

SecMaster

Getting Started

Issue 01
Date 2023-12-30



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. 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 Overview.....	1
2 Purchasing SecMaster.....	3
3 Configuring Service Authorization.....	6
4 Creating a Workspace.....	8
5 Enabling Data Access.....	10
5.1 Enabling Asset Subscription.....	10
5.2 Enabling Log Access.....	11
6 Configuring and Enabling Related Checks.....	13
6.1 Configuring Policies.....	13
6.2 Enabling an Alert Model.....	14
6.3 Enabling a Playbook.....	18
6.4 Performing Baseline Inspection.....	19
7 Creating a Report.....	21
8 Security Operations.....	24
9 Getting Started with Common Practices.....	27
A Change History.....	28

1 Overview

SecMaster is a next-generation cloud native security operations platform. 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.

This document describes the process of using the professional SecMaster. The process is as follows:

Table 1-1 Process

No.	Operation		Description
1	Buy SecMaster		Provides guidelines on how to purchase the professional SecMaster and value-added functions (large screen, intelligent analysis, and security orchestration).
2	Configuring Service Authorization		After purchasing SecMaster, you need to authorize it to access some of your services.
3	Creating a Workspace		This topic describes how to create a workspace, which is the top-level workbench in SecMaster.
4	Access Data	Enabling Asset Subscription	This topic describes how to enable asset subscription so that asset information of the logged-in account can be synchronized to the current workspace.
		Enabling Log Access	After logs of cloud services such as WAF, HSS, and OBS are integrated into SecMaster, you can use SecMaster to query and analyze them for centralized O&M.

No.	Operation	Description	
5	Configuring and Enabling Related Checks	Configuring Policies	You can enable, configure, and apply protection policies for 7 layers of defense and enjoy comprehensive protection.
		Enabling a Model	If you enable intelligent modeling, information such as alerts, incidents, and indicators can be automatically extracted by models.
		Enabling a Playbook	Playbooks are used to automatically handle alerts, incidents, and threat intelligence.
		Performing Baseline Inspection	SecMaster can scan cloud services for risks in key configuration items, report scan results by category, generate alerts for risky settings, and provide hardening suggestions and guidelines.
6	Report Management	You can specify how you would like SecMaster to automatically send reports.	
7	Security Operations	After data integration is configured, you can perform operations such as asset management, threat detection, and alert investigation based on the integrated data.	

2 Purchasing SecMaster

This topic walks you through how to buy SecMaster professional edition and value-added packages that are billed yearly/monthly.

Edition Description

SecMaster provides the basic, standard, and professional editions. Before you make a purchase, get yourself familiar with their differences and pricing details. For details, see [Edition Differences](#) and [Billing Overview](#).

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.
- Step 3** On the **Overview** page, click **Buy SecMaster** in the upper right corner. The **Buy SecMaster** page is displayed.
- Step 4** On the purchase page, configure required parameters.

Figure 2-1 Purchasing SecMaster professional edition in yearly/monthly mode

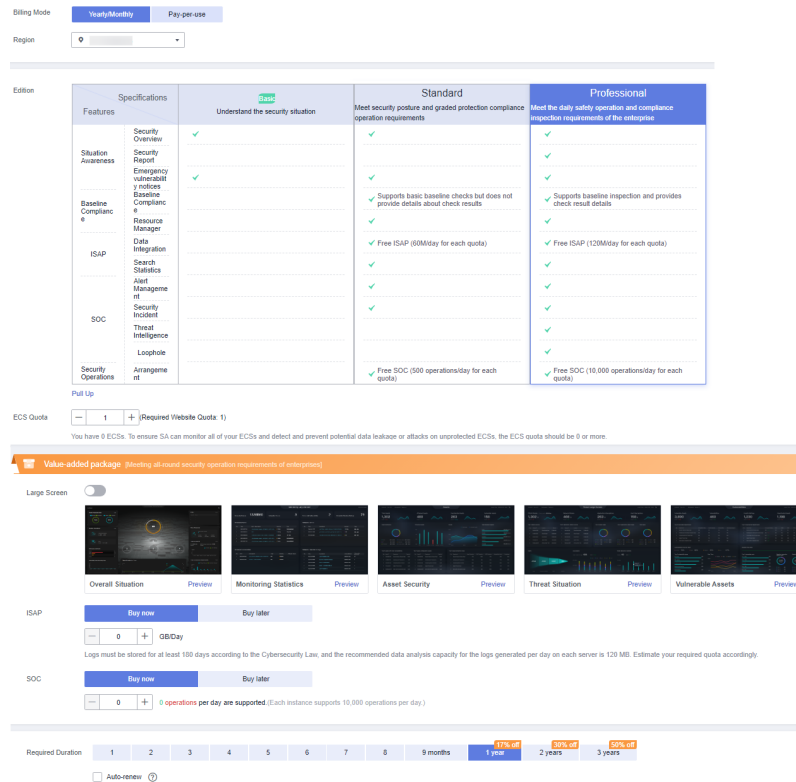


Table 2-1 Parameters for purchasing the professional edition in yearly/monthly mode

Name	Description
Billing Mode	Select Yearly/Monthly .
Component	Select your region.
Edition	Select Professional .
ECS Quota	<p>The ECS quota indicates the maximum number of ECSs that can be protected.</p> <p>The total ECS quota must be greater than or equal to the total number of hosts within your account. This value cannot be changed to a smaller one after your purchase is complete.</p> <p>NOTE</p> <ul style="list-style-type: none"> The maximum ECS quota cannot exceed 10,000. If some of your ECSs are not protected by SecMaster, threats to them cannot be detected in a timely manner, which may result in security risks, such as data leakage. Increase the ECS quota timely when the number of host assets increases.
Value-added Package	Enable or purchase the Large Screen , ISAP , or SOC functions.

Name	Description
Required Duration	Specify Required Duration . You can select a required duration in the range from one month to three years. NOTE The Auto-renew option enables the system to renew your service by the purchased period when the service is about to expire.

Step 5 Confirm the product details and click **Next**.

Step 6 After confirming that the order details are correct, read the *SecMaster Disclaimer* and select "I have read agree to SecMaster Disclaimer", and click **Pay**.

Step 7 On the payment page, select a payment method and complete the payment.

----End

3 Configuring Service Authorization


Before using SecMaster, you need to authorize SecMaster to access some services. If you have obtained such permissions, skip over this section.

Prerequisites

The IAM account has been authorized. For details, see [How Do I Grant Permissions to an IAM User?](#)

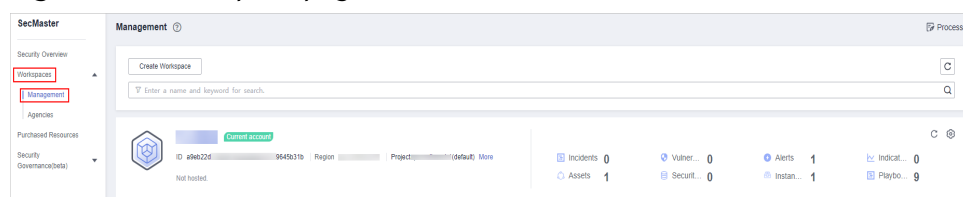
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.

Step 3 In the navigation pane, choose **Workspaces**.

Figure 3-1 Workspace page



Step 4 In the upper part of the workspace management page, choose **Entrusted Service Authorization - Current Tenant**.

Figure 3-2 Authorizing for SecMaster



Step 5 On the page for assigning permissions, select all required permissions (which are selected by default), select **Agree to authorize**, and click **Confirm**.

----End

4 Creating a Workspace

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

Before using functions such as security analysis and data consumption, you need to create a workspace to group resources based on working scenarios. This makes your resources easier for search and use.


This topic describes how to create a workspace.

Limitations and Constraints

- 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.

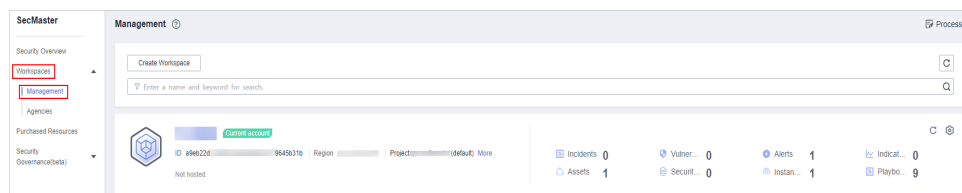
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.

Step 3 In the navigation pane, choose **Workspaces**.

Figure 4-1 Workspace page



Step 4 On the **Management** page, click **Create Workspace**. The **Create Workspace** slide-out panel is displayed.

Step 5 Configure workspace parameters by referring to the following table.

Table 4-1 Parameters for creating a workspace

Parameter	Description
Region	Select the region where the workspace to be added is located.
Project Type	<p>Select the type of project that the workspace you want to create belongs to.</p> <p>If you select Enterprise Project, you need to select an enterprise project from the drop-down list.</p> <p>This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects.</p> <p>To learn more, see Enabling the Enterprise Center. You can use enterprise projects to more efficiently manage cloud resources and project members.</p> <p>NOTE Value default indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.</p>
Workspace Name	<p>Create a name for your workspace. The name must meet the following requirements:</p> <ul style="list-style-type: none"> • Only letters (A to Z and a to z), numbers (0 to 9), and the following special characters are allowed: -_() • A maximum of 64 characters are allowed.
Tag	(Optional) Tag of the workspace, which is used to identify the workspace and help you classify and track your workspaces.
Description	(Optional) User remarks

Step 6 Click **OK**.

----End

5 Enabling Data Access

5.1 Enabling Asset Subscription

SecMaster can synchronize asset information only in the workspace where asset subscription is enabled. If you enable asset subscription, the resource information will be synchronized within one minute.

This section describes how to make a subscription to resources.

NOTE

Only cloud resources can be subscribed to and synchronized. Subscribing to resource information to multiple workspaces in a region is not recommended.

Procedure


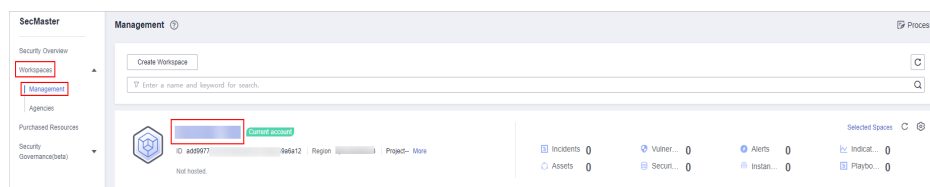
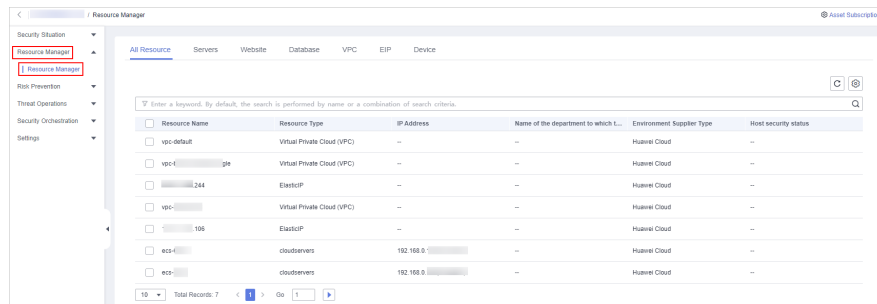
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 5-1 Workspace management page



- Step 4** In the navigation pane on the left, choose **Resource Manager** > **Resource Manager**.

Figure 5-2 Resource Manager



- Step 5** On the **Resource Manager** page, click **Asset Subscription** in the upper right corner.
- Step 6** On the **Asset Subscription** page sliding from the right, locate the row that contains the region where the target resource is located, and enable subscription.
- Step 7** Click **OK**.

After the subscription, the resource information will be displayed within one minute.

----End

5.2 Enabling Log Access

SecMaster can integrate log data of multiple Huawei Cloud services, such as Web Application Firewall (WAF), Host Security Server (HSS), and Object Storage Service (OBS). After the integration, you can search for and analyze all collected logs.

Allowing SecMaster to Access Service Logs


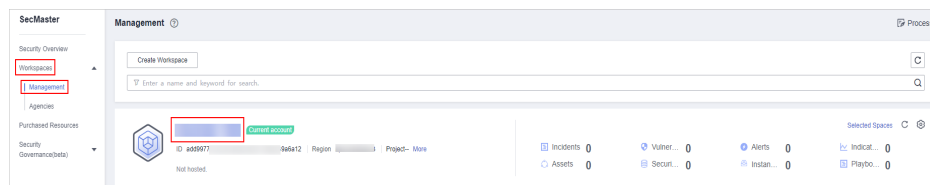
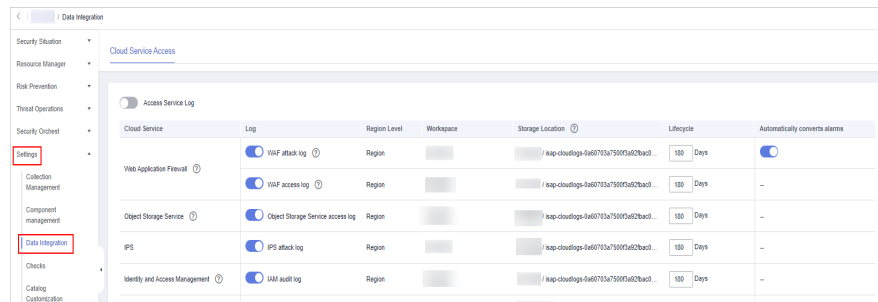
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.


Figure 5-3 Workspace management page




- Step 4** In the navigation pane on the left, choose **Settings > Data Integration**.

Figure 5-4 Data Integration page




Step 5 Locate the cloud service for which you want to collect logs, click  in the **Log** column to enable the log function.

You are advised to click  on the left of **Access Service Log** to access all cloud service logs in the current region.

Step 6 Set the lifecycle. You are advised to retain the default value.

Step 7 (Optional) Set **Automatically converts alarms**.



Locate the target cloud service, click  in the **Automatically converts alarms** column to enable the function. Then, if a cloud service log meets certain alarm rules, the log is converted into an alert.

Step 8 Click **Save**.

After the access completes, a default data space and pipeline are created.

----End

Related Operations

- Canceling Data Access
 - a. In the **Log** column of the target cloud service, click  to disable access to logs of the cloud service.
 - b. Click **Save**.
- Edit the data access lifecycle.
 - a. In the **Lifecycle** column of the target cloud service, enter a data storage period.
 - b. Click **Save**.
- Cancel automatic converting to alarms.
 - a. In the row of the target cloud service, click  in the **Automatically converts alarms** column to disable the function.
 - b. Click **Save**.

6 Configuring and Enabling Related Checks

6.1 Configuring Policies

You can enable, configure, and apply protection policies for 7 layers of defense and enjoy comprehensive protection.

This topic walks you how to configure a protection policy in WAF in the application defense layer.

Procedure


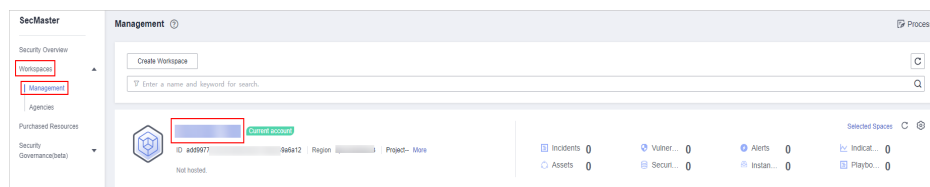
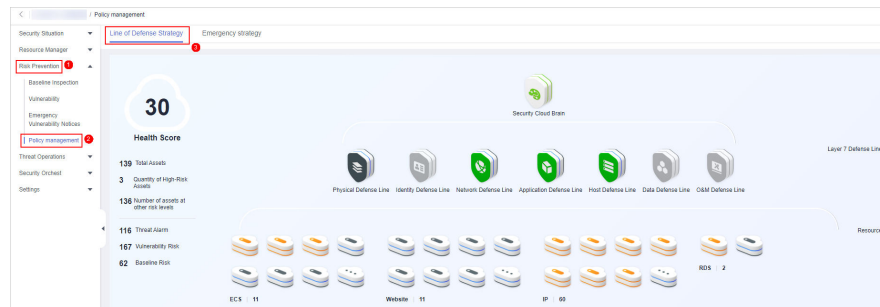
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 6-1 Workspace management page



- Step 4** In the navigation pane on the left, choose **Risk Prevention > Policy Management**.

Figure 6-2 Line of Defense Strategy



- Step 5** Click the name of the application defense line. The cloud product information corresponding to the application defense line is displayed on the right.
- Step 6** On the WAF tab, click **Protection Policy**. The WAF protection policy configuration page is displayed.
If you have not purchased WAF, click **WAF**. On the WAF console page displayed, click **Buy WAF**. On the purchase page displayed, enable WAF by referring to [Buying WAF](#).
- Step 7** On the WAF protection policy configuration page, click the **Policy Management** tab. On the displayed page, click **Add Policy** in the upper left corner of the list.
- Step 8** In the displayed dialog box, enter the policy name and click **Confirm**. The added policy will be displayed in the policy list.
- Step 9** In the row containing the target policy, click the policy name. On the displayed page, add rules to the policy by referring to [Configuring Protection Rules](#).

----End

6.2 Enabling an Alert Model


SecMaster uses models to scan log data in pipelines. If the data is not within the model range, an alert will be generated. After data access, you can enable alert models for automated threat detection.

SecMaster provides the following built-in templates to create and enable alert models:

Application-WAF Key Attack Alert, Host-Virtual Machine Lateral Connection, Network-High-Risk Port Exposure to the Outside, Network-Login Brute Force Alarm, Host-Suspected External Connection, Network-Source IP Attacking Multiple Targets, Network-Command Injection Alert, Network-Malicious External Communications, Host-Reverse Shell, Host-Malware, Application-distributed URL Traversal Attack, Application-Source IP Conducting URL Traversal, Host-High-risk Command Detection, Application-Source IP Brute-Forcing Domain Names, Host-Brute Force Crack Success, Host-Abnormal Shell, Host-Weak Password, Host-Remote Login, and Host-Rootkit Events.

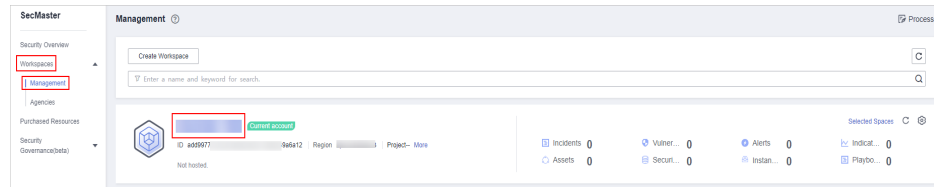
Creating an Alert Model

- Step 1** Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.

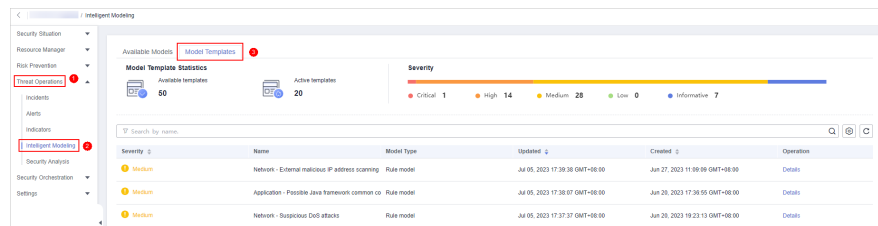
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 6-3 Workspace management page



Step 4 In the navigation tree on the left, choose **Threat Operations > Intelligent Modeling**. On the Intelligent Modeling page that is displayed, click the **Model Templates** tab. The Model Template page is displayed.

Figure 6-4 Model Templates tab page



Step 5 In the model template list, click **Details** in the **Operation** column of the target model template. The template details page is displayed on the right.

Figure 6-5 Model template details

Severity	Name	Model Type	Updated	Created	Operation
Critical	Host-Rootkit Events	Rule model	Feb 15, 2023 15:57:08 GMT+08:00	Feb 15, 2023 15:57:08 GMT+08:00	Details
Medium	Host-Abnormal Location Login	Rule model	Feb 15, 2023 15:54:44 GMT+08:00	Feb 15, 2023 15:54:44 GMT+08:00	Details
Medium	Host-Weak Password	Rule model	Feb 15, 2023 15:52:05 GMT+08:00	Feb 15, 2023 15:52:05 GMT+08:00	Details

Step 6 On the details page, click **Create Model** in the lower right corner. The page for creating an alert model is displayed.

Step 7 On the **Create Alarm Model** page, configure basic information.

- Pipeline Name: Select an execution pipeline for the alert model.

Table 6-1 Available pipelines

Alert Template	Execution Pipeline
Application-WAF Key Attack Alert	sec-waf-attack
Host-Virtual Machine Lateral Connection	sec-hss-log

Alert Template	Execution Pipeline
Network-High-Risk Port Exposure to the Outside	sec-nip-attack
Network-Login Brute Force Alarm	sec-nip-attack
Host-Suspected External Connection	sec-hss-log
Network-Source IP Attacking Multiple Targets	sec-nip-attack
Network-Command Injection Alert	sec-nip-attack
Network-Malicious External Communications	sec-nip-attack
Host-Reverse Shell	sec-hss-alarm
Host-Malware	sec-hss-alarm
Application-Distributed URL Traversal Attack	sec-waf-access
Application-Source IP Conducting URL Traversal	sec-waf-access
Host-High-risk Command Detection	sec-hss-alarm
Application-Source IP Brute-Forcing Domain Names	sec-waf-attack
Host-Brute Force Crack Success	sec-hss-alarm
Host-Abnormal Shell	sec-hss-alarm
Host-Weak Password	sec-hss-alarm
Host-Remote Login	sec-hss-alarm
Host-Rootkit Events	sec-hss-alarm

- Retain default values of other parameters.

Figure 6-6 Basic Settings

★ Pipeline Name: sec-waf-attack

★ Model Name: Application - WAF Key Attack Alert

★ Severity: Critical High Medium Low Informative

★ Alarm Type: Exploit Attack/General Exploit

Model Type: Rule model

★ Description: [Scenario Description] WAF is a security device or software specifically designed to protect web applications, which can detect and prevent various types of web attacks. Hackers who exploit vulnerabilities or defects in web applications may cause harm such as information leakage, website paralysis, malware propagation, and website tampering. [Model Principle] Analyze the WAF attack logs within five minutes every five minutes, bubbling up some key WAF alerts, such as attacks using deserialization vulnerabilities, Weblogic RCE attacks, Log4j2 remote code execution vulnerabilities and their deformation attacks.

Status:

Step 8 After the setting is complete, click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.

Step 9 Set the model logic. You are advised to retain the default value.

For details, see [Creating an Alert Model](#).

Step 10 After completing the basic settings, click **Next** in the lower right corner of the page.

Step 11 After confirming that the model is correct, click **OK** in the lower right corner of the page.

Step 12 Repeat [Step 5](#) to [Step 11](#) to create alert models with other templates.

----End

Enabling an Alert Model

Step 1 In the navigation pane on the left, choose **Threat Operations > Intelligent Modeling**.

Figure 6-7 Available Models

Severity	NameID	Status	Debugging	Pipeline Name	Model Type	Built-in	Updated	Created	Operation
High	87318122-0883-46D-8a24-71	Enable	Disable	sec-rip-attack	Rule model	No	Jun 02, 2023 16:50:53 GMT+	Jun 02, 2023 16:14:20 GMT+	Disable Edit Delete
Medium	64415a45-5a37-4a47-8000-64	Enable	Disable	sec-rip-attack	Rule model	No	Jun 02, 2023 17:33:52 GMT+	Jun 02, 2023 16:15:20 GMT+	Disable Edit Delete

Step 2 To enable models in batches, select all models you want to enable and click **Enable** in the upper left corner of the list.

- Step 3** If the model status changes to **Enabled**, the model is successfully started.
----End

6.3 Enabling a Playbook

SecMaster provides response playbooks for cloud security incidents. You can use playbooks to implement efficient and automatic response to security incidents. After data access, you can enable a playbook for automatic responses.

- You can enable the following workflows for playbooks. Built-in workflows are enabled by default.

WAF uncapping, Synchronization of HSS alert status, Fetching indicator from alert, WAF interception, and Automatic closing of repeated alerts.

- You can enable the following playbooks (built-in playbooks have been reviewed and their initial version v1 has been activated by default, so you can enable them directly):

Fetching indicator from alert, Synchronization of HSS alert status, and Automatic closing of repeated alerts

Procedure


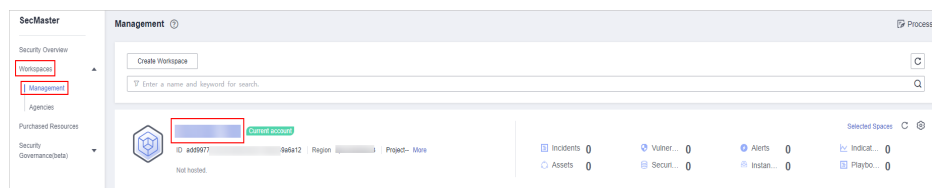
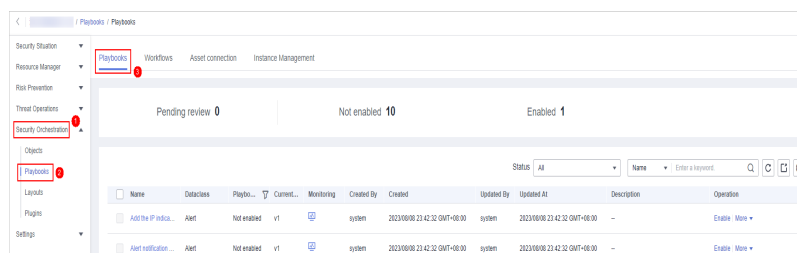
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 6-8 Workspace management page



- Step 4** In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 6-9 Accessing the Playbooks tab



- Step 5** On the playbook page, click **Enable** in the **Operation** column of each target playbook.

Figure 6-10 Enabling a Playbook

<input type="checkbox"/>	Name	Dataclass	Play...	Cur...	Monitor...	Created By	Created	Updated By	Updated At	Description	Operation
<input type="checkbox"/>	Synchronization of HDS...	Alert	Not ena...	--		system	2023/06/01 00:00:01 GMT+08...	system	2023/06/01 00:00:01 GMT+08:00	--	Enable More ▾
<input type="checkbox"/>	Capture asset data	Common...	Enabled	v1		system	2023/06/01 00:00:01 GMT+08...	system	2023/06/01 00:00:10 GMT+08:00	--	Disable Version Management
<input type="checkbox"/>	Automatic renaming of ...	Alert	Not ena...	--		system	2023/06/01 00:00:01 GMT+08...	system	2023/06/01 00:00:01 GMT+08:00	--	Enable More ▾

- Step 6** In the displayed dialog box, select the version v1 you want to enable and click **OK**.
----End

6.4 Performing Baseline Inspection

After data access, you need to set baseline inspection standards to check key configuration items of assets on the cloud. SecMaster can scan cloud services for risks in key configuration items, report scan results by category, generate alerts for risk settings, and provide hardening suggestions and guidelines.

You are advised to enable the following check standards: **Cloud Security Compliance Check 1.0**

Procedure


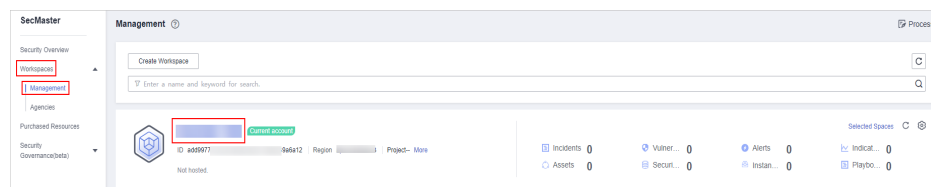
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

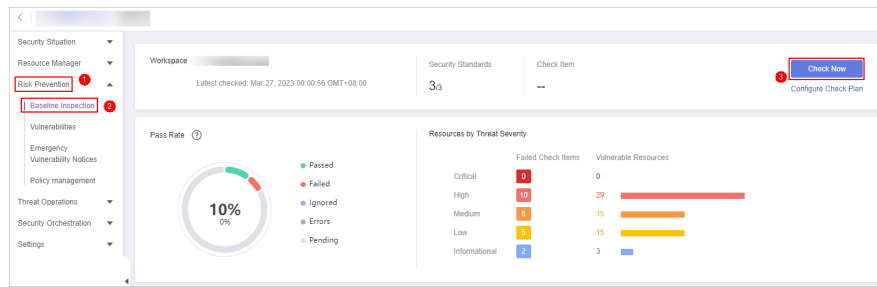
Figure 6-11 Workspace management page



- Step 4** In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. In the upper right corner of the page, click **Check Now** to execute the task immediately.

Refresh the page. To check whether the displayed result is the latest, click **View Details** in the **Operation** column and check the time in **Latest Check**.

Figure 6-12 Check Now




----End

7 Creating a Report

You can specify how you would like SecMaster to automatically send reports.

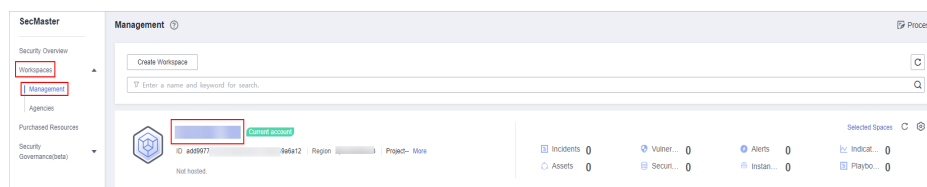
Creating a Report

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.

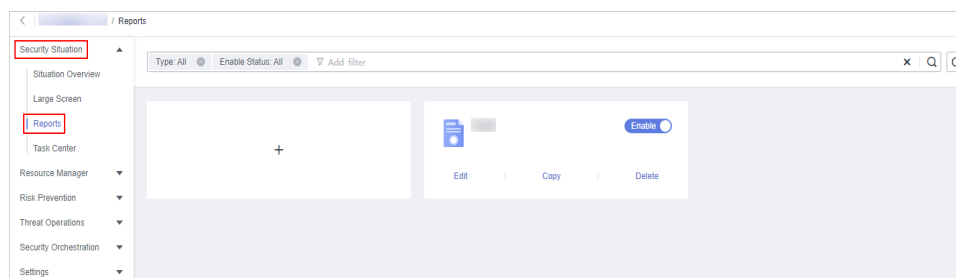
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.


Figure 7-1 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Situation > Reports**.

Figure 7-2 Reports



Step 5 On the **Reports** page, click  to go to the basic configuration page.

Step 6 Configure basic information of the report.

Table 7-1 Report parameters

Parameter	Description
Report Name	Name of the report you want to create.
Schedule	Select a report type. <ul style="list-style-type: none"> • Daily: SecMaster collects security information from 0:00 to 24:00 of the previous day by default. • Monthly: SecMaster collects statistics on security information from 00:00 on the first day to 24:00 on the last day of the previous month. • Custom: Customize a time range.
Data Scope	This field displays the data scope based on Schedule you specified. If you select Daily or Monthly for Schedule , the system displays the report data scope accordingly.
Schedule	If you select Daily or Monthly for Schedule , you only need to set when you want the reports are sent. <ul style="list-style-type: none"> • Daily: By default, SecMaster sends a report that includes security information generated from 00:00:00 to 23:59:59 on the previous day every day at the time you specify. • Monthly: By default, the system sends a report that includes the security information for the previous month on a monthly basis at the time you specify.
Send Interval	If you select Custom for Schedule , you need to set a report send interval.
Send Rule	If you select Custom for Schedule , you need to set when to send the report and the data scope. You can set up to five rules for sending reports.
Email Subject	Set the subject of the email for sending the report.
Recipient Email	Add the email address of each recipient. <ul style="list-style-type: none"> • You can add up to 100 email addresses. • Separate multiple email addresses with commas (,). Example: test01@example.com,test02@example.com
(Optional) Copy To	Add the email address of each recipient you want to copy the report to. <ul style="list-style-type: none"> • You can add up to 100 email addresses. • Separate multiple email addresses with commas (,). Example: test03@example.com,test04@example.com
(Optional) Remarks	Remarks for the security report.

Step 7 Click **Next: Report Choose** in the upper right corner. The **Report Selection** page is displayed.

Step 8 In the existing report layout area on the left, select a report layout. After selecting, you can preview the report layout in the right pane.

If you select **Daily** or **Monthly** for **Schedule**, select a corresponding report layout.

- Viewing a report in full screen: Click  in the upper left corner of the preview page on the right.

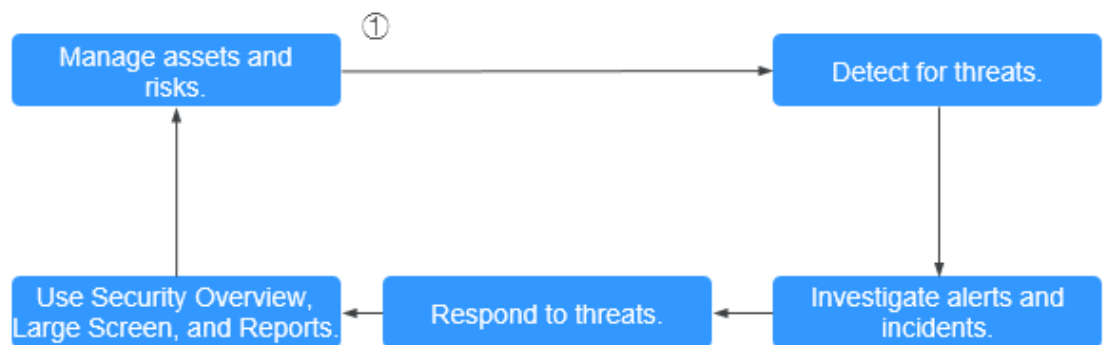
Step 9 Click **Complete** in the lower right corner. On the displayed **Reports** page, view the created report.

----End

8 Security Operations

After data integration is configured, you can perform operations such as asset management, threat detection, and alert investigation based on the integrated data.

Figure 8-1 Security Operations



Step 1: Manage Assets and Risks

The essence of security operations is security risk management. According to the definition of ISO, there are three elements, assets, vulnerabilities, and threats involved in security operations. Sorting the assets you want to protect is the starting point of the security operations service flow.

- **Resource Manager**

SecMaster helps you:

- Aggregate cloud assets from different accounts and regions into one place.
- Import off-cloud assets to SecMaster and mark the environment assets belong to.
- SecMaster marks asset security status to show whether there are unsafe settings, OS or application vulnerabilities, suspicious intrusions, or unprotected cloud services. For example, all ECSs must be protected with HSS, and all domain names must be protected with WAF.

For details, see [Managing Assets](#).

- **Checking and clearing unsafe settings**

During security operations, the most common "vulnerability" is unsafe settings. Based on security compliance experience, SecMaster forms a baseline for automatic checks and provides baseline check packages based on common specifications and standards in the industry.

- SecMaster can automatically check cloud service settings. For example, SecMaster can check whether permissions are assigned by roles in IAM, whether security groups allow all inbound access in VPC, and whether WAF protection policies are enabled. You can harden the configuration based on the recommended methods.

For details, see [Baseline Inspection](#).

- **Discovering and fixing vulnerabilities**

SecMaster can also help you detect and fix security vulnerabilities. SecMaster allows you to manage Linux, Windows, Web-CMS, and application vulnerabilities. It also gives you an overview of vulnerabilities in real time, including vulnerability scan details, vulnerability statistics, vulnerability types and distribution, top 5 vulnerabilities, and the top 5 risky servers.

For details, see [Vulnerability Management](#).

Step 2: Detect for Threats

After data sources are connected to SecMaster, we have counted the assets we need to protect and fixed unsafe settings and vulnerabilities. The next move is to identify suspicious activities and threats.

SecMaster provides multiple built-in templates designed by security experts and analysis teams based on known threats, common attack media, and suspicious activity reporting chains. With these templates, you will receive notifications of such threats when performing certain operations. These templates automatically search for suspicious activities throughout the environment. In addition, you can customize templates based on your needs to search for or find out activities.

SecMaster also supports cloud service security log data retrieval and analysis. In doing this, it provides professional security analysis and protects cloud workloads, applications, and data.

For details, see [Viewing Existing Model Templates](#) and [Security Analysis Overview](#).

Step 3: Investigate Alerts and Incidents

- **Investigating alerts**

Threat detection models analyze a large number of security cloud service logs to find suspected intrusion behaviors and generate alerts. An alert in SecMaster contains the following fields: name, severity, asset/threat that initiates suspicious behavior, and compromised assets. On-duty security personnel need to determine how bad an alert is within a very short period of time. If the risk is low, they will disable the alert (such as repeated alerts and O&M operations). If the risk is high, they will convert the alert to an incident.

For more details, see [Viewing Alerts](#) and [Converting an Alert to an Incident](#).

- **Investigating incidents**

After an alert is converted to an incident, you can view the incident on the incident management page and investigate and analyze it. You can associate an incident with entities related to suspicious behavior, such as assets (such as VMs), indicators (such as attack source IP addresses), accounts (such as leaked accounts), and processes (such as Trojans). You can also associate an incident with similar historical alerts or incidents.

For details, see [Viewing an Incident](#) and [Editing an Incident](#).

Step 4: Respond to Threats

With real-time automation, SecMaster can automatically respond to duplicate alerts to reduce your analysis workloads. SecMaster also provides automatic playbooks so that some threats can be handled automatically.

For details, see [Security Orchestration](#).

Step 5: Use Security Overview, Large Screen, and Reports

- **Security Overview**

This page displays the overall security assessment status of resources in the current workspace in real time so that you can learn cloud security posture and manage risks in a centralized manner.

- **Large Screen**

- Overall Situation: This screen gives an overview of attack status and predicts attack trends. You can view historical attacks and global metrics of security operations.
- Monitoring Statistics: You can view unhandled security risks, such as alerts, incidents, vulnerabilities, and unsafe baseline settings.
- Asset Security: On this screen, you can view risks by assets. You can learn how many assets you have, how many of them have been attacked, and how many of them are unprotected.
- Threat Situation: On this screen, you can view identified attacks, including the number of DDoS attacks, number of network attacks, number of blocked application attacks, and number of host attacks.
- Vulnerability screen: You can view the trend and distribution of vulnerable configurations or assets, such as vulnerable assets, vulnerabilities, baselines, and unprotected assets.

- **Security Report**

A security report includes details such as security scores, baseline check results, security vulnerabilities, and what policies are enabled. You can create security reports to learn about asset security status in a timely manner.

For more details, see [Situation Overview](#), [Large Screen](#), and [Reports](#).

9 Getting Started with Common Practices

After creating a workspace, collecting data, and enabling some checks in SecMaster, you can refer to practices provided in this topic to meet your service requirements.

Table 9-1 Common practices

Practice	Description
Security Panels	SecMaster can work with other security services and display overall cloud asset security posture in real time on SecMaster security panels.
Resource Manager	SecMaster automatically discovers and manages all assets on and off the cloud and displays the real-time security status of your assets.
Security Analysis	This topic describes how to use SecMaster to manage, aggregate, and analyze security alarms and logs of other cloud products concurrently so that you can obtain attack information and proactively discover threats.
Automatic Response Playbooks	This topic introduces security orchestration in SecMaster, which can help automatically respond to and handle security incidents in time.
Operation Guide to Data Transfer	This topic describes log collection methods, how to parse, transfer, query the collected log data in a visualized manner, as well as how to create threat models.

A Change History

Date	Description
2023-12-30	This issue is the first official release.