SecMaster

Getting Started

Issue	02
Date	2024-12-26

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 How to Buy and Use SecMaster Basic Edition

Scenario

SecMaster is a next-generation cloud native security operations center Huawei Cloud provides for you. With SecMaster, you can enjoy one-stop cloud security management. You can centrally manage cloud assets, security posture, security information, and incidents, improving security operations efficiency and responding to threats faster.

The following describes how to buy SecMaster in the EU-Dublin region for the first time and how to use the first workspace with only default settings for security operations.

- Billing mode: yearly/monthly
- Edition: basic edition
- ECS quota: 50

The following shows the operation process in this scenario.

Figure 1-1 Operation Process

Buy SecMaster.
Create a workspace.
Start security operations.

Operation Process

Procedure	Description
Preparations	Sign up for a Huawei account (HUAWEI ID), enable Huawei Cloud services, top up your account, and assign SecMaster permissions to the account.
Step 1: Buy SecMaster Basic Edition	Select a SecMaster edition, configure the ECS quota, and complete the purchase. (The basic edition is used as an example in this topic.)

Procedure	Description
Step 2: Create a Workspace	Create the first workspace for security operations.
Step 3: Start Security Operations	After the first workspace is created, SecMaster automatically initializes it. After the initialization is complete, you can experience SecMaster functions.

Preparations

1. Before purchasing SecMaster, sign up for a Huawei ID and enable Huawei Cloud services. For details, see **Registering a Huawei ID and Enabling Huawei Cloud Services** and **Real-Name Authentication**.

   If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Ensure that your account has sufficient balance or has a valid payment method configured. For details, see **Top-Up and Payment**.
3. Ensure that the **SecMaster FullAccess** permission has been assigned to the account. For details, see **Creating a User and Granting Permissions**.

   When purchasing SecMaster, you also need to grant the **BSS Administrator** permission to the account.

Step 1: Buy SecMaster Basic Edition

SecMaster provides **basic**, **standard**, and **professional** editions. Each edition has situation awareness, baseline inspection, query and analysis, and security orchestration functions.

This step shows how to configure parameters for buying SecMaster basic edition. For details about how to buy other SecMaster editions, see **Buying SecMaster**.

1. Log in to Huawei Cloud management console.
2. In the upper part of the page, select a region and choose **Security & Compliance** > **SecMaster** from the service list.
3. On the overview page, click **Buy SecMaster**. On the access authorization panel displayed, select **Agree** and click **OK**.
4. On the purchase page, configure required parameters.

   This example only introduces mandatory parameters. Configure other parameters as needed.

Table 1-1 Parameters for buying SecMaster

Parameter	Example Value	Description
Billing Mode	**Yearly/ Monthly**	Billing mode of your SecMaster. Select **Yearly/Monthly**.

Parameter	Example Value	Description
Region	**EU-Dublin**	Select the region based on where your cloud resources are located.
Edition	**Basic**	SecMaster provides basic, standard, and professional editions for your choice. For details about their differences, see **Edition Differences**.
Quota	**1**	The maximum number of ECSs you want to protect. 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. ● 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. To prevent this, increase the quota upon an increase of your host quantity.
Required Duration	**1 month**	How long you want to use the service. Select a duration based on your needs.

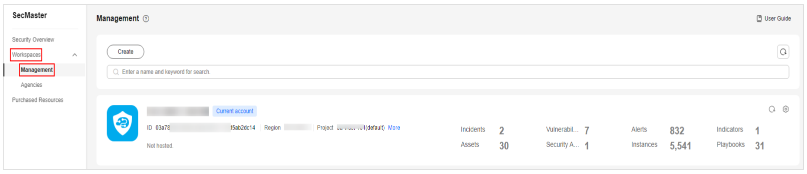
5. Confirm the product details and click **Next**.
6. After confirming that the order details are correct, read the *SecMaster Disclaimer* and select "I have read and agree to the SecMaster Disclaimer", and click **Pay Now**.
7. On the payment page, select a payment method and complete the payment.
8. Return to the SecMaster console.

Step 2: Create a Workspace

Workspaces are top-level workbenches in SecMaster. Before using SecMaster, you need to create a workspace first.

1. In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 1-2 Workspaces > Management



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

   SecMaster depends on some other cloud services, so to better use SecMaster, you can authorize SecMaster to perform some operations on certain cloud services on your behalf. For example, you can allow SecMaster to execute scheduling tasks and manage resources.

   Your authorization is required first time you try to use SecMaster.

3. On the workspace management page, click **Create** and set workspace parameters.

   This example only introduces mandatory parameters. Configure other parameters as needed.

   Table 1-2 Parameters for creating a workspace

Parameter	Example Value	Description
Region	**EU-Dublin**	Select the region based on where your cloud resources are deployed.
Project Type	**Common Project**	Project that the workspace belongs to
Workspace Name	**SecMaster**	Name of the workspace used for security operations.

4. Click **OK**

Step 3: Start Security Operations

After the first workspace is created, SecMaster automatically initializes it. After the initialization is complete, you can experience SecMaster functions.

1. Managing 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, in security operations. Sorting the assets you want to protect is the starting point of the security operations service flow.

   – **Asset management**

     SecMaster helps you enable cross-region, cross-account, and cross-environment aggregation of assets. For assets from other environments, SecMaster will mark the environments these assets belong to. After the aggregation, 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. This makes it possible for you to view security of all your assets in one place.

     For details, see **Managing Assets**.

- **Detecting and clearing unsafe settings**

  During security operations, the most common vulnerabilities are 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 role 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**.

2. On the dashboard for security situation, you can check security scores of resources in the current workspace and quickly learn about the overall security.

   For details, see **Situation Overview**.

Related Information

Since you have experienced the SecMaster basic edition, you may need SecMaster standard and professional editions to meet your ever-changing security requirements. These two editions provide more features, such as more security data sources, comprehensive security models, and threat response playbooks. You will get more in-depth, comprehensive security analysis and tailored security strategies. Specifically, you can:

- **Enable log access**: You can enable access to logs of cloud services for centralized log management, retrieval, and analysis. So, you can monitor your service environment in real time and detect abnormal behavior and potential threats in a timely manner.
- **Collect logs**: You can also use SecMaster to collect logs from non-Huawei Cloud services. Security data from a variety of sources is aggregated in SecMaster. This makes it possible for you to analyze security situation more deeply and comprehensively, locate fault causes more easily, and address security issues more quickly.
- **Manage vulnerabilities**: After configuration risks are fixed, SecMaster can help detect and fix security vulnerabilities. You can use SecMaster to centrally manage Linux, Windows, Web-CMS, application, and website vulnerabilities. You will have an overview of vulnerabilities in real time, including vulnerability scan details, vulnerability statistics, vulnerability types and distribution, top 5 vulnerabilities, and top 5 risky servers.
- **Check alerts**: Threat detection models in SecMaster analyze a large number of logs reported by security cloud services to identify suspected intrusions and generate alerts. An alert in SecMaster contains the following fields: name, severity, asset/threat that initiates suspicious activities, and compromised assets. Security operations engineers need to analyze and investigate alerts to find out real threats. If the risk is low, they will close the alert (such as repeated alerts and O&M operations). If the risk is high, they will convert the alert into an incident.
- **View Incidents**: If an alert is converted into an incident, you can check the incident on the **Incidents** page. You can investigate the incident and take an

emergency response. You can associate an incident with entities related to suspicious activities. The entities include 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.

- **Create an alert model**: You can use models to monitor logs in pipelines. If a log matches any trigger condition set in a model, the model will report an alert.
- **Start security analysis**: You can further analyze logs and filter threats precisely.
- **Enable a playbook**: You can use playbooks to enable automated security incident responses. This will greatly reduce the mean time to repair (MTTR) and improve the overall protection.
- **Create an emergency policy**: You can use emergency policies to quickly handle cyber security threats and restrict or block access from specific IP addresses, protecting your network resources and customers' data.
- **Create security report**: SecMaster will send security reports to you in the way you specify. You will see security scores, baseline check results, security vulnerabilities, and policy coverage in a security report. This helps you learn about asset security status in a timely manner.
- **Enable large screens**: Through large screens, you can check real-time resource security situation and handles attacks. This function helps security operations teams monitor and analyze security threats and incidents in real time and quickly respond to them.

2 How to Buy and Use SecMaster Standard Edition

Scenario

SecMaster is ready for out-of-the-box. By default, for the first workspace in each region, all assets in the current region are automatically loaded, access to recommended cloud service logs enabled, and select preconfigured models and playbooks enabled. This frees you from complex manual configurations, simplifies the use process, and improves efficiency. For non-first workspaces, you need to manually configure and enable security and asset data access.

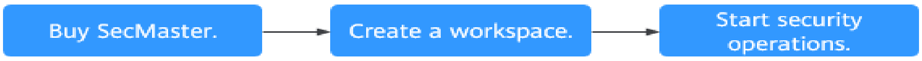
After purchasing SecMaster and creating the first workspace, you can view the resource security situation, manage assets centrally, comprehensively analyze log data, and automate security orchestration and incident response. These help you build a comprehensive security system for your assets, implement automated security operations and management, and meet your security requirements with ease.

The following describes how to buy SecMaster in the EU-Dublin region for the first time and how to use the first workspace with only default settings for security operations.

- Billing mode: yearly/monthly
- Edition: standard edition
- ECS quota: 50

The following shows the operation process in this scenario.

Figure 2-1 Operation Process



Operation Process

Procedure	Description
Preparations	Sign up for a Huawei account (HUAWEI ID), enable Huawei Cloud services, top up your account, and assign SecMaster permissions to the account.
Step 1: Buy SecMaster Standard Edition	Select a SecMaster edition, configure the ECS quota, and complete the purchase. (The standard edition is used as an example in this topic.)
Step 2: Create a Workspace	Create the first workspace for security operations.
Step 3: Start Security Operations	After the first workspace in a region is created, SecMaster automatically initializes it. After the initialization completes, you can start managing assets, checking for threats, investigating alerts, handling threats, as well as other security operations activities. You can also view the security situation on the situation overview page and large screens. During the initialization, SecMaster enables access to all assets and recommended cloud service logs, such as WAF attack logs, in the current account in the current region on the cloud, as well as select preconfigured threat models and playbooks, such as the model of HSS abnormal network connection and playbook of automatic notification of high-risk vulnerabilities.

Preparations

1. Before purchasing SecMaster, sign up for a Huawei ID and enable Huawei Cloud services. For details, see **Registering a Huawei ID and Enabling Huawei Cloud Services** and **Real-Name Authentication**.

   If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Ensure that your account has sufficient balance or has a valid payment method configured. For details, see **Top-Up and Payment**.
3. Ensure that the **SecMaster FullAccess** permission has been assigned to the account. For details, see **Creating a User and Granting Permissions**.

   When purchasing SecMaster, you also need to grant the **BSS Administrator** permission to the account.

Step 1: Buy SecMaster Standard Edition

SecMaster provides **basic**, **standard**, and **professional** editions. Each edition has situation awareness, baseline inspection, query and analysis, and security orchestration functions.

This step shows how to configure parameters for buying SecMaster standard edition. For details about how to buy other SecMaster editions, see **Buying SecMaster**.

1. Log in to Huawei Cloud management console.
2. In the upper part of the page, select a region and choose **Security & Compliance** > **SecMaster** from the service list.
3. On the overview page, click **Buy SecMaster**. On the access authorization panel displayed, select **Agree** and click **OK**.
4. On the purchase page, configure required parameters.

Table 2-1 Parameters for buying SecMaster

Parameter	Example Value	Description
Billing Mode	**Yearly/ Monthly**	Billing mode of your SecMaster. Select **Yearly/Monthly**.
Region	**EU-Dublin**	Select the region based on where your cloud resources are located.
Edition	**Standard**	SecMaster provides basic, standard, and professional editions for your choice. For details about their differences, see **Edition Differences**.
Quota	**50**	The maximum number of ECSs you want to protect. 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. ● 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. To prevent this, increase the quota upon an increase of your host quantity.
Large Screen	**Disabled**	**Large Screen**, **Log Audit**, **Security Analysis**, and **Security Orchestration** are optional functions. To buy them, set the purchase quantity as required. For details about the value-added package and recommended configurations, see **Value-Added Package Description**.
Log Audit	**Buy later**	
Security Analysis	**Buy later**	
Security Orchestration	**Buy later**	

Parameter	Example Value	Description
Tag	- **Tag key**: **test** - **Tag value**: **01**	Tags attached to SecMaster to identify resources. For details about tags, see Tag Management Service.
Required Duration	**1 month**	Select the required duration as required. You do not need to configure this parameter in **pay-per-use** mode. The **Auto-renew** option enables the system to renew your service by the purchased period when the service is about to expire.

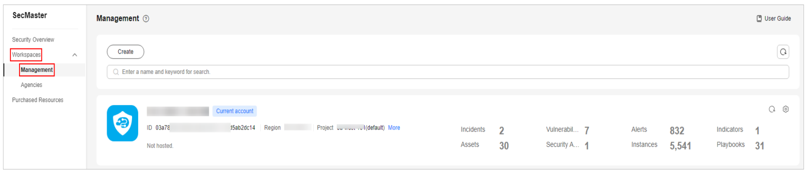
5. Confirm the product details and click **Next**.
6. After confirming that the order details are correct, read the *SecMaster Disclaimer* and select "I have read and agree to the SecMaster Disclaimer", and click **Pay Now**.
7. On the payment page, select a payment method and complete the payment.
8. Return to the SecMaster console.

Step 2: Create a Workspace

Workspaces are top-level workbenches in SecMaster. Before using SecMaster, you need to create a workspace first.

1. In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 2-2 Workspaces > Management



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

   SecMaster depends on some other cloud services, so to better use SecMaster, you can authorize SecMaster to perform some operations on certain cloud services on your behalf. For example, you can allow SecMaster to execute scheduling tasks and manage resources.

   Your authorization is required first time you try to use SecMaster.
3. On the workspace management page, click **Create** and set workspace parameters.

   This example only introduces mandatory parameters. Configure other parameters as needed.

Table 2-2 Parameters for creating a workspace

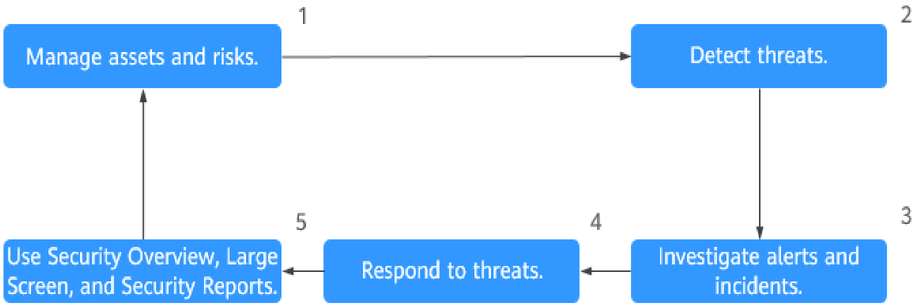
Parameter	Example Value	Description
Region	**EU-Dublin**	Select the region based on where your cloud resources are deployed.
Project Type	**Common Project**	Project that the workspace belongs to
Workspace Name	**SecMaster**	Name of the workspace used for security operations.

4. Click **OK**

Step 3: Start Security Operations

After the first workspace is created, SecMaster automatically initializes it. After the initialization completes, you can start managing assets, checking for threats, investigating alerts, handling threats, as well as other security operations activities. You can also view the security situation on the situation overview page and large screens.

Figure 2-3 Secure operations


1
Manage assets and risks.
2
Detect threats.
3
Investigate alerts and incidents.
4
Respond to threats.
5
Use Security Overview, Large Screen, and Security Reports.

1. Managing 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, in security operations. Sorting the assets you want to protect is the starting point of the security operations service flow.

   - **Asset management**

     SecMaster helps you enable cross-region, cross-account, and cross-environment aggregation of assets. For assets from other environments, SecMaster will mark the environments these assets belong to. After the aggregation, 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. This makes it possible for you to view security of all your assets in one place.

For details, see **Managing Assets**.

- **Detecting and clearing unsafe settings**

  During security operations, the most common vulnerabilities are 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 role 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. You can use SecMaster to centrally manage Linux, Windows, Web-CMS, application, and website vulnerabilities. You will have an overview of vulnerabilities in real time, including vulnerability scan details, vulnerability statistics, vulnerability types and distribution, top 5 vulnerabilities, and top 5 risky servers.

  For details, see **Vulnerability Management**.

2. Detecting threats

   As we have sorted out the assets we need to protect and fixed unsafe settings and vulnerabilities, after data sources are connected to SecMaster, the next move is to identify suspicious activities and threats.

   SecMaster provides many preconfigured threat detection models. These models were designed by security experts and analysis teams based on known threats, common attack media, and suspicious activities. You will receive notifications once suspicious activities trigger those models. These models automatically search the entire environment for suspicious activities. You can also create custom threat detection models to meet your needs.

   SecMaster also provides the log data query function to help you discover threats.

   For details, see **Managing Model Templates** and **Security Analysis**.

3. Investigating alerts and incidents

   - **Investigating alerts**

     Threat detection models analyze 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 activities, and compromised assets. Security operations engineers need to analyze and investigate alerts to find out real threats. 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 into an incident.

     For more details, see **Viewing Alerts** and **Converting an Alert into an Incident**.

   - **Investigating incidents**

     After an alert is converted into an incident, you can view incident in the incident management module. You can investigate the incident and take emergency response to it. You can associate an incident with entities related to suspicious activities. The entities include 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**.

4. Responding to threats

   You can use playbooks to enable automated alert and incident responses.

   For details, see **Security Orchestration**.

5. Use **Security Overview**, **Large Screen**, and **Security Reports**.
   - **Security Overview**

     This page displays the security scores of resources in the current workspace, so you can quickly learn about the security status.
   - **Large Screen**

     You can view the real-time situation of resources and handle attack incidents. This function helps security operations teams monitor and analyze security threats and incidents in real time and quickly respond to them.
   - **Security reports**

     Security reports are sent by SecMaster automatically. You will see security scores, baseline check results, security vulnerabilities, and policy coverage in a security report. This helps you learn about asset security status in a timely manner.

   For more details, see **Situation Overview**, **Large Screen**, and **Security Reports**.

Related Information

You can also enable access to a variety of data sources, activate all models and playbooks to analyze security status deeply and comprehensively, and configure security policies best fit your environment.

- **Enable log access**: You can enable access to logs of cloud services for centralized log management, retrieval, and analysis. So, you can monitor your service environment in real time and detect abnormal behavior and potential threats in a timely manner.

  NOTE

  You are advised to enable access to asset details, asset alerts, baseline inspection results, vulnerability data, and logs in one workspace. This will make it easier for centralized security operations and association analysis.
- **Collect logs**: You can also use SecMaster to collect logs from non-Huawei Cloud services. Security data from a variety of sources is aggregated in SecMaster. This makes it possible for you to analyze security situation more deeply and comprehensively, locate fault causes more easily, and address security issues more quickly.
- **Create an alert model**: You can use models to monitor logs in pipelines. If a log matches any trigger condition set in a model, the model will report an alert.

- **Enable a playbook**: You can use playbooks to enable automated security incident responses. This will greatly reduce the mean time to repair (MTTR) and improve the overall protection.
- **Start a baseline check**: You can start a baseline check to assess how secure your OSs, software, databases are. This helps you rectify security risks, mitigate potential threats, and meet compliance requirements.
- **Create an emergency policy**: You can use emergency policies to quickly handle cyber security threats and restrict or block access from specific IP addresses, protecting your network resources and customers' data.
- **Create security report**: SecMaster will send security reports to you in the way you specify. You will see security scores, baseline check results, security vulnerabilities, and policy coverage in a security report. This helps you learn about asset security status in a timely manner.

3 How to Buy and Use SecMaster Professional Edition

Scenario

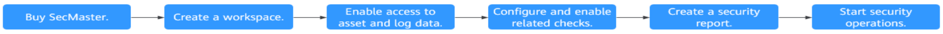
SecMaster is a next-generation cloud native security operations center Huawei Cloud provides for you. With SecMaster, you can enjoy one-stop cloud security management. You can centrally manage cloud assets, security posture, security information, and incidents, improving security operations efficiency and responding to threats faster.

The following describes how to buy SecMaster in the EU-Dublin region for the first time and how to use the first workspace for security operations.

- Billing mode: yearly/monthly
- Edition: Professional edition
- ECS quota: 50
- Value-added package: large screen, log audit, security analysis, and security orchestration

The following shows the operation process in this scenario.

Figure 3-1 Operation Process


Buy SecMaster.
Create a workspace.
Enable access to asset and log data.
Configure and enable related checks.
Create a security report.
Start security operations.

Operation Process

Procedure	Description
Preparations	Sign up for a Huawei account (HUAWEI ID), enable Huawei Cloud services, top up your account, and assign SecMaster permissions to the account.
Step 1: Buy SecMaster Professional Edition	Select a SecMaster edition, configure the ECS quota, and complete the purchase. (The professional edition is used as an example in this topic.)

Procedure	Description
Step 2: Create a Workspace	Create the first workspace for security operations.
Step 3: Access Security Data	You can enable security data access to SecMaster and manage all security data in SecMaster. ● Subscribe to asset data: Subscribe to all asset data in the current region under the current account for centralized asset management. ● Enable log access: Logs of other services are aggregated into SecMaster for centralized management and analysis. – Aggregation of logs from other Huawei Cloud services – (Optional) Enabling access to logs from non-Huawei Cloud services
Step 4: Configure and Enable Related Checks	You can enable alert models, activate playbooks, start baseline inspections, and configure security policies. SecMaster will help check all your resources comprehensively. ● Enable preconfigured models: You can use models to monitor logs. If any content that meets the trigger condition is detected, an alert is generated. ● Enable playbooks: You can use playbooks to enable automated security incident responses. ● Perform a baseline check: You can learn the latest baseline configuration status and risky settings. ● (Optional) Configure defense policies and emergency policies: You can configure defense policies to implement full-process protection and configure emergency policies to control risks.
Step 5: Create a Security Report	You can specify how you would like SecMaster to automatically send security operations reports.
Step 6: Start Security Operations	You can now start security operations, such as asset management, threat detection, and alert investigation, based on the integrated data.

Preparations

1. Before purchasing SecMaster, sign up for a Huawei ID and enable Huawei Cloud services. For details, see **Registering a Huawei ID and Enabling Huawei Cloud Services** and **Real-Name Authentication**.

If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.

2. Ensure that your account has sufficient balance or has a valid payment method configured. For details, see **Top-Up and Payment**.
3. Ensure that the **SecMaster FullAccess** permission has been assigned to the account. For details, see **Creating a User and Granting Permissions**.

   When purchasing SecMaster, you also need to grant the **BSS Administrator** permission to the account.

Step 1: Buy SecMaster Professional Edition

SecMaster provides **basic**, **standard**, and **professional** editions. Each edition has situation awareness, baseline inspection, query and analysis, and security orchestration functions.

This step shows how to configure parameters for buying SecMaster professional edition. For details about how to buy other SecMaster editions, see **Buying SecMaster**.

1. Log in to Huawei Cloud management console.
2. In the upper part of the page, select a region and choose **Security & Compliance** > **SecMaster** from the service list.
3. On the overview page, click **Buy SecMaster**. On the access authorization panel displayed, select **Agree** and click **OK**.
4. On the purchase page, configure required parameters.

Table 3-1 Parameters for buying SecMaster

Parameter	Example Value	Description
Billing Mode	**Yearly/ Monthly**	Billing mode of your SecMaster. ● Yearly/Monthly is a prepaid billing mode. You pay in advance for a subscription term. The longer you use the service, the more discounts you got. ● Pay-per-use billing is a postpaid mode in which you pay for what you use. You are billed by second based on the actual usage. Your bill is settled by the hour. With the pay-per-use billing mode, you can easily adapt to resource requirement changes, reducing the risk of over-provisioning of resources or lacking capacity. In this mode, there are no upfront commitments required.
Region	**EU-Dublin**	Select the region based on where your cloud resources are located.

Parameter	Example Value	Description
Edition	**Professional**	SecMaster provides basic, standard, and professional editions for your choice. For details about their differences, see **Edition Differences**.
Quota	**50**	The maximum number of ECSs you want to protect. 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. ● 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. To prevent this, increase the quota upon an increase of your host quantity.
Large Screen	**Enabled**	**Large Screen**, **Log Audit**, **Security Analysis**, and **Security Orchestration** are optional functions. To buy them, set the purchase quantity as required. For details about the value-added package and recommended configurations, see **Value-Added Package Description**.
Log Audit	**Buy now** and set the specifications based on the number of logs generated each day.	
Security Analysis	**Buy now** and set the daily quota for each server as needed.	
Security Orchestration	**Buy now** and set the data collection and retention quotas.	
Tag	● **Tag key**: **test** ● **Tag value**: **01**	Tags attached to SecMaster to identify resources. For details about tags, see **Tag Management Service**.

Parameter	Example Value	Description
Required Duration	**1 month**	Select the required duration as required. You do not need to configure this parameter in **pay-per-use** mode. The **Auto-renew** option enables the system to renew your service by the purchased period when the service is about to expire.

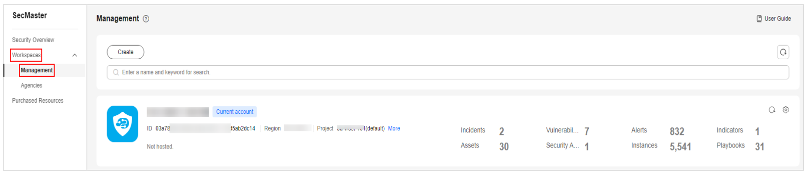
5. Confirm the product details and click **Next**.
6. After confirming that the order details are correct, read the *SecMaster Disclaimer*, select "I have read and agree to the SecMaster Disclaimer", and click **Pay Now**.
7. On the payment page, select a payment method and complete the payment.
8. Return to the SecMaster console.

Step 2: Create a Workspace

Workspaces are top-level workbenches in SecMaster. Before using SecMaster, you need to create a workspace first.

1. In the navigation pane on the left, choose **Workspaces** > **Management**.

   Figure 3-2 Workspaces > Management

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

   SecMaster depends on some other cloud services, so to better use SecMaster, you can authorize SecMaster to perform some operations on certain cloud services on your behalf. For example, you can allow SecMaster to execute scheduling tasks and manage resources.

   Your authorization is required first time you try to use SecMaster.

3. On the workspace management page, click **Create** and set workspace parameters.

   This example only introduces mandatory parameters. Configure other parameters as needed.

Table 3-2 Parameters for creating a workspace

Parameter	Example Value	Description
Region	**EU-Dublin**	Select the region based on where your cloud resources are deployed.
Project Type	**Common Project**	Project that the workspace belongs to.
Workspace Name	**SecMaster**	Name of the workspace used for security operations.

4. Click **OK**

Step 3: Access Security Data

Security data in SecMaster comes from other cloud services. So, after creating a workspace, you need to enable security data access to SecMaster for centralized management.

- **Enabling asset subscription**

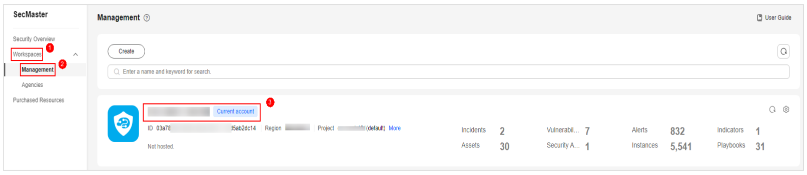
  SecMaster manages assets such as websites, ECSs, databases, IP addresses, and VPCs, and associates them with corresponding security services. During network protection and KEA, SecMaster aspires to build an overall network protection architecture from multiple aspects, such as the network layer, application layer, host layer, and data layer, to ensure the security and stability of user service systems.

  The first workspace in each region automatically loads all assets in the corresponding region. The non-first workspaces do not load assets automatically. You need to manually configure asset subscriptions based on your security operations needs.

  This part describes how to manually access asset data.

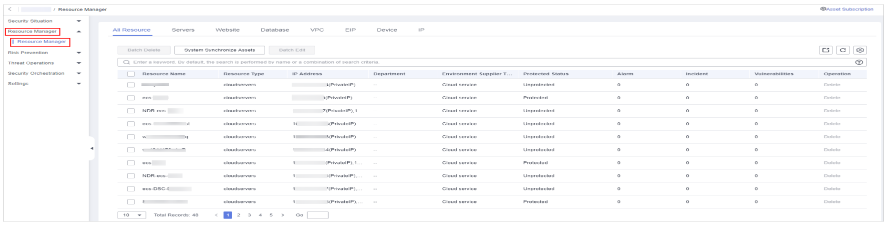
  a. In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

  Figure 3-3 Workspace management page

  b. In the navigation pane on the left, choose **Resource Manager** > **Resource Manager**.

Figure 3-4 Resource Manager



< [redacted] / Resource Manager Asset Subscription

	Resource Name	Resource Type	IP Address	Department	Environment Supplier T...	Protected Status	Alarm	Incident	Vulnerabilities	Operation
□	[redacted]	cloudservers	[redacted]4(PrivateIP)	--	Cloud service	Unprotected	0	0	0	Delete
□	ecs-[redacted]	cloudservers	[redacted]3(PrivateIP)	--	Cloud service	Protected	0	0	0	Delete
□	NDR-ecs-[redacted]	cloudservers	[redacted]7(PrivateIP),1...	--	Cloud service	Unprotected	0	0	0	Delete
□	ecs-[redacted]st	cloudservers	1[redacted](PrivateIP)	--	Cloud service	Unprotected	0	0	0	Delete
□	w[redacted]q	cloudservers	1[redacted]3(PrivateIP)	--	Cloud service	Unprotected	0	0	0	Delete
□	[redacted]	cloudservers	1[redacted]4(PrivateIP)	--	Cloud service	Unprotected	0	0	0	Delete
□	ecs[redacted]	cloudservers	1[redacted](PrivateIP),1...	--	Cloud service	Protected	0	0	0	Delete
□	NDR-ecs-[redacted]	cloudservers	1[redacted](PrivateIP),...	--	Cloud service	Unprotected	0	0	0	Delete
□	ecs-DSC-[redacted]	cloudservers	1[redacted](PrivateIP),...	--	Cloud service	Unprotected	0	0	0	Delete
□	s[redacted]	cloudservers	1[redacted]3(PrivateIP),...	--	Cloud service	Protected	0	0	0	Delete

10 Total Records: 48 < 1 2 3 4 5 > Go

c. On the **Resource Manager** page, click **Asset Subscription** in the upper right corner.

d. 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.

e. Click **OK**.

   If you enable asset subscription, SecMaster updates asset information within one minute. Then, SecMaster updates asset information automatically every night.

- **Aggregation of logs from other cloud services**

  Logs are important security data for secure operations. In SecMaster, you can quickly enable access to logs of many cloud services, such as WAF and HSS. After you enable the access, you can manage logs centrally and search and analyze all collected logs.

  For the first workspace in each region, SecMaster automatically enables access to logs of most cloud services. For non-first workspaces, you need to manually configure log data access based on your security operations needs.

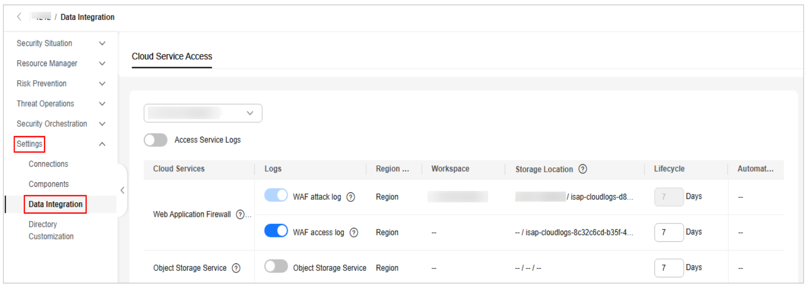
  NOTE

  > You are advised to enable access to asset details, asset alerts, baseline inspection results, vulnerability data, and logs in one workspace. This will make it easier for centralized security operations and association analysis.

  This part describes how to manually enable access to cloud service logs you may need.

  a. In the navigation pane on the left, choose **Settings** > **Data Integration**.

Figure 3-5 Data Integration page



< [redacted] / Data Integration

Cloud Services	Logs	Region ...	Workspace	Storage Location	Lifecycle	Automat...
Web Application Firewall	WAF attack log	Region	[redacted]	[redacted] / isap-cloudlogs-d8...	7 Days	--
	WAF access log	Region	--	-- / isap-cloudlogs-8c32c6cd-b35f-4...	7 Days	--
Object Storage Service	Object Storage Service	Region	--	-- / -- / --	7 Days	--

  b. Locate the target cloud service and click ○ in the **Logs** column.

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

c. Set the lifecycle. The default value is recommended.

d. 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 will be converted into an alert.

e. Click **Save**.

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

- (Optional) Enabling access to logs from non-Huawei Cloud services

  You can aggregate security logs from third-party (non-Huawei Cloud) services to SecMaster. For details, see **Data Collection**.

Step 4: Configure and Enable Related Checks

- **Creating and enabling an alert model**

  SecMaster provides preconfigured security analysis models based on application, network, and host security data to automatically aggregate, analyze, and report alerts.

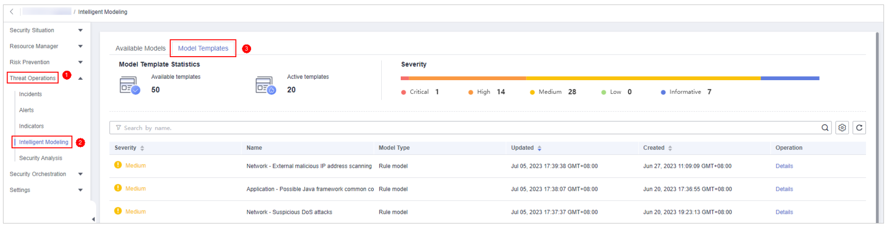
  Aggregating and analyzing alerts through models cut the false positive rate and make on-duty personnel respond more efficiently. You can also adjust models in different scenarios to filter out false alerts as many as possible.

  For the first workspace in each region, SecMaster automatically enables some preconfigured models. For non-first workspaces in each region, you need to enable preconfigured models manually and create custom alert models to meet your operation needs.

  To use preconfigured models that have not been enabled by SecMaster, you can create custom models from model templates by referring to the following steps:

a. In the navigation pane on the left, choose **Threat Operations** > **Intelligent Modeling**, and select the **Model Templates** tab.

Figure 3-6 Model Templates tab



Model Template Statistics

Available templates 50

Active templates 20

Severity

Critical 1 High 14 Medium 28 Low 0 Informative 7

Severity	Name	Model Type	Updated	Created	Operation
Medium	Network - External malicious IP address scanning	Rule model	Jul 05, 2023 17:39:38 GMT+08:00	Jun 27, 2023 11:09:09 GMT+08:00	Details
Medium	Application - Possible Java framework common co	Rule model	Jul 05, 2023 17:38:07 GMT+08:00	Jun 20, 2023 17:36:55 GMT+08:00	Details
Medium	Network - Suspicious DoS attacks	Rule model	Jul 05, 2023 17:37:37 GMT+08:00	Jun 20, 2023 19:23:13 GMT+08:00	Details

b. In the model template list, locate the target model template and click **Details** in the **Operation** column. On the template details panel displayed on the right, click **Create Model** in the lower right corner.

c. On the **Create Alert Model** page, configure basic information.

   - **Pipeline Name**: Select a pipeline for the alert model. You can select a pipeline based on the **Usage constraints** in the description.
   - Retain default values of other parameters.

d. Complete all settings and click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.

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

f. Complete all settings and click **Next** in the lower right corner of the page.

g. Review all settings and click **OK** in the lower right corner of the page.

h. Repeat **b** to **g** to create alert models with other templates.

- **Enabling a playbook**

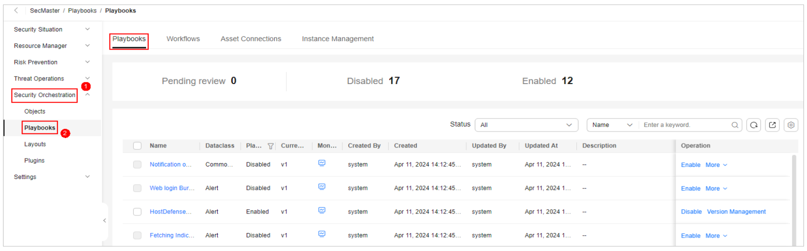
  SecMaster provides response playbooks for cloud security incidents. You can use playbooks to implement efficient and automatic response to security incidents.

  For the first workspace in each region, SecMaster enables preconfigured workflows as well as the most commonly used playbooks. You can use them directly. For non-first workspaces in each region, you need to manually enable playbooks to meet your security operations needs.

  You can follow the following procedure to enable other playbooks:

  a. In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

  Figure 3-7 Accessing the Playbooks tab



	Name	Dataclass	Pla...	Curre...	Mon...	Created By	Created	Updated By	Updated At	Description	Operation
□	Notification o...	Commo...	Disabled	v1		system	Apr 11, 2024 14:12:45...	system	Apr 11, 2024 1...	--	Enable More
□	Web login Bur...	Alert	Disabled	v1		system	Apr 11, 2024 14:12:45...	system	Apr 11, 2024 1...	--	Enable More
□	HostDefense...	Alert	Enabled	v1		system	Apr 11, 2024 14:12:45...	system	Apr 11, 2024 1...	--	Disable Version Management
□	Fetching Indic...	Alert	Disabled	v1		system	Apr 11, 2024 14:12:45...	system	Apr 11, 2024 1...	--	Enable More

  b. On the **Playbooks** tab, locate the target playbook and click **Enable** in the **Operation** column.

  c. In the displayed dialog box, select version v1 and click **OK**.

- **Conducting a baseline inspection**

  After enabling access to security data, you can check key configuration items of cloud assets in accordance with appliable baseline inspection standards. 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. The baseline inspection supports periodic and immediate checks.

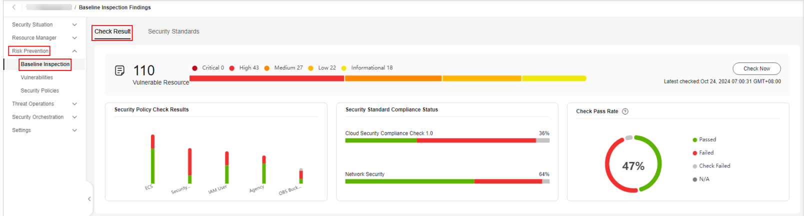
  – Periodic check: SecMaster periodically executes the default check plan or the check plans you configure.

  – Immediate check: You can start check items in all security standards or a specific check plan anytime.

  The following describes how to start an immediate check for check items in a compliance pack.

  a. In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**.

Figure 3-8 Accessing the check result page



b. On the **Check Result** page, click **Check Now**. In the dialog box displayed, click **OK**.

   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**.

- (Optional) **Configuring defense policies and emergency policies**

  You can enable, configure, and apply protection policies for seven layers of defense and enjoy comprehensive protection. You can configure emergency policies to control security risks in a timely manner.

  a. Configuring an emergency policy

     i. In the navigation pane on the left, choose **Risk Prevention** > **Security Policies**. Then, go to the emergency policy page.

     ii. On the **Emergency Policies** tab, click **Add**. The page for adding policies slides out from the right of the page.

     iii. On the page for adding a policy, configure the policy details.

Table 3-3 Emergency policy parameters

Parameter	Description
Blocked Object Type	Type of the object you want to block. You can select **IP** or **IAM**.

Parameter	Description
Block Object	● If you select **IP** for **Blocked Object Type**, enter one or more IP addresses or IP address ranges you want to block. If there are multiple IP addresses or IP address ranges, separate them with commas (,). ● If you select **IAM** for **Blocked Object Type**, enter IAM user names. ● There are some restrictions on delivery of blocked objects: – When a policy needs to be delivered to CFW, each time a maximum of 50 IP addresses can be added as blocked objects for each account. – When a policy needs to be delivered to WAF, each time a maximum of 50 IP addresses can be added as blocked objects for each account. – When a policy needs to be delivered to VPC, each time a maximum of 20 IP addresses can be added as blocked objects within 1 minute for each account. – When a policy needs to be delivered to IAM, each time a maximum of 50 IAM users can be added as blocked objects for each account.
Label	Label of a custom emergency policy.
Operation Connection	Asset connections that are used to operate blocking workflows of security services in the seven layers of defense. Select the operation connection for the policy.
Block Aging	Check whether the policy needs to be stopped. ● If you select **Yes**, set the aging time of the policy. For example, if you set the aging time to 180 days, the policy is valid within 180 days after the setting. After 180 days, the IP address/range or the IAM user will not be blocked. ● If you select **No**, the policy is always valid and blocks the specified IP address/range or the IAM user.
Reason Description	Description of the custom policy.

iv. Click **OK**

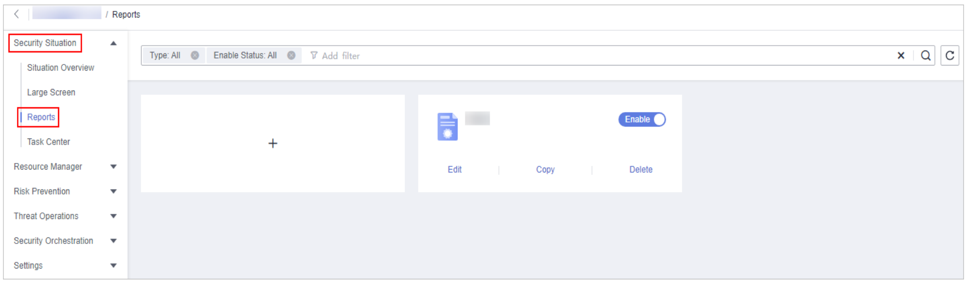
Step 5: Create a Security Report

Security reports are sent by SecMaster automatically. You will see security scores, baseline check results, security vulnerabilities, and policy coverage in a security report. This helps you learn about asset security status in a timely manner.

This step describes how to create a daily security operations report.

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

Figure 3-9 Reports



2. On the security report page, click +. On the displayed page, configure basic report information.

Table 3-4 Security report parameters

Parameter	Example Value	Description
Report Name	**Security situation report - Daily report**	Name you specify for the security report.
Schedule	**Daily**	Select the schedule of the security situation report.
Data Scope	--	This field displays the data scope based on **Schedule** you specified. No manual actions are required.
Report Schedule	--	Set the time when you want SecMaster to send the security report. For daily reports, the security data from 00:00:00 to 23:59:59 on the previous day will be sent by default.
Email Subject	**SecMaster Security Situation Daily Report**	Set the subject of the email for sending the report.

Parameter	Example Value	Description
Recipient Email	**test01@example.com**	Add the email address of each recipient. ● You can add up to 100 email addresses. ● Separate multiple email addresses with semicolons (;). Example: test01@example.com;test02@example.com
(Optional) Copy To	**test03@example.com**	Add the email address of each recipient you want to copy the report to. ● You can add up to 100 email addresses. ● Separate multiple email addresses with semicolons (;). Example: test03@example.com;test04@example.com
(Optional) Remarks	--	Remarks for the security report.

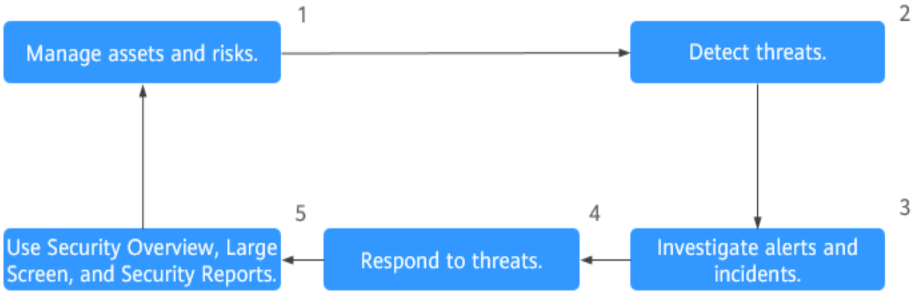
3. Click **Next: Report Choose** in the upper right corner.
4. In the existing report layout area on the left, select a report layout. Then, you can preview the report layout in the right pane.

   In this example, **Daily** is selected.
5. Click **Complete** in the lower right corner. Go back to the **Security Reports** page, view the created security report.

Step 6: Start Security Operations

After the first workspace is created, SecMaster automatically initializes it. After the initialization completes, you can start managing assets, checking for threats, investigating alerts, handling threats, as well as other security operations activities. You can also view the security situation on the situation overview page and large screens.

Figure 3-10 Secure operations


1
Manage assets and risks.
2
Detect threats.
3
Investigate alerts and incidents.
4
Respond to threats.
5
Use Security Overview, Large Screen, and Security Reports.

1. Managing 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, 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 enable cross-region, cross-account, and cross-environment aggregation of assets. For assets from other environments, SecMaster will mark the environments these assets belong to. After the aggregation, 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. This makes it possible for you to view security of all your assets in one place.

     For details, see **Managing Assets**.

   – **Detecting and clearing unsafe settings**

     During security operations, the most common vulnerabilities are 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 role 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. You can use SecMaster to centrally manage Linux, Windows, Web-CMS, application, and website vulnerabilities. You will have an overview of vulnerabilities in real time, including vulnerability scan details, vulnerability statistics, vulnerability types and distribution, top 5 vulnerabilities, and top 5 risky servers.

     For details, see **Vulnerability Management**.

2. Detecting threats

   As we have sorted out the assets we need to protect and fixed unsafe settings and vulnerabilities, after data sources are connected to SecMaster, the next move is to identify suspicious activities and threats.

   SecMaster provides many preconfigured threat detection models. These models were designed by security experts and analysis teams based on known threats, common attack media, and suspicious activities. You will receive notifications once suspicious activities trigger those models. These models automatically search the entire environment for suspicious activities. You can also create custom threat detection models to meet your needs.

   SecMaster also provides the log data query function to help you discover threats.

   For details, see **Managing Model Templates** and **Security Analysis**.

3. Investigating alerts and incidents
   - **Investigating alerts**

     Threat detection models analyze 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 activities, and compromised assets. Security operations engineers need to analyze and investigate alerts to find out real threats. 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 into an incident.

     For more details, see **Viewing Alerts** and **Converting an Alert into an Incident**.

   - **Investigating incidents**

     After an alert is converted into an incident, you can view incident in the incident management module. You can investigate the incident and take emergency response to it. You can associate an incident with entities related to suspicious activities. The entities include 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**.

4. Responding to threats

   You can use playbooks to enable automated alert and incident responses.

   For details, see **Security Orchestration**.

5. Use **Security Overview**, **Large Screen**, and **Security Reports**.
   - **Security Overview**

     This page displays the security scores of resources in the current workspace, so you can quickly learn about the security status.

   - **Large Screen**

     You can view the real-time situation of resources and handle attack incidents. This function helps security operations teams monitor and analyze security threats and incidents in real time and quickly respond to them.

   - **Security reports**

     Security reports are sent by SecMaster automatically. You will see security scores, baseline check results, security vulnerabilities, and policy coverage in a security report. This helps you learn about asset security status in a timely manner.

   For more details, see **Situation Overview**, **Large Screen**, and **Security Reports**.

4 Getting Started Through 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 4-1 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.
Aggregating Log Data from a Non-Huawei Cloud System or Product to SecMaster or Transferring Security Logs from SecMaster to a Third-Party System or Product	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.