities by Severity:** statistically display the distribution of High, Medium, and Low-risk vulnerabilities found.
- **TOP5 Vulnerable Groups:** Show the TOP5 groups with the most vulnerabilities, and emphasize the number of high-risk vulnerabilities;
- **Search Vulnerability:** The administrator can enter the vulnerability

name/CVE to query the vulnerability detection results;

- **Vulnerabilities:** You can filter by IP, Name, or CVE ID. The administrator can click the specific risk name to view the vulnerability details. At the same time, the vulnerability can be marked in the **Operation** column, as shown in the figure below.

Weak Password

A weak password refers to a low-strength password. For example, it is a simple combination of numerals, the same as the account, or in a short length. A weak password can be easily cracked and used by hackers. Therefore, legitimate accounts and passwords can be used for login control and have higher confidentiality.

Filter the weak password by selecting the period, **Criticality**, **Account Type**, and **Login Status**.

Weak Password

Weak Password RulesAuto-ScanExportRefresh

Weak Password: All

Account Type: AllAdmin

Login Status: AllSuccessful

Weak Password: All

Last 7 days

Recommendation

1. Weak passwords most often consist of few and simple characters or are the same as the corresponding username. Weak passwords can be easily cracked without the user's notice, resulting in unauthorized logins.

2. It is recommended to change weak passwords to ones longer than 8 characters, consisting of two or three of the following: letters, numbers, and special characters.

Asset Group

Servers

Fixed

No. Server Asset Group Weak Accounts Top 3 Weak Password Types Last Detected Status

1 Mail Server (1.1.1.1) Customer A 25 FTP(4)IMAP(4)WEB(4) 2022-04-28 03:00:36 Pending

No. Username Password Base64 Decoded Accounts Possible Password URL Type Login Status Last Login Status Operation

1 admin ***** Password***** http://10.100.12.13:808... WEB Successful 2022-04-28 03:00:36 Pending Proof

2 admin! ***** Password***** admin http://10.100.12.13:808... WEB Successful 2022-04-28 03:00:36 Pending Proof

3 test ***** Password***** admin http://10.100.12.13:808... WEB Successful 2022-04-28 03:00:36 Pending Proof

4 abcde ***** Password***** admin http://10.100.12.13:808... WEB Successful 2022-04-28 03:00:36 Pending Proof

Weakness Awareness

OverviewWeak PasswordWeb Cleartext TransferWrong Configuration

Weak Password

Weak Password OptionsExportRefresh

Weak Password: All

Account Type: AllAdmin

Login Status: AllSuccessful

Weak Password: All

Last 7 days

Suggestions

1. Weak password refer to low-strength passwords such as password with combination of numbers, password same as username, and password that is too short. It can be easily cracked and used by hackers for login, which is hard to be detected.

2. Change the password to a new one with more than 8 characters consisting of two or three of the following: letters, numbers, and special characters.

Business Systems: Key ones only

Business system name

Mark as FixedAdmin accountSuccessful loginsShow passwordAll typesAll branches

None(1)

No. Server Business System Branch Accounts with Weak Top 3 Weak Passwords Last Detected Status

1 200.200.0.1 Server Group1 4 IMAP weak pass... 2020-03-28 17:05:04 Unfixed

No. Username Password Possible L Possible F URL Type Tags Login Sta Last Login Status Operation

1 admin... ***** TELNE... Log in... 2020-03-28 ... Unfixed Logs

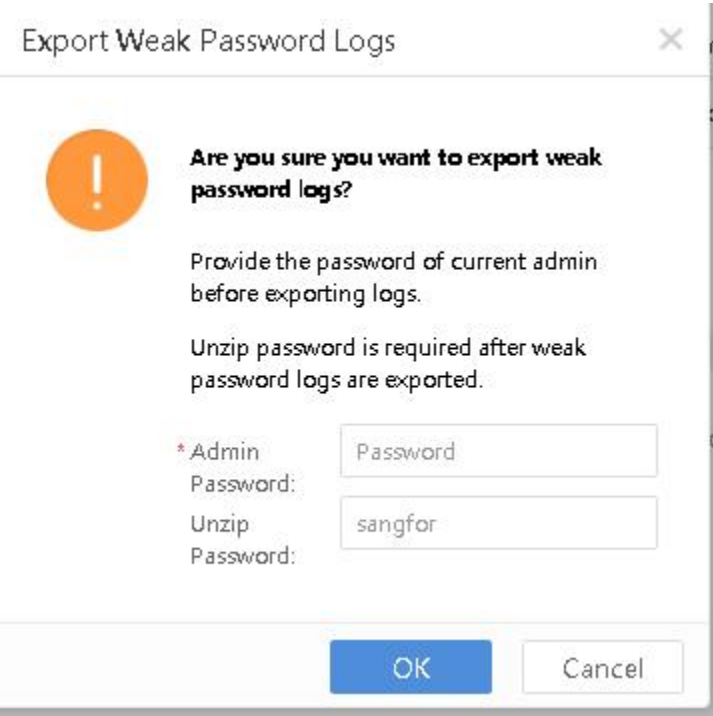
2 admin... ***** SMTP ... Log in... 2020-03-28 ... Unfixed Preview

3 admin... ***** FTP w... Log in... 2020-03-28 ... Unfixed Preview

4 admin... ***** IMAP ... Log in... 2020-03-28 ... Unfixed Preview

Click **Export** to export the weak password logs as a compressed package. Enter the

Admin account and password to proceed.

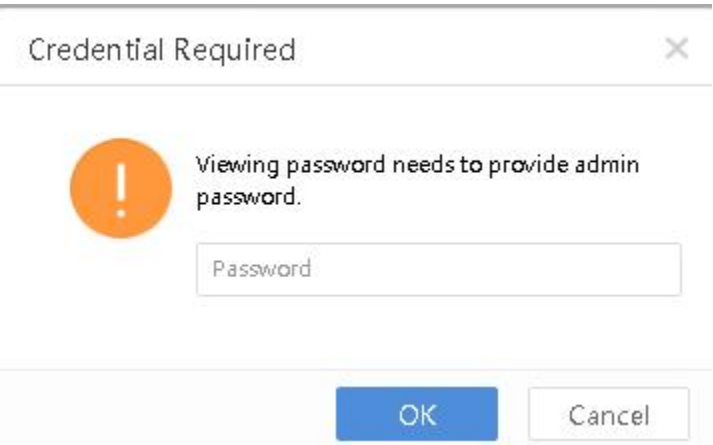


Export to obtain the compressed package with the unzipped password, i.e., sangfor.

Weak Password Logs															
Filter															
Period	2022-04-10 00:00:00 - 2022-04-20 22:59:59														
Asset Group	All Asset Groups														
No.	Username	Password	Result	Decoded	Account	Possible Passwords	URL	Data Product	Product	Device	Asset Group	Last Login IP	Type	Login Status	Last Detected
1	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
2	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
3	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
4	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
5	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
6	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
7	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
8	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
9	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
10	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
11	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
12	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
13	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
14	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
15	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
16	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
17	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
18	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
19	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
20	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
21	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
22	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
23	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
24	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
25	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
26	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
27	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00
28	admin	admin	Success		admin	admin	10.10.10.10	SSH	SSH	SSH	Customer A	10.10.10.10	SSH	Success	2022-04-10 00:00:00

To view a successfully logged-in account, check **Successful logins**.

To view the password on the platform, check **Show password**, and a dialog box shown in the following figure appears.



Enter the Admin password to view the account password.

Servers

Fixed

Show password

Search

No.	Server	Asset Group	Weak Accounts	Top 3 Weak Password Types	Last Detected	Status
1	Mail Server (1.1.1.1)	Customer A	25	FTP(4),IMAP(4),WEB(4)	2022-04-28 03:00:36	Pending

No.	Username	Password	Base64 Decoded	Accounts	Possible Passwords	URL	Type	Login Status	Last Login	Status	Operation
1	admin	*****	Password*****		*****	http://10.100.12.13.8081/ad...	WEB	Successful	2022-04-28 03:00:36	Pending	Proof
2	admin1	*****	Password*****	admin	*****	http://10.100.12.13.8081/ad...	WEB	Successful	2022-04-28 03:00:36	Pending	Proof
3	test	*****	Password*****	admin	*****	http://10.100.12.13.8081/ad...	WEB	Successful	2022-04-28 03:00:36	Pending	Proof
4	abcde	*****	Password*****	admin	*****	http://10.100.12.13.8081/ad...	WEB	Successful	2022-04-28 03:00:36	Pending	Proof

25 entries

123»

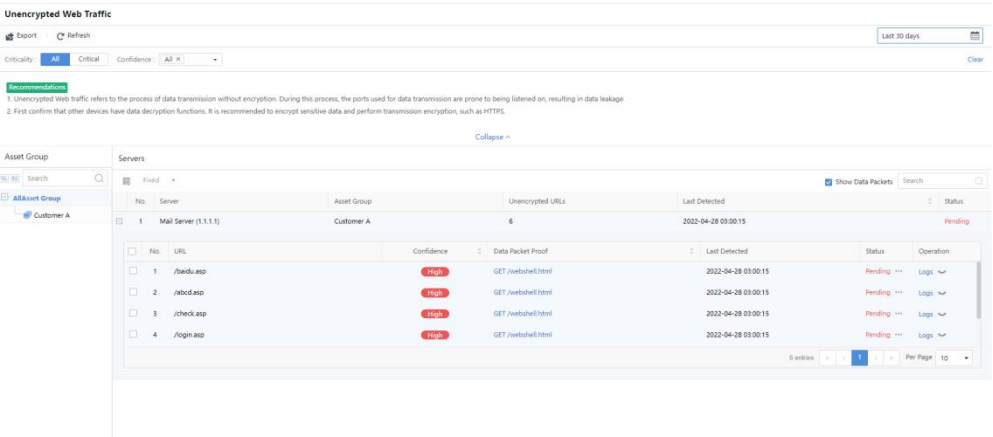
Per Page 10

- **Username:** Refer to accounts with a weak password.
- **Password:** Refer to the weak password of an account.
- **Base64 Decoded:** Refer to the password in Base64-decoded.
- **Accounts:** Refer to the password’s account.
- **Possible Passwords:** Refer to the possibility of the password.
- **URL:** Refer to the URL with a weak password if the platform is a web application.
- **Type:** Refer to types of weak passwords, including WEB, FTP, and LDAP.
- **Login Status:** Refer to whether the platform is successfully logged in, and the status includes Succeeded, Failed, and Unknown.
- **Last Login:** Refer to the last time logging in by using the account.
- **Status:** Refer to whether the weak password is fixed. If yes, manually mark the status as Fixed.
- **Operation:** Click **Proof** to view the proof.

Unencrypted Web Traffic

Unencrypted web traffic is a data transfer process without encryption. It is easy to get monitored to cause a data breach.

Filter the unencrypted web traffic by selecting the **period**, **Criticality**, or **Confidence**.



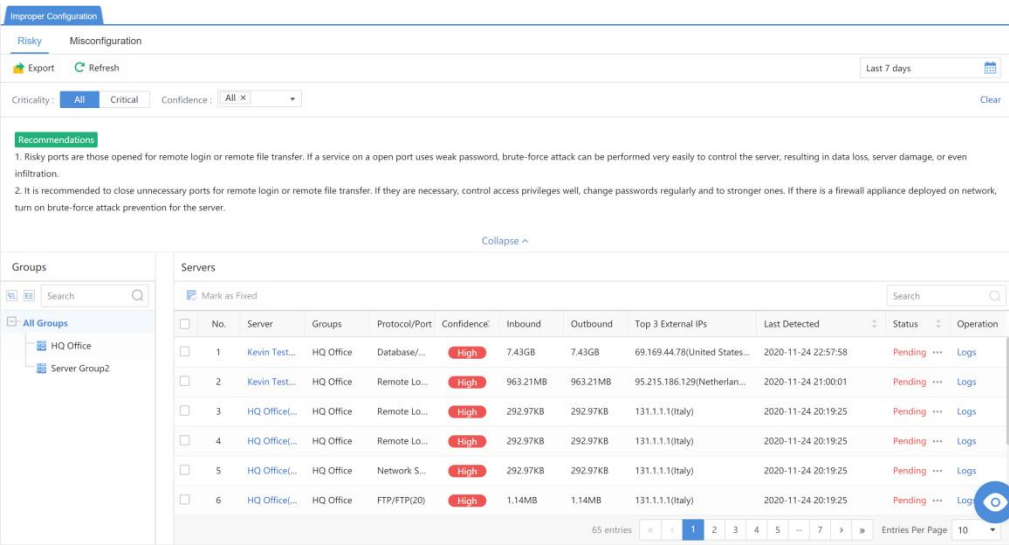
- **Server:** Refer to the IP address information of the server with unencrypted web traffic.
- **Groups:** Refer to the group to which the server belongs.
- **Unencrypted URLs:** Show the number of unencrypted URLs.
- **Last Detected:** Refer to the last occurrence time of unencrypted web traffic.
- **Status:** Refer to whether the weak password is fixed. If yes, manually mark the status as Fixed.
- **Operation:** Click View Log to redirect to **Detection > Logs**, and then the system automatically filters corresponding logs.

Click **Export** to export the information as a compressed package.

Cleartext Transfer Log							
Filter							
Time Range:	2018-09-11 2018-09-17						
Business System:	Unclassified Server						
Result							
No.	Domain Name/URL	Server	Branch	Business System	Data Packet Proof	Last Detected	Status
1	/cgi-bin/login.cgi	200.200.0.1	Headquarters	-	REQUEST: GET /cgi-bin/login.cgi?user_name=root&passwd=1 HTTP/1.1 Accept:	2018-09-17 23:58:11	Unfixed
2	/v1/login	200.200.0.1	Headquarters	-	REQUEST: GET /v1/login?user=administrator&passwd=1111 HTTP/1.1 Accept:	2018-09-17 23:29:33	Unfixed
3	/shop/verify	200.200.0.1	Headquarters	-	REQUEST: GET /shop/verify?user=2356&passwd=testabc HTTP/1.1 Accept: */*	2018-09-17 22:22:55	Unfixed
4	/index.htm	200.200.0.2	Headquarters	-	REQUEST: GET /index.htm?user=admin&passwd=1234567 HTTP/1.1 Accept: */*	2018-09-17 21:09:37	Unfixed
5	/index.htm	200.200.0.1	Headquarters	-	REQUEST: GET /index.htm?user=admin&passwd=1234567 HTTP/1.1 Accept: */*	2018-09-17 20:38:15	Unfixed

Improper Configuration

A risky port is when the service has opened to the Internet for remote login or remote file transfer. If a weak password exists for the service corresponding to the open port, it is easy for criminals to blast and log in to control the server directly, causing data loss or server damage. After the criminals control the server, they can penetrate other internal network hosts.



- **Server:** The IP address of the server is at risk of configuration.
- **Groups:** All groups of the server.
- **Protocol/Port:** The detected risky port.
- **Confidence:** The degree of confidence of the risky port.
- **Inbound:** The amount of detected inbound traffic.
- **Outbound:** The amount of detected outbound traffic.
- **Top 3 External IPs:** Internet IP accesses up to 3 risky port IPs.
- **Last Detected:** The last detected time.
- **Status:** Fixed, Fixing, Whitelist, or Suspend.
- **Operation:** Click **Logs** to view the log.

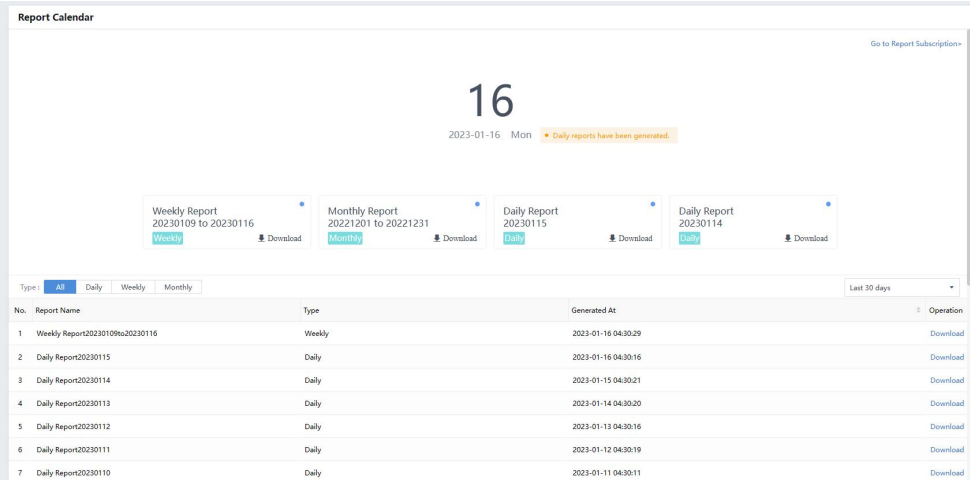
3.9 Reports

The reports are divided into **Security Risk Reports** and **Notification**. The security risk reports show LAN’s security situations, and notification sends risky hosts or Security Incidents to the administrator in time.

3.9.1 Security Risk Reports

Report Calendar

Report Calendar will generate reports based on a daily, weekly, and monthly basis. The weekly report will be generated every Monday for the last week, and the monthly report will be generated every first day of the month.



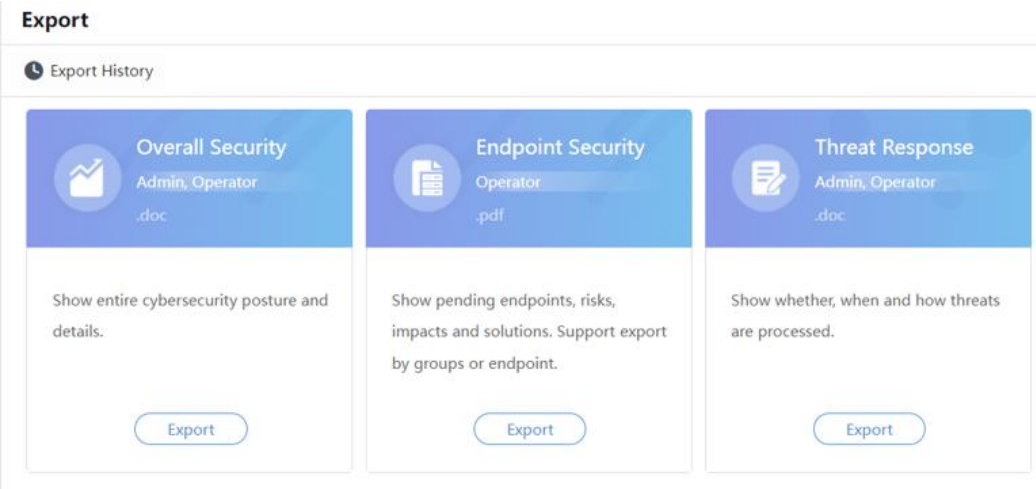
Subscription

You can subscribe to the daily, weekly, and monthly reports and send them to the recipient. Tick the **Enable Report Subscription**, **Report Type** and select the **Recipient**.

The screenshot shows the 'Report Subscription' configuration window. It has a sidebar with options: 'Security Risk Reports', 'Report Calendar', 'Export', 'Subscription' (selected), and 'Settings'. The main area contains the following settings: 'Enable Report Subscription' is checked; 'Report Type' has three options: 'Daily' (selected), 'Weekly', and 'Monthly'; 'Recipient' is a text input field with a user icon button next to it. An 'OK' button is at the bottom.

Export

Manually export **Overall Security**, **Endpoint Security**, and **Threat Response** Reports.



The **Overall Security** report applies to the administrator, displays overall security situation statistics and situations in summary, and supports exporting per site (branch). The format of the report is pdf.

The **Endpoint Security** report applies to the O&M personnel and displays all risky hosts and detailed risk situations to be processed. It provides explanations and solutions for reference and supports exporting per site (branch) and host. The format of the report is pdf.

The **Threat Response** report applies to the Admin and operator to show whether, when, and how the threats proceeded. The format of the report is pdf.

Click **Export** on **Overall Security**, and select the required details, as shown below:

Export Overall Security

Period:

Last 7 days

Groups:

All

Format:

☒ .doc

Report Name:

☒ Default

☐ Custom

Security Incidents:

Top 10

* Inbound Threats:

☒ High

☒ Medium

☒ Low

Server Threats:

Top 10

Host Threats:

Top 10

Export

Cancel

- **Period:** Refer to the time range for statistics of report data.
- **Groups:** Refer to **All**, **Specified IP Groups**, or **Specified IP Ranges**.
- **Format:** The format of the report is **.doc**.
- **Report Name:** Use **Default** or **Custom**.
- **Security Incidents:** Select Top 5, Top 10, Top 20, Top 50, or all.

Click **Export** on **Endpoint Security** and select the required details, as shown below:

Export Endpoint Security

Period:

Last 7 days

Groups:

All

Format:

☒ .pdf

Report Name:

☒ Default

☐ Custom

* Items ⓘ:

☒ Latent Threat

☐ Weakness

Export

Cancel

- **Period:** Refer to the time range for statistics of report data.
- **Groups:** Refer to **All**, **Specified IP Groups**, or **Specified IP Ranges**.

- **Format:** The format of the report is **pdf**.
- **Report Name:** Use **Default** or **Custom**.
- **Items:** The required content is **Latent Threat**. The optional contents include **Weakness**.

Click **Export** on **Threat Response** and select the required details, as shown below:

Export Threat Response

Period:

Last 7 days

Groups:

All

Format:

☒ .doc

Report Name:

☒ Default

☐ Custom

Export

Cancel

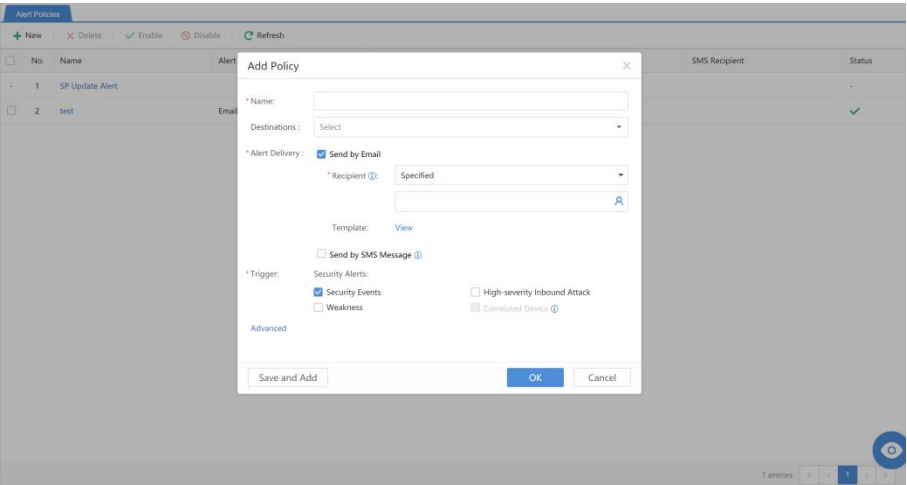
- **Period:** Refer to the time range for statistics of report data.
- **Groups:** Refer to **Specified IP Groups**, **Specified IP Ranges**, and **All**.
- **Format:** The format of the report is **.doc**.
- **Report Name:** Use **Default** or **Custom**.

3.9.2 Notification

The notification module can meet customers who need to subscribe to and regularly push notifications to enable operation and maintenance personnel to understand the platform security status better.

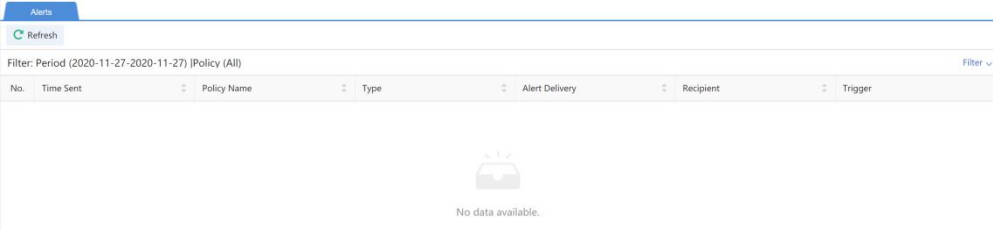
New Subscription

Click **New** to add a new subscription, as shown below:



Alerts

You can view the historical notification records on **Reports > Notification > Notifications**, as shown below.



3.9.3 Security Incidents Database

Share the threat intelligence database with the professional security organization to expand security detection and analysis scope and depth. Then adopt specific prevention measures. Go to **More > Toolkit > Security Incident Database**.

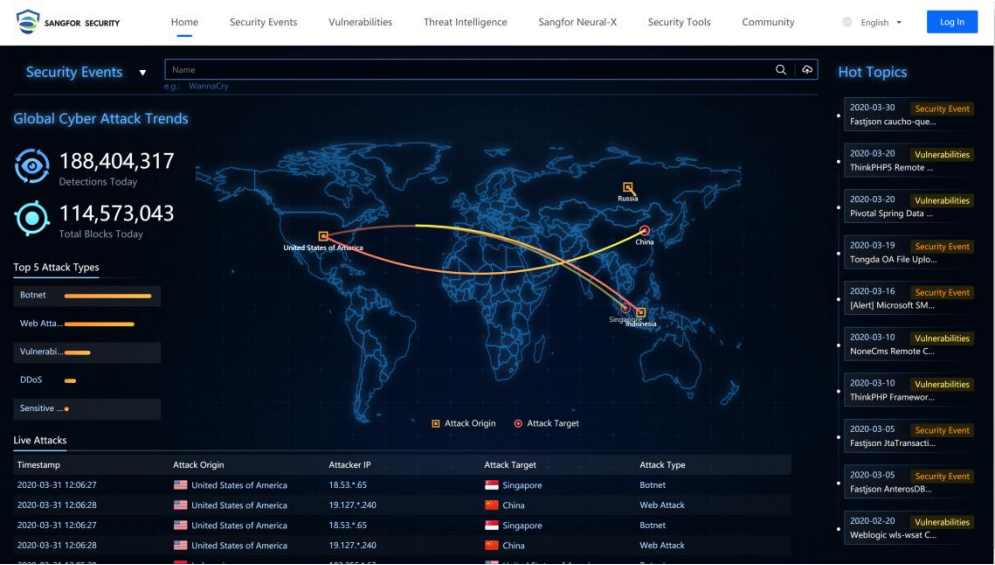


Security Event Database

A database offered by Sangfor Security team, with professional and detailed introduction to common vulnerabilities, attack techniques, etc., as well as specialized and practical security suggestion.

[Details](#)

Click **Details**, and it will redirect to **Sangfor Security**, as shown below:



3.9.4 Data Sharing

Data sharing can realize the **opening** and **sharing** of data resources with third-party platforms through the **RESTful API/syslog** interface, realizing greater data value. Go to **More > Compliance and Sharing > Data Sharing** and click **Details**.

On **Third-Party Platforms**, click **Add** and fill in all the required information.

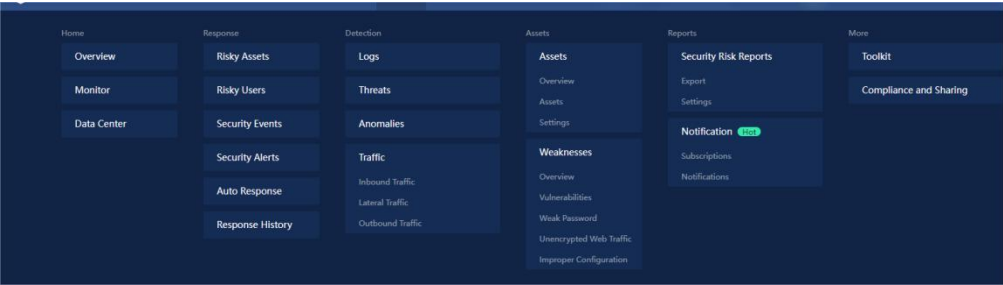
The screenshot shows the 'Third-Party Platform' configuration window. A 'New' dialog box is open, allowing users to add a third-party platform. The dialog box contains the following fields and options:

- Name:** Text input field.
- IP Address:** Text input field.
- Protocol:** Radio buttons for **Restful API** (selected) and **syslog**.
- Username:** Text input field with placeholder 'Please enter your username.'
- Auth Password:** Text input field with placeholder 'Please enter your password.'
- Data Type:** Checkboxes for various data types: IP Group/Branch, Servers, Hosts, Asset Info - Branch, Risky Hosts, Risky Business System, Security Events, Weak Password, Vulnerability Details, and Cleartext Transmission.

Buttons for 'OK' and 'Cancel' are at the bottom of the dialog box.

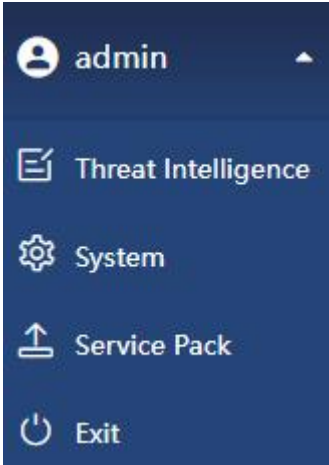
3.10 Navigation

On the Navigation page, all functions are clear and can be directly accessed with one click.



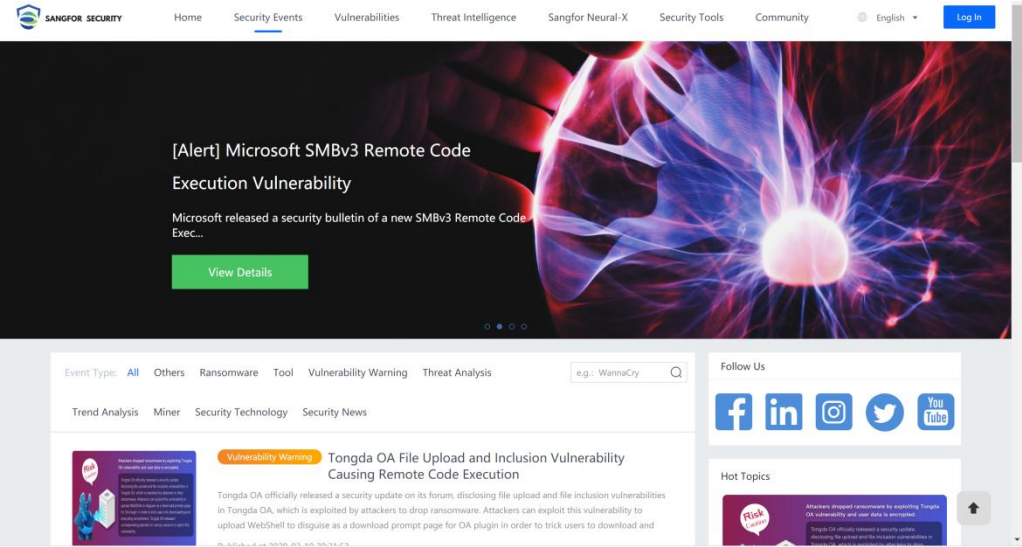
3.11 Other Settings

Enter from the login username at the upper right of the interface to finish the basic configuration of the system and other operations, covering **Threat Intelligence**, **System**, **Service Pack**, and **Exit**.



3.11.1 Threat Intelligence

The Threat Intelligence of Sangfor Security Center updates current security events in real time and provides a detailed analysis process and solutions for the security events. Address: <https://sec.sangfor.com.cn/wiki-safe-events?lang=EN-US>



3.11.2 System

Devices

Sensor Devices

Check the situations of accessed devices, as shown below.

Sensor Devices

Refresh

Total Logs (today): 01 Sangfor devices licensed, 99 licenses remaining (excluding STA)

HCI

Online: 1Offline: 0

N/A (sync not supported)

STA

Online: 0Offline: 0

Today's Synced Logs: 0

Endpoint Secure

Online: 0Offline: 0

Today's Synced Logs: 0

NGAF

Online: 0Offline: 0

Today's Synced Logs: 0

IAG

Connected: 0Offline: 0

N/A (sync not supported)

NewDeleteSTA Connection ConfigurationRefresh

Search

No.	Device Name	Type	IP Address	Version	License Status	Sync Mode	Today's Synced Logs	Total Synced Logs	Today's Logs	Last Synced	Status	Alerts (30 days)	Operation
1	Sangfor HCI	Hyper Conver...	192.168.20.2	-	Licensed	Standard	-	-	-	2022-07-13 16:50:02	Normal	0	-

- **Device Name (IP Address):** Refer to the accessed device's name (IP Address).
- **Type:** The types of accessed devices include STA, NGAF, and Endpoint Secure.
- **IP Address:** Refer to the IP address of the accessed device.
- **Version:** Shows the version of the device that is integrated.
- **License Status:** Shows the license status of the device.
- **Sync Mode:** Defines whether the device has access authorization.

- **Today's Synced Logs:** View the amount of log data uploaded by this accessed device. The units include B, KB, and MB.
- **Total Synced Logs:** View the total amount of log data uploaded by this accessed device. The units include B, KB, and MB.
- **Today's Logs:** View the number of logs uploaded by this accessed device. The unit is pcs.
- **Last Synced:** View the last logs upload time of this accessed device.
- **Status:** Show whether the accessed device is online or offline and display IAG and SSL VPN statuses with dashes (-).
- **Alert (30days):** Shows the alert of the integrated device.
- **Operation:** Choose the details of the device if supported, if not supported with come out with dashes (-).

Click **New** to add the accessed device, as shown below:

New

Type:

Internet Access Gateway

* Device Name:

Sangfor IAG

* Device IP:

Version:

Earlier than 12.0.27

12.0.27 or Later

STA and NGAF can be connected without being configured on Cyber Command.

Shared Key:

Remarks:

Advanced

OK

Cancel

Cyber Command is integrated with other Sangfor devices, such as **Internet Access**

Gateway (IAG), Endpoint Secure (ES), SSL VPN, Network Controller, Hyper-Converged Infrastructure, and SaaS Endpoint Secure.

- **Internet Access Gateway configuration:** A shared password with the same IAG configuration is needed.
- **Endpoint Secure configuration:** An authentication account and an authentication password, the same as the Endpoint Secure.
- **SSL VPN:** Only access to the device IP address of SSL.

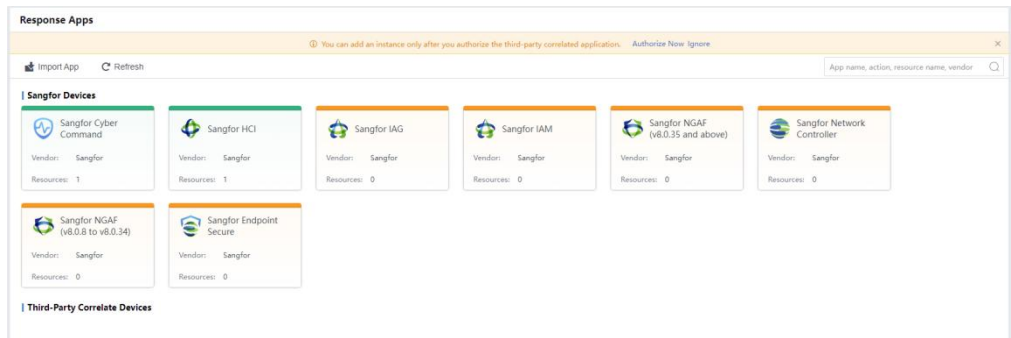
Since STA and NGAF only need to be configured on STA and NGAF pages, they are not added here.

For more information, refer to the Latest Configuration Guide released knowledge base: <https://knowledgebase.sangfor.com/>

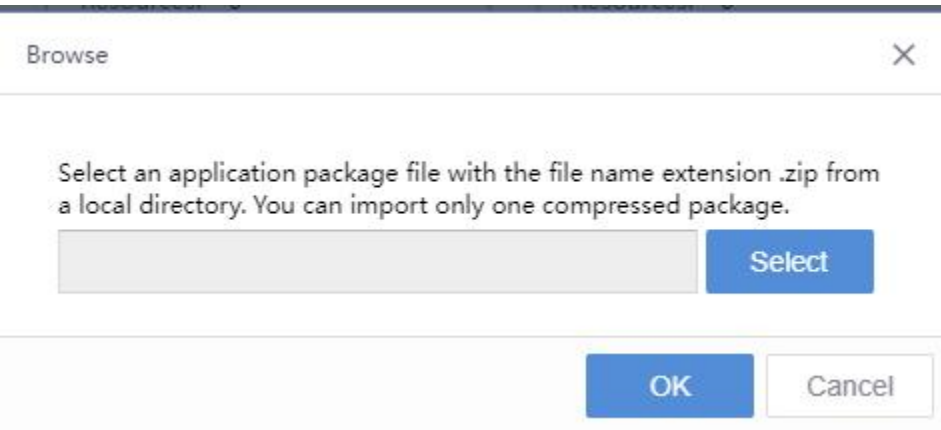
Response Apps

On the **System > Devices > Response Apps** page is mainly the integration response function, which is mainly to configure the applications and devices that need to be connected and maintain and manage the devices that need to be integrated.

Cyber Command has built-in some linked applications with the version. To add other applications, you can import more docking applications through the import application function. The development of currently connected applications can submit docking requirements and related interface documents to the vendor. The package is developed by the vendor and imported into Cyber Command, as shown in the figure below.



Click **Import APP** to import the application package in **.zip format**. The compressed package can support multiple applications, and multiple applications that need to be docked can be imported at once. In addition, the applications updated by subsequent manufacturers can also be imported after obtaining the compressed package, as shown in the following figure.



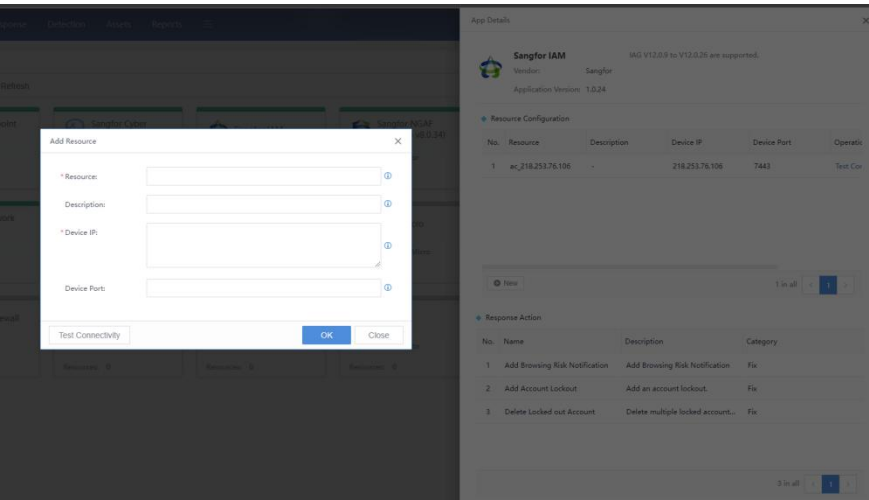
Click the application icon to view the **App Details** page on the right. After entering the specific application, you can view the details of the application, including supported device versions, application updates, supported actions, and adding resources corresponding to the application. The application needs to add specific docking device resources to take effect, and the parameters for adding resources to different applications are different.

You must acquire the **Access SN for Third-Party Correlated Application** license to activate the **Third-Party Correlate Devices** feature.



Sangfor Cyber Command

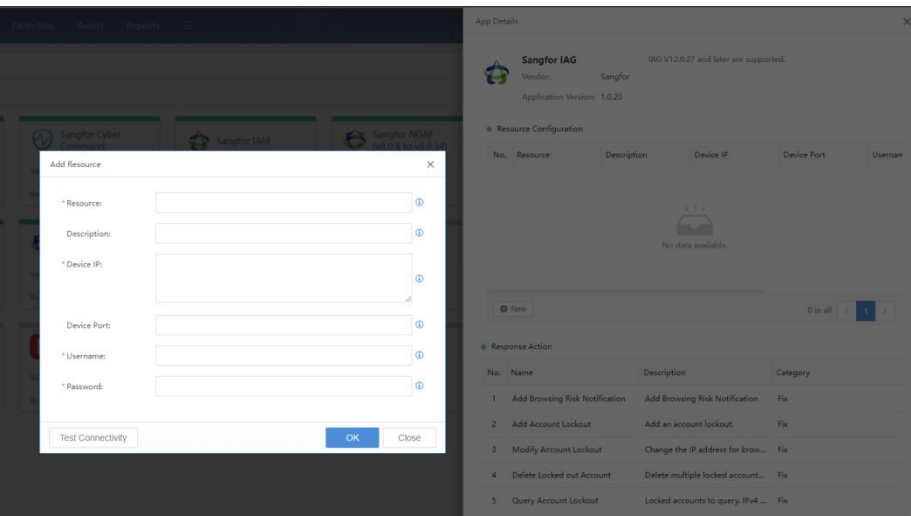
For v12.0.27 and later, the standard API interface is already available in this version and above. The content that needs to be filled in is shown in the figure below.



- **Resource:** fill in the name of the device that is easy to remember. The application supports multiple docking devices.
- **Description:** Describe the specific scope or functional properties.
- Request **address:** The address of the connected device, which can be an IP or a domain name, ensures that the network can be communicated.
- **Device port:** The specific port opened or mapped by the docking device

Sangfor IAG

For versions earlier than v12.0.27, it is using the non-public interface is used. The content that needs to be filled in is shown in the figure below.

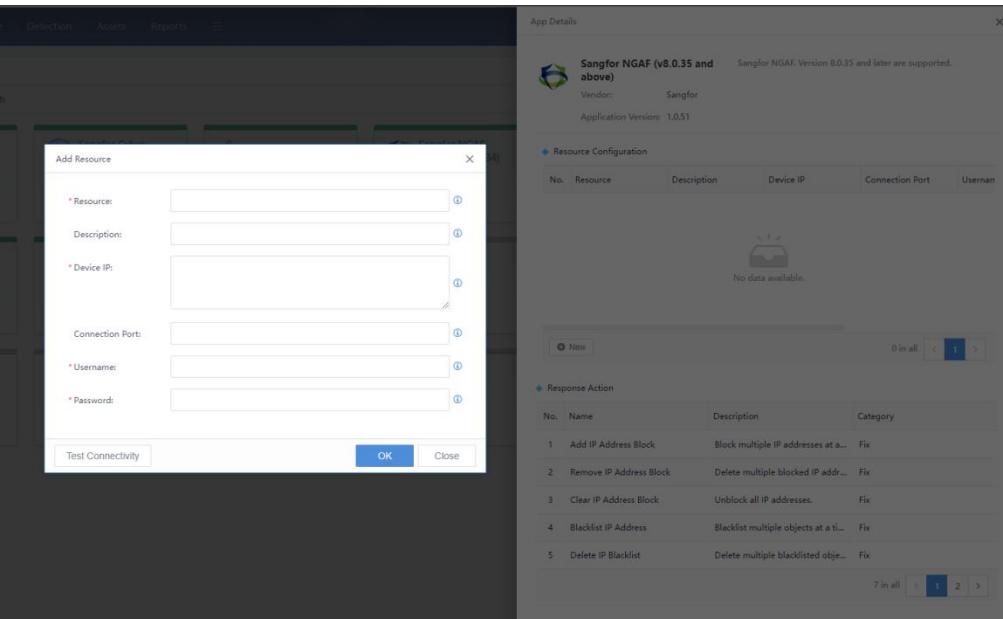


- **Resource:** fill in the device's name that is easy to remember. The application supports multiple docking devices.

- **Description:** Describe the specific scope or functional properties.
- **Device IP:** The address of the connected device, which can be an IP or a domain name, ensures that the network can be communicated.
- **Device port:** The specific port opened or mapped by the docking device.
- **Username:** Username of IAG
- **Password:** Password of IAG

Sangfor NGAF (v8.0.35 and above)

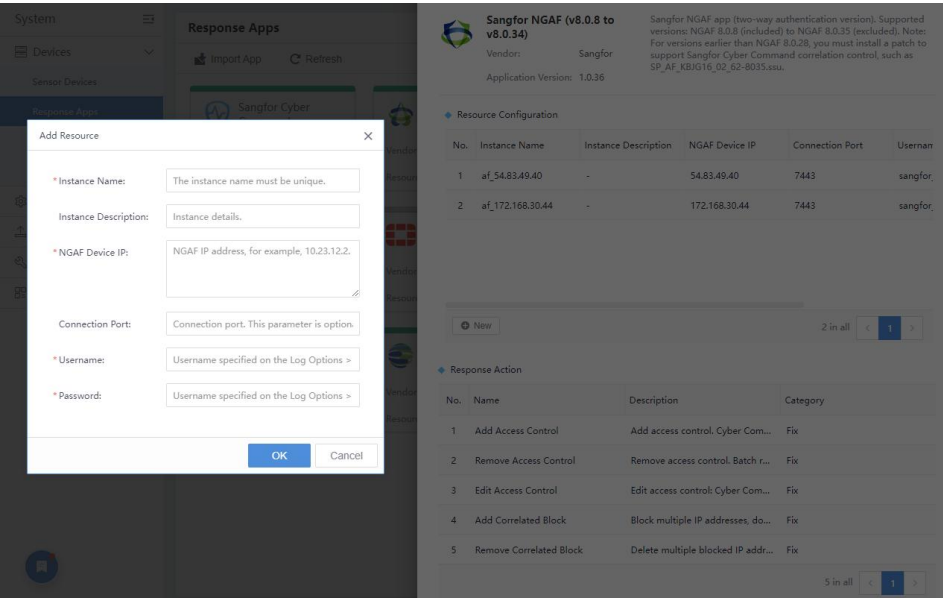
For Sangfor NGAF v8.0.35 and later, the standard external interface is used. The configuration that needs to be filled in is shown in the figure below.



- **Resource:** fill in the device's name that is easy to remember. The application supports multiple docking devices.
- **Description:** Describe the specific scope or functional properties.
- **Device IP:** The address of the connected device, which can be an IP or a domain name, ensures that the network can be communicated.
- **Device port:** The specific port opened or mapped by the docking device. The default is port 443.
- **Username:** The **username** for integration.
- **Password:** Password for Integration.

Sangfor Network Secure (v8.0.8 to v8.0.34)

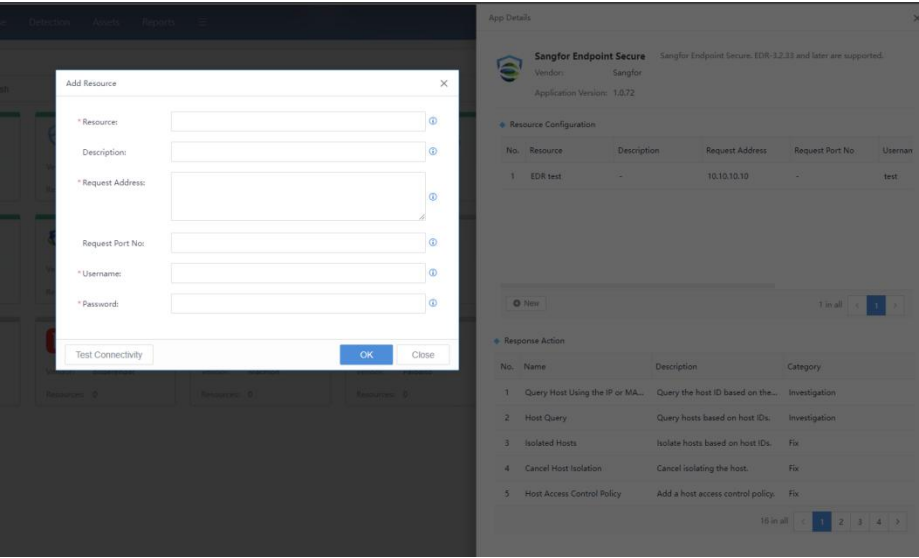
For Sangfor Network Secure v8.0.8 to v8.0.35 (not included), the old interface is used, and the configuration that needs to be filled is shown in the figure below.



- **Resources:** fill in the device's name that is easy to remember. The application supports multiple docking devices.
- **Description:** Describe the specific scope or functional properties.
- **Device IP:** The address of the connected device, which can be an IP or a domain name, ensures that the network can be communicated.
- **Device Port:** The specific port opened or mapped by the docking device. The default port is 443.
- **Username:** The **username** for integration.
- **Password:** Password for integration.

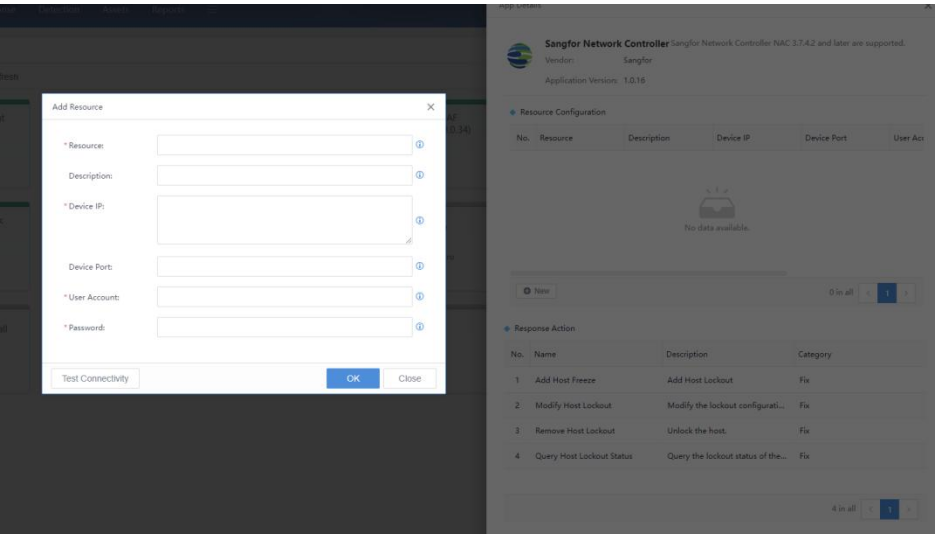
Sangfor Endpoint Secure

For Sangfor Endpoint Secure v3.2.33 and later, the configuration that needs to be filled in is shown in the figure below.



- **Resources:** fill in the name of the device that is easy to remember. The application supports multiple docking devices.
- **Description:** Describe the specific scope or functional properties.
- **Request address:** The address of the connected device, which can be an IP or a domain name, ensures that the network can be communicated.
- **Request port number:** The docking device's specific port or maps to the outside world. The default port is 443.
- **Account:** The username for docking. Activate it on the HCI platform.
- **Password:** Password for docking.

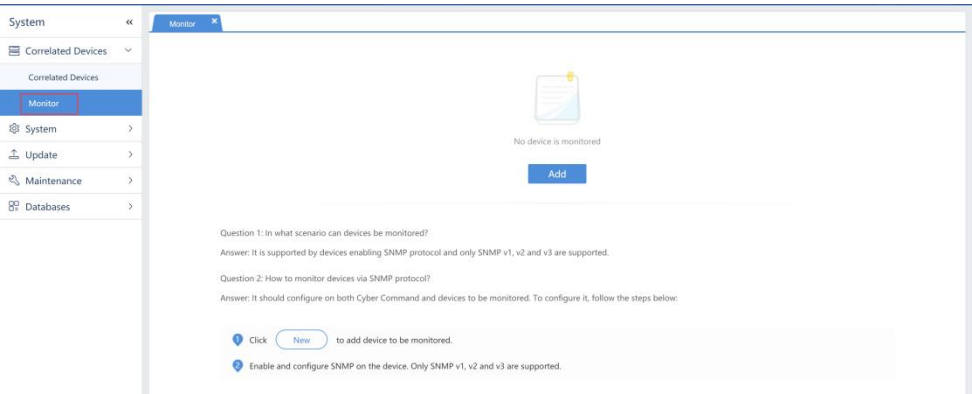
Sangfor Network Controller



- **Resources:** fill in the device's name that is easy to remember. The application supports multiple docking devices.
- **Description:** Describe the specific scope or functional properties.
- **Device IP:** The address of the connected device, which can be an IP or a domain name, ensures that the network can be communicated.
- **Device Port:** The specific port opened or mapped by the docking device. The default port is 443.
- **Username:** The username for integration.
- **Password:** Password for integration.

Device Monitoring

Monitor the running of the accessed device through the Simple Network Management Protocol (SNMP). The protocol versions of the SNMP enabled in this device include V1, V2, and V3.



Click **New** to add a device that needs to be monitored.

New

* Type: ☒ Router ☐ Switch ☐ Others

* Device IP:

Scanner:

SNMP

☒ SNMP V1/SNMP V2 ⓘ

Community:

☐ SNMP V3

Username:

Security:

Auth Method:

Auth Password: ⓘ

Encryption Method:

OK Cancel

- **Device IP:** Refer to the IP address of the accessed device.
- **SNMP V1/SNMP V2:** Configure a group name set on the accessed device.
- **SNMP V3:** Implement bidirectional authentication on V3 by configuring username, security level, authentication method, authentication password, encryption method, and encryption password information corresponding to the accessed device.

Click **Advanced** to obtain CPU free space, total memory size, remaining memory, outbound traffic of the networking interface, and inbound traffic through OID, which shall correspond to the accessed device.

New

Encryption Password:

Context:

OID Setup

OID for Free CPU

OID for Total Memory:

OID for Free Memory

OID for Outbound Traffic:

OID for Inbound Traffic:

OID for Platform/Device Name:

Collapse ^

Inconsistent SNMP settings, or wrong IP configuration on either this Cyber Command or the device may cause data unavailable.

OK

Cancel

The SNMP V1/SNMP V2 does not support obtaining the traffic information. Therefore, there will be no data in the related traffic display. If required to obtain the traffic information, please select SNMP V 3.

Data Sharing

Data Upload

I. Connect to Sangfor Cyber Guardian Platform

Cyber Command can be connected to Sangfor Cyber Guardian Platform. This way, data such as security logs, security alerts, security events, assets, and audit logs can be reported to Sangfor Cyber Guardian Platform through cloud data channels. Security administrators can use this feature to perform security maintenance operations.

The following content shows how to use this feature.

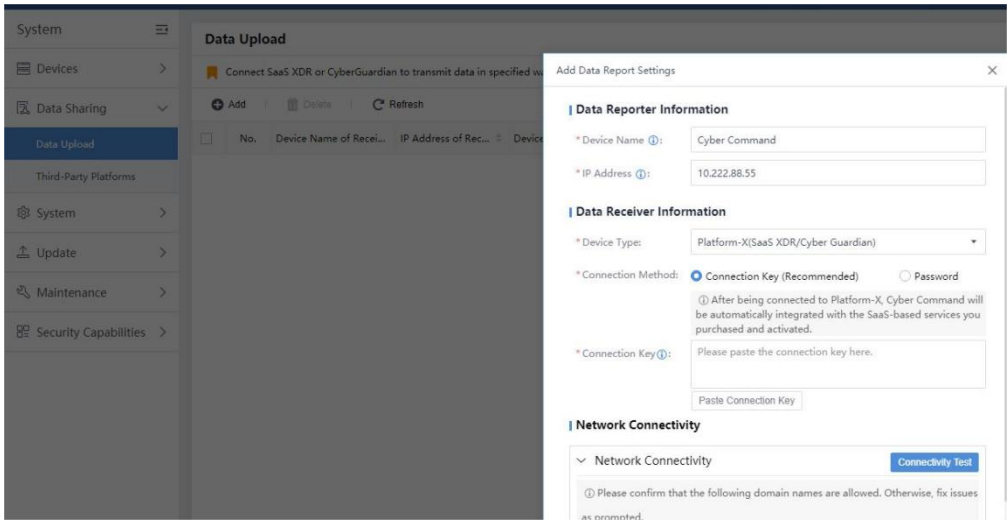
Steps

1. Log in to the Cyber Command console as a security administrator, move

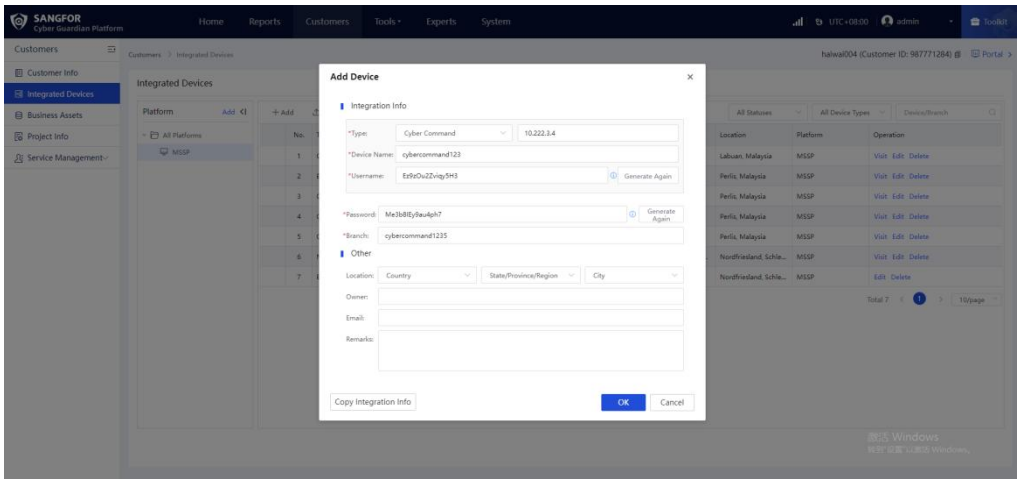
Version 01 (May 30, 2024)

137

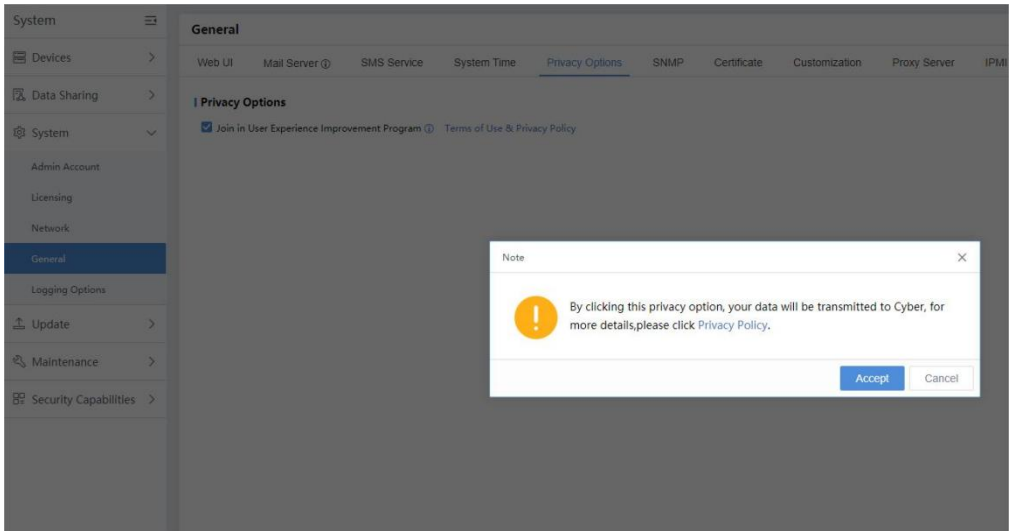
the pointer over the user avatar in the upper-right corner, and select **System**. Go to **System > Data Sharing > Data Upload**, click **Add**, and configure parameters as required, as shown in the following figure.



2. Log in to the Sangfor Cyber Guardian Platform console, go to **Customers > Integrated Devices**, and click **Add**. In the dialog box that appears, configure relevant parameters as required. Take note that you must visit <https://soar.sea.sangfor.com/> to register a tenant for integration.

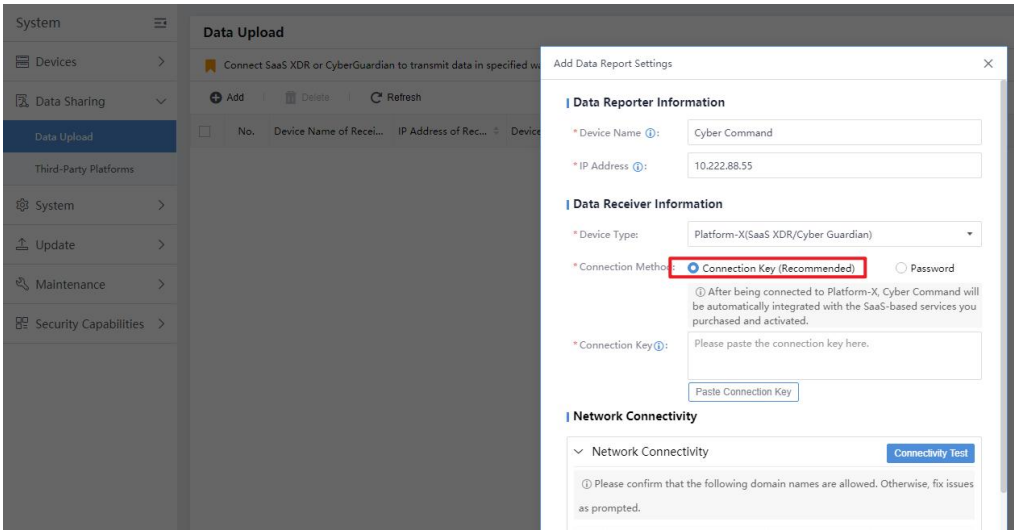


3. Go to **System > System > General > Privacy Options**, and select **Join in User Experience Improvement Program**. Otherwise, data is not reported to Cyber Command.



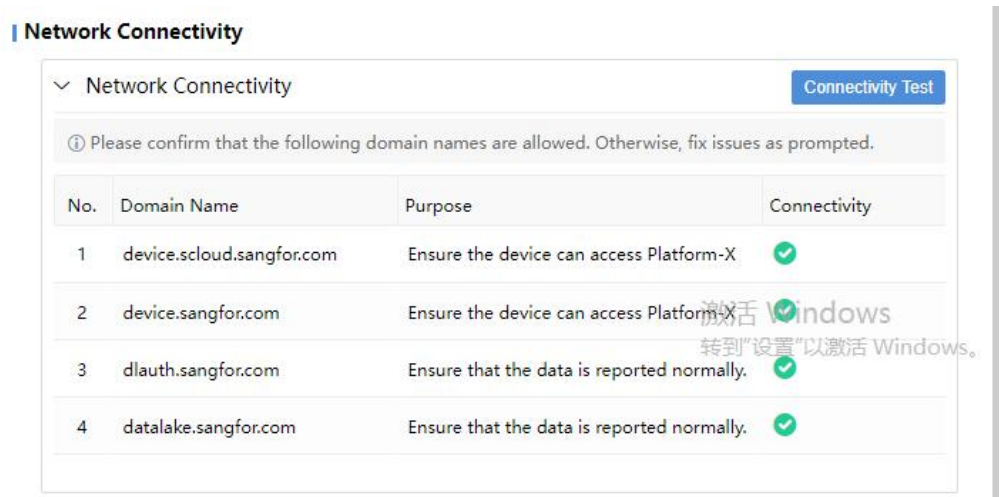
Usage Notes

Connection through the connection key is not supported.



Troubleshooting

- Before Cyber Command is connected to Sangfor Cyber Guardian Platform, check the network connectivity to the domain names listed in the **Network Connectivity** section.



- If the connection fails, troubleshoot errors based on the log file: `tail -f /var/log/today/sis_infoshare_ci.log`.

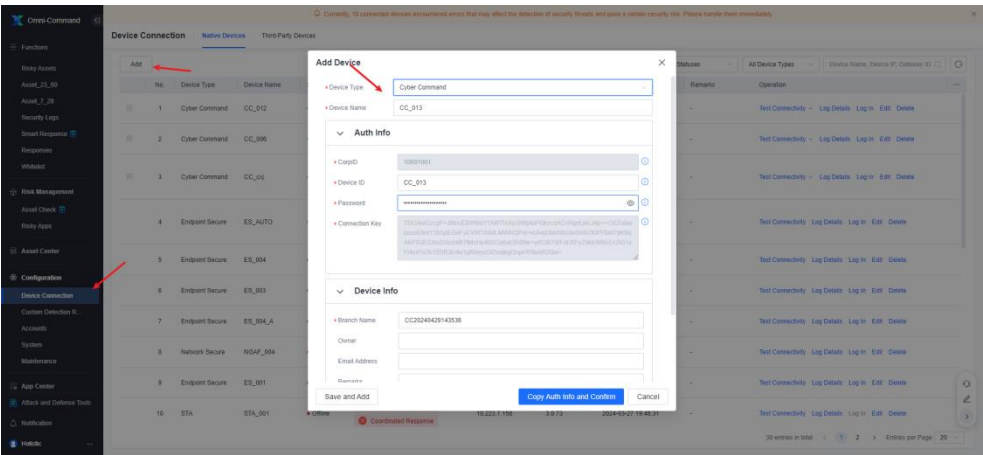
II. Connect to Omni-Command

Cyber Command can be connected to Omni-Command. This way, data such as security logs, audit logs, vulnerabilities and weak passwords, assets, security events, and security alerts can be reported to Omni-Command. Engineers such as security administrators and security maintenance experts can use this feature to perform security maintenance operations.

The following content shows how to use this feature.

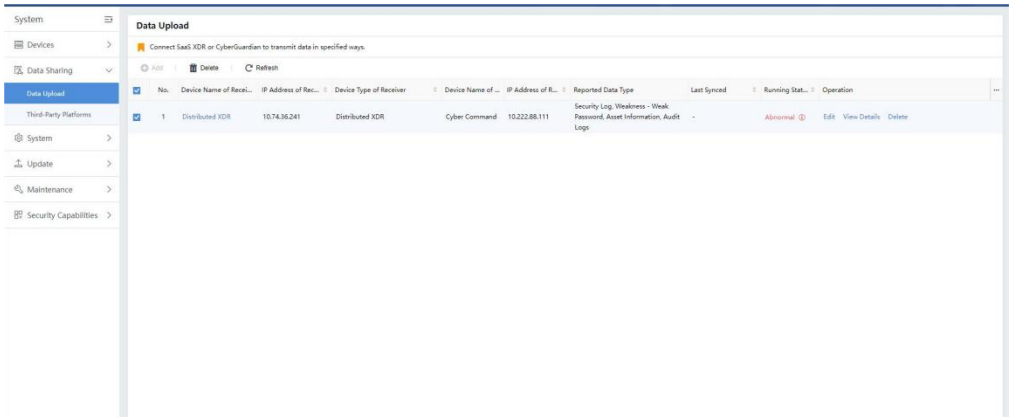
Steps

1. Log in to the Omni-Command console, go to **Configuration > Device Connection > Native Devices**, and click **Add** to add a Cyber Command data source, as shown in the following figure.

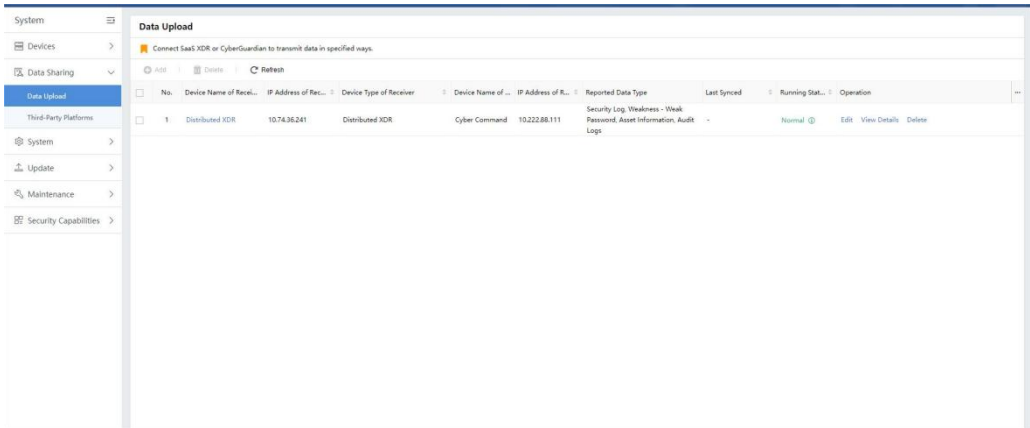
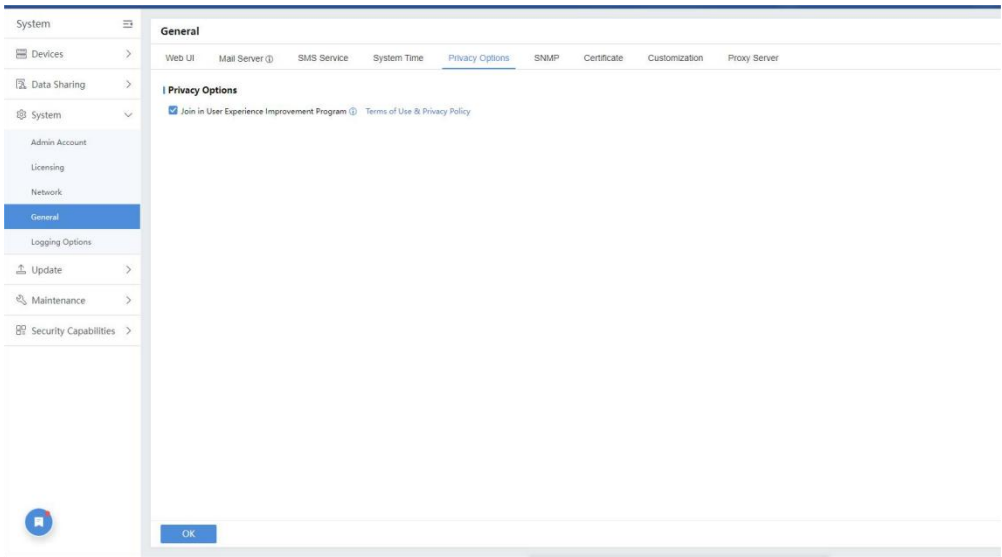


2. Log in to the Cyber Command console, move the pointer over the user avatar, and select **System**. Go to **System > Data Sharing > Data Upload**,

and click **Add**. In the dialog box that appears, set **Device Type** to **Distributed XDR**, configure other parameters as required, and then click **OK**.



3. Go to **System > System > General > Privacy Options**, and select **Join in User Experience Improvement Program**. Then, the **Running Status** of the newly added device changes to **Normal**.

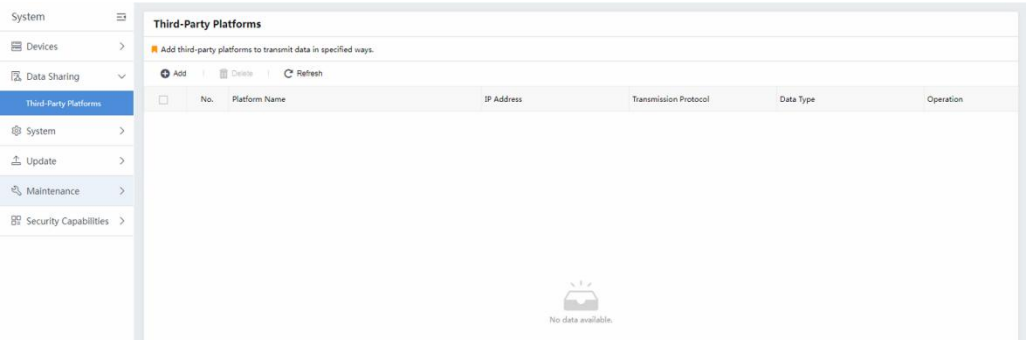


Usage Notes

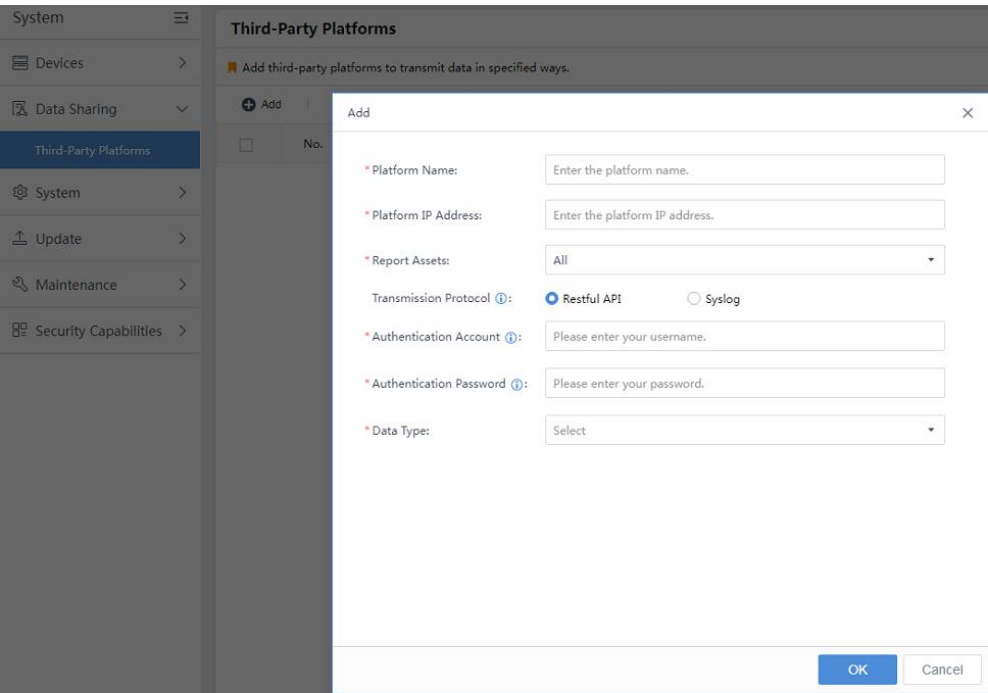
Connection through the connection key is not supported.

Third-Party Platforms

You can share data from Cyber Command to third-party platform by either API or syslog.



Click **Add** to add a new item for sharing.



For Restful API Type

- **Platform Name:** Custom the target platform name.
- **Platform IP Address:** Fill in the target IP address.
- **Report Assets:** Select specific assets group for sharing.

- **Transmission Protocol:** Restful API and syslog are supported. For example, select Restful API.
- **Authentication Account:** Fill in API account created in target platform.
- **Authentication Password:** Fill in API password created in target platform.
- **Data Type:** Pull down and select data type you need to share.

Add

×

* Platform Name:

Enter the platform name.

* Platform IP Address:

Enter the platform IP address.

* Report Assets:

All

Transmission Protocol ⓘ:

☒ Restful API ☐ Syslog

* Authentication Account ⓘ:

Please enter your username.

* Authentication Password ⓘ:

Please enter your password.

* Data Type:

Select

For Syslog Type

- **Platform Name:** Custom the target platform name.
- **Platform IP Address:** Fill in the target IP address.
- **Report Assets:** Select specific assets group for sharing.
- **Transmission Protocol:** Either Restful API or syslog is optional, here for example select syslog type.
- **Data Type:** Generally it contains security alerts and security incidents, meanwhile you can filter specific data by "Severity", "Threat Type", "Data Format", "Confidence" and "Synchronization Time".
- **Port:** By default, it is transmitted by UDP 514, you can modify it according to syslog server's setting.

×

Add

* Platform Name:

Enter the platform name.

* Platform IP Address:

Enter the platform IP address.

* Report Assets:

All

Transmission Protocol ⓘ:

☐ Restful API
 ☒ Syslog

* Data Type:

☒ Security Incident

* Threat Type:

All

* Severity:

All ×

* Data Format:

SEF(Sangfor Event For...

* Synchronization Time ⓘ:

-

10

+

Minute(s)

☒ Security Alert

* Threat Type:

All

OK

Cancel



The data type to be shared differs if you select a different transmission protocol. For example, when you select "Restful API" type, third-party platform will not receive security alerts. Proceed with caution.

Transmission Protocol : ☒ Restful API ☐ Syslog

* Authentication Account :

* Authentication Password :

* Data Type:

Select 

☐ IP Group/Branch

☐ Server

☒ Host

☐ Risky Host

☐ Risky Server

☐ Security Incident

☐ Weak Password

☐ Vulnerability Details

☐ Unencrypted Traffic

System

Admin Account

I. Overview

On the **Admin Account** page, you can add an account, change the account password, and grant permissions to the account. The administrator account has the highest level of permissions.

Admin Account

Admin Account

Role

New

Delete

Enable

Disable

Refresh

Login Management

Password Security Policy

Search

☐	No.	Username	Description	Administrative Realm	Role	Owner	Status ⓘ	Validity Period	Operation
☐	1	admin	admin	All	Super Admin	-	✓	Long Term	Change Password

To add an administrator account, click **New**.

Admin Account

Admin AccountRole

NewDeleteEnableDisableRefreshLogin ManagementPassword Security Policy

☐	No.	Username	Description
☐	1	admin	admin

New

*Username:

ⓘ

*Role:

▼

Owner:

ⓘ

Description:

ⓘ

Login SecurityAdministrative RealmPermissionApp Permission

*Authentication Method:

Password

▼

*Password:

ⓘ

*Retype Password:

IP Address:

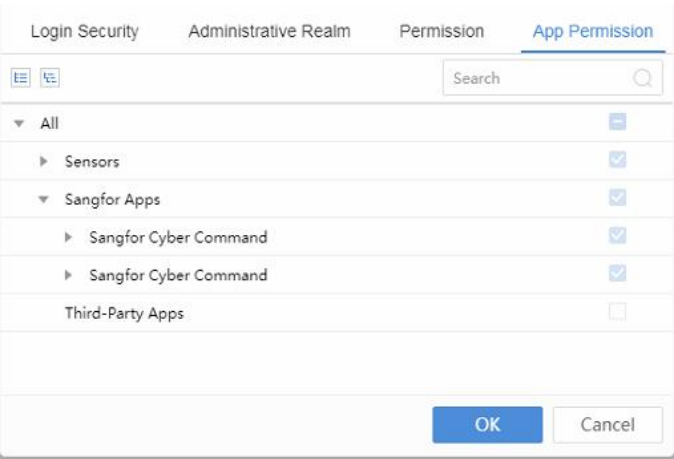
☐ Only allow login from specified IP addresses

OK

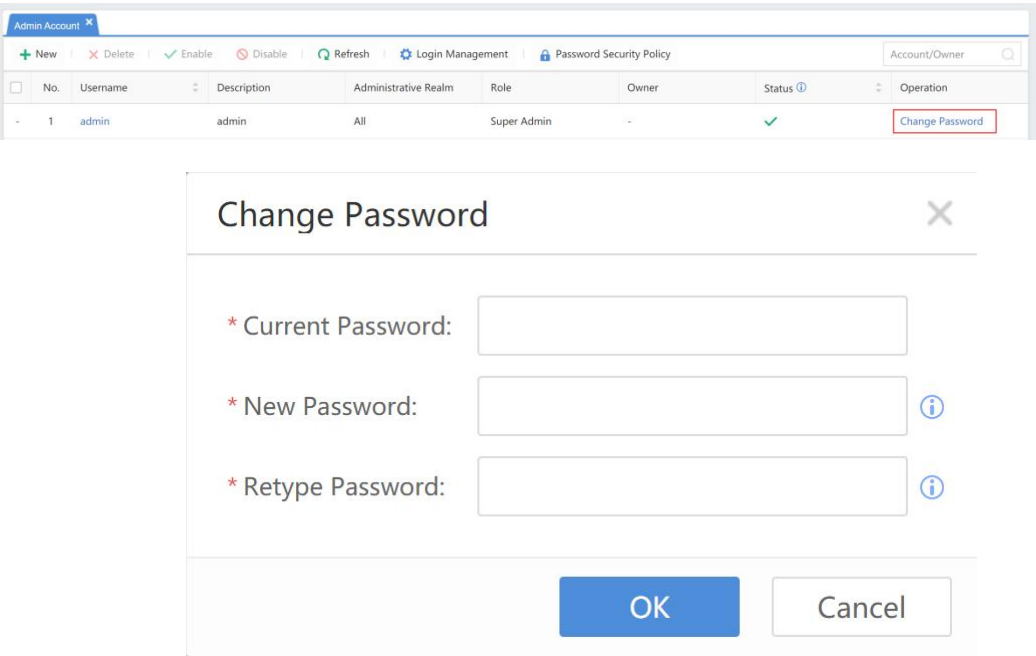
Cancel

- **Username:** Create a username for the login account.
- **Role:** Select the role of the administrator.
- **Owner:** The Administrator’s owner.
- **Description:** Describe this account.
- **Password:** Refer to the password for logging in using the username.
- **Retype Password:** Confirm the password.

- **Administrative Realm:** It is used in a multi-branch scenario. Recommended administrators for different branches only can view the information of corresponding branches.
- **Permission:** Refer to Administration and View, and there is permission for editing in Administration.
- **App Permission:** It is used to bond a specific account with specific correlation App, which can be set in the first step of creating a role.



For the created account, click **Username** to change the account permission.
Click **Change Password** to change the account password.



- **Change Password:** When changing the password of the current login account, enter an existing password. When changing an account password created by the current login account, directly change a new password.



- 1. The password cannot contain a username.
- 2. It must be 8 to 64 characters.
- 3. Cannot contain Chinese characters, spaces, or full-length characters.
- 4. It must contain irregular characters that consist of any three of the following: uppercase letters, lowercase letters, digits, and special characters.
- 5. It cannot contain sensitive characters.

Cyber Command support adding the Google authenticator as the OTP account to do two-factor authentication.

Edit

* Username:

admin

* Role:

Super Admin

Owner:

Description:

admin

Login Security

Administrative Realm

Permission

* Authentication Method:

Password

IP Address:

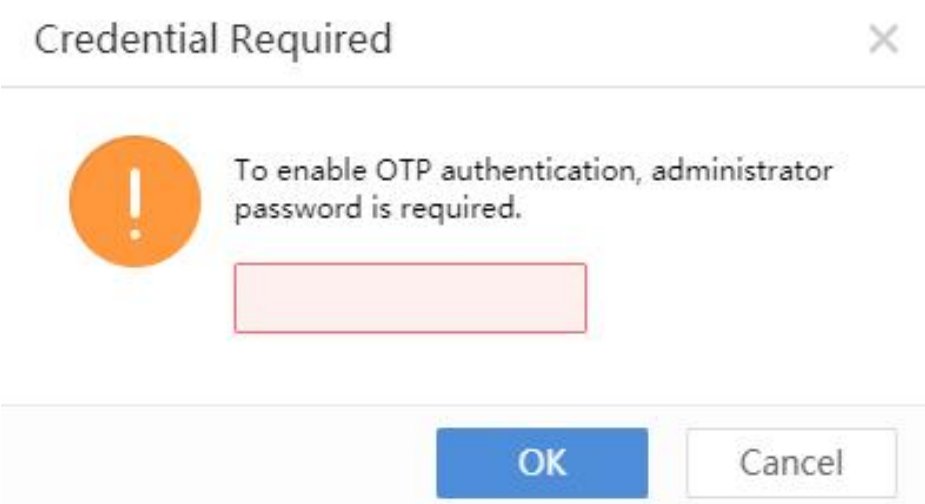
☐

Only allow login from specified IP addresses

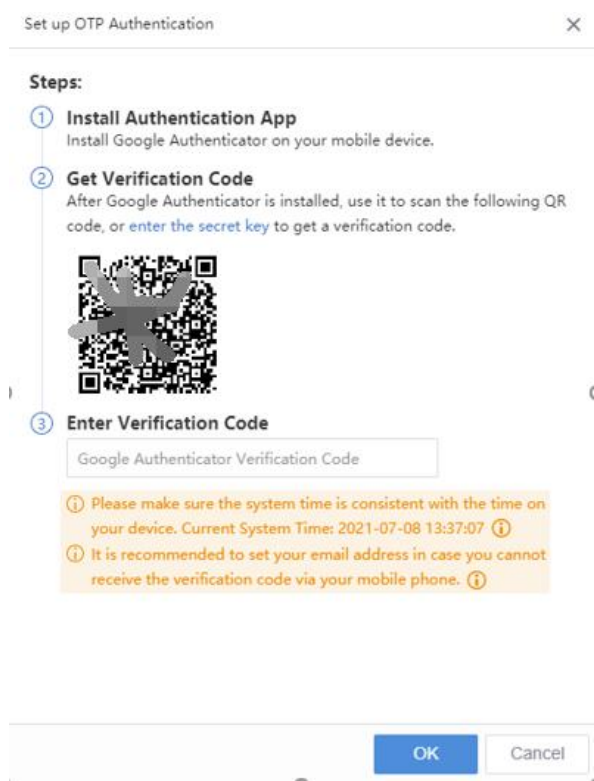
OK

Cancel

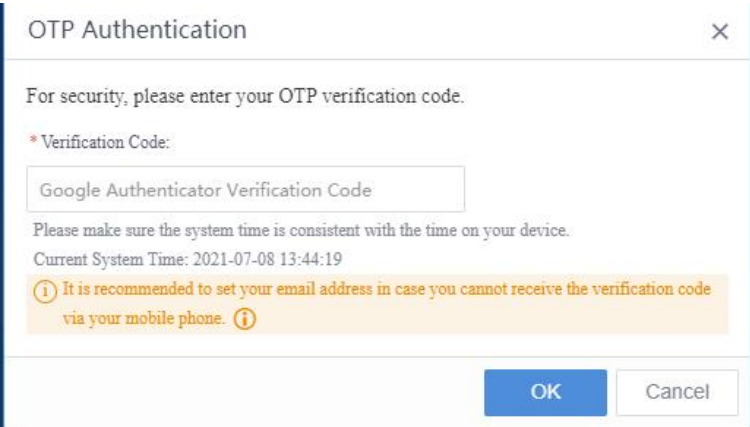
Click the **Authentication Method** drop-down list and select **Password + OTP**.
When you click **Set up TOP authentication**, the page shown in the following figure appears.



After entering the account password, it will show the QR verification code.
Follow the instructions stated below and use the Google Authenticator to scan the verification code.



Once login from the web console interface will pop out and key in the verification code.
You are required to key in the verification code generated on your Google Authenticator Apps to proceed with the login.

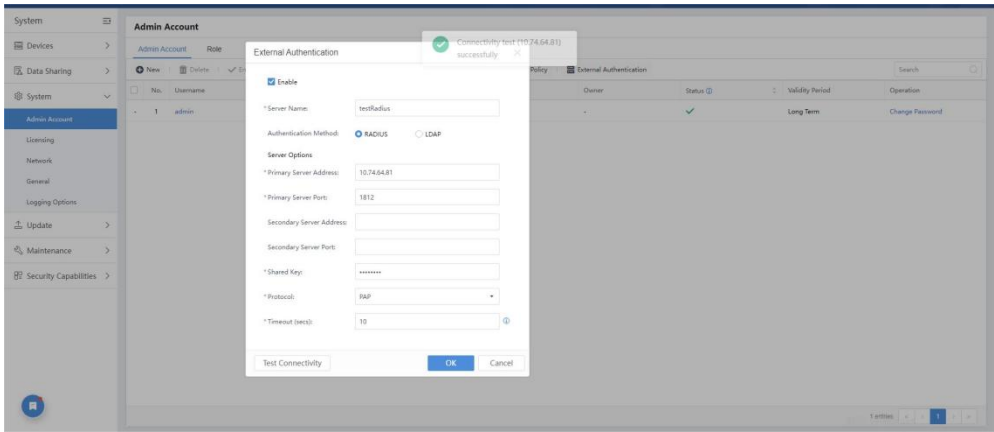


II. Add Administrator Accounts for Users from the RADIUS Authentication Server

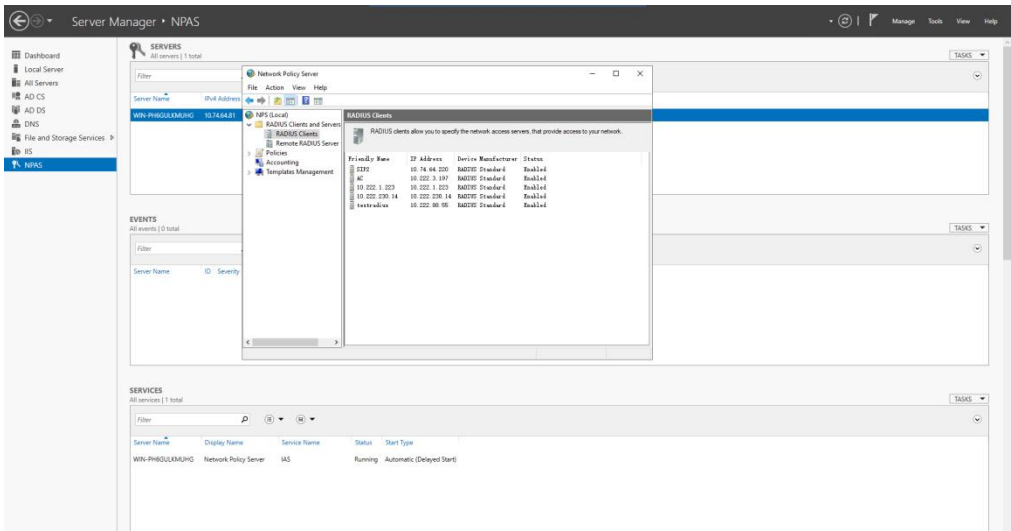
On the **Admin Account** page, security administrators and security O&M experts can add system administrator accounts and regular administrator accounts for users from the RADIUS authentication server. This way, users from the RADIUS authentication server can log in to Cyber Command. This feature is applicable to security maintenance scenarios.

Steps

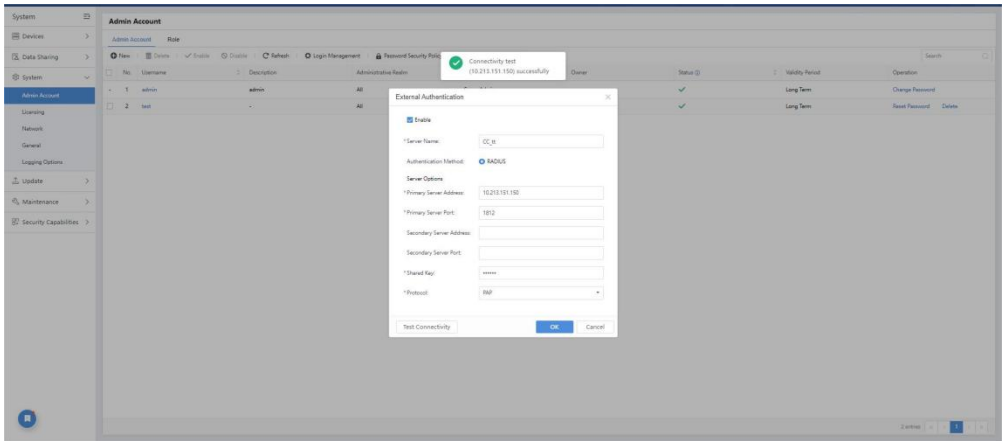
- 1. Go to **System > System > Admin Account**, and click **External Authentication**. In the dialog box that appears, select **RADIUS** for **Authentication Method**, set other parameters as needed, and then click **OK**. The default value of **Primary Server Port** is 1812.



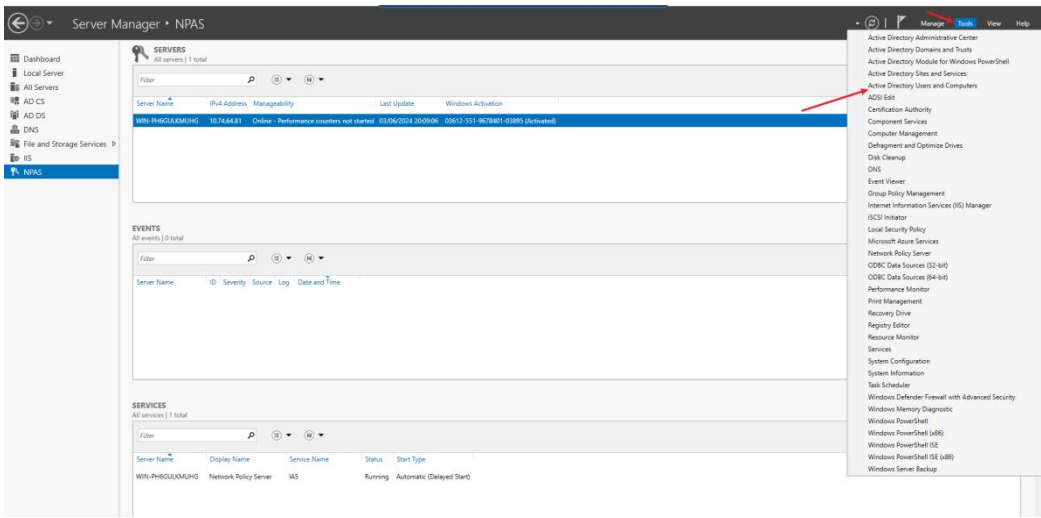
Configure the shared secret on both the RADIUS client and server. The following figure shows how to configure the shared secret for the RADIUS server in Windows Server 2019.

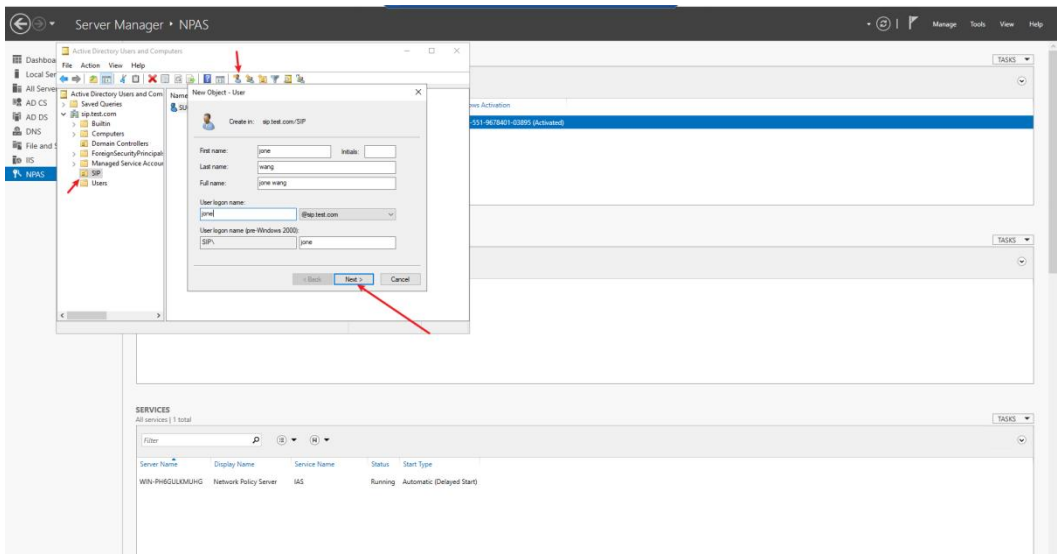


2. Test the connectivity.

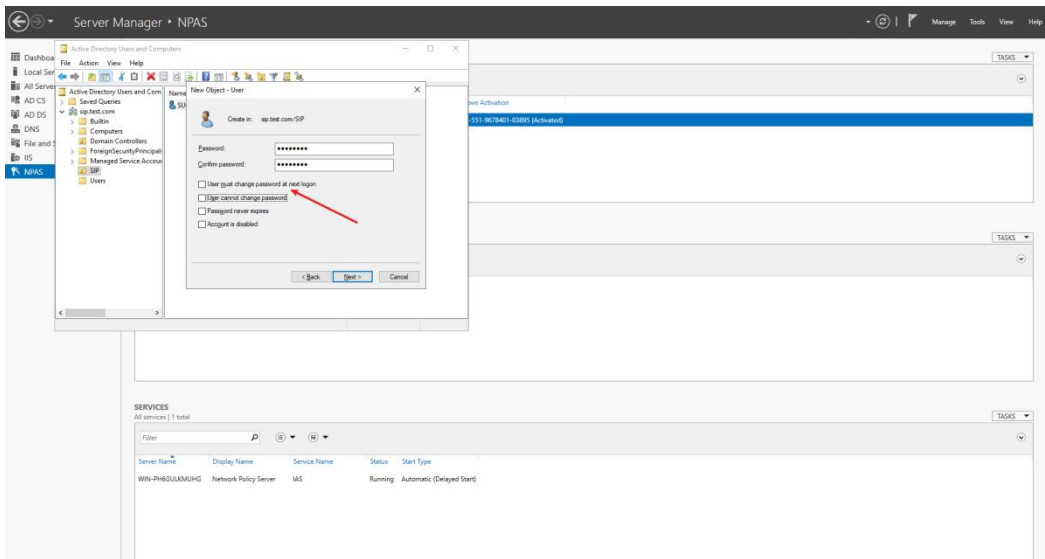


3. After settings on the RADIUS authentication server and Cyber Command are completed, users on the RADIUS authentication server can log in to Cyber Command. The following figures show how to create a user.

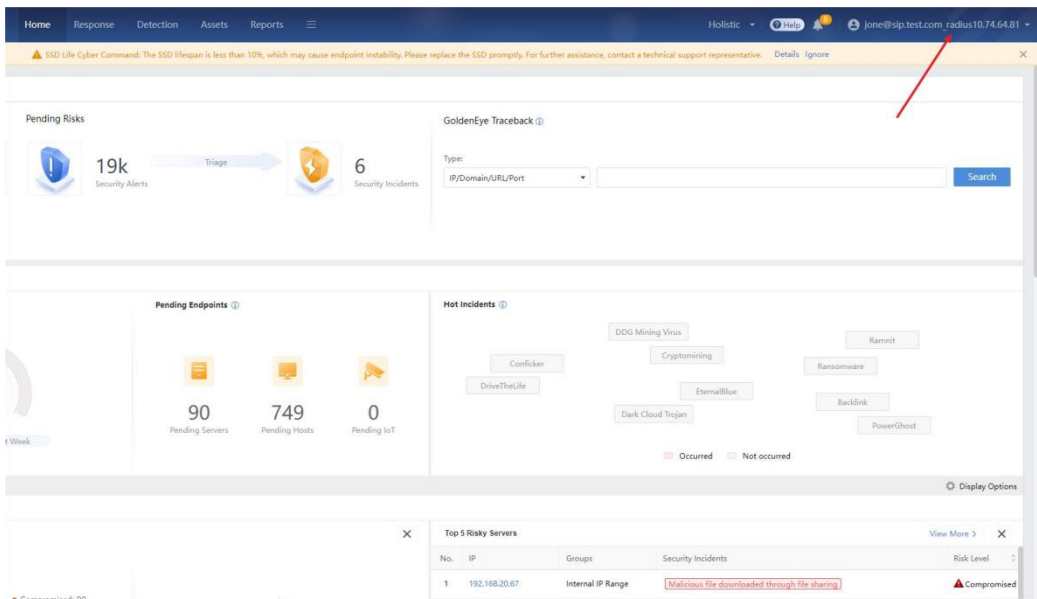




4. Complete password settings. Make sure that **User must change password at next login** is deselected. Otherwise, the login from the authentication server may fail.

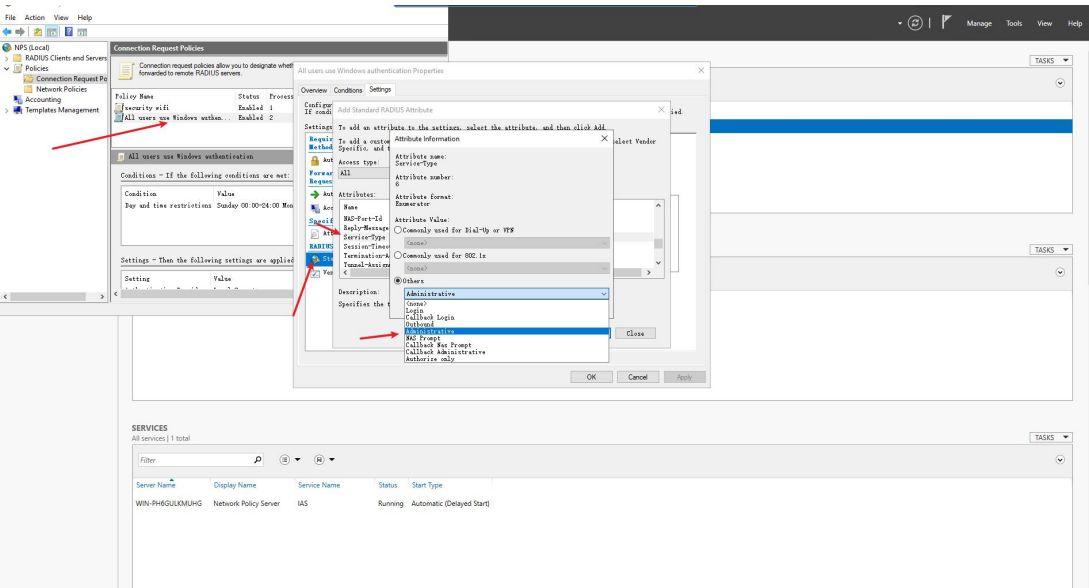


5. After the user is successfully registered, the user can successfully log in to Cyber Command by using the registered user name.



Usage Notes

- Make sure that **User must change password at next login** is deselected when you configure password settings.
- If active and secondary RADIUS servers are configured, make sure that both RADIUS servers use the same authentication key. If different authentication keys are used, the configuration applies only to the RADIUS server whose authentication key is valid.
- During the configuration of user permissions in RADIUS, the user whose **Attribute Value** is set to **administrative** corresponds to the system administrator, whereas other users are regular administrators.



Troubleshooting

The following table describes the RADIUS client vendors that support RADIUS.

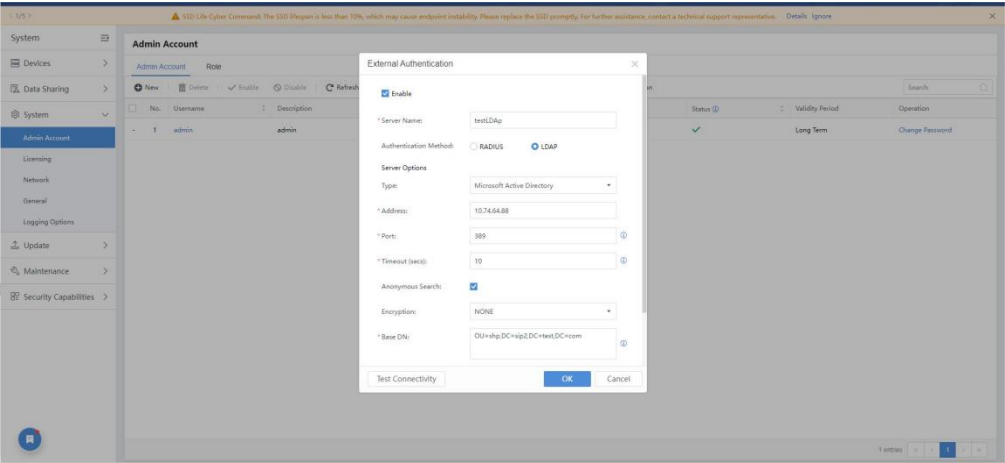
RADIUS Client Vendor	Supported
3Com	Supported
ACC	Supported
ADC Kentrox	Supported
Ascend Communications	Supported
BBN	Supported
BinTec Communications GmbH	Supported
Cabletron Systems	Supported
Cisco	Supported
Digi International	Supported
Eicon Networks Corporation	Supported
Gandalf	Supported
Intel Corporation	Supported
Lantronix	Supported
Livingston Enterprises	Supported
Proteon	Supported
Shiva Corporation	Supported
Telebit	Supported
U.S. Robotics	Supported
Xylogics	Supported
Microsoft	Supported
RedBack Networks	Supported
Nortel Networks	Supported

III. Add Administrator Accounts for Users from the LDAP Authentication Server

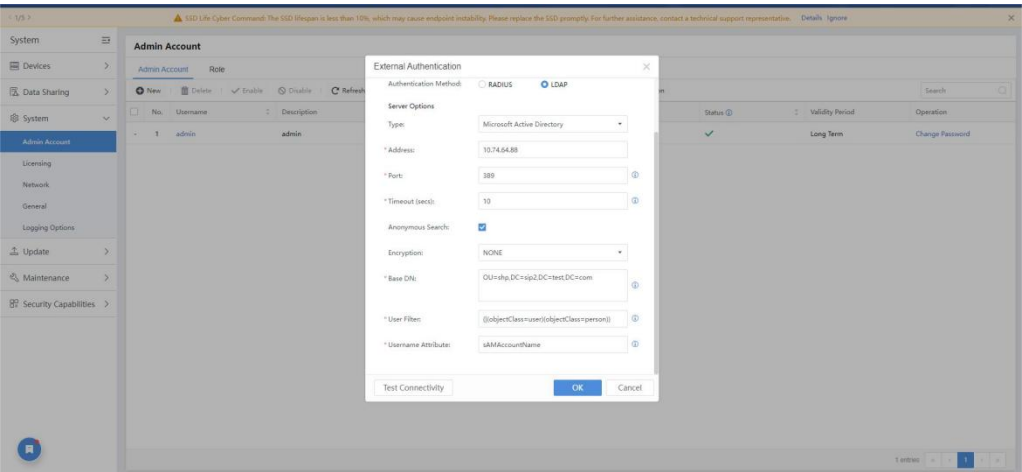
On the **Admin Account** page, security administrators can add regular administrator accounts for users from the LDAP authentication server, so that the users can log in to Cyber Command as regular administrators. This feature is applicable to security maintenance scenarios.

The following content describes how to use this feature.

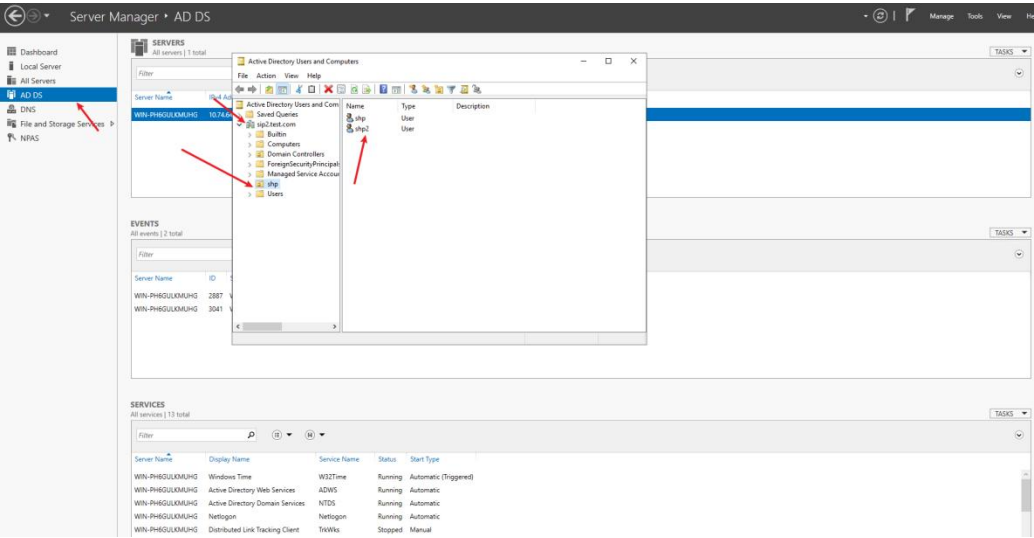
Go to **System > System > Admin Account**, and click **External Authentication**. In the dialog box that appears, select **LDAP** for **Authentication Method**, and set other parameters as needed.



The following figure provides an example on how to configure parameters for the LDAP authentication server.



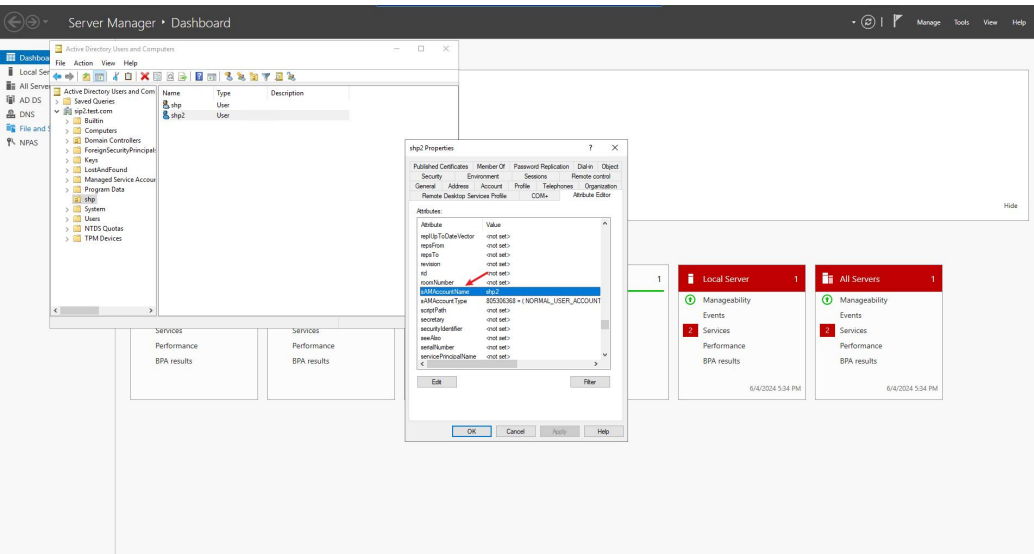
Base DN specifies the domain name and OU information of the AD domain server.



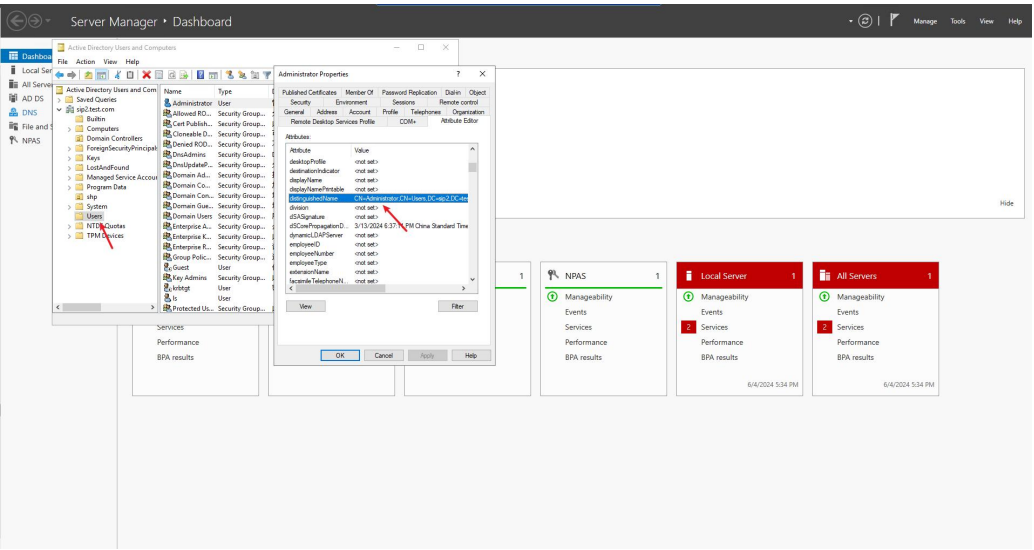
Set **User Filter** based on the standard user filter formats provided by the AD domain server. Examples:

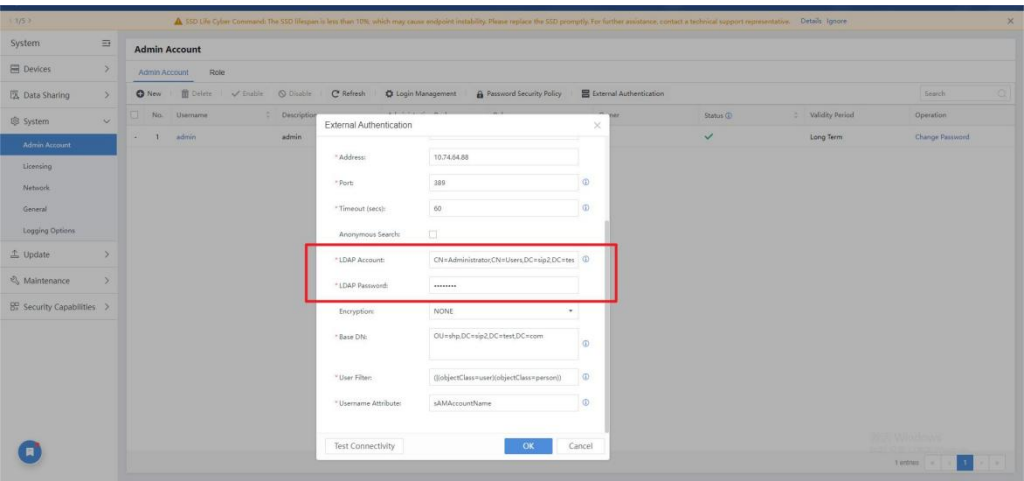
- (objectClass=*): indicates all objects.
- (& (objectCategory=person) (objectClass=user) (! (cn=andy))): indicates all users except "andy" in the "person" category.
- (sn=sm*): indicates all objects whose surnames start with "sm".
- (& (objectCategory=person) (objectClass=contact) (| (sn=Smith) (sn=Johnson))): indicates all contacts surnamed "Smith" or "Johnson".
- (!(email=*))): indicates all objects without email addresses.

Username Attribute specifies the username of a user, which corresponds to the username attribute defined in the AD domain server. The specific configuration may vary depending on the AD domain server. In this example, set **Username Attribute** to sAMAccountName.

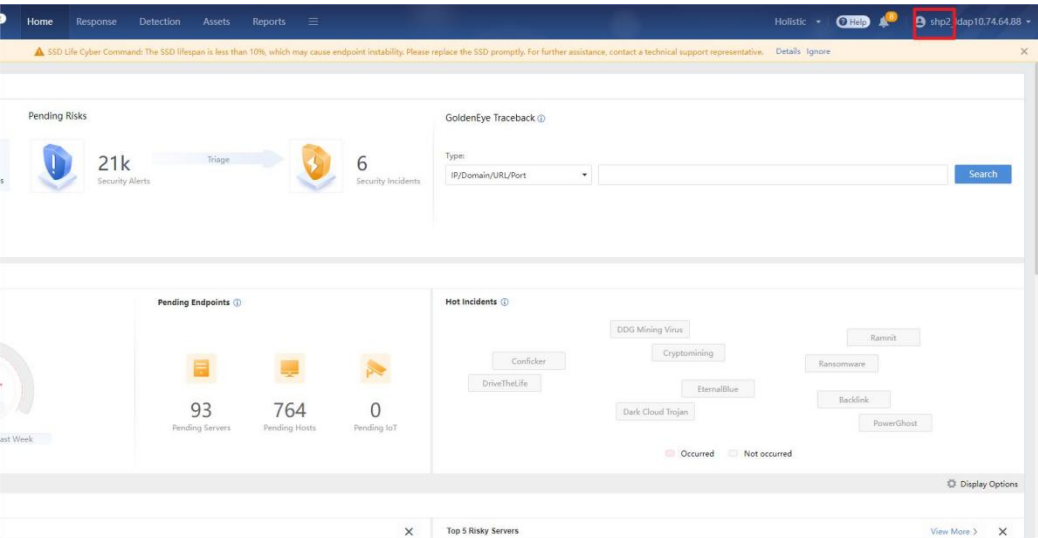


By default, **Anonymous Search** is deselected. In this case, you must specify **LDAP Account** and **LDAP Password** in Cyber Command. Select any AD domain user that satisfies the specified user filter condition, and set **LDAP Account** and **LDAP Password** based on the **distinguishedName** attribute and password defined for the user on the AD domain server.



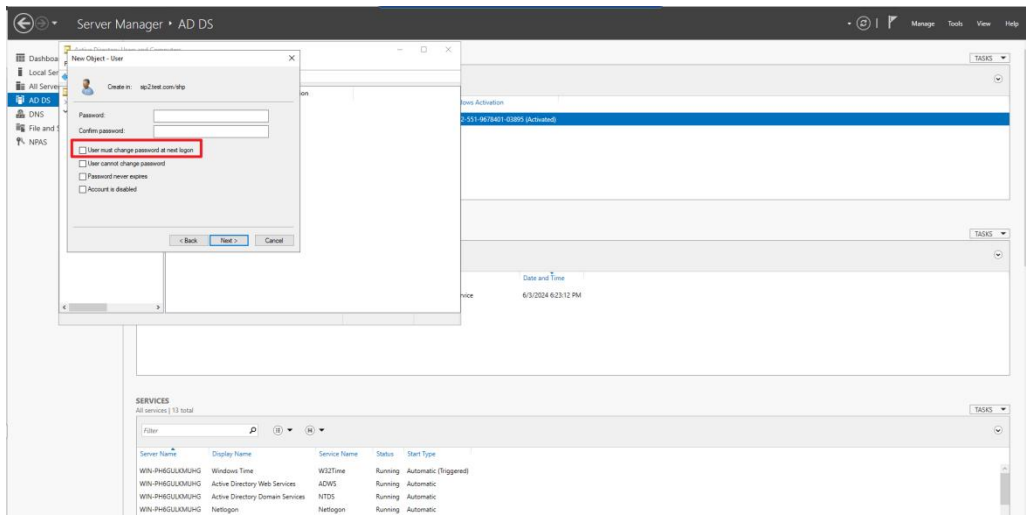


After the configuration passes the connectivity test, click **OK**. Then, you can log in to Cyber Command as an AD domain user that satisfies the specified user filter condition.



Usage Notes

- A user for whom **User must change password at next login** is selected cannot log in to Cyber Command by using this feature.



- LDAP v3 is supported, and Cyber Command is compatible with Active Directory 2012, Active Directory 2019, and Active Directory 2022.
- Troubleshooting can be performed based on the `tail -f /var/log/today/auth_server_idp/error.log` file.

Licensing

View whether the functional license key and license key use time are **correct**. It is divided into **Basic Licenses** and **Function Module Licenses**.

The **Basic Licenses** include the **Platform License**, **Software Upgrade License**, and **Database Upgrade License**.

The **Function Module Licenses** include **Sensor Device License**, **Multifunction License**, and **Access SN Third-Party Correlated Application**.

Licensing

Basic Info

Status: Licensed Manual License Update

Gateway ID: A4CAA7F2

Status: Test

Licensed User: test

Device Version: 3.0.65

Model: vCC-3000

Basic Licenses

Platform License

Licensed

Enable this to use the basic functions provided by ...

Expiration Date: 2023-05-08

Software Upgrade License

Licensed

Keep devices up-to-date. Upgrade License can be ...

Expiration Date: 2023-05-08

Database Upgrade License

Licensed

Keep security databases up to date.

Expiration Date: 2023-05-08

Function Module Licenses

Sensor Device License

Licensed

Enable the connection of Sangfor devices to Cybe...

Sangfor Devices: 100

Expiration Date: 2023-05-08

Multifunction License

Licensed

Enable functions as required. It is recommended t...

UEBA: Licensed

Weakness: Licensed

Traffic Visualization: Licensed

File Threats: Licensed

Expiration Date: 2023-05-08

Access SN for Third-Party Correlated Application

Licensed

After a third-party correlated application is access...

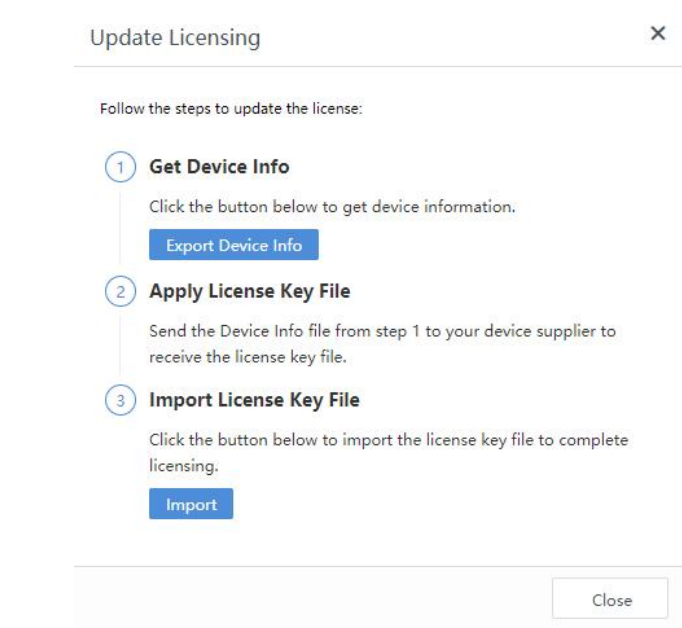
Authorized third-party correlated applications: 100

Expiration Date: 2023-05-08

Version 01 (May 30, 2024)

158

It supports importing the license file by clicking the **Manual License Update**.



Network

It is required to enable the networking interface first and then configure the interface address. Connect the network cable until the networking interface light is on when enabling the network interface.

Network						
Interfaces Static Routes DNS Servers Connectivity Test						
✓ Enable ⚙ Disable ⚙ Cluster Interfaces ⚙ Docker Interface 🔄 Refresh						
☐	No.	Interface Name	Description	IP Address	Status	
☐	1	eth0		10.251.251.252/24 172.17.0.1/24	✓	
☐	2	eth1			✓	

Click the interface name to enter the interface configuration interface, as shown below:

Edit Interface

Status:

☒ Enable

Name:

eth0

Description:

IP Address:

10.251.251.252/24
192.168.1.188/24

OK

Cancel

- **Status:** Check the **Enable** checkbox.
- **IP Address:** Refer to the IP address for configuring the networking interface, and you can configure multiple IP addresses.
- Click **OK** to submit.

Configure the **Static Routes** default route for the STA Device.

Network

Interfaces

Static Routes

DNS Servers

Connectivity Test

New

Delete

Refresh

No.	Dst IP	Netmask	Next-Hop IP	Operation
1	0.0.0.0	0.0.0.0		Delete

Add Static Route

Protocol:

☒ IPv4

☐ IPv6

* Dst IP:

* Netmask:

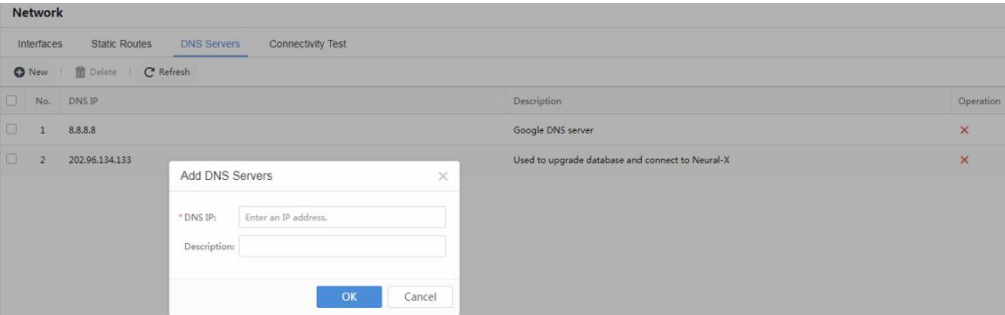
* Next-Hop IP:

OK

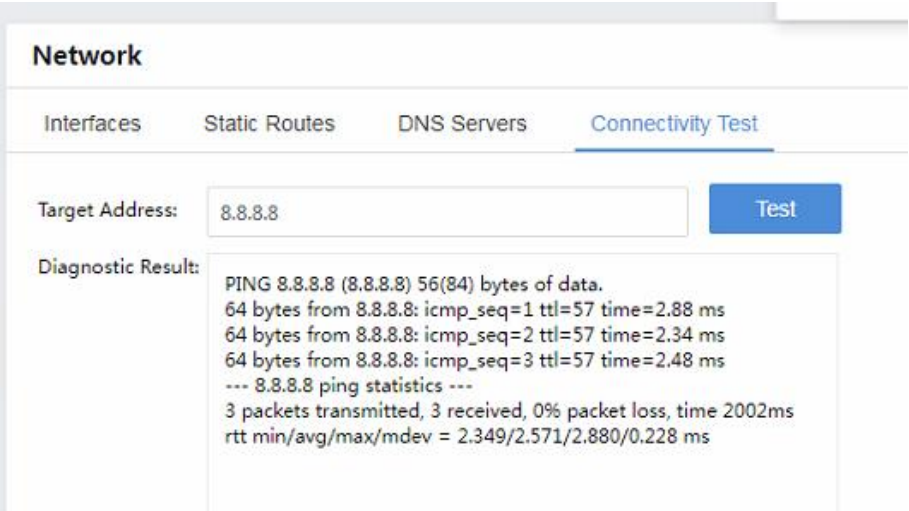
Cancel

After the configuration, click **OK** to submit.

Configure the **DNS Servers** for Cyber Command to resolve domains.



You can take basic ICMP testing for some target IP addresses (not including URL) with **Connectivity Test**.



General

General

Web UI

Mail Server ⓘ

SMS Service

System Time

Privacy Options

Certificate

Inactivity Timeout

* Timeout: 10 (mins)

Remote Control

☒ Temporarily Enable SSH ⓘ

☒ Enable Src IP Access Control ⓘ

One IP per Row

Web Console Protection

☐ Temporarily Disabled

Enabling or disabling Web console protection will interrupt network for 1 minute. The protection will be enabled again 1 day after this option is selected.

☐ Temporarily Disable Shell Semantics Analysis Engine

Enabling or disabling the shell semantics analysis engine will interrupt network for 1 minute. The engine will be enabled again 1 day after this option is selected.

Service Control

☐ Enable ICMP Timestamp Reply

High Performance Mode

☒ Enabled ⓘ

Detection Mode

☒ Standard (to balance detection effect and resource costs during normal operating, engines may encounter delay)

☐ POC (To gain higher detection effect and timely results during POC testing, resource cost will get higher.)

Country/Region

Country/Region: Malaysia

Enterprise Location

* Location: Kuala Lumpur

OK

- **Inactivity Timeout:** WebUI will become inactive after a specific time.
- **Remote Control:** You can **Temporarily Enable SSH** and **Enable Src IP Access Control**.
- **Web Console Protection:** Temporarily disable the web console or temporarily disable Shell Semantics Analysis Engine.
- **Service Control:** You can choose to **Enable ICMP Timestamp Reply**.
- **High Performance Mode:** The mode will enable caching techniques to offer a smoother experience.

- **Detection Mode:** Choose the detection mode.
- **Country/Region:** Select the current Country/Region.

1. Configure **Mail Server** as shown below.

The screenshot shows the 'Mail Server' configuration page. The left sidebar has a 'System' menu with options like 'Admin Account', 'Licensing', 'Network', 'General' (selected), 'Logging Options', 'Update', 'Maintenance', and 'Security Capabilities'. The main content area has tabs for 'Web UI', 'Mail Server', 'SMS Service', 'System Time', 'Privacy Options', 'Certificate', and 'Proxy Server'. The 'Mail Server' tab is active, showing fields for: * Sender Address (xxx@example.com), * Protocol (SMTP), * Mail Server (smtp.example.com), * Port (465), Password (masked), and Proxy Settings (checkbox for 'Enable Proxy Server').

- **Sender Address:** Refer to the email for sending warnings or reports.
- **Protocol:** Select **SMTP** or **Exchange**.
- **Mail Server:** Refer to the email server address for sending the email.
- **Port:** Refer to the port of the email server, which is a 25 port by default.
- **Password:** Refer to the password for logging in to the email address.
- **Proxy Settings:** Check to send email via proxy server.

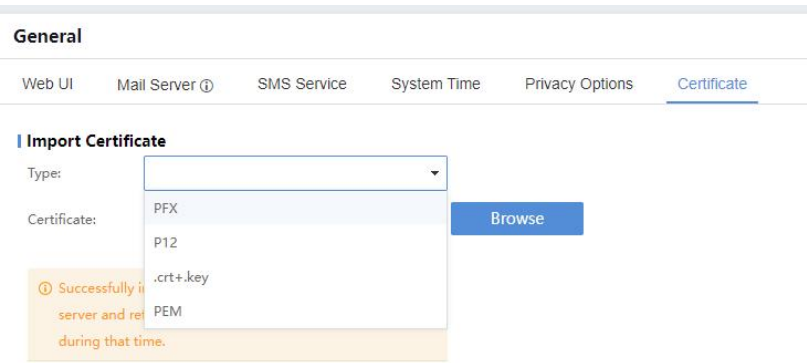
Click **Send Test Email** to test whether the configured email information is correct.

The 'Send Test Email' dialog box is shown. It has a title bar with a close button. The main area has a label '* Recipient Address:' followed by an empty text input field. At the bottom, there are 'OK' and 'Cancel' buttons.

Enter an email address for receiving the email. Click **OK**.

2. Configure the **Certificate** as below:

Cyber Command supports imports **PFX**, **P12**, **.crt + .key**, or **PEM** certificates to the web console as web console certificates.

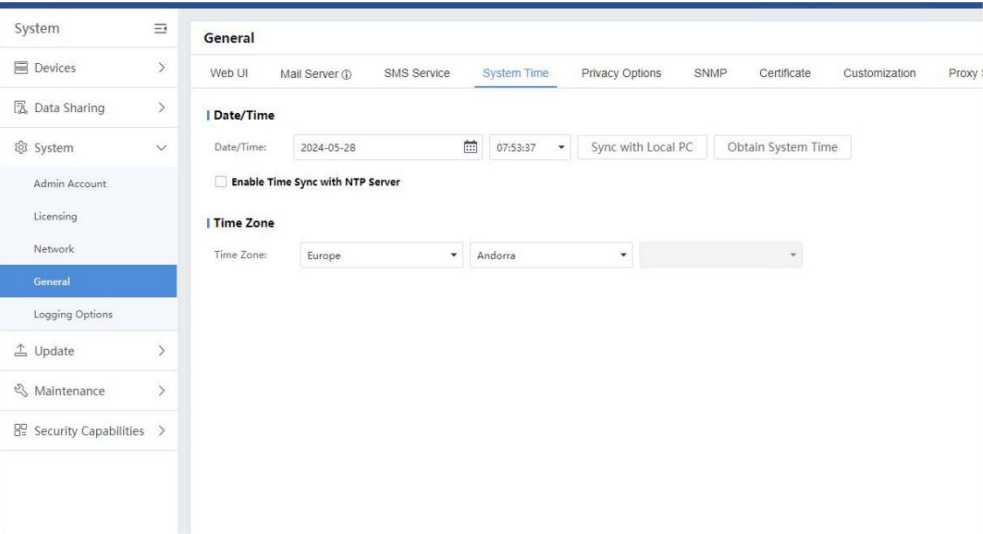


Cyber Command optimizes the system time settings and supports the daylight saving time. Engineers such as security administrators and security O&M experts can customize time settings and configure daylight saving time based on their actual needs.

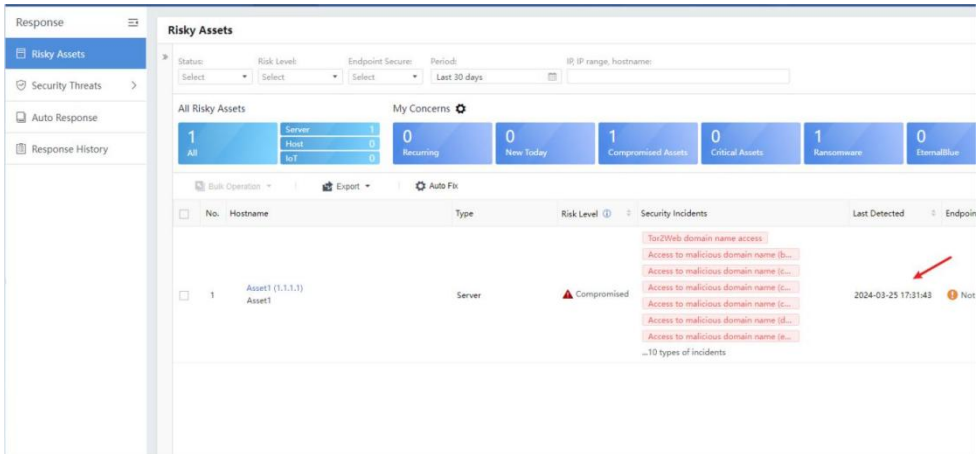
The following content shows how to use this feature.

Steps

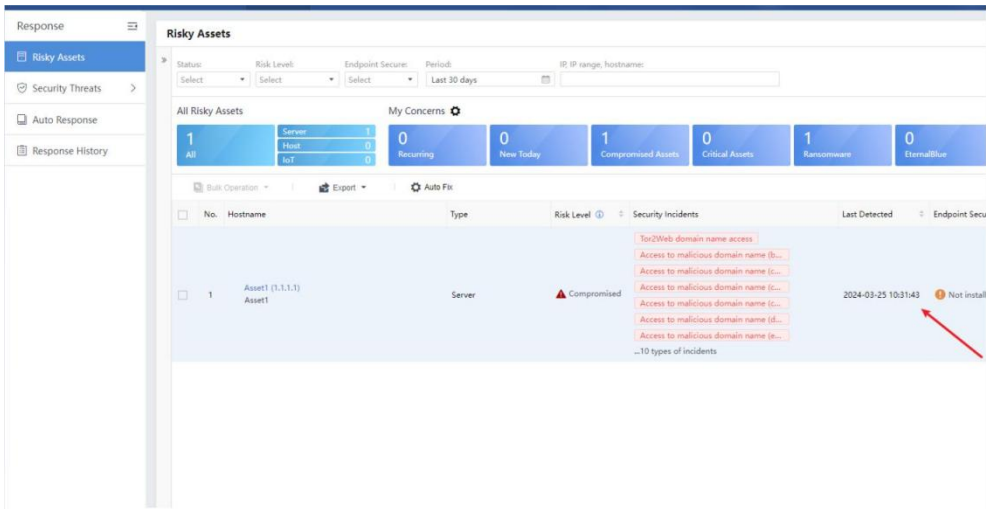
- 1. Go to **System > System > General > System Time**, and configure relevant parameters as needed.



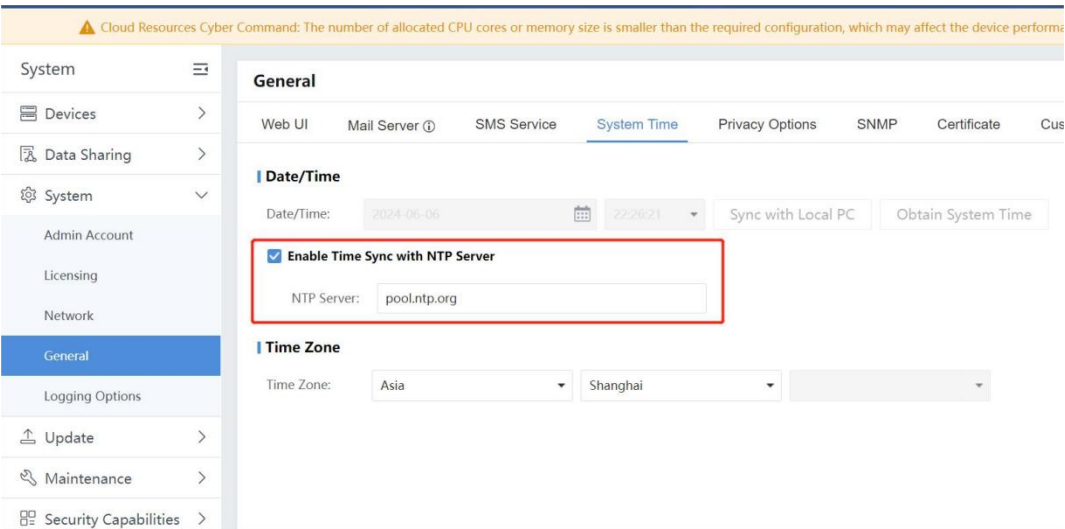
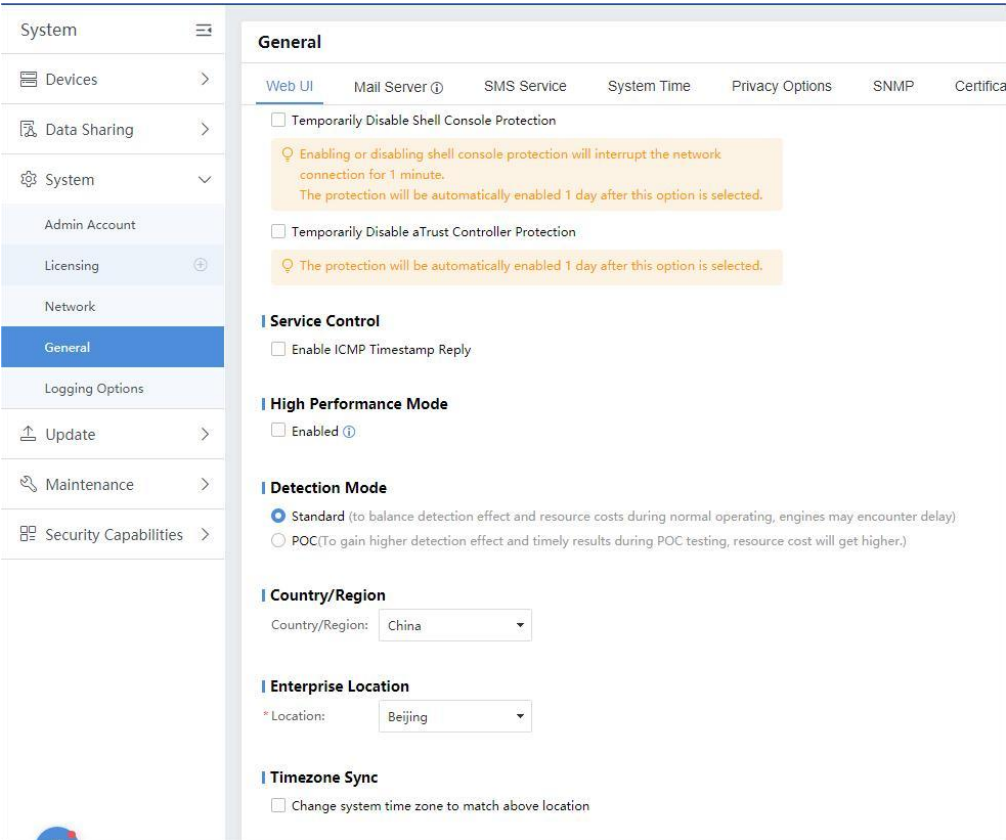
- 2. Go to **Responses > Risky Assets** to view the **Last Detected** time of a risky asset, where the display time is synchronized with the time zone configured for the local device.



After the time zone is changed, the display time is as follows.



3. Go to **System > System > General > Web UI**, and select **Change system time zone to match above location of Timezone Sync**. Then, go to **System > System > General > System Time**, select **Enable Time Sync with NTP Server**, and specify **NTP Server** and **Time Zone**. The time zone of the device is synchronized with the specified time zone.



Logging Options

Set log data recorded by the Cyber Command.

Logging Options

Storage Usage:

2%

Used: 6.80G

Free: 485.20G

Usage Threshold for Cleanup

80

%

Security Incidents

Retention:

Custom

180

days

No limit

Malicious Files

Retention:

Custom

180

days

No limit

Security Logs

Retention:

Custom

180

days

No limit

Advanced

- **Usage Threshold Cleanup:** Logs will be automatically deleted when the stored logs exceed the set ratio.
- **Security Logs:** Including vulnerabilities exploitation, web attacks, botnet, business system weakness, DNS attacks, email security, file security, etc.

Update

This module is used to update the platform's management, STA, and signature database.

System Update

Import the update package through the console, and downgrading is not supported.

System

Devices

System

Update

System Update

Service Packs

Security Databases

Security Engines

Update Options

Maintenance

Security Capabilities

System Update

Packages

Policy options are not configured. Devices cannot communicate with Neural-IT and cannot obtain the latest version information and offline update package. Configure

Cyber Command Update

Version: S153.0.60.0 EN Build20220223

You are using the latest version. Last Updated: -

To update to another version, upload an update package. Import Obtain Offline Update Package

Update Options Update History

STA Update

Last Updated: -

Import Obtain Offline Update Package

Refresh

Update Status: Pending Updating Device name: 0

No.	STA Name	IP Address	Online Status	Current Version	Time Updated	Update Status
1	SANGFOR TS	210.5.180.158	Offline	3.0.25	2021-06-02 06:06:47	Update Successful

1 in all 1 Per Page 10

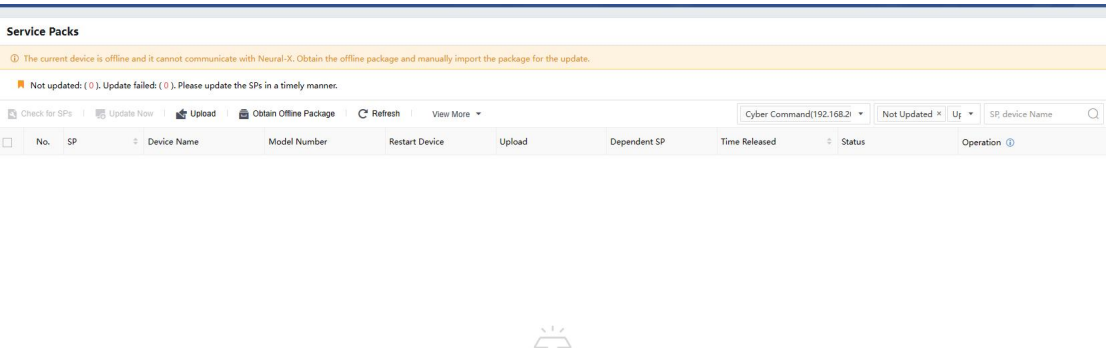


1. STA software update: Detect whether there is a new version on the platform every 10 minutes. When there are multiple STAs, only one can download the update package within

- each period, thereby reducing the impacts on the network by high traffic.
2. STA rule database update: Detect the STA rule database and platform every hour. The STA is not required to access the Internet to update the signature database.

Service Pack Update

Service packs is to shows the service pack file installation status for Cyber Command.



Security Database

The Cyber Command security database can be updated online or through manual import.

System

Correlated Devices

System

Update

CCOM

STA

Security Database

Security Engine

Update Options

Maintenance

Databases

Security Database

Enable Auto Update

Disable Auto Update

Update Browser Proxy

Refresh

No.	Database Name	Current Version	Latest Version	Auto Update in the C/C	Operation	
1	Security Signature Database	2020-03-24	2020-03-24		Update in the Cloud	Manual Update
2	System Update	-	-		Update in the Cloud	Manual Update
3	Security Library	2020-03-17	2020-03-17		Update in the Cloud	Manual Update
4	IOC Threat Intelligence Database	2020-03-25	2020-03-25		Update in the Cloud	Manual Update
5	Hot Event Database	2020-03-24	2020-03-24		Update in the Cloud	Manual Update
6	File Threat Signature Database	2011-01-01	2011-01-01		Update in the Cloud	Manual Update
7	File Analytics Model Database	2019-10-28	2019-10-28		Update in the Cloud	Manual Update
8	Whitelist Database	2020-03-17	2020-03-17		Update in the Cloud	Manual Update

Security Engines

The security engines analyze and locate security risks by recognizing malicious behaviors.

System

Correlated Devices

System

Update

Cyber Command

STA

Security Database

Security Engine

Update Options

Service Packs

Maintenance

Databases

Security Engine

Update in the Cloud | Manual Update | Update by Proxy Browser | Refresh

Enable Auto Update

No.	Engine Name	Current Version	Latest Version
1	Security Log Analysis Engine	2020-12-24	2020-12-24
2	DNS Flow Analytics	2020-12-24	2020-12-24
3	Http Flow Analytics	2021-04-08	2021-04-08
4	Mail Flow Analytics	2020-12-24	2020-12-24
5	SMB Flow Analytics	2020-12-24	2020-12-24
6	Intelligence Correlation	2020-12-30	2020-12-30
7	File Threat Detection	2020-12-24	2020-12-24
8	AD Domain Analytics	2020-12-24	2020-12-24
9	Attack Analytics	2020-12-24	2020-12-24
10	Correlation	2021-04-08	2021-04-08
11	Account Analytics	2021-04-08	2021-04-08
12	Script Analytics	2020-12-24	2020-12-24
13	Weakness Detection	2020-08-05	2020-08-05
14	HTTPS Flow Analytics	2020-12-24	2020-12-24
15	SSH Analytics	2020-12-24	2020-12-24
16	TCP Analytics	2020-12-24	2020-12-24
17	SOCKS Flow Analytics	2020-12-24	2020-12-24

19 entries

Update Options

Configure the Internet settings of Cyber Command to access the **Update Server**.

Update Options

Update Server

Server: Default Server Test Validity

Server 4

121.46.26.221

Proxy Settings

☐ Enable Proxy Server

The following **Update Servers** are involved:

- Server 1: update1.sangfor.net
- Server 2: update2.sangfor.net
- Server 3: update3.sangfor.net
- Server 4: 121.46.26.221

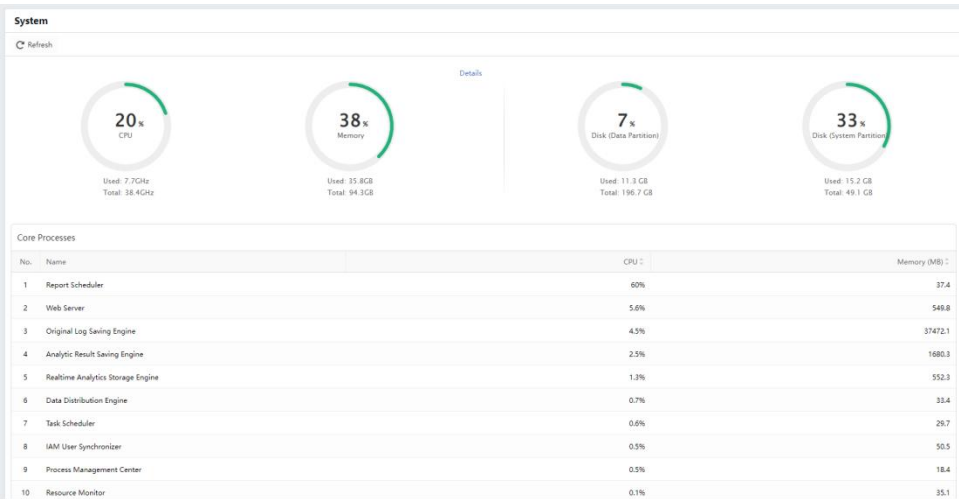
Proxy Settings: The user can use proxy settings when an HTTP proxy server is in the network. Click **OK**.

Maintenance

This module is designed for engineers to perform troubleshooting.

System

The user can view the usage of the platform CPU, memory, disk (data partition), and disk (system partition).



Data Backup

Back up security logs in Cyber Command, and upload them to the FTP server.

The Data Backup configuration window includes a table of scheduled tasks and an "Add Backup Task" modal form.

Scheduled Tasks Table:

No.	Name	Interval	Start Time	Last Backup	Status
[Empty row]					

Add Backup Task Modal Form:

- Name:** [Text input field]
- Path:** [FTP path only] [Test Connectivity]
- Username:** [Text input field]
- Password:** [Text input field]
- Start Time:** 2022-04-26 [Calendar icon]
- Interval:** ☒ Every day
- Next backup will start at:** 2022-04-27 02:00
- Buttons:** OK, Cancel

- **Name:** The name of the policy.
- **Path:** Configure a path for storing backup files on the FTP server.
- **Username:** Refer to the account of the FTP server.
- **Password:** Refer to the password of the FTP server account.
- **Start Time:** Select the time for starting the backup.
- **Interval:** Back up every day.

Restore/Restart

It is to restore factory settings and restart Cyber Command. Click **Restore Factory Defaults**, and all data and settings of the platform will be deleted. Please be cautious.

Click **Restart** to restart the Cyber Command. Since Cyber Command is deployed in a one-arm mode, it will not impact the network.

Restore/Restart

Restore Factory Defaults

Restart Cyber Command

Restore User Configuration

Restore Factory Defaults

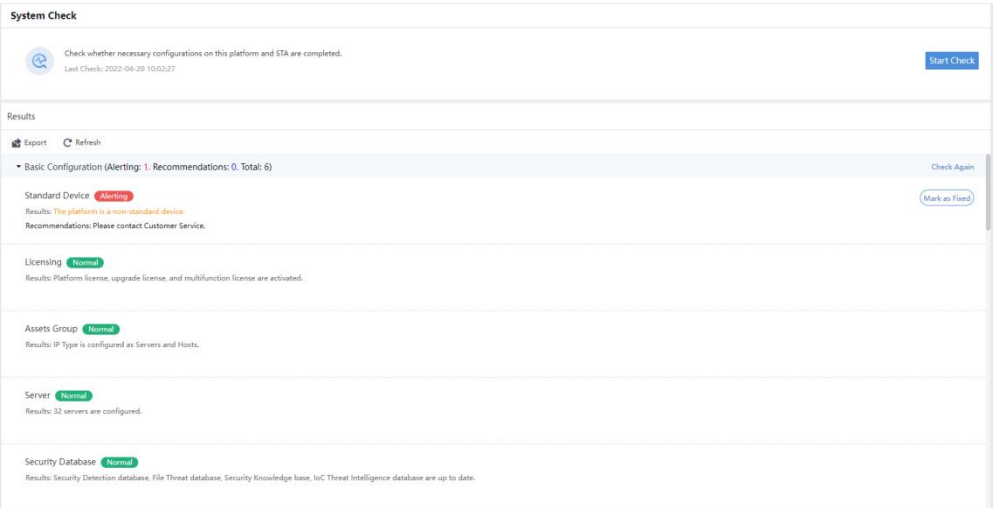
Restart

Import User Configuration

Export User Configuration

System Check

One-click system health check to see whether the platform and STA configurations are complete. If the platform is just installed or the device is reporting alerts, please pay attention to the items.



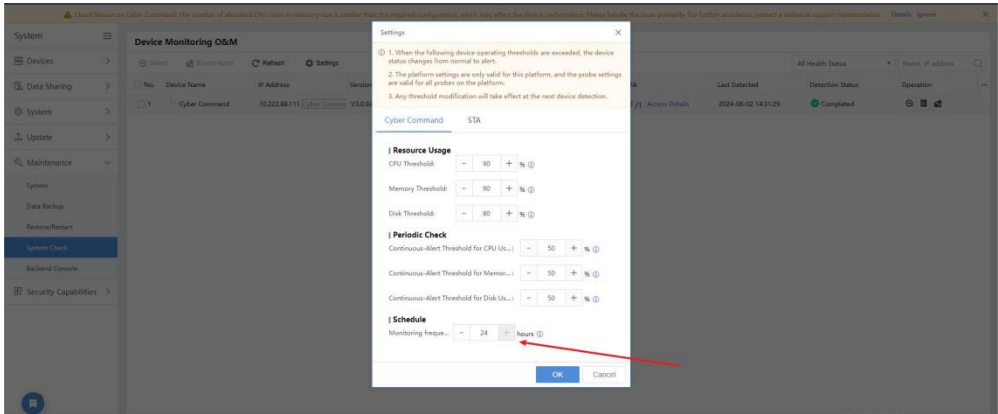
- **Basic Configuration:** Check basic configuration items, including standard device inspection, license key, monitored internal IP address group, business system/server, rule database, and log analysis engine.
- **Licensing:** Check whether the Platform license, upgrade license, and multifunction license are activated.
- **Connected Devices:** Inspect the connectivity of the platform access port and access device.
- **Traffic Detection:** Inspect whether the traffic image is correct. The monitored internal IP address group shall be configured in advance.
- **Proxy Detection:** Recognize the proxy server.

Hardware Health Monitoring

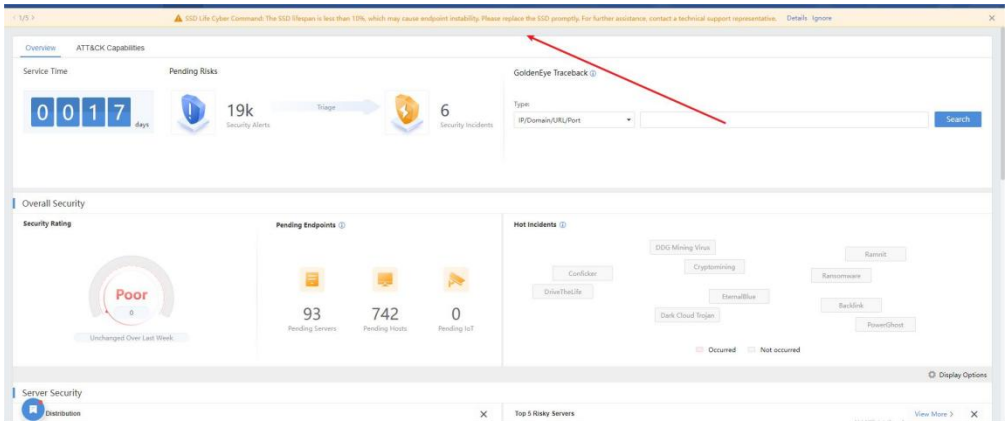
Cyber Command can periodically perform O&M checks on a redundant array of independent disks (RAID) cards, disks, network interface controllers (NICs), and memories of hardware devices. If a hardware failure is detected, an alert is generated and displayed in the banner at the top of the home page.

The following content describes how to use this feature.

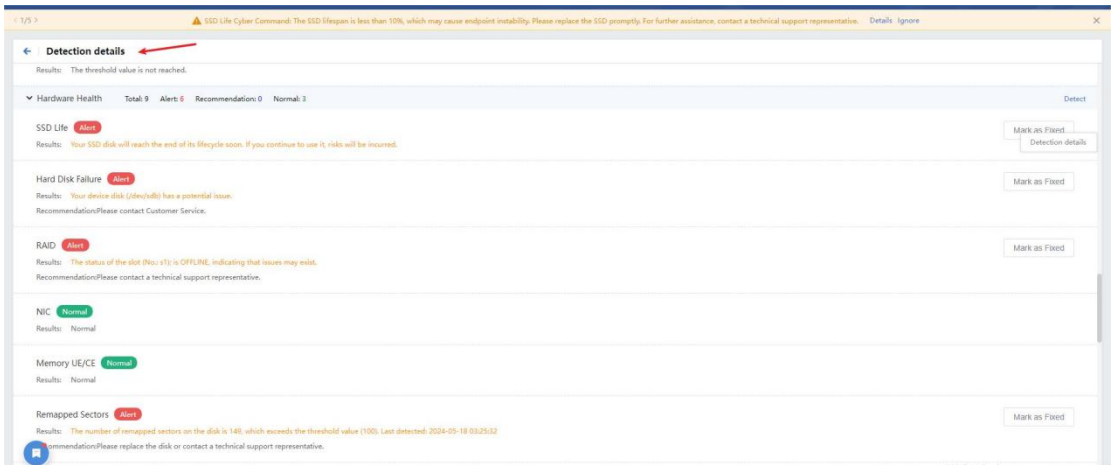
1. Go to **System > Maintenance > System Check**, click **Settings**, and configure **Schedule** as needed.



2. If a hardware failure is detected during the check, an alert is generated and displayed in the banner at the top of the home page.



3. To view the newly added hardware check items, click **Detection details** in the **Operation** column of the selected device on the **Device Monitoring O&M** page. On the **Detection details** page that appears, view the newly added hardware check items in the **Hardware Health** section, as shown in the following figure.



Usage Notes

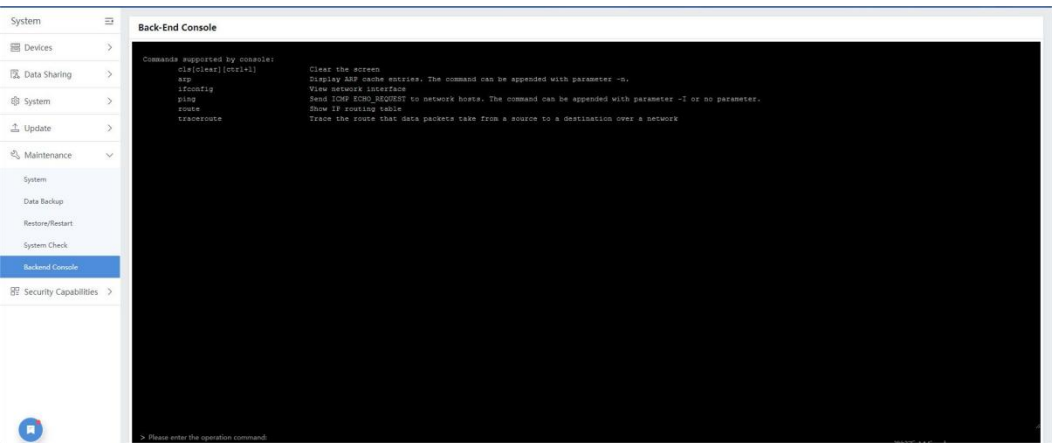
- This feature is unavailable for products in virtualization deployment.

- An ignored alert does not appear in the banner within 7 days even if the same hardware failure is repeatedly detected.

Backend Console

Cyber Command provides the backend console for engineers such as security administrators and security O&M experts to enter and run commands.

To use this feature, go to **System > Maintenance > Backend Console**, and enter and run a command supported by the console. For more information about the commands supported by the console, enter and run the help command.



Usage Notes

- The execution duration of a command cannot exceed 2 minutes. Otherwise, an execution failure is returned.
- If the entered command is not supported by the console, the error message "Invalid Command" is returned.
- A command starts to run only after the command execution result of a previous command is returned. You cannot run multiple commands concurrently in the console.
- The redirection from another page to the backend console clears historical command execution records.

3.11.3 Security Capabilities

Security capability configuration includes **Security Database, Whitelists, File Detection**, and **Weak Password Rules**.

Detection Engine

The detection engine mainly implements the five built-in detection engines: **Rule Detection Engine**, **Intelligence Detection Engine**, **File Analysis Engine**, **Attack Analysis**, and **Abnormal Behavior Engine**, to perform operations such as rule editing, display query, and addition.

Display query

On the **System > Security Capability > Detection Engine** page, each detection engine identifies the number of rules and engine profiles. Place the mouse on the **Threat Name** position to see the specific content. The attributes of each rule in the list include **Alert ID**, **Incident ID**, **Threat Name**, **Severity**, **Threat Type**, **Time Created**, **Status**, **Security Alert**, **Security Incidents**, **Operation**, etc., as shown in the figure below.

Security Alert/Incidents Detection Engine

Intelligence Detection Engine
Total Rules: 1588

File Analytics
Total Rules: 51

Attack Analytics
Total Rules: 710

Abnormal Behavior Engine
Total Rules: 218

Logic of the routine operation detection mode: Generate security incidents for alerts with high risk and definite threats. You can customize the policy for alert and event generation and restore all configurations to defaults. Restore Defaults

Engine Type	No.	Alert ID	Event ID	Threat Name	Severity	Threat Type	Time Created	Status	Security Alerts	Security Incidents	Operation
Intelligence Detect...	1	217950036	117950036	Infected with a mini...	High	Cryptomining	2021-09-30 17:58:46	✓	Generate	Do Not Generate	
Ransomware Intell...	2	217910006	117910006	Infected with ransom...	High	Ransomware	2021-06-07 23:17:24	✓	Generate	Do Not Generate	
Cryptomining Intell...	3	217910005	117910005	Ransomware attack	High	Ransomware	2021-06-07 23:17:24	✓	Generate	Do Not Generate	
Normal Virus Intell...	4	217910004	117910004	Infected with ransom...	High	Ransomware	2021-06-07 23:17:24	✓	Generate	Do Not Generate	
Custom Threat Int...	5	217860005	117860005	Outgoing data detect...	High	DNS Tunneling	2021-12-17 09:17:17	✓	Generate	Do Not Generate	
Others	6	217830015	117830015	Infected with ransom...	High	Ransomware	2021-09-24 17:07:18	✓	Generate	Generate	
File Analytics	7	217830014	117830014	Accessed website in...	High	Cryptomining	2021-09-16 08:47:36	✓	Generate	Do Not Generate	
Attack Analytics	8	217830013	117830013	Mining code impla...	High	Cryptomining	2021-09-17 15:09:17	✓	Generate	Do Not Generate	
Reconnaissance D...	9	217830006	117830006	Infected with Locky...	High	Ransomware	2021-09-24 17:07:48	✓	Generate	Do Not Generate	
Email Detection M...	10	217830003	117830003	Infected with a mini...	High	Cryptomining	2022-04-18 14:49:18	✓	Generate	Generate	
Tunnel Detection ...	11	217773002	117773002	Encrypted mining tr...	High	Cryptomining	2022-04-21 10:03:14	✓	Generate	Generate	
Lateral Movement ...	12	217640211	117640211	Communication via...	High	WebShell Access	2021-09-24 17:03:06	✓	Generate	Do Not Generate	
Backdoor Commu...	13	217640210	117640210	Communication via...	High	WebShell Access	2021-09-24 17:03:05	✓	Generate	Do Not Generate	
Illegal Profit Dete...	14	217640209	117640209	Communication via...	High	WebShell Managemen...	2021-09-24 17:03:02	✓	Generate	Do Not Generate	
Database Attack D...	15	217640208	117640208	Communication via...	High	WebShell Managemen...	2021-09-24 17:03:01	✓	Generate	Do Not Generate	
Attack and Exploit ...											
Others											
Abnormal Behavi...											
Abnormal Behavi...											

- **Severity:** divided into High, Medium, and Low.
- **Threat type:** consistent with the classification of Security Incidents and Security Alert threats in the processing center.
- **Library type:** the classification name of the rule library.
- **Status:** You can manually modify the status of each rule. ✓ represents the enabled status, and ⛔ represents the disabled status.

The rule list can be classified and displayed according to the **Threat type** and **Severity**, and the rules can be fuzzy searched according to the keyword/rule ID, as shown in the figure below.

Security Detection Engines

Intelligence Detection Engine ⓘ

Total Rules: 1584k

File Analytics ⓘ

Total Rules: 50

Attack Analytics ⓘ

Total Rules: 622

Abnormal Behavior Engine ⓘ

Total Rules: 219

Logic of the routine operation detection mode: Generate security incidents for alerts with high risk and definite threats. You can customize the policy for alert and incident generation and restore all configurations to defaults.

Restore Defaults

Engine Type

Q

New

Enable

Disable

Restore

All Alerts

All Incidents

Hack

X

Q

All	☐	No.	Alert ID	Incident ID	Threat Name	Severity	Threat Type	Time Created	Status	Security Alerts	Security Incidents	Operation
Intelligence Detect...	☐	1	2145001209	1145001209	Infected with cobalt...	High	Others	2022-07-05 09:54:25	✓	Generate	Do Not Generate	
Ransomware Intell...	☐	2	2145001065	1145001065	Infected with drin...	High	Others	2022-07-05 09:54:30	✓	Generate	Do Not Generate	
Cryptomining Intell...	☐	3	2145000964	1145000964	Infected with purp...	High	Others	2022-07-05 09:54:31	✓	Generate	Do Not Generate	
Normal Virus Intell...	☐	4	2145000902	1145000902	Infected with blaco...	High	Others	2022-07-05 09:54:34	✓	Generate	Do Not Generate	
Custom Threat Inte...	☐	5	2145000820	1145000820	Infected with cano...	High	Others	2022-07-05 11:05:53	✓	Generate	Do Not Generate	
Others	☐	6	2145000518	1145000518	Infected with remot...	High	Others	2022-07-05 09:54:24	✓	Generate	Do Not Generate	
File Analytics	☐	7	2145000482	1145000482	Infected with mimik...	High	Others	2022-07-05 09:54:36	✓	Generate	Do Not Generate	
Attack Analytics	☐	8	2145000464	1145000464	Infected with noob...	High	Others	2022-07-05 09:54:25	✓	Generate	Do Not Generate	
Abnormal Behavio...	☐	9	2145000457	1145000457	Infected with pros...	High	Others	2022-07-05 09:54:23	✓	Generate	Do Not Generate	
	☐	10	2145000304	1145000304	Infected with winac...	High	Others	2022-07-05 09:54:29	✓	Generate	Do Not Generate	
	☐	11	2145000172	1145000172	Infected with pony...	High	Others	2022-07-05 09:54:33	✓	Generate	Do Not Generate	
	☐	12	2140111883	1140111883	Infected with TA210...	High	Data Theft Program	2022-07-05 11:05:51	✓	Generate	Do Not Generate	
	☐	13	2140061606	1140061606	Infected with Crypt...	High	Cryptomining	2022-07-05 09:54:25	✓	Generate	Generate	
	☐	14	2140050888	1140050888	Infected with Hacke...	High	Trojan	2022-07-05 11:05:48	✓	Generate	Generate	

You can also perform a fuzzy search in the search bar based on the keywords, as shown in the figure below.

Detection Engines

Rule Detection Engine ⓘ

Total Rules: 19k

Intelligence Detection Engine ⓘ

Total Rules: 1448k

File Analytics ⓘ

Total Rules: 20

Engines

Q

New

Enable

Disable

Realtime

All

Rule Detection Eng...

Realtime Vulnerabi...

☐	No.	Rule ID	Threat Name	Severity	Threat Type
☐	1	80020004	Backlink Injection	High	Backlink
☐	2	80020002	Backlink Injection	High	Backlink
☐	3	80020001	Backlink Injection	High	Backlink
☐	4	80010007	Web server weak password	High	Weak Password
☐	5	80010006	TELNET server weak password	High	Weak Password
☐	6	80010005	SMTP server weak password	High	Weak Password
☐	7	80010004	POP3 server weak password	High	Weak Password

In the rule list, you can click the of each rule to edit the rule.

Edit the Rule

On the **System Settings > Security Capability Configuration > Detection Engine page**, select one or more rules and click **Enable**, **Disable** to enable/disable in batches, as shown in the figure below.

Security Detection Engines

Intelligence Detection Engine ⓘ

Total Rules: 1584k

File Analytics ⓘ

Total Rules: 50

Attack Analytics ⓘ

Total Rules: 622

Abnormal Behavior Engine ⓘ

Total Rules: 219

Logic of the routine operation detection mode: Generate security incidents for alerts with high risk and definite threats. You can customize the policy for alert and incident generation and restore all configurations to defaults.

Restore Defaults

Engine Type

Q

New

Enable

Disable

Restore

All Alerts

All Incidents

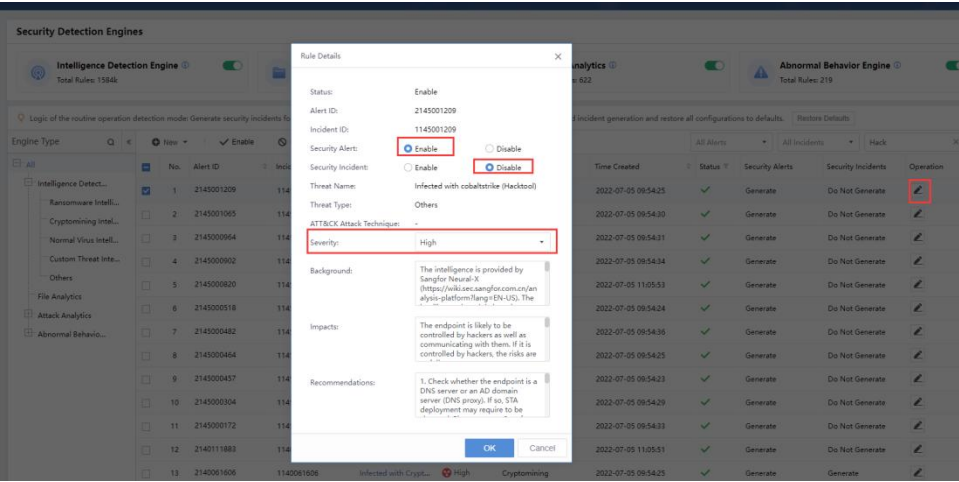
Hack

X

Q

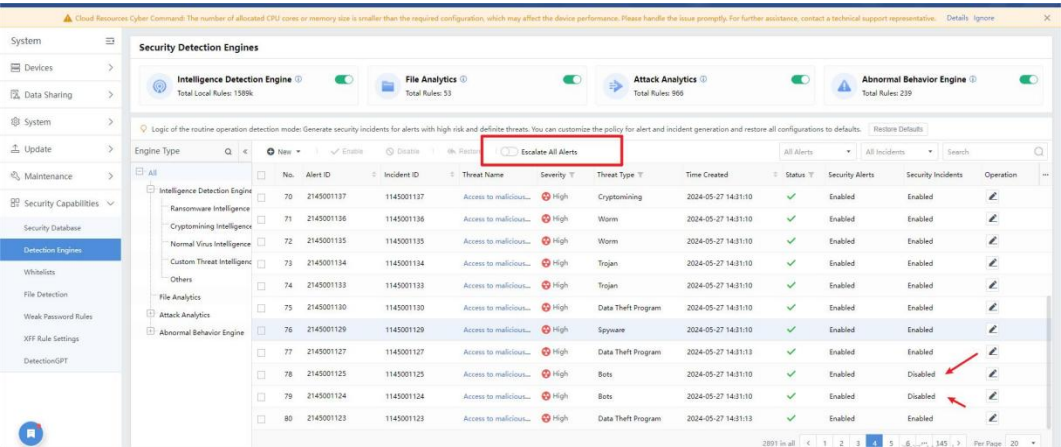
All	☐	No.	Alert ID	Incident ID	Threat Name	Severity	Threat Type	Time Created	Status	Security Alerts	Security Incidents	Operation
Intelligence Detect...	☒	1	2145001209	1145001209	Infected with cobalt...	High	Others	2022-07-05 09:54:25	✓	Generate	Do Not Generate	
Ransomware Intell...	☒	2	2145001065	1145001065	Infected with drin...	High	Others	2022-07-05 09:54:30	✓	Generate	Do Not Generate	
Cryptomining Intell...	☒	3	2145000964	1145000964	Infected with purp...	High	Others	2022-07-05 09:54:31	✓	Generate	Do Not Generate	
Normal Virus Intell...	☐	4	2145000902	1145000902	Infected with blaco...	High	Others	2022-07-05 09:54:34	✓	Generate	Do Not Generate	
Custom Threat Inte...	☐	5	2145000820	1145000820	Infected with cano...	High	Others	2022-07-05 11:05:53	✓	Generate	Do Not Generate	
Others	☐	6	2145000518	1145000518	Infected with remot...	High	Others	2022-07-05 09:54:24	✓	Generate	Do Not Generate	
File Analytics	☐	7	2145000482	1145000482	Infected with mimik...	High	Others	2022-07-05 09:54:36	✓	Generate	Do Not Generate	
Attack Analytics	☐	8	2145000464	1145000464	Infected with noob...	High	Others	2022-07-05 09:54:25	✓	Generate	Do Not Generate	

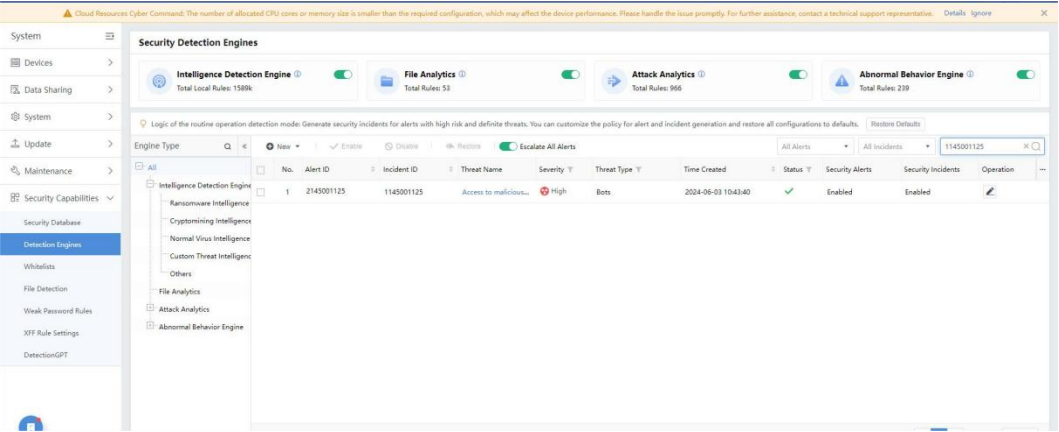
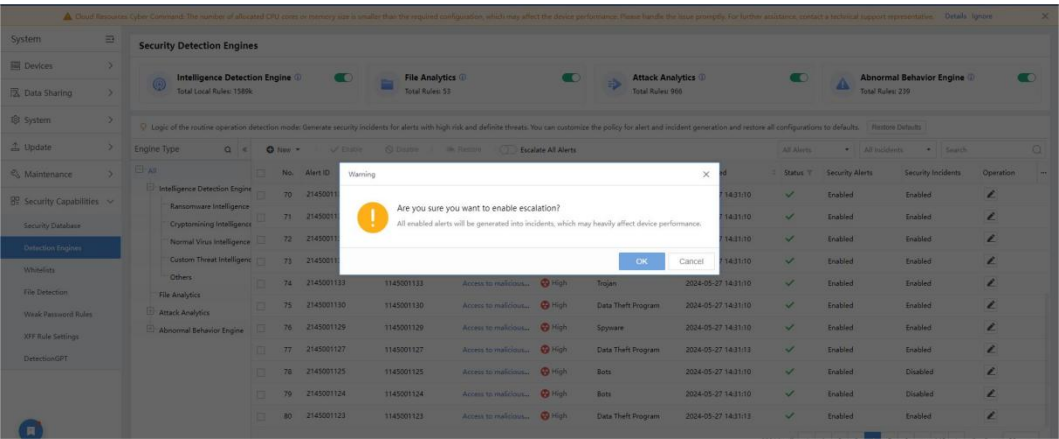
Click the Edit icon to enter the rule details page, including **Status**, **Rule ID**, **Threat Name**, **Threat Type**, **Impacts**, **Severity**, etc. You can manually select **Enabled** or **Disabled**, or select the **Severity** level from the drop-down list, as shown in the figure below.



Escalate All Alerts

Cyber Command provides the **Escalate All Alerts** feature. Security administrators and security O&M experts can go to **System > Security Capabilities > Detection Engines** to enable the **Escalate All Alerts** feature to generate security events based on the security rules.





After you disable the **Escalate All Alerts** feature, the configuration is automatically restored to the previous state where the feature is not enabled, and custom changes made to specific rules after the feature is enabled are retained.

Custom Intelligence

On the **System Settings > Security Capability** page, click **New** and select **Custom Intelligence**, as shown in the figure below.

Rule Details

Status:

Enable

Security Alert:

Enable

Disable

Security Incident:

Enable

Disable

Intelligence Type:

Domain Name

* Intelligence Indicator:

Import File

One entry per row, e.g., www.google.com

Threat Type:

Trojan

Severity:

High

Intelligence Source:

Specify the intelligence source.

Save and Add

OK

Cancel

- **Status:** Enabled by default.
- **Security Alert:** Select **Enabled** to generate the security alert.
- **Security Incident:** Select **Enabled** to generate the security incident.
- **Intelligence Type:** Choose the intelligence type.
- **Intelligence Indication:** Import the .txt file up to 50000 IOCs.
- **Threat Type:** Select the threat type.
- **Severity:** The Severity of the rules is divided into **High**, **Medium**, and **Low**.
- **Intelligence Source:** Specify the Intelligence source.

Whitelists

Add proxy servers, missed scanning devices, and other devices judged to be known business behaviors into the whitelist. The whitelist includes a security whitelist and

an audit whitelist. The overview page is shown below.



- **Audit whitelist:** Traffic that matches the whitelist will not be audited.
- **Security whitelist:** No alerts or events will be generated for the logs that match the whitelist. The platform no longer generates corresponding alerts and events, including the Security Alert whitelist and vulnerability monitoring whitelist, as shown in the figure below.

Security Whitelist

Audit Whitelist

Alert Whitelist

Weakness Scan Whitelist

Add

Import

Export

Enable

Disable

Delete

Refresh

☐	No.	Src IP	Src Type	Dst IP	Dst Type	Dst Port	Domain Name/URL	Threat Type
☐	1	192.168.20.1-19...	-	-	-	-	-	All

- **Analysis:** The stage of generating Security Alerts and then generating Security Incidents.

1. Create a Security Whitelist

The security whitelist is suitable for scenarios where Security Alerts or Security Incidents are whitened and adjusted at the log level.

2. Add Whitelist Entry

On the **Security Capability > Whitelists** page, click **Security Whitelist**, select the **Alert Whitelist** subtab, and click **Add** to enter the **Add Security Alert Whitelist** page.

Add Security Alert Whitelist

Notes:
1. If multiple conditions are specified, the whitelist entry will take effect only when all the conditions are met.
2. After the whitelist entry is added, no alert will be triggered for the logs hitting this entry.

*Threat Type:

Rule ID:

Src IP:

Src Type:

Dst IP:

Dst Type:

Dst Port:

Separate ports with comma

Domain Name/URL:

*Apply To:

All

*Schedule:

Never Expire

Remarks:

OK

Cancel

- **Src IP:** After added, data with this IP as the source will not record alerts.

Version 01 (May 30, 2024)

180

- **Dst IP:** After added, data with the purpose of this IP will not record alerts.
- **Domain Name/URL:** After joining, no alert will be recorded when accessing the data of the domain name/URL.
- **Threat Type:** matched alert classification.
- **Rule ID:** No alert will be recorded if the corresponding rule ID is matched.
- **Apply to:** The effective range of the whitelist applied.
- **Remarks:** Fill in the remark information.

A fuzzy search can be performed, as shown in the figure below.

Add Security Alert Whitelist

Notes:
1. If multiple conditions are specified, the whitelist entry will take effect only when all the conditions are met.
2. After the whitelist entry is added, no alert will be triggered for the logs hitting this entry.

*Threat Type:

Search

All

Weaknesses Risk

Access Risk

Service Detection

Endpoint Detection

Website Attack

Backdoor Communication

Account Attack

Rule ID:

Src Type:

Dst Type:

Domain Name/URL:

*Schedule:

Never Expire

Src IP:

Dst IP:

Dst Port:

*Apply To:

Remarks:

OK

Cancel

3. Import and Export Configuration

You can import and export the Alert whitelist configuration in the .xlsx file.

Import File:

Security Whitelist

Audit Whitelist

Alert Whitelist

Weakness Scan Whitelist

Add

Import

No.	Src IP	Src	Domain Name/URL
1	192.168.20.1-19...		

Browse

Select a .xlsx file Sample File

Select

OK

Cancel

Version 01 (May 30, 2024)

181

Export File:

Security Whitelist

Audit Whitelist

Alert Whitelist

Weakness Scan Whitelist

Add

Import

Export

Enable

Disable

Delete

☐	No.	Src IP	Src Type	Dst IP	Dst Type	Dst
☐	1	192.168.20.1-19...	-	-	-	-



1. There is a one-to-one correspondence between the types of alerts on the page and the types of threats in the Security Incidents/Security Alert in the handling center.
2. Multi-condition combination, the whitelist will only take effect after each condition is hit.

Weakness Scan Whitelist

Under the **Weakness Scan Whitelist** sub-tab, click **Add** to enter the new Weakness Scan Whitelist page, enter the IP address, URL, username, rule ID, asset group, risk type, and other information, and click **OK**, as shown below.

Add Whitelist Entry

* IP Address:

e.g., 192.168.8.80 or 2005::1

URL:

One entry per row, e.g., qiye.163.com/login

Username:

Rule ID:

* Asset Group:

All

* Risk Type:

☐ Exploit

☐ Improper Configuration

☐ Weak Password

☐ Unencrypted Web Traffic

Remarks:

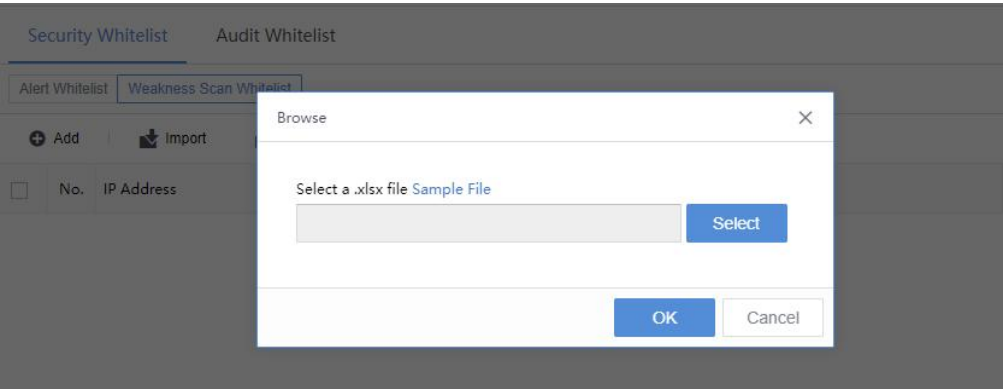
OK

Cancel

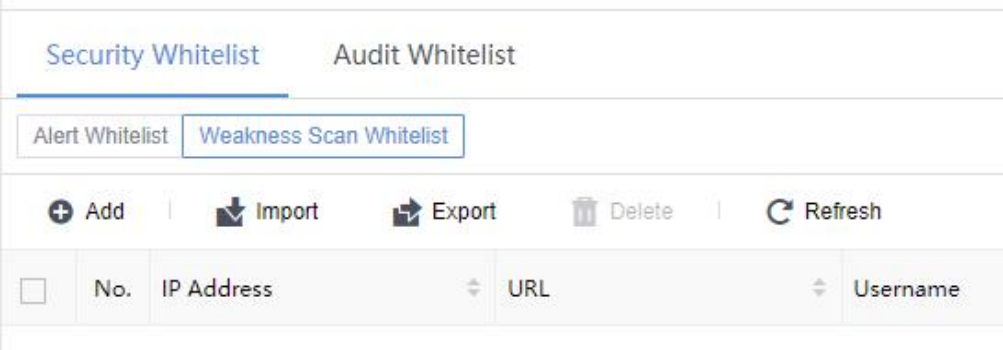
Import and Export

You can import and export the **Weakness Scan Whitelist** configuration in the .xlsx file.

Import file:



Export File:



Audit Whitelist

The audit whitelist scenario is suitable for whitening logs at the traffic level. The whitelisted IP addresses will not generate logs. Else, it will generate Security Alerts and Security Incidents.

On the **System > Security Capabilities > Whitelist** page, under the **Audit Whitelist** sub-tab, click **Add** to enter the **Add Whitelist Entry** dialog box. Next, fill in the source IP, destination IP, log type, and other information, as shown below.

Add Whitelist Entry

Description:

1. If multiple conditions are specified, the whitelist will take effect only when all the conditions are met.
2. The traffic that matches this whitelist entry will not be audited.
3. Only Stealth Threat Analytics (STA) V3.0.34 or later is supported. When STA is connected to two platforms, STA takes effect for the audit whitelist of only the primary platform.

Src IP:

Src Port:

Multiple source ports can be separated with comm

Dst IP:

Dst Port:

Separate ports with comma

Log Type:

All

Remarks:

OK

Cancel

In the **Risk Type** drop-down list, you can perform a fuzzy search based on keywords, as shown in the figure below.

Add Whitelist Entry

* IP Address:

e.g., 192.168.8.80 or 2005::1

URL:

One entry per row, e.g., qiye.163.com/login

Username:

Rule ID:

* Asset Group:

All

* Risk Type:

Search

All

Internal IP Range

Demo Environment

Production Environment

Testing Environment

bs

Remarks:

- **Source IP:** After being added, the data with this IP as the source will not be recorded in the log.
- **Destination IP:** After being added, the data of the destination IP will not be recorded in the log.
- **Log type:** The category of the matched log.
- **Remarks:** Fill in the remark information.

Import and Export Configuration

You can import and export the Audit whitelist configuration in the .xlsx format.

Import File:

Security Whitelist

Audit Whitelist

Add

Import

Export

No.

Src IP

Src Port

Browse

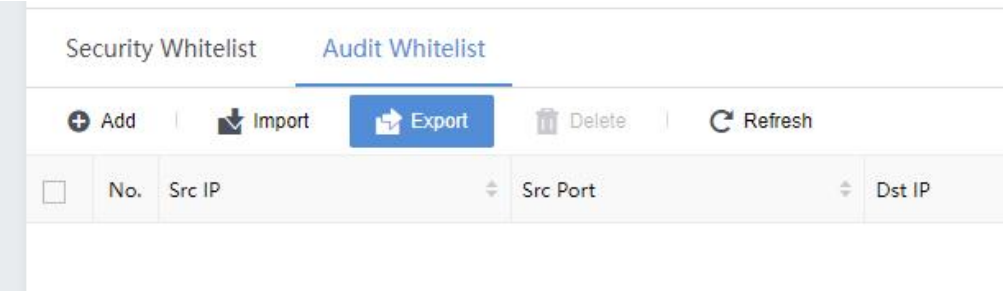
Select a .xlsx file [Sample File](#)

Select

OK

Cancel

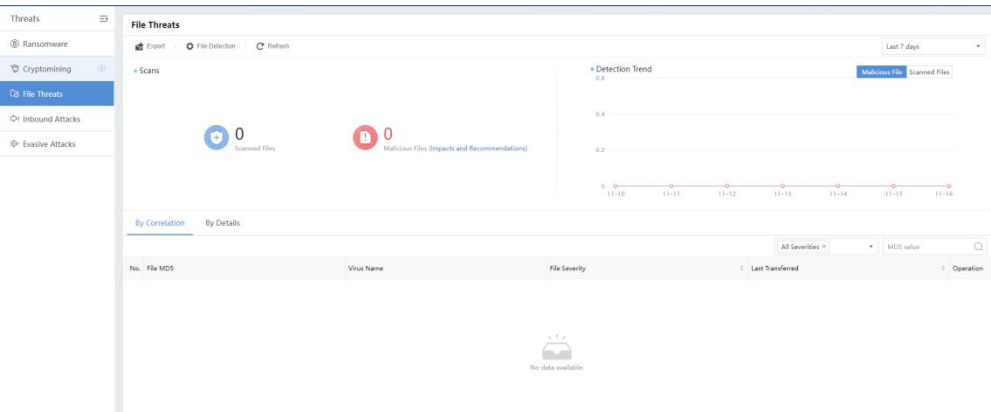
Export File:



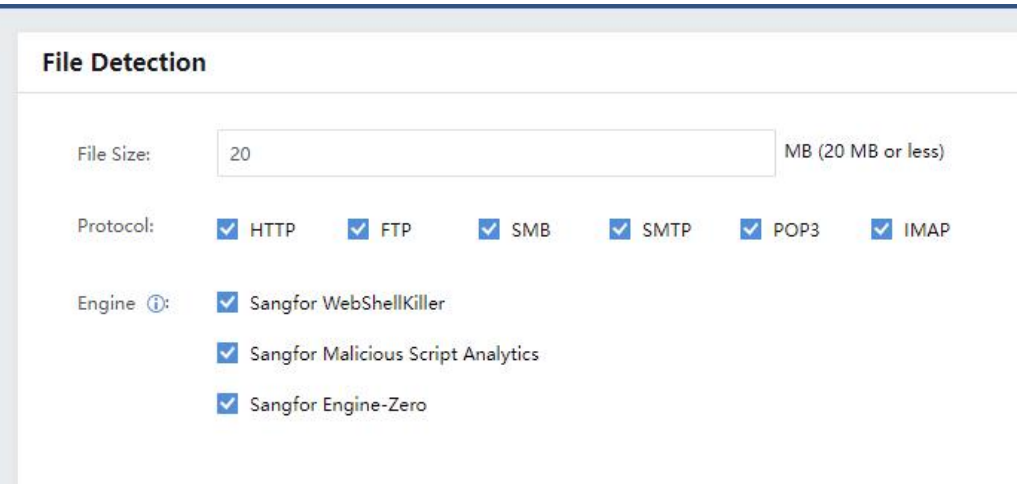
1. Once the IP has been whitelisted, the system will filter the matched traffic data.

File Detection

The **File Detection** function page corresponds to the **Detection > Threats > File Threat** function module, as shown in the figure below.



The administrator can adjust the file detection settings, including file analysis size (maximum 20MB), recognized protocol type, selected detection engine, etc., as shown in the following figure.

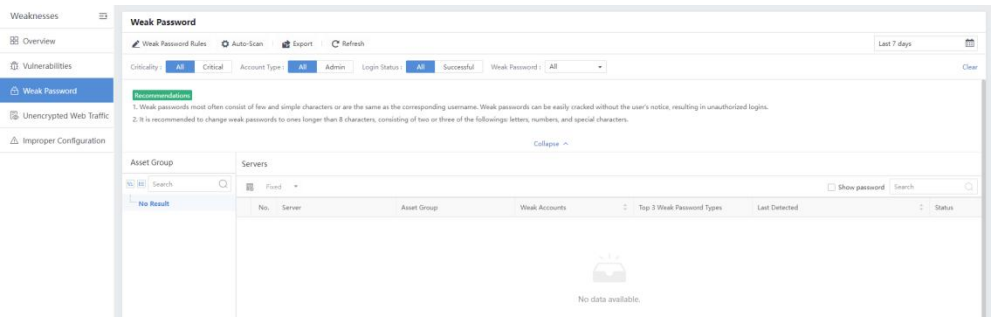


Select the required protocol types: **HTTP, FTP, SMB, SMTP, POP3, IMAP.**

Detection engines include **Sangfor WebshellKiller, Sangfor Malicious Script Analytics,** and **Sangfor Engine-Zero.**

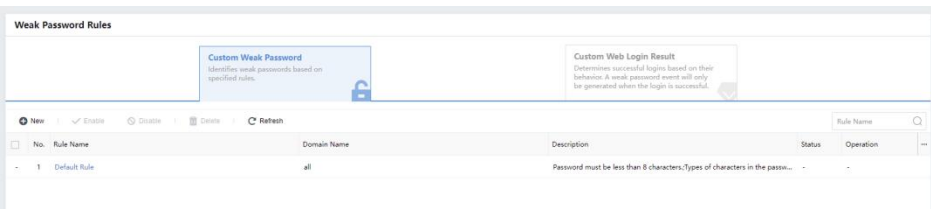
Weak Password Rules

The **Weak Password Rules** correspond to the **Asset > Weakness > Weak Password** functional module, as shown below.



The weak password configuration is divided into default rules and custom rules. The built-in rules identify and detect all applications (web and non-web). The figure below shows that the default rules cannot be edited, modified, or deleted by default.

Custom Weak Password



Click the **New** button to enter the custom weak password rule. The custom weak password rule is mainly for web applications. You need to specify the effective domain name, conditions, account whitelist, password whitelist, weak password, etc., as shown below.

Add Rule

* Rule Name:

* Domain Name:

Enter multiple endpoints with one entry per line. Only

Conditions

☒ Length < 8 characters

☒ < 2 factors, and < 16 characters

☒ Alphabetical order

☒ Same as username

☐ Blank web-access password

Account Whitelist:

One account per line

Password Whitelist:

One password per line

Weak Passwords:

Import File

One weak password per line

Save and Add

OK

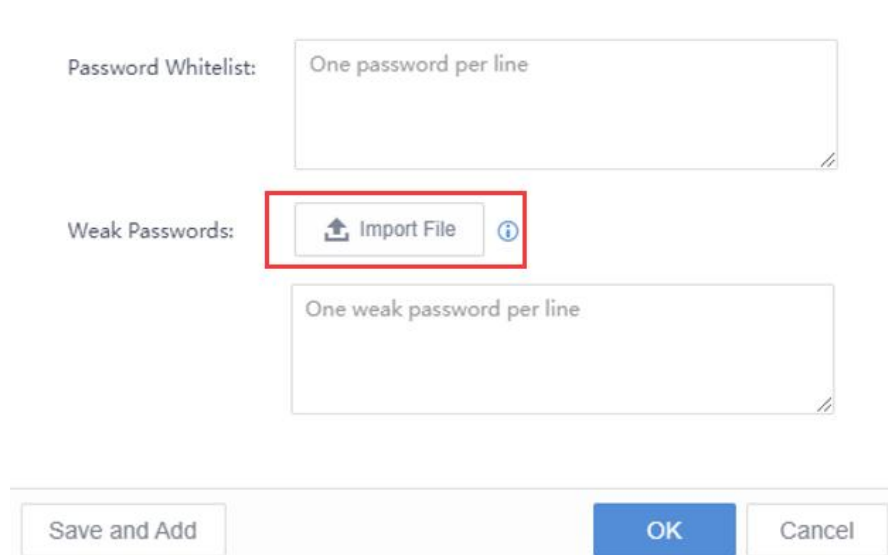
Cancel

- **Rule Name:** The name of the custom weak password database.
- **Domain Name:** The domain name/URL to which the rule applies, for example, <http://xxx:80/a/b/c?1=1>

Among them, HTTP:// belongs to the request protocol of the traffic, xxx belongs to the host address, which can be a domain name or hostname or IP, 80 connected with: belongs to the port, /a/b/c belongs to the resource path, and 1= connected with? 1 is a parameter.

The rule needs to be configured with the domain name's content by referring to the host value in the request traffic.
- **Conditions:** including minimum password length, number of character types and digits, alphabetical order, same as username and Blank web-access password.

- **Account Whitelist:** If the weak password obtained through product-side analysis does not meet the customer's business scenario/actual status.
- **Weak Passwords:** In the case of a small number, you can fill in the blank directly, or you can import in .txt format. Click **Import File**, as shown in the figure below.

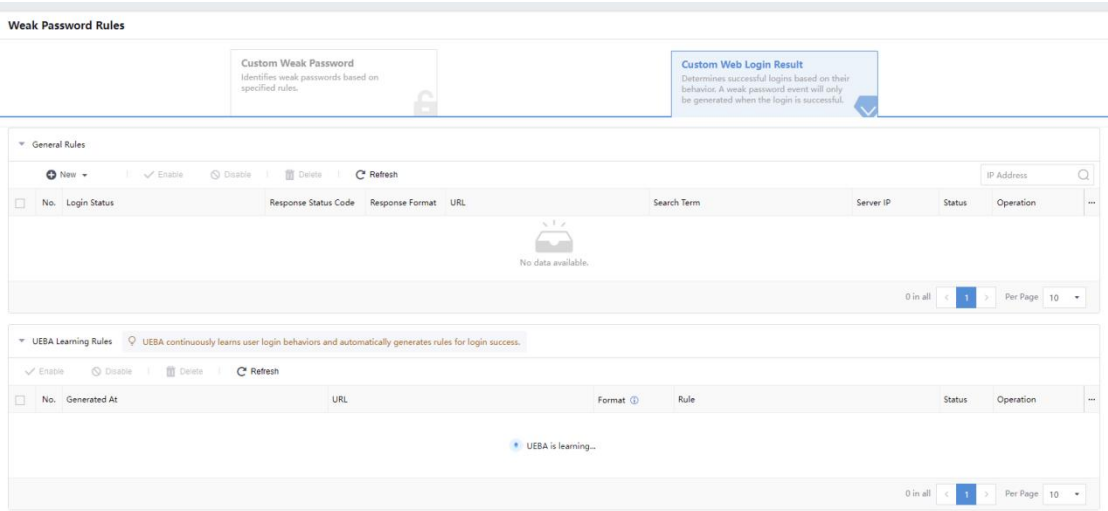


NOTE

1. For custom weak password rules, and associated web domains/URLs, the maximum number does not exceed 50.
2. Priority order: The priority of the custom weak password rule is higher than the default rule. It is to match the custom rule first and then the default rule.

Custom Web Login Result

Go to **System > Security Capabilities > Weak Password Rules** and select the Custom Web Login Result sub-tab.



WEB login results are divided into **Rule for Login Success** and **Rules for Login Failure**. The web login success and login failure information identified by Cyber Command in the customer’s actual network is different from the real situation of the business.

Therefore, manual correction is carried out based on HTTP. The protocol's two types of **Respond Status Codes**, are carried out by matching the content of the successful login, the server IP address, etc., as shown in the figure below.

Add Rule for Login Success

* Response Status Code:200

* Response Format:HTML

URL:One URL per line

* Search Term:Response identifier, e.g., login successful

* Server IP:e.g., 192.168.8.80 or 2005::1

* Asset Group:All

Save and Add

OK

Cancel

Add Rule for Login Failure

* Response Status Code:

200

* Response Format:

HTML

URL:

One URL per line

* Search Term:

Response identifier, e.g., login successful

* Server IP:

e.g., 192.168.8.80 or 2005::1

* Asset Group:

All

Save and Add

OK

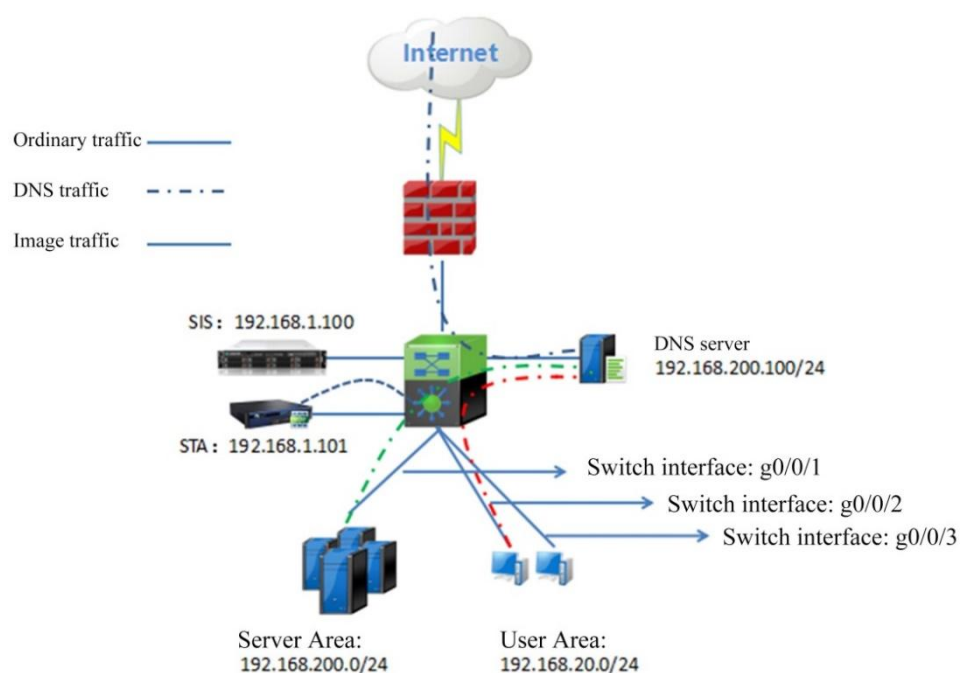
Cancel

4 Attachments

4.1 Attachment

The deployment description in the special scenario includes the DNS, AD, and DHCP environments.

4.1.1 DNS Environment



Notes: When the STA receives image data that is the proxy of the LAN DNS, it identifies the DNS as a risky host or business system and, therefore, cannot locate the actual risky service.

Logic: Image the data before the proxy of LAN DNS from the PC (or business system) to LAN DNS. Capture the address of LAN DNS and the data packet of the 53 port.

- If the IP address of LAN DNS is both the source and the destination, add the DNS to the global whitelist.
- If the IP address of LAN DNS is only the source, it indicates that the imaged data only includes proxy data, and the data shall be imaged again.
- If the IP address of LAN DNS is only the destination, it indicates that the data is imaged correctly.

- Then add the DNS to the whitelist. (Also, add the IP address of the scanner to the whitelist.)

Configuration Steps:

Method I: Add the IP address of DNS into **Audit Whitelist**. (Recommended)

Whitelists

Audit Whitelist: Traffic that matches the whitelist will not be audited.

Security Whitelist: No alerts or incidents will be generated for the logs that matches the whitelist.

Traffic data is filtered based on the audit whitelist first and then the security whitelist. Traffic that is not whitelisted is then analyzed, and alerts are generated.

Traffic

Audit Whitelist

Security Whitelist

Analyze

Security Whitelist

Audit Whitelist

Add

Import

Export

Delete

Refresh

IP Address/Log Type/Remarks

☐	No.	Src IP	Src Port	Dst IP	Dst Port	Rule Match	Time Added	Remarks	Op...
☐	1	10.251.251.251, 192.168.20.189	-	-	-	Log Type: All	-	ts	
☐	2	-	-	10.251.251.251, 192.168.20.189	-	Log Type: All	-	ts	
☐	3	192.168.1.201	-	-	-	Log Type: All	-	ts	
☐	4	-	-	192.168.1.201	-	Log Type: All	-	ts	

4 in all 1 Per Page 20

Method II: Add the IP address of Audit Whitelist.

Whitelists

Audit Whitelist: Traffic that matches the whitelist will not be audited.

Security Whitelist: No alerts or incidents will be generated for the logs that matches the whitelist.

Traffic data is filtered based on the audit whitelist first and then the security whitelist. Traffic that is not whitelisted is then analyzed, and alerts are generated.

Traffic

Audit Whitelist

Security Whitelist

Analyze

Security Whitelist

Audit Whitelist

Add

Import

Export

Delete

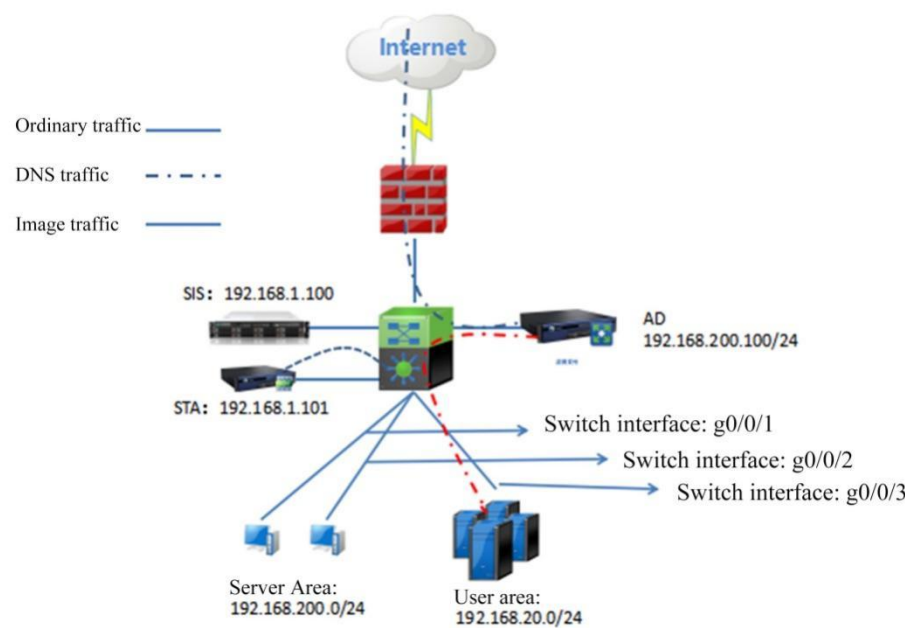
Refresh

IP Address/Log Type/Remarks

☐	No.	Src IP	Src Port	Dst IP	Dst Port	Rule Match	Time Added	Remarks	Op...
☐	1	10.251.251.251, 192.168.20.189	-	-	-	Log Type: All	-	ts	
☐	2	-	-	10.251.251.251, 192.168.20.189	-	Log Type: All	-	ts	
☐	3	192.168.1.201	-	-	-	Log Type: All	-	ts	
☐	4	-	-	192.168.1.201	-	Log Type: All	-	ts	

4 in all 1 Per Page 20

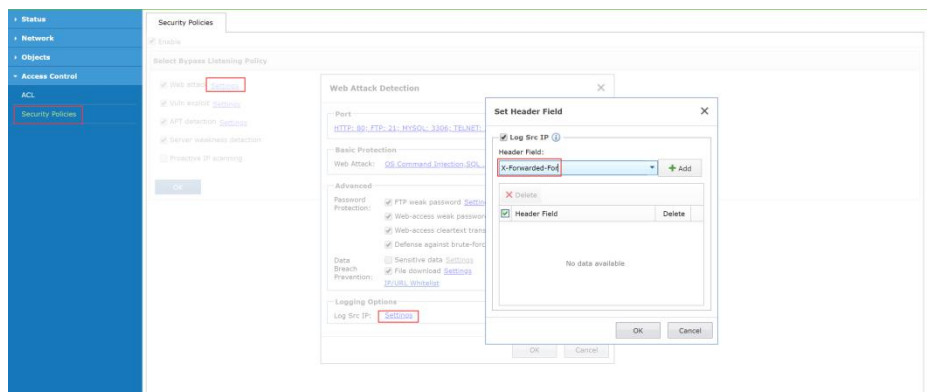
4.1.2 HCI Environment



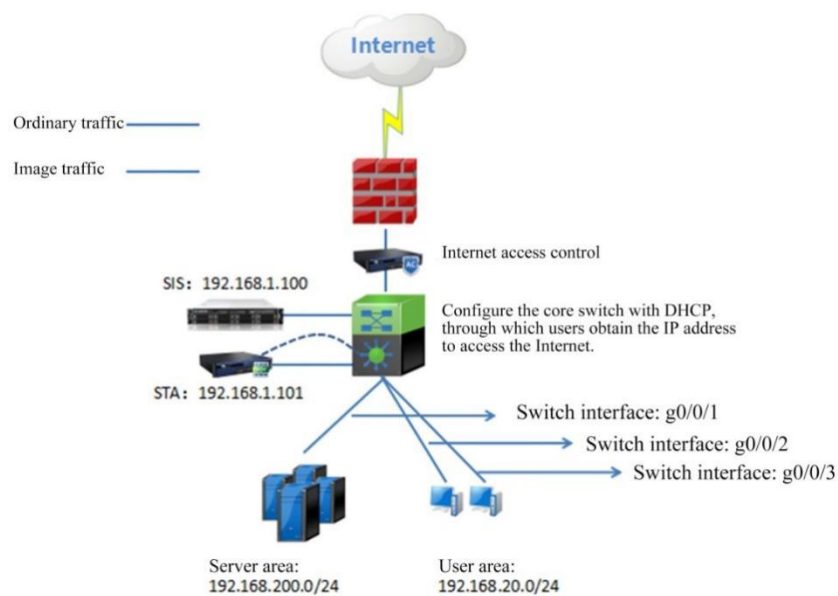
Deployment of AD in a single-arm mode transfers the IP addresses of the public network to those of AD.

Logic:

- It is recommended that the STA's image traffic be the traffic between the server and AD, through which risky servers can be recognized. However, the risky hosts cannot be located when the STA is deployed between the AD and the Internet.
- It is recommended to enable the XFF field to detect launched attacks and recognize a source IP address of WAF attacks on the STA using the XFF.



4.1.3 DHCP Environment



As shown above, if a security issue occurs on the endpoint user's part, the specific endpoint with the security issue cannot be located due to DHCP's dynamic provisioning of IP addresses.

Solution:

If the DHCP lease time is set as one week, it indicates that the lease time is prolonged, i.e., the user's IP address is indirectly bound.

By correlating Cyber Command with IAG, the IAG uploads a username to Cyber Command. The security issue corresponds to the username on IAG because the risky endpoints can be confirmed without changing the username.



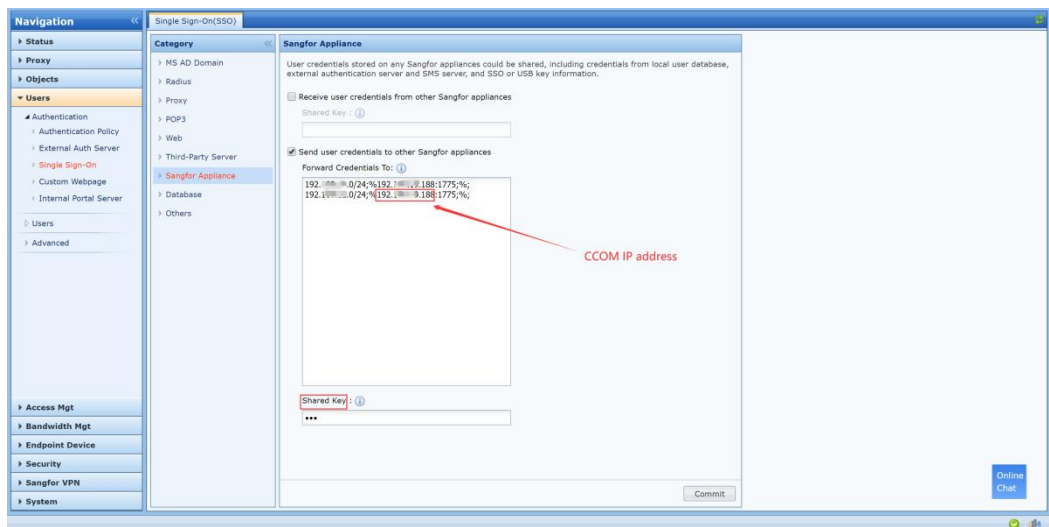
When IAG is configured with globally excluded IP addresses, the excluded domain names automatically initiate a DNS request.

The excluded IP addresses automatically initiate a request to search for the domain names. It is related to the validity of the mechanism with which IAG automatically detects the globally excluded IP addresses. As this may result in the C&C communication behavior of IAG being identified by Cyber Command, it is required to add IAG's IP addresses to the global whitelist of Cyber Command.

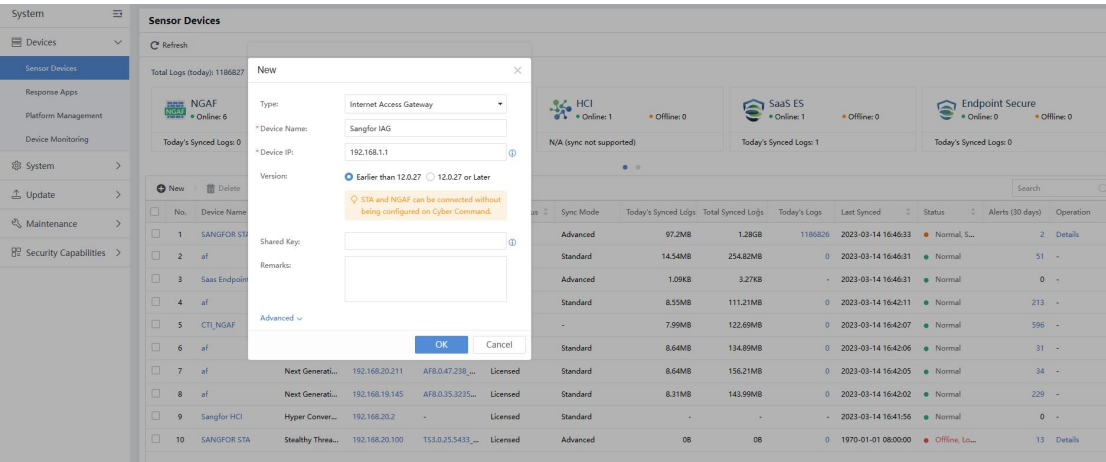
The configuration is as follows:

IAG should be updated to version 11.X, or above. Or add a corresponding patch using version IAG 12.0.5 or IAG 12.0.6 to release the correlation policy.

IAG Configuration:



Cyber Command configuration:



- **Online Conditions:** When logging in, the IAG user shall adopt password authentication because single sign-on information will not be sent to Cyber Command when password authentication is not performed.
- **Online Effect:** The device is online when IAG appears on the interface. However, the IAG does not upload the behavior logs, so all items are displayed as (-).

