SecMaster

Service Overview

Issue 06

Date 2024-09-26

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 What Is SecMaster?

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

Why SecMaster?

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

For more information about the advantages of SecMaster, see **Product Advantages**.

2 What Is a SOC?

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

What a SOC Does

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

- **Asset and tool inventory**

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

- **Reducing attack surface**

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

- **Continuous monitoring**

  A SOC team uses a security analysis solution to monitor the entire environment, covering on-premises, cloud, applications, networks, and devices, all day to detect abnormal or suspicious behavior. The solution can be

a security information enterprise management (SIEM), security orchestration, automation, and response (SOAR), and extended detection and response (XDR) solution. These tools collect telemetry data, aggregate the data, and, in some cases, automate incident responses.

- **Threat intelligence**

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

- **Threat detection**

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

- **Log management**

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

- **Incident response**

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

- **Recovery and remediation**

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

- **Root cause investigation**

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

- **Security refinement**

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

- **Compliance management**

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

Key Roles in a SOC

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

- **Incident response director**

  This role, which is typically planned in very large organizations, is responsible for coordinating detection, analysis, containment, and recovery during a security incident. They also manage communication with corresponding stakeholders.

- **SOC manager**

  A SOC manager oversees the SOC. They are responsible for reporting to the Chief Information Security Officer (CISO). Their responsibilities include supervising personnel, running services, training new employees and managing finance.

- **Security engineer**

  Security engineers are responsible for operating of the organization's security system. This includes designing security architectures and researching, implementing, and maintaining security solutions.

- **Security analyst**

  A security analyst is the first responder in a security incident. They are responsible for identifying threats, prioritizing threats, and then taking actions to contain damage. During an online attack, they may need to isolate infected hosts, clients, or users. In some organizations, security analysts are graded based on the security severity of the threats they are responsible for addressing.

- **Threat hunter**

  In some organizations, the most experienced security analysts are called threat hunters. They identify and respond to advanced threats that are not detected by automated tools. This role is proactive and designed to deepen the organization's understanding of known threats and reveal unknown threats before attacks actually occur.

- **Forensics analyst**

  Large organizations may also hire forensic analysts who are responsible for collecting intelligence to determine the root causes of violations. They search for system vulnerabilities, violations against security policies, and cyber attack patterns that may be useful in preventing similar intrusions in the future.

Types of SOCs

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

Importance of a SOC Team

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

Benefits of a SOC

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

- **Strong security situation**

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

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

- **Compliance with privacy laws and regulations**

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

- **Swift incident responses**

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

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

- **Reduced breach costs**

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

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

Best Practices for SOC Teams

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

- **Service-aligned strategy**

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

- **Talented, well-trained employees**

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

- **End-to-end visibility**

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

- **Right tools**

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

SOC Tools and Technologies

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

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

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

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

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

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

- **Firewall**

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

- **Log management**

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

- **Vulnerability management**

  Vulnerability management tools scan the network to help identify any weaknesses that attackers may exploit.

- **User and entity behavior analytics (UEBA)**

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

FAQs

1. What does a SOC team need to do?

   A SOC team monitors servers, devices, databases, network applications, websites, and other systems to detect potential threats in real time. The team performs proactive security efforts. They keep abreast of the latest threats and discover and resolve system or process vulnerabilities before attackers exploit them. If an organization is being attacked, the SOC team is responsible for eradicating the threat and restoring the system and backup as needed.

2. What are the key components in a SOC?

   A SOC consists of people, tools, and processes that help protect the organization from cyber attacks. To achieve its objectives, an SOC performs the following functions: inventory of all assets and security techniques, routine maintenance and preparation, continuous monitoring, threat detection, threat intelligence, log management, incident response, recovery and remediation, root cause investigation, security optimization, and compliance management.

3. Why do organizations need strong SOCs?

   A strong SOC helps organizations manage security more efficiently and effectively through unified defense, threat detection tools, and security processes. Organizations with SOCs can improve their security processes,

respond to threats faster, and better manage compliance than those without SOCs.

4. What are the differences between a SIEM and a SOC?

   A SOC consists of the personnel, processes, and tools responsible for protecting organizations from cyber attacks. A SIEM is one of the many tools used by a SOC to maintain visibility and respond to attacks. A SIEM aggregates logs and uses analytics and automation to reveal credible threats to SOC members who decide how to respond.

3 Product Advantages

Refined Indicators and Intuitive Situation Display

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

Cloud Native Asset Stocktaking and Risk Prevention

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

Intelligent and Efficient Threat Detection, Response, and Handling

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

Environment Integration and Operational Collaboration for Ultimate Flexibility

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

4 Application Scenarios

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

Routine Security Operation

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

Key Incident Assurance

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

Security Drills

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

Security Evaluation

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

5 Functions

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

SecMaster provides basic, standard, and professional editions as well as value-added functions to help meet security requirements in different scenarios.

- Basic edition: helps learn about security posture.
- Standard edition: helps meet operations requirements on security situation and DJCP compliance.
- Professional edition: helps meet requirements on daily operations and regulation compliance.

This topic introduces SecMaster editions and their function differences.

NOTE

- The value-added package provides extra functions like large screen, security analysis, and security orchestration beyond the standard and professional editions. To use such extra functions, the standard or professional edition must be enabled first.
- The following symbols are used in this topic:
  - √: indicates that the function is supported in the corresponding edition.
  - ×: indicates that the function is not supported in the corresponding edition.

Security Overview

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

Table 5-1 Functions

Function Module	Description	Basic	Standard	Professional
Security Overview	• **Security Score**: A security score shows the overall health status of your workloads on the cloud so you can quickly learn of unhandled risks and their threats to your assets. The lower the security score, the greater the overall asset security risk. • **Security Monitoring**: You can view how many threats, vulnerabilities, and compliance violations that are not handled and view their details. • **Security Scores over the Time**: You can view the trend of the asset health scores for the last seven days.	√	√	√

Workspace Management

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

Table 5-2 Functions

Function Module	Description	Basic	Standard	Professional
Workspaces	• Workspace management: Workspaces are top-level workbenches in SecMaster. A single workspace can be bound to projects and regions to support workspace operational modes in different scenarios. • Workspace hosting: You can create an agency and use it to view the asset risks, alerts, and incidents of multiple workspaces across accounts.	√	√	√

Security Governance

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

Table 5-3 Functions

Function Module	Description	Basic	Standard	Professional
Security Governance	• Compliance Pack Huawei's open security governance templates include original standards and regulation terms, check policies, compliance evaluation items, and improvement suggestions from Huawei experts, covering PCI DSS, ISO27701, ISO27001, privacy protection, and other regulations and standards. You can subscribe to and unsubscribe from security compliance packs and view the evaluation results. • Policy Check Security Governance periodically detects the compliance status of cloud assets through code-based scanning. You can view compliance risks on the dashboard, and obtain corresponding improvement suggestions from Huawei experts. • Compliance Evaluation Security Governance integrates regulatory clauses and standard requirements into compliance pack check items. You complete evaluation of your services using the compliance pack, and view evaluation results. You can also view historical results, upload and download evidence, and take actions based on Huawei experts' improvement suggestions. • Result Display	×	×	√

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

Purchased Resources

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

Table 5-4 Functions

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

Security Situation

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

Table 5-5 Functions

Function Module	Description	Basic	Standard	Professional
Situation Overview	• **Security Score**: A security score shows the overall health status of your workloads on the cloud so you can quickly learn of unhandled risks and their threats to your assets. The lower the security score, the greater the overall asset security risk. • **Security Monitoring**: You can view how many threats, vulnerabilities, and compliance violations that are not handled and view their details. • **Security Scores over the Time**: You can view the trend of the asset health scores for the last seven days.	√	√	√
Large Screen	SecMaster leverages AI to analyze and classify massive cloud security data and then displays real-time results on a large screen. In a simple, intuitive, and efficient way, you will learn of what risks your cloud environment are facing and how secure your cloud environment is. **NOTE** The large screen function needs to be purchased separately based on the standard or professional edition.	×	√	√
Security Reports	You can generate analysis reports and periodically send them to specified recipients by email. In this way, all recipients can learn about the security status of your assets in a timely manner.	×	×	√
Task Center	All tasks that need to be processed are displayed centrally.	×	√	√

Resource Manager

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

Table 5-6 Functions

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

Risk Prevention

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

Table 5-7 Functions

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

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

Threat Operations

Threat operation provides various threat detection models to help you detect threats from massive security logs and generate alerts; provides various security response playbooks to help you automatically analyze and handle alerts, and automatically harden security defense and security configurations.

Table 5-8 Functions

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

Function Module	Description	Basic	Standard	Professional
Security Analysis	• **Query and Analysis** – Search and analysis: Supports quick data search and analysis, quick filtering of security data for security survey, and quick locating of key data. – Statistics filtering: SecMaster supports quick analysis and statistics of data fields and quick data filtering based on the analysis result. Time series data supports statistics collection by default time partition, allowing data volume trend to be quickly spotted. SecMaster supports analysis, statistics, and sorting functions, and supports quick building of security analysis models. – Visualization: Visualized data analysis intuitively reflects service structure and trend, enabling customized analysis reports and analysis indicators to be easily created. • **Data Delivery**: Data can be delivered to other pipelines or Huawei Cloud products in real time so that you can store data to or retrieve data from other systems. • **Data Monitoring**: Data streams are monitored and managed in an end-to-end manner. • **Data Consumption**: SecMaster provides streaming communication	×	√	√

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

Security Orchestration

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

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

Table 5-9 Functions

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

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

Data Collection

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

Table 5-10 Functions

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

Data Integration

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

Table 5-11 Functions

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

Directory Customization

You can customize directories as needed.

Table 5-12 Functions

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

Free Quota Description

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

Table 5-13 Free Quota Description

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

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

6 Limitations and Constraints

The following table lists the limitations and constraints on using SecMaster.

Table 6-1 Limitations and constraints

Module	Limitations and Constraints
Billing	• The basic edition does not support the value-added packages. To use functions in the value-added packages, upgrade the basic edition to the standard or professional edition. • Value-added packages cannot be used independently. – To purchase a value-added package, purchase the standard or professional edition first. – If you unsubscribe from the pay-per-use professional edition, the system automatically unsubscribes from the value-added packages. – If you unsubscribe from the yearly/monthly standard or professional edition, you need to manually unsubscribe from the value-added packages you have.
Managed environments	• Edge sites, such as IEC, DeC, and IES, cannot be managed. • Only the default project can be managed. Sub-projects cannot be managed. • Resources cannot be managed by EPS.

Module	Limitations and Constraints
Workspaces	• Paid SecMaster: A maximum of five workspaces can be created for a single account in a single region. • Free SecMaster: Only one workspace can be created for a single account in a single region. • Permanent deletion of workspaces: Workspaces are deleted immediately and cannot be restored. • Workspace agencies: – A maximum of one workspace agency view can be created for an account in a region. – A maximum of 100 workspaces can be managed in a workspace agency view in a region for a single account or across several accounts. – A maximum of 10 workspaces can be managed in a workspace agency view under a single account in a region. – A maximum of 10 agencies can be created under a single account. • Currently, performing operations in different workspaces in multiple windows of the same browser is not supported.
Data Space/ Pipeline	• A maximum of five data spaces can be created in a workspace in a region for a single account. • A maximum of 20 pipelines can be created in a data space in a region for a single account.
Security Reports	A maximum of 10 security reports (including daily, weekly, and monthly reports) can be created in a single workspace of a single account.
Alert Models	• A maximum of 100 alert models can be created in a single workspace under a single account in a single region. • The running interval of an alert model must be greater than or equal to 5 minutes, and the time range for querying data must be less than or equal to 14 days.

Module	Limitations and Constraints
Query and Analysis	• A maximum of 500 results can be returned for a single analysis query. • A maximum of 50 shortcut queries can be created in a pipeline. That is, a maximum of 50 query analysis criteria can be saved as shortcut queries. • If there are over 50,000 results for a single query, the accuracy may decrease. In this case, you can select a short time range or apply more filter criteria to reduce the number of query results. • In aggregation queries (for example, GROUP BY statement) based on several fields, the default number of buckets for the second field is 10. If more than 10 buckets are generated, part of qualified data will be lost. In this case, the query results are not accurate.
Incidents, alerts, indicators, and vulnerabilities	• In a workspace of a single account, a maximum of 100 new alerts, incidents, indicators, or vulnerabilities can be added each day. • In a workspace of a single account, a maximum of 100 alerts can be converted into incidents each day.
Playbooks	• In a single workspace of an account, the scheduling frequency of a single playbook is greater than or equal to 5 minutes.
Playbook and Workflow Instances	The maximum number of retries within a day for a single workspace of a single account is as follows: • Manual retry: 100. After a retry, the playbook cannot be retried until the current execution is complete. • API retry: 100. After a retry, the playbook cannot be retried until the current execution is complete.
Classification & Mapping	• In a single workspace of a single account, a maximum of 50 classification & mapping templates can be created. • In a single workspace of a single account, the proportion of a classification to its mappings is 1:100. • A maximum of 100 classifications and mappings can be added to a workspace of a single account.

7 Security

7.1 Shared Responsibilities

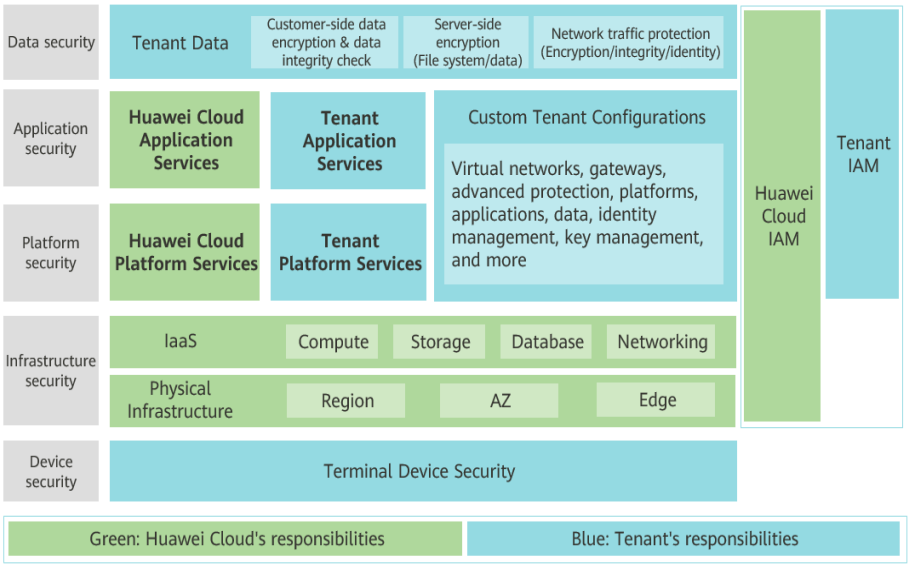
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 7-1 illustrates the responsibilities shared by Huawei Cloud and users.

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

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

Figure 7-1 Huawei Cloud shared security responsibility model



7.2 Identity Authentication and Access Control

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

Identity and Access Management (IAM) is a basic service of Huawei Cloud that provides permissions management to help you securely control access to SecMaster. With IAM, you can add users to a user group and configure policies to control their access to SecMaster resources. You can allow or deny access to a specific SecMaster resource in a fine-grained manner.

7.3 Data Protection Technologies

SecMaster takes different measures to keep data secure and reliable.

Table 7-1 SecMaster data protection methods and features

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

Method	Description
Data integrity verification	1. Data integrity is verified when SecMaster accesses cloud service alerts, vulnerabilities, and baselines. 2. When the SecMaster core data plane process is started, the configuration data enters the reliable mode to ensure data integrity (in scenarios such as network jitter, delay, and configuration data retransmission and retry).
Data isolation mechanism	SecMaster isolates its tenant zone from its management plane. Operation permissions for CFW are isolated by user. Your policies and logs are isolated from those of others.
Data destruction mechanism	To prevent information leakage caused by residual data, Huawei Cloud sets different retention periods based on the customer level. If the customer does not renew the subscription or recharge the account after the retention period expires, the data stored in the cloud service will be deleted and the cloud service resources will be released. SecMaster automatically detects cloud service subscription status and releases resources when the retention period expires.

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

7.4 Audit Logs

- Audit

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

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

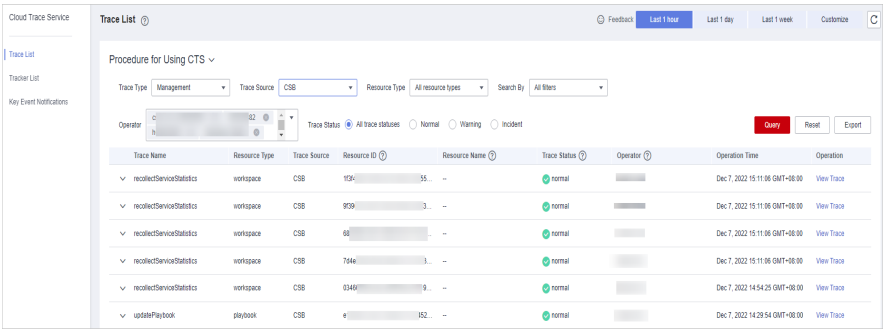
  For details about how to enable and configure CTS, see **Enabling CTS**.

- Logs
  - Querying logs

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

    Figure 7-2 shows how to view CTS logs.

Figure 7-2 Querying logs

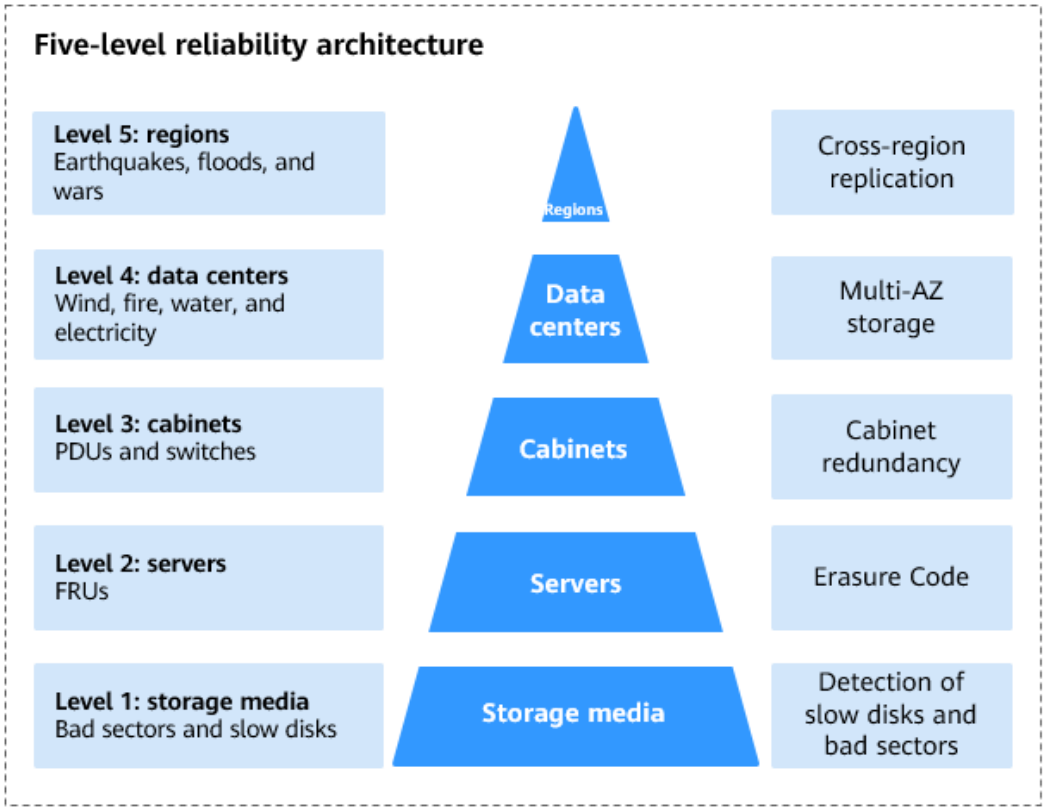


7.5 Service Resilience

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

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

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



7.6 Risk Monitoring

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

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

For details about how to enable and configure CTS, see **Enabling CTS**.

Table 7-2 Risk monitoring

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

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

For details about monitoring alerts, see:

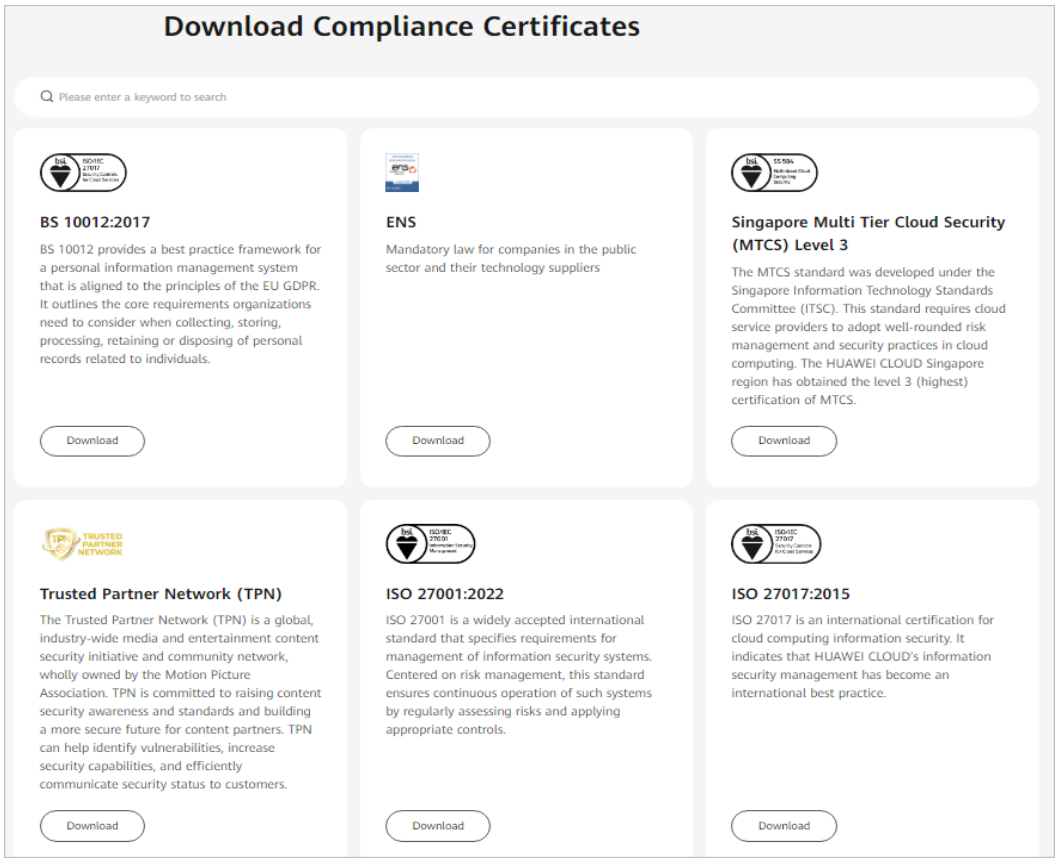
- **Vulnerability Management**
- **Cloud Service Baseline Overview**
- **Security Report**

7.7 Certificates

Compliance Certificates

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

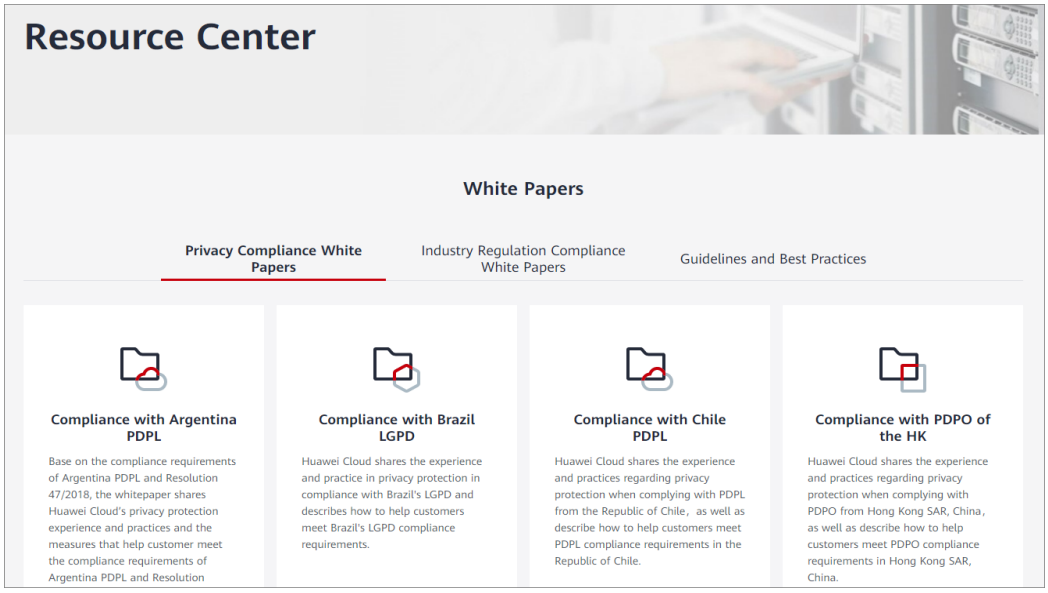
Figure 7-3 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 7-4 Resource center



7.8 Security Orchestration

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

- Playbook management: you can use the built-in automatic response playbooks or customize playbooks.

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

For details about how to configure Security Orchestration, see **Security Orchestration**.

8 Permissions Management

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

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

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

IAM is free. You pay only for the resources in your account. For more information about IAM, see **IAM Service Overview**.

SecMaster Permissions

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

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

You can grant users permissions by using roles and policies.

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

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

Table 8-1 lists all SecMaster system permissions.

Table 8-1 System-defined permissions supported by SecMaster

Policy Name	Description	Type	Dependency
SecMaster FullAccess	All permissions of SecMaster.	System-defined policy	None
SecMaster ReadOnlyAccess	SecMaster read-only permission. Users granted with these permissions can only view SecMaster data but cannot configure SecMaster.	System-defined policy	None

SecMaster FullAccess Policy

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "secmaster:*:*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:vpcs:list",
                "vpc:subnets:get",
                "vpcep:endpoints:*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "obs:bucket:ListBucketVersions"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:permissions:checkRoleForAgencyOnDomain",
                "iam:permissions:checkRoleForAgencyOnProject",
                "iam:permissions:checkRoleForAgency",
                "iam:permissions:grantRoleToAgency",
                "iam:permissions:grantRoleToAgencyOnDomain",
                "iam:permissions:grantRoleToAgencyOnProject",
                "iam:policies:*",
                "iam:agencies:*",
                "iam:roles:*",
                "iam:users:listUsers",
```



```
            "iam:tokens:assume"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "organizations:organizations:get",
            "organizations:delegatedAdministrators:list",
            "organizations:roots:list",
            "organizations:ous:list",
            "organizations:accounts:list"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "ecs:cloudServers:list"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "sts:agencies:assume"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "lts:log*:list*"
        ],
        "Effect": "Allow"
    }
  ]
}
```

SecMaster ReadOnlyAccess Policy

```
{
  "Version": "1.1",
  "Statement": [
    {
        "Action": [
            "secmaster:*:get*",
            "secmaster:*:list*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "vpc:vpcs:list",
            "vpc:subnets:get",
            "vpcep:endpoints:get",
            "vpcep:endpoints:list"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "obs:bucket:ListBucketVersions"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "iam:permissions:checkRoleForAgencyOnDomain",
            "iam:permissions:checkRoleForAgencyOnProject",
            "iam:permissions:checkRoleForAgency",
            "iam:policies:get*",
            "iam:policies:list*",
```

```
            "iam:agencies:get*",
            "iam:agencies:list*",
            "iam:roles:get*",
            "iam:roles:list*",
            "iam:users:listUsers"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "organizations:organizations:get",
            "organizations:delegatedAdministrators:list",
            "organizations:roots:list",
            "organizations:ous:list",
            "organizations:accounts:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "ecs:cloudServers:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "lts:log*:list*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

9 SecMaster and Other Services

This topic describes SecMaster and its linked services.

Security Services

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

Elastic Cloud Server (ECS)

SecMaster detects threats to your **ECSs** with linked service HSS, comprehensively displays ECS security risks, and provides protection suggestions.

Cloud Trace Service (CTS)

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

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

Cloud Eye

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

TMS

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

Table 9-1 SecMaster operations supported by TMS

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

Enterprise Management

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

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

10 Basic Concepts

This topic describes concepts used in SecMaster.

Security Risk

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

Threat Alert

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

Workspace

Workspaces are the root of SecMaster resources. A single workspace can be bound to common projects, enterprise projects, and regions for different application scenarios.

Data Space

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

Data Pipelines

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

Classification and Mapping

Type matching and field mapping for cloud service alarms.

Security Orchestration

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

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

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

Producer

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

Subscriber

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

Consumer

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

Message Queue

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

Threat Detection Model

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

