SecMaster

Service Overview

Issue 04

Date 2025-02-17

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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?

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	• **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	• 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.	√	√	√

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 4-3 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 4-4 Functions

Function Module	Description	Basic	Standard	Professional
Situation Overview	• **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	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. **NOTE** The large screen function needs to be purchased separately based on the standard or professional edition.	×	√	√
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 4-5 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 4-6 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
Security Policies	SecMaster supports centralized management of defense and emergency policies.	×	√	√

Threat Operations

SecMaster provides many threat detection models in the Threat Operations 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 4-7 Functions of the Threat Operations 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	• **Query and Analysis** – 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
	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 plug-in Logstash. You can enable custom data consumers and producers. **NOTE** You need to purchase the security analysis function in the value-added package at an extra cost.			

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 4-8 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.	×	√	√
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.	×	√	√

Function Module	Description	Basic	Standard	Professional
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 4-9 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 4-10 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 4-11 Functions

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

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 alarm status synchronization, automatic notification of high-risk alarms, association between application defense alarms and historical handling information, automatic closure of repeated alarms, association between network defense alarms and historical handling information, automatic notification of high-risk vulnerabilities, association between identity defense alarms and historical handling information, alarm IP address metric marking, and association of HSS alarms with historical handling details

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 do-to 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

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	• 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	• 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. – 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	• 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	• 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	• 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	• 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	• 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	• 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	The maximum number of retries within a day for a single workspace of an account is as follows: • 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	• 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 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 8-1 lists all SecMaster system permissions.

Table 8-1 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 8-2 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**.

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.

9 SecMaster and Other Services

This topic describes SecMaster and its linked services.

Security Services

SecMaster obtains necessary security incident records from other 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 9-1 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.

10 Basic Concepts

10.1 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.

10.2 Security Overview and 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 10-1 Security score table

Severity	Security Score	Description
Secure	100	Congratulations. Your assets are secure.
Informational	80 ≤ Security Score < 100	Your system should be hardened as several security risks have been detected.
Low	60 ≤ Security Score < 80	Your system should be hardened in a timely manner as too many security risks have been detected.
Medium	40 ≤ Security Score < 60	Your system should be hardened, or your assets will be vulnerable to attacks.
High	20 ≤ Security Score < 40	Detected risks should be handled immediately, or your assets will be vulnerable to attacks.

Severity	Security Score	Description
Critical	0≤ 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 10-2 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		
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		

Category	Unscored Item	Unscored Point	Suggestion	Maximum Unscored Point
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		

10.3 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.

10.4 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.

10.5 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.

10.6 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.

