

SecMaster

Service Overview

Issue 07
Date 2025-02-24



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 What Is SecMaster?	1
2 Product Advantages	2
3 Application Scenarios	3
4 Functions	4
5 Personal Data Protection	17
6 Experience Packages	20
6.1 Preconfigured Playbooks	20
6.2 Preset Types	24
7 Limitations and Constraints	86
8 Security	90
8.1 Shared Responsibilities	90
8.2 Identity Authentication and Access Control	91
8.3 Data Protection Technologies	91
8.4 Audit Logs	92
8.5 Service Resilience	93
8.6 Risk Monitoring	94
8.7 Certificates	96
8.8 Security Orchestration	98
9 Permissions Management	99
10 SecMaster and Other Services	104
11 Basic Concepts	106
11.1 SOC	106
11.2 Security Overview and Situation Overview	112
11.3 Workspaces	115
11.4 Alert Management	116
11.5 Security Orchestration	116
11.6 Security Analysis	118

1 What Is SecMaster?

SecMaster is a next-generation cloud native **security operations center**. Based on years of Huawei Cloud experience in cloud security, it enables integrated and automatic security operations through cloud asset management, security posture management, security information and incident management, security orchestration and automatic response, cloud security overview, simplified cloud security configuration, configurable defense policies, and intelligent and fast threat detection and response.

Why SecMaster?

- One-click security compliance: Huawei's accumulated global security compliance experience enables one click generation of compliance reports, helping users quickly implement cloud service security/privacy protection compliance.
- Comprehensive awareness on one screen: Alert incidents of security services are collected, associated, sorted, and made available for retrieval, enabling security operation situations to be comprehensively evaluated and dynamically displayed on a large screen.
- Global analysis across the cloud: Based on hundreds of millions of threat indicators accumulated by Huawei Cloud every day, SecMaster enables associated analysis to locate security threats, eliminate invalid alerts, and identify potential advanced threats.
- Integrated global handling: The built-in alert processing playbooks enable minute-level automatic response to more than 99% security incidents.

For more information about the advantages of SecMaster, see [Product Advantages](#).

2 Product Advantages

Refined Indicators and Intuitive Situation Display

You can view the security overview on the large screen in real time and periodically subscribe to security operation reports to know the core security indicators.

Cloud Native Asset Stocktaking and Risk Prevention

All assets and security configurations on the cloud are automatically checked, and automatic hardening is provided to help you fix risky assets and insecure configurations. This avoids implicit channels and security device vulnerabilities introduced by traditional bolted-on security solutions.

Intelligent and Efficient Threat Detection, Response, and Handling

SecMaster focuses on finding true threats. By analyzing billions of security logs daily and leveraging the years of experience accumulated by the Huawei Cloud security operations team, SecMaster utilizes built-in models and analysis playbooks to reduce the interference from normal incidents. Threat and asset security profiling enables restoration of the entire attack chain. Risk handling playbooks can be configured for automatic response, simplifying operations and improving security and efficiency.

Environment Integration and Operational Collaboration for Ultimate Flexibility

You can connect to all security products, devices, and tools to connect data and operations (Bidirectional interconnection is supported). You can also define your own response models and analysis/handling playbooks to best meet your security requirements. You can use workspaces to enable large-scale organization collaboration and MSSP (Managed Security Service Provider) services.

3 Application Scenarios

The principle of cloud security is "30% R&D + 70% Operations". The "70% Operations" is where SecMaster is applied. The specific application scenarios of SecMaster are as follows:

Routine Security Operation

Inspect check items and implement the security operation process to achieve security objectives. Identify and mitigate risks, and continuously improve the process to prevent risk recurrence.

Key Incident Assurance

Provide 24/7 assurance during major festivals, holidays, activities, and conferences through attack defense to ensure service availability.

Security Drills

Provides security assurance in the attack defense drills organized by regulatory institutions through intrusion prevention, helping organizations pass the assessments in the drills.

Security Evaluation

Perform the white box baseline test, black box attack surface assessment, and attack vector detection before key incidents or drills to identify vulnerabilities.

4 Functions

Based on cloud native security, SecMaster provides a comprehensive closed-loop security response process that contains log collection, security governance, intelligent analysis, situation awareness, orchestration, and response, helping you protect cloud security.

SecMaster provides basic, standard, and professional editions for you to help meet security requirements in different scenarios. You can select the one that best fits your service needs.

Security Overview

The [Security Overview](#) page gives you a comprehensive view of your asset security posture together with other linked cloud security services to centrally display security assessment findings.

Table 4-1 Functions

Function Module	Description	Basic	Standard	Professional
Security Overview	<ul style="list-style-type: none"> • Security Score: A security score shows the overall health status of your workloads on the cloud so you can quickly learn of unhandled risks and their threats to your assets. The lower the security score, the greater the overall asset security risk. • Security Monitoring: You can view how many threats, vulnerabilities, and compliance violations that are not handled and view their details. • Security Scores over the Time: You can view the trend of the asset health scores for the last seven days. 	√	√	√

Workspace Management

Workspaces are top-level workbenches in SecMaster. A single workspace can be bound to general projects, enterprise projects, and regions for different application scenarios.

Table 4-2 Functions

Function Module	Description	Basic	Standard	Professional
Workspaces	<ul style="list-style-type: none"> • Workspace management: Workspaces are top-level workbenches in SecMaster. A single workspace can be bound to projects and regions to support workspace operational modes in different scenarios. • Workspace hosting: You can create an agency and use it to view the asset risks, alerts, and incidents of multiple workspaces across accounts. 	√	√	√

Security Governance

Security Governance provides you with a security governance template and compliance scanning service and converts the standard clauses in security compliance packs into check items.

Table 4-3 Functions

Function Module	Description	Basic	Standard	Professional
Security Governance	<ul style="list-style-type: none"> ● Compliance Pack Huawei's open security governance templates include original standards and regulation terms, check policies, compliance evaluation items, and improvement suggestions from Huawei experts, covering PCI DSS, ISO27701, ISO27001, privacy protection, and other regulations and standards. You can subscribe to and unsubscribe from security compliance packs and view the evaluation results. ● Policy Check Security Governance periodically detects the compliance status of cloud assets through code-based scanning. You can view compliance risks on the dashboard, and obtain corresponding improvement suggestions from Huawei experts. ● Compliance Evaluation Security Governance integrates regulatory clauses and standard requirements into compliance pack check items. You complete evaluation of your services using the compliance pack, and view evaluation results. You can also view historical results, upload and download evidence, and take actions based on Huawei experts' improvement suggestions. ● Result Display 	×	×	√

Function Module	Description	Basic	Standard	Professional
	<p>Security Governance displays the evaluation results and compliance status on the dashboard, including the compliance rates of the compliance packs you subscribed to, and the compliance rate of each term the regulations and standards, each security, as well as the policy check results.</p> <p>NOTE Before using security governance in SecMaster, you need to submit a service ticket to enable the service.</p>			

Purchased Resources

Purchased Resources centrally displays the resources purchased by the current account, making it easier for you to manage them in one place.

Table 4-4 Functions

Function Module	Description	Basic	Standard	Professional
Purchased Resources	You can view resources purchased by the current account on the Purchased Resources page and manage them centrally.	√	√	√

Security Situation

You can view the security overview on the large screen in real time and periodically subscribe to security operation reports to know the core security indicators.

Table 4-5 Functions

Function Module	Description	Basic	Standard	Professional
Situation Overview	<ul style="list-style-type: none"> • Security Score: A security score shows the overall health status of your workloads on the cloud so you can quickly learn of unhandled risks and their threats to your assets. The lower the security score, the greater the overall asset security risk. • Security Monitoring: You can view how many threats, vulnerabilities, and compliance violations that are not handled and view their details. • Security Scores over the Time: You can view the trend of the asset health scores for the last seven days. 	√	√	√
Large Screen	<p>SecMaster leverages AI to analyze and classify massive cloud security data and then displays real-time results on a large screen. In a simple, intuitive, and efficient way, you will learn of what risks your cloud environment are facing and how secure your cloud environment is.</p> <p>NOTE The large screen function needs to be purchased separately based on the standard or professional edition.</p>	×	√	√
Security Reports	You can generate analysis reports and periodically send them to specified recipients by email. In this way, all recipients can learn about the security status of your assets in a timely manner.	×	×	√
Task Center	All tasks that need to be processed are displayed centrally.	×	√	√

Resource Manager

Resource Manager supports centralized management of assets on the cloud and assets outside the cloud and displays their security status in real time.

Table 4-6 Functions

Function Module	Description	Basic	Standard	Professional
Resource Manager	SecMaster can synchronize the security statistics of all resources. So that you can check the name, service, and security status of a resource to quickly locate security risks.	√	√	√

Risk Prevention

Risk prevention provides baseline inspection, vulnerability management, and security policy management to help you check cloud security configurations and meet requirements in many security standards, such as DJCP, ISO, and PCI, as well as Huawei Cloud security best practice standards. You can learn about where vulnerabilities are located in the entire environment and fix them in just a few clicks.

Table 4-7 Functions

Function Module	Description	Basic	Standard	Professional
Baseline Inspection	SecMaster can scan cloud baseline configurations to find out unsafe settings, report alerts for incidents, and offer hardening suggestions to you.	√	√	√
Vulnerabilities	SecMaster automatically synchronizes vulnerability scan result from Host Security Service (HSS), displays vulnerability scan details by category, and provides vulnerability fixing suggestions.	×	×	√

Function Module	Description	Basic	Standard	Professional
Emergency Vulnerability Notices	SecMaster collects the latest information on known host security vulnerabilities every 5 minutes.	√	√	√
Security Policies	SecMaster supports centralized management of defense and emergency policies.	×	√	√

Threats

SecMaster provides many threat detection models in the Threats module to help customers detect threats from massive security logs and generate alerts. Beyond that, it provides built-in security response playbooks to help automatically analyze and handle alerts, and automatically harden security defense lines and security configurations.

Table 4-8 Functions of the Threats module

Function Module	Description	Basic	Standard	Professional
Incidents	SecMaster centrally displays incident details and allows you to manually or automatically convert alerts into incidents.	×	√	√
Alerts	Alerts of other cloud services such as HSS, WAF, and DDoS Mitigation are integrated for central display and management.	×	√	√
Indicators	Metrics can be extracted from alerts and incidents based on custom rules.	×	×	√
Intelligent Modeling	Models are supported to scan log data in pipelines. If SecMaster detects data that hits the trigger in a model, SecMaster generates an alert.	×	√	√

Function Module	Description	Basic	Standard	Professional
Security Analysis	<ul style="list-style-type: none"> ● Query and Analysis <ul style="list-style-type: none"> - Search and analysis: Supports quick data search and analysis, quick filtering of security data for security survey, and quick locating of key data. - Statistics filtering: SecMaster supports quick analysis and statistics of data fields and quick data filtering based on the analysis result. Time series data supports statistics collection by default time partition, allowing data volume trend to be quickly spotted. SecMaster supports analysis, statistics, and sorting functions, and supports quick building of security analysis models. - Visualization: Visualized data analysis intuitively reflects service structure and trend, enabling customized analysis reports and analysis indicators to be easily created. ● Data Delivery: Data can be delivered to other pipelines or Huawei Cloud products in real time so that you can store data to or retrieve data from other systems. ● Data Monitoring: Data streams are monitored and managed in an end-to-end manner. ● Data Consumption: SecMaster provides streaming communication 	×	√	√

Function Module	Description	Basic	Standard	Professional
	<p>interfaces for data consumption and production, as well as data pipeline SDKs. So that you can use SDKs to integrate data across systems, and specify custom data producers and consumers. SecMaster provides open-source log collection plugin Logstash. You can enable custom data consumers and producers.</p> <p>NOTE You need to purchase the security analysis function in the value-added package at an extra cost. However, there are some free quotas of security analysis, preconfigured playbooks, and security orchestration. For details, see Free Quota Description.</p>			

Security Orchestration

Security Orchestration supports playbook management, process management, data class management (security entity objects), and asset connection management. You can also customize playbooks and processes.

Security Orchestration allows you to flexibly orchestrate security response playbooks through drag-and-drop according to your service requirements. You can also flexibly extend and define security operation objects and interfaces.

Table 4-9 Functions

Function Module	Description	Basic	Standard	Professional
Objects	Manages operation objects such as data classes, data class types, and categorical mappings in a centralized manner.	×	√	√

Function Module	Description	Basic	Standard	Professional
Playbooks	Supports full lifecycle management of playbooks, processes, connections, and instances. NOTE You need to purchase the security orchestration function in the value-added package at an extra cost. However, there are some free quotas of security analysis, built-in playbooks, and security orchestration. For details, see Free Quota Description .	×	√	√
Layouts	Provides a visualized low-code development platform for customized layout of security analysis reports, alarm management, incident management, vulnerability management, baseline management, and threat indicator library management.	×	√	√
Plugins	Plug-ins used in the security orchestration process can be managed centrally.	×	×	√

Data Collection

Collects varied log data in multiple modes. After data is collected, historical data analysis and comparison, data association analysis, and unknown threat discovery can be quickly implemented.

Table 4-10 Functions

Function Module	Description	Basic	Standard	Professional
Data Collection (Collections and Components)	Logstash is used to collect varied log data in multiple modes. After data is collected, historical data analysis and comparison, data association analysis, and unknown threat discovery can be quickly implemented.	×	√	√

Data Integration

Integrates security ecosystem products for associated operations or data interconnection. After the integration, you can search for and analyze all collected logs.

Table 4-11 Functions

Function Module	Description	Basic	Standard	Professional
Data Integration	SecMaster provides a preset log collection system. You can enable access to logs of other cloud services in just a few clicks. After the integration, you can search for and analyze all collected logs.	×	√ (Only cloud service alerts can be integrated.)	√

Directory Customization

You can customize directories as needed.

Table 4-12 Functions

Function Module	Description	Basic	Standard	Professional
Directory Customization	You can view in-use directories and change their layouts.	×	√	√

Free Quota Description

SecMaster provides some free quotas for security analysis and security orchestration in the value-added package. While the free quotas vary depending on the SecMaster editions. The details are as follows:

Table 4-13 Free Quota Description

Function		Standard	Professional
Security Analysis	Security data collection	120 MB/day/quota	120 MB/day/quota
	Security data retention	120 MB/day/quota	120 MB/day/quota
	Security data export	120 MB/day/quota	120 MB/day/quota

Function		Standard	Professional
	Platform security data	40 MB/day/quota	40 MB/day/quota
	Security modeling analysis	×	120 MB/day/quota
Threat Management	Preset threat models	×	Calculation model data: 120 MB/day/quota; Preset models: 200
	Preset response playbooks	×	Preset playbooks: 30
Security Orchestration (SOC)	Security Orchestration	×	Operations: 7,000

5 Personal Data Protection

To ensure that your personal data, such as the username, password, and email, will not be obtained by unauthorized or unauthenticated entities or people and to prevent data leakage, SecMaster encrypts your personal data before storing it to control access to the data and records logs for operations performed on the data.

Personal Data to Be Collected

Table 5-1 describes the personal data generated or collected by SecMaster.

Table 5-1 Personal data scope

Type	Collection Method	Modifiable	Mandatory
Email address	Some playbooks in SecMaster may need to send email notifications to you. So SecMaster needs to obtain the email addresses you specify while you subscribe to SMN topics. If you enable scheduled security reports, SecMaster needs to email security reports to you. To this end, SecMaster needs to obtain the recipient email addresses you enter on the console with the authorization of recipients.	Yes	Yes
Source IP address	If you enable WAF in SecMaster, WAF blocks or logs IP addresses of attacks against domain names it protects. SecMaster will collect those attack source IP addresses as well.	No	Yes

Type	Collection Method	Modifiable	Mandatory
URL	If you enable WAF in SecMaster, WAF logs URLs of domain names it protects when there are attacks against the domain names. SecMaster will collect those URLs as well.	No	Yes
HTTP/HTTPS header information (including the cookie)	If you enable WAF in SecMaster and there are attacks hit a CC attack or precise protection rule, SecMaster will generate alerts. Those alerts may include the cookie and header information entered on the configuration page.	No	No If the configured cookie and header fields do not contain users' personal information, the requests recorded by SecMaster will not collect or generate such personal data.
Request parameters (Get and Post)	IF you enable WAF in SecMaster, SecMaster will collect request details that are recorded by WAF in protection events.	No	No If request parameters do not contain users' personal information, the requests recorded by WAF will not collect or generate such personal data.
Login location	If you enable HSS in SecMaster, HSS logs user login locations for protected cloud servers. SecMaster will collect the login locations.	No	Yes

Storage

SecMaster uses encryption algorithms to encrypt users' sensitive data and stores encrypted data.

- Emails are encrypted before storage.
- Login locations are not sensitive data and stored in plaintext.
- For request source IP addresses, URLs, HTTP/HTTPS header information (including cookies), and request parameters (Get and Post) in logs, sensitive fields are anonymized, and other fields are stored in plaintext.

Access Control

User personal data is encrypted before being stored in the SecMaster database. A trustlist is used to control access to the database.

Users can view only logs related to their own services.

6 Experience Packages

6.1 Preconfigured Playbooks

In security orchestration module, SecMaster provides preconfigured playbooks. You can use them without extra settings.

Preconfigured Playbooks

The following playbooks are enabled by default:

HSS alert status synchronization, automatic notification of high-risk vulnerabilities, historical handling information associated with host defense alarms, SecMaster and WAF address group association policy, historical handling information associated with application defense alarms, historical handling information associated with network defense alarms, automatic closure of repeated alarms, and alarm IP metric marking Asset protection status statistics notification, automatic alarm statistics notification, and automatic high-risk alarm notification

Table 6-1 Built-in playbooks

Security Layer	Playbook Name	Description	Data Class
Server security	HSS alert synchronization	Automatically synchronizes HSS alerts generated for servers.	Alert
	Auto High-Risk Vulnerability Notification	Sends email or SMS notifications to specified recipients when vulnerabilities rated as high severity are discovered.	Vulnerability
	Attack Link Analysis Alert Notification	Analyzes attack links. If HSS generates an alert for a server, the system checks the website running on the server. If the website information and alert exist, the system sends an alert notification.	Alert

Security Layer	Playbook Name	Description	Data Class
	Server vulnerability notification	Checks servers with EIPs bound on the resource manager page and notifies of discovered vulnerabilities.	CommonContext
	HSS Isolation and Killing of Malware	Automatically isolates and kills malware.	Alert
	Mining host isolation	Isolates the server for which an alert of mining program or software was generated. The playbook also adds the server into a security group that allows no inbound or outbound traffic.	Alert
	Ransomware host isolation	Isolates the server for which an alert of ransomware was generated. The playbook also adds the server into a security group that allows no inbound or outbound traffic.	Alert
	Host Defense Alarms Are Associated With Historical Handling Information	Associates new HSS alerts with HSS alerts handled earlier and adds historical handling details to the comment area for the corresponding HSS alerts.	Alert
	Add host asset protection status notification	Checks new servers and notifies you of servers unprotected by HSS.	Resource
	HSS High-Risk Alarm Interception Notification	Checks HSS high-risk alarms and generates to-do task notifications for source IP addresses that are not blocked by security groups. The to-do tasks will be reviewed manually. Once confirmed, the source IP addresses will be added to VPC block policy in SecMaster.	Alert
	Automated handling of host Rootkit event attacks	If a Rootkit alert is generated, this playbook automatically isolates the affected host by adding it to a security group that blocks all inbound and outbound traffic, and closes the alert.	Alert
	Automated handling of host rebound Shell attacks	If a reverse shell alert is generated, this playbook automatically isolates the affected host by adding it to a security group that blocks all inbound and outbound traffic, and closes the alert.	Alert

Security Layer	Playbook Name	Description	Data Class
Application security	SecMaster WAF Address Group Association Policy	Associates SecMaster and WAF blacklist address groups for all enterprise projects.	CommonContext
	WAF clear Non-domain Policy	Checks WAF protection policies at 09:00 every Monday and deletes policies with no rules included.	CommonContext
	Application Defense Alarms Are Associated With Historical Handling Information	Associates new WAF alerts with WAF alerts handled earlier and adds historical handling details to the comment area for the new alerts.	Alert
	Web login burst interception	Checks IP addresses that establish brute-force login connections. If the IP addresses are not whitelisted, the workflow generates a to-do task. The to-do task will be reviewed manually. Once it is confirmed that the IP addresses should be blocked, the IP addresses will be added to a WAF block policy in SecMaster.	Alert
O&M security	Real-time Notification of Critical Organization and Management Operations	Sends real-time notifications for O&M alerts generated by models. Currently, SMN notifications can be sent for three key O&M operations: attaching NICs, creating VPC peering connections, and binding EIPs to resources.	Alert
Identity security	Identity Defense Alarms Are Associated With Historical Handling Information	Associates new IAM alerts with IAM alerts handled earlier and adds historical handling details to the comment area for the new alerts.	Alert
Network security	Network Defense Alarms Are Associated With Historical Handling Information	Associates new CFW alerts with CFW alerts handled earlier and adds historical handling details to the comment area for new alerts.	Alert
Others/General	Automatic Notification of High-Risk Alerts	Sends email or SMS notifications when there are alerts rated as High or Fatal.	Alert

Security Layer	Playbook Name	Description	Data Class
	Alert metric extraction	Extracts IP addresses from alerts, checks the IP addresses against the intelligence system, sets alert indicators for confirmed malicious IP addresses, and associates the indicators with the source alerts.	Alert
	Automatic Disabling of Repeated Alerts	Closes the status of duplicate alerts when they are generated next time for the last 7 days and associates the alerts with the same name for the last 7 days.	Alert
	Automatic renaming of alert names	Generates custom alert names by combining specified key fields.	Alert
	Alert IP metric labeling	Adds attack source IP address and attacked IP address labels for alerts.	Alert
	IP intelligence association	Associates alerts with SecMaster intelligence (preferred) and ThreatBook intelligence.	Alert
	Asset Protection Status Statistics Notification	Collects statistics on asset protection status every week and sends notifications to customers by email or SMS.	CommonContext
	Alert statistics Notify	At 19:00 every day, collects statistics on alerts that are not cleared and sends notifications to customers by email or SMS.	Alert
	Auto Blocking for High-risk Alerts	If a source IP address launched more than three attacks, triggered high-risk or critical alerts, and hit the malicious label in ThreatBook, this playbook triggers the corresponding security policies in WAF, VPC, CFW, or IAM to block the IP address.	Alert
	Automatic clearing of low-risk alerts	This playbook automatically clear low-risk and informative alerts.	Alert
	CFW Synchronizes Black IP Addresses to Intelligence	This playbook synchronizes the IP address blacklist configured in CFW to the Indicators page in SecMaster.	CommonContext

Security Layer	Playbook Name	Description	Data Class
	WAF Synchronizes Black IP Addresses to Intelligence	This playbook synchronizes the IP address blacklist configured in WAF to the Indicators page in SecMaster.	CommonContext

6.2 Preset Types

This section describes alert, incident, threat indicator, and vulnerability types preset in SecMaster.

Preset Alert Types

Table 6-2 Preset alert types

Type Name	Sub Type/Sub Type Tag	Preset	Description
DDoS attack	DNS protocol attacks Tcps Dns	Yes	DNS protocol attacks
	Unusual ports Unusual Network Port	Yes	Unusual ports
	Abnormal protocol attacks Unusual Protocol	Yes	Abnormal protocol attacks
	ACK Flood ACK Flood	Yes	ACK Flood
	BGP flood BGP Flood Attack	Yes	BGP flood
	DNS IP TTL DNS IP TTL Check Fail	Yes	DNS IP TTL
	DNS reply flood DNS Reply Flood	Yes	DNS reply flood
	DNS query flood DNS Query Flood	Yes	DNS query flood

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Abnormal DNS size DNS Size Abnormal	Yes	Abnormal DNS size
	DNS reflection DNS Reflection	Yes	DNS reflection
	Abnormal DNS response flow DNS Reply Domain Flow Abnormal	Yes	Abnormal DNS response flow
	Invalid DNS format DNS Format Error	Yes	Invalid DNS format
	DNS cache matching DNS Cache Match	Yes	DNS cache matching
	DNS cache poisoning DNS Cache Poisoning	Yes	DNS cache poisoning
	Abnormal DNS request flow DNS Request Domain Flow Abnormal	Yes	Abnormal DNS request flow
	DNS domain name errors DNS No Such Name	Yes	DNS domain name errors
	FIN/RST Flood FIN/RST Flood	Yes	FIN/RST Flood
	HTTPS Flood HTTPS Flood	Yes	HTTPS Flood
	HTTP slow attacks HTTP Slow Attack	Yes	HTTP slow attacks
	ICMP blocking ICMP Protocol Block	Yes	ICMP blocking

Type Name	Sub Type/Sub Type Tag	Preset	Description
	IP reputation IP Reputation	Yes	IP reputation
	SIP Flood SIP Flood	Yes	SIP Flood
	Abnormal SIP source rate SIP Source Rate Abnormity	Yes	Abnormal SIP source rate
	SYN Flood SYN Flood	Yes	SYN Flood
	SYN-ACK Flood SYN-ACK Flood	Yes	SYN-ACK Flood
	TCP bandwidth overflow TCP Bandwidth Overflow	Yes	TCP bandwidth overflow
	TCP multi-connection attacks TCP Connection Flood	Yes	TCP multi-connection attacks
	TCP fragment bandwidth overflow TCP Fragment Bandwidth Overflow	Yes	TCP fragment bandwidth overflow
	TCP fragment attacks TCP Fragment Flood	Yes	TCP fragment attacks
	Malformed TCP packets TCP Malformed	Yes	Malformed TCP packets
	TCP/UDP attacks TCP-authenticated UDP Attack	Yes	TCP/UDP attacks
	TCP blocking TCP Protocol Block	Yes	TCP blocking

Type Name	Sub Type/Sub Type Tag	Preset	Description
	UDP bandwidth overflow UDP Bandwidth Overflow	Yes	UDP bandwidth overflow
	UDP fragments UDP Fragment Flood	Yes	UDP fragments
	UDP fragment bandwidth overflow UDP Fragment Bandwidth Overflow	Yes	UDP fragment bandwidth overflow
	Malformed UDP packets UDP Malformed	Yes	Malformed UDP packets
	UDP blocking UDP Protocol Block	Yes	UDP blocking
	URI monitoring URI Monitor	Yes	URI monitoring
	Dark web IP addresses Dark IP	Yes	Dark web IP addresses
	Single EIP bandwidth overflow Single IP Bandwidth Overflow	Yes	Single EIP bandwidth overflow
	Current connection flood attacks Concurrent Connections Flood	Yes	Current connection flood attacks
	Port scan attacks Port Scanning Attack	Yes	Port scan attacks

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Malicious domain name attacks Malicious Domains Attack	Yes	Malicious domain name attacks
	Anti-malware Anti-Malware	Yes	Anti-malware
	DDoS attacks DDOS	Yes	DDoS attacks
	Partition bandwidth overflow Zone Bandwidth Overflow	Yes	Partition bandwidth overflow
	Filter attacks Filter Attack	Yes	Filter attacks
	Blacklist Blacklist	Yes	Blacklist
	Botnets/Trojans/Worms Botnets/Trojan horses/Worms Attack	Yes	Botnets/Trojans/Worms
	Destination IP new session rate limiting Destination IP new session rate limiting	Yes	Destination IP new session rate limiting
	Other flood attacks Other Flood	Yes	Other flood attacks
	Other bandwidth overflow Other Bandwidth Overflow	Yes	Other bandwidth overflow
	Other global exceptions Global Other Abnormal	Yes	Other global exceptions

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Other protocol blocking Other Protocol Block	Yes	Other protocol blocking
	Global ICMP exception Global ICMP Abnormal	Yes	Global ICMP exception
	Abnormal global TCP fragments Global TCP Fragment Abnormal	Yes	Abnormal global TCP fragments
	Global TCP exception Global TCP Abnormal	Yes	Global TCP exception
	Abnormal global UDP fragments Global UDP Fragment Abnormal	Yes	Abnormal global UDP fragments
	Global UDP exception Global UDP Abnormal	Yes	Global UDP exception
	Web attacks Web Attack	Yes	Web attacks
	Geolocation attacks Location Attack	Yes	Geolocation attacks
	Connection flood attack New Connections Flood	Yes	Connection flood attack
	Domain hijacking Domain Hijacking	Yes	Domain hijacking

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Abnormal source DNS response traffic Source DNS Reply Flow Abnormal	Yes	Abnormal source DNS response traffic
	Abnormal source DNS request traffic Source DNS Request Flow Abnormal	Yes	Abnormal source DNS request traffic
	Host traffic overflow Host Traffic Over Flow	Yes	Host traffic overflow
	HTTP Flood HTTP Flood	Yes	HTTP Flood
	ICMP Flood ICMP Flood	Yes	ICMP Flood
	SSL Flood SSL Flood	Yes	SSL Flood
	TCP Flood TCP Flood	Yes	TCP Flood
	UDP Flood UDP Flood	Yes	UDP Flood
	XML Flood XML Flood	Yes	XML Flood
	Amplification attacks Amplification	Yes	Amplification attacks
Malicious code	Hidden link Web Page Dark Link	Yes	Hidden link
	Web page Trojan Web Page Trojan	Yes	Web page Trojan

Type Name	Sub Type/Sub Type Tag	Preset	Description
Web attacks	Webshell Webshell	Yes	Webshell
	WAF robot WAF Robot	Yes	WAF robot
	IP address whitelist White IP	Yes	IP address whitelist
	Known attack source Known Attack Source	Yes	Known attack source
	IP address blacklist Black IP	Yes	IP address blacklist
	Vulnerability exploits Vulnerability Attack	Yes	Vulnerability exploits
	Data masking Leakage	Yes	Data masking
	Default Default	Yes	Default
	Scanners/Crawlers Scanner & Crawler	Yes	Scanners/Crawlers
	CC attacks Challenge Collapsar	Yes	CC attacks
	IP reputation database IP Reputaion	Yes	IP reputation database
	SQL injection SQL Injection	Yes	SQL injection
	XSS Cross-Site Scripting	Yes	XSS
	Local file inclusion Local Code Inclusion	Yes	Local file inclusion

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Geolocation access control Geo IP	Yes	Geolocation access control
	Malicious crawlers Malicious Web Crawlers	Yes	Malicious crawlers
	Anti-crawler Anticrawler	Yes	Anti-crawler
	Web tampering protection AntiTamper	Yes	Web tampering protection
	Invalid requests Illegal Access	Yes	Invalid requests
	Blacklist or whitelist alarms White or Black IP	Yes	Blacklist or whitelist alarms
	Precise protection Custom Rule	Yes	Precise protection
	Command injection Command Injection	Yes	Command injection
	Path Traversal Path Traversal	Yes	Path Traversal
	Website Trojans Website Trojan	Yes	Website Trojans
	Website data leakage Information Leakage	Yes	Website data leakage
	Information leakage Web Service Exfiltration	Yes	Information leakage

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Remote code execution Remote Code Execute	Yes	Remote code execution
	Remote file inclusion Remote Code Inclusion	Yes	Remote file inclusion
Malware	Encrypted currency mining Cryptomining	Yes	Encrypted currency mining
	Docker malicious program Docker Malware	Yes	Docker malicious program
	Fishing Phishing	Yes	Fishing
	Malicious adware Adware	Yes	Malicious adware
	Malware Malicious Software	Yes	Malware
	Hacker tool Hacktool	Yes	Hacker tool
	Grayware Grayware	Yes	Grayware
	Spyware Spyware	Yes	Spyware
	Spam Spam	Yes	Spam
	Rootkit Rootkit	Yes	Rootkit
	Webshell Webshell	Yes	Webshell
	Virus/Worm Virus and Worm	Yes	Virus/Worm

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Malicious file Malicious File	Yes	Malicious file
	Reverse shell Reverse Shell	Yes	Reverse shell
	Trojan Backdoor Trojan	Yes	Trojan
	Botnet Botnet Program	Yes	Botnet
	Ransomware Ransomware	Yes	Ransomware
	Bitcoin Miner Bitcoin Miner	Yes	Bitcoin Miner
	Mining software Mining Software	Yes	Mining software
Risk Audit	Web-CMS Vulnerability Webcms Vulnerability	Yes	Web-CMS Vulnerability
	Windows OS vulnerabilities Windows Vulnerability	Yes	Windows OS vulnerabilities
	Local access vulnerability Local Access Vulnerability	Yes	Local access vulnerability
	Incorrect configuration policy Mis-Configured Policy	Yes	Incorrect configuration policy
	Other OS vulnerability Other OS Vulnerability	Yes	Other OS vulnerability
	Other vulnerability Other Vulnerability	Yes	Other vulnerability

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Application vulnerability Application Vulnerability	Yes	Application vulnerability
	Remote access vulnerability Remote Access Vulnerability	Yes	Remote access vulnerability
Risk Audit	Weak Password Weak Password	Yes	Weak Password
	Risky system configuration System Risk Configuration	Yes	Risky system configuration
Attacks	Fishing Phishing	Yes	Fishing
	Network topology Map Network Topology	Yes	Network topology
	Account and group information collection Identify Groups/Roles	Yes	Account and group information collection
	Fingerprint scan Fingerprinting	Yes	Fingerprint scan
	Host discovery Determine IP Address	Yes	Host discovery

Type Name	Sub Type/Sub Type Tag	Preset	Description
Vulnerability exploit	ActiveX vulnerability exploit ActiveX Exploit	Yes	ActiveX vulnerability exploit
	CGI attack CGI Attack	Yes	CGI attack
	DNS vulnerability exploit DNS Exploit	Yes	DNS vulnerability exploit
	FTP vulnerability exploit FTP Exploit	Yes	FTP vulnerability exploit
	Hadoop vulnerability exploit Hadoop Vulnerability Exploit	Yes	Hadoop vulnerability exploit
	Vulnerability exploit of hypervisor Hypervisor Exploit	Yes	Vulnerability exploit of hypervisor
	LDAP injection LDAP Injection Attack	Yes	LDAP injection
	MacOS vulnerability exploit MacOS Exploit	Yes	MacOS vulnerability exploit
	MySQL vulnerability exploit MySQL Vulnerability Exploit	Yes	MySQL vulnerability exploit
	Vulnerability exploit of Office software Office Exploit	Yes	Vulnerability exploit of Office software

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Redis vulnerability exploit Redis Vulnerability Exploit	Yes	Redis vulnerability exploit
	RPC vulnerability exploit RPC Exploit	Yes	RPC vulnerability exploit
	SQL injection SQL Injection	Yes	SQL injection
	SSH vulnerability exploit SSH Exploit	Yes	SSH vulnerability exploit
	SSI injection attack SSI Injection Attack	Yes	SSI injection attack
	Struts2 OGNL injection Struts2 OGNL Injection	Yes	Struts2 OGNL injection
	Telnet vulnerability exploit TELNET Exploit	Yes	Telnet vulnerability exploit
	Unix vulnerability exploit Unix Exploit	Yes	Unix vulnerability exploit
	Web vulnerability exploit Web Exploit	Yes	Web vulnerability exploit
	Cross site scripting (XSS) Cross-Site Scripting	Yes	Cross site scripting (XSS)
	Local file inclusion Local File Inclusion	Yes	Local file inclusion
	Malicious file delivery Malicious File Delivery	Yes	Malicious file delivery

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Malicious file execution Malicious File Execution	Yes	Malicious file execution
	Buffer overflow attack Buffer Overflow	Yes	Buffer overflow attack
	Session hijacking Session Hijack	Yes	Session hijacking
	Password guessing Password Cracking	Yes	Password guessing
	Browser vulnerability exploit Browser Exploit	Yes	Browser vulnerability exploit
	Weak password access Weak Password Access	Yes	Weak password access
	Database vulnerability exploit Database Exploit	Yes	Database vulnerability exploit
	Unknown vulnerability exploit Unknown Exploit	Yes	Unknown vulnerability exploit
	Hidden link access Hide Link Access	Yes	Hidden link access
	Email vulnerability exploit Mail Exploit	Yes	Email vulnerability exploit
	Remote code execution Remote Code Execution	Yes	Remote code execution

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Remote access vulnerability exploit Remote Access Exploit	Yes	Remote access vulnerability exploit
	Remote file inclusion prevention Remote File Inclusion	Yes	Remote file inclusion prevention
	Remote file injection Remote File Injection	Yes	Remote file injection
	Combined vulnerability exploit Misc Exploit	Yes	Combined vulnerability exploit
	CMS vulnerability CMS Exploit	Yes	CMS vulnerability
	CSRF attack CSRF Attack	Yes	CSRF attack
	JNDI injection JNDI Injection Attack	Yes	JNDI injection
	Linux vulnerability Linux Exploit	Yes	Linux vulnerability
	SMB vulnerability SMB Exploit	Yes	SMB vulnerability
	Windows vulnerability Windows Exploit	Yes	Windows vulnerability
	XML injection XML Injection	Yes	XML injection
	Code Injection Code Injection	Yes	Code Injection

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Vulnerability escape Vulnerability Escape Attack	Yes	Vulnerability escape
	Command execution Command Execution	Yes	Command execution
	Command injection Command Injection	Yes	Command injection
	File escape File Escape Attack	Yes	File escape
	VM escape VM Escape Attack	Yes	VM escape
	Common vulnerability exploit General Exploit	Yes	Common vulnerability exploit
Command and control	Message sent from current ECS IP address to high-risk network Command Control Activity	Yes	Message sent from current ECS IP address to high-risk network
	Dynamic resolution Dynamic Resolution	Yes	Dynamic resolution
	Other suspicious connection Abnormal Connection	Yes	Other suspicious connection
	Other suspicious behavior Abnormal Behaviour	Yes	Other suspicious behavior

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Malicious DNS connection Malicious Domain Query	Yes	Malicious DNS connection
	Malicious IP address connection Malicious Ip Address Query	Yes	Malicious IP address connection
	Covert tunnel Protocol Tunneling	Yes	Covert tunnel
	Mining pool communication Mining Pool Communication	Yes	Mining pool communication
Other	Public_Opinion Public_Opinion	Yes	Public_Opinion
	Cloud firewall attack CFW_RISK	Yes	Cloud firewall attack
Data leakage	Data theft Steal Data	Yes	Data theft
	Unauthorized data transfer Transfer Data Abnormal	Yes	Unauthorized data transfer
Abnormal network behavior	Abnormal access frequency of IP addresses IP Access Frequency Abnormal	Yes	Abnormal access frequency of IP addresses
	Abnormal IP address switch IP Switch Abnormal	Yes	Abnormal IP address switch
	First login from an IP address IP First Access	Yes	First login from an IP address

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Sinkhole attack IP address access Sink Hole	Yes	Sinkhole attack IP address access
	Proxy IP address access Proxy	Yes	Proxy IP address access
	Malicious resource access Resource Permissions	Yes	Malicious resource access
	Fraudulent payment website IP address/domain name access Payment	Yes	Fraudulent payment website IP address/domain name access
	Onion website IP access Tor	Yes	Onion website IP access
	C&C abnormal communication C&C Abnormal Communication	Yes	C&C abnormal communication
	Blacklisted IP address access IP Blacklist Access	Yes	Blacklisted IP address access
	URL blacklist access URL Blacklist Access	Yes	URL blacklist access
	Malicious URL access Malicious URL Access	Yes	Malicious URL access
	Malicious domain name access Malicious Domain Name Access	Yes	Malicious domain name access

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Unauthorized access attempt Unauthorized Access Attempt	Yes	Unauthorized access attempt
	Suspicious network traffic Suspicious Network Traffic	Yes	Suspicious network traffic
	Container-network external connection Container Network Connect	Yes	Container-network external connection
	Unknown network access Unknown Abnormal Network Access	Yes	Unknown network access
	File MD5 blacklist access File MD5 Blacklist Access	Yes	File MD5 blacklist access
	Abnormal external connection Abnormal External Behavior	Yes	Abnormal external connection
	Domain name blacklist access Domain Name Blacklist Access	Yes	Domain name blacklist access
	Periodic external communication Periodic Outreach	Yes	Periodic external communication
	Suspicious port forwarding Suspicious Port Forward	Yes	Suspicious port forwarding
Fileless attacks	VDSO hijacking VDSO Hijacking	Yes	VDSO hijacking

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Dynamic library injection Dynamic Library Inject Process	Yes	Dynamic library injection
	Key configuration change Critical File Change	Yes	Key configuration change
	Environment variable change Environment Change	Yes	Environment variable change
	Process injection Process Inject	Yes	Process injection
	Memory file process Memfd Process	Yes	Memory file process
	File manipulation File Manipulation	Yes	File manipulation
Abnormal system behavior	Suspicious crontab task Crontab Suspicious Task	Yes	Suspicious crontab task
	Socket connection error Abnormal Socket Connection	Yes	Socket connection error
	Backup deletion Backup Deletion	Yes	Backup deletion
	Unauthorized database access Unauthorized Database Access	Yes	Unauthorized database access
	Abnormal permission access Privilege Abnormal Access	Yes	Abnormal permission access

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Abnormal log change Unexpected Log Change	Yes	Abnormal log change
	Exit the container process Container Process Exist	Yes	Exit the container process
	Abnormal behavior of unknown server Unknown Host Abnormal Activity	Yes	Abnormal behavior of unknown server
	File blacklist access File blocklist access	Yes	File blacklist access
	Abnormal change of file permission Unexpected File Permission Change	Yes	Abnormal change of file permission
	System protection disabled System Security Protection disabled	Yes	System protection disabled
	System account change System Account Change	Yes	System account change
	Suspicious registry operation Abnormal Registry Operation	Yes	Suspicious registry operation
	Crontab script privilege escalation Crontab Script Privilege Escalation	Yes	Crontab script privilege escalation

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Crontab script modification Crontab Script Change	Yes	Crontab script modification
	High-risk command execution High-risk Command Execution	Yes	High-risk command execution
	High-risk system call High-Risk Syscall	Yes	High-risk system call
	Important file/directory change File/Directory Change	Yes	Important file/directory change
	Critical file change Key File Change	Yes	Critical file change
	Process privilege escalation Process Privilege Escalation	Yes	Process privilege escalation
	Abnormal process behavior Process Abnormal Activity	Yes	Abnormal process behavior
	Sensitive file access Sensitive File Access	Yes	Sensitive file access
	Abnormal container process Container Abnormal Process	Yes	Abnormal container process
	Abnormal container startup Container Abnormal Start	Yes	Abnormal container startup

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Abnormal database connection Abnormal Database Connection	Yes	Abnormal database connection
	NIC in promiscuous mode Network Adapter Promiscuous Mode	Yes	NIC in promiscuous mode
	File privilege escalation File Privilege Escalation	Yes	File privilege escalation
	Abnormal file deletion File Abnormal Delete	Yes	Abnormal file deletion
	System startup script modification System Start Script Change	Yes	System startup script modification
	Abnormal shell Abnormal Shell	Yes	Abnormal shell
	Abnormal command execution Abnormal Command Execution	Yes	Abnormal command execution
Data damage	Information tampering Information Tampering	Yes	Information tampering
	Information loss Information Loss	Yes	Information loss
	Information counterfeiting Information Masquerading	Yes	Information counterfeiting

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Information theft Information Interception	Yes	Information theft
	Information leakage Information Disclosure	Yes	Information leakage
	Linux web tampering Linux Web Page Tampering	Yes	Linux web tampering
	Windows web tampering Windows Web Page Tampering	Yes	Windows web tampering
	Path Traversal Directory Traversal	Yes	Path Traversal
Abnormal user behavior	Malicious use of token Token Leakage	Yes	Malicious use of token
	Malicious token exploit success Token Leakage Success	Yes	Malicious token exploit success
	First login by an abnormal user User First Cross Domain Access	Yes	First login by an abnormal user
	Abnormal user access frequency User Access Frequency Abnormal	Yes	Abnormal user access frequency
	Abnormal time segment User Hour Level Access Abnormal	Yes	Abnormal time segment

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Abnormal user download behavior through a specific IP address User IP Download Abnormal	Yes	Abnormal user download behavior through a specific IP address
	First access to an object Client First Access	Yes	First access to an object
	Abnormal user download behavior User Download Abnormal	Yes	Abnormal user download behavior
	Brute-force attack Brute Force Cracking	Yes	Brute-force attack
	Illegal login Illegal Login	Yes	Illegal login
	Abnormal behavior of unknown users Unknown User Abnormal Activity	Yes	Abnormal behavior of unknown users
	Abnormal login Abnormal Login	Yes	Abnormal login
	Login attempt User Login Attempt	Yes	Login attempt
	Password theft User Password Theft	Yes	Password theft
	Successful user privilege escalation User Privilege Escalation Succeeded	Yes	Successful user privilege escalation

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Failed to elevate user rights User Privilege Escalation Failed	Yes	Failed to elevate user rights
	First login User First login	Yes	First login
	Account deletion User Account Removed	Yes	Account deletion
	Account creation User Account Added	Yes	Account creation
	User group change User Group Changed	Yes	User group change
	User group deletion User Group Removed	Yes	User group deletion
	User group addition User Group Added	Yes	User group addition
	Account spoofing Account Forgery	Yes	Account spoofing
	Suspicious ECS account creation Suspicious Ecs User Create	Yes	Suspicious ECS account creation
	ECS account permission escalation ECS User Escalate Privilege	Yes	ECS account permission escalation
	Suspicious IAM account creation Suspicious IAM Account Create	Yes	Suspicious IAM account creation

Type Name	Sub Type/Sub Type Tag	Preset	Description
	IAM permission escalation IAM Permissions Escalation	Yes	IAM permission escalation
	ECS login through brute-force attack ECS BruteForce Login	Yes	ECS login through brute-force attack
	IAM login through brute-force attack IAM BruteForce Login	Yes	IAM login through brute-force attack
	Invalid account Invalid System Account	Yes	Invalid account
	Unsafe account Risky Account	Yes	Unsafe account
	ECS login from suspicious IP address Suspicious IP Address Login	Yes	ECS login from suspicious IP address
	Suspicious IP address login to IAM Suspicious IP Address Login	Yes	Suspicious IP address login to IAM
	Abnormal login to IAM IAM Abnormal Login	Yes	Abnormal login to IAM
	Remote login to ECS Instance Credential Exfiltration	Yes	Remote login to ECS
	User login success User Login Success	Yes	User login success
	User login denial User Login Denied	Yes	User login denial

Type Name	Sub Type/Sub Type Tag	Preset	Description
	User account change User Account Changed	Yes	User account change
Resource manipulation	Malicious logic insertion Malicious Logic Insertion	Yes	Malicious logic insertion
	Infrastructure manipulation Infrastructure Manipulation	Yes	Infrastructure manipulation
	Configuration/environment manipulation Configuration/Environment Manipulation	Yes	Configuration/environment manipulation
	Container escape Container Escape	Yes	Container escape
	Container resource manipulation Container Resource Manipulation	Yes	Container resource manipulation
	Software integrity Software Integrity Attack	Yes	Software integrity
	Resource scanning	Abnormal number of detected ports Port Detection	Yes
ARP scan ARP Scan		Yes	ARP scan
DNS test DNS Recon		Yes	DNS test
Hypervisor detection Hypervisor Recon		Yes	Hypervisor detection

Type Name	Sub Type/Sub Type Tag	Preset	Description
	ICMP detection ICMP Recon	Yes	ICMP detection
	Linux detection Linux Recon	Yes	Linux detection
	MacOS detection MacOS Recon	Yes	MacOS detection
	Nmap scan NMAP Scan	Yes	Nmap scan
	RPC request detection RPC Recon	Yes	RPC request detection
	SNMP scan SNMP Recon	Yes	SNMP scan
	TCP scan TCP Recon	Yes	TCP scan
	UDP scan UDP Recon	Yes	UDP scan
	Unix detection Unix Recon	Yes	Unix detection
	Web detection Web Recon	Yes	Web detection
	Windows probing Windows Recon	Yes	Windows probing
	Encrypted penetration scan Encrypted Penetration Scan	Yes	Encrypted penetration scan
	Common scan event General Scanner	Yes	Common scan event
	Database detection Database Recon	Yes	Database detection
	Mail detection Mail Recon	Yes	Mail detection

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Server scan Host Scan	Yes	Server scan
	Combined detection Misc Recon	Yes	Combined detection
	Port scan Port Scan	Yes	Port scan

Preset Incident Types

Table 6-3 Preset incident types

Type Name	Sub Type/Sub Type Tag	Preset	Description
DDoS attack	DNS protocol attacks Tcp Dns	Yes	DNS protocol attacks
	Unusual ports Unusual Network Port	Yes	Unusual ports
	Abnormal protocol attacks Unusual Protocol	Yes	Abnormal protocol attacks
	ACK Flood ACK Flood	Yes	ACK Flood
	BGP flood BGP Flood Attack	Yes	BGP flood
	DNS IP TTL DNS IP TTL Check Fail	Yes	DNS IP TTL
	DNS reply flood DNS Reply Flood	Yes	DNS reply flood
	DNS query flood DNS Query Flood	Yes	DNS query flood

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Abnormal DNS size DNS Size Abnormal	Yes	Abnormal DNS size
	DNS reflection DNS Reflection	Yes	DNS reflection
	Abnormal DNS response flow DNS Reply Domain Flow Abnormal	Yes	Abnormal DNS response flow
	Invalid DNS format DNS Format Error	Yes	Invalid DNS format
	DNS cache matching DNS Cache Match	Yes	DNS cache matching
	DNS cache poisoning DNS Cache Poisoning	Yes	DNS cache poisoning
	Abnormal DNS request flow DNS Request Domain Flow Abnormal	Yes	Abnormal DNS request flow
	DNS domain name errors DNS No Such Name	Yes	DNS domain name errors
	FIN/RST Flood FIN/RST Flood	Yes	FIN/RST Flood
	HTTPS Flood HTTPS Flood	Yes	HTTPS Flood
	HTTP slow attacks HTTP Slow Attack	Yes	HTTP slow attacks
	ICMP blocking ICMP Protocol Block	Yes	ICMP blocking

Type Name	Sub Type/Sub Type Tag	Preset	Description
	IP reputation IP Reputation	Yes	IP reputation
	SIP Flood SIP Flood	Yes	SIP Flood
	Abnormal SIP source rate SIP Source Rate Abnormity	Yes	Abnormal SIP source rate
	SYN Flood SYN Flood	Yes	SYN Flood
	SYN-ACK Flood SYN-ACK Flood	Yes	SYN-ACK Flood
	TCP bandwidth overflow TCP Bandwidth Overflow	Yes	TCP bandwidth overflow
	TCP multi-connection attacks TCP Connection Flood	Yes	TCP multi-connection attacks
	TCP fragment bandwidth overflow TCP Fragment Bandwidth Overflow	Yes	TCP fragment bandwidth overflow
	TCP fragment attacks TCP Fragment Flood	Yes	TCP fragment attacks
	Malformed TCP packets TCP Malformed	Yes	Malformed TCP packets
	TCP/UDP attacks TCP-authenticated UDP Attack	Yes	TCP/UDP attacks
	TCP blocking TCP Protocol Block	Yes	TCP blocking

Type Name	Sub Type/Sub Type Tag	Preset	Description
	UDP bandwidth overflow UDP Bandwidth Overflow	Yes	UDP bandwidth overflow
	UDP fragments UDP Fragment Flood	Yes	UDP fragments
	UDP fragment bandwidth overflow UDP Fragment Bandwidth Overflow	Yes	UDP fragment bandwidth overflow
	Malformed UDP packets UDP Malformed	Yes	Malformed UDP packets
	UDP blocking UDP Protocol Block	Yes	UDP blocking
	URI monitoring URI Monitor	Yes	URI monitoring
	Dark web IP addresses Dark IP	Yes	Dark web IP addresses
	Single EIP bandwidth overflow Single IP Bandwidth Overflow	Yes	Single EIP bandwidth overflow
	Current connection flood attacks Concurrent Connections Flood	Yes	Current connection flood attacks
	Port scan attacks Port Scanning Attack	Yes	Port scan attacks

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Malicious domain name attacks Malicious Domains Attack	Yes	Malicious domain name attacks
	Anti-malware Anti-Malware	Yes	Anti-malware
	DDoS attacks DDOS	Yes	DDoS attacks
	Partition bandwidth overflow Zone Bandwidth Overflow	Yes	Partition bandwidth overflow
	Filter attacks Filter Attack	Yes	Filter attacks
	Blacklist Blacklist	Yes	Blacklist
	Botnets/Trojans/Worms Botnets/Trojan horses/Worms Attack	Yes	Botnets/Trojans/Worms
	Destination IP new session rate limiting Destination IP new session rate limiting	Yes	Destination IP new session rate limiting
	Other flood attacks Other Flood	Yes	Other flood attacks
	Other bandwidth overflow Other Bandwidth Overflow	Yes	Other bandwidth overflow
	Other global exceptions Global Other Abnormal	Yes	Other global exceptions

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Other protocol blocking Other Protocol Block	Yes	Other protocol blocking
	Global ICMP exception Global ICMP Abnormal	Yes	Global ICMP exception
	Abnormal global TCP fragments Global TCP Fragment Abnormal	Yes	Abnormal global TCP fragments
	Global TCP exception Global TCP Abnormal	Yes	Global TCP exception
	Abnormal global UDP fragments Global UDP Fragment Abnormal	Yes	Abnormal global UDP fragments
	Global UDP exception Global UDP Abnormal	Yes	Global UDP exception
	Web attacks Web Attack	Yes	Web attacks
	Geolocation attacks Location Attack	Yes	Geolocation attacks
	Connection flood attack New Connections Flood	Yes	Connection flood attack
	Domain hijacking Domain Hijacking	Yes	Domain hijacking

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Abnormal source DNS response traffic Source DNS Reply Flow Abnormal	Yes	Abnormal source DNS response traffic
	Abnormal source DNS request traffic Source DNS Request Flow Abnormal	Yes	Abnormal source DNS request traffic
	Host traffic overflow Host Traffic Over Flow	Yes	Host traffic overflow
	HTTP Flood HTTP Flood	Yes	HTTP Flood
	ICMP Flood ICMP Flood	Yes	ICMP Flood
	SSL Flood SSL Flood	Yes	SSL Flood
	TCP Flood TCP Flood	Yes	TCP Flood
	UDP Flood UDP Flood	Yes	UDP Flood
	XML Flood XML Flood	Yes	XML Flood
	Amplification attacks Amplification	Yes	Amplification attacks
Malicious code	Hidden link Web Page Dark Link	Yes	Hidden link
	Web page Trojan Web Page Trojan	Yes	Web page Trojan

Type Name	Sub Type/Sub Type Tag	Preset	Description
Web attacks	Webshell Webshell	Yes	Webshell
	WAF robot WAF Robot	Yes	WAF robot
	IP address whitelist White IP	Yes	IP address whitelist
	Known attack source Known Attack Source	Yes	Known attack source
	IP address blacklist Black IP	Yes	IP address blacklist
	Vulnerability exploits Vulnerability Attack	Yes	Vulnerability exploits
	Data masking Leakage	Yes	Data masking
	Default Default	Yes	Default
	Scanners/Crawlers Scanner & Crawler	Yes	Scanners/Crawlers
	CC attacks Challenge Collapsar	Yes	CC attacks
	IP reputation database IP Reputaion	Yes	IP reputation database
	SQL injection SQL Injection	Yes	SQL injection
	XSS Cross-Site Scripting	Yes	XSS
	Local file inclusion Local Code Inclusion	Yes	Local file inclusion

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Geolocation access control Geo IP	Yes	Geolocation access control
	Malicious crawlers Malicious Web Crawlers	Yes	Malicious crawlers
	Anti-crawler Anticrawler	Yes	Anti-crawler
	Web tampering protection AntiTamper	Yes	Web tampering protection
	Invalid requests Illegal Access	Yes	Invalid requests
	Blacklist or whitelist alarms White or Black IP	Yes	Blacklist or whitelist alarms
	Precise protection Custom Rule	Yes	Precise protection
	Command injection Command Injection	Yes	Command injection
	Path Traversal Path Traversal	Yes	Path Traversal
	Website Trojans Website Trojan	Yes	Website Trojans
	Website data leakage Information Leakage	Yes	Website data leakage
	Information leakage Web Service Exfiltration	Yes	Information leakage

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Remote code execution Remote Code Execute	Yes	Remote code execution
	Remote file inclusion Remote Code Inclusion	Yes	Remote file inclusion
Malware	Encrypted currency mining Cryptomining	Yes	Encrypted currency mining
	Docker malicious program Docker Malware	Yes	Docker malicious program
	Fishing Phishing	Yes	Fishing
	Malicious adware Adware	Yes	Malicious adware
	Malware Malicious Software	Yes	Malware
	Hacker tool Hacktool	Yes	Hacker tool
	Grayware Grayware	Yes	Grayware
	Spyware Spyware	Yes	Spyware
	Spam Spam	Yes	Spam
	Rootkit Rootkit	Yes	Rootkit
	Webshell Webshell	Yes	Webshell
	Virus/Worm Virus and Worm	Yes	Virus/Worm

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Malicious file Malicious File	Yes	Malicious file
	Reverse shell Reverse Shell	Yes	Reverse shell
	Trojan Backdoor Trojan	Yes	Trojan
	Botnet Botnet Program	Yes	Botnet
	Ransomware Ransomware	Yes	Ransomware
	Bitcoin Miner Bitcoin Miner	Yes	Bitcoin Miner
	Mining software Mining Software	Yes	Mining software
Risk Audit	Web-CMS Vulnerability Webcms Vulnerability	Yes	Web-CMS Vulnerability
	Windows OS vulnerabilities Windows Vulnerability	Yes	Windows OS vulnerabilities
	Local access vulnerability Local Access Vulnerability	Yes	Local access vulnerability
	Incorrect configuration policy Mis-Configured Policy	Yes	Incorrect configuration policy
	Other OS vulnerability Other OS Vulnerability	Yes	Other OS vulnerability
	Other vulnerability Other Vulnerability	Yes	Other vulnerability

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Application vulnerability Application Vulnerability	Yes	Application vulnerability
	Remote access vulnerability Remote Access Vulnerability	Yes	Remote access vulnerability
Risk Audit	Weak Password Weak Password	Yes	Weak Password
	Risky system configuration System Risk Configuration	Yes	Risky system configuration
Attacks	Fishing Phishing	Yes	Fishing
	Network topology Map Network Topology	Yes	Network topology
	Account and group information collection Identify Groups/Roles	Yes	Account and group information collection
	Fingerprint scan Fingerprinting	Yes	Fingerprint scan
	Host discovery Determine IP Address	Yes	Host discovery

Type Name	Sub Type/Sub Type Tag	Preset	Description
Vulnerability exploit	ActiveX vulnerability exploit ActiveX Exploit	Yes	ActiveX vulnerability exploit
	CGI attack CGI Attack	Yes	CGI attack
	DNS vulnerability exploit DNS Exploit	Yes	DNS vulnerability exploit
	FTP vulnerability exploit FTP Exploit	Yes	FTP vulnerability exploit
	Hadoop vulnerability exploit Hadoop Vulnerability Exploit	Yes	Hadoop vulnerability exploit
	Vulnerability exploit of hypervisor Hypervisor Exploit	Yes	Vulnerability exploit of hypervisor
	LDAP injection LDAP Injection Attack	Yes	LDAP injection
	MacOS vulnerability exploit MacOS Exploit	Yes	MacOS vulnerability exploit
	MySQL vulnerability exploit MySQL Vulnerability Exploit	Yes	MySQL vulnerability exploit
Vulnerability exploit of Office software Office Exploit	Yes	Vulnerability exploit of Office software	

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Redis vulnerability exploit Redis Vulnerability Exploit	Yes	Redis vulnerability exploit
	RPC vulnerability exploit RPC Exploit	Yes	RPC vulnerability exploit
	SQL injection SQL Injection	Yes	SQL injection
	SSH vulnerability exploit SSH Exploit	Yes	SSH vulnerability exploit
	SSI injection attack SSI Injection Attack	Yes	SSI injection attack
	Struts2 OGNL injection Struts2 OGNL Injection	Yes	Struts2 OGNL injection
	Telnet vulnerability exploit TELNET Exploit	Yes	Telnet vulnerability exploit
	Unix vulnerability exploit Unix Exploit	Yes	Unix vulnerability exploit
	Web vulnerability exploit Web Exploit	Yes	Web vulnerability exploit
	Cross site scripting (XSS) Cross-Site Scripting	Yes	Cross site scripting (XSS)
	Local file inclusion Local File Inclusion	Yes	Local file inclusion
	Malicious file delivery Malicious File Delivery	Yes	Malicious file delivery

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Malicious file execution Malicious File Execution	Yes	Malicious file execution
	Buffer overflow attack Buffer Overflow	Yes	Buffer overflow attack
	Session hijacking Session Hijack	Yes	Session hijacking
	Password guessing Password Cracking	Yes	Password guessing
	Browser vulnerability exploit Browser Exploit	Yes	Browser vulnerability exploit
	Weak password access Weak Password Access	Yes	Weak password access
	Database vulnerability exploit Database Exploit	Yes	Database vulnerability exploit
	Unknown vulnerability exploit Unknown Exploit	Yes	Unknown vulnerability exploit
	Hidden link access Hide Link Access	Yes	Hidden link access
	Email vulnerability exploit Mail Exploit	Yes	Email vulnerability exploit
	Remote code execution Remote Code Execution	Yes	Remote code execution

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Remote access vulnerability exploit Remote Access Exploit	Yes	Remote access vulnerability exploit
	Remote file inclusion prevention Remote File Inclusion	Yes	Remote file inclusion prevention
	Remote file injection Remote File Injection	Yes	Remote file injection
	Combined vulnerability exploit Misc Exploit	Yes	Combined vulnerability exploit
	CMS vulnerability CMS Exploit	Yes	CMS vulnerability
	CSRF attack CSRF Attack	Yes	CSRF attack
	JNDI injection JNDI Injection Attack	Yes	JNDI injection
	Linux vulnerability Linux Exploit	Yes	Linux vulnerability
	SMB vulnerability SMB Exploit	Yes	SMB vulnerability
	Windows vulnerability Windows Exploit	Yes	Windows vulnerability
	XML injection XML Injection	Yes	XML injection
	Code Injection Code Injection	Yes	Code Injection

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Vulnerability escape Vulnerability Escape Attack	Yes	Vulnerability escape
	Command execution Command Execution	Yes	Command execution
	Command injection Command Injection	Yes	Command injection
	File escape File Escape Attack	Yes	File escape
	VM escape VM Escape Attack	Yes	VM escape
	Common vulnerability exploit General Exploit	Yes	Common vulnerability exploit
Command and control	Message sent from current ECS IP address to high-risk network Command Control Activity	Yes	Message sent from current ECS IP address to high-risk network
	Dynamic resolution Dynamic Resolution	Yes	Dynamic resolution
	Other suspicious connection Abnormal Connection	Yes	Other suspicious connection
	Other suspicious behavior Abnormal Behaviour	Yes	Other suspicious behavior

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Malicious DNS connection Malicious Domain Query	Yes	Malicious DNS connection
	Malicious IP address connection Malicious Ip Address Query	Yes	Malicious IP address connection
	Covert tunnel Protocol Tunneling	Yes	Covert tunnel
	Mining pool communication Mining Pool Communication	Yes	Mining pool communication
Other	Public_Opinion Public_Opinion	Yes	Public_Opinion
	Cloud firewall attack CFW_RISK	Yes	Cloud firewall attack
Data leakage	Data theft Steal Data	Yes	Data theft
	Unauthorized data transfer Transfer Data Abnormal	Yes	Unauthorized data transfer
Abnormal network behavior	Abnormal access frequency of IP addresses IP Access Frequency Abnormal	Yes	Abnormal access frequency of IP addresses
	Abnormal IP address switch IP Switch Abnormal	Yes	Abnormal IP address switch
	First login from an IP address IP First Access	Yes	First login from an IP address

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Sinkhole attack IP address access Sink Hole	Yes	Sinkhole attack IP address access
	Proxy IP address access Proxy	Yes	Proxy IP address access
	Malicious resource access Resource Permissions	Yes	Malicious resource access
	Fraudulent payment website IP address/domain name access Payment	Yes	Fraudulent payment website IP address/ domain name access
	Onion website IP access Tor	Yes	Onion website IP access
	C&C abnormal communication C&C Abnormal Communication	Yes	C&C abnormal communication
	Blacklisted IP address Access IP Blacklist Access	Yes	Blacklisted IP address Access
	URL blacklist access URL Blacklist Access	Yes	URL blacklist access
	Malicious URL access Malicious URL Access	Yes	Malicious URL access
	Malicious domain name access Malicious Domain Name Access	Yes	Malicious domain name access

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Unauthorized access attempt Unauthorized Access Attempt	Yes	Unauthorized access attempt
	Suspicious network traffic Suspicious Network Traffic	Yes	Suspicious network traffic
	Container-network external connection Container Network Connect	Yes	Container-network external connection
	Unknown network access Unknown Abnormal Network Access	Yes	Unknown network access
	File MD5 blacklist access File MD5 Blacklist Access	Yes	File MD5 blacklist access
	Abnormal external connection Abnormal External Behavior	Yes	Abnormal external connection
	Domain name blacklist access Domain Name Blacklist Access	Yes	Domain name blacklist access
	Periodic external communication Periodic Outreach	Yes	Periodic external communication
	Suspicious port forwarding Suspicious Port Forward	Yes	Suspicious port forwarding
Fileless attacks	VDSO hijacking VDSO Hijacking	Yes	VDSO hijacking

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Dynamic library injection Dynamic Library Inject Process	Yes	Dynamic library injection
	Key configuration change Critical File Change	Yes	Key configuration change
	Environment variable change Environment Change	Yes	Environment variable change
	Process injection Process Inject	Yes	Process injection
	Memory file process Memfd Process	Yes	Memory file process
	File manipulation File Manipulation	Yes	File manipulation
Abnormal system behavior	Suspicious crontab task Crontab Suspicious Task	Yes	Suspicious crontab task
	Socket connection error Abnormal Socket Connection	Yes	Socket connection error
	Backup deletion Backup Deletion	Yes	Backup deletion
	Unauthorized database access Unauthorized Database Access	Yes	Unauthorized database access
	Abnormal permission access Privilege Abnormal Access	Yes	Abnormal permission access

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Abnormal log change Unexpected Log Change	Yes	Abnormal log change
	Exit the container process Container Process Exist	Yes	Exit the container process
	Abnormal behavior of unknown server Unknown Host Abnormal Activity	Yes	Abnormal behavior of unknown server
	File blacklist access File blocklist access	Yes	File blacklist access
	Abnormal change of file permission Unexpected File Permission Change	Yes	Abnormal change of file permission
	System protection disabled System Security Protection disabled	Yes	System protection disabled
	System account change System Account Change	Yes	System account change
	Suspicious registry operation Abnormal Registry Operation	Yes	Suspicious registry operation
	Crontab script privilege escalation Crontab Script Privilege Escalation	Yes	Crontab script privilege escalation

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Crontab script modification Crontab Script Change	Yes	Crontab script modification
	High-risk command execution High-risk Command Execution	Yes	High-risk command execution
	High-risk system call High-Risk Syscall	Yes	High-risk system call
	Important file/directory change File/Directory Change	Yes	Important file/directory change
	Critical file change Key File Change	Yes	Critical file change
	Process privilege escalation Process Privilege Escalation	Yes	Process privilege escalation
	Abnormal process behavior Process Abnormal Activity	Yes	Abnormal process behavior
	Sensitive file access Sensitive File Access	Yes	Sensitive file access
	Abnormal container process Container Abnormal Process	Yes	Abnormal container process
	Abnormal container startup Container Abnormal Start	Yes	Abnormal container startup

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Abnormal database connection Abnormal Database Connection	Yes	Abnormal database connection
	NIC in promiscuous mode Network Adapter Promiscuous Mode	Yes	NIC in promiscuous mode
	File privilege escalation File Privilege Escalation	Yes	File privilege escalation
	Abnormal file deletion File Abnormal Delete	Yes	Abnormal file deletion
	System startup script modification System Start Script Change	Yes	System startup script modification
	Abnormal shell Abnormal Shell	Yes	Abnormal shell
	Abnormal command execution Abnormal Command Execution	Yes	Abnormal command execution
Data damage	Information tampering Information Tampering	Yes	Information tampering
	Information loss Information Loss	Yes	Information loss
	Information counterfeiting Information Masquerading	Yes	Information counterfeiting

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Information theft Information Interception	Yes	Information theft
	Information leakage Information Disclosure	Yes	Information leakage
	Linux web tampering Linux Web Page Tampering	Yes	Linux web tampering
	Windows web tampering Windows Web Page Tampering	Yes	Windows web tampering
	Path Traversal Directory Traversal	Yes	Path Traversal
Abnormal user behavior	Malicious use of token Token Leakage	Yes	Malicious use of token
	Malicious token exploit success Token Leakage Success	Yes	Malicious token exploit success
	First login by an abnormal user User First Cross Domain Access	Yes	First login by an abnormal user
	Abnormal user access frequency User Access Frequency Abnormal	Yes	Abnormal user access frequency
	Abnormal time segment User Hour Level Access Abnormal	Yes	Abnormal time segment

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Abnormal user download behavior through a specific IP address User IP Download Abnormal	Yes	Abnormal user download behavior through a specific IP address
	First access to an object Client First Access	Yes	First access to an object
	Abnormal user download behavior User Download Abnormal	Yes	Abnormal user download behavior
	Brute-force attacks Brute Force Cracking	Yes	Brute-force attacks
	Illegal login Illegal Login	Yes	Illegal login
	Abnormal behavior of unknown users Unknown User Abnormal Activity	Yes	Abnormal behavior of unknown users
	Abnormal login Abnormal Login	Yes	Abnormal login
	Login attempt User Login Attempt	Yes	Login attempt
	Password theft User Password Theft	Yes	Password theft
	Successful user privilege escalation User Privilege Escalation Succeeded	Yes	Successful user privilege escalation

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Failed to elevate user rights User Privilege Escalation Failed	Yes	Failed to elevate user rights
	First login User First login	Yes	First login
	Account deletion User Account Removed	Yes	Account deletion
	Account creation User Account Added	Yes	Account creation
	User group change User Group Changed	Yes	User group change
	User group deletion User Group Removed	Yes	User group deletion
	User group addition User Group Added	Yes	User group addition
	Account spoofing Account Forgery	Yes	Account spoofing
	Suspicious ECS account creation Suspicious Ecs User Create	Yes	Suspicious ECS account creation
	ECS account permission escalation ECS User Escalate Privilege	Yes	ECS account permission escalation
	Suspicious IAM account creation Suspicious IAM Account Create	Yes	Suspicious IAM account creation

Type Name	Sub Type/Sub Type Tag	Preset	Description
	IAM permission escalation IAM Permissions Escalation	Yes	IAM permission escalation
	ECS login through brute-force attack ECS BruteForce Login	Yes	ECS login through brute-force attack
	IAM login through brute-force attack IAM BruteForce Login	Yes	IAM login through brute-force attack
	Invalid account Invalid System Account	Yes	Invalid account
	Unsafe account Risky Account	Yes	Unsafe account
	ECS login from suspicious IP address Suspicious IP Address Login	Yes	ECS login from suspicious IP address
	Suspicious IP address login to IAM Suspicious IP Address Login	Yes	Suspicious IP address login to IAM
	Abnormal login to IAM IAM Abnormal Login	Yes	Abnormal login to IAM
	Remote login to ECS Instance Credential Exfiltration	Yes	Remote login to ECS
	User login success User Login Success	Yes	User login success
	User login denial User Login Denied	Yes	User login denial

Type Name	Sub Type/Sub Type Tag	Preset	Description
	User account change User Account Changed	Yes	User account change
Resource manipulation	Malicious logic insertion Malicious Logic Insertion	Yes	Malicious logic insertion
	Infrastructure manipulation Infrastructure Manipulation	Yes	Infrastructure manipulation
	Configuration/environment manipulation Configuration/Environment Manipulation	Yes	Configuration/environment manipulation
	Container escape Container Escape	Yes	Container escape
	Container resource manipulation Container Resource Manipulation	Yes	Container resource manipulation
	Software integrity Software Integrity Attack	Yes	Software integrity
	Resource scanning	Abnormal number of detected ports Port Detection	Yes
ARP scan ARP Scan		Yes	ARP scan
DNS test DNS Recon		Yes	DNS test
Hypervisor detection Hypervisor Recon		Yes	Hypervisor detection

Type Name	Sub Type/Sub Type Tag	Preset	Description
	ICMP detection ICMP Recon	Yes	ICMP detection
	Linux detection Linux Recon	Yes	Linux detection
	MacOS detection MacOS Recon	Yes	MacOS detection
	Nmap scan NMAP Scan	Yes	Nmap scan
	RPC request detection RPC Recon	Yes	RPC request detection
	SNMP scan SNMP Recon	Yes	SNMP scan
	TCP scan TCP Recon	Yes	TCP scan
	UDP scan UDP Recon	Yes	UDP scan
	Unix detection Unix Recon	Yes	Unix detection
	Web detection Web Recon	Yes	Web detection
	Windows probing Windows Recon	Yes	Windows probing
	Encrypted penetration scan Encrypted Penetration Scan	Yes	Encrypted penetration scan
	Common scan event General Scanner	Yes	Common scan event
	Database detection Database Recon	Yes	Database detection
	Mail detection Mail Recon	Yes	Mail detection

Type Name	Sub Type/Sub Type Tag	Preset	Description
	Server scan Host Scan	Yes	Server scan
	Combined detection Misc Recon	Yes	Combined detection
	Port scan Port Scan	Yes	Port scan

Preset Threat Indicator Types

Table 6-4 Preset threat indicator types

Type Name/Type Tag	Preset	Description
IPv4 IPv4	Yes	IPv4
IPv6 IPv6	Yes	IPv6
Email Email	Yes	Email
Domain name domain	Yes	Domain name
URL URL	Yes	URL
Other Unclassified	Yes	Other

Preset Vulnerability Types

Table 6-5 Preset vulnerability types

Type Name/Type Tag	Preset	Description
Website vulnerabilities Website Vulnerabilities	Yes	Website vulnerabilities

Type Name/Type Tag	Preset	Description
Linux vulnerabilities Linux Vulnerabilities	Yes	Linux vulnerabilities
Web-CMS vulnerabilities Web-CMS Vulnerabilities	Yes	Web-CMS vulnerabilities
Windows vulnerabilities Windows Vulnerabilities	Yes	Windows vulnerabilities
Application vulnerabilities Application Vulnerabilities	Yes	Application vulnerabilities

7 Limitations and Constraints

This section describes the limitations and constraints on using SecMaster.

About Purchase

Table 7-1 Purchase operations

Module	Limitations and Constraints
Quota	<ul style="list-style-type: none"> • The quota must be greater than or equal to the total number of ECSs within your account. This value cannot be changed to a smaller one after your purchase is complete. • The maximum quota is 10,000.
Value-added package	<ul style="list-style-type: none"> • The basic edition does not support the value-added packages. To use functions in the value-added packages, upgrade the basic edition to the standard or professional edition. • Value-added packages cannot be used independently. <ul style="list-style-type: none"> – To purchase a value-added package, purchase the standard or professional edition first. – If you unsubscribe from the pay-per-use professional edition, the system automatically unsubscribes from the value-added packages. – If you unsubscribe from the yearly/monthly standard or professional edition, you need to manually unsubscribe from the value-added packages you have.
Tag	A maximum of 10 tags can be added for SecMaster.

Workspaces

Table 7-2 Workspaces

Module	Limitations and Constraints
Workspaces	<ul style="list-style-type: none"> ● Paid SecMaster: A maximum of five workspaces can be created for a single account in a single region. ● Free SecMaster: Only one workspace can be created for a single account in a single region. ● Currently, performing operations across different workspaces in multiple browser windows at the same time is not supported.
Managed environments	<ul style="list-style-type: none"> ● Edge sites, such as IEC, DeC, and IES, cannot be managed. ● Only the default project can be managed. Sub-projects cannot be managed. ● Resources cannot be managed by EPS.
Agencies	<ul style="list-style-type: none"> ● A maximum of one workspace agency view can be created for an account in a region. ● A maximum of 150 workspaces from different regions and accounts can be managed by a workspace agency view. ● A maximum of 10 agencies can be created for an account.

Security Reports

Table 7-3 Security Reports

Module	Limitations and Constraints
Security Reports	A maximum of 10 security reports (including daily, weekly, and monthly reports) can be created in a workspace of an account.

Alert Models

Table 7-4 Alert Models

Module	Limitations and Constraints
Alert Models	<ul style="list-style-type: none"> • A maximum of 100 alert models can be created in a single workspace under a single account in a single region. • The running interval of an alert model must be greater than or equal to 5 minutes, and the time range for querying data must be less than or equal to 14 days.

Security Analysis

Table 7-5 Security Analysis

Module	Limitations and Constraints
Query and analysis	<ul style="list-style-type: none"> • A maximum of 500 results can be returned for a single analysis query. • A maximum of 50 shortcut queries can be created in a pipeline. That is, a maximum of 50 query analysis criteria can be saved as shortcut queries. • If there are over 50,000 results for a single query, the accuracy may decrease. In this case, you can select a short time range or apply more filter criteria to reduce the number of query results. • In aggregation queries (for example, GROUP BY statement) based on several fields, the default number of buckets for the second field is 10. If more than 10 buckets are generated, part of qualified data will be lost. In this case, the query results are not accurate. • A maximum of 100 query and analysis results can be saved as metric cards in a workspace for an account.
Data Space	A maximum of five data spaces can be created in a workspace in a region for an account.
Data Pipelines	A maximum of 20 pipelines can be created in a data space in a region for an account.

Incidents, Alerts, Indicators, And Vulnerabilities

Table 7-6 Security Reports

Module	Limitations and Constraints
Vulnerabilities	A maximum of 100 vulnerabilities can be added every day in a workspace for an account.
Alerts	<ul style="list-style-type: none"> • A maximum of 100 alerts can be added every day in a workspace of an account. • In a workspace of an account, a maximum of 100 alerts can be converted into incidents each day.
Incidents	A maximum of 100 incidents can be added every day in a workspace of an account.
Indicators	A maximum of 100 indicators can be added every day in a workspace of an account.

Security Orchestration

Table 7-7 Security Orchestration

Module	Limitations and Constraints
Playbooks	In a single workspace of an account, the scheduling frequency of a single playbook is greater than or equal to 5 minutes.
Playbook and workflow instances	<p>The maximum number of retries within a day for a single workspace of an account is as follows:</p> <ul style="list-style-type: none"> • Manual retries: 100. After a retry, the playbook cannot be retried until the current execution is complete. • API retries: 100. After a retry, the playbook cannot be retried until the current execution is complete.
Classification & Mapping	<ul style="list-style-type: none"> • In a single workspace of a single account, a maximum of 50 classification & mapping templates can be created. • In a single workspace of a single account, the proportion of a classification to its mappings is 1:100. • A maximum of 100 classifications and mappings can be added to a workspace of a single account.

8 Security

8.1 Shared Responsibilities

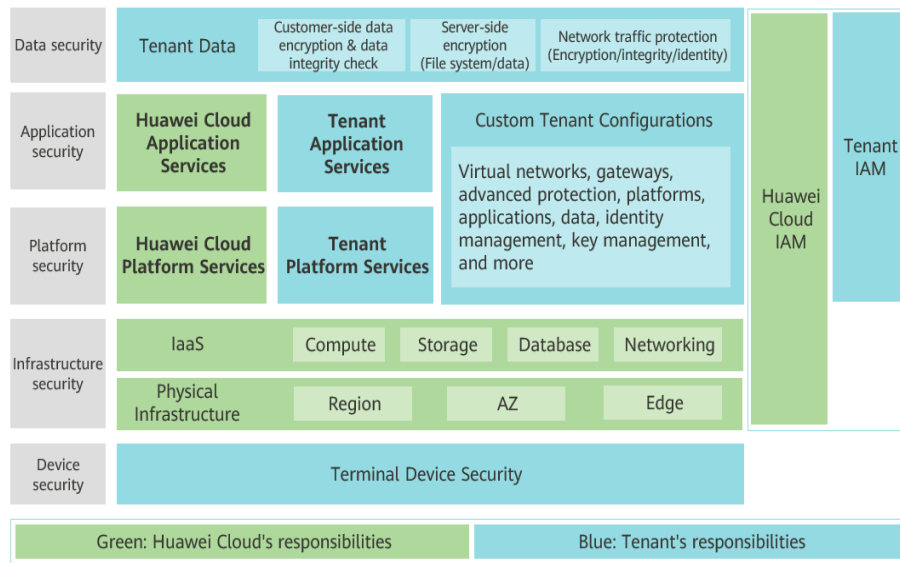
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 8-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud:** Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant:** Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 8-1 Huawei Cloud shared security responsibility model



8.2 Identity Authentication and Access Control

SecMaster works with Identity and Access Management (IAM). SecMaster authenticates user identities and controls access to SecMaster through IAM.

Identity and Access Management (IAM) is a basic service of Huawei Cloud that provides permissions management to help you securely control access to SecMaster.

With IAM, you can add users to a user group and configure policies to control their access to SecMaster resources. You can allow or deny access to a specific SecMaster resource in a fine-grained manner.

8.3 Data Protection Technologies

SecMaster takes different measures to keep data secure and reliable.

Table 8-1 SecMaster data protection methods and features

Method	Description
Static data protection	SecMaster encrypts sensitive data in your website traffic to keep the data from leakage.
Protection for data in transit	Data is encrypted when it is transmitted between microservices to prevent leakage or tampering during transmission. SecMaster keeps your configuration data secure as the configuration data is transmitted over HTTPS.

Method	Description
Data integrity verification	<ol style="list-style-type: none"> 1. Data integrity is verified when SecMaster accesses cloud service alerts, vulnerabilities, and baselines. 2. When the SecMaster core data plane process is started, the configuration data enters the reliable mode to ensure data integrity (in scenarios such as network jitter, delay, and configuration data retransmission and retry).
Data isolation mechanism	SecMaster isolates its tenant zone from its management plane. Operation permissions for CFW are isolated by user. Your policies and logs are isolated from those of others.
Data destruction mechanism	To prevent information leakage caused by residual data, Huawei Cloud sets different retention periods based on the customer level. If the customer does not renew the subscription or recharge the account after the retention period expires, the data stored in the cloud service will be deleted and the cloud service resources will be released. SecMaster automatically detects cloud service subscription status and releases resources when the retention period expires.

In addition, SecMaster fully respects user privacy, complies with laws and regulations, and does not collect or store any user privacy data. For more privacy data usage and protection issues, see [Privacy Statement](#).

8.4 Audit Logs

- Audit

Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

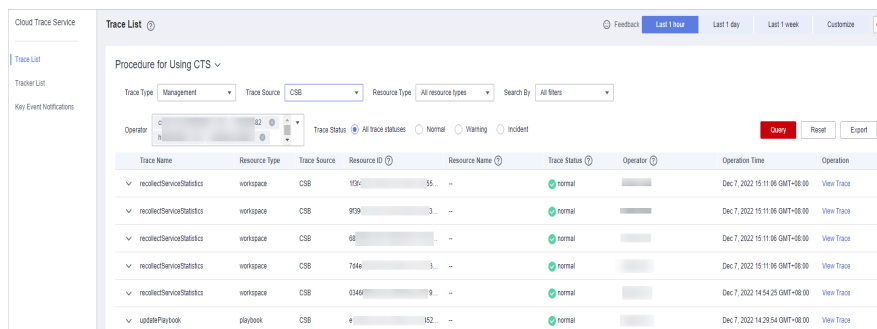
After you enable CTS and configure a tracker, CTS can record management and data traces of SecMaster for auditing.

For details about how to enable and configure CTS, see [Enabling CTS](#).
- Logs
 - Querying logs

After you enable CTS, the system starts recording operations on SecMaster. You can view the operation records of the last 7 days on the CTS console.

[Figure 8-2](#) shows how to view CTS logs.

Figure 8-2 Querying logs

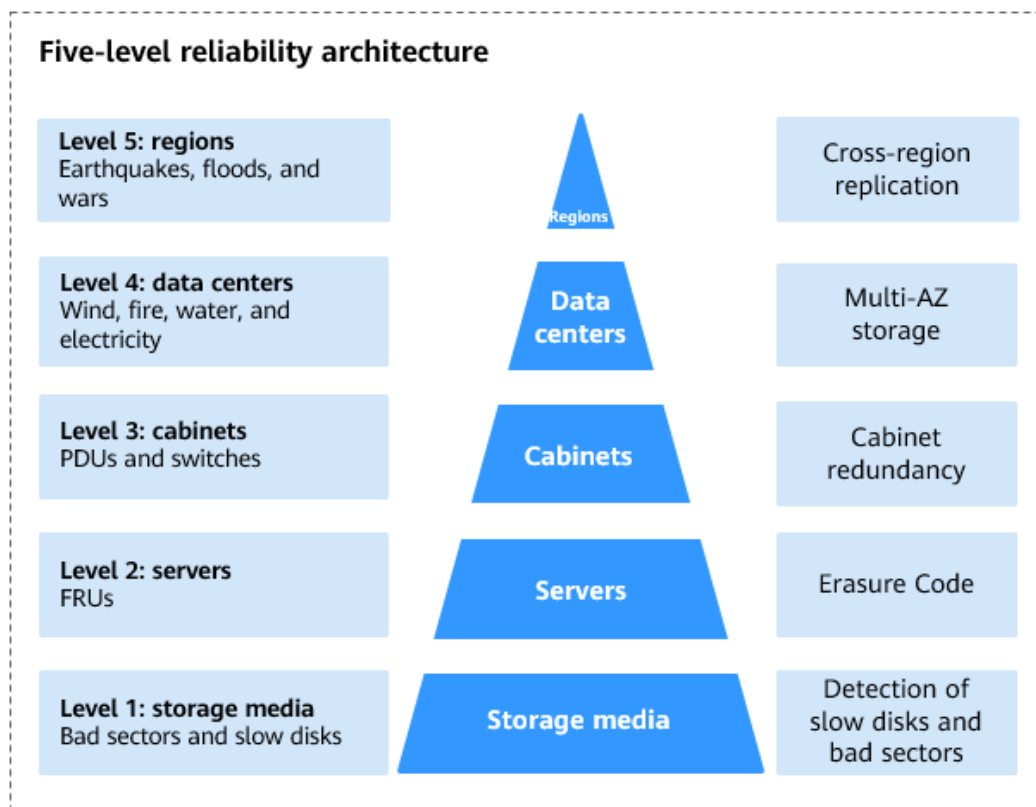


8.5 Service Resilience

Huawei Cloud SecMaster is mainly deployed in China. All deployed data centers are running properly. A data center serves as disaster recovery center for another. If a data center in city A is down, the data center in city B automatically takes over the job and serves your applications and data in compliance with the regulations to ensure service continuity. To minimize the service interruptions caused by hardware failures, natural disasters, or other disastrous incidents, Huawei Cloud SecMaster provides a DR plan.

SecMaster has high availability, fault tolerance, and scalability. If a fault occurs, the five-level reliability architecture of SecMaster supports different levels of reliability.

Currently, Huawei Cloud SecMaster is mainly deployed in China with many regions. All SecMaster components such as the management plane and engine are deployed as active/standby or cluster instances.



8.6 Risk Monitoring

SecMaster has interconnected with Cloud Eye. You can view SecMaster running metrics on the Cloud Eye console. Cloud Eye is a multi-dimensional monitoring platform provided by Huawei Cloud for a wide range of cloud resources. With Cloud Eye, you can learn about the resource usage and service running status on the cloud, receive alerts in a timely manner, and respond quickly to exceptions to keep your cloud services stable.

As a cloud security operations platform, SecMaster can access security alerts of other cloud services and display alerts by alert type and level. SecMaster can accurately monitor threats and attacks on the cloud in real time and detect security alert incidents in your assets. You can define and schedule threat alert notifications to learn about threats and risks in a timely manner. The notification items you can define include threat list, alert type, and risk severity. This feature helps you learn about your security status in a timely manner.

For details about how to enable and configure Cloud Eye, see [Enabling Cloud Eye](#).

Table 8-2 Risk monitoring

Incident Source	Incident	Alert Severity	Description	Handling Suggestion	Impact
SYS. Sec Master	Failed to create an exclusive engine.	Major	The underlying resources are insufficient.	Submit a service ticket to request adequate resources from the O&M personnel and try again.	The exclusive engine cannot be created.
SYS. Sec Master	The exclusive engine is not running properly.	Critical	The traffic is too heavy or there are malicious processes or plug-ins.	<ol style="list-style-type: none"> 1. Check the executions of plug-ins and processes, see if they occupy too many resources. 2. Check the instance monitoring information to see whether there is a sharp instance increase. 	The instance cannot be executed.
SYS. Sec Master	Failed to execute the playbook instance.	Minor	Playbooks or processes are wrongly configured.	Check the instance monitoring information to find the cause of the failure, and modify the playbook and process configuration.	None
SYS. Sec Master	The number of playbook instances increases sharply.	Minor	Playbooks or processes are wrongly configured.	Check the instance monitoring information to find the cause of the sharp increase, and modify the playbook and process configuration.	None
SYS. Sec Master	Log messages increase sharply.	Major	The upstream service suddenly generates a large number of logs.	Check whether the upstream service is normal.	None

Incident Source	Incident	Alert Severity	Description	Handling Suggestion	Impact
SYS. Sec Master	Log messages decrease sharply.	Major	Logs generated by the upstream service suddenly decrease.	Check whether upstream services are normal.	None

For details about monitoring alerts, see:

- [Vulnerability Management](#)
- [Cloud Service Baseline Overview](#)
- [Security Report](#)

8.7 Certificates







Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can [download](#) them from the console.

Figure 8-3 Downloading compliance certificates

Download Compliance Certificates

Q Please enter a keyword to search

 <p>BS 10012:2017</p> <p>BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.</p> <p style="text-align: center; margin-top: 10px;">Download</p>	 <p>ENS</p> <p>Mandatory law for companies in the public sector and their technology suppliers</p> <p style="text-align: center; margin-top: 10px;">Download</p>	 <p>Singapore Multi Tier Cloud Security (MTCS) Level 3</p> <p>The MTCS standard was developed under the Singapore Information Technology Standards Committee (ITSC). This standard requires cloud service providers to adopt well-rounded risk management and security practices in cloud computing. The HUAWEI CLOUD Singapore region has obtained the Level 3 (highest) certification of MTCS.</p> <p style="text-align: center; margin-top: 10px;">Download</p>
 <p>Trusted Partner Network (TPN)</p> <p>The Trusted Partner Network (TPN) is a global, industry-wide media and entertainment content security initiative and community network, wholly owned by the Motion Picture Association. TPN is committed to raising content security awareness and standards and building a more secure future for content partners. TPN can help identify vulnerabilities, increase security capabilities, and efficiently communicate security status to customers.</p> <p style="text-align: center; margin-top: 10px;">Download</p>	 <p>ISO 27001:2022</p> <p>ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.</p> <p style="text-align: center; margin-top: 10px;">Download</p>	 <p>ISO 27017:2015</p> <p>ISO 27017 is an international certification for cloud computing information security. It indicates that HUAWEI CLOUD's information security management has become an international best practice.</p> <p style="text-align: center; margin-top: 10px;">Download</p>

Resource Center





Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see [Resource Center](#).

Figure 8-4 Resource center

Resource Center

White Papers

Privacy Compliance White Papers	Industry Regulation Compliance White Papers	Guidelines and Best Practices
--	---	-------------------------------

 <p>Compliance with Argentina PDPL</p> <p>Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution</p>	 <p>Compliance with Brazil LGPD</p> <p>Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.</p>	 <p>Compliance with Chile PDPL</p> <p>Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile, as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.</p>	 <p>Compliance with PDPO of the HK</p> <p>Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China, as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.</p>
--	---	--	--

8.8 Security Orchestration

SecMaster Security Orchestration provides response playbooks for cloud security incidents. You can use playbooks to implement efficient and automatic response to security incidents. Its functions are as follows:

- **Playbook management:** you can use the built-in automatic response playbooks or customize playbooks.
Orchestrating a playbook is to build the manual security operation process and software into a machine playbook.
- **Workflow:** Allows you to draw a playbook triggering flowchart.
- **Asset Management:** manages and displays key assets in a unified manner.
- **Instance management:** allows you to monitor and manage running instances and view records.
- **Security Orchestration, Automation and Response (SOAR):** You can orchestrate workflows to let SecMaster automatically handle security incidents and suspicious incidents.

For details about how to configure Security Orchestration, see [Security Orchestration](#).

9 Permissions Management

If you want to assign different permissions to employees in your enterprise to access your SecMaster resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage access to your Huawei Cloud resources.

With IAM, you can create IAM users under your account for your employees, and assign permissions to the users to control their access to specific resource types. For example, you can use policies to grant different permissions to software developers in your enterprises to allow them to only use SecMaster but not perform certain high-risk operations, such as deletion of SecMaster data.

If your account does not need individual IAM users for permissions management, then you may skip over this section.

IAM is free. You pay only for the resources in your account. For more information about IAM, see [IAM Service Overview](#).

SecMaster Permissions

By default, new IAM users do not have any permissions assigned. You can add a user to one or more groups to allow them to inherit the permissions from the groups to which they are added.

SecMaster is a project-level service deployed and accessed in specific physical regions. To assign permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. To access SecMaster, the users need to switch to a region where they have been authorized to use cloud services.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. Only a limited number of service-level roles for authorization are available. When using roles to grant permissions, you also need to assign dependency roles. Roles are not ideal for fine-grained authorization and secure access control.
- **Policies:** A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under

certain conditions. This mechanism allows for more flexible policy-based authorization and meets secure access control requirements. For example, you can grant SecMaster users only the permissions for managing a certain type of resources.

Table 9-1 lists all SecMaster system permissions.

Table 9-1 System-defined permissions supported by SecMaster

Policy Name	Description	Type
SecMaster FullAccess	All permissions of SecMaster.	System-defined policy
SecMaster ReadOnlyAccess	SecMaster read-only permission. Users granted with these permissions can only view SecMaster data but cannot configure SecMaster.	System-defined policy

Roles or Policies Required for Operations on the SecMaster Console

If you grant the **region-level** SecMaster FullAccess permission to an IAM user, you still need to grant the IAM user the permissions to create agencies and configure agency policies when authorizing SecMaster on its console. The details are as follows.

Table 9-2 Roles or policies required for SecMaster console operations

Console Function	Dependent Service	Role/Policy Required
Service authorization	Identity and Access Management (IAM)	If an IAM user has been assigned the region-level SecMaster FullAccess permission, you need to grant the permissions for creating agencies and configuring agency policies to the IAM user. For details, see Granting Permissions to an IAM User .

Related Topics

- [IAM Service Overview](#)
- [Creating User Groups and Users and Granting SecMaster Permissions](#)
- [SecMaster Custom Policies](#)
- [SecMaster Permissions and Supported Actions](#)

SecMaster FullAccess Policy

```
{
  "Version": "1.1",
```

```

"Statement": [
  {
    "Action": [
      "secmaster:*:*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "vpc:vpcs:list",
      "vpc:subnets:get",
      "vpcep:endpoints:*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "obs:bucket:ListBucketVersions"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "iam:permissions:checkRoleForAgencyOnDomain",
      "iam:permissions:checkRoleForAgencyOnProject",
      "iam:permissions:checkRoleForAgency",
      "iam:permissions:grantRoleToAgency",
      "iam:permissions:grantRoleToAgencyOnDomain",
      "iam:permissions:grantRoleToAgencyOnProject",
      "iam:policies:*",
      "iam:agencies:*",
      "iam:roles:*",
      "iam:users:listUsers",
      "iam:tokens:assume"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "organizations:organizations:get",
      "organizations:delegatedAdministrators:list",
      "organizations:roots:list",
      "organizations:ous:list",
      "organizations:accounts:list"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "ecs:cloudServers:list"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "sts:agencies:assume"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "lts:log*:list*"
    ],
    "Effect": "Allow"
  }
]
}

```


SecMaster ReadOnlyAccess Policy

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "secmaster:*.get*",
        "secmaster:*.list*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:vpcs:list",
        "vpc:subnets:get",
        "vpcep:endpoints:get",
        "vpcep:endpoints:list"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "obs:bucket:ListBucketVersions"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "iam:permissions:checkRoleForAgencyOnDomain",
        "iam:permissions:checkRoleForAgencyOnProject",
        "iam:permissions:checkRoleForAgency",
        "iam:policies:get*",
        "iam:policies:list*",
        "iam:agencies:get*",
        "iam:agencies:list*",
        "iam:roles:get*",
        "iam:roles:list*",
        "iam:users:listUsers"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "organizations:organizations:get",
        "organizations:delegatedAdministrators:list",
        "organizations:roots:list",
        "organizations:ous:list",
        "organizations:accounts:list"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:cloudServers:list"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "lts:log*:list*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Granting Permissions to an IAM User

SecMaster is a project-level service deployed and accessed in specific physical regions. So, during authorization, you need to select **Region-specific projects** for **Scope** first. Then, you can specify specific projects for which you want the permission to work.

After SecMaster FullAccess is granted to an IAM user for a region-level project, you need to grant global action permissions to the IAM user because SecMaster depends on other cloud service resources. The permissions to be added are as follows:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:roles:listRoles",
        "iam:agencies:listAgencies",
        "iam:permissions:checkRoleForAgencyOnDomain",
        "iam:permissions:checkRoleForAgencyOnProject",
        "iam:permissions:checkRoleForAgency",
        "iam:agencies:createAgency",
        "iam:permissions:grantRoleToAgencyOnDomain",
        "iam:permissions:grantRoleToAgencyOnProject",
        "iam:permissions:grantRoleToAgency"
      ]
    }
  ]
}
```

iam:permissions:grantRoleToAgencyOnDomain, **iam:permissions:grantRoleToAgency**, **iam:permissions:grantRoleToAgencyOnProject**, and **iam:agencies:createAgency** are permissions required for using SecMaster. You need to grant such permissions when you **authorize SecMaster**. They are not mandatory for IAM users. Configure them as required. The authorization details are as follows:

- Unauthorized: Only the account used to create the IAM user can authorize SecMaster. If an IAM user attempts to authorize SecMaster, an error message will be displayed.
- Authorized: Both IAM users and the account used to create them can authorize SecMaster.

10 SecMaster and Other Services

This topic describes SecMaster and its linked services.

Security Services

SecMaster obtains necessary security incident records from security services such as [Host Security Service \(HSS\)](#), [Web Application Firewall \(WAF\)](#), and [Anti-DDoS](#). SecMaster then uses big data mining and machine learning to intelligently analyze and identify attacks and intrusions, helping you understand the attack and intrusion processes. SecMaster also provides protective measures for you. For more details, see [What Are the Dependencies and Differences Between SecMaster and Other Security Services?](#)

Elastic Cloud Server (ECS)

SecMaster detects threats to your [ECSs](#) with linked service HSS, comprehensively displays ECS security risks, and provides protection suggestions.

Cloud Trace Service (CTS)

[CTS](#) generates traces to enable you to get a history of operations performed on SecMaster, allowing you to query, audit, and backtrack resource operation requests initiated from the management console as well as the responses to those requests.

CTS is used to record the operations you have performed on SecMaster for later querying, auditing, or backtracking.

Cloud Eye

Cloud Eye is a comprehensive platform to monitor a variety of cloud resources such as ECS and bandwidth usage. You can learn SecMaster indicators in a timely manner and respond to alerts in a timely manner to ensure smooth service running. For details, see the *Cloud Eye User Guide*.

TMS

Tag Management Service (TMS) is a visualization service that allows you to quickly and centrally manage tags, helping you manage workspace instances by tag.

Table 10-1 SecMaster operations supported by TMS

Operation	Resource Type	Incident Name
Querying the resource instance list	Workspace	listResourceInstance
Querying the number of resource instances	Workspace	countResourceInstance
Batch querying resource tags	Tag	batchTagResources
Batch deleting resource tags	Tag	batchUntagResources
Querying project tags	Tag	listProjectTag
Updating a tag value	Tag	updateTagValue
Querying resource tags	Tag	listResourceTag

Enterprise Management

You can manage multiple projects in an enterprise, separately settle their costs, and assign different personnel for them. A project can be started or stopped independently without affecting others. With **Enterprise Management**, you can easily manage your projects after creating an enterprise project for each of them.

SecMaster supports enterprise management. You can manage resources on SecMaster by enterprise project and set user permissions for each enterprise project.

11 Basic Concepts

11.1 SOC

A security operations center (SOC) is a centralized function or team that checks all activities on endpoints, servers, databases, network applications, websites, and other systems around the clock to detect potential threats in real time. It aims to improve enterprise cybersecurity posture by prevention, analysis, and responses of cybersecurity events. A SOC also obtains latest threat intelligence to keep up-to-date information about threat groups and infrastructure. As a proactive defense system, a SOC always identifies and handles vulnerabilities in services systems or processes before attackers exploit them. Most SOCs run around the clock, seven days a week. Some cross-countries/regions enterprises or organizations may also rely on Global Security Operations Centers (GSOCs) to learn of global security threats and coordinate detection and response across local SOCs.

What a SOC Does

A SOC team has the following responsibilities to help prevent, respond to, and recover services from attacks.

- **Asset and tool inventory**

To eliminate blind spots in protection, a SOC needs to know every asset that needs to be protected and all tools used to protect them in the organization. This means a SOC needs to cover all databases, cloud services, identities, applications, and clients across on-premises data centers and clouds. A SOC also needs to know all security solutions used in the organization, for example, firewalls, anti-malware, anti-ransomware, and monitoring software.

- **Reducing attack surface**

A key responsibility of a SOC is to reduce the attack surface of the organization. To do this, SOC needs to maintain an exhaustive inventory of all workloads and assets, apply security patches to software and firewalls, identify misconfigurations, and discover and add new assets as they come online. SOC team members are also responsible for researching emerging threats and analyzing risks. This helps the SOC keep ahead of the latest threats.

- **Continuous monitoring**

A SOC team uses a security analysis solution to monitor the entire environment, covering on-premises, cloud, applications, networks, and devices, all day to detect abnormal or suspicious behavior. The solution can be a security information enterprise management (SIEM), security orchestration, automation, and response (SOAR), and extended detection and response (XDR) solution. These tools collect telemetry data, aggregate the data, and, in some cases, automate incident responses.
- **Threat intelligence**

A SOC also uses data analysis, external sources, and product threat reports to gain an in-depth insight into attacker behavior, infrastructure, and motives. This intelligence provides a comprehensive view of what is happening across the Internet and helps the team understand how groups work. With this information, the SOC can quickly detect threats and enhance the responses to emerging risks.
- **Threat detection**

SOC teams use the data generated by the SIEM and XDR solutions to identify threats. This first step is to filter out false positives from real issues. They then prioritize threats by severity and potential impact on services.
- **Log management**

A SOC also collects, maintains, and analyzes log data generated by each client, operating system, VM, local application, and network incident. SOC's analysis helps establish a baseline for normal activity and reveals anomalies that may indicate malware, ransomware, or viruses.
- **Incident response**

Once an online attack is identified, the SOC quickly takes actions to limit the damage to the organization with as little impacts on services as possible. Those actions may include shutting down or isolating affected clients and applications, suspending compromised accounts, removing infected files, and running anti-virus and anti-malware software.
- **Recovery and remediation**

After an attack, a SOC is responsible for restoring organization's services to its original state. The team will erase and reconnect the disk, identity, email, and clients, restart the application, switch to the backup system, and restore data.
- **Root cause investigation**

To prevent similar attacks from happening again, the SOC conducts a thorough investigation to identify vulnerabilities, ineffective security processes, and other experiences that led to the incident.
- **Security refinement**

A SOC uses any intelligence gathered during an incident to fix vulnerabilities, improve processes and policies, and update the security roadmap.
- **Compliance management**

A key part of a SOC's responsibility is to ensure that applications, security tools, and processes comply with privacy regulations, such as *PCI DSS Security Compliance Package*, *ISO 27701 Security Compliance Package*, and *ISO 27001 Security Compliance Package*. The team regularly reviews the system to ensure compliance and to make sure that regulators, law enforcement, and customers are notified of data breaches.

Key Roles in a SOC

Based on the scale of an organization, a typical SOC includes the following roles:

- **Incident response director**
This role, which is typically planned in very large organizations, is responsible for coordinating detection, analysis, containment, and recovery during a security incident. They also manage communication with corresponding stakeholders.
- **SOC manager**
A SOC manager oversees the SOC. They are responsible for reporting to the Chief Information Security Officer (CISO). Their responsibilities include supervising personnel, running services, training new employees and managing finance.
- **Security engineer**
Security engineers are responsible for operating of the organization's security system. This includes designing security architectures and researching, implementing, and maintaining security solutions.
- **Security analyst**
A security analyst is the first responder in a security incident. They are responsible for identifying threats, prioritizing threats, and then taking actions to contain damage. During an online attack, they may need to isolate infected hosts, clients, or users. In some organizations, security analysts are graded based on the security severity of the threats they are responsible for addressing.
- **Threat hunter**
In some organizations, the most experienced security analysts are called threat hunters. They identify and respond to advanced threats that are not detected by automated tools. This role is proactive and designed to deepen the organization's understanding of known threats and reveal unknown threats before attacks actually occur.
- **Forensics analyst**
Large organizations may also hire forensic analysts who are responsible for collecting intelligence to determine the root causes of violations. They search for system vulnerabilities, violations against security policies, and cyber attack patterns that may be useful in preventing similar intrusions in the future.

Types of SOCs

There are several ways for organizations to set up their SOCs. Some organizations choose to build dedicated SOCs with full-time employees. This type of SOC can be internal, with a physical local location, or can be virtual, with employees coordinating their work remotely using digital tools. Many virtual SOCs have both contract workers and full-time employees. An outsourced SOC, also called "managed SOC" or "SOC as a service", is run by a managed security service provider who is responsible for preventing, detecting, investigating, and responding to threats. An organization may also use a combination of internal employees and a managed security service provider. This way is called a co-managed or hybrid SOC. Organizations use this approach to increase the influence of their employees. For example, if they do not have threat investigators, it may be easier to hire third parties than to equip them internally.

Importance of a SOC Team

A strong SOC can help enterprises, governments, and other organizations stay ahead of an evolving online threat landscape. It is not an easy task. Both attacks and defense communities often develop new technologies and strategies, and it takes time and efforts to manage all changes. A SOC can leverage its understanding of the broader cybersecurity environment and of internal weaknesses and service priorities to help organizations develop a security roadmap that meets long-term business needs. SOCs can also limit the impact of attacks on services. Since they are continuously monitoring the network and analyzing alert data, they are more likely to detect threats earlier than other teams scattered among other priorities. Through regular training and well-documented processes, SOCs can quickly handle current incidents, even under great pressure. This can be difficult for teams that do not have a round-the-clock focus on secure operations.

Benefits of a SOC

By unifying the personnel, tools, and processes to protect an organization from threats, a SOC helps the organization defend against attacks and breaches more effectively and efficiently.

- **Strong security situation**

Improving the security of an organization is a job that has no ends. It requires continuous monitoring, analysis, and planning to discover vulnerabilities and master changing technologies. If several tasks have the same priority, it is more likely to ignore security and focus on tasks that seem more urgent.

A centralized SOC helps make sure that processes and technologies are improved continuously, reducing the risk of successful attacks.

- **Compliance with privacy laws and regulations**

In different industries, countries, and regions, there are many regulations that govern the collection, storage, and use of data. Many regulations require organizations to report data breaches and detect personal data upon user requests. Developing appropriate processes and procedures is as important as having the right technology. SOC members help organizations comply with these regulations by taking responsibility for keeping technology and data processes up to date.

- **Swift incident responses**

How quickly cyber attacks can be detected and prevented is critical. With appropriate tools, personnel, and intelligence, vulnerabilities can be curbed before they cause any damage. But bad actors are also smart, they may hide in the system to steal massive amount of data and escalate their permissions before anyone notices. A security incident is also a very stressful thing, especially for those who lack experience in incident response.

With unified threat intelligence and well-documented procedures, a SOC team can quickly detect, respond to, and recover from attacks.

- **Reduced breach costs**

A successful intrusion can be very expensive for organizations. It may lead to a long downtime before service recovery. Some organizations may lose customers or find it difficult to win new customers shortly after an incident.

By acting ahead of attackers and responding quickly, a SOC helps organizations save time and money when they return to normal operations.

Best Practices for SOC Teams

With so many things to be responsible for, a SOC must effectively manage to achieve expected results. Organizations with strong SOCs implement the following security practices:

- **Service-aligned strategy**

Even the most well-funded SOC has to decide where to spend its time and money. Organizations usually conduct risk assessments first to identify the aspects that are most vulnerable to risks and the greatest business opportunities. This helps to determine what needs to be protected. A SOC also needs to know the environment where the assets are located. Many enterprises have complex environments, with some data and applications on-premises and some distributed across clouds. A strategy helps determine whether security professionals need to be available at all hours every day and whether it is better to set up an in-house SOC or to use professional services.

- **Talented, well-trained employees**

The key to an effective SOC lies in highly skilled and progressive employees. The first step is to find the best talent. However, this can be tricky as the market for security personnel is really competitive. To avoid skill gaps, many organizations try to find people with a variety of expertise, including systems and intelligence monitoring, alert management, incident detection and analysis, threat hunting, ethical hacking, cyber forensics, and reverse engineering. They also deploy technologies that automate tasks to make smaller teams more efficient and improve the output of junior analysts. Investing in regular training helps organizations keep key employees, fill skills gaps, and develop employees' careers.

- **End-to-end visibility**

An attack may start with a single client, so it is critical for the SOC to understand the entire environment of the organization, including anything managed by a third party.

- **Right tools**

There are so many security incidents that teams can be easily overwhelmed. Effective SOCs invest in excellent security tools that work well together and use AI and automation to report major risks. Interoperability is the key to avoiding coverage gaps.

SOC Tools and Technologies

- **Security information and event management (SIEM)**

One of the most important tools in a SOC is a cloud-based SIEM solution, which aggregates data from multiple security solutions and log files. With threat intelligence and AI, these tools help SOCs detect evolving threats, accelerate incident response, and act before attackers.

- **Security orchestration, automation and response (SOAR)**

A SOAR automates periodic and predictable actions, response, and remediation tasks, freeing up time and resources for more in-depth investigations and hunting.

- **Extended detection and response (XDR)**

XDR is a service-oriented software tool that provides comprehensive and better security by integrating security products and data into simplified solutions. Organizations use these solutions to proactively and effectively address an evolving threat landscape and complex security challenges across clouds. Compared with systems such as endpoint detection and response (EDR), XDR expands the security scope to integrate protection across a wider range of products, including organization's endpoints, servers, cloud applications, and emails. On this basis, XDR combines prevention, detection, investigation, and response to provide visibility, analysis, correlated incident alerts, and automated response to enhance data security and combat threats.
- **Firewall**

A firewall monitors incoming and outgoing network traffic and allows or blocks the traffic based on the security rules defined by the SOC.
- **Log management**

A log management solution is usually part of a SIEM. It logs all alerts from each software, hardware, and client running in the organization. These logs provide information about network activities.
- **Vulnerability management**

Vulnerability management tools scan the network to help identify any weaknesses that attackers may exploit.
- **User and entity behavior analytics (UEBA)**

User and entity behavior analytics (UEBA) is built in many modern security tools. UEBA uses AI to analyze data collected from varied devices to establish a baseline of normal activity for each user and entity. When an event deviates from the baseline, it will be marked for further analysis.

SOC and SIEM

Without a SIEM, a SOC will be difficult to accomplish its tasks. Today's SIEM provides the following functions:

- **Log aggregation:** A SIEM collects log data and associates alerts. Analysts can use the information to detect and search for threats.
- **Context:** SIEM collects data across all technologies in the organization, so it helps connect points between individual incidents and identify sophisticated attacks.
- **Alert reduction:** A SIEM uses analytics and AI to correlate alerts and identify the most serious incidents, reducing the number of false positives.
- **Automatic response:** A SIEM uses built-in rules to identify and prevent possible threats without human interaction.

NOTE

It is also important to note that a SIEM alone is not enough to protect the organization. Users need to integrate a SIEM with other systems, define parameters for rule-based detection, and evaluate alerts. So it is critical to define the SOC strategy and hire the appropriate staff.

SOC Solution

There are multiple solutions that can be used to help a SOC protect the organization. The best solution works together with other security services to provide complete coverage across on-premises and multiple clouds. Our company provides a comprehensive solution to help SOCs narrow the gap in protection coverage and give a 360-degree view of your environment. SecMaster integrates the detection and response solution to provide analysts and threat hunters with the data they need to find and contain cyber attacks.

FAQs

1. What does a SOC team need to do?
A SOC team monitors servers, devices, databases, network applications, websites, and other systems to detect potential threats in real time. The team performs proactive security efforts. They keep abreast of the latest threats and discover and resolve system or process vulnerabilities before attackers exploit them. If an organization is being attacked, the SOC team is responsible for eradicating the threat and restoring the system and backup as needed.
2. What are the key components in a SOC?
A SOC consists of people, tools, and processes that help protect the organization from cyber attacks. To achieve its objectives, an SOC performs the following functions: inventory of all assets and security techniques, routine maintenance and preparation, continuous monitoring, threat detection, threat intelligence, log management, incident response, recovery and remediation, root cause investigation, security optimization, and compliance management.
3. Why do organizations need strong SOCs?
A strong SOC helps organizations manage security more efficiently and effectively through unified defense, threat detection tools, and security processes. Organizations with SOCs can improve their security processes, respond to threats faster, and better manage compliance than those without SOCs.
4. What are the differences between a SIEM and a SOC?
A SOC consists of the personnel, processes, and tools responsible for protecting organizations from cyber attacks. A SIEM is one of the many tools used by a SOC to maintain visibility and respond to attacks. A SIEM aggregates logs and uses analytics and automation to reveal credible threats to SOC members who decide how to respond.

11.2 Security Overview and Situation Overview

Security Overview

On the **Security Overview** page, SecMaster displays the overall security assessment result of your assets in real time. SecMaster works together with other cloud security services to centrally display security assessment and monitoring results, as well as your cloud security scores over time. The **Security Overview** page displays the overall security assessment of all workspaces in real time. For details about how to view the result, see [Checking Security Overview](#).

Situation Overview

The **Situation Overview** page displays the overall security assessment status of resources in the current workspace in real time. You will view the security assessment results, security monitoring details, and security trend of your assets. The **Security Situation > Situation Overview** page of the target workspace displays the security assessment result of the current workspace. For details about how to check the result, see [Checking Situation Overview](#).

Security Risk

A security risk is a comprehensive evaluation of your assets, reflecting the security level of your assets within a period of time by a security score. A security score is for your reference to learn about the security situation of your assets.

Security Score

SecMaster assesses the overall security situation of your cloud assets in real time and scores your assets based on the SecMaster edition you are using.

The security score is automatically updated at 02:00 every day. You can also click **Check Again** to update it immediately.

This following part describes how your security score is calculated.

- Security Score
 - SecMaster evaluates the over security posture of your assets based on the SecMaster edition you are using.
 - There are six risk severity levels, **Secure, Informational, Low, Medium, High, and Critical**.
 - The score ranges from 0 to 100. The higher the security score, the lower the risk severity level.
 - The security score starts from **0** and the risk severity level is escalated up from **Secure** to the next level every 20 points. For example, for scores ranging from **40** to **60**, the risk severity is **Medium**.
 - The color keys listed on the right of the chart show the names of donut slices. Different color represents different risk severity levels. For example, the yellow slice indicates that your asset risk severity is **Medium**.
 - If you have fixed asset risks and refreshed the alert status, you can click **Check Again** to update the security score.

NOTE

After risks are fixed, manually ignore or handle alert incidents and update the alert incident status in the alert list. The risk severity can be down to a proper level accordingly.

Table 11-1 Security score table

Severity	Security Score	Description
Secure	100	Congratulations. Your assets are secure.

Severity	Security Score	Description
Informational	$80 \leq$ Security Score < 100	Your system should be hardened as several security risks have been detected.
Low	$60 \leq$ Security Score < 80	Your system should be hardened in a timely manner as too many security risks have been detected.
Medium	$40 \leq$ Security Score < 60	Your system should be hardened, or your assets will be vulnerable to attacks.
High	$20 \leq$ Security Score < 40	Detected risks should be handled immediately, or your assets will be vulnerable to attacks.
Critical	$0 \leq$ Security Score < 20	Detected risks should be handled immediately, or your assets may be attacked.

- Unscored check items

The following table lists the security check items and corresponding points.

Table 11-2 Unscored check items

Category	Unscored Item	Unscored Point	Suggestion	Maximum Unscored Point
Enabling of security services	Security-related services not enabled	No points deducted	Enable security-related services.	30
Compliance Check	Critical non-compliance items not fixed	10	Fix compliance violations by referring recommended fixes and start a scan again. The security score will be updated.	20
	High-risk non-compliance items not fixed	5		
	Medium-risk non-compliance items not fixed	2		
	Low-risk non-compliance items not fixed	0.1		

Category	Unscored Item	Unscored Point	Suggestion	Maximum Unscored Point
Vulnerabilities	Critical vulnerabilities not fixed	10	Fix vulnerabilities by referring corresponding suggestions and start a scan again. The security score will be updated.	20
	High-risk vulnerabilities not fixed	5		
	Medium-risk vulnerabilities not fixed	2		
	Low-risk vulnerabilities not fixed	0.1		
Threat Alerts	Critical alerts not fixed	10	Fix the threats by referring to the suggestions. The security score will be updated accordingly.	30
	High-risk alerts not fixed	5		
	Medium-risk alerts not fixed	2		
	Low-risk alerts not fixed	0.1		

11.3 Workspaces

Workspace

Workspaces are top-level workbenches in SecMaster. A workspace can be bound to common projects, enterprise projects, and regions for different application scenarios.

Data Space

A data space is a unit for data grouping, load balancing, and flow control. Data in the same data space shares the same load balancing policy.

Data Pipelines

A data transfer message topic and a storage index form a pipeline.

11.4 Alert Management

Threat Alerts

In general, threat alerts refer to threats that, due to natural, human, software, or hardware reasons, are detrimental to information systems or cause negative effects on the society. In SecMaster, threat alerts are detected security incidents that threaten asset security through big data technology.

Incidents

An incident is a broad concept. It can include but is not limited to alerts. It can be a part of normal system operations, exceptions, or errors. In the O&M and security fields, an incident usually refers to a problem or fault that has occurred and needs to be focused on, investigated, and handled. An incident may be triggered by one or more alerts or other factors, such as user operations and system logs.

An incident is usually used to record and report historical activities in a system for analysis and audits.

Alerts

An alert is a notification of abnormal signals in O&M. It is usually automatically generated by a monitoring system or security device when detecting an exception in the system or networks. For example, when the CPU usage of a server exceeds 90%, the system may generate an alert. These exceptions may include system faults, security threats, or performance bottlenecks.

Generally, an alert can clearly indicate the location, type, and impact of an exception. In addition, alerts can be classified by severity, such as critical, major, and minor, so that O&M personnel can determine which alerts need to be handled first based on their severity.

The purpose of an alert is to notify related personnel in a timely manner so that they can make a quick response and take measures to fix the problem.

When SecMaster detects an exception (for example, a malicious IP address attacks an asset or an asset has been hacked into) in cloud resources, it generates an alert and displays the threat information on the **Alerts** page in SecMaster.

11.5 Security Orchestration

Classification and Mapping

Classification and mapping are to perform class matching and field mapping for cloud service alerts.

Security Orchestration

Security orchestration is a process that combines security capabilities (applications) and manual checks based on certain logical relationships to

complete a specific security operations procedure. Security functions of different security operations systems or components are encapsulated through programmable interfaces (APIs) during this process.

Security orchestration is a collaborative work mode that integrates various capabilities related to security operations, such as tools/technologies, workflows, and personnel.

Playbooks

A playbook is a formal expression of the security operations process in the security orchestration system. It converts the security operations process and regulations into machine-read workflows.

Playbooks embody the logic of security controls and schedule security capabilities. Playbooks are flexible and scalable. They can be modified and extended based on actual requirements to adapt to ever-changing security threats and service requirements.

Workflows

A workflow is a collaborative work mode that integrates various capabilities related to security operation, such as tools, technologies, workflows, and personnel. It consists of multiple connected components. After defined in a workflow, these components can be triggered externally. For example, when a new service ticket is generated, the automatic service ticket review workflow is automatically triggered. You can use the visual canvas to define component actions for each node in a workflow.

A workflow determines how security controls respond when a playbook is triggered. Workflows convert instructions and procedures in the corresponding playbook into specific actions and execution steps.

Relationship Between Playbooks and Workflows

- **Relationship:** A playbook provides guidance and rules for secure operations, and its workflow is responsible for converting these rules into specific execution steps and actions. A playbook and its workflow depend on each other. The playbook guides the execution of the workflow, while the workflow implements the intent and requirements of the playbook.
- **Differences:** There are also some differences between playbooks and workflows. First, playbooks focus more on defining and describing security operations processes and regulations, so they focus on the overall framework and policies. Workflows focus more on specific actions and execution steps, so they focus on how to convert requirements in playbooks into actual actions. Second, playbooks are flexible and scalable, and can be modified and extended as required. However, workflows are relatively fixed. Once the design is complete, they need to follow the specified steps.

Example: Take a specific cyber security incident response case as an example. When an organization suffers from a cyber attack, the security orchestration system first identifies the attack type and severity based on the preset playbook. Then, the system automatically triggers corresponding security controls based on the workflow defined in the playbook, such as isolating the attacked system, collecting attack data, and notifying the security team. During the process,

playbooks and workflows work closely to ensure the accuracy and timeliness of security responses.

Plug-in Management

- Plug-in: an aggregation of functions, connectors, and public libraries. There are two types of plug-ins: custom plug-ins and commercial plug-ins. Custom plug-ins can be displayed in marts or used in playbooks.
- Plug-in set: a set of plug-ins that have the same service scenario.
- Function: an executable function that can be selected in a playbook to perform a specific behavior in the playbook.
- Connector: connects to data sources and sends security data such as alerts and incidents to SecMaster. Connectors are classified into incident-triggered connectors and scheduled connectors.
- Public library: a public module that contains API calls and public functions that will be used in other components.

Asset Connections

An asset connection includes the domain name and authentication parameters required by each plug-in node in the security orchestration process. During security orchestration, each plug-in node transfers the domain name to be connected and the authentication information, such as the username, password, and account AK/SK, to establish connections.

Relationship Between Asset Connections and Plug-ins

Plug-ins access other cloud services or third-party services through domain names and authentication. So, domain name parameters (endpoints) and authentication parameters (username/password, account AK/SK, etc.) are defined in the login credential parameters of plug-ins. An asset connection configures login credential parameters for a plug-in. In a workflow, each plug-in node is associated with different asset connections so that the plug-in can access different services.

Instance Monitoring

After a playbook or workflow is executed, a playbook or workflow instance is generated in the instance management list for monitoring. Each record in the instance monitoring list is an instance. You can view the historical instance task list and the statuses of historical instance tasks.

11.6 Security Analysis

Producer

A producer is a logical object used to construct data and transmit it to the server. It stores data in message queues.

Subscriber

A subscriber is used to subscribe to SecMaster pipeline messages. A pipeline can be subscribed to by multiple subscribers. SecMaster distributes messages through subscribers.

Consumer

A consumer is a running entity that receives and processes data. It consumes and processes messages in the SecMaster pipeline through subscribers.

Message Queue

A message queue is the container for data storage and transmission.

Threat Detection Model

A threat detection model is a trained AI recognition algorithm model. A threat detection model can automatically aggregate, analyze, and generate alerts for specific threats. This type of model has good generalization and anti-evasion capabilities. They can work in different service systems to defend against sophisticated emerging attacks.